PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2025/848

ze dne 6. května 2025,

kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o registraci stran spoléhajících se na peněženku

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. 5b odst. 11 uvedeného nařízení,

vzhledem k těmto důvodům:

1) Pro účely registrace spoléhajících se stran, které mají v úmyslu spoléhat se na evropské peněženky digitální identity („peněženky“) při poskytování digitálních veřejných nebo soukromých služeb, jak to vyžaduje nařízení (EU) č. 910/2014, by členské státy měly zřídit a vést vnitrostátní registry stran spoléhajících se na peněženku usazených na jejich území.

2) Komise pravidelně posuzuje nové technologie, postupy, normy a 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 podle doporučení Komise (EU) 2021/946 ([2]), a zejména o architekturu a referenční rámec, které jsou jeho součástí. V souladu se 75. bodem odůvodnění nařízení Evropského parlamentu a Rady (EU) 2024/1183 ([3]) by Komise měla toto nařízení přezkoumat a v případě potřeby aktualizovat, aby bylo v souladu s globálním vývojem, architekturou a referenčním rámcem a aby byly dodržovány osvědčené postupy na vnitřním trhu.

3) Pro zajištění širokého přístupu k registrům a dosažení interoperability by členské státy měly vytvořit rozhraní jak pro člověka, tak strojově čitelná, která splňují technické specifikace stanovené v tomto nařízení. Poskytovatelé přístupových certifikátů strany spoléhající se na peněženku a registračních certifikátů strany spoléhající se na peněženku, pokud jsou k dispozici, by měli mít možnost se pro účely vydávání těchto certifikátů rovněž spoléhat na tato rozhraní.

4) Vzhledem k tomu, že zásady registrace poskytují jasné pokyny stranám spoléhajícím se na peněženku ohledně procesu registrace, měly by členské státy stanovit a zveřejnit zásady registrace platné pro vnitrostátní registry usazené na jejich území.

5) Účelem registrace stran spoléhajících se na peněženku je vybudovat důvěru v používání peněženek prostřednictvím větší transparentnosti. Členské státy by proto měly příslušné informace zpřístupnit veřejnosti způsobem, který je čitelný jak pro člověka, tak strojově. Za tímto účelem by měly strany spoléhající se na peněženku poskytnout do vnitrostátních registrů nezbytné informace, včetně svého oprávnění nebo svých oprávnění.

6) Dále by měly strany spoléhající se na peněženku v zájmu transparentnosti prohlásit, zda se hodlají spoléhat na elektronickou identifikaci fyzických osob.

7) Aby se zajistilo, že proces registrace bude nákladově efektivní a úměrný riziku, měli by registrátoři pro strany spoléhající se na peněženku zavést procesy registrace, které budou snadno použitelné, on-line a v příslušných případech automatizované. Registrátoři by měli ověřovat žádosti o registraci bez zbytečného odkladu.

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

([2]) Doporučení Komise (EU) 2021/946 ze dne 3. června 2021 o společném souboru nástrojů Unie pro koordinovaný přístup k rámci pro evropskou digitální identitu (Úř. věst. L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) 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).

8) Členské státy zajistí, aby peněženky byly schopny autentizovat strany spoléhající se na peněženku bez ohledu na to, kde jsou v Unii usazeny. Za tímto účelem by strany spoléhající se na peněženku měly při své identifikaci vůči jednotkám peněženky používat přístupové certifikáty strany spoléhající se na peněženku. Aby byla zaručena interoperabilita těchto certifikátů se všemi peněženkami poskytovanými v Unii, měly by přístupové certifikáty strany spoléhající se na peněženku splňovat společné požadavky stanovené v příloze. Komise by měla vypracovat harmonizované certifikační politiky a prohlášení o certifikačních postupech, které by členské státy měly implementovat. Komise by měla ve spolupráci s členskými státy pečlivě sledovat vývoj nových nebo alternativních norem, na jejichž základě by mohly být přístupové certifikáty strany spoléhající se na peněženku implementovány. Posuzovat by se měly zejména modely důvěry, které v členských státech prokázaly svou účinnost a bezpečnost.

9) Jak je stanoveno v nařízení (EU) č. 910/2014, strany spoléhající se na peněženku nesmějí od uživatelů požadovat poskytnutí žádných jiných údajů než těch, které byly uvedeny pro zamýšlené použití peněženek během procesu registrace. Uživatelé peněženky by měli mít možnost ověřit registrační údaje stran spoléhajících se na peněženku. Aby si uživatelé peněženky mohli ověřit, že atributy, o které žádá strana spoléhající se na peněženku, spadají do rozsahu registrovaných atributů, mohou členské státy vyžadovat vydávání registračních certifikátů strany spoléhající se na peněženku registrovaným stranám spoléhajícím se na peněženku. Aby byla zajištěna interoperabilita registračních certifikátů strany spoléhající se na peněženku, měly by členské státy zajistit, aby tyto certifikáty splňovaly požadavky a normy stanovené v příloze. Pro účely transparentnosti by zejména strany spoléhající se na peněženku měly prohlásit, zda mají v úmyslu spoléhat se na elektronickou identifikaci fyzických osob, aby splnily jeden z požadavků stanovených v čl. 6 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2016/679 ([4]). Dále spoléhající se strany neodmítnou používání pseudonymů, pokud identifikace uživatele není vyžadována právem Unie nebo vnitrostátním právem.

10) Aby byli uživatelé chráněni před nadměrným sdílením informací se stranami spoléhajícími se na peněženku a aby byli v takových případech varováni, měly by členské státy do svých certifikačních politik zahrnout společné zásady přístupu, které by umožnily, aby řešení peněženky informovalo uživatele peněženky, kdykoli strana spoléhající se na peněženku požaduje více informací, než které zaregistrovala nebo k nimž je oprávněna přistupovat.

11) Aby byli uživatelé peněženky chráněni, měli by mít registrátoři možnost pozastavit nebo zrušit registraci jakékoli strany spoléhající se na peněženku bez předchozího upozornění, pokud mají důvod se domnívat, že registrace obsahuje nepřesné, neaktuální nebo zavádějící informace, že strana spoléhající se na peněženku nedodržuje zásady registrace nebo že strana spoléhající se na peněženku jinak porušuje právo Unie nebo vnitrostátní právo nebo evropské prohlášení o digitálních právech a zásadách pro digitální dekádu ([5]) způsobem, který souvisí s její rolí strany spoléhající se na peněženku, například pokud strana spoléhající se na peněženku řádně neminimalizovala soubor atributů, ke kterým požaduje přístup. V zájmu zachování stability ekosystému evropské peněženky digitální identity („ekosystém peněženky“) by rozhodnutí o pozastavení nebo zrušení registrace mělo být přiměřené narušení služby způsobenému pozastavením nebo zrušením a souvisejícím nákladům a nepříjemnostem pro poskytovatele služby a uživatele. Podle čl. 46a odst. 4 písm. f) nařízení (EU) č. 910/2014 jsou orgány dohledu rovněž oprávněny v případě potřeby pozastavit a zrušit registraci.

12) Pro účely následného sledování, vyšetřování ze strany donucovacích orgánů a řešení sporů by měli registrátoři po dobu 10 let uchovávat záznamy o všech informacích poskytnutých stranami spoléhajícími se na peněženku, které jsou zapsány v jejich vnitrostátním registru.

13) Na činnosti zpracování osobních údajů podle tohoto nařízení se vztahuje nařízení (EU) 2016/679 a v příslušných případech směrnice Evropského parlamentu a Rady 2002/58/ES ([6]).

([4]) 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).

([5]) Úř. věst. C 23, 23.1.2023, s. 1.

([6]) 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).

14) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([7]) byl konzultován evropský inspektor ochrany údajů, který vydal své stanovisko dne 31. ledna 2025.

15) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru zřízeného článkem 48 nařízení (EU) č. 910/2014,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Předmět a oblast působnosti

Toto nařízení stanoví pravidla pro registraci stran spoléhajících se na peněženku.

Článek 2

Definice

Pro účely tohoto nařízení se rozumí:

1) „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;

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) „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;

4) „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;

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

6) „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;

7) „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;

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

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

10) „vnitrostátním registrem stran spoléhajících se na peněženku“ vnitrostátní elektronický registr používaný členským státem ke zveřejňování informací o stranách spoléhajících se na peněženku registrovaných v tomto členském státě, jak je stanoveno v čl. 5b odst. 5 nařízení (EU) č. 910/2014;

11) „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;

([7]) 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).

12) „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;

13) „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;

14) „registrátorem stran spoléhajících se na peněženku“ subjekt odpovědný za sestavení a vedení seznamu registrovaných stran spoléhajících se na peněženku usazených na jeho území, který byl určen členským státem;

15) „registračním certifikátem strany spoléhající se na peněženku“ datový objekt, který popisuje zamýšlené použití spoléhající se strany a uvádí atributy, které spoléhající se strana zaregistrovala a které hodlá požadovat od uživatelů;

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

Článek 3

Vnitrostátní registry

1. Členské státy zřídí a vedou alespoň jeden vnitrostátní registr stran spoléhajících se na peněženku s informacemi o registrovaných stranách spoléhajících se na peněženku usazených v daném členském státě.

2. Registr musí obsahovat alespoň informace uvedené v příloze I.

3. Členské státy určí alespoň jednoho registrátora, který bude spravovat a provozovat alespoň jeden vnitrostátní registr stran spoléhajících se na peněženku.

4. Členské státy zveřejní informace uvedené v příloze I o registrovaných stranách spoléhajících se na peněženku on-line, a to jak v podobě čitelné pro člověka, tak v podobě vhodné pro automatizované zpracování.

5. Informace uvedené v odstavci 2 jsou k dispozici prostřednictvím jednotného společného rozhraní pro programování aplikací („rozhraní API“) a na vnitrostátní internetové stránce. Musí být registrátorem nebo jeho jménem opatřeny elektronickým podpisem nebo pečetí v souladu se společnými požadavky na jednotné rozhraní API stanovenými v oddíle 1 přílohy II.

6. Členské státy zajistí, aby rozhraní API uvedené v odstavci 5 splňovalo společné požadavky stanovené v oddíle 2 přílohy II.

7. Členské státy zajistí, aby registry byly v souladu s příslušnými společnými zásadami registrace stanovenými v článku 4.

Článek 4

Zásady registrace

1. Členské státy stanoví a zveřejní jednu nebo více vnitrostátních zásad registrace, které se vztahují na vnitrostátní registry usazené na jejich území.

2. Členské státy mohou zahrnout nebo znovu použít stávající odvětvové nebo vnitrostátní zásady registrace.

3. Vnitrostátní zásady registrace obsahují alespoň informace o:

a) postupech identifikace a autentizace, které se vztahují na strany spoléhající se na peněženku během procesu registrace;

b) požadovaných podpůrných dokladech týkajících se totožnosti, registrace podniku, příslušného oprávnění nebo příslušných oprávnění a dalších relevantních informací o straně spoléhající se na peněženku;

c) autentických zdrojích nebo jiných úředních elektronických záznamech, a zda se lze na tyto zdroje nebo záznamy spolehnout, že poskytují přesné údaje;

d) veškerých dalších informacích nebo jiných důkazech požadovaných v rámci procesu registrace;

e) v příslušných případech automatizovaných prostředcích umožňujících stranám spoléhajícím se na peněženku zaregistrovat se nebo aktualizovat stávající registraci;

f) mechanismu nápravy, který mají strany spoléhající se na peněženku k dispozici podle právních předpisů a postupů členského státu, v němž je vnitrostátní registr usazen;

g) pravidlech a postupech pro ověřování totožnosti registrovaných stran spoléhajících se na peněženku a všech dalších relevantních informací, které tato strana poskytla.

4. Postupy a dokumentace uvedené v odst. 3 písm. (a) a (b) umožní stranám spoléhajícím se na peněženku uvést, na základě jakého konkrétního oprávnění nebo konkrétních oprávnění jednají, jak je uvedeno v příloze I.

5. Požadavky stanovené v zásadách registrace nebrání v příslušných případech automatizovanému procesu registrace.

Článek 5

Informace poskytované vnitrostátním registrům

1. Strany spoléhající se na peněženku poskytnou vnitrostátním registrům alespoň informace uvedené v příloze I.

2. Strany spoléhající se na peněženku zajistí, aby byly poskytnuté informace v době registrace přesné.

3. Strany spoléhající se na peněženku bez zbytečného odkladu aktualizují veškeré informace dříve zapsané ve vnitrostátním registru stran spoléhajících se na peněženku.

Článek 6

Proces registrace

1. Registrátoři zavedou snadno použitelné elektronické a pokud možno automatizované procesy registrace pro strany spoléhající se na peněženku.

2. Registrátoři zpracovávají žádosti o registraci bez zbytečného odkladu a odpoví žadateli na žádost o registraci ve lhůtě stanovené v příslušných zásadách registrace, a to vhodnými prostředky a v souladu s právními předpisy a postupy členského státu, v němž je vnitrostátní registr usazen.

3. Je-li to možné, registrátoři automatizovaně ověřují:

a) přesnost, platnost, pravost a integritu informací požadovaných podle článku 5;

b) v příslušných případech plné moci zástupců stran spoléhajících se na peněženku vyhotovené a předložené v souladu s právními předpisy a postupy členského státu, v němž je registr usazen;

c) druh oprávnění stran spoléhajících se na peněženku, jak stanoví příloha I;

d) neexistenci registrace v jiném vnitrostátním registru.

4. Registrátoři ověří informace uvedené v odstavci 3 na základě podpůrných dokladů poskytnutých stranami spoléhajícími se na peněženku nebo na základě příslušných autentických zdrojů nebo jiných úředních elektronických záznamů v členském státě, v němž je vnitrostátní registr usazen, k nimž mají registrátoři přístup v souladu s platnými vnitrostátními právními předpisy a postupy.

5. Ověřování oprávnění stran spoléhajících se na peněženku uvedené v odst. 3 písm. (c) se provádí v souladu s přílohou III.

6. Pokud registrátor nemůže informace ověřit v souladu s odstavci 3 až 5, registraci zamítne.

7. Pokud se strana spoléhající se na peněženku již nehodlá spoléhat na jednotky peněženky pro poskytování veřejných nebo soukromých služeb v rámci určité registrace, oznámí to bez zbytečného odkladu příslušnému registrátorovi a požádá o zrušení této registrace.

Článek 7

Přístupové certifikáty strany spoléhající se na peněženku

1. Členské státy pověří alespoň jeden certifikační orgán vydáváním přístupových certifikátů strany spoléhající se na peněženku.

2. Členské státy zajistí, aby poskytovatelé přístupových certifikátů strany spoléhající se na peněženku vydávali přístupové certifikáty strany spoléhající se na peněženku výhradně registrovaným stranám spoléhajícím se na peněženku.

3. Členské státy syntakticky a sémanticky harmonizovaným způsobem implementují certifikační politiky a prohlášení o certifikačních postupech pro přístupové certifikáty strany spoléhající se na peněženku v souladu s požadavky stanovenými v příloze IV.

Článek 8

Registrační certifikáty strany spoléhající se na peněženku

1. Členské státy mohou pověřit alespoň jeden certifikační orgán vydáváním registračních certifikátů strany spoléhající se na peněženku.

2. Pokud členský stát povolil vydání registračního certifikátu strany spoléhající se na peněženku, tento členský stát:

a) vyžaduje, aby poskytovatelé registračních certifikátů strany spoléhající se na peněženku vydávali registrační certifikáty strany spoléhající se na peněženku výhradně registrovaným stranám spoléhajícím se na peněženku;

b) zajistí, aby v registračních certifikátech strany spoléhající se na peněženku bylo uvedeno každé zamýšlené použití;

c) zajistí, aby registrační certifikáty strany spoléhající se na peněženku obsahovaly obecné zásady přístupu, které budou syntakticky a sémanticky harmonizované v celé Unii a které uživatele informují o tom, že strana spoléhající se na peněženku smí požadovat pouze údaje uvedené v registračních certifikátech pro zamýšlené použití zapsané v registračních certifikátech;

d) zajistí, aby poskytovatelé řešení peněženky usazení v tomto členském státě dodržovali obecné zásady přístupu tím, že budou uživatele informovat, pokud strana spoléhající se na peněženku požaduje údaje, které nejsou uvedeny v registračních certifikátech;

e) implementuje registrační certifikáty strany spoléhající se na peněženku syntakticky a sémanticky harmonizovaným způsobem a v souladu s požadavky stanovenými v příloze V;

f) uplatňuje zvláštní zásady certifikátů a prohlášení o certifikačních postupech pro registrační certifikáty strany spoléhající se na peněženku v souladu s požadavky stanovenými v příloze V;

g) zajistí, aby strany spoléhající se na peněženku poskytly adresu URL zásad ochrany soukromí týkajících se zamýšleného použití.

3. Zásady uvedené v písmenu g) se uvedou v registračním certifikátu strany spoléhající se na peněženku.

Článek 9

Pozastavení a zrušení registrace

1. Registrátoři pozastaví nebo zruší registraci strany spoléhající se na peněženku, pokud o takové pozastavení nebo zrušení požádá orgán dohledu podle čl. 46a odst. 4 písm. f) nařízení (EU) č. 910/2014.

2. Registrátoři mohou pozastavit nebo zrušit registraci strany spoléhající se na peněženku, pokud mají důvod se domnívat, že je splněna jedna z následujících podmínek:

a) registrace obsahuje nepřesné, neaktuální nebo zavádějící informace;

b) strana spoléhající se na peněženku nedodržuje zásady registrace;

c) strana spoléhající se na peněženku žádá o více atributů, než kolik jich zaregistrovala v souladu s články 5 a 6;

d) strana spoléhající se na peněženku porušuje právo Unie nebo vnitrostátní právo jiným způsobem, který souvisí s její rolí strany spoléhající se na peněženku.

3. Registrátoři pozastaví nebo zruší registraci strany spoléhající se na peněženku, pokud žádost o zrušení nebo pozastavení podá tatáž strana spoléhající se na peněženku.

4. Při zvažování pozastavení nebo zrušení podle odstavce 2 provede registrátor posouzení přiměřenosti, přičemž zohlední dopad na základní práva, bezpečnost a důvěrnost uživatelů v ekosystému, jakož i očekávanou závažnost narušení způsobeného pozastavením nebo zrušením a související náklady jak pro stranu spoléhající se na peněženku, tak pro uživatele. Na základě výsledku tohoto posouzení může registrátor pozastavit nebo zrušit registraci s předchozím oznámením dotčené straně spoléhající se na peněženku nebo bez něj.

5. Pokud je registrace strany spoléhající se na peněženku pozastavena nebo zrušena, registrátor o tomto opatření bez zbytečného odkladu, nejpozději však do 24 hodin od pozastavení nebo zrušení, informuje poskytovatele příslušných přístupových certifikátů strany spoléhající se na peněženku, poskytovatele příslušných registračních certifikátů strany spoléhající se na peněženku a dotčenou stranu spoléhající se na peněženku. Toto oznámení musí obsahovat informace o důvodech pozastavení nebo zrušení a o dostupných opravných prostředcích nebo možnostech odvolání.

6. Poskytovatel přístupových certifikátů strany spoléhající se na peněženku a poskytovatel registračních certifikátů strany spoléhající se na peněženku v příslušných případech bez zbytečného odkladu zneplatní přístupové certifikáty strany spoléhající se na peněženku a registrační certifikáty strany spoléhající se na peněženku, pokud jde o stranu spoléhající se na peněženku, jejíž registrace byla pozastavena nebo zrušena.

Článek 10

Vedení záznamů

Registrátoři uchovávají záznamy o informacích poskytnutých stranami spoléhajícími se na peněženku a zaregistrovaných v souladu s přílohou I za účelem registrace strany spoléhající se na peněženku a vydání přístupových certifikátů strany spoléhající se na peněženku a registračních certifikátů strany spoléhající se na peněženku a o všech následných změnách těchto informací po dobu deseti let.

Článek 11

Vstup v platnost

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

Použije se ode dne 24. prosince 2026.

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

V Bruselu dne 6. května 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA I

Informace o stranách spoléhajících se na peněženku

1. V příslušných případech název strany spoléhající se na peněženku, jak je uveden v úředním záznamu, spolu s identifikačními údaji tohoto úředního záznamu.

   a) Neexistuje-li žádný použitelný, použije se bod 2.

2. V příslušných případech uživatelsky přívětivý název strany spoléhající se na peněženku, což může být obchodní název nebo název služby, který je pro uživatele rozpoznatelný.

3. V příslušných případech jeden nebo více identifikátorů strany spoléhající se na peněženku uvedených v úředním záznamu spolu s identifikačními údaji tohoto úředního záznamu, vyjádřenými jako:

   a) registrační a identifikační číslo hospodářských subjektů („EORI“) uvedené v prováděcím nařízení Komise (EU) č. 1352/2013 ([1]);

   b) registrační číslo zapsané ve vnitrostátním obchodním rejstříku;

   c) identifikační kód právnické osoby („LEI“) uvedený v prováděcím nařízení Komise (EU) 2022/1860 ([2]);

   d) identifikační číslo pro účely daně z přidané hodnoty („DPH“);

   e) číslo pro účely spotřebních daní uvedené v čl. 2 bodě 12 nařízení Rady (EU) č. 389/2012 ([3]);

   f) daňové registrační číslo;

   g) jedinečný evropský identifikační kód („EUID“) uvedený v prováděcím nařízení Komise (EU) 2021/1042 ([4]);

   h) jiný vnitrostátní identifikátor nebo identifikátory.

4. Fyzická adresa, na které je usazena strana spoléhající se na peněženku.

5. V příslušných případech adresa URL strany spoléhající se na peněženku.

6. Pokud je identifikátor vyjádřen v souladu s bodem 3 písm. (a), (d), (f) nebo (h), uvede se před ním kód země členského státu, v němž je strana spoléhající se na peněženku usazena, s použitím kódů ISO 3166-1 Alpha 2, s výjimkou kódu země pro Řecko, který je „EL“.

7. Kontaktní údaje strany spoléhající se na peněženku – alespoň jeden z těchto údajů:

   a) internetové stránky, jejichž prostřednictvím lze stranu spoléhající se na peněženku kontaktovat v záležitostech týkajících se poskytování asistenční služby a podpory;

   b) telefonní číslo, na kterém lze stranu spoléhající se na peněženku kontaktovat v záležitostech týkajících se její registrace a zamýšleného použití jednotek peněženky;

   c) e-mailová adresa, na níž lze stranu spoléhající se na peněženku kontaktovat v záležitostech týkajících se její registrace a zamýšleného použití jednotky peněženky.

8. Popis typu služeb, které strana spoléhající se na peněženku poskytuje.

([1]) Prováděcí nařízení Komise (EU) č. 1352/2013 ze dne 4. prosince 2013, kterým se zavádějí formuláře upravené nařízením Evropského parlamentu a Rady (EU) č. 608/2013 o vymáhání práv duševního vlastnictví celními orgány (Úř. věst. L 341, 18.12.2013, s. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([2]) Prováděcí nařízení Komise (EU) 2022/1860 ze dne 10. června 2022, kterým se stanoví prováděcí technické normy pro uplatňování nařízení Evropského parlamentu a Rady (EU) č. 648/2012, pokud jde o standardy, formáty, četnost a metody a mechanismy oznamování (Úř. věst. L 262, 7.10.2022, s. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Nařízení Rady (EU) č. 389/2012 ze dne 2. května 2012 o správní spolupráci v oblasti spotřebních daní a o zrušení nařízení (ES) č. 2073/2004 (Úř. věst. L 121, 8.5.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

([4]) Prováděcí nařízení Komise (EU) 2021/1042 ze dne 18. června 2021, kterým se stanoví prováděcí pravidla ke směrnici Evropského parlamentu a Rady (EU) 2017/1132, pokud jde o technické specifikace a postupy pro systém propojení rejstříků, a zrušuje prováděcí nařízení Komise (EU) 2020/2244 (Úř. věst. L 225, 25.6.2021, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2021/1042/oj).

9. Pro každé zamýšlené použití seznam údajů, včetně potvrzení a atributů, které spoléhající se strana hodlá požadovat, uživatelsky přívětivý název a technický název, typ potvrzení a případné další syntaxe, pod nimiž jsou údaje seskupeny, ve strojově čitelném formátu pro automatizované zpracování.

10. Pro každé zamýšlené použití popis zamýšleného použití údajů, které strana spoléhající se na peněženku hodlá požadovat od jednotek peněženky.

11. Údaj o tom, zda je strana spoléhající se na peněženku subjektem veřejného sektoru.

12. Oprávnění strany spoléhající se na peněženku, které je vyjádřeno nebo která jsou vyjádřena takto:

    a) „Service_Provider“ pro vyjádření oprávnění strany spoléhající se na peněženku jako poskytovatele služeb;

    b) „QEAA_Provider“ pro vyjádření oprávnění strany spoléhající se na peněženku jako kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikovaná elektronická potvrzení atributů;

    c) „Non_Q_EAA_Provider“ pro vyjádření oprávnění strany spoléhající se na peněženku jako poskytovatele služeb vytvářejících důvěru, který vydává nekvalifikovaná elektronická potvrzení atributů;

    d) „PUB_EAA_Provider“ pro vyjádření oprávnění strany spoléhající se na peněženku jako poskytovatele elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem;

    e) „PID_Provider“ pro vyjádření oprávnění strany spoléhající se na peněženku jako poskytovatele osobních identifikačních údajů;

    f) „QCert_for_ESeal_Provider“ pro vyjádření oprávnění strany spoléhající se na peněženku jako kvalifikovaného poskytovatele služeb vytvářejících důvěru vydávajícího kvalifikované certifikáty pro elektronické pečetě;

    g) „QCert_for_ESig_Provider“ pro vyjádření oprávnění strany spoléhající se na peněženku jako kvalifikovaného poskytovatele služeb vytvářejících důvěru vydávajícího kvalifikované certifikáty pro elektronické podpisy;

    h) „rQSigCDs_Provider“ pro vyjádření oprávnění strany spoléhající se na peněženku jako kvalifikovaného poskytovatele služeb vytvářejících důvěru poskytujícího kvalifikované služby vytvářející důvěru pro správu kvalifikovaného prostředku pro vytváření elektronických podpisů na dálku;

    i) „rQSealCDs_Provider“ pro vyjádření oprávnění strany spoléhající se na peněženku jako kvalifikovaného poskytovatele služeb vytvářejících důvěru poskytujícího kvalifikované služby vytvářející důvěru pro správu kvalifikovaného prostředku pro vytváření elektronických pečetí na dálku;

    j) „ESig_ESeal_Creation_Provider“ pro vyjádření oprávnění strany spoléhající se na peněženku jako nekvalifikovaného poskytovatele služeb vytvářejících důvěru poskytujícího nekvalifikovanou službu vytvářející důvěru pro vytváření elektronických podpisů nebo elektronických pečetí na dálku.

13. Pokud jde o bod 12 písm. (c), členské státy mohou stanovit další dílčí oprávnění, aby uvedly, která potvrzení konkrétní nekvalifikovaný vydavatel elektronických potvrzení atributů vydává.

14. V příslušných případech údaj o tom, že se strana spoléhající se na peněženku spoléhá na zprostředkovatele jednajícího jménem spoléhající se strany, která má v úmyslu spoléhat se na peněženku.

15. V příslušných případech propojení se zprostředkovatelem, na kterého se strana spoléhající se na peněženku spoléhá a který jedná jménem spoléhající se strany, která má v úmyslu spoléhat se na peněženku.

PŘÍLOHA II

1. POŽADAVKY NA ELEKTRONICKÉ PODPISY NEBO PEČETĚ, KTERÝMI SE OPATŘUJÍ ZPŘÍSTUPŇOVANÉ INFORMACE O REGISTROVANÝCH STRANÁCH SPOLÉHAJÍCÍCH SE NA PENĚŽENKU, UVEDENÉ V ČLÁNKU 3

— JavaScriptová objektová notace („JSON“);

— standard IETF 7515 pro podpisy JSON Web Signature.

2. POŽADAVKY NA JEDNOTNÉ SPOLEČNÉ ROZHRANÍ API UVEDENÉ V ČLÁNKU 3

1. Jednotné společné rozhraní API:

a) je rozhraním REST API, které podporuje formát JSON a podpisy v souladu s příslušnými požadavky uvedenými v oddíle 1;

b) umožňuje každému žadateli, aby bez předchozí autentizace prohledával rejstřík a žádal o úplné seznamy, pokud jde o informace o registrovaných stranách spoléhající se na peněženku, přičemž umožňuje částečné shody na základě definovaných parametrů, v příslušných případech včetně úředního registračního čísla nebo registračního čísla podniku strany spoléhající se na peněženku, názvu strany spoléhající se na peněženku nebo informací uvedených v čl. 8 odst. 2 písm. g) a v bodech 12, 13, 14 a 15 přílohy I;

c) zajišťuje, aby odpovědi na žádosti uvedené v písmenu (b), které odpovídají alespoň jedné straně spoléhající se na peněženku, obsahovaly jedno nebo více prohlášení o informacích o registrovaných stranách spoléhajících se na peněženku a informace v souladu s přílohou I, aktuální a historické přístupové certifikáty strany spoléhající se na peněženku a registrační certifikáty strany spoléhající se na peněženku, avšak neobsahovaly kontaktní údaje uvedené v bodě 4 přílohy I;

d) se zveřejní jako OpenAPI verze 3 spolu s příslušnou dokumentací a technickými specifikacemi zajišťujícími interoperabilitu v celé Unii;

e) poskytuje bezpečnostní funkce, včetně zásady „security by default and by design“ (bezpečnost jako standard a již od fáze návrhu), aby byla zajištěna dostupnost a integrita rozhraní API a dostupnost informací prostřednictvím tohoto rozhraní.

2. Prohlášení uvedená v písmenu (c) mají formu souborů JSON opatřených elektronickým podpisem nebo pečetí, jejichž formát a struktura jsou v souladu s požadavky na elektronické podpisy nebo pečetě stanovenými v oddíle 1.

PŘÍLOHA III

Zdroj podpůrných dokladů pro ověření oprávnění stran spoléhajících se na peněženku uvedených v článku 6

1. Ověření, že strana spoléhající se na peněženku je poskytovatelem kvalifikovaných elektronických potvrzení atributů, poskytovatelem kvalifikovaných certifikátů pro elektronické podpisy nebo pečetě nebo poskytovatelem kvalifikované služby vytvářející důvěru pro správu kvalifikovaných prostředků pro vytváření elektronických podpisů nebo pečetí na dálku, se zakládá na vnitrostátních důvěryhodných seznamech zveřejněných v souladu s článkem 22 nařízení (EU) č. 910/2014.

2. Ověření, že strana spoléhající se na peněženku je poskytovatelem nekvalifikovaných elektronických potvrzení atributů nebo poskytovatelem služby vytváření elektronických podpisů nebo pečetí na dálku jako nekvalifikované služby vytvářející důvěru, se v příslušných případech zakládá na vnitrostátních důvěryhodných seznamech zveřejněných v souladu s článkem 22 nařízení (EU) č. 910/2014, nebo v případě poskytovatelů nekvalifikovaných služeb vytvářejících důvěru, kteří nejsou zapsáni ve vnitrostátních důvěryhodných seznamech, na postupech ověřování, které členské státy stanovily ve svých zásadách registrace, jak stanoví článek 4.

3. Ověření, zda je strana spoléhající se na peněženku poskytovatelem osobních identifikačních údajů, se zakládá na seznamu poskytovatelů osobních identifikačních údajů zveřejněném Komisí v souladu s čl. 5a odst. 18 nařízení (EU) č. 910/2014.

4. Ověření, že strana spoléhající se na peněženku je poskytovatelem elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem, se zakládá na seznamu zveřejněném Komisí v souladu s čl. 45f odst. 3 nařízení (EU) č. 910/2014.

PŘÍLOHA IV

Požadavky na přístupové certifikáty strany spoléhající se na peněženku uvedené v článku 7

1. Certifikační politika pro přístupové certifikáty strany spoléhající se na peněženku použitelná na poskytování přístupových certifikátů strany spoléhající se na peněženku popisuje bezpečnostní požadavky, které se vztahují na přístupový certifikát strany spoléhající se na peněženku, a pravidla, která určují jeho použitelnost, aby mohly být stranám spoléhajícím se na peněženku tyto certifikáty vydávány a strany spoléhající se na peněženku je mohly používat při interakci s řešeními peněženky.

2. Prohlášení o certifikačních postupech pro přístupové certifikáty strany spoléhající se na peněženku použitelné na poskytování přístupových certifikátů strany spoléhající se na peněženku popisuje postupy, které poskytovatel přístupových certifikátů strany spoléhající se na peněženku používá při vydávání, správě, zneplatňování a změnách klíčů přístupových certifikátů strany spoléhající se na peněženku.

3. Certifikační politika a prohlášení o certifikačních postupech použitelné na poskytování přístupových certifikátů strany spoléhající se na peněženku jsou syntakticky a sémanticky harmonizovány v celé Unii a v příslušných případech splňují alespoň požadavky normalizované certifikační politiky („NCP“) stanovené v normě ETSI EN 319411-1, verzi 1.4.1 (2023-10) a obsahují:

   a) jasný popis hierarchie infrastruktury veřejných klíčů a certifikačních cest od přístupových certifikátů strany spoléhající se na peněženku jakožto koncové entity až po vrchol hierarchie používané pro jejich vydávání, přičemž se uvede očekávaný zdroj nebo zdroje důvěry v této hierarchii a cesty, které by se měly opírat o rámec pro důvěryhodnost zavedený v souladu s čl. 5a odst. 18 nařízení (EU) č. 910/2014;

   b) úplný popis postupů pro vydávání přístupových certifikátů strany spoléhající se na peněženku, včetně ověřování totožnosti a veškerých dalších atributů strany spoléhající se na peněženku, které má být certifikát strany spoléhající se na peněženku vydán;

   c) povinnost poskytovatelů přístupových certifikátů strany spoléhající se na peněženku při vydávání přístupového certifikátu strany spoléhající se na peněženku ověřit, že:

      — strana spoléhající se na peněženku je s platným registračním statusem vedena ve vnitrostátním registru stran spoléhajících se na peněženku členského státu, v němž je tato strana spoléhající se na peněženku usazena,

      — všechny informace v přístupovém certifikátu strany spoléhající se na peněženku jsou přesné a v souladu s informacemi o registraci dostupnými z tohoto registru;

   d) úplný popis postupů pro zneplatnění přístupových certifikátů strany spoléhající se na peněženku;

   e) povinnost poskytovatelů přístupových certifikátů strany spoléhající se na peněženku zavést opatření a postupy pro:

      — průběžné sledování veškerých změn ve vnitrostátním registru stran spoléhajících se na peněženku, v němž jsou registrovány strany spoléhající se na peněženku, kterým vydali přístupové certifikáty strany spoléhající se na peněženku,

      — zneplatnění, pokud to vyžadují změny, jakékoli certifikátu strany spoléhající se na peněženku, který poskytovatel vydal příslušné straně spoléhající se na peněženku, zejména pokud obsah certifikátu již není přesný a v souladu s registrovanými informacemi nebo pokud je registrace strany spoléhající se na peněženku pozastavena nebo zrušena;

   f) úplný popis postupů a mechanismů pro harmonizované ověřování platnosti přístupových certifikátů strany spoléhající se na peněženku v celé Unii;

   g) povinnost poskytovatelů přístupových certifikátů strany spoléhající se na peněženku umožnit příslušným zúčastněným stranám, včetně stran spoléhajících se na peněženku, pokud jde o jejich vlastní certifikáty, příslušných orgánů dohledu a úřadů pro ochranu osobních údajů, požádat o zneplatnění přístupových certifikátů strany spoléhající se na peněženku;

   h) povinnost poskytovatelů přístupových certifikátů strany spoléhající se na peněženku registrovat všechna taková zneplatnění ve své databázi certifikátů a zveřejnit stav zneplatnění certifikátu včas, v každém případě do 24 hodin po obdržení žádosti o zneplatnění;

i) povinnost poskytovatelů přístupových certifikátů strany spoléhající se na peněženku poskytovat informace o stavu platnosti nebo zneplatnění certifikátů strany spoléhající se na peněženku vydaných tímto poskytovatelem;

j) v příslušných případech popis toho, jak poskytovatel přístupových certifikátů strany spoléhající se na peněženku zaznamenává do protokolu všechny vydané přístupové certifikáty strany spoléhající se na peněženku v souladu s dokumentem IETF RFC 9162 Certificate Transparency verze 2.0;

k) povinnost, aby přístupové certifikáty strany spoléhající se na peněženku obsahovaly:

— umístění, kde je dostupný certifikát podporující zaručený elektronický podpis nebo zaručenou elektronickou pečeť na tomto certifikátu, aby byla vytvořena celá certifikační cesta až k očekávanému zdroji důvěry v hierarchii infrastruktury veřejných klíčů používané poskytovatelem,

— strojově zpracovatelný odkaz na příslušnou certifikační politiku a prohlášení o certifikačních postupech,

— informace uvedené v bodech 1, 2, 3, 5 a 6 a v bodě 7 písm. (a), (b) a (c) přílohy I.

4. Zneplatnění uvedené v bodě 3 písm. (g) nabývá účinnosti ihned po zveřejnění.

5. Informace uvedené v bodě 3 písm. (h) se poskytnou alespoň pro každý certifikát, a to kdykoli alespoň po skončení doby platnosti certifikátu, automatizovaným způsobem, který je spolehlivý, bezplatný a účinně v souladu s certifikační politikou.

PŘÍLOHA V

Požadavky na registrační certifikáty strany spoléhající se na peněženku uvedené v článku 8

1. Certifikační politika pro registrační certifikáty strany spoléhající se na peněženku použitelná na poskytování registračních certifikátů strany spoléhající se na peněženku popisuje bezpečnostní požadavky, které se vztahují na registrační certifikát strany spoléhající se na peněženku, a pravidla, která určují použitelnost těchto certifikátů, pokud jde o jejich vydávání stranám spoléhajícím se na peněženku a používání stranami spoléhajícími se na peněženku při interakci s řešeními peněženky. Certifikační politika pro registrační certifikáty strany spoléhající se na peněženku se zveřejňuje ve formátu čitelném pro člověka.

2. Prohlášení o certifikačních postupech pro registrační certifikáty strany spoléhající se na peněženku použitelné na poskytování registračních certifikátů strany spoléhající se na peněženku popisuje postupy, které poskytovatel registračních certifikátů strany spoléhající se na peněženku používá při vydávání, správě, zneplatňování a změně klíče registračních certifikátů strany spoléhající se na peněženku a v příslušných případech i to, jak souvisí s přístupovými certifikáty strany spoléhající se na peněženku vydávanými stranám spoléhajícím se na peněženku. Prohlášení o certifikačních postupech pro registrační certifikáty strany spoléhající se na peněženku se zveřejňuje ve formátu čitelném pro člověka.

3. Certifikační politika a prohlášení o certifikačních postupech pro registrační certifikáty strany spoléhající se na peněženku použitelné na poskytování registračních certifikátů strany spoléhající se na peněženku jsou syntakticky a sémanticky harmonizovány v celé Unii, splňují alespoň použitelné požadavky NCP stanovené v normě ETSI EN 319411-1, verzi 1.4.1 (2023-10) a obsahují:

   a) jasný popis hierarchie infrastruktury veřejných klíčů a certifikačních cest od registračních certifikátů strany spoléhající se na peněženku jakožto koncové entity až po vrchol hierarchie používané pro jejich vydávání, přičemž se uvede očekávaný zdroj nebo zdroje důvěry v této hierarchii a cestách;

   b) úplný popis postupů pro vydávání registračních certifikátů strany spoléhající se na peněženku, včetně ověření totožnosti a všech atributů strany spoléhající se na peněženku, které má být certifikát strany spoléhající se na peněženku vydán;

   c) povinnost poskytovatele registračních certifikátů strany spoléhající se na peněženku při vydávání registračního certifikátu strany spoléhající se na peněženku ověřit, že:

      — strana spoléhající se na peněženku je s platným registračním statusem vedena ve vnitrostátním registru stran spoléhajících se na peněženku členského státu, v němž je tato strana spoléhající se na peněženku usazena,

      — informace v registračním certifikátu strany spoléhající se na peněženku jsou přesné a odpovídají informacím o registraci dostupným z tohoto registru;

      — přístupový certifikát strany spoléhající se na peněženku je platný;

      — popis postupů pro zneplatnění registračních certifikátů strany spoléhající se na peněženku je úplný;

   d) povinnost poskytovatele registračních certifikátů strany spoléhající se na peněženku zavést opatření a postupy pro:

      — průběžné automatizované sledování veškerých změn ve vnitrostátním registru stran spoléhajících se na peněženku, v němž jsou registrovány strany spoléhající se na peněženku, kterým vydal registrační certifikáty strany spoléhající se na peněženku,

      — opětovné vydání registračního certifikátu strany spoléhající se na peněženku,

      — zneplatnění jakékoli registračního certifikátu strany spoléhající se na peněženku, který vydal příslušné straně spoléhající se na peněženku, pokud to vyžadují změny, zejména pokud obsah certifikátu již není přesný a v souladu s registrovanými informacemi nebo pokud je registrace strany spoléhající se na peněženku změněna, pozastavena nebo zrušena;

   e) úplný popis postupů a mechanismů pro harmonizované ověřování platnosti registračních certifikátů strany spoléhající se na peněženku;

f) povinnost poskytovatele registračních certifikátů strany spoléhající se na peněženku umožnit příslušným zúčastněným stranám, včetně stran spoléhajících se na peněženku, pokud jde o jejich vlastní certifikáty, příslušných orgánů dohledu a úřadů pro ochranu osobních údajů, požádat o zneplatnění registračních certifikátů strany spoléhající se na peněženku;

g) povinnost poskytovatele registračních certifikátů strany spoléhající se na peněženku registrovat všechna taková zneplatnění ve své databázi certifikátů a zveřejnit stav zneplatnění certifikátu včas, v každém případě do 24 hodin po obdržení žádosti o zneplatnění;

h) povinnost poskytovatelů registračních certifikátů strany spoléhající se na peněženku poskytovat informace o stavu platnosti nebo zneplatnění registračních certifikátů strany spoléhající se na peněženku vydaných tímto poskytovatelem.

i) v příslušných případech popis způsobu, jakým poskytovatel registračních certifikátů strany spoléhající se na peněženku zaznamenává do protokolu všechny jím vydané registrační certifikáty strany spoléhající se na peněženku;

j) povinnost, aby registrační certifikáty strany spoléhající se na peněženku:

— obsahovaly umístění, kde jsou k dispozici data pro ověření platnosti zaručeného elektronického podpisu nebo zaručené elektronické pečeti certifikátu použitého k podepsání nebo zapečetění registračního certifikátu, aby bylo možné sestavit celý řetězec důvěry až k očekávanému zdroji důvěry,

— obsahovaly strojově čitelný odkaz na příslušnou certifikační politiku a prohlášení o certifikačních postupech,

— obsahovaly informace uvedené v bodech 1, 2, 3, 5, 6, 8, 9, 10, 11, 12, 13, 14 a 15 přílohy I,

— obsahovaly adresu URL zásad ochrany soukromí uvedených v čl. 8 odst. 2 písm. g),

— obsahovaly obecné zásady přístupu uvedené v čl. 8 odst. 3.

4. Formátem pro výměnu dat pro registrační certifikát spoléhající se strany je podepsaný formát JSON Web Tokens (IETF RFC 7519) a CBOR Web Tokens (IETF RFC 8392).

5. Zneplatnění uvedené v bodě 3 písm. (g) nabývá účinnosti ihned po zveřejnění.

6. Informace uvedené v bodě 3 písm. (h) se poskytnou alespoň pro každý certifikát, a to kdykoli alespoň po skončení doby platnosti certifikátu, automatizovaným způsobem, který je spolehlivý, bezplatný a účinně v souladu s certifikační politikou.