2024/2979

4.12.2024

# PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2024/2979

## ze dne 28. listopadu 2024,

## kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o integritu a základní funkce evropských peněženek digitální identity

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES ([1]), a zejména na čl. 5a odst. 23 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Evropský rámec pro digitální identitu zřízený nařízením (EU) č. 910/2014 je klíčovým prvkem při vytváření bezpečného a interoperabilního ekosystému digitální identity v celé Unii. Základem rámce jsou evropské peněženky digitální identity (dále jen „peněženky“), jejichž cílem je usnadnit fyzickým a právnickým osobám přístup ke službám v členských státech a zároveň zajistit ochranu osobních údajů a soukromí.

(2) Na všechny činnosti zpracování osobních údajů podle tohoto nařízení se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ([2]) a v příslušných případech směrnice Evropského parlamentu a Rady 2002/58/ES ([3]).

(3) Ustanovení čl. 5a odst. 23 nařízení (EU) č. 910/2014 pověřuje Komisi, aby v případě potřeby stanovila příslušné specifikace a postupy. Toho je dosaženo prostřednictvím čtyř prováděcích nařízení, která se zabývají protokoly a rozhraními: prováděcí nařízení Komise (EU) 2024/2982 ([4]), integritou a základními funkcemi: prováděcí nařízení Komise (EU) 2024/2979 ([5]), digitální identity, osobními identifikačními údaji a elektronickým potvrzením atributů: prováděcí nařízení Komise (EU) 2024/2977 ([6]), , jakož i oznámeními Komisi: prováděcí nařízení Komise (EU) 2024/2980 ([7]). Toto nařízení stanoví příslušné požadavky na integritu a základní funkce evropských peněženek digitální identity.

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

([2]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([4]) Prováděcí nařízení Komise (EU) 2024/2982 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o protokoly a rozhraní, které mají být podporovány evropským rámcem pro digitální identitu (Úř. věst. L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Prováděcí nařízení Komise (EU) 2024/2979 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o integritu a základní funkce evropských peněženek digitální identity (Úř. věst. L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Prováděcí nařízení Komise (EU) 2024/2977 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o osobní identifikační údaje a elektronická potvrzení atributů vydávané k evropským peněženkám digitální identity (Úř. věst. L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Prováděcí nařízení Komise (EU) 2024/2980 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o oznámení Komisi týkající se ekosystému evropských peněženek digitální identity (Úř. věst. L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) Komise pravidelně posuzuje nové technologie, postupy, normy nebo technické specifikace. V zájmu zajištění co nejvyšší úrovně harmonizace mezi členskými státy při vývoji a certifikaci peněženek se technické specifikace stanovené v tomto nařízení opírají o práci provedenou na základě doporučení Komise (EU) 2021/946 ze dne 3. června 2021 o společném souboru nástrojů Unie pro koordinovaný přístup k evropskému digitálnímu rámci ([8]), a zejména o architekturu a referenční rámec. V souladu se 75. bodem odůvodnění nařízení Evropského parlamentu a Rady (EU) 2024/1183 ([9]) by Komise měla toto prováděcí nařízení přezkoumat a v případě potřeby ho aktualizovat, aby bylo v souladu s globálním vývojem, architekturou a referenčním rámcem a aby byly dodržovány osvědčené postupy na vnitřním trhu.

(5) Aby byla zajištěna přesná komunikace, technická diferenciace a jasné rozdělení odpovědnosti, je nezbytné rozlišovat mezi různými komponenty a konfiguracemi peněženek. Řešení peněženky by mělo být chápáno jako úplný systém poskytnutý poskytovatelem peněženky, který je nezbytný pro její provoz. Mělo by zahrnovat softwarové a hardwarové komponenty, jakož i služby, nastavení a konfigurace potřebné k zajištění řádného fungování peněženky. Řešení peněženky se může nacházet v zařízeních a prostředích uživatelů a v backendové struktuře poskytovatele. Jednotka peněženky by měla být chápána jako specifické uspořádání řešení peněženky pro jednotlivého uživatele. Její součástí by měla být aplikace instalovaná v zařízení nebo prostředí uživatele peněženky, kterou uživatel peněženky používá k přímé interakci (dále jen „instance peněženky“), a nezbytné bezpečnostní prvky k ochraně údajů a transakcí uživatelů. Tyto bezpečnostní prvky by měly zahrnovat zvláštní software nebo hardware pro šifrování a zabezpečení citlivých informací. Instance peněženky by měla být součástí jednotky peněženky a měla by uživateli peněženky umožňovat přístup k funkcím jeho peněženky.

(6) Bezpečné kryptografické aplikace peněženky jako samostatné specializované komponenty v rámci jednotky peněženky jsou nezbytné nejen pro ochranu kritických aktiv, jako jsou kryptografické soukromé klíče, ale také pro poskytování klíčových funkcí, jako je například předkládání elektronických potvrzení atributů. Používání obecných technických specifikací může poskytovatelům peněženek usnadnit přístup k vestavěným zabezpečeným prvkům. Bezpečné kryptografické aplikace peněženky mohou být poskytovány různými způsoby a pro různé druhy bezpečných kryptografických prostředků peněženky. Pokud poskytovatelé peněženek poskytují zakázkové bezpečné kryptografické aplikace jako aplet Java Card pro vestavěné zabezpečené prvky, měli by se poskytovatelé peněženek řídit normami uvedenými v příloze I nebo rovnocennými technickými specifikacemi.

(7) Jednotky peněženky mají poskytovatelům osobních identifikačních údajů nebo elektronických potvrzení atributů umožnit ověřit, že tyto údaje nebo potvrzení vydávají ke skutečným jednotkám peněženky uživatele peněženky.

(8) Aby byla zajištěna záměrná a standardní ochrana údajů, měly by být peněženky vybaveny dostupnými nejmodernějšími metodami zvyšujícími ochranu soukromí. Tyto funkce by měly umožnit používání peněženek, aniž by bylo možné sledovat uživatele peněženky u různých stran spoléhajících se na peněženku, pokud je to v daném scénáři použití možné. Poskytovatelé peněženek by například měli zvážit nejmodernější opatření ke zmírnění dopadů na soukromí ve vztahu k potvrzením jednotek peněženky, jako je používání dočasných potvrzení jednotek peněženky nebo jejich hromadné vydávání. Kromě toho by vložené zásady zpřístupňování informací měly uživatele peněženky varovat před nevhodným nebo nezákonným zveřejněním atributů z elektronických potvrzení atributů.

(9) Potvrzení jednotky peněženky by měla stranám spoléhajícím se na peněženku, které požadují atributy z jednotek peněženky, umožnit ověřit stav platnosti jednotky peněženky, se kterou komunikují, protože potvrzení jednotek peněženky mají být zneplatněna, pokud již není jednotka peněženky považována za platnou. Informace o stavu platnosti jednotek peněženky by měly být k dispozici interoperabilním způsobem, aby bylo zajištěno, že je mohou používat všechny strany spoléhající se na peněženku. Navíc v případech, kdy uživatelé peněženky své jednotky peněženky ztratí nebo nad nimi již nemají kontrolu, by poskytovatelé peněženek měli uživatelům peněženek umožnit požádat o zneplatnění jednotky peněženky. Aby bylo zajištěno soukromí a nepropojitelnost, měly by členské státy používat techniky ochrany soukromí i pro potvrzení jednotky peněženky. Může jít například o použití více potvrzení jednotky peněženky pro různé účely, při němž dojde ke zpřístupnění pouze minimálně relevantních informací o peněžence nezbytných pro transakci, nebo o omezení životnosti potvrzení jednotky peněženky jako alternativy k používání identifikátorů v případě zneplatnění.

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

([9]) Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu (Úř. věst. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(10) Aby bylo zajištěno, že všechny peněženky budou technicky schopny přijímat a předkládat osobní identifikační údaje a elektronická potvrzení atributů v přeshraničních scénářích bez narušení interoperability, měly by peněženky podporovat předem stanovené typy datových formátů a výběrové zpřístupňování. Jak je stanoveno v nařízení (EU) č. 910/2014, koncept výběrového zpřístupňování opravňuje vlastníka údajů zpřístupnit pouze určité části většího souboru údajů, aby přijímající subjekt získal pouze ty informace, které jsou nezbytné pro poskytnutí služby požadované uživatelem. Vzhledem k tomu, že peněženky mají uživateli umožnit výběrové zpřístupňování atributů, měly by být normy uvedené v příloze II prováděny tak, aby umožňovaly tento prvek peněženek. Kromě toho mohou peněženky podporovat další formáty a funkce k usnadnění konkrétních případů použití.

(11) Zaznamenávání transakcí je důležitým nástrojem pro zajištění transparentnosti v podobě přehledu transakcí pro uživatele peněženky. Kromě toho by měly být protokoly využívány tak, aby v případě podezřelého chování stran spoléhajících se na peněženku umožňovaly na žádost uživatele peněženky rychlé a snadné sdílení určitých informací s příslušnými dozorovými úřady zřízenými podle článku 51 nařízení (EU) 2016/679.

(12) Aby uživatel peněženky mohl elektronicky podepisovat, měl by mu být vydán kvalifikovaný certifikát, který je vázán na kvalifikovaný prostředek pro vytváření elektronických podpisů. Uživatel peněženky by měl mít přístup k aplikaci pro vytváření podpisů. Zatímco vydávání kvalifikovaných certifikátů je službou kvalifikovaných poskytovatelů služeb vytvářejících důvěru, poskytovatelé peněženek nebo jiné subjekty by měli být schopni poskytovat ostatní komponenty. Prostředky pro vytváření kvalifikovaných elektronických podpisů mohou být například spravovány kvalifikovanými poskytovateli služeb vytvářejících důvěru jako služba nebo mohou být umístěny v zařízení uživatele peněženky, například jako čipová karta. Podobně mohou být aplikace pro vytváření podpisů integrovány do instance peněženky, mohou být samostatnou aplikací v zařízení uživatele peněženky nebo mohou být poskytovány na dálku.

(13) Osobní identifikační údaje a elektronická potvrzení atributů, které byly vydány ke konkrétní jednotce peněženky, mohou zaznamenávat objekty exportu a přenositelnosti údajů. Tyto objekty umožňují uživatelům peněženky získat příslušné údaje z jejich jednotky peněženky, čímž posilují jejich právo na přenositelnost údajů. Poskytovatelům peněženek se doporučuje, aby stejná technická řešení použili také při zavádění procesů zálohování a obnovy jednotek peněženky, což umožní obnovu ztracených jednotek peněženky nebo přenos informací od jednoho poskytovatele peněženek k jinému, pokud je to vhodné a pokud to lze provést bez narušení práva na ochranu údajů a bezpečnosti ekosystému digitální identity.

(14) Generování pseudonymů specifických pro stranu spoléhající se na peněženku by mělo uživatelům peněženky umožnit samostatnou autentizaci, aniž by stranám spoléhajícím se na peněženku poskytovali zbytečné informace. Jak je stanoveno v nařízení (EU) č. 910/2014, uživatelům peněženek nesmí být bráněno v přístupu ke službám prostřednictvím pseudonymů, pokud nebyl pro účely autentizace stanoven právní požadavek uvádět právní identitu. Proto mají peněženky obsahovat funkci pro generování pseudonymů, které si uživatel zvolí a spravuje a které slouží k autentizaci při přístupu k on-line službám. Tato funkce by se měla odpovídajícím způsobem umožnit prováděním specifikací uvedených v příloze V. Kromě toho nesmějí strany spoléhající se na peněženku od uživatelů požadovat žádné jiné údaje než ty, které jsou uvedeny pro zamýšlené použití peněženek v registru spoléhajících se stran. Uživatelé peněženky by měli mít možnost kdykoli ověřit registrační údaje spoléhajících se stran.

(15) Jak je stanoveno v nařízení (EU) 2024/1183, členské státy nesmí přímo ani nepřímo omezovat přístup k veřejným nebo soukromým službám fyzickým či právnickým osobám, které se rozhodly evropskou peněženku digitální identity nepoužívat, a musí zpřístupnit vhodná alternativní řešení.

(16) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([10]) byl konzultován evropský inspektor ochrany údajů, který vydal své stanovisko dne 30. září 2024.

([10]) Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(17) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru uvedeného v článku 48 nařízení (EU) č. 910/2014,

PŘIJALA TOTO NAŘÍZENÍ:

KAPITOLA I

**OBECNÁ USTANOVENÍ**

*Článek 1*

**Předmět a oblast působnosti**

Toto nařízení stanoví pravidla pro integritu a základní funkce peněženek, která je třeba pravidelně aktualizovat, aby byla v souladu s vývojem technologií a norem a s prací prováděnou na základě doporučení (EU) 2021/946, a zejména s architekturou a referenčním rámcem.

*Článek 2*

**Definice**

Pro účely tohoto nařízení se rozumí:

1) „bezpečnou kryptografickou aplikací peněženky“ aplikace, která spravuje kritická aktiva prostřednictvím propojení s kryptografickými a nekryptografickými funkcemi poskytovanými bezpečným kryptografickým prostředkem peněženky a jejich využívání;

2) „jednotkou peněženky“ jedinečná konfigurace řešení peněženky, která zahrnuje instance peněženky, bezpečné kryptografické aplikace peněženky a bezpečné kryptografické prostředky peněženky, které poskytovatel peněženky poskytuje jednotlivému uživateli peněženky;

3) „kritickými aktivy“ aktiva v rámci jednotky peněženky nebo ve vztahu k ní, která jsou tak mimořádně důležitá, že ohrožení jejich dostupnosti, důvěrnosti nebo integrity by mělo velmi vážný a oslabující účinek na schopnost spoléhat se na jednotku peněženky;

4) „poskytovatelem osobních identifikačních údajů“ fyzická nebo právnická osoba odpovědná za vydávání a zneplatnění osobních identifikačních údajů a za zajištění kryptografického provázání osobních identifikačních údajů uživatele s jednotkou peněženky;

5) „uživatelem peněženky“ uživatel, který má jednotku peněženky pod kontrolou;

6) „stranou spoléhající se na peněženku“ spoléhající se strana, která má v úmyslu spoléhat se na jednotky peněženky při poskytování veřejných nebo soukromých služeb prostřednictvím digitální interakce;

7) „poskytovatelem peněženky“ fyzická nebo právnická osoba, která poskytuje řešení peněženky;

8) „potvrzením jednotky peněženky“ datový objekt, který popisuje komponenty jednotky peněženky nebo umožňuje autentizaci a ověření platnosti těchto komponentů;

9) „vloženými zásadami zpřístupňování informací“ soubor pravidel, který je součástí elektronického potvrzení atributů jeho poskytovatelem a ve kterém jsou uvedeny podmínky, jež musí strana spoléhající se na peněženku splnit, aby získala přístup k elektronickému potvrzení atributů;

10) „instancí peněženky“ aplikace nainstalovaná a nakonfigurovaná v zařízení nebo prostředí uživatele peněženky, která je součástí jednotky peněženky a kterou uživatel peněženky používá k interakci s jednotkou peněženky;

11) „řešením peněženky“ kombinace softwaru, hardwaru, služeb, nastavení a konfigurací, včetně instancí peněženky, jedné nebo více bezpečných kryptografických aplikací peněženky a jednoho nebo více bezpečných kryptografických prostředků peněženky;

12) „bezpečným kryptografickým prostředkem peněženky“ prostředek odolný proti neoprávněné manipulaci, který poskytuje prostředí propojené s bezpečnou kryptografickou aplikací peněženky a používaný touto aplikací k ochraně kritických aktiv a poskytování kryptografických funkcí pro bezpečné provádění kritických operací;

13) „kryptografickou operací peněženky“ kryptografický mechanismus nezbytný v souvislosti s autentizací uživatele peněženky a vydáváním nebo předkládáním osobních identifikačních údajů nebo elektronických potvrzení atributů;

14) „přístupovým certifikátem strany spoléhající se na peněženku“ certifikát pro elektronické pečetě nebo podpisy ověřující pravost a platnost strany spoléhající se na peněženku vydaný poskytovatelem přístupových certifikátů strany spoléhající se na peněženku;

15) „poskytovatelem přístupových certifikátů strany spoléhající se na peněženku“ fyzická nebo právnická osoba pověřená členským státem vydáváním přístupových certifikátů strany spoléhající se na peněženku stranám spoléhajícím se na peněženku registrovaným v tomto členském státě.

KAPITOLA II

## INTEGRITA EVROPSKÝCH PENĚŽENEK DIGITÁLNÍ IDENTITY

*Článek 3*

### Integrita jednotky peněženky

1. Jednotky peněženky nesmí provést žádnou funkci uvedenou v čl. 5a odst. 4 nařízení (EU) č. 910/2014, kromě autentizace uživatele peněženky za účelem získání přístupu k jednotce peněženky, dokud jednotka peněženky úspěšně neautentizuje uživatele peněženky.

2. Poskytovatelé peněženek pro každou jednotku peněženky podepíší nebo opatří pečetí alespoň jedno potvrzení jednotky peněženky splňující požadavky stanovené v článku 6. Certifikát používaný k podpisu potvrzení jednotky peněženky nebo k jeho opatření pečetí se vydává na základě certifikátu uvedeného na důvěryhodném seznamu podle prováděcího nařízení (EU) 2024/2980.

*Článek 4*

### Instance peněženky

1. Instance peněženky používají ke správě kritických aktiv alespoň jeden bezpečný kryptografický prostředek peněženky.

2. Poskytovatelé peněženek zajistí integritu, pravost a důvěrnost komunikace mezi instancemi peněženky a bezpečnými kryptografickými aplikacemi peněženky.

3. Pokud se kritická aktiva týkají provádění elektronické identifikace na vysoké úrovni záruky, musí být kryptografické operace peněženky nebo jiné operace zpracovávající kritická aktiva prováděny v souladu s požadavky na vlastnosti a formu prostředků pro elektronickou identifikaci na vysoké úrovni záruky, jak je stanoveno v prováděcím nařízení Komise (EU) 2015/1502 ([11]).

*Článek 5*

### Bezpečné kryptografické aplikace peněženky

1. Poskytovatelé peněženek zajistí, že bezpečné kryptografické aplikace peněženky:

a) provedou kryptografické operace peněženky s jinými kritickými aktivy než těmi, které jednotka peněženky potřebuje k autentizaci uživatele peněženky, pouze v případech, kdy tyto aplikace úspěšně autentizovaly uživatele peněženky;

([11]) Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (Úř. věst. L 235, 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

b) autentizují uživatele peněženky v rámci provádění elektronické identifikace na vysoké úrovni záruky; provedou autentizaci uživatelů peněženky v souladu s požadavky na vlastnosti a formu prostředků pro elektronickou identifikaci na vysoké úrovni záruky, jak je stanoveno v prováděcím nařízení (EU) 2015/1502;

c) jsou schopny bezpečně generovat nové kryptografické klíče;

d) jsou schopny bezpečně vymazat kritická aktiva;

e) jsou schopny vygenerovat důkaz o vlastnictví soukromých klíčů;

f) chrání soukromé klíče generované těmito bezpečnými kryptografickými aplikacemi peněženky po dobu existence těchto klíčů;

g) splňují požadavky na vlastnosti a formu prostředků pro elektronickou identifikaci na vysoké úrovni záruky, jak je stanoveno v prováděcím nařízení (EU) 2015/1502;

h) jsou jedinými komponenty schopnými provádět kryptografické operace peněženky a jakékoli jiné operace s kritickými aktivy v rámci provádění elektronické identifikace na vysoké úrovni záruky.

2. Pokud se poskytovatelé peněženek rozhodnou poskytnout bezpečnou kryptografickou aplikaci pro vestavěný zabezpečený prvek, založí své technické řešení na technických specifikacích uvedených v příloze I nebo na jiných rovnocenných technických specifikacích.

*Článek 6*

**Pravost a platnost jednotky peněženky**

1. Poskytovatelé peněženek zajistí, aby každá jednotka peněženky obsahovala potvrzení jednotky peněženky.

2. Poskytovatelé peněženek zajistí, aby potvrzení jednotky peněženky uvedená v odstavci 1 obsahovala veřejné klíče a aby příslušné soukromé klíče byly chráněny bezpečným kryptografickým prostředkem peněženky.

3. Poskytovatelé peněženek:

a) informují uživatele peněženky o jejich právech a povinnostech v souvislosti s jejich jednotkou peněženky;

b) poskytují mechanismy pro bezpečnou identifikaci a autentizaci uživatelů peněženek, které jsou nezávislé na jednotkách peněženky;

c) zajistí, aby uživatelé peněženky měli právo požádat o zneplatnění potvrzení jejich jednotky peněženky pomocí mechanismů autentizace uvedených v písmenu (b).

*Článek 7*

**Zneplatnění potvrzení jednotky peněženky**

1. Poskytovatelé peněženek jsou jedinými subjekty, které mohou zneplatnit potvrzení jednotky peněženky, která poskytli.

2. Poskytovatelé peněženek stanoví veřejně dostupné zásady, v nichž uvedou podmínky a časový rámec pro zneplatnění potvrzení jednotky peněženky.

3. Pokud poskytovatelé peněženek zneplatní potvrzení jednotky peněženky, informují o zneplatnění jednotek peněženky dotčené uživatele peněženky do 24 hodin, včetně uvedení důvodu zneplatnění a důsledků pro uživatele peněženky. Tyto informace se poskytují stručným a snadno přístupným způsobem a s využitím jasného a srozumitelného jazyka.

4. Pokud poskytovatelé peněženek zneplatní potvrzení jednotky peněženky, zveřejní stav platnosti potvrzení jednotky peněženky způsobem zachovávajícím soukromí a popíší umístění těchto informací v potvrzení jednotky peněženky.

KAPITOLA III

## ZÁKLADNÍ FUNKCE A VLASTNOSTI EVROPSKÝCH PENĚŽENEK DIGITÁLNÍ IDENTITY

*Článek 8*

### Formáty pro osobní identifikační údaje a elektronická potvrzení atributů

Poskytovatelé peněženek zajistí, aby řešení peněženky podporovala používání osobních identifikačních údajů a elektronických potvrzení atributů vydaných v souladu se seznamem norem uvedených v příloze II.

*Článek 9*

### Protokoly transakcí

1. Bez ohledu na to, zda je transakce úspěšně dokončena, instance peněženky zaznamenávají všechny transakce se stranami spoléhajícími se na peněženku a s ostatními jednotkami peněženky, včetně elektronického podepisování a opatřování elektronickou pečetí.

2. Zaznamenané informace musí obsahovat alespoň:

a) čas a datum transakce;

b) jméno, kontaktní údaje a jedinečný identifikátor příslušné strany spoléhající se na peněženku a členský stát, v němž je tato strana spoléhající se na peněženku usazena, nebo v případě jiných jednotek peněženky příslušné informace z potvrzení jednotky peněženky;

c) typ nebo typy údajů požadovaných a předkládaných v transakci;

d) v případě nedokončených transakcí důvod jejich nedokončení.

3. Poskytovatelé peněženek zajistí integritu, pravost a důvěrnost zaznamenaných informací.

4. Instance peněženky zaznamenávají zprávy zaslané uživatelem peněženky úřadům pro ochranu osobních údajů prostřednictvím jeho jednotky peněženky.

5. Protokoly uvedené v odstavcích 1 a 2 jsou přístupné poskytovateli peněženky, pokud je to nezbytné pro poskytování služeb peněženky, na základě výslovného předchozího souhlasu uživatele peněženky.

6. Protokoly uvedené v odstavcích 1 a 2 zůstávají přístupné po dobu, po kterou to vyžaduje právo Unie nebo členských států.

7. Poskytovatelé peněženek umožňují uživatelům peněženek export zaznamenaných informací uvedených v odstavci 2.

*Článek 10*

### Vložené zpřístupňování informací

1. Poskytovatelé peněženek zajistí, aby elektronická potvrzení atributů, jejichž součástí jsou obecné vložené zásady zpřístupňování informací uvedené v příloze III, mohla být zpracovávána jimi poskytovanými jednotkami peněženky.

2. Instance peněženky jsou schopny zpracovávat a předkládat tyto vložené zásady zpřístupňování informací uvedené v odstavci 1 ve spojení s údaji obdrženými od žádající strany spoléhající se na peněženku.

3. Instance peněženky ověří, zda strana spoléhající se na peněženku splňuje požadavky vložených zásad zpřístupňování informací, a o výsledku informuje uživatele peněženky.

*Článek 11*

**Kvalifikované elektronické podpisy a pečetě**

1. Poskytovatelé peněženek zajistí, aby uživatelé peněženek mohli získat kvalifikované certifikáty pro kvalifikované elektronické podpisy nebo pečetě, které jsou spojeny s kvalifikovanými prostředky pro vytváření podpisů nebo pečetí, jež jsou ve vztahu k instancím peněženky místní, externí nebo dálkové.

2. Poskytovatelé peněženek zajistí, aby řešení peněženky podporovala bezpečné rozhraní k jednomu z následujících typů kvalifikovaných prostředků pro vytváření podpisů nebo pečetí: místní, externí nebo na dálku spravované kvalifikované prostředky pro vytváření podpisů nebo pečetí pro účely používání kvalifikovaných certifikátů uvedených v odstavci 1.

3. Poskytovatelé peněženek zajistí, aby uživatelé peněženek, kteří jsou fyzickými osobami, měli alespoň pro neprofesní účely bezplatný přístup k aplikacím pro vytváření podpisů, které umožňují vytváření bezplatných kvalifikovaných elektronických podpisů pomocí certifikátů uvedených v odstavci 1.

*Článek 12*

**Aplikace pro vytváření podpisů**

1. Aplikace pro vytváření podpisů používané jednotkami peněženky mohou být poskytovány poskytovateli peněženek, poskytovateli služeb vytvářejících důvěru, nebo stranami spoléhajícími se na peněženku.

2. Aplikace pro vytváření podpisů mají tyto funkce:

a) podepisování údajů poskytnutých uživatelem peněženky nebo jejich opatřování pečetí;

b) podepisování údajů poskytnutých spoléhající se stranou nebo jejich opatřování pečetí;

c) vytváření podpisů nebo pečetí v souladu alespoň s povinným formátem uvedeným v příloze IV;

d) informování uživatelů peněženky o výsledku procesu vytváření podpisu nebo pečeti.

3. Aplikace pro vytváření podpisů mohou být buď integrovány do instancí peněženky, nebo mohou být externí. Pokud se aplikace pro vytváření podpisů spoléhají na kvalifikované prostředky pro vytváření podpisů na dálku a pokud jsou integrovány do instancí peněženky, musí podporovat aplikační programovací rozhraní uvedené v příloze IV.

*Článek 13*

**Export a přenositelnost údajů**

Jednotky peněženky musí, pokud je to technicky proveditelné a s výjimkou případů kritických aktiv, podporovat bezpečný export a přenositelnost osobních údajů uživatele peněženky, aby uživatel peněženky mohl přejít na jiné řešení peněženky způsobem, který zajišťuje vysokou úroveň záruky, jak je stanoveno v prováděcím nařízení (EU) 2015/1502.

*Článek 14*

**Pseudonymy**

1. Jednotky peněženky musí podporovat generování pseudonymů pro uživatele peněženky v souladu s technickými specifikacemi uvedenými v příloze V.

2. Jednotky peněženky podporují na žádost strany spoléhající se na peněženku generování pseudonymu, který je specifický a jedinečný pro danou stranu spoléhající se na peněženku, a poskytnou tento pseudonym straně spoléhající se na peněženku buď samostatně, nebo v kombinaci s jakýmikoliv osobními identifikačními údaji nebo elektronickým potvrzením atributů, o nějž si tato strana spoléhající se na peněženku požádá.

KAPITOLA IV

**ZÁVĚREČNÁ USTANOVENÍ**

*Článek 15*

**Vstup v platnost**

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 28. listopadu 2024.

*Za Komisi*
*předsedkyně*
Ursula VON DER LEYEN

*PŘÍLOHA I*

**SEZNAM NOREM 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.

*PŘÍLOHA II*

**SEZNAM NOREM UVEDENÝCH V ČLÁNKU 8**

— ISO/IEC.18013-5:2021,

— „Verifiable Credentials Data Model 1.1.“, doporučení W3C ze dne 3. března 2022.

*PŘÍLOHA III*

**SEZNAM OBECNÝCH VLOŽENÝCH ZÁSAD ZVEŘEJŇOVÁNÍ INFORMACÍ UVEDENÝCH V ČLÁNKU 10**

1. „Žádné zásady“, což znamená, že se na elektronická potvrzení atributů nevztahují žádné zásady.
2. „Zásady týkající se pouze oprávněných spoléhajících se stran“, což znamená, že uživatelé peněženky mohou zpřístupnit elektronická potvrzení atributů pouze autentizovaným spoléhajícím se stranám, které jsou výslovně uvedeny v zásadách zveřejňování.
3. „Specifický kořen důvěry“ (specific root of trust), což znamená že uživatelé peněženky by měli specifická elektronická potvrzení atributů sdílet pouze s autentizovanými stranami spoléhajícími se na peněženku, jež mají přístupové certifikáty strany spoléhající se na peněženku odvozené od specifického kořenového certifikátu (nebo seznamu specifických kořenů) nebo zprostředkujícího certifikátu (zprostředkujících certifikátů).

*PŘÍLOHA IV*

**SEZNAM FORMÁTŮ PODPISU A PEČETI UVEDENÝCH V ČLÁNKU 12**

1. Povinný formát podpisu nebo pečeti:

   a) PAdES (zaručený elektronický podpis PDF), jak je specifikováno v normě ETSI EN 319 142-1 V1.1.1 (2016-04); Elektronické podpisy a infrastruktury (ESI); Digitální podpisy PAdES; Část 1: Stavební bloky a základní podpisy PAdES.

2. Seznam volitelných formátů podpisu nebo pečeti:

   a) XAdES, jak je specifikováno v normě „ETSI EN 319 132-1 V1.2.1 (2022-02) Elektronické podpisy a infrastruktury (ESI); Digitální podpisy XAdES; Část 1: Stavební bloky a základní podpisy XAdES (XAdES)“ pro podepisování formátu XML;

   b) JAdES, jak je specifikováno v normě „ETSI TS 119 182-1 V1.2.1 (2024-07) Elektronické podpisy a infrastruktury (ESI); Digitální podpisy JAdES; Část 1: Stavební bloky a základní podpisy JAdES“ pro podepisování formátu JSON;

   c) CAdES (zaručený elektronický podpis CMS), jak je specifikováno v normě „ETSI EN 319 122-1 V1.3.1 (2023-06) Elektronické podpisy a infrastruktury (ESI); Digitální podpisy CAdES; Část 1: Stavební bloky a základní podpisy CAdES“ pro podepisování formátu CMS;

   d) ASiC (přidružený zásobník podpisu), jak je specifikováno v normě „ETSI EN 319 162-1 V1.1.1 (2016-04) Elektronické podpisy a infrastruktury (ESI); Přidružené zásobníky podpisu (ASiC); Část 1: Stavební bloky a základní zásobníky ASiC a norma ETSI EN 319 162-2 V1.1.1 (2016-04) Elektronické podpisy a infrastruktury (ESI); Přidružené zásobníky podpisu (ASiC); Část 2: Dodatečné zásobníky ASiC pro podepisování zásobníků.

3. Aplikační programovací rozhraní:

   — specifikace konsorcia Cloud Signature Consortium (CSC) v2.0 (20. dubna 2023).

*PŘÍLOHA V*

**TECHNICKÉ SPECIFIKACE PRO GENEROVÁNÍ PSEUDONYMŮ PODLE ČLÁNKU 14**

Technické požadavky:

— WebAuthn – doporučení W3C ze dne 8. dubna 2021, úroveň 2, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.