Europos Sąjungos
oficialusis leidinys

LT
L serija

2024/2979

2024 12 4

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2024/2979

2024 m. lapkričio 28 d.

kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 taikymo taisyklės, susijusios su europinių skaitmeninės tapatybės dėklių vientisumu ir pagrindinėmis funkcijomis

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) Reglamentu (ES) Nr. 910/2014 nustatyta Europos skaitmeninės tapatybės sistema atlieka labai svarbų vaidmenį kuriant saugią ir sąveikią skaitmeninės tapatybės ekosistemą visoje Sąjungoje. Sistemos kertiniu akmeniu – europinėmis skaitmeninės tapatybės dėklėmis (toliau – dėklės) – siekiama palengvinti fizinių ir juridinių asmenų prieigą prie paslaugų visose valstybėse narėse, kartu užtikrinant asmens duomenų ir privatumo apsaugą;

(2) visai asmens duomenų tvarkymo veiklai pagal šį reglamentą taikomi Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 ([2]) ir, kai aktualu, Europos Parlamento ir Tarybos direktyva 2002/58/EB ([3]);

(3) Reglamento (ES) Nr. 910/2014 5a straipsnio 23 dalimi Komisija įgaliojama prireikus nustatyti atitinkamas specifikacijas ir procedūras. Tai pasiekiama keturiais įgyvendinimo reglamentais, kuriais reglamentuojami: protokolai ir sąsajos – Komisijos įgyvendinimo reglamentu (ES) 2024/2982 ([4]), vientisumas ir pagrindinės funkcijos – Komisijos įgyvendinimo reglamentu (ES) 2024/2979 ([5]), asmens tapatybės duomenys ir elektroninis požymių liudijimas – Komisijos įgyvendinimo reglamentu (ES) 2024/2977 ([6]), taip pat pranešimai Komisijai – Komisijos įgyvendinimo reglamentas (ES) 2024/2980 ([7]). Šiuo reglamentu nustatomi atitinkami europinių skaitmeninės tapatybės dėklių vientisumo ir pagrindinių funkcijų reikalavimai;

([1]) OL L 257, 2014 8 28, p. 73, ELI: https://eur-lex.europa.eu/eli/reg/2014/910/oj.

([2]) 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).

([3]) 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).

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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).

(4) Komisija reguliariai vertina naujas technologijas, praktiką, standartus ar techninės specifikacijas. Siekiant užtikrinti aukščiausią valstybių narių suderinimo lygį kuriant ir sertifikuojant dėkles, šiame reglamente nustatytos techninės specifikacijos grindžiamos darbu, atliktu remiantis 2021 m. birželio 3 d. Komisijos rekomendacija (ES) 2021/946 dėl bendro Sąjungos priemonių rinkinio darniam Europos skaitmeninės tapatybės sistemos kūrimui užtikrinti ([8]), visų pirma architektūra ir pamatine sistema. Pagal Europos Parlamento ir Tarybos reglamento (ES) 2024/1183 ([9]) 75 konstatuojamąją dalį, Komisija prireikus turėtų šį įgyvendinimo reglamentą peržiūrėti ir atnaujinti, kad jis atitiktų pasaulinius pokyčius, architektūrą ir pamatinę sistemą ir būtų laikomasi geriausios vidaus rinkos praktikos;

(5) siekiant užtikrinti tikslų bendravimą, techninį diferencijavimą ir aiškų pareigų paskirstymą, būtina atskirti skirtingus dėklių komponentus ir konfigūracijas. Dėklės sprendinys turėtų būti suprantamas kaip visa dėklės teikėjo teikiama sistema, būtina dėklei valdyti. Tai turėtų apimti programinės ir aparatinės įrangos komponentus, taip pat paslaugas, nuostačius ir konfigūracijas, kurių reikia tinkamam dėklės veikimui užtikrinti. Dėklės sprendinys gali būti įdiegtas naudotojo įrenginiuose ir aplinkoje, taip pat paslaugų teikėjo vidinės sistemos struktūroje. Dėklės vienetas turėtų būti suprantamas kaip konkreti individualaus naudotojo dėklės sprendinio sąranka. Ji turėtų apimti dėklės naudotojo įrenginyje arba aplinkoje įdiegtą taikomąją programą, su kuria dėklės naudotojas palaiko tiesioginį ryšį, (toliau – dėklės egzempliorius) ir apsaugos priemones, būtinas naudotojų duomenims ir sandoriams apsaugoti. Šios apsaugos priemonės turėtų apimti specialią programinę arba aparatinę įrangą neskelbtinai informacijai šifruoti ir apsaugoti. Dėklės egzempliorius turėtų būti dėklės vieneto dalis ir sudaryti sąlygas dėklės naudotojui naudotis savo dėklės funkcijomis;

(6) saugios dėklės šifravimo programos, kaip atskiri specializuoti dėklės vieneto komponentai, yra būtinos ne tik ypatingos svarbos turtui, pavyzdžiui, kriptografiniams privatiesiems raktams, apsaugoti, bet ir esminėms funkcijoms, pavyzdžiui, elektroninių požymių liudijimų pateikimui, užtikrinti; Naudojant bendrąsias techninės specifikacijas, dėklės teikėjų prieiga prie įmontuotų saugių elementų gali būti lengvesnė. Saugios dėklės šifravimo programos gali būti teikiamos įvairiais būdais ir įvairiems saugiems dėklės šifravimo įrenginiams. Kai įmontuotiems saugiems elementams dėklės teikėjai teikia individualizuotas saugias dėklės šifravimo programas, pvz., „Java Card“ programėles, dėklės teikėjai turėtų laikytis I priede išvardytų standartų arba lygiaverčių techninių specifikacijų;

(7) dėklės vienetai turi suteikti galimybę asmens tapatybės duomenų arba elektroninių požymių liudijimų teikėjams patikrinti, ar jie šiuos duomenis ar liudijimus išduoda naudodamiesi tikraisiais dėklės naudotojo dėklės vienetais;

(8) siekiant užtikrinti pritaikytąją ir standartizuotąją duomenų apsaugą, dėklėms turėtų būti suteiktos prieinamos pažangiausios privatumą didinančios funkcijos. Šios funkcijos turėtų suteikti galimybę dėkles naudoti taip, kad dėklės naudotojo nebūtų galima atsekti tarp skirtingų dėklės pasikliaujančiųjų šalių, jei pagal naudojimo scenarijų tai yra įmanoma. Pavyzdžiui, dėklės teikėjai turėtų apsvarstyti pažangiausias privatumo mažinimo priemones, susijusias su dėklės vieneto liudijimais, pavyzdžiui, trumpalaikių dėklės vieneto liudijimų naudojimą arba jų išdavimą partijomis. Be to, pagal integruotą informacijos atskleidimo politiką dėklės naudotojai turėtų būti įspėjami apie netinkamą ar neteisėtą elektroninių požymių liudijimų požymių atskleidimą;

(9) dėklės vieneto liudijimai turėtų suteikti galimybę dėklės pasikliaujančiosioms šalims, kurios prašo dėklės vienetų požymių, patikrinti dėklės vieneto, su kuriuo jos bendrauja, galiojimo statusą, nes kai dėklės vienetas nebelaikomas galiojančiu, dėklės vieneto liudijimai turi būti atšaukti. Informacija apie dėklės vienetų galiojimo statusą turėtų būti prieinama sąveikiu būdu, siekiant užtikrinti, kad ja galėtų naudotis visos dėklės pasikliaujančiosios šalys. Be to, tais atvejais, kai dėklės naudotojai savo dėklės vienetus praranda arba jų nebekontroliuoja, dėklės teikėjai turėtų sudaryti sąlygas dėklės naudotojams prašyti atšaukti jų dėklės vienetą. Siekdamos užtikrinti privatumą ir nesusiejimą, valstybės narės turėtų taikyti privatumo išsaugojimo metodus ir dėklės vieneto liudijimui. Tai gali apimti kelių dėklės vieneto liudijimų naudojimą skirtingais tikslais, tik minimaliai svarbios informacijos apie dėklę, būtinos sandoriui, atskleidimą arba dėklės vieneto liudijimų galiojimo trukmės apribojimą, kaip atšaukimo identifikatorių naudojimo alternatyvą;

([8]) OL L 210, 2021 6 14, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) 2024 m. balandžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1183, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014, kiek tai susiję su Europos skaitmeninės tapatybės sistemos nustatymu, (OL L, 2024/1183, 2024 4 30, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(10) siekiant užtikrinti, kad visos dėklės techniniu požiūriu galėtų priimti ir pateikti asmens tapatybės duomenis ir elektroninius požymių liudijimus tarpvalstybiniais atvejais, nedarant neigiamo poveikio sąveikumui, dėklės turėtų palaikyti iš anksto nustatytų rūšių duomenų formatus ir pasirinktinį atskleidimą. Kaip nustatyta Reglamente (ES) Nr. 910/2014, pasirinktinis atskleidimas – tai koncepcija, kuria duomenų savininkui suteikiama teisė atskleisti tik tam tikras didesnio duomenų rinkinio dalis, kad gaunantis subjektas gautų tik tokią informaciją, kuri yra būtina paslaugai, kurios prašo naudotojas, teikti. Kadangi dėklės turi suteikti naudotojui galimybę pasirinktinai atskleisti požymius, II priede išvardyti standartai turėtų būti įgyvendinami taip, kad būtų sudarytos sąlygos naudoti šią dėklių funkciją. Be to, kad dėkles būtų lengviau naudoti tam tikrais atvejais, jos gali palaikyti kitus formatus ir funkcijas;

(11) sandorių registravimas žurnale yra svarbi skaidrumo užtikrinimo priemonė, nes dėklės naudotojui pateikiama sandorių apžvalga. Be to, žurnalai turėtų būti naudojami esant įtartinam dėklės pasikliaujančiųjų šalių elgesiui tam, kad dėklės naudotojo prašymu būtų galima greitai ir lengvai dalytis tam tikra informacija su kompetentingomis priežiūros institucijomis, įsteigtomis pagal Reglamento (ES) 2016/679 51 straipsnį;

(12) kad dėklės naudotojas galėtų pasirašyti elektroniniu būdu, dėklės naudotojui turėtų būti išduotas kvalifikuotas sertifikatas, susietas su kvalifikuotu elektroninio parašo kūrimo įtaisu. Dėklės naudotojas turėtų turėti prieigą prie parašo kūrimo taikomosios programos. Nors kvalifikuotų sertifikatų išdavimas yra kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų teikiama paslauga, dėklės teikėjai ar kiti subjektai turėtų galėti teikti kitus komponentus. Pavyzdžiui, kvalifikuotus elektroninio parašo kūrimo įtaisus kaip paslaugą gali valdyti kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai arba jie gali būti įdedami į dėklės naudotojo įrenginį, pavyzdžiui, kaip lustinė kortelė. Panašiai parašo kūrimo taikomosios programos gali būti integruotos į dėklės egzempliorių, būti atskira programėlė dėklės naudotojo įrenginyje arba būti teikiamos nuotoliniu būdu;

(13) duomenų eksporto ir perkeliamumo objektai gali registruoti asmens tapatybės duomenis ir elektroninius požymių liudijimus, kurie buvo išduoti naudojantis konkrečiu dėklės vienetu. Šie objektai leidžia dėklės naudotojams gauti atitinkamus duomenis iš savo dėklės vieneto, kad būtų sustiprinta jų teisė į duomenų perkeliamumą. Dėklės teikėjai raginami naudoti tuos pačius techninius sprendimus, kad taip pat įgyvendintų dėklės vienetų atsarginių kopijų kūrimo ir atkūrimo procesus ir būtų galima atgauti prarastus dėklės vienetus arba perduoti informaciją iš vieno dėklės teikėjo kitam, jei tai galima padaryti nepakenkiant teisei į duomenų apsaugą ir skaitmeninės tapatybės ekosistemos saugumui;

(14) dėl konkrečių dėklės pasikliaujančiosioms šalims skirtų slapyvardžių kūrimo dėklės naudotojams turėtų būti suteikiama galimybė patvirtinti savo tapatumą neteikiant dėklės pasikliaujančiosioms šalims nereikalingos informacijos. Kaip nustatyta Reglamente (ES) Nr. 910/2014, dėklės naudotojams neturi būti trukdoma naudotis paslaugomis pasitelkiant slapyvardžius, kai nėra teisinio reikalavimo dėl teisinės tapatybės tapatumo nustatymo tikslais. Todėl dėklės turi turėti funkciją, skirtą naudotojo laisvai pasirinktiems ir valdomiems slapyvardžiams generuoti tapatumo nustatymo tikslu siekiant prieigos prie internetinių paslaugų. Įgyvendinus V priede nustatytas specifikacijas, atitinkamai turėtų būti įmanoma naudotis šiomis funkcijomis. Be to, dėklės pasikliaujančiosios šalys neturi prašyti naudotojų pateikti jokių kitų duomenų, išskyrus duomenis, kurie pasikliaujančiųjų šalių registre nurodyti numatomam dėklių naudojimui. Dėklės naudotojams turėtų būti suteikta galimybė bet kuriuo metu patikrinti pasikliaujančiųjų šalių registracijos duomenis;

(15) kaip nustatyta Reglamente (ES) 2024/1183, valstybės narės neturi nei tiesiogiai, nei netiesiogiai riboti prieigos prie viešųjų ar privačiųjų paslaugų fiziniams ar juridiniams asmenims, kurie pasirinko nenaudoti dėklių, ir turi užtikrinti tinkamus alternatyvius sprendimus;

(16) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([10]) 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir 2024 m. rugsėjo 30 d. jis pateikė nuomonę;

([10]) 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).

(17) šiame reglamente numatytos priemonės atitinka Reglamento (ES) Nr. 910/2014 48 straipsnyje nurodyto komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas ir taikymo sritis

Šiuo reglamentu nustatomos taisyklės dėl dėklių vientisumo ir pagrindinių funkcijų; jis turi būti reguliariai atnaujinamas, kad atitiktų su technologijomis ir standartais susijusius pokyčius ir darbą, atliktą remiantis Rekomendacija (ES) 2021/946, visų pirma architektūrą ir pamatinę sistemą.

2 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) saugi dėklės šifravimo programa – taikomoji programa ypatingos svarbos turtui valdyti, susieta su saugiu dėklės šifravimo įrenginiu ir naudojanti jo teikiamas šifravimo ir kitas funkcijas;

2) dėklės vienetas – unikalios konfigūracijos dėklės sprendinys, apimantis dėklės egzempliorius, saugias dėklės šifravimo programas ir saugius dėklės šifravimo įrenginius, kuriuos dėklės teikėjas teikia atskiram dėklės naudotojui;

3) ypatingos svarbos turtas – dėklės vienetui priklausantis arba su juo susijęs turtas, kurio svarba tokia didelė, kad pažeistas jo prieinamumas, konfidencialumas ar vientisumas turėtų labai didelį neigiamą poveikį patikimam dėklės vieneto naudojimui;

4) asmens tapatybės duomenų teikėjas – fizinis arba juridinis asmuo, atsakingas už asmens tapatybės duomenų išdavimą ir atšaukimą bei užtikrinimą, kad naudotojo asmens tapatybės duomenys būtų kriptografiškai susieti su dėklės vienetu;

5) dėklės naudotojas – naudotojas, valdantis dėklės vienetą;

6) dėklės pasikliaujančioji šalis – pasikliaujančioji šalis, kuri skaitmenine sąveika teikdama viešąsias ar privačiąsias paslaugas, ketina kliautis dėklės vienetais;

7) dėklės teikėjas – fizinis arba juridinis asmuo, teikiantis dėklės sprendinius;

8) dėklės vieneto liudijimas – duomenų objektas, kuris apibūdina dėklės vieneto komponentus arba leidžia nustatyti tų komponentų tapatumą ir juos patvirtinti;

9) integruota informacijos atskleidimo politika – taisyklių rinkinys, kurį elektroninio požymių liudijimo teikėjas įtraukia į elektroninį požymių liudijimą ir kuriame nurodomos sąlygos, kurias turi atitikti dėklės pasikliaujančioji šalis, kad gautų prieigą prie elektroninio požymių liudijimo;

10) dėklės egzempliorius – dėklės naudotojo įrenginyje arba aplinkoje įdiegta ir sukonfigūruota taikomoji programa, kuri yra dėklės vieneto dalis ir kurią dėklės naudotojas naudoja sąveikai su dėklės vienetu;

11) dėklės sprendinys – programinės ir aparatinės įrangos, paslaugų, nuostačių ir konfigūracijų derinys, apimantis dėklės egzempliorius, vieną ar daugiau saugių dėklės šifravimo programų ir vieną ar daugiau saugių dėklės šifravimo įrenginių;

12) saugus dėklės šifravimo įrenginys – manipuliavimui atsparus įrenginys, suteikiantis aplinką, kuri susieta su saugia dėklės šifravimo programa ir kurią ši programa naudoja ypatingos svarbos turtui apsaugoti ir šifravimo funkcijoms atlikti, kad būtų galima saugiai vykdyti ypatingos svarbos operacijas;

13) dėklės šifravimo operacija – šifravimo mechanizmas, būtinas dėklės naudotojo tapatumui nustatyti ir asmens tapatybės duomenims arba elektroniniams požymių liudijimams išduoti ar pateikti;

14) dėklės pasikliaujančiosios šalies prieigos sertifikatas – dėklės pasikliaujančiosios šalies prieigos sertifikatų teikėjo išduotas elektroninių spaudų ar parašų sertifikatas, kuriuo nustatomas ir patvirtinamas dėklės pasikliaujančiosios šalies tapatumas;

15) dėklės pasikliaujančiosios šalies prieigos sertifikatų teikėjas – fizinis arba juridinis asmuo, valstybės narės įgaliotas išduoti pasikliaujančiosios šalies prieigos sertifikatus toje valstybėje narėje registruotoms dėklės pasikliaujančiosioms šalims.

II SKYRIUS

EUROPINIŲ SKAITMENINĖS TAPATYBĖS DĖKLIŲ VIENTISUMAS

3 straipsnis

Dėklės vienetų vientisumas

1. Kol dėklės vienetas sėkmingai nenustato dėklės naudotojo tapatumo, dėklės vienetai neatlieka jokių Reglamento (ES) Nr. 910/2014 5a straipsnio 4 dalyje išvardytų funkcijų, išskyrus dėklės naudotojo tapatumo nustatymą, kad jis galėtų prisijungti prie dėklės vieneto.

2. Kiekvieno dėklės vieneto atveju dėklės teikėjai pasirašo arba spaudu patvirtina bent vieną dėklės vieneto liudijimą, atitinkantį 6 straipsnyje nustatytus reikalavimus. Sertifikatas, naudojamas dėklės vieneto liudijimui pasirašyti arba spaudu patvirtinti, išduodamas pagal sertifikatą, įtrauktą į patikimą Įgyvendinimo reglamente (ES) 2024/2980 nurodytą sąrašą.

4 straipsnis

Dėklės egzemplioriai

1. Dėklės egzemplioriai naudoja bent vieną saugų dėklės šifravimo įrenginį ypatingos svarbos turtui valdyti.

2. Dėklės teikėjai užtikrina dėklės egzempliorių ir saugių dėklės šifravimo programų sąveikos vientisumą, autentiškumą ir konfidencialumą.

3. Kai ypatingos svarbos turtas yra susijęs su aukšto saugumo užtikrinimo lygio elektroninės atpažinties vykdymu, dėklės šifravimo operacijos ar kitos operacijos, kurių metu tvarkomas ypatingos svarbos turtas, atliekamos laikantis aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonių savybių ir struktūros reikalavimų, nustatytų Komisijos įgyvendinimo reglamente (ES) 2015/1502 ([11]).

5 straipsnis

Saugios dėklės šifravimo programos

1. Dėklės teikėjai užtikrina, kad saugios dėklės šifravimo programos:

a) vykdytų dėklės šifravimo operacijas, susijusias su ypatingos svarbos turtu, išskyrus tas, kurių reikia, kad dėklės vienetas galėtų nustatyti dėklės naudotojo tapatumą tik tais atvejais, kai tomis taikomosiomis programomis sėkmingai nustatytas dėklės naudotojų tapatumas;

([11]) 2015 m. rugsėjo 8 d. Komisijos įgyvendinimo reglamentas (ES) 2015/1502, kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 8 straipsnio 3 dalį nustatomos minimalios techninės specifikacijos ir procedūros dėl elektroninės atpažinties priemonių saugumo užtikrinimo lygių, (OL L 235, 2015 9 9, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

b) tuo atveju, kai jos nustato dėklės naudotojų tapatumą vykdant elektroninę atpažintį aukštu saugumo užtikrinimo lygiu, nustatytų dėklės naudotojų tapatumą pagal aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonių savybių ir struktūros reikalavimus, nustatytus Įgyvendinimo reglamente (ES) 2015/1502;

c) galėtų saugiai generuoti naujus kriptografinius raktus;

d) galėtų saugiai ištrinti ypatingos svarbos turtą;

e) galėtų sugeneruoti įrodymą apie turimus privačiuosius raktus;

f) apsaugotų privačiuosius raktus, sugeneruotus naudojant tas saugias dėklės šifravimo programas, visu raktų naudojimo laikotarpiu;

g) atitiktų aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonių savybių ir struktūros reikalavimus, nustatytus Įgyvendinimo reglamente (ES) 2015/1502;

h) būtų vieninteliai komponentai, galintys atlikti dėklės šifravimo operacijas ir bet kokias kitas operacijas, susijusias su ypatingos svarbos turtu, vykdant elektroninę atpažintį aukštu saugumo užtikrinimo lygiu.

2. Jei dėklės teikėjai nusprendžia teikti saugią dėklės šifravimo programą įmontuotam saugiam elementui, šie dėklės teikėjai savo techninį sprendimą grindžia I priede išvardytomis techninėmis specifikacijomis arba kitomis lygiavertėmis techninėmis specifikacijomis.

6 straipsnis

Dėklės vienetų autentiškumas ir galiojimas

1. Dėklės teikėjai užtikrina, kad kiekviename dėklės vienete būtų dėklės vieneto liudijimų.

2. Dėklės teikėjai užtikrina, kad 1 dalyje nurodytuose dėklės vieneto liudijimuose būtų viešieji raktai ir kad atitinkami privatieji raktai būtų apsaugoti saugiu dėklės šifravimo įrenginiu.

3. Dėklės teikėjai:

a) informuoja dėklės naudotojus apie jų teises ir pareigas, susijusias su jų dėklės vienetu;

b) numato nuo dėklės vienetų nepriklausomus mechanizmus, kad būtų galima saugiai nustatyti dėklės naudotojų tapatybę ir jų tapatumą;

c) užtikrina, kad dėklės naudotojai turėtų teisę prašyti atšaukti jų dėklės vienetų liudijimus, naudodamiesi b punkte nurodytais tapatumo nustatymo mechanizmais.

7 straipsnis

Dėklės vienetų liudijimų atšaukimas

1. Dėklės teikėjai yra vieninteliai subjektai, galintys atšaukti jų suteiktų dėklės vienetų liudijimus.

2. Dėklės teikėjai parengia viešai prieinamą politiką, kurioje nustatomos dėklės vienetų liudijimų atšaukimo sąlygos ir laikotarpis.

3. Jei dėklės teikėjai dėklės vieneto liudijimus atšaukė, jie per 24 valandas informuoja susijusius dėklės naudotojus apie jų dėklės vienetų atšaukimą, įskaitant atšaukimo priežastį ir pasekmes dėklės naudotojui. Ši informacija pateikiama glaustai, lengvai prieinamu būdu ir naudojant aiškią bei paprastą kalbą.

4. Jei dėklės teikėjai dėklės vieneto liudijimus atšaukia, jie viešai paskelbia dėklės vieneto liudijimo galiojimo statusą išsaugodami privatumą ir nurodo, kur dėklės vieneto liudijime ta informacija pateikta.

III SKYRIUS

EUROPINIŲ SKAITMENINĖS TAPATYBĖS DĖKLIŲ PAGRINDINĖS FUNKCIJOS IR SAVYBĖS

8 straipsnis

Asmens tapatybės duomenų ir elektroninių požymių liudijimų formatai

Dėklės teikėjai užtikrina, kad dėklės sprendiniai palaikytų asmens tapatybės duomenų ir elektroninių požymių liudijimų, išduotų laikantis II priede pateikto standartų sąrašo, naudojimą.

9 straipsnis

Sandorių žurnalai

1. Nepriklausomai nuo to, ar sandoris yra sėkmingai užbaigtas, dėklės egzemplioriai registruoja visus sandorius su dėklės pasikliaujančiosiomis šalimis ir kitais dėklės vienetais, įskaitant elektroninį pasirašymą ir patvirtinimą spaudu.

2. Registruojama informacija turi apimti bent:

a) sandorio dieną ir laiką;

b) atitinkamos dėklės pasikliaujančiosios šalies vardą, pavardę (pavadinimą) ir valstybės narės, kurioje ta dėklės pasikliaujančioji šalis yra įsisteigusi, pavadinimą bei unikalų identifikatorių, o kitų dėklės vienetų atveju – atitinkamą informaciją iš dėklės vieneto liudijimo;

c) per sandorį prašomų ir pateiktų duomenų rūšį (-is);

d) neužbaigtų sandorių atveju – tokio nebaigimo priežastis.

3. Dėklės teikėjai užtikrina registruojamos informacijos vientisumą, autentiškumą ir konfidencialumą.

4. Dėklės egzemplioriai registruoja ataskaitas, kurias dėklės naudotojas per savo dėklės vienetą siunčia duomenų apsaugos institucijoms.

5. 1 ir 2 dalyse nurodyti žurnalai turi būti prieinami dėklės teikėjui, kai tai būtina dėklės paslaugoms teikti, gavus aiškų išankstinį dėklės naudotojo sutikimą.

6. 1 ir 2 dalyse nurodyti žurnalai turi būti prieinami tol, kol jų reikalaujama pagal Sąjungos arba nacionalinę teisę.

7. Dėklės teikėjai sudaro sąlygas dėklės naudotojams eksportuoti 2 dalyje nurodytą registruojamą informaciją.

10 straipsnis

Integruotas informacijos atskleidimas

1. Dėklių teikėjai užtikrina, kad jų teikiami dėklių vienetai galėtų tvarkyti elektroninius požymių liudijimus taikydami III priede nustatytą bendrąją integruotą informacijos atskleidimo politiką.

2. Dėklės egzemplioriai turi galėti tvarkyti ir pateikti tokią 1 dalyje nurodytą integruotą informacijos atskleidimo politiką kartu su duomenimis, gautais iš prašančiosios dėklės pasikliaujančiosios šalies.

3. Dėklės egzemplioriai patikrina, ar dėklės pasikliaujančioji šalis laikosi integruotos informacijos atskleidimo politikos reikalavimų, ir dėklės naudotoją informuoja apie rezultatą.

11 straipsnis

Kvalifikuoti elektroniniai parašai ir spaudai

1. Dėklės teikėjai užtikrina, kad dėklės naudotojai galėtų gauti kvalifikuotus kvalifikuotų elektroninių parašų arba spaudų sertifikatus, kurie yra susieti su kvalifikuotais parašo ar spaudo kūrimo įtaisais, kurie įdedami į dėklės egzempliorių, prijungiami išoriškai arba valdomi nuotoliniu būdu.

2. Dėklės teikėjai užtikrina, kad dėklės sprendinių sąveika su vieno iš šių tipų kvalifikuotais parašo ar spaudo kūrimo įtaisais – į vidų įdedamais, išorėje prijungiamais arba nuotoliniu būdu valdomais kvalifikuotais parašo ar spaudo kūrimo įtaisais 1 dalyje nurodytiems kvalifikuotiems sertifikatams naudoti – yra saugi.

3. Dėklės teikėjai užtikrina, kad dėklės naudotojai, kurie yra fiziniai asmenys, bent jau neprofesiniais tikslais turėtų nemokamą prieigą prie parašo kūrimo taikomųjų programų, leidžiančių nemokamai kurti kvalifikuotus elektroninius parašus naudojant 1 dalyje nurodytus sertifikatus.

12 straipsnis

Parašo kūrimo taikomosios programos

1. Dėklės vienetų naudojamas parašo kūrimo taikomąsias programas gali teikti dėklės teikėjai, patikimumo užtikrinimo paslaugų teikėjai arba dėklės pasikliaujančiosios šalys.

2. Parašo kūrimo taikomosiomis programomis atliekamos šios funkcijos:

a) pasirašomi arba spaudu patvirtinami dėklės naudotojų pateikti duomenys;

b) pasirašomi arba spaudu patvirtinami pasikliaujančiųjų šalių pateikti duomenys;

c) sukuriami parašai arba spaudai bent IV priede nurodytais privalomais formatais;

d) dėklės naudotojai informuojami apie parašo arba spaudo kūrimo proceso rezultatus.

3. Parašo kūrimo taikomosios programos gali būti integruotos į dėklės egzempliorius arba būti išorinės. Kai parašo kūrimo taikomosios programos grindžiamos nuotoliniais kvalifikuotais parašo kūrimo įtaisais ir kai jos integruotos į dėklės egzempliorius, jos palaiko IV priede nurodytą taikomųjų programų sąsają.

13 straipsnis

Duomenų eksportas ir perkeliamumas

Dėklės vienetai, kai tai techniškai įmanoma ir išskyrus ypatingos svarbos turto atvejus, padeda užtikrinti saugų dėklės naudotojo asmens duomenų eksportą ir perkeliamumą, kad dėklės naudotojas galėtų pereiti prie kitą dėklės sprendinį palaikančio dėklės vieneto taip, kad būtų užtikrintas aukštas saugumo užtikrinimo lygis, kaip nustatyta Įgyvendinimo reglamente (ES) 2015/1502.

14 straipsnis

Slapyvardžiai

1. Dėklės vienetai palaiko slapyvardžių dėklės naudotojams kūrimą laikantis V priede nustatytų techninių specifikacijų.

2. Dėklės pasikliaujančiosios šalies prašymu dėklės vienetai palaiko slapyvardžio, kuris tai dėklės pasikliaujančiajai šaliai yra konkretus ir unikalus, kūrimą ir šį slapyvardį pateikia dėklės pasikliaujančiajai šaliai atskirai arba kartu su bet kokiais asmens tapatybės duomenimis arba elektroniniais požymių liudijimais, kurių prašo ta dėklės pasikliaujančioji šalis.

IV SKYRIUS

BAIGIAMOSIOS NUOSTATOS

15 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 2024 m. lapkričio 28 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

I PRIEDAS

5 STRAIPSNYJE NURODYTŲ STANDARTŲ SĄRAŠAS

— *SAM.01 Secured Applications for Mobile - Requirements for supporting 3rd party Applets on eSIM and eSE via SAM. v1.1 2023*, GSMA,

— GPC_GUI_ 217 GlobalPlatform SAM Configuration Technical specification for implementation of SAM v1.0 2024-04,

— GPC_SPE_0 34 GlobalPlatform Card Specification Technical specification for smart cards v2.3.1 2018-03,

— GPC_SPE_0 07 GlobalPlatform Amendment A Confidential Card Content Management v1.2 2019-07,

— GPC_SPE_0 13 GlobalPlatform Amendment D Secure Channel Protocol 03 v1.2 2020-04,

— GPC_SPE_0 93 GlobalPlatform Amendment F Secure Channel Protocol 11 v1.4 2024-03,

— GPD_SPE_0 75 Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices. v3.3 2018-08, GlobalPlatform.

II PRIEDAS

8 STRAIPSNYJE NURODYTŲ STANDARTŲ SĄRAŠAS

— ISO/IEC.18013-5:2021,

— 2022 m. kovo 3 d. W3C rekomendacija *Verifiable Credentials Data Model 1.1*.

III PRIEDAS

10 STRAIPSNYJE NURODYTOS BENDROSIOS INTEGRUOTOS INFORMACIJOS ATSKLEIDIMO POLITIKOS NUOSTATŲ SĄRAŠAS

1. Jokios politikos – nurodoma, kad elektroniniams požymių liudijimams netaikoma jokia politika.
2. Tik įgaliotųjų pasikliaujančiųjų šalių politika – nurodoma, kad dėklės naudotojai elektroninius požymių liudijimus gali atskleisti tik pasikliaujančiosioms šalims, kurių tapatumas nustatytas ir kurios aiškiai išvardytos atskleidimo politikoje.
3. Konkretus patikimumo užtikrinimo pagrindas – nurodoma, kad dėklės naudotojai konkretų elektroninį požymių liudijimą turėtų atskleisti tik dėklės pasikliaujančiosioms šalims, kurių tapatumas nustatytas ir kurios turi dėklės pasikliaujančiosios šalies prieigos sertifikatus, gautus iš konkrečios šakninės zonos (arba konkrečių šakninių zonų sąrašo) arba tarpinio sertifikato (-ų).

IV PRIEDAS

12 STRAIPSNYJE NURODYTI PARAŠO IR SPAUDO FORMATAI

1. Privalomas parašo arba spaudo formatas:

   a) PAdES (PDF pažangusis elektroninis parašas), nurodytas ETSI EN 319 142-1 V1.1.1 (2016-04); Elektroniniai parašai ir infrastruktūros (ESI); PAdES skaitmeniniai parašai; 1 dalis. Komponentai ir PAdES baziniai parašai.

2. Neprivalomų parašo arba spaudo formatų sąrašas:

   a) XAdES, nurodytas „ETSI EN 319 132-1 V1.2.1 (2022-02) elektroniniai parašai ir infrastruktūros (ESI)“; XAdES skaitmeniniai parašai; 1 dalis. Komponentai ir XAdES baziniai parašai (XAdES). XML formato dokumentų pasirašymas;

   b) JAdES, nurodytas „ETSI TS 119 182–1 V1.2.1 (2024-07) elektroniniai parašai ir infrastruktūros (ESI)“; JAdES skaitmeniniai parašai; 1 dalis. Komponentai ir JAdES baziniai parašai. JSON formato dokumentų pasirašymas;

   c) CAdES (CMS pažangusis elektroninis parašas), nurodytas „ETSI EN 319 122-1 V1.3.1 (2023-06) elektroniniai parašai ir infrastruktūros (ESI)“; CAdES skaitmeniniai parašai; 1 dalis. Komponentai ir CAdES baziniai parašai. CMS formato dokumentų pasirašymas;

   d) ASiC (susietojo parašo talpyklė), nurodyta „ETSI EN 319 162-1 V1.1.1 (2016-04) elektroniniai parašai ir infrastruktūros (ESI)“; Susietųjų parašų talpyklės (ASiC); 1 dalis. Komponentai, ASiC bazinės talpyklės ir ETSI EN 319 162-2 V1.1.1 (2016-04) elektroniniai parašai ir infrastruktūros (ESI); Susietųjų parašų talpyklės (ASiC); 2 dalis. Papildomos ASiC talpyklės talpyklėms pasirašyti.

3. Taikomųjų programų sąsaja.

   — Debesijos parašų konsorciumo (CSC) specifikacija v2.0 (2023 m. balandžio 20 d.).

V PRIEDAS

14 STRAIPSNYJE NURODYTOS SLAPYVARDŽIŲ KŪRIMO TECHNINĖS SPECIFIKACIJOS

Techninės specifikacijos.

— 2021 m. balandžio 8 d. W3C rekomendacija *WebAuthn*, 2 lygis, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.