Uradni list
Evropske unije

SL
Serija L

2026/1731

22.7.2026

IZVEDBENA UREDBA KOMISIJE (EU) 2026/1731

z dne 15. julija 2026

o spremembi izvedbenih uredb (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 in (EU) 2024/2982 glede veljavnih standardov in specifikacij

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES ([1]) ter zlasti člena 5a(23) Uredbe,

ob upoštevanju naslednjega:

(1) Za zagotovitev najvišje ravni harmonizacije med državami članicami za razvoj evropskih denarnic za digitalno identiteto se tehnične specifikacije za denarnice opirajo na delo, opravljeno na podlagi Priporočila Komisije (EU) 2021/946 ([2]) ter zlasti arhitekturnega in referenčnega okvira. Ker sta se arhitekturni in referenčni okvir od sprejetja izvedbenih uredb Komisije (EU) 2024/2977 ([3]), (EU) 2024/2979 ([4]), (EU) 2024/2980 ([5]) in (EU) 2024/2982 ([6]) znatno razvila, bi bilo treba navedene izvedbene uredbe zdaj spremeniti, da se uskladijo z novimi standardi, specifikacijami in postopki.

V skladu s cilji Uredbe (EU) št. 910/2014 je bilo za izpolnitev teh posebnih zahtev izbranih več standardov. Ti standardi bi morali odražati ustaljene prakse in biti splošno priznani v ustreznih sektorjih. Na primer, ker se oblika W3C VCDM uporablja kot referenčna oblika za potrdila zlasti v izobraževalnem sektorju, bi morale evropske denarnice za digitalno identiteto to obliko podpirati tudi, ko bodo na voljo novi profili za obliko W3C VCDM. Po potrebi bi jih bilo treba prilagoditi ali dopolniti, da se zagotovita varnost in zanesljivost evropskih denarnic za digitalno identiteto, hkrati pa spodbudita čezmejna interoperabilnost in učinkovito delovanje notranjega trga.

(2) Rešitve denarnice morajo pri vsaki uporabi denarnice, pri kateri se zahteva predložitev fotografije uporabnika denarnice, podpirati funkcionalnost selektivnega razkritja, razkritje pa mora biti v celoti pod nadzorom uporabnika. Da bi zaščitili možnost odločanja o razkritju in fotografijo pred nenamerno ali nepooblaščeno zahtevo za razkritje, bi morala arhitekturna zasnova evropskih denarnic za digitalno identiteto določati mehanizme opozarjanja in beleženje vseh transakcij, povezanih z uporabo fotografije. Za zagotovitev seznanjenosti uporabnika denarnice z izmenjavo biometričnih podatkov bi bilo treba v opozorilih navesti, da zahteva vključuje deljenje biometričnih podatkov, in

([1]) UL L 257, 28.8.2014, str. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Priporočilo Komisije (EU) 2021/946 z dne 3. junija 2021 o skupnem unijskem naboru orodij za usklajen pristop k okviru za evropsko digitalno identiteto (UL L 210, 14.6.2021, str. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([3]) Izvedbena uredba Komisije (EU) 2024/2977 z dne 28. novembra 2024 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede identifikacijskih podatkov osebe in elektronskih potrdil o atributih, izdanih evropskim denarnicam za digitalno identiteto (UL L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).
([4]) Izvedbena uredba Komisije (EU) 2024/2979 z dne 28. novembra 2024 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede celovitosti in temeljnih funkcionalnosti evropskih denarnic za digitalno identiteto (UL L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).
([5]) Izvedbena uredba Komisije (EU) 2024/2980 z dne 28. novembra 2024 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede priglasitev Komisiji v zvezi z ekosistemom evropske denarnice za digitalno identiteto (UL L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).
([6]) Izvedbena uredba Komisije (EU) 2024/2982 z dne 28. novembra 2024 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede protokolov in vmesnikov, ki jih mora podpirati okvir za evropsko digitalno identiteto (UL L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

izrecno zahtevati, da uporabnik potrdi razkritje. Kadar zanašajoča se stranka obdeluje fotografijo za namene edinstvene identifikacije fizične osebe ali za potrditev njene zatrjevane identitete, se uporabljata člena 6 in 9 Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta ([7]) ter vse druge zahteve iz navedene uredbe, vključno s tem, da bi morala biti obdelava fotografije s strani zanašajočih se strank omejena na to, kar je potrebno za predvideno uporabo. Predvidena uporaba bi se morala uporabniku denarnice sporočiti skupaj z zahtevo za razkritje v jasnem in razumljivem jeziku. Da bi se ustrezno upoštevala občutljivost biometričnih podatkov, bi moral uporabnik denarnice izrecno in specifično potrditi razkritje fotografije. Neodziv ali vnaprej označena okenca se ne bi smela šteti za potrditev uporabnika denarnice. Izrecna potrditev uporabnika denarnice bi morala biti tehnični zaščitni ukrep in sama po sebi ne bi smela biti pravna podlaga za obdelavo. V skladu s členom 9(4) Uredbe (EU) 2016/679 lahko države članice ohranijo ali uvedejo dodatne pogoje, tudi omejitve, glede obdelave genetskih, biometričnih podatkov ali podatkov v zvezi z zdravjem.

(3) Da bi države članice imele dovolj časa za prilagoditev svojih nacionalnih postopkov, je lahko fotografija uporabnika denarnice del obveznih identifikacijskih podatkov fizične osebe šele od 11. avgusta 2028. Kadar se te podobe pridobijo iz obstoječih osebnih dokumentov, kot so osebne izkaznice ali potni listi, se uporabljajo ustrezne zahteve iz uredb Sveta (EU) 2025/1208 ([8]) oziroma (ES) št. 2252/2004 ([9]).

(4) V skladu z Uredbo (EU) št. 910/2014 je treba omogočiti, da se z denarnicami prikaže znak zaupanja za evropsko denarnico za digitalno identiteto, tj. preverljiva, preprosta in prepoznavna navedba, da je denarnica zagotovljena v skladu z Uredbo. Z uporabo takega znaka zaupanja se bo podprlo učinkovito delovanje notranjega trga, zagotovila lojalna konkurenca in zaščitili interesi potrošnikov. Da bi se omogočila uporaba takega znaka zaupanja, bi bilo treba določiti njegove vizualne in tehnične značilnosti.

(5) Kot je določeno v členu 12b Uredbe (EU) št. 910/2014, vratarji ponudnikom evropskih denarnic za digitalno identiteto in izdajateljem priglašenih sredstev elektronske identifikacije za namene interoperabilnosti omogočijo učinkovito interoperabilnost z istimi funkcijami operacijskega sistema ter strojne opreme ali programske opreme in dostop do njih. Taka učinkovita interoperabilnost in dostop se zagotovita brezplačno in ne glede na to, ali so te funkcije strojne ali programske opreme del operacijskega sistema, ki so navedenemu vratarju na voljo ali jih ta uporablja pri zagotavljanju takih storitev. Ker bi morale vse rešitve denarnic podpirati skupen nabor protokolov in vmesnikov, da se zagotovijo uporabnost, varnost in interoperabilnost med državami članicami, bi morali vratarji omogočiti funkcije operacijskega sistema, strojne opreme ali programske opreme, potrebne za izvajanje protokolov in vmesnikov iz Priloge XII k tej uredbi. V zvezi s tem bi morali vratarji pri spletnih tokovih med napravami tako za fizično preverjanje bližine kot prenos podatkov med obema napravama dati prednost lokalnemu komunikacijskemu kanalu, kot ga omogoča različica 2.3 specifikacije protokola odjemalca do avtentikatorja (CTAP) ([10]), pred uporabo storitev hibridnega predora CTAP.

(6) Da bi imele države članice, ponudniki potrdil o registraciji na denarnice zanašajočih se strank in ponudniki denarnic dovolj časa, da enotam denarnic omogočijo avtentikacijo in potrjevanje potrdil o registraciji na denarnice zanašajočih se strank, bi se morala ta zahteva uporabljati šele od 11. avgusta 2028.

(7) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta ter, kadar je ustrezno, Direktiva 2002/58/ES Evropskega parlamenta in Sveta ([11]) se uporabljata za vse dejavnosti obdelave osebnih podatkov na podlagi te uredbe.

([7]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Uredba Sveta (EU) 2025/1208 z dne 12. junija 2025 o okrepitvi varnosti osebnih izkaznic državljanov Unije in dokumentov za prebivanje, izdanih državljanom Unije in njihovim družinskim članom, ki uresničujejo svojo pravico do prostega gibanja (UL L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Uredba Sveta (ES) št. 2252/2004 z dne 13. decembra 2004 o standardih za varnostne značilnosti in biometrične podatke v potnih listih in potovalnih dokumentih, ki jih izdajo države članice (UL L 385, 29.12.2004, str. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Predlagani standard FIDO Alliance, *Client to Authenticator Protocol (CTAP)* (protokol odjemalca do avtentikatorja (CTAP), 26. februar 2026.

([11]) Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([12]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 17. aprila 2026 ([13]).

(9) Ukrepi iz te uredbe so v skladu z mnenjem odbora, ustanovljenega s členom 48 Uredbe (EU) št. 910/2014 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Spremembe Izvedbene uredbe (EU) 2024/2977

Izvedbena uredba (EU) 2024/2977 se spremeni:

(1) vstavi se naslednji člen 3a:

„*Člen 3a*

Varstvo fotografije

1. Poleg zahtev glede informacij v skladu z Uredbo (EU) 2016/679 ponudniki denarnic zagotovijo, da rešitve denarnic, ki jih zagotavljajo, uporabnikom denarnic izdajo opozorila, kadar na denarnice zanašajoče se stranke zahtevajo razkritje fotografije, pri čemer opozorila navajajo, da je v zahtevi vključeno deljenje biometričnih podatkov in da se zahteva potrditev selektivnega razkritja fotografije.

2. Za izvajanje selektivnega razkritja fotografije na denarnice zanašajoči se stranki ponudniki denarnic zagotovijo, da rešitve denarnice od uporabnika denarnice zahtevajo, da izrecno in specifično potrdi predložitev fotografije.

3. Na denarnice zanašajoče se stranke fotografije ne hranijo, razen če je njena obdelava potrebna za namene ugotavljanja identitete in avtentikacije v skladu s pravom Unije o varstvu podatkov ali kadar je to določeno s pravom Unije ali nacionalnim pravom, v skladu s pravom Unije o varstvu podatkov. Fotografija se ne posreduje tretjim državam ali mednarodnim organizacijam, razen če je to dovoljeno s pravom Unije o varstvu podatkov.“;

(2) v členu 4 se odstavek 1 nadomesti z naslednjim:

„1. Elektronska potrdila o atributih, izdana enotam denarnice, izpolnjujejo najmanj enega od standardov iz Priloge II k Izvedbeni uredbi (EU) 2024/2979.“;

(3) v členu 5, odstavek 4, se točka (b) nadomesti z naslednjim:

„(b) kadar je bilo potrdilo o enoti denarnice za enoto denarnice, ki so ji bili izdani identifikacijski podatki osebe, preklicano;“;

(4) Priloga se nadomesti z besedilom iz Priloge I k tej uredbi.

([12]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) Uradne pripombe ENVP k osnutku Izvedbene uredbe v zvezi z veljavnimi standardi in specifikacijami ter popravkom Izvedbene uredbe (EU) 2024/2980 | Evropski nadzornik za varstvo podatkov.

Člen 2

Spremembe Izvedbene uredbe (EU) 2024/2979

Izvedbena uredba (EU) 2024/2979 se spremeni:

(1) v členu 3 se črta odstavek 2;

(2) v členu 5, odstavek 1, se točka (a) nadomesti z naslednjim:

„(a) izvajajo kriptografske operacije denarnice, ki vključujejo kritična sredstva, ki so shranjena v varni kriptografski napravi denarnice in niso potrebna za avtentikacijo uporabnika denarnice, samo v primerih, ko so te aplikacije uspešno avtenticirale uporabnike denarnice;“;

(3) vstavi se naslednji člen 5a:

„*Člen 5a*

Kriptografski mehanizmi

Ponudniki denarnic za namene člena 4(2) uporabljajo le kriptografske mehanizme iz Priloge Ia.“;

(4) člen 6 se spremeni:

(a) odstavek 1 se nadomesti z naslednjim:

„1. Ponudniki denarnic za vsako enoto denarnice izdajo potrdila o enoti denarnice. Ponudniki denarnic potrdila o enoti denarnice podpišejo ali ožigosajo tako, da je veljavnost podpisov ali žigov mogoče preveriti s certifikatom, uvrščenim na seznam v skladu z oddelkom 2, točka (1)(h), Priloge II k Izvedbeni uredbi (EU) 2024/2980.“;

(b) odstavek 2 se nadomesti z naslednjim:

„2. Ponudniki denarnic zagotovijo, da so potrdila o enoti denarnice iz odstavka 1 skladna s tehničnimi specifikacijami iz Priloge Ib.“;

(c) v odstavku 3 se točka (b) nadomesti z naslednjim:

„(b) zagotovijo mehanizme za varno identifikacijo in avtentikacijo uporabnikov denarnic, ki so neodvisni od enot denarnice“;

(5) v členu 9(2) se točka (b) nadomesti z naslednjim:

„(b) naziv, kontaktne podatke in edinstveno identifikacijsko oznako ustrezne na denarnice zanašajoče se stranke, ter državo članico, v kateri ima sedež;“;

(6) v členu 10 se odstavek 1 nadomesti z naslednjim:

„1. Ponudniki denarnic zagotovijo, da lahko enote denarnice, ki jih zagotavljajo, obdelajo elektronska potrdila o atributih, izdana v skladu s tehničnimi specifikacijami, ki se uporabljajo za skupne vgrajene politike razkrivanja iz Priloge III.“;

(7) člen 12 se spremeni:

(a) v odstavku 2 se točka (c) nadomesti z naslednjim:

„(c) ustvarjanje podpisov ali žigov vsaj v obvezni obliki podpisa ali žiga iz Priloge IV;“;

(b) odstavek 3 se nadomesti z naslednjim:

„3. Aplikacije za ustvarjanje podpisa so lahko vgrajene v instance denarnice ali zunanje.“;

(c) vstavi se naslednji odstavek:

„4. Aplikacije za ustvarjanje podpisa, ki jih uporabljajo enote denarnice, podpirajo vsaj vmesnik za aplikacijsko programiranje iz Priloge IV.“;

(8) v členu 14 se odstavek 1 črta;

(9) vstavi se naslednji člen 14a:

„Člen 14a

Znak zaupanja za evropsko denarnico za digitalno identiteto

1. Ponudniki denarnic zagotovijo, da je na enotah denarnice prikazan znak zaupanja za evropsko denarnico za digitalno identiteto. Znak zaupanja za evropsko denarnico za digitalno identiteto je v obliki, ki je določena v prilogah VI in VII.

2. Ponudniki denarnic zagotovijo, da enote denarnice uporabnikom denarnice omogočajo dostop do informacij, na podlagi katerih lahko preverijo status certificiranja rešitve denarnice. V ta namen ponudniki denarnic zagotovijo, da ustrezne enote denarnice po registraciji rešitve denarnice vsebujejo naslove URL, ki jih za tako preverjanje zagotovi Evropska komisija. Ponudniki denarnic zagotovijo, da imajo njihove enote denarnice dostop do podatkov o znaku zaupanja za evropsko denarnico za digitalno identiteto, ki so v skladu s tehničnimi specifikacijami iz Priloge VIII.

3. Referenčne barve za znak zaupanja za evropsko denarnico za digitalno identiteto so Pantone št. 661 in 116 ali modra (100 % cianova + 67 % škrlatna + 0 % rumena + 40 % črna) in rumena (0 % cianova + 20 % škrlatna + 100 % rumena * 0 % črna), kadar se uporablja štiribarvni tisk; kadar se uporabljajo barve RGB, sta referenčni barvi modra (0 rdeča + 51 zelena + 153 modra) in rumena (255 rdeča + 204 zelena + 0 modra).

4. Znak zaupanja za evropsko denarnico za digitalno identiteto se v črno-beli različici, kot je določena v Prilogi VII, lahko uporablja le v primerih, ko uporaba barv ni praktično izvedljiva.

5. Kadar se znak zaupanja za evropsko denarnico za digitalno identiteto uporablja na temnem ozadju, se lahko uporabi v negativu z uporabo iste barve ozadja. Kadar se znak zaupanja za evropsko denarnico za digitalno identiteto uporablja v barvah na barvnem ozadju, zaradi česar je težko viden, se lahko okrog znaka uporabi razmejevalni rob, da se izboljša kontrast z barvnim ozadjem.

6. Znak zaupanja za evropsko denarnico za digitalno identiteto ni manjši od 64 × 85 slikovnih pik pri ločljivosti 150 dpi.

7. Ponudniki denarnic zagotovijo, da se znak zaupanja za evropsko denarnico za digitalno identiteto uporablja tako, da omogoča jasno označitev enote denarnice, na katero se ta znak nanaša. Znak zaupanja za evropsko denarnico za digitalno identiteto se lahko združuje z grafičnimi ali besedilnimi elementi, iz katerih je jasno razvidna enota denarnice, za katero se uporablja, če se z njimi ne spremeni njegova prepoznavnost kot znaka zaupanja za evropsko denarnico za digitalno identiteto niti povezava s seznamom certificiranih evropskih denarnic za digitalno identiteto iz člena 5d Uredbe (EU) št. 910/2014.

8. Kadar ponudniki denarnic prekličejo potrdilo o enoti denarnice, zagotovijo, da na zadevni enoti denarnice ni več prikazan znak zaupanja za evropsko denarnico za digitalno identiteto.“;

(10) Prilogi Ia in Ib se dodata, kot je določeno v Prilogi II in Prilogi III k tej uredbi;

(11) Priloga II se nadomesti s Prilogo IV k tej uredbi;

(12) Priloga III se nadomesti s Prilogo V k tej uredbi;

(13) Priloga IV se spremeni v skladu s Prilogo VI k tej uredbi;

(14) Priloga V se črta;

(15) besedilo iz Priloge VII k tej uredbi se vstavi kot Priloga VI;

(16) besedilo iz Priloge VIII k tej uredbi se vstavi kot Priloga VII;

(17) besedilo iz Priloge IX k tej uredbi se vstavi kot Priloga VIII.

Člen 3

Spremembe Izvedbene uredbe (EU) 2024/2980

Izvedbena uredba (EU) 2024/2980 se spremeni:

1. v členu 5 se odstavek 2 nadomesti z naslednjim:

„2. Kadar je ustrezno, Komisija pripravi, vzdržuje in objavi seznam, na katerem so zbrane priglašene informacije države članice o ponudnikih denarnic, ponudnikih identifikacijskih podatkov osebe, ponudnikih potrdil o dostopu za na denarnice zanašajoče se stranke in ponudnikih potrdil o registraciji za na denarnice zanašajoče se stranke, kot je navedeno v oddelkih 2, 3, 4 in 5 Priloge II.“;

2. Priloga II k Izvedbeni uredbi (EU) 2024/2980 se spremeni, kot je določeno v Prilogi X k tej uredbi.

Člen 4

Spremembe Izvedbene uredbe (EU) 2024/2982

Izvedbena uredba (EU) 2024/2982 se spremeni:

(1) v členu 1 se odstavek 2 nadomesti z naslednjim:

„(2) predložitev atributov identifikacijskih podatkov osebe in elektronskih potrdil o atributih na denarnice zanašajočim se strankam;“;

(2) člen 3 se spremeni:

(a) odstavek 1 se nadomesti z naslednjim:

„(1) avtenticirajo in potrdijo potrdila o dostopu za na denarnice zanašajoče se stranke ob interakciji z njimi, ne da bi se izvajanje teh postopkov preneslo na brskalnik operacijskega sistema ali drugo posredniško aplikacijo;“;

(b) odstavek 2 se črta;

(c) odstavek 3 se nadomesti z naslednjim:

„(3) avtenticirajo in potrdijo zahtevke, vložene z uporabo potrdil o dostopu za na denarnice zanašajoče se stranke;“;

(d) odstavek 4 se nadomesti z naslednjim:

„(4) avtenticirajo in potrdijo potrdilo o registraciji na denarnice zanašajoče stranke;“;

(e) odstavek 5 se nadomesti z naslednjim:

„(5) uporabnikom denarnic prikažejo informacije iz potrdil o dostopu za na denarnice zanašajoče se stranke;“;

(f) odstavek 8 se črta;

(g) odstavek 9 se nadomesti z naslednjim:

„(9) na denarnice zanašajočim se strankam ne predložijo zahtevanih atributov, dokler ni izpolnjeno naslednje:

(a) potrditev, da so bile v enoti denarnice obdelane vgrajene politike razkrivanja v skladu s členom 10 Izvedbene uredbe (EU) 2024/2979;

(b) potrditev, da so uporabniki denarnice delno ali v celoti odobrili predstavitev.“;

(3) v členu 4 se odstavek 1 nadomesti z naslednjim:

„1. Ponudniki denarnic zagotovijo, da rešitve denarnic podpirajo protokole in vmesnike iz Priloge I za izdajanje identifikacijskih podatkov osebe in elektronskih potrdil o atributih enotam denarnic.“;

(4) člen 5 se spremeni:

(a) odstavka 1 in 2 se nadomestita z naslednjim:

„1. Ponudniki denarnic zagotovijo, da rešitve denarnic podpirajo protokole in vmesnike za predstavitev atributov na denarnice zanašajočim se strankam na daljavo in, kadar je primerno, v bližini, v skladu s tehničnimi specifikacijami iz Priloge II.

2. Ponudniki denarnic zagotovijo, da enote denarnice na zahtevo uporabnikov odgovorijo na uspešno avtenticirane in potrjene zahteve na denarnice zanašajočih se strank iz člena 3 v skladu s tehničnimi specifikacijami iz Priloge II.“;

(b) odstavek 5 se črta.

(5) člen 8 se nadomesti z naslednjim:

„*Člen 8*

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Člen 3(4) se uporablja od 11. avgusta 2028.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.“;

(6) Priloga se črta;

(7) besedilo iz Priloge XI k tej uredbi se doda kot Priloga I;

(8) besedilo iz Priloge XII k tej uredbi se doda kot Priloga II.

Člen 5

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 15. julija 2026

Za Komisijo
predsednica
Ursula VON DER LEYEN

PRILOGA I

„PRILOGA

Tehnične specifikacije za identifikacijske podatke osebe iz člena 3(3)

1. Oddelek 1: Nabor identifikacijskih podatkov fizične osebe

Preglednica 1

Obvezni identifikacijski podatki fizične osebe za selektivno razkritje

Identifikator podatkov	Opredelitev
`family_name`	Sedanji priimki uporabnika, na katerega se nanašajo identifikacijski podatki osebe.
`given_name`	Sedanja imena, vključno z morebitnimi srednjimi imeni, uporabnika, na katerega se nanašajo identifikacijski podatki osebe.
`birth_date`	Dan, mesec in leto rojstva uporabnika, na katerega se nanašajo identifikacijski podatki osebe.
`birth_place`	Država v obliki kode države alpha-2, kot je določena v standardu ISO 3166-1, zvezna država, pokrajina, okrožje, lokalno območje, občina, mesto, naselje ali vas rojstva uporabnika, na katerega se nanašajo identifikacijski podatki osebe.
`nationality`	Ena ali več kod držav alpha-2, kot so določene v standardu ISO 3166-1, ki predstavljajo državljanstvo uporabnika, na katerega se nanašajo identifikacijski podatki osebe.
`portrait`	Podoba obraza uporabnika, na katerega se nanašajo identifikacijski podatki osebe, ki izpolnjuje zahteve glede kakovosti za tip slike s celotno frontalno podobo, kot je določena v standardu ISO/IEC 39794-5 ali, zaradi povratne združljivosti, v določbah 8.2, 8.3 in 8.4 standarda ISO/IEC 19794-5, zagotovljena kot kodirani podatki o sliki brez glav ali blokov, kot so določeni v določbi 5 standarda ISO/IEC 19794-5, razen samih podatkov o sliki (JPEG), uporablja od 11. avgusta 2028, razen če uporabnik to izrecno zavrne, če je ustrezno.

— Države članice lahko določijo, da ima uporabnik možnost zavrniti vstavitev fotografije k identifikacijskim podatkom osebe.

— Države članice zagotovijo, da se selektivno razkritje uporablja za vsak identifikator podatkov, vključno s fotografijo.

— Kadar datum rojstva fizične osebe ni znan, države članice izberejo ustrezne vrednosti, ki so skladne s specifikacijami iz oddelka 4.1 ali 4.2 te priloge, kakor je ustrezno.

— Kadar državljanstvo fizične osebe ni znano, države članice uporabijo vrednost ‚QU‘.

— Kadar fizična oseba nima državljanstva, države članice uporabijo vrednost ‚QS‘.

— Če uporabnik zavrne vključitev fotografije, države članice to vrednost nastavijo na ‚empty‘.

Preglednica 2

Neobvezni identifikacijski podatki fizične osebe za selektivno razkritje

Identifikator podatkov	Opredelitev
`resident_address`	Polni naslov sedanjega prebivališča ali kontaktni naslov uporabnika, na katerega se nanašajo identifikacijski podatki osebe (ulica, hišna številka, kraj itd.).
`resident_country`	Država sedanjega prebivališča uporabnika, na katerega se nanašajo identifikacijski podatki osebe, v obliki kode države alpha-2, kot je določena v standardu ISO 3166-1.
`resident_state`	Zvezna država, pokrajina, okrožje ali lokalno območje sedanjega prebivališča uporabnika, na katerega se nanašajo identifikacijski podatki osebe.
`resident_city`	Občina, mesto, naselje ali vas sedanjega prebivališča uporabnika, na katerega se nanašajo identifikacijski podatki osebe.
`resident_postal_code`	Poštna številka sedanjega prebivališča uporabnika, na katerega se nanašajo identifikacijski podatki osebe.
`resident_street`	Ulica sedanjega prebivališča uporabnika, na katerega se nanašajo identifikacijski podatki osebe, vključno s hišno številko in morebitnimi dodatnimi oznakami ali priponami.
`personal_administrative_-number`	Vrednost, dodeljena uporabniku, na katerega se nanašajo identifikacijski podatki osebe, ki je edinstvena med vsemi osebnimi upravnimi številkami, ki jih izda ponudnik identifikacijskih podatkov osebe. Kadar se države članice odločijo za vključitev tega atributa, v svojih shemah elektronske identifikacije, v okviru katerih se izdajo identifikacijski podatki osebe, opišejo politiko, ki jo uporabljajo za vrednosti tega atributa, vključno s posebnimi pogoji za obdelavo te vrednosti, kadar je to ustrezno.
`family_name_birth`	Rojstni priimki uporabnika, na katerega se nanašajo identifikacijski podatki osebe.
`given_name_birth`	Rojstna imena, vključno s srednjimi imeni, uporabnika, na katerega se nanašajo identifikacijski podatki osebe.
`sex`	Vrednost je ena od naslednjih: 0 = ni znano; 1 = moški; 2 = ženska; 3 = drugo; 4 = interspolna oseba; 5 = raznoliko; 6 = odprto; 9 = ni relevantno; pri čemer se za vrednosti 0, 1, 2 in 9 uporablja standard ISO/IEC 5218.
`email_address`	Elektronski naslov uporabnika, na katerega se nanašajo identifikacijski podatki osebe [v skladu s standardom RFC 5322 ([1])].

Identifikator podatkov	Opredelitev
`mobile_phone_number`	Številka mobilnega telefona uporabnika, na katerega se nanašajo identifikacijski podatki osebe, ki se začne s simbolom „+ , kot mednarodno predpono in kodo države, ki ji sledijo samo številke.

([1]) Resnick, P. (ur.), Internet Message Format (Oblika internetnega sporočila), RFC 5322, oktober 2008.

2. Oddelek 2: Nabor identifikacijskih podatkov pravne osebe

Preglednica 3

Obvezni identifikacijski podatki pravne osebe

Identifikator podatkov
Trenutno pravno ime
Edinstveni identifikator, ki ga je ustvarila država članica pošiljateljica v skladu s tehničnimi specifikacijami za namene čezmejne identifikacije in je časovno čim bolj obstojen.

— Kadar identifikator podatkov za osebo ni znan ali ga ni mogoče drugače izdati kot del nabora identifikacijskih podatkov osebe, države članice namesto tega uporabijo vrednost atributa, ki ustreza razmeram.

Preglednica 4

Neobvezni identifikacijski podatki pravne osebe

Identifikator podatkov
Trenutni naslov
Identifikacijska številka za DDV
Davčna sklicna številka
Evropski enotni identifikator iz Direktive (EU) 2017/1132 Evropskega parlamenta in Sveta ([1])
Identifikator pravnih subjektov (LEI) iz Izvedbene uredbe Komisije (EU) 2022/1860 ([2])
Registracijska in identifikacijska številka gospodarskega subjekta (EORI) iz Izvedbene uredbe Komisije (EU) št. 1352/2013 ([3])
Trošarinska številka iz člena 2(12) Uredbe Sveta (EU) št. 389/2012 ([4])

([1]) Direktiva (EU) 2017/1132 Evropskega parlamenta in Sveta z dne 14. junija 2017 o določenih vidikih prava družb (UL L 169, 30.6.2017, str. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Izvedbena uredba Komisije (EU) 2022/1860 z dne 10. junija 2022 o določitvi izvedbenih tehničnih standardov za uporabo Uredbe (EU) št. 648/2012 Evropskega parlamenta in Sveta v zvezi s standardi, oblikami, pogostostjo ter metodami in ureditvami za poročanje (UL L 262, 7.10.2022, str. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Izvedbena uredba Komisije (EU) št. 1352/2013 z dne 4. decembra 2013 o določitvi obrazcev iz Uredbe (EU) št. 608/2013 Evropskega parlamenta in Sveta o uveljavljanju pravic intelektualne lastnine s strani carinskih organov (UL L 341, 18.12.2013, str. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Uredba Sveta (EU) št. 389/2012 z dne 2. maja 2012 o upravnem sodelovanju na področju trošarin in o razveljavitvi Uredbe (ES) št. 2073/2004 (UL L 121, 8.5.2012, str. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3. Oddelek 3: Nabor metapodatkov o identifikacijskih podatkih osebe

Preglednica 5

Metapodatki o identifikacijskih podatkih osebe

Identifikator podatkov	Opredelitev	Navedba
`issuing_authority`	Ime upravnega organa izdajatelja identifikacijskih podatkov osebe ali koda ISO 3166 alpha-2 zadevne države članice, če ni ločenega organa, ki bi bil pooblaščen za izdajanje identifikacijskih podatkov osebe.	obvezna
`issuing_country`	Koda alpha-2, kot je določena v standardu ISO 3166-1, države ali ozemlja ponudnika identifikacijskih podatkov osebe.	obvezna
`expiry_date`	Datum (in po možnosti čas) poteka obdobja veljavnosti identifikacijskih podatkov osebe.	neobvezna
`document_number`	Številka za identifikacijske podatke osebe, ki jo dodeli ponudnik identifikacijskih podatkov osebe.	neobvezna
`issuing_jurisdiction`	Koda podregije države jurisdikcije, ki je izdala identifikacijske podatke osebe, kot je določena v določbi 8 standarda ISO 3166-2:2020. Prvi del kode je enak vrednosti za državo izdajateljico.	neobvezna
`issuance_date`	Datum in po možnosti čas začetka obdobja veljavnosti identifikacijskih podatkov osebe.	neobvezna

4. Oddelek 4: Kodiranje atributov identifikacijskih podatkov fizične osebe

— Identifikacijski podatki fizične osebe se izdajo v skladu s standardi iz Priloge II k Izvedbeni uredbi (EU) 2024/2979, in sicer iz določb 5 (oblika SD-JWT VC) in 6 (oblika ISO/IEC-mdoc), kot se uporabljata za elektronska potrdila o atributih. Določbe 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3,6.2.4 in 6.2.5 se ne uporabljajo.

— Kodiranje identifikacijskih podatkov fizične osebe je skladno s tehničnimi specifikacijami iz oddelkov 4.1 in 4.2 te priloge.

4.1 Kodiranje identifikacijskih podatkov fizične osebe v obliki ISO/IEC-mdoc

— Vrsta potrdila za identifikacijske podatke osebe v obliki ISO/IEC mdoc je ‚eu.europa.ec.eudi.pid.1'. Identifikator imenskega prostora za atribute identifikacijskih podatkov osebe, določene v tej prilogi, je ‚eu.europa.ec.eudi.pid.1'.

— Kadar identifikacijski podatki osebe vključujejo podatke, za katere identifikatorji podatkov v tej prilogi niso določeni, se ti podatki opredelijo v okviru nacionalnega imenskega prostora za identifikacijske podatke osebe, ki uporablja splošno obliko eu.europa.ec.eudi.pid.[koda države alpha-2 po standardu ISO 3166-1 ali koda regije po standardu ISO 3166-2], ki ji sledita neobvezna pika in številka različice.

— Kadar se uporablja nacionalni imenski prostor, se njegova shema, vključno z vsemi identifikatorji podatkov, njihovimi opredelitvami, navedbami in oblikami kodiranja, objavi v skladu s členom 8 Izvedbene uredbe Komisije (EU) 2025/1569 ([1]).

— Identifikacijski podatki osebe in njihovi metapodatki iz oddelkov 1 in 3 te priloge se vključijo v elemente identifikacijskih podatkov osebe v smislu specifikacij za obliko ISO/IEC mdoc.

— Član deviceKey znotraj člana deviceKeyInfo instance vrste MobileSecurityObject vsebuje javni ključ.

— Ta javni ključ ustreza zasebnemu ključu, ki je shranjen v varni kriptografski napravi denarnice (WSCD) uporabnika denarnice.

— Parametra zaščitene glave digitalnega podpisa CB-AdES, s katerim se podpišejo identifikacijski podatki osebe v obliki ISO/IEC-mdoc, sta x5u in x5t, ki sta določena v RFC 9360 ([2]).

— Kodirni algoritem, ki se uporablja v parametru glave x5t, je SHA-256.

— Zahteve za kodiranje identifikacijskih podatkov osebe v obliki ISO/IEC-mdoc so določene v preglednici 6.

Preglednica 6

Zahteve za kodiranje identifikacijskih podatkov osebe v obliki ISO/IEC-mdoc

Identifikator podatkov	Identifikator atributa	Oblika kodiranja
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) Izvedbena uredba Komisije (EU) 2025/1569 z dne 29. julija 2025 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede kvalificiranih elektronskih potrdil o atributih in elektronskih potrdil o atributih, izdanih s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir (UL L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([2]) Schaad, J., *CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates* (Podpisovanje in šifriranje objekta s CBOR: parametri glave za izvajanje certifikatov X.509 in sklicevanje nanje) (https://datatracker.ietf.org/doc/rfc9360/).

Identifikator podatkov	Identifikator atributa	Oblika kodiranja
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate ali full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate ali full-date

— Pri zapisu oblike kodiranja atributov iz preglednice 6 se uporabijo vrste predstavitve, določene v RFC 8610 ([3]), z naslednjimi dodatnimi zahtevami:

(a) tstr se kodira v UTF-8;

(b) tstr podpira celoten razpon Unicode;

(c) tstr ima največ 150 znakov;

(d) datum se kodira, kot je določeno v RFC 8943 ([4]);

(e) full-date se razlaga kot #6.1004(tstr), pri čemer je tag 1004 določen v RFC 8943;

(f) atribut tdate vsebuje niz datum-čas, kot je določeno v RFC 3339 ([5]);

(g) atribut full-date vsebuje niz full-date, kot je določeno v RFC 3339, v skladu z RFC 8943;

(h) če ni navedeno drugače, se pri predstavitvi datuma v atributih:

— ne uporabljajo deli sekund,

— ne uporablja lokalni zamik od UTC, zamik časa, določen v RFC 3339, pa je ‚Z‘;

(i) celo število z glavnima vrstama 0 in 1 je čim krajše, kot je določeno v RFC 8949 ([6]), oddelek 4.2;

(j) place_of_birth vsebuje vsaj enega od naslednjih parov ključ-vrednost: ‚country‘, ‚region‘ ali ‚locality‘;

(k) navedba dolžine v bstr, tstr, polju ali mapi je čim krajša, kot je določeno v RFC 8949, oddelek 4.2;

([3]) Vigano, C., in Birkholz, H., *Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures* (Strnjeni jezik za opredelitev podatkov (CDDL): konvencija za zapisovanje, ki omogoča strnjeno predstavitev binarnega objekta (CBOR) v strukturah podatkov JSON), RFC 8610, junij 2019.
([4]) Jones, M., Nadalin, A., in Richter, J., *Concise Binary Object Representation (CBOR) Tags for Date*, (Strnjena predstavitev binarnega objekta (CBOR), oznake za datume), RFC 8943, november 2020.
([5]) Klyne, G., in Newman, C., *Date and Time on the Internet: Timestamps* (Datum in čas na internetu: časovni žigi), RFC 3339, julij 2002.
([6]) Bormann, C., in Hoffman, P., *Concise Binary Object Representation (CBOR)* (Strnjena predstavitev binarnega objekta (CBOR)), RFC 8949, december 2020.

(l) atribut državljanstva se kodira kot polje kod držav alpha-2, določenih v standardu ISO 3166-1. Kadar se uporablja zapis CDDL, kot je določen v RFC 8610, je kodiranje tega atributa naslednje:

— nationalities = [+ CountryCode];

— CountryCode = tstr; koda države alpha-2, določena v standardu ISO 3166-1;

— kadar ima uporabnik denarnice, na katerega se nanašajo identifikacijski podatki osebe, več državljanstev, ponudnik identifikacijskih podatkov osebe pa ta državljanstva potrdi, lahko ponudnik identifikacijskih podatkov osebe v te podatke vključi vsa državljanstva;

— atribut place_of_birth se kodira kot vrsta place_of_birth. Kadar se uporablja zapis CDDL, kot je določen v RFC 8610, je kodiranje tega atributa naslednje:

place_of_birth =

{

? ‚country‘: tstr; ena koda države alpha-2, določena v standardu ISO 3166-1

? ‚region‘: tstr; ime zvezne države, pokrajine, okrožja ali lokalnega območja

? ‚locality‘: tstr; ime občine, mesta, naselja ali vasi

}

4.2 Zahteve za kodiranje identifikacijskih podatkov osebe v obliki SD-JWT VC

— Identifikacijski podatki osebe in njihovi metapodatki, določeni v tem oddelku, se vključijo v identifikacijske podatke osebe kot trditve v smislu specifikacij oblike SD-JWT VC.

— Vsako posamezno trditev v izdanih identifikacijskih podatkih osebe, navedene v prejšnji alinei, je mogoče selektivno razkriti, razen tistih, ki so opredeljene kot trditve, ki jih je mogoče razkriti neselektivno v obliki SD-JWT VC.

— V preglednici 7 je določeno kodiranje imen trditev, ki so javna imena.

— V preglednici 8 je določeno kodiranje imen trditev, ki so specifična za identifikacijske podatke osebe.

— Niz JSON, ki se uporablja v identifikacijskih podatkih osebe, kodiranih v obliki SD-JWT VC, se kodira v UTF-8 in podpira celoten razpon Unicode, razen če je v preglednici 8 v nadaljevanju ali njenih sklicih izrecno določeno drugače.

— Trditvi JWT nbf in exp, kot sta opredeljeni v RFC 7519 ([7]), se uporabljata za navedbo obdobja tehnične veljavnosti identifikacijskih podatkov osebe, skladnih z obliko SD-JWT VC.

([7]) Jones, J., idr., *JSON Web Token (JWT)* (Spletni žeton JSON (JWT)), RFC 7519, maj 2015.

— Identifikacijski podatki osebe vključujejo trditev cnf, kot je opredeljena v RFC 7800 ([8]), ki je javni ključ, ustvarjen iz zasebnega ključa, shranjenega v WSCD enote denarnice uporabnika denarnice.

— Parametra zaščitene glave digitalnega podpisa, s katerim se podpišejo identifikacijski podatki osebe v obliki SD-JWT VC, sta x5u in x5t#S256, ki sta določena v RFC 7515 ([9]).

Preglednica 7

Zahteve za kodiranje identifikacijskih podatkov osebe v obliki SD-JWT VC z uporabo javnih imen

Identifikator podatkov	Identifikator atributa	Oblika kodiranja
`family_name`	`family_name`	niz
`given_name`	`given_name`	niz
`birth_date`	`birthdate`	niz, ISO 8601-1, oblika LLLL-MM-DD
`birth_place`	`place_of_birth`	struktura JSON
`nationality`	`nationalities`	polje nizov
`resident_address`	`address.formatted`	niz
`resident_country`	`address.country`	niz
`resident_state`	`address.region`	niz
`resident_city`	`address.locality`	niz
`resident_postal_code`	`address.postal_code`	niz
`resident_street`	`address.street_address`	niz
`family_name_birth`	`birth_family_name`	niz
`given_name_birth`	`birth_given_name`	niz
`email_address`	`email`	niz
`mobile_phone_number`	`phone_number`	niz
`portrait`	`picture`	niz; URL s podatki, ki vsebuje fotografijo, kodirano z base64, v obliki JPEG

([8]) Jones, M., idr., *Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)* (Semantika dokazil o imetju ključev za spletne žetone JSON (JWT)), RFC 7800, april 2016.

([9]) Jones, M., idr. *JSON Web Signature (JWS)* (Spletni podpis JSON (JWS)), RFC 7515, maj 2015.

Preglednica 8

Zahteve za kodiranje identifikacijskih podatkov osebe v obliki SD-JWT VC z uporabo zasebnih imen

Identifikator podatkov	Identifikator atributa	Oblika kodiranja
`expiry_date`	`date_of_expiry`	niz, ISO 8601-1, oblika LLLL-MM-DD
`issuance_date`	`date_of_issuance`	niz, ISO 8601-1, oblika LLLL-MM-DD
`personal_administrative_number`	`personal_administrative_number`	niz
`sex`	`sex`	število
`issuing_authority`	`issuing_authority`	niz
`issuing_country`	`issuing_country`	niz
`document_number`	`document_number`	niz
`issuing_jurisdiction`	`issuing_jurisdiction`	niz

— Osnovna vrsta identifikacijskih podatkov osebe je ‚urn:eudi:pid:1‘ in je vključena v trditev vct. Vsi identifikacijski podatki osebe uporabljajo vrste v imenskem prostoru ‚urn:eudi:pid:‘.

— Kadar identifikacijski podatki osebe vključujejo atribute, ki niso določeni v tej prilogi, se ti atributi opredelijo v okviru nacionalne vrste.

— Kadar se uporablja nacionalna vrsta, se njena shema, vključno z vsemi identifikatorji podatkov, njihovimi opredelitvami, navedbami in oblikami kodiranja, opredeli v shemi, ki se objavi v skladu s členom 8 Izvedbene uredbe (EU) 2025/1569.

5. Oddelek 5: Podatki o infrastrukturi zaupanja

Seznam ponudnikov identifikacijskih podatkov osebe, ki ga Komisija da na voljo v skladu z Izvedbeno uredbo (EU) 2024/2980, omogoča avtentikacijo identifikacijskih podatkov osebe.“

PRILOGA II

„*PRILOGA Ia*

Kriptografski mehanizmi iz člena 5a

Evropska certifikacijska skupina za kibernetsko varnost, podskupina za kriptografijo: „Dogovorjeni kriptografski mehanizmi‘, ki jih je objavila Agencija Evropske unije za kibernetsko varnost (ENISA) ([1]).“

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

PRILOGA III

„PRILOGA Ib

Tehnične specifikacije za potrdila o enoti denarnice iz člena 6(2a)

1. Potrdilo o enoti denarnice vključuje eno ali več potrdil o instanci denarnice in eno ali več potrdil ključa.

2. Potrdilo o instanci denarnice in potrdila ključa izpolnjujejo naslednje zahteve:

   (a) Zahteve glede oblike

   — FR-WIA-1: potrdilo o instanci denarnice je JSON Web Token (JWT), kot je določeno v RFC 7519 ([1]), ki ga ponudnik denarnice podpiše ali ožigosa z uporabo strnjenega izhodiščnega podpisa JAdES B:

   — FR-WIA-1.1: potrdilo o instanci denarnice je potrdilo denarnice, kot je določeno v Dodatku E k prvi različici dokumenta OpenID za izdaji preverljivih poverilnic ([2]) (OID4VCI), in razširjeno, kot je določeno v C-WIA-1 in C-WIA-2 v nadaljevanju.

   — FR-KA-1: potrdilo o ključu je JWT, kot je določeno v RFC 7519, ki ga ponudnik denarnice podpiše ali ožigosa z uporabo strnjenega izhodiščnega podpisa JAdES B:

   — FR_KA_1.1: potrdilo o ključu je potrdilo, kot je določeno v Dodatku D OID4VCI, in razširjeno, kot je določeno v C_KA-1 in C_KA-2 v nadaljevanju.

   (b) Zahteve glede prenosa

   — TR-WIA-1: enota denarnice uporablja potrdilo o instanci denarnice pri izdaji identifikacijskih podatkov osebe, kvalificiranih ali nekvalificiranih elektronskih potrdil o atributih ali elektronskih potrdil o atributih, ki jih zagotovi organ javnega sektorja, pristojen za verodostojni vir, ali ki se zagotovijo v njegovem imenu.

   — TR-WIA-2: ponudnik denarnice preveri celovitost instance denarnice ter podpiše ali ožigosa potrdilo o instanci denarnice:

   — TR-WIA-2.1: kadar ponudnik denarnice izda potrdilo o instanci denarnice, je razlika med časom, ko je ponudnik denarnice preveril celovitost instance denarnice, in časom, ki ga navede v parametru glave ‚exp' izdanega potrdila o instanci denarnice, krajša od 24 ur,

   — TR-WIA-2.2: ponudnik denarnice zagotovi, da enota denarnice vsebuje potrdila o instanci denarnice, ki so potrebna za izdajo identifikacijskih podatkov osebe in elektronskih potrdil o atributih.

   — TR-WIA-3: med izdajo enota denarnice pošlje potrdilo o instanci denarnice v avtorizacijski strežnik s potisnjeno zahtevo za avtorizacijo in zahtevo za žeton, kot je določeno v OID4VCI:

   — TR-WIA-3.1: enota denarnice pošlje potrdilo o instanci denarnice skupaj z dokazilom o posedovanju (*Proof-of-Possession* –PoP), kot je določeno v Dodatku E k OID4VCI,

   — TR-WIA-3.2: enota denarnice pošlje isto potrdilo o instanci denarnice samo v en avtorizacijski strežnik:

([1]) RFC 7519: *JSON Web Token (JWT)* (Spletni žeton JSON (JWT)), maj 2015.
([2]) *OpenID for Verifiable Credential Issuance v1.0* (OpenID za izdajo preverljivih poverilnic, 1. različica), https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: kadar ponudnik denarnice uporablja možnost ‚per-issuer reuse', določeno v R_WIA_1 v nadaljevanju, lahko enota denarnice isto potrdilo o instanci denarnice večkrat pošlje v isti avtorizacijski strežnik,

— TR-WIA-3.2.2: kadar ponudnik denarnice ne uporablja možnosti ‚per-issuer reuse', enota denarnice uporabi potrdilo o instanci denarnice v največ enem postopku izdaje.

— TR-WIA-4: kadar avtorizacijski strežnik prejme potrdilo o instanci denarnice, preveri podpis potrdila o instanci denarnice z javnim ključem v potrdilu o podpisu, vključenem v parameter ‚x5c' v glavi JOSE potrdila o instanci denarnice:

— TR-WIA-4.1: avtorizacijski strežnik preveri tudi, ali je to potrdilo o podpisu mogoče preveriti s sidrom zaupanja na seznamu ponudnikov denarnic iz člena 5 Izvedbene uredbe (EU) 2024/2980, po potrebi z uporabo vmesnih potrdil, vključenih v parameter ‚x5c',

— TR-WIA-4.2: avtorizacijski strežnik preveri, da potrdilo o instanci denarnice ni poteklo,

— TR-WIA-4.3: avtorizacijski strežnik preveri podpis PoP z javnim ključem iz trditve ‚cnf'.

— TR_KA-1: enota denarnice uporablja potrdilo o ključu pri izdaji identifikacijskih podatkov osebe ter pri izdaji kvalificiranih ali nekvalificiranih elektronskih potrdil o atributih ali elektronskih potrdil o atributih, ki jih zagotovi organ javnega sektorja, pristojen za verodostojni vir, ali ki se zagotovijo v njegovem imenu in ki so vezana na napravo:

— TR_KA-1.1: enota denarnice ne uporablja potrdila o ključu pri izdaji kvalificiranih ali nekvalificiranih elektronskih potrdil o atributih ali elektronskih potrdil o atributih, ki jih zagotovi organ javnega sektorja, pristojen za verodostojni vir, ali ki se zagotovijo v njegovem imenu in ki niso vezana na napravo.

— TR_KA-2: ponudnik denarnice zagotovi enoti denarnice različna potrdila o ključu za WSCD enote denarnice in za vsako njeno shrambo ključev:

— TR_KA-2.1: ponudnik denarnice podpiše ali ožigosa potrdilo o ključu, ko preveri, da so ključi, potrjeni v potrdilu o ključu, shranjeni v WSCD enote denarnice ali shrambi ključev, opisani v potrdilu o ključu,

— TR_KA-2.2: potrdilo o ključu vsebuje vsaj en potrjen javni ključ. Število ključev v potrdilu o ključu, poslanem izdajatelju poverilnic, ne bi smelo presegati največje velikosti serije, ki jo ta izdajatelj poverilnic določi v svojih metapodatkih izdajatelja poverilnic, glej ETSI TS 119 472-3 ([3]), parameter ‚credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size',

— TR_KA-2.3: ponudnik denarnice vključi javni ključ (ki ustreza zasebnemu ključu, shranjenemu v WSCD ali shrambi ključev enote denarnice) v največ eno potrdilo o ključu,

— TR_KA-2.4: enota denarnice uporablja potrdilo o ključu v največ enem postopku izdaje ali ponovne izdaje poverilnice,

— TR_KA-2.5: ponudnik denarnice zagotovi, da ima enota denarnice potrdila o ključu, ki so potrebna za izdajo identifikacijskih podatkov osebe in elektronskih potrdil o atributih, vezanih na napravo.

([3]) ETSI, „Elektronski podpisi in infrastrukture (ESI); digitalni podpisi JAdES – 3. del: Ravni JAdES in osnovni profili", ETSI TS 119 472-3, V1.1.1, marec 2026.

— TR_KA-3: kadar je to med izdajo potrebno, enota denarnice vključi potrdilo o ključu v polje ‚proofs‘ zahteve za poverilnico, poslane izdajatelju poverilnic, kot je določeno v OID4VCI, in sicer kot dokazilo vrste ‚jwt‘ ali vrste ‚attestation‘:

— TR_KA_3.1: kadar enota denarnice v element ‚jwt‘ vključi potrdilo o ključu, podpiše ali ožigosa potrdilo o ključu z zasebnim ključem, ki ustreza javnemu ključu z indeksom 0 v polju ‚attested_keys‘ v objektu ‚key_attestation‘.

— TR_KA-4: kadar izdajatelj poverilnic izdaja poverilnice, vezane na napravo, v parametru ‚proof_types_supported‘ v svojih metapodatkih o poverilnicah izdajatelja, kot je določeno v oddelku 12.2.4 OID4VCI, navede, da podpira vrsti dokazila vrste ‚jwt‘ in ‚attestation‘ za potrdila o ključu, ki vključujejo objekt ‚key_attestation_required‘:

— TR_KA-4.1: kadar izdajatelj poverilnic izdaja poverilnice, ki niso vezane na napravo, v metapodatkih izdajatelja poverilnic izpusti parametra ‚proof_types_supported‘ in ‚cryptographic_binding_methods_supported‘.

— TR_KA-5: kadar izdajatelj poverilnic prejme potrdilo o ključu v dokazilu vrste ‚jwt‘ ali ‚attestation‘, preveri podpis potrdila o ključu z javnim ključem v potrdilu o podpisu, vključenem v parameter ‚x5c‘ v glavi JOSE potrdila o ključu, ter preveri, ali je to potrdilo o podpisu mogoče preveriti s sidrom zaupanja na seznamu ponudnikov denarnic iz člena 5 Izvedbene uredbe (EU) 2024/2980, po potrebi z uporabo vmesnih potrdil, vključenih v parameter ‚x5c‘.

— TR_KA-6: kadar izdajatelj poverilnic prejme potrdilo o ključu v dokazilu vrste ‚jwt‘, preveri podpis elementa ‚jwt‘ s ključem z indeksom 0 v polju ‚attested_keys‘ v objektu ‚key_attestation‘, vključenem v element ‚jwt‘:

— TR_KA-6.1: izdajatelj poverilnic preveri, ali polje ‚nonce‘ elementa ‚jwt‘ vsebuje veljaven c_nonce iz njegovega nonce_endpoint, kot je določeno v OID4VCI.

— TR_KA-7: kadar izdajatelj poverilnic prejme potrdilo o ključu v dokazilu vrste ‚attestation‘, preveri, ali objekt ‚key_attestation‘ vsebuje veljaven c_nonce iz njegove nonce_endpoint.

— TR_KA-8: ponudnik identifikacijskih podatkov osebe zagotovi, da so identifikacijski podatki osebe vezani na javni ključ, ki izvira iz potrdila o ključu, v katerem je navedena WSCD.

(c) Zahteve glede vsebine

— C_WIA-1: potrdilo o instanci denarnice vključuje naslednje:

— trditev ‚wallet_name‘, določeno v Dodatku E k OID4VCI, katere vrednost je identifikator rešitve denarnice, ki je na seznamu ponudnikov denarnic iz člena 5 Izvedbene uredbe (EU) 2024/2980,

— trditev ‚wallet_version‘ ([4]), ki je niz, katerega vrednost je različica rešitve denarnice,

— trditev ‚wallet_solution_certification_information‘, ki je objekt JSON z informacijami o organu za ugotavljanje skladnosti, ki je certificiral rešitev denarnice, številko certifikata, kadar je to ustrezno, in drugimi ustreznimi podrobnostmi v zvezi s certificiranjem,

([4]) Ta trditev je opredeljena v tej izvedbeni uredbi, saj ni del specifikacije OID4VCI.

— trditev ‚client_status‘, ki vsebuje dve podpolji:

— ‚status‘: sklic na seznam statusov, kot je določen v Dodatku E k OID4VCI, ki predstavlja status preklica instance denarnice. Podrobnosti so navedene v točki (e) v nadaljevanju,

— ‚exp‘: NumericDate, kot je določen v RFC 7519, ki določa čas, do katerega bo ponudnik denarnice ohranjal status preklica pri indeksu seznama statusov iz ‚status‘,

— trditev ‚exp‘, določena v Dodatku E k OID4VCI.

— *OPOMBA:* trditev ‚client_status.status‘ v potrdilu o instanci denarnice predstavlja status preklica instance denarnice, ne pa statusa preklica samega potrdila. Kot je opisano v R_WIA-1 v nadaljevanju, se lahko ponudnik denarnice odloči, da bo vsako potrdilo o instanci denarnice omejil na določen avtorizacijski strežnik, ker vsa potrdila, poslana temu strežniku, vsebujejo isto vrednost indeksa v vnosu ‚client_status.status‘.

— *OPOMBA:* vrednost ‚idx‘ v trditvi ‚status‘ se lahko uporablja (po parih) kot edinstveni identifikator instance denarnice in enote denarnice.

— C_WIA-2: potrdilo o instanci denarnice bi moralo vključevati tudi trditev ‚wallet_link‘, določeno v Dodatku E k OID4VCI, vrednost te trditve pa je URI, pri kateri je mogoče pridobiti dodatne informacije o rešitvi denarnice.

— C_WIA-3: avtorizacijski strežnik parametra ‚exp‘ na najvišji ravni potrdila o instanci denarnice ne razlaga kot konec obdobja ohranjanja statusa preklica instance denarnice.

— *OPOMBA:* parameter ‚exp‘ na najvišji ravni potrdila o instanci denarnice označuje čas, ko poteče samo potrdilo.

— C_KA-1: potrdilo o ključu vključuje:

— trditvi ‚key_storage‘ in ‚user_authentication‘, določeni v Dodatku D k OID4VCI:

— vrednost atributov ‚key_storage‘ in ‚user_authentication‘ je ‚iso_18045_high‘, kadar je v potrdilu o ključu navedena WSCD,

— trditev ‚certification‘, določeno v Dodatku D k OID4VCI, ki vsebuje URL, pri kateri je mogoče pridobiti informacije o certificiranju z WSCD ali shrambo ključev, med drugim o shemi, kot sta Common Criteria ali GlobalPlatform, ocenjenih zahtevah, kot je veljavni profil zaščite, ter ravni ocenjevanja:

— iz teh informacij mora biti mogoče ugotoviti, ali je shramba ključev WSCD,

— trditev ‚key_storage_status‘, ki vsebuje dve podpolji:

— ‚status‘: sklic na seznam statusov, kot je določen v Dodatku D.1 k OID4VCI. Vrednost predstavlja status preklica WSCD ali vrsto shrambe ključev, ki se uporablja za shranjevanje potrjenih ključev, bodisi – v okviru možnosti indeksa per-key-attestation – status preklica WSCD posamezne enote denarnice ali shrambe ključev. Razpoložljive možnosti dodelitve indeksov so navedene v R_KA_1 v nadaljevanju,

— ‚exp‘: NumericDate, kot je določen v RFC 7519, ki določa čas, do katerega bo ponudnik denarnice ohranjal status preklica pri indeksu seznama statusov iz ‚status‘,

— trditev ‚exp‘, določeno v Dodatku D k OID4VCI.

— *OPOMBA* glede vrednosti ‚idx' v trditvi ‚key_storage_status.status' v potrdilu o ključu: kadar ponudnik denarnice uporablja možnost ‚type-shared index' (glej R_KA_1 v nadaljevanju), imajo vsa potrdila o ključu za isto vrsto WSCD ali shrambe ključev isti indeks seznama statusov. Zato vrednost ‚idx' ni edinstvena za posamezno enoto denarnice. Kadar pa ponudnik denarnice uporablja možnost ‚per-key-attestation index', je vrednost ‚idx' edinstvena za enoto denarnice (ali edinstvena po parih na izdajatelja poverilnic). Za vse primere pa velja, da izdajatelj poverilnic ne uporablja vrednosti ‚idx' v potrdilu o ključu kot identifikatorja enote denarnice, temveč namesto tega uporablja vrednost ‚idx' v potrdilu o instanci denarnice.

— C_KA-2: kadar je potrdilo o ključu poslano v dokazilu vrste ‚attestation', vključuje tudi veljaven ‚c_nonce', kot je določen v Dodatku F.3 k OID4VCI.

— C_KA-3: izdajatelj poverilnic parametra ‚exp' na najvišji ravni potrdila o ključu ne razlaga kot konec obdobja ohranjanja statusa preklica WSCD ali shrambe ključev.

— *OPOMBA:* parameter ‚exp' na najvišji ravni potrdila o ključu označuje čas, ko poteče samo potrdilo o ključu.

(d) Zahteve glede življenjskega cikla

— V tej prilogi so določeni naslednji parametri metapodatkov izdajatelja poverilnic:

  — ‚preferred_client_status_period': OPTIONAL. Celo število, ki določa želeno preostalo obdobje ohranjanja statusa potrdila o instanci denarnice, ki ga enota denarnice predloži med izdajo, v sekundah. Preostalo obdobje ohranjanja statusa je opredeljeno kot vrednost ‚client_status.exp' v potrdilu minus čas prejema potrdila,

  — ‚preferred_key_storage_status_period': OPTIONAL. Celo število, ki določa želeno preostalo obdobje ohranjanja statusa potrdila o ključu, ki ga enota denarnice predloži med izdajo, v sekundah. Preostalo obdobje ohranjanja statusa je opredeljeno kot vrednost ‚key_storage_-status.exp' v potrdilu minus čas prejema potrdila.

— LC_WIA-1: avtorizacijski strežnik lahko svoje preference glede preostalega obdobja ohranjanja statusa v potrdilih o instanci denarnice sporoči tako, da v svojo končno točko metapodatkov izdajatelja poverilnic vključi parameter metapodatkov ‚preferred_client_status_period', kot je določeno v oddelku 12.2.2 OID4VCI:

  — LC_WIA-1.1: to polje se umesti na najvišjo raven metapodatkov izdajatelja poverilnic.

— LC_WIA_2: avtorizacijski strežnik parametra ‚exp' na najvišji ravni potrdila o instanci denarnice ne razlaga kot konec obdobja ohranjanja statusa preklica instance denarnice.

— LC_WIA_3: kadar ponudnik denarnice podpiše ali ožigosa potrdilo o instanci denarnice, ohranja status preklica zadevne instance denarnice, dokler ne poteče ‚wallet_instance_status.exp', naveden v tem potrdilu o instanci denarnice.

— LC_KA-1: kadar je potrebno potrdilo o ključu, lahko izdajatelj poverilnic svoje preference glede preostalega obdobja ohranjanja statusa v potrdilih o ključu sporoči tako, da v svojo končno točko metapodatkov izdajatelja poverilnic vključi zgoraj navedeni parameter metapodatkov ‚preferred_key_storage_status_period', kot je določeno v oddelku 12.2.2 OID4VCI:

  — LC_KA-1.1: to polje se umesti v objekt ‚key_attestations_required', kot je določeno v oddelku 12.2.4 OID4VCI.

— LC_KA-2: ponudnik denarnice določi obdobje tehnične veljavnosti potrdil o ključu, ki jih izdaja.

— LC_KA-3: kadar ponudnik denarnice podpiše ali ožigosa potrdilo o ključu, ohranja status preklica zadevne WSCD ali shrambe ključev, dokler ne poteče ‚key_storage_status.exp', naveden v tem potrdilu o ključu.

— LC_GEN-1: ponudnik denarnice zagotovi, da lahko enota denarnice vedno predloži potrdila o enoti denarnice in potrdila o ključu, katerih ‚client_status.exp' oziroma ‚key_storage_status.exp' sta v trenutku predložitve avtorizacijskemu strežniku ali izdajatelju poverilnic vsaj 31 dni v prihodnosti.

— *OPOMBA:* s tem se zagotovi, da se lahko ponudniki identifikacijskih podatkov osebe oprejo na veriženje preklicev, ne da bi morali izdati kratkotrajne identifikacijske podatke osebe.

— LC_GEN-2: ponudnik denarnice zagotovi, da enota denarnice med izdajo pridobi metapodatke izdajatelja poverilnic:

  — LC_GEN_2.1: če ta metapodatek vključuje polje ‚preferred_key_storage_status_duration', enota denarnice pošlje potrdilo o ključu, pri katerem je (‚key_storage_status.exp' – trenutni čas) – ‚preferred_key_storage_status_duration' čim manjši, vendar ni negativen. Če enota denarnice takega potrdila o ključu nima na voljo, od ponudnika denarnice pridobi novo potrdilo o ključu, ki izpolnjuje pogoj ‚key_storage_status.exp' – trenutni čas ≥ ‚preferred_key_storage_status_duration',

  — LC_GEN_2.2: če ta metapodatek vključuje polje ‚preferred_client_status_duration', enota denarnice pošlje potrdilo o instanci denarnice, pri katerem je (‚client_status.exp' – trenutni čas) – ‚preferred_client_status_duration' čim manjši, vendar ni negativen. Če enota denarnice takega potrdila o instanco denarnice nima na voljo, od ponudnika denarnice zahteva novo potrdilo o instanci denarnice, ki izpolnjuje pogoj ‚client_status.exp' – trenutni čas ≥ ‚preferred_client_status_duration'.

— LC_GEN-3: obdobje tehnične veljavnosti podatkov za ugotavljanje identitete osebe se izteče pred iztekom ‚client_status.exp' potrdila o instanci denarnice in ‚key_storage_status.exp' potrdila o ključu, poslanega ponudniku identifikacijskih podatkov osebe v postopku izdaje.

— LC_GEN-4: ponudnik identifikacijskih podatkov osebe s tehnično veljavnostjo, daljšo od 24 ur, med obdobjem tehnične veljavnosti teh podatkov vsaj enkrat na 24 ur preveri status preklica potrdila o instanci denarnice in potrdila o ključu, prejetega med izdajo. Če je katero koli od teh potrdil preklicano, ponudnik prekliče identifikacijske podatke osebe.

(e) Zahteve glede preklica

— R_GEN-1: ponudnik denarnice uporablja sezname statusov žetonov (določene na seznamu statusov žetonov IETF) kot mehanizem preklica za potrdila o ključu in potrdila o instanci denarnice, kot je določeno v dodatku D oziroma E k OID4VCI.

— *OPOMBA:* za izboljšanje nadgradljivosti svojih seznamov statusov lahko ponudnik denarnice uporabi naslednje optimizacije:

  — razdelitev seznama statusov na več segmentov, kadar imajo ponudniki denarnice veliko število uporabnikov in izdanih potrdil. Obstaja več strategij razdeljevanja, na primer na podlagi fiksne velikosti ali časovnega obdobja. Izbira strategije razdeljevanja je prepuščena presoji ponudnika denarnice. Pri tem se lahko upoštevata velikost seznama statusov za prenos in zasebnost uporabnika,

  — uporaba več seznamov statusov,

  — stiskanje seznama statusov za zmanjšanje njegove velikosti.

— R_WIA-1: ponudnik denarnice lahko vsem potrdilom o instanci denarnice, ki jih določena enota denarnice predloži istemu avtorizacijskemu strežniku, dodeli isto vrednost trditvi ‚idx' v trditvi ‚client_status.status'. To se imenuje možnost ‚per-issuer reuse'. Če se uporablja ta možnost:

— R_WIA-1.1: enota denarnice mora shraniti podatke o tem, katero vrednost indeksa je uporabila za vsak avtorizacijski strežnik, s katerim je že komunicirala, in mora pri ponovni komunikaciji z istim avtorizacijskim strežnikom zahtevati potrdilo o instanci denarnice, ki vsebuje enako vrednost indeksa,

— R_WIA-1.2: kadar ponudnik denarnice prejme zahtevo za potrdilo o instanci denarnice, ki vsebuje določeno vrednost indeksa, pred izdajo novega potrdila o instanci denarnice s to vrednostjo indeksa preveri, ali je enota denarnice, ki zahtevo vlaga, to vrednost indeksa že prejela,

— R_WIA-1.3: enota denarnice iste vrednosti indeksa ne uporablja ponovno v komunikaciji z različnimi avtorizacijskimi strežniki.

— *OPOMBA:* če se uporablja možnost ‚per-issuer reuse', bo ponudnik denarnice lahko ugotovil, s koliko avtorizacijskimi strežniki je enota denarnice komunicirala in kako pogosto komunicira z vsakim od njih.

— R_WIA-2: ponudnik denarnice v svoji politiki zasebnosti dokumentira, ali za preklic instance denarnice uporablja možnost ‚per-issuer reuse'.

— R_WIA-3: kadar ponudnik denarnice ne uporablja možnosti ‚per-issuer reuse', vsakemu potrdilu o instanci denarnice, ki ga izda, dodeli novo, nepovezljivo vrednost indeksa.

— R_WIA-4: če je treba enoto denarnice preklicati, ponudnik denarnice prekliče vrednosti indeksa v trditvi ‚client_status.status' v vseh potrdilih o instanci denarnice, povezanih s to enoto denarnice.

— R_WIA-5: ponudnik denarnice pri določanju velikosti svojih seznamov statusa potrdil o instanci denarnice upošteva obseg namestitve in osnovno arhitekturo ter zagotovi, da so dovolj veliki za preprečevanje korelacije in varovanje zasebnosti uporabnika. Seznam statusov se, kadar je to mogoče, nanaša vsaj na 10 000 potrdil.

— R_KA_1: ponudnik denarnice izbere eno od naslednjih možnosti dodelitve indeksov za trditev ‚key_storage_status.status' v potrdilu o ključu:

— možnost 1, imenovano ‚type-shared index', pri kateri vsa potrdila o ključu, ki potrjujejo ključe, shranjene v isti vrsti WSCD ali shrambi ključev, vsebujejo isto vrednost indeksa v ‚key_storage_status.status',

— možnost 2, imenovano ‚per-key-attestion index', pri kateri potrdilo o ključu, ki potrjuje ključe, shranjene v posamezni WSCD ali shrambi ključev, vsebuje (po parih) edinstveno vrednost indeksa v ‚key_storage_status.status'.

— *OPOMBA:* kadar ponudnik denarnice uporablja možnost 1, en sam ukrep preklica razveljavi vsa potrdila o ključu zadevne vrste v vseh enotah denarnice. Poleg tega, ker imajo vsa potrdila o ključu za isto vrsto WSCD ali shrambe ključev skupen indeks seznama statusov, število vnosov na seznamu statusa potrdil o ključu odraža število vrst WSCD ali shramb ključev, ki jih podpira ponudnik denarnice, in ne števila nameščenih enot denarnice. Vidiki zasebnosti, ki utemeljujejo najmanjšo velikost seznamov statusov potrdil o instanci denarnice, zato pri možnosti 1 ne veljajo za sezname statusov potrdil o ključu, če isto vrsto WSCD ali shrambe ključev uporablja dovolj veliko število enot denarnice.

— *OPOMBA:* kadar ponudnik denarnice uporablja možnost 2, vsak indeks predstavlja stanje preklica posamezne WSCD ali shrambe ključev, potrjene v navedenem potrdilu o ključu.

— *OPOMBA:* kadar ponudnik denarnice uporablja možnost 2, se lahko posamezna WSCD ali shramba ključev prekliče tudi na zahtevo uporabnika.

— R_KA-2: kadar ponudnik denarnice uporablja možnost 2, lahko ponudnik denarnice neobvezno uporablja možnost ‚per-issuer reuse', opisano v R_WIA-1. Če ponudnik denarnice uporablja to možnost, se zahteve R_WIA-1–R_WIA-3 uporabljajo *mutatis mutandis*.

— R_KA-3: kadar ponudnik denarnice uporablja možnost 2, pri določanju velikosti svojih seznamov statusa potrdil o ključu upošteva obseg namestitve in osnovno arhitekturo ter zagotovi, da so dovolj veliki za preprečevanje korelacije in varovanje zasebnosti uporabnika. Seznam statusov se, kadar je to mogoče, nanaša vsaj na 10 000 potrdil o ključu.

— R_KA-4: kadar ponudnik denarnice uporablja možnost 1 (type-shared index), ponudnik denarnice prekliče vnos ‚key_storage_status.status' samo, če sta vrsta WSCD ali shramba ključev varnostno ranljivi.

(f) Zahteve glede algoritmov za podpis

— SA-1: za podpisovanje potrdil o instanci denarnice, potrdil o ključu, povezanih dokazil o imetju in seznamov statusa žetonov se uporabi eden od naslednjih algoritmov:

— ES256 (ECDSA s SHA-256 in P-256),

— ES384 (ECDSA s SHA-384 in P-384),

— ES512 (ECDSA s SHA-512 in P-521).

— SA-2: ponudnik denarnice izbere, katerega od algoritmov, navedenih v SA-1, bo uporabljal.

— SA-3: avtorizacijski strežnik ali izdajatelj poverilnic (kot je določeno v OID4VCI) podpira vse algoritme, navedene v SA-1."

PRILOGA IV

„PRILOGA II

Seznam standardov iz člena 8

Uporabljajo se tehnične specifikacije iz določb 2 do 6 standarda ETSI TS 119 472-1 V1.2.1 (2026-02). Uporabljajo se z naslednjimi prilagoditvami.

1. 2.1 Normative references (Normativne reference)

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): ‚Elektronski podpisi in infrastrukture zaupanja (ESI); Profili potrdil – 1. del: Pregled in skupne podatkovne strukture‘.

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): ‚Elektronski podpisi in infrastrukture zaupanja (ESI); Profili potrdil – 6. del: Zahteve glede profilov potrdil za ponudnike identifikacijskih podatkov osebe, denarnic, elektronskih potrdil o atributih, kvalificiranih elektronskih potrdil o atributih in elektronskih potrdil o atributih organov javnega sektorja‘.

— [25] Seznam statusov žetonov IETF (TSL), draft-ietf-oauth-status-list-20: ‚Seznam statusov žetonov‘, 20. april 2026.

2. 4.2.11.1 General requirements (Splošne zahteve)

— EAA-4.2.11.1-06: Kadar se element statusa uporablja za identifikacijske podatke osebe, kvalificirana elektronska potrdila o atributih ali elektronska potrdila o atributih, ki jih zagotavlja organ javnega sektorja, pristojen za verodostojen vir, ali ki se zagotavljajo v njegovem imenu, se z njim navede le, ali je potrdilo preklicano ali ne, in ne sme podpirati nobenih drugih vrednosti statusa, med drugim začasnega preklica.

— EAA-4.2.11.1-06.1: kadar je potrdilo preklicano, je trajno preklicano.

3. 4.2.13 EAA short-lived (Kratkotrajna elektronska potrdila o atributih)

— EAA-4.2.13-03: kadar se izdajo kratkotrajna elektronska potrdila o atributih z obdobjem veljavnosti 24 ur ali manj, preklic ni potreben.

4. 4.6.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (Zahteve za elektronsko potrdilo o atributih EU, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir) (PuB-EAA)

— PuB-EAA-4.6.2-03: neveljavno.

— PuB-EAA-4.6.2-04: neveljavno.

— PuB-EAA-4.6.3-03: digitalni podpis PuB-EAA bi moral vsebovati kvalificirano potrdilo, ki podpira digitalni podpis PuB-EAA.

— PuB-EAA-4.6.3-04: kvalificirano potrdilo, ki podpira digitalni podpis PuB-EAA, izpolnjuje zahteve iz določbe 8 standarda ETSI TS 119 412-6 V1.1.1 in vsebuje izjavo QcType qcStatement, kot je opredeljena v standardu ETSI EN 319 412-5 V2.5.1, z vrednostjo id-etsi-qct-eidaspsbeaa, opredeljeno na naslednji način:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } – Potrdilo iz člena 45f(1), točka (b), ki podpira kvalificirani elektronski podpis ali kvalificirani elektronski žig organa javnega sektorja iz člena 3, točka 46, Uredbe (EU) št. 910/2014.

5. 5.2.10.1 General requirements (Splošne zahteve)

— EAA-5.2.10.1-04: neveljavno.

— EAA-5.2.10.1-05: neveljavno.

— EAA-5.2.10.1-06: Član statusa lahko vsebuje člana status_list, kot je določeno v določbi 6.2 IETF draft-ietf-oauth-status-list-20 [25].

— EAA-5.2.10.1-07: neveljavno.

— EAA-5.2.10.1-08: neveljavno.

— EAA-5.2.10.1-09: neveljavno.

— EAA-5.2.10.1-10: neveljavno.

— EAA-5.2.10.1-11: neveljavno.

— EAA-5.2.10.1-12: neveljavno.

6. 6.2.10.1 General requirements (Splošne zahteve)

— EAA-6.2.10.1-01: kadar elektronsko potrdilo o atributih, skladno z ISO/IEC mdoc, uporablja mehanizem seznama statusa potrdil, kot je določen v EAA-6.2.10.1-02.2, ali mehanizem seznama preklicev potrdil, kot je določen v EAA-6.2.10.1-02.3, njegov mobilni varnostni objekt (*Mobile Security Object* –MSO) vsebuje strukturo statusa, kot je določena v EAA-6.2.10.1-17, ki vsebuje informacije o preklicu MSO.

— EAA-6.2.10.1-01.1: pri izvajanju mehanizma seznama identifikatorjev element statusa vsebuje element identifier_list, kot je določen v EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: pri izvajanju mehanizma seznama statusov element statusa vsebuje element status_list, kot je določen v EAA-6.2.10.1-13.

— *OPOMBA:*

  — struktura statusa vsebuje sklic na seznam preklicev MSO,

  — seznam preklicev MSO je struktura COSE_Sign1, ki označuje, ali je določen MSO preklican ali ne,

  — struktura statusa vsebuje vse informacije, ki jih na denarnice zanašajoča se stranka potrebuje, da bi ugotovila, ali je seznam preklica MSO verodostojen.

— EAA-6.2.10.1-02: ponudnik identifikacijskih podatkov osebe, ponudnik kvalificiranih elektronskih potrdil o atributih ali ponudnik elektronskih potrdil o atributih, ki jih zagotavlja organ javnega sektorja, pristojen za verodostojen vir, ali ki se zagotavljajo v njegovem imenu, uporabi eno od naslednjih metod za preklic identifikacijskih podatkov osebe, kvalificiranih elektronskih potrdil o atributih ali elektronskih potrdil o atributih, ki jih zagotavlja organ javnega sektorja, pristojen za verodostojen vir, ali ki se zagotavljajo v njegovem imenu:

— EAA-6.2.10.1-02.1: kadar izdaja kratkotrajna elektronska potrdila o atributih z obdobjem veljavnosti 24 ur ali manj, preklic ni potreben,

— EAA-6.2.10.1-02.2: mehanizem seznama statusov potrdil se uporabi, da se informacije o preklicu vpišejo kot seznam statusa,

— EAA-6.2.10.1-02.2.1: mehanizem seznama statusov prekliče MSO na podlagi tega, ali je binarna števka na mestu binarne števke, ki jo izdajatelj opredeli v MSO, v seznamu statusa nastavljen na ‚true‘,

— EAA-6.2.10.1-02.2.2: mehanizem seznama statusov se določi v specifikaciji seznama statusov žetonov (draft-ietf-oauth-status-list-20),

— EAA-6.2.10.1-02.3: mehanizem seznama preklicev potrdil se uporabi, da se informacije o preklicu vpišejo kot seznam identifikatorjev,

— EAA-6.2.10.1-02.3.1: mehanizem seznama identifikatorjev prekliče MSO na podlagi tega, ali je identifikator, ki ga izdajatelj opredeli v MSO, na seznamu identifikatorjev,

— EAA-6.2.10.1-02.3.2: EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 in EAA-6.2.10.1-11 določajo mehanizem seznama identifikatorjev na podlagi zahtev iz specifikacije seznama statusov žetonov, vključno s skupnimi značilnostmi mehanizma seznama statusov in mehanizma seznama identifikatorjev.

— EAA-6.2.10.1-03: kadar se element statusa uporablja za identifikacijske podatke osebe, kvalificirana elektronska potrdila o atributih ali elektronska potrdila o atributih, ki jih zagotavlja organ javnega sektorja, pristojen za verodostojen vir, ali ki se zagotavljajo v njegovem imenu, se uporabi izključno status ‚preklican'.

— EAA-6.2.10.1-03.1: to za seznam statusa pomeni, da se uporabljata le vrednosti ‚valid' in ‚invalid', kot sta določeni v specifikaciji seznama statusov žetonov,

— EAA-6.2.10.1-03.2: na seznam identifikatorjev se uvrstijo le preklicani MSO, ne pa začasno zadržani MSO.

— EAA-6.2.10.1-04: kadar je MSO preklican, je trajno preklican.

— EAA-6.2.10.1-05: preverjanje seznama preklicev MSO je za na denarnice zanašajočo se stranko neobvezno; kadar se uporablja, mora biti skladno z zahtevami za preverjanje, določenimi v specifikaciji seznama statusov žetonov ter specifikaciji strukture statusa iz EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: kadar mora biti na denarnice zanašajoča se stranka zmožna preveriti status preklica identifikacijske podatkov osebe ali elektronskih potrdil o atributih, se podpreta mehanizem seznama statusov potrdil in mehanizem seznama preklicev potrdil iz EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: identifier_list in status_list v MSO lahko vsebujeta element certifikata:

— EAA-6.2.10.1-06.1: kadar je element certifikata naveden, vsebuje potrdilo, ki vsebuje javni ključ, s katerim je bilo podpisano ali ožigosano potrdilo najvišje ravni v elementu x5chain v strukturi seznama preklicev MSO:

— EAA-6.2.10.1-06.1.1: instanca na denarnice zanašajočo se stranko uporabi to potrdilo kot sidro zaupanja za preverjanje elementa x5chain v strukturi seznama preklicev MSO,

— EAA-6.2.10.1-06.2: kadar element certifikata ni naveden, mora biti potrdilo najvišje ravni v elementu x5chain v strukturi seznama preklicev MSO podpisano ali ožigosano s potrdilom, uporabljenim za podpis potrdila v elementu x5chain MSO:

— EAA-6.2.10.1-06.2.1: instanca na denarnice zanašajočo se stranko uporabi to potrdilo kot sidro zaupanja za preverjanje elementa x5chain v strukturi seznama preklicev MSO.

— EAA-6.2.10.1-07: seznam preklicev MSO se izvaja v skladu s specifikacijo seznama statusov žetonov kot žeton s seznama statusov v formatu CWT.

— EAA-6.2.10.1-08: za seznam preklicev MSO za mehanizem seznama identifikatorjev in mehanizem seznama statusov se uporabljajo naslednje zahteve:

  — navedena je trditev exp,

  — lahko je navedena trditev ttl,

  — trditev aggregation_uri je lahko navedena v trditvi IdentifierList ali StatusList, ponudnik identifikacijskih podatkov osebe, ponudnik kvalificiranih elektronskih potrdil o atributih ali ponudnik elektronskih potrdil o atributih, ki jih zagotavlja organ javnega sektorja, pristojen za verodostojen vir, ali ki se

zagotavljajo v njegovem imenu, pa lahko trditev aggregation_uri uporabi za označevanje podpore mehanizmu za združevanje, kot je določen v specifikaciji seznama statusov žetonov,

— CWT je objekt COSE_Sign1, pri katerem se za izračun podpisa uporabi eden od naslednjih algoritmov za podpis:

(a) ‚ES256‘ (ECDSA s krivuljo NIST P-256 in SHA-256);

(b) ‚ES384‘ (ECDSA s krivuljo NIST P-384 in SHA-384);

(c) ‚ES512‘ (ECDSA s krivuljo NIST P-521 in SHA-512);

(d) ‚ESB256‘ (ECDSA s krivuljo brainpoolP256r1 in SHA-256);

(e) ‚ESB384‘ (ECDSA s krivuljo brainpoolP384r1 in SHA-384);

(f) ‚ESB512‘ (ECDSA s krivuljo brainpoolP512r1 in SHA-512);

— CWT v zaščiteni glavi vsebuje x5chain, ki vsebuje potrdilo ali verigo potrdil za preverjanje podpisa seznama preklicev MSO,

— razširjena uporaba ključa identifikatorja objekta, določenega v specifikaciji seznama statusov žetonov, se lahko uporablja za potrdilo o podpisu seznama statusov in seznama identifikatorjev, instance na denarnice zanašajočih se strank pa lahko podpirajo razširjeno uporabo ključa identifikatorja objekta, določenega v specifikaciji seznama statusov žetonov, za identifikator objekta pa ponudnik kvalificiranih elektronskih potrdil o atributih ali ponudnik elektronskih potrdil o atributih, ki jih zagotavlja organ javnega sektorja ali se zagotavljajo v njegovem imenu, ne sme določiti razširjenega polja uporabe ključa kot obveznega pri uporabi razširjenega OID uporabe ključa, določenega v specifikaciji seznama statusov žetonov.

— EAA-6.2.10.1-09: z odstopanjem od zahtev specifikacije seznama statusov žetonov za mehanizem seznama identifikatorjev se uporabljajo naslednje zahteve:

— vrednost trditve type je ‚application/identifierlist+cwt‘,

— trditev StatusList ni navedena v naboru trditev CWT,

— struktura IdentifierList, opredeljena v EAA-6.2.10.1-11, je kot trditev navedena v naboru zahtevkov CWT z uporabo ključa 65530.

— EAA-6.2.10.1-10: struktura IdentifierList je struktura CBOR z naslednjim CDDL:

```
IdentifierList = {

    ‚identifiers‘: { * Identifier => IdentifierInfo },

    ? ‚aggregation_uri‘: Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: kadar je identifikator v IdentifierList naveden, je MSO, ki vsebuje identifikator v elementu statusa, preklican,

— EAA-6.2.10.1-10.2: trditev Aggregation_uri je določena v oddelku 9.2 specifikacije seznama statusov žetonov,

— EAA-6.2.10.1-10.3: vrsta vsebine seznama identifikatorjev je ‚application/identifierlist+cwt', kot je določena v zahtevah iz oddelka 8.2 specifikacije seznama statusov žetonov.

— EAA-6.2.10.1-11: za element identifier_list v MSO se uporabljajo naslednje zahteve (glej EAA-6.2.10.1-17):

— EAA-6.2.10.1-11.1: element identifier_list je struktura CBOR z naslednjim CDDL:

```
IdentifierListInfo = {

        ‚id': Identifier ,

        ‚uri': URI,

        ? ‚certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: da se prepreči uporaba identifikatorja za korelacijo med predložitvami, je ta edinstven za vsak MSO.

— EAA-6.2.10.1-12: za seznam statusov se uporabljajo naslednje zahteve:

  — EAA-6.2.10.1-12.1: element binarnih števk v strukturi StatusList je nastavljen na 1.

— EAA-6.2.10.1-13: za element status_list v MSO veljajo naslednje zahteve (glej EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: element seznama statusov mora izpolnjevati zahteve za strukturo StatusListInfo, kot je določena v specifikaciji seznama statusov žetonov, in doda se neobvezni element certifikata, opredeljen v EAA-6.2.10.1-06,

  — EAA-6.2.10.1-13.2: da se indeks statusa ne bi uporabil za korelacijo med predložitvami, je kombinacija indeksa statusa in URI edinstvena vsak MSO.

— EAA-6.2.10.1-14: ponudnik denarnice za preklic potrdila o instanci denarnice ali za preklic potrdila o ključu uporabi drugo (EAA-6.2.10.1-02.2) ali tretjo (EAA-6.2.10.1-02.3) od metod, določenih v EAA-6.2.10.1-02.

— EAA-6.2.10.1-15: ponudnik denarnice v svoji rešitvi denarnice izvaja mehanizme preklica potrdil, določene v EAA-6.2.10.1-02.

— EAA-6.2.10.1-16: ponudnik identifikacijskih podatkov osebe in ponudnik elektronskih potrdil o atributih podpirata mehanizem seznama statusov potrdil in mehanizem seznama preklicev potrdil, ki sta določena v EAA-6.2.10.1-02, za preverjanje statusa preklicev potrdil o instanci denarnice in potrdil o ključu.

— EAA-6.2.10.1-17: struktura statusa v MSO je struktura CBOR z naslednjim CDDL:

Status = {

? ‚identifier_list': IdentifierListInfo,

? ‚status_list': StatusListInfo,

* tstr => RFU

}“

PRILOGA V

„PRILOGA III

Tehnične specifikacije iz člena 10

— Tehnične specifikacije:

  — Določba 4.2.5 standarda ETSI TS 119 472-3 V1.1.1 (2026-03).“

PRILOGA VI

Priloga IV k Izvedbeni uredbi (EU) 2024/2979 se spremeni:

1. točka 1 se nadomesti z naslednjim:

„1. Obvezna oblika podpisa ali žiga:

(a) PAdES (PDF Advanced Electronic Signature), kot je določen v ETSI EN 319 142-1 V1.2.1 (2024-01); Elektronski podpisi in infrastruktura (ESI) Digitalni podpisi PAdES; 1. del: Gradniki in izhodiščni podpisi PAdES.“;

2. točka 3 se nadomesti z naslednjim:

„3. Vmesnik za aplikacijsko programiranje:
ETSI TS 119 432 v1.3.1 (2026-03), določbe 6.4.3, A.6, A.7 in A.8.“.

PRILOGA VII

„*PRILOGA VI*

Znak zaupanja za evropsko denarnico za digitalno identiteto v barvah



“

PRILOGA VIII

„PRILOGA VII

Znak zaupanja za evropsko denarnico za digitalno identiteto v črno-beli različici



“

PRILOGA IX

„PRILOGA VIII

Podatki o znaku zaupanja za evropsko denarnico za digitalno identiteto

Podatki	Opis	Kodiranje	Status
TrustMarkResourceURL	URL grafičnih elementov znaka zaupanja za evropsko denarnico za digitalno identiteto in virov z informacijami za uporabnika v uporabniškem vmesniku denarnice.	URL	obvezno
ListOfCertifiedWalletsURL	URL javnega seznama certificiranih rešitev denarnic v EU, kot je določen v Izvedbeni uredbi Komisije (EU) 2025/849 ([1]).	URL	obvezno
ListOfCertifiedWalletsQRCode	QR Code, ki vsebuje informacije iz ListOfCertifiedWalletsURL.	ISO-8859-1 Byte mode QR code	neobvezno
WalletSolutionInfoPageURL	URL strani z informacijami o certificirani rešitvi denarnice na strani seznama certificiranih rešitev denarnic z ListOfCertifiedWalletsURL, kjer se URL doda ‚?' in identifikator WalletSolutionID rešitve denarnice.	URL	obvezno
WalletSolutionInfoPageQRCode	Koda QR, ki vsebuje informacije iz WalletSolutionInfoPageURL.	ISO-8859-1 Byte mode QR code	neobvezno
WalletVerifierToolURL*	URL, ki kaže na končno točko orodja za preverjanje denarnice */.well-known/openid-credential-issuer*, ki se uporablja za pridobivanje metapodatkov ponudnika potrdil.	URL	neobvezno

([1]) Izvedbena uredba Komisije (EU) 2025/849 z dne 6. maja 2025 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede predložitve informacij Komisiji in skupini za sodelovanje za seznam certificiranih evropskih denarnic za digitalno identiteto (UL L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).“

PRILOGA X

Priloga II k Izvedbeni uredbi (EU) 2024/2980 se spremeni:

1. v Prilogi II, oddelek 1, se točka 1(i) nadomesti z naslednjim:

„(i) eno ali več potrdil, skladnih s standardom ETSI EN 319 412-2 V2.4.1 (2025-06) ali standardom ETSI EN 319 412-3 V1.3.1 (2023-09), ki se lahko uporabijo za preverjanje podpisa ali žiga, ki ga je ustvaril registrator na podatkih iz registra, in za katerega potrjeni podatki o identiteti vključujejo ime registratorja in, kadar je ustrezno, njegovo registrsko številko, kot je določeno v točki (c) oziroma (d);“;

2. v Prilogi II, oddelek 2, se točka 1(h) nadomesti z naslednjim:

„(h) eno ali več potrdil, skladnih s standardom ETSI EN 319 412-2 V2.4.1 (2025-06) ali standardom ETSI EN 319 412-3 V1.3.1 (2023-09), ki se lahko uporabijo za avtentikacijo in potrditev potrdil o enoti denarnice, ki jih je izdal ponudnik denarnice, in za katera potrjeni podatki o identiteti vključujejo ime ponudnika denarnice in, kadar je ustrezno, njegovo registrsko številko, kot je določeno v točki (a) oziroma (b);“;

3. v Prilogi II, oddelek 3, se točka 1(h) nadomesti z naslednjim:

„(h) eno ali več potrdil, skladnih s standardom ETSI EN 319 412-2 V2.4.1 (2025-06) ali standardom ETSI EN 319 412-3 V1.3.1 (2023-09), ki se lahko uporabijo za preverjanje podpisa ali žiga, ki ga je na identifikacijskih podatkih osebe ustvaril njihov ponudnik, in za katere potrjeni podatki o identiteti vključujejo ime ponudnika identifikacijskih podatkov osebe in, kadar je ustrezno, njegovo registrsko številko, kot je določeno v točki (a) oziroma (b).“;

4. v Prilogi II, oddelek 4, se točka 1(g) nadomesti z naslednjim:

„(g) eno ali več potrdil, skladnih s standardom ETSI EN 319 412-2 V2.4.1 (2025-06) ali standardom ETSI EN 319 412-3 V1.3.1 (2023-09), ki se lahko uporabijo za preverjanje podpisa ali žiga, ki ga je na potrdilu o dostopu za na denarnice zanašajoče se stranke ustvaril njegov ponudnik, in, kadar je ustrezno, potrebne informacije za razlikovanje potrdil o dostopu za na denarnice zanašajoče se stranke od drugih potrdil.“;

5. v Prilogo II se doda oddelek 5, ki se glasi:

„5. Priglasitve informacij o ponudnikih potrdil o registraciji za na denarnice zanašajoče se stranke

1. Države članice Komisiji predložijo naslednje informacije o ponudnikih potrdil o registraciji za na denarnice zanašajoče se stranke:

(a) ime ponudnika potrdil o registraciji za na denarnice zanašajoče se stranke;

(b) kadar je ustrezno, registracijsko številko ponudnika potrdil o registraciji za na denarnice zanašajoče se stranke;

(c) državo članico sedeža ponudnika potrdil o registraciji za na denarnice zanašajoče se stranke;

(d) kontaktni elektronski naslov in telefonsko številko ponudnika potrdil o registraciji za na denarnice zanašajoče se stranke za zadeve, povezane s potrdili o registraciji, ki jih zagotavlja na denarnice zanašajočim se strankam;

(e) kadar je ustrezno, URL spletne strani ponudnika potrdil o registraciji za na denarnice zanašajoče se stranke, ki vsebuje dodatne informacije o ponudniku in potrdilih o registraciji, ki jih zagotavlja na denarnice zanašajočim se strankam;

(f) URL spletne strani s politikami in pogoji ponudnika, ki se uporabljajo za izdajo in uporabo potrdil o registraciji, ki jih zagotavlja na denarnice zanašajočim se strankam;

(g) eno ali več potrdil, skladnih s standardom ETSI EN 319 412-2 V2.4.1 (2025-06) ali standardom ETSI EN 319 412-3 V1.3.1 (2023-09), ki se lahko uporabijo za preverjanje podpisa ali žiga, ki ga je na potrdilu o registraciji za na denarnice zanašajoče se stranke ustvaril njegov ponudnik, in, kadar je ustrezno, potrebne informacije za razlikovanje potrdil o registraciji za na denarnice zanašajoče se stranke od drugih potrdil.

2. Informacije iz točke 1 se zagotovijo za vsakega ponudnika potrdil o registraciji za na denarnice zanašajoče se stranke.“.

PRILOGA XI

„PRILOGA I

Protokoli in vmesniki iz člena 4

Tehnična specifikacija ETSI TS 119 472-3 V1.1.1 (2026-03) se uporablja z naslednjimi prilagoditvami:

1. 4.1 General requirements (Splošne zahteve)

   — GEN-REQ-4.1-05: neveljavno

   — *OPOMBA:* neveljavno

2. 4.2.3 Provision of registration certificates of PID/EAA Provider to EUDI Wallet (Zagotavljanje potrdil o registraciji ponudnika identifikacijskih podatkov osebe/elektronskih potrdil o atributih evropski denarnici za digitalno identiteto)

   — ISS-MDATA-REG_CERT-4.2.3-04: eden od elementov parametra polja issuer_info vsebuje potrdilo o registraciji ponudnika identifikacijskih podatkov osebe/elektronskih potrdil o atributih.

   — ISS-MDATA-REG_CERT-4.2.3-07: neveljavno

   — ISS-MDATA-REG_CERT-4.2.3-08: neveljavno

   — ISS-MDATA-REG_CERT-4.2.3-09: neveljavno

   — ISS-MDATA-REG_CERT-4.2.3-10: neveljavno

   — ISS-MDATA-REG_CERT-4.2.3-11: neveljavno

   — ISS-MDATA-REG_CERT-4.2.3-12: neveljavno

   — ISS-MDATA-REG_CERT-4.2.3-13: neveljavno

3. 4.2.4.2 ARF pre-defined PID/EAA reuse policy (Politika ponovne uporabe vnaprej določenih PID/EAA ARF)

   — ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Kadar ima član id vrednost ‚arf_annex_ii', polje, povezano z oznako ‚details', pa vsebuje vrednost ‚once_only' ali vrednost ‚per-relying-party', objekt JSON, ki vsebuje to polje, povezano z oznako ‚details', vsebuje tudi število JSON, povezano z oznako ‚reissue_trigger_unused'.

4. Priloga A se ne uporablja."

PRILOGA XII

„PRILOGA II

Tehnične specifikacije iz člena 5

Uporablja se tehnična specifikacija iz Priloge C k ISO/IEC 18013-7:2025.

Tehnične specifikacije iz določb 4.1, 4.2, 5 in 6 standarda ETSI TS 119 472-2 V1.2.1 (2026-03) se uporabljajo z naslednjimi prilagoditvami, vključno z vstavitvijo nove določbe 4.3:

1. 1 Scope (Področje uporabe)

— Ta dokument dva (2) profila protokolov, ki zanašajočim se strankam (*Relying Parties* – RP) omogočata, da od evropska denarnica za digitalno identiteto zahtevajo EAAP ali identifikacijske podatke osebe (*Personal Identification Data* – PID), evropska denarnica za digitalno identiteto pa RP pošlje zahtevane EAAP/PID. Vsak od profilov podpira dva mehanizma prenosa, in sicer: s posredovanjem in brez posredovanja API, kot je prikazano v nadaljevanju:

(a) profil temelji na:

— ISO/IEC 18013-5 [10], vendar samo za mehanizem prenosa brez posredovanja API, in

— Prilogi C k standardu ISO/IEC 18013-7 [16] za mehanizem prenosa s posredovanjem API.

Ta profil se imenuje profil ISO/IEC-mdoc in je opredeljen v določbi 5 tega dokumenta;

(b) profil temelji na:
OpenID4VC-HAIP [11] za mehanizma prenosa s posredovanjem in brez posredovanja API, kot sledi:

— na oddelkih 5, 5.1, 5.3, 7 in 8 dokumenta [11] za prenos prek preusmeritev ali za mehanizem prenosa brez posredovanja API in

— na oddelkih 5, 5.2, 5.3, 7 in 8 dokumenta [11] za mehanizem prenosa s posredovanjem API.

Ta profil se imenuje profil OpenID4VC-HAIP in je opredeljen v določbi 6 tega dokumenta.

2. 2.1 Normative references (Normativne reference)

— [15] ISO 639: ‚Language code' (Kode jezikov)

— [16] ISO/IEC 18013-7:2025 ‚Osebna identifikacija – vozniško dovoljenje, ki je v skladu s standardom ISO – 7. del: Dodatne funkcije mobilnega vozniškega dovoljenja (mDL)'

3. 4.1 EAAP implementation based on SD-JWT VC (Izvajanje predstavitve elektronskega potrdila o atributih na podlagi SD-JWT VC)

— EAAP-SD-JWT VC-04: neveljavno.

4. 4.2 EAAP implementation based on ISO/IEC-mdoc (Izvajanje predstavitve elektronskega potrdila o atributih na podlagi ISO/IEC-mdoc)

— EAAP-ISO/IEC-mdoc-01: neveljavno.

— *Opomba 2:* neveljavno.

— EAAP-ISO/IEC-mdoc-02: neveljavno.

5. 4.3 EAAP implementation with mediating API (Izvajanje predstavitve elektronskega potrdila o atributih s posredniškim API)

— EAAP-API-GEN-01: evropska denarnica za digitalno identiteto podpira posredniški API, ki podpira oba protokola, opredeljena v določbi 5.2 dokumenta [11] in v Prilogi C k [16].

— *OPOMBA:* kadar naprava, na kateri je nameščena evropska denarnica za digitalno identiteto, ne podpira obeh protokolov, te zahteve ni mogoče izpolniti, kar povzroči neskladnost, ker osnovni operacijski sistemi in brskalniki ne izvajajo potrebnih funkcij interoperabilnosti.

— EAAP-API-GEN-02: Evropska denarnica za digitalno identiteto podpira posredniški API vsaj za identifikacijske podatke osebe in vrste elektronskih potrdil o atributih, registrirane v katalogu shem, kot je opredeljen v Izvedbeni uredbi (EU) 2025/1569, in vsaj za vse oblike, opredeljene v Prilogi II k Izvedbeni uredbi (EU) 2024/2979.

— *OPOMBA 1:* kadar osnovni operacijski sistem, brskalnik, posredniški API ali katera koli druga tehnična raven, ki je zunaj nadzora evropske denarnice za digitalno identiteto, omejuje, filtrira, predhodno izbira ali kako drugače omejuje oblike poverilnic ter vrste identifikacijskih podatkov osebe in elektronskih potrdil o atributih, registrirane v katalogu shem, te zahteve ni mogoče izpolniti. Kadar evropska denarnica za digitalno identiteto zaradi take omejitve ne more podpreti registrirane vrste ali oblike poverilnice, se nastala neskladnost pripiše temu, da ti osnovni operacijski sistemi, brskalniki, posredniški API ali druga ustrezna tehnična raven ne zagotavljajo potrebnih funkcij interoperabilnosti.

6. 4.4 Wallet-relying party validation and overasking checks (Preverjanje na denarnico zanašajoče se stranke in prekomernih zahtev)

— WRP-VALIDATION-01: evropska denarnica za digitalno identiteto preveri potrdilo o registraciji na denarnico zanašajoče se stranke, prejeto v zahtevi, pred predložitvijo katerega koli zahtevanega identifikacijskega podatka osebe ali elektronskega potrdila o atributih uporabniku denarnice v odobritev.

— WRP-VALIDATION-02: kadar preverjanje potrdila o registraciji na denarnico zanašajoče se stranke ni uspešno, med drugim tudi v primerih, v katerih je potrdilo poteklo, bilo preklicano, ga ni izdal veljaven zaupanja vreden ponudnik potrdil o registraciji za na denarnico zanašajoče se stranke, je nepravilno oblikovano ali ga ni mogoče kriptografsko preveriti, evropska denarnica za digitalno identiteto uporabnika denarnice opozori, da na denarnico zanašajoče se stranke ni bilo mogoče preveriti, in zahteve ne predstavi kot uspešno preverjene. Uporabnik denarnice izrecno odobri zahtevo na denarnico zanašajoče se stranke. Neodziv ali vnaprej označena okenca ne zadostujejo za izrecno odobritev.

— WRP-VALIDATION-03: ponudnik denarnice na podlagi svoje analize tveganja in varnostne politike določi, ali in pod katerimi pogoji lahko uporabnik denarnice obide posamezna neuspešna preverjanja veljavnosti.

— WRP-OVERASKING-01: evropska denarnica za digitalno identiteto primerja potrdila in atribute, ki jih zahteva na denarnico zanašajoča se stranka, z registriranimi potrdili in atributi v potrdilu o registraciji na denarnico zanašajoče se stranke.

— WRP-OVERASKING-02: kadar na denarnico zanašajoča se stranka zahteva identifikacijske podatke osebe, elektronska potrdila o atributih ali trditve, ki niso zajete s potrdilom o registraciji na denarnico zanašajoče se stranke, evropska denarnica za digitalno identiteto uporabnika denarnice jasno opozori pred kakršnim koli razkritjem. V opozorilu mora biti navedeno, da na denarnico zanašajoča se stranka zahteva več informacij, kot jih je registrirala. Uporabnik denarnice izrecno odobri zahtevo na denarnico zanašajoče se stranke. Neodziv ali vnaprej označena okenca ne zadostujejo za izrecno odobritev.

— WRP-OVERASKING-03: ponudnik denarnice na podlagi svoje analize tveganja, varnostne politike in veljavnega prava določi, ali lahko uporabnik denarnice kljub takemu opozorilu nadaljuje, ali se lahko razkrije le del zahtevanih podatkov, zajeta s potrdilom o registraciji, ali pa se zahteva zavrne.

7. 5.1 Introduction (Uvod)

— V določbi 5 in njenih poddoločbah je določen profil protokola, ki RP omogoča, da zahteva EAAP ali PID za evropsko denarnico za digitalno identiteto, od evropske denarnice za digitalno identiteto pa, da RP pošlje zahtevane EAAP/PID z uporabo mehanizma prenosa brez posredovanja API, ki temelji na standardu ISO/IEC 18013-5 [10], ali z uporabo mehanizma prenosa s posredovanjem API, ki temelji na Prilogi C k standardu ISO/IEC 18013-7 [16], za prenos ustrezno vdelanih podatkovnih struktur, določenih v standardu ISO/IEC 18013-5 [10].

— Preostali del določbe 5 je strukturiran, kot sledi:

  — v določbi 5.2 so določene zahteve glede podpore profilu in mehanizmom prenosa s strani RP in evropske denarnice za digitalno identiteto,

  — v določbi 5.3 so določene zahteve, ki so značilne za mehanizem prenosa brez posredovanja API,

  — v določbi 5.4 in njenih podtočkah so določene zahteve, ki so značilne za mehanizem prenosa s posredovanjem API.

8. 5.2 Requirements on EUDI Wallet and RP support (Zahteve glede evropske denarnice za digitalno identiteto in podpiranja RP)

— ISO/IEC 18013-SUPPORT-01: enote denarnice, ponudniki PID, ponudniki potrdil, ponudniki denarnic in na denarnice zanašajoče se stranke ne smejo podpirati pridobivanja s strežnika, kot je določeno v standardu ISO/IEC 18013-5 [10], za zahtevanje in predložitev PID ali potrdil o atributih.

— ISO/IEC 18013-SUPPORT-02: evropska denarnica za digitalno identiteto izpolnjuje zahteve, določene v določbah 5.3 in 5.4 tega dokumenta.

— ISO/IEC 18013-SUPPORT-04: na denarnice zanašajoča se stranka bi morala izvajati profil, opredeljen v določbi 5.4 tega dokumenta.

9. 5.3.2 ISO/IEC-mdoc EAAP Request contents (Vsebina zahteve EAAP ISO/IEC-mdoc)

— ISO/IEC 18013-5-REQ-04: Zahteve naprave, poslane evropskim denarnicam za digitalno identiteto, vsebujejo par ključ-vrednost ‚requestInfo‘, določen v določbi 8.3.2.1.2.1 dokumenta [10]. Vrednost tega para je vrsta RequestInfo.

— ISO/IEC 18013-5-REQ-05: Vrsta RequestInfo je skladna z opredelitvijo CDDL v nadaljevanju.

RequestInfo = {

‚euWrprc‘: bstr; vsebuje potrdilo o registraciji (glej zahteve spodaj)

}

— ISO/IEC 18013-5-REQ-06: Navedeni član requestInfo vsebuje člana z oznako ‚euWrprc‘

— ISO/IEC 18013-5-REQ-07: vrednost ‚euWrprc‘ je potrdilo o registraciji, kodirano v CBOR.

— ISO/IEC 18013-5-REQ-08: neveljavno.

— *OPOMBA 3:* neveljavno.

— ISO/IEC 18013-5-REQ-09: neveljavno.

— ISO/IEC 18013-5-REQ-10: neveljavno.

— ISO/IEC 18013-5-REQ-11: neveljavno.

10. 5.3.3 ISO/IEC-mdoc EAAP Response profile (Profil odziva EAAP ISO/IEC-mdoc)

— V tej določbi so določene zahteve za vrsto sporočila DeviceResponse, ki je skupna obema vrstama mehanizmov prenosa (s posredovanjem in brez posredovanja API).

— *OPOMBA 1:* kadar se uporablja mehanizem brez posredovanja API, ki temelji na standardu ISO/IEC 18013-5 [10], je odgovor EAAP natančno instanca DeviceResponse, kot je profilirana v tej določbi, kadar pa se uporablja mehanizem s posredovanjem API, ki temelji na Prilogi C k standardu ISO/IEC 18013-7 [16], se instanca DeviceRequest vdela, kot je določeno v Prilogi C k [16].

— ISO/IEC 18013-5-RESP-02: ponudnik identifikacijskih podatkov osebe in elektronskih potrdil o atributih v mapo KeyAuthorizations mobilnega varnostnega objekta ne vključi nobenih podatkovnih elementov identifikacijskih podatkov osebe in elektronskih potrdil o atributih, ki jih izda, razen podatkovnih elementov, ki jih na denarnice zanašajoča se stranka zagotovi v podatkih o transakcijah v zahtevi mdoc, da jih enota denarnice podpiše ali ožigosa z zasebnim ključem identifikacijskih podatkov osebe ali elektronskih potrdil o atributih.

— *OPOMBA 2:* posledično enote denarnice ne morejo na denarnice zanašajočim se strankam predložiti nobenih podatkovnih elementov, podpisanih z napravo, razen za podpisovanje podatkov, ki jih je zagotovila na denarnico zanašajoča se stranka, na primer v primerih uporabe za varno avtentikacijo uporabnika.

— *OPOMBA 3:* standard ISO/IEC 18013-5:2021 ne določa, kako lahko na denarnice zanašajoče se stranke v zahtevo mdoc vključijo podatke o transakcijah. Vključitev podatkov o transakcijah v zahtevo mdoc se izvede z dodajanjem tehničnih specifikacij.

— ISO/IEC 18013-5-RESP-03: ponudniki identifikacijskih podatkov osebe ne dovolijo, da zasebni ključ identifikacijskih podatkov osebe podpisuje podatkovne elemente, ki jih na denarnico zanašajoča se stranka zagotovi v podatkih o transakcijah v zahtevi mdoc.

11. 5.4 Requirements for API mediated mechanism (Zahteve za mehanizem s posredovanjem API)

5.4.1 ISO/IEC 18013-7-related requirements (Zahteve glede ISO/IEC 18013-7)

V tej določbi so določene zahteve za mehanizem prenosa s posredovanjem API v zvezi z zahtevami, opredeljenimi v Prilogi C k [16].

— ISO/IEC 18013-7-API-01: profil, ki podpira predložitve s posredovanjem API, je skladen z zahtevami iz Priloge C k standardu ISO/IEC 18013-7 [16], kot so dodatno profilirane v določbah 5.3 in 5.4 tega dokumenta.

— ISO/IEC 18013-7-API-02: uporabljajo se vse obvezne zahteve, opredeljene v Prilogi C k [16], kot so dodatno profilirane v določbah 5.3 in 5.4 tega dokumenta.

— ISO/IEC 18013-7-API-03: vse neobvezne zahteve, opredeljene v Prilogi C k [16], so še naprej neobvezne, razen če je v tem dokumentu določeno drugače.

12. 5.4.2 Additional requirements (Dodatne zahteve)

— V tej določbi so določene dodatne zahteve za mehanizem prenosa s posredovanjem API.

— ISO/IEC 18013-ADD-API-01: evropska denarnica za digitalno identiteto privzeto razkrije navedbo vseh vrst shranjenih elektronskih potrdil o atributih posredniškemu API, ki deluje v skladu s Prilogo C k [16], vendar ne razkrije atributov in njihovih vrednosti v teh elektronskih potrdilih o atributih:

  — *OPOMBA 1:* omejitev glede vrednosti atributov velja tudi, če bi se s takim razkritjem izboljšale storitve, ki jih operacijski sistem zagotavlja evropski denarnici za digitalno identiteto, na primer izbiro potrdil v okviru posredniškega API.

— Obstajajo pomisleki v zvezi z operacijskimi sistemi in brskalniki, ki niso pod nadzorom izvajalcev, ki se lahko upoštevajo, kot je navedeno v naslednjih opombah 2 do 4:

  — *OPOMBA 2:* zahtevo za predložitev, ki jo poda na denarnico zanašajoča se stranka, ki se sklicuje na Prilogo C k [16], lahko brskalnik in/ali operacijski sistem obdelata za iskanje razpoložljivih elektronskih potrdil o atributih, preprečevanje goljufij, usmerjenih proti uporabniku, ali za odpravljanje težav,

  — *OPOMBA 3:* zahtevo za predložitev, ki jo poda na denarnico zanašajoča se stranka, ki se sklicuje na Prilogo C k [16], naj bi brskalnik in/ali operacijski sistem obdelala za namene varnosti uporabnika,

— *OPOMBA 4:* zahtevo za predložitev, ki jo poda na denarnico zanašajoča se stranka, ki se sklicuje na Prilogo C k [16], naj brskalnik in/ali operacijski sistem ne bi obdelovala za namene tržne analize (niti kot sekundarni namen) ali za notranje namene brskalnika in/ali operacijskega sistema.

— ISO/IEC 18013-ADD-API-02: kadar evropska denarnica za digitalno identiteto na zahtevo uporabnika izbriše PID ali EAA, ki sta bila predhodno razkrita posredniškemu API, ki deluje v skladu s Prilogo C k [16], posredniškemu API razkrije dejstvo, da tega PID ali EAA ne hrani več.

— ISO/IEC 18013-ADD-API-03: če uporabnik odstrani svojo evropsko denarnico za digitalno identiteto, slednja posredniškemu API, ki deluje v skladu s Prilogo C k [16], razkrije dejstvo, da ne hrani več nobenega prej razkritega PID ali EAA.

— ISO/IEC 18013-ADD-API-04: evropska denarnica za digitalno identiteto mora zagotoviti globalno uporabniško nastavitev za onemogočenje razkrivanja shranjenih EAA prek posredniškega API, ki deluje, kot je določeno v standardu ISO/IEC 18013-ADD-API-01. Kadar je ta nastavitev onemogočena, evropska denarnica za digitalno identiteto ne oglašuje ali odgovarja na zahteve za predložitev ali izdajo prek API.

— ISO/IEC 18013-ADD-API-05: evropske denarnice za digitalno identiteto v tokovih med napravami s posredniškim API z uporabo varnega, neposrednega in lokalnega komunikacijskega kanala za preverjanje fizične bližine, ki jo posreduje uporabnik, kot je brezžična komunikacijska tehnologija kratkega dosega, preverijo, ali je naprava v interakciji v neposredni fizični bližini evropske denarnice za digitalno identiteto.

— *OPOMBA:* CTAP 2.3 omogoča uporabo BLE za preverjanje neposredne fizične bližine in, kadar ga izvajata obe napravi, tudi prenos podatkov med napravama prek prenosnih tehnologij kratkega dosega. Osnovni operacijski sistemi, brskalniki, posredniški API ali katera koli druga tehnična raven, ki je zunaj nadzora evropske denarnice za digitalno identiteto, bi morali dajati prednost preverjanju fizične bližine in prenosa podatkov med napravama z uporabo lokalnega komunikacijskega kanala, kot ga omogoča CTAP 2.3, namesto uporabi hibridnih tunelskih storitev CTAP.

13. 6.2 Requirements on EUDI Wallet and RP support (Zahteve glede evropske denarnice za digitalno identiteto in podpiranja RP)

— OIDFVP-HAIP-SUPPORT-02: evropska denarnica za digitalno identiteto izpolnjuje zahteve, določene v določbi 6.5 te priloge.

— OIDFVP-HAIP-SUPPORT-03: evropska denarnica za digitalno identiteto ne bi smela podpirati mehanizma na podlagi preusmeritev, določenega v določbi 6.4, za tokove predložitev med napravami.

— *OPOMBA 3:* Uporaba tega mehanizma je ranljiva za napade, kot je ugrabljenje seje (t. i. *session fixation*). Ublažitev takih napadov je prepuščena zanašajočim se strankam. Izvajanje tega mehanizma ne bi smelo povzročiti neskladnosti.

— OIDFVP-HAIP-SUPPORT-05: Na denarnico zanašajoča se stranka izpolnjuje zahteve, določene v določbi 6.5 te priloge.

— *OPOMBA 5:* neveljavno.

14. 6.3.1 General requirements (Splošne zahteve)

— OIDFVP-HAIP-GEN-01: Uporabljajo se vse obvezne zahteve, določene v določbah 5, 5.3, 7 in 8 dokumenta HAIP [11].

— *OPOMBA 1:* ‚HAIP [11], oddelek 5', se nanaša samo na zahteve neposredno pod naslovom oddelka 5. To ne vključuje oddelkov 5.1, 5.2 in 5.3.

— OIDFVP-HAIP-GEN-03: če se s to prilogo spremeni zahteva iz OpenID4VC-HAIP [11], prevlada spremenjena zahteva iz te priloge.

— *OPOMBA 2:* to bi na primer omogočilo, da se neobvezna zahteva iz OpenID4VC-HAIP [11] spremeni v obvezno ali da se obvezne zahteve razširijo.

— OIDFVP-HAIP-GEN-04: kadar je oblika zahtevanega potrdila skladna z [10], na denarnice zanašajoče se stranke in evropske denarnice za digitalno identiteto ravnajo v skladu s profilom ‚ISO mdocs' iz oddelka 6 dokumenta [11].

— *OPOMBA 3:* Zaradi jasnosti profil ‚ISO mdocs' v dokumentu HAIP pomeni, da morajo na denarnice zanašajoče se stranke in evropske denarnice za digitalno identiteto ravnati v skladu z veljavnimi zahtevami iz Priloge B.2 k [7].

— OIDFVP-HAIP-GEN-05: kadar je oblika zahtevanega potrdila skladna s [2], na denarnice zanašajoče se stranke in evropske denarnice za digitalno identiteto ravnajo v skladu s profilom ‚IETF SD-JWT VCs' iz oddelka 6 [11].

— *OPOMBA 4:* zaradi jasnosti profil ‚IETF SD-JWT VCs' pomeni, da morajo na denarnice zanašajoče se stranke in evropske denarnice za digitalno identiteto ravnati v skladu z zahtevami iz Priloge B.3 k [7] in zahtevami iz oddelka 6.1 [11].

15. 6.3.2.1 General requirements (Splošne zahteve)

— OIDFVP-HAIP-COMMON-REQ-01: neveljavno.

16. 6.3.2.2 Requirements for the Request Object (Zahteve za predmet zahteve)

— OIDFVP-HAIP-COMMON-REQ-RO-02: neveljavno

— OIDFVP-HAIP-COMMON-REQ-RO-03: neveljavno

— OIDFVP-HAIP-COMMON-REQ-RO-04: neveljavno

— OIDFVP-HAIP-COMMON-REQ-RO-05: neveljavno

— OIDFVP-HAIP-COMMON-REQ-RO-06: neveljavno.

— OIDFVP-HAIP-COMMON-REQ-RO-07: neveljavno

— OIDFVP-HAIP-COMMON-REQ-RO-08: neveljavno

— OIDFVP-HAIP-COMMON-REQ-RO-09: neveljavno

— OIDFVP-HAIP-COMMON-REQ-RO-10: neveljavno

— OIDFVP-HAIP-COMMON-REQ-RO-11: neveljavno

— OIDFVP-HAIP-COMMON-REQ-RO-12: neveljavno

— *Opomba 2:* neveljavno

— OIDFVP-HAIP-COMMON-REQ-RO-13: Eden od elementov parametra verifier_info vsebuje potrdilo o registraciji.

— OIDFVP-HAIP-COMMON-REQ-RO-23: potrdilo končnega subjekta, navedeno v oddelku 5.9.3 OpenID4VP za uporabo z x509_hash Client Identifier Prefix, je potrdilo o dostopu RP, kot je določeno v ETSI TS 119 475 [14].

17. 6.3.3 Authorization Response (EAAP response) profile (Profil odgovora na avtorizacijo (odgovor EAAP))

— OIDFVP-HAIP-COMMON-RESP-01: neveljavno.

18. 6.4.1 General requirements (Splošne zahteve)

— OIDFVP-HAIP-REDIRECTS-04: neveljavno.

— *OPOMBA:* neveljavno.

19. 6.5.2 Additional requirements (Dodatne zahteve)

— OIDFVP-HAIP-ADD-API-01: evropska denarnica za digitalno identiteto privzeto razkrije navedbo vseh vrst elektronskih potrdil o atributih posredniškemu API, ki deluje v skladu z določbo 5.2 k [11], vendar ne razkrije atributov in njihovih vrednosti v teh elektronskih potrdilih o atributih.

— OIDFVP-HAIP-ADD-API-04: če evropska denarnica za digitalno identiteto podpira posredniški API, ki deluje, kot je določeno v OIDFVP-HAIP-ADD-API-01, zagotovi globalno uporabniško nastavitev, da se onemogoči razkrivanje shranjenih EAAs prek posredniškega API. Kadar je s to nastavitvijo onemogočeno razkrivanje, bi morala evropska denarnica za digitalno identiteto uporabniku nato omogočiti, da izbere posamezna potrdila, ki se razkrijejo posredniškemu API.

— OIDFVP-HAIP-ADD-API-05: evropske denarnice za digitalno identiteto v tokovih med napravami s posredniškim API z uporabo varnega, neposrednega in lokalnega komunikacijskega kanala za preverjanje fizične bližine, ki jo posreduje uporabnik, kot je brezžična komunikacijska tehnologija kratkega dosega, preverijo, ali je naprava v interakciji v neposredni fizični bližini evropske denarnice za digitalno identiteto.

— *OPOMBA 5:* CTAP 2.3 omogoča uporabo BLE za preverjanje neposredne fizične bližine in, kadar ga izvajata obe napravi, tudi prenos podatkov med napravama prek prenosnih tehnologij kratkega dosega. Osnovni operacijski sistemi, brskalniki, posredniški API ali katera koli druga tehnična raven, ki je zunaj nadzora evropske denarnice za digitalno identiteto, bi morali dajati prednost preverjanju fizične bližine in prenosa podatkov med napravama z uporabo lokalnega komunikacijskega kanala, kot ga omogoča CTAP 2.3, namesto uporabi hibridnih tunelskih storitev CTAP.

20. 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP (Posebne zahteve pri zahtevanju EAAP po ISO/IEC 18013-5)

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Vse zahteve, določene v tem dokumentu, ki se uporabljajo za strukturi zahtev za napravo in odgovorov naprave, določeni v standardu ISO/IEC 18013-5, se uporabljajo tudi, kadar evropska denarnica za digitalno identiteto prejme zahtevo za predložitev ISO/IEC mdoc z mehanizmom prenosa prek API, določenega v določbi C.1 [16].“