Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2024/2979

4.12.2024.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2024/2979

(2024. gada 28. novembris),

ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes maku integritāti un pamatfunkcijām

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

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

tā kā:

(1) Eiropas digitālās identitātes satvars, kas izveidots ar Regulu (ES) Nr. 910/2014, ir būtisks drošas un sadarbspējīgas digitālās identitātes ekosistēmas izveides elements visā Savienībā. Eiropas digitālās identitātes maki ("maki") ir satvara stūrakmens, un tā mērķis ir atvieglot fizisku un juridisku personu piekļuvi pakalpojumiem visās dalībvalstīs, vienlaikus nodrošinot personas datu un privātuma aizsardzību.

(2) Visām šajā regulā paredzētajām personas datu apstrādes darbībām piemēro Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([2]) un, attiecīgā gadījumā, Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([3]).

(3) Ar Regulas (ES) Nr. 910/2014 5.a panta 23. punktu Komisija ir pilnvarota vajadzības gadījumā noteikt attiecīgās specifikācijas un procedūras. To panāk ar četrām īstenošanas regulām, kuras attiecas uz: protokoliem un saskarnēm – Komisijas Īstenošanas regula (ES) 2024/2982 ([4]); integritāti un pamatfunkcijām – Komisijas Īstenošanas regula (ES) 2024/2979 ([5]); personas identifikācijas datiem un atribūtu elektroniskajiem apliecinājumiem – Komisijas Īstenošanas regula (ES) 2024/2977 ([6]), kā arī paziņojumiem Komisijai – Komisijas Īstenošanas regula (ES) 2024/2980 ([7]). Šajā regulā nosaka attiecīgās prasības attiecībā uz Eiropas digitālās identitātes maku integritāti un pamatfunkcijām.

([1]) OV L 257, 28.8.2014., 73. lpp., ELI: http://data.europa.eu/eli/reg/2014/910/oj.

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

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

([4]) Komisijas Īstenošanas regula (ES) 2024/2982 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes satvara atbalstāmajiem protokoliem un saskarnēm (OV L, 2024/2982, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Komisijas Īstenošanas regula (ES) 2024/2979 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes maku integritāti un pamatfunkcijām (OV L, 2024/2979, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Komisijas Īstenošanas regula (ES) 2024/2977 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes makiem izsniegtajiem personas identifikācijas datiem un atribūtu elektroniskajiem apliecinājumiem (OV L, 2024/2977, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Komisijas Īstenošanas regula (ES) 2024/2980 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz paziņojumiem Komisijai par Eiropas digitālās identitātes maku ekosistēmu (OV L, 2024/2980, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) Komisija regulāri novērtē jaunās tehnoloģijas, praksi, standartus un tehniskās specifikācijas. Lai nodrošinātu visaugstāko saskaņotības līmeni starp dalībvalstīm attiecībā uz maku izstrādi un sertifikāciju, šajā regulā izklāstīto tehnisko specifikāciju pamatā ir darbs, kas veikts, pamatojoties uz Komisijas 2021. gada 3. jūnija Ieteikumu (ES) 2021/946 par kopīgu Savienības rīkkopu koordinētai pieejai Eiropas digitālajam satvaram ([8]) un jo īpaši arhitektūru un atsauces sistēmu. Saskaņā ar Eiropas Parlamenta un Padomes Regula Regulas (ES) 2024/1183 ([9]) 75. apsvērumu Komisijai šī īstenošanas regula vajadzības gadījumā būtu jāpārskata un jāatjaunina, lai tā atbilstu pasaules norisēm, arhitektūrai un atsauces sistēmai un tajā būtu ņemta vērā paraugprakse iekšējā tirgū.

(5) Lai nodrošinātu precīzu saziņu, tehnisku diferenciāciju un skaidru pienākumu sadali, ir jānošķir dažādi maku komponenti un konfigurācijas. Maka risinājums būtu jāsaprot kā visa sistēma, ko nodrošina maka nodrošinātājs un kas ir nepieciešama maka darbībai. Tam būtu jāietver programmatūras un aparatūras komponenti, kā arī pakalpojumi, iestatījumi un konfigurācijas, kas vajadzīgi, lai nodrošinātu maka pienācīgu darbību. Maka risinājums var atrasties lietotāju ierīcēs un vidēs, kā arī uz pakalpojumu sniedzēja aizmugursistēmā. Maka vienība būtu jāsaprot kā konkrēta maka risinājuma iestatne individuālam lietotājam. Tajā būtu jāiekļauj lietojumprogramma, kas uzstādīta maka lietotāja ierīcē vai vidē, ar kuru maka lietotājs mijiedarbojas tieši ("maka instance"), un nepieciešamie drošības elementi lietotāja datu un darījumu aizsardzībai. Šiem drošības elementiem būtu jāietver īpaša programmatūra vai aparatūra, kas paredzēta sensitīvas informācijas šifrēšanai un aizsardzībai. Maka instancei vajadzētu būt daļai no maka vienības un ļaut maka lietotājam piekļūt sava maka funkcijām.

(6) Maka drošas kriptogrāfijas lietojumprogrammas kā atsevišķi specializēti maka vienības komponenti ir vajadzīgi ne tikai kritiski svarīgu aktīvu, piemēram, privāto kriptogrāfijas atslēgu, aizsardzībai, bet arī kritiski svarīgu funkciju nodrošināšanai, piemēram, atribūtu elektronisko apliecinājumu uzrādīšanai. Vienotu tehnisko specifikāciju izmantošana var sekmēt maku nodrošinātāju piekļuvi iegultiem aizsardzības elementiem. Maka drošas kriptogrāfijas lietojumprogrammas var nodrošināt dažādos veidos un dažādām maka drošas kriptogrāfijas ierīcēm. Ja attiecībā uz iegultajiem aizsardzības elementiem maka nodrošinātāji izmanto maka drošas kriptogrāfijas pasūtījumlietojumprogrammas, piemēram *Java Card* sīklietotnes, maka nodrošinātājiem būtu jāievēro I pielikumā norādītie standarti vai līdzvērtīgas tehniskās specifikācijas.

(7) Maka vienībām jādod personas identifikācijas datu vai atribūtu elektronisko apliecinājumu nodrošinātājiem iespēja verificēt, vai tie izdod šos datus un apliecinājumus īstām maka lietotāja maka vienībām.

(8) Lai nodrošinātu integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma, makiem būtu jānodrošina pieejami, mūsdienīgi privātuma uzlabošanas paņēmieni. Šīm funkcijām būtu jādod iespēja makus izmantot bez iespējas maka lietotāju izsekot starp dažādām maka atkarīgajām pusēm, ja tas ir piemērojams attiecīgajā lietošanas scenārijā. Piemēram, maka nodrošinātājiem būtu jāapsver mūsdienīgi privātuma apdraudējumu mazināšanas pasākumi attiecībā uz maka vienības apliecinājumiem, piemēram, īslaicīgu maka vienības apliecinājumu izdošana vai apliecinājuma izdošana paketēm. Turklāt iegultām informācijas izpaušanas procedūrām būtu jābrīdina maka lietotāji par atribūtu elektronisko apliecinājumu neatbilstīgu vai nelikumīgu izpaušanu.

(9) Maka vienības apliecinājumiem būtu jādod iespēja maka atkarīgajām pusēm, kas pieprasa atribūtus no maka vienībām, verificēttās maka vienības spēkā esības statusu, ar kuru tās sazinās, jo maka vienības apliecinājumi ir jāatsauc, kad maka vienību vairs neuzskata par derīgu. Informācija par maka vienību spēkā esības statusu būtu jādara pieejama sadarbspējīgā veidā, lai nodrošinātu, ka to var izmantot visas maka atkarīgās puses. Turklāt gadījumos, kad maka lietotāji ir nozaudējuši savas maka vienības vai tiem vairs nav kontroles pār šīm maka vienībām, maka nodrošinātājiem būtu jāļauj maka lietotājiem pieprasīt viņu maka vienības atsaukšanu. Lai nodrošinātu privātumu un nesasaistāmību, dalībvalstīm būtu jāizmanto privātuma saglabāšanas metodes arī attiecībā uz maka vienības apliecinājumu. Tās var ietvert vairāku maka vienības apliecinājumu izmantošanu dažādiem mērķiem, tikai tādas minimālas informācijas atklāšanu par maku, kas nepieciešama darījumam, vai maka vienības apliecinājuma derīguma laika ierobežošanu kā alternatīvu atsaukšanas identifikatoru izmantošanai.

([8]) OV L 210, 14.6.2021., 51. lpp., ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) Eiropas Parlamenta un Padomes Regula (ES) 2024/1183 (2024. gada 11. aprīlis), ar ko groza Regulu (ES) Nr. 910/2014 attiecībā uz Eiropas digitālās identitātes satvara izveidi (OV L, 2024/1183, 30.4.2024., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(10) Lai nodrošinātu, ka visi maki tehniski spēj saņemt un uzrādīt personas identifikācijas datus un atribūtu elektroniskos apliecinājumus pārrobežu scenārijos, nemazinot sadarbspēju, makiem būtu jāatbalsta iepriekš noteikti datu formātu veidi un selektīva datu izpaušana. Kā noteikts Regulā (ES) Nr. 910/2014, selektīva izpaušana ir jēdziens, kas datu īpašniekam ļauj izpaust tikai konkrētas daļas no kādas lielākas datu kopas, lai saņēmēja puse iegūtu tikai to informāciju, kura ir vajadzīga lietotāja pieprasītā pakalpojuma sniegšanai. Tā kā makam ir jāiespējo izvēle, ka lietotājs atribūtus var izpaust selektīvi, II pielikumā norādītos standartus būtu jāpiemēro tā, lai šādu funkciju makiem iespējotu. Turklāt maki var atbalstīt citus formātus un funkcijas, lai atvieglotu izmantošanu konkrētos gadījumos.

(11) Darījumu reģistrēšana ir svarīgs rīks pārredzamības nodrošināšanai, kas izpaužas kā darījumu pārskata sniegšana maka lietotājam. Turklāt žurnāli būtu jāizmanto, lai pēc maka lietotāja pieprasījuma varētu ātri un viegli kopīgot konkrētu informāciju ar kompetentajām uzraudzības iestādēm, kas izveidotas saskaņā ar Regulas (ES) 2016/679 51. pantu, ja maka atkarīgo pušu rīcība ir aizdomīga.

(12) Lai maka lietotājs varētu parakstīties elektroniski, maka lietotājam būtu jāizsniedz kvalificēts sertifikāts, kas piesaistīts kvalificēta elektroniskā paraksta izveides ierīcei. Maka lietotājam vajadzētu būt piekļuvei paraksta izveides lietojumprogrammai. Lai gan kvalificētu sertifikātu izdošana ir pakalpojums, ko sniedz kvalificētu uzticamības pakalpojumu sniedzēji, maka nodrošinātājiem vai citām struktūrām vajadzētu būt iespējai nodrošināt pārējos komponentus. Piemēram, kvalificētas elektroniskā paraksta izveides ierīces kā pakalpojumu var pārvaldīt kvalificēti uzticamības pakalpojumu sniedzēji, vai tās var būt lokālas maka lietotāja ierīcei, piemēram, kā viedkarte. Tāpat paraksta izveides lietojumprogrammas var integrēt maka instancē, tās var būt atsevišķa lietojumprogramma maka lietotāja ierīcē vai tikt nodrošinātas attālināti.

(13) Datu eksporta un pārnesamības objekti var reģistrēt personas identifikācijas datus un atribūtu elektroniskos apliecinājumus, kas izdoti konkrētai maka vienībai. Šie objekti ļauj maku lietotājiem izgūt attiecīgos datus no savas maka vienības, lai pastiprinātu viņu tiesības uz datu pārnesamību. Maka nodrošinātāji tiek mudināti izmantot tos pašus tehniskos risinājumus, lai īstenotu arī maka vienību dublēšanas un atgūšanas procesus, dodot iespēju atgūt nozaudētās maka vienības vai pārsūtīt informāciju no viena maka nodrošinātāja citam, ja tas ir lietderīgi un ciktāl to var izdarīt, nekaitējot tiesībām uz datu aizsardzību un digitālās identitātes ekosistēmas drošībai.

(14) Maka atkarīgo pušu specifisko pseidonīmu ģenerēšanai būtu jāļauj maka lietotājiem autentificēties, nesniedzot maka atkarīgajām pusēm nevajadzīgu informāciju. Kā noteikts Regulā (ES) Nr. 910/2014, maka lietotājus nedrīkstētu atturēt no piekļūšanas pakalpojumiem ar pseidonīmu, ja vien nav juridiskas prasības autentifikācijas vajadzībām sniegt juridisko identitāti. Tāpēc makos būtu jāiekļauj funkcija lietotāja izvēlētu un pārvaldītu pseidonīmu ģenerēšanai, lai autentificētos, piekļūstot tiešsaistes pakalpojumiem. Regulas V pielikumā izklāstīto specifikāciju īstenošana attiecīgi iespējos minētās funkcijas. Visbeidzot, maka atkarīgajām pusēm nav jāpieprasa lietotājiem sniegt nekādus citus datus, izņemot tos, kas norādīti atkarīgo pušu reģistrā attiecībā uz maku paredzēto izmantošanu. Maka lietotājiem vajadzētu būt iespējai jebkurā brīdī verificēt atkarīgo pušu reģistrācijas datus.

(15) Kā noteikts Regulā (ES) 2024/1183, dalībvalstīm nav tieši vai netieši jāierobežo tādu fizisku vai juridisku personu piekļuve publiskiem un privātiem pakalpojumiem, kuras neizmanto makus, un būtu jādara pieejami piemēroti alternatīvi risinājumi.

(16) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([10]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2024. gada 30. septembrī sniedza savu atzinumu.

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

(17) Šajā regulā paredzētie pasākumi ir saskaņā ar Regulas (ES) Nr. 910/2014 48. pantā minētās komitejas atzinumu,

IR PIEŅĒMUSI ŠO REGULU.

I NODAĻA

VISPĀRĪGIE NOTEIKUMI

1. pants

Priekšmets un darbības joma

Šajā regulā ir paredzēti noteikumi par maku integritāti un pamatfunkcijām, un šie noteikumi regulāri jāatjaunina, lai nodrošinātu atbilstību tehnoloģiju un standartu attīstībai un darbam, kas veikts, pamatojoties uz Ieteikumu (ES) 2021/946 un jo īpaši arhitektūru un atsauces sistēmu.

2. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "maka drošas kriptogrāfijas lietojumprogramma" ir lietojumprogramma, kura sasaistē ar kriptogrāfiskām un nekriptogrāfiskām funkcijām, ko nodrošina maka drošas kriptogrāfijas ierīce, un, izmantojot šīs funkcijas, pārvalda kritiski svarīgus aktīvus;

2) "maka vienība" ir maka risinājuma unikāla konfigurācija, kas ietver maka instances, maka drošas kriptogrāfijas lietojumprogrammas un maka drošas kriptogrāfijas ierīces, ko maka nodrošinātājs nodrošina individuālam maka lietotājam;

3) "kritiski svarīgi aktīvi" ir aktīvi maka vienībā vai saistībā ar to, kas ir tik ārkārtīgi svarīgi, ka, ja to pieejamība, konfidencialitāte vai integritāte tiktu kompromitēta, tas ļoti nopietni un negatīvi ietekmētu spēju paļauties uz maka vienību;

4) "personas identifikācijas datu sniedzējs" ir fiziska vai juridiska persona, kas atbild par personas identifikācijas datu izdošanu un atsaukšanu un nodrošina, ka lietotāja personas identifikācijas dati ir kriptogrāfiski saistīti ar maka vienību;

5) "maka lietotājs" ir lietotājs, kas kontrolē maka vienību;

6) "maka atkarīgā puse" ir atkarīgā puse, kas, izmantojot digitālu mijiedarbību, plāno paļauties uz maka vienībām, lai sniegtu publiskus vai privātus pakalpojumus;

7) "maka nodrošinātājs" ir fiziska vai juridiska persona, kas nodrošina maka risinājumus;

8) "maka vienības apliecinājums" ir datu objekts, kas apraksta maka vienības komponentus vai ļauj šos komponentus autentificēt un validēt;

9) "iegultā informācijas izpaušanas procedūra" ir noteikumu kopums, kuru atribūtu elektroniskajā apliecinājumā iegūlis tā izsniedzējs un kurā norādīti nosacījumi, kas maka atkarīgajai pusei ir jāizpilda, lai piekļūtu atribūtu elektroniskajam apliecinājumam;

10) "maka instance" ir lietojumprogramma, kas uzstādīta un konfigurēta maka lietotāja ierīcē vai vidē, tā ir daļa no maka vienības un maka lietotājs to izmanto, lai mijiedarbotos ar maka vienību;

11) "maka risinājums" ir programmatūras, aparatūras, pakalpojumu, iestatījumu un konfigurāciju kombinācija, kas ietver maka instances, vienu vai vairākas maka drošas kriptogrāfijas lietojumprogrammas un vienu vai vairākas maka drošas kriptogrāfijas ierīces;

12) "maka drošas kriptogrāfijas ierīce" ir pret nesankcionētām manipulācijām noturīga ierīce, kas nodrošina vidi, kura ir sasaistīta ar maka drošas kriptogrāfijas lietojumprogrammu, kas šo vidi izmanto, lai aizsargātu kritiski svarīgus aktīvus un nodrošinātu kriptogrāfijas funkcijas kritiski svarīgu operāciju drošai izpildei;

13) “maka kriptogrāfijas operācija” ir kriptogrāfisks mehānisms, kas nepieciešams saistībā ar maka lietotāja autentificēšanu un personas identifikācijas datu vai atribūtu elektronisko apliecinājumu izdošanu vai uzrādīšanu;

14) “maka atkarīgās puses piekļuves sertifikāts” ir elektronisko zīmogu vai parakstu sertifikāts, ar ko autentificē un validē maka atkarīgo pusi un ko izdevis maka atkarīgās puses piekļuves sertifikātu nodrošinātājs;

15) “maka atkarīgās puses piekļuves sertifikātu nodrošinātājs” ir fiziska vai juridiska persona, ko dalībvalsts pilnvarojusi izdot atkarīgās puses piekļuves sertifikātus minētajā dalībvalstī reģistrētām maka atkarīgajām pusēm.

II NODAĻA

EIROPAS DIGITĀLĀS IDENTITĀTES MAKU INTEGRITĀTE

3. pants

Maka vienības integritāte

1. Pirms maka vienība nav sekmīgi autentificējusi maka lietotāju, maka vienības neveic nevienu no Regulas (ES) Nr. 910/2014 5.a panta 4. punktā uzskaitītajām funkcijām, izņemot maka lietotāja autentificēšanu, lai piekļūtu maka vienībai.

2. Maka nodrošinātāji katrai maka vienībai, parakstam vai zīmogam nodrošina vismaz vienu maka vienības apliecinājumu, kas atbilst 6. pantā noteiktajām prasībām. Sertifikātu, ko izmanto maka vienības apliecinājuma parakstīšanai vai apzīmogošanai, izdod saskaņā ar sertifikātu, kas iekļauts uzticamajā sarakstā, kurš minēts Īstenošanas regulā (ES) 2024/2980.

4. pants

Maka instances

1. Maka instances kritiski svarīgu aktīvu pārvaldībai izmanto vismaz vienu maka drošas kriptogrāfijas ierīci.

2. Maka nodrošinātāji nodrošina sakaru starp maka instancēm un maka drošās kriptogrāfijas lietojumprogrammām integritāti, autentiskumu un konfidencialitāti.

3. Ja kritiski svarīgie aktīvi ir saistīti ar elektroniskās identifikācijas veikšanu augstā uzticamības līmenī, maka kriptogrāfijas un citas darbības, kuru laikā apstrādā kritiski svarīgus aktīvus, veic saskaņā ar prasībām par elektroniskās identifikācijas līdzekļu īpašībām un izveidi augstā uzticamības līmenī, kā noteikts Komisijas Īstenošanas regulā (ES) 2015/1502 ([11]).

5. pants

Maka drošas kriptogrāfijas lietojumprogrammas

1. Maka nodrošinātāji nodrošina, ka maka drošas kriptogrāfijas lietojumprogrammas:

a) maka kriptogrāfijas operācijas ar kritiski svarīgiem aktīviem, kas nav nepieciešami maka vienībai maka lietotāja autentificēšanas nolūkā, veic tikai gadījumos, kad minētās lietojumprogrammas ir sekmīgi autentificējušas maka lietotājus;

([11]) Komisijas Īstenošanas regula(ES) 2015/1502 (2015. gada 8. septembris), kas saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 8. panta 3. punktu nosaka elektroniskās identifikācijas līdzekļu uzticamības līmeņu minimālās tehniskās specifikācijas un procedūras (OV L 235, 9.9.2015., 7. lpp., ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

b) ja tās autentificē maka lietotājus saistībā ar elektronisko identifikāciju augstā uzticamības līmenī, tās veic maka lietotāju autentifikāciju saskaņā ar prasībām par elektroniskās identifikācijas līdzekļu īpašībām un izveidi augstā uzticamības līmenī, kā noteikts Īstenošanas regulā (ES) 2015/1502;

c) spēj droši ģenerēt jaunas kriptogrāfiskās atslēgas;

d) spēj droši dzēst kritiski svarīgus aktīvus;

e) spēj ģenerēt pierādījumus par privātu atslēgu esību;

f) aizsargā privātās atslēgas, ko ģenerē minētās maka drošās kriptogrāfijas lietojumprogrammas, kamēr šīs atslēgas pastāv;

g) atbilst prasībām par elektroniskās identifikācijas līdzekļu īpašībām un izveidi augstā uzticamības līmenī, kā noteikts Īstenošanas regulā (ES) 2015/1502;

h) ir vienīgie komponenti, kas spēj veikt maka kriptogrāfijas un jebkādas citas darbības ar kritiski svarīgiem aktīviem saistībā ar elektroniskās identifikācijas veikšanu augstā uzticamības līmenī.

2. Ja maka nodrošinātāji nolemj maka drošas kriptogrāfijas lietojumprogrammu nodrošināt iegultam aizsardzības elementam, maka nodrošinātāji savu tehnisko risinājumu izstrādā, balstoties uz I pielikumā minētajām tehniskajām specifikācijām vai citām līdzvērtīgām tehniskajām specifikācijām.

6. pants

Maka vienības autentiskums un spēkā esība

1. Maka nodrošinātāji nodrošina, ka katrā maka vienībā ir maka vienības apliecinājumi.

2. Maka nodrošinātāji nodrošina, ka 1. punktā minētie maka vienības apliecinājumi satur publiskas atslēgas un ka attiecīgās privātās atslēgas ir aizsargātas ar maka drošas kriptogrāfijas ierīci.

3. Maka nodrošinātāji:

a) informē maka lietotājus par viņu tiesībām un pienākumiem saistībā ar viņu maka vienību;

b) nodrošina mehānismus, kas ir neatkarīgi no maka vienībām, lai droši identificētu un autentificētu maka lietotājus;

c) nodrošina, ka maka lietotājiem ir tiesības pieprasīt maka vienības apliecinājumu atsaukšanu, izmantojot b) apakšpunktā minētos autentifikācijas mehānismus.

7. pants

Maka vienības apliecinājumu atsaukšana

1. Maka nodrošinātāji ir vienīgās struktūras, kas spēj atsaukt to sniegtos maka vienības apliecinājumus.

2. Maka nodrošinātāji izstrādā publiski pieejamu procedūru, kurā precizē nosacījumus un termiņus maka vienības apliecinājumu atsaukšanai.

3. Ja maka nodrošinātāji ir atsaukuši maka vienības apliecinājumus, tie 24 stundu laikā informē ietekmētos maka lietotājus par viņu maka vienību atsaukšanu, norādot atsaukšanas iemeslu un sekas maka lietotājam. Šo informāciju sniedz kodolīgā, viegli saprotamā, skaidrā un vienkāršā valodā.

4. Ja maka nodrošinātāji ir atsaukuši maka vienības apliecinājumus, tie publiski informē par maka vienības apliecinājuma spēkā esības statusu, saglabājot privātumu, un apraksta minētās informācijas atrašanās vietu maka vienības atestācijā.

III NODAĻA

EIROPAS DIGITĀLĀS IDENTITĀTES MAKU PAMATFUNKCIJAS UN IEZĪMES

8. pants

Personas identifikācijas datu un atribūtu elektronisko apliecinājumu formāti

Maka nodrošinātāji nodrošina, ka maka risinājumi atbalsta tādu personas identifikācijas datu un atribūtu elektronisko apliecinājumu izmantošanu, kas izdoti saskaņā ar II pielikumā izklāstīto standartu sarakstu.

9. pants

Darījumu žurnāli

1. Neatkarīgi no tā, vai darījums tiek sekmīgi pabeigts, maka instances reģistrē visus darījumus ar maka atkarīgajām pusēm un citām maka vienībām, ieskaitot elektronisku parakstīšanu un apzīmogošanu.

2. Reģistrētā informācija ietver vismaz:

a) darījuma laiku un datumu;

b) attiecīgās maka atkarīgās puses un tās dalībvalsts nosaukumu un unikālo identifikatoru, kurā minētā maka atkarīgā puse ir reģistrēta, vai citu maka vienību gadījumā – attiecīgo informāciju no maka vienības apliecinājuma;

c) darījumā pieprasīto un uzrādīto datu veidu vai veidus;

d) nepabeigtu darījumu gadījumā – šādas nepabeigšanas iemeslu.

3. Maka nodrošinātāji nodrošina reģistrētās informācijas integritāti, autentiskumu un konfidencialitāti.

4. Maka instances reģistrē ziņojumus, ko maka lietotājs nosūta datu aizsardzības iestādēm, izmantojot savu maka vienību.

5. Šā panta 1. un 2. punktā minētie žurnāli, pamatojoties uz maka lietotāja nepārprotamu iepriekšēju piekrišanu, ir pieejami maka nodrošinātājam, ja tas nepieciešams maka pakalpojumu sniegšanai.

6. Žurnāli, kas minēti 1. un 2. punktā, ir pieejami tik ilgi, cik noteikts Savienības vai valsts tiesību aktos.

7. Maka nodrošinātāji ļauj maka lietotājiem eksportēt 2. punktā minēto reģistrēto informāciju.

10. pants

Iegultā informācijas izpaušanas procedūra

1. Maka nodrošinātāji nodrošina, ka to maka vienības var apstrādāt atribūtu elektroniskos apliecinājumus ar iegultām informācijas izpaušanas procedūrām, kas aprakstītas III pielikumā.

2. Maka instances spēj apstrādāt un uzrādīt šādas 1. punktā minētās iegultās informācijas izpaušanas procedūras saistībā ar datiem, kas saņemti no maka atkarīgās puses, kura ir pieprasījuma iesniedzējs.

3. Maka instances verificē, vai maka atkarīgā puse atbilst iegultās informācijas izpaušanas procedūras prasībām, un informē maka lietotāju par rezultātu.

11. pants

Kvalificētie elektroniskie paraksti un zīmogi

1. Maka nodrošinātāji nodrošina, ka maka lietotāji var saņemt kvalificētus sertifikātus attiecībā uz kvalificētiem elektroniskajiem parakstiem vai zīmogiem, kas ir saistīti ar kvalificēta paraksta vai zīmoga izveides ierīcēm, kuras var būt vietējas, ārējas vai attālinātas attiecībā pret maka instancēm.

2. Maka nodrošinātāji nodrošina, ka maka risinājumi spēj droši mijiedarboties ar vienu no šādiem kvalificētu paraksta vai zīmoga izveides ierīču veidiem: vietējas, ārējas vai attālināti pārvaldītas kvalificēta paraksta vai zīmoga izveides ierīces 1. punktā minēto kvalificēto sertifikātu izmantošanai.

3. Maka nodrošinātāji nodrošina, ka maka lietotājiem, kas ir fiziskas personas, vismaz neprofesionāliem mērķiem ir bezmaksas piekļuve paraksta izveides lietojumprogrammām, kas ļauj izveidot kvalificētus bezmaksas elektroniskos parakstus, izmantojot 1. punktā minētos sertifikātus.

12. pants

Paraksta izveides lietojumprogrammas

1. Paraksta izveides lietojumprogrammas, ko izmanto maka vienības, var nodrošināt maka nodrošinātāji, uzticamības pakalpojumu sniedzēji vai maka atkarīgās puses.

2. Paraksta izveides lietojumprogrammām ir šādas funkcijas:

a) maka lietotāju sniegto datu parakstīšana vai apzīmogošana;

b) atkarīgās puses sniegto datu parakstīšana vai apzīmogošana;

c) parakstu vai zīmogu izveide saskaņā vismaz ar IV pielikumā minētajiem obligātajiem formātiem;

d) maka lietotāju informēšana par paraksta vai zīmoga izveides procesa rezultātiem.

3. Paraksta izveides lietojumprogrammas var integrēt maka instancēs, vai tās var atrasties ārpus maka instancēm. Ja paraksta izveides lietojumprogrammu pamatā ir attālinātas kvalificēta paraksta izveides ierīces un ja tās ir integrētas maka instancēs, tās atbalsta IV pielikumā minēto lietojumprogrammu saskarni.

13. pants

Datu eksportēšana un pārnesamība

Ja tas ir tehniski iespējams un izņemot kritiski svarīgu aktīvu gadījumus, maka vienības atbalsta maka lietotāja personas datu drošu eksportu un pārnesamību, lai maka lietotājs varētu pāriet uz cita maka risinājuma maka vienību veidā, kas nodrošina augstu uzticamības līmeni, kā noteikts Īstenošanas regulā (ES) 2015/1502.

14. pants

Pseidonīmi

1. Maka vienības atbalsta pseidonīmu ģenerēšanu maka lietotājiem saskaņā ar V pielikumā noteiktajām tehniskajām specifikācijām.

2. Maka vienības atbalsta, ka pēc maka atkarīgās puses pieprasījuma tiek ģenerēts pseidonīms, kas ir specifisks un unikāls minētajai maka atkarīgajai pusei, un šo pseidonīmu maka atkarīgajai pusei nodrošina vai nu vienu pašu, vai kopā ar tādiem personas identifikācijas datiem vai atribūtu elektronisko apliecinājumu, ko pieprasījusi minētā maka atkarīgā puse.

IV NODAĻA

NOBEIGUMA NOTEIKUMI

15. pants

Stāšanās spēkā

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

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

Briselē, 2024. gada 28. novembrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

I PIELIKUMS

5. PANTĀ MINĒTO STANDARTU SARAKSTS

— SAM.01 Drošās lietojumprogrammas mobilajām ierīcēm – prasības, kas jāizpilda, lai atbalstītu trešo pušu sīklietotnes uz eSIM un eSE, izmantojot SAM. v1.1 2023, GSMA,

— GPC_GUI_ 217 *GlobalPlatform* SAM konfigurācija – tehniskā specifikācija SAM v1.0 2024-04 īstenošanai,

— GPC_SPE_0 34 *GlobalPlatform* kartes specifikācija – tehniskā specifikācija viedkartēm v2.3.1 2018-03,

— GPC_SPE_0 07 *GlobalPlatform* grozījums "A" – konfidenciālu karšu satura pārvaldība v1.2 2019-07,

— GPC_SPE_0 13 *GlobalPlatform* grozījums "D" – drošu kanālu protokols 03 v1.2 2020-04,

— GPC_SPE_0 93 *GlobalPlatform* grozījums "F" – drošu kanālu protokols 11 v1.4 2024-03,

— GPD_SPE_ 0 75 *Open Mobile API* specifikācija "OMAPI API", kas paredzēta mobilajām lietotnēm, lai piekļūtu aizsardzības elementiem uz lietotāju ierīcēm, v3.3 2018-08, *GlobalPlatform*.

II PIELIKUMS

8. PANTĀ MINĒTO STANDARTU SARAKSTS

— ISO/IEC.18013-5:2021

— "Verificējams akreditācijas datu modelis 1.1." (Globālā tīmekļa konsorcija ieteikums, 2022. gada 3. marts).

III PIELIKUMS

10. PANTĀ MINĒTO KOPĒJO IEGULTO INFORMĀCIJAS IZPAUŠANAS PROCEDŪRU SARAKSTS

1. Norāde “Nav procedūras” nozīmē, ka uz atribūtu elektroniskajiem apliecinājumiem neattiecas neviena procedūra.
2. “Tikai pilnvarotām atkarīgajām pusēm politika” nozīmē, ka maka lietotāji var izpaust atribūtu elektroniskos apliecinājumus tikai autentificētām atkarīgajām pusēm, kuras ir skaidri uzskaitītas informācijas izpaušanas procedūrā.
3. “Konkrēta uzticamības sakne” nozīmē, ka maka lietotājiem konkrētais atribūtu elektroniskais apliecinājums būtu jāatklāj tikai autentificētām maka atkarīgajām pusēm, kurām ir maka atkarīgās puses piekļuves sertifikāti, kas iegūti no konkrētas saknes (vai konkrētu sakņu saraksta) vai starpposma sertifikāta(-iem).

IV PIELIKUMS

12. PANTĀ MINĒTIE PARAKSTU UN ZĪMOGU FORMĀTI

1. Obligātais paraksta vai zīmoga formāts:

   PAdES (*PDF* uzlabots elektroniskais paraksts), kā norādīts ETSI EN 319 142-1 V1.1.1 (2016-04), elektroniskie paraksti un infrastruktūras (ESI), PAdES elektroniskie paraksti, 1. daļa. Pamatelementi un PAdES pamata paraksti.

2. Neobligāto parakstu vai zīmogu formātu saraksts:

   a) XAdES, kā norādīts ETSI EN 319 132-1 V1.2.1 (2022-02) "Elektroniskie paraksti un infrastruktūras (ESI)", XAdES elektroniskie paraksti, 1. daļa. "Pamatelementi un XAdES pamata paraksti (XAdES)" XML formāta parakstīšanai;

   b) JAdES, kā norādīts ETSI TS 119 182-1 V1.2.1 (2024-07) "Elektroniskie paraksti un infrastruktūras (ESI)", JAdES elektroniskie paraksti, 1. daļa. "Pamatelementi un JAdES pamata paraksti" JSON formāta parakstīšanai;

   c) CAdES (CMS uzlabots elektroniskais paraksts), kā norādīts ETSI EN 319 122-1 V1.3.1 (2023-06) "Elektroniskie paraksti un infrastruktūras (ESI)", CAdES elektroniskie paraksti, 1. daļa. "Pamatelementi un CAdES pamata paraksti" CMS formāta parakstīšanai;

   d) ASiC (saistītais paraksta konteiners), kā norādīts ETSI EN 319 162-1 V1.1.1 (2016-04) "Elektroniskie paraksti un infrastruktūras (ESI)", saistītie paraksta konteineri (ASiC), 1. daļa. ASiC (saistītais paraksta konteiners), kā norādīts ETSI EN 319 162-2 V1.1.1 (2016-04) "Elektroniskie paraksti un infrastruktūras (ESI)", saistītie paraksta konteineri (ASiC), 2. daļa. "Pamatelementi un ASiC pamata konteineri" konteineru parakstīšanai.

3. Lietojumprogrammas saskarne:

   — *Cloud Signature Consortium* (*CSC*) specifikācija v2.0 (2023. gada 20. aprīlis).

V PIELIKUMS

14. PANTĀ MINĒTĀS PSEIDONĪMU ĢENERĒŠANAS TEHNISKĀS SPECIFIKĀCIJAS

Tehniskās specifikācijas:

— *WebAuthn* – Globālā tīmekļa konsorcija ieteikums, 2021. gada 8. aprīlis, 2. līmenis, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.