2026/1731

22.7.2026.

PROVEDBENA UREDBA KOMISIJE (EU) 2026/1731

od 15. srpnja 2026.

o izmjeni provedbenih uredbi (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 i (EU) 2024/2982 u pogledu mjerodavnih normi i specifikacija

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ ([1]), a posebno njezin članak 5.a stavak 23.,

budući da:

(1) Kako bi države članice u najvećoj mogućoj mjeri usklađeno razvijale i certificirale europske lisnice za digitalni identitet, tehničke specifikacije tih lisnica temelje se na Preporuci Komisije (EU) 2021/946 ([2]), osobito na njezinu arhitekturnom i referentnom okviru. Budući da su se od donošenja provedbenih uredbi Komisije (EU) 2024/2977 ([3]), (EU) 2024/2979 ([4]), (EU) 2024/2980 ([5]) i (EU) 2024/2982 ([6]) arhitekturni i referentni okvir znatno promijenili, te bi uredbe trebalo izmijeniti kako bi ih se uskladilo s novim normama, specifikacijama i postupcima.

U skladu s ciljevima Uredbe (EU) br. 910/2014 odabran je niz normi kako bi se ispunili ti specifični zahtjevi. Te bi norme trebale odražavati ustaljenu praksu i biti općepriznate u relevantnim sektorima. Na primjer, budući da se format W3C VCDM upotrebljava kao referentni format za potvrde, posebno u obrazovnom sektoru, europske lisnice za digitalni identitet trebale bi ga podržavati i kad budu dostupni novi profili na temelju tog formata. Kako bi se zajamčila sigurnost i vjerodostojnost europskih lisnica za digitalni identitet te olakšala prekogranična interoperabilnost i učinkovito funkcioniranje unutarnjeg tržišta, norme bi trebalo prema potrebi prilagođavati i dopunjavati.

(2) Izvedbe lisnice za svaku upotrebu koja zahtijeva predočavanje portreta korisnika moraju podržavati funkciju selektivnog otkrivanja, a otkrivanje mora biti pod potpunom kontrolom korisnika. Radi zaštite mogućnosti odlučivanja nakon otkrivanja i portreta od nenamjernog ili neovlaštenog zahtjeva za otkrivanje, arhitektura europskih lisnica za digitalni identitet trebala bi omogućavati mehanizme upozoravanja i evidentiranje svih transakcija povezanih s upotrebom portreta. Kako bi bilo sigurno da je korisnik lisnice svjestan dijeljenja biometrijskih podataka, u upozorenjima bi trebalo navesti da zahtjev obuhvaća dijeljenje biometrijskih podataka i

([1]) SL L 257, 28.8.2014., str. 73., ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Preporuka Komisije (EU) 2021/946 od 3. lipnja 2021. o zajedničkom Unijinu paketu alata za koordinirani pristup europskom okviru za digitalni identitet (SL L 210, 14.6.2021., str. 51., ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([3]) Provedbena uredba Komisije (EU) 2024/2977 od 28. studenoga 2024. o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu osobnih identifikacijskih podataka i elektroničkih potvrda atributa koji se izdaju europskim lisnicama za digitalni identitet (SL L, 2024/2977, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).
([4]) Provedbena uredba Komisije (EU) 2024/2979 od 28. studenog 2024. o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu cjelovitosti i osnovnih funkcionalnosti europskih lisnica za digitalni identitet (SL L, 2024/2979, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).
([5]) Provedbena uredba Komisije (EU) 2024/2980 od 28. studenoga 2024. o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu prijava Komisiji koje se odnose na ekosustav europskih lisnica za digitalni identitet (SL L, 2024/2980, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).
([6]) Provedbena uredba Komisije (EU) 2024/2982 od 28. studenoga 2024. o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu protokola i sučelja koje treba podržavati europski okvir za digitalni identitet (SL L, 2024/2982, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

izričito zahtijevati od korisnika da potvrdi otkrivanje. Ako pouzdajuća strana obrađuje portret u svrhu nedvosmislene identifikacije fizičke osobe ili potvrđivanja deklariranog identiteta te osobe, primjenjuju se članci 6. i 9. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća ([7]) te svi drugi zahtjevi iz te uredbe, među ostalim to da bi obrada portreta koju provode pouzdajuće strane trebala biti ograničena na ono što je nužno za predviđenu upotrebu. Korisnika lisnice trebalo bi uz zahtjev za otkrivanje jasnim i razumljivim jezikom obavijestiti o predviđenoj upotrebi. Kako bi se osjetljivost biometrijskih podataka primjereno uvažila, korisnik lisnice trebao bi posebno i izričito potvrditi otkrivanje portreta. Izostanak korisnikove radnje ili unaprijed označene kućice ne bi se trebale smatrati korisnikovom potvrdom. Izričita potvrda korisnika lisnice trebala bi biti tehnička zaštitna mjera, a ne sama po sebi činiti pravnu osnovu za obradu. Kako je utvrđeno u članku 9. stavku 4. Uredbe (EU) 2016/679, države članice mogu zadržati ili uvesti dodatne uvjete, uključujući ograničenja s obzirom na obradu genetskih podataka, biometrijskih podataka ili podataka koji se odnose na zdravlje.

(3) Kako bi države članice imale dovoljno vremena za prilagodbu nacionalnih procedura, portret korisnika lisnice može biti dio obveznih osobnih identifikacijskih podataka za fizičke osobe od 11. kolovoza 2028. Ako se ti prikazi uzimaju iz postojećih osobnih isprava, kao što su osobne iskaznice ili putovnice, primjenjuju se relevantni zahtjevi iz uredbi Vijeća (EU) 2025/1208 ([8]) odnosno (EZ) br. 2252/2004 ([9]).

(4) Prema Uredbi (EU) br. 910/2014 lisnice moraju moći prikazivati EU znak pouzdanosti lisnice za digitalni identitet kao provjerljivu, jednostavnu i prepoznatljivu oznaku da je lisnica stavljena na raspolaganje u skladu s tom uredbom. Primjena takvog znaka pouzdanosti pridonijet će učinkovitom funkcioniranju unutarnjeg tržišta, zajamčiti pravedno tržišno natjecanje i zaštititi interese potrošača. Da bi se on mogao upotrebljavati, trebalo bi utvrditi njegove vizualne i tehničke karakteristike.

(5) Kako je utvrđeno u članku 12.b Uredbe (EU) br. 910/2014, nadzornici pristupa moraju pružateljima europskih lisnica za digitalni identitet i izdavateljima prijavljenih sredstava elektroničke identifikacije dopustiti djelotvornu interoperabilnost s istim značajkama operativnog sustava, hardvera ili softvera i pristup tim značajkama u svrhu interoperabilnosti. Takva djelotvorna interoperabilnost i pristup moraju biti besplatni i nezavisni od toga jesu li te hardverske ili softverske značajke dio operativnog sustava, jesu li dostupne tom nadzorniku pristupa ili koristi li ih taj nadzornik pristupa kad pruža te usluge. Budući da bi sve izvedbe lisnice trebale podržavati zajednički skup protokola i sučelja kako bi se zajamčile upotrebljivost, sigurnost i interoperabilnost u svim državama članicama, nadzornici pristupa trebali bi omogućiti značajke operativnog sustava, hardvera ili softvera potrebne za provedbu protokola i sučelja utvrđenih u Prilogu XII. ovoj Uredbi. U tom kontekstu, u internetskim međuuređajnim (*cross-device*) tokovima, i za provjeru fizičke blizine i za prijenos podataka između dva uređaja, nadzornici pristupa trebali bi prednost dati lokalnom komunikacijskom kanalu prema specifikaciji Client To Authenticator Protocol (CTAP), verzija 2.3. ([10]), a ne CTAP-ovu hibridnom tunelu.

(6) Kako bi se državama članicama, pružateljima registracijskih certifikata pouzdajuće strane lisnice i pružateljima lisnice dalo dovoljno vremena da omoguće da jedinice lisnice autentificiraju i validiraju registracijske certifikate pouzdajuće strane lisnice, taj bi se zahtjev trebao primjenjivati tek od 11. kolovoza 2028.

(7) Na sve aktivnosti obrade osobnih podataka na temelju ove Uredbe primjenjuju se Uredba (EU) 2016/679 Europskog parlamenta i Vijeća ([11]) i, prema potrebi, Direktiva 2002/58/EZ Europskog parlamenta i Vijeća.

([7]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Uredba Vijeća (EU) 2025/1208 od 12. lipnja 2025. o jačanju sigurnosti osobnih iskaznica građana Unije i boravišnih isprava koje se izdaju građanima Unije i članovima njihovih obitelji koji ostvaruju pravo na slobodno kretanje (SL L, 2025/1208, 20.6.2025., ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Uredba Vijeća (EZ) br. 2252/2004 od 13. prosinca 2004. o standardima za sigurnosna obilježja i biometrijske podatke u putovnicama i putnim ispravama koje izdaju države članice (SL L 385, 29.12.2004., str. 1., ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Prijedlog norme organizacije FIDO Alliance, Client to Authenticator Protocol (CTAP), 26. veljače 2026.

([11]) Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([12]) te je on dao mišljenje 17. travnja 2026 ([13]).

(9) Mjere predviđene u ovoj Uredbi u skladu su s mišljenjem Odbora osnovanog člankom 48. Uredbe (EU) br. 910/2014,

DONIJELA JE OVU UREDBU:

Članak 1.

Izmjene Provedbene uredbe (EU) 2024/2977

Provedbena uredba (EU) 2024/2977 mijenja se kako slijedi:

(1) umeće se sljedeći članak 3.a:

„*Članak 3.a*

Zaštita portreta

1. „Uz poštovanje zahtjeva iz Uredbe (EU) 2016/679 koji se odnose na informacije, pružatelji lisnice osiguravaju da izvedbe lisnice koje pružaju korisnicima lisnice daju upozorenja kad pouzdajuće strane lisnice zahtijevaju otkrivanje portreta u kojima se navodi da taj zahtjev uključuje dijeljenje biometrijskih podataka i da je za njega potrebno odobrenje za selektivno otkrivanje portreta.

2. U svrhu primjene selektivnog otkrivanja portreta pouzdajućoj strani lisnice pružatelji lisnice osiguravaju da izvedbe lisnice od korisnika lisnice zahtijevaju da izričito i posebno potvrdi prikaz portreta.

3. Pouzdajuće strane lisnice ne smiju zadržati portret osim ako je njegova obrada potrebna u svrhu identifikacije i autentifikacije u skladu s pravom Unije o zaštiti podataka ili ako je to propisano pravom Unije ili nacionalnim pravom u skladu s pravom Unije o zaštiti podataka. Portret se ne smije prenositi trećim zemljama ili međunarodnim organizacijama osim ako je to dopušteno pravom Unije o zaštiti podataka.”;

(2) u članku 4. stavak 1. zamjenjuje se sljedećim:

„1. Elektroničke potvrde atributa koje se izdaju jedinicama lisnice moraju biti u skladu s najmanje jednom od normi utvrđenih u Prilogu II. Provedbenoj uredbi (EU) 2024/2979.”;

(3) u članku 5. stavku 4. točka (b) zamjenjuje se sljedećim:

„(b) ako je jedinici lisnice kojoj su izdani osobni identifikacijski podaci opozvana potvrda jedinice lisnice;”;

(4) Prilog se zamjenjuje tekstom iz Priloga I. ovoj Uredbi.

([12]) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) Službene primjedbe Europskog nadzornika za zaštitu podataka na nacrt provedbene uredbe u pogledu mjerodavnih normi i specifikacija za registraciju pouzdajućih strana lisnice te ispravku Provedbene uredbe (EU) 2024/2980 | Europski nadzornik za zaštitu podataka.

Članak 2.

Izmjene Provedbene uredbe (EU) 2024/2979

Provedbena uredba (EU) 2024/2979 mijenja se kako slijedi:

(1) u članku 3. briše se stavak 2.;

(2) u članku 5. stavku 1. točka (a) zamjenjuje se sljedećim:

„(a) izvršavaju kriptografske operacije lisnice u kojima se koriste ključni resursi koji su pohranjeni u sigurni kriptografski uređaj lisnice i nisu potrebni za autentifikaciju korisnika lisnice samo u slučajevima kad su te aplikacije uspješno autentificirale korisnike lisnice”;

(3) umeće se sljedeći članak 5.a:

„*Članak 5.a*

Kriptografski mehanizmi

Pružatelji lisnice za potrebe članka 4. stavka 2. koriste samo kriptografske mehanizme iz Priloga I.a.”;

(4) članak 6. mijenja se kako slijedi:

(a) stavak 1. zamjenjuje se sljedećim:

„1. Pružatelji lisnice izdaju potvrde jedinice lisnice za svaku jedinicu lisnice. Pružatelji lisnice potpisuju ili pečate potvrde jedinice lisnice tako da se potpisi ili pečati mogu validirati certifikatom navedenim u skladu s odjeljkom 2. točkom 1. podtočkom (h) Priloga II. Provedbenoj uredbi (EU) 2024/2980.”;

(b) stavak 2. zamjenjuje se sljedećim:

„2. Pružatelji lisnica osiguravaju da potvrde jedinice lisnice iz stavka 1. odgovaraju tehničkim specifikacijama iz Priloga I.b.”;

(c) u stavku 3. točka (b) zamjenjuje se sljedećim:

„(b) korisnicima lisnice staviti na raspolaganje mehanizme za sigurnu identifikaciju i autentifikaciju koji su neovisni o jedinicama lisnice”;

(5) u članku 9. stavku 2. točka (b) zamjenjuje se sljedećim:

„(b) ime, podatke za kontakt i jedinstveni identifikator odgovarajuće pouzdajuće strane lisnice te državu članicu u kojoj ta strana ima poslovni nastan;”;

(6) u članku 10. stavak 1. zamjenjuje se sljedećim:

„1. Pružatelji lisnice osiguravaju da jedinice lisnice koje su stavili na raspolaganje mogu obrađivati elektroničke potvrde atributa izdane u skladu s tehničkim specifikacijama koje vrijede za zajedničke ugrađene politike otkrivanja iz Priloga III.”;

(7) članak 12. mijenja se kako slijedi:

(a) u stavku 2. točka (c) zamjenjuje se sljedećim:

„(c) izrada potpisa ili pečata barem u obveznim formatima potpisa ili pečata iz Priloga IV.;”;

(b) stavak 3. zamjenjuje se sljedećim:

„3. Aplikacije za izradu potpisa mogu biti integrirane u instance lisnice ili se nalaziti izvan njih.”;

(c) umeće se sljedeći stavak:

„4. Aplikacije za izradu potpisa koje koriste jedinice lisnice moraju podržavati barem aplikacijsko programsko sučelje iz Priloga IV.”;

(8) u članku 14. briše se stavak 1.;

(9) umeće se sljedeći članak 14.a:

„*Članak 14.a*

EU znak pouzdanosti lisnice za digitalni identitet

1. Pružatelji lisnice osiguravaju da jedinice lisnice prikazuju EU znak pouzdanosti lisnice za digitalni identitet. EU znak pouzdanosti lisnice za digitalni identitet mora imati oblik utvrđen u prilozima VI. i VII.

2. Pružatelji lisnice osiguravaju da jedinice lisnice korisnicima lisnice dopuštaju pristup informacijama koje im omogućuju provjeru certifikacijskog statusa izvedbe lisnice. U tu svrhu pružatelji lisnice osiguravaju, nakon registracije izvedbe lisnice, da odgovarajuće jedinice lisnice sadržavaju URL-ove koje je za tu provjeru dala Europska komisija. Pružatelji lisnice osiguravaju da njihove jedinice lisnice imaju pristup podacima EU znaka pouzdanosti lisnice za digitalni identitet koji su u skladu s tehničkim specifikacijama iz Priloga VIII.

3. Referentne boje EU znaka pouzdanosti lisnice za digitalni identitet su Pantone br. 661 i 116, odnosno plava (100 % cijan + 67 % magenta + 0 % žuta + 40 % crna) i žuta (0 % cijan + 20 % magenta + 100 % žuta + 0 % crna) ako se koristi četverobojni postupak ili plava (0 crvena + 51 zelena + 153 plava) i žuta (255 crvena + 204 zelena + 0 plava) ako se koristi model boja RGB.

4. Crno-bijeli EU znak pouzdanosti lisnice za digitalni identitet kako je utvrđen u Prilogu VII. smije se koristiti samo kad nije moguće upotrijebiti boju.

5. Ako se EU znak pouzdanosti lisnice za digitalni identitet aplicira na tamnu podlogu, može se aplicirati u negativu s istom bojom podloge. Ako je slabije vidljiv kad je apliciran u boji na obojenu podlogu, smije mu se dodati obrub kako bi se poboljšao kontrast u odnosu na boje podloge.

6. Minimalne dimenzije EU znaka pouzdanosti lisnice za digitalni identitet su 64 × 85 piksela pri 150 dpi.

7. Pružatelji lisnice osiguravaju da se EU znak pouzdanosti lisnice za digitalni identitet upotrebljava tako da omogućuje jasno prepoznavanje jedinice lisnice na koju se odnosi. Može ga se povezati s grafičkim ili tekstualnim elementima koji jasno označavaju jedinicu lisnice za koju se upotrebljava ako oni ne mijenjaju njegovu prepoznatljivost kao EU znaka pouzdanosti lisnice za digitalni identitet ni vezu s popisom certificiranih europskih lisnica za digitalni identitet iz članka 5.d Uredbe (EU) br. 910/2014.

8. Ako pružatelji lisnice opozovu potvrdu jedinice lisnice, moraju osigurati da odgovarajuća jedinica lisnice više ne prikazuje EU znak pouzdanosti lisnice za digitalni identitet.”;

(10) Prilozi I.a i I.b dodaju se kako je utvrđeno u prilozima II. i III. ovoj Uredbi;

(11) Prilog II. zamjenjuje se Prilogom IV. ovoj Uredbi;

(12) Prilog III. zamjenjuje se Prilogom V. ovoj Uredbi;

(13) Prilog IV. mijenja se u skladu s Prilogom VI. ovoj Uredbi;

(14) Prilog V. briše se;

(15) tekst u Prilogu VII. ovoj Uredbi umeće se kao Prilog VI.;

(16) tekst u Prilogu VIII. ovoj Uredbi umeće se kao Prilog VII.;

(17) tekst u Prilogu IX. ovoj Uredbi umeće se kao Prilog VIII.

Članak 3.

Izmjene Provedbene uredbe (EU) 2024/2980

Provedbena uredba Komisije (EU) 2024/2980 mijenja se kako slijedi:

1. u članku 5. stavak 2. zamjenjuje se sljedećim:

„2. Komisija prema potrebi sastavlja, vodi i objavljuje popis informacija koje države članice dostave o pružateljima lisnice, pružateljima osobnih identifikacijskih podataka, pružateljima pristupnih certifikata pouzdajuće strane lisnice i pružateljima registracijskih certifikata pouzdajućih strana lisnice kako je navedeno u odjeljcima 2., 3., 4. i 5. Priloga II.";

2. Prilog II. Provedbenoj uredbi (EU) 2024/2980 mijenja se kako je navedeno u Prilogu X. ovoj Uredbi.

Članak 4.

Izmjene Provedbene uredbe (EU) 2024/2982

Provedbena uredba (EU) 2024/2982 mijenja se kako slijedi:

(1) u članku 1. stavak 2. zamjenjuje se sljedećim:

„2. predočavanje atributa osobnih identifikacijskih podataka i elektroničkih potvrda atributa pouzdajućim stranama lisnice;";

(2) članak 3. mijenja se kako slijedi:

(a) stavak 1. zamjenjuje se sljedećim:

„1. autentificiraju i validiraju pristupne certifikate pouzdajućih strana lisnice pri interakciji s njima, a da izvršavanje tih procesa ne delegiraju pregledniku koji je dio operativnog sustava ili nekoj drugoj aplikaciji koja bi služila kao posrednik;";

(b) stavak 2. briše se;

(c) stavak 3. zamjenjuje se sljedećim:

„3. autentificiraju i validiraju zahtjeve podnesene pomoću pristupnih certifikata pouzdajućih strana lisnice;";

(d) stavak 4. zamjenjuje se sljedećim:

„4. autentificiraju i validiraju registracijski certifikat pouzdajuće strane lisnice;";

(e) stavak 5. zamjenjuje se sljedećim:

„5. korisnicima lisnice prikazuju informacije iz pristupnih certifikata pouzdajuće strane lisnice;";

(f) stavak 8. briše se;

(g) stavak 9. zamjenjuje se sljedećim:

„9. pouzdajućim stranama lisnice ne predočuju zatražene atribute ako nisu završeni sljedeći koraci:

(a) provjera da su u jedinici lisnice obrađene ugrađene politike otkrivanja u skladu s člankom 10. Provedbene uredbe (EU) 2024/2979;

(b) provjera da su korisnici lisnice djelomično ili u cijelosti odobrili predočenje.";

(3) u članku 4. stavak 1. zamjenjuje se sljedećim:

„1. Pružatelji lisnice osiguravaju da izvedbe lisnice podržavaju protokole i sučelja iz Priloga I. za izdavanje osobnih identifikacijskih podataka i elektroničkih potvrda atributa jedinicama lisnice.";

(4) članak 5. mijenja se kako slijedi:

(a) stavci 1. i 2. zamjenjuju se sljedećim:

„1. Pružatelji lisnice osiguravaju da izvedbe lisnice podržavaju protokole i sučelja za predočavanje atributa pouzdajućim stranama lisnice, na daljinu i, prema potrebi, u blizini, u skladu s tehničkim specifikacijama iz Priloga II.

2. Pružatelji lisnice osiguravaju da na zahtjev korisnika jedinice lisnice odgovaraju na uspješno autentificirane i validirane zahtjeve pouzdajućih strana lisnice iz članka 3., u skladu s tehničkim specifikacijama iz Priloga II.”;

(b) stavak 5. briše se.;

(5) članak 8. zamjenjuje se sljedećim:

„*Članak 8.*

Stupanje na snagu

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Članak 3. stavak 4. primjenjuje se od 11. kolovoza 2028.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.”;

(6) Prilog se briše;

(7) tekst u Prilogu XI. ovoj Uredbi dodaje se kao Prilog I.;

(8) tekst u Prilogu XII. ovoj Uredbi dodaje se kao Prilog II.

Članak 5.

Stupanje na snagu

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 15. srpnja 2026.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

PRILOG I.

„PRILOG

Tehničke specifikacije za osobne identifikacijske podatke iz članka 3. stavka 3.

(1) Odjeljak 1.: Skup osobnih identifikacijskih podataka za fizičke osobe

Tablica 1

Obvezni osobni identifikacijski podaci o fizičkoj osobi za selektivno otkrivanje

Identifikacijska oznaka podatka	Definicija
`family_name`	Sadašnje prezime (prezimena) korisnika na kojeg se odnose osobni identifikacijski podaci.
`given_name`	Sadašnje ime (imena) korisnika na kojeg se odnose osobni identifikacijski podaci, uključujući srednje ime (srednja imena) ako je to primjenjivo.
`birth_date`	Dan, mjesec i godina rođenja korisnika na kojeg se odnose osobni identifikacijski podaci.
`birth_place`	Zemlja navedena kao alpha-2 oznaka zemlje prema normi ISO 3166-1 ili država, pokrajina, okrug ili lokalno područje ili općina, grad, mjesto ili selo u kojem je rođen korisnik na kojeg se odnose osobni identifikacijski podaci.
`nationality`	Jedna ili više alpha-2 oznaka zemlje prema normi ISO 3166-1 koje predstavljaju državljanstvo korisnika na kojeg se odnose osobni identifikacijski podaci.
`portrait`	Osim ako korisnik izričito odbije njegovo uključivanje, prikaz lica korisnika na kojeg se odnose osobni identifikacijski podaci koji mora ispunjavati zahtjeve kvalitete za potpunu frontalnu snimku iz norme ISO/IEC 39794-5 ili, radi povratne kompatibilnosti, točaka 8.2., 8.3. i 8.4. norme ISO/IEC 19794-5 i davati u enkodiranom obliku bez zaglavlja ili blokova prema točki 5. te norme, ali s uključenim samim slikovnim podacima (JPEG), primjenjuje se od 11. kolovoza 2028.

— Države članice mogu odrediti da korisnik ima mogućnost odbiti uključivanje portreta u osobne identifikacijske podatke.

— Države članice osiguravaju da se selektivno otkrivanje primjenjuje na svaku identifikacijsku oznaku podataka, uključujući portret.

— Ako nije poznat datum rođenja fizičke osobe, države članice odabiru odgovarajuće vrijednosti sukladne sa specifikacijama iz odjeljka 4.1. ili 4.2. (ovisno o slučaju) ovog Priloga.

— Ako nije poznato državljanstvo fizičke osobe, države članice upotrebljavaju vrijednost „QU”.

— Ako fizička osoba nema državljanstvo, države članice upotrebljavaju vrijednost „QS”.

— Ako korisnik odbije uključivanje portreta, države članice vrijednost ostavljaju praznom.

Tablica 2

Neobvezni osobni identifikacijski podaci o fizičkoj osobi za selektivno otkrivanje

Identifikacijska oznaka podatka	Definicija
resident_address	Potpuna adresa na kojoj korisnik na kojeg se odnose osobni identifikacijski podaci trenutačno boravi ili na kojoj se s njime može stupiti u kontakt (ime ulice, kućni broj, mjesto itd.).
resident_country	Zemlja u kojoj trenutačno boravi korisnik na kojeg se odnose osobni identifikacijski podaci, navedena kao alpha-2 oznaka zemlje prema normi ISO 3166-1.
resident_state	Savezna zemlja, pokrajina, okrug ili lokalno područje gdje trenutačno boravi korisnik na kojeg se odnose osobni identifikacijski podaci.
resident_city	Općina, grad, mjesto ili selo gdje trenutačno boravi korisnik na kojeg se odnose osobni identifikacijski podaci.
resident_postal_code	Poštanski broj mjesta u kojem trenutačno boravi korisnik na kojeg se odnose osobni identifikacijski podaci.
resident_street	Ime ulice u kojoj trenutačno boravi korisnik na kojeg se odnose osobni identifikacijski podaci, uključujući kućni broj i eventualne dodatke broju.
personal_administrative_-number	Vrijednost koja je dodijeljena korisniku na kojeg se odnose osobni identifikacijski podaci i različita od svih drugih osobnih administrativnih brojeva koje je izdao pružatelj osobnih identifikacijskih podataka. Ako države članice odluče uključiti taj atribut, u svojim sustavima elektroničke identifikacije u okviru kojih se izdaju osobni identifikacijski podaci moraju opisati politiku koju primjenjuju na njegove vrijednosti, uključujući, prema potrebi, posebne uvjete za obradu te vrijednosti.
family_name_birth	Prezime (prezimena) korisnika na kojeg se odnose osobni identifikacijski podaci u trenutku rođenja.
given_name_birth	Ime (imena), uključujući srednje ime (imena), korisnika na kojeg se odnose osobni identifikacijski podaci u trenutku rođenja.
sex	Navodi se jedna od sljedećih vrijednosti: 0 = nepoznat; 1 = muški; 2 = ženski; 3 = drugi; 4 = inter; 5 = raznolik; 6 = otvoren; 9 = ne primjenjuje se. Za vrijednosti 0, 1, 2 i 9 primjenjuje se ISO/IEC 5218.
email_address	Adresa elektroničke pošte korisnika na kojeg se odnose osobni identifikacijski podaci [u skladu s normom RFC 5322 ([1])]

Identifikacijska oznaka podatka	Definicija
`mobile_phone_number`	Broj mobilnog telefona korisnika na kojeg se odnose osobni identifikacijski podaci, koji započinje znakom „+” kao međunarodnim prefiksom i pozivnim brojem zemlje, nakon čega slijede samo brojke.

([1]) P. Resnick, ur., *Internet Message Format*, RFC 5322, listopad 2008.

(2) Odjeljak 2.: Skup osobnih identifikacijskih podataka za pravne osobe

Tablica 3

Obvezni osobni identifikacijski podaci za pravnu osobu

Identifikacijska oznaka podatka
Sadašnje ime pravne osobe
Jedinstveni identifikator koji izrađuje država članica pošiljateljica u skladu s tehničkim specifikacijama za potrebe prekogranične identifikacije i koji mora biti što je moguće trajniji.

— Ako identifikacijska oznaka podatka za osobu nije poznata ili se iz nekog drugog razloga ne može izdati kao dio skupa osobnih identifikacijskih podataka, države članice umjesto njega navode vrijednost atributa primjerenu situaciji.

Tablica 4

Neobvezni osobni identifikacijski podaci za pravnu osobu

Identifikacijska oznaka podatka
Sadašnja adresa
PDV identifikacijski broj
Referentni porezni broj
Europski jedinstveni identifikator iz Direktive (EU) 2017/1132 Europskog parlamenta i Vijeća ([1])
Identifikacijska oznaka pravne osobe (LEI) iz Provedbene uredbe Komisije (EU) 2022/1860 ([2])
Registracijski i identifikacijski broj gospodarskog subjekta (EORI) iz Provedbene uredbe Komisije (EU) br. 1352/2013 ([3])
Broj trošarine iz članka 2. stavka 12. Uredbe Vijeća (EU) br. 389/2012 ([4])

([1]) Direktiva (EU) 2017/1132 Europskog parlamenta i Vijeća od 14. lipnja 2017. o određenim aspektima prava društava (SL L 169, 30.6.2017., str. 46., ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Provedbena uredba Komisije (EU) 2022/1860 od 10. lipnja 2022. o utvrđivanju provedbenih tehničkih standarda za primjenu Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća u pogledu standarda, formata, učestalosti te metoda i mehanizama za izvješćivanje (SL L 262, 7.10.2022., str. 68., ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Provedbena uredba Komisije (EU) br. 1352/2013 od 4. prosinca 2013. o uspostavi obrazaca utvrđenih Uredbom (EU) br. 608/2013 Europskog parlamenta i Vijeća o carinskoj provedbi prava intelektualnog vlasništva (SL L 341, 18.12.2013., str. 10., ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Uredba Vijeća (EU) br. 389/2012 od 2. svibnja 2012. o upravnoj suradnji u području trošarina i stavljanju izvan snage Uredbe (EZ) br. 2073/2004 (SL L 121, 8.5.2012., str. 1., ELI: http://data.europa.eu/eli/reg/2012/389/oj).

(3) Odjeljak 3.: Skup metapodataka o osobnim identifikacijskim podacima

Tablica 5

Metapodaci o osobnim identifikacijskim podacima

Identifikacijska oznaka podatka	Definicija	Korištenje
`issuing_authority`	Ime upravnog tijela koje je izdalo osobne identifikacijske podatke ili, ako ne postoji zasebno tijelo ovlašteno za izdavanje osobnih identifikacijskih podataka, alpha-2 oznaka zemlje prema normi ISO 3166 za dotičnu državu članicu.	Obvezno
`issuing_country`	Alpha-2 oznaka zemlje prema normi ISO 3166-1 za zemlju ili državno područje pružatelja osobnih identifikacijskih podataka.	Obvezno
`expiry_date`	Datum (i, ako je moguće, vrijeme) isteka razdoblja upravne valjanosti osobnih identifikacijskih podataka.	Neobvezno
`document_number`	Broj koji osobnim identifikacijskim podacima dodjeljuje pružatelj tih podataka.	Neobvezno
`issuing_jurisdiction`	Oznaka potpodjele države za jurisdikciju koja je izdala osobne identifikacijske podatke, kako je utvrđeno u točki 8. norme ISO 3166-2:2020. Prvi dio oznake mora biti jednak vrijednosti za zemlju izdavanja.	Neobvezno
`issuance_date`	Datum (i, ako je moguće, vrijeme) početka razdoblja upravne valjanosti osobnih identifikacijskih podataka.	Neobvezno

(4) Odjeljak 4.: Enkodiranje atributa identifikacijskih podataka fizičke osobe

— Identifikacijski podaci fizičke osobe izdaju se u skladu s normama utvrđenima u točkama 5. (format SD-JWT VC) i 6. (format ISO/IEC-mdoc) Priloga II. Provedbenoj uredbi (EU) 2024/2979 kako se primjenjuju na elektroničke potvrde atributa. Ne primjenjuju se točke 5.2.2., 5.2.4., 5.2.5., EAA-6.1-03, 6.2.2., 6.2.3., 6.2.4. i 6.2.5.

— Enkodiranje identifikacijskih podataka fizičke osobe mora biti sukladno s tehničkim specifikacijama iz odjeljaka 4.1. i 4.2. ovog Priloga.

4.1. Enkodiranje identifikacijskih podataka fizičke osobe u formatu ISO/IEC-mdoc

— Vrsta potvrde za identifikacijske podatke fizičke osobe u formatu ISO/IEC-mdoc mora biti „eu.europa.ec.eudi.pid.1”. Identifikator imenskog prostora za atribute osobnih identifikacijskih podataka utvrđene u ovom Prilogu mora biti „eu.europa.ec.eudi.pid.1”.

— Ako osobni identifikacijski podaci sadržavaju podatke za koje identifikacijske oznake nisu utvrđene u ovom Prilogu, ti se podaci moraju definirati u domaćem imenskom prostoru osobnih identifikacijskih podataka koji koristi opći format eu.europa.ec.eudi.pid. (alpha-2 oznaka zemlje prema ISO 3166-1ili oznaka regije prema ISO 3166-2), a zatim mogu slijediti neobvezna točka i broj verzije.

— Ako se upotrebljava domaći imenski prostor, njegova struktura, uključujući sve identifikacijske oznake podataka, njihove definicije, obveznost i formate enkodiranja, mora se objaviti u skladu s člankom 8. Provedbene uredbe Komisije (EU) 2025/1569 ([1]).

— Osobni identifikacijski podaci i njihovi metapodaci utvrđeni u odjeljcima 1. i 3. ovog Priloga moraju biti dio elemenata osobnih identifikacijskih podataka u smislu specifikacija formata ISO/IEC mdoc.

— Član deviceKey unutar člana deviceKeyInfo u instanci tipa MobileSecurityObject mora sadržavati javni ključ.

— Taj javni ključ mora odgovarati privatnom ključu pohranjenom na sigurnom kriptografskom uređaju lisnice (WSCD) korisnika lisnice.

— Zaštićeno zaglavlje CB-AdES digitalnog potpisa koji potpisuje osobne identifikacijske podatke u formatu ISO/IEC-mdoc mora sadržavati parametre zaglavlja x5u i x5t, oba specificirana u normi RFC 9360 ([2]).

— Algoritam za izračunavanje sažetka u parametru zaglavlja x5t mora biti SHA-256.

— Zahtjevi za enkodiranje osobnih identifikacijskih podataka u formatu ISO/IEC-mdoc utvrđeni su u tablici 6:

Tablica 6

Zahtjevi za enkodiranje osobnih identifikacijskih podataka u formatu ISO/IEC-mdoc

Identifikacijska oznaka podatka	Identifikacijska oznaka atributa	Format enkodiranja
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]) Provedbena uredba Komisije (EU) 2025/1569 od 29. srpnja 2025. o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu kvalificiranih elektroničkih potvrda atributa i elektroničkih potvrda atributa koje izdaje tijelo javnog sektora odgovorno za autentični izvor ili koje se izdaju u njegovo ime (SL L, 2025/1569, 30.7.2025., ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([2]) J. Schaad, *CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates* (https://datatracker.ietf.org/doc/rfc9360/).

Identifikacijska oznaka podatka	Identifikacijska oznaka atributa	Format enkodiranja
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate ili 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 ili full-date

— Sustav zapisivanja formata enkodiranja atributa iz tablice 6 mora koristiti reprezentacijske tipove specificirane u normi RFC 8610 ([3]), uz sljedeće dodatne zahtjeve:

(a) tstr se mora enkodirati u standardu UTF-8;

(b) tstr mora podržavati sve znakove sustava Unicode;

(c) tstr smije imati najviše 150 znakova;

(d) datum se mora enkodirati kako je specificirano u normi RFC 8943 ([4]);

(e) full-date se tumači kao #6.1004(tstr), pri čemu tag 1004 mora biti kako je specificiran u normi RFC 8943;

(f) atribut tdate mora sadržavati niz date-time kako je specificiran u normi RFC 3339 ([5]);

(g) atribut full-date mora sadržavati niz full-date kako je specificiran u normi RFC 3339, u skladu s RFC 8943;

(h) osim ako je drukčije navedeno, u reprezentaciji datuma u atributima:

— ne smiju se koristiti dijelovi sekunde;

— ne smije se koristiti lokalna razlika od UTC-a, a time-offset specificiran u normi RFC 3339 mora se postaviti na „Z”;

(i) cijeli broj s glavnim tipovima 0 i 1 mora biti što manji, kako je specificirano u odjeljku 4.2. norme RFC 8949 ([6]);

(j) place_of_birth mora sadržavati najmanje jedan od ovih parova ključ-vrijednost: „country”, „region” ili „locality”;

(k) izraz duljine u bstr, tstr, polju ili mapi mora biti što kraći, kako je specificirano u odjeljku 4.2. norme RFC 8949;

([3]) C. Vigano i H. Birkholz, *Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures*, RFC 8610, lipanj 2019.
([4]) M. Jones, A. Nadalin i J. Richter, *Concise Binary Object Representation (CBOR) Tags for Date*, RFC 8943, studeni 2020.
([5]) G. Klyne i C. Newman, *Date and Time on the Internet: Timestamps*, RFC 3339, srpanj 2002.
([6]) C. Vigano i H. Birkholz, *Concise Binary Object Representation (CBOR) Tags for Date*, RFC 8949, prosinac 2020.

(l) atribut nationality mora se enkodirati kao polje alfa-2 oznaka zemalja kako su navedene u normi ISO 3166-1. Ako se upotrebljava zapisivanje CDDL specificirano u normi RFC 8610, taj atribut mora biti:

— nationalities = [+ CountryCode],

— CountryCode = tstr; alpha-2 oznaka zemlje specificirana u ISO 3166-1,

— ako korisnik lisnice na kojeg se odnose osobni identifikacijski podaci ima više državljanstava i pružatelj osobnih identifikacijskih podataka potvrdi ta višestruka državljanstva, pružatelj osobnih identifikacijskih podataka može u osobne identifikacijske podatke uključiti sva državljanstva,

— atribut place_of_birth enkodira se kao tip place_of_birth. Ako se upotrebljava zapisivanje CDDL specificirano u normi RFC 8610, taj atribut mora biti:

place_of_birth =

{

? 'country': tstr; jedna alpha-2 oznaka zemlje specificirana u ISO 3166-1:

? 'region': tstr; ime savezne države, pokrajine, okruga ili lokalnog područja

? 'locality': tstr; ime općine, mjesta, grada ili sela

}

4.2. Zahtjevi za enkodiranje osobnih identifikacijskih podataka u formatu SD-JWT VC

— Osobni identifikacijski podaci i njihovi metapodaci specificirani u ovom odjeljku moraju se uključiti u osobne identifikacijske podatke kao tvrdnje u smislu specifikacija formata SD-JWT VC.

— Sve tvrdnje u izdanim osobnim identifikacijskim podacima iz prethodne alineje mora biti moguće selektivno pojedinačno otkriti, osim onih za koje je u formatu SD-JWT VC definirano da se mogu neselektivno otkrivati.

— U tablici 7. specificirano je enkodiranje imena tvrdnji koja su javna imena.

— U tablici 8. specificirano je enkodiranje naziva tvrdnji specifičnih za konkretne osobne identifikacijske podatke.

— JSON niz u osobnim identifikacijskim podacima enkodiranima u formatu SD-JWT VC mora se enkodirati u standardu UTF-8 i podržavati sve znakove sustava Unicode, osim ako je u tablici 8 u nastavku ili u upućivanjima u njoj izričito navedeno drukčije.

— JWT tvrdnje nbf i exp kako su definirane u normi RFC 7519 ([7]) služe za izražavanje razdoblja tehničke valjanosti osobnih identifikacijskih podataka prema formatu SD-JWT VC.

([7]) J. Jones, et al., *JSON Web Token (JWT)*, RFC 7519, svibanj 2015.

— Osobni identifikacijski podaci moraju obuhvaćati tvrdnju cnf, kako je definirana u normi RFC 7800 ([8]), koja mora biti javni ključ generiran iz privatnog ključa pohranjenog u WSCD-u jedinice lisnice korisnika lisnice.

— Zaštićeno zaglavlje digitalnog potpisa koji potpisuje osobne identifikacijske podatke u formatu SD-JWT VC mora sadržavati parametre zaglavlja x5u i x5t#S256, oba specificirana u normi RFC 7515 ([9]).

Tablica 7

Zahtjevi za enkodiranje osobnih identifikacijskih podataka u formatu SD-JWT VC kad se koriste javna imena

Identifikacijska oznaka podatka	Identifikacijska oznaka atributa	Format enkodiranja
`family_name`	`family_name`	niz
`given_name`	`given_name`	niz
`birth_date`	`birthdate`	niz, ISO 8601-1, format GGGG-MM-DD
`birth_place`	`place_of_birth`	JSON struktura
`nationality`	`nationalities`	polje nizova
`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 podataka koji sadržava portret u formatu JPEG enkodiran u Base64.

([8]) M. Jones, et al., *Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)*, RFC 7800, travanj 2016.
([9]) M. Jones, et al., *JSON Web Signature (JWS)*, RFC 7515, svibanj 2015.

Tablica 8

Zahtjevi za enkodiranje osobnih identifikacijskih podataka u formatu SD-JWT VC kad se koriste privatna imena

Identifikacijska oznaka podatka	Identifikacijska oznaka atributa	Format enkodiranja
`expiry_date`	`date_of_expiry`	niz, ISO 8601-1, format GGGG-MM-DD
`issuance_date`	`date_of_issuance`	niz, ISO 8601-1, format GGGG-MM-DD
`personal_administrative_number`	`personal_administrative_number`	niz
`sex`	`sex`	broj
`issuing_authority`	`issuing_authority`	niz
`issuing_country`	`issuing_country`	niz
`document_number`	`document_number`	niz
`issuing_jurisdiction`	`issuing_jurisdiction`	niz

— Osnovni tip osobnih identifikacijskih podataka je „urn:eudi:pid:1” i uključen je u tvrdnju vct. Svi osobni identifikacijski podaci moraju koristiti tipove u imenskom prostoru „urn:eudi:pid:”.

— Ako osobni identifikacijski podaci uključuju atribute koji nisu specificirani u ovom Prilogu, ti se atributi moraju definirati unutar domaćeg tipa.

— Ako se upotrebljava domaći tip, njegovu strukturu, uključujući sve identifikacijske oznake podataka, njihove definicije, obveznost i formate enkodiranja, mora se definirati u shemi koja se objavljuje u skladu s člankom 8. Provedbene uredbe (EU) 2025/1569.

(5) Odjeljak 5.: Pojedinosti o infrastrukturi povjerenja

Popis pružatelja osobnih identifikacijskih podataka koji Komisija stavlja na raspolaganje u skladu s Provedbenom uredbom (EU) 2024/2980 mora omogućivati autentifikaciju osobnih identifikacijskih podataka.”

PRILOG II.

„PRILOG I.a

Kriptografski mehanizmi iz članka 5.a

Europska skupina za kibernetičkosigurnosnu certifikaciju, podskupina za kriptografiju: „Dogovoreni kriptografski mehanizmi”, publikacija Agencije Europske unije za kibersigurnost („ENISA”) ([1]).”

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

PRILOG III.

„PRILOG I.b

Tehničke specifikacije za potvrde jedinice lisnice iz članka 6. stavka 2.a

(1) Potvrda jedinica lisnice obuhvaća jednu ili više potvrda instance lisnice i jednu ili više potvrda ključa.

(2) Potvrda instance lisnice i potvrde ključa moraju ispunjavati sljedeće zahtjeve:

(a) Zahtjevi za format

— FR-WIA-1: Potvrda instance lisnice mora biti JSON Web Token (JWT), kako je specificiran u normi RFC 7519 ([1]), koji je pružatelj lisnice potpisao ili zapečatio kompaktnim JAdES baseline B potpisom.

— FR-WIA-1.1: Potvrda instance lisnice mora biti potvrda lisnice kako je specificirana u Dodatku E specifikacije OpenID for Verifiable Credential Issuance v1.0 ([2]) („OID4VCI”) i proširena kako je navedeno u C-WIA-1 i C-WIA-2.

— FR-KA-1: Potvrda ključa mora biti JSON Web Token (JWT), kako je specificiran u normi RFC 7519, koji je pružatelj lisnice potpisao ili zapečatio kompaktnim JAdES baseline B potpisom.

— FR_KA_1.1: Potvrda ključa mora biti potvrda ključa specificirana u Dodatku D OID4VCI-ja i proširena kako je navedeno u C_KA-1 i C_KA-2.

(b) Zahtjevi za transport

— TR-WIA-1: Jedinica lisnice mora koristiti potvrdu jedinice lisnice tijekom izdavanja osobnih identifikacijskih podataka, kvalificiranih ili nekvalificiranih elektroničkih potvrda atributa ili elektroničkih potvrda atributa koje daje tijelo javnog sektora odgovorno za autentični izvor ili koje se daju u njegovo ime.

— TR-WIA-2: Pružatelj lisnice mora provjeriti cjelovitost instance lisnice i potpisati ili zapečatiti potvrdu instance lisnice.

— TR-WIA-2.1: Ako pružatelj lisnice izdaje potvrdu instance lisnice, razlika između vremena kad je pružatelj lisnice verificirao cjelovitost instance lisnice i vremena koje će navesti u parametru zaglavlja „exp” izdane potvrde instance lisnice mora biti manja od 24 sata.

— TR-WIA-2.2: Pružatelj lisnice mora osigurati da jedinica lisnice sadržava potvrde instance lisnice potrebne za izdavanje osobnih identifikacijskih podataka i elektroničkih potvrda atributa.

— TR-WIA-3: U procesu izdavanja jedinica lisnice mora poslati potvrdu instance lisnice autorizacijskom poslužitelju u direktnom zahtjevu za autorizaciju (*Pushed Authorisation Request*) i u zahtjevu za token, kako je specificirano u OID4VCI-ju.

— TR-WIA-3.1: Jedinica lisnice mora poslati potvrdu instance lisnice zajedno s dokazom posjedovanja („PoP”) kako je specificirano u Dodatku E OID4VCI-ju.

— TR-WIA-3.2: Jedinica lisnice smije poslati istu potvrdu instance lisnice na jedan autorizacijski poslužitelj.

([1]) RFC 7519: JSON Web Token (JWT), svibanj 2015.
([2]) OpenID for Verifiable Credential Issuance v1.0, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: Ako pružatelj lisnice koristi opciju „per-issuer reuse” specificiranu u točki R_WIA_1, jedinica lisnice može potvrdu instance lisnice više puta poslati istom autorizacijskom poslužitelju.

— TR-WIA-3.2.2: Ako pružatelj lisnice ne koristi opciju „per-issuer reuse”, jedinica lisnice smije iskoristiti potvrdu instance lisnice u najviše jednom procesu izdavanja.

— TR-WIA-4: Kad autorizacijski poslužitelj primi potvrdu instance lisnice, mora provjeriti potpis potvrde instance lisnice pomoću javnog ključa u potpisnom certifikatu koji je u parametru „x5c” JOSE zaglavlja potvrde instance lisnice.

— TR-WIA-4.1: Autorizacijski poslužitelj mora provjeriti i može li se taj potpisni certifikat provjeriti pomoću točke povjerenja s popisa pružatelja lisnice iz članka 5. Provedbene uredbe (EU) 2024/2980, potencijalno koristeći posredne certifikate u parametru x5c.

— TR-WIA-4.2: Autorizacijski poslužitelj mora provjeriti da potvrda instance lisnice nije istekla.

— TR-WIA-4.3: Autorizacijski poslužitelj mora provjeriti potpis PoP-a pomoću javnog ključa u tvrdnji „cnf”.

— TR_KA-1: Jedinica lisnice mora koristiti potvrdu ključa tijekom izdavanja osobnih identifikacijskih podataka i tijekom izdavanja elektroničkih potvrda atributa vezanih uz uređaj, bez obzira na to jesu li kvalificirane, nekvalificirane ili ih daje tijelo javnog sektora odgovorno za autentični izvor ili se daju u njegovo ime.

— TR_KA-1.1: Jedinica lisnice ne smije koristiti potvrdu ključa tijekom izdavanja elektroničkih potvrda atributa koje nisu vezane uz uređaj, bez obzira na to jesu li kvalificirane, nekvalificirane ili ih daje tijelo javnog sektora odgovorno za autentični izvor ili koje se daju u njegovo ime.

— TR_KA-2: Pružatelj lisnice stavlja na raspolaganje jedinicu lisnice s različitim potvrdama ključa za WSCD jedinice lisnice i za svaki njezin spremnik ključeva (keystore).

— TR_KA-2.1: Pružatelj lisnice mora potpisati ili pečatirati potvrdu ključa nakon što se uvjerio da su ključevi potvrđeni u potvrdi ključa pohranjeni na WSCD-u jedinice lisnice ili spremniku ključeva opisanom u potvrdi ključa.

— TR_KA-2.2: Potvrda ključa mora sadržavati barem jedan potvrđeni javni ključ. Broj ključeva u potvrdi ključa poslanoj izdavatelju vjerodajnica ne bi trebao premašiti maksimalnu veličinu skupa ključeva koju je taj izdavatelj odredio u svojim metapodacima o izdavatelju vjerodajnice; vidjeti ETSI TS 119 472-3 ([3]), parametar „credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size”.

— TR_KA-2.3: Pružatelj lisnice mora uključiti javni ključ (koji odgovara privatnom ključu pohranjenom u WSCD-u ili spremniku ključeva jedinice lisnice) u najmanje jednu potvrdu ključa.

— TR_KA-2.4: Jedinica lisnice smije koristiti jednu potvrdu ključa tijekom najviše jednog postupka izdavanja ili ponovnog izdavanja vjerodajnice.

— TR_KA-2.5: Pružatelj lisnice mora osigurati da jedinica lisnice posjeduje potvrde ključa potrebne za izdavanje osobnih identifikacijskih podataka i elektroničkih potvrda atributa vezanih uz uređaj.

([3]) ETSI, „Elektronički potpisi i infrastrukture (ESI); JAdES digitalni potpisi – 3. dio: JAdES razine i osnovni profili”, ETSI TS 119 472-3, V1.1.1, ožujak 2026.

— TR_KA-3: Ako je to potrebno tijekom izdavanja, jedinica lisnice mora uključiti potvrdu ključa u dokaz tipa „jwt” ili „attestation” u polje „proofs” zahtjeva za vjerodajnicu upućenog izdavatelju vjerodajnica, kako je specificirano u OID4VCI-ju.

— TR_KA_3.1: Ako jedinica lisnice uključuje potvrdu ključa u element „jwt”, potvrdu ključa mora potpisati ili zapečatiti pomoću privatnog ključa koji odgovara javnom ključu na indeksu 0 polja „attested_keys” unutar objekta „key_attestation”.

— TR_KA-4: Ako izdavatelj vjerodajnica izdaje vjerodajnice vezane uz uređaj, u parametru „proof_types_-supported” u metapodacima o izdavatelju vjerodajnice, kako su specificirani u odjeljku 12.2.4. OID4VCI-ja, navodi da podržava tipove dokaza „jwt” i „attestation” za potvrde ključa koje moraju uključivati objekt „key_attestations_required”.

— TR_KA-4.1: Ako izdavatelj vjerodajnica izdaje vjerodajnice koje nisu vezane uz uređaj, u metapodacima o izdavatelju vjerodajnica izostavlja parametre „proof_types_supported” i „cryptographic_binding_methods_supported”.

— TR_KA-5: Ako izdavatelj vjerodajnica primi potvrdu ključa u tipu dokaza „jwt” ili „attestation”, mora provjeriti potpis potvrde ključa pomoću javnog ključa u potpisnom certifikatu u parametru „x5c” u JOSE zaglavlju potvrde ključa i da je taj potpisni certifikat s točkom povjerenja na popisu pružatelja lisnice iz članka 5. Provedbene uredbe (EU) 2024/2980, potencijalno koristeći posredne certifikate u parametru „x5c”.

— TR_KA-6: Ako izdavatelj vjerodajnica primi potvrdu ključa u tipu dokaza „jwt”, mora provjeriti potpis elementa „jwt” pomoću ključa na indeksu 0 polja „attested_keys” unutar objekta „key_attestation” uključenog u element „jwt”.

— TR_KA-6.1: Izdavatelj vjerodajnica mora provjeriti da polje „nonce” elementa „jwt” sadržava valjani c_nonce od svojeg nonce_endpoint, kako je specificirano u OID4VCI-ju.

— TR_KA-7: Ako izdavatelj vjerodajnica primi potvrdu ključa u tipu dokaza „attestation”, mora provjeriti da objekt „key_attestation” sadržava valjan c_nonce od svojeg nonce_endpoint.

— TR_KA-8: Pružatelj osobnih identifikacijskih podataka mora osigurati da su osobni identifikacijski podaci vezani uz javni ključ koji potječe iz potvrde ključa u kojoj se navodi WSCD.

(c) Zahtjevi za sadržaj

— C_WIA-1: Potvrda instance lisnice mora sadržavati:

— tvrdnju „wallet_name” specificiranu u Dodatku E OID4VCI-ju, čija vrijednost mora biti identifikator izvedbe lisnice koji se može pronaći na popisu pružatelja lisnice iz članka 5. Provedbene uredbe (EU) 2024/2980,

— tvrdnju „wallet_version” ([4]), koja mora biti niz koji ima vrijednost verzije izvedbe lisnice,

— tvrdnju „wallet_solution_ certification_information”, koja mora biti JSON objekt s informacijama o tijelu za ocjenjivanje sukladnosti koje je certificiralo izvedbu lisnice, certifikacijskim brojem prema potrebi i drugim relevantnim pojedinostima o certifikaciji,

([4]) Ta je tvrdnja definirana u ovoj provedbenoj uredbi jer nije dio specifikacije OID4VCI-ja.

— tvrdnju „client_status” s dva potpolja:

— „status”: upućivanje na popis statusa kako je specificirano u Dodatku E OID4VCI-ju koje predstavlja status opoziva instance lisnice. Za pojedinosti vidjeti odjeljak (e),

— „exp”: NumericDate, kako je specificirano u RFC 7519, kojim se definira vrijeme do kojeg će pružatelj lisnice zadržati status opoziva na indeksu popisa statusa na koji upućuje „status”,

— tvrdnju „exp” specificiranu u Dodatku E OID4VCI-ju.

— *NAPOMENA:* Tvrdnja „client_status.status” u potvrdi instance lisnice predstavlja status opoziva instance lisnice, a ne status opoziva same potvrde. Kako je opisano u R_WIA-1, pružatelj lisnice može odlučiti vezati svaku instancu lisnice uz specifični autorizacijski poslužitelj na temelju činjenice da sve potvrde poslane na taj poslužitelj sadržavaju istu vrijednost indeksa u unosu „client_status.status”.

— *NAPOMENA:* Vrijednost „idx” u tvrdnji „status” može se upotrijebiti kao jedinstveni (za svaki par) identifikator instance lisnice i jedinice lisnice.

— C_WIA-2: Potvrda instance lisnice trebala bi uključivati i tvrdnju „wallet_link” specificiranu u Dodatku E OID4VCI-ju, a vrijednost te tvrdnje mora biti URI na kojem se mogu dobiti dodatne informacije o izvedbi lisnice.

— C_WIA-3: Autorizacijski poslužitelj ne smije tumačiti parametar „exp” na najvišoj razini potvrde instance lisnice kao kraj razdoblja održavanja opoziva instance lisnice.

— *NAPOMENA:* Parametar „exp” na najvišoj razini potvrde instance lisnice označava datum isteka same potvrde.

— C_KA-1: Potvrda ključa mora sadržavati:

— tvrdnje „key_storage” i „user_authentication” specificirane u Dodatku D OID4VCI-ju,

— atributi „key_storage” i „user_authentication” moraju imati vrijednost „iso_18045_high” ako se u potvrdi ključa spominje WSCD,

— tvrdnju „certification” specificiranu u Dodatku D OID4VCI-ju koja sadržava URL na kojem se mogu dobiti informacije o certifikaciji postignutoj WSCD-om ili spremnikom ključeva, među ostalim sustav kao što je Common Criteria ili GlobalPlatform, evaluirane zahtjeve kao što je primjenjivi profil zaštite i razinu evaluacije.

— Iz tih informacija mora biti moguće ustanoviti je li spremnik ključeva WSCD,

— tvrdnju „key_storage_status” s dva potpolja:

— „status”: upućivanje na popis statusa kako je specificiran u Dodatku D.1 OID4VCI-ju, Vrijednost predstavlja status opoziva WSCD-a ili tipa spremnika ključeva koji služi za pohranu potvrđenih ključeva ili, kad se koristi opcija per-key-attestation index, status opoziva WSCD-a ili spremnika ključeva pojedinačne jedinice lisnice. Više o dostupnim opcijama za dodjelu indeksa vidjeti u R_KA_1,

— „exp”: NumericDate, kako je specificirano u RFC 7519, kojim se definira vrijeme do kojeg će pružatelj lisnice zadržati status opoziva na indeksu popisa statusa na koji upućuje „status”,

— tvrdnju „exp” kako je specificirana u Dodatku D OID4VCI-ju.

— *NAPOMENA* o vrijednosti „idx” u tvrdnji „key_storage_status.status u potvrdi ključa: Ako pružatelj lisnice koristi opciju „type-shared index” (vidjeti R_KA_1), sve potvrde ključa za isti tip WSCD-a ili spremnika ključeva dijele isti indeks popisa statusa. Stoga vrijednost „idx” nije jedinstvena po jedinici lisnice. Nasuprot tome, ako pružatelj lisnice koristi opciju „per-key-attestation index”, vrijednost „idx” jedinstvena je za jedinicu lisnice (ili za svaki par). Izdavatelj vjerodajnica, međutim, ni u kojem slučaju ne smije koristiti vrijednost „idx” u potvrdi ključa kao identifikator jedinice lisnice, nego je mora koristiti u potvrdi instance lisnice.

— C_KA-2: Ako se potvrda ključa šalje kao tip dokaza „attestation”, ona mora sadržavati i valjani c_nonce kako je specificiran u Dodatku F.3. OID4VCI-ju.

— C_KA-3: Izdavatelj vjerodajnica ne smije tumačiti parametar „exp” na najvišoj razini potvrde ključa kao kraj razdoblja održavanja opoziva WSCD-a ili spremnika ključeva.

— *NAPOMENA:* Parametar „exp” na najvišoj razini potvrde ključa označava datum isteka same potvrde ključa.

(d) Zahtjevi za životni ciklus

— U ovom se Prilogu utvrđuju sljedeći parametri metapodataka o izdavatelju vjerodajnica:

— „preferred_client_status_period”: NEOBVEZNO. Cijeli broj koji označava preferirano preostalo razdoblje održavanja statusa potvrde instance lisnice koju jedinica lisnice mora predočiti tijekom izdavanja, u sekundama. Preostalo razdoblje održavanja statusa definira se kao vrijednost „client_status.exp” u potvrdi umanjena za vrijeme primitka potvrde.

— „preferred_key_storage_status_period”: NEOBVEZNO. Cijeli broj koji znači preferirano preostalo razdoblje održavanja statusa potvrde instance lisnice koju jedinica lisnice mora predočiti tijekom izdavanja, u sekundama. Preostalo razdoblje održavanja statusa definira se kao vrijednost „key_storage_status.exp” u potvrdi umanjena za vrijeme primitka potvrde.

— LC_WIA-1: Autorizacijski poslužitelj može javiti svoje preferencije za preostalo razdoblje održavanja statusa u potvrdama instance lisnice uključivanjem parametra metapodataka „preferred_client_status_period” u krajnju točku svojih metapodataka o izdavatelju vjerodajnica kako je specificirano u odjeljku 12.2.2. OID4VCI-ja.

— LC_WIA-1.1: Ovo se polje mora postaviti na najvišu razinu metapodataka o izdavatelju vjerodajnica.

— LC_WIA_2: Autorizacijski poslužitelj ne smije tumačiti parametar „exp” na najvišoj razini potvrde instance lisnice kao kraj razdoblja održavanja opoziva instance lisnice.

— LC_WIA_3: Ako pružatelj lisnice potpiše ili stavi pečat na potvrdu instance lisnice, mora zadržati status opoziva relevantne instance lisnice dok ne istekne „wallet_instance_status.exp” naveden u toj potvrdi instance lisnice.

— LC_KA-1: Ako je potrebna potvrda ključa, izdavatelj vjerodajnica može javiti svoje preferencije za preostalo razdoblje održavanja statusa u potvrdama ključa uključivanjem parametra metapodataka „preferred_key_storage_status_period” u krajnju točku svojih metapodataka o izdavatelju vjerodajnica kako je specificirano u odjeljku 12.2.2. OID4VCI-ja.

— LC_KA-1.1: Ovo se polje mora staviti unutar objekta „key_attestations_required” kako je specificirano u odjeljku 12.2.4. OID4VCI-ja.

— LC_KA-2: Pružatelj lisnice odabire razdoblje tehničke valjanosti ključnih potvrda koje izdaje.

— LC_KA-3: Ako pružatelj lisnice potpiše ili stavi pečat na potvrdu ključa, mora zadržati status opoziva relevantnog WSCD-a ili spremnika podataka dok ne istekne „key_storage_status.exp” naveden u toj potvrdi ključa.

— LC_GEN-1: Pružatelj lisnice mora osigurati da jedinica lisnice može uvijek predočiti potvrde jedinice lisnice i potvrde ključa čiji su „client_status.exp” i „key_storage_status.exp” u trenutku predočenja autorizacijskom poslužitelju ili izdavatelju vjerodajnica najmanje 31 dan u budućnosti.

— *NAPOMENA:* To jamči da se pružatelji osobnih identifikacijskih podataka mogu osloniti na lanac opoziva, a da nisu prisiljeni izdavati kratkotrajne osobne identifikacijske podatke.

— LC_GEN-2: Pružatelj lisnice mora osigurati da jedinica lisnice tijekom izdavanja dohvaća metapodatke o izdavatelju vjerodajnica.

  — LC_GEN_2.1: Ako je u te metapodatke uključeno polje „preferred_key_storage_status_period”, jedinica lisnice mora poslati potvrdu ključa sa što manjom, ali ne negativnom razlikom („key_storage_status.exp” − trenutačno vrijeme) − „preferred_key_storage_status_period”. Ako takva potvrda ključa nije dostupna jedinici lisnice, ona od pružatelja lisnice mora pribaviti novu potvrdu ključa koja zadovoljava uvjet „key_storage_status.exp” − trenutačno vrijeme ≥ „preferred_key_storage_status_period”.

  — LC_GEN_2.2: Ako je u te metapodatke uključeno polje „preferred_key_storage_status_key_period”, jedinica lisnice mora poslati potvrdu instance lisnice sa što manjom, ali ne negativnom razlikom („client_status.exp” − trenutačno vrijeme) − „preferred_client_status_period”. Ako takva potvrda instance lisnice nije dostupna jedinici lisnice, ona od pružatelja lisnice mora pribaviti novu potvrdu ključa koja zadovoljava uvjet „client_status.exp” − trenutačno vrijeme) ≥ „preferred_client_status_period”.

— LC_GEN-3: Razdoblje tehničke valjanosti osobnih identifikacijskih podataka mora završiti prije „client_status.exp” potvrde instance lisnice i prije „key_storage_status.exp” potvrde ključa poslanih pružatelju osobnih identifikacijskih podataka u postupku izdavanja.

— LC_GEN-4: Kad je tehničko razdoblje valjanosti osobnih identifikacijskih podataka dulje od 24 sata, njihov pružatelj mora najmanje jedanput svaka 24 sata tijekom tog razdoblja provjeriti status opoziva potvrde instance lisnice i potvrde ključa primljenih tijekom izdavanja. U slučaju da se bilo koja od njih opozove, pružatelj mora opozvati osobne identifikacijske podatke.

(e) Zahtjevi za opoziv

— R_GEN-1: Pružatelj lisnice mora koristiti popise statusa tokena (specificirane u IETF Token Status List) kao mehanizam opoziva i za potvrde instance lisnice i za potvrde ključa, kako je specificirano u Dodatku D odnosno Dodatku E OID4VCI-ju.

— *NAPOMENA:* Kako bi poboljšao skalabilnost svojih popisa statusa, pružatelj lisnice može primijeniti sljedeće optimizacije:

  — dijeljenje popisa statusa na više blokova ako pružatelj lisnice ima znatan broj korisnika i izdao je potvrde. Ima mnogo strategija dijeljenja, primjerice prema fiksnoj veličini ili razdoblju. Odabir strategije prepušten je diskreciji pružatelja lisnice. U obzir se, među ostalim, mogu uzeti veličina popisa statusa za preuzimanje i privatnost korisnika;

  — više popisa statusa;

  — sažimanje popisa statusa radi smanjenja veličine.

— R_WIA-1: Pružatelj lisnice može dodijeliti istu vrijednost tvrdnji „idx” u tvrdnji „client_status.status” u svim potvrdama instance lisnice koje dana jedinica lisnice predoči istom autorizacijskom poslužitelju. To je opcija „per-issuer reuse”. Ako se koristi ta opcija:

  — R_WIA-1.1: Jedinica lisnice mora spremati vrijednosti indeksa koje je koristila za svaki autorizacijski poslužitelj s kojim je prethodno komunicirala i u ponovnoj interakciji s istim poslužiteljem zatražiti potvrdu instance lisnice s istom vrijednosti indeksa.

  — R_WIA-1.2: Ako pružatelj lisnice primi zahtjev za potvrdu instance lisnice s određenom vrijednosti indeksa, prije izdavanja nove potvrde instance lisnice s tom vrijednošću indeksa mora provjeriti je li jedinica lisnice koja je uputila zahtjev prethodno primila tu vrijednost indeksa.

  — R_WIA-1.3: Jedinica lisnice ne smije iskoristiti istu vrijednost indeksa za interakcije s različitim autorizacijskim poslužiteljima.

— *NAPOMENA:* Ako se koristi opcija „per-issuer reuse”, pružatelj lisnice moći će odrediti s koliko je autorizacijskih poslužitelja jedinica lisnice bila u interakciji i koliko je često u interakciji sa svakim od njih.

— R_WIA-2: U svojoj politici zaštite privatnosti pružatelj lisnice mora dokumentirati koristi li opciju „per-issuer reuse” za opoziv instance lisnice.

— R_WIA-3: Ako pružatelj lisnice ne koristi opciju „per-issuer reuse”, pružatelj lisnice mora dodijeliti novu, nepovezivu vrijednost indeksa svakoj potvrdi instance lisnice koju izda.

— R_WIA-4: Ako se jedinica lisnice mora opozvati, pružatelj lisnice mora opozvati vrijednosti indeksa u tvrdnji „client_status.status” u svim potvrdama instance lisnice povezanima s tom jedinicom lisnice.

— R_WIA-5: Kad određuje veličinu svojih popisa statusa potvrda jedinice lisnice, pružatelj lisnice mora uzeti u obzir opseg njezina korištenja i osnovnu arhitekturu i osigurati da su ti popisi dovoljno veliki da onemoguće korelaciju i zaštite privatnost korisnika. Minimum je da se popis statusa mora, kad je to moguće, odnositi na najmanje 10 000 potvrda.

— R_KA_1: Pružatelj lisnice odabire jednu od sljedećih opcija dodjele indeksa za tvrdnju „key_storage_status.status” u potvrdi ključa:

  — opciju 1 ili „type-shared index”, u kojoj sve potvrde ključa koje potvrđuju ključeve pohranjene u istom tipu WSCD-a ili spremnika ključeva sadržavaju istu vrijednost indeksa u „key_storage_status.status”,

  — opciju 2 ili „per-key-attestion index”, u kojoj potvrda ključa koja potvrđuje ključeve pohranjene u pojedinačnom WSCD-u ili spremniku ključeva sadržavaju jedinstvenu (za svaki par) vrijednost indeksa u „key_storage_status.status”.

— *NAPOMENA:* Ako pružatelj lisnice koristi opciju 1, jedna opozivna radnja poništava sve potvrde ključa predmetnog tipa u svim jedinicama lisnice. Nadalje, budući da sve potvrde ključa za isti tip WSCD-a ili spremnika ključeva dijele isti indeks popisa statusa, broj unosa na popisu statusa potvrda ključeva odražava broj WSCD-a ili spremnika ključeva koje podržava pružatelj lisnice, a ne broj jedinica lisnice u upotrebi. Razlozi zaštite privatnosti zbog kojih se traži minimalna veličina za popise statusa instance lisnice stoga se ne odnose na popise statusa potvrda ključeva iz opcije 1 pod uvjetom da postoji dovoljan broj jedinica lisnice koje koriste isti tip WSCD-a ili spremnika ključeva.

— *NAPOMENA:* Ako pružatelj lisnice koristi opciju 2, svaki indeks označava stanje opoziva konkretnog WSCD-a ili spremnika ključeva potvrđenog u toj potvrdi ključa.

— *NAPOMENA:* Ako pružatelj lisnice koristi opciju 2, konkretni WSCD ili spremnik ključeva može se opozvati i na korisnikov zahtjev.

— R_KA-2: Ako pružatelj lisnice koristi opciju 2, može opcionalno koristiti opciju „per-issuer reuse” opisanu u R_WIA-1. Ako je koristi, zahtjevi iz točaka R_WIA-1 – R_WIA-3 primjenjuju se *mutatis mutandis*.

— R_KA-3: Ako pružatelj lisnice koristi opciju 2, mora uzeti u obzir opseg korištenja lisnice i osnovnu arhitekturu kad određuje veličinu svojih popisa statusa potvrda ključeva i osigurati da su dovoljno veliki da onemoguće korelaciju i zaštite privatnost korisnika. Minimum je da se popis statusa mora, kad je to moguće, odnositi na najmanje 10 000 potvrda ključa.

— R_KA-4: Ako pružatelj lisnice koristi opciju 1 (type-shared index), unos „key_storage_status.status” smije opozvati samo ako tip WSCD-a ili spremnika ključeva ima sigurnosnu ranjivost.

(f) Zahtjevi za potpisne algoritme

— SA-1: Za potpisivanje potvrda instance lisnice, potvrda ključa, povezanih dokaza o posjedovanju i popisa statusa tokena mora se koristiti jedan od sljedećih algoritama:

  — ES256 (ECDSA sa SHA-256 i P-256)

  — ES384 (ECDSA sa SHA-384 i P-384)

  — ES512 (ECDSA sa SHA-512 i P-521)

— SA-2: Pružatelj lisnice odabire koje će algoritme iz točke SA-1 koristiti.

— SA-3: Autorizacijski poslužitelj ili izdavatelj vjerodajnica (kako je specificirano u OID4VCI-ju) moraju podržavati sve algoritme iz točke SA-1.”

PRILOG IV.

„PRILOG II.

Popis normi iz članka 8.

Primjenjuju se tehničke specifikacije utvrđene u točkama od 2. do 6. norme ETSI TS 119 472-1 V1.2.1 (2026-02) i sadržavaju sljedeće prilagodbe:

(1) 2.1. Normative references (Normativna upućivanja)

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): Elektronički potpisi i infrastrukture (ESI) – Profili certifikata – 1. dio: Pregled i struktura zajedničkih podataka".

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): „Elektronički potpisi i infrastruktura povjerenja (ESI); Profili certifikata – 6. dio: Zahtjevi za profil certifikata za pružatelje PID-ova, lisnice, EAA-ova, QEAA-ova i PSBEAA-ova".

— [25] IETF Token Status List (TSL), draft-ietf-oauth-status-list-20: „Token Status List", 20. travnja 2026.

(2) 4.2.11.1. General requirements (Opći zahtjevi)

— EAA-4.2.11.1-06: Ako se element statusa upotrebljava za osobne identifikacijske podatke, kvalificirane elektroničke potvrde atributa ili elektroničke potvrde atributa koje izdaje tijelo javnog sektora odgovorno za autentični izvor ili koje se izdaju u njegovo ime, on smije samo pokazivati je li potvrda opozvana ili nije i ne smije omogućivati druge vrijednosti statusa, primjerice suspenziju.

— EAA-4.2.11.1-06.1: Ako se potvrda opozove, taj je opoziv trajan.

(3) 4.2.13. EAA short-lived (Kratkotrajni EAA)

— EAA-4.2.13-03: Ako se izdaju kratkotrajne elektroničke potvrde atributa s razdobljem valjanosti od 24 sata ili kraćim, opoziv nije obvezan.

(4) 4.6.3. Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA) (Zahtjevi za EU EAA koji izdaje tijelo javnog sektora odgovorno za autentični izvor ili koji se izdaje u njegovo ime (PuB-EAA))

— PuB-EAA-4.6.2-03: nevažeće.

— Pub-EAA-4.6.2-04: nevažeće.

— PuB-EAA-4.6.3-03: Digitalni potpis PuB-EAA-a trebao bi sadržavati kvalificirani certifikat koji podržava taj digitalni potpis.

— PuB-EAA-4.6.3-04: Kvalificirani certifikat koji podržava digitalni potpis PuB-EAA-a mora ispunjavati zahtjeve iz točke 8. norme ETSI TS 119 412-6 v1.1.1 i sadržavati QcType QcStatement kako je definirano u normi ETSI EN 319 412-5 v2.5.1, pri čemu je vrijednost id-etsi-qct-eidaspsbeaa definirana kako slijedi:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } -- Certifikat iz članka 45.f stavka 1. točke (b) koji podržava kvalificirani elektronički potpis ili kvalificirani elektronički pečat tijela javnog sektora iz članka 3. točke 46. Uredbe (EU) br. 910/2014.

(5) 5.2.10.1. General requirements (Opći zahtjevi)

— EAA-5.2.10.1-04: nevažeće.

— EAA-5.2.10.1-05: nevažeće.

— EAA-5.2.10.1-06: Član status može sadržavati član status_list kako je specificirano u točki 6.2. draft-ietf-oauth-status-list-20 IETF-a [25].

— EAA-5.2.10.1-07: nevažeće.

— EAA-5.2.10.1-08: nevažeće.

— EAA-5.2.10.1-09: nevažeće.

— EAA-5.2.10.1-10: nevažeće.

— EAA-5.2.10.1-11: nevažeće.

— EAA-5.2.10.1-12: nevažeće.

(6) 6.2.10.1. General requirements (Opći zahtjevi)

— EAA-6.2.10.1-01: Ako se za elektroničku potvrdu atributa sukladnu s normom ISO/IEC mdoc upotrebljava mehanizam popisa statusa potvrda kako je utvrđen u EAA-6.2.10.1.-02,2. ili mehanizam popisa opozvanih potvrda kako je utvrđen u EAA-6.2.10.1.-02,3., njezin mobilni sigurnosni objekt („MSO”) mora sadržavati strukturu statusa, kako je specificirana u EAA-6.2.10.1.-17., s informacijama o opozivu MSO-a.

— EAA-6.2.10.1-01.1: Kad se primjenjuje mehanizam popisa identifikatora, element statusa mora sadržavati element identifier_list kako je utvrđen u EAA-6.2.10.1.-11.

— EAA-6.2.10.1-01.2: Kad se primjenjuje mehanizam popisa statusa, element statusa mora sadržavati element status_list kako je utvrđen u EAA-6.2.10.1.-13.

— *NAPOMENA:*

  — Struktura statusa sadržava upućivanje na popis opozvanih MSO-ova.

  — Popis opozvanih MSO-ova je COSE_Sign1 struktura koja pokazuje je li određeni MSO opozvan ili nije.

  — Struktura statusa sadržava sve informacije koje su pouzdajućoj strani lisnice potrebne da utvrdi je li popis opozvanih MSO-ova vjerodostojan.

— EAA-6.2.10.1-02: Pružatelj osobnih identifikacijskih podataka, pružatelj kvalificiranih elektroničkih potvrda atributa ili pružatelj elektroničkih potvrda atributa koje izdaje tijelo javnog sektora odgovorno za autentični izvor ili koje se izdaju u njegovo ime mora primjenjivati jednu od sljedećih metoda za opoziv osobnih identifikacijskih podataka, kvalificiranih elektroničkih potvrda atributa ili elektroničkih potvrda atributa koje izdaje tijelo javnog sektora odgovorno za autentični izvor ili koje se izdaju u njegovo ime:

— EAA-6.2.10.1-02.1: Ako izdaje kratkotrajne elektroničke potvrde atributa s razdobljem valjanosti od 24 sata ili manje, opoziv nije obvezan.

— EAA-6.2.10.1-02.2: Koristiti mehanizam popisa statusa potvrda za enkodiranje informacija o opozivu kao što je popis statusa.

— EAA-6.2.10.1-02.2.1: Mehanizam popisa statusa opoziva MSO na temelju toga je li bit pozicije bita koju je odredio izdavatelj u MSO-u postavljen na „true” na popisu statusa.

— EAA-6.2.10.1-02.2.2: Mehanizam popisa statusa određen je u specifikaciji popisa statusa tokena (draft-ietf-oauth-status-list-20).

— EAA-6.2.10.1-02.3: Koristiti mehanizam popisa opozvanih potvrda za enkodiranje informacija o opozivu kao što je popis identifikatora.

— EAA-6.2.10.1-02.3.1: Mehanizam popisa identifikatora opoziva MSO na temelju toga nalazi li se identifikator u MSO-u koji je odredio izdavatelj na popisu identifikatora.

— EAA-6.2.10.1-02.3.2: U točkama EAA-6.2.10.1.-06., EAA-6.2.10.1.-08., EAA-6.2.10.1.-09., EAA-6.2.10.1.-10. i EAA-6.2.10.1.-11. specificiran je mehanizam popisa identifikatora na temelju zahtjeva iz specifikacije popisa statusa tokena, uključujući ujednačenost popisa statusa i mehanizma popisa identifikatora.

— EAA-6.2.10.1-03: Ako se element statusa upotrebljava za osobne identifikacijske podatke, kvalificirane elektroničke potvrde atributa ili elektroničke potvrde atributa koje izdaje tijelo javnog sektora odgovorno za autentični izvor ili koje se izdaju u njegovo ime, isključivo je dopušten status „revoked”.

— EAA-6.2.10.1-03.1: Za popis statusa to znači da se upotrebljavaju samo vrijednosti „valid” i „invalid”, kako je navedeno u specifikaciji popisa statusa tokena.

— EAA-6.2.10.1-03.2: Na popis identifikatora smiju se uvrstiti samo opozvani MSO-ovi, a ne i privremeno suspendirani.

— EAA-6.2.10.1-04: Ako se MSO opozove, taj je opoziv trajan.

— EAA-6.2.10.1-05: Provjera popisa opozvanih MSO-a nije obvezna za pouzdajuću stranu lisnice, a, ako je primjenjivo, mora ispunjavati zahtjeve za provjeru iz specifikacije popisa statusa tokena i specfikacije strukture statusa iz točke EAA-6.2.10.1.-01.

— EAA-6.2.10.1-05.1: Ako pouzdajuća strana lisnice mora moći provjeriti status opoziva osobnih identifikacijskih podataka ili elektroničkih potvrda atributa, ona mora podržavati i mehanizam popisa statusa potvrda i mehanizam popisa opozvanih potvrda iz točke EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: Identifier_list and status_list u MSO-u mogu sadržavati element certifikata.

— EAA-6.2.10.1-06.1: Ako postoji element certifikata, on mora sadržavati certifikat s javnim ključem koji je potpisao ili zapečatio certifikat najviše razine u elementu x5chain u strukturi popisa opozvanih MSO-ova.

— EAA-6.2.10.1-06.1.1: Instanca pouzdajuće strane lisnice mora koristiti taj certifikat kao točku povjerenja za provjeru elementa x5chain u strukturi popisa opozvanih MSO-ova.

— EAA-6.2.10.1-06.2: Ako element certifikata nije prisutan, certifikat najviše razine u elementu x5chain u strukturi popisa opozvanih MSO-ova mora biti potpisan ili zapečaćen certifikatom pomoću kojeg je potpisan certifikat u elementu x5chain MSO-a.

— EAA-6.2.10.1-06.2.1: Instanca pouzdajuće strane lisnice mora koristiti taj certifikat kao točku povjerenja za provjeru elementa x5chain u strukturi popisa opozvanih MSO-ova.

— EAA-6.2.10.1-07: Popis opozvanih MSO-a implementira se kao token popisa statusa u formatu CWT u skladu sa specifikacijom popisa statusa tokena.

— EAA-6.2.10.1-08: Kad je riječ o popis opozvanih MSO-a za popis identifikatora i mehanizam popisa statusa primjenjuju se sljedeći zahtjevi:

  — tvrdnja exp mora biti prisutna,

  — tvrdnja ttl mora biti prisutna,

  — tvrdnja aggregation_uri u IdentifierList ili StatusList može biti prisutna, a pružatelj osobnih identifikacijskih podataka, pružatelj kvalificiranih elektroničkih potvrda atributa ili pružatelj elektroničkih potvrda atributa koje pruža tijelo javnog sektora odgovorno za autentični izvor ili koje se

pružaju u njegovo ime može upotrijebiti tvrdnju aggregation_uri da označi podršku za agregacijski mehanizam kako je specificiran u specifikaciji popisa statusa tokena,

— CWT mora biti COSE_Sign1 objekt koji koristi jedan od sljedećih potpisnih algoritama za izračun potpisa:

(a) „ES256” (ECDSA s krivuljom NIST P-256 i SHA-256);

(b) „ES384” (ECDSA s krivuljom NIST P-384 i SHA-384);

(c) „ES512” (ECDSA s krivuljom NIST P-521 i SHA-512);

(d) „ESB256” (ECDSA s krivuljom brainpoolP256r1 i SHA-256);

(e) „ESB384” (ECDSA s krivuljom brainpoolP384r1 i SHA-384);

(f) „ESB512” (ECDSA s krivuljom brainpoolP512r1 i SHA-512);

— CWT mora sadržavati x5chain u zaštićenom zaglavlju s certifikatom ili lancem certifikata za provjeru potpisa popisa opozvanih MSO-ova,

— „extended key usage” identifikatora objekta navedenog u specifikaciji tokenskog popisa statusa može se upotrebljavati za potpisni certifikat popisa statusa i popisa identifikatora, a instance pouzdajuće strane lisnice mogu podržavati „extended key usage” identifikatora objekta iz specifikacije popisa statusa tokena, a za identifikator objekta pružatelj kvalificiranih elektroničkih potvrda atributa ili pružatelj elektroničkih potvrda atributa koje izdaje tijelo javnog sektora ili koje se izdaju u njegovo ime ne smije polje „extended key usage” napraviti kritičnim kad koristi „extended key usage” OID iz specifikacije popisa statusa tokena.

— EAA-6.2.10.1-09: Odstupajući od zahtjeva specifikacije popisa statusa tokena, za mehanizam popisa identifikatora vrijede sljedeći zahtjevi:

— vrijednost tipa tvrdnja mora biti „application/identifierlist+cwt”;

— tvrdnja StatusList ne smije biti prisutna u skupu CWT tvrdnji,

— struktura IdentifierList definirana u točki EAA-6.2.10.1.-11. mora se uključiti u skup CWT tvrdnji koristeći ključ 65530.

— EAA-6.2.10.1-10: Struktura IdentifierList mora biti CBOR struktura sa sljedećim CDDL-om:

```
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: Ako je prisutan identifikator iz IdentifierList, MSO koji sadržava identifikator u elementu statusa opoziva se.

— EAA-6.2.10.1-10.2: Tvrdnja Aggregation_uri specificirana je u odjeljku 9.2. specifikacije popisa statusa tokena.

— EAA-6.2.10.1-10.3: Vrsta sadržaja popisa identifikatora mora biti „application/identifierlist+cwt” utvrđena u zahtjevima iz odjeljka 8.2. specifikacije popisa statusa tokena.

— EAA-6.2.10.1-11: Za element identifier_list u MSO-u (vidjeti EAA-6.2.10.1.-17.) vrijede sljedeći zahtjevi:

— EAA-6.2.10.1-11.1: Element identifier_list je CBOR struktura sa sljedećim CDDL-om:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: Kako se identifikator ne bi mogao koristiti za korelaciju među predočenjima, on mora biti jedinstven za MSO.

— EAA-6.2.10.1-12: Za popis statusa vrijede sljedeći zahtjevi:

  — EAA-6.2.10.1-12.1: Element bits u strukturi StatusList mora biti 1.

— EAA-6.2.10.1-13: Za element status_list u MSO-u (vidjeti EAA-6.2.10.1.-17.) vrijede sljedeći zahtjevi:

  — EAA-6.2.10.1-13.1: Element status_list mora biti u skladu sa zahtjevima za strukturu StatusListInfo iz specifikacije popisa statusa tokena i dodaje mu se neobvezni element certifikata definiran u EAA-6.2.10.1.-06.

  — EAA-6.2.10.1-13.2: Kako se indeks statusa ne bi služio za korelaciju među predočenjima, kombinacija indeksa statusa i URI-ja mora biti jedinstvena za MSO.

— EAA-6.2.10.1-14: Pružatelj lisnice za opoziv potvrde instance lisnice (WIA) i za opoziv potvrde ključa (KA) primjenjuje drugu (EAA-6.2.10.1-02.2) ili treću (EAA-6.2.10.1-02.3) metodu iz točke EAA-6.2.10.1-02.

— EAA-6.2.10.1-15: Pružatelj lisnice u svojoj izvedbi lisnice primjenjuje mehanizme opoziva potvrda iz EAA-6.2.10.1-02.

— EAA-6.2.10.1-16: Pružatelj osobnih identifikacijskih podataka i pružatelj elektroničkih potvrda atributa moraju podržavati i mehanizam popisa statusa potvrda i mehanizam popisa opozvanih potvrda iz EAA-6.2.10.1.02. za provjeru statusa opoziva potvrde instance lisnice (WIA) i za opoziv potvrde ključa (KA).

— EAA-6.2.10.1-17: Struktura statusa u MSO-u mora biti CBOR struktura sa sljedećim CDDL-om:

Status = {

? 'identifier_list' : IdentifierListInfo,

? 'status_list' : StatusListInfo,

* tstr => RFU

}”

PRILOG V.

„PRILOG III.

Tehničke specifikacije iz članka 10.

— Tehničke specifikacije:

— Točka 4.2.5. norme ETSI TS 119 472-3 V1.1.1 (2026-03).”

PRILOG VI.

Prilog IV. Provedbenoj uredbi (EU) 2024/2979 mijenja se kako slijedi:

(1) točka 1. zamjenjuje se sljedećim:

„1. Obvezni format potpisa ili pečata:

(a) PAdES (PDF Advanced Electronic Signature) kako je specificiran u normi „ETSI EN 319 142-1 V1.2.1 (2024-01) – Elektronički potpisi i infrastrukture (ESI) – PAdES digitalni potpisi – 1. dio: Izgrađujući blokovi i PAdES temeljni potpisi.";

(2) točka 3. zamjenjuje se sljedećim:

„3. Aplikacijsko programsko sučelje:
točke 6.4.3, A.6, A.7 i A.8 norme ETSI TS 119 432 v1.3.1 (2026-03).".

PRILOG VII.

„PRILOG VI.

EU znak pouzdanosti lisnice za digitalni identitet u boji



„

PRILOG VIII.

„PRILOG VII.

Crno-bijeli EU znak pouzdanosti lisnice za digitalni identitet



„

PRILOG IX.

„PRILOG VIII.

Podaci EU znaka pouzdanosti lisnice za digitalni identitet

Podaci	Opis	Enkodiranje	Status
TrustMarkResourceURL	URL grafičkih elemenata znaka pouzdanosti EU lisnice za digitalni identitet i resursa za korisničke informacije u korisničkom sučelju lisnice.	URL	Obvezno
ListOfCertifiedWalletsURL	URL javnog popisa certificiranih izvedbi lisnice u EU-u kako je utvrđeno u Provedbenoj uredbi Komisije (EU) 2025/849 ([1]).	URL	Obvezno
ListOfCertifiedWalletsQRCode	QR kod s informacijama o ListOfCertifiedWalletsURL	ISO-8859-1 Byte mode QR code	Neobvezno
WalletSolutionInfoPageURL	URL na informativnu stranicu certificirane izvedbe lisnice s popisa certificiranih izvedbi lisnice s URL-a ListOfCertifiedWalletsURL s nastavkom koji se sastoji od „?” i identifikatora WalletSolutionID te izvedbe lisnice.	URL	Obvezno
WalletSolutionInfoPageQRCode	QR kod s informacijama o WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	Neobvezno
WalletVerifierToolURL*	URL koji upućuje na alat za provjeru lisnice*//.well-known/openid-credential-issuer* krajnju točku koja služi za dohvaćanje metapodataka o pružatelju potvrde.	URL	Neobvezno

([1]) Provedbena uredba Komisije (EU) 2025/849 od 6. svibnja 2025. o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu dostavljanja informacija Komisiji i Skupini za suradnju za popis certificiranih europskih lisnica za digitalni identitet (SL L, 2025/849, 7.5.2025., ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).”

PRILOG X.

Prilog II. Provedbenoj uredbi (EU) 2024/2980 mijenja se kako slijedi:

(1) u Prilogu II., odjeljku 1., točka 1.(i) zamjenjuje se sljedećim:

„(i) jedan ili više certifikata u skladu s normom ETSI EN 319 412-2 V2.4.1 (2025-06) ili ETSI EN 319 412-3 V1.3.1 (2023-09) koji se mogu upotrebljavati za provjeru potpisa ili pečata koje voditelj registra stavi na podatke iz registra i za koje certificirani podaci o identitetu sadržavaju ime i, ako je to primjenjivo, registracijski broj voditelja registra, iz točke (c) odnosno (d);";

(2) u Prilogu II., odjeljku 2., točka 1.(h) zamjenjuje se sljedećim:

„(h) jedan ili više certifikata u skladu s normom ETSI EN 319 412-2 V2.4.1 (2025-06) ili ETSI EN 319 412-3 V1.3.1 (2023-09) koji se mogu upotrebljavati za autentifikaciju i validaciju potvrda jedinice lisnice koje je izdao pružatelj lisnice i za koje certificirani podaci o identitetu sadržavaju ime i, ako je to primjenjivo, registracijski broj pružatelja lisnice, iz točke (a) odnosno (b);";

(3) u Prilogu II., odjeljku 3., točka 1.(h) zamjenjuje se sljedećim:

„(h) jedan ili više certifikata u skladu s normom ETSI EN 319 412-2 V2.4.1 (2025-06) ili ETSI EN 319 412-3 V1.3.1 (2023-09) koji se mogu upotrebljavati za provjeru potpisa ili pečata koje pružatelj osobnih identifikacijskih podataka stavi na osobne identifikacijske podatke koje pruža i za koje certificirani podaci o identitetu sadržavaju ime i, ako je to primjenjivo, registracijski broj pružatelja osobnih identifikacijskih podataka, kako je navedeno u točki (a) odnosno (b).";

(4) u Prilogu II., odjeljku 4., točka 1.(g) zamjenjuje se sljedećim:

„(g) jedan ili više certifikata u skladu s normom ETSI EN 319 412-2 V2.4.1 (2025-06) ili ETSI EN 319 412-3 V1.3.1 (2023-09) koji se mogu upotrebljavati za provjeru potpisa ili pečata koje pružatelj pristupnih certifikata pouzdajuće strane lisnice stavi na pristupne certifikate koje pruža pouzdajućim stranama lisnice zajedno s informacijama, ako je to primjenjivo, koje su potrebne da bi se pristupni certifikati pouzdajuće strane lisnice razlikovali od drugih certifikata.";

(5) u Prilogu II. dodaje se odjeljak 5. kako slijedi:

„5. Prijava informacija o pružateljima registracijskih certifikata pouzdajuće strane lisnice

1. Države članice Komisiji dostavljaju sljedeće informacije o pružateljima registracijskih certifikata pouzdajuće strane lisnice:

(a) ime pružatelja registracijskih certifikata pouzdajuće strane lisnice;

(b) ako je to primjenjivo, registracijski broj pružatelja registracijskih certifikata pouzdajuće strane lisnice;

(c) državu članicu u kojoj pružatelj registracijskih certifikata pouzdajuće strane lisnice ima poslovni nastan;

(d) e-adresu i telefonski broj pružatelja registracijskih certifikata pouzdajuće strane lisnice za pitanja povezana s registracijskim certifikatima koje izdaje pouzdajućim stranama lisnice;

(e) ako je to primjenjivo, URL internetske stranice pružatelja registracijskih certifikata pouzdajuće strane lisnice koja sadržava dodatne informacije o pružatelju i registracijskim certifikatima koje izdaje pouzdajućim stranama lisnice;

(f) URL internetske stranice koja sadržava pravila i uvjete koji se primjenjuju na pružanje i korištenje registracijskih certifikata koje taj pružatelj izdaje pouzdajućim stranama lisnice;

(g) jedan ili više certifikata u skladu s normom ETSI EN 319 412-2 V2.4.1 (2025-06) ili ETSI EN 319 412-3 V1.3.1 (2023-09) koji se mogu upotrebljavati za provjeru potpisa ili pečata koje pružatelj registracijskih certifikata pouzdajuće strane lisnice stavi na registracijske certifikate koje pruža pouzdajućim stranama lisnice zajedno s informacijama, ako je to primjenjivo, koje su potrebne da bi se registracijski certifikati pouzdajuće strane lisnice razlikovali od drugih certifikata.

2. Informacije iz točke 1. dostavljaju se za svakog pružatelja registracijskih certifikata pouzdajućih strana lisnice.”

PRILOG XI.

„PRILOG I.

Protokoli i sučelja iz članka 4.

Tehnička specifikacija ETSI TS 119 472-3 V1.1.1 (2026-03) primjenjuje se uz sljedeće prilagodbe:

(1) 4.1. General requirements (Opći zahtjevi)

— GEN-REQ-4.1-05: nevažeće.

— NAPOMENA: nevažeće.

(2) 4.2.3. Provision of registration certificates of PID/EAA Provider to EUDI Wallet (Pružanje registracijskih certifikata pružatelja PID-ova/EAA-ova EU lisnici za digitalni identitet)

— ISS-MDATA-REG_CERT-4.2.3-04: Jedan od elemenata parametra polja issuer_info mora sadržavati registracijski certifikat pružatelja PID/EAA-ova.

— ISS-MDATA-REG_CERT-4.2.3-07: nevažeće.

— ISS-MDATA-REG_CERT-4.2.3-08: nevažeće.

— ISS-MDATA-REG_CERT-4.2.3-09: nevažeće.

— ISS-MDATA-REG_CERT-4.2.3-10: nevažeće.

— ISS-MDATA-REG_CERT-4.2.3-11: nevažeće.

— ISS-MDATA-REG_CERT-4.2.3-12: nevažeće.

— ISS-MDATA-REG_CERT-4.2.3-13: nevažeće.

(3) 4.2.4.2. ARF pre-defined PID/EAA reuse policy (Unaprijed definirana politika iskorištavanja postojećih PID-ova/EAA-ova prema ARF-u)

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Ako član id ima vrijednost „arf_annex_ii”, a polje povezano s oznakom „details” sadržava vrijednost „once_only” ili „per-relying-party”, onda objekt JSON s tim poljem povezanim s oznakom „details” mora sadržavati i JSON broj povezan s oznakom „reissue_trigger_unused”.

(4) Prilog A se ne primjenjuje.”

PRILOG XII.

„PRILOG II.

Tehničke specifikacije iz članka 5.

Primjenjuje se tehnička specifikacija u Prilogu C normi ISO/IEC 18013-7:2025.

Tehničke specifikacije u točkama 4.1., 4.2., 5. i 6. norme ETSI TS 119 472-2 V1.2.1 (2026-03) primjenjuje se uz sljedeće prilagodbe, uključujući umetanje nove točke 4.3.:

(1) 1. Scope (Područje primjene)

— U ovom dokumentu specificirana su dva profila protokola na temelju kojih pouzdajuće strane (RP) mogu EU lisnici za digitalni identitet poslati zahtjev za EAAP-ove ili osobne identifikacijske podatke (PID) u, a ta lisnica tražene EAAP-ove/PID-ove poslati RP-u. Svaki profil podržava dva mehanizma prijenosa: s API-jem kao posrednikom i bez API-ja, kako je opisano u nastavku:

(a) Profil se temelji na:

— normi ISO/IEC 18013-5 [10] samo za mehanizam prijenosa bez API-ja, i

— Prilogu C normi ISO/IEC 18013-7 [16] za mehanizam prijenosa s API-jem kao posrednikom.

Taj se profil zove ISO/IEC-mdoc profil i definiran je u točki 5. ovog dokumenta.

(b) Profil se temelji na:

OpenID4VC-HAIP [11] za mehanizme prijenosa s API-jem kao posrednikom i one bez API-ja, kako slijedi:

— odjeljcima 5., 5.1., 5.3., 7. i 8. specifikacije [11] za prijenos putem preusmjeravanja ili mehanizam prijenosa bez API-ja, i

— odjeljcima 5., 5.2., 5.3., 7. i 8. specifikacije [11] za mehanizam prijenosa s API-jem kao posrednikom.

Taj se profil zove OpenID4VC-HAIP profil i definiran je u točki 6. ovog dokumenta.

(2) 2.1. Normative references (Normativna upućivanja)

— [15] ISO 639: „Kodovi za prikaz naziva jezika”

— [16] ISO/IEC 18013-7:2025 „Osobna identifikacija – ISO – sukladna vozačka dozvola – 7. dio: Dodatne funkcije mobilne vozačke dozvole (mDL)”.

(3) 4.1. EAAP implementation based on SD-JWT VC (Implementacija EAAP-a na temelju formata SD-JWT VC)

— EAAP-SD-JWT VC-04: nevažeće.

(4) 4.2. EAAP implementation based on ISO/IEC-mdoc (Implementacija EAAP-a na temelju formata ISO/IEC-mdoc)

— EAAP-ISO/IEC-mdoc-01: nevažeće.

— *Napomena 2:* nevažeće.

— EAAP-ISO/IEC-mdoc-02: nevažeće.

(5) 4.3. EAAP implementation with mediating API (Implementacija EAAP-a s API-jem posrednikom)

— EAAP-API-GEN-01: EU lisnica za digitalni identitet mora podržavati API posrednik koji podržava oba protokola definirana u točki 5.2. specifikacije [11] i Prilogu C norme [16].

— *NAPOMENA:* Ako uređaj na koji je instalirana EU lisnica za digitalni identitet ne podržava oba protokola, taj se zahtjev ne može ispuniti, pa je to nesukladnost zbog neimplementiranja potrebne interoperabilnosti u temeljnim operativnim sustavima i preglednicima.

— EAAP-API-GEN-02: EU lisnica za digitalni identitet mora podržavati API posrednik barem za vrste PID-ova i EAA-ova registrirane u katalogu sustava kako je definiran u Provedbenoj uredbi (EU) 2025/1569 i barem za sve formate definirane u Prilogu II. Provedbenoj uredbi (EU) 2024/2979.

— *NAPOMENA 1:* Ako temeljni operativni sustav, preglednik, API-ji posrednici ili bilo koji drugi tehnički sloj koji je izvan kontrole EU lisnice za digitalni identitet ograničava, filtrira, unaprijed odabire ili na neki drugi način limitira formate vjerodajnica i vrste PID-ova i EAA-ova registrirane u katalogu sustava, taj se zahtjev ne može ispuniti. Ako takvo ograničenje sprečava EU lisnicu za digitalni identitet da podržava registriranu vrstu ili format vjerodajnice, rezultirajuća nesukladnost može se pripisati nemogućnosti tih temeljnih operativnih sustava, preglednika, API-ja posrednika ili drugog relevantnog tehničkog sloja da osigura potrebnu interoperabilnost.

(6) 4.4. Wallet-relying party validation and overasking checks (Validacija pouzdajuće strane lisnice i provjere prekomjernosti upita)

— WRP-VALIDATION-01: EU lisnica za digitalni identitet mora validirati registracijski certifikat pouzdajuće strane lisnice primljen u zahtjevu prije nego što korisniku lisnice predoči na odobrenje bilo koji traženi PID ili elektroničku potvrdu atributa.

— WRP-VALIDATION-02: Ako validacija registracijskog certifikata pouzdajuće strane lisnice ne uspije, među ostalim ako je certifikat istekao, opozvan, ako ga nije izdao valjani pouzdani pružatelj registracijskih certifikata pouzdajuće strane lisnice, ako je nepravilan ili se ne može kriptografski provjeriti, EU lisnica za digitalni identitet mora upozoriti korisnika lisnice da se pouzdajuća strana lisnice ne može validirati i ne smije zahtjev predočiti kao uspješno validiran. Korisnik lisnice mora izričito odobriti zahtjev pouzdajuće strane. Izostanak korisnikove radnje ili unaprijed označene kućice ne smatraju se izričitim odobrenjem.

— WRP-VALIDATION-03: Pružatelj lisnice mora na temelju svoje analize rizika i sigurnosne politike odrediti može li i pod kojim uvjetima korisnik lisnice zaobići pojedine neuspjele validacijske provjere.

— WRP-OVERASKING-01: EU lisnica za digitalni identitet mora potvrde i atribute koje je zatražila pouzdajuća strana lisnice usporediti s registriranim potvrdama i atributima u registracijskom certifikatu pouzdajuće strane lisnice.

— WRP-OVERASKING-02: Ako pouzdajuća strana lisnice zatraži PID ili elektroničke potvrde atributa ili tvrdnje koje nisu obuhvaćene registracijskim certifikatom pouzdajuće strane lisnice, EU lisnica za digitalni identitet mora jasno upozoriti korisnika lisnice prije nego što se bilo što otkrije. U upozorenju se mora navesti da pouzdajuća strana lisnice traži više informacija nego što je registrirala. Korisnik lisnice mora izričito odobriti zahtjev pouzdajuće strane. Izostanak korisnikove radnje ili unaprijed označene kućice ne smatraju se izričitim odobrenjem.

— WRP-OVERASKING-03: Pružatelj lisnice mora na temelju svoje analize rizika, sigurnosne politike i mjerodavnog prava odrediti može li korisnik lisnice nastaviti s korištenjem unatoč takvom upozorenju, smije li se otkriti samo podskup traženih podataka obuhvaćenih registracijskim certifikatom ili se zahtjev mora odbiti.

(7) 5.1. Introduction (Uvod)

— U točki 5. i njezinim podtočkama definiran je profil za protokol na temelju kojeg RP može zatražiti EAAP-ove ili PID-ove u EU lisnicu za digitalni identitet, a ona poslati zatražene EAAP-ove/PID-ove RP-u mehanizmom prijenosa bez API-ja, koji se temelji na normi ISO/IEC 18013-5 [10], ili mehanizmom prijenosa s API-jem kao posrednikom, koji se temelji na Prilogu C normi ISO/IEC 18013-7 [16], za prijenos podatkovnih struktura definiranih u normi ISO/IEC 18013-5 [10] u odgovarajućem formatu.

— Ostatak članka 5. organiziran je na sljedeći način:

— u točki 5.2. utvrđuju se zahtjevi za podržavanje profila i mehanizama prijenosa koje moraju ispunjavati RP-ovi i EU lisnica za digitalni identitet;

— u točki 5.3. utvrđuju se zahtjevi koji su specifični za mehanizam prijenosa bez API-ja;

— u točki 5.4. utvrđuju se zahtjevi koji su specifični za mehanizam prijenosa s API-jem kao posrednikom;

(8) 5.2. Requirements on EUDI Wallet and RP support (Zahtjevi za EU lisnicu za digitalni identitet i podršku pouzdajuće strane)

— ISO/IEC 18013-SUPPORT-01: Jedinice lisnice, pružatelji PID-ova, pružatelji potvrda, pružatelji lisnica i pouzdajuće strane ne smiju podržavati dohvaćanje s poslužitelja kako je specificirano u normi ISO/IEC 18013-5 [10] za traženje i predočavanje atributa osobnih identifikacijskih podataka ili potvrda.

— ISO/IEC 18013-SUPPORT-02: EU lisnica za digitalni identitet mora ispunjavati zahtjeve definirane u točkama 5.3. i 5.4. ovog dokumenta.

— ISO/IEC 18013-SUPPORT-04: Pouzdajuća strana trebala bi implementirati profil definiran u točki 5.4. ovog dokumenta.

(9) 5.3.2. ISO/IEC-mdoc EAAP Request contents (Sadržaj EEAP zahtjeva u formatu ISO/IEC-mdoc)

— ISO/IEC 18013-5-REQ-04: Zahtjevi uređaja poslani EU lisnicama za digitalni identitet moraju sadržavati par ključ-vrijednost „requestInfo” specificiran u točki 8.3.2.1.2.1. norme [10]. Vrijednost tog para je tipa RequestInfo.

— IEC 18013-5-REQ-05: Tip RequestInfo mora biti u skladu s CDDL definicijom u nastavku.

```
RequestInfo = {

    'euWrprc': bstr ; sadržava registracijski certifikat (zahtjeve vidjeti u nastavku)

}
```

— ISO/IEC 18013-5-REQ-06: Navedeni član requestInfo sadržava član s oznakom „euWrprc”

— ISO/IEC 18013-5-REQ-07: Vrijednost „euWrprc” mora biti registracijski certifikat enkodiran u CBOR-u.

— IEC 18013-5-REQ-08: nevažeće.

— *NAPOMENA 3:* nevažeće.

— ISO/IEC 18013-5-REQ-09: nevažeće.

— IEC 18013-5-REQ-10: nevažeće.

— ISO/IEC 18013-5-REQ-11: nevažeće.

(10) 5.3.3. ISO/IEC-mdoc EAAP Response profile (Profil EEAP odgovora u formatu ISO/IEC-mdoc)

— U ovoj su točki utvrđeni zahtjevi za tip poruke DeviceResponse, koja je zajednička za dvije vrste mehanizma prijenosa (s API-jem kao posrednikom i bez API-ja).

— *NAPOMENA 1:* Ako se upotrebljava mehanizam bez API-ja koji se temelji na normi ISO/IEC 18013-5 [10], EAAP odgovor mora biti točno instanca DeviceResponse kako je profilirana u ovoj točki. Ako se upotrebljava mehanizam s API-jem kao posrednikom koji se temelji na Prilogu C normi ISO/IEC 18013-7 [16], instanca DeviceRequest mora biti upakirana kako je specificirano u Prilogu C normi [16].

— ISO/IEC 18013-5-RESP-02: Pružatelj osobnih identifikacijskih podataka i elektroničkih potvrda atributa ne smije uključiti nikakve podatkovne elemente u mapu KeyAuthorisations u mobilnom sigurnosnom objektu osobnih identifikacijskih podataka i elektroničkih potvrda atributa koje izdaje, osim podatkovnih elemenata koje pouzdajuća strana lisnice daje u transakcijskim podacima u mdoc zahtjevu koji jedinica lisnice treba potpisati ili zapečatiti privatnim ključem osobnih identifikacijskih podataka ili elektroničkih potvrda atributa.

— *NAPOMENA 2:* Zbog toga jedinice lisnice pouzdajućim stranama lisnice ne mogu predočavati nikakve podatkovne elemente koje je potpisao uređaj, osim u slučaju potpisivanja podataka koje je dostavila pouzdajuća strana lisnice, na primjer kad je potrebna sigurna autentifikacija korisnika.

— *NAPOMENA 3:* U normi ISO/IEC 18013-5:2021 nije određeno kako pouzdajuće strane lisnice mogu uključiti transakcijske podatke u mdoc zahtjev. Za uključivanje tih podataka u mdoc zahtjev nužne su dodatne tehničke specifikacije.

— ISO/IEC 18013-5-RESP-03: Pružatelji osobnih identifikacijskih podataka ne dopuštaju privatnom ključu osobnih identifikacijskih podataka potpisivanje podatkovnih elemenata koje je pouzdajuća strana lisnice dala u transakcijskim podacima u mdoc zahtjevu.

(11) 5.4. Requirements for API mediated mechanism (Zahtjevi za mehanizam s API-jem kao posrednikom)

5.4.1. ISO/IEC 18013-7-related requirements (Zahtjevi povezani s normom ISO/IEC 18013-7)

U ovoj su točki utvrđeni zahtjevi za mehanizam prijenosa s API-jem kao posrednikom povezani sa zahtjevima definiranima u Prilogu C normi [16].

— ISO/IEC 18013-7-API-01: Profil koji podržava predočavanja s API-jem kao posrednikom mora ispunjavati zahtjeve iz Priloga C normi ISO/IEC 18013-7 [16] kako su dodatno specificirani u točkama 5.3. i 5.4. ovog dokumenta.

— ISO/IEC 18013-7-API-02: Vrijede svi obvezni zahtjevi utvrđeni u Prilogu C normi [16] kako su dodatno specificirani u točkama 5.3. i 5.4. ovog dokumenta.

— ISO/IEC 18013-7-API-03: Svi neobvezni zahtjevi iz Priloga C normi [16] ostaju neobvezni osim ako je u ovom dokumentu navedeno drukčije.

(12) 5.4.2. Additional requirements (Dodatni zahtjevi)

— U ovoj su točki utvrđeni dodatni zahtjevi za mehanizam prijenosa s API-jem kao posrednikom.

— ISO/IEC 18013-ADD-API-01: EU lisnica za digitalni identitet API-ju posredniku koji radi u skladu s Prilogom C normi [16] mora po zadanim postavkama javiti koje sve vrste elektroničkih potvrda atributa pohranjuje, ali mu ne smije javiti atribute i njihove vrijednosti u tim potvrdama.

  — *NAPOMENA 1:* Zabrana za vrijednosti atributa primjenjuje se čak i ako bi javljanje poboljšalo usluge koje operativni sustav pruža EU lisnici za digitalni identitet, primjerice odabir potvrda kad djeluje kao API posrednik.

— Ima čimbenika povezanih s operativnim sustavima i preglednicima koji su izvan kontrole implementatora, a mogu se uzeti u obzir kako je navedeno u sljedećim napomenama od 2. do 4.:

  — *NAPOMENA 2:* Preglednik i/ili operativni sustav mogu obraditi zahtjev za predočenje od pouzdajuće strane koja podržava Prilog C normi [16] radi traženja dostupnih elektroničkih potvrda atributa, sprečavanja prijevara korisnika ili rješavanja problema.

  — *NAPOMENA 3:* Od preglednika i/ili operativnog sustava očekuje se da će obraditi zahtjev za predočenje od pouzdajuće strane koja podržava Prilog C normi [16] kad je to potrebno za sigurnost korisnika.

— *NAPOMENA 4:* Od preglednika i/ili operativnog sustava očekuje se da neće obraditi zahtjev za predočenje od pouzdajuće strane koja podržava Prilog C normi [16] za potrebe analize tržišta (čak ni kad je to sekundarna svrha) ili za interne potrebe preglednika i/ili operativnog sustava.

— ISO/IEC 18013-ADD-API-02: Ako EU lisnica za digitalni identitet na korisnikov zahtjev izbriše PID ili EAA koji je već javljen API-ju posredniku koji radi u skladu s Prilogom C normi [16], onda tom API-ju mora javiti da više nema pohranjen taj PID ili EAA.

— ISO/IEC 18013-ADD-API-03: Ako korisnik deinstalira svoju EU lisnicu za digitalni identitet, ona API-ju posredniku koji radi u skladu s Prilogom C normi [16] mora javiti da više nema pohranjene već javljene PID-ove ili EAA-ove.

— ISO/IEC 18013-ADD-API-04: EU lisnica za digitalni identitet mora imati univerzalnu postavku koja korisniku omogućuje da spriječi javljanje pohranjenih EAA-ova putem API-ja posrednika koji radi u skladu s normom ISO/IEC 18013-ADD-API-01. Kad je ta postavka isključena, EU lisnica za digitalni identitet ne smije signalizirati spremnost za ni odgovarati na zahtjeve za predočavanje ili izdavanje upućene posredstvom API-ja.

— ISO/IEC 18013-ADD-API-05: Kad je riječ o međuuređajnim (*cross-device*) tokovima, EU lisnica za digitalni identitet mora preko API-ja posrednika provjeriti da se uređaj koji je u interakciji nalazi u njezinoj neposrednoj fizičkoj blizini korištenjem sigurnog i izravnog lokalnog komunikacijskog kanala s korisnikom kao posrednikom, kao što je bežična komunikacijska tehnologija kratkog dometa, za provjeru fizičke blizine.

— *NAPOMENA:* CTAP 2.3 omogućuje da se za provjeru neposredne fizičke blizine koristi BLE, a kad je implementiran na oba uređaja, omogućuje i prijenos podataka između njih tehnologijama prijenosa malog dometa. Temeljni operativni sustavi, preglednici, API-ji posrednici i svi drugi tehnički slojevi izvan kontrole EU lisnice za digitalni identitet trebali bi za obavljanje provjere fizičke blizine i prijenosa podataka između dva uređaja prednost davati korištenju lokalnog komunikacijskog kanala prema CTAP-u 2.3, a ne CTAP-ovu hibridnom tunelu.

(13) 6.2. Requirements on EUDI Wallet and RP support (Zahtjevi za EU lisnicu za digitalni identitet i podršku pouzdajuće strane)

— OIDFVP-HAIP-SUPPORT-02: EU lisnica za digitalni identitet mora ispunjavati zahtjeve iz točke 6.5. ovog Priloga.

— OIDFVP-HAIP-SUPPORT-03: Za međuuređajne (*cross-device*) tokove predočavanja EU lisnica za digitalni identitet ne bi trebala podržavati mehanizam koji se temelji na preusmjeravanju određen u točki 6.4. ovog Priloga.

— *NAPOMENA 3:* Korištenje tog mehanizma osjetljivo je na napade, npr. fiksaciju sesije. Ublažavanje takvih napada ovisi o pouzdajućim stranama. Implementacija tog mehanizma ne bi trebala uzrokovati nesukladnost.

— OIDFVP-HAIP-SUPPORT-05: Pouzdajuća strana mora ispunjavati zahtjeve iz točke 6.5. ovog Priloga.

— *NAPOMENA 5:* nevažeće.

(14) 6.3.1. General requirements (Opći zahtjevi)

— OIDFVP-HAIP-GEN-01: Primjenjuju se svi obvezni zahtjevi navedeni u točkama 5., 5.3., 7. i 8. HAIP-a [11].

— *NAPOMENA 1:* „HAIP [11], odjeljak 5." odnosi se samo na zahtjeve izravno pod naslovom odjeljka 5. To ne uključuje odjeljke 5.1., 5.2. i 5.3.

— OIDFVP-HAIP-GEN-03: Ako se ovim Prilogom mijenja zahtjev iz specifikacije OpenID4VC-HAIP [11], prednost ima izmijenjeni zahtjev utvrđen ovim Prilogom.

— *NAPOMENA 2:* To bi, na primjer, omogućilo pretvaranje neobveznog zahtjeva iz specifikacije OpenID4VC-HAIP [11] u obvezni ili proširenje obveznih zahtjeva.

— OIDFVP-HAIP-GEN-04: Ako je format tražene potvrde sukladan s normom [10], pouzdajuće strane i EU lisnice za digitalni identitet moraju biti sukladne s profilom „ISO mdocs” iz odjeljka 6. specifikacije [11].

— *NAPOMENA 3:* Radi jasnoće: „ISO mdocs profile” u HAIP-u podrazumijeva da pouzdajuće strane i EU lisnice za digitalni identitet moraju ispunjavati mjerodavne zahtjeve iz [7] Priloga B.2.

— OIDFVP-HAIP-GEN-05: Ako je format tražene potvrde sukladan s normom [2], pouzdajuće stranke i EU lisnice za digitalni identitet moraju biti sukladne s profilom IETF SD-JWT VCs iz odjeljka 6. specifikacije [11].

— *NAPOMENA 4:* Radi jasnoće: „IETF SD-JWT VCs profile” podrazumijeva da pouzdajuće strane i EU lisnice za digitalni identitet moraju ispunjavati zahtjeve iz [7] Priloga B.3. i zahtjeve iz odjeljka 6.1. specifikacije [11].

(15) 6.3.2.1. General requirements (Opći zahtjevi)

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

(16) 6.3.2.2. Requirements for the Request Object (Zahtjevi za Request Object)

— OIDFVP-HAIP-COMMON-REQ-RO-02: nevažeće.

— OIDFVP-HAIP-COMMON-REQ-RO-03: nevažeće.

— OIDFVP-HAIP-COMMON-REQ-RO-04: nevažeće.

— OIDFVP-HAIP-COMMON-REQ-RO-05: nevažeće.

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

— OIDFVP-HAIP-COMMON-REQ-RO-07: nevažeće.

— OIDFVP-HAIP-COMMON-REQ-RO-08: nevažeće.

— OIDFVP-HAIP-COMMON-REQ-RO-09: nevažeće.

— OIDFVP-HAIP-COMMON-REQ-RO-10: nevažeće.

— OIDFVP-HAIP-COMMON-REQ-RO-11: nevažeće.

— OIDFVP-HAIP-COMMON-REQ-RO-12: nevažeće.

— *Napomena 2:* nevažeće.

— OIDFVP-HAIP-COMMON-REQ-RO-13: Jedan od elemenata parametra verifier_info mora sadržavati registracijski certifikat.

— OIDFVP-HAIP-COMMON-REQ-RO-23: Certifikat krajnjeg subjekta (*leaf*) iz odjeljka 5.9.3. OpenID4VP-a za upotrebu s x509_hash Client Identifier Prefix mora biti pristupni certifikat RP-u kako je specificiran u normi ETSI TS 119 475 [14].

(17) 6.3.3. Authorization Response (EAAP response) profile (Profil autorizacijskog odgovora (EEAP odgovora))

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

(18) 6.4.1. General requirements (Opći zahtjevi)

— OIDFVP-HAIP-REDIRECTS-04: nevažeće.

— *NAPOMENA:* nevažeće.

(19) 6.5.2. Additional requirements (Dodatni zahtjevi)

— OIDFVP-HAIP-ADD-API-01: EU lisnica za digitalni identitet po zadanim postavkama API-ju posredniku koji radi u skladu s točkom 5.2. specifikacije [11] mora javiti koje sve vrste elektroničkih potvrda atributa pohranjuje, ali mu ne smije javiti atribute i njihove vrijednosti u tim potvrdama.

— OIDFVP-HAIP-ADD-API-04: Ako EU lisnica za digitalni identitet podržava API posrednik koji radi prema OIDFVP-HAIP-ADD-API-01, ona mora imati univerzalnu postavku kojim korisnik može spriječiti javljanje pohranjenih EAA-ova preko API-ja posrednika. Kad se ta postavka namjesti tako da sprečava javljanje, EU lisnica za digitalni identitet trebala bi zatim omogućiti korisniku da odabere pojedinačne potvrde koje se mogu javiti API-ju posredniku.

— OIDFVP-HAIP-ADD-API-05: Kad je riječ o međuuređajnim (*cross-device*) tokovima, EU lisnica za digitalni identitet mora provjeriti, preko API-ja posrednika, da se uređaj koji je u interakciji nalazi u njezinoj neposrednoj fizičkoj blizini korištenjem sigurnog i izravnog lokalnog komunikacijskog kanala s korisnikom kao posrednikom, kao što je bežična komunikacijska tehnologija kratkog dometa, za provjeru fizičke blizine.

— *NAPOMENA 5:* CTAP 2.3 omogućuje da se za provjeru neposredne fizičke blizine koristi BLE, a kad je implementiran na oba uređaja, omogućuje i prijenos podataka između njih tehnologijama prijenosa malog dometa. Temeljni operativni sustavi, preglednici, API-ji posrednici i svi drugi tehnički slojevi izvan kontrole EU lisnice za digitalni identitet trebali bi za obavljanje provjere fizičke blizine i prijenosa podataka između dva uređaja prednost davati korištenju lokalnog komunikacijskog kanala prema CTAP-u 2.3, a ne CTAP-ovu hibridnom tunelu.

(20) 6.5.3. Specific requirements when requesting ISO/IEC 18013-5 EAAP

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Svi zahtjevi u ovom dokumentu koji vrijede za strukture zahtjeva uređaju i odgovora uređaja specificirane u normi ISO/IEC 18013-5 vrijede i kad EU lisnica za digitalni identitet primi zahtjev za ISO/IEC mdoc predočenje putem mehanizma prijenosa preko API-ja iz točke C.1. norme [16].”