Euroopa Liidu
Teataja

ET
L-seeria

2026/1731

22.7.2026

KOMISJONI RAKENDUSMÄÄRUS (EL) 2026/1731,

15. juuli 2026,

millega muudetakse rakendusmäärusi (EL) 2024/2977, (EL) 2024/2979, (EL) 2024/2980 ja (EL) 2024/2982 kohaldatavate standardite ja spetsifikatsioonide osas

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ), ([1]) eriti selle artikli 5a lõiget 23,

ning arvestades järgmist:

(1) Et tagada Euroopa digiidentiteedikukrute arendamise jaoks kõrgeimal tasemel ühtlustamine liikmesriikide vahel, tuginevad kukrute tehnilised spetsifikatsioonid tööle, mida on tehtud komisjoni soovituse (EL) 2021/946 ([2]) põhjal, ja eeskätt selle osaks olevale arhitektuurile ja võrdlusraamistikule. Kuna arhitektuur ja võrdlusraamistik on pärast komisjoni rakendusmääruste (EL) 2024/2977, ([3]) (EL) 2024/2979, ([4]) (EL) 2024/2980 ([5]) ja (EL) 2024/2982 ([6]) vastuvõtmist märkimisväärselt muutunud, tuleks nimetatud rakendusmäärusi nüüd muuta, et viia need uute standardite, spetsifikatsioonide ja menetlustega kooskõlla.

Kooskõlas määruse (EL) nr 910/2014 eesmärkidega on selliste erinõuete täitmiseks välja valitud mitu standardit. Standardid peaksid kajastama väljakujunenud tavasid ja olema asjaomastes sektorites laialdaselt tunnustatud. Näiteks kuna tõendite standardvorminguna kasutatakse eriti haridussektoris W3C VCDM-vormingut, peaksid Euroopa digiidentiteedikukrud jätkama selle vormingu toetamist ka pärast W3C VCDM-vormingu kättesaadavaks muutumist. Vajaduse korral tuleks neid standardeid kohandada või täiendada, et tagada Euroopa digiidentiteedikukrute turvalisus ja usaldusväärsus ning soodustada samal ajal piiriülest koostalitlusvõimet ja siseturu tõrgeteta toimimist.

(2) Kõigil kukru kasutamise juhtudel, mille puhul tuleb esitada kukrukasutaja portreefoto, peab kukrulahendus toetama võimalust avaldada andmeid valikuliselt ja avaldamine peab olema kasutaja täieliku kontrolli all. Selleks et tagada võimalus otsustada avaldamise üle ja portreefoto kaitse ebasihipäraste või loata avaldamistaotluste eest, peaks Euroopa digiidentiteedikukru arhitektuuri ülesehitus olema varustatud hoiatusmehhanismidega ja logima kõik portreefoto kasutamisega seotud tehingud. Selleks et kukrukasutaja oleks kindlasti teadlik, et ta jagab biomeetrilisi andmeid, peaks hoiatustes olema ära näidatud, et taotlusega kaasneb biomeetriliste andmete jagamine, ja nõutud

([1]) ELT L 257, 28.8.2014, lk 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Komisjoni 3. juuni 2021. aasta soovitus (EL) 2021/946, mis käsitleb ühiseid liidu tööriistu Euroopa digiidentiteedi raamistiku koordineeritud käsitlusviisi jaoks (ELT L 210, 14.6.2021, lk 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([3]) Komisjoni 28. novembri 2024. aasta rakendusmäärus (EL) 2024/2977, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses Euroopa digiidentiteedikukrutesse väljastatavate isikutuvastusandmete ja elektrooniliste tõenditega (ELT L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).
([4]) Komisjoni 28. novembri 2024. aasta rakendusmäärus (EL) 2024/2979, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses Euroopa digiidentiteedikukrute tervikluse ja tuumikfunktsioonidega (ELT L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).
([5]) Komisjoni 28. novembri 2024. aasta rakendusmäärus (EL) 2024/2980, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses komisjonile Euroopa digiidentiteedikukrute ökosüsteemi kohta saadetavate teavitustega (ELT L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).
([6]) Komisjoni 28. novembri 2024. aasta rakendusmäärus (EL) 2024/2982, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses protokollide ja liidestega, mida Euroopa digiidentiteedi raamistik peab toetama (ELT L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

kasutajalt eraldi kinnitust avaldamise kohta. Kui tuginev isik töötleb portreefotot füüsilise isiku üheseks identimiseks või selle isiku väidetava identiteedi kinnitamiseks, kohaldatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 ([7]) artikleid 6 ja 9, samuti kõiki muid kõnealuse määruse kohaseid nõudeid, sealhulgas nõuet, et portreefoto töötlemine tuginevate isikute poolt peaks piirduma kavandatud kasutusotsarbel vajalikuga. Kavandatud kasutusotstarve ja avaldamistaotlus tuleks kasutajale esitada selges ja arusaadavas keeles. Selleks et võtta nõuetekohaselt arvesse biomeetriliste andmete tundlikkust, peaks kukrukasutaja portreefoto avaldamise sõnaselgelt ja konkreetselt kinnitama. Vaikimist või eelmärgistatud kastikesi ei tuleks lugeda kukrukasutaja kinnituseks. Kukrukasutaja sõnaselge kinnitus peaks olema tehniline kaitsemeede ja mitte andma iseenesest seaduslikku alust töötlemiseks. Vastavalt määruse (EL) 2016/679 artikli 9 lõikele 4 võivad liikmesriigid säilitada või kehtestada täiendavad tingimused, sealhulgas piirangud seoses geneetiliste, biomeetriliste või terviseandmete töötlemisega.

(3) Selleks et anda liikmesriikidele küllaldaselt aega oma riigisiseste menetluste kohandamiseks, võib kukrukasutaja portreefoto olla füüsiliste isiku identimiseks kohustuslike isikutuvastusandmete hulgas alles alates 11. augustist 2028. Kui nimetatud kujutiste allikaks on olemasolev isikut tõendav dokument, nagu isikut tõendav dokument või pass, kohaldatakse vastavalt kas nõukogu määrusega (EL) 2025/1208 ([8]) või nõukogu määrusega (EÜ) nr 2252/2004 ([9]) kehtestatud nõudeid.

(4) Määruse (EL) nr 910/2014 kohaselt peab kukkur võimaldama kuvada ELi digiidentiteedikukru usaldusmärki kui kontrollitavat, lihtsat ja äratuntavat märget selle kohta, et kukrut pakutakse kooskõlas määrusega. Sellise usaldusmärgi kasutamine soodustab siseturu tõrgeteta toimimist, tagab ausa konkurentsi ja kaitseb tarbijate huve. Sellise usaldusmärgi kasutamise võimaldamiseks tuleks kindlaks määrata usaldusmärgi visuaalsed ja tehnilised näitajad.

(5) Vastavalt määruse (EL) nr 910/2014 artiklile 12b, peavad pääsuvalitsejad võimaldama Euroopa digiidentiteedikukru pakkujatele ja teavitatud e-identimise vahendite väljastajatele tõhusa koostalitlusvõime sama operatsioonisüsteemi ja samade riist- või tarkvarafunktsioonidega ning koostalitlusvõime eesmärgil juurdepääsu sellistele funktsioonidele. Selline tõhus koostalitlusvõime ja juurdepääs peab olema tasuta ja ei tohi oleneda sellest, kas riist- või tarkvarafunktsioonid on osa operatsioonisüsteemist või on asjaomasele pääsuvalitsejale selliste teenuste osutamisel kättesaadavad või tema kasutuses. Selleks et tagada kõigis liikmesriikides kasutatavus, turvalisus ja koostalitlusvõime, peaksid kõik kukrulahendused toetama ühtset protokollide ja liideste kogumit; seepärast peaksid pääsuvalitsejad võimaldama operatsioonisüsteemi ning riist- või tarkvarafunktsioone, mis on vajalikud käesoleva määruse XII lisas esitatud protokollide ja liideste rakendamiseks. Selles kontekstis peaksid pääsuvalitsejad eelistama veebis seadmetevaheliste voogude puhul nii füüsiliseks läheduskontrolliks kui ka andmete ühest seadmest teise edastamiseks protokolli *Client To Authenticator Protocol* (CTAP) hübriidtunnelduse teenustele CTAPi spetsifikatsiooni versiooni 2.3 ([10]).

(6) Selleks et anda liikmesriikidele, kukrule tuginevate isikute registreerimissertifikaatide pakkujatele ja kukruteenuse pakkujatele küllaldaselt aega, et võimaldada kukrukomplektidel kukrule tuginevate isikute registreerimissertifikaatide autentsust ja kehtivust kinnitada, tuleks seda nõuet kohaldada alles alates 11. augustist 2028.

(7) Isikuandmete kõigi selliste töötlemistoimingute suhtes, mis toimuvad käesoleva määruse alusel, kohaldatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2016/679 ning vajaduse korral Euroopa Parlamendi ja nõukogu direktiivi 2002/58/EÜ ([11]).

([7]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Nõukogu 12. juuni 2025. aasta määrus (EL) 2025/1208, mis käsitleb liidu kodanike isikutunnistuste ning vaba liikumise õigust kasutavatele liidu kodanikele ja nende pereliikmetele väljaantavate elamislubade turvalisuse suurendamist (ELT L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Nõukogu 13. detsembri 2004. aasta määrus (EÜ) nr 2252/2004 liikmesriikide poolt väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta (ELT L 385, 29.12.2004, lk 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) FIDO liidu kavandatav standard „Client to Authenticator Protocol (CTAP)“, 26. veebruar 2026.

([11]) Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([12]) artikli 42 lõikele 1 on konsulteeritud Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse 17. aprillil 2026 ([13]).

(9) Käesoleva määrusega ette nähtud meetmed on kooskõlas määruse (EL) nr 910/2014 artikli 48 alusel loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Rakendusmääruse (EL) 2024/2977 muudatused

Rakendusmäärust (EL) 2024/2977 muudetakse järgmiselt:

1) lisatakse artikkel 3a:

„*Artikkel 3a*

Portreefoto kaitse

1. Lisaks määruse (EL) 2016/679 kohaste teavitamisnõuete täitmisele tagavad kukruteenuse pakkujad, et nende pakutavate kukrulahendustega hoiatatakse kukrukasutajat, kui kukrule tuginevad isikud taotlevad portreefoto avaldamist, ja antakse teada, et taotlusega kaasneb biomeetriliste andmete jagamine ja see nõuab portreefoto valikulise avaldamise kinnitamist.

2. Portreefoto kukrule tuginevale isikule valikulise avaldamise teostamiseks tagavad kukruteenuse pakkujad, et kukrulahendustega nõutakse kukrukasutajalt sõnaselget ja konkreetset kinnitust portreefoto esitamise kohta.

3. Kukrule tuginevad isikud ei säilita portreefotot, välja arvatud juhul, kui selle töötlemine on vajalik liidu andmekaitseõiguse kohase identimise ja autentimise eesmärgil või kui see on ette nähtud liidu või riigisisese õigusega, kooskõlas liidu andmekaitseõigusega. Portreefotot ei edastata kolmandatele riikidele ega rahvusvahelistele organisatsioonidele, välja arvatud juhul, kui see on liidu andmekaitseõigusega lubatud.“;

2) artikli 4 lõige 1 asendatakse järgmisega:

„1. Kukrukomplektidesse väljastatud elektroonilised tõendid vastavad vähemalt ühele rakendusmääruse (EL) 2024/2979 II lisas esitatud standardile.“;

3) artiklit 5 lõike 4 punkt b asendatakse järgmisega:

„b) kui kehtetuks on tunnistatud selle kukrukomplekti tõend, kuhu isikutuvastusandmed väljastati;“;

4) lisa asendatakse käesoleva määruse I lisas esitatud tekstiga.

([12]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) EDPS Formal comments on the draft Implementing Regulation as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980 | European Data Protection Supervisor.

Artikkel 2

Rakendusmääruse (EL) 2024/2979 muudatused

Rakendusmäärust (EL) 2024/2979 muudetakse järgmiselt:

1) artikli 3 lõige 2 jäetakse välja;

2) artikli 5 lõike 1 punkt a asendatakse järgmisega:

„a) sooritavad kukru krüptograafilisi toiminguid, mis puudutavad kukru turvalises krüptoseadmes säilitatavat kriitilise tähtsusega vara, mida ei ole vaja kukrukasutaja autentimiseks, ainult juhul, kui asjaomased rakendused on kukrukasutaja autentinud;“;

3) lisatakse artikkel 5 a:

„*Artikkel 5a*

Krüptomehhanismid

Artikli 4 lõike 2 kohaldamisel kasutavad kukruteenuse pakkujad ainult Ia lisas osutatud krüptomehhanisme.“;

4) artiklit 6 muudetakse järgmiselt:

a) lõige 1 asendatakse järgmisega:

„1. Kukruteenuse pakkujad väljastavad igale kukrukomplektile kukrukomplekti tõendi. Kukruteenuse pakkujad annavad kukrukomplekti tõendile allkirja või loovad templi selliselt, et allkirju ja templeid saab valideerida sertifikaadiga, mis on vastavalt rakendusmääruse (EL) 2024/2980 II lisa punkti 2 punkti 1 alapunktile h loetellu kantud.“;

b) lõige 2 asendatakse järgmisega:

„2. Kukruteenuse pakkujad tagavad, et lõikes 1 osutatud kukrukomplekti tõendid vastavad Ib lisas esitatud tehnilistele spetsifikatsioonidele.“;

c) lõike 3 punkt b asendatakse järgmisega:

„b) näevad ette kukrukomplektist sõltumatud mehhanismid kukrukasutajate turvaliseks identimiseks ja autentimiseks“;

5) artikli 9 lõike 2 punkt b asendatakse järgmisega:

„b) vastava kukrule tugineva isiku nimi, kontaktandmed ja kordumatu tunnus ning liikmesriik, kus see kukrule tuginev isik on asutatud;“;

6) artikli 10 lõige 1 asendatakse järgmisega:

„1. Kukruteenuse pakkujad tagavad, et III lisas esitatud ühise lõimitud avalikustamispoliitika suhtes kohaldatavate tehniliste spetsifikatsioonide kohaselt väljastatud elektroonilisi tõendeid on võimalik nende pakutavates kukrukomplektides töödelda.“;

7) artiklit 12 muudetakse järgmiselt:

a) lõike 2 punkt c asendatakse järgmisega:

„c) allkirjade või templite loomine, mis on kooskõlas vähemalt IV lisas osutatud kohustusliku vorminguga;“;

b) lõige 3 asendatakse järgmisega:

„3. Allkirja andmise rakendused võivad olla kukrueksemplari integreeritud või selle välised.“;

c) lisatakse järgmine lõige:

„4. Kukrukomplektides kasutatavad allkirja andmise rakendused peavad toetama vähemalt IV lisas osutatud rakendusliidest.“;

8) artikli 14 lõige 1 jäetakse välja;

9) lisatakse artikkel 14a:

„*Artikkel 14a*

ELi digiidentiteedikukru usaldusmärk

1. Kukruteenuse pakkujad tagavad, et kukrukomplektid kuvavad ELi digiidentiteedikukru usaldusmärki. ELi digiidentiteedikukru usaldusmärk esitatakse VI ja VII lisas kindlaksmääratud kujul.

2. Kukruteenuse pakkujad tagavad, et kukrukomplektid võimaldavad kukrukasutajatel kasutada teavet, mille alusel nad saavad kontrollida kukrulahenduse sertifitseerimise staatust. Sel eesmärgil tagavad kukruteenuse pakkujad, et pärast kukrulahenduse registreerimist sisaldavad vastavad kukrukomplektid URLe, mille Euroopa Komisjon on nimetatud kontrolli eesmärgil esitanud. Kukruteenuse pakkujad tagavad, et nende kukrukomplektidel on juurdepääs ELi digiidentiteedikukru usaldusmärgi andmetele, mis vastavad VIII lisas esitatud tehnilistele spetsifikatsioonidele.

3. ELi digiidentiteedikukru usaldusmärgi etalonvärvid on Pantone 661 ja 116 või neljavärvitrüki kasutamisel sinine (100 % tsüaansinine + 67 % magenta + 0 % kollane + 40 % must) ja kollane (0 % tsüaansinine + 20 % magenta + 100 % kollane + 0 % must); RGB-mudeli kasutamisel on etalonvärvid sinine (punane 0 + roheline 51 + sinine 153) ja kollane (punane 255 + roheline 204 + sinine 0).

4. ELi digiidentiteedikukru usaldusmärki võib VII lisas esitatud must-valgel kujul kasutada ainult juhul, kui värve ei ole võimalik kasutada.

5. Kui ELi digiidentiteedikukru usaldusmärki kasutatakse tumedal taustal, võib seda kasutada negatiivis, kasutades sama taustavärvi. Kui ELi digiidentiteedikukru usaldusmärki kasutatakse värvilisena värvilisel taustal, mistõttu on seda raske eristada, võib usaldusmärgi ja taustavärvi kontrasti suurendamiseks ümbritseda usaldusmärgi piirjoonega.

6. ELi digiidentiteedikukru usaldusmärgi minimaalne suurus on 64 × 85 pikslit eraldusvõimega 150 dpi.

7. Kukruteenuse pakkujad tagavad, et ELi digiidentiteedikukru usaldusmärki kasutatakse viisil, mis võimaldab ELi digiidentiteedikukru usaldusmärki kandvat kukrukomplekti selgelt märgistada. ELi digiidentiteedikukru usaldusmärki võib kasutada koos graafiliste või tekstielementidega, mis seda kandvat kukrukomplekti selgelt märgistavad, tingimusel et need ei muuda ELi digiidentiteedikukru usaldusmärgi äratuntavust ega moonuta seost määruse (EL) nr 910/2014 artiklis 5d osutatud sertifitseeritud Euroopa digiidentiteedikukrute loeteluga.

8. Kui kukruteenuse pakkujad on kukrukomplekti tõendi kehtetuks tunnistanud, peavad nad tagama, et vastav kukrukomplekt ei kanna enam ELi digiidentiteedikukru usaldusmärki.“;

10) lisatakse Ia ja Ib lisa vastavalt käesoleva määruse II lisale ja III lisale;

11) II lisa asendatakse käesoleva määruse IV lisas esitatud tekstiga;

12) III lisa asendatakse käesoleva määruse V lisas esitatud tekstiga;

13) IV lisa muudetakse vastavalt käesoleva määruse VI lisale;

14) V lisa jäetakse välja;

15) käesoleva määruse VII lisas esitatud tekst lisatakse VI lisana;

16) käesoleva määruse VIII lisas esitatud tekst lisatakse VII lisana;

17) käesoleva määruse IX lisas esitatud tekst lisatakse VIII lisana.

Artikkel 3

Rakendusmääruse (EL) 2024/2980 muudatused

Rakendusmäärust (EL) 2024/2980 muudetakse järgmiselt:

1) artikli 5 lõige 2 asendatakse järgmisega:

„2. Kui see on asjakohane, koostab komisjon loetelu, kuhu koondatakse II lisa punktides 2, 3, 4 ja 5 osutatud informatsioon, mille liikmesriigid on esitanud kukruteenuse pakkujate, isikutuvastusandmete pakkujate, kukrule tuginevate isikute pääsusertifikaatide pakkujate ja kukrule tuginevate isikute registreerimissertifikaatide pakkujate kohta, haldab nimetatud loetelu ja avaldab selle.“

2) Rakendusmääruse (EL) 2024/2980 II lisa muudetakse vastavalt käesoleva määruse X lisale.

Artikkel 4

Rakendusmääruse (EL) 2024/2982 muudatused

Rakendusmäärust (EL) 2024/2982 muudetakse järgmiselt:

1) artikli 1 punkt 2 asendatakse järgmisega:

„2) esitada kukrule tuginevatele isikutele isikutuvastusandmete ja elektrooniliste tõendite atribuute;“;

2) artiklit 3 muudetakse järgmiselt:

a) punkt 1 asendatakse järgmisega:

„1) kinnitavad kukrule tuginevate isikutega interaktsioonis olles kukrule tuginevate isikute pääsusertifikaatide autentsust ja kehtivust, ilma et nad delegeeriksid nende protsesside täitmist operatsioonisüsteemile, veebibrauserile või muule vaherakendusele;“;

b) punkt 2 jäetakse välja;

c) punkt 3 asendatakse järgmisega:

„3) kinnitavad selliste taotluste autentsust ja kehtivust, mille puhul on kasutatud kukrule tuginevate isikute pääsusertifikaate;“;

d) punkt 4 asendatakse järgmisega:

„4) kinnitavad kukrule tugineva isiku registreerimissertifikaadi autentsust ja kehtivust;“;

e) punkt 5 asendatakse järgmisega:

„5) kuvavad kukrukasutajatele kukrule tugineva isiku pääsusertifikaatides sisalduvat teavet;“;

f) punkt 8 jäetakse välja;

g) punkt 9 asendatakse järgmisega:

„9) ei esita kukrule tuginevatele isikutele ühtegi küsitud atribuuti enne, kui on sooritatud järgmised toimingud:

a) on kontrollitud, et kukrukomplekt on töödelnud lõimitud avalikustamispoliitikat kooskõlas rakendusmääruse (EL) 2024/2979 artikliga 10;

b) on kontrollitud, et kukrukasutajad on esitamise osaliselt või täielikult heaks kiitnud.“;

3) artikli 4 lõige 1 asendatakse järgmisega:

„1. Kukruteenuse pakkujad tagavad, et kukrulahendused toetavad I lisas loetletud protokolle ja liideseid isikutuvastusandmete ja elektrooniliste tõendite väljastamiseks kukrukomplektidesse.“;

4) artiklit 5 muudetakse järgmiselt:

   a) lõiked 1 ja 2 asendatakse järgmisega:

      „1. Kukruteenuse pakkujad tagavad, et kukrulahendused toetavad protokolle ja liideseid atribuutide esitamiseks kukrule tuginevatele isikutele kaugside vahendusel ja vajaduse korral lähiside abil kooskõlas II lisas esitatud tehniliste spetsifikatsioonidega.

      2. Kukruteenuse pakkujad tagavad, et kasutaja taotluse korral vastavad kukrulahendused kukrule tuginevate isikute autentseks ja kehtivaks tunnistatud taotlustele, millele on osutatud artiklis 3, kooskõlas II lisas esitatud tehniliste spetsifikatsioonidega.“;

   b) lõige 5 jäetakse välja;

5) artikkel 8 asendatakse järgmisega:

   „*Artikkel 8*

   Jõustumine

   Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

   Artikli 3 lõiget 4 kohaldatakse alates 11. augustist 2028.

   Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.“;

6) lisa jäetakse välja;

7) käesoleva määruse XI lisas esitatud tekst lisatakse I lisana;

8) käesoleva määruse XII lisas esitatud tekst lisatakse II lisana.

Artikkel 5

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 15. juuli 2026

Komisjoni nimel
president
Ursula VON DER LEYEN

I LISA

„LISA

Artikli 3 lõikes 3 osutatud isikutuvastusandmete tehnilised kirjeldused

1. 1. jagu. Isikutuvastusandmete kogum: füüsiline isik

Tabel 1

Füüsilise isiku puhul kohustuslikud isikutuvastusandmed valikulise avalikustamise korral

Andmete identifikaator	Määratlus
`family_name`	Selle kasutaja praegune perekonnanimi / praegused perekonnanimed, kelle kohta isikutuvastusandmed käivad
`given_name`	Selle kasutaja praegune eesnimi / praegused eesnimed (sealhulgas vajaduse korral keskmine nimi / keskmised nimed), kelle kohta isikutuvastusandmed käivad
`birth_date`	Selle kasutaja sünnikuupäev, -kuu ja -aasta, kelle kohta isikutuvastusandmed käivad
`birth_place`	Riik (standardis ISO 3166-1 esitatud kahetähelise (alpha-2) riigikoodina) või liidumaa, provints, rajoon, kohalik piirkond või omavalitsusüksus, linn või küla, kus kasutaja, kelle kohta isikutuvastusandmed käivad, sündis
`nationality`	Standardis ISO 3166-1 esitatud kahetäheline (alpha-2) riigikood/riigikoodid, mis tähistab/tähistavad selle kasutaja kodakondsust, kelle kohta isikutuvastusandmed käivad
`portrait`	Välja arvatud juhul, kui kasutaja sellest sõnaselgelt keeldub, kui see on asjakohane, selle kasutaja näokujutis, kelle kohta isikutuvastusandmed käivad, mis vastab tervikliku eestvaates näokujutise kvaliteedinõuetele, mida on kirjeldatud standardis ISO/IEC 39794-5, või tagasiühilduvusnõuetele, mida on kirjeldatud standardi ISO/IEC 19794-5 punktides 8.2, 8.3 ja 8.4, ning mis esitatakse kodeeritud kujutise andmetena, millel puuduvad andmepäised või -plokid, nagu on kirjeldatud standardi ISO/IEC 19794-5 punktis 5, välja arvatud kujutise enese andmed (JPEG) – kohaldatakse alates 11. augustist 2028

— Liikmesriigid võivad ette näha, et kasutajal on võimalik keelduda portreefoto lisamisest isikutuvastusandmetele.

— Liikmesriigid tagavad, et valikulist avalikustamist kohaldatakse kõikide andmete identifikaatorite, sealhulgas portree suhtes.

— Kui füüsilise isiku sünnikuupäev ei ole teada, valivad liikmesriigid sobivad väärtused, mis vastavad käesoleva lisa punktiga 4.1 või 4.2 (vastavalt vajadusele) ette nähtud kirjeldustele.

— Kui füüsilise isiku kodakondsus ei ole teada, kasutavad liikmesriigid väärtust 'QU'.

— Kui füüsilisel isikul puudub kodakondsus, kasutavad liikmesriigid väärtust 'QS'.

— Kui kasutaja keeldub portreefoto lisamisest, määrab liikmesriik väärtuseks empty.

Tabel 2

Füüsilise isiku puhul vabatahtlikud isikutuvastusandmed valikulise avalikustamise korral

Andmete identifikaator	Määratlus
resident_address	Selle koha täielik aadress, kus kasutaja, kelle kohta isikutuvastusandmed käivad, praegu elab või kus temaga saab ühendust võtta (tänavanimi, majanumber, linn jne)
resident_country	Riik (standardis ISO 3166-1 esitatud kahetähelise (alpha-2) riigikoodina), kus kasutaja, kelle kohta isikutuvastusandmed käivad, parajasti elab
resident_state	Liidumaa, provints, rajoon või kohalik piirkond, kus kasutaja, kelle kohta isikutuvastusandmed käivad, parajasti elab
resident_city	Omavalitsusüksus, linn või küla, kus kasutaja, kelle kohta isikutuvastusandmed käivad, parajasti elab
resident_postal_code	Selle koha sihtnumber, kus kasutaja, kelle kohta isikutuvastusandmed käivad, parajasti elab
resident_street	Selle tänava nimi, kus kasutaja, kelle kohta isikutuvastusandmed käivad, parajasti elab (sealhulgas majanumber ja võimalikud liited)
personal_administrative_-number	Kasutajale, kelle kohta isikutuvastusandmed käivad, määratud väärtus, mis on kõigi isikutuvastusandmete pakkuja väljastatud personaalsete haldusnumbrite seas kordumatu Kui liikmesriigid otsustavad selle atribuudi kasutusele võtta, kirjeldavad nad oma e-identimise süsteemides, mille raames isikutuvastusandmed on väljastatud, milliseid eeskirju nad selle atribuudi väärtuste suhtes rakendavad, sealhulgas vajaduse korral selle väärtuse töötlemise konkreetseid tingimusi
family_name_birth	Selle kasutaja sünnijärgne perekonnanimi / sünnijärgsed perekonnanimed, kelle kohta isikutuvastusandmed käivad
given_name_birth	Selle kasutaja sünnijärgne eesnimi / sünnijärgsed eesnimed (sealhulgas keskmine nimi / keskmised nimed), kelle kohta isikutuvastusandmed käivad
sex	Väärtus tuleb esitada ühena järgmistest: 0 = ei ole teada; 1 = meessoost; 2 = naissoost; 3 = muu; 4 = intersooline; 5 = varia; 6 = määratlemata; 9 = ei kohaldata. Väärtuste 0, 1, 2 ja 9 puhul kohaldatakse standardit ISO/IEC 5218
email_address	Selle kasutaja e-posti aadress, kelle kohta isikutuvastusandmed käivad [kooskõlas standardiga RFC 5322 ([1])]

Andmete identifikaator	Määratlus
`mobile_phone_number`	Selle kasutaja mobiiltelefoni number, kelle kohta isikutuvastusandmed käivad. Numbri ette tuleb rahvusvahelise suunakoodina märkida sümbol „+“ ja riigikood ning see peab koosnema ainult numbritest

([1]) P. Resnick, Ed., „Internet Message Format“, RFC 5322, oktoober 2008.

2. 2. jagu. Isikutuvastusandmete kogum: juriidiline isik

Tabel 3

Juriidilise isiku puhul kohustuslikud isikutuvastusandmed

Andmete identifikaator
Kehtiv juriidiline nimi
Kordumatu tunnus, mille andmeid esitav liikmesriik on loonud vastavalt tehnilistele kirjeldustele piiriülese identimise eesmärgil ja mis on ajas nii muutumatu kui võimalik

— Kui andmete identifikaator ei ole isiku puhul teada või kui seda ei saa muul viisil isikutuvastusandmestiku osana väljastada, kasutab liikmesriik atribuudi puhul konkreetses olukorras sobilikku väärtust.

Tabel 4

Juriidilise isiku puhul vabatahtlikud isikutuvastusandmed

Andmete identifikaator
Kehtiv aadress
Käibemaksukohustuslasena registreerimise number
Maksuviitenumber
Euroopa kordumatu tunnus, millele on osutatud Euroopa Parlamendi ja nõukogu direktiivis (EL) 2017/1132 ([1])
Juriidilise isiku tunnus (LEI), millele on osutatud komisjoni rakendusmääruses (EL) 2022/1860 ([2])
Ettevõtjate registreerimis- ja identifitseerimisnumber (EORI-number), millele on osutatud komisjoni rakendusmääruses (EL) nr 1352/2013 ([3])
Nõukogu määruse (EL) nr 389/2012 ([4]) artikli 2 punktis 12 määratletud aktsiisinumber

([1]) Euroopa Parlamendi ja nõukogu 14. juuni 2017. aasta direktiiv äriühinguõiguse teatavate aspektide kohta (EL) 2017/1132 (ELT L 169, 30.6.2017, lk 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Komisjoni 10. juuni 2022. aasta rakendusmäärus (EL) 2022/1860, millega kehtestatakse rakenduslikud tehnilised standardid Euroopa Parlamendi ja nõukogu määruse (EL) nr 648/2012 kohaldamiseks seoses aruandluse standardite, vormingute, sageduse, meetodite ja korraga (ELT L 262, 7.10.2022, lk 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Komisjoni 4. detsembri 2013. aasta rakendusmäärus (EL) nr 1352/2013, millega kehtestatakse vormid, mis on ette nähtud Euroopa Parlamendi ja nõukogu määrusega (EL) nr 608/2013, mis käsitleb intellektuaalomandi õiguskaitse tagamist tollis (ELT L 341, 18.12.2013, lk 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Nõukogu 2. mai 2012. aasta määrus (EL) nr 389/2012, milles käsitletakse halduskoostööd aktsiisimaksude valdkonnas ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2073/2004 (ELT L 121, 8.5.2012, lk 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3. 3. jagu. Isikutuvastusandmete kohta käivate metaandmete kogum

Tabel 5

Isikutuvastusandmete kohta käivad metaandmed

Andmete identifikaator	Määratlus	Märkimine
`issuing_authority`	Isikutuvastusandmed välja andnud haldusasutuse nimi või vastava liikmesriigi kahetäheline (alpha-2) riigikood vastavalt standardile ISO 3166, kui puudub eraldi asutus, kes on volitatud isikutuvastusandmeid välja andma	Kohustuslik
`issuing_country`	Standardis ISO 3166-1 esitatud kahetäheline (alpha-2) riigikood, mis tähistab isikutuvastusandmete pakkuja riiki või territooriumi	Kohustuslik
`expiry_date`	Isikutuvastusandmete halduskehtivuse aegumise kuupäev (ja võimaluse korral kellaaeg)	Vabatahtlik
`document_number`	Isikutuvastusandmete number, mille on määranud isikutuvastusandmete pakkuja	Vabatahtlik
`issuing_jurisdiction`	Riigi alljaotuse kood, mis on isikutuvastusandmed välja andnud jurisdiktsioonil, vastavalt standardi ISO 3166-2:2020 punktile 8. Koodi esimene osa peab olema sama nagu väljaandva riigi kohta märgitud väärtus	Vabatahtlik
`issuance_date`	Isikutuvastusandmete halduskehtivuse alguse kuupäev ja võimaluse korral kellaaeg	Vabatahtlik

4. 4. jagu. Isikutuvastusandmete atribuutide kodeering: füüsiline isik

— Füüsilise isiku tuvastusandmed väljastatakse kooskõlas rakendusmääruse (EL) 2024/2979 II lisa punktides 5 (SD-JWT VC vorming) ja 6 (ISO/IEC-mdoc-vorming) loetletud standarditega, mida kohaldatakse elektrooniliste tõendite suhtes. Punkte 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3,6.2.4 ja 6.2.5 ei kohaldata.

— Füüsilise isiku tuvastusandmete kodeering peab vastama käesoleva lisa punktides 4.1 ja 4.2 esitatud tehnilistele spetsifikatsioonidele.

4.1. Füüsilise isiku tuvastusandmete ISO/IEC-mdoc-vormingus kodeering

— ISO/IEC-mdoc-vormingus isikutuvastusandmete tõendi atribuudi liik on 'eu.europa.ec.eudi.pid.1'. Käesolevas lisas esitatud isikutuvastusandmete atribuutide nimeruumi identifikaator on 'eu.europa.ec.eudi.pid.1'.

— Kui isikutuvastusandmed sisaldavad andmeid, mille tarbeks ei ole käesoleva lisaga ette nähtud andmete identifikaatoreid, tähistatakse need andmed riigisisese isikutuvastusandmete nimeruumi raames, mille puhul kasutatakse üldvormingut 'eu.europa.ec.eudi.pid.' [standardis ISO 3166-1 esitatud kahetäheline (alpha-2) riigikood või standardis ISO 3166-2 esitatud piirkonnakood], millele järgneb valikuline punkt ja versiooni number.

— Riigisisese nimeruumi kasutamise korral avaldatakse selle tõendamise kava, sealhulgas kõik andmete identifikaatorid, nende määratlused, kasutus ja kodeeringu vormingud kooskõlas komisjoni rakendusmääruse (EL) 2025/1569 ([1]) artikliga 8.

— Käesoleva lisa 1. ja 3. jao kohased isikutuvastusandmed ja nende metaandmed lisatakse isikutuvastusandmete elementidele ISO/IEC-mdoc-vormingu spetsifikatsioonide tähenduses.

— MobileSecurityObject-tüübi eksemplari andmeliikme deviceKeyInfo andmeliige deviceKey peab sisaldama avalikku võtit.

— See avalik võti vastab privaatvõtmele, mida säilitatakse kukrukasutaja kukru turvalises krüptoseadmes (edaspidi „WSCD“).

— ISO/IEC-mdoc-vormingus isikutuvastusandmeid allkirjastava CB-AdES digitaalallkirja kaitstud andmepäis peab sisaldama päise parameetreid 'x5u' ja 'x5t', mis on mõlemad esitatud dokumendis RFC 9360 ([2]).

— Päise parameetris 'x5t' kasutatakse räsialgoritmi SHA-256.

— Isikutuvastusandmete ISO/IEC-mdoc-vormingus kodeeringu nõuded on esitatud tabelis 6.

Tabel 6

Nõuded isikutuvastusandmete ISO/IEC-mdoc-vormingus kodeerimisele

Andmete identifikaator	Atribuudi identifikaator	Kodeeringu vorming
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]) Komisjoni 29. juuli 2025. aasta rakendusmäärus (EL) 2025/1569, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel pakutavate kvalifitseeritud elektrooniliste tõendite ja elektrooniliste tõenditega (ELT 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/).

Andmete identifikaator	Atribuudi identifikaator	Kodeeringu vorming
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate või 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 või full-date

— Tabelis 6 esitatud atribuutide kodeeringu vormingu tähistamiseks kasutatakse dokumendi RFC 8610 ([3]) kohaseid tähistusviise, võttes arvesse järgmisi lisanõudeid:

a) tstr tuleb kodeerida UTF-8 vormingus;

b) tstr peab toetama kogu Unicode'i standardi vahemikku;

c) tstr maksimaalne pikkus on 150 tähemärki;

d) kuupäev tuleb kodeerida vastavalt dokumendile RFC 8943 ([4]);

e) full-date tuleb tõlgendada kui #6.1004(tstr), mille puhul tag 1004 peab vastama dokumendile RFC 8943;

f) tdate-tüüpi atribuut peab sisaldama dokumendi RFC 3339 ([5]) kohast kuupäeva ja kellaaja stringi;

g) full-date-tüüpi atribuut peab sisaldama dokumendi RFC 3339 kohast stringi full-date kooskõlas dokumendiga RFC 8943;

h) kuupäev peab atribuutides olema esitatud järgmiselt (kui ei ole märgitud teisiti):

— ilma et oleks kasutatud sekundi murdosi;

— ilma et oleks kasutatud koordineeritud maailmaaja kohalikku aega ning dokumendile RFC 3339 vastav ajanihe peab olema 'Z';

i) täisarv peamiste tüübiväärtustega 0 ja 1 peab olema võimalikult väike, nagu on kirjeldatud dokumendi RFC 8949 ([6]) punktis 4.2;

j) place_of_birth peab sisaldama vähemalt ühte järgmistest võti-väärtus-paaridest: 'country', 'region' või 'locality';

k) pikkus väljendatuna bstr, tstr, massiivi või kujundina peab olema võimalikult lühike, nagu on kirjeldatud dokumendi RFC 8949 punktis 4.2;

([3]) C. Vigano ja H. Birkholz, „Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, juuni 2019.
([4]) M. Jones, A. Nadalin ja J. Richter, „Concise Binary Object Representation (CBOR) Tags for Date", RFC 8943, november 2020.
([5]) G. Klyne ja C. Newman, „Date and Time on the Internet: Timestamps", RFC 3339, juuli 2002.
([6]) C. Bormann ja P. Hoffman, „Concise Binary Object Representation (CBOR)", RFC 8949, detsember 2020.

l) kodakondsust näitav atribuut kodeeritakse kahetäheliste (alpha-2) riigikoodide massiivina, nagu on kirjeldatud standardis ISO 3166-1. Dokumendi RFC 8610 kohase CDDL notatsiooni kasutamise korral kodeeritakse see atribuut järgmiselt:

— nationalities = [+ CountryCode];

— CountryCode = tstr; standardis ISO 3166-1 esitatud kahetäheline (alpha-2) riigikood;

— kui kukrukasutajal, kelle kohta isikutuvastusandmed käivad, on mitu kodakondsust ja isikutuvastusandmete pakkuja neid mitut kodakondsust tõendab, võib isikutuvastusandmete pakkuja lisada isikutuvastusandmetesse kõik kodakondsused;

— atribuut place_of_birth kodeeritakse tüübina place_of_birth. Dokumendi RFC 8610 kohase CDDL notatsiooni kasutamise korral kodeeritakse see atribuut järgmiselt:

place_of_birth =

{

? 'country': tstr; üksainus standardis ISO 3166-1 esitatud kahetäheline (alpha-2) riigikood

? 'region': tstr; liidumaa, provintsi, rajooni või kohaliku piirkonna nimi

? 'locality': tstr; omavalitsusüksuse, linna või küla nimi

}

4.2. Nõuded isikutuvastusandmete SD-JWT VC vormingus kodeerimisele

— Käesolevas punktis nimetatud isikutuvastusandmed ja nende metaandmed lisatakse isikutuvastusandmetele väidetena SD-JWT VC vormingu spetsifikatsioonide tähenduses.

— Kõik väljastatud isikutuvastusandmetes sisalduvad väited, millele on viidatud eelmises taandes, peavad olema üksikult valikuliselt avalikustatavad, välja arvatud need väited, mis on SD-JWT VC vormingu puhul määratletud kui mittevalikuliselt avalikustatavad.

— Tabelis 7 on esitatud nende väitenimede kodeering, mis on avalikud nimed.

— Tabelis 8 on esitatud isikutuvastusandmetele vastavate väitenimede kodeering.

— SD-JWT VC vormingus kodeeritud isikutuvastusandmetes kasutatav JSON string kodeeritakse UTF-8 vormingus ja see peab toetama kogu Unicode'i standardi vahemikku, välja arvatud juhul, kui allpool olevas tabelis 8 või selles esitatud viidetes on sõnaselgelt teisiti kindlaks määratud.

— Dokumendis RFC 7519 ([7]) määratletud JWT väiteid nbf ja exp kasutatakse SD-JWT VC vormingule vastavate isikutuvastusandmete tehnilise kehtivusaja väljendamiseks.

([7]) J. Jones jt, „JSON Web Token (JWT)", RFC 7519, mai 2015.

— Isikutuvastusandmed sisaldavad väidet cnf, nagu see on määratletud dokumendis RFC 7800, ([8]) mis on kukrukasutaja kukrukomplekti WSCDs säilitatavast privaatvõtmest genereeritud avalik võti.

— SD-JWT VC vormingus isikutuvastusandmeid allkirjastava digitaalallkirja kaitstud andmepäis sisaldab päise parameetreid x5u ja x5t#S256, mis on esitatud dokumendis RFC 7515 ([9]).

Tabel 7

Nõuded isikutuvastusandmete kodeerimisele SD-JWT VC vormingus avalikke nimesid kasutades

Andmete identifikaator	Atribuudi identifikaator	Kodeeringu vorming
`family_name`	`family_name`	string
`given_name`	`given_name`	string
`birth_date`	`birthdate`	string, standard ISO 8601-1, vormingus AAAA-KK-PP
`birth_place`	`place_of_birth`	JSON struktuur
`nationality`	`nationalities`	stringide massiiv
`resident_address`	`address.formatted`	string
`resident_country`	`address.country`	string
`resident_state`	`address.region`	string
`resident_city`	`address.locality`	string
`resident_postal_code`	`address.postal_code`	string
`resident_street`	`address.street_address`	string
`family_name_birth`	`birth_family_name`	string
`given_name_birth`	`birth_given_name`	string
`email_address`	`email`	string
`mobile_phone_number`	`phone_number`	string
`portrait`	`picture`	string; andmete URL, mis sisaldab base64-kodeeringuga portreed, mis on JPEG-vormingus

([8]) M. Jones jt, „Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)“, RFC 7800, aprill 2016.
([9]) M. Jones jt „JSON Web Signature (JWS)“, RFC 7515, mai 2015.

Tabel 8

Nõuded isikutuvastusandmete kodeerimisele SD-JWT VC vormingus privaatseid nimesid kasutades

Andmete identifikaator	Atribuudi identifikaator	Kodeeringu vorming
`expiry_date`	`date_of_expiry`	string, standard ISO 8601-1, vormingus AAAA-KK-PP
`issuance_date`	`date_of_issuance`	string, standard ISO 8601-1, vormingus AAAA-KK-PP
`personal_administrative_number`	`personal_administrative_number`	string
`sex`	`sex`	arv
`issuing_authority`	`issuing_authority`	string
`issuing_country`	`issuing_country`	string
`document_number`	`document_number`	string
`issuing_jurisdiction`	`issuing_jurisdiction`	string

— Isikutuvastusandmete atribuudi baastüüp peab olema 'urn:eudi:pid:1', mis on esitatud väites vct. Kõikide isikutuvastusandmete korral tuleb nimeruumi puhul kasutada atribuuti 'urn:eudi:pid:'.

— Kui isikutuvastusandmed sisaldavad atribuute, mida ei ole käesolevas lisas esitatud, määratletakse need atribuudid riigispetsiifilise tüübi raames.

— Riigispetsiifilise tüübi kasutamise korral määratletakse selle tõendamise kava, sealhulgas kõik andmete identifikaatorid, nende definitsioonid, kasutus ja kodeeringu vormingud kavas, mis avaldatakse kooskõlas rakendusmääruse (EL) 2025/1569 artikliga 8.

5. 5. jagu. Usaldustaristu andmed

Isikutuvastusandmete autentsust võimaldab kinnitada isikutuvastusandmete pakkujate loetelu, mille komisjon teeb kättesaadavaks vastavalt rakendusmäärusele (EL) 2024/2980.“

II LISA

„Ia LISA

Artiklis 5a osutatud krüptograafilised mehhanismid

Euroopa küberturvalisuse sertifitseerimise rühm, krüptograafia alarühm: „Agreed Cryptographic Mechanisms“, avaldanud Euroopa Liidu Küberturvalisuse Amet (ENISA) ([1])."

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

III LISA

„Ib LISA

Artikli 6 lõikes 2a osutatud kukrukomplekti tõendite tehnilised spetsifikatsioonid

1. Kukrukomplekti tõend koosneb ühest või mitmest kukrueksemplari tõendist ning ühest või mitmest võtme tõendist.

2. Kukrueksemplari tõend ja võtme tõendid peavad vastama järgmistele nõuetele.

a) Vormingu nõuded

— FR-WIA-1: kukrueksemplari tõend on dokumendi RFC 7519 ([1]) kohane JSON Web Token (JWT), mille kukruteenuse pakkuja on allkirjastanud või tempiga varustanud, kasutades JAdES kompaktset baastaseme B allkirja.

— FR-WIA-1.1: kukrueksemplari tõend on standardi „OpenID for Verifiable Credential Issuance v1.0“ ([2]) (edaspidi „OID4VCI“) E liites esitatud kukrutõend, mida laiendatakse vastavalt allpool esitatud nõuetele C-WIA-1 ja C-WIA-2.

— FR-KA-1: võtme tõend on dokumendi RFC 7519 kohane JWT, mille kukruteenuse pakkuja on allkirjastanud või tempiga varustanud, kasutades JAdES kompaktset baastaseme B allkirja.

— FR_KA_1.1: võtme tõend on OID4VCI D liites kirjeldatud võtme tõend, mida laiendatakse vastavalt allpool esitatud nõuetele C_KA-1 ja C_KA-2.

b) Edastusnõuded

— TR-WIA-1: kukrukomplekt kasutab isikutuvastusandmete, kvalifitseeritud või kvalifitseerimata elektrooniliste tõendite või autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel pakutavate elektrooniliste tõendite väljastamisel kukrueksemplari tõendit.

— TR-WIA-2: kukruteenuse pakkuja kontrollib kukrueksemplari terviklust ja allkirjastab kukrueksemplari tõendi või varustab selle tempiga.

— TR-WIA-2.1: kui kukruteenuse pakkuja väljastab kukrueksemplari tõendi, ei tohi aeg, kui kukruteenuse pakkuja kontrollis kukrueksemplari terviklust, erineda ajast, mille ta märgib kukrueksemplari tõendi päise parameetrisse 'exp', rohkem kui 24 tundi.

— TR-WIA-2.2: kukruteenuse pakkuja tagab, et kukrukomplekt sisaldab isikutuvastusandmete ja elektrooniliste tõendite väljastamiseks vajalikke kukrueksemplari tõendeid.

— TR-WIA-3: väljastamise ajal saadab kukrukomplekt kukrueksemplari tõendi tõukelise volituspäringu ja tokeni päringu kaudu autoriseerimisserverile, nagu on kirjeldatud OID4VCI nõuetes.

— TR-WIA-3.1: kukrukomplekt saadab kukrueksemplari tõendi koos omamistõestusega (*Proof-of-Possession*, edaspidi „PoP“), nagu on kirjeldatud OID4VCI E liites.

— TR-WIA-3.2: kukrukomplekt saadab sama kukrueksemplari tõendi üksnes ühele autoriseerimis-serverile.

([1]) RFC 7519: JSON Web Token (JWT), mai 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: kui kukruteenuse pakkuja kasutab allpool nõudes R_WIA_1 esitatud valikut 'per-issuer reuse', võib kukrukomplekt saata kukrueksemplari tõendi samale autoriseerimisserverile mitu korda.

— TR-WIA-3.2.2: kui kukruteenuse pakkuja valikut 'per-issuer reuse' ei kasuta, võib kukrukomplekt kukrueksemplari tõendit kasutada mitte rohkem kui ühes väljastamisprotsessis.

— TR-WIA-4: kui autoriseerimisserver saab kukrueksemplari tõendi, kontrollib see kukrueksemplari tõendi allkirja allkirjastamise sertifikaadi avaliku võtme abil, mis sisaldub kukrueksemplari tõendi JOSE andmepäise parameetris 'x5c'.

— TR-WIA-4.1: autoriseerimisserver kontrollib ka seda, kas allkirjastamise sertifikaati saab kontrollida rakendusmääruse (EL) 2024/2980 artiklis 5 osutatud kukruteenuse pakkujate loendis oleva usaldusankruga, kasutades võimaluse korral parameetris 'x5c' sisalduvaid vahesertifikaate.

— TR-WIA-4.2: autoriseerimisserver kontrollib seda, et kukrueksemplari tõend ei ole aegunud.

— TR-WIA-4.3: autoriseerimisserver kontrollib väites 'cnf' sisalduva avaliku võtme abil PoPi allkirja.

— TR_KA-1: kukrukomplekt kasutab isikutuvastusandmete väljastamisel ning seadmepõhiste kvalifitseeritud või kvalifitseerimata elektrooniliste tõendite või autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel pakutavate elektrooniliste tõendite väljastamisel võtme tõendit.

— TR_KA-1.1: kukrukomplekt ei kasuta võtme tõendit seadmega sidumata kvalifitseeritud või kvalifitseerimata elektrooniliste tõendite või autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel pakutavate elektrooniliste tõendite väljastamisel.

— TR_KA-2: kukruteenuse pakkuja tagab kukrukomplektile erinevad võtme tõendid kukrukomplekti WSCD-sse ja selle iga võtmehoidla jaoks.

— TR_KA-2.1: kukruteenuse pakkuja allkirjastab võtme tõendi või varustab selle templiga pärast seda, kui ta on kontrollinud, et võtme tõendiga tõendatud võtmed on salvestatud võtme tõendis kirjeldatud kukrukomplekti WSCD-sse või võtmehoidlasse.

— TR_KA-2.2: võtme tõend sisaldab vähemalt ühte tõendatud avalikku võtit. Mandaadi väljastajale saadetud võtme tõendis sisalduvate võtmete arv ei tohiks ületada maksimaalset partii suurust, mille mandaadi väljastaja on kindlaks määranud oma mandaadi väljastaja metaandmetes; vt ETSI TS 119 472-3, ([3]) parameeter 'credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size'.

— TR_KA-2.3: kukruteenuse pakkuja lisab avaliku võtme (mis vastab kukrukomplekti WSCD-sse või võtmehoidlasse salvestatud privaatvõtmele) mitte rohkem kui ühele võtme tõendile.

— TR_KA-2.4: kukrukomplekt kasutab võtme tõendit mitte rohkem kui ühe mandaadi väljastamise või uuesti väljastamise protsessi ajal.

— TR_KA-2.5: kukruteenuse pakkuja tagab, et kukrukomplektil on isikutuvastusandmete ja seadmepõhiste elektrooniliste tõendite väljastamiseks vajalikud võtme tõendid.

([3]) ETSI, „Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 3: JAdES levels and baseline profiles“, ETSI TS 119 472-3, V1.1.1, märts 2026.

— TR_KA-3: kui see on väljastamisel vajalik, lisab kukrukomplekt mandaadi väljastajale esitatava mandaaditaotluse väljale 'proofs' võtme tõendi, nagu on kirjeldatud OID4VCI nõuetes, mille puhul tõestuse tüüp on 'jwt' või 'attestation'.

— TR_KA_3.1: kui kukrukomplekti andmeelementi 'jwt' kuulub võtme tõend, allkirjastab komplekt võtme tõendi või varustab selle templiga, kasutades privaatvõtit, mis vastab objekti 'key_attestation' massiivi 'attested_keys' indeksi 0 avalikule võtmele.

— TR_KA-4: kui mandaadi väljastaja väljastab seadmepõhiseid mandaate, märgib ta mandaadi väljastaja metaandmete parameetris 'proof_types_supported' kooskõlas OID4VCI punktiga 12.2.4, et see toetab nii 'jwt' kui ka 'attestation' tüüpi tõestust võtme tõendite puhul, mis hõlmavad objekti 'key_attestations_required'.

— TR_KA-4.1: kui mandaadi väljastaja väljastab seadmega sidumata mandaate, jätab ta mandaadi väljastaja metaandmetest välja parameetrid 'proof_types_supported' ja 'cryptographic_binding_methods_supported'.

— TR_KA-5: kui tõendi väljastaja saab võtme tõendi, mille tõestuse tüüp on 'jwt' või 'attestation', kontrollib ta võtme tõendi JOSE andmepäise parameetris 'x5c' sisalduva allkirjastamise sertifikaadi avaliku võtme abil võtme tõendi allkirja ja allkirjastamise sertifikaati rakendusmääruse (EL) 2024/2980 artiklis 5 osutatud kukruteenuse pakkujate loendis oleva usaldusankruga, kasutades võimaluse korral parameetris 'x5c' sisalduvaid vahesertifikaate.

— TR_KA-6: kui tõendi väljastaja saab võtme tõendi, mille tõestuse tüüp on 'jwt', kontrollib ta andmeelemendi 'jwt' allkirja sellesse elementi lisatud objekti 'key_attestation' massiivi 'attested_keys' indeksi 0 võtme abil.

— TR_KA-6.1: mandaadi väljastaja kontrollib, kas elemendi 'jwt' väljal 'nonce' on üks tema nonce_endpoint kehtiv c_nonce, nagu on kirjeldatud OID4VCIs.

— TR_KA-7: kui tõendi väljastaja saab võtme tõendi, mille tõestuse tüüp on 'attestation', kontrollib ta, kas objekt 'key_attestation' sisaldab üht tema nonce_endpoint kehtivat c_nonce.

— TR_KA-8: isikutuvastusandmete pakkuja tagab, et isikutuvastusandmed on seotud avaliku võtmega, mis pärineb võtme tõendist, milles on nimetatud WSCD-d.

c) Sisunõuded

— C_WIA-1: kukrueksemplari tõend sisaldab järgmist:

— OID4VCI E liites esitatud väide 'wallet_name', mille väärtus on kukrulahenduse identifikaator, mis on leitav rakendusmääruse (EL) 2024/2980 artiklis 5 osutatud kukruteenuse pakkujate loendist;

— väide 'wallet_version', ([4]) mis on string, mille väärtus on kukrulahenduse versioon;

— väide 'wallet_solution_certification_information', mis on JSONi objekt, mis sisaldab teavet kukrulahenduse sertifitseerinud vastavushindamisasutuse kohta, sertifitseerimisnumbrit, kui see on asjakohane, ja muid sertifitseerimisega seotud asjakohaseid üksikasju;

([4]) See väide määratletakse asjaomases ühises isikuandmete hoidlas, kuna see ei ole osa OID4VCI spetsifikatsioonist.

— väide 'client_status', mis sisaldab kahte alamvälja:

— 'status': OID4VCI E liites esitatud olekuloendi viide, mis tähistab kukrueksemplari kehtetuks tunnistamise olekut. Üksikasjalikum teave on esitatud allpool punktis e;

— 'exp': dokumendi RFC 7519 kohane NumericDate, millega määratakse kindlaks tähtaeg, mille lõpuni kukruteenuse pakkuja säilitab elemendis 'status' osutatud olekuloendi indeksis kehtetuks tunnistamise oleku.

— OID4VCI E liites määratletud väide 'exp'.

— *MÄRKUS:* väide 'client_status.status' kukrueksemplari tõendis tähistab kukrueksemplari kehtetuks tunnistamise olekut, mitte tõendi enda kehtetuks tunnistamise olekut. Nagu on kirjeldatud allpool nõudes R_WIA-1, võib kukruteenuse pakkuja otsustada, et iga kukrueksemplari tõend kehtib konkreetses autoriseerimisserveris, tuginedes asjaolule, et kõigi sellesse serverisse saadetud tõendite kirjes 'client_status.status' on sama indeksiväärtus.

— *MÄRKUS:* väites 'status' esitatud väärtust 'idx' saab kasutada kukrueksemplari ja kukrukomplekti (paarina) kordumatu tunnusena.

— C_WIA-2: kukrueksemplari tõend peaks sisaldama ka OID4VCI E liites määratletud väidet 'wallet_link' ning selle väite väärtus on URI, mille kaudu saab lisateavet kukrulahenduse kohta.

— C_WIA-3: autoriseerimisserver ei tohi kukrueksemplari tõendi tipptaseme parameetrit 'exp' tõlgendada kukrueksemplari kehtetuks tunnistamise säilitamise perioodi lõpuna.

— *MÄRKUS:* kukrueksemplari tõendi tipptaseme parameeter 'exp' tähistab tõendi enda aegumist.

— C_KA-1: võtme tõend peab sisaldama järgmist:

— OID4VCI D liites määratletud väited 'key_storage' ja 'user_authentication';

— atribuutide 'key_storage' ja 'user_authentication' väärtus on 'iso_18045_high', kui võtme tõendis on nimetatud WSCD-d;

— OID4VCI D liites nimetatud väide 'certification', mis sisaldab URLi, mille kaudu on võimalik saada teavet WSCD või võtmehoidla sertifitseerimise, harilikult kava (nagu näiteks Common Criteria või GlobalPlatform), hinnatud nõuete (nagu näiteks kohaldatav kaitseprofiil) ja hindamise taseme kohta.

— Selle teabe põhjal peab olema võimalik kindlaks teha, kas võtmehoidla on WSCD;

— väide 'key_storage_status', mis sisaldab kahte alamvälja:

— 'status': OID4VCI D.1 liites esitatud olekuloendi viide. Väärtus kajastab kas tõendatud võtmete salvestamiseks kasutatava WSCD või võtmehoidla kehtetuks tunnistamise olekut või kui valitud on per-key-attestation-indeks, konkreetse kukrukomplekti WSCD või võtmehoidla kehtetuks tunnistamise staatust. Olemasolevate indeksi määramise võimaluste kohta vt R_KA_1 nõudeid allpool;

— 'exp': dokumendi RFC 7519 kohane NumericDate, millega määratakse kindlaks tähtaeg, mille lõpuni kukruteenuse pakkuja säilitab elemendis 'status' osutatud olekuloendi indeksis kehtetuks tunnistamise oleku.

— OID4VCI D liites esitatud väide 'exp'.

— *MÄRKUS:* võtme tõendis esitatud väites 'key_storage_status.status' sisalduva väärtuse 'idx' kohta: kui kukruteenuse pakkuja kasutab valikut 'type-shared index' (vt allpool nõue R_KA_1), on kõigil sama liiki WSCD või võtmehoidla võtme tõenditel sama olekuloendi indeks. Seetõttu ei ole väärtus 'idx' iga kukrukomplekti puhul kordumatu. Seevastu juhul kui kukruteenuse pakkuja kasutab valikut 'per-key-attestation index', on väärtus 'idx' iga kukrukomplekti puhul kordumatu (või iga tõendi väljastaja puhul paarina kordumatu). Igal juhul ei kasuta tõendi väljastaja kukrukomplekti identifikaatorina mitte võtme tõendis olevat väärtust 'idx', vaid kukrueksemplari tõendis esitatud väärtust 'idx'.

— C_KA-2: kui võtme tõendi puhul märgitakse saatmisel tõestuse tüübiks 'attestation', peab sellel olema ka kehtiv c_nonce, nagu on kirjeldatud OID4VCI F.3 liites.

— C_KA-3: tõendi väljastaja ei tohi tõlgendada võtme tõendi tipptaseme parameetrit 'exp' WSCD või võtmehoidla kehtetuks tunnistamise säilimise perioodi lõpuna.

— *MÄRKUS:* võtme tõendi tipptaseme parameeter 'exp' tähistab tõendi enda aegumist.

d) Nõuded elutsüklile

— Käesolevas lisas määratakse kindlaks järgmised tõendi väljastaja metaandmete parameetrid:

— 'preferred_client_status_period': OPTIONAL. Täisarv, mis näitab kukrueksemplari tõendi eelistatud järelejäänud oleku säilimise perioodi (sekundites), mille kukrukomplekt peab väljastamise ajal esitama. Oleku säilitamise järelejäänud periood on määratletud kui tõendis olev väärtus 'client_status.exp', millest on lahutatud tõendi saamise aeg;

— 'preferred_key_storage_status_period': OPTIONAL. Täisarv, mis näitab võtme tõendi oleku säilitamise eelistatud järelejäänud perioodi (sekundites), mille kukrukomplekt peab väljastamise ajal esitama. Oleku säilitamise järelejäänud periood on määratletud kui tõendis olev väärtus 'key_storage_status.exp', millest on lahutatud tõendi saamise aeg.

— LC_WIA-1: autoriseerimisserver võib edastada oma eelistused kukrueksemplari tõendite oleku säilitamise järelejäänud perioodi kohta, lisades oma tõendi väljastaja metaandmete otspunkti metaandmete parameetri 'preferred_client_status_period', nagu on kirjeldatud OID4VCI punktis 12.2.2.

— LC_WIA-1.1: see väli paigutatakse tõendi väljastaja metaandmete tipptasemele.

— LC_WIA_2: autoriseerimisserver ei tohi kukrueksemplari tõendi tipptaseme parameetrit 'exp' tõlgendada kukrueksemplari kehtetuks tunnistamise säilitamise perioodi lõpuna.

— LC_WIA_3: kui kukruteenuse pakkuja allkirjastab kukrueksemplari tõendi või varustab selle templiga, säilitab ta asjaomase kukrueksemplari kehtetuks tunnistamise oleku seni, kuni asjaomases kukrueksemplari tõendis märgitud 'wallet_instance_status.exp' on möödunud.

— LC_KA-1: kui on vaja võtme tõendit, võib tõendi väljastaja teatada oma eelistused oleku säilitamise järelejäänud perioodi kohta võtme tõendites, lisades eespool kirjeldatud metaandmete parameetri 'preferred_key_storage_status_period' oma tõendi väljastaja metaandmete otspunkti, nagu on kirjeldatud OID4VCI punktis 12.2.2.

— LC_KA-1.1: see väli paigutatakse objekti 'key_attestations_required', nagu on kirjeldatud OID4VCI punktis 12.2.4.

— LC_KA-2: kukruteenuse pakkujal tuleb valida enda väljastatavate võtme tõendite tehniline kehtivusaeg.

— LC_KA-3: kui kukruteenuse pakkuja allkirjastab võtme tõendi või varustab selle templiga, säilitab ta asjaomase WSCD või võtmehoidla kehtetuks tunnistamise oleku seni, kuni võtme tõendis märgitud 'key_storage_status.exp' on möödunud.

— LC_GEN-1: kukruteenuse pakkuja tagab, et kukrukomplekt esitab alati kukrukomplekti tõendid ja võtme tõendid, mille vastavalt kas 'client_status.exp' või 'key_storage_status.exp' kehtib autoriseerimisserverile või mandaadi väljastajale esitamise ajal vähemalt 31 päeva.

— *MÄRKUS:* see tagab, et isikutuvastusandmete pakkujad saavad tugineda kehtetuks tunnistamise ahelale, ilma et nad oleksid sunnitud väljastama lühiajalisi isikutuvastusandmeid.

— LC_GEN-2: kukruteenuse pakkuja tagab, et väljastamise ajal võtab kukrukomplekt tõendi väljastaja metaandmed.

  — LC_GEN_2.1: kui need metaandmed sisaldavad välja 'preferred_key_storage_status_period', saadab kukrukomplekt võtme tõendi, mille ('key_storage_status.exp' − hetkeaeg) − 'preferred_key_storage_status_period' on võimalikult väike, kuid mitte negatiivne. Kui selline võtme tõend ei ole kukrukomplektile kättesaadav, hangib see kukruteenuse pakkujalt uue võtme tõendi, mis vastab nõudele, et 'key_storage_status.exp' – hetkeaeg ≥ 'preferred_key_storage_status_period'.

  — LC_GEN_2.2: kui need metaandmed sisaldavad välja 'preferred_client_status_period', saadab kukrukomplekt kukrueksemplari tõendi, mille ('client_status.exp' – hetkeaeg) – 'preferred_client_status_period' on võimalikult väike, kuid mitte negatiivne. Kui selline kukrueksemplari tõend ei ole kukrukomplektile kättesaadav, taotleb ta kukruteenuse pakkujalt uut kukrueksemplari tõendit, mis vastab nõudele, et 'client_status.exp' – hetkeaeg ≥ 'preferred_client_status_period'.

— LC_GEN-3: isikutuvastusandmete tehniline kehtivusaeg lõpeb nii enne kukrueksemplari tõendi 'client_status.exp' kui ka isikutuvastusandmete pakkujale väljastamise protsessi käigus saadetud võtme tõendi 'key_storage_status.exp' saabumist.

— LC_GEN-4: selliste isikutuvastusandmete pakkuja, mille tehniline kehtivusaeg on enam kui 24 tundi, kontrollib nii kukrueksemplari tõendi kui ka väljastamise ajal saadud võtme tõendi kehtetuks tunnistamise olekut isikutuvastusandmete tehnilise kehtivusaja jooksul vähemalt kord iga 24 tunni jooksul. Kui üks neist tunnistatakse kehtetuks, tunnistab pakkuja isikutuvastusandmed kehtetuks.

e) Nõuded kehtetuks tunnistamisele

— R_GEN-1: kukruteenuse pakkuja kasutab nii võtme tõendite kui ka kukrueksemplari tõendite kehtetuks tunnistamise mehhanismina tokenite olekuloendeid (mis on esitatud dokumendis „IETF Token Status List“) vastavalt OID4VCI D ja E liitele.

— *MÄRKUS:* kukruteenuse pakkuja saab oma olekuloendite paremaks mastaabitavuseks kasutada järgmisi optimeerimisvõimalusi:

  — jagada olekuloend mitmeks tombuks, kui kukruteenuse pakkujal on märkimisväärne arv kasutajaid ja väljastatud tõendeid. Olemas on palju tombustusmeetodeid, mis põhinevad näiteks kindlaksmääratud suurusel või ajavahemikul. Tombustusmeetodi üle otsustab kukruteenuse pakkuja. Arvesse võib võtta allalaaditava olekuloendi suurust ja kasutaja privaatsust;

  — kasutada mitut olekuloendit;

  — olekuloendit tihendada, et vähendada selle suurust.

— R_WIA-1: kukruteenuse pakkuja võib määrata väite 'client_status.status' väitele 'idx' sama väärtuse kõikide kukrueksemplari tõendite puhul, mille konkreetne kukrukomplekt esitab samale autoriseerimisserverile. Seda valikut nimetatakse 'per-issuer reuse'. Selle valiku kasutamise korral:

  — R_WIA-1.1: kukrukomplekt säilitab oleku vastavalt sellele, millist indeksiväärtust on kasutatud iga autoriseerimisserveri puhul, millega ta on varem suhelnud, ning taotleb sama autoriseerimisserveriga uuesti suheldes sama indeksiväärtust sisaldavat kukrueksemplari tõendit.

  — R_WIA-1.2: kui kukruteenuse pakkuja saab kukrueksemplari tõendi päringu, mis sisaldab konkreetset indeksiväärtust, kontrollib ta enne selle indeksiväärtusega uue kukrueksemplari tõendi väljastamist, kas päringu esitanud kukrukomplektile on see indeksiväärtus varem omistatud.

  — R_WIA-1.3: kukrukomplekt ei tohi sama indeksiväärtust uuesti kasutada erinevate autoriseerimisserveritega suhtlemise puhul.

— *MÄRKUS:* valiku 'per-issuer reuse' kasutamise korral saab kukruteenuse pakkuja kindlaks teha, kui mitme autoriseerimisserveriga on kukrukomplekt suhelnud ja kui sageli see igaühega neist suhtleb.

— R_WIA-2: kukruteenuse pakkuja märgib oma isikuandmete kaitse põhimõtetes, kas ta kasutab kukrueksemplari kehtetuks tunnistamisel valikut 'per-issuer reuse'.

— R_WIA-3: kui kukruteenuse pakkuja ei kasuta valikut 'per-issuer reuse', määrab ta igale väljastatavale kukrueksemplari tõendile uue seostamatu indeksiväärtuse.

— R_WIA-4: kui kukrukomplekt tuleb kehtetuks tunnistada, tühistab kukruteenuse pakkuja väites 'client_status.status' sisalduvad indeksiväärtused kõigis selle kukrukomplektiga seotud kukrueksemplari tõendites.

— R_WIA-5: kukruteenuse pakkuja võtab oma kukrueksemplaride tõendite olekuloendite suuruse kindlaksmääramisel arvesse kasutamisulatust ja tugiarhitektuuri, tagades nende piisava suuruse, et ära hoida korrelatsiooni ja kaitsta kasutajate eraelu puutumatust. Olekuloend peaks võimaluse korral puudutama vähemalt 10 000 tõendit.

— R_KA_1: kukruteenuse pakkuja valib võtme tõendi väite 'key_storage_status.status' jaoks ühe järgmistest indeksi määramise võimalustest:

  — 1. võimalus ehk 'type-shared index', mille puhul kõik võtme tõendid, mis tõendavad sama liiki WSCD-sse või võtmehoidlasse salvestatud võtmeid, sisaldavad väljal 'key_storage_status.status' sama indeksiväärtust;

  — 2. võimalus ehk 'per-key-attestion index', mille puhul võtme tõendis, mis tõendab konkreetsesse WSCD-sse või võtmehoidlasse salvestatud võtmeid, on väljal 'key_storage_status.status' (paarina) kordumatu indeksiväärtus.

— *MÄRKUS:* kui kukruteenuse pakkuja kasutab 1. võimalust, muudab üks kehtetuks tunnistamise toiming kehtetuks kõik mõjutatud liiki võtme tõendid kõigis kukrukomplektides. Kuna kõigil sama liiki WSCD või võtmehoidla võtme tõenditel on ühine olekuloendi indeks, kajastab võtme tõendite olekuloendi kannete arv kukruteenuse pakkuja toetatud WSCD või võtmehoidla liikide arvu, mitte kasutusele võetud kukrukomplektide arvu. Privaatsuskaalutlused, millest sõltub kukrueksemplaride olekuloendi minimaalne suurus, ei kehti seega 1. võimalusega ette nähtud võtme tõendite olekuloendite suhtes, tingimusel et on piisavalt palju kukrukomplekte, mis kasutavad sama liiki WSCD-d või võtmehoidlat.

— *MÄRKUS:* kui kukruteenuse pakkuja kasutab 2. võimalust, tähistab iga indeks konkreetse WSCD või võtmehoidla kehtetuks tunnistamise olekut, mida tõendab asjaomane võtme tõend.

— *MÄRKUS:* kui kukruteenuse pakkuja kasutab 2. võimalust, saab konkreetse WSCD või võtmehoidla kehtetuks tunnistada ka kasutaja taotluse alusel.

— R_KA-2: kui kukruteenuse pakkuja kasutab 2. võimalust, võib ta soovi korral kasutada ka nõudes R_WIA-1 kirjeldatud valikut 'per-issuer reuse'. Kui kukruteenuse pakkuja otsustab seda võimalust kasutada, kohaldatakse nõudeid R_WIA-1 kuni R_WIA-3 *mutatis mutandis*.

— R_KA-3: kui kukruteenuse pakkuja kasutab 2. võimalust, võtab ta oma võtme tõendite olekuloendite suuruse kindlaksmääramisel arvesse kasutusulatust ja tugiarhitektuuri, tagades nende piisava suuruse, et ära hoida korrelatsiooni ja kaitsta kasutajate eraelu puutumatust. Olekuloend peaks võimaluse korral hõlmama vähemalt 10 000 võtme tõendit.

— R_KA-4: kui kukruteenuse pakkuja kasutab 1. võimalust (type-shared index), tuleb kehtetuks tunnistada üksnes kirje 'key_storage_status.status', kui vastavat liiki WSCD-l või võtmehoidlal on mõni turvanõrkus.

f) Nõuded digitaalallkirja algoritmidele

— SA-1: kukrueksemplari tõendite, võtme tõendite, nendega seotud omamistõestustega ja tokenite olekuloendite allkirjastamiseks kasutatakse üht järgmistest algoritmidest:

— ES256 (ECDSA koos SHA-256 ja P-256)

— ES384 (ECDSA koos SHA-384 ja P-384)

— ES512 (ECDSA koos SHA-512 ja P-521)

— SA-2: kukruteenuse pakkuja valib, milliseid nõudes SA-1 nimetatud algoritme ta kasutab.

— SA-3: autoriseerimisserver või tõendi väljastaja (nagu on kirjeldatud OID4VCI nõuetes) tagab kõigi nõudes SA-1 nimetatud algoritmide toetamise.“

IV LISA

„II LISA

Artiklis 8 osutatud standardite loetelu

Kohaldatakse standardi ETSI TS 119 472-1 V1.2.1 (2026-02) punktides 2–6 esitatud tehnilisi spetsifikatsioone. Neid kasutatakse järgmiste kohandustega.

1. 2.1 Normative references

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures“.

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): „Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers“.

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

2. 4.2.11.1 General requirements

— EAA-4.2.11.1-06: kui isikutuvastusandmete, kvalifitseeritud elektrooniliste tõendite või autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel pakutavate elektrooniliste tõendite puhul kasutatakse olekuelementi, märgitakse selles üksnes see, kas tõend tunnistatakse kehtetuks või mitte, ning see ei toeta muid olekut näitavaid väärtusi, näiteks peatamist.

— EAA-4.2.11.1-06.1: kui tõend kehtetuks tunnistatakse, on see kehtetuks tunnistatud lõplikult.

3. 4.2.13 EAA short-lived

— EAA-4.2.13-03: kui väljastatakse lühiajalisi elektroonilisi tõendeid, mille kehtivusaeg on 24 tundi või vähem, ei ole kehtetuks tunnistamine nõutav.

4. 4.6.3 Autentse allika eest vastutava avaliku sektori asutuse (PuB-EAA) poolt või nimel välja antud nõuded ELi EMPile

— PuB-EAA-4.6.2-03: kehtetu.

— Pub-EAA-4.6.2-04: kehtetu.

— PuB-EAA-4.6.3-03: PuB-EAA digitaalallkiri peaks sisaldama PuB-EAA digitaalallkirja toetavat kvalifitseeritud sertifikaati.

— PuB-EAA-4.6.3-04: PuB-EAA digitaalallkirja toetav kvalifitseeritud sertifikaat vastab standardi ETSI TS 119 412-6 v1.1.1 punkti 8 nõuetele ja selles sisaldub standardis ETSI EN 319 412-5 v2.5.1 määratletud QcType qcStatement, mille väärtus 'id-etsi-qct-eidaspsbeaa' on määratletud järgmiselt:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } -- määruse (EL) nr 910/2014 artikli 3 punktis 46 osutatud avaliku sektori asutuse kvalifitseeritud e-allkirja või kvalifitseeritud e-templit toetav sertifikaat, millele on osutatud artikli 45f lõike 1 punktis b.

5. 5.2.10.1 General requirements

— EAA-5.2.10.1-04: kehtetu.

— EAA-5.2.10.1-05: kehtetu.

— EAA-5.2.10.1-06: Andmeliige status võib sisaldada andmeliiget status_list, nagu on kirjeldatud IETF draft-ietf-oauth-status-list-20 [25] punktis 6.2.

— EAA-5.2.10.1-07: kehtetu.

— EAA-5.2.10.1-08: kehtetu.

— EAA-5.2.10.1-09: kehtetu.

— EAA-5.2.10.1-10: kehtetu.

— EAA-5.2.10.1-11: kehtetu.

— EAA-5.2.10.1-12: kehtetu.

6. 6.2.10.1 General requirements

— EAA-6.2.10.1-01: kui ISO/IEC mdoc-vormingule vastavas elektroonilises tõendis kasutatakse nõudes EAA-6.2.10.1-02.2 esitatud tõendite olekuloendi mehhanismi või nõudes EAA-6.2.10.1-02.3 esitatud tõendite kehtetuks tunnistamise loendi mehhanismi, peab selle mobiilturvaobjektil (*Mobile Security Object*, edaspidi „MSO“) olema nõudes EAA-6.2.10.1-17 kirjeldatud olekustruktuur, mis sisaldab teavet selle MSO kehtetuks tunnistamise kohta.

— EAA-6.2.10.1-01.1: identifikaatorite loendi mehhanismi rakendamise korral peab olekuelement sisaldama elementi identifier_list, nagu on kirjeldatud EAA-6.2.10.1-11 nõuetes.

— EAA-6.2.10.1-01.2: olekuloendi mehhanismi rakendamise korral peab olekuelement sisaldama elementi status_list, nagu on kirjeldatud EAA-6.2.10.1-13 nõuetes.

— *MÄRKUS:*

  — olekustruktuur sisaldab viidet MSO kehtetuks tunnistamise loendile.

  — MSO kehtetuks tunnistamise loend on COSE_Sign1 struktuur, mis näitab, kas konkreetne MSO tunnistatakse kehtetuks või mitte.

  — Olekustruktuur sisaldab kogu teavet, mida kukrule tuginev isik vajab, et teha kindlaks, kas MSO kehtetuks tunnistamise loend on autentne.

— EAA-6.2.10.1-02: isikutuvastusandmete pakkuja, kvalifitseeritud elektrooniliste tõendite pakkuja või autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel pakutavate elektrooniliste tõendite pakkuja kasutab isikutuvastusandmete, kvalifitseeritud elektrooniliste tõendite või autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel pakutavate elektrooniliste tõendite kehtetuks tunnistamiseks üht järgmistest meetoditest.

— EAA-6.2.10.1-02.1: kui nad väljastavad lühiajalisi elektroonilisi tõendeid, mille kehtivusaeg on 24 tundi või vähem, ei ole kehtetuks tunnistamine vajalik.

— EAA-6.2.10.1-02.2: kehtetuks tunnistamise teabe kodeerimiseks olekuloendina kasutatakse tõendite olekuloendi mehhanismi.

— EAA-6.2.10.1-02.2.1: olekuloendi mehhanism tunnistab MSO kehtetuks vastavalt sellele, kas väljastaja määratletava bitikoha bitt on olekuloendis seatud väärtusele tõene.

— EAA-6.2.10.1-02.2.2: olekuloendi mehhanism määratakse kindlaks tokenite olekuloendi (draft-ietf-oauth-status-list-20) kirjelduses.

— EAA-6.2.10.1-02.3: tõendite kehtetuks tunnistamise loendi mehhanismi kasutamine kehtetuks tunnistamise teabe kodeerimiseks identifikaatorite loendina.

— EAA-6.2.10.1-02.3.1: identifikaatorite loendi mehhanism tunnistab MSO kehtetuks vastavalt sellele, kas MSOs sisalduv väljastaja määratletav identifikaator on identifikaatorite loendis olemas.

— EAA-6.2.10.1-02.3.2: nõuetes EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 ja EAA-6.2.10.1-11 on kindlaks määratud identifikaatorite loendi mehhanism, tuginedes tokenite olekuloendi kirjelduse nõuetele, sealhulgas olekuloendi ja identifikaatorite loendi mehhanismi sarnasusele.

— EAA-6.2.10.1-03: kui isikutuvastusandmete, kvalifitseeritud elektrooniliste tõendite või autentse allika eest vastutava avaliku sektori asutuse poolt või tema nimel pakutavate elektrooniliste tõendite puhul kasutatakse olekuelementi, kasutatakse üksnes olekut 'revoked'.

— EAA-6.2.10.1-03.1: olekuloendi puhul tähendab see, et kasutada tuleb ainult väärtusi 'valid' ja 'invalid' vastavalt tokenite olekuloendi kirjelduses.

— EAA-6.2.10.1-03.2: identifikaatorite loendisse kantakse üksnes kehtetuks tunnistatud MSOd, mitte ajutiselt peatatud MSOd.

— EAA-6.2.10.1-04: MSO kehtetuks tunnistamise korral on MSO lõplikult kehtetuks tunnistatud.

— EAA-6.2.10.1-05: MSOde kehtetuks tunnistamise loendi kontrollimine on kukrule tugineva isiku puhul vabatahtlik ning vajaduse korral vastab kontroll tokenite olekuloendi kirjelduses esitatud kontrollinõuetele ja nõudes EAA-6.2.10.1-01 esitatud olekustruktuuri spetsifikatsioonile.

— EAA-6.2.10.1-05.1: kui kukrule tugineval isikul peab olema võimalik kontrollida isikutuvastusandmete või elektrooniliste tõendite kehtetuks tunnistamise olekut, peab ta toetama nii tõendite olekuloendi mehhanismi kui ka tõendite kehtetuks tunnistamise loendi mehhanismi vastavalt nõudele EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: MSO identifier_list ja status_list võivad sisaldada sertifikaadielementi.

— EAA-6.2.10.1-06.1: sertifikaadielemendi kasutamise korral peab see sisaldama sertifikaati, mis sisaldab avalikku võtit, millega allkirjastati või varustati tempiga tipptaseme sertifikaat MSO kehtetuks tunnistamise loendi struktuuri elemendis x5chain.

— EAA-6.2.10.1-06.1.1: kukrule tugineva isiku eksemplar kasutab seda sertifikaati usaldusankruna MSO kehtetuks tunnistamise loendi struktuuris sisalduva andmeelemendi x5chain kontrollimiseks.

— EAA-6.2.10.1-06.2: kui sertifikaadielementi ei kasutata, tuleb MSO kehtetuks tunnistamise loendi struktuuri elemendis 'x5chain' olev tipptaseme sertifikaat allkirjastada või tempiga varustada sellise sertifikaadi abil, mida kasutatakse MSO elemendis x5chain oleva sertifikaadi allkirjastamiseks.

— EAA-6.2.10.1-06.2.1: kukrule tugineva isiku eksemplar kasutab seda sertifikaati usaldusankruna MSO kehtetuks tunnistamise loendi struktuuris sisalduva andmeelemendi x5chain kontrollimiseks.

— EAA-6.2.10.1-07: MSO kehtetuks tunnistamise loendit rakendatakse vastavalt tokenite olekuloendi kirjeldusele CWT-vormingus olekuloendi tokenina.

— EAA-6.2.10.1-08: identifikaatorite loendi ja olekuloendi mehhanismi MSO kehtetuks tunnistamise loendi suhtes kohaldatakse järgmisi nõudeid:

  — väide exp peab olema märgitud;

  — väide ttl võib olla märgitud;

  — IdentifierList või StatusList võib sisaldada väidet aggregation_uri ning isikutuvastusandmete pakkuja, kvalifitseeritud elektrooniliste tõendite pakkuja või autentse allika eest vastutava avaliku sektori asutuse

poolt või tema nimel pakutavate elektrooniliste tõendite pakkuja võib kasutada väidet aggregation_uri, et näidata ära agregeerimismehhanismi tugi, nagu on kirjeldatud tokenite olekuloendi kirjelduses;

— CWT on COSE_Sign1 objekt, mille puhul kasutatakse allkirja arvutamiseks ühte järgmistest signatuurialgoritmidest:

a) 'ES256' (ECDSA kõveral NIST P-256, SHA-256);

b) 'ES384' (ECDSA kõveral NIST P-384, SHA-384);

c) 'ES512' (ECDSA kõveral NIST P-521, SHA-512);

d) 'ESB256' (ECDSA kõveral brainpoolP256r1, SHA-256);

e) 'ESB384' (ECDSA kõveral brainpoolP384r1, SHA-384);

f) 'ESB512' (ECDSA kõveral brainpoolP512r1, SHA-512);

— CWT kaitstud andmepäises peab sisalduma x5chain, mis sisaldab sertifikaati või sertifikaatide ahelat, et kontrollida MSO kehtetuks tunnistamise loendi allkirja;

— tokenite olekuloendi kirjelduses kindlaks määratud objekti identifikaatori laiendatud võtmekasutust võib kasutada olekuloendi ja identifikaatorite loendi allkirjastamise sertifikaadi tarbeks ning kukrule tuginevate isikute eksemplarid võivad toetada tokenite olekuloendi kirjelduses kindlaks määratud objekti identifikaatorite laiendatud võtmekasutust; objekti identifikaatorite puhul ei tohi kvalifitseeritud elektrooniliste tõendite pakkuja ega avaliku sektori asutuse poolt või tema nimel pakutavate elektrooniliste tõendite pakkuja juhul, kui kasutatakse tokenite olekuloendi kirjelduses kindlaks määratud laiendatud võtmekasutuse OIDd, määratleda laiendatud võtmekasutuse välja kaalukana.

— EAA-6.2.10.1-09: erinevalt tokenite olekuloendi kirjelduse nõuetest kohaldatakse identifikaatorite loendi mehhanismi suhtes järgmisi nõudeid:

— väite type väärtus on 'application/identifierlist+cwt';

— CWT väidete kogum ei sisalda väidet StatusList;

— nõudes EAA-6.2.10.1-11 määratletud IdentifierList struktuur esitatakse väitena CWT väidete kogumis, kasutades võtit 65530.

— EAA-6.2.10.1-10: IdentifierList struktuur on CBORi struktuur, mille CDDL on järgmine:

```
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: kui IdentifierList sisaldab identifikaatorit, tunnistatakse olekuelemendis identifikaatorit sisaldav MSO kehtetuks.

— EAA-6.2.10.1-10.2: väide Aggregation_uri on kindlaks määratud tokenite olekuloendi kirjelduse punktis 9.2.

— EAA-6.2.10.1-10.3: identifikaatorite loendi sisutüüp on 'application/identifierlist+cwt', nagu on kirjeldatud tokenite olekuloendi kirjelduse punktis 8.2 esitatud nõuetes.

— EAA-6.2.10.1-11: MSOs sisalduva elemendi identifier_list suhtes kohaldatakse järgmisi nõudeid (vt EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: element identifier_list on CBORi struktuur, mille CDDL on järgmine:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: et takistada identifikaatori kasutamist korrelatsioonis teiste esitustega, peab see iga MSO puhul olema kordumatu.

— EAA-6.2.10.1-12: olekuloendi suhtes kohaldatakse järgmisi nõudeid:

  — EAA-6.2.10.1-12.1: StatusList struktuuri bitte sisaldava andmeelemendi väärtuseks seatakse 1.

— EAA-6.2.10.1-13: MSOs sisalduva andmeelemendi status_list suhtes kohaldatakse järgmisi nõudeid (vt EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: element status_list peab vastama StatusListInfo struktuurile esitatavatele nõuetele, mis on kindlaks määratud tokenite olekuloendi kirjelduses, ning lisatakse nõudes EAA-6.2.10.1-06 kindlaks määratud vabatahtlik sertifikaadielement.

  — EAA-6.2.10.1-13.2: et takistada olekuindeksi kasutamist korrelatsioonis teiste esitustega, peab olekuindeksi ja URI kombinatsioon olema iga MSO puhul kordumatu.

— EAA-6.2.10.1-14: kukruteenuse pakkuja kasutab kukrukomplekti tõendi ja võtme tõendi kehtetuks tunnistamiseks nõudes EAA-6.2.10.1-02 kirjeldatud teist (EAA-6.2.10.1-02.2) või kolmandat (EAA-6.2.10.1-02.3) meetodit.

— EAA-6.2.10.1-15: kukruteenuse pakkuja rakendab oma kukrulahenduse puhul nõudes EAA-6.2.10.1-02 kirjeldatud tõendite kehtetuks tunnistamise mehhanisme.

— EAA-6.2.10.1-16: selleks et kontrollida kukrukomplekti tõendi ja võtme tõendi kehtetuks tunnistamise olekut, toetavad isikutuvastusandmete pakkuja ja elektrooniliste tõendite pakkuja nii tõendite olekuloendi mehhanismi kui ka tõendite kehtetuks tunnistamise loendi mehhanismi, mida on kirjeldatud nõudes EAA-6.2.10.1-02.

— EAA-6.2.10.1-17: MSOs sisalduv olekustruktuur on CBORi struktuur, mille CDDL on järgmine:

Status = {

? 'identifier_list': IdentifierListInfo,

? 'status_list': StatusListInfo,

* tstr => RFU

}“

V LISA

„III LISA

Artiklis 10 osutatud tehnilised spetsifikatsioonid

— Tehnilised spetsifikatsioonid:

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

VI LISA

Rakendusmääruse (EL) 2024/2979 IV lisa muudetakse järgmiselt.

1. Punkt 1 asendatakse järgmisega:

„1. Kohustuslik allkirja- või templivorming:

a) PAdES (PDF Advanced Electronic Signature) vastavalt standardile ETSI EN 319 142-1 V1.2.1 (2024-01); „Electronic Signatures and Trust Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

2. Punkt 3 asendatakse järgmisega:

„3. Rakendusliides:
standardi ETSI TS 119 432 v1.3.1 (2026-03) punktid 6.4.3, A.6, A.7 ja A.8.".

VII LISA

„VI LISA

ELi digiidentiteedikukru usaldusmärk värvilisena



“

VIII LISA

„VII LISA

ELi digiidentiteedikukru usaldusmärk must-valgena



„

IX LISA

„VIII LISA

ELi digiidentiteedikukru usaldusmärgi andmed

Andmed	Kirjeldus	Kodeering	Staatus
TrustMarkResourceURL	ELi digiidentiteedikukru usaldusmärgi graafika ja kasutajateabe ressursside URL digiidentiteedikukru kasutajaliideses	URL	Kohustuslik
ListOfCertifiedWalletsURL	Komisjoni rakendusmääruses (EL) 2025/849 ([1]) esitatud ELi sertifitseeritud kukrulahenduste avaliku loetelu URL	URL	Kohustuslik
ListOfCertifiedWalletsQRCode	QR Code, mis sisaldab ListOfCertifiedWalletsURL teavet	ISO-8859-1 Byte mode QR code	Vabatahtlik
WalletSolutionInfoPageURL	Sertifitseeritud kukrulahenduse teabelehe URL, mis asub sertifitseeritud kukrulahenduste loendi lehel ListOfCertifiedWalletsURL, millele on lisatud „?“ ning kukrulahenduse identifikaator WalletSolutionID.	URL	Kohustuslik
WalletSolutionInfoPageQRCode	Ruutkood, mis sisaldab WalletSolutionInfoPageURL teavet	ISO-8859-1 Byte mode QR code	Vabatahtlik
WalletVerifierToolURL*	URL, mis osutab kukrute kontrollimise vahendi otspunktile */.well-known/openid-credential-issuer*, mida kasutatakse tõendite pakkujate metaandmete saamiseks	URL	Vabatahtlik

([1]) Komisjoni 6. mai 2025. aasta rakendusmäärus (EL) 2025/849, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses teabe esitamisega komisjonile ja koostöörühmale sertifitseeritud Euroopa digiidentiteedikukrute loetelu jaoks (ELT L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).“

X LISA

Rakendusmääruse (EL) 2024/2980 II lisa muudetakse järgmiselt:

1. II lisa 1. jao punkti 1 alapunkt i asendatakse järgmisega:

„i) üks või mitu standardile ETSI EN 319 412-2 V2.4.1 (2025-06) või standardile ETSI EN 319 412-3 V1.3.1 (2023-09) vastavat sertifikaati, mida saab kasutada registripidaja poolt registriandmeid kasutades loodud allkirja või templi kontrolliks ja mille puhul sertifitseeritud identiteediandmed sisaldavad registripidaja nime ning registripidaja registreerimisnumbrit (selle olemasolul) vastavalt punktidele c ja d;“;

2. II lisa 2. jao punkti 1 alapunkt h asendatakse järgmisega:

„h) üks või mitu standardile ETSI EN 319 412-2 V2.4.1 (2025-06) või standardile ETSI EN 319 412-3 V1.3.1 (2023-09) vastavat sertifikaati, mida saab kasutada kukruteenuse pakkuja väljastatud kukrukomplekti tõendite autentsuse ja kehtivuse kinnitamiseks ning mille puhul sertifitseeritud identiteediandmed sisaldavad kukruteenuse pakkuja nime ning kukruteenuse pakkuja registreerimisnumbrit (selle olemasolul) vastavalt punktidele a ja b;“;

3. II lisa 3. jao punkti 1 alapunkt h asendatakse järgmisega:

„h) üks või mitu standardile ETSI EN 319 412-2 V2.4.1 (2025-06) või standardile ETSI EN 319 412-3 V1.3.1 (2023-09) vastavat sertifikaati, mida saab kasutada isikutuvastusandmete pakkuja poolt tema pakutavate isikutuvastusandmete jaoks loodud allkirja või templi kontrolliks ning mille puhul sertifitseeritud identiteediandmed sisaldavad isikutuvastusandmete pakkuja nime ning isikutuvastusandmete pakkuja registreerimisnumbrit (kui see on asjakohane) vastavalt punktidele a ja b.“;

4. II lisa 4. jao punkti 1 alapunkt g asendatakse järgmisega:

„g) üks või mitu standardile ETSI EN 319 412-2 V2.4.1 (2025-06) või standardile ETSI EN 319 412-3 V1.3.1 (2023-09) vastavat sertifikaati, mida saab kasutada kukrule tugineva isiku pääsusertifikaatide pakkuja poolt tema poolt kukrule tuginevatele isikutele pakutavate pääsusertifikaatide jaoks loodud allkirja või templi kontrolliks ning mille puhul sertifitseeritud identiteediandmed sisaldavad kukrule tugineva isiku pääsusertifikaatide pakkuja nime ja vajaduse korral teavet, mida on vaja kukrule tugineva isiku pääsusertifikaatide eristamiseks teistest sertifikaatidest.“;

5. II lisasse lisatakse 5. jagu:

„5. Kukrule tugineva isiku registreerimissertifikaatide pakkujate kohta käive teabe esitamine

1. Liikmesriigid esitavad kukrule tugineva isiku registreerimissertifikaatide pakkujate kohta komisjonile järgmise teabe:

a) kukrule tugineva isiku registreerimissertifikaatide pakkuja nimi;

b) kukrule tugineva isiku registreerimissertifikaatide pakkuja registreerimisnumber, kui see on asjakohane;

c) liikmesriik, kus kukrule tugineva isiku registreerimissertifikaatide pakkuja on asutatud;

d) kukrule tugineva isiku registreerimissertifikaatide pakkuja e-posti aadress ja telefoninumber tema poolt kukrule tuginevatele isikutele pakutavaid registreerimissertifikaate puudutavates küsimuses kontakteerumiseks;

e) kui on olemas veebileht lisateabega kukrule tugineva isiku registreerimissertifikaatide pakkuja ja tema poolt kukrule tuginevatele isikutele pakutavate registreerimissertifikaatide kohta, selle URL;

f) sellise veebilehe URL, kus on esitatud kukrule tugineva isiku registreerimissertifikaatide pakkuja põhimõtted ja tingimused, mida ta kohaldab tema poolt kukrule tuginevatele isikutele pakutavate registreerimissertifikaatide pakkumise ja kasutamise suhtes;

g) üks või mitu standardile ETSI EN 319 412-2 V2.4.1 (2025-06) või standardile ETSI EN 319 412-3 V1.3.1 (2023-09) vastavat sertifikaati, mida saab kasutada kukrule tugineva isiku pääsusertifikaatide pakkuja poolt tema poolt kukrule tuginevatele isikutele pakutavate registreerimissertifikaatide jaoks loodud allkirja või templi kontrolliks ning mille puhul sertifitseeritud identiteediandmed sisaldavad kukrule tugineva isiku registreerimissertifikaatide pakkuja nime ja vajaduse korral teavet, mida on vaja kukrule tugineva isiku registreerimissertifikaatide eristamiseks teistest sertifikaatidest.

2. Punktis 1 osutatud teave tuleb esitada iga kukrule tugineva isiku registreerimissertifikaatide pakkuja kohta.“

XI LISA

„I LISA

Artiklis 4 osutatud protokollid ja liidesed

Tehnilist spetsifikatsiooni ETSI TS 119 472-3 V1.1.1 (2026-03) kohaldatakse järgmiste kohandustega:

1. 4.1 General requirements

   — GEN-REQ-4.1-05: kehtetu.

   — *MÄRKUS*: kehtetu.

2. 4.2.3 Provision of registration certificates of PID/EAA Provider to EUDI Wallet

   — ISS-MDATA-REG_CERT-4.2.3-04: üks issuer_info parameetermassiivi andmeelementidest peab sisaldama isikutuvastusandmete / elektroonilise tõendi teenuse pakkuja registreerimissertifikaati.

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

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

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

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

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

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

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

3. 4.2.4.2 ARF pre-defined PID/EAA reuse policy

   — ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: kui andmeliikme id väärtus on 'arf_annex_ii' ning märgendiga 'details' seotud massiiv sisaldab väärtust 'once_only' või väärtust 'per-relying-party', peab märgendiga 'details' seotud massiivi sisaldav JSONi objekt sisaldama ka märgendiga 'reissue_trigger_unused' seotud JSON numbrit.

4. A lisa ei kohaldata.“

XII LISA

„II LISA

Artiklis 5 osutatud tehnilised spetsifikatsioonid

Kohaldatakse ISO/IEC 18013-7:2025 C lisas esitatud tehnilist spetsifikatsiooni.

ETSI TS 119 472-2 V1.2.1 (2026-03) punktides 4.1, 4.2, 5 ja 6 esitatud tehnilisi spetsifikatsioone kohaldatakse järgmiste kohandustega, sh lisades uue punkti 4.3:

1. 1 Scope

— Käesolevas dokumendis määratakse kindlaks kaks protokolli profiili, mis võimaldavad tuginevatel isikutel (edaspidi „RP“) taotleda Euroopa digiidentiteedikukrult elektrooniliste tõendite esitusi (*Presentation of Electronic Attestation of Attributes*, edaspidi „EAAP“) ja isikutuvastusandmeid (edaspidi „PID“) ning Euroopa digiidentiteedikukrul saata RPle EAAPsid/PIDe. Mõlemad profiilid toetavad kaht edastusmehhanismi, API vahendatud ja muud kui API vahendatud edastust, nagu allpool kirjeldatud.

a) Profiil tugineb järgmisele:

— ISO/IEC 18013-5 [10] üksnes muu kui API vahendatud edastusmehhanismi puhul;

— ISO/IEC 18013-7 [16] C lisale API vahendatud edastusmehhanismi puhul.

Profiili nimetatakse ISO/IEC-mdoc profiiliks ning seda on kirjeldatud käesoleva dokumendi punktis 5.

b) Profiil tugineb järgmisele:

OpenID4VC-HAIP [11] nii API vahendatud kui ka muu kui API vahendatud edastusmehhanismi puhul:

— ümbersuunamiste või muu kui API vahendatud edastusmehhanismi kaudu edastamise puhul [11] punktid 5, 5.1, 5.3, 7 ja 8;

— API vahendatud edastusmehhanismi puhul [11] punktid 5, 5.2, 5.3, 7 ja 8.

Profiili nimetatakse OpenID4VC-HAIP ning seda on kirjeldatud käesoleva dokumendi punktis 6.

2. 2.1 Normative references

— [15] ISO 639: 'Language code'

— [16] ISO/IEC 18013-7:2025 „Personal identification – ISO-compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions“

3. 4.1 EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: kehtetu.

4. 4.2 EAAP implementation based on ISO/IEC-mdoc

— EAAP-ISO/IEC-mdoc-01: kehtetu.

— *Märkus 2:* kehtetu.

— EAAP-ISO/IEC-mdoc-02: kehtetu.

5. 4.3 EAAP implementation with mediating API

— EAAP-API-GEN-01: ELi digiidentiteedikukkur toetab vahendavat API-t, mis toetab mõlemat protokolli, mis on määratletud [11] punktis 5.2 ja [16] C lisas.

— *MÄRKUS:* juhul kui seade, millesse ELi digiidentiteedikukkur on installitud, ei toeta mõlemat protokolli, ei ole seda nõuet võimalik täita ja see käivitab mittevastavuse, kuna aluseks olevates operatsioonisüsteemides ja veebilehitsejates ei ole kasutusele võetud vajalikke koostalitlusvõime funktsioone.

— EAAP-API-GEN-02: ELi digiidentiteedikukkur toetab vahendavat API-t vähemalt selliste PIDe ja elektrooniliste tõendite (edaspidi „EAA“) liikide puhul, mis on registreeritud rakendusmääruses (EL) 2025/1569 määratletud tõendamise kavade kataloogis, ning vähemalt kõigi rakendusmääruse (EL) 2024/2979 II lisas määratletud vormingute puhul.

— *MÄRKUS 1:* kui aluseks olev operatsioonisüsteem, veebilehitseja, vahendav API või mõni ELi digiidentiteedikukru kontrollile mitte alluv tehniline kiht piirab, filtreerib, teeb eelvaliku või muul viisil seab piirid sellele, milliseid on tõendite vormingud ning tõendamise kavade kataloogis registreeritud PID ja EAA liigid, ei saa seda nõuet täita. Kui selline piirang ei lase ELi digiidentiteedikukrul toetada registreeritud tõendite liiki või vormingut, siis sellest tingitud mittevastavus tuleneb sellest, et asjaomased aluseks olevad operatsioonisüsteemid, veebilehitsejad, vahendavad APId või muu asjaomane tehniline kiht ei võimalda vajalikke koostalitlusvõime funktsioone.

6. 4.4 Wallet-relying party validation and overasking checks

— WRP-VALIDATION-01: Enne taotletud PID või elektroonilise tõendi esitamist kukrukasutajale tema nõusoleku saamiseks valideerib ELi digiidentiteedikukkur kukrule tugineva isiku registreerimissertifikaadi, mis sisaldub taotluses.

— WRP-VALIDATION-02: kui kukrule tugineva isiku registreerimissertifikaadi valideerimine ebaõnnestub, sealhulgas juhul, kui sertifikaat on aegunud, kehtetuks tunnistatud, seda ei ole väljastanud kukrule tugineva isiku registreerimissertifikaatide valideeritav usaldusväärne pakkuja, see on vigane või seda ei saa krüptograafiliselt kontrollida, hoiatab ELi digiidentiteedikukkur kukrukasutajat, et kukrule tuginevat isikut ei olnud võimalik valideerida, ning taotlust ei kajastata edukalt valideerituna. Kukrukasutaja peab sõnaselgelt väljendama oma nõusolekut kukrule tugineva isiku taotlus rahuldada. Vaikimine ega eelmärgistatud kastikesed ei ole selge nõusoleku väljendamiseks piisavad.

— WRP-VALIDATION-03: kukruteenuse pakkuja määrab oma riskianalüüsi ja turbepõhimõtete põhjal kindlaks, kas ja millistel tingimustel võib kukrukasutaja konkreetseid ebaõnnestunud valideerimiskontrolle arvestamata jätta.

— WRP-OVERASKING-01: ELi digiidentiteedikukkur võrdleb kukrule tugineva isiku taotletud tõendeid ja atribuute kukrule tugineva isiku registreerimissertifikaadis registreeritud tõendite ja atribuutidega.

— WRP-OVERASKING-02: Kui kukrule tuginev isik taotleb PIDe või elektroonilisi tõendeid või väiteid, mida kukrule tugineva isiku registreerimissertifikaat ei hõlma, saadab ELi digiidentiteedikukkur kukrukasutajale enne iga avalikustamist selgesõnalise hoiatuse. Hoiatuses märgitakse, et kukrule tuginev isik taotleb rohkem teavet, kui ta on registreerinud. Kukrukasutaja peab sõnaselgelt väljendama oma nõusolekut kukrule tugineva isiku taotlus rahuldada. Vaikimine ega eelmärgistatud kastikesed ei ole selge nõusoleku väljendamiseks piisavad.

— WRP-OVERASKING-03: kukruteenuse pakkujad määravad oma riskianalüüsi, turbepõhimõtete ja kohaldatavate normide alusel kindlaks selle, kas kukrukasutaja võib sellest hoiatusest hoolimata jätkata, kas avalikustada lubatakse ainult see andmete alamhulg, mis on registreerimissertifikaadiga hõlmatud, või kas taotlus lükatakse tagasi.

7. 5.1 Introduction

— Punktis 5 ja selle alapunktides on kirjeldatud sellise protokolli profiili, mis võimaldab RP-l taotleda Euroopa digiidentiteedikukrult EAAPsid või PIDe ning Euroopa digiidentiteedikukrul saata RP-le taotletud EAAPsid/PIDe, kasutades kas standardil ISO/IEC 18013-5 [10] põhinevat muud kui API vahendatud edastusmehhanismi või standardi ISO/IEC 18013-7 [16] C lisal põhinevat API vahendatud edastusmehhanismi standardis ISO/IEC 18013-5 [10] määratletud andmestruktuuride edastamiseks sobival viisil kapseldatult.

— Punkti 5 ülejäänud osa on hõlmab järgmist:

— punktis 5.2 on kindlaks määratud RPdele ja Euroopa digiidentiteedikukrule ette nähtud nõuded profiilide ja edastusmehhanismide toetamiseks;

— punktis 5.3 on esitatud muule kui API vahendatud edastusmehhanismile esitatavad nõuded;

— punktis 5.4 ja selle alapunktides on esitatud API vahendatud edastusmehhanismile esitatavad nõuded.

8. 5.2 Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: kukrukomplektid, PIDide pakkujad, elektrooniliste tõendite pakkujad, kukruteenuse pakkujad ja tuginevad isikud ei toeta standardis ISO/IEC 18013-5 [10] kirjeldatud serveriotsingut isikutuvastusandmete või elektrooniliste tõendite taotlemiseks ja esitamiseks.

— ISO/IEC 18013-SUPPORT-02: Euroopa digiidentiteedikukrud peavad vastama käesoleva dokumendi punktides 5.3 ja 5.4 määratletud nõuetele.

— ISO/IEC 18013-SUPPORT-04: tugineval isikul tuleks rakendada käesoleva dokumendi punktis 5.4 määratletud profiili.

9. 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: Euroopa digiidentiteedikukrutesse saadetavad seadmepäringud peavad sisaldama [10] punkti 8.3.2.1.2.1 kohast võti-väärtus-paari 'requestInfo'. Paari väärtus peab olema RequestInfo tüüpi.

— ISO/IEC 18013-5-REQ-05: RequestInfo tüüp peab vastama allpool esitatud CDDLi määratlusele.

RequestInfo = {

'euWrprc': bstr; sisaldab registreerimissertifikaati (vt nõuded allpool)

}

— ISO/IEC 18013-5-REQ-06: nimetatud andmeliige requestInfo sisaldab andmeliiget märgendiga 'euWrprc'

— ISO/IEC 18013-5-REQ-07: 'euWrprc' väärtus peab olema CBORis kodeeritud registreerimissertifikaat.

— ISO/IEC 18013-5-REQ-08: kehtetu.

— *MÄRKUS 3:* kehtetu.

— ISO/IEC 18013-5-REQ-09: kehtetu.

— ISO/IEC 18013-5-REQ-10: kehtetu.

— ISO/IEC 18013-5-REQ-11: kehtetu.

10. 5.3.3 ISO/IEC-mdoc EAAP Response profile

— Käesolevas punktis määratakse kindlaks sõnumitüübile DeviceResponse esitatavad nõuded, mida rakendatakse mõlema edastusmehhanismi puhul (API vahendatud ja muu kui API vahendatud).

— *MÄRKUS 1:* kui kasutatakse standardil ISO/IEC 18013-5 [10] põhinevat muud kui API vahendatud edastusmehhanismi, on EAAP vastus täpselt käesolevas punktis kirjeldatud sõnumitüübi DeviceResponse eksemplar. Kui kasutatakse standardi ISO/IEC 18013-7 [16] C lisale tuginevat API vahendatud edastusmehhanismi, kapseldatakse sõnumitüübi DeviceRequest eksemplar vastavalt [16] C lisale.

— ISO/IEC 18013-5-RESP-02: isikutuvastusandmete pakkuja ja elektrooniliste tõendite pakkuja ei tohi lisada enda väljastatavate isikutuvastusandmete ja elektrooniliste tõendite mobiilturvaobjektis sisalduvale kujundile KeyAuthorizations ühtegi andmeelementi, välja arvatud need andmeelemendid, mille kukrule tuginev isik esitab mdoc-päringus sisalduvates edastatavates andmetes, mille kukrukomplekt isikutuvastusandmete või elektrooniliste tõendite privaatvõtmega allkirjastab või tempiga varustab.

— *MÄRKUS 2:* selle tulemusena ei saa kukrukomplektid esitada kukrule tuginevatele isikutele seadmega allkirjastatud andmeelemente, välja arvatud kukrule tugineva isiku esitatud andmete allkirjastamiseks, näiteks kui see toimub kasutaja turvaliseks autentimiseks.

— *MÄRKUS 3:* standardis ISO/IEC 18013-5:2021 ei ole kirjeldatud, kuidas kukrule tuginevad isikud saavad lisada mdoc-päringusse tehinguandmeid. Tehinguandmed lisatakse mdoc-päringusse vastavalt lisanduvatele tehnilistele spetsifikatsioonidele.

— ISO/IEC 18013-5-RESP-03: isikutuvastusandmete pakkujad ei tohi lubada selliste andmeelementide allkirjastamist isikutuvastusandmete privaatvõtmega, mille kukrule tuginev isik on esitanud mdoc-päringus sisalduvates tehinguandmetes.

11. 5.4 Requirements for API mediated mechanism

5.4.1 ISO/IEC 18013-7-related requirements

Käesolevas punktis esitatakse API vahendatud edastusmehhanismile esitatavad nõuded, mis on seotud [16] C lisas määratletud nõuetega.

— ISO/IEC 18013-7-API-01: API vahendatud esitusi toetav profiil peab vastama standardi ISO/IEC 18013-7 [16] C lisa nõuetele, mida on täpsemalt kirjeldatud käesoleva dokumendi punktides 5.3 ja 5.4.

— ISO/IEC 18013-7-API-02: kohaldatakse kõiki [16] C lisas esitatud kohustuslikke nõudeid, nagu on täpsemalt kirjeldatud käesoleva dokumendi punktides 5.3 ja 5.4.

— ISO/IEC 18013-7-API-03: kõik [16] C lisas esitatud vabatahtlikud nõuded on jätkuvalt vabatahtlikud, kui käesolevas dokumendis ei ole nõutud teisiti.

12. 5.4.2 Additional requirements

— Käesolevas punktis kirjeldatakse täpsemalt API vahendatud edastusmehhanismile esitatavaid lisanõudeid.

— ISO/IEC 18013-ADD-API-01: Euroopa digiidentiteedikukkur avalikustab vaikimisi kõigi salvestatud elektrooniliste tõendite olemasoluteabe [16] C lisa kohaselt toimivale vahendavale API-le, kuid ei avalikusta neis elektroonilistes tõendites sisalduvaid atribuute ja nende väärtusi.

— *MÄRKUS 1:* atribuudi väärtuse piirangut kohaldatakse isegi juhul, kui selline avalikustamine parandaks teenuseid, mida operatsioonisüsteem osutab Euroopa digiidentiteedikukrule, näiteks tõendi valimine vahendava API kontekstis.

— Rakendajad ei saa mõjutada teatavaid operatsioonisüsteemide ja veebilehitsejatega seotud aspekte, mida võib vastavalt järgnevalt esitatud märkustele 2–4 arvesse võtta.

— *MÄRKUS 2:* veebilehitseja ja/või operatsioonisüsteem võivad töödelda [16] C lisa toetava tugineva isiku esituspäringut, et otsida olemasolevaid elektroonilisi tõendeid (edaspidi „EAA“), hoida ära kasutajate vastu suunatud pettusi või leida rikkeid.

— *MÄRKUS 3:* kasutajate turvalisuse eesmärgil peaks veebilehitseja ja/või operatsioonisüsteem töötlema [16] C lisa toetava tugineva isiku esituspäringut.

— *MÄRKUS 4:* eeldatakse, et veebilehitseja ja/või operatsioonisüsteem ei töötle [16] C lisa toetava tugineva isiku esituspäringut turuanalüüsi eesmärgil (sealhulgas teisese eesmärgina) ega veebilehitseja ja/või operatsioonisüsteemi sise-eesmärkidel.

— ISO/IEC 18013-ADD-API-02: kui Euroopa digiidentiteedikukkur kustutab kasutaja taotlusel PIDi või EAA, mis oli eelnevalt avalikustatud [16] C lisa kohaselt toimivale vahendavale API-le, avalikustab Euroopa digiidentiteedikukkur vahendavale API-le asjaolu, et PID või EAA on kustutatud.

— ISO/IEC 18013-ADD-API-03: kui kasutaja oma Euroopa digiidentiteedikukru desinstallib, avalikustab Euroopa digiidentiteedikukkur [16] C lisa kohaselt toimivale vahendavale API-le asjaolu, et eelnevalt avalikustatud PIDid ja EAAd on kustutatud.

— ISO/IEC 18013-ADD-API-04: Euroopa digiidentiteedikukkur peab sisaldama üldseadeid, mis võimaldavad blokeerida salvestatud EAAde avalikustamise vahendava API kaudu, mis toimib vastavalt standardile ISO/IEC 18013-ADD-API-01. Kui need seaded on blokeeritud, ei teata Euroopa digiidentiteedikukkur API vahendatud esitus- või väljastamispäringutest ega vasta neile.

— ISO/IEC 18013-ADD-API-05: ELi digiidentiteedikukrud kontrollivad seadmetevaheliste voogude puhul vahendava API abil, kas suhtlev seade asub ELi digiidentiteedikukru vahetus läheduses, kasutades lähedalasuvate seadmete kindlakstegemiseks turvalist ja kasutaja vahendatavat kohalikku otsesidekanalit, näiteks traadita lähitoimeside tehnoloogiat.

— *MÄRKUS:* CTAP 2.3 võimaldab BLE kasutamist lähedalasuvate seadmete kindlakstegemiseks ja – kui mõlemad seadmed seda rakendavad – ka seadmetevahelist andmeedastust lähitoimeside tehnoloogia abil. Aluseks olevad operatsioonisüsteemid, veebilehitsejad, vahendavad API-d või muud ELi digiidentiteedikukru kontrollile mitte alluvad tehnilised kihid peaksid protokolli CTAP hübriidtunnelduse teenuste kasutamise asemel eelistama nii füüsiliseks läheduskontrolliks kui ka andmete ühest seadmest teise edastamiseks kohalikku sidekanalit, nagu seda võimaldab CTAP 2.3.

13. 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: Euroopa digiidentiteedikukkur peab vastama käesoleva lisa punktis 6.5 esitatud nõuetele.

— OIDFVP-HAIP-SUPPORT-03: Euroopa digiidentiteedikukkur ei tohiks toetada punktis 6.4 kirjeldatud ümbersuunamispõhist mehhanismi seadmetevaheliste esitusvoogude jaoks.

— *MÄRKUS 3:* asjaomase mehhanismi kasutamine ei taga kaitset rünnete eest, näiteks seansipetete puhul. Selliste rünnete mõju leevendamine on kukrule tugineva isiku ülesanne. Mehhanismi rakendamine ei tohiks põhjustada nõuete täitmata jätmist.

— OIDFVP-HAIP-SUPPORT-05: tuginev isik peab vastama käesoleva lisa punktis 6.5 esitatud nõuetele.

— *MÄRKUS 5:* kehtetu.

14. 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: kohaldatakse kõiki HAIP [11] punktides 5, 5.3, 7 ja 8 esitatud kohustuslikke nõudeid.

— *MÄRKUS 1:* „HAIP [11] 5. jagu“ tähistab üksnes vahetult 5. jao pealkirja all esitatud nõudeid. See ei hõlma punkte 5.1, 5.2 ja 5.3.

— OIDFVP-HAIP-GEN-03: kui käesoleva lisaga muudetakse OpenID4VC-HAIP [11] nõudeid, on ülimuslik käesolevas lisas kirjeldatud muudetud nõue.

— *MÄRKUS 2*: see võimaldaks näiteks muuta OpenID4VC-HAIP [11] vabatahtliku nõude kohustuslikuks või kohustuslikke nõudeid laiendada.

— OIDFVP-HAIP-GEN-04: kui taotletud tõendi vorming vastab standardile [10], peavad tuginevad isikud ja Euroopa digiidentiteedikukrud vastama [11] 6. jao ISO mdoc-profiilile.

— *MÄRKUS 3:* selguse huvides olgu märgitud, et HAIPis sisalduv „ISO mdoc-profiil“ osutab sellele, et tuginevad isikud ja Euroopa digiidentiteedikukrud peavad vastama [7] B lisa punktist 2 tulenevatele kohaldatavatele nõuetele.

— OIDFVP-HAIP-GEN-05: kui taotletud tõendi vorming vastab standardile [2], peavad tuginevad isikud ja Euroopa digiidentiteedikukrud vastama [11] 6. jaos esitatud IETF SD-JWT VC profiilile.

— *MÄRKUS 4:* selguse huvides olgu märgitud, et IETF SD-JWT VC profiil osutab sellele, et tuginevad isikud ja Euroopa digiidentiteedikukrud peavad vastama [7] B lisa punkti 3 nõuetele ning [11] jao 6.1 nõuetele.

15. 6.3.2.1 General requirements

— OIDFVP-HAIP-COMMON-REQ-01: kehtetu.

16. 6.3.2.2 Requirements for the Request Object

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

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

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

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

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

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

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

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

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

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

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

— *Märkus 2:* kehtetu.

— OIDFVP-HAIP-COMMON-REQ-RO-13: üks parameetri verifier_info andmeelementidest hõlmab registreerimissertifikaati.

— OIDFVP-HAIP-COMMON-REQ-RO-23: OpenID4VP punktis 5.9.3 nimetatud nn lehesertifikaat (*leaf certificate*), mida kasutatakse koos kliendiidentifikaatori prefiksiga x509_hash, on RP pääsusertifikaat, nagu on kirjeldatud standardis ETSI TS 119 475 [14].

17. 6.3.3 Authorization Response (EAAP response) profile

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

18. 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: kehtetu.

— *MÄRKUS:* kehtetu.

19. 6.5.2 Additional requirements

— OIDFVP-HAIP-ADD-API-01: Euroopa digiidentiteedikkur avalikustab vaikimisi kõigi salvestatud EAAde olemasoluteabe vahendavale API-le, mis toimib kooskõlas [11] punktiga 5.2, kuid ei avalikusta neis elektroonilistes tõendites sisalduvaid atribuute ja nende väärtusi.

— OIDFVP-HAIP-ADD-API-04: kui Euroopa digiidentiteedikukkur toetab vahendavat API-t, mis toimib vastavalt standardile OIDFVP-HAIP-ADD-API-01, peavad selle üldised kasutajaseaded võimaldama salvestatud EAAde avalikustamise blokeerimist vahendusliidese kaudu. Kui avalikustamine on seadetes blokeeritud, peaks Euroopa digiidentiteedikukkur võimaldama kasutajal valida üksikuid tõendeid, mis avalikustatakse vahendavale API-le.

— OIDFVP-HAIP-ADD-API-05: ELi digiidentiteedikukrud kontrollivad seadmetevaheliste voogude puhul vahendava API abil, kas suhtlev seade asub ELi digiidentiteedikukru vahetus läheduses, kasutades lähedalasuvate seadmete kindlakstegemiseks turvalist ja kasutaja vahendatavat kohalikku otsesidekanalit, näiteks traadita lähitoimeside tehnoloogiat.

— *MÄRKUS 5:* CTAP 2.3 võimaldab BLE kasutamist lähedalasuvate seadmete kindlakstegemiseks ja – kui mõlemad seadmed seda rakendavad – ka seadmetevahelist andmeedastust lähitoimeside tehnoloogia abil. Aluseks olevad operatsioonisüsteemid, veebilehitsejad, vahendavad API-d või muud ELi digiidentiteedikukru kontrollile mitte alluvad tehnilised kihid peaksid protokolli CTAP hübriidtunnelduse teenuste kasutamise asemel eelistama nii füüsiliseks läheduskontrolliks kui ka andmete ühest seadmest teise edastamiseks kohalikku sidekanalit, nagu seda võimaldab CTAP 2.3.

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

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: kõiki käesolevas dokumendis kirjeldatud nõudeid, mida kohaldatakse standardis ISO/IEC 18013-5 esitatud seadme päringu- ja vastusestruktuuride suhtes, kohaldatakse ka siis, kui Euroopa digiidentiteedikukrule esitatakse ISO/IEC mdoc-esitust puudutav päring [16] punktis C.1 kirjeldatud API vahendatud edastusmehhanismi kaudu.“