Europos Sąjungos
oficialusis leidinys

LT
L serija

2026/1731

2026 7 22

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2026/1731

2026 m. liepos 15 d.

kuriuo dėl taikytinų standartų ir specifikacijų iš dalies keičiami įgyvendinimo reglamentai (ES) 2024/2977, (ES) 2024/2979, (ES) 2024/2980 ir (ES) 2024/2982

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB ([1]), ypač į jo 5a straipsnio 23 dalį,

kadangi:

(1) siekiant užtikrinti aukščiausią valstybių narių suderinimo lygį kuriant europines skaitmeninės tapatybės dėkles, techninės dėklių specifikacijos yra grindžiamos darbu, atliktu remiantis Komisijos rekomendacija (ES) 2021/946 ([2]), ypač architektūra ir pamatine sistema. Architektūra ir pamatinė sistema gerokai pasikeitė po Komisijos įgyvendinimo reglamentų (ES) 2024/2977 ([3]), (ES) 2024/2979 ([4]), (ES) 2024/2980 ([5]) ir (ES) 2024/2982 ([6]) priėmimo, todėl dabar tie įgyvendinimo reglamentai turėtų būti atitinkamai iš dalies pakeisti, kad būtų suderinti su naujais standartais, specifikacijomis ir procedūromis.

Kad šie konkretūs reikalavimai būtų įvykdyti, pagal Reglamento (ES) Nr. 910/2014 tikslus buvo atrinkti keli standartai. Šie standartai turėtų atitikti nusistovėjusią praktiką ir būti plačiai pripažįstami atitinkamuose sektoriuose. Pavyzdžiui, Žiniatinklio konsorciumo (W3C) patikrinamų kredencialų duomenų modelio formatas (VCDM) yra pamatinis, ypač švietimo sektoriaus, pažymėjimų formatas, todėl europinės skaitmeninės tapatybės dėklės turėtų būti tinkamos tokio formato duomenims, kai bus parengti nauji W3C VCDM formato profiliai. Prireikus šie standartai turėtų būti pritaikyti arba papildyti, kad būtų užtikrintas europinių skaitmeninės tapatybės dėklių saugumo ir patikimumo lygis ir drauge sudarytos geresnės sąlygos tarpvalstybiniam sąveikumui ir efektyviam vidaus rinkos veikimui;

(2) Visada, kai naudojant dėklę reikia pateikti dėklės naudotojo veido atvaizdą, dėklės sprendiniai turi palaikyti pasirinktinio atskleidimo funkciją, o atskleidimą turi visiškai kontroliuoti naudotojas. Kad būtų apsaugota galimybė spręsti dėl veido atvaizdo atskleidimo ir kad veido atvaizdas būtų apsaugotas nuo atsitiktinio arba neleistino prašymo jį atskleisti, europinės skaitmeninės tapatybės dėklės architektūroje turėtų būti numatytas įspėjimo mechanizmas ir visų su veido atvaizdo naudojimu susijusių operacijų registravimas žurnale. Siekiant užtikrinti, kad dėklės naudotojas žinotų apie dalijimąsi biometriniais duomenimis, įspėjimuose turėtų būti nurodyta, kad prašymas

([1]) OL L 257, 2014 8 28, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) 2021 m. birželio 3 d. Komisijos rekomendacija (ES) 2021/946 dėl bendro Sąjungos priemonių rinkinio darniam Europos skaitmeninės tapatybės sistemos kūrimui užtikrinti (OL L 210, 2021 6 14, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([3]) 2024 m. lapkričio 28 d. Komisijos įgyvendinimo reglamentas (ES) 2024/2977, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 nuostatų dėl naudojantis europinėmis skaitmeninės tapatybės dėklėmis išduodamų asmens tapatybės duomenų ir elektroninių požymių liudijimų taikymo taisyklės, (OL L, 2024/2977, 2024 12 4, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).
([4]) 2024 m. lapkričio 28 d. Komisijos įgyvendinimo reglamentas (ES) 2024/2979, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 taikymo taisyklės, susijusios su europinių skaitmeninės tapatybės dėklių vientisumu ir pagrindinėmis funkcijomis, (OL L, 2024/2979, 2024 12 4, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).
([5]) 2024 m. lapkričio 28 d. Komisijos įgyvendinimo reglamentas (ES) 2024/2980, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 taikymo taisyklės, susijusios su pranešimais Komisijai dėl europinių skaitmeninės tapatybės dėklių ekosistemos, (OL L, 2024/2980, 2024 12 4, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).
([6]) 2024 m. lapkričio 28 d. Komisijos įgyvendinimo reglamentas (ES) 2024/2982, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 nuostatų dėl Europos skaitmeninės tapatybės sistemos palaikytinų protokolų ir sąsajų taikymo taisyklės, (OL L, 2024/2982, 2024 12 4, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

yra susijęs su dalijimusi biometriniais duomenimis ir kad veido atvaizdą atskleisti galima tik gavus naudotojo patvirtinimą. Jei pasikliaujančioji šalis veido atvaizdą apdoroja tam, kad vienareikšmiškai nustatytų fizinio asmens tapatybę arba patvirtintų to asmens deklaruojamą tapatybę, taikomi Europos Parlamento ir Tarybos reglamento (ES) 2016/679 ([7]) 6 ir 9 straipsniai, taip pat visi kiti to reglamento reikalavimai, įskaitant reikalavimą, kad pasikliaujančiosios šalys veido atvaizdą apdorotų tik tiek, kiek to būtinai reikia numatytais tikslais. Dėklės naudotojui apie numatytus tikslus turėtų būti aiškiai ir suprantamai pranešama kartu su veido atvaizdo atskleidimo prašymu. Kad būtų visapusiškai atsižvelgta į biometrinių duomenų neskelbtinumą, dėklės naudotojas turėtų aiškiai ir konkrečiai patvirtini veido atvaizdo atskleidimą. Nutylėjimas ar iš anksto pažymėti žymimieji langeliai neturėtų būti laikomi dėklės naudotojo duotu patvirtinimu. Aiškus dėklės naudotojo duotas patvirtinimas turėtų būti techninis saugiklis, tačiau jis savaime neturėtų būti teisinis apdorojimo pagrindas. Pagal Reglamento (ES) 2016/679 9 straipsnio 4 dalį valstybės narės gali toliau taikyti arba nustatyti papildomas sąlygas, įskaitant genetinių duomenų, biometrinių duomenų arba sveikatos duomenų tvarkymo apribojimus;

(3) kad valstybės narės turėtų pakankamai laiko pritaikyti savo nacionalines procedūras, dėklės naudotojo veido atvaizdas į privalomus asmens tapatybės duomenis fiziniams asmenims gali būti įtrauktas tik nuo 2028 m. rugpjūčio 11 d. Jei tokie atvaizdai gaunami iš turimų asmens tapatybės dokumentų, pavyzdžiui, iš tapatybės kortelių arba pasų, turėtų būti taikomi atitinkamai Tarybos reglamentuose (ES) 2025/1208 ([8]) arba (EB) Nr. 2252/2004 ([9]) nustatyti aktualūs reikalavimai;

(4) Reglamente (ES) Nr. 910/2014 reikalaujama, kad su dėklėmis būtų galima rodyti ES skaitmeninės tapatybės dėklės patikimumo ženklą kaip patikrinamą, paprastą ir atpažįstamą požymį, kad dėklė suteikta pagal tą reglamentą. Naudojamas patikimumo ženklas padės vidaus rinkai veikti efektyviai, užtikrins sąžiningą konkurenciją ir apsaugos naudotojų interesus. Kad būtų sudarytos sąlygos naudoti tokį patikimumo ženklą, turėtų būti nustatytos patikimumo ženklo pavidalo ir techninės charakteristikos;

(5) Reglamento (ES) Nr. 910/2014 12b straipsnyje nustatyta, kad prieigos valdytojai turi europinės skaitmeninės tapatybės dėklės teikėjams ir elektroninės atpažinties priemonių, apie kurias pranešta, išdavėjams leisti užtikrinti veiksmingą sąveikumą su tomis pačiomis operacinės sistemos, aparatinės įrangos ar programinės įrangos funkcijomis, o sąveikumo tikslais suteikti galimybę jomis naudotis. Toks veiksmingas sąveikumas ir prieiga suteikiami nemokamai ir nepriklausomai nuo to, ar aparatinės ar programinės įrangos funkcijos, kurios yra prieinamos tam prieigos valdytojui, kai jis teikia tokias paslaugas, ar yra jo naudojamos, yra operacinės sistemos dalis. Visi dėklės sprendiniai turėtų būti pritaikyti bendram protokolų ir sąsajų rinkiniui siekiant užtikrinti tinkamumą naudoti, saugumą ir sąveikumą visose valstybėse narėse, todėl prieigos valdytojai turėtų įjungti operacinės sistemos, aparatinės arba programinės įrangos funkcijas, būtinas šio reglamento XII priede nustatytiems protokolams ir sąsajoms įgyvendinti. Todėl prieigos valdytojai, organizuodami elektroninius duomenų srautus tarp įrenginių, tiek fiziniam artumui patikrinti, tiek duomenims perduoti tarp dviejų įrenginių turėtų pirmenybę teikti pagal protokolo *Client To Authenticator* (CTAP) 2.3 versijos specifikaciją ([10]) sukurtam vietinio ryšio kanalui, o ne CTAP hibridinio tunelio paslaugoms;

(6) kad valstybės narės, dėklės pasikliaujančiosios šalies prieigos sertifikatų teikėjai ir dėklės teikėjai turėtų pakankamai laiko dėklės vienetuose suaktyvinti dėklės pasikliaujančiosios šalies registracijos liudijimo tapatumo nustatymą ir patvirtinimą, šis reikalavimas turėtų būti taikomas tik nuo 2028 m. rugpjūčio 11 d.;

(7) visai asmens duomenų tvarkymo pagal šį reglamentą veiklai taikomas Reglamentas (ES) 2016/679 ir, kai aktualu, Europos Parlamento ir Tarybos direktyva 2002/58/EB ([11]);

([7]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) 2025 m. birželio 12 d. Tarybos reglamentas (ES) 2025/1208, dėl Sąjungos piliečių tapatybės kortelių ir Sąjungos piliečiams bei jų šeimos nariams, kurie naudojasi laisvo judėjimo teise, išduodamų teisę gyventi šalyje patvirtinančių dokumentų saugumo didinimo, (OL L, 2025/1208, 2025 6 20, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) 2004 m. gruodžio 13 d. Tarybos reglamentas (EB) Nr. 2252/2004 dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų (OL L 385, 2004 12 29, p. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Standartas *Client to Authenticator Protocol* (CTAP), kurį pasiūlė *Fido Alliance*, 2026 m. vasario 26 d.

([11]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([12]) 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir 2026 m. balandžio 17 d. jis pateikė nuomonę ([13]);

(9) šiame reglamente numatytos priemonės atitinka pagal Reglamento (ES) Nr. 910/2014 48 straipsnį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Įgyvendinimo reglamento (ES) 2024/2977 pakeitimai

Įgyvendinimo reglamentas (ES) 2024/2977 iš dalies keičiamas taip:

1) įterpiamas 3a straipsnis:

„*3a straipsnis*

Veido atvaizdo apsauga

1) Be to, kad laikosi Reglamente (ES) 2016/679 informacijai keliamų reikalavimų, dėklės teikėjai užtikrina, kad jų pateikti dėklės sprendiniai įspėtų dėklės naudotojus, kai dėklės pasikliaujančiosios šalys prašo atskleisti veido atvaizdą, ir praneštų, kad toks prašymas yra susijęs su dalijimusi biometriniais duomenimis ir kad pasirinkimą atskleisti veido atvaizdą reikia patvirtinti.

2) Siekdami įgyvendinti veido atvaizdo atskleidimo dėklės pasikliaujančiajai šaliai pasirinktinumo principą, dėklės teikėjai užtikrina, kad dėklės sprendiniuose būtų įdiegtas reikalavimas, kad dėklės naudotojas aiškiai ir konkrečiai patvirtintų sutikimą pateikti veido atvaizdą.

3) Laikydamosi Sąjungos duomenų apsaugos teisės aktų, dėklės pasikliaujančiosios šalys veido atvaizdo nepasilieka, nebent jį reikia toliau apdoroti tapatybės ir tapatumo nustatymo tikslais pagal Sąjungos duomenų apsaugos teisės aktus arba taip numatyta Sąjungos arba nacionaliniuose teisės aktuose. Veido atvaizdas neperduodamas trečiosioms valstybėms arba tarptautinėms organizacijoms, išskyrus, kai tai leidžiama pagal Sąjungos duomenų apsaugos teisės aktus.“;

2) 4 straipsnio 1 dalis pakeičiama taip:

„1. Naudojantis dėklės vienetais išduodami elektroniniai požymių liudijimai turi atitikti bent vieną iš standartų, nustatytų Įgyvendinimo reglamento (ES) 2024/2979 II priede.“;

3) 5 straipsnio 4 dalies b punktas pakeičiamas taip:

„b) jei su dėklės vienetu susijęs dėklės vieneto liudijimas, kuriam buvo išduoti asmens tapatybės duomenys, buvo atšauktas;“;

4) Priedas pakeičiamas šio reglamento I priede pateikiamu tekstu.

([12]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) Europos duomenų apsaugos priežiūros pareigūno oficialios pastabos dėl Įgyvendinimo reglamento, kuriuo nustatomi taikytini standartai ir specifikacijos ir ištaisomas Įgyvendinimo reglamentas (ES) 2024/2980, projekto. Europos duomenų apsaugos priežiūros pareigūnas.

2 straipsnis

Įgyvendinimo reglamento (ES) 2024/2979 pakeitimai

Įgyvendinimo reglamentas (ES) 2024/2979 iš dalies keičiamas taip:

1) 3 straipsnio 2 dalis išbraukiama;

2) 5 straipsnio 1 dalies a punktas pakeičiamas taip:

„a) vykdytų dėklės šifravimo operacijas, susijusias su ypatingos svarbos turtu, laikomu saugiame dėklės šifravimo įrenginyje ir nebūtinu dėklės naudotojo tapatumui nustatyti, tik tada, kai tomis taikomosiomis programomis sėkmingai nustatytas dėklės naudotojo tapatumas;“;

3) įterpiamas 5a straipsnis:

„*5a straipsnis*

Šifravimo mechanizmai

Dėklės teikėjai 4 straipsnio 2 dalies tikslais naudoja tik Ia priede nurodytus šifravimo mechanizmus.“;

4) 6 straipsnis iš dalies keičiamas taip:

a) 1 dalis pakeičiama taip:

„1. Dėklės teikėjai išduoda kiekvieno dėklės vieneto liudijimus. Dėklės teikėjai pasirašo arba spaudu patvirtina dėklės vieneto liudijimus taip, kad parašus arba spaudus būtų galima patvirtinti naudojant sertifikatą, įrašytą į sąrašą pagal Įgyvendinimo reglamento (ES) 2024/2980 II priedo 2 skirsnio 1 punkto h papunktį.“;

b) 2 dalis pakeičiama taip:

„2. Dėklės teikėjai užtikrina, kad 1 dalyje nurodyti dėklės vieneto liudijimai atitiktų Ib priede pateiktas technines specifikacijas.“;

c) 3 dalies b punktas pakeičiamas taip:

„b) užtikrina saugaus dėklės naudotojų tapatybės ir jų tapatumo nustatymo mechanizmus, nepriklausomus nuo dėklės vienetų;“;

5) 9 straipsnio 2 dalies b punktas pakeičiamas taip:

„b) atitinkamos dėklės pasikliaujančiosios šalies vardą, pavardę (pavadinimą), kontaktinius duomenis ir unikalų identifikatorių, taip pat valstybės narės, kurioje ta dėklės pasikliaujančioji šalis yra įsisteigusi, pavadinimą;“;

6) 10 straipsnio 1 dalis pakeičiama taip:

„1. Dėklių teikėjai užtikrina, kad jų teikiami dėklės vienetai galėtų apdoroti elektroninius požymių liudijimus, išduotus pagal technines specifikacijas, taikytinas III priede nustatytai bendrajai integruotai informacijos atskleidimo politikai.“;

7) 12 straipsnis iš dalies keičiamas taip:

a) 2 dalies c punktas pakeičiamas taip:

„c) sukuriami parašai arba spaudai bent IV priede nurodytu privalomu parašo arba spaudo formatu;“;

b) 3 dalis pakeičiama taip:

„3. Parašo kūrimo taikomosios programos gali būti integruotos į dėklės egzempliorius arba būti išorinės.“;

c) įterpiama ši dalis:

„4. Parašo kūrimo taikomosios programos, kurias naudoja dėklės vienetai, palaiko bent IV priede nurodytą taikomųjų programų sąsają.“;

8) 14 straipsnio 1 dalis išbraukiama;

9) įterpiamas 14a straipsnis:

„*14a straipsnis*

ES skaitmeninės tapatybės dėklės patikimumo ženklas

1) Dėklės teikėjai užtikrina, kad su dėklės vienetais būtų rodomas ES skaitmeninės tapatybės dėklės patikimumo ženklas. ES skaitmeninės tapatybės dėklės patikimumo ženklas turi būti tokios formos, kokia nustatyta VI ir VII prieduose.

2) Dėklės teikėjai užtikrina, kad dėklės naudotojams dėklės vienetai suteiktų prieigą prie informacijos, kurią turėdami jie galėtų patikrinti dėklės sprendinio sertifikavimo statusą. Todėl dėklės teikėjai užtikrina, kad, užregistravus dėklės sprendinį, į atitinkamus dėklės vienetus būtų įtraukti universalieji išteklius adresai (URL), kuriuos tokiam patikrinimui pateikė Europos Komisija. Dėklės teikėjai užtikrina, kad jų dėklės vienetuose būtų prieiga prie ES skaitmeninės tapatybės dėklės patikimumo ženklo duomenų, atitinkančių VIII priede pateiktas technines specifikacijas.

3) ES skaitmeninės tapatybės dėklės patikimumo ženklo standartinės spalvos: *Pantone* Nr. 661 ir 116 arba mėlyna (100 % žydros + 67 % purpurinės + 0 % geltonos + 40 % juodos) ir geltona (0 % žydros + 20 % purpurinės + 100 % geltonos + 0 % juodos), jei taikomas keturių spalvų procesas; jei naudojamos RGB spalvos, standartinės spalvos yra mėlyna (0 raudonos + 51 žalios + 153 mėlynos) ir geltona (255 raudonos + 204 žalios + 0 mėlynos).

4) ES skaitmeninės tapatybės dėklės patikimumo ženklas gali būti nespalvotas, kaip nustatyta VII priede, tik jei naudoti kitų spalvų praktiškai neįmanoma.

5) Jei ES skaitmeninės tapatybės dėklės patikimumo ženklas naudojamas tamsiame fone, jis gali būti naudojamas negatyvo forma su ta pačia fono spalva. Jei ES skaitmeninės tapatybės dėklės patikimumo ženklas naudojamas spalvotame fone, dėl kurio tą ženklą sunku atskirti, ES skaitmeninės tapatybės dėklės patikimumo ženklas gali būti apvestas išorine kontūro linija, kad ženklas geriau atsiskirtų nuo fono spalvų.

6) Minimalus ES skaitmeninės tapatybės dėklės patikimumo ženklo dydis yra 64 × 85 pikselių (150 taškų colyje).

7) Dėklės teikėjai užtikrina, kad ES skaitmeninės tapatybės dėklės patikimumo ženklas būtų naudojamas taip, kad būtų aišku, su kuriuo dėklės vienetu yra siejamas ES skaitmeninės tapatybės dėklės patikimumo ženklas. ES skaitmeninės tapatybės dėklės patikimumo ženklas gali būti derinamas su grafikos arba teksto elementais, aiškiai nurodančiais, su kuriuo dėklės vienetu naudojamas tas ženklas, jei tokie elementai netrukdo atpažinti, kad tai ES skaitmeninės tapatybės dėklės patikimumo ženklas, ir nekeičia susiejimo su Reglamento (ES) Nr. 910/2014 5d straipsnyje nurodytu Sertifikuotų europinių skaitmeninės tapatybės dėklių sąrašu.

8) Atšaukę dėklės vieneto liudijimą, dėklės teikėjai užtikrina, kad atitinkamas dėklės vienetas neberodytų ES skaitmeninės tapatybės dėklės patikimumo ženklo.“;

10) pridedami Ia ir Ib priedai, kaip nustatyta šio reglamento II ir III prieduose;

11) II priedas pakeičiamas šio reglamento IV priedu;

12) III priedas pakeičiamas šio reglamento V priedu;

13) IV priedas iš dalies keičiamas pagal šio reglamento VI priedą;

14) V priedas išbraukiamas;

15) šio reglamento VII priede išdėstytas tekstas įterpiamas kaip VI priedas;

16) šio reglamento VIII priede išdėstytas tekstas įterpiamas kaip VII priedas;

17) šio reglamento IX priede išdėstytas tekstas įterpiamas kaip VIII priedas.

3 straipsnis

Įgyvendinimo reglamento (ES) 2024/2980 pakeitimai

Įgyvendinimo reglamentas (ES) 2024/2980 iš dalies keičiamas taip:

1) 5 straipsnio 2 dalis pakeičiama taip:

„2. Kai taikytina, Komisija sudaro, tvarko ir skelbia valstybių narių pateiktos II priedo 2, 3, 4 ir 5 skirsniuose nurodytos informacijos apie dėklės teikėjus, asmens tapatybės duomenų teikėjus, dėklės pasikliaujančiosios šalies prieigos sertifikatų teikėjus ir dėklės pasikliaujančiosios šalies registracijos sertifikatų teikėjus sąrašą.“;

2) Įgyvendinimo reglamento (ES) 2024/2980 II priedas iš dalies keičiamas, kaip nustatyta šio reglamento X priede.

4 straipsnis

Įgyvendinimo reglamento (ES) 2024/2982 pakeitimai

Įgyvendinimo reglamentas (ES) 2024/2982 iš dalies keičiamas taip:

1) 1 straipsnio 2 dalis pakeičiama taip:

„2) asmens tapatybės duomenų požymių ir elektroninių požymių liudijimų pateikimu dėklės pasikliaujančiosioms šalims;“;

2) 3 straipsnis iš dalies keičiamas taip:

a) 1 punktas pakeičiamas taip:

„1) vykstant sąveikai su dėklės pasikliaujančiosiomis šalimis, nustatytų dėklės pasikliaujančiosios šalies prieigos sertifikatų autentiškumą bei juos patvirtintų ir neperduotų šių procesų vykdymo operacinės sistemos naršyklei ar kitai tarpinei taikomajai programai;“;

b) 2 punktas išbraukiamas;

c) 3 punktas pakeičiamas taip:

„3) atliktų tapatumo nustatymą, kai prašymai teikiami naudojantis pasikliaujančiosios šalies prieigos sertifikatais, ir tuos prašymus patvirtintų;“;

d) 4 punktas pakeičiamas taip:

„4) nustatytų dėklės pasikliaujančiosios šalies registracijos liudijimo tapatumą ir jį patvirtintų;“;

e) 5 punktas pakeičiamas taip:

„5) dėklės naudotojams rodytų dėklės pasikliaujančiosios šalies prieigos sertifikate esančią informaciją;“;

f) 8 punktas išbraukiamas;

g) 9 punktas pakeičiamas taip:

„9) dėklės pasikliaujančiosioms šalims nepateiktų jokių prašomų požymių, kol neatlikti šie veiksmai:

a) patikrinta, ar dėklės vienete buvo atlikti integruotos informacijos atskleidimo politikos taikymo veiksmai pagal Įgyvendinimo reglamento (ES) 2024/2979 10 straipsnį;

b) patikrinta, ar dėklės naudotojai iš dalies arba visiškai patvirtino pateiktą informaciją.“;

3) 4 straipsnio 1 dalis pakeičiama taip:

„1. Dėklės teikėjai užtikrina, kad dėklės sprendiniai palaikytų asmens I priede nustatytus asmens tapatybės duomenų ir elektroninių požymių liudijimų išdavimo dėklės vienetams protokolus ir sąsajas.“;

4) 5 straipsnis iš dalies keičiamas taip:

   a) 1 ir 2 dalys pakeičiamos taip:

      „1. Dėklės teikėjai užtikrina, kad dėklės sprendiniai palaikytų protokolus ir sąsajas, skirtus požymiams dėklės pasikliaujančiosioms šalims pateikti nuotolinio ir, kai tinkama, artimojo veikimo atvejais, laikantis II priede nustatytų techninių specifikacijų.

      2. Dėklės teikėjai užtikrina, kad naudotojų prašymu dėklės vienetai atsakytų į 3 straipsnyje nurodytų dėklės pasikliaujančiųjų šalių prašymus, kurių teikėjo tapatumas buvo sėkmingai nustatytas ir kurie buvo patvirtinti, laikydamiesi II priede nustatytų techninių specifikacijų.“;

   b) 5 dalis išbraukiama.

5) 8 straipsnis pakeičiamas taip:

   „*8 straipsnis*

   Įsigaliojimas

   Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

   3 straipsnio 4 punktas taikomas nuo 2028 m. rugpjūčio 11 d.

   Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.“

6) Priedas išbraukiamas.

7) Šio reglamento XI priede pateiktas tekstas pridedamas kaip I priedas.

8) Šio reglamento XII priede pateiktas tekstas pridedamas kaip II priedas.

5 straipsnis

Įsigaliojimas

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2026 m. liepos 15 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

I PRIEDAS

„PRIEDAS

3 straipsnio 3 dalyje nurodytų asmens tapatybės duomenų techninės specifikacijos

1) 1 skirsnis. Fizinio asmens tapatybės duomenų rinkinys

1 lentelė

Privalomi fizinio asmens pasirinktinai atskleidžiami tapatybės duomenys

Duomenų identifikatorius	Apibrėžtis
`family_name`	Naudotojo, su kuriuo susiję asmens tapatybės duomenys, dabartinė pavardė (-ės).
`given_name`	Naudotojo, su kuriuo susiję asmens tapatybės duomenys, dabartinis vardas (-ai), įskaitant kitus vardus (jei yra).
`birth_date`	Naudotojo, su kuriuo susiję asmens tapatybės duomenys, gimimo diena, mėnuo ir metai.
`birth_place`	ISO 3166-1 nurodytas alpha-2 šalies kodas arba valstybė, apskritis, rajonas, vietovė arba savivaldybė, miestas ar kaimas, kuriame gimė naudotojas, su kuriuo susiję asmens tapatybės duomenys.
`nationality`	Vienas ar keli ISO 3166-1 nustatyti alpha-2 šalių kodai, nurodantys naudotojo, su kuriuo susiję asmens tapatybės duomenys, pilietybę.
`portrait`	Išskyrus atvejus, kai naudotojas aiškiai atsisako, naudotojo, su kuriuo susiję asmens tapatybės duomenys, veido atvaizdas, atitinkantis viso priekinio atvaizdo tipo kokybės reikalavimus, nustatytus standarte ISO/IEC 39794-5 arba, siekiant užtikrinti atgalinį suderinamumą, standarto ISO/IEC 19794-5 8.2, 8.3 ir 8.4 punktuose, kai taikytina, pateikiamas koduotais vaizdo duomenimis, be antraščių ar blokų, kaip nurodyta standarto ISO/IEC 19794-5 5 punkte, išskyrus pačius atvaizdo duomenis (JPEG); taikoma nuo 2028 m. rugpjūčio 11 d.

— Valstybės narės gali nustatyti, kad naudotojas turi galimybę atsisakyti į asmens tapatybės duomenis įterpti veido atvaizdą.

— Valstybės narės užtikrina, kad pasirinktinis atskleidimas būtų taikomas kiekvienam duomenų identifikatoriui, įskaitant veido atvaizdą.

— Jei tiksli fizinio asmens gimimo data nežinoma, valstybės narės pasirenka atitinkamas vertes, atitinkančias šio priedo 4.1 arba 4.2 skirsnyje (atitinkamai) nustatytas specifikacijas.

— Jei fizinio asmens pilietybė nežinoma, valstybės narės naudoja vertę „QU“.

— Jei fizinis asmuo pilietybės neturi, valstybės narės naudoja vertę „QS“.

— Kai naudotojas atsisako įtraukti veido atvaizdą, valstybės narės vertę palieka tuščią.

2 lentelė

Neprivalomi fizinio asmens pasirinktinai atskleidžiami tapatybės duomenys

Duomenų identifikatorius	Apibrėžtis
resident_address	Tikslus vietos, kurioje naudotojas, su kuriuo susiję asmens tapatybės duomenys, šiuo metu gyvena arba su juo galima susisiekti, adresas (gatvė, namo numeris, miestas ir t. t.).
resident_country	ISO 3166-1 nurodytas alpha-2 šalies, kurioje šiuo metu gyvena naudotojas, su kuriuo susiję asmens tapatybės duomenys, kodas
resident_state	Valstybė, apskritis, rajonas ar vietovė, kurioje šiuo metu gyvena naudotojas, su kuriuo susiję asmens tapatybės duomenys.
resident_city	Savivaldybė, miestas ar kaimas, kuriame šiuo metu gyvena naudotojas, su kuriuo susiję asmens tapatybės duomenys.
resident_postal_code	Vietovės, kurioje šiuo metu gyvena naudotojas, su kuriuo susiję asmens tapatybės duomenys, pašto kodas.
resident_street	Gatvės, kurioje šiuo metu gyvena naudotojas, su kuriuo susiję asmens tapatybės duomenys, pavadinimas ir namo numeris, įskaitant jo priešdėlį ar priesagą.
personal_administrative_-number	Naudotojui, su kuriuo susiję asmens tapatybės duomenys, priskirta vertė, kuri iš visų asmens tapatybės duomenų teikėjo išduotų asmens administracinių numerių yra unikali. Jei valstybės narės nusprendžia šį požymį įtraukti, jos savo elektroninės atpažinties schemose, pagal kurias išduodami asmens tapatybės duomenys, aprašo politiką, kurią jos taiko šio požymio vertėms, įskaitant, kai taikytina, konkrečias šios vertės tvarkymo sąlygas.
family_name_birth	Naudotojo, su kuriuo susiję asmens tapatybės duomenys, pavardė (-ės) gimimo metu.
given_name_birth	Naudotojo, su kuriuo susiję asmens tapatybės duomenys, vardas (-ai), įskaitant kitus vardus (jei yra), gimimo metu.
sex	Vertė yra viena iš šių: 0 = nežinoma; 1 = vyras; 2 = moteris; 3 = kita; 4 = interlytis asmuo; 5 = tradicinių lyčių normų neatitinkantis asmuo; 6 = atviro lytiškumo asmuo; 9 = netaikoma. 0, 1, 2 ir 9 vertėms taikomas ISO/IEC 5218.
email_address	Naudotojo, su kuriuo susiję asmens tapatybės duomenys, elektroninio pašto adresas [pagal RFC 5322 ([1])].

Duomenų identifikatorius	Apibrėžtis
`mobile_phone_number`	Naudotojo, su kuriuo susiję asmens tapatybės duomenys, mobiliojo telefono numeris, prasidedantis ženklu „+“, kaip tarptautinio kodo prefiksu, ir šalies kodu, po kurio rašomi tik skaičiai.

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

2) 2 skirsnis. Juridinio asmens tapatybės duomenų rinkinys

3 lentelė

Privalomi juridinio asmens tapatybės duomenys

Duomenų identifikatorius
dabartinis teisinis pavadinimas
pagal technines specifikacijas tarpvalstybinės atpažinties tikslu siunčiančiosios valstybės narės sukurtas unikalus identifikatorius, kuris turi būti kuo pastovesnis

— Jei duomenų identifikatorius asmeniui nežinomas arba negali būti kitaip išduotas kaip asmens tapatybės duomenų rinkinio dalis, valstybės narės vietoj to taiko padėtį atitinkančią požymio vertę.

4 lentelė

Neprivalomi juridinio asmens tapatybės duomenys

Duomenų identifikatorius
dabartinis adresas
PVM mokėtojo kodas
mokesčių mokėtojo registracijos kodas
Europos Parlamento ir Tarybos direktyvoje (ES) 2017/1132 ([1]) nurodytas Europos unikalus atpažinties kodas
Komisijos įgyvendinimo reglamente (ES) 2022/1860 ([2]) nurodytas juridinio asmens identifikatorius (LEI)
Komisijos įgyvendinimo reglamente (ES) Nr. 1352/2013 ([3]) nurodytas ekonominės veiklos vykdytojo registracijos ir identifikavimo kodas (EORI kodas)
Tarybos reglamento (ES) Nr. 389/2012 ([4]) 2 straipsnio 12 dalyje nurodytas akcizo numeris

([1]) 2017 m. birželio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2017/1132 dėl tam tikrų bendrovių teisės aspektų (OL L 169, 2017 6 30, p. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) 2022 m. birželio 10 d. Komisijos įgyvendinimo reglamentas (ES) 2022/1860. kuriuo nustatomi Europos Parlamento ir Tarybos reglamento (ES) Nr. 648/2012 taikymo techniniai įgyvendinimo standartai, susiję su duomenų teikimo standartais, formatais, dažnumu, metodais ir tvarka (OL L 262, 2022 10 7, p. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) 2013 m. gruodžio 4 d. Komisijos įgyvendinimo reglamentas (ES) Nr. 1352/2013, kuriuo nustatomos Europos Parlamento ir Tarybos reglamente (ES) Nr. 608/2013 dėl muitinės atliekamo intelektinės nuosavybės teisių vykdymo užtikrinimo numatytos formos (OL L 341, 2013 12 18, p. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) 2012 m. gegužės 2 d. Tarybos reglamentas (ES) Nr. 389/2012 dėl administracinio bendradarbiavimo akcizų srityje ir panaikinantis Reglamentą (EB) Nr. 2073/2004 (OL L 121, 2012 5 8, p. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3) 3 skirsnis. Asmens tapatybės duomenų metaduomenų rinkinys

5 lentelė

Asmens tapatybės duomenų metaduomenys

Duomenų identifikatorius	Apibrėžtis	Naudojimas
`issuing_authority`	Asmens tapatybės duomenis išdavusios administracinės institucijos pavadinimas arba atitinkamos valstybės narės ISO 3166 alpha-2 šalies kodas, jei nėra atskiros asmens tapatybės duomenis išduoti teisę turinčios institucijos.	privalomas
`issuing_country`	Asmens tapatybės duomenų teikėjo šalies arba teritorijos alpha-2 šalies kodas, nurodytas ISO 3166-1.	privalomas
`expiry_date`	Asmens tapatybės duomenų administracinio galiojimo laikotarpio pabaigos data (ir, jei įmanoma, laikas).	neprivalomas
`document_number`	Asmens tapatybės duomenų teikėjo suteiktas asmens tapatybės duomenų numeris.	neprivalomas
`issuing_jurisdiction`	Asmens tapatybės duomenis suteikusios jurisdikcijos šalies smulkesnių administracinių vienetų kodas, nustatytas standarto ISO 3166-2:2020 8 punkte. Pirmoji kodo dalis turi sutapti su išdavusios šalies verte.	neprivalomas
`issuance_date`	Asmens tapatybės duomenų administracinio galiojimo laikotarpio pradžios data (ir, jei įmanoma, laikas).	neprivalomas

4) 4 skirsnis. Fizinio asmens tapatybės duomenų požymių kodavimas

— Fizinio asmens tapatybės duomenys išduodami pagal elektroniniams požymių liudijimams taikomus standartus, nustatytus Įgyvendinimo reglamento (ES) 2024/2979 II priedo 5 punkte (SD-JWT VC formatas) ir 6 punkte (ISO/IEC-mdoc formatas). 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3, 6.2.4 ir 6.2.5 punktai netaikomi.

— Fizinio asmens tapatybės duomenų kodavimas turi atitikti šio priedo 4.1 ir 4.2 skirsniuose pateiktas technines specifikacijas.

4.1. Fizinio asmens tapatybės duomenų kodavimas ISO/IEC-mdoc formatu

— Asmens tapatybės duomenų liudijimo tipas ISO/IEC mdoc formatu yra „eu.europa.ec.eudi.pid.1“. Šiame priede nustatytų asmens tapatybės duomenų požymių vardų srities identifikatorius yra „eu.europa.ec.eudi.pid.1“.

— Jei asmens tapatybės duomenys apima duomenis, kurių identifikatoriai nėra nustatyti šiame priede, šie duomenys apibrėžiami šalies asmens tapatybės duomenų vardų srityje, kurioje naudojamas bendrasis formatas eu.europa.ec.eudi.pid. [ISO 3166-1 alpha-2 šalies kodas arba ISO 3166-2 regiono kodas], o po jo gali būti dedamas taškas ir nurodomas versijos numeris.

— Jei naudojama vidaus vardų sritis, jos schema, įskaitant visus duomenų identifikatorius, jų apibrėžtis, naudojimą ir kodavimo formatus, skelbiama pagal Komisijos įgyvendinimo reglamento (ES) 2025/1569 ([1]) 8 straipsnį.

— Šio priedo 1 ir 3 skirsniuose nurodyti asmens tapatybės duomenys ir jų metaduomenys įtraukiami į asmens tapatybės duomenų elementus, kaip apibrėžta ISO/IEC mdoc formato specifikacijose.

— „MobileSecurityObject“ tipo egzemplioriaus naryje „deviceKeyInfo“ esančiame naryje „deviceKey“ patalpinamas viešasis raktas.

— Tas viešasis raktas turi atitikti privatųjį raktą, saugomą dėklės naudotojo saugiame dėklės šifravimo įrenginyje (WSCD).

— Į apsaugotą CB-AdES skaitmeninio parašo, kuriuo pasirašomi asmens tapatybės duomenys ISO/IEC-mdoc formatu, antraštę įtraukiami antraštės parametrai „x5u“ ir „x5t“, nustatyti RFC 9360 ([2]).

— Antraštės parametrui „x5t“ naudojamas maišos algoritmas yra SHA-256.

— Asmens tapatybės duomenų kodavimo ISO/IEC-mdoc formatu reikalavimai nustatyti 6 lentelėje.

6 lentelė

Asmens tapatybės duomenų kodavimo ISO/IEC-mdoc formatu reikalavimai

Duomenų identifikatorius	Požymio identifikatorius	Kodavimo formatas
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]) 2025 m. liepos 29 d. Komisijos įgyvendinimo reglamentas (ES) 2025/1569, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 nuostatų dėl kvalifikuotų elektroninių požymių liudijimų ir elektroninių požymių liudijimų, kuriuos teikia už autentišką šaltinį atsakinga viešojo sektoriaus įstaiga arba kurie teikiami jos vardu, taikymo taisyklės (OL L, 2025/1569, 2025 7 30, 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/).

Duomenų identifikatorius	Požymio identifikatorius	Kodavimo formatas
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate arba 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 arba full-date

— 6 lentelėje nurodytas požymių kodavimo formatas žymimas naudojant RFC 8610 ([3]) nustatytus atvaizdavimo tipus ir laikantis šių papildomų reikalavimų:

a) tstr koduojamas naudojant UTF-8;

b) tstr turi būti suderinamas su visu „Unicode“ intervalu;

c) tstr turi būti ne ilgesnis kaip 150 ženklų;

d) data koduojama taip, kaip nustatyta RFC 8943 ([4]);

e) visa data turi būti aiškinama kaip #6.1004(tstr), čia žymė „tag 1004“ yra tokia, kokia nustatyta RFC 8943;

f) požymis „tdate“ turi apimti datos ir laiko eilutę, kaip nustatyta RFC 3339 ([5]);

g) požymis „full-date“ turi apimti „full-date“ eilutę, kaip nustatyta RFC 3339, pagal RFC 8943;

h) datos pateikimas požymiuose, jei nenurodyta kitaip:

— nenaudoti sekundės dalių;

— nenaudoti vietos laiko skirtumo nuo UTC, o laiko skirtumą, nustatytą RFC 3339, žymėti raide Z;

i) pagrindinių tipų 0 ir 1 sveikasis skaičius turi būti kuo mažesnis, kaip nustatyta RFC 8949 ([6]) 4.2 skirsnyje;

j) elementas „place_of_birth“ turi apimti bent vieną iš šių rakto ir vertės porų: „country“, „region“ arba „locality“;

k) ilgio išraiška „bstr“, „tstr“, masyve arba atvaizdyje turi būti kuo trumpesnė, kaip nustatyta RFC 8949 4.2 skirsnyje;

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

l) požymis „nationality“ koduojamas kaip alpha-2 šalių kodų, nustatytų ISO 3166-1, masyvas. Kai naudojamas CDDL žymėjimas, kaip nustatyta RFC 8610, šis požymis koduojamas taip:

— nationalities = [+ CountryCode]

— CountryCode = tstr ; alpha-2 šalies kodas nustatytas ISO 3166-1;

— kai dėklės naudotojas, su kuriuo susiję asmens tapatybės duomenys, turi kelias pilietybes, o asmens tapatybės duomenų teikėjas šias kelias pilietybes paliudija, asmens tapatybės duomenų teikėjas į asmens tapatybės duomenis gali įtraukti visas pilietybes;

— požymis „place_of_birth“ koduojamas kaip tipas „place_of_birth“. Kai naudojamas CDDL žymėjimas, kaip nustatyta RFC 8610, šis požymis koduojamas taip:

place_of_birth =

{

? „country“: tstr ; vienas alpha-2 šalies kodas, nustatytas ISO 3166-1

? „region“: tstr ; valstijos, provincijos, rajono ar teritorinio vieneto pavadinimas

? „locality“: tstr ; savivaldybės, miesto ar kaimo pavadinimas

}

4.2. Asmens tapatybės duomenų kodavimo SD-JWT VC formatu reikalavimai

— Šiame skirsnyje nurodyti asmens tapatybės duomenys ir jų metaduomenys įtraukiami į asmens tapatybės duomenis kaip teiginiai, kaip apibrėžta SD-JWT VC formato specifikacijose.

— Visus teiginius, įtrauktus į išduotus asmens tapatybės duomenis, nurodytus ankstesnėje įtraukoje, turi būti galima pasirinktinai atskleisti individualiai, išskyrus teiginius, kurie SD-JWT VC formatu apibrėžiami kaip neatrankiai atskleidžiami teiginiai.

— 7 lentelėje nustatytas teiginių pavadinimų, kurie yra viešieji pavadinimai, kodavimas.

— 8 lentelėje nustatytas teiginių pavadinimų, kurie yra specifiniai asmens tapatybės duomenims, kodavimas.

— JSON eilutė, naudojama asmens tapatybės duomenims, užkoduotiems SD-JWT VC, koduojama naudojant UTF-8 ir turi palaikyti visą „Unicode“ intervalą, nebent 8 lentelėje arba joje pateiktose nuorodose aiškiai nustatyta kitaip.

— JWT teiginiai „nbf“ ir „exp“, kaip apibrėžta RFC 7419 ([7]), naudojami asmens tapatybės duomenų, atitinkančių SD-JWT VC formatą, techninio galiojimo laikotarpiui nurodyti.

([7]) J. Jones, et al., „JSON Web Token (JWT)“, RFC 7519, May 2015.

— Į asmens tapatybės duomenis įtraukiamas teiginys „cnf“, apibrėžtas RFC 7800 ([8]), t. y. viešasis raktas, sugeneruotas iš privačiojo rakto, saugomo dėklės naudotojo dėklės vieneto WSCD.

— Į apsaugotą skaitmeninio parašo, kuriuo pasirašomi asmens tapatybės duomenys SD-JWT VC formatu, antraštę įtraukiami antraštės parametrai „x5u“ ir „x5t#S256“, nustatyti RFC 7515 ([9]).

7 lentelė

Asmens tapatybės duomenų kodavimo SD-JWT VC formatu naudojant viešuosius pavadinimus reikalavimai

Duomenų identifikatorius	Požymio identifikatorius	Kodavimo formatas
`family_name`	`family_name`	eilutė
`given_name`	`given_name`	eilutė
`birth_date`	`birthdate`	eilutė, ISO 8601-1, MMMM-MM-DD formatas
`birth_place`	`place_of_birth`	JSON struktūra
`nationality`	`nationalities`	eilučių masyvas
`resident_address`	`address.formatted`	eilutė
`resident_country`	`address.country`	eilutė
`resident_state`	`address.region`	eilutė
`resident_city`	`address.locality`	eilutė
`resident_postal_code`	`address.postal_code`	eilutė
`resident_street`	`address.street_address`	eilutė
`family_name_birth`	`birth_family_name`	eilutė
`given_name_birth`	`birth_given_name`	eilutė
`email_address`	`email`	eilutė
`mobile_phone_number`	`phone_number`	eilutė
`portrait`	`picture`	eilutė; duomenų URL, kur yra „base64“ užkoduotas atvaizdas, kurio formatas JPEG

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

8 lentelė

Asmens tapatybės duomenų kodavimo SD-JWT VC formatu naudojant privačiuosius pavadinimus reikalavimai

Duomenų identifikatorius	Požymio identifikatorius	Kodavimo formatas
`expiry_date`	`date_of_expiry`	eilutė, ISO 8601-1, MMMM-MM-DD formatas
`issuance_date`	`date_of_issuance`	eilutė, ISO 8601-1, MMMM-MM-DD formatas
`personal_administrative_number`	`personal_administrative_number`	eilutė
`sex`	`sex`	skaičius
`issuing_authority`	`issuing_authority`	eilutė
`issuing_country`	`issuing_country`	eilutė
`document_number`	`document_number`	eilutė
`issuing_jurisdiction`	`issuing_jurisdiction`	eilutė

— Pagrindinis asmens tapatybės duomenų tipas yra „urn:eudi:pid:1“, įtrauktas į teiginį „vct“. Visuose asmens tapatybės duomenyse turi būti naudojami vardų srityje „urn:eudi:pid:“ nurodyti tipai.

— Jei asmens tapatybės duomenys apima šiame priede nenurodytus požymius, šie požymiai apibrėžiami pagal šalyje naudojamą tipą.

— Jei naudojamas šalies vidaus tipas, jo schema, įskaitant visus duomenų identifikatorius, jų apibrėžtis, naudojimą ir kodavimo formatus, nustatoma schemoje, kuri skelbiama pagal Įgyvendinimo reglamento (ES) 2025/1569 8 straipsnį.

5) 5 skirsnis. Patikimumo užtikrinimo infrastruktūros informacija

Asmens tapatybės duomenų teikėjų sąrašas, Komisijos pateiktas pagal Įgyvendinimo reglamentą (ES) 2024/2980, užtikrina galimybę nustatyti asmens tapatybės duomenų autentiškumą.“

II PRIEDAS

„Ia PRIEDAS

5a straipsnyje nurodyti šifravimo mechanizmai

Europos kibernetinio saugumo sertifikavimo grupės šifravimo klausimų pogrupis. „Agreed Cryptographic Mechanisms“ (suderintieji šifravimo mechanizmai), paskelbė Europos Sąjungos kibernetinio saugumo agentūra (ENISA) ([1]).“

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

III PRIEDAS

„Ib PRIEDAS

6 straipsnio 2a dalyje nurodytos dėklės vieneto liudijimų techninės specifikacijos

1) Dėklės vieneto liudijimą sudaro vienas ar daugiau dėklės egzemplioriaus liudijimų ir vienas ar daugiau rakto liudijimų.

2) Dėklės egzemplioriaus liudijimas ir rakto liudijimas turi atitikti šiuos reikalavimus:

a) Formato reikalavimai

— FR-WIA-1: dėklės egzemplioriaus liudijimas yra „JSON Web Token“ (JWT), kaip nustatyta RFC 7519 ([1]), patvirtintas dėklės teikėjo parašu arba spaudu naudojant kompaktišką JAdES bazinį B parašą.

— FR-WIA-1.1: dėklės egzemplioriaus liudijimas yra dėklės liudijimas, kaip nustatyta „OpenID“ E priedėlyje dėl patikrinamų kredencialų išdavimo v1.0 ([2]) (OID4VCI) ir išplėstas, kaip nurodyta toliau C-WIA-1 ir C-WIA-2 punktuose.

— FR-KA-1: rakto liudijimas yra JWT, kaip nustatyta RFC 7519, patvirtintas dėklės teikėjo parašu arba spaudu naudojant kompaktišką JAdES bazinį B parašą.

— FR_KA_1.1: rakto liudijimas yra OID4VCI D priedėlyje nustatytas rakto liudijimas, išplėstas, kaip nustatyta toliau C_KA-1 ir C_KA-2 punktuose.

b) Perdavimo reikalavimai

— TR-WIA-1: dėklės vienetas, išduodamas asmens tapatybės duomenis, kvalifikuotus arba nekvalifikuotus elektroninius požymių liudijimus arba elektroninius požymių liudijimus, kuriuos teikia už autentišką šaltinį atsakinga viešojo sektoriaus įstaiga arba kurie teikiami jos vardu, naudoja dėklės egzemplioriaus liudijimą.

— TR-WIA-2: dėklės teikėjas patikrina dėklės egzemplioriaus vientisumą ir pasirašo arba antspauduoja dėklės egzemplioriaus liudijimą.

— TR-WIA-2.1: jei dėklės teikėjas išduoda dėklės egzemplioriaus liudijimą, laiko, kada dėklės teikėjas patikrina dėklės egzemplioriaus vientisumą, ir laiko, kurį jis nurodys išduoto dėklės egzemplioriaus liudijimo antraštės parametre „exp“, skirtumas turi būti mažesnis nei 24 valandos.

— TR-WIA-2.2: dėklės teikėjas užtikrina, kad dėklės vienete būtų dėklės egzemplioriaus liudijimai, reikalingi asmens tapatybės duomenims ir elektroniniams požymių liudijimams išduoti.

— TR-WIA-3: išdavimo metu dėklės vienetas siunčia dėklės egzemplioriaus liudijimą autorizavimo serveriui stūmos būdu siunčiamoje leidimo užklausoje ir prieigos rakto užklausoje, kaip nustatyta OID4VCI.

— TR-WIA-3.1: dėklės vienetas siunčia dėklės egzemplioriaus liudijimą kartu su turėjimo įrodymu („PoP“), kaip nustatyta OID4VCI E priedėlyje.

— TR-WIA-3.2: dėklės vienetas siunčia tą patį dėklės egzemplioriaus liudijimą ne daugiau kaip vienam autorizavimo serveriui.

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

— TR-WIA-3.2.1: kai dėklės teikėjas naudojasi toliau punkte R_WIA_1 nurodyta parinktimi „per-issuer reuse“, dėklės vienetas gali siųsti dėklės egzemplioriaus liudijimą tam pačiam autorizavimo serveriui kelis kartus.

— TR-WIA-3.2.2: kai dėklės teikėjas nesinaudoja parinktimi „per-issuer reuse“, dėklės vienetas dėklės egzemplioriaus liudijimą panaudoja ne daugiau kaip per vieną išdavimo procesą.

— TR-WIA-4: kai autorizavimo serveris gauna dėklės egzemplioriaus liudijimą, jis patikrina dėklės egzemplioriaus liudijimo parašą naudodamas pasirašymo sertifikato viešąjį raktą, įtrauktą į dėklės egzemplioriaus liudijimo JOSE antraštės parametrą „x5c“.

— TR-WIA-4.1: autorizavimo serveris taip pat patikrina, ar šį pasirašymo sertifikatą galima patikrinti naudojantis patikimumo užtikrinimo priemone, įtraukta į dėklės teikėjų sąrašą, nurodytą Įgyvendinimo reglamento (ES) 2024/2980 5 straipsnyje, galbūt naudodamas tarpinius sertifikatus, įtrauktus į parametrą x5c.

— TR-WIA-4.2: autorizavimo serveris patikrina, ar dėklės egzemplioriaus liudijimo galiojimas nėra pasibaigęs.

— TR-WIA-4.3: autorizavimo serveris patikrina PoP parašą pagal viešąjį raktą, esantį teiginyje „cnf“.

— TR_KA-1: dėklės vienetas, išduodamas asmens tapatybės duomenis, taip pat išduodamas su įrenginiu susietus kvalifikuotus arba nekvalifikuotus elektroninius požymių liudijimus arba elektroninius požymių liudijimus, kuriuos teikia už autentišką šaltinį atsakinga viešojo sektoriaus įstaiga arba kurie teikiami jos vardu, naudoja rakto liudijimą.

— TR_KA-1.1: dėklės vienetas, išduodamas su įrenginiu nesusietus kvalifikuotus arba nekvalifikuotus elektroninius požymių liudijimus arba elektroninius požymių liudijimus, kuriuos teikia už autentišką šaltinį atsakinga viešojo sektoriaus įstaiga arba kurie teikiami jos vardu, rakto liudijimo nenaudoja.

— TR_KA-2: dėklės teikėjas dėklės vienetui pateikia skirtingus dėklės vieneto WSCD ir kiekvienos jo raktų saugyklos raktų liudijimus.

— TR_KA-2.1: dėklės teikėjas pasirašo arba antspauduoja rakto liudijimą po to, kai patikrina, kad rakto liudijime patvirtinti raktai yra saugomi dėklės vieneto WSCD arba raktų saugykloje, aprašytuose rakto liudijime.

— TR_KA-2.2: rakto liudijime turi būti bent vienas paliudytas viešasis raktas. Kredencialų išdavėjui siunčiamame rakto liudijime esančių raktų skaičius turėtų neviršyti to kredencialų išdavėjo metaduomenyse nustatyto maksimalaus partijos dydžio; žr. ETSI TS 119 472-3 ([3]), parametrą „credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size“.

— TR_KA-2.3: dėklės teikėjas įtraukia viešąjį raktą (atitinkantį privatųjį raktą, saugomą dėklės vieneto WSCD arba raktų saugykloje) ne daugiau kaip į vieną rakto liudijimą.

— TR_KA-2.4: dėklės vienetas naudoja rakto liudijimą ne daugiau kaip per vieną kredencialų išdavimo arba pakartotinio išdavimo procesą.

— TR_KA-2.5: dėklės teikėjas užtikrina, kad dėklės vienetas turėtų raktų liudijimus, reikalingus asmens tapatybės duomenims ir su įrenginiu susietiems elektroniniams požymių liudijimams išduoti.

([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, March 2026.

— TR_KA-3: kai reikia išdavimo metu, dėklės vienetas įtraukia rakto liudijimą į kredencialų išdavėjui siunčiamos kredencialų užklausos laukelį „proofs“, kaip nustatyta OID4VCI, į „jwt“ arba „attestation“ tipo įrodymą.

— TR_KA_3.1: kai dėklės vienetas įtraukia rakto liudijimą į „jwt“ elementą, jis rakto liudijimą pasirašo naudodamas privatųjį raktą, atitinkantį viešąjį raktą ties 0 indeksu masyve „attested_keys“, kuris yra objekte „key_attestation“.

— TR_KA-4: kai kredencialų išdavėjas išduoda su įrenginiu susietus kredencialus, jis parametre „proof_types_supported“ savo išdavėjo kredencialų metaduomenyse nurodo, kaip nustatyta OID4VCI 12.2.4 skirsnyje, kad jie suderinami ir su „jwt“, ir su „attestation“ tipų įrodymais, raktų liudijimams, į kuriuos įtraukiamas objektas „key_attestations_required“.

— TR_KA-4.1: kai kredencialų išdavėjas išduoda su įrenginiu nesusietus kredencialus, jis kredencialų išdavėjo metaduomenyse praleidžia parametrus „proof_types_supported“ ir „cryptographic_binding_methods_supported“.

— TR_KA-5: kai kredencialų išdavėjas gauna rakto liudijimą kaip „jwt“ arba „attestation“ tipo įrodymą, jis patikrina rakto liudijimo parašą pagal viešąjį raktą, įtrauktą į pasirašymo sertifikatą kaip „x5c“ parametrą rakto liudijimo JOSE antraštėje, ir tai, ar šis pasirašymo sertifikatas susietas su patikimumo užtikrinimo priemone dėklių teikėjų sąraše, nurodytame Įgyvendinimo reglamento (ES) 2024/2980 5 straipsnyje, galbūt naudodamas tarpinius sertifikatus, įtrauktus į „x5c“ parametrą.

— TR_KA-6: kai kredencialų išdavėjas gauna rakto liudijimą kaip „jwt“ tipo įrodymą, jis patikrina „jwt“ elemento parašą ties 0 indeksu masyve „attested_keys“, kuris yra objekte „key_attestation“, įtrauktame į „jwt“ elementą.

— TR_KA-6.1: kredencialų išdavėjas patikrina, ar į elemento „jwt“ lauką „nonce“ įtrauktas galiojantis „c_nonce“ iš jų „nonce_endpoint“, kaip nustatyta OID4VCI.

— TR_KA-7: kai kredencialų išdavėjas gauna rakto liudijimą kaip „attestation“ tipo įrodymą, jis patikrina, ar į objektą „key_attestation“ įtrauktas galiojantis „c_nonce“ iš jų „nonce_endpoint“.

— TR_KA-8: asmens tapatybės duomenų teikėjas užtikrina, kad asmens tapatybės duomenys būtų susieti su viešuoju raktu, kurio kilmė yra rakto liudijimas, kuriame nurodytas WSCD.

c) Turinio reikalavimai

— C_WIA-1: į dėklės egzemplioriaus liudijimą įtraukiami šie dalykai:

— teiginys „wallet_name“, nustatytas OID4VCI E priedėlyje, kurio vertė yra dėklės sprendinio identifikatorius, kurį galima rasti dėklės teikėjų sąraše, nurodytame Įgyvendinimo reglamento (ES) 2024/2980 5 straipsnyje;

— teiginys „wallet_version“ ([4]), t. y. eilutė, kurios vertė yra dėklės sprendinio versija;

— teiginys „wallet_solution_certification_information“, kuris yra JSON objektas, kuriame yra informacija apie dėklės sprendinį sertifikavusią atitikties vertinimo įstaigą, sertifikato numeris, jei taikytina, taip pat kita aktuali sertifikavimo informacija;

([4]) Šis teiginys apibrėžtas šiame Komisijos įgyvendinimo reglamente, nes jis nėra OID4VCI specifikacijos dalis.

— teiginys „client_status“, kurį sudaro du polaukiai:

— „status“: OID4VCI E priedėlyje nustatyta statuso sąrašo nuoroda, rodanti dėklės egzemplioriaus atšaukimo statusą. Išsamesnę informaciją žr. e skirsnyje toliau;

— „exp“: „NumericDate“, kaip nustatyta RFC 7519, nurodant laiką, iki kurio dėklės teikėjas išlaikys atšaukimo statusą lauke „status“ nurodytoje statuso sąrašo rodyklėje;

— teiginys „exp“, nustatytas OID4VCI E priedėlyje.

— PASTABA. Teiginys „client_status.status“ dėklės egzemplioriaus liudijime rodo dėklės egzemplioriaus statusą, o ne paties liudijimo atšaukimo statusą. Kaip aprašyta toliau R_WIA-1 punkte, dėklės teikėjas gali nuspręsti kiekvieno dėklės egzemplioriaus liudijimo taikymo sritį susieti su konkrečiu autorizavimo serveriu, atsižvelgiant į tai, kad visų tam serveriui siunčiamų liudijimų įraše „client_status.status“ yra ta pati rodyklės vertė.

— PASTABA. Parametro „idx“ vertė teiginyje „status“ gali būti naudojama kaip unikalus dėklės egzemplioriaus ir dėklės vieneto identifikatorius (poromis).

— C_WIA-2: į dėklės egzemplioriaus liudijimą turėtų būti įtrauktas ir teiginys „wallet_link“, nustatytas OID4VCI E priedėlyje, ir šio teiginio vertė turi būti URI, kur galima gauti išsamesnę informaciją apie dėklės sprendinį.

— C_WIA-3: autorizavimo serveris parametro „exp“ aukščiausiame dėklės egzemplioriaus liudijimo lygmenyje neturi interpretuoti kaip dėklės egzemplioriaus atšaukimo išlaikymo laikotarpio pabaigos.

— PASTABA. Parametras „exp“ aukščiausiame dėklės egzemplioriaus liudijimo lygmenyje rodo, kada baigiasi paties liudijimo galiojimas.

— C_KA-1: į rakto liudijimą įtraukiama:

— teiginiai „key_storage“ ir „user_authentication“, nustatyti OID4VCI D priedėlyje;

— požymių „key_storage“ ir „user_authentication“ vertė yra „iso_18045_high“, kai rakto liudijime paminėtas WSCD;

— teiginys „certification“, nustatytas OID4VCI D priedėlyje, į kurį įtraukiamas URL, kur galima gauti informaciją apie sertifikavimą, kurį užtikrina WSCD arba raktų saugykla, nurodant schemą, kaip antai „Common Criteria“ ar „GlobalPlatform“, reikalavimus, pagal kuriuos vertinta, kaip antai taikytiną apsaugos profilį, ir įvertinimo lygį;

— iš šios informacijos turi būti galima nustatyti, ar raktų saugykla yra WSCD;

— teiginys „key_storage_status“, kurį sudaro du polaukiai:

— „status“: statuso sąrašo nuoroda, kaip nustatyta OID4VCI D.1 priedėlyje. Vertė nurodo arba WSCD atšaukimo statusą arba raktų saugyklos, naudojamos paliudytiems raktams saugoti, tipą, arba – kai naudojama rodyklės parinktis „per-key-attestation“ – atskiro dėklės vieneto WSCD arba raktų saugyklos atšaukimo statusą. Galimas rodyklės priskyrimo parinktis žr. R_KA_1 punkte toliau;

— „exp“: „NumericDate“, kaip nustatyta RFC 7519, nurodant laiką, iki kurio dėklės teikėjas išlaikys atšaukimo statusą lauke „status“ nurodytoje statuso sąrašo rodyklėje;

— teiginys „exp“, nustatytas OID4VCI D priedėlyje.

— PASTABA dėl „idx“ vertės teiginyje „key_storage_status.status“ rakto liudijime. Kai dėklės teikėjas naudoja parinktį „type-shared index“ (žr. R_KA_1 toliau), visų to paties tipo WSCD ar raktų saugyklos raktų liudijimų statuso sąrašo rodyklė yra ta pati. Todėl kiekvieno dėklės vieneto „idx“ vertė nėra unikali. Priešingai, kai dėklės teikėjas naudoja parinktį „per-key-attestation index“, kiekvieno dėklės vieneto „idx“ vertė yra unikali (arba unikali pora kiekvienam kredencialų išdavėjui). Tačiau visais atvejais kredencialų išdavėjas nenaudoja „idx“ vertės rakto liudijime kaip dėklės vieneto identifikatoriaus, o vietoj to naudoja „idx“ vertę dėklės egzemplioriaus liudijime.

— C_KA-2: kai rakto liudijimas siunčiamas kaip „attestation“ tipo įrodymas, į jį įtraukiamas ir galiojantis „c_nonce“, kaip nustatyta OID4VCI F.3 priedėlyje.

— C_KA-3: kredencialų išdavėjas parametro „exp“ aukščiausiame rakto liudijimo lygmenyje neturi interpretuoti kaip WSCD ar raktų saugyklos atšaukimo išlaikymo laikotarpio pabaigos.

— PASTABA. Parametras „exp“ aukščiausiame rakto liudijimo lygmenyje rodo, kada baigiasi paties rakto liudijimo galiojimas.

d) Gyvavimo ciklo reikalavimai

— Šiame priede nustatomi šie kredencialų išdavėjo metaduomenų parametrai:

— „preferred_client_status_period“: NEPRIVALOMAS. Sveikasis skaičius, nurodantis pageidaujamą likusį dėklės egzemplioriaus liudijimo, kurį dėklės vienetas turi pateikti išdavimo metu, statuso išlaikymo laikotarpį (sekundėmis). Likęs statuso išlaikymo laikotarpis apibrėžiamas kaip „client_status.exp“ vertė liudijime, atėmus liudijimo gavimo laiką.

— „preferred_key_storage_status_period“: NEPRIVALOMAS. Sveikasis skaičius, nurodantis pageidaujamą likusį rakto liudijimo, kurį dėklės vienetas turi pateikti išdavimo metu, statuso išlaikymo laikotarpį (sekundėmis). Likęs statuso išlaikymo laikotarpis apibrėžiamas kaip „key_storage_status.exp“ vertė liudijime, atėmus liudijimo gavimo laiką.

— LC_WIA-1: autorizavimo serveris gali pranešti savo pageidavimus dėl likusio statuso išlaikymo laikotarpio dėklės egzemplioriaus liudijimuose, įtraukdamas metaduomenų parametrą „preferred_client_status_period“ į savo kredencialų išdavėjo metaduomenų galutinį tašką, kaip nustatyta OID4VCI 12.2.2 skirsnyje.

— LC_WIA-1.1: šis laukas įtraukiamas aukščiausiame kredencialų išdavėjo metaduomenų lygmenyje.

— LC_WIA_2: autorizavimo serveris parametro „exp“ aukščiausiame dėklės egzemplioriaus liudijimo lygmenyje neturi interpretuoti kaip dėklės egzemplioriaus atšaukimo išlaikymo laikotarpio pabaigos.

— LC_WIA_3: kai dėklės teikėjas pasirašo arba antspauduoja dėklės egzemplioriaus liudijimą, jis išlaiko atitinkamo dėklės egzemplioriaus atšaukimo statusą tol, kol praeina tame dėklės egzemplioriuje nurodytas „wallet_instance_status.exp“.

— LC_KA-1: kai reikia rakto liudijimo, kredencialų išdavėjas gali pranešti savo pageidavimus dėl likusio statuso išlaikymo laikotarpio raktų liudijimuose, įtraukdamas pirmiau nustatytą metaduomenų parametrą „preferred_key_storage_status_period“ į savo kredencialų išdavėjo metaduomenų galutinį tašką, kaip nustatyta OID4VCI 12.2.2 skirsnyje.

— LC_KA-1.1: šis laukas įtraukiamas į objektą „key_attestations_required“, kaip nustatyta OID4VCI 12.2.4 skirsnyje.

— LC_KA-2: dėklės teikėjas pasirenka savo išduodamų raktų liudijimų techninio galiojimo laikotarpį.

— LC_KA-3: kai dėklės teikėjas pasirašo arba antspauduoja rakto liudijimą, jis išlaiko atitinkamo WSCD ar raktų saugyklos atšaukimo statusą tol, kol praeina tame rakto liudijime nurodytas „key_storage_status.exp“.

— LC_GEN-1: dėklės teikėjas užtikrina, kad dėklės vienetas galėtų visada pateikti dėklės vieneto liudijimus ir raktų liudijimus, kurių „client_status.exp“ ir „key_storage_status.exp“ (atitinkamai) yra bent 31 diena ateityje pateikimo autorizavimo serveriui ar kredencialų išdavėjui metu.

— *PASTABA*. Taip užtikrinama, kad asmens tapatybės duomenų teikėjai galėtų pasikliauti atšaukimo grandine ir nebūtų priversti išduoti trumpo galiojimo asmens tapatybės duomenų.

— LC_GEN-2: dėklės teikėjas užtikrina, kad dėklės vienetas išdavimo metu pasiimtų kredencialų išdavėjo metaduomenis.

  — LC_GEN_2.1: jei į šiuos metaduomenis yra įtrauktas laukas „preferred_key_storage_status_period“, dėklės vienetas siunčia rakto liudijimą su („key_storage_status.exp“ – dabartinis laikas) – „preferred_key_storage_status_period“ – jis turi būti kuo trumpesnis, bet ne neigiamas. Jei tokio dėklės vienetui prieinamo rakto liudijimo nėra, jis iš dėklės teikėjo gauna naują rakto liudijimą, kuris tenkina „key_storage_status.exp“ – dabartinis laikas ≥ „preferred_key_storage_status_period“ sąlygą.

  — LC_GEN_2.2: jei į šiuos metaduomenis yra įtrauktas laukas „preferred_client_status_period“, dėklės vienetas siunčia dėklės egzemplioriaus liudijimą su („client_status.exp“ – dabartinis laikas) – „preferred_client_status_period“ – jis turi būti kuo trumpesnis, bet ne neigiamas. Jei tokio dėklės vienetui prieinamo dėklės egzemplioriaus liudijimo nėra, jis iš dėklės teikėjo pareikalauja naujo dėklės egzemplioriaus liudijimo, kuris tenkina „client_status.exp“ – dabartinis laikas ≥ „preferred_client_status_period“ sąlygą.

— LC_GEN-3: techninis asmens tapatybės duomenų galiojimo laikotarpis baigiasi tiek prieš dėklės egzemplioriaus liudijimo „client_status.exp“, tiek prieš rakto liudijimo, vykdant išdavimo procesą nusiųsto asmens tapatybės duomenų teikėjui, „key_storage_status.exp“.

— LC_GEN-4: asmens tapatybės duomenų, kurių techninio galiojimo laikotarpis yra ilgesnis nei 24 valandos, teikėjas asmens tapatybės duomenų techninio galiojimo laikotarpiu bent kartą per 24 valandas tikrina dėklės egzemplioriaus liudijimo ir rakto liudijimo, gautų išdavimo metu, atšaukimo statusą. Jei kuris nors iš jų atšaukiamas, teikėjas atšaukia asmens tapatybės duomenis.

e) Atšaukimo reikalavimai

— R_GEN-1: dėklės teikėjas naudoja prieigos rakto statuso sąrašus (nustatytus IETF prieigos raktų sąrašo parametru) kaip raktų liudijimų ir dėklės egzemplioriaus liudijimų atšaukimo mechanizmą, kaip nustatyta OID4VCI atitinkamai D ir E priedėliuose.

— PASTABA. Siekdamas pagerinti savo statuso sąrašų išplečiamumą, dėklės teikėjas gali naudoti šiuos optimizavimo būdus:

  — suskaidyti statuso sąrašą į kelias dalis, jei dėklės teikėjas turi daug naudotojų ir yra išdavęs daug liudijimų. Yra daug skaidymo į dalis strategijų, pvz., remiantis fiksuotu dydžiu arba laikotarpiu. Skaidymo į dalis strategiją dėklės teikėjas renkasi savo nuožiūra. Motyvai gali apimti statuso sąrašo, kurį reikia atsisiųsti, dydį ir naudotojo privatumą;

  — turėti kelis statuso sąrašus;

  — suglaudinti statuso sąrašą, kad sumažėtų jo dydis.

— R_WIA-1: dėklės teikėjas gali priskirti tą pačią vertę teiginiui „idx“ teiginyje „client_status.status“ visuose dėklės egzemplioriaus liudijimuose, kuriuos tam tikras dėklės vienetas pateikia tam pačiam autorizavimo serveriui. Tai vadinama parinktimi „per-issuer reuse“. Jei naudojama ši parinktis:

  — R_WIA-1.1: dėklės vienetas įsimena, kurią rodyklės vertę naudojo kiekvienam autorizavimo serveriui, į kurį kreipėsi anksčiau, ir, pakartotinai sąveikaudamas su tuo pačiu autorizavimo serveriu, pareikalauja dėklės egzemplioriaus liudijimo, kuriame yra ta pati rodyklės vertė;

  — R_WIA-1.2: kai dėklės teikėjas gauna prašymą išduoti dėklės egzemplioriaus liudijimą su konkrečia rodyklės verte, prieš išduodamas naują dėklės egzemplioriaus liudijimą su ta rodyklės verte, jis patikrina, ar prašantysis dėklės vienetas yra gavęs tą rodyklės vertę anksčiau;

  — R_WIA-1.3: dėklės vienetas sąveikai su skirtingais autorizavimo serveriais nenaudoja tos pačios rodyklės vertės.

— PASTABA. Jei naudojama parinktis „per-issuer reuse“, dėklės teikėjas galės nustatyti, su kiek autorizavimo serverių dėklės vienetas sąveikavo ir kaip dažnai jis sąveikauja su kiekvienu iš jų.

— R_WIA-2: savo privatumo politikoje dėklės teikėjas nurodo, ar jis naudoja parinktį „per-issuer reuse“ dėklės egzemplioriams atšaukti.

— R_WIA-3: kai dėklės teikėjas nenaudoja parinkties „per-issuer reuse“, jis kiekvienam savo išduodamam dėklės egzemplioriaus liudijimui priskiria naują nesusiejamą rodyklės vertę.

— R_WIA-4: kai dėklės vienetą būtina atšaukti, dėklės teikėjas atšaukia rodyklės vertes teiginyje „client_status.status“ visuose su tuo dėklės vienetu susijusiuose dėklės egzemplioriaus liudijimuose.

— R_WIA-5: nustatydamas dėklės egzemplioriaus liudijimų statuso sąrašų dydį, dėklės teikėjas atsižvelgia į savo diegimo mastą ir pagrindinę architektūrą, užtikrindamas, kad jie būtų pakankamai dideli, kad būtų išvengta koreliacijos ir apsaugotas naudotojų privatumas. Jei įmanoma, statuso sąrašas turėtų būti siejamas bent su 10 000 liudijimų.

— R_KA_1: dėklės teikėjas teiginiui „key_storage_status.status“ rakto liudijime pasirenka vieną iš šių rodyklės priskyrimo parinkčių:

  — 1 parinktis, vadinama „type-shared index“, pagal kurią visuose raktų liudijimuose, kuriais liudijami raktai, saugomi to paties tipo WSCD arba raktų saugykloje, teiginyje „key_storage_status.status“ nurodyta ta pati rodyklės vertė;

  — 2 parinktis, vadinama „per-key-attestation index“, pagal kurią rakto liudijime, kuriuo liudijami raktai, saugomi atskirame WSCD arba raktų saugykloje, teiginyje „key_storage_status.status“ nurodyta unikali rodyklės vertė (poromis).

— PASTABA. Kai dėklės teikėjas naudoja 1 parinktį, vienu atšaukimo veiksmu visi paveikto tipo raktų liudijimai visuose dėklės vienetuose tampa negaliojantys. Be to, kadangi visiems to paties tipo WSCD ar raktų saugyklos raktų liudijimams priskirta ta pati statuso sąrašo rodyklė, raktų liudijimų statuso sąrašo įrašų skaičius rodo dėklės teikėjo palaikomų WSCD ar raktų saugyklų tipų skaičių, o ne įdiegtų dėklės vienetų skaičių. Todėl privatumo motyvas, kuriuo grindžiamas minimalus dėklės egzemplioriaus statuso sąrašų dydis, negalioja raktų liudijimų statuso sąrašams naudojant 1 parinktį, su sąlyga, kad yra pakankamas skaičius dėklės vienetų, kuriuose naudojami to paties tipo WSCD arba raktų saugyklos.

— PASTABA. Kai dėklės teikėjas naudoja 2 parinktį, kiekviena rodyklė atitinka tame rakto liudijime liudijamo konkretaus WSCD arba raktų saugyklos atšaukimo statusą.

— PASTABA. Kai dėklės teikėjas naudoja 2 parinktį, konkretus WSCD arba raktų saugykla gali būti atšaukti naudotojo prašymu.

— R_KA-2: kai dėklės teikėjas naudoja 2 parinktį, jis gali pasirinktinai naudoti parinktį „per-issuer reuse“, aprašytą R_WIA-1 punkte. Jei dėklės teikėjas naudoja šią parinktį, *mutatis mutandis* taikomi R_WIA-1 – R_WIA-3 reikalavimai.

— R_KA-3: kai dėklės teikėjas naudoja 2 parinktį, nustatydamas raktų liudijimų statuso sąrašų dydį, dėklės teikėjas atsižvelgia į savo diegimo mastą ir pagrindinę architektūrą, užtikrindamas, kad jie būtų pakankamai dideli, kad būtų išvengta koreliacijos ir apsaugotas naudotojų privatumas. Jei įmanoma, statuso sąrašas turėtų būti siejamas bent su 10 000 raktų liudijimų.

— R_KA-4: kai dėklės teikėjas naudoja 1 parinktį (tipui bendra rodyklė), jis įrašą „key_storage_status.status“ atšaukia tik tuo atveju, jei esama WSCD arba raktų saugyklos tipo saugumo pažeidžiamumo.

f) Parašo algoritmų reikalavimai

— SA-1: dėklės egzemplioriaus liudijimams, raktų liudijimams, susijusiems turėjimo įrodymams ir prieigos raktų statuso sąrašams pasirašyti naudojamas vienas iš šių algoritmų:

— ES256 (ECDSA su SHA-256 ir P-256);

— ES384 (ECDSA su SHA-384 ir P-384);

— ES512 (ECDSA su SHA-512 ir P-521).

— SA-2: dėklės teikėjas pasirenka, kurį iš SA-1 punkte nurodytų algoritmų jis naudos.

— SA-3: kredencialų išdavėjo autorizavimo serveris (kaip nustatyta OID4VCI) turi būti suderinamas su visais SA-1 punkte nurodytais algoritmais.“

IV PRIEDAS

„II PRIEDAS

8 straipsnyje nurodytų standartų sąrašas

Taikomos standarto ETSI TS 119 472-1 V1.2.1 (2026-02) 2–6 punktuose nustatytos techninės specifikacijos. Jos pritaikomos taip:

1) 2.1. Normative references (norminės nuorodos)

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

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

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

2) 4.2.11.1. General requirements (bendrieji reikalavimai)

— EAA-4.2.11.1-06: kai asmens tapatybės duomenims, kvalifikuotiems elektroniniams požymių liudijimams arba elektroniniams požymių liudijimams, kuriuos teikia už autentišką šaltinį atsakinga viešojo sektoriaus įstaiga arba kurie teikiami jos vardu, naudojamas statuso elementas, jame nurodoma tik tai, ar liudijimas atšaukiamas, ar ne, ir negali būti naudojamos jokios kitos statuso vertės, kaip antai galiojimo sustabdymas.

— EAA-4.2.11.1-06.1: kai liudijimas atšaukiamas, jis atšaukiamas visam laikui.

3) 4.2.13. EAA short-lived (trumpo galiojimo EAA)

— EAA-4.2.13-03: kai išduodami trumpo galiojimo elektroniniai požymių liudijimai, kurių galiojimo laikotarpis ne ilgesnis kaip 24 valandos, atšaukimo nereikalaujama.

4) 4.6.3. Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA) (ES EAA, kuriuos išduoda už autentišką šaltinį atsakinga viešojo sektoriaus įstaiga arba kurie išduodami jos vardu, reikalavimai)

— PuB-EAA-4.6.2-03: negalioja.

— PuB-EAA-4.6.2-04: negalioja.

— PuB-EAA-4.6.3-03: Į PuB-EAA skaitmeninį parašą įtraukiamas kvalifikuotas sertifikatas, suderinamas su PuB-EAA skaitmeniniu parašu.

— PuB-EAA-4.6.3-04: Kvalifikuotas sertifikatas, suderinamas su PuB-EAA skaitmeniniu parašu, turi atitikti ETSI TS 119 412-6 v1.1.1 8 punkto reikalavimus ir jame turi būti „QcType qcStatement“, apibrėžtas ETSI EN 319 412-5 v2.5.1, kurio vertė „id-etsi-qct-eidaspsbeaa“ apibrėžiama taip:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } – 45f straipsnio 1 dalies b punkte nurodytas sertifikatas, suderinamas su Reglamento (ES) Nr. 910/2014 3 straipsnio 46 punkte nurodytu viešojo sektoriaus įstaigos kvalifikuotu elektroniniu parašu arba kvalifikuotu elektroniniu spaudu.

5) 5.2.10.1. General requirements (bendrieji reikalavimai)

— EAA-5.2.10.1-04: negalioja.

— EAA-5.2.10.1-05: negalioja.

— EAA-5.2.10.1-06: Naryje „status“ gali būti narys „status_list“, kaip nustatyta IETF draft-ietf-oauth-status-list-20 [25] 6.2 punkte.

— EAA-5.2.10.1-07: negalioja.

— EAA-5.2.10.1-08: negalioja.

— EAA-5.2.10.1-09: negalioja.

— EAA-5.2.10.1-10: negalioja.

— EAA-5.2.10.1-11: negalioja.

— EAA-5.2.10.1-12: negalioja.

6) 6.2.10.1. General requirements (bendrieji reikalavimai)

— EAA-6.2.10.1-01: kai elektroniniam požymių liudijimui, suderinamam su ISO/IEC mdoc, naudojamas liudijimo statuso sąrašo mechanizmas, nustatytas EAA-6.2.10.1-02.2, arba liudijimų atšaukimo sąrašo mechanizmas, nustatytas EAA-6.2.10.1-02.3, jo mobiliajame saugumo objekte (MSO) turi būti statuso struktūra, nustatyta EAA-6.2.10.1-17, kurioje nurodoma MSO atšaukimo informacija.

— EAA-6.2.10.1-01.1: kai įgyvendinamas identifikatorių sąrašo mechanizmas, elemente „status“ turi būti elementas „identifier_list“, kaip nustatyta EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: kai įgyvendinamas statuso sąrašo mechanizmas, elemente „status“ turi būti elementas „status_list“, kaip nustatyta EAA-6.2.10.1-13.

— *PASTABA*.

  — Statuso struktūroje pateikiama nuoroda į MSO atšaukimų sąrašą.

  — MSO atšaukimų sąrašas yra struktūra „COSE_Sign1“, kuria nurodoma, ar konkretus MSO yra atšauktas, ar ne.

  — Statuso struktūroje pateikiama visa informacija, būtina dėklės pasikliaujančiajai šaliai, kad ji galėtų nustatyti, ar MSO atšaukimų sąrašas yra autentiškas.

— EAA-6.2.10.1-02: asmens tapatybės duomenų teikėjas, kvalifikuotų elektroninių požymių liudijimų teikėjas arba elektroninių požymių liudijimų, kuriuos teikia už autentišką šaltinį atsakinga viešojo sektoriaus įstaiga arba kurie teikiami jos vardu, teikėjas taiko vieną iš šių asmens tapatybės duomenų, kvalifikuotų elektroninių požymių liudijimų arba elektroninių požymių liudijimų, kuriuos teikia už autentišką šaltinį atsakinga viešojo sektoriaus įstaiga arba kurie teikiami jos vardu, atšaukimo metodų:

— EAA-6.2.10.1-02.1: kai jie išduoda trumpo galiojimo elektroninius požymių liudijimus, kurių galiojimo laikotarpis ne ilgesnis kaip 24 valandos, atšaukimo nereikalaujama;

— EAA-6.2.10.1-02.2: naudojamas liudijimų statuso sąrašo mechanizmas atšaukimo informacijai užkoduoti kaip statuso sąrašui;

— EAA-6.2.10.1-02.2.1: statuso sąrašo mechanizmu MSO atšaukiamas remiantis tuo, ar statuso sąraše išdavėjo nustatytoje MSO pozicijoje bito vertė yra „true“;

— EAA-6.2.10.1-02.2.2: statuso sąrašo mechanizmas nustatytas prieigos raktų statuso sąrašo (draft-ietf-oauth-status-list-20) specifikacijoje;

— EAA-6.2.10.1-02.3: naudojamas liudijimų atšaukimo sąrašo mechanizmas atšaukimo informacijai užkoduoti kaip identifikatorių sąrašui;

— EAA-6.2.10.1-02.3.1: identifikatorių sąrašo mechanizmu MSO atšaukiamas remiantis tuo, ar statuso sąraše išdavėjo nustatytas MSO identifikatorius yra identifikatorių sąraše;

— 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 ir EAA-6.2.10.1-11 nustatytas identifikatorių sąrašo mechanizmas, grindžiamas prieigos raktų statuso sąrašo specifikacijos reikalavimais, įskaitant bendrus statuso sąrašo ir identifikatorių sąrašo mechanizmų dalykus.

— EAA-6.2.10.1-03: kai asmens tapatybės duomenims, kvalifikuotiems elektroniniams požymių liudijimams arba elektroniniams požymių liudijimams, kuriuos teikia už autentišką šaltinį atsakinga viešojo sektoriaus įstaiga arba kurie teikiami jos vardu, naudojamas statuso elementas, nurodomas tik statusas „revoked“.

— EAA-6.2.10.1-03.1: statuso sąraše tai reiškia, kad gali būti naudojamos tik vertės „valid“ ir „invalid“, kaip nustatyta prieigos raktų statuso sąrašo specifikacijoje.

— EAA-6.2.10.1-03.2: identifikatorių sąraše nurodomi tik atšaukti MSO, o ne MSO, kurių galiojimas laikinai sustabdytas.

— EAA-6.2.10.1-04: kai MSO atšaukiamas, jis atšaukiamas visam laikui.

— EAA-6.2.10.1-05: MSO atšaukimų sąrašo patikra dėklės pasikliaujančiajai šaliai neprivaloma ir, kai taikytina, patikra turi atitikti patikros reikalavimus, nustatytus prieigos raktų statuso sąrašo specifikacijoje, ir statuso struktūros specifikaciją, nustatytą EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: kai dėklės pasikliaujančioji šalis turi turėti galimybę patikrinti asmens tapatybės duomenų arba elektroninio požymių liudijimo atšaukimo statusą, ji turi palaikyti ir liudijimų statuso sąrašo mechanizmą, ir liudijimų atšaukimų sąrašo mechanizmą, nustatytus EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: į MSO elementus „identifier_list“ ir „status_list“ gali būti įtraukiamas sertifikato elementas.

— EAA-6.2.10.1-06.1: jei įtraukiamas sertifikato elementas, jame turi būti sertifikatas, kuriame yra viešasis raktas, kuriuo pasirašytas arba antspauduotas aukščiausiojo lygio sertifikatas elemente „x5chain“ MSO atšaukimų sąrašo struktūroje.

— EAA-6.2.10.1-06.1.1: dėklės pasikliaujančiosios šalies egzempliorius naudoja tą sertifikatą kaip patikimumo užtikrinimo priemonę elemento „x5chain“ patikrai MSO atšaukimų sąrašo struktūroje.

— EAA-6.2.10.1-06.2: kai sertifikato elemento nėra, aukščiausiojo lygio sertifikatas elemente „x5chain“ MSO atšaukimų sąrašo struktūroje pasirašomas arba antspauduojamas naudojant sertifikatą, kuris buvo naudotas pasirašant MSO „x5chain“ elementą.

— EAA-6.2.10.1-06.2.1: dėklės pasikliaujančiosios šalies egzempliorius naudoja tą sertifikatą kaip patikimumo užtikrinimo priemonę elemento „x5chain“ patikrai MSO atšaukimų sąrašo struktūroje.

— EAA-6.2.10.1-07: MSO atšaukimų sąrašas įgyvendinamas pagal prieigos raktų statuso sąrašo specifikacijas kaip statuso sąrašo prieigos raktas CWT formatu.

— EAA-6.2.10.1-08: identifikatorių sąrašo ir statuso sąrašo mechanizmų MSO atšaukimų sąrašui taikomi šie reikalavimai:

  — turi būti įtrauktas teiginys „exp“;

  — gali būti įtrauktas teiginys „ttl“;

  — į teiginį „IdentifierList“ arba „StatusList“ gali būti įtrauktas teiginys „aggregation_uri“, o asmens tapatybės duomenų teikėjas, kvalifikuotų elektroninių požymių liudijimų teikėjas arba elektroninių požymių liudijimų, kuriuos teikia už autentišką šaltinį atsakinga viešojo sektoriaus įstaiga arba kurie teikiami jos

vardu, teikėjas gali naudoti teiginį „aggregation_uri“, kad nurodytų suderinamumą su telkimo mechanizmu, kaip nustatyta prieigos raktų statuso sąrašo specifikacijoje.

— CWT yra „COSE_Sign1“ objektas, kuriam naudojamas vienas iš šių parašo algoritmų parašui apskaičiuoti:

(a) „ES256“ (ECDSA su kreive NIST P-256 ir SHA-256);

(b) „ES384“ (ECDSA su kreive NIST P-384 ir SHA-384);

(c) „ES512“ (ECDSA su kreive NIST P-521 ir SHA-512);

(d) „ESB256“ (ECDSA su kreive „brainpoolP256r1“ ir SHA-256);

(e) „ESB384“ (ECDSA su kreive „brainpoolP384r1“ ir SHA-384);

(f) „ESB512“ (ECDSA su kreive „brainpoolP512r1“ ir SHA-512);

— į CWT įtraukiamas „x5chain“ apsaugotoje antraštėje, kurioje yra sertifikatas ar sertifikatų seka MSO atšaukimų sąrašo parašui patikrinti;

— prieigos raktų statuso sąrašo specifikacijoje nustatytas objekto identifikatoriaus rakto išplėstinis naudojimas gali būti panaudotas statuso sąrašo ir identifikatorių sąrašo sertifikate, ir dėklės pasikliaujančiosios šalies egzemplioriai gali palaikyti prieigos raktų statuso sąrašo specifikacijoje nurodytų objektų identifikatorių išplėstinį rakto naudojimą, o kalbant apie objekto identifikatorių, kvalifikuotų elektroninių požymių liudijimų teikėjas arba elektroninių požymių liudijimų, kuriuos teikia viešojo sektoriaus įstaiga arba kurie teikiami jos vardu, teikėjas, kai naudoja išplėstinio rakto naudojimo OID, nustatytą prieigos raktų statuso sąrašo specifikacijoje, neturi išplėstinio rakto naudojimo lauko daryti kritinio.

— EAA-6.2.10.1-09: nukrypstant nuo prieigos raktų statuso sąrašo specifikacijos reikalavimų, identifikatorių sąrašo mechanizmui taikomi šie reikalavimai:

— teiginio „type“ vertė yra „application/identifierlist+cwt“;

— teiginio „StatusList“ neturi būti CWT teiginių rinkinyje;

— struktūra „IdentifierList“, apibrėžta EAA-6.2.10.1-11, turi būti įtraukta kaip teiginys į CWT teiginių rinkinį naudojant raktą 65530.

— EAA-6.2.10.1-10: struktūra „IdentifierList“ turi būti CBOR struktūra su šiuo 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: kai sąraše „IdentifierList“ yra identifikatorius, MSO, kurio statuso elemente yra identifikatorius, atšaukiamas.

— EAA-6.2.10.1-10.2: teiginys „Aggregation_uri“ nustatytas prieigos raktų statuso sąrašo specifikacijos 9.2 skirsnyje.

— EAA-6.2.10.1-10.3: identifikatorių sąrašo turinio tipas turi būti „application/identifierlist+cwt“, nustatytas prieigos raktų statuso sąrašo specifikacijos 8.2 skirsnio reikalavimuose.

— EAA-6.2.10.1-11: toliau pateikti reikalavimai taikomi MSO elementui „identifier_list“ (žr. EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: elementas „identifier_list“ turi būti CBOR struktūra su šiuo CDDL:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: siekiant išvengti identifikatoriaus panaudojimo pateikimų koreliacijai, kiekvienam MSO jis turi būti unikalus.

— EAA-6.2.10.1-12: statuso sąrašui taikomi šie reikalavimai:

  — EAA-6.2.10.1-12.1: struktūros „StatusList“ bitų elementas prilyginamas 1.

— EAA-6.2.10.1-13: MSO elementui „status_list“ (žr. EAA-6.2.10.1-17) taikomi šie reikalavimai:

  — EAA-6.2.10.1-13.1: elementas „status_list“ turi atitikti struktūros „StatusListInfo“ reikalavimus, nustatytus prieigos raktų statuso sąrašo specifikacijoje, ir pridedamas neprivalomas sertifikato elementas, nustatytas EAA-6.2.10.1-06;

  — EAA-6.2.10.1-13.2: siekiant išvengti statuso rodyklės panaudojimo pateikimų koreliacijai, kiekvienam MSO statuso rodyklės ir URI derinys turi būti unikalus.

— EAA-6.2.10.1-14: dėklės egzemplioriaus liudijimui (WIA) ir rakto liudijimui (KA) atšaukti dėklės teikėjas naudoja antrąjį (EAA-6.2.10.1-02.2) arba trečiąjį (EAA-6.2.10.1-02.3) iš EAA-6.2.10.1-02 nurodytų metodų.

— EAA-6.2.10.1-15: savo dėklės sprendinyje dėklės teikėjas įgyvendina liudijimų atšaukimo mechanizmus, nustatytus EAA-6.2.10.1-02.

— EAA-6.2.10.1-16: asmens tapatybės duomenų teikėjas ir elektroninių požymių liudijimų teikėjas palaiko tiek liudijimų statuso sąrašo mechanizmą, tiek liudijimų atšaukimų sąrašo mechanizmą, nurodytus EAA-6.2.10.1-02, dėklės egzemplioriaus liudijimo (WIA) ir rakto liudijimo (KA) atšaukimo statusui patikrinti.

— EAA-6.2.10.1-17: MSO statuso struktūra turi būti CBOR struktūra su šiuo CDDL:

Status = {

? 'identifier_list' : IdentifierListInfo,

? 'status_list' : StatusListInfo,

* tstr => RFU

}“

V PRIEDAS

„III PRIEDAS

10 straipsnyje nurodytos techninės specifikacijos

— Techninės specifikacijos:

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

VI PRIEDAS

Įgyvendinimo reglamento (ES) 2024/2979 IV priedas iš dalies keičiamas taip:

1) 1 punktas pakeičiamas taip:

„1. Privalomas parašo arba spaudo formatas:

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

2) 3 punktas pakeičiamas taip:

„3. Taikomųjų programų sąsaja.
ETSI TS 119 432 v1.3.1 (2026-03) 6.4.3, A.6, A.7 ir A.8 punktai.“

VII PRIEDAS

„VI PRIEDAS

Spalvotas ES skaitmeninės tapatybės dėklės patikimumo ženklas



“

VIII PRIEDAS

„VII PRIEDAS

Nespalvotas ES skaitmeninės tapatybės dėklės patikimumo ženklas



“

IX PRIEDAS

„VIII PRIEDAS

ES skaitmeninės tapatybės dėklės patikimumo ženklo duomenys

Duomenys	Aprašymas	Kodavimas	Statusas
TrustMarkResourceURL	ES skaitmeninės tapatybės dėklės patikimumo ženklo paveikslėlio URL ir naudotojo informacijos ištekliai dėklės naudotojo sąsajoje.	URL	privalomas
ListOfCertifiedWalletsURL	Sertifikuotų dėklės sprendinių ES viešo sąrašo URL, kaip nustatyta Komisijos įgyvendinimo reglamente (ES) 2025/849 ([1]).	URL	privalomas
ListOfCertifiedWalletsQRCode	QR kodas, kuriame pateikiama „ListOfCertifiedWalletsURL“ informacija.	ISO-8859-1 Byte mode QR code	neprivalomas
WalletSolutionInfoPageURL	URL į sertifikuoto dėklės sprendinio informacijos puslapį sertifikuotų dėklės sprendinių sąrašo puslapyje iš „ListOfCertifiedWalletsURL“ URL, su prijungtu „?“ ir dėklės sprendinio identifikatoriumi „WalletSolutionID“.	URL	privalomas
WalletSolutionInfoPageQRCode	QR kodas, kuriame pateikiama „WalletSolutionInfoPageURL“ informacija.	ISO-8859-1 Byte mode QR code	neprivalomas
WalletVerifierToolURL*	URL į dėklės patikrinimo priemonės */.well-known/openid-credential-issuer* galutinį tašką, naudojamą liudijimo teikėjo metaduomenų paieškai.	URL	neprivalomas

([1]) 2025 m. gegužės 6 d. Komisijos įgyvendinimo reglamentas (ES) 2025/849, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 taikymo taisyklės dėl informacijos, skirtos sertifikuotų europinių skaitmeninės tapatybės dėklių sąrašui, teikimo Komisijai ir Bendradarbiavimo grupei (OL L, 2025/849, 2025 5 7, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).“

X PRIEDAS

Įgyvendinimo reglamento (ES) 2024/2980 II priedas iš dalies keičiamas taip:

1) II priedo 1 skirsnio 1 punkto i papunktis pakeičiamas taip:

„i) vieną ar daugiau standarto ETSI EN 319 412-2 V2.4.1 (2025-06) arba standarto ETSI EN 319 412-3 V1.3.1 (2023-09) reikalavimus atitinkančių sertifikatų, kurie gali būti naudojami registruotojo sukurtam parašui arba spaudui patikrinti pagal registro duomenis ir kurių sertifikuoti tapatybės duomenys apima registruotojo pavadinimą ir, kai taikytina, registruotojo registracijos numerį, kaip nurodyta atitinkamai c ir d punktuose.“;

2) II priedo 2 skirsnio 1 punkto h papunktis pakeičiamas taip:

„h) vieną ar daugiau standarto ETSI EN 319 412-2 V2.4.1 (2025-06) arba standarto ETSI EN 319 412-3 V1.3.1 (2023-09) reikalavimus atitinkančių sertifikatų, kurie gali būti naudojami dėklės teikėjo išduotų dėklės vieneto liudijimų tapatumui nustatyti ir jiems patvirtinti ir kurių sertifikuoti tapatybės duomenys apima dėklės teikėjo pavadinimą ir, kai taikytina, registracijos numerį, kaip nustatyta atitinkamai a ir b punktuose;“;

3) II priedo 3 skirsnio 1 punkto h papunktis pakeičiamas taip:

„h) vieną ar daugiau standarto ETSI EN 319 412-2 V2.4.1 (2025-06) arba standarto ETSI EN 319 412-3 V1.3.1 (2023-09) reikalavimus atitinkančių sertifikatų, kurie gali būti naudojami asmens tapatybės duomenų teikėjo sukurtam parašui arba spaudui jo teikiamuose asmens tapatybės duomenyse patikrinti ir kurių sertifikuotuose tapatybės duomenyse yra asmens tapatybės duomenų teikėjo pavadinimas ir, kai taikytina, registracijos numeris, kaip nustatyta atitinkamai a ir b punktuose.“;

4) II priedo 4 skirsnio 1 punkto g papunktis pakeičiamas taip:

„g) vieną ar daugiau standarto ETSI EN 319 412-2 V2.4.1 (2025-06) arba standarto ETSI EN 319 412-3 V1.3.1 (2023-09) reikalavimus atitinkančių sertifikatų, kurie gali būti naudojami dėklės pasikliaujančiosios šalies prieigos sertifikatų teikėjo sukurtam parašui arba spaudui prieigos sertifikatuose, kuriuos jis teikia dėklės pasikliaujančiosioms šalims, patikrinti, pasitelkiant, kai taikytina, informaciją, kurios reikia norint atskirti dėklės pasikliaujančiosios šalies prieigos sertifikatus nuo kitų sertifikatų.“;

5) II priedas papildomas 5 skirsniu:

„5. Informaciniai pranešimai apie dėklės pasikliaujančiosios šalies registracijos liudijimų teikėjus

1. Valstybės narės gali Komisijai pateikti šią informaciją apie dėklės pasikliaujančiosios šalies registracijos liudijimus:

a) dėklės pasikliaujančiosios šalies registracijos liudijimų teikėjo pavadinimą;

b) kai taikytina, dėklės pasikliaujančiosios šalies registracijos liudijimų teikėjo registracijos numerį;

c) valstybės narės, kurioje įsisteigęs dėklės pasikliaujančiosios šalies registracijos liudijimų teikėjas, pavadinimą;

d) dėklės pasikliaujančiosios šalies registracijos liudijimų teikėjo kontaktinį e. pašto adresą ir telefono numerį, kuriais galima susisiekti klausimais, susijusiais su dėklės pasikliaujančiosioms šalims jo teikiamais registracijos liudijimais;

e) kai taikytina, dėklės pasikliaujančiosios šalies registracijos liudijimų teikėjo tinklalapio, kuriame pateikiama papildoma informacija apie teikėją ir dėklės pasikliaujančiosioms šalims jo teikiamus registracijos liudijimus, URL;

f) tinklalapio, kuriame pateikiama dėklės pasikliaujančiosioms šalims jo teikiamų registracijos liudijimų teikimo ir naudojimo politika, nuostatos ir sąlygos, URL;

g) vieną ar daugiau standarto ETSI EN 319 412-2 V2.4.1 (2025-06) arba standarto ETSI EN 319 412-3 V1.3.1 (2023-09) reikalavimus atitinkančių sertifikatų, kurie gali būti naudojami dėklės pasikliaujančiosios šalies registracijos liudijimų teikėjo sukurtam parašui arba spaudui registracijos liudijimuose, kuriuos jis teikia dėklės pasikliaujančiosioms šalims, patikrinti, ir, kai taikytina, informaciją, kurios reikia norint atskirti dėklės pasikliaujančiosios šalies registracijos liudijimus nuo kitų sertifikatų.“;

2. 1 punkte nurodyta informacija pateikiama apie kiekvieną dėklės pasikliaujančiosios šalies registracijos liudijimų teikėją.“

XI PRIEDAS

„I PRIEDAS

4 straipsnyje nurodyti protokolai ir sąsajos

Techninė specifikacija ETSI TS 119 472-3 V1.1.1 (2026-03) taikoma su šiais pakeitimais:

1) 4.1. General requirements (bendrieji reikalavimai)

— GEN-REQ-4.1-05: negalioja;

— PASTABA: negalioja;

2) 4.2.3. Provision of registration certificates of PID/EAA Provider to EUDI Wallett (PID/EAA teikėjo registracijos liudijimų pateikimas EUDI dėklei)

— ISS-MDATA-REG_CERT-4.2.3-04: į vieną iš masyvo „issuer_info array“ parametrų įtraukiamas PID/EAA teikėjo registracijos liudijimas.

— ISS-MDATA-REG_CERT-4.2.3-07: negalioja;

— ISS-MDATA-REG_CERT-4.2.3-08: negalioja;

— ISS-MDATA-REG_CERT-4.2.3-09: negalioja;

— ISS-MDATA-REG_CERT-4.2.3-10: negalioja;

— ISS-MDATA-REG_CERT-4.2.3-11: negalioja;

— ISS-MDATA-REG_CERT-4.2.3-12: negalioja;

— ISS-MDATA-REG_CERT-4.2.3-13: negalioja;

3) 4.2.4.2. ARF pre-defined PID/EAA reuse policy (ARF iš anksto nustatyta PID/EAA pakartotinio naudojimo politika)

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: kai nario „id“ vertė yra „arf_annex_ii“ ir su žyme „details“ susietame masyve yra vertė „once_only“ arba vertė „per-relying-party“, tuomet į JSON objektą, kuriame yra šis su žyme „details“ susietas masyvas, įtraukiamas ir JSON skaičius, susietas su žyme „reissue_trigger_unused“.

4) A priedas netaikomas.“

XII PRIEDAS

„II PRIEDAS

5 straipsnyje nurodytos techninės specifikacijos

Taikoma standarto ISO/IEC 18013-7:2025 C priede pateikta techninė specifikacija.

Standarto ETSI TS 119 472-2 V1.2.1 (2026-03) 4.1, 4.2, 5 ir 6 punktuose pateiktos techninės specifikacijos taikomos su šiais pakeitimais (įskaitant įterptą naują 4.3 punktą):

1) 1. Scope (taikymo sritis)

— Šiame dokumente nustatomi du protokolų profiliai, kad pasikliaujančiosios šalys (toliau – RP) galėtų prašyti EAAP arba asmens tapatybės duomenų (toliau – PID) į EUDI dėklę, o EUDI dėklė prašomus EAAP/PID galėtų nusiųsti RP. Kiekvienas iš profilių palaiko du perdavimo mechanizmus, būtent: su API tarpininkavimu ir be API tarpininkavimo, kaip parodyta toliau:

a) Profilis grindžiamas:

— ISO/IEC 18013-5 [10] tik perdavimo mechanizmui be API tarpininkavimo ir

— standarto ISO/IEC 18013-7 [16] C priedu perdavimo mechanizmui su API tarpininkavimu.

Šis profilis vadinamas ISO/IEC-mdoc profiliu ir nustatytas šio dokumento 5 punkte.

b) Profilis grindžiamas:

OpenID4VC-HAIP [11] – tiek perdavimo mechanizmams su API tarpininkavimu, tiek mechanizmams be API tarpininkavimo taip:

— [11] 5, 5.1, 5.3, 7 ir 8 skirsniai – perdavimams su peradresavimais arba perdavimo mechanizmui be API tarpininkavimo ir

— [11] 5, 5.2, 5.3, 7 ir 8 skirsniai – perdavimo mechanizmui su API tarpininkavimu.

Šis profilis vadinamas OpenID4VC-HAIP profiliu ir nustatytas šio dokumento 6 punkte.

2) 2.1. Normative references (norminės nuorodos)

— [15] ISO 639: „Language code“.

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

3) 4.1. EAAP implementation based on SD-JWT VC (EAAP įgyvendinimas, grindžiamas SD-JWT VC)

— EAAP-SD-JWT VC-04: negalioja.

4) 4.2. EAAP implementation based on ISO/IEC-mdoc (EAAP įgyvendinimas, grindžiamas ISO/IEC-mdoc)

— EAAP-ISO/IEC-mdoc-01: negalioja.

— Note2: negalioja.

— EAAP-ISO/IEC-mdoc-02: negalioja.

5) 4.3. EAAP implementation with mediating API (EAAP įgyvendinimas, grindžiamas tarpininkėmis API)

— EAAP-API-GEN-01: EUDI dėklė turi palaikyti tarpininkavimo API, kuri yra suderinama su abiem [11] 5.2 punkte ir [16] C priede nustatytais protokolais.

— PASTABA. Kai įrenginys, kuriame įdiegta EUDI dėklė, nepalaiko abiejų protokolų, šis reikalavimas neįvykdomas ir tai lemia neatitiktį dėl to, kad pagrindinėse operacinėse sistemose ir naršyklėse neįgyvendintos būtinos sąveikumo funkcijos.

— EAAP-API-GEN-02: EUDI dėklė turi palaikyti tarpininkavimo API bent PID ir EAA tipams, užregistruotiems schemų kataloge, kaip nustatyta Įgyvendinimo reglamente (ES) 2025/1569, ir bent visiems formatams, nustatytiems Reglamento (ES) 2024/2979 II priede.

— 1 PASTABA. Kai pagrindinė operacinė sistema, naršyklė, tarpininkės API ar bet kuris kitas techninis lygmuo, kurio nekontroliuoja EUDI dėklė, apriboja, filtruoja, iš anksto atrenka ar kitaip apriboja kredencialų formatus ir schemų kataloge užregistruotus PID ir EAA tipus, šis reikalavimas neįvykdomas. Kai dėl tokio apribojimo EUDI dėklė tampa nesuderinama su užregistruotu kredencialų tipu ar formatu, tokia neatitiktis kyla dėl tų pagrindinių operacinių sistemų, naršyklių, tarpininkių API ar kito atitinkamo techninio lygmens negebėjimo užtikrinti būtinas sąveikumo funkcijas.

6) 4.4. Wallet-relying party validation and overasking checks (dėklės pasikliaujančiosios šalies patvirtinimas ir perklausimas dėl tikrinimų)

— WRP-VALIDATION-01: EUDI dėklė patvirtina gautą dėklės pasikliaujančiosios šalies registracijos liudijimą, prieš pateikdama bet kokius prašomus PID ar elektroninį požymių liudijimą dėklės naudotojui, kad šis patvirtintų.

— WRP-VALIDATION-02: kai dėklės pasikliaujančiosios šalies registracijos liudijimo patvirtinimas nepavyksta, įskaitant atvejus, kai yra pasibaigęs liudijimo galiojimas, jis yra atšauktas, išduotas ne galiojančio patikimo dėklės pasikliaujančiosios šalies registracijos liudijimų teikėjo, iškreiptas ar jo negalima kriptografiškai patikrinti, EUDI dėklė įspėja dėklės naudotoją, kad dėklės pasikliaujančiosios šalies negalima patvirtinti, ir užklausos nepateikia kaip sėkmingai patvirtintos. Dėklės naudotojas turi aiškiai patvirtinti pasikliaujančiosios šalies užklausą. Nutylėjimo ar iš anksto pažymėtų žymimųjų langelių aiškiam patvirtinimui nepakanka.

— WRP-VALIDATION-03: dėklės teikėjas, remdamasis rizikos analize ir saugumo politika, nustato, ar konkrečius nepavykusius patvirtinimo tikrinimus dėklės naudotojas gali praleisti ir kokiomis sąlygomis tai gali būti daroma.

— WRP-OVERASKING-01: EUDI dėklė palygina dėklės pasikliaujančiosios šalies prašomus liudijimus ir požymius su dėklės pasikliaujančiosios šalies registracijos liudijime užregistruotais liudijimais ir požymiais.

— WRP-OVERASKING-02: kai dėklės pasikliaujančioji šalis prašo PID ar elektroninių požymių liudijimų ar teiginių, kurių neapima dėklės pasikliaujančiosios šalies registracijos liudijimas, EUDI dėklė, prieš bet ką atskleisdama, aiškiai įspėja dėklės naudotoją. Įspėjime nurodoma, kad dėklės pasikliaujančioji šalis prašo daugiau informacijos, nei yra užregistravusi. Dėklės naudotojas turi aiškiai patvirtinti pasikliaujančiosios šalies užklausą. Nutylėjimo ar iš anksto pažymėtų žymimųjų langelių aiškiam patvirtinimui nepakanka.

— WRP-OVERASKING-03: dėklės teikėjas, remdamasis savo rizikos analize, saugumo politika ir taikytinais teisės aktais, nustato, ar dėklės naudotojas gali tęsti procesą nepaisydamas tokio įspėjimo, ar galima atskleisti tik prašomų duomenų poaibį, kurį apima registracijos liudijimas, ar užklausą reikia atmesti.

7) 5.1. Introduction (įvadas)

— 5 punkte ir jo papunkčiuose nustatomas protokolo, leidžiančio RP teikti EAAP arba PID užklausas į EUDI dėklę ir EUDI dėklei prašomus EAAP/PID siųsti RP naudojant perdavimo mechanizmą be API tarpininkavimo, grindžiamą ISO/IEC 18013-5 [10], arba perdavimo mechanizmą su API tarpininkavimu, grindžiamą ISO/IEC 18013-7 [16] C priedu, profilis, skirtas ISO/IEC 18013-5 [10] nustatytoms duomenų struktūroms perduoti tinkamai inkapsuliuotoms.

— Likusi 5 punkto dalis organizuota taip:

— 5.2 papunktyje nustatomi RP ir EUDI dėklės reikalavimai dėl profilio ir perdavimo mechanizmų palaikymo;

— 5.3 papunktyje nustatomi reikalavimai, taikomi perdavimo mechanizmui be API tarpininkavimo;

— 5.4 papunktyje nustatomi reikalavimai, taikomi perdavimo mechanizmui su API tarpininkavimu.

8) 5.2. Requirements on EUDI Wallet and RP support (EUDI dėklės ir RP palaikymo reikalavimai)

— ISO/IEC 18013-SUPPORT-01: dėklės vienetai, PID teikėjai, liudijimų teikėjai, dėklės teikėjai ir pasikliaujančiosios šalys PID ar požymių liudijimų užklausoms ir pateikimui nepalaiko paieškos serveryje, kaip nustatyta ISO/IEC 18013-5 [10].

— ISO/IEC 18013-SUPPORT-02: EUDI dėklė atitinka šio dokumento 5.3 ir 5.4 punktuose nustatytus reikalavimus.

— ISO/IEC 18013-SUPPORT-04: pasikliaujančioji šalis turėtų įgyvendinti profilį, nustatytą šio dokumento 5.4 punkte.

9) 5.3.2. ISO/IEC-mdoc EAAP Request contents (ISO/IEC-mdoc EAAP užklausos turinys)

— ISO/IEC 18013-5-REQ-04: įrenginio užklausose, siunčiamose EUDI dėklėms, turi būti rakto ir vertės pora „requestInfo“, nustatyta [10] 8.3.2.1.2.1 punkte. Šios poros vertė turi būti „RequestInfo“ tipo.

— ISO/IEC 18013-5-REQ-05: Tipas „RequestInfo“ turi būti kaip CDDL apibrėžtis, parodyta toliau.

```
RequestInfo = {

    'euWrprc': bstr ; čia yra registracijos liudijimas (žr. reikalavimus toliau)

}
```

— ISO/IEC 18013-5-REQ-06: minėtame naryje „requestInfo“ turi būti narys, pažymėtas „euWrprc“.

— ISO/IEC 18013-5-REQ-07: „euWrprc“ vertė yra CBOR koduotas registracijos liudijimas.

— ISO/IEC 18013-5-REQ-08: negalioja.

— 3 PASTABA: negalioja.

— ISO/IEC 18013-5-REQ-09: negalioja.

— ISO/IEC 18013-5-REQ-10: negalioja.

— ISO/IEC 18013-5-REQ-11: negalioja.

10) 5.3.3. ISO/IEC-mdoc EAAP Response profile (ISO/IEC-mdoc EAAP atsako profilis)

— Šiame punkte nustatomi „DeviceResponse“ pranešimo tipo reikalavimai, bendri abiem perdavimo mechanizmo tipams (su API tarpininkavimu ir be API tarpininkavimo).

— *1 PASTABA*. Kai naudojamas mechanizmas be API tarpininkavimo, grindžiamas ISO/IEC 18013-5 [10], EAAP atsakas yra tiksliai „DeviceResponse“ egzempliorius, atitinkantis šiame punkte nurodytą profilį, o kai naudojamas mechanizmas su API tarpininkavimu, grindžiamas ISO/IEC 18013-7 [16] C priedu, „DeviceRequest“ egzempliorius inkapsuliuojamas, kaip nustatyta [16] C priede.

— ISO/IEC 18013-5-RESP-02: asmens tapatybės duomenų ir elektroninių požymių liudijimų teikėjas į savo išduodamų asmens tapatybės duomenų ir elektroninių požymių liudijimų mobiliojo saugumo objekto „KeyAuthorizations“ atvaizdį neįtraukia jokių duomenų elementų, išskyrus duomenų elementus, kuriuos dėklės pasikliaujančioji šalis pateikia transakcijos duomenyse, pateiktuose „mdoc“ užklausoje, kurią dėklės vienetas turi pasirašyti arba antspauduoti naudodamas asmens tapatybės duomenų arba elektroninių požymių liudijimų privatųjį raktą.

— *2 PASTABA*. Todėl dėklės vienetai negali dėklės pasikliaujančiosioms šalims pateikti jokių įrenginio pasirašytų duomenų elementų, išskyrus tuos, kurių reikia duomenims, kuriuos pateikė dėklės pasikliaujančioji šalis, pasirašyti, pavyzdžiui, kai naudojamas saugus naudotojo tapatumo nustatymas.

— *3 PASTABA*. ISO/IEC 18013-5:2021 nenustatyta, kaip dėklės pasikliaujančiosios šalys gali įtraukti transakcijų duomenis į „mdoc“ užklausą. Transakcijų duomenys į „mdoc“ užklausą įtraukiami kartu su techninėmis specifikacijomis.

— ISO/IEC 18013-5-RESP-03: asmens tapatybės duomenų teikėjai neleidžia asmens tapatybės duomenų privačiuoju raktu pasirašyti duomenų elementų, kuriuos „mdoc“ užklausoje transakcijos duomenyse pateikia dėklės pasikliaujančioji šalis.

11) 5.4. Requirements for API mediated mechanism (mechanizmo su API tarpininkavimu reikalavimai)

5.4.1. ISO/IEC 18013-7-related requirements (su ISO/IEC 18013-7 susiję reikalavimai)

Šiame punkte nustatomi perdavimo mechanizmo su API tarpininkavimu reikalavimai, susiję su [16] C priede nustatytais reikalavimais.

— ISO/IEC 18013-7-API-01: profilis, palaikantis pateiktis su API tarpininkavimu, turi atitikti ISO/IEC 18013-7 [16] C priedo reikalavimus, išsamiau nustatytus šio dokumento 5.3 ir 5.4 punktuose.

— ISO/IEC 18013-7-API-02: Taikomi visi privalomi [16] C priede nustatyti reikalavimai, išsamiau nustatyti šio dokumento 5.3 ir 5.4 punktuose.

— ISO/IEC 18013-7-API-03: Visi [16] C priede nustatyti neprivalomi reikalavimai išlieka neprivalomi, nebent šiame dokumente nurodyta kitaip.

12) 5.4.2. Additional requirements (papildomi reikalavimai)

— Šiame punkte nustatomi papildomi reikalavimai perdavimo mechanizmui su API tarpininkavimu.

— ISO/IEC 18013-ADD-API-01: pagal numatytąją nuostatą EUDI dėklė tarpininkei API, veikiančiai pagal [16] C priedą, atskleidžia, kad yra visų saugomų elektroninių požymių liudijimų tipai, tačiau neatskleidžia šiuose elektroniniuose požymių liudijimuose esančių požymių ar jų verčių.

— *1 PASTABA*. Požymio vertės apribojimas taikomas net jei toks atskleidimas pagerintų operacinės sistemos EUDI dėklei teikiamas paslaugas, pavyzdžiui, liudijimų atranką API tarpininkavimo kontekste.

— Yra su operacinėmis sistemomis ir naršyklėmis susijusių aspektų, kurių įgyvendintojai negali kontroliuoti ir į kuriuos galima atsižvelgti, kaip nurodyta toliau pateiktose 2–4 pastabose:

— *2 PASTABA*. Pasikliaujančiosios šalies informacijos pateikimo užklausą, suderinamą su [16] C priedu, gali apdoroti naršyklė ir (arba) operacinė sistema, kad būtų galima atlikti esamų EAA paiešką, užkirsti kelią prieš naudotoją nukreiptam sukčiavimui arba pašalinti triktis.

— *3 PASTABA*. Pasikliaujančiosios šalies informacijos pateikimo užklausą, suderinamą su [16] C priedu, naršyklė ir (arba) operacinė sistema turi apdoroti naudotojo saugumo tikslais.

— *4 PASTABA*. Pasikliaujančiosios šalies informacijos pateikimo užklausos, suderinamos su [16] C priedu, naršyklė ir (arba) operacinė sistema neturi apdoroti rinkos analizės tikslais (įskaitant kaip antrinį tikslą) ar naršyklės ir (arba) operacinės sistemos vidaus tikslais.

— ISO/IEC 18013-ADD-API-02: kai EUDI dėklė naudotojo prašymu pašalina PID arba EAA, anksčiau atskleistus tarpininkei API, kuri veikia pagal [16] C priedą, EUDI dėklė tarpininkei API atskleidžia tai, kad joje nebelaikomi šie PID ar EAA.

— ISO/IEC 18013-ADD-API-03: jei naudotojas pašalina savo EUDI dėklę, EUDI dėklė tarpininkei API, kuri veikia pagal [16] C priedą, atskleidžia tai, kad joje nebelaikomi jokie anksčiau atskleisti PID ar EAA.

— ISO/IEC 18013-ADD-API-04: EUDI dėklėje turi būti pateikiamas bendras naudotojo nuostatis, kuriuo galima išjungti saugomų EAA atskleidimą per tarpininkę API, kuri veikia kaip nustatyta ISO/IEC 18013-ADD-API-01. Kai šis nuostatis išjungtas, EUDI dėklė neskelbia API tarpininkaujamų pateikimo ar išdavimo užklausų ir į jas neatsako.

— ISO/IEC 18013-ADD-API-05: EUDI dėklės, naudodamos tarpininkę API, tarp įrenginių vykstančiuose duomenų srautuose patikrina, ar sąveikaujantis įrenginys yra fiziškai prie pat EUDI dėklės, fiziniam artumui patikrinti naudodamos saugų tiesioginį naudotojo tarpininkaujamą vietos ryšio kanalą, kaip antai trumpojo nuotolio belaidžio ryšio technologiją.

— *PASTABA*. CTAP 2.3 užtikrina galimybę naudoti BLE fiziniam artumui patikrinti ir, kai funkcija įgyvendinta abiejuose įrenginiuose, taip pat užtikrina galimybę perduoti duomenis tarp įrenginių naudojant trumpojo nuotolio siuntimo technologijas. Pagrindinėse operacinėse sistemose, naršyklėse, tarpininkėse API ar bet kuriame kitame techniniame lygmenyje, kurio EUDI dėklė nekontroliuoja, tiek fizinio artumo patikrinimui, tiek duomenų perdavimui tarp įrenginių turėtų būti pirmiausia naudojamas vietos ryšio kanalas, kurio galimybę užtikrina CTAP 2.3, o ne CTAP hibridinio tunelio paslaugos.

13) 6.2. Requirements on EUDI Wallet and RP support (EUDI dėklės ir RP palaikymo reikalavimai)

— OIDFVP-HAIP-SUPPORT-02: EUDI dėklė atitinka šio priedo 6.5 punkte nustatytus reikalavimus.

— OIDFVP-HAIP-SUPPORT-03: pateikimo į kitą įrenginį srautams EUDI dėklė neturėtų palaikyti 6.4 punkte nurodyto peradresavimu grindžiamo mechanizmo.

— *3 PASTABA*. Šio mechanizmo naudojimui būdingas pažeidžiamumas išpuoliams, kaip antai seanso fiksavimas. Tokių išpuolių pavojaus mažinimas yra pasikliaujančiųjų šalių atsakomybė. Šio mechanizmo įgyvendinimas neturėtų lemti neatitikties.

— OIDFVP-HAIP-SUPPORT-05: pasikliaujančioji šalis turi atitikti šio priedo 6.5 punkte nustatytus reikalavimus.

— *5 PASTABA:* negalioja.

14) 6.3.1. General requirements (bendrieji reikalavimai)

— OIDFVP-HAIP-GEN-01: taikomi visi privalomi reikalavimai, nustatyti HAIP [11] 5, 5.3, 7 ir 8 punktuose.

— *1 PASTABA*. „HAIP [11] 5 skirsnis“ reiškia tik reikalavimus, pateiktus tiesiogiai po 5 skirsnio antrašte. Tai neapima 5.1, 5.2 ir 5.3 skirsnių.

— OIDFVP-HAIP-GEN-03: jei šiame priede keičiamas OpenID4VC-HAIP [11] reikalavimas, viršesnis yra šiame priede nustatytas reikalavimas.

— *2 PASTABA*. Tai leistų, pvz., konvertuoti OpenID4VC-HAIP [11] neprivalomą reikalavimą į privalomą arba išplėsti privalomus reikalavimus.

— OIDFVP-HAIP-GEN-04: kai prašomo liudijimo formatas atitinka [10], pasikliaujančiosios šalys ir EUDI dėklės turi atitikti [11] 6 skirsnyje pateiktą „ISO mdocs“ profilį.

— *3 PASTABA*. Dėl aiškumo: HAIP nustatytas „ISO mdocs profilis“ reiškia, kad pasikliaujančiosios šalys ir EUDI dėklės turi atitikti taikytinus reikalavimus, nustatytus [7] B.2 priede.

— OIDFVP-HAIP-GEN-05: kai prašomo liudijimo formatas atitinka [2], pasikliaujančiosios šalys ir EUDI dėklės turi atitikti „IETF SD-JWT VCs“ profilį [11] 6 skirsnyje.

— *4 PASTABA*. Dėl aiškumo: „IETF SD-JWT VCs profilis“ reiškia, kad pasikliaujančiosios šalys ir EUDI dėklės turi atitikti [7] B.3 priedo reikalavimus, taip pat [11] 6.1 skirsnio reikalavimus.

15) 6.3.2.1. General requirements (bendrieji reikalavimai)

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

16) 6.3.2.2. Requirements for the Request Object (objekto užklausos reikalavimai)

— OIDFVP-HAIP-COMMON-REQ-RO-02: negalioja;

— OIDFVP-HAIP-COMMON-REQ-RO-03: negalioja;

— OIDFVP-HAIP-COMMON-REQ-RO-04: negalioja;

— OIDFVP-HAIP-COMMON-REQ-RO-05: negalioja;

— OIDFVP-HAIP-COMMON-REQ-RO-06: negalioja;

— OIDFVP-HAIP-COMMON-REQ-RO-07: negalioja;

— OIDFVP-HAIP-COMMON-REQ-RO-08: negalioja;

— OIDFVP-HAIP-COMMON-REQ-RO-09: negalioja;

— OIDFVP-HAIP-COMMON-REQ-RO-10: negalioja;

— OIDFVP-HAIP-COMMON-REQ-RO-11: negalioja;

— OIDFVP-HAIP-COMMON-REQ-RO-12: negalioja;

— *2 pastaba:* negalioja;

— OIDFVP-HAIP-COMMON-REQ-RO-13: į vieną iš parametro „verifier_info“ elementų įtraukiamas registracijos liudijimas.

— OIDFVP-HAIP-COMMON-REQ-RO-23: OpenID4VP 5.9.3 skirsnyje paminėtas galinio elemento sertifikatas, skirtas naudoti su „x509_hash Client Identifier Prefix“, yra RP prieigos sertifikatas, kaip nustatyta ETSI TS 119 475 [14].

17) 6.3.3. Authorization Response (EAAP response) profile (autorizacijos atsako (EAAP atsako) profilis)

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

18) 6.4.1. General requirements (bendrieji reikalavimai)

— OIDFVP-HAIP-REDIRECTS-04: negalioja.

— *PASTABA:* negalioja.

19) 6.5.2. Additional requirements (papildomi reikalavimai)

— OIDFVP-HAIP-ADD-API-01: pagal numatytąją nuostatą EUDI dėklė tarpininkei API, veikiančiai pagal [11] 5.2 punktą, atskleidžia, kad yra visų saugomų EAA tipai, tačiau neatskleidžia šiuose EAA esančių požymių ar jų verčių.

— OIDFVP-HAIP-ADD-API-04: jei EUDI dėklė palaiko tarpininkę API, veikiančią, kaip nustatyta OIDFVP-HAIP-ADD-API-01, joje turi būti pateikiamas bendras naudotojo nuostatis, kuriuo galima išjungti saugomų EAA atskleidimą per tarpininkę API. Kai šis nuostatis nustatomas taip, kad informacija nebūtų atskleidžiama, EUDI dėklė vėliau turėtų suteikti naudotojui galimybę pasirinkti atskirus liudijimus, kuriuos galima atskleisti tarpininkei API.

— OIDFVP-HAIP-ADD-API-05: EUDI dėklės, naudodamos tarpininkę API, tarp įrenginių vykstančiuose duomenų srautuose patikrina, ar sąveikaujantis įrenginys yra fiziškai prie pat EUDI dėklės, fiziniam artumui patikrinti naudodamos saugų tiesioginį naudotojo tarpininkaujamą vietos ryšio kanalą, kaip antai trumpojo nuotolio belaidžio ryšio technologiją.

— 5 PASTABA. CTAP 2.3 užtikrina galimybę naudoti BLE fiziniam artumui patikrinti ir, kai funkcija įgyvendinta abiejuose įrenginiuose, taip pat užtikrina galimybę perduoti duomenis tarp įrenginių naudojant trumpojo nuotolio siuntimo technologijas. Pagrindinėse operacinėse sistemose, naršyklėse, tarpininkėse API ar bet kuriame kitame techniniame lygmenyje, kurio EUDI dėklė nekontroliuoja, tiek fizinio artumo patikrinimui, tiek duomenų perdavimui tarp įrenginių turėtų būti pirmiausia naudojamas vietos ryšio kanalas, kurio galimybę užtikrina CTAP 2.3, o ne CTAP hibridinio tunelio paslaugos.

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

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: visi šiame dokumente nustatyti reikalavimai, taikytini įrenginio užklausos ir įrenginio atsako struktūroms, nustatytoms ISO/IEC 18013-5, taikomi ir tada, kai EUDI dėklė gauna užklausą pateikti ISO/IEC mdoc per API perdavimo mechanizmą, nustatytą [16] C.1 punkte.“