Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2026/1731

22.7.2026.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2026/1731

(2026. gada 15. jūlijs),

ar ko attiecībā uz piemērojamajiem standartiem un specifikācijām groza Īstenošanas regulu (ES) 2024/2977, (ES) 2024/2979, (ES) 2024/2980 un (ES) 2024/2982

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK ([1]), un jo īpaši tās 5.a panta 23. punktu,

tā kā:

(1) Lai nodrošinātu visaugstāko saskaņotības līmeni starp dalībvalstīm attiecībā uz Eiropas digitālās identitātes maku izstrādi, maku tehnisko specifikāciju pamatā ir darbs, kas veikts, pamatojoties uz Komisijas Ieteikumu (ES) 2021/946 ([2]), un jo īpaši arhitektūra un atsauces sistēma. Kopš Komisijas Īstenošanas regulu (ES) 2024/2977 ([3]), (ES) 2024/2979 ([4]), (ES) 2024/2980 ([5]) un (ES) 2024/2982 ([6]) pieņemšanas arhitektūra un atsauces sistēma ir ievērojami attīstījušās, un tāpēc minētās īstenošanas regulas tagad būtu jāgroza, lai tās saskaņotu ar jauniem standartiem, specifikācijām un procedūrām.

Saskaņā ar Regulas (ES) Nr. 910/2014 mērķiem šo īpašo prasību izpildei ir atlasīti vairāki standarti. Šādiem standartiem būtu jāatspoguļo iedibinātā prakse un jābūt plaši atzītiem attiecīgajās nozarēs. Piemēram, tā kā W3C VCDM formātu izmanto kā apliecinājumu atsauces formātu, it īpaši izglītības nozarē, arī Eiropas digitālās identitātes makiem būtu jāatbalsta šis formāts, ja ir pieejami jaunie profili W3C VCDM formātā. Vajadzības gadījumā šie standarti būtu jāpielāgo vai jāpapildina, lai nodrošinātu Eiropas digitālās identitātes maku drošību un uzticamību, vienlaikus veicinot pārrobežu sadarbspēju un iekšējā tirgus efektīvu darbību.

(2) Attiecībā uz maka izmantošanu, kad ir jāuzrāda maka lietotāja ģīmetne, maka risinājumiem ir jāatbalsta selektīvās izpaušanas funkcija, un izpaušanai ir jābūt pilnīgā lietotāja kontrolē. Lai aizsargātu spēju lemt par izpaušanu un ģīmetni pret netīšu vai neatļautu izpaušanas pieprasījumu, Eiropas digitālās identitātes maku arhitektūras dizainam būtu jāparedz brīdināšanas mehānismi un jāreģistrē visi darījumi, kas saistīti ar ģīmetnes izmantošanu. Lai nodrošinātu, ka maka lietotājs apzinās, ka tas kopīgo biometriskos datus, brīdinājumos būtu jānorāda, ka pieprasījums ietver biometrisko datu kopīgošanu, un jo īpaši jāpieprasa lietotājam apstiprināt izpaušanu. Ja atkarīgā

([1]) OV L 257, 28.8.2014., 73. lpp., ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Komisijas Ieteikums (ES) 2021/946 (2021. gada 3. jūnijs) par kopīgu Savienības rīkkopu koordinētai pieejai Eiropas digitālās identitātes satvaram (OV L 210, 14.6.2021., 51. lpp., ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([3]) Komisijas Īstenošanas regula (ES) 2024/2977 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes makiem izsniegtajiem personas identifikācijas datiem un atribūtu elektroniskajiem apliecinājumiem (OV L, 2024/2977, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).
([4]) Komisijas Īstenošanas regula (ES) 2024/2979 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes maku integritāti un pamatfunkcijām (OV L, 2024/2979, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).
([5]) Komisijas Īstenošanas regula (ES) 2024/2980 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz paziņojumiem Komisijai par Eiropas digitālās identitātes maku ekosistēmu (OV L, 2024/2980, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).
([6]) Komisijas Īstenošanas regula (ES) 2024/2982 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes satvara atbalstāmajiem protokoliem un saskarnēm (OV L, 2024/2982, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

puse apstrādā ģīmetni, lai unikāli identificētu fizisku personu vai apstiprinātu minētās personas apgalvoto identitāti, piemēro Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 ([7]) 6. un 9. pantu, kā arī visas pārējās minētās regulas prasības, tai skaitā to, ka ģīmetnes apstrādei, ko veic atkarīgās puses, būtu jāaprobežojas tikai ar to, kas ir nepieciešams paredzētajai izmantošanai. Paredzētā izmantošana būtu jāpaziņo maka lietotājam kopā ar izpaušanas pieprasījumu skaidrā un saprotamā valodā. Lai pienācīgi ņemtu vērā biometrisko datu sensitivitāti, maka lietotājam būtu skaidri un konkrēti jāapstiprina ģīmetnes izpaušana. Klusēšana vai iepriekš atzīmēti lodziņi netiek uzskatīti par maka lietotāja apstiprinājumu. Maka lietotāja skaidram apstiprinājumam vajadzētu būt tehniskam drošības pasākumam, nevis pašam par sevi būt apstrādes juridiskajam pamatam. Kā noteikts Regulas (ES) 2016/679 9. panta 4. punktā, dalībvalstis var saglabāt vai ieviest papildu nosacījumus, tostarp ierobežojumus, attiecībā uz ģenētisko datu, biometrisko datu vai veselības datu apstrādi.

(3) Lai dalībvalstīm dotu pietiekami daudz laika pielāgot valsts procedūras, maka lietotāja ģīmetne var būt daļa no fiziskās personas obligātajiem identifikācijas datiem tikai no 2028. gada 11. augusta. Ja šos attēlus iegūst no esošiem personu apliecinošiem dokumentiem, piemēram, personas apliecībām vai pasēm, piemēro attiecīgās prasības, kas noteiktas attiecīgi Padomes Regulās (ES) 2025/1208 ([8]) vai (EK) Nr. 2252/2004 ([9]).

(4) Regulā (ES) Nr. 910/2014 ir noteikts, ka makiem jāspēj parādīt ES digitālās identitātes maka uzticamības marķējumu kā pārbaudāmu, vienkāršu un atpazīstamu norādi, ka maks ir nodrošināts saskaņā ar regulu. Šāda uzticamības marķējuma izmantošana veicinās iekšējā tirgus efektīvu darbību, garantēs godīgu konkurenci un aizsargās patērētāju intereses. Lai varētu izmantot šādu uzticamības marķējumu, būtu jānosaka uzticamības marķējuma vizuālās un tehniskās īpašības.

(5) Kā noteikts Regulas (ES) Nr. 910/2014 12.b pantā, vārtziņi Eiropas digitālās identitātes maku nodrošinātājiem un paziņotu elektroniskās identifikācijas līdzekļu izdevējiem nodrošina efektīvu sadarbspēju ar tām pašām operētājsistēmas, aparatūras vai programmatūras funkcijām un dod tiem iespēju sadarbspējas nolūkā tām piekļūt. Šāda efektīva sadarbspēja un piekļuve ir jānodrošina bez maksas un neatkarīgi no tā, vai minētās aparatūras vai programmatūras funkcijas ir daļa no operētājsistēmas, ir pieejamas minētajam vārtzinim vai minētais vārtzinis tās izmanto, sniedzot šādus pakalpojumus. Tā kā visiem maka risinājumiem būtu jāatbalsta vienots protokolu un saskarņu kopums, lai nodrošinātu lietojamību, drošību un sadarbspēju starp dalībvalstīm, vārtziņiem būtu jānodrošina operētājsistēmas, aparatūras vai programmatūras funkcijas, kas vajadzīgas šīs regulas XII pielikumā noteikto protokolu un saskarņu īstenošanai. Šajā kontekstā tiešsaistes starpierīču plūsmās gan fiziskā tuvuma pārbaudei, gan datu pārsūtīšanai starp abām ierīcēm vārtziņiem būtu jādod priekšroka vietējam sakaru kanālam, ko nodrošina Klienta autentifikācijas protokola (*CTAP*) specifikācijas 2.3. versija ([10]), nevis *CTAP* hibrīdā tuneļa pakalpojumu izmantošanai.

(6) Lai dalībvalstīm, maka atkarīgās puses reģistrācijas sertifikātu nodrošinātājiem un maka nodrošinātājiem dotu pietiekami daudz laika, lai maka vienības spētu autentificēt un validēt maka atkarīgās puses reģistrācijas sertifikātus, šī prasība būtu jāpiemēro tikai no 2028. gada 11. augusta.

(7) Visām šajā regulā paredzētajām personas datu apstrādes darbībām piemēro Regulu (ES) 2016/679 un, attiecīgā gadījumā, Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([11]).

([7]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Padomes Regula (ES) 2025/1208 (2025. gada 12. jūnijs) par Savienības pilsoņu personas apliecību un Savienības pilsoņiem un viņu ģimenes locekļiem, kuri izmanto tiesības brīvi pārvietoties, izsniegto uzturēšanās dokumentu drošības uzlabošanu (OV L, 2025/1208, 20.6.2025., ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Padomes Regula (EK) Nr. 2252/2004 (2004. gada 13. decembris) par drošības elementu un biometrijas standartiem dalībvalstu izdotās pasēs un ceļošanas dokumentos (OV L 385, 29.12.2004., 1. lpp., ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) FIDO alianses ierosinātais standarts "Klienta autentifikācijas protokols" ("Client to Authenticator Protocol") (*CTAP*), 2026. gada 26. februāris.

([11]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([12]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2026. gada 17. aprīlī sniedza atzinumu ([13]).

(9) Šajā regulā noteiktie pasākumi saskan ar atzinumu, ko sniegusi ar Regulas (ES) Nr. 910/2014 48. pantu izveidotā komiteja,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Īstenošanas regulas (ES) 2024/2977 grozījumi

Īstenošanas regulu (ES) 2024/2977 groza šādi:

1) regulā iekļauj šādu 3.a pantu:

"*3.a pants*

Ģīmetnes aizsardzība

1) Papildus informācijas prasībām, kas noteiktas Regulā (ES) 2016/679, maka nodrošinātāji nodrošina, ka to nodrošinātie maka risinājumi izdod brīdinājumus maka lietotājiem, ja maka atkarīgās puses pieprasa ģīmetnes izpaušanu, norādot, ka pieprasījums ietver biometrisko datu kopīgošanu un prasa ģīmetnes selektīvas izpaušanas apstiprinājumu.

2) Lai īstenotu ģīmetnes selektīvu izpaušanu maka atkarīgajai pusei, maka nodrošinātāji nodrošina, ka maka risinājumi prasa maka lietotājam skaidri un konkrēti apstiprināt ģīmetnes parādīšanu.

3) Maka atkarīgās puses ģīmetni nesaglabā, ja vien tās turpmāka apstrāde nav nepieciešama identifikācijas un autentifikācijas nolūkos saskaņā ar Savienības datu aizsardzības tiesību aktiem vai ja tas ir paredzēts Savienības vai valsts tiesību aktos atbilstīgi Savienības datu aizsardzības tiesību aktiem. Ģīmetni nenodod trešām valstīm vai starptautiskām organizācijām, ja vien to neatļauj Savienības datu aizsardzības tiesību akti.";

2) regulas 4. panta 1. punktu aizstāj ar šādu:

"1. Atribūtu elektroniskie apliecinājumi, kas izdoti maka vienībām, atbilst vismaz vienam no standartiem, kas noteikti Īstenošanas regulas (ES) 2024/2979 II pielikumā.";

3) regulas 5. panta 4. punkta b) apakšpunktu aizstāj ar šādu:

"b) ja ir atsaukts maka vienības apliecinājums tai maka vienībai, kurai izsniegti personas identifikācijas dati;";

4) regulas pielikumu aizstāj ar šīs regulas I pielikumā izklāstīto tekstu.

([12]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) EDAU oficiālās piezīmes par īstenošanas regulas projektu attiecībā uz piemērojamajiem standartiem un specifikācijām un Īstenošanas regulas (ES) 2024/2980 labojumiem |Eiropas Datu aizsardzības uzraudzītājs.

2. pants

Īstenošanas regulas (ES) 2024/2979 grozījumi

Īstenošanas regulu (ES) 2024/2979 groza šādi:

1) regulas 3. panta 2. punktu svītro;

2) regulas 5. panta 1. punkta a) apakšpunktu aizstāj ar šādu:

"a) maka kriptogrāfijas operācijas ar kritiski svarīgiem aktīviem, ko glabā maka drošas kriptogrāfijas ierīcē un kas nav nepieciešami maka lietotāja autentificēšanas nolūkā, veic tikai gadījumos, kad minētās lietojumprogrammas ir sekmīgi autentificējušas maka lietotājus;";

3) regulā iekļauj šādu 5.a pantu:

"*5.a pants*

Kriptogrāfijas mehānismi

Maka nodrošinātāji 4. panta 2. punkta nolūkos izmanto tikai Ia pielikumā minētos kriptogrāfijas mehānismus.";

4) regulas 6. pantu groza šādi:

a) panta 1. punktu aizstāj ar šādu:

"1. Maka nodrošinātāji izdod maka vienības apliecinājumus par katru maka vienību. Maka nodrošinātāji paraksta vai apzīmogo maka vienības apliecinājumus tā, lai parakstus vai zīmogus varētu validēt ar sertifikātu, kas norādīts sarakstā saskaņā ar Īstenošanas regulas (ES) 2024/2980 II pielikuma 2. iedaļas 1. punkta h) apakšpunktu.";

b) panta 2. punktu aizstāj ar šādu:

"2. Maka nodrošinātāji nodrošina, ka 1. punktā minētie maka vienības apliecinājumi atbilst Ib pielikumā noteiktajām tehniskajām specifikācijām.";

c) panta 3. punkta b) apakšpunktu aizstāj ar šādu:

"b) nodrošina maka lietotājiem drošus identifikācijas un autentifikācijas mehānismus, kas ir neatkarīgi no maka vienībām;";

5) regulas 9. panta 2. punkta b) apakšpunktu aizstāj ar šādu:

"b) attiecīgās maka atkarīgās puses nosaukumu, kontaktinformāciju un unikālo identifikatoru un dalībvalsti, kurā minētā maka atkarīgā puse ir reģistrēta;";

6) regulas 10. panta 1. punktu aizstāj ar šādu:

"1. Maka nodrošinātāji nodrošina, ka to nodrošinātās maka vienības spēj apstrādāt atribūtu elektroniskos apliecinājumus, kas izdoti saskaņā ar III pielikumā noteiktajām tehniskajām specifikācijām, kuras piemēro kopējām iegultām informācijas izpaušanas procedūrām.";

7) regulas 12. pantu groza šādi:

a) panta 2. punkta c) apakšpunktu aizstāj ar šādu:

"c) parakstu vai zīmogu izveide saskaņā vismaz ar obligāto paraksta vai zīmoga formātu, kas minēts IV pielikumā;";

b) panta 3. punktu aizstāj ar šādu:

"3. Paraksta izveides lietojumprogrammas var integrēt maka instancēs, vai tās var atrasties ārpus maka instancēm.";

c) pantā iekļauj šādu punktu:

"4. Maka vienību izmantotās paraksta izveides lietojumprogrammas atbalsta vismaz IV pielikumā minēto lietojumprogrammas saskarni.";

8) regulas 14. panta 1. punktu svītro;

9) regulā iekļauj šādu 14.a pantu:

"*14.a pants*

ES digitālās identitātes maka uzticamības marķējums

1) Maka nodrošinātāji nodrošina, ka maka vienībām ir ES digitālās identitātes maka uzticamības marķējums. ES digitālās identitātes maka uzticamības marķējums ir VI un VII pielikumā noteiktajā formā.

2) Maka nodrošinātāji nodrošina, ka maka vienības ļauj maka lietotājiem piekļūt informācijai, kas tiem ļauj verificēt maka risinājuma sertifikācijas statusu. Šajā nolūkā maka nodrošinātāji nodrošina, ka pēc maka risinājuma reģistrācijas attiecīgajās maka vienībās ir iekļauti Eiropas Komisijas nodrošinātie URL, ko izmanto šādai verifikācijai. Maka nodrošinātāji nodrošina, ka to maka vienībām ir piekļuve ES digitālās identitātes maka uzticamības marķējuma datiem, kas atbilst VIII pielikumā noteiktajām tehniskajām specifikācijām.

3) ES digitālās identitātes maka uzticamības marķējuma atsauces krāsas ir *Pantone* Nr. 661 un 116 vai, ja izmanto četru krāsu procesu, zila (100 % ciānkrāsa + 67 % fuksīns + 0 % dzeltens + 40 % melns) un dzeltena (0 % ciāns + 20 % fuksīns + 100 % dzeltens + 0 % melns); ja izmanto *RGB* krāsas, atsauces krāsas ir zila (0 sarkana + 51 zaļa + 153 zila) un dzeltena (255 sarkana + 204 zaļa + 0 zila).

4) Tikai tad, ja krāsu izmantošana nav praktiski iespējama, var izmantot melnbaltu ES digitālās identitātes maka uzticamības marķējumu, kā noteikts VII pielikumā.

5) Ja ES digitālās identitātes maka uzticamības marķējumu izmanto uz tumša fona, to var izmantot negatīvā formātā, izmantojot to pašu fona krāsu. Ja ES digitālās identitātes maka uzticamības marķējums ir krāsains un atrodas uz krāsaina fona, kas apgrūtina tā saskatīšanu, ap ES digitālās identitātes maka uzticamības marķējumu var izmantot norobežojošu ārējo līniju, lai uzlabotu kontrastu ar fona krāsām.

6) ES digitālās identitātes maka uzticamības marķējuma minimālais izmērs ir 64 × 85 pikseļi 150 dpi.

7) Maka nodrošinātāji nodrošina, ka ES digitālās identitātes maka uzticamības marķējums tiek izmantots tādā veidā, kas ļauj skaidri norādīt maka vienību, uz kuru attiecas ES digitālās identitātes maka uzticamības marķējums. ES digitālās identitātes maka uzticamības marķējumu var sasaistīt ar grafiskiem vai teksta elementiem, kas skaidri parāda maka vienību, kurai to izmanto, ar nosacījumu, ka tie nemaina tā kā ES digitālās identitātes maka uzticamības marķējuma atpazīstamību, kā arī nemaina saikni ar sertificēto Eiropas digitālās identitātes maku sarakstu, kas minēts Regulas (ES) Nr. 910/2014 5.d pantā.

8) Ja maka nodrošinātāji ir atsaukuši maka vienības apliecinājumu, tie nodrošina, ka attiecīgā maka vienība vairs nerāda ES digitālās identitātes maka uzticamības marķējumu.";

10) iekļauj Ia un Ib pielikumu, kā noteikts šīs regulas II un III pielikumā;

11) II pielikumu aizstāj ar šīs regulas IV pielikumu;

12) III pielikumu aizstāj ar šīs regulas V pielikumu;

13) IV pielikumu groza saskaņā ar šīs regulas VI pielikumu;

14) V pielikumu svītro;

15) šīs regulas VII pielikumā izklāstīto tekstu iekļauj kā VI pielikumu;

16) šīs regulas VIII pielikumā izklāstīto tekstu iekļauj kā VII pielikumu;

17) šīs regulas IX pielikumā izklāstīto tekstu iekļauj kā VIII pielikumu.

3. pants

Īstenošanas regulas (ES) 2024/2980 grozījumi

Īstenošanas regulu (ES) 2024/2980 groza šādi:

1) regulas 5. panta 2. punktu aizstāj ar šādu:

"2. Attiecīgā gadījumā Komisija izveido, uztur un publicē sarakstu, kurā apkopota informācija, ko dalībvalstis paziņojušas par maka nodrošinātājiem, personas identifikācijas datu sniedzējiem, maka atkarīgās puses piekļuves sertifikātu nodrošinātājiem un maka atkarīgās puses reģistrācijas sertifikātu nodrošinātājiem, kā noteikts II pielikuma 2., 3., 4. un 5. iedaļā.";

2) Īstenošanas regulas (ES) 2024/2980 II pielikumu groza, kā noteikts šīs regulas X pielikumā.

4. pants

Īstenošanas regulas (ES) 2024/2982 grozījumi

Īstenošanas regulu (ES) 2024/2982 groza šādi:

1) regulas 1. panta 2. punktu aizstāj ar šādu:

"2) personas identifikācijas datu un atribūtu elektronisko apliecinājumu uzrādīšanai maka atkarīgajām pusēm;";

2) regulas 3. pantu groza šādi:

a) panta 1. punktu aizstāj ar šādu:

"1) autentificē un validē maka atkarīgās puses piekļuves sertifikātus, ja tie mijiedarbojas ar maka atkarīgajām pusēm, nedeleģējot šo procesu izpildi operētājsistēmas pārlūkprogrammai vai citai starpnieklietotnei;";

b) panta 2. punktu svītro;

c) panta 3. punktu aizstāj ar šādu:

"3) autentificē un validē pieprasījumus, kas iesniegti, izmantojot maka atkarīgās puses piekļuves sertifikātus;";

d) panta 4. punktu aizstāj ar šādu:

"4) autentificē un validē maka atkarīgās puses reģistrācijas sertifikātu;";

e) panta 5. punktu aizstāj ar šādu:

"5) parāda maka lietotājiem informāciju, kas ietverta maka atkarīgās puses piekļuves sertifikātos;";

f) panta 8. punktu svītro;

g) panta 9. punktu aizstāj ar šādu:

"9) nesniedz nekādus pieprasītos atribūtus maka atkarīgajām pusēm, kamēr nav pabeigtas šādas darbības:

a) ir verificēts, ka maka vienībās ir apstrādātas iegultās informācijas atklāšanas procedūras saskaņā ar Īstenošanas regulas (ES) 2024/2979 10. pantu;

b) ir verificēts, ka maka lietotāji ir daļēji vai pilnībā apstiprinājuši uzrādīšanu.";

3) regulas 4. panta 1. punktu aizstāj ar šādu:

"1. Maka nodrošinātāji nodrošina, ka maka risinājumi atbalsta protokolus un saskarnes, kas norādītas I pielikumā, attiecībā uz personas identifikācijas datu un atribūtu elektronisko apliecinājumu izdošanu maka vienībām.";

4) regulas 5. pantu groza šādi:

   a) panta 1. un 2. punktu aizstāj ar šādiem:

   "1. Maka nodrošinātāji nodrošina, ka maka risinājumi atbalsta protokolus un saskarnes atribūtu uzrādīšanai maka atkarīgajām pusēm attālināti un attiecīgā gadījumā tuvā attālumā saskaņā ar II pielikumā noteiktajām tehniskajām specifikācijām.

   2. Maka nodrošinātāji nodrošina, ka pēc lietotāju pieprasījuma maka vienības atbild uz sekmīgi autentificētiem un validētiem 3. pantā minēto maka atkarīgo pušu pieprasījumiem saskaņā ar II pielikumā noteiktajām tehniskajām specifikācijām.";

   b) panta 5. punktu svītro;

5) regulas 8. pantu aizstāj ar šādu:

"*8. pants*

Stāšanās spēkā

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

3. panta 4. punktu piemēro no 2028. gada 11. augusta.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.";

6) regulas pielikumu svītro;

7) šīs regulas XI pielikumā izklāstīto tekstu pievieno kā I pielikumu;

8) šīs regulas XII pielikumā izklāstīto tekstu pievieno kā II pielikumu.

5. pants

Stāšanās spēkā

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2026. gada 15. jūlijā

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

I PIELIKUMS

"PIELIKUMS

3. panta 3. punktā minēto personas identifikācijas datu tehniskā specifikācija

1. 1. iedaļa. Fiziskas personas identifikācijas datu kopa

1. tabula

Obligātie fiziskas personas identifikācijas dati selektīvai izpaušanai

Datu identifikators	Definīcija
`family_name`	Lietotāja, ar kuru saistīti personas identifikācijas dati, pašreizējais(-ie) uzvārds(-i).
`given_name`	Lietotāja, ar kuru saistīti personas identifikācijas dati, pašreizējais(-ie) vārds(-i), attiecīgā gadījumā arī otrais(-ie) vārds(-i).
`birth_date`	Lietotāja, ar kuru saistīti personas identifikācijas dati, dzimšanas diena, mēnesis un gads.
`birth_place`	Valsts, kurā dzimis lietotājs, uz kuru attiecas personas identifikācijas dati, kā norādīts ISO 3166-1, izmantojot valsts divburtu kodu, vai pavalsts, province, rajons vai vietējais apgabals, vai pašvaldība, pilsēta vai ciems, kurā dzimis lietotājs, uz kuru attiecas personas identifikācijas dati.
`nationality`	Viens vai vairāki ISO 3166-1 noteiktie valstu divburtu kodi, kas atbilst tā lietotāja valstspiederībai, ar kuru saistīti personas identifikācijas dati.
`portrait`	Izņemot gadījumus, kad lietotājs skaidri pauž nepiekrišanu, attiecīgā gadījumā, tā lietotāja, uz kuru attiecas personas identifikācijas dati, sejas attēls, kurš atbilst pilna frontālā attēla tipa kvalitātes prasībām, kas noteiktas ISO/IEC 39794-5, vai — attiecībā uz atpakaļsaderības prasībām — ISO/IEC 19794-5 8.2., 8.3. un 8.4. punktam, ko nodrošina kā kodētus attēla datus bez galvenēm vai blokiem, kā noteikts ISO/IEC 19794-5 5. punktā, izņemot pašus attēla datus (*JPEG*), piemēro no 2028. gada 11. augusta.

— Dalībvalstis var paredzēt, ka lietotājam ir iespēja atteikties no ģīmetnes ievietošanas personas identifikācijas datos.

— Dalībvalstis nodrošina, ka selektīvā izpaušana attiecas uz katru datu identifikatoru, tai skaitā ģīmetni.

— Ja fiziskās personas dzimšanas datums nav zināms, dalībvalstis izvēlas atbilstošas vērtības, kas atbilst šā pielikuma 4.1. vai 4.2. iedaļā (pēc vajadzības) noteiktajām specifikācijām.

— Ja fiziskās personas valstspiederība nav zināma, dalībvalstis izmanto vērtību "QU".

— Ja fiziskajai personai nav valstspiederības, dalībvalstis izmanto vērtību "QS".

— Ja lietotājs izvēlas neiekļaut ģīmetni, dalībvalstis vērtību iestata tukšu.

2. tabula

Fakultatīvi fiziskas personas identifikācijas dati selektīvai izpaušanai

Datu identifikators	Definīcija
`resident_address`	Tās vietas pilna adrese, kurā lietotājs, uz kuru attiecas personas identifikācijas dati, pašlaik dzīvo vai kurā ar viņu var sazināties (ielas nosaukums, mājas numurs, pilsēta utt.).
`resident_country`	Valsts, kurā pašlaik dzīvo lietotājs, uz kuru attiecas personas identifikācijas dati, kā norādīts *ISO* 3166-1, izmantojot valsts divburtu kodu.
`resident_state`	Pavalsts, province, rajons vai vietējais apgabals, kur pašlaik dzīvo lietotājs, ar kuru saistīti personas identifikācijas dati.
`resident_city`	Pašvaldība, pilsēta vai ciems, kur pašlaik dzīvo lietotājs, ar kuru saistīti personas identifikācijas dati.
`resident_postal_code`	Tās vietas pasta indekss, kur pašlaik dzīvo lietotājs, ar kuru saistīti personas identifikācijas dati.
`resident_street`	Tās ielas nosaukums, kurā pašlaik dzīvo lietotājs, uz kuru attiecas personas identifikācijas dati, tajā skaitā mājas numurs un jebkāds afikss vai sufikss.
`personal_administrative_number`	Lietotājam, uz kuru attiecas personas identifikācijas dati, piešķirta vērtība, kas ir unikāla starp visiem personas administratīvajiem numuriem, kurus piešķīris personas identifikācijas datu sniedzējs. Ja dalībvalstis izvēlas iekļaut šo atribūtu, tās savās elektroniskās identifikācijas shēmās, saskaņā ar kurām tiek izdoti personas identifikācijas dati, apraksta procedūru, ko tās piemēro šā atribūta vērtībām, tajā skaitā attiecīgā gadījumā īpašus nosacījumus šīs vērtības apstrādei.
`family_name_birth`	Lietotāja, uz kuru attiecas personas identifikācijas dati, uzvārds(-i) dzimšanas brīdī.
`given_name_birth`	Lietotāja, uz kuru attiecas personas identifikācijas dati, vārds(-i), arī otrais(-ie) vārds(-i), dzimšanas brīdī.
`sex`	Jābūt vienai no šādām vērtībām: 0 = nav zināms; 1 = vīriešu; 2 = sieviešu; 3 = cits; 4 = starp; 5 = daudzveidīgs; 6 = atvērts; 9 = neattiecas. Vērtībām 0, 1, 2 un 9 piemēro ISO/IEC 5218.
`email_address`	Lietotāja, uz kuru attiecas personas identifikācijas dati, elektroniskā pasta adrese [saskaņā ar RFC 5322 ([1])].

Datu identifikators	Definīcija
`mobile_phone_number`	Lietotāja, uz kuru attiecas personas identifikācijas dati, mobilā tālruņa numurs, kas sākas ar starptautiskā koda simbolu "+", kam seko valsts kods un tālruņa numurs (tikai ar cipariem).

([1]) *P. Resnick, Ed., Internet Message Format*, RFC 5322, 2008. gada oktobris.

2. 2. iedaļa. Juridiskas personas identifikācijas datu kopa

3. tabula

Obligātie juridiskas personas identifikācijas dati

Datu identifikators
Pašreizējais juridiskais nosaukums
Unikāls identifikators, ko sūtītāja dalībvalsts sastādījusi saskaņā ar tehniskajām specifikācijām pārrobežu identifikācijas vajadzībām un kas saglabājas pēc iespējas ilgāk

— Ja personas datu identifikatora vērtība nav zināma vai to citādi nevar izdot kā daļu no personas identifikācijas datu kopas, dalībvalstis tā vietā izmanto situācijai atbilstošu atribūta vērtību.

4. tabula

Neobligātie juridiskas personas identifikācijas dati

Datu identifikators
Pašreizējā adrese
PVN reģistrācijas numurs
Nodokļu maksātāja numurs
Eiropas unikālais identifikators, kas minēts Eiropas Parlamenta un Padomes Direktīvā (ES) 2017/1132 ([1])
Juridiskās personas identifikators (*LEI*), kas minēts Komisijas Īstenošanas regulā (ES) 2022/1860 ([2])
Ekonomikas dalībnieku reģistrācija un identifikācija (*EORI*), kas minēta Komisijas Īstenošanas regulā (ES) Nr. 1352/2013 ([3])
Akcīzes numurs, kas paredzēts Padomes Regulas (ES) Nr. 389/2012 ([4]) 2. panta 12. punktā

([1]) Eiropas Parlamenta un Padomes Direktīva (ES) 2017/1132 (2017. gada 14. jūnijs) attiecībā uz sabiedrību tiesību dažiem aspektiem (OV L 169, 30.6.2017., 46. lpp., ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Komisijas Īstenošanas regula (ES) 2022/1860 (2022. gada 10. jūnijs), ar ko nosaka īstenošanas tehniskos standartus Eiropas Parlamenta un Padomes Regulas (ES) Nr. 648/2012 piemērošanai attiecībā uz ziņošanas standartiem, formātiem, biežumu, metodēm un kārtību (OV L 262, 7.10.2022., 68. lpp., ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Komisijas Īstenošanas regula (ES) Nr. 1352/2013 (2013. gada 4. decembris), ar ko izveido veidlapas, kuras paredzētas Eiropas Parlamenta un Padomes Regulā (ES) Nr. 608/2013 par muitas darbu intelektuālā īpašuma tiesību īstenošanā (OV L 341, 18.12.2013., 10. lpp., ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Padomes Regula (ES) Nr. 389/2012 (2012. gada 2. maijs) par administratīvu sadarbību akcīzes nodokļu jomā un ar ko atceļ Regulu (EK) Nr. 2073/2004 (OV L 121, 8.5.2012., 1. lpp., ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3. 3. iedaļa. Metadatu kopa par fiziskas personas identifikācijas datiem

5. tabula

Metadati par personas identifikācijas datiem

Datu identifikators	Definīcija	Izmantošana
`issuing_authority`	Tās administratīvās iestādes nosaukums, kas izdevusi personas identifikācijas datus, vai attiecīgās dalībvalsts ISO 3166 valsts divburtu kods, ja nav atsevišķas iestādes, kas būtu tiesīga izsniegt personas identifikācijas datus.	obligāti
`issuing_country`	Personas identifikācijas datu sniedzēja valsts vai teritorijas divburtu kods, kā norādīts ISO 3166-1.	obligāti
`expiry_date`	Datums (un, ja iespējams, laiks), kad beigsies personas identifikācijas datu administratīvā derīguma periods.	neobligāti
`document_number`	Personas identifikācijas datu numurs, ko piešķir personas identifikācijas datu sniedzējs.	neobligāti
`issuing_jurisdiction`	Tās jurisdikcijas valsts apakšiedalījuma kods, kurā izdoti personas identifikācijas dati, kā noteikts ISO 3166-2:2020 8. punktā. Koda pirmā daļa ir tāda pati kā izdevējvalsts vērtība.	neobligāti
`issuance_date`	Datums (un, ja iespējams, laiks), kad sākās personas identifikācijas datu administratīvā derīguma periods.	neobligāti

4. 4. iedaļa. Fiziskas personas identifikācijas datu atribūtu kodēšana

— Fiziskas personas identifikācijas datus izdod saskaņā ar Īstenošanas regulas (ES) 2024/2979 II pielikuma 5. punktā (*SD-JWT VC* formāts) un 6. punktā (*ISO/IEC-mdoc* formāts) noteiktajiem standartiem, kas piemērojami atribūtu elektroniskajiem apliecinājumiem. Nepiemēro 5.2.2., 5.2.4., 5.2.5., EAA-6.1-03., 6.2.2., 6.2.3., 6.2.4. un 6.2.5. punktu.

— Fiziskas personas identifikācijas datu kodēšana atbilst tehniskajām specifikācijām šā pielikuma 4.1. un 4.2. iedaļā.

4.1. Fiziskas personas identifikācijas datu kodēšana *ISO/IEC-mdoc* formātā

— Personas identifikācijas datu apliecinājuma veids *ISO/IEC mdoc* formātā ir "eu.europa.ec.eudi.pid.1". Šajā pielikumā noteikto personas identifikācijas datu atribūtu nosaukumu telpas identifikators ir "eu.europa.ec.eudi.pid.1".

— Ja personas identifikācijas dati ietver datus, kuru datu identifikatori nav noteikti šajā pielikumā, šos datus definē iekšzemes personas identifikācijas datu nosaukumu telpā, kurā izmanto vispārējo formātu "eu.europa.ec.eudi.pid." [ISO 3166-1 valsts divburtu kods vai ISO 3166-2 reģiona kods], kam seko neobligāts punkts un versijas numurs.

— Ja izmanto iekšzemes nosaukumu telpu, tās shēmu, tostarp visus datu identifikatorus, to definīcijas, klātbūtnes un kodēšanas formātus, publicē saskaņā ar Komisijas Īstenošanas regulas (ES) 2025/1569 ([1]) 8. pantu.

— Šā pielikuma 1. un 3. iedaļā minētos personas identifikācijas datus un to metadatus iekļauj personas identifikācijas datu elementos *ISO/IEC mdoc* formāta specifikāciju nozīmē.

— *deviceKey* elements *MobileSecurityObject* tipa instances *deviceKeyInfo* elementā ietver publisko atslēgu.

— Minētā publiskā atslēga atbilst privātai atslēgai, kas tiek glabāta maka lietotāja maka drošas kriptogrāfijas ierīcē ("WSCD").

— *CB-AdES* digitālā paraksta aizsargātā galvene, kas paraksta personas identifikācijas datus *ISO/IEC-mdoc* formātā, satur x5u un x5t galvenes parametrus, kas norādīti RFC 9360 ([2]).

— Jaucējfunkcijas algoritms, ko izmanto x5t galvenes parametrā, ir SHA-256.

— Prasības personas identifikācijas datu kodēšanai *ISO/IEC-mdoc* formātā ir izklāstītas 6. tabulā.

6. tabula

Prasības personas identifikācijas datu kodēšanai *ISO/IEC-mdoc* formātā

Datu identifikators	Atribūta identifikators	Kodēšanas formāts
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]) Komisijas Īstenošanas regula (ES) 2025/1569 (2025. gada 29. jūlijā), kas nosaka noteikumus par Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 piemērošanu attiecībā uz kvalificētiem atribūtu elektroniskajiem apliecinājumiem un par autentisku avotu atbildīgas publiskas iestādes vai tās vārdā sniegtiem atribūtu elektroniskajiem apliecinājumiem (OV 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/).

Datu identifikators	Atribūta identifikators	Kodēšanas formāts
`email_address`	`email_address`	tstr
`mobile_phone_number`	`mobile_phone_number`	tstr
`expiry_date`	`expiry_date`	tdate vai 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 vai full-date

— 6. tabulā norādīto atribūtu kodēšanas formāta apzīmējumā izmanto atveidojuma veidus, kā norādīts RFC 8610 ([3]), ievērojot šādas papildu prasības:

a) tstr kodē UTF-8;

b) tstr atbalsta pilnu *unicode* diapazonu;

c) tstr maksimālais garums ir 150 rakstzīmes;

d) datumu kodē, kā norādīts RFC 8943 ([4]);

e) pilnu datumu interpretē kā #6.1004(tstr), kur tag 1004 ir tāds, kā norādīts RFC 8943;

f) tdate atribūts satur datuma un laika virkni, kā norādīts RFC 3339 ([5]);

g) *full-date* atribūts satur *full-date* virkni, kā norādīts RFC 3339, saskaņā ar RFC 8943;

h) ja vien nav norādīts citādi, datuma attēlojumā atribūtos:

— neizmanto sekunžu daļas,

— neizmanto lokālo nobīdi no UTC, un RFC 3339 norādītā laika nobīde ir iestatīta uz "Z";

i) vesels skaitlis ar galvenajiem tipiem 0 un 1 ir pēc iespējas mazāks, kā norādīts RFC 8949 ([6]) 4.2. iedaļā;

j) *place_of_birth* satur vismaz vienu no šādiem atslēgas un vērtības pāriem: "valsts", "reģions" vai "apvidus";

k) garuma izteiksme bstr, tstr, masīvā vai kartē ir pēc iespējas īsāka, kā norādīts RFC 8949 4.2. iedaļā;

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

l) atribūta valstspiederību kodē kā valsts divburtu kodu masīvu, kā noteikts ISO 3166-1. Ja izmanto *CDDL* apzīmējumu, kā norādīts RFC 8610, šā atribūta kods ir:

— nationalities = [+ CountryCode],

— CountryCode = tstr ; ISO 3166-1 norādītais valsts divburtu kods,

— ja maka lietotājam, uz kuru attiecas personas identifikācijas dati, ir vairākas valstspiederības un personas identifikācijas datu sniedzējs apliecina šīs vairākas valstspiederības, personas identifikācijas datu sniedzējs personas identifikācijas datos var iekļaut visas valstspiederības,

— atribūtu *place_of_birth* kodē kā tipu *place_of_birth*. Ja izmanto *CDDL* apzīmējumu, kā norādīts RFC 8610, šā atribūta kods ir:

place_of_birth =

{

? 'country': tstr; viens valsts divburtu kods, kā norādīts ISO 3166-1

? 'region': tstr; valsts, provinces, rajona vai vietējās teritorijas nosaukums

? 'locality': tstr; pašvaldības, pilsētas vai ciemata nosaukums

}

4.2. Prasības personas identifikācijas datu kodēšanai *SD-JWT VC* formātā

— Šajā iedaļā norādītos personas identifikācijas datus un to metadatus iekļauj personas identifikācijas datos kā apgalvojumus (*claims*) *SD-JWT VC* formāta specifikāciju nozīmē.

— Visi apgalvojumi izdotajos personas identifikācijas datos, kas minēti iepriekšējā ievilkumā, ir selektīvi atklājami atsevišķi, izņemot tos apgalvojumus, kas definēti kā neselektīvi atklājami *SD-JWT VC* formātā.

— 7. tabulā ir precizēta apgalvojumu nosaukumu, kas ir publiski nosaukumi, kodēšana.

— 8. tabulā ir precizēta apgalvojumu nosaukumu kodēšana, kas ir specifiska personas identifikācijas datiem.

— *JSON* virkni, ko izmanto personas identifikācijas datos, kuri kodēti *SD-JWT VC*, kodē UTF-8, un tā atbalsta pilnu *Unicode* diapazonu, ja vien 8. tabulā vai tajā ietvertajās atsaucēs nav nepārprotami norādīts citādi.

— *JWT* apgalvojumus nbf un exp , kas definēti RFC 7519 ([7]), izmanto, lai izteiktu *SD-JWT VC* formātam atbilstošu personas identifikācijas datu tehniskā derīguma termiņu.

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

— Personas identifikācijas datos iekļauj cnf apgalvojumu, kā definēts RFC 7800 ([8]), kas ir publiska atslēga, kura ģenerēta no privātas atslēgas, kas tiek glabāta maka lietotāju maka vienības *WSCD*.

— Elektroniskā paraksta aizsargātā galvene, kas paraksta personas identifikācijas datus*SD-JWT VC* formātā, satur RFC 7515 ([9]) norādītos x5u un x5t#S256 galvenes parametrus.

7. tabula

Prasības personas identifikācijas datu kodēšanai *SD-JWT VC* formātā, izmantojot publiskos nosaukumus

Datu identifikators	Atribūta identifikators	Kodēšanas formāts
`family_name`	`family_name`	virkne
`given_name`	`given_name`	virkne
`birth_date`	`birthdate`	virkne, ISO 8601-1, GGGG-MM-DD formāts
`birth_place`	`place_of_birth`	*JSON* struktūra
`nationality`	`nationalities`	virkņu masīvs
`resident_address`	`address.formatted`	virkne
`resident_country`	`address.country`	virkne
`resident_state`	`address.region`	virkne
`resident_city`	`address.locality`	virkne
`resident_postal_code`	`address.postal_code`	virkne
`resident_street`	`address.street_address`	virkne
`family_name_birth`	`birth_family_name`	virkne
`given_name_birth`	`birth_given_name`	virkne
`email_address`	`email`	virkne
`mobile_phone_number`	`phone_number`	virkne
`portrait`	`picture`	virkne; datu URL, kas satur ar base64 kodētu ģīmetni *JPEG* formātā

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

8. tabula

Prasības personas identifikācijas datu kodēšanai *SD-JWT VC* formātā, izmantojot privātus nosaukumus

Datu identifikators	Atribūta identifikators	Kodēšanas formāts
`expiry_date`	`date_of_expiry`	virkne, ISO 8601-1, GGGG-MM-DD formāts
`issuance_date`	`date_of_issuance`	virkne, ISO 8601-1, GGGG-MM-DD formāts
`personal_administrative_number`	`personal_administrative_number`	virkne
`sex`	`sex`	skaitlis
`issuing_authority`	`issuing_authority`	virkne
`issuing_country`	`issuing_country`	virkne
`document_number`	`document_number`	virkne
`issuing_jurisdiction`	`issuing_jurisdiction`	virkne

— Personas identifikācijas datu pamattips ir "urn:eudi:pid:1", kas iekļauts *vct* apgalvojumā. Visiem personas identifikācijas datiem izmanto tipus nosaukumu telpā "urn:eudi:pid:".

— Ja personas identifikācijas dati ietver atribūtus, kas nav norādīti šajā pielikumā, šos atribūtus definē iekšzemes tipa ietvaros.

— Ja izmanto iekšzemes tipu, tā shēmu, tostarp visus datu identifikatorus, to definīcijas, klātbūtnes un kodēšanas formātus, publicē saskaņā ar Īstenošanas regulas (ES) 2025/1569 8. pantu.

5. 5. iedaļa. Informācija par uzticamības infrastruktūru

Personas identifikācijas datu sniedzēju saraksts, ko Komisija darījusi pieejamu saskaņā ar Īstenošanas regulu (ES) 2024/2980, ļauj autentificēt personas identifikācijas datus."

II PIELIKUMS

"*Ia PIELIKUMS*

Kriptogrāfijas mehānismi, kas minēti 5.a pantā

Eiropas Kiberdrošības sertifikācijas grupas apakšgrupa kriptogrāfijas jautājumos – "Saskaņoti kriptogrāfijas mehānismi", ko publicējusi Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) ([1])."

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

III PIELIKUMS

"Ib PIELIKUMS

6. panta 2.a punktā minēto maka vienību apliecinājumu tehniskā specifikācija

1. Maka vienības apliecinājums sastāv no viena vai vairākiem maka instances apliecinājumiem un viena vai vairākiem atslēgu apliecinājumiem.

2. Maka instances apliecinājums un atslēgas apliecinājumi atbilst turpmāk norādītajām prasībām.

a) Prasības attiecībā uz formātu

— FR-WIA-1: maka instances apliecinājums ir *JSON Web Token (JWT)*, kas norādīts RFC 7519 ([1]) un ko maka nodrošinātājs parakstījis vai apzīmogojis ar kompaktu *JAdES* pamata parakstu B.

— FR-WIA-1.1: maka instances apliecinājums ir maka apliecinājums, kas norādīts dokumenta "OpenID for Verifiable Credential Essuance" ([2]) 1.0. versijas E papildinājumā (*OID4VCI*) un plašāk precizēts C-WIA-1 un C-WIA-2 tālāk tekstā.

— FR-KA-1: atslēgas apliecinājums ir *JWT*, kā norādīts RFC 7519, ko maka nodrošinātājs parakstījis vai apzīmogojis ar kompaktu *JAdES* pamata parakstu B.

— FR_KA_1.1: atslēgas apliecinājums ir atslēgas apliecinājums, kas norādīts *OID4VCI* D papildinājumā un paplašināts, kā norādīts C_KA-1 un C_KA-2 tālāk tekstā.

b) Prasības attiecībā uz nosūtīšanu

— TR-WIA-1: personas identifikācijas datu izdošanas laikā maka vienība izmanto maka instances apliecinājumu, kvalificētus vai nekvalificētus atribūtu elektroniskos apliecinājumus vai atribūtu elektroniskos apliecinājumus, ko sniegusi par autentisku avotu atbildīga publiskā iestāde vai kas sniegti tās vārdā.

— TR-WIA-2: maka nodrošinātājs verificē maka instances integritāti un paraksta vai apzīmogo maka instances apliecinājumu.

— TR-WIA-2.1: ja maka nodrošinātājs izdod maka instances apliecinājumu, starpība starp laiku, kad maka nodrošinātājs verificējis maka instances integritāti, un laiku, ko tas norādīs izdotā maka instances apliecinājuma galvenes parametrā "exp", ir mazāka par 24 stundām.

— TR-WIA-2.2: maka nodrošinātājs nodrošina, ka maka vienība ietver maka instances apliecinājumus, kas vajadzīgi personas identifikācijas datu un atribūtu elektronisko apliecinājumu izdošanai.

— TR-WIA-3: izdošanas laikā maka vienība nosūta maka instances apliecinājumu autorizācijas serverim sūtītajā autorizācijas pieprasījumā un marķiera pieprasījumā, kā norādīts *OID4VCI*.

— TR-WIA-3.1: maka vienība nosūta maka instances apliecinājumu kopā ar valdījuma apliecinājumu ("PoP"), kā norādīts *OID4VCI* E papildinājumā.

— TR-WIA-3.2: maka vienība nosūta to pašu maka instances apliecinājumu tikai vienam autorizācijas serverim.

([1]) RFC 7519: *JSON Web Token (JWT)*, 2015. gada maijs.
([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: ja maka nodrošinātājs izmanto R_WIA_1 norādīto iespēju “per-issuer reuse” (izdevēja atkalizmantošanai), maka vienība var nosūtīt maka instances apliecinājumu tam pašam autorizācijas serverim vairākas reizes.

— TR-WIA-3.2.2: ja maka nodrošinātājs neizmanto iespēju “*per-issuer reuse*” (izdevēja atkalizmantošanai), maka vienība izmanto maka instances apliecinājumu ne vairāk kā vienā izdošanas procesā.

— TR-WIA-4: ja autorizācijas serveris saņem maka instances apliecinājumu, tas verificē maka instances apliecinājuma parakstu, izmantojot publisko atslēgu parakstīšanas sertifikātā, kas iekļauts parametrā “x5c” maka instances apliecinājuma *JOSE* galvenē.

— TR-WIA-4.1: autorizācijas serveris arī verificē, vai šo parakstīšanas sertifikātu var verificēt ar uzticamības enkuru maka nodrošinātāju uzticamības sarakstā, kas minēts Īstenošanas regulas (ES) 2024/2980 5. pantā, iespējams, izmantojot x5c parametrā iekļautos starpnieksertifikātus.

— TR-WIA-4.2: autorizācijas serveris pārbauda, vai nav beidzies maka instances apliecinājuma derīguma termiņš.

— TR-WIA-4.3: autorizācijas serveris pārbauda *PoP* parakstu, izmantojot publisko atslēgu, kas norādīta apgalvojumā “cnf”.

— TR_KA-1: maka vienība izmanto atslēgas apliecinājumu personas identifikācijas datu izdošanas laikā, kā arī laikā, kad tiek izdoti ar ierīci saistīti kvalificēti vai nekvalificēti atribūtu elektroniskie apliecinājumi vai tādi atribūtu elektroniskie apliecinājumi, ko sniegusi par autentisku avotu atbildīga publiskā iestāde vai kas sniegti tās vārdā.

— TR_KA-1.1: maka vienība neizmanto atslēgas apliecinājumu, izdodot kvalificētus vai nekvalificētus atribūtu elektroniskos apliecinājumus, kas nav saistīti ar ierīci, vai atribūtu elektroniskos apliecinājumus, ko sniedz par autentisku avotu atbildīga publiskā iestāde vai kas tiek sniegti tās vārdā.

— TR_KA-2: maka nodrošinātājs maka vienībai sniedz dažādus atslēgu apliecinājumus *WSCD* un katrai tās atslēgu glabātuvei.

— TR_KA-2.1: maka nodrošinātājs paraksta vai apzīmogo atslēgas apliecinājumu pēc tam, kad maka nodrošinātājs ir pārliecinājies, ka atslēgas, kas apliecinātas atslēgas apliecinājumā, tiek glabātas *WSCD* vai atslēgu glabātuvē, kas aprakstīta atslēgas apliecinājumā.

— TR_KA-2.2: atslēgas apliecinājumā ir vismaz viena apliecināta publiskā atslēga. Atslēgu skaits akreditācijas izdevējam nosūtītajā atslēgas apliecinājumā nedrīkst pārsniegt maksimālo partijas apjomu, ko akreditācijas izdevējs norādījis savos akreditācijas izdevēja metadatos; sk. ETSI TS 119 472-3 ([3]), parametrs “credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size”.

— TR_KA-2.3: maka nodrošinātājs ne vairāk kā vienā atslēgas apliecinājumā iekļauj publisko atslēgu (kas atbilst privātai atslēgai, kura tiek glabāta *WSCD* vai maka vienības atslēgu glabātuvē).

— TR_KA-2.4: maka vienība izmanto atslēgas apliecinājumu ne vairāk kā vienā akreditācijas izdošanas vai atkārtotas izdošanas procesā.

— TR_KA-2.5: maka nodrošinātājs nodrošina, ka maka vienības rīcībā ir atslēgas apliecinājumi, kas vajadzīgi personas identifikācijas datu un atribūtu elektronisko apliecinājumu, kas saistīti ar ierīci, izdošanai.

([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, 2026. gada marts.

— TR_KA-3: ja tas nepieciešams izdošanas laikā, maka vienība akreditācijas devējam akreditācijas pieprasījuma laukā “proofs”, kā norādīts *OID4VCI*, iekļauj atslēgas apliecinājumu “jwt” vai “attestation” veidā.

— TR_KA_3.1: ja maka vienība satur atslēgas apliecinājumu elementā “jwt”, tā paraksta vai apzīmogo atslēgas apliecinājumu, izmantojot privāto atslēgu, kas atbilst “attested_keys” masīva publiskās atslēgas indeksam 0 objektā “key_attestation”.

— TR_KA-4: ja akreditācijas izdevējs izdod ar ierīci saistītu akreditāciju, tas sava izdevēja akreditācijas metadatu parametrā “proof_types_supported”, kā norādīts *OID4VCI* 12.2.4. iedaļā , norāda, ka tas atbalsta gan “jwt”, gan “attestation” apliecinājuma veidu tādiem atslēgas apliecinājumiem, kas ietver objektu “key_attestations_required”.

— TR_KA-4.1: ja akreditācijas izdevējs izdod ar ierīci nesaistītus akreditācijas datus, tas akreditācijas izdevēja metadatos izlaiž parametrus “proof_types_supported” un “cryptographic_binding_methods_supported”.

— TR_KA-5: ja akreditācijas izdevējs saņem atslēgas apliecinājumu “jwt” vai “attestation” apstiprinājuma veidā, tas verificē atslēgas apliecinājuma parakstu, kas norādīts publiskajā atslēgā parakstīšanas sertifikātā, kurš iekļauts parametrā “x5c” atslēgas apliecinājuma *JOSE* galvenē, un to, ka šis parakstīšanas sertifikāts ar uzticamības enkuru ir maka nodrošinātāju sarakstā, kas minēts Īstenošanas regulas (ES) 2024/2980 5. pantā, iespējams, izmantojot starpposma sertifikātus, kas iekļauti parametrā “x5c”.

— TR_KA-6: ja akreditācijas izdevējs saņem atslēgas apliecinājumu “jwt” apstiprinājuma veidā, tas verificē atslēgas “jwt” elementu pie indeksa 0 “attested_keys” masīvā “key_attestation” objektā, kas iekļauts “jwt” elementā.

— TR_KA-6.1: akreditācijas izdevējs pārbauda, vai elementa “jwt” laukā “nonce” ir iekļauts derīgs c_nonce no tā nonce_endpoint, kā norādīts *OID4VCI*.

— TR_KA-7: ja akreditācijas izdevējs saņem atslēgas apliecinājumu “attestation” apstiprinājuma veidā, tas pārbauda, vai objektā “key_attestation” ir derīgs c_nonce no tā nonce_endpoint.

— TR_KA-8: personas identifikācijas datu sniedzējs nodrošina, ka personas identifikācijas dati ir piesaistīti publiskai atslēgai, kas izriet no atslēgas apliecinājuma, kurā minēta *WSCD*.

c) Prasības attiecībā uz saturu

— C_WIA-1: Maka instances apliecinājumā iekļauj turpmāk norādīto informāciju.

— Apgalvojums “wallet_name”, kas minēts *OID4VCI* E papildinājumā, un tā vērtība ir maka risinājuma identifikators, kas atrodams Īstenošanas regulas (ES) 2024/2980 5. pantā minētajā maka nodrošinātāju sarakstā.

— Apgalvojums “wallet_version” ([4]), kas ir virkne, kuras vērtība ir maka risinājuma versija.

— Apgalvojums “wallet_solution_certification_information”, kas ir *JSON* objekts, kurš satur informāciju par atbilstības novērtēšanas struktūru, kura sertificējusi maka risinājumu, attiecīgā gadījumā sertifikācijas numuru un citu būtisku informāciju par sertifikāciju.

([4]) Šis apgalvojums ir definēts šajā Komisijas Īstenošanas regulā, jo tas nav daļa no *OID4VCI* specifikācijas.

— Apgalvojums “client_status”, kas ietver divus apakšlaukus:

— “status”: statusa saraksta atsauce, kā norādīts *OID4VCI* E papildinājumā, kas atspoguļo maka instances atsaukšanas statusu. Sīkāku informāciju sk. e) iedaļā turpmāk tekstā;

— “exp”: *NumericDate*, kā norādīts RFC 7519, kas nosaka laiku, līdz kuram maka nodrošinātājs glabās atsaukšanas statusu tā saraksta indeksā, uz kuru ir atsauce vienumā “status”.

— Apgalvojums “exp”, kas norādīts *OID4VCI* E papildinājumā.

— *PIEZĪME*. Apgalvojums “client_status.status” maka instances apliecinājumā ir maka instances atsaukšanas statuss, nevis paša apliecinājuma atsaukšanas statuss. Kā aprakstīts tālāk R_WIA-1, maka nodrošinātājs var nolemt katru maka instances apliecinājumu attiecināt uz konkrētu autorizācijas serveri, pamatojoties uz to, ka visos apliecinājumos, kas nosūtīti minētajam serverim, ierakstā “client_status.status” ir norādīta tā pati indeksa vērtība.

— *PIEZĪME*. Apgalvojumā “status” minēto vērtību “idx” var izmantot kā maka instances un maka vienības (pāra) unikālu identifikatoru.

— C_WIA-2: Maka instances apliecinājumā būtu jāiekļauj arī apgalvojums “wallet_link”, kas minēts *OID4VCI* E papildinājumā, un šā apgalvojuma vērtība ir *URI*, kur var iegūt papildu informāciju par maka risinājumu.

— C_WIA-3: Autorizācijas serveris neinterpretē parametru “exp” maka instances apliecinājuma augšējā līmenī kā maka instances atsaukšanas uzturēšanas perioda beigas.

— *PIEZĪME*. Parametrs “exp” maka instances apliecinājuma augšējā līmenī apzīmē brīdi, kad beidzas paša apliecinājuma termiņš.

— C_KA-1: Atslēgas apliecinājumā iekļauj tālāk izklāstīto informāciju.

— Apgalvojumi “key_storage” un “user_authentication”, kas minēti *OID4VCI* D papildinājumā.

— Atribūtu “key_storage” un “user_authentication” vērtība ir “iso_18045_high”, ja atslēgas apliecinājumā ir minēta *WSCD*.

— Apgalvojums “certification”, kas minēts *OID4VCI* D papildinājumā un satur *URL*, kurā var iegūt informāciju par *WSCD* vai atslēgu glabātuves saņemto sertifikāciju, tajā skaitā par shēmu, piemēram, vienoto kritēriju standartu vai *GlobalPlatform*, izvērtētajām prasībām, piemēram, piemērojamo aizsardzības profilu, un izvērtēšanas līmeni.

— Izmantojot šo informāciju, ir iespējams noteikt, vai atslēgu glabātuve ir *WSCD*.

— Apgalvojums “key_storage_status”, kurā ir divi apakšlauki:

— “status”: statusa saraksta atsauce, kā norādīts *OID4VCI* D.1. papildinājumā. Šī vērtība atspoguļo vai nu *WSCD* atsaukšanas statusu, vai atslēgu glabātuves veidu, ko izmanto apliecināto atslēgu glabāšanai, vai – “per-key-attestation” indeksa iespējas gadījumā – atsevišķas maka vienības *WSCD* vai atslēgu glabātuves atsaukšanas statusu. Pieejamās indeksa piešķiršanas iespējas sk. R_KA_1 turpmāk tekstā;

— “exp”: *NumericDate*, kā norādīts RFC 7519, kas nosaka laiku, līdz kuram maka nodrošinātājs glabās atsaukšanas statusu tā saraksta indeksā, uz kuru ir atsauce vienumā “status”.

— Apgalvojums “exp” , kas minēts *OID4VCI* D papildinājumā.

— *PIEZĪME* par vērtību “idx” atslēgas apliecinājuma apgalvojumā “key_storage_status.status”. Ja maka nodrošinātājs izmanto iespēju “type-shared index” (sk. R_KA_1 turpmāk tekstā), visiem atslēgas apliecinājumiem, kas attiecas uz tā paša veida *WSCD* vai atslēgu glabātuvi, ir tas pats statusa saraksta indekss. Tāpēc “idx” vērtība nav unikāla katrai maka vienībai. Turpretim, ja maka nodrošinātājs izmanto iespēju “per-key-attestation index”, vērtība “idx” ir unikāla maka vienībai (vai unikāla pārim katram akreditācijas izdevējam). Tomēr visos gadījumos akreditācijas izdevējs neizmanto atslēgas apliecinājumā norādīto “idx” vērtību kā maka vienības identifikatoru, bet tā vietā maka instances apliecinājumā izmanto vērtību “idx”.

— C_KA-2: Ja atslēgas apliecinājums tiek nosūtīts “attestation” apstiprinājuma veidā, tajā iekļauj arī derīgu c_nonce, kā norādīts *OID4VCI* F.3. papildinājumā.

— C_KA-3: Akreditācijas izdevējs neinterpretē parametru “exp” *WSCD* vai atslēgu glabātuves atslēgas apliecinājuma augšējā līmenī kā maka instances atsaukšanas uzturēšanas perioda beigas.

— *PIEZĪME*. Parametrs “exp” atslēgas apliecinājuma augšējā līmenī norāda, kad beidzas paša atslēgas apliecinājuma derīguma termiņš.

d) Aprites cikla prasības

— Šajā pielikumā ir precizēti tālāk norādītie akreditācijas izdevēja metadatu parametri.

— “preferred_client_status_period”: PĒC IZVĒLES. Vesels skaitlis, kas norāda maka instances apliecinājuma vēlamo atlikušo statusa uzturēšanas periodu, kas maka vienībai jānorāda izdošanas laikā (sekundēs). Atlikušo statusa uzturēšanas periodu apliecinājumā definē kā “client_status.exp” vērtību, no kuras atņemts apliecinājuma saņemšanas laiks.

— “preferred_key_storage_status_period”: PĒC IZVĒLES. Vesels skaitlis, kas norāda vēlamā atlikušā statusa uzturēšanas periodu atslēgas apliecinājumam, kurš maka vienībai jānorāda izdošanas laikā (sekundēs). Atlikušo statusa uzturēšanas periodu definē kā apliecinājuma vērtību “key_storage_status.exp”, no kuras atņemts apliecinājuma saņemšanas laiks.

— LC_WIA-1: Autorizācijas serveris var paziņot savas preferences attiecībā uz atlikušo statusa uzturēšanas periodu maka instances apliecinājumos, iekļaujot metadatu parametru “preferred_client_status_period” tā akreditācijas izdevēja metadatu galapunktā, kā norādīts *OID4VCI*. 12.2.2. iedaļā.

— LC_WIA-1.1: Šo lauku novieto akreditācijas izdevēja metadatu augšējā līmenī.

— LC_WIA_2: Autorizācijas serveris neinterpretē parametru “exp” maka instances apliecinājuma augšējā līmenī kā maka instances atsaukšanas uzturēšanas perioda beigas.

— LC_WIA_3: Ja maka nodrošinātājs paraksta vai apzīmogo maka instances apliecinājumu, tas saglabā attiecīgās maka instances atsaukšanas statusu līdz brīdim, kad ir beidzies minētajā maka instances apliecinājumā norādītais “wallet_instance_status.exp”.

— LC_KA-1: Ja ir vajadzīgs atslēgas apliecinājums, akreditācijas izdevējs var paziņot savas preferences attiecībā uz atlikušo statusa uzturēšanas periodu atslēgas apliecinājumos, iekļaujot iepriekš norādīto metadatu parametru “preferred_key_storage_status_period” savā akreditācijas izdevēja metadatu galapunktā, kā norādīts *OID4VCI* 12.2.2. iedaļā.

— LC_KA-1.1: Šo lauku iekļauj objektā “key_attestations_required”, kā norādīts dokumenta *OID4VCI* 12.2.4. iedaļā.

— LC_KA-2: Maka nodrošinātājs izvēlas tā izdoto atslēgu apliecinājumu tehniskā derīguma termiņu.

— LC_KA-3: Ja maka nodrošinātājs paraksta vai apzīmogo atslēgas apliecinājumu, tas saglabā attiecīgās *WSCD* vai atslēgu glabātuves atsaukšanas statusu, līdz minētajā atslēgas apliecinājumā ir pagājis "key_storage_status.exp".

— LC_GEN-1: Maka nodrošinātājs nodrošina, ka maka vienība vienmēr var sniegt maka vienības apliecinājumus un atslēgu apliecinājumus, kuru "client_status.exp" un "key_storage_status.exp" (attiecīgi) brīdī, kad šie apliecinājumi tiek sniegti autorizācijas serverim vai akreditācijas izdevējam, ir vismaz 31 dienu nākotnē.

— *PIEZĪME.* Tas garantē, ka personas identifikācijas datu sniedzēji var paļauties uz atsaukšanas ķēdi, neesot spiesti izdot personas identifikācijas datus ar īsu termiņu.

— LC_GEN-2: maka nodrošinātājs nodrošina, ka izdošanas laikā maka vienība saņem akreditācijas izdevēja metadatus.

  — LC_GEN_2.1: Ja šajos metadatos ir iekļauts lauks "preferred_key_storage_status_period", maka vienība nosūta atslēgas apliecinājumu ar ("key_storage_status.exp" − pašreizējais laiks) − "preferred_key_storage_status_period", kas ir pēc iespējas mazāks, bet ne negatīvs. Ja šāds atslēgas apliecinājums maka vienībai nav pieejams, tā no maka nodrošinātāja saņem jaunu atslēgas apliecinājumu, kas atbilst "key_storage_status.exp" − pašreizējais laiks ≥ "preferred_key_storage_status_period".

  — LC_GEN_2.2: Ja šajos metadatos ir iekļauts lauks "preferred_client_status_period", maka vienība nosūta maka instances apliecinājumu ar ("client_status.exp" − pašreizējais laiks) − "preferred_client_status_period", kas ir pēc iespējas mazāks, bet ne negatīvs. Ja maka vienībai šāds maka instances apliecinājums nav pieejams, tā no maka nodrošinātāja pieprasa jaunu maka instances apliecinājumu, kas atbilst "client_status.exp" − pašreizējais laiks ≥ "preferred_client_status_period".

— LC_GEN-3: Personas identifikācijas datu tehniskā derīguma termiņš beidzas gan pirms maka instances apliecinājuma "client_status.exp", gan pirms atslēgas apliecinājuma "key_storage_status.exp", kas izdošanas procesā nosūtīts personas identifikācijas datu sniedzējam.

— LC_GEN-4: tādu personas identifikācijas datu sniedzējs, kuru tehniskā derīguma termiņš pārsniedz 24 stundas, personas identifikācijas datu tehniskā derīguma termiņa laikā vismaz reizi 24 stundās pārbauda izdošanas laikā saņemtā maka instances apliecinājuma un atslēgas apliecinājuma atsaukšanas statusu. Ja kāds no tiem ir atsaukts, sniedzējs atsauc personas identifikācijas datus.

e) Atcelšanas prasības

— R_GEN-1: Maka nodrošinātājs izmanto marķiera statusa sarakstus (norādīti *IETF* marķiera statusa sarakstā) kā atsaukšanas mehānismu gan atslēgu apliecinājumiem, gan maka instances apliecinājumiem, kā norādīts attiecīgi *OID4VCI* D un E papildinājumā.

— *PIEZĪME.* Lai uzlabotu savu statusa sarakstu mērogojamību, maka nodrošinātājs var izmantot tālāk aprakstītās optimizācijas iespējas.

  — Statusa saraksta sadalīšana vairākās daļās, ja maka nodrošinātājiem ir ievērojams lietotāju skaits un tie ir izdevuši apliecinājumus. Pastāv daudzas datgrupes stratēģijas, piemēram, pamatojoties uz fiksētu lielumu vai laika periodu. Datgrupes stratēģiju izvēlas maka nodrošinātājs. Var ņemt vērā tādus apsvērumus kā lejupielādei paredzētā statusa saraksta lielums un lietotāja privātums.

  — Ir vairāki statusa saraksti.

  — Statusa saraksta saspiešana, lai samazinātu tā lielumu.

— R_WIA-1: Maka nodrošinātājs var piešķirt tādu pašu vērtību apgalvojumam “idx” apgalvojumā “client_status.status” visos maka instances apliecinājumos, ko konkrēta maka vienība iesniedz tam pašam autorizācijas serverim. To sauc par “per-issuer reuse” iespēju. Ja izmanto šo iespēju:

  — R_WIA-1.1: maka vienība saglabā informāciju par to, kādu indeksa vērtību tā ir izmantojusi katram autorizācijas serverim, ar kuru tā iepriekš ir mijiedarbojusies, un pieprasa maka instances apliecinājumu ar to pašu indeksa vērtību, kad tā atkal mijiedarbojas ar to pašu autorizācijas serveri.

  — R_WIA-1.2: ja maka nodrošinātājs saņem maka instances apliecinājuma pieprasījumu, kas satur konkrētu indeksa vērtību, tas pirms jauna maka instances apliecinājuma izdošanas ar minēto indeksa vērtību pārbauda vai pieprasītāja maka vienība iepriekš ir saņēmusi minēto indeksa vērtību.

  — R_WIA-1.3: maka vienība neizmanto to pašu indeksa vērtību mijiedarbībai ar dažādiem autorizācijas serveriem.

— *PIEZĪME.* Ja tiek izmantota iespēja “per-issuer reuse”, maka nodrošinātājs varēs noteikt, ar cik autorizācijas serveriem maka vienība ir mijiedarbojusies un cik bieži tā mijiedarbojas ar katru no tiem.

— R_WIA-2: Maka nodrošinātājs savā privātuma politikā dokumentē, vai tas maka instances atsaukšanai izmanto iespēju “per-issuer reuse”.

— R_WIA-3: Ja maka nodrošinātājs neizmanto “per-issuer reuse” iespēju, maka nodrošinātājs piešķir jaunu, nesasaistāmu indeksa vērtību katram maka instances apliecinājumam, ko tas izdod.

— R_WIA-4: Ja maka vienība ir jāatsauc, maka nodrošinātājs atsauc indeksa vērtības apgalvojumā “client_status.status” visos maka instances apliecinājumos, kas saistīti ar minēto maka vienību.

— R_WIA-5: maka nodrošinātājs, nosakot maka instances apliecinājuma statusa saraksta lielumu, ņem vērā tā ieviešanas mērogu un pamatā esošo arhitektūru, nodrošinot, ka šie elementi ir pietiekami lieli, lai novērstu korelāciju un aizsargātu lietotāju privātumu. Ja iespējams, statusa saraksts attiecas vismaz uz 10 000 apliecinājumiem.

— R_KA_1: Maka nodrošinātājs atslēgas apliecinājumā apgalvojumam “key_storage_status.status” izvēlas vienu no šādām indeksa piešķiršanas iespējām:

  — 1. iespēja, ko sauc par “type-shared index” un kurā visos atslēgu apliecinājumos, kas apliecina tajā pašā *WSCD* vai atslēgu glabātuvē glabātas atslēgas, ir tā pati indeksa vērtība “key_storage_status.status”.

  — 2. iespēja, ko sauc par “per-key-attestion index”, kurā atslēgas apliecinājums, kas apliecina atsevišķā *WSCD* vai atslēgu glabātuvē glabātās atslēgas, satur (pāra) unikālu indeksa vērtību “key_storage_status.status”.

— *PIEZĪME.* Ja maka nodrošinātājs izmanto 1. iespēju, ar vienu atsaukšanas darbību visi skartā veida atslēgas apliecinājumi visās maka vienībās tiek padarīti par nederīgiem. Turklāt, tā kā visiem tā paša veida *WSCD* vai atslēgu glabātuves koplieto vienu statusa saraksta indeksu, ierakstu skaits atslēgas apliecinājuma statusa sarakstā atspoguļo *WSCD* vai atslēgu glabātuvju veidu skaitu, ko atbalsta maka nodrošinātājs, nevis izvietoto maka vienību skaitu. Tāpēc ar privātumu saistīti apsvērumi, kas pamato maka instances statusa sarakstu minimālo statusa saraksta lielumu, neattiecas uz atslēgas apliecinājuma statusa sarakstiem saskaņā ar 1. iespēju, ja ir pietiekami daudz maka vienību, kas izmanto tā paša veida *WSCD* vai atslēgu glabātuvi.

— *PIEZĪME.* Ja maka nodrošinātājs izmanto 2. iespēju, katrs indekss atbilst konkrētās *WSCD* vai atslēgu glabātuves atsaukšanas statusam, kas apliecināts minētajā atslēgas apliecinājumā.

— *PIEZĪME.* Ja maka nodrošinātājs izmanto 2. iespēju, pēc lietotāja pieprasījuma var atsaukt arī konkrētu *WSCD* vai atslēgu glabātuvi.

— R_KA-2: Ja maka nodrošinātājs izmanto 2. iespēju, maka nodrošinātājs pēc izvēles var izmantot R_WIA-1 aprakstīto iespēju "per-issuer reuse". Ja maka nodrošinātājs izmanto šo iespēju, prasības R_WIA-1 - R_WIA-3 piemēro *mutatis mutandis*.

— R_KA-3: ja maka nodrošinātājs izmanto 2. iespēju, maka nodrošinātājs, nosakot atslēgas apliecinājuma statusa sarakstu lielumu, ņem vērā tā ieviešanas mērogu un pamatā esošo arhitektūru, nodrošinot, ka šie elementi ir pietiekami lieli, lai novērstu korelāciju un aizsargātu lietotāju privātumu. Ja iespējams, statusa saraksts attiecas vismaz uz 10 000 atslēgu apliecinājumiem.

— R_KA-4: Ja maka nodrošinātājs izmanto 1. iespēju (tipa koplietots indekss), maka nodrošinātājs ierakstu "key_storage_status.status" atsauc tikai tad, ja *WSCD* vai atslēgu glabātuves veidam ir drošības ievainojamība.

f) Prasības attiecībā uz paraksta algoritmiem

— SA-1: maka instances apliecinājumi, atslēgu apliecinājumu, saistīto valdījuma apliecinājumu un marķieru statusu sarakstu parakstīšanai izmanto vienu no šādiem algoritmiem:

— ES256 (*ECDSA* ar SHA-256 un P-256);

— ES384 (*ECDSA* ar SHA-384 un P-384);

— ES512 (*ECDSA* ar SHA-512 un P-521);

— SA-2: Maka nodrošinātājs izvēlas, kuru no SA-1 minētajiem algoritmiem tas izmantos.

— SA-3: Autorizācijas serveris vai akreditācijas izdevējs (kā norādīts *OID4VCI*) atbalsta visus SA-1minētos algoritmus."

IV PIELIKUMS

"II PIELIKUMS

8. pantā minēto standartu saraksts

Piemēro ETSI TS 119 472-1 V1.2.1 (2026-02) 2.–6. punktā noteiktās tehniskās specifikācijas. Tās lasa, piemērojot tālāk norādītos pielāgojumus.

1) 2.1. Normatīvās atsauces

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): "Elektroniskie paraksti un infrastruktūras (*ESI*), sertifikātu profili; 1. daļa. Pārskats un kopīgas datu struktūras".

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): "Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*); sertifikātu profili; 6. daļa. Sertifikātu profilu prasības *PID*, makam, *EAA*, *QEAA* un *PSBEAA* sniedzējiem".

— [25] *IETF* marķieru statusu saraksts (*TSL*), draft-ietf-oauth-status-list-20: "Marķieru statusa saraksts", 2026. gada 20. aprīlis.

2) 4.2.11.1. Vispārīgas prasības

— EAA-4.2.11.1-06: Ja personas identifikācijas datiem, kvalificētiem atribūtu elektroniskajiem apliecinājumiem vai atribūtu elektroniskajiem apliecinājumiem, ko sniegusi par autentisku avotu atbildīga publiskā iestāde vai kas sniegti tās vārdā, izmanto statusa elementu, tajā norāda tikai to, vai apliecinājums ir vai nav atsaukts, un tas neatbalsta nekādas citas statusa vērtības (piemēram, apturēšanu).

— EAA-4.2.11.1-06.1: ja apliecinājums tiek atsaukts, to atsauc neatgriezeniski.

3) 4.2.13. Īslaicīgi *EAA*

— EAA-4.2.13-03: Ja tiek izdoti īslaicīgi elektroniski atribūtu apliecinājumi, kuru derīguma termiņš ir 24 stundas vai mazāks, atsaukšana nav nepieciešama.

4) 4.6.3. Prasības attiecībā uz ES *EAA*, ko izdevusi par autentisku avotu atbildīga publiska struktūra vai kas izdots tās vārdā (*PuB-EAA*)

— PuB-EAA-4.6.2-03: nav spēkā.

— Pub-EAA-4.6.2-04: nav spēkā.

— PuB-EAA-4.6.3-03: *PuB-EAA* digitālajam parakstam būtu jāsatur kvalificēts sertifikāts, kas atbalsta *PuB-EAA* digitālo parakstu.

— PuB-EAA-4.6.3-04: Kvalificētais sertifikāts, kas atbalsta *PuB-EAA* digitālo parakstu, atbilst ETSI TS 119 412-6 v1.1.1 8. punkta prasībām un ietver *QcType QcStatement*, kā noteikts ETSI EN 319 412-5 v2.5.1, ar vērtību "id-etsi-qct-eidaspsbeaa", kas definēta šādi:

ID-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER::= {id-etsi-eidas2-qct-extensions 3} — 45.f panta 1. punkta b) apakšpunktā minētais sertifikāts, kas atbalsta Regulas (ES) Nr. 910/2014 3. panta 46. punktā minētās publiskās iestādes kvalificēto elektronisko parakstu vai kvalificēto elektronisko zīmogu.

5) 5.2.10.1. Vispārīgas prasības

— EAA-5.2.10.1-04: nav spēkā.

— EAA-5.2.10.1-05: nav spēkā.

— EAA-5.2.10.1-06: statusa elements var ietvert status_list elementu, kā norādīts *IETF* draft-ietf-oauth-status-list-20 6.2. punktā [25].

— EAA-5.2.10.1-07: nav spēkā.

— EAA-5.2.10.1-08: nav spēkā.

— EAA-5.2.10.1-09: nav spēkā.

— EAA-5.2.10.1-10: nav spēkā.

— EAA-5.2.10.1-11: nav spēkā.

— EAA-5.2.10.1-12: nav spēkā.

6) 6.2.10.1. Vispārīgas prasības

— EAA-6.2.10.1-01: ja atribūtu elektroniskajam apliecinājumam, kas atbilst *ISO/IEC mdoc*, izmanto apliecinājuma statusa saraksta mehānismu, kā noteikts EAA-6.2.10.1-02.2, vai apliecinājuma atsaukšanas saraksta mehānismu, kā noteikts EAA-6.2.10.1-02.3, tā mobilais drošības objekts (*MSO*) ietver statusa struktūru, kā noteikts EAA-6.2.10.1-17, kas satur *MSO* atsaukšanas informāciju.

— EAA-6.2.10.1-01.1: īstenojot identifikatoru saraksta mehānismu, statusa elements ietver elementu identifier_list, kā noteikts EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: īstenojot statusa saraksta mehānismu, statusa elements ietver elementu status_list, kā noteikts EAA-6.2.10.1-13.

— *PIEZĪME.*

  — Statusa struktūrā ir atsauce uz *MSO* atsaukšanas sarakstu.

  — *MSO* atsaukšanas saraksts ir *COSE_Sign1* struktūra, kas norāda, vai konkrēts *MSO* ir atsaukts.

  — Statusa struktūra satur visu informāciju, kas maka atkarīgajai pusei vajadzīga, lai noteiktu, vai *MSO* atsaukšanas saraksts ir autentisks.

— EAA-6.2.10.1-02: personas identifikācijas datu sniedzējs, kvalificētu atribūtu elektronisko apliecinājumu sniedzējs vai par autentisku avotu atbildīgas publiskas iestādes vai tās vārdā sniegtu atribūtu elektronisko apliecinājumu sniedzējs personas identifikācijas datu, atribūtu kvalificēto elektronisko apliecinājumu vai par autentisku avotu atbildīgas publiskas iestādes vai tās vārdā sniegtu atribūtu elektronisko apliecinājumu atsaukšanai izmanto vienu no šādām metodēm:

— EAA-6.2.10.1-02.1: ja tie izdod īslaicīgus atribūtu elektroniskos apliecinājumus, kuru derīguma termiņš ir 24 stundas vai īsāks, atsaukšana nav nepieciešama.

— EAA-6.2.10.1-02.2: izmanto apliecinājuma statusa saraksta mehānismu, lai atsaukšanas informāciju kodētu kā statusa sarakstu.

— EAA-6.2.10.1-02.2.1: statusu saraksta mehānisms atsauc *MSO*, pamatojoties uz to, vai izdevēja noteiktās bita pozīcijas bits *MSO* ir iestatīts kā patiess statusa sarakstā.

— EAA-6.2.10.1-02.2.2: statusu saraksta mehānisms ir norādīts marķieru statusu saraksta (draft-ietf-oauth-status-list-20) specifikācijā.

— EAA-6.2.10.1-02.3: izmanto apliecinājuma atsaukšanas saraksta mehānismu, lai atsaukšanas informāciju kodētu kā identifikatoru sarakstu.

— EAA-6.2.10.1-02.3.1: identifikatoru saraksta mehānisms atsauc *MSO*, pamatojoties uz to, vai identifikatoru sarakstā ir iekļauts izdevēja noteikts identifikators, kas norādīts *MSO*.

— EAA-6.2.10.1-02.3.2: EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 un EAA-6.2.10.1-11 ir norādīts identifikatoru saraksta mehānisms, pamatojoties uz prasībām, kas noteiktas marķieru statusu saraksta specifikācijā, kas ietver statusu saraksta un identifikatoru saraksta mehānisma kopīgos elementus.

— EAA-6.2.10.1-03: ja statusa elementu izmanto personas identifikācijas datiem, kvalificētiem atribūtu elektroniskajiem apliecinājumiem vai atribūtu elektroniskajiem apliecinājumiem, ko sniegusi par autentisku avotu atbildīga publiskā iestāde vai kas sniegti tās vārdā, izmanto tikai statusu "atsaukts".

— EAA-6.2.10.1-03.1: statusu saraksta gadījumā tas nozīmē, ka tiek izmantotas tikai vērtības "valid" un "invalid", kā norādīts marķieru statusu saraksta specifikācijā.

— EAA-6.2.10.1-03.2: identifikatoru sarakstā iekļauj tikai atsauktos *MSO*, nevis uz laiku apturētos *MSO*.

— EAA-6.2.10.1-04: ja *MSO* tiek atsaukts, *MSO* tiek neatgriezeniski atsaukts.

— EAA-6.2.10.1-05: *MSO* atsaukšanas saraksta verifikācija maka atkarīgajai pusei nav obligāta, un attiecīgā gadījumā verifikācija atbilst verifikācijas prasībām, kas norādītas marķieru statusu saraksta specifikācijā un statusa struktūras specifikācijā, kas noteiktas EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: ja maka atkarīgajai pusei jāspēj verificēt personas identifikācijas datu vai atribūtu elektronisko apliecinājumu atsaukšanas statusu, tā atbalsta gan apliecinājuma statusa saraksta mehānismu, gan apliecinājuma atsaukšanas saraksta mehānismu, kas noteikti EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: *identifier_list un status_list*, kas iekļauti *MSO*, var būt ietverts sertifikāta elements.

— EAA-6.2.10.1-06.1: ja ir sertifikāta elements, tajā iekļauj sertifikātu, kas satur publisko atslēgu, ar kuru parakstīts vai apzīmogots augstākā līmeņa sertifikāts elementā x5chain *MSO* atsaukšanas saraksta struktūrā.

— EAA-6.2.10.1-06.1.1: maka atkarīgās puses instance izmanto minēto sertifikātu kā uzticamības enkuru x5chain elementa verifikācijai *MSO* atsaukšanas saraksta struktūrā.

— EAA-6.2.10.1-06.2: ja sertifikāta elementa nav, *MSO* atsaukšanas saraksta struktūras elementa x5chain augstākā līmeņa sertifikātu paraksta vai apzīmogo ar sertifikātu, ko izmanto MSO elementā x5chain.

— EAA-6.2.10.1-06.2.1: maka atkarīgās puses instance izmanto minēto sertifikātu kā uzticamības enkuru x5chain elementa verifikācijai *MSO* atsaukšanas saraksta struktūrā.

— EAA-6.2.10.1-07: *MSO* atsaukšanas sarakstu īsteno saskaņā ar marķieru statusu saraksta specifikāciju kā statusu saraksta marķieri *CWT* formātā.

— EAA-6.2.10.1-08: attiecībā uz *MSO* atsaukšanas sarakstu identifikatoru sarakstam un statusa saraksta mehānismam piemēro šādas prasības:

  — jāiekļauj apgalvojums *exp*,

  — jāiekļauj apgalvojums *ttl*,

  — var būt apgalvojums *aggregation_uri*, kas iekļauts *IdentifierList* vai *StatusList*, un personas identifikācijas datu nodrošinātājs, atribūtu kvalificēto elektronisko apliecinājumu nodrošinātājs vai par autentisku

avotu atbildīgas publiskās iestādes vai tās vārdā sniegtu atribūtu elektronisko apliecinājumu nodrošinātājs var izmantot apgalvojumu *aggregation_uri*, lai informētu par atbalstu agregēšanas mehānismam, kā norādīts marķieru statusu saraksta specifikācijā,

— *CWT* ir COSE_Sign1 objekts, kas paraksta aprēķināšanai izmanto vienu no šādiem paraksta algoritmiem:

a) "ES256" (*ECDSA* ar līkni NIST P-256 un SHA-256);

b) "ES384" (*ECDSA* ar līkni NIST P-384 un SHA-384);

c) "ES512" (*ECDSA* ar līkni NIST P-521 un SHA-512);

d) "ESB256" (*ECDSA* ar līkni brainpoolP256r1 un SHA-256);

e) "ESB384" (*ECDSA* ar līkni brainpoolP384r1 un SHA-384);

f) "ESB512" (*ECDSA* ar līkni brainpoolP512r1 un SHA-512);

— *CWT* ietver x5chain aizsargātajā galvenē, kurā ir sertifikāts vai sertifikātu ķēde, lai verificētu *MSO* atsaukšanas saraksta parakstu.

— Marķieru statusu saraksta specifikācijā norādītā objekta identifikatora paplašinātās atslēgas lietojumu var izmantot statusu saraksta un identifikatora saraksta parakstīšanas sertifikāta vajadzībām, un maka atkarīgās puses instances var atbalstīt marķieru statusu saraksta specifikācijā norādīto objekta identifikatoru paplašinātās atslēgas lietojumu, un attiecībā uz objekta identifikatoru, atribūtu kvalificēto elektronisko apliecinājumu sniedzējs vai publiskās iestādes vai tās vārdā sniegtu atribūtu elektronisko apliecinājumu sniedzējs nedrīkst padarīt paplašinātās atslēgas lietojuma lauku kritiski svarīgu, izmantojot marķieru statusu saraksta specifikācijā norādīto paplašinātās atslēgas lietojuma *OID*.

— EAA-6.2.10.1-09: novirzoties no marķieru statusu saraksta specifikācijas prasībām, identifikatoru saraksta mehānismam piemēro šādas prasības:

— apgalvojuma "type" vērtība ir "application/identifierlist+cwt";

— apgalvojumu *StatusList* neiekļauj *CWT* apgalvojumu kopumā;

— *IdentifierList* struktūru, kas noteikta EAA-6.2.10.1-11, nenorāda kā apgalvojumu *CWT* apgalvojumu kopumā, izmantojot atslēgu 65530.

— EAA-6.2.10.1-10: *IdentifierList* struktūra ir *CBOR* struktūra ar šādu *CDDL*:

```
IdentifierList = {

    'identifiers': { * Identifier => IdentifierInfo },

    ? 'aggregation_uri': Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: ja ir identifikators *IdentifierList*, atsauc *MSO*, kas satur identifikatoru statusa elementā.

— EAA-6.2.10.1-10.2: apgalvojums *Aggregation_uri* ir noteikts marķieru statusu saraksta specifikācijas 9.2. iedaļā.

— EAA-6.2.10.1-10.3: identifikatoru saraksta satura tips ir "application/identifierlist+cwt", kas noteikts marķieru statusu saraksta specifikācijas 8.2. iedaļā izklāstītajās prasībās.

— EAA-6.2.10.1-11: identifikatoru saraksta elementam *MSO* piemēro tālāk izklāstītās prasības (sk. EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: elements *Identifier_list* ir *CBOR* struktūra ar šādu *CDDL*:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: lai novērstu to, ka identifikatoru izmanto kā korelāciju starp sniegtajiem datiem, tas ir unikāls katram *MSO*.

— EAA-6.2.10.1-12: statusa sarakstam piemēro šādas prasības:

  — EAA-6.2.10.1-12.1: bitu elementu *StatusList* struktūrā iestata uz 1.

— EAA-6.2.10.1-13: *MSO* elementam *status_list* piemēro šādas prasības (sk. EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: elements *status_list* atbilst *StatusListInfo* struktūras prasībām, kas norādītas marķieru statusu saraksta specifikācijā, un pievieno neobligāto sertifikāta elementu, kas noteikts EAA-6.2.10.1-06.

  — EAA-6.2.10.1-13.2: lai novērstu to, ka statusa indekss ir korelācija starp sniegtajiem datiem, statusa indeksa un *URI* kombinācija ir unikāla katram *MSO*.

— EAA-6.2.10.1-14: maka nodrošinātājs izmanto otro (EAA-6.2.10.1-02.2) vai trešo (EAA-6.2.10.1-02.3) metodi, kas norādītas EAA-6.2.10.1-02, lai atsauktu maka vienības apliecinājumu (*WIA*) un atslēgas apliecinājumu (*KA*).

— EAA-6.2.10.1-15: maka nodrošinātājs savā maka risinājumā ievieš apliecinājuma atsaukšanas mehānismus, kas norādīti EAA-6.2.10.1-02.

— EAA-6.2.10.1-16: personas identifikācijas datu sniedzējs un atribūtu elektronisko apliecinājumu sniedzējs atbalsta gan apliecinājuma statusa saraksta mehānismu, gan apliecinājuma atsaukšanas saraksta mehānismu, kas norādīti EAA-6.2.10.1-02, lai verificētu maka vienības apliecinājuma (*WIA*) un atslēgas apliecinājuma (*KA*) atsaukšanas statusu.

— EAA-6.2.10.1-17: statusa struktūra *MSO* ir *CBOR* struktūra ar šādu *CDDL*:

Status = {

? 'identifier_list' : IdentifierListInfo,

? 'status_list' : StatusListInfo,

* tstr => RFU

}”

V PIELIKUMS

"III PIELIKUMS

10. pantā minētās tehniskās specifikācijas

— Tehniskās specifikācijas:

  — ETSI TS 119 472-3 V1.1.1 (2026-03) 4.2.5. punkts."

VI PIELIKUMS

Īstenošanas regulas (ES) 2024/2979 IV pielikumu groza šādi:

1) pielikuma 1. punktu aizstāj ar šādu:

"1. Obligātais paraksta vai zīmoga formāts:

a) PAdES (PDF uzlabots elektroniskais paraksts), kā norādīts ETSI EN 319 142-1 V1.2.1 (2024-01), elektroniskie paraksti un infrastruktūras (*ESI*), PAdES elektroniskie paraksti, 1. daļa. Pamatelementi un PAdES pamata paraksti.";

2) pielikuma 3. punktu aizstāj ar šādu:

"3. Lietojumprogrammas saskarne:
ETSI TS 119 432 v1.3.1 (2026-03) 6.4.3., A.6., A.7. un A.8. punkts."

VII PIELIKUMS

"VI PIELIKUMS

Krāsains ES digitālās identitātes maka uzticamības marķējums



"

VIII PIELIKUMS

"VII PIELIKUMS

Melnbalts ES digitālās identitātes maka uzticamības marķējums



"

IX PIELIKUMS

"VIII PIELIKUMS

ES digitālās identitātes maka uzticamības marķējuma dati

Dati	Apraksts	Kodēšana	Statuss
TrustMarkResourceURL	ES digitālās identitātes maka uzticamības marķējuma grafikas un lietotāja informācijas resursu *URL* maka lietotāja saskarnē.	*URL*	obligāti
ListOfCertifiedWalletsURL	Komisijas Īstenošanas regulā (ES) 2025/849 ([1]) noteiktā ES sertificēto maka risinājumu publiskā saraksta *URL*.	*URL*	obligāti
ListOfCertifiedWalletsQRCode	*QR* kods, kas satur *ListOfCertifiedWalletsURL* informāciju	ISO-8859-1 Baita režīma *QR* kods	neobligāti
WalletSolutionInfoPageURL	*URL* uz sertificētā maka risinājuma informācijas lapu sertificētā maka risinājuma lapas sarakstā no *ListOfCertifiedWalletsURL URL*, kas pievienots ar"?" un maka risinājuma *WalletSolutionID* identifikatoru.	*URL*	obligāti
WalletSolutionInfoPageQRCode	*QR* kods, kas satur *WalletSolutionInfoPageURL* informāciju	ISO-8859-1 Baita režīma *QR* kods	neobligāti
WalletVerifierToolURL*	*URL*, kas ved uz maka verifikācijas rīka */.well-known/openid-credential-issuer* galapunktu, ko izmanto apliecinājuma sniedzēja metadatu izgūšanai.	*URL*	neobligāti

([1]) Komisijas Īstenošanas regula (ES) 2025/849 (2025. gada 6. maijs), kas nosaka noteikumus par Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 piemērošanu informācijas iesniegšanā Komisijai un Sadarbības grupai sertificēto Eiropas digitālās identitātes maku sarakstam (OV L, 2025/849, 7.5.2025., ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj)."

X PIELIKUMS

Īstenošanas regulas (ES) 2024/2980 II pielikumu groza šādi:

1) Regulas II pielikuma 1. iedaļas 1. punkta i) apakšpunktu aizstāj ar šādu:

"i) viens vai vairāki standartam ETSI EN 319 412-2 V2.4.1 (2025-06) vai standartam ETSI EN 319 412-3 V1.3.1 (2023-09) atbilstoši sertifikāti, kurus var izmantot, lai verificētu reģistrētāja izveidoto parakstu vai zīmogu reģistra datos, un kuriem sertificētajos identitātes datos ir iekļauts reģistrētāja nosaukums un attiecīgā gadījumā – reģistrētāja reģistrācijas numurs, kā noteikts attiecīgi c) un d) apakšpunktā;".

2) Regulas II pielikuma 2. iedaļas 1. punkta h) apakšpunktu aizstāj ar šādu:

"h) viens vai vairāki standartam ETSI EN 319 412-2 V2.4.1 (2025-06) vai standartam ETSI EN 319 412-3 V1.3.1 (2023-09) atbilstoši sertifikāti, kurus var izmantot, lai autentificētu un validētu maka vienības apliecinājumus, ko izdevis maka nodrošinātājs, un kuru sertificētajos identitātes datos ir iekļauts maka nodrošinātāja nosaukums un attiecīgā gadījumā – maka nodrošinātāja reģistrācijas numurs, kā noteikts attiecīgi a) un b) apakšpunktā;";

3) Regulas II pielikuma 3. iedaļas 1. punkta h) apakšpunktu aizstāj ar šādu:

"h) viens vai vairāki standartam ETSI EN 319 412-2 V2.4.1 (2025-06) vai standartam ETSI EN 319 412-3 V1.3.1 (2023-09) atbilstoši sertifikāti, kurus var izmantot, lai verificētu personas identifikācijas datu sniedzēja izveidoto parakstu vai zīmogu, kas piemērots tā sniegtajiem personas identifikācijas datiem, un kuriem sertificētajos identitātes datos ir iekļauts personas identifikācijas datu sniedzēja nosaukums un attiecīgā gadījumā – reģistrācijas numurs, kā noteikts attiecīgi a) un b) apakšpunktā.';

4) Regulas II pielikuma 4. iedaļas 1. punkta g) apakšpunktu aizstāj ar šādu:

"g) viens vai vairāki standartam ETSI EN 319 412-2 V2.4.1 (2025-06) vai standartam ETSI EN 319 412-3 V1.3.1 (2023-09) atbilstoši sertifikāti, ko var izmantot, lai verificētu maka atkarīgās puses piekļuves sertifikātu nodrošinātāja radīto parakstu vai zīmogu uz piekļuves sertifikāta, ko tas sniedz maka atkarīgajām pusēm, attiecīgā gadījumā norādot informāciju, kas nepieciešama, lai atšķirtu maka atkarīgās puses piekļuves sertifikātus no citiem sertifikātiem.".

5) Regulas II pielikumam pievieno šādu 5. iedaļu:

"5. Informācijas paziņojumi par maka atkarīgās puses reģistrācijas sertifikātu nodrošinātājiem

1. Dalībvalstis sniedz Komisijai šādu informāciju par maka atkarīgās puses reģistrācijas sertifikātu nodrošinātājiem:

a) maka atkarīgās puses reģistrācijas sertifikātu nodrošinātāja nosaukums;

b) attiecīgā gadījumā – maka atkarīgās puses reģistrācijas sertifikātu nodrošinātāja reģistrācijas numurs;

c) dalībvalsts, kurā reģistrēts maka atkarīgās puses reģistrācijas sertifikātu nodrošinātājs;

d) maka atkarīgās puses reģistrācijas sertifikātu nodrošinātāja e-pasta adrese un kontakttālruņa numurs jautājumiem, kas saistīti ar reģistrācijas sertifikātiem, kurus tas sniedz maka atkarīgajām pusēm;

e) attiecīgā gadījumā – maka atkarīgās puses reģistrācijas sertifikātu nodrošinātāja tīmekļvietnes *URL*, kurā ir papildu informācija par nodrošinātāju un reģistrācijas sertifikātiem, ko tas sniedz maka atkarīgajām pusēm;

f) tīmekļvietnes *URL*, kurā ir procedūras un noteikumi, kas attiecas uz to reģistrācijas sertifikātu izsniegšanu un izmantošanu, kurus tas sniedz maka atkarīgajām pusēm;

g) viens vai vairāki standartam ETSI EN 319 412-2 V2.4.1 (2025-06) vai standartam ETSI EN 319 412-3 V1.3.1 (2023-09) atbilstoši sertifikāti, ko var izmantot, lai verificētu maka atkarīgās puses reģistrācijas sertifikātu nodrošinātāja radīto parakstu vai zīmogu uz reģistrācijas sertifikātiem, ko tas sniedz maka atkarīgajām pusēm, attiecīgā gadījumā norādot informāciju, kas nepieciešama, lai atšķirtu maka atkarīgās puses reģistrācijas sertifikātus no citiem sertifikātiem.

2. Informāciju, kas prasīta 1. punktā sniedz par katru maka atkarīgās puses piekļuves sertifikātu nodrošinātāju."

XI PIELIKUMS

"I PIELIKUMS

4. pantā minētie protokoli un saskarnes

Tehnisko specifikāciju ETSI TS 119 472-3 V1.1.1 (2026-03) piemēro ar šādiem pielāgojumiem:

1) 4.1. Vispārīgas prasības

— GEN-REQ-4.1-05: nav spēkā.

— PIEZĪME: nav spēkā.

2) 4.2.3 *PID*/*EAA* nodrošinātāja reģistrācijas apliecību nodrošināšana *EUDI* makam

— ISS-MDATA-REG_CERT-4.2.3-04: Viens no *issuer_info* masīva parametra elementiem ietver *PID*/*EAA* nodrošinātāja reģistrācijas apliecību.

— ISS-MDATA-REG_CERT-4.2.3-07: nav spēkā.

— ISS-MDATA-REG_CERT-4.2.3-08: nav spēkā.

— ISS-MDATA-REG_CERT-4.2.3-09: nav spēkā.

— ISS-MDATA-REG_CERT-4.2.3-10: nav spēkā.

— ISS-MDATA-REG_CERT-4.2.3-11: nav spēkā.

— ISS-MDATA-REG_CERT-4.2.3-12: nav spēkā.

— ISS-MDATA-REG_CERT-4.2.3-13: nav spēkā.

3) 4.2.4.2. *ARF* iepriekš noteikta *PID*/*EAA* atkalizmantošanas politika

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Ja elementam "id" ir vērtība "arf_annex_ii" un masīvs, kas kartēts atbilstoši birkai "details", ietver vērtību "once_only" vai vērtību "per-relying-party", tad *JSON* objekts, kas ietver šo masīvu, kurš kartēts atbilstoši birkai "details", ietver arī *JSON* numuru, kas kartēts atbilstoši birkai "reissue_trigger_unused".

4) A pielikumu nepiemēro."

XII PIELIKUMS

"II PIELIKUMS

5. pantā minētās tehniskās specifikācijas

Piemēro ISO/IEC 18013-7:2025 C pielikumā noteikto tehnisko specifikāciju.

Tehniskās specifikācijas ETSI TS 119 472-2 V1.2.1 (2026-03) 4.1., 4.2., 5. un 6. punktā piemēro ar šādiem pielāgojumiem, ieskaitot jauna 4.3. punkta iekļaušanu:

1) 1 Darbības joma

— Šajā dokumentā ir noteikti 2 (divi) protokolu profili, kas ļauj atkarīgajām pusēm (turpmāk *RP*) pieprasīt *EAAP* vai personas identifikācijas datus (turpmāk *PID*) *EUDI* makam un *EUDI* makam nosūtīt pieprasītos *EAAP*/*PID RP*. Katrs profils atbalsta divus pārraides mehānismus, proti, ar *API* starpniecību un bez *API* starpniecības, kā norādīts turpmāk tekstā.

a) Profila pamatā ir:

— ISO/IEC 18013-5 [10] tikai attiecībā uz pārraides mehānismu bez *API* starpniecības un

— ISO/IEC 18013-7 [16] C pielikums attiecībā uz pārraides mehānismu ar *API* starpniecību.

Šo profilu sauc par *ISO*/*IEC-mdoc* profilu, un tas ir definēts šā dokumenta 5. punktā.

b) Profila pamatā ir:

OpenID4VC-HAIP [11] gan pārraides mehānismiem ar *API* starpniecību, gan bez *API* starpniecības, kā norādīts turpmāk tekstā:

— [11] 5., 5.1., 5.3., 7. un 8. iedaļa attiecībā uz pārraidi, izmantojot *Redirects* vai pārraides mehānismu bez *API* starpniecības, un

— [11] 5., 5.2., 5.3., 7. un 8. iedaļa attiecībā uz pārraides mehānismu ar *API* starpniecību.

Šo profilu sauc par OpenID4VC-HAIP profilu, un tas ir definēts šā dokumenta 6. punktā.

2) 2.1. Normatīvās atsauces

— [15] ISO 639: "Valodas kods".

— [16] ISO/IEC 18013-7:2025 "Personas identifikācija – ISO – prasībām atbilstoša vadītāja apliecība – 7. daļa: Mobilās vadītāja apliecības (MVA) papildfunkcijas".

3) 4.1. *EAAP* īstenošana, pamatojoties uz *SD-JWT VC*

— EAAP-SD-JWT VC-04: nav spēkā.

4) 4.2. *EAAP* īstenošana, pamatojoties uz *ISO*/*IEC-mdoc*

— EAAP-ISO/IEC-mdoc-01: nav spēkā.

— Note2: nav spēkā.

— EAAP-ISO/IEC-mdoc-02: nav spēkā.

5) 4.3. *EAAP* īstenošana ar *API* starpniecību

— EAAP-API-GEN-01: *EUDI* maks atbalsta starpniecības *API*, kas atbalsta abus protokolus, kuri noteikti [11] 5.2. punktā un [16] C pielikumā.

— *PIEZĪME*. Ja ierīce, kurā ir instalēts *EUDI* maks, neatbalsta abus protokolus, šo prasību nevar izpildīt un tā izraisa neatbilstību sakarā ar to, ka pamatā esošās operētājsistēmas un pārlūkprogrammas neīsteno nepieciešamās sadarbspējas funkcijas.

— EAAP-API-GEN-02: *EUDI* maks atbalsta starpniecības *API* vismaz attiecībā uz *PID* un *EAA* veidiem, kas reģistrēti shēmu katalogā, kā definēts Īstenošanas regulā (ES) 2025/1569, un vismaz attiecībā uz visiem formātiem, kas definēti Īstenošanas regulas (ES) 2024/2979 II pielikumā.

— 1. *PIEZĪME*. Šo prasību nevar izpildīt, ja pamatā esošā operētājsistēma, pārlūkprogramma, starpniecības *API* vai jebkurš cits tehniskais slānis ārpus *EUDI* maka kontroles jomas, ierobežo, filtrē, iepriekš atlasa vai citādi ierobežo apliecinājuma dokumentu formātus un shēmu katalogā reģistrētos *PID* un *EAA* veidus. Ja šāds ierobežojums liedz *EUDI* makam atbalstīt reģistrētu apliecinājuma dokumenta veidu vai formātu, izrietošā neatbilstība ir attiecināma uz minēto pamatā esošo operētājsistēmu, pārlūkprogrammu, starpniecības API vai cita attiecīgā tehniskā slāņa nespēju nodrošināt nepieciešamās sadarbspējas funkcijas.

6) 4.4. Maka atkarīgās puses validācijas un pārvērtēšanas pārbaudes

— WRP-VALIDATION-01: *EUDI* maks validē pieprasījumā saņemto maka atkarīgās puses reģistrācijas sertifikātu pirms jebkura pieprasītā *PID* vai atribūtu elektroniskā apliecinājuma uzrādīšanas maka lietotājam apstiprināšanai.

— WRP-VALIDATION-02: Ja maka atkarīgās puses reģistrācijas sertifikāta validācija neizdodas, tai skaitā, ja sertifikāta derīguma termiņš ir beidzies, tas ir atsaukts, to nav izdevis derīgs uzticams maka atkarīgās puses reģistrācijas sertifikātu nodrošinātājs, tas ir nepareizi veidots vai to nevar kriptogrāfiski verificēt, *EUDI* maks brīdina maka lietotāju, ka maka atkarīgo pusi nevar validēt, un neiesniedz pieprasījumu kā sekmīgi validētu. Maka lietotājs skaidri apstiprina atkarīgās puses pieprasījumu. Klusēšana vai iepriekš atzīmēti lodziņi netiek uzskatīti par skaidru piekrišanu.

— WRP-VALIDATION-03: Maka nodrošinātājs, pamatojoties uz savu riska analīzi un drošības politiku, nosaka, vai un ar kādiem nosacījumiem maka lietotājs var apiet konkrētas neveiksmīgas validācijas pārbaudes.

— WRP-OVERASKING-01: *EUDI* maks salīdzina maka atkarīgās puses pieprasītos apliecinājumus un atribūtus ar maka atkarīgās puses reģistrācijas sertifikātā reģistrētajiem apliecinājumiem un atribūtiem.

— WRP-OVERASKING-02: Ja maka atkarīgā puse pieprasa *PID* vai atribūtu elektroniskos apliecinājumus, vai apgalvojumus, uz kuriem neattiecas maka atkarīgās puses reģistrācijas sertifikāts, *EUDI* maks pirms jebkādas izpaušanas skaidri brīdina maka lietotāju. Brīdinājumā norāda, ka maka atkarīgā puse pieprasa vairāk informācijas, nekā tā ir reģistrējusi. Maka lietotājs skaidri apstiprina atkarīgās puses pieprasījumu. Klusēšana vai iepriekš atzīmēti lodziņi netiek uzskatīti par skaidru piekrišanu.

— WRP-OVERASKING-03: Maka nodrošinātājs, pamatojoties uz savu riska analīzi, drošības politiku un piemērojamiem tiesību aktiem, nosaka, vai maka lietotājs var turpināt darbību, neraugoties uz šādu brīdinājumu, vai drīkst izpaust tikai to pieprasīto datu apakškopu, uz kuru attiecas reģistrācijas sertifikāts, vai arī pieprasījums ir jānoraida.

7) 5.1. Ievads

— 5. punktā un tā apakšpunktos ir noteikts profils tādam protokolam, kas ļauj *RP* pieprasīt *EUDI* makam *EAAP* vai *PID*, un *EUDI* makam nosūtīt *RP* pieprasītos *EAAP*/*PID*, izmantojot vai nu pārraides mehānismu bez *API* starpniecības, kura pamatā ir ISO/IEC 18013-5 [10], vai pārraides mehānismu ar *API* starpniecību, kura pamatā ir ISO/IEC 18013-7 [16] C pielikums, lai nosūtītu ISO/IEC 18013-5 [10] noteiktās datu struktūras, kas ir atbilstoši ietvertas.

— Pārējo 5. punkta daļu organizē šādi:

  — 5.2. punktā ir noteiktas prasības attiecībā uz *RP* un *EUDI* maka profila un pārraides mehānismu atbalstu,

  — 5.3. punktā noteiktas prasības, kas ir specifiskas pārraides mehānismam bez *API* starpniecības,

  — 5.4. punktā un tā apakšpunktos ir noteiktas prasības, kas ir specifiskas pārraides mehānismam ar *API* starpniecību.

8) 5.2. Prasības attiecībā uz *EUDI* maku un *RP* atbalstu

— ISO/IEC 18013-SUPPORT-01: maka vienības, *PID* sniedzēji, apliecināšanas pakalpojumu sniedzēji, maka pakalpojumu sniedzēji un atkarīgās puses neatbalsta datu izgūšanu no servera, kā noteikts ISO/IEC 18013-5 [10], lai pieprasītu un sniegtu *PID* vai apliecinājuma atribūtus.

— ISO/IEC 18013-SUPPORT-02: *EUDI* maks atbilst šā dokumenta 5.3. un 5.4. punktā noteiktajām prasībām.

— ISO/IEC 18013-SUPPORT-04: atkarīgajai pusei būtu jāīsteno šā dokumenta 5.4. punktā noteiktais profils.

9) 5.3.2. *ISO/IEC-mdoc EAAP* pieprasījuma saturs

— ISO/IEC 18013-5-REQ-04: *EUDI* makiem nosūtītajos ierīču pieprasījumos ir "requestInfo" atslēgas un vērtības pāris, kas norādīts [10] daļas 8.3.2.1.2.1. punktā. Šā pāra vērtība ir RequestInfo tips.

— ISO/IEC 18013-5-REQ-05: RequestInfo tipam jābūt tādam, kā norādīts turpmāk *CDDL* definīcijā.

RequestInfo = {

"euWrprc": bstr; ietver reģistrācijas sertifikātu (sk. turpmāk minētās prasības)

}

— ISO/IEC 18013-5-REQ-06: Minētā requestInfo loceklis ietver locekli ar marķējumu "euWrprc".

— ISO/IEC 18013-5-REQ-07: "euWrprc" vērtība ir *CBOR* kodēts reģistrācijas sertifikāts.

— ISO/IEC 18013-5-REQ-08: nav spēkā.

— 3. *PIEZĪME.* nav spēkā.

— ISO/IEC 18013-5-REQ-09: nav spēkā.

— ISO/IEC 18013-5-REQ-10: nav spēkā.

— ISO/IEC 18013-5-REQ-11: nav spēkā.

10) 5.3.3. *ISO/IEC-mdoc EAAP* atbildes profils

— Šajā punktā ir noteiktas prasības ziņojuma veidam *DeviceResponse*, kas ir kopīgas abiem pārraides mehānismu veidiem (ar *API* starpniecību un bez *API* starpniecības).

— *1. PIEZĪME.* Ja tiek izmantots mehānisms bez *API* starpniecības, kura pamatā ir ISO/IEC 18013-5 [10], *EAAP* atbilde ir tieši tāda *DeviceResponse* instance, kāda norādīta šajā punktā. Ja tiek izmantots mehānisms ar *API* starpniecību, kura pamatā ir ISO/IEC 18013-7 [16] C pielikums, *DeviceRequest* instance tiek ietverta, kā norādīts [16] C pielikumā.

— ISO/IEC 18013-5-RESP-02: personas identifikācijas datu un atribūtu elektronisko apliecinājumu sniedzējs neiekļauj nekādus datu elementus to izdoto personas identifikācijas datu un atribūtu elektronisko apliecinājumu mobilās drošības objekta *KeyAuthorizations* kartē, izņemot datu elementus, ko maka atkarīgā puse sniedz darījuma datos mdoc pieprasījumā, kas maka vienībai jāparaksta vai jāapzīmogo, izmantojot personas identifikācijas datu vai atribūtu elektronisko apliecinājumu privāto atslēgu.

— *2. PIEZĪME.* Tā rezultātā maka vienības nevar sniegt nekādus ar ierīci parakstītus datu elementus maka atkarīgajām pusēm, izņemot attiecībā uz parakstīšanas datiem, kuriem maka atkarīgā puse nodrošinājusi, piemēram, drošas lietotāju autentifikācijas lietošanas gadījumos.

— *3. PIEZĪME.* ISO/IEC 18013-5:2021 nav precizēts, kā maka atkarīgās puses var iekļaut darījumu datus mdoc pieprasījumā. Darījumu datu iekļaušana mdoc pieprasījumā notiek, pievienojot tehniskās specifikācijas.

— ISO/IEC 18013-5-RESP-03: personas identifikācijas datu sniedzēji neļauj personas identifikācijas datu privātajai atslēgai parakstīt datu elementus, ko maka atkarīgā puse sniegusi mdoc pieprasījumā iekļautajos darījumu datos.

11) 5.4. Prasības attiecībā uz API starpniecības mehānismu

5.4.1. Ar ISO/IEC 18013-7 saistītas prasības

Šajā punktā ir noteiktas prasības pārraides mehānismam ar *API* starpniecību saistībā ar prasībām, kas noteiktas [16] C pielikumā.

— ISO/IEC 18013-7-API-01: profils, kas atbalsta datu sniegšanu ar *API* starpniecību, atbilst ISO/IEC 18013-7 [16] C pielikuma prasībām, kas sīkāk izklāstītas šā dokumenta 5.3. un 5.4. punktā.

— ISO/IEC 18013-7-API-02: visas obligātās prasības, kas noteiktas [16] C pielikumā, piemēro, kā sīkāk izklāstīts šā dokumenta 5.3. un 5.4. punktā.

— ISO/IEC 18013-7-API-03: visas neobligātās prasības, kas noteiktas [16] C pielikumā, joprojām nav obligātas, ja vien šajā dokumentā nav noteikts citādi.

12) 5.4.2 Papildu prasības

— Šajā punktā ir noteiktas papildu prasības attiecībā uz pārraides mehānismu ar *API* starpniecību.

— ISO/IEC 18013-ADD-API-01: *EUDI* maks pēc noklusējuma atklāj visu uzglabāto atribūtu tipa elektronisko apliecinājumu klātbūtni starpnieka *API*, kas darbojas saskaņā ar [16] C pielikumu, bet neatklāj atribūtus un to vērtības šajos atribūtu elektroniskajos apliecinājumos.

— *1. PIEZĪME.* Atribūtu vērtības ierobežojums ir piemērojams pat tad, ja šāda izpaušana uzlabotu pakalpojumus, ko operētājsistēma sniedz *EUDI* makam, piemēram, apliecinājuma atlasi saistībā ar starpnieka *API*.

— Ir apsvērumi, kas saistīti ar operētājsistēmām un pārlūkprogrammām, kuras nav īstenotāju kontrolē, un tos var ņemt vērā, kā norādīts 2.–4. piezīmē.

— *2. PIEZĪME.* Pārlūkprogramma un/vai operētājsistēma var apstrādāt atkarīgās puses iesniegtu sniegšanas pieprasījumu, kas atbalsta [16] C pielikumu, lai meklētu pieejamos *EAA* un novērstu krāpšanu, kas vērsta pret lietotāju, vai veiktu traucējummeklēšanu.

— *3. PIEZĪME.* Gaidāms, ka pārlūkprogramma un/vai operētājsistēma lietotāja drošības nolūkos apstrādās atkarīgās puses iesniegtu sniegšanas pieprasījumu, kas atbalsta [16] C pielikumu.

— 4. *PIEZĪME.* Gaidāms, ka pārlūkprogramma un/vai operētājsistēma neapstrādās atkarīgās puses sniegšanas pieprasījumu, kas atbalsta [16] C pielikumu, tirgus analīzes nolūkos (arī kā sekundāru nolūku) vai pārlūkprogrammas un/vai operētājsistēmas iekšējos nolūkos.

— ISO/IEC 18013-ADD-API-02: Ja *EUDI* maks pēc lietotāja pieprasījuma dzēš *PID* vai *EAA*, kas iepriekš izpausts starpnieka *API*, kura darbojas saskaņā ar [16] C pielikumu, *EUDI* maks atklāj, ka tas vairs neglabā šo PID vai EAA , starpnieka *API*.

— ISO/IEC 18013-ADD-API-03: Ja lietotājs atinstalē savu *EUDI* maku, *EUDI* maks atklāj to, ka tas vairs neglabā iepriekš izpaustus *PID* vai *EAA* starpnieka *API*, kas darbojas saskaņā ar [16] C pielikumu.

— ISO/IEC 18013-ADD-API-04: *EUDI* maks nodrošina globālu lietotāja iestatījumu, lai atspējotu glabāto *EAA* atklāšanu, izmantojot starpnieka *API*, kas darbojas, kā noteikts ISO/IEC 18013-ADD-API-01. Ja šis iestatījums ir atspējots, *EUDI* maks nereklamē ar *API* palīdzību sagatavotus sniegšanas vai izdošanas pieprasījumus un neatbild uz tiem.

— ISO/IEC 18013-ADD-API-05: *EUDI* maki, izmantojot starpniecības *API*, starpierīču plūsmās pārbauda, vai mijiedarbīgā ierīce atrodas tiešā fiziskā *EUDI* maka tuvumā, fiziskā tuvuma pārbaudes veikšanai izmantojot drošu, tiešu un lietotāja vadītu vietējo sakaru kanālu, piemēram, tuva darbības rādiusa bezvadu sakaru tehnoloģiju.

— *PIEZĪME.* CTAP 2.3 ļauj izmantot *BLE* tuvā fiziskā tuvuma pārbaudei, un, ja to izmanto abas ierīces, arī nodrošina datu pārraidi starp ierīcēm, izmantojot maza darbības attāluma pārraides tehnoloģijas. Attiecībā uz CTAP hibrīdtuneļa pakalpojumu izmantošanu būtu jādod priekšroka gan fiziska tuvuma pārbaudei, gan datu pārsūtīšanai starp abām ierīcēm, izmantojot vietējo sakaru kanālu, ko nodrošina CTAP 2.3., izmantojot pamatā esošās operētājsistēmas, pārlūkprogrammas, starpnieka *API* vai jebkuru citu tehnisku slāni, ko *EUDI* maks nevar kontrolēt.

13) 6.2. Prasības attiecībā uz *EUDI* maku un *RP* atbalstu

— OIDFVP-HAIP-SUPPORT-02: *EUDI* maks atbilst šā pielikuma 6.5. punktā noteiktajām prasībām.

— OIDFVP-HAIP-SUPPORT-03: *EUDI* makam nevajadzētu atbalstīt 6.4. punktā noteikto pārvirzīšanas mehānismu starpierīču uzrādīšanas plūsmām.

— 3. *PIEZĪME.* Šā mehānisma izmantošana ir neaizsargāta pret uzbrukumiem, piemēram, sesiju fiksāciju. Šādu uzbrukumu mazināšana ir atkarīga no atkarīgajām pusēm. Šā mehānisma īstenošanai nevajadzētu izraisīt neatbilstību.

— OIDFVP-HAIP-SUPPORT-05: atkarīgā puse atbilst šā pielikuma 6.5. punktā noteiktajām prasībām.

— 5. *PIEZĪME.* Nav spēkā.

14) 6.3.1. Vispārīgas prasības

— OIDFVP-HAIP-GEN-01: piemēro visas *HAIP* [11] 5., 5.3., 7. un 8. punktā noteiktās obligātās prasības.

— 1. *PIEZĪME.* "*HAIP* [11] 5. iedaļa" attiecas tikai uz prasībām tieši zem 5. iedaļas virsraksta. Tas neietver 5.1., 5.2. un 5.3. iedaļu.

— OIDFVP-HAIP-GEN-03: Ja ar šo pielikumu groza kādu *OpenID4VC-HAIP* [11] prasību, noteicošā ir ar šo pielikumu noteiktā grozītā prasība.

— 2. *PIEZĪME.* Tas ļautu, piemēram, pārveidot *OpenID4VC-HAIP* [11] neobligātu prasību par obligātu prasību vai paplašināt obligātās prasības.

— OIDFVP-HAIP-GEN-04: Ja pieprasītā apliecinājuma formāts atbilst [10], atkarīgās puses un *EUDI* maki atbilst "ISO mdocs" profilam [11] 6. iedaļā.

— *3. PIEZĪME.* Skaidrības labad jānorāda, ka "ISO mdocs profils" *HAIP* nozīmē, ka atkarīgajām pusēm un *EUDI* makiem ir jāatbilst piemērojamajām prasībām, kas noteiktas [7] B.2. pielikumā.

— OIDFVP-HAIP-GEN-05: Ja pieprasītā apliecinājuma formāts atbilst [2], atkarīgās puses un *EUDI* maki atbilst "IETF SD-JWT VC" profilam [11] 6. iedaļā.

— *4. PIEZĪME.* Skaidrības labad jānorāda, ka "IETF SD-JWT VC profils" nozīmē, ka atkarīgajām pusēm un *EUDI* makiem ir jāatbilst [7] B.3. pielikuma prasībām un [11] 6.1. iedaļas prasībām.

15) 6.3.2.1. Vispārīgas prasības

— OIDFVP-HAIP-COMMON-REQ-01: nav spēkā.

16) 6.3.2.2. Prasības attiecībā uz pieprasījuma priekšmetu

— OIDFVP-HAIP-COMMON-REQ-RO-02: nav spēkā.

— OIDFVP-HAIP-COMMON-REQ-RO-03: nav spēkā.

— OIDFVP-HAIP-COMMON-REQ-RO-04: nav spēkā.

— OIDFVP-HAIP-COMMON-REQ-RO-05: nav spēkā.

— OIDFVP-HAIP-COMMON-REQ-RO-06: nav spēkā.

— OIDFVP-HAIP-COMMON-REQ-RO-07: nav spēkā.

— OIDFVP-HAIP-COMMON-REQ-RO-08: nav spēkā.

— OIDFVP-HAIP-COMMON-REQ-RO-09: nav spēkā.

— OIDFVP-HAIP-COMMON-REQ-RO-10: nav spēkā.

— OIDFVP-HAIP-COMMON-REQ-RO-11: nav spēkā.

— OIDFVP-HAIP-COMMON-REQ-RO-12: nav spēkā.

— *2. PIEZĪME.* nav spēkā.

— OIDFVP-HAIP-COMMON-REQ-RO-13: viens no *verifier_info* parametra elementiem ietver reģistrācijas apliecību.

— OIDFVP-HAIP-COMMON-REQ-RO-23: lapas sertifikāts, kas minēts *OpenID4VP* 5.9.3. iedaļā lietošanai ar x509_hash klienta identifikatora prefiksu, ir *RP* piekļuves sertifikāts, kā noteikts ETSI TS 119 475 [14].

17) 6.3.3. Atļaujas reakcijas (EAAP atbildes) profils

— OIDFVP-HAIP-COMMON-RESP-01: nav spēkā.

18) 6.4.1. Vispārīgas prasības

— OIDFVP-HAIP-REDIRECTS-04: nav spēkā.

— *PIEZĪME.* nav spēkā.

19) 6.5.2. Papildu prasības

— OIDFVP-HAIP-ADD-API-01: *EUDI* maks pēc noklusējuma atklāj visu glabāto *EAA* veidu klātbūtni starpnieka *API*, kas darbojas saskaņā ar [11] 5.2. punktu, bet neatklāj atribūtus un to vērtības šajos *EAA*.

— OIDFVP-HAIP-ADD-API-04: ja *EUDI* maks atbalsta starpnieka *API*, kas darbojas, kā norādīts OIDFVP-HAIP-ADD-API-01, tas nodrošina globālu lietotāja iestatījumu, lai atspējotu uzglabāto *EAA* atklāšanu, izmantojot starpnieka *API*. Kad šis iestatījums ir iestatīts, lai atspējotu izpaušanu, *EUDI* makam pēc tam būtu jāļauj lietotājam izvēlēties individuālus apliecinājumus, kas izpaužami starpnieka *API*.

— OIDFVP-HAIP-ADD-API-05: *EUDI* maki, izmantojot starpniecības *API*, starpierīču plūsmās pārbauda, vai mijiedarbīgā ierīce atrodas tiešā fiziskā *EUDI* maka tuvumā, fiziskā tuvuma pārbaudes veikšanai izmantojot drošu, tiešu un lietotāja vadītu vietējo sakaru kanālu, piemēram, tuva darbības rādiusa bezvadu sakaru tehnoloģiju.

— *5. PIEZĪME.* CTAP 2.3 ļauj izmantot *BLE* tuvā fiziskā tuvuma pārbaudei, un, ja to izmanto abas ierīces, arī nodrošina datu pārraidi starp ierīcēm, izmantojot maza darbības attāluma pārraides tehnoloģijas. Attiecībā uz CTAP hibrīdtuneļa pakalpojumu izmantošanu būtu jādod priekšroka gan fiziska tuvuma pārbaudei, gan datu pārsūtīšanai starp abām ierīcēm, izmantojot vietējo sakaru kanālu, ko nodrošina CTAP 2.3., izmantojot pamatā esošās operētājsistēmas, pārlūkprogrammas, starpnieka *API* vai jebkuru citu tehnisku slāni, ko *EUDI* maks nevar kontrolēt.

20) 6.5.3. Īpašas prasības, pieprasot ISO/IEC 18013-5 *EAAP*

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: visas šajā dokumentā noteiktās prasības, kas piemērojamas ISO/IEC 18013-5 norādītajām ierīču pieprasījumu un ierīču atbildes struktūrām, piemēro arī tad, ja *EUDI* maks saņem pieprasījumu par *ISO/IEC mdoc* lietošanu, izmantojot *API* pārraidītu mehānismu, kas minēts [16] C.1. punktā.”