Úradný vestník
Európskej únie

SK
Séria L

2024/2979

4.12.2024

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2024/2979

z 28. novembra 2024,

ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o integritu a základné funkcie európskych peňaženiek digitálnej identity

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES ([1]), a najmä na jeho článok 5a ods. 23,

keďže:

(1) Európsky rámec digitálnej identity stanovený nariadením (EÚ) č. 910/2014 je kľúčovým prvkom pri vytváraní bezpečného a interoperabilného ekosystému digitálnej identity v celej Únii. Keďže základným kameňom rámca sú európske peňaženky digitálnej identity (ďalej len „peňaženky“), jeho cieľom je uľahčiť fyzickým a právnickým osobám prístup k službám vo všetkých členských štátoch a zároveň zabezpečiť ochranu osobných údajov a súkromia.

(2) Na všetky činnosti spracúvania osobných údajov podľa tohto nariadenia sa vzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 ([2]) a v relevantných prípadoch smernica Európskeho parlamentu a Rady 2002/58/ES ([3]).

(3) V článku 5a ods. 23 nariadenia (EÚ) č. 910/2014 sa Komisia poveruje, aby v prípade potreby stanovila príslušné špecifikácie a postupy. Dosahuje sa to prostredníctvom štyroch vykonávacích nariadení, ktoré sa zaoberajú protokolmi a rozhraniami: vykonávacie nariadenie Komisie (EÚ) 2024/2982 ([4]), integritou a základnými funkciami: vykonávacie nariadenie Komisie (EÚ) 2024/2979 ([5]), osobnými identifikačnými údajmi a elektronickým osvedčením atribútov: vykonávacie nariadenie Komisie (EÚ) 2024/2977 ([6]), ako aj oznámeniami Komisii: vykonávacie nariadenie Komisie (EÚ) 2024/2980 ([7]). Týmto nariadením sa stanovujú príslušné požiadavky na integritu a základné funkcie európskych peňaženiek digitálnej identity.

([1]) Ú. v. EÚ L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([4]) Vykonávacie nariadenie Komisie (EÚ) 2024/2982 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o protokoly a rozhrania, ktoré má podporovať európsky rámec digitálnej identity (Ú. v. EÚ L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Vykonávacie nariadenie Komisie (EÚ) 2024/2979 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o integritu a základné funkcie európskych peňaženiek digitálnej identity, Ú. v. EÚ L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Vykonávacie nariadenie Komisie (EÚ) 2024/2977 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o osobné identifikačné údaje a elektronické osvedčenia atribútov vydané pre európske peňaženky digitálnej identity (Ú. v. EÚ L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Vykonávacie nariadenie Komisie (EÚ) 2024/2980 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o oznámenia Komisii týkajúce sa ekosystému európskej peňaženky digitálnej identity (Ú. v. EÚ L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) Komisia pravidelne posudzuje nové technológie, postupy, normy alebo technické špecifikácie. S cieľom zabezpečiť čo najvyššiu úroveň harmonizácie medzi členskými štátmi pri vývoji a certifikácii peňaženiek sa technické špecifikácie stanovené v tomto nariadení opierajú o prácu vykonanú na základe odporúčania Komisie (EÚ) 2021/946 z 3. júna 2021 o spoločnom súbore nástrojov Únie pre koordinovaný prístup k európskemu digitálnemu rámcu ([8]), a najmä o architektúru a referenčný rámec. V súlade s odôvodnením 75 nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1183 ([9]) by Komisia mala toto vykonávacie nariadenie podľa potreby preskúmať a aktualizovať, aby bolo v súlade s globálnym vývojom, architektúrou a referenčným rámcom a aby sa na vnútornom trhu dodržiavali najlepšie postupy.

(5) S cieľom zabezpečiť presnú komunikáciu, technickú diferenciáciu a jasné rozdelenie zodpovedností je potrebné rozlišovať medzi rôznymi komponentmi a konfiguráciami peňaženiek. Riešenie peňaženky by sa malo chápať ako kompletný systém poskytovaný poskytovateľom peňaženky, ktorý je potrebný na prevádzku peňaženky. To by malo zahŕňať softvérové a hardvérové komponenty, ako aj služby, nastavenia a konfigurácie potrebné na zabezpečenie správneho fungovania peňaženky. Riešenie peňaženky sa môže nachádzať v zariadeniach a prostrediach používateľov a v backendovej štruktúre poskytovateľa. Jednotka peňaženky by sa mala chápať ako špecifické nastavenie riešenia peňaženky pre jednotlivého používateľa. Mala by zahŕňať aplikáciu nainštalovanú v zariadení alebo prostredí používateľa peňaženky, s ktorou používateľ peňaženky priamo komunikuje (ďalej len „inštancia peňaženky“), a potrebné bezpečnostné prvky na ochranu údajov a transakcií používateľov. Tieto bezpečnostné prvky by mali zahŕňať špeciálny softvér alebo hardvér na šifrovanie a ochranu citlivých informácií. Inštancia peňaženky by mala byť súčasťou jednotky peňaženky a mala by používateľovi peňaženky umožňovať prístup k funkciám jeho peňaženky.

(6) Sú potrebné zabezpečené kryptografické aplikácie peňaženky ako samostatné špecializované komponenty v rámci jednotky peňaženky, a to nielen na ochranu kritických aktív, ako sú kryptografické súkromné kľúče, ale aj na poskytovanie kľúčových funkcií, ako je napríklad predkladanie elektronických osvedčení atribútov. Používanie spoločných technických špecifikácií môže poskytovateľom peňaženky uľahčiť prístup k zabudovaným zabezpečeným prvkom. Zabezpečené kryptografické aplikácie peňaženky sa môžu poskytovať rôznymi spôsobmi a pre rôzne druhy zabezpečených kryptografických zariadení peňaženky. Ak poskytovatelia peňaženky poskytujú zabezpečené kryptografické aplikácie peňaženky na mieru ako aplety Java Card pre zabudované zabezpečené prvky, poskytovatelia peňaženky by mali dodržiavať normy uvedené v prílohe I alebo rovnocenné technické špecifikácie.

(7) Jednotky peňaženky majú umožniť poskytovateľom osobných identifikačných údajov alebo elektronických osvedčení atribútov overiť, že tieto údaje alebo osvedčenia vydávajú pravým jednotkám peňaženky daného používateľa peňaženky.

(8) V záujme zabezpečenia štandardnej ochrany údajov už v štádiu návrhu by peňaženky mali byť vybavené dostupnými najmodernejšími technikami na zvýšenie ochrany súkromia. Tieto funkcie by mali poskytovať možnosť, aby sa peňaženky mohli používať bez toho, aby bol používateľ peňaženky vysledovateľný v rôznych stranách spoliehajúcich sa na peňaženku, ak je to v scenári používania možné. Poskytovatelia peňaženky by mali napríklad zvážiť najmodernejšie zmierňujúce opatrenia v oblasti ochrany súkromia v súvislosti s osvedčeniami jednotky peňaženky, ako je používanie krátkodobých osvedčení jednotiek peňaženky alebo hromadné vydávanie. Okrem toho by sa v zahrnutých pravidlách sprístupňovania informácií mali pre používateľov peňaženky uvádzať varovania pred nevhodným alebo nezákonným sprístupňovaním atribútov z elektronických osvedčení atribútov.

(9) Osvedčenia jednotiek peňaženky by mali stranám spoliehajúcim sa na peňaženku, ktoré požadujú atribúty od jednotiek peňaženky, umožňovať overiť stav platnosti jednotky peňaženky, s ktorou komunikujú, keďže osvedčenia jednotiek peňaženky sa majú zrušiť, keď sa jednotka peňaženky už nepovažuje za platnú. Informácie týkajúce sa stavu platnosti jednotiek peňaženky by mali byť k dispozícii interoperabilným spôsobom, aby sa zabezpečilo, že ich môžu používať všetky strany spoliehajúce sa na peňaženku. Okrem toho v prípadoch, keď používatelia peňaženky stratili svoje jednotky peňaženky alebo nad nimi už nemajú kontrolu, by poskytovatelia peňaženky mali používateľom peňaženky umožniť požiadať o zrušenie ich jednotky peňaženky. S cieľom zabezpečiť súkromie a neprepojiteľnosť by členské štáty mali používať techniky ochrany súkromia aj v prípade osvedčenia jednotky peňaženky. Môže sem patriť používanie viacerých osvedčení jednotky peňaženky na rôzne účely, zverejňovanie len minimálneho množstva relevantných informácií o peňaženke, ktoré sú nevyhnutné na transakciu, alebo obmedzenie životnosti osvedčenia jednotky peňaženky ako alternatívy k používaniu identifikátorov v prípade zrušenia.

([8]) Ú. v. EÚ L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o zriadenie európskeho rámca digitálnej identity (Ú. v. EÚ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(10) S cieľom zabezpečiť, aby všetky peňaženky boli technicky schopné prijímať a predkladať osobné identifikačné údaje a elektronické osvedčenia atribútov v cezhraničných scenároch bez narušenia interoperability, peňaženky by mali podporovať vopred určené typy formátov údajov a selektívne sprístupňovanie informácií. Ako sa stanovuje v nariadení (EÚ) č. 910/2014, selektívne sprístupňovanie informácií je koncepcia, ktorá oprávňuje vlastníka údajov zverejniť len určité časti väčšieho súboru údajov, aby prijímajúci subjekt získal len také informácie, ktoré sú potrebné na poskytovanie služby, ktorú požaduje používateľ. Keďže peňaženky majú používateľovi umožniť selektívne zverejňovanie atribútov, normy uvedené v prílohe II by sa mali uplatňovať spôsobom, ktorý umožňuje túto funkciu peňaženiek. Okrem toho môžu peňaženky podporovať aj iné formáty a funkcie na uľahčenie špecifických prípadov použitia.

(11) Zaznamenávanie transakcií je dôležitým nástrojom na zabezpečenie transparentnosti formou poskytovania prehľadu transakcií používateľovi peňaženky. Okrem toho by sa v prípade podozrivého správania strán spoliehajúcich sa na peňaženku mali na žiadosť používateľa peňaženky používať logy umožňujúce rýchlu a jednoduchú výmenu určitých informácií s príslušnými dozornými orgánmi zriadenými podľa článku 51 nariadenia (EÚ) 2016/679.

(12) Aby sa mohol používateľ peňaženky elektronicky podpisovať, mal by mu byť vydaný kvalifikovaný certifikát, ktorý je viazaný na zariadenie na vyhotovenie kvalifikovaného elektronického podpisu. Používateľ peňaženky by mal mať prístup k aplikácii na vyhotovenie podpisu. Zatiaľ čo vydávanie kvalifikovaných certifikátov je službou kvalifikovaných poskytovateľov dôveryhodných služieb, poskytovatelia peňaženky alebo iné subjekty by mali byť schopné poskytovať ostatné komponenty. Napríklad zariadenia na vyhotovenie kvalifikovaného elektronického podpisu môžu byť spravované kvalifikovanými poskytovateľmi dôveryhodných služieb ako služba alebo sa môžu nachádzať lokálne v zariadení používateľa peňaženky, napríklad ako čipová karta. Podobne aj aplikácie na vyhotovenie podpisu môžu byť integrované v inštancii peňaženky, môžu byť samostatnou aplikáciou v zariadení používateľa peňaženky alebo môžu byť poskytované na diaľku.

(13) Objekty exportu a prenosnosti údajov môžu zaznamenávať osobné identifikačné údaje a elektronické osvedčenia atribútov, ktoré boli vydané konkrétnej jednotke peňaženky. Tieto objekty umožňujú používateľom peňaženky extrahovať príslušné údaje z ich jednotky peňaženky s cieľom posilniť ich právo na prenosnosť údajov. Poskytovatelia peňaženky sa vyzývajú, aby používali rovnaké technické riešenia aj na zavedenie procesov zálohovania a obnovy jednotiek peňaženky, ktoré umožnia obnovu stratených jednotiek peňaženky alebo prenos informácií od jedného poskytovateľa peňaženky k druhému, ak je to vhodné a pokiaľ sa to dá vykonať bez toho, aby sa narušilo právo na ochranu údajov a bezpečnosť ekosystému digitálnej identity.

(14) Vytváranie pseudonymov špecifických pre strany spoliehajúce sa na peňaženku by používateľom peňaženky malo umožniť autentifikovať sa bez toho, aby poskytovali stranám spoliehajúcim sa na peňaženku informácie, ktoré nie sú nevyhnutné. Ako sa stanovuje v nariadení (EÚ) č. 910/2014, používateľom peňaženky sa nesmie brániť v prístupe k službám pod pseudonymom, ak pre právnu identitu neexistuje právna požiadavka na autentifikáciu. Peňaženky preto majú obsahovať funkciu umožňujúcu používateľom vytvárať si pseudonymy, ktoré si sami vyberú a spravujú a ktoré slúžia na autentifikáciu pri prístupe k online službám. Vykonávaním špecifikácií stanovených v prílohe V by sa mali zodpovedajúcim spôsobom zaktivovať tieto funkcie. Ďalej strany spoliehajúce sa na peňaženku nemajú od používateľov požadovať poskytnutie žiadnych iných údajov okrem údajov, ktoré sú uvedené na zamýšľané použitie peňaženiek v registri spoliehajúcej sa strany. Používatelia peňaženky by mali mať možnosť kedykoľvek overiť registračné údaje spoliehajúcich sa strán.

(15) Ako je uvedené v nariadení (EÚ) 2024/1183, členské štáty nesmú priamo ani nepriamo obmedzovať prístup k verejným alebo súkromným službám pre fyzické alebo právnické osoby, ktoré sa rozhodnú nepoužívať peňaženky, a musia sprístupniť vhodné alternatívne riešenia.

(16) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([10]) sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 30. septembra 2024 svoje stanovisko.

([10]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(17) Opatrenia ustanovené v tomto nariadení sú v súlade so stanoviskom výboru uvedeného v článku 48 nariadenia (EÚ) č. 910/2014,

PRIJALA TOTO NARIADENIE:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy a rozsah pôsobnosti

Týmto nariadením sa stanovujú pravidlá integrity a základných funkcií peňaženiek, ktoré sa majú pravidelne aktualizovať, aby boli v súlade s vývojom technológií a noriem a s prácou vykonanou na základe odporúčania (EÚ) 2021/946, a najmä s architektúrou a referenčným rámcom.

Článok 2

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „zabezpečená kryptografická aplikácia peňaženky“ je aplikácia, ktorá spravuje kritické aktíva tak, že je prepojená s kryptografickými a nekryptografickými funkciami poskytovanými zabezpečeným kryptografickým zariadením peňaženky a tieto funkcie využíva;
2. „jednotka peňaženky“ je jedinečná konfigurácia riešenia peňaženky, ktorá zahŕňa inštancie peňaženky, zabezpečené kryptografické aplikácie peňaženky a zabezpečené kryptografické zariadenia peňaženky, ktoré poskytovateľ peňaženky poskytuje jednotlivým používateľom peňaženky;
3. „kritické aktíva“ sú aktíva v rámci jednotky peňaženky alebo v súvislosti s ňou, ktoré majú taký mimoriadny význam, že narušenie ich dostupnosti, dôvernosti alebo integrity by malo veľmi vážny, oslabujúci účinok na schopnosť spoliehať sa na jednotku peňaženky;
4. „poskytovateľ osobných identifikačných údajov“ je fyzická alebo právnická osoba zodpovedná za vydávanie a zrušenie osobných identifikačných údajov a za zabezpečenie kryptografickej väzby osobných identifikačných údajov používateľa na jednotku peňaženky;
5. „používateľ peňaženky“ je používateľ, ktorý má kontrolu nad jednotkou peňaženky;
6. „strana spoliehajúca sa na peňaženku“ je spoliehajúca sa strana, ktorá má v úmysle spoliehať sa na jednotky peňaženky pri poskytovaní verejných alebo súkromných služieb prostredníctvom digitálnej interakcie;
7. „poskytovateľ peňaženky“ je fyzická alebo právnická osoba, ktorá poskytuje riešenia peňaženky;
8. „osvedčenie jednotky peňaženky“ je dátový objekt, ktorý opisuje komponenty jednotky peňaženky alebo umožňuje autentifikáciu a validáciu týchto komponentov;
9. „zahrnuté pravidlá sprístupňovania informácií“ sú súbor pravidiel zakotvených v elektronickom osvedčení atribútov jeho poskytovateľom, v ktorom sa uvádzajú podmienky, ktoré musí strana spoliehajúca sa na peňaženku splniť, aby mala prístup k elektronickému osvedčeniu atribútov;
10. „inštancia peňaženky“ je aplikácia nainštalovaná a nakonfigurovaná v zariadení alebo prostredí používateľa peňaženky, ktorá je súčasťou jednotky peňaženky a ktorú používateľ peňaženky používa na interakciu s jednotkou peňaženky;
11. „riešenie peňaženky“ je kombinácia softvéru, hardvéru, služieb, nastavení a konfigurácií vrátane inštancií peňaženky, jednej alebo viacerých zabezpečených kryptografických aplikácií peňaženky a jedného alebo viacerých zabezpečených kryptografických zariadení peňaženky;
12. „zabezpečené kryptografické zariadenie peňaženky“ je zariadenie odolné voči neoprávnenej manipulácii, poskytujúce prostredie, ktoré je prepojené so zabezpečenou kryptografickou aplikáciou peňaženky a ktoré zabezpečená kryptografická aplikácia peňaženky využíva na ochranu kritických aktív a poskytovanie kryptografických funkcií na účely bezpečného vykonávania kritických operácií;

13. „kryptografická operácia peňaženky“ je kryptografický mechanizmus potrebný v súvislosti s autentifikáciou používateľa peňaženky a vydaním alebo predložením osobných identifikačných údajov alebo elektronického osvedčenia atribútov;

14. „prístupový certifikát strany spoliehajúcej sa na peňaženku“ je certifikát pre elektronické pečate alebo podpisy, ktorým sa autentifikuje a validuje strana spoliehajúca sa na peňaženku a ktorý vydal poskytovateľ prístupových certifikátov strany spoliehajúcej sa na peňaženku;

15. „poskytovateľ prístupových certifikátov strany spoliehajúcej sa na peňaženku“ je fyzická alebo právnická osoba, ktorú členský štát poveril vydávaním prístupových certifikátov spoliehajúcej sa strany stranám spoliehajúcim sa na peňaženku registrovaným v danom členskom štáte.

KAPITOLA II

INTEGRITA EURÓPSKYCH PEŇAŽENIEK DIGITÁLNEJ IDENTITY

Článok 3

Integrita jednotky peňaženky

1. Jednotky peňaženky nesmú vykonávať žiadnu funkciu uvedenú v článku 5a ods. 4 nariadenia (EÚ) č. 910/2014 s výnimkou autentifikácie používateľa peňaženky na získanie prístupu k jednotke peňaženky, kým jednotka peňaženky nevykoná úspešnú autentifikáciu daného používateľa peňaženky.

2. Poskytovatelia peňaženky pre každú jednotku peňaženky podpíšu alebo zapečatia aspoň jedno osvedčenie jednotky peňaženky, ktoré je v súlade s požiadavkami stanovenými v článku 6. Certifikát použitý na podpísanie alebo zapečatenie osvedčenia jednotky peňaženky sa vydáva na základe certifikátu uvedeného v dôveryhodnom zozname uvedenom vo vykonávacom nariadení (EÚ) 2024/2980.

Článok 4

Inštancie peňaženky

1. Inštancie peňaženky používajú na správu kritických aktív aspoň jedno zabezpečené kryptografické zariadenie peňaženky.

2. Poskytovatelia peňaženky zabezpečia integritu, pravosť a dôvernosť komunikácie medzi inštanciami peňaženky a zabezpečenými kryptografickými aplikáciami peňaženky.

3. Ak sa kritické aktíva týkajú vykonávania elektronickej identifikácie na úrovni zabezpečenia „vysoká“, kryptografické operácie peňaženky alebo iné operácie spracúvajúce kritické aktíva sa vykonávajú v súlade s požiadavkami na vlastnosti a uspôsobenie prostriedkov elektronickej identifikácie na úrovni zabezpečenia „vysoká“, ako sa stanovuje vo vykonávacom nariadení Komisie (EÚ) 2015/1502 ([11]).

Článok 5

Zabezpečené kryptografické aplikácie peňaženky

1. Poskytovatelia peňaženky zaistia, aby zabezpečené kryptografické aplikácie peňaženky:

a) vykonávali kryptografické operácie peňaženky zahŕňajúce kritické aktíva iné než tie, ktoré jednotka peňaženky potrebuje na autentifikáciu používateľa peňaženky, len v prípadoch, keď tieto aplikácie úspešne autentifikovali používateľov peňaženky;

([11]) Vykonávacie nariadenie Komisie (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (Ú. v. EÚ L 235, 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

b) ak autentifikujú používateľov peňaženky v kontexte vykonávania elektronickej identifikácie na úrovni zabezpečenia „vysoká“, vykonávali autentifikáciu používateľov peňaženky v súlade s požiadavkami na vlastnosti a uspôsobenie prostriedkov elektronickej identifikácie na úrovni zabezpečenia „vysoká“, ako sa stanovuje vo vykonávacom nariadení (EÚ) 2015/1502;

c) boli schopné bezpečne generovať nové kryptografické kľúče;

d) boli schopné bezpečne vymazať kritické aktíva;

e) boli schopné vygenerovať dôkaz o vlastníctve súkromných kľúčov;

f) chránili súkromné kľúče vygenerované týmito zabezpečenými kryptografickými aplikáciami peňaženky počas existencie kľúčov;

g) spĺňali požiadavky na vlastnosti a uspôsobenie prostriedkov elektronickej identifikácie na úrovni zabezpečenia „vysoká“, ako sa stanovuje vo vykonávacom nariadení (EÚ) 2015/1502;

h) boli jedinými komponentmi, ktoré sú schopné vykonávať kryptografické operácie peňaženky a akékoľvek iné operácie s kritickými aktívami v kontexte vykonávania elektronickej identifikácie na úrovni zabezpečenia „vysoká“.

2. Ak sa poskytovatelia peňaženky rozhodnú poskytnúť zabudovanému zabezpečenému prvku zabezpečenú kryptografickú aplikáciu peňaženky, títo poskytovatelia peňaženky postavia svoje technické riešenie na technických špecifikáciách uvedených v prílohe I alebo na iných rovnocenných technických špecifikáciách.

Článok 6

Pravosť a platnosť jednotky peňaženky

1. Poskytovatelia peňaženky zabezpečia, aby každá jednotka peňaženky obsahovala osvedčenia jednotky peňaženky.

2. Poskytovatelia peňaženky zabezpečia, aby osvedčenia jednotiek peňaženky uvedené v odseku 1 obsahovali verejné kľúče a aby príslušné súkromné kľúče boli chránené zabezpečeným kryptografickým zariadením peňaženky.

3. Poskytovatelia peňaženky:

a) informujú používateľov peňaženky o ich právach a povinnostiach v súvislosti s ich jednotkou peňaženky;

b) poskytujú mechanizmy na bezpečnú identifikáciu a autentifikáciu používateľov peňaženky, ktoré sú nezávislé od jednotiek peňaženky;

c) zabezpečia, aby používatelia peňaženky mali právo požiadať o zrušenie svojich osvedčení jednotky peňaženky pomocou mechanizmov autentifikácie uvedených v písmene b).

Článok 7

Zrušenie osvedčení jednotky peňaženky

1. Poskytovatelia peňaženky sú jedinými subjektmi, ktoré môžu zrušiť osvedčenia jednotky peňaženky, ktoré poskytli.

2. Poskytovatelia peňaženky vypracujú verejne dostupné pravidlá, v ktorých stanovia podmienky a časový rámec pre zrušenie osvedčení jednotiek peňaženky.

3. Ak poskytovatelia peňaženky zrušili osvedčenia jednotiek peňaženky, do 24 hodín informujú dotknutých používateľov peňaženky o zrušení ich jednotiek peňaženky vrátane dôvodu zrušenia a dôsledkov pre používateľa peňaženky. Tieto informácie sa poskytujú stručným a ľahko dostupným spôsobom v zrozumiteľnom a jednoduchom jazyku.

4. Ak poskytovatelia peňaženky zrušili osvedčenia jednotiek peňaženky, zverejnia stav platnosti osvedčenia jednotky peňaženky spôsobom zachovávajúcim súkromie a opíšu umiestnenie týchto informácií v osvedčení jednotky peňaženky.

KAPITOLA III

ZÁKLADNÉ FUNKCIE A VLASTNOSTI EURÓPSKYCH PEŇAŽENIEK DIGITÁLNEJ IDENTITY

Článok 8

Formáty osobných identifikačných údajov a elektronických osvedčení atribútov

Poskytovatelia peňaženky zabezpečia, aby riešenia peňaženky podporovali používanie osobných identifikačných údajov a elektronických osvedčení atribútov vydaných v súlade so zoznamom noriem uvedených v prílohe II.

Článok 9

Logy transakcií

1. Inštancie peňaženky zaznamenávajú všetky transakcie so stranami spoliehajúcimi sa na peňaženku a s inými jednotkami peňaženky vrátane elektronického podpisovania a pečatenia bez ohľadu na to, či bola transakcia úspešne dokončená alebo nie.

2. Zaznamenané informácie musia obsahovať aspoň:

a) čas a dátum transakcie;

b) meno, kontaktné údaje a jedinečný identifikátor príslušnej strany spoliehajúcej sa na peňaženku a členský štát, v ktorom je táto strana spoliehajúca sa na peňaženku usadená, alebo v prípade iných jednotiek peňaženky príslušné informácie z osvedčenia jednotky peňaženky;

c) typ alebo typy údajov požadovaných a predložených v transakcii;

d) v prípade nedokončených transakcií dôvod ich nedokončenia.

3. Poskytovatelia peňaženky zabezpečia integritu, pravosť a dôvernosť zaznamenaných informácií.

4. Inštancie peňaženky zaznamenávajú správy, ktoré používateľ peňaženky zasiela orgánom pre ochranu údajov prostredníctvom svojej jednotky peňaženky.

5. Logy uvedené v odsekoch 1 a 2 sú prístupné poskytovateľovi peňaženky, ak je to potrebné na poskytovanie služieb peňaženky, na základe výslovného predchádzajúceho súhlasu používateľa peňaženky.

6. Logy uvedené v odsekoch 1 a 2 zostávajú prístupné tak dlho, ako sa to vyžaduje v právnych predpisoch Únie alebo vo vnútroštátnych právnych predpisoch.

7. Poskytovatelia peňaženky umožnia používateľom peňaženky exportovať zaznamenané informácie uvedené v odseku 2.

Článok 10

Zahrnuté sprístupňovanie informácií

1. Poskytovatelia peňaženky zabezpečia, aby jednotky peňaženky, ktoré poskytujú, mohli spracúvať elektronické osvedčenia atribútov so spoločnými zahrnutými pravidlami sprístupňovania informácií uvedenými v prílohe III.

2. Inštancie peňaženky musia byť schopné spracovať a predkladať takéto zahrnuté pravidlá sprístupňovania informácií uvedené v odseku 1 spolu s údajmi prijatými od žiadajúcej strany spoliehajúcej sa na peňaženku.

3. Inštancie peňaženky overia, či strana spoliehajúca sa na peňaženku spĺňa požiadavky zahrnutých pravidiel sprístupňovania informácií a o výsledku informujú používateľa peňaženky.

Článok 11

Kvalifikované elektronické podpisy a pečate

1. Poskytovatelia peňaženky zabezpečia, aby používatelia peňaženky mohli získať kvalifikované certifikáty pre kvalifikované elektronické podpisy alebo pečate, ktoré sú spojené so zariadeniami na vyhotovenie kvalifikovaného podpisu alebo pečate, ktoré sú vo vzťahu k inštanciám peňaženky buď lokálne, externé alebo vzdialené.

2. Poskytovatelia peňaženky zabezpečia, aby riešenia peňaženky bolo možné bezpečne prepojiť s jedným z nasledujúcich typov zariadení na vyhotovenie kvalifikovaného podpisu alebo pečate: lokálne, externé alebo vzdialene spravované zariadenia na vyhotovenie kvalifikovaného podpisu alebo pečate na účely používania kvalifikovaných certifikátov uvedených v odseku 1.

3. Poskytovatelia peňaženky zabezpečia, aby používatelia peňaženky, ktorí sú fyzickými osobami, mali aspoň na neprofesionálne účely bezplatný prístup k aplikáciám na vyhotovenie podpisu, ktoré umožňujú bezplatné vyhotovenie kvalifikovaných elektronických podpisov s použitím certifikátov uvedených v odseku 1.

Článok 12

Aplikácie na vyhotovenie podpisu

1. Aplikácie na vyhotovenie podpisu, ktoré používajú jednotky peňaženky, môžu poskytovať buď poskytovatelia peňaženky, poskytovatelia dôveryhodných služieb alebo strany spoliehajúce sa na peňaženku.

2. Aplikácie na vyhotovenie podpisu majú tieto funkcie:

a) podpisovanie alebo pečatenie údajov poskytnutých používateľom peňaženky;

b) podpisovanie alebo pečatenie údajov poskytnutých spoliehajúcou sa stranou;

c) vyhotovenie podpisov alebo pečatí aspoň v súlade s povinnými formátmi uvedenými v prílohe IV;

d) informovanie používateľov peňaženky o výsledku procesu vyhotovenia podpisu alebo pečate.

3. Aplikácie na vyhotovenie podpisu môžu byť buď integrované do inštancií peňaženky, alebo môžu byť externé. Ak sa aplikácie na vyhotovenie podpisu spoliehajú na zariadenia na vyhotovenie kvalifikovaného podpisu na diaľku a ak sú integrované do inštancií peňaženky, podporujú aplikačné programovacie rozhranie uvedené v prílohe IV.

Článok 13

Export a prenosnosť údajov

Jednotky peňaženky podporujú bezpečný export a prenosnosť osobných údajov používateľa peňaženky, ak je to technicky možné a s výnimkou prípadov kritických aktív, s cieľom umožniť používateľovi peňaženky migrovať do jednotky peňaženky iného riešenia peňaženky spôsobom zaručujúcim úroveň zabezpečenia „vysoká“, ako sa stanovuje vo vykonávacom nariadení (EÚ) 2015/1502.

Článok 14

Pseudonymy

1. Jednotky peňaženky podporujú vytváranie pseudonymov pre používateľov peňaženky v súlade s technickými špecifikáciami uvedenými v prílohe V.

2. Jednotky peňaženky podporujú vytvorenie pseudonymu, ktorý je špecifický a jedinečný pre danú stranu spoliehajúcu sa na peňaženku, na žiadosť strany spoliehajúcej sa na peňaženku a poskytujú tento pseudonym strane spoliehajúcej sa na peňaženku, a to samostatne alebo v kombinácii s akýmikoľvek osobnými identifikačnými údajmi alebo elektronickým osvedčením atribútu, ktoré požaduje daná strana spoliehajúca sa na peňaženku.

KAPITOLA IV

ZÁVEREČNÉ USTANOVENIA

Článok 15

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 28. novembra 2024

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

PRÍLOHA I

ZOZNAM NORIEM UVEDENÝCH V ČLÁNKU 5

— 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.

PRÍLOHA II

ZOZNAM NORIEM UVEDENÝCH V ČLÁNKU 8

— ISO/IEC.18013-5:2021

— „Verifiable Credentials Data Model 1.1.“ (model údajov overiteľných certifikátov), odporúčanie W3C, 3. marec 2022.

PRÍLOHA III

ZOZNAM SPOLOČNÝCH ZAHRNUTÝCH PRAVIDIEL SPRÍSTUPŇOVANIA INFORMÁCIÍ UVEDENÝCH V ČLÁNKU 10

1. „Žiadne pravidlá“ – znamená, že na elektronické osvedčenia atribútov sa nevzťahujú žiadne pravidlá.
2. „Pravidlá týkajúce sa len oprávnených spoliehajúcich sa strán“ – znamená, že používatelia peňaženky môžu sprístupňovať elektronické osvedčenia atribútov len autentifikovaným spoliehajúcim sa stranám, ktoré sú výslovne uvedené v pravidlách sprístupňovania informácií.
3. „Konkrétny koreň dôvery“ – znamená, že používatelia peňaženky by mali sprístupňovať konkrétne elektronické osvedčenie atribútov len autentifikovaným stranám spoliehajúcim sa na peňaženku, ktoré disponujú prístupovými certifikátmi strany spoliehajúcej sa na peňaženku odvodenými od konkrétneho koreňového certifikátu (prípadne zoznamu konkrétnych koreňových certifikátov) alebo sprostredkovateľského certifikátu (certifikátov).

PRÍLOHA IV

FORMÁTY PODPISU A PEČATE UVEDENÉ V ČLÁNKU 12

1. Povinný formát podpisu alebo pečate:

   PAdES (zdokonalený elektronický podpis PDF) špecifikovaný v ETSI EN 319 142-1 V1.1.1 (2016-04); elektronické podpisy a infraštruktúra (ESI); digitálne podpisy PAdES; časť 1: Základné moduly a základné podpisy PAdES.

2. Zoznam voliteľných formátov podpisov alebo pečatí:

   a) XAdES špecifikovaný v „ETSI EN 319 132-1 V1.2.1 (2022-02) Elektronické podpisy a infraštruktúra (ESI); digitálne podpisy XAdES; časť 1: Základné moduly a základné podpisy XAdES (XAdES)“ pre podpisovanie formátu XML;

   b) JAdES špecifikovaný v „ETSI TS 119 182-1 V1.2.1 (2024-07) Elektronické podpisy a infraštruktúra (ESI); digitálne podpisy JAdES; časť 1: Základné moduly a základné podpisy JAdES“ pre podpisovanie formátu JSON;

   c) CAdES (zdokonalený elektronický podpis CMS) špecifikovaný v „ETSI EN 319 122-1 V1.3.1 (2023-06) Elektronické podpisy a infraštruktúra (ESI); digitálne podpisy CAdES; časť 1: Základné moduly a základné podpisy CAdES“ pre podpisovanie formátu CMS;

   d) ASiC (pridružený podpisový kontajner) špecifikovaný v „ETSI EN 319 162-1 V1.1.1 (2016-04) Elektronické podpisy a infraštruktúra (ESI); pridružené podpisové kontajnery (ASiC); časť 1: Základné moduly a základné kontajnery ASiC a ETSI EN 319 162-2 V1.1.1 (2016-04) Elektronické podpisy a infraštruktúra (ESI); pridružené podpisové kontajnery (ASiC); časť 2: Doplňujúce kontajnery ASiC“ pre podpisovanie kontajnerov.

3. Aplikačné programovacie rozhranie:

   — Špecifikácia konzorcia pre cloudové podpisy (CSC) v2.0 (20. apríla 2023).

PRÍLOHA V

TECHNICKÉ ŠPECIFIKÁCIE PRE VYTVÁRANIE PSEUDONYMOV UVEDENÉ V ČLÁNKU 14

Technické špecifikácie:

— WebAuthn – Odporúčanie W3C, 8. apríl 2021, úroveň 2, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.