2026/1731

22.7.2026

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2026/1731

ze dne 15. července 2026,

kterým se mění prováděcí nařízení (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 a (EU) 2024/2982, pokud jde o použitelné normy a specifikace

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) V zájmu zajištění co nejvyšší úrovně harmonizace mezi členskými státy při vývoji evropských peněženek digitální identity se technické specifikace peněženek opírají o práci provedenou na základě doporučení Komise (EU) 2021/946 ([2]), a zejména o architekturu a referenční rámec. Vzhledem k tomu, že se architektura a referenční rámec od vydání prováděcích nařízení Komise (EU) 2024/2977 ([3]), (EU) 2024/2979 ([4]), (EU) 2024/2980 ([5]) a (EU) 2024/2982 ([6]) výrazně vyvinuly, měla by být tato prováděcí nařízení nyní změněna tak, aby byla v souladu s novými normami, specifikacemi a postupy.

V souladu s cíli nařízení (EU) č. 910/2014 byla pro splnění těchto zvláštních požadavků vybrána řada norem. Tyto normy by měly odrážet zavedené postupy a měly by být v příslušných odvětvích široce uznávány. Vzhledem k tomu, že formát W3C VCDM se používá jako referenční formát pro potvrzení zejména v oblasti vzdělávání, měly by evropské peněženky digitální identity podporovat také tento formát, jakmile budou k dispozici nové profily formátu W3C VCDM. V případě potřeby by měly být tyto normy upraveny nebo doplněny, aby byla zajištěna bezpečnost a důvěryhodnost evropských peněženek digitální identity a zároveň usnadněna přeshraniční interoperabilita a účinné fungování vnitřního trhu.

(2) Při jakémkoli použití peněženky, které vyžaduje předložení portrétu uživatele peněženky, musí řešení peněženky podporovat funkci výběrového zpřístupňování a zpřístupnění musí být plně pod kontrolou uživatele. Aby byla chráněna schopnost rozhodovat o zpřístupňování a portrét před nezamýšlenými nebo neoprávněnými žádostmi o zpřístupnění, měl by architektonický návrh evropských peněženek digitální identity stanovit mechanismy varování a zaznamenávání všech transakcí souvisejících s použitím portrétu. Aby bylo zajištěno, že si je uživatel peněženky vědom sdílení biometrických údajů, měla by varování uvádět, že žádost zahrnuje sdílení biometrických údajů,

([1]) Úř. věst. L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/ces.
([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/ces).
([3]) 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).
([4]) 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).
([5]) 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 evropských peněženek digitální identity (Úř. věst. L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).
([6]) 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).

a konkrétně požadovat, aby uživatel zpřístupnění potvrdil. Pokud spoléhající se strana zpracovává portrét za účelem jedinečné identifikace fyzické osoby nebo potvrzení deklarované totožnosti této osoby, použijí se články 6 a 9 nařízení Evropského parlamentu a Rady (EU) 2016/679 ([7]), jakož i všechny ostatní požadavky uvedeného nařízení, včetně toho, že zpracování portrétu spoléhajícími se stranami by mělo být omezeno na to, co je nezbytné pro zamýšlené použití. Zamýšlené použití by mělo být uživateli peněženky sděleno spolu s žádostí o zpřístupnění jasným a srozumitelným jazykem. Aby byla řádně zohledněna citlivost biometrických údajů, měl by uživatel peněženky výslovně a konkrétně potvrdit zpřístupnění portrétu. Za potvrzení uživatelem peněženky by se nemělo považovat mlčení nebo předem zaškrtnutá políčka. Výslovné potvrzení uživatelem peněženky by mělo být technickou zárukou a samo o sobě by nemělo představovat právní základ zpracování. Jak je stanoveno v čl. 9 odst. 4 nařízení (EU) 2016/679, členské státy mohou zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování genetických údajů, biometrických údajů či údajů o zdravotním stavu.

(3) Aby měly členské státy dostatek času na přizpůsobení svých vnitrostátních postupů, může být portrét uživatele peněženky součástí povinných osobních identifikačních údajů fyzické osoby až od 11. srpna 2028. Pokud tato zobrazení pocházejí ze stávajících dokladů totožnosti, jako jsou občanské průkazy nebo cestovní pasy, použijí se příslušné požadavky stanovené v nařízeních Rady (EU) 2025/1208 ([8]) nebo (ES) č. 2252/2004 ([9]).

(4) Nařízení (EU) č. 910/2014 vyžaduje, aby peněženky byly schopny zobrazovat značku důvěry EU pro peněženku digitální identity jako ověřitelné, jednoduché a rozpoznatelné označení, které sděluje, že peněženka byla poskytnuta v souladu s uvedeným nařízením. Používání této značky důvěry podpoří účinné fungování vnitřního trhu, zaručí spravedlivou hospodářskou soutěž a ochrání zájmy spotřebitelů. Aby bylo možné takovou značku důvěry používat, měly by být stanoveny její vizuální a technické vlastnosti.

(5) Jak je stanoveno v článku 12b nařízení (EU) č. 910/2014, strážci přístupu mají umožnit poskytovatelům evropských peněženek digitální identity a vydavatelům oznámených prostředků pro elektronickou identifikaci účinnou interoperabilitu a pro účely interoperability přístup ke stejnému operačnímu systému, hardwarovým nebo softwarovým prvkům. Tato účinná interoperabilita a přístup musí být umožněny bezplatně a bez ohledu na to, zda jsou tyto hardwarové nebo softwarové prvky součástí operačního systému, zda jsou dostupné strážci přístupu nebo zda jsou strážcem přístupu používané při poskytování těchto služeb. Vzhledem k tomu, že všechna řešení peněženky by měla podporovat společný soubor protokolů a rozhraní, aby byla zajištěna použitelnost, bezpečnost a interoperabilita ve všech členských státech, měli by strážci přístupu umožnit použití operačního systému, hardwarových nebo softwarových prvků nezbytných k zavedení protokolů a rozhraní uvedených v příloze XII tohoto nařízení. V této souvislosti by strážci přístupu měli v online tocích mezi zařízeními, pokud jde o kontrolu fyzické blízkosti i přenos dat mezi uvedenými dvěma zařízeními, upřednostňovat místní komunikační kanál, který umožňuje specifikace protokolu CTAP (Client To Authenticator Protocol) verze 2.3 ([10]), před použitím hybridních tunelových služeb CTAP.

(6) Aby měli členské státy, poskytovatelé registračních certifikátů strany spoléhající se na peněženku a poskytovatelé peněženek dostatek času na to, aby jednotkám peněženky umožnili autentizovat registrační certifikáty strany spoléhající se na peněženku a ověřovat jejich platnost, měl by se tento požadavek použít až od 11. srpna 2028.

(7) Na všechny činnosti zpracování osobních údajů podle tohoto nařízení se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679 a v příslušných případech směrnice Evropského parlamentu a Rady 2002/58/ES ([11]).

([7]) 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).

([8]) Nařízení Rady (EU) 2025/1208 ze dne 12. června 2025 o posílení zabezpečení průkazů totožnosti občanů Unie a povolení k pobytu vydávaných občanům Unie a jejich rodinným příslušníkům, kteří vykonávají své právo volného pohybu (Úř. věst. L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Nařízení Rady (ES) č. 2252/2004 ze dne 13. prosince 2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy (Úř. věst. L 385, 29.12.2004, s. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Norma navržená aliancí FIDO, Client to Authenticator Protocol (CTAP), 26. února 2026.

([11]) 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).

(8) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([12]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 17. dubna 2026 ([13]).

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

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Změny prováděcího nařízení (EU) 2024/2977

Prováděcí nařízení (EU) 2024/2977 se mění takto:

1) vkládá se nový článek 3a, který zní:

„*Článek 3a*

Ochrana portrétu

1. Kromě požadavků na informace podle nařízení (EU) 2016/679 poskytovatelé peněženek zajistí, aby v případě, že strany spoléhající se na peněženku požadují zpřístupnění portrétu, jimi poskytovaná řešení peněženky vydávala varování pro uživatele peněženek, v nichž se uvádí, že žádost zahrnuje sdílení biometrických údajů a vyžaduje potvrzení výběrového zpřístupnění portrétu.

2. Pro účely zavedení výběrového zpřístupňování portrétu straně spoléhající se na peněženku poskytovatelé peněženek zajistí, aby řešení peněženky vyžadovala od uživatele peněženky výslovné a konkrétní potvrzení předložení portrétu.

3. Strany spoléhající se na peněženku portrét neuchovávají, pokud jeho zpracování není nezbytné pro účely identifikace a autentizace v souladu s právem Unie v oblasti ochrany údajů nebo pokud to nestanoví právo Unie nebo vnitrostátní právo v souladu s právem Unie v oblasti ochrany údajů. Portrét nesmí být předán do třetích zemí nebo mezinárodním organizacím, pokud to nepovoluje právo Unie v oblasti ochrany údajů.“;

2) v článku 4 se odstavec 1 nahrazuje tímto:

„1. Elektronická potvrzení atributů vydávaná k jednotkám peněženek splňují alespoň jednu z norem uvedených v příloze II prováděcího nařízení (EU) 2024/2979.“;

3) v čl. 5 odst. 4 se písmeno b) nahrazuje tímto:

„b) pokud bylo zneplatněno potvrzení jednotky peněženky, ke které byly osobní identifikační údaje vydány;“

4) příloha se nahrazuje zněním uvedeným v příloze I tohoto nařízení.

([12]) 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).

([13]) EDPS Formal comments on the draft Implementing Regulation as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980 | European Data Protection Supervisor (Formální připomínky evropského inspektora ochrany údajů k návrhu prováděcího nařízení, pokud jde o použitelné normy a specifikace a opravu prováděcího nařízení (EU) 2024/2980 – evropský inspektor ochrany údajů).

Článek 2

Změny prováděcího nařízení (EU) 2024/2979

Prováděcí nařízení (EU) 2024/2979 se mění takto:

1) v článku 3 se zrušuje odstavec 2;

2) v čl. 5 odst. 1 se písmeno a) nahrazuje tímto:

„a) provedou kryptografické operace peněženky s kritickými aktivy uloženými v bezpečném kryptografickém prostředku peněženky, která nejsou vyžadována k autentizaci uživatele peněženky, pouze v případech, kdy tyto aplikace úspěšně autentizovaly uživatele peněženky;“

3) vkládá se nový článek 5a, který zní:

„*Článek 5a*

Kryptografické mechanismy

Poskytovatelé peněženek používají pro účely čl. 4 odst. 2 pouze kryptografické mechanismy uvedené v příloze Ia.“;

4) článek 6 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. Poskytovatelé peněženek vydají potvrzení jednotky peněženky pro každou jednotku peněženky. Poskytovatelé peněženek podepíší nebo opatří pečetí potvrzení jednotky peněženky tak, aby platnost podpisů nebo pečetí mohla být ověřena prostřednictvím certifikátu uvedeného na seznamu v souladu s přílohou II oddílem 2 bodem 1 písm. h) prováděcího nařízení (EU) 2024/2980.“;

b) odstavec 2 se nahrazuje tímto:

„2. Poskytovatelé peněženek zajistí, aby potvrzení jednotky peněženky uvedená v odstavci 1 splňovala technické specifikace stanovené v příloze Ib.“;

c) v odstavci 3 se písmeno b) nahrazuje tímto:

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

5) v čl. 9 odst. 2 se písmeno b) nahrazuje tímto:

„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;“

6) v článku 10 se odstavec 1 nahrazuje tímto:

„1. Poskytovatelé peněženek zajistí, aby elektronická potvrzení atributů vydaná v souladu s technickými specifikacemi platnými pro obecné vložené zásady zpřístupňování informací uvedené v příloze III mohla být zpracovávána jimi poskytovanými jednotkami peněženky.“;

7) článek 12 se mění takto:

a) v odstavci 2 se písmeno c) nahrazuje tímto:

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

b) odstavec 3 se nahrazuje tímto:

„3. Aplikace pro vytváření podpisů mohou být buď integrovány do instancí peněženky, nebo mohou být externí.“;

c) vkládá se nový odstavec, který zní:

„4. Aplikace pro vytváření podpisů používané jednotkami peněženky podporují alespoň aplikační programovací rozhraní uvedené v příloze IV.“;

8) v článku 14 se zrušuje odstavec 1;

9) vkládá se nový článek 14a, který zní:

„Článek 14a

Značka důvěry EU pro peněženku digitální identity

1. Poskytovatelé peněženek zajistí, aby jednotky peněženky zobrazovaly značku důvěry EU pro peněženku digitální identity. Značka důvěry EU pro peněženku digitální identity má podobu uvedenou v přílohách VI a VII.

2. Poskytovatelé peněženek zajistí, aby jednotky peněženky umožňovaly uživatelům peněženek přístup k informacím, které jim umožní ověřit stav certifikace řešení peněženky. Za tímto účelem poskytovatelé peněženek zajistí, aby po registraci řešení peněženky příslušné jednotky peněženky obsahovaly adresy URL poskytnuté Evropskou komisí pro toto ověření. Poskytovatelé peněženek zajistí, aby jejich jednotky peněženky měly přístup k údajům týkajícím se značky důvěry EU pro peněženku digitální identity, které jsou v souladu s technickými specifikacemi uvedenými v příloze VIII.

3. Referenčními barvami pro značku důvěry EU pro peněženku digitální identity jsou Pantone č. 661 a 116 nebo modrá (100 % azurová +67 % purpurová +0 % žlutá +40 % černá) a žlutá (0 % azurová +20 % purpurová +100 % žlutá +0 % černá), pokud se používá čtyřbarevný tisk; při použití barev RGB jsou referenčními barvami modrá (0 červená + 51 zelená + 153 modrá) a žlutá (255 červená + 204 zelená + 0 modrá).

4. Pouze v případech, kdy barvu není možné použít, lze značku důvěry EU pro peněženku digitální identity použít v černobílém provedení, jak je uvedeno v příloze VII.

5. Pokud je značka důvěry EU pro peněženku digitální identity použita na tmavém pozadí, lze ji použít v negativním formátu se stejnou barvou pozadí. Pokud je značka důvěry EU pro peněženku digitální identity použita barevně na barevném pozadí, které ztěžuje její viditelnost, může být kolem značky důvěry EU pro peněženku digitální identity použita ohraničující vnější linie, která zlepší kontrast s barvami pozadí.

6. Značka důvěry EU pro peněženku digitální identity má minimální velikost 64 × 85 pixelů při rozlišení 150 dpi.

7. Poskytovatelé peněženek zajistí, aby se značka důvěry EU pro peněženku digitální identity používala způsobem, který umožní jasné označení jednotky peněženky, jíž se značka důvěry EU pro peněženku digitální identity týká. Značka důvěry EU pro peněženku digitální identity může být spojena s grafickými nebo textovými prvky, které jasně označují jednotku peněženky, pro kterou je použita, za předpokladu, že nemění její rozpoznatelnost jako značky důvěry EU pro peněženku digitální identity ani její spojení se seznamem certifikovaných evropských peněženek digitální identity podle článku 5d nařízení (EU) č. 910/2014.

8. Pokud poskytovatelé peněženek zneplatnili potvrzení jednotky peněženky, zajistí, aby značka důvěry EU pro peněženku digitální identity již nebyla u příslušné jednotky peněženky zobrazena.“;

10) doplňují se přílohy Ia a Ib ve znění uvedeném v příloze II a příloze III tohoto nařízení;

11) příloha II se nahrazuje zněním uvedeným v příloze IV tohoto nařízení;

12) příloha III se nahrazuje zněním uvedeným v příloze V tohoto nařízení;

13) příloha IV se mění v souladu s přílohou VI tohoto nařízení;

14) příloha V se zrušuje;

15) znění uvedené v příloze VII tohoto nařízení se vkládá jako příloha VI;

16) znění uvedené v příloze VIII tohoto nařízení se vkládá jako příloha VII;

17) znění uvedené v příloze IX tohoto nařízení se vkládá jako příloha VIII.

Článek 3

Změny prováděcího nařízení (EU) 2024/2980

Prováděcí nařízení (EU) 2024/2980 se mění takto:

1. v článku 5 se odstavec 2 nahrazuje tímto:

„2. Komise v příslušných případech vytvoří, vede a zveřejní seznam obsahující informace oznámené členskými státy o poskytovatelích peněženek, poskytovatelích osobních identifikačních údajů, poskytovatelích přístupových certifikátů stran spoléhajících se na peněženku a poskytovatelích registračních certifikátů stran spoléhajících se na peněženku, jak je uvedeno v oddílech 2, 3, 4 a 5 přílohy II.“;

2. příloha II prováděcího nařízení (EU) 2024/2980 se mění v souladu s přílohou X tohoto nařízení.

Článek 4

Změny prováděcího nařízení (EU) 2024/2982

Prováděcí nařízení (EU) 2024/2982 se mění takto:

1) v článku 1 se bod 2 nahrazuje tímto:

„2) předkládání atributů osobních identifikačních údajů a elektronických potvrzení atributů stranám spoléhajícím se na peněženku;“

2) článek 3 se mění takto:

a) bod 1 se nahrazuje tímto:

„1) při interakci se stranami spoléhajícími se na peněženku autentizovaly přístupové certifikáty stran spoléhajících se na peněženku a ověřovaly jejich platnost, aniž by bylo provádění těchto procesů delegováno na operační systém, prohlížeč nebo jinou zprostředkující aplikaci;“

b) bod 2 se zrušuje;

c) bod 3 se nahrazuje tímto:

„3) autentizovaly žádosti podané pomocí přístupových certifikátů stran spoléhajících se na peněženku a ověřovaly jejich platnost;“

d) bod 4 se nahrazuje tímto:

„4) autentizovaly a ověřovaly platnost registračního certifikátu strany spoléhající se na peněženku;“

e) bod 5 se nahrazuje tímto:

„5) uživatelům peněženky zobrazovaly informace obsažené v přístupových certifikátech stran spoléhajících se na peněženku;“

f) bod 8 se zrušuje;

g) bod 9 se nahrazuje tímto:

„9) nepředkládaly stranám spoléhajícím se na peněženku žádné požadované atributy, dokud nebudou dokončeny následující kroky:

a) ověření, zda byly vložené zásady zpřístupnění zpracovány v rámci jednotky peněženky v souladu s článkem 10 prováděcího nařízení (EU) 2024/2979;

b) ověření, zda uživatelé peněženky předložení schválili částečně nebo v plném rozsahu;“

3) v článku 4 se odstavec 1 nahrazuje tímto:

„1. Poskytovatelé peněženek zajistí, aby řešení peněženky podporovala protokoly a rozhraní stanovená v příloze I pro vydávání osobních identifikačních údajů a elektronických potvrzení atributů k jednotkám peněženky.“;

4) článek 5 se mění takto:

   a) odstavce 1 a 2 se nahrazují tímto:

      „1. Poskytovatelé peněženek zajistí, aby řešení peněženky podporovala protokoly a rozhraní pro předkládání atributů stranám spoléhajícím se na peněženku, a to na dálku a případně v blízkosti, v souladu s technickými specifikacemi uvedenými v příloze II.

      2. Poskytovatelé peněženek zajistí, aby jednotky peněženky na žádost uživatelů odpovídaly na úspěšně autentizované žádosti s ověřenou platností od stran spoléhajících se na peněženku uvedené v článku 3 v souladu s technickými specifikacemi uvedenými v příloze II.“;

   b) odstavec 5 se zrušuje;

5) článek 8 se nahrazuje tímto:

   „Článek 8

   Vstup v platnost

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

   Ustanovení čl. 3 bodu 4 se použije ode dne 11. srpna 2028.

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

6) příloha se zrušuje;

7) znění uvedené v příloze XI tohoto nařízení se doplňuje jako příloha I;

8) znění uvedené v příloze XII tohoto nařízení se doplňuje jako příloha II.

Článek 5

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 15. července 2026.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA I

„PŘÍLOHA

Technické specifikace pro osobní identifikační údaje podle čl. 3 odst. 3

1) Oddíl 1: Soubor osobních identifikačních údajů fyzické osoby

Tabulka 1

Povinné osobní identifikační údaje fyzické osoby pro výběrové zpřístupňování

Identifikátor údajů	Definice
`family_name`	Aktuální příjmení uživatele, k němuž se vztahují osobní identifikační údaje.
`given_name`	Aktuální jméno (jména), případně včetně druhého jména (dalších jmen), uživatele, k němuž se vztahují osobní identifikační údaje.
`birth_date`	Den, měsíc a rok narození uživatele, k němuž se vztahují osobní identifikační údaje.
`birth_place`	Země jako kód země alpha-2 dle normy ISO 3166-1 nebo stát, provincie, okres či místní oblast nebo obec, město nebo vesnice, kde se uživatel, k němuž se vztahují osobní identifikační údaje, narodil.
`nationality`	Jeden nebo více kódů země alpha-2 dle normy ISO 3166-1, které představují státní příslušnost uživatele, k němuž se vztahují osobní identifikační údaje.
`Portrait`	V příslušných případech zobrazení obličeje uživatele (kromě případů, kdy se uživatel výslovně rozhodne jej nepoužívat), k němuž se vztahují osobní identifikační údaje, splňující požadavky na kvalitu pro plný frontální typ obrazu, jak je stanoveno v normě ISO/IEC 39794-5 nebo pro zpětnou kompatibilitu v bodech 8.2, 8.3 a 8.4 normy ISO/IEC 19794-5, které se poskytuje jako kódovaná obrazová data bez záhlaví nebo bloků, jak je stanoveno v bodě 5 normy ISO/IEC 19794-5, s výjimkou samotných obrazových dat (JPEG), platí od 11. srpna 2028.

— Členské státy mohou stanovit, že uživatel má možnost odmítnout vložení portrétu do osobních identifikačních údajů.

— Členské státy zajistí, aby se výběrové zpřístupňování vztahovalo na každý identifikátor údajů, včetně portrétu.

— Pokud není známo datum narození fyzické osoby, zvolí členské státy vhodné hodnoty, které splňují specifikace stanovené v oddílech 4.1 nebo 4.2 (podle potřeby) této přílohy.

— Není-li známa státní příslušnost fyzické osoby, použijí členské státy hodnotu „QU“.

— Pokud fyzická osoba nemá státní příslušnost, použijí členské státy hodnotu „QS“.

— Pokud se uživatel rozhodne odmítnout zahrnutí portrétu, členské státy nastaví hodnotu jako prázdnou.

Tabulka 2

Nepovinné osobní identifikační údaje fyzické osoby pro výběrové zpřístupňování

Identifikátor údajů	Definice
resident_address	Úplná adresa místa, kde uživatel, k němuž se vztahují osobní identifikační údaje, v současné době bydlí nebo kde ho lze kontaktovat (název ulice, číslo popisné, město atd.).
resident_country	Země, ve které uživatel, k němuž se vztahují osobní identifikační údaje, v současné době bydlí, jako kód země alpha-2 dle normy ISO 3166-1.
resident_state	Stát, provincie, okres nebo místní oblast, kde uživatel, k němuž se vztahují osobní identifikační údaje, v současné době bydlí.
resident_city	Obec, město nebo vesnice, kde uživatel, k němuž se vztahují osobní identifikační údaje, v současné době bydlí.
resident_postal_code	Poštovní směrovací číslo místa, kde uživatel, k němuž se vztahují osobní identifikační údaje, v současné době bydlí.
resident_street	Název ulice, kde uživatel, k němuž se vztahují osobní identifikační údaje, v současné době bydlí, včetně čísla domu a případného afixu nebo sufixu.
personal_administrative_-number	Hodnota přiřazená uživateli, k němuž se vztahují osobní identifikační údaje, která je v rámci všech osobních administrativních čísel vydaných poskytovatelem osobních identifikačních údajů jedinečná. Pokud se členské státy rozhodnou tento atribut zahrnout, popíší ve svých systémech elektronické identifikace, v jejichž rámci jsou osobní identifikační údaje vydávány, zásady, které uplatňují na hodnoty tohoto atributu, včetně případných zvláštních podmínek pro zpracování této hodnoty.
family_name_birth	Příjmení uživatele, k němuž se vztahují osobní identifikační údaje, v době narození.
given_name_birth	Jméno (jména), včetně druhého jména (dalších jmen), uživatele, k němuž se vztahují osobní identifikační údaje, v době narození.
Sex	Zvolí se jedna z těchto hodnot: 0 = není známo; 1 = muž; 2 = žena; 3 = jiné; 4 = intersexuální osoba; 5 = genderově nonkonformní osoba; 6 = otevřené; 9 = není relevantní. Pro hodnoty 0, 1, 2 a 9 platí norma ISO/IEC 5218.
email_address	Adresa elektronické pošty uživatele, k němuž se vztahují osobní identifikační údaje [v souladu s RFC 5322 ([1])].

Identifikátor údajů	Definice
mobile_phone_number	Číslo mobilního telefonu uživatele, k němuž se vztahují osobní identifikační údaje, začínající symbolem „+“ jako mezinárodní předvolbou a kódem země, za nímž následují pouze čísla.

([1]) P. Resnick, Ed., „Internet Message Format“ (Formát internetových zpráv), RFC 5322, říjen 2008.

2) Oddíl 2: Soubor osobních identifikačních údajů právnické osoby

Tabulka 3

Povinné osobní identifikační údaje právnické osoby

Identifikátor údajů
současný oficiální název
jedinečný identifikátor vytvořený odesílajícím členským státem v souladu s technickými specifikacemi pro účely přeshraniční identifikace a pokud možno následně neměnný

— Pokud není identifikátor údajů pro danou osobu znám nebo jej nelze jinak vydat jako součást souboru osobních identifikačních údajů, použijí členské státy místo něj hodnotu atributu odpovídající dané situaci.

Tabulka 4

Nepovinné osobní identifikační údaje právnické osoby

Identifikátor údajů
současná adresa
identifikační číslo pro účely DPH
daňové registrační číslo
jedinečný evropský identifikační kód uvedený ve směrnici Evropského parlamentu a Rady (EU) 2017/1132 ([1])
identifikační kód právnické osoby (LEI) uvedený v prováděcím nařízení Komise (EU) 2022/1860 ([2])
registrační a identifikační číslo hospodářských subjektů (EORI) uvedené v prováděcím nařízení Komise (EU) č. 1352/2013 ([3])
číslo pro účely spotřebních daní stanovené v čl. 2 bodu 12 nařízení Rady (EU) č. 389/2012 ([4])

([1]) Směrnice Evropského parlamentu a Rady (EU) 2017/1132 ze dne 14. června 2017 o některých aspektech práva obchodních společností (Úř. věst. L 169, 30.6.2017, s. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/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/2013/1352/oj).

([3]) 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).

([4]) 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).

3) Oddíl 3: Soubor metadat o osobních identifikačních údajích

Tabulka 5

Metadata o osobních identifikačních údajích

Identifikátor údajů	Definice	Užití
`issuing_authority`	Název správního orgánu, který osobní identifikační údaje vydal, nebo kód země alpha-2 dle normy ISO 3166 týkající se příslušného členského státu, pokud neexistuje samostatný orgán oprávněný vydávat osobní identifikační údaje.	Povinné
`issuing_country`	Kód země alpha-2 dle ISO 3166-1 týkající se země nebo území poskytovatele osobních identifikačních údajů.	Povinné
`expiry_date`	Datum (a pokud možno čas), kdy vyprší administrativní platnost osobních identifikačních údajů.	Nepovinné
`document_number`	Číslo osobních identifikačních údajů přidělené poskytovatelem osobních identifikačních údajů.	Nepovinné
`issuing_jurisdiction`	Kód nižší územní jednotky země jurisdikce, která vydala osobní identifikační údaje, jak je uvedeno v ISO 3166-2:2020, bodě 8. První část kódu je stejná jako hodnota pro vydávající zemi.	Nepovinné
`issuance_date`	Datum a pokud možno čas, kdy začala administrativní platnost osobních identifikačních údajů.	Nepovinné

4) Oddíl 4: Kódování atributů osobních identifikačních údajů fyzické osoby

— Osobní identifikační údaje fyzické osoby se vydávají v souladu s normami stanovenými v příloze II prováděcího nařízení (EU) 2024/2979, body 5 (formát SD-JWT VC) a 6 (formát ISO/IEC-mdoc), které se vztahují na elektronická potvrzení atributů. Body 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3, 6.2.4 a 6.2.5 se nepoužijí.

— Kódování osobních identifikačních údajů fyzické osoby musí být v souladu s technickými specifikacemi uvedenými v oddílech 4.1 a 4.2 této přílohy.

4.1 Kódování osobních identifikačních údajů fyzické osoby ve formátu ISO/IEC-mdoc

— Typem potvrzení pro osobní identifikační údaje ve formátu ISO/IEC mdoc je „eu.europa.ec.eudi.pid.1“. Identifikátorem jmenného prostoru (namespace) pro atributy osobních identifikačních údajů uvedené v této příloze je „eu.europa.ec.eudi.pid.1“.

— Pokud osobní identifikační údaje zahrnují údaje, jejichž identifikátory nejsou uvedeny v této příloze, jsou tyto údaje definovány v rámci domácího jmenného prostoru osobních identifikačních údajů, který používá obecný formát eu.europa.ec.eudi.pid. [kód země alpha-2 dle normy ISO 3166-1 nebo kód regionu dle normy ISO 3166-2], za nímž následuje nepovinná tečka a číslo verze.

— Pokud se používá domácí jmenný prostor, zveřejní se jeho schéma, včetně všech identifikátorů údajů, jejich definic, přítomnosti a formátů kódování, v souladu s článkem 8 prováděcího nařízení Komise (EU) 2025/1569 ([1]).

— Osobní identifikační údaje a jejich metadata, jež jsou uvedeny v oddílech 1 a 3 této přílohy, jsou zahrnuty do prvků osobních identifikačních údajů ve smyslu specifikací formátu ISO/IEC mdoc.

— Člen deviceKey v rámci členu deviceKeyInfo instance typu MobileSecurityObject obsahuje veřejný klíč.

— Tento veřejný klíč odpovídá soukromému klíči, který je uložen v bezpečném kryptografickém prostředku peněženky („WSCD“) uživatele peněženky.

— Chráněná hlavička digitálního podpisu CB-AdES, kterým se podepisují osobní identifikační údaje ve formátu ISO/IEC-mdoc, obsahuje parametry hlavičky x5u a x5t, které jsou specifikovány v RFC 9360 ([2]).

— V parametru hlavičky x5t se používá hašovací (digest) algoritmus SHA-256.

— Požadavky na kódování osobních identifikačních údajů ve formátu ISO/IEC-mdoc jsou uvedeny v tabulce 6.

Tabulka 6

Požadavky na kódování osobních identifikačních údajů ve formátu ISO/IEC-mdoc

Identifikátor údajů	Identifikátor atributu	Formát kódování
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) Prováděcí nařízení Komise (EU) 2025/1569 ze dne 29. července 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o kvalifikovaná elektronická potvrzení atributů a elektronická potvrzení atributů poskytovaná subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem (Úř. věst. L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([2]) J. Schaad, „*CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates*“ (Podepisování a šifrování objektů CBOR (COSE): Parametry hlavičky pro přenos certifikátů X.509 a odkazování na ně) (https://datatracker.ietf.org/doc/rfc9360/).

Identifikátor údajů	Identifikátor atributu	Formát kódování
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate nebo full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate nebo full-date

— Zápis formátu kódování atributů uvedených v tabulce 6 používá typy reprezentace uvedené v RFC 8610 ([3]) s následujícími dodatečnými požadavky:

a) atribut tstr musí být kódován pomocí UTF-8;

b) atribut tstr podporuje celý rozsah Unicode;

c) atribut tstr má maximální délku 150 znaků;

d) datum se kóduje podle specifikace v RFC 8943 ([4]);

e) plné datum se interpretuje jako #6.1004(tstr), kde tag 1004 je specifikován v RFC 8943;

f) atribut tdate musí obsahovat řetězec data a času podle specifikace v RFC 3339 ([5]);

g) atribut full-date musí obsahovat řetězec full-date podle specifikace v RFC 3339 v souladu s RFC 8943;

h) reprezentace data v atributech, pokud není uvedeno jinak:

— nepoužívá zlomky sekund,

— nepoužívá místní posun od UTC a časový posun uvedený v RFC 3339 je nastaven na „Z“;

i) celé číslo s hlavními typy 0 a 1 musí být co nejmenší, jak je uvedeno v RFC 8949 ([6]), oddíl 4.2;

j) atribut place_of_birth musí obsahovat alespoň jeden z následujících párů klíč-hodnota: „country“, „region“ nebo „locality“;

k) vyjádření délky v atributech bstr, tstr, poli nebo mapě musí být co nejkratší, jak je uvedeno v RFC 8949, oddíl 4.2;

([3]) C. Vigano a H. Birkholz, „*Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures*“ (Jazyk pro stručné definice dat (CDDL): Zápisová konvence pro vyjádření datových struktur CBOR (Stručné binární reprezentace objektů) a JSON), RFC 8610, červen 2019.

([4]) C. Vigano a H. Birkholz, „*Concise Binary Object Representation (CBOR) Tags for Date*“ (Štítky pro stručnou reprezentaci binárních objektů (CBOR) pro datum), RFC 8943, listopad 2020.

([5]) G. Klyne a C. Newman, „*Date and Time on the Internet: Timestamps*“ (Datum a čas na internetu: časová razítka), RFC 3339, červenec 2002.

([6]) C. Bormann a P. Hoffman, „*Concise Binary Object Representation (CBOR)*“ (Stručná binární objektová reprezentace (CBOR)), RFC 8949, prosinec 2020.

l) atribut nationality (státní příslušnost) se kóduje jako pole kódů zemí alpha-2 podle specifikace v ISO 3166-1. Pokud se používá zápis CDDL podle specifikace v RFC 8610, musí být kódování tohoto atributu následující:

— nationalities = [+ CountryCode],

— CountryCode = tstr; kód země alpha-2 podle normy ISO 3166-1,

— pokud má uživatel peněženky, k němuž se vztahují osobní identifikační údaje, více státních příslušností a poskytovatel osobních identifikačních údajů těchto více státních příslušností potvrdí, může poskytovatel osobních identifikačních údajů zahrnout do osobních identifikačních údajů všechny státní příslušnosti,

— atribut place_of_birth se kóduje jako typ place_of_birth. Pokud se používá zápis CDDL podle specifikace v RFC 8610, musí být kódování tohoto atributu následující:

place_of_birth =

{

? „country“: tstr; jeden kód země alpha-2 podle specifikace v ISO 3166-1

? „region“: tstr; název státu, provincie, okresu nebo místní oblasti

? „locality“: tstr; název obce, města nebo vesnice

}

4.2 Požadavky na kódování osobních identifikačních údajů ve formátu SD-JWT VC

— Osobní identifikační údaje a jejich metadata, jež jsou uvedeny v tomto oddíle, jsou zahrnuty do osobních identifikačních údajů jako tvrzení ve smyslu specifikací formátu SD-JWT VC.

— Všechna tvrzení ve zveřejněných osobních identifikačních údajích, na něž se odkazuje v předchozí odrážce, jsou selektivně zveřejnitelná jednotlivě, s výjimkou tvrzení, která jsou ve formátu SD-JWT VC definována jako neselektivně zveřejnitelná.

— Tabulka 7 specifikuje kódování názvů tvrzení, které jsou veřejnými názvy.

— Tabulka 8 specifikuje kódování názvů tvrzení, které jsou specifické pro osobní identifikační údaje.

— Řetězec JSON použitý v osobních identifikačních údajích kódovaných ve formátu SD-JWT VC musí být zakódován pomocí UTF-8 a musí podporovat celý rozsah Unicode, pokud není v tabulce 8 níže nebo v odkazech v ní výslovně uvedeno jinak.

— K vyjádření doby technické platnosti osobních identifikačních údajů ve formátu SD-JWT VC se použijí tvrzení JWT nbf a exp definované v RFC 7519 ([7]).

([7]) J. Jones a další, *„JSON Web Token (JWT)“* (JSON webový token (JWT)), RFC 7519, květen 2015.

— Osobní identifikační údaje obsahují tvrzení cnf podle definice v RFC 7800 ([8]), což je veřejný klíč vygenerovaný ze soukromého klíče uloženého ve WSCD jednotky peněženky uživatele peněženky.

— Chráněná hlavička digitálního podpisu, kterým se podepisují osobní identifikační údaje ve formátu SD-JWT VC, obsahuje parametry hlavičky x5u a x5t#S256 uvedené v RFC 7515 ([9]).

Tabulka 7

Požadavky na kódování osobních identifikačních údajů ve formátu SD-JWT VC s použitím veřejných názvů

Identifikátor údajů	Identifikátor atributu	Formát kódování
`family_name`	`family_name`	řetězec
`given_name`	`given_name`	řetězec
`birth_date`	`birthdate`	řetězec, ISO 8601-1, formát RRRR-MM-DD
`birth_place`	`place_of_birth`	struktura JSON
`nationality`	`nationalities`	pole řetězců
`resident_address`	`address.formatted`	řetězec
`resident_country`	`address.country`	řetězec
`resident_state`	`address.region`	řetězec
`resident_city`	`address.locality`	řetězec
`resident_postal_code`	`address.postal_code`	řetězec
`resident_street`	`address.street_address`	řetězec
`family_name_birth`	`birth_family_name`	řetězec
`given_name_birth`	`birth_given_name`	řetězec
`email_address`	`email`	řetězec
`mobile_phone_number`	`phone_number`	řetězec
`portrait`	`picture`	řetězec; datová adresa URL obsahující portrét ve formátu JPEG kódovaný pomocí base64

([8]) M. Jones a další, *„Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)"* (Sémantika klíče prokazování vlastnictví pro webové tokeny JSON (JWT)), RFC 7800, duben 2016.

([9]) M. Jones a další, *„JSON Web Signature (JWS)"* (Webový podpis JSON (JWS)), RFC 7515, květen 2015.

Tabulka 8

Požadavky na kódování osobních identifikačních údajů ve formátu SD-JWT VC s použitím soukromých názvů

Identifikátor údajů	Identifikátor atributu	Formát kódování
`expiry_date`	`date_of_expiry`	řetězec, ISO 8601-1, formát RRRR-MM-DD
`issuance_date`	`date_of_issuance`	řetězec, ISO 8601-1, formát RRRR-MM-DD
`personal_administrative_number`	`personal_administrative_number`	řetězec
`sex`	`sex`	číslo
`issuing_authority`	`issuing_authority`	řetězec
`issuing_country`	`issuing_country`	řetězec
`document_number`	`document_number`	řetězec
`issuing_jurisdiction`	`issuing_jurisdiction`	řetězec

— Základním typem osobních identifikačních údajů je „urn:eudi:pid:1“, který je součástí tvrzení vct. Všechny osobní identifikační údaje používají typy ve jmenném prostoru „urn:eudi:pid:“.

— Pokud osobní identifikační údaje obsahují atributy, které nejsou specifikovány v této příloze, musí být tyto atributy definovány v rámci domácího typu.

— V případě použití domácího typu je jeho schéma, včetně všech identifikátorů údajů, jejich definic, užití a formátů kódování, definováno schématem zveřejněným v souladu s článkem 8 prováděcího nařízení (EU) 2025/1569.

5) Oddíl 5: Podrobnosti o důvěryhodné infrastruktuře

Seznam poskytovatelů osobních identifikačních údajů, který Komise zpřístupňuje v souladu s prováděcím nařízením (EU) 2024/2980, umožňuje autentizaci osobních identifikačních údajů.“

PŘÍLOHA II

„PŘÍLOHA Ia

Kryptografické mechanismy podle článku 5a

Evropská skupina pro certifikaci kybernetické bezpečnosti, podskupina pro kryptografii: „Dohodnuté kryptografické mechanismy“ zveřejněné Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) ([1]).“

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

PŘÍLOHA III

„PŘÍLOHA Ib

Technické specifikace pro potvrzení jednotky peněženky podle čl. 6 odst. 2a

1) Potvrzení jednotky peněženky obsahuje jedno nebo více potvrzení instance peněženky a jedno nebo více potvrzení klíče.

2) Potvrzení instance peněženky a potvrzení klíče musí splňovat následující požadavky:

a) Požadavky na formát

— FR-WIA-1: Potvrzením instance peněženky je JSON Web Token (JWT), jak je uvedeno v RFC 7519 ([1]), podepsaný nebo opatřený pečetí poskytovatelem peněženky pomocí kompaktního podpisu JAdES baseline B.

— FR-WIA-1.1: Potvrzení instance peněženky je potvrzení peněženky, jak je uvedeno v dodatku E k dokumentu OpenID for Verifiable Credential Issuance v1.0 ([2]) („OID4VCI“), a rozšířené, jak je uvedeno níže v C-WIA-1 a C-WIA-2.

— FR-KA-1: Potvrzením klíče musí být JWT podle specifikace v RFC 7519, podepsané nebo opatřené pečetí poskytovatelem peněženky pomocí kompaktního podpisu JAdES baseline B.

— FR_KA_1.1: Potvrzení klíče je potvrzení klíče, jak je uvedeno v dodatku D k OID4VCI, rozšířené podle specifikace v C_KA-1 a C_KA-2 níže.

b) Požadavky na přenos

— TR-WIA-1: Jednotka peněženky používá při vydávání osobních identifikačních údajů, kvalifikovaných nebo nekvalifikovaných elektronických potvrzení atributů nebo elektronických potvrzení atributů poskytovaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem potvrzení instance peněženky.

— TR-WIA-2: Poskytovatel peněženky ověří integritu instance peněženky a podepíše nebo opatří pečetí potvrzení instance peněženky.

— TR-WIA-2.1: Pokud poskytovatel peněženky vydá potvrzení instance peněženky, rozdíl mezi časem, kdy poskytovatel peněženky ověřil integritu instance peněženky, a časem, který uvede v parametru hlavičky „exp“ vydaného potvrzení instance peněženky, musí být kratší než 24 hodin.

— TR-WIA-2.2: Poskytovatel peněženky zajistí, aby jednotka peněženky obsahovala potvrzení instance peněženky potřebná pro vydání osobních identifikačních údajů a elektronických potvrzení atributů.

— TR-WIA-3: Při vydávání jednotka peněženky zašle autorizačnímu serveru potvrzení instance peněženky v rámci zaslané žádosti o autorizaci a žádosti o token, jak je stanoveno v OID4VCI.

— TR-WIA-3.1: Jednotka peněženky zašle potvrzení instance peněženky spolu s důkazem o vlastnictví („PoP“), jak je uvedeno v dodatku E k OID4VCI.

— TR-WIA-3.2: Jednotka peněženky zašle stejné potvrzení instance peněženky pouze jednomu autorizačnímu serveru.

([1]) RFC 7519: *JSON Web Token (JWT)*, květen 2015.
([2]) *OpenID for Verifiable Credential Issuance v1.0*, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: Pokud poskytovatel peněženky používá možnost „per-issuer reuse“ uvedenou níže v R_WIA_1, může jednotka peněženky odeslat potvrzení instance peněženky stejnému autorizačnímu serveru vícekrát.

— TR-WIA-3.2.2: Pokud poskytovatel peněženky možnost „per-issuer reuse“ nepoužívá, musí jednotka peněženky použít potvrzení instance peněženky při nejvýše jednom procesu vydávání.

— TR-WIA-4: Pokud autorizační server obdrží potvrzení instance peněženky, ověří podpis potvrzení instance peněženky pomocí veřejného klíče v podpisovém certifikátu obsaženém v parametru „x5c“ v hlavičce JOSE potvrzení instance peněženky.

— TR-WIA-4.1: Autorizační server rovněž ověří, zda lze tento podpisový certifikát ověřit pomocí zdroje důvěry (trust anchor) na seznamu poskytovatelů peněženek uvedeném v článku 5 prováděcího nařízení (EU) 2024/2980, případně s využitím zprostředkujících certifikátů obsažených v parametru x5c.

— TR-WIA-4.2: Autorizační server ověří, zda nevypršela platnost potvrzení instance peněženky.

— TR-WIA-4.3: Autorizační server ověří podpis PoP pomocí veřejného klíče uvedeného v tvrzení „cnf“.

— TR_KA-1: Jednotka peněženky používá potvrzení klíče při vydávání osobních identifikačních údajů a při vydávání kvalifikovaných nebo nekvalifikovaných elektronických potvrzení atributů nebo elektronických potvrzení atributů poskytovaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem, jež jsou vázána na zařízení.

— TR_KA-1.1: Jednotka peněženky nepoužívá potvrzení klíče při vydávání kvalifikovaných nebo nekvalifikovaných elektronických potvrzení atributů nebo elektronických potvrzení atributů poskytovaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem, jež nejsou vázána na zařízení.

— TR_KA-2: Poskytovatel peněženky poskytne jednotce peněženky různá potvrzení klíčů pro WSCD jednotky peněženky a pro každý z jeho úložišť klíčů.

— TR_KA-2.1: Poskytovatel peněženky podepíše nebo opatří pečetí potvrzení klíče poté, co ověřil, že klíče uvedené v potvrzení klíče jsou uloženy v WSCD jednotky peněženky nebo úložišti klíčů popsaném v potvrzení klíče.

— TR_KA-2.2: Potvrzení klíče obsahuje alespoň jeden ověřený veřejný klíč. Počet klíčů v potvrzení klíče zaslaném vydavateli pověření by neměl překročit maximální velikost dávky, kterou tento vydavatel pověření uvedl ve svých metadatech vydavatele pověření; viz ETSI TS 119 472-3 ([3]), parametr „credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size“.

— TR_KA-2.3: Poskytovatel peněženky zahrne veřejný klíč (odpovídající soukromému klíči uloženému v WSCD nebo úložišti klíčů jednotky peněženky) do nejvýše jednoho potvrzení klíče.

— TR_KA-2.4: Jednotka peněženky použije potvrzení klíče při nejvýše jednom procesu vydávání nebo opětovného vydávání pověření.

— TR_KA-2.5: Poskytovatel peněženky zajistí, aby jednotka peněženky měla k dispozici potvrzení klíče potřebná pro vydávání osobních identifikačních údajů a elektronických potvrzení atributů vázaných na zařízení.

([3]) ETSI, „*Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 3: JAdES levels and baseline profiles*“ (Elektronické podpisy a infrastruktury (ESI); Digitální podpisy JAdES; Část 3: Úrovně a základní profily JAdES), ETSI TS 119 472-3, V1.1.1, březen 2026.

— TR_KA-3: Pokud je to při vydávání nutné, jednotka peněženky zahrne potvrzení klíče v rámci žádosti o vydání pověření vydavateli pověření v poli „proofs“, jak je uvedeno v OID4VCI, v ověření typu „jwt“, nebo typu „attestation“.

— TR_KA_3.1: Pokud jednotka peněženky obsahuje potvrzení klíče v prvku „jwt“, podepíše nebo opatří pečetí potvrzení klíče pomocí soukromého klíče odpovídajícího veřejnému klíči na indexu 0 pole „attested_keys“ v rámci objektu „key_attestation“.

— TR_KA-4: Pokud vydavatel pověření vydává pověření vázaná na zařízení, uvede v parametru „proof_types_supported“ v metadatech vydavatele pověření, jak je uvedeno v oddíle 12.2.4 OID4VCI, že podporuje typ ověření „jwt“ i typ ověření „attestation“ pro potvrzení klíče, která obsahují objekt „key_attestations_required“.

— TR_KA-4.1: Pokud vydavatel pověření vydává pověření, která nejsou vázána na zařízení, vynechá parametry „proof_types_supported“ a „cryptographic_binding_methods_supported“ v metadatech vydavatele pověření.

— TR_KA-5: Pokud vydavatel pověření obdrží potvrzení klíče v typu ověření „jwt“ nebo „attestation“, ověří podpis potvrzení klíče pomocí veřejného klíče v podpisovém certifikátu obsaženém v parametru „x5c“ v hlavičce potvrzení klíče JOSE a ověří tento podpisový certifikát pomocí zdroje důvěry (trust anchor) na seznamu poskytovatelů peněženek uvedeném v článku 5 prováděcího nařízení (EU) 2024/2980, případně s využitím zprostředkujících certifikátů obsažených v parametru „x5c“.

— TR_KA-6: Pokud vydavatel pověření obdrží potvrzení klíče v typu ověření „jwt“, ověří podpis prvku „jwt“ podle klíče na indexu 0 pole „attested_keys“ v rámci objektu „key_attestation“ obsaženého v prvku „jwt“.

— TR_KA-6.1: Vydavatel pověření ověří, že pole „nonce“ prvku „jwt“ obsahuje platný c_nonce z nonce_endpoint, jak je uvedeno v OID4VCI.

— TR_KA-7: Pokud vydavatel pověření obdrží potvrzení klíče v typu ověření „attestation“, ověří, že objekt „key_attestation“ obsahuje platný c_nonce z nonce_endpoint.

— TR_KA-8: Poskytovatel osobních identifikačních údajů zajistí, aby osobní identifikační údaje byly vázány na veřejný klíč, který pochází z potvrzení klíče uvádějícího WSCD.

c) Požadavky na obsah

— C_WIA-1: Potvrzení instance peněženky obsahuje následující údaje:

— tvrzení „wallet_name“ uvedené v dodatku E k OID4VCI, přičemž jeho hodnotou je identifikátor řešení peněženky, který lze nalézt na seznamu poskytovatelů peněženek uvedeném v článku 5 prováděcího nařízení (EU) 2024/2980,

— tvrzení „wallet_version“ ([4]), což je řetězec, jehož hodnotou je verze řešení peněženky,

— tvrzení „wallet_solution_certification_information“, což je objekt JSON obsahující informace o subjektu posuzování shody, který certifikoval řešení peněženky, případně číslo certifikace a další relevantní údaje týkající se certifikace,

([4]) Toto tvrzení je definováno v tomto prováděcím nařízen Komise, protože není součástí specifikace OID4VCI.

— tvrzení „client_status“ obsahující dvě podpole:

— „status“: odkaz na seznam stavů podle dodatku E k OID4VCI, který představuje stav zneplatnění instance peněženky. Podrobnosti viz oddíl e) níže,

— „exp“: NumericDate, jak je uvedeno v RFC 7519, definující dobu, po kterou bude poskytovatel peněženky udržovat stav zneplatnění na indexu seznamu stavů, na který odkazuje podpole „status“,

— tvrzení „exp“ uvedené v dodatku E k OID4VCI.

— POZNÁMKA: Tvrzení „client_status.status“ v potvrzení instance peněženky představuje stav zneplatnění instance peněženky, nikoli stav zneplatnění samotného potvrzení. Jak je popsáno v R_WIA-1 níže, poskytovatel peněženky se může rozhodnout, že každé potvrzení instance peněženky se bude vztahovat na určitý autorizační server na základě skutečnosti, že všechna potvrzení zaslaná tomuto serveru obsahují stejnou hodnotu indexu v položce „client_status.status“.

— POZNÁMKA: Hodnotu „idx“ v tvrzení „status“ lze použít jako (párově) jedinečný identifikátor instance peněženky a jednotky peněženky.

— C_WIA-2: Potvrzení instance peněženky by mělo obsahovat také tvrzení „wallet_link“ uvedené v dodatku E k OID4VCI a hodnota tohoto tvrzení musí být URI, kde lze získat další informace o řešení peněženky.

— C_WIA-3: Autorizační server neinterpretuje parametr „exp“ v nejvyšší úrovni potvrzení instance peněženky jako konec doby udržování zneplatnění instance peněženky.

— POZNÁMKA: Parametr „exp“ v nejvyšší úrovni potvrzení instance peněženky označuje, kdy vyprší platnost samotného potvrzení.

— C_KA-1: Potvrzení klíče obsahuje:

— tvrzení „key_storage“ a „user_authentication“ uvedená v dodatku D k OID4VCI,

— atributy „key_storage“ a „user_authentication“ mají hodnotu „iso_18045_high“, kde potvrzení klíče uvádí WSCD,

— tvrzení „certification“ uvedené v dodatku D k OID4VCI, obsahující URL, kde lze získat informace o certifikaci, které dosáhl WSCD nebo úložiště klíčů, například Common Criteria nebo GlobalPlatform, hodnocené požadavky, jako je příslušný profil ochrany, a úroveň hodnocení,

— z těchto informací musí být možné určit, zda je úložiště klíčů WSCD,

— tvrzení „key_storage_status“ obsahující dvě podpole:

— „status“: odkaz na seznam stavů, jak je uvedeno v dodatku D.1 k OID4VCI. Hodnota představuje buď stav zneplatnění WSCD, nebo typu úložiště klíčů použitého k uložení ověřovaných klíčů, nebo – pod možností indexu per-key-attestation – stav zneplatnění WSCD nebo úložiště klíčů jednotlivé jednotky peněženky. Viz R_KA_1 níže, kde jsou uvedeny dostupné možnosti přiřazení indexů,

— „exp“: NumericDate, jak je uvedeno v RFC 7519, definující dobu, po kterou bude poskytovatel peněženky udržovat stav zneplatnění na indexu seznamu stavů, na který odkazuje podpole „status“,

— tvrzení „exp“ uvedené v dodatku D k OID4VCI.

— POZNÁMKA k hodnotě „idx“ v tvrzení „key_storage_status.status“ v potvrzení klíče: Pokud poskytovatel peněženky používá možnost „type-shared index“ (viz R_KA_1 níže), sdílejí všechna potvrzení klíčů pro stejný typ WSCD nebo úložiště klíčů stejný index seznamu stavů. Hodnota „idx“ proto není pro každou jednotku peněženky jedinečná. Naopak v případě, že poskytovatel peněženky používá možnost „per-key-attestation index“, je hodnota „idx“ jedinečná pro jednotku peněženky (nebo párově jedinečná pro vydavatele pověření). Ve všech případech však vydavatel pověření nepoužije hodnotu „idx“ v potvrzení klíče jako identifikátor jednotky peněženky, ale místo toho použije hodnotu „idx“ v potvrzení instance peněženky.

— C_KA-2: Pokud je potvrzení klíče zasíláno v typu ověření „attestation“, obsahuje také platný c_nonce, jak je uvedeno v dodatku F.3 k OID4VCI.

— C_KA-3: Vydavatel pověření neinterpretuje parametr „exp“ v nejvyšší úrovni potvrzení klíče jako konec doby udržování zneplatnění WSCD nebo úložiště klíčů.

— POZNÁMKA: Parametr „exp“ v nejvyšší úrovni potvrzení klíče označuje, kdy vyprší platnost samotného potvrzení klíče.

d) Požadavky na životní cyklus

— Tato příloha specifikuje následující parametry metadat vydavatele pověření:

— „preferred_client_status_period“: OPTIONAL. Celé číslo udávající preferovanou zbývající dobu udržování stavu potvrzení instance peněženky, kterou má jednotka peněženky předložit během vydávání, v sekundách. Zbývající doba udržování stavu je definována jako hodnota „client_status.exp“ v potvrzení minus čas přijetí potvrzení.

— „preferred_key_storage_status_period“: OPTIONAL. Celé číslo udávající preferovanou zbývající dobu udržování stavu potvrzení klíče, kterou má jednotka peněženky předložit během vydávání, v sekundách. Zbývající doba udržování stavu je definována jako hodnota „key_storage_status.exp“ v potvrzení minus čas přijetí potvrzení.

— LC_WIA-1: Autorizační server může sdělit své preference pro zbývající dobu udržování stavu v potvrzeních instance peněženky tím, že uvede parametr metadat „preferred_client_status_period“ v koncovém bodu metadat vydavatele pověření, jak je uvedeno v oddíle 12.2.2 dokumentu OID4VCI.

— LC_WIA-1.1: Toto pole se umístí na nejvyšší úroveň metadat vydavatele pověření.

— LC_WIA_2: Autorizační server neinterpretuje parametr „exp“ v nejvyšší úrovni potvrzení instance peněženky jako konec doby udržování zneplatnění instance peněženky.

— LC_WIA_3: Pokud poskytovatel peněženky podepíše nebo opatří pečetí potvrzení instance peněženky, udržuje stav zneplatnění příslušné instance peněženky až do doby, než uplyne lhůta „wallet_instance_-status.exp“ uvedená v tomto potvrzení instance peněženky.

— LC_KA-1: Pokud je třeba potvrzení klíče, může vydavatel pověření sdělit své preference pro zbývající dobu udržování stavu v potvrzeních klíče tím, že do koncového bodu metadat vydavatele pověření zahrne parametr metadat „preferred_key_storage_status_period“ uvedený výše, jak je uvedeno v oddíle 12.2.2 dokumentu OID4VCI.

— LC_KA-1.1: Toto pole se umístí do objektu „key_attestations_required“, jak je uvedeno v oddíle 12.2.4 dokumentu OID4VCI.

— LC_KA-2: Poskytovatel peněženky si zvolí dobu technické platnosti potvrzení klíče, která vydává.

— LC_KA-3: Pokud poskytovatel peněženky podepíše nebo opatří pečetí potvrzení klíče, udržuje stav zneplatnění příslušného WSCD nebo úložiště klíčů až do doby, než uplyne lhůta „key_storage_-status.exp“ uvedená v tomto potvrzení klíče.

— LC_GEN-1: Poskytovatel peněženky zajistí, aby jednotka peněženky mohla vždy předložit potvrzení jednotky peněženky a potvrzení klíče, jejichž lhůty „client_status.exp“ a „key_storage_status.exp“ (v tomto pořadí) jsou v době předložení autorizačnímu serveru nebo vydavateli pověření platné minimálně ještě 31 dní.

— *POZNÁMKA*: To zaručuje, že se poskytovatelé osobních identifikačních údajů mohou spolehnout na řetězení zneplatnění, aniž by byli nuceni vydávat krátkodobé osobní identifikační údaje.

— LC_GEN-2: Poskytovatel peněženky zajistí, aby jednotka peněženky při vydávání získala metadata vydavatele pověření.

  — LC_GEN_2.1: Pokud je v těchto metadatech zahrnuto pole „preferred_key_storage_status_period“, pak jednotka peněženky odešle potvrzení klíče s hodnotou („key_storage_status.exp“ – aktuální čas) – „preferred_key_storage_status_period“, která je co nejmenší, ale ne záporná. Pokud jednotka peněženky nemá k dispozici žádné takové potvrzení klíče, získá od poskytovatele peněženky nové potvrzení klíče, které splňuje požadavek „key_storage_status.exp“ – aktuální čas ≥ „preferred_key_-storage_status_period“.

  — LC_GEN_2.2: Pokud je v těchto metadatech zahrnuto pole „preferred_client_status_period“, pak jednotka peněženky odešle potvrzení instance peněženky s hodnotou („client_status.exp“ – aktuální čas) – „preferred_client_status_period“, která je co nejmenší, ale ne záporná. Pokud jednotka peněženky nemá k dispozici žádné takové potvrzení instance peněženky, vyžádá si od poskytovatele peněženky nové potvrzení instance peněženky, které splňuje požadavek „client_status.exp“ – aktuální čas ≥ „preferred_client_status_period“.

— LC_GEN-3: Doba technické platnosti osobních identifikačních údajů končí předtím, než uplyne lhůta „client_status.exp“ potvrzení instance peněženky a lhůta „key_storage_status.exp“ potvrzení klíče zaslaného poskytovateli osobních identifikačních údajů v procesu vydávání.

— LC_GEN-4: Poskytovatel osobních identifikačních údajů s dobou technické platnosti delší než 24 hodin kontroluje stav zneplatnění potvrzení instance peněženky i potvrzení klíče obdrženého při vydávání nejméně jednou za 24 hodin během doby technické platnosti osobních identifikačních údajů. Pokud je některé z nich zneplatněno, poskytovatel zneplatní osobní identifikační údaje.

e) Požadavky na zneplatnění

— R_GEN-1: Poskytovatel peněženky používá seznamy stavů tokenů (specifikované v IETF Token Status List) jako mechanismus zneplatnění pro potvrzení klíče i potvrzení instance peněženky, jak je uvedeno v dodatcích D a E k OID4VCI.

— POZNÁMKA: Pro zlepšení škálovatelnosti seznamů stavů může poskytovatel peněženky použít následující optimalizace:

  — Rozdělit seznam stavů na více částí, pokud mají poskytovatelé peněženek velký počet uživatelů a vydaných potvrzení. Existuje mnoho strategií rozdělení na části, například na základě pevně stanovené velikosti nebo podle časového období. Strategie rozdělení na části je ponechána na uvážení poskytovatele peněženky. V úvahu lze vzít mimo jiné velikost seznamu stavů pro stahování a soukromí uživatele.

  — Mít více seznamů stavů.

  — Zkomprimovat seznam stavů za účelem zmenšení jeho velikosti.

— R_WIA-1: Poskytovatel peněženky může přiřadit stejnou hodnotu k tvrzení „idx“ v tvrzení „client_status.status“ ve všech potvrzeních instance peněženky, která daná jednotka peněženky předkládá stejnému autorizačnímu serveru. Tomu se říká možnost „per-issuer reuse“. Pokud je tato možnost použita:

  — R_WIA-1.1: Jednotka peněženky udržuje stav, pokud jde o hodnotu indexu, kterou použila pro každý autorizační server, se kterým dříve komunikovala, a při opětovné interakci se stejným autorizačním serverem si vyžádá potvrzení instance peněženky obsahující stejnou hodnotu indexu.

  — R_WIA-1.2: Pokud poskytovatel peněženky obdrží žádost o potvrzení instance peněženky obsahující určitou hodnotu indexu, ověří před vydáním nového potvrzení instance peněženky s touto hodnotou indexu, že žádající jednotka peněženky tuto hodnotu indexu již dříve obdržela.

  — R_WIA-1.3: Jednotka peněženky nesmí opakovaně používat stejnou hodnotu indexu pro interakce s různými autorizačními servery.

— POZNÁMKA: Pokud bude použita možnost „per-issuer reuse“, bude poskytovatel peněženky schopen určit, s kolika autorizačními servery jednotka peněženky komunikovala a jak často s každým z nich komunikuje.

— R_WIA-2: Poskytovatel peněženky ve svých zásadách ochrany osobních údajů zdokumentuje, zda používá možnost „per-issuer reuse“ pro zneplatnění instance peněženky.

— R_WIA-3: Pokud poskytovatel peněženky nepoužívá možnost „per-issuer reuse“, přiřadí každému vydávanému potvrzení instance peněženky novou, nepropojitelnou hodnotu indexu.

— R_WIA-4: Pokud je nutné jednotku peněženky zneplatnit, poskytovatel peněženky zneplatní hodnoty indexů v tvrzení „client_status.status“ ve všech potvrzeních instance peněženky souvisejících s touto jednotkou peněženky.

— R_WIA-5: Poskytovatel peněženky zohlední při určování velikosti seznamů stavů potvrzení instance peněženky míru nasazení a základní architekturu a zajistí, aby seznamy byly dostatečně velké, aby se zabránilo korelaci a chránilo soukromí uživatelů. Pokud je to možné, musí se seznam stavů vztahovat alespoň k 10 000 potvrzení.

— R_KA_1: Poskytovatel peněženky si zvolí jednu z následujících možností přiřazení indexu pro tvrzení „key_storage_status.status“ v potvrzení klíče:

  — Možnost 1, tzv. „type-shared index“, při níž všechna potvrzení klíčů potvrzující klíče uložené ve stejném typu WSCD nebo úložiště klíčů obsahují stejnou hodnotu indexu v „key_storage_status.status“.

  — Možnost 2, tzv. „per-key-attestion index“, při níž potvrzení klíče potvrzující klíče uložené v individuálním WSCD nebo úložišti klíčů obsahuje (párově) jedinečnou hodnotu indexu v „key_storage_status.status“.

— POZNÁMKA: Pokud poskytovatel peněženky použije možnost 1, jediná akce zneplatnění zneplatní všechna potvrzení klíčů dotčeného typu ve všech jednotkách peněženky. Kromě toho, jelikož všechna potvrzení klíčů pro stejný typ WSCD nebo úložiště klíčů sdílejí jeden index seznamu stavů, počet položek v seznamu stavů potvrzení klíčů odráží počet typů WSCD nebo úložišť klíčů podporovaných poskytovatelem peněženky, nikoli počet nasazených jednotek peněženky. Úvahy o ochraně soukromí, které odůvodňují minimální velikost seznamu stavů pro seznamy stavů instance peněženky, se proto nevztahují na seznamy stavů potvrzení klíče v rámci možnosti 1, pokud existuje dostatečný počet jednotek peněženky používajících stejný typ WSCD nebo úložiště klíčů.

— POZNÁMKA: Pokud poskytovatel peněženky použije možnost 2, představuje každý index stav zneplatnění konkrétního WSCD nebo úložiště klíčů potvrzeného v tomto potvrzení klíče.

— POZNÁMKA: Pokud poskytovatel peněženky použije možnost 2, lze na žádost uživatele rovněž zneplatnit konkrétní WSCD nebo úložiště klíčů.

— R_KA-2: Pokud poskytovatel peněženky použije možnost 2, může volitelně použít i možnost „per-issuer reuse“ popsanou v R_WIA-1. Pokud poskytovatel peněženky použije tuto možnost, použijí se obdobně požadavky R_WIA-1 – R_WIA-3.

— R_KA-3: Pokud poskytovatel peněženky použije možnost 2, zohlední při určování velikosti seznamů stavů potvrzení klíčů míru nasazení a základní architekturu a zajistí, aby seznamy byly dostatečně velké, aby se zabránilo korelaci a chránilo soukromí uživatelů. Pokud je to možné, musí se seznam stavů vztahovat alespoň k 10 000 potvrzení klíče.

— R_KA-4: Pokud poskytovatel peněženky použije možnost 1 (type-shared index), zneplatní položku „key_storage_status.status“ pouze v případě, že typ WSCD nebo úložiště klíčů vykazuje bezpečnostní zranitelnost.

f) Požadavky na podpisové algoritmy

— SA-1: Pro podepisování potvrzení instance peněženky, potvrzení klíče, souvisejících důkazů o vlastnictví a seznamů stavů tokenů se použije jeden z následujících algoritmů:

— ES256 (ECDSA s SHA-256 a P-256)

— ES384 (ECDSA s SHA-384 a P-384)

— ES512 (ECDSA s SHA-512 a P-521)

— SA-2: Poskytovatel peněženky si zvolí, který z algoritmů uvedených v SA-1 použije.

— SA-3: Autorizační server nebo vydavatel pověření (jak je uvedeno v OID4VCI) podporuje všechny algoritmy uvedené v SA-1.“

PŘÍLOHA IV

„PŘÍLOHA II

Seznam norem podle článku 8

Platí technické specifikace uvedené v bodech 2 až 6 ETSI TS 119 472-1 V1.2.1 (2026-02). Použijí se s těmito úpravami:

1) 2.1 Normative references

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures“.

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): „Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers“.

— [25] IETF Token Status List (TSL), draft-ietf-oauth-status-list-20: „Token Status List“, 20. dubna 2026.

2) 4.2.11.1 General requirements

— EAA-4.2.11.1-06: Pokud se prvek stavu používá pro osobní identifikační údaje, kvalifikovaná elektronická potvrzení atributů nebo elektronická potvrzení atributů poskytovaná subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem, uvádí pouze, zda je potvrzení zneplatněno, nebo zneplatněno není, a nepodporuje žádné jiné hodnoty stavu, např. pozastavení.

— EAA-4.2.11.1-06.1: Pokud je potvrzení zneplatněno, je zneplatněno trvale.

3) 4.2.13 EAA short-lived

— EAA-4.2.13-03: Pokud jsou vydávána krátkodobá elektronická potvrzení atributů s dobou platnosti 24 hodin nebo kratší, zneplatnění se nevyžaduje.

4) 4.6.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA)

— PuB-EAA-4.6.2-03: neplatné.

— Pub-EAA-4.6.2-04: neplatné.

— PuB-EAA-4.6.3-03: Digitální podpis PuB-EAA by měl obsahovat kvalifikovaný certifikát podporující digitální podpis PuB-EAA.

— PuB-EAA-4.6.3-04: Kvalifikovaný certifikát podporující digitální podpis PuB-EAA musí splňovat požadavky bodu 8 normy ETSI TS 119 412-6 v1.1.1 a musí obsahovat QcType qcStatement podle definice v normě ETSI EN 319 412-5 v2.5.1 s hodnotou id-etsi-qct-eidaspsbeaa definovanou takto:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } -- Certifikát uvedený v čl. 45f odst. 1 písm. b) podporující kvalifikovaný elektronický podpis nebo kvalifikovanou elektronickou pečeť subjektu veřejného sektoru uvedeného v čl. 3 bodu 46 nařízení (EU) č. 910/2014.

5) 5.2.10.1 General requirements

— EAA-5.2.10.1-04: neplatné.

— EAA-5.2.10.1-05: neplatné.

— EAA-5.2.10.1-06: Člen stav může obsahovat člen status_list, jak je uvedeno v odstavci 6.2 dokumentu IETF draft-ietf-oauth-status-list-20 [25].

— EAA-5.2.10.1-07: neplatné.

— EAA-5.2.10.1-08: neplatné.

— EAA-5.2.10.1-09: neplatné.

— EAA-5.2.10.1-10: neplatné.

— EAA-5.2.10.1-11: neplatné.

— EAA-5.2.10.1-12: neplatné.

6) 6.2.10.1 General requirements

— EAA-6.2.10.1-01: Pokud elektronické potvrzení atributů vyhovující normě ISO/IEC mdoc používá mechanismus seznamu stavů potvrzení podle EAA-6.2.10.1-02.2 nebo mechanismus seznamu zneplatnění potvrzení podle EAA-6.2.10.1-02.3, obsahuje jeho mobilní bezpečnostní objekt (MSO) strukturu stavu podle EAA-6.2.10.1-17, která obsahuje informace o zneplatnění MSO.

— EAA-6.2.10.1-01.1: Při implementaci mechanismu seznamu identifikátorů obsahuje prvek stavu prvek identifier_list, jak je stanoveno v EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: Při implementaci mechanismu seznamu stavů obsahuje prvek stavu prvek status_list, jak je stanoveno v EAA-6.2.10.1-13.

— *POZNÁMKA:*

  — Struktura stavu obsahuje odkaz na seznam zneplatnění MSO.

  — Seznam zneplatnění MSO je struktura COSE_Sign1, která označuje, zda je konkrétní MSO zneplatněn, či nikoli.

  — Struktura stavu obsahuje všechny informace potřebné k tomu, aby strana spoléhající se na peněženku mohla určit, zda je seznam zneplatnění MSO pravý.

— EAA-6.2.10.1-02: Poskytovatel osobních identifikačních údajů, poskytovatel kvalifikovaných elektronických potvrzení atributů nebo poskytovatel elektronických potvrzení atributů poskytovaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem použije pro zneplatnění osobních identifikačních údajů, kvalifikovaných elektronických potvrzení atributů nebo elektronických potvrzení atributů poskytovaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem jednu z těchto metod:

— EAA-6.2.10.1-02.1: Pokud vydávají krátkodobá elektronická potvrzení atributů s dobou platnosti 24 hodin nebo kratší, není zneplatnění nutné.

— EAA-6.2.10.1-02.2: K zakódování informací o zneplatnění jako seznamu stavů se použije mechanismus seznamu stavů potvrzení.

— EAA-6.2.10.1-02.2.1: Mechanismus seznamu stavů zneplatňuje MSO na základě toho, zda je bit na pozici definované vydavatelem v MSO v seznamu stavů nastaven na hodnotu true.

— EAA-6.2.10.1-02.2.2: Mechanismus seznamu stavů je specifikován ve specifikaci seznamu stavů tokenů (draft-ietf-oauth-status-list-20).

— EAA-6.2.10.1-02.3: K zakódování informací o zneplatnění jako seznamu identifikátorů se použije mechanismus seznamu zneplatnění potvrzení.

— EAA-6.2.10.1-02.3.1: Mechanismus seznamu identifikátorů zneplatňuje MSO na základě toho, zda se identifikátor definovaný vydavatelem v MSO nachází v seznamu identifikátorů.

— EAA-6.2.10.1-02.3.2: EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 a EAA-6.2.10.1-11 specifikují mechanismus seznamu identifikátorů na základě požadavků ze specifikace seznamu stavů tokenů, včetně společné charakteristiky mezi mechanismem seznamu stavů a seznamu identifikátorů.

— EAA-6.2.10.1-03: Pokud se prvek stavu používá pro osobní identifikační údaje, kvalifikovaná elektronická potvrzení atributů nebo elektronická potvrzení atributů poskytovaná subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem, použije se výhradně stav „revoked“ („zneplatněno“).

— EAA-6.2.10.1-03.1: Pro seznam stavů to znamená, že se použijí pouze hodnoty „valid“ a „invalid“, jak je uvedeno ve specifikaci seznamu stavů tokenů.

— EAA-6.2.10.1-03.2: Do seznamu identifikátorů se zařadí pouze zneplatněné MSO, a nikoli dočasně pozastavené MSO.

— EAA-6.2.10.1-04: Pokud je MSO zneplatněn, je zneplatněn trvale.

— EAA-6.2.10.1-05: Ověření seznamu zneplatnění MSO je pro stranu spoléhající se na peněženku nepovinné, přičemž v příslušných případech ověření splňuje požadavky na ověření uvedené ve specifikaci seznamu stavů tokenů a specifikaci struktury stavů podle EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: Pokud musí být strana spoléhající se na peněženku schopna ověřit stav zneplatnění osobních identifikačních údajů nebo elektronických potvrzení atributů, podporuje mechanismus seznamu stavů potvrzení i mechanismus seznamu zneplatnění potvrzení podle EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: Prvky identifier_list a status_list v MSO mohou obsahovat prvek certifikátu.

— EAA-6.2.10.1-06.1: Pokud je prvek certifikátu přítomen, obsahuje certifikát obsahující veřejný klíč, který podepsal nebo opatřil pečetí certifikát nejvyšší úrovně v prvku x5chain ve struktuře seznamu zneplatnění MSO.

— EAA-6.2.10.1-06.1.1: Instance strany spoléhající se na peněženku použije tento certifikát jako zdroj důvěry (trust anchor) pro ověření prvku x5chain ve struktuře seznamu zneplatnění MSO.

— EAA-6.2.10.1-06.2: Pokud prvek certifikátu přítomen není, je certifikát nejvyšší úrovně v prvku x5chain ve struktuře seznamu zneplatnění MSO podepsán nebo opatřen pečetí certifikátem použitým k podepsání certifikátu v prvku x5chain v MSO.

— EAA-6.2.10.1-06.2.1: Instance strany spoléhající se na peněženku použije tento certifikát jako zdroj důvěry (trust anchor) pro ověření prvku x5chain ve struktuře seznamu zneplatnění MSO.

— EAA-6.2.10.1-07: Seznam zneplatnění MSO musí být implementován v souladu se specifikací seznamu stavů tokenů jako token seznamu stavů ve formátu CWT.

— EAA-6.2.10.1-08: Pro seznam zneplatnění MSO pro mechanismus seznamu identifikátorů a seznamu stavů platí následující požadavky:

  — je uvedeno tvrzení exp,

  — může být uvedeno tvrzení ttl,

  — může být uvedeno tvrzení aggregation_uri v rámci tvrzení IdentifierList nebo StatusList a poskytovatel osobních identifikačních údajů, poskytovatel kvalifikovaných elektronických potvrzení atributů nebo

poskytovatel elektronických potvrzení atributů poskytovaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem může použít tvrzení aggregation_uri k označení podpory agregačního mechanismu, jak je uvedeno ve specifikaci seznamu stavů tokenů,

— CWT je objekt COSE_Sign1, který používá jeden z následujících podpisových algoritmů pro výpočet podpisu:

a) „ES256“ (ECDSA s křivkou NIST P-256 a SHA-256);

b) „ES384“ (ECDSA s křivkou NIST P-384 a SHA-384);

c) „ES512“ (ECDSA s křivkou NIST P-521 a SHA-512);

d) „ESB256“ (ECDSA s křivkou brainpoolP256r1 a SHA-256);

e) „ESB384“ (ECDSA s křivkou brainpoolP384r1 a SHA-384);

f) „ESB512“ (ECDSA s křivkou brainpoolP512r1 a SHA-512),

— CWT obsahuje x5chain v chráněné hlavičce, která obsahuje certifikát nebo řetězec certifikátů pro ověření podpisu seznamu zneplatnění MSO,

— rozšířené použití klíče identifikátoru objektu uvedené ve specifikaci seznamu stavů tokenů lze použít pro seznam stavů a podpisový certifikát seznamu identifikátorů a instance strany spoléhající se na peněženku mohou podporovat rozšířené použití klíče identifikátorů objektu uvedené ve specifikaci seznamu stavů tokenů a pro identifikátor objektu; poskytovatel kvalifikovaných elektronických potvrzení atributů nebo poskytovatel elektronických potvrzení atributů poskytovaných subjektem veřejného sektoru nebo jeho jménem neučiní při použití rozšířeného použití klíče OID uvedeného ve specifikaci seznamu stavů tokenů pole rozšířeného použití klíče kritickým.

— EAA-6.2.10.1-09: Odchylně od požadavků specifikace seznamu stavů tokenů platí pro mechanismus seznamu identifikátorů následující požadavky:

— hodnota tvrzení o typu je „application/identifierlist+cwt“,

— tvrzení StatusList nesmí být uvedeno v souboru tvrzení CWT,

— struktura IdentifierList definovaná v EAA-6.2.10.1-11 je uvedena jako tvrzení v tvrzeních CWT pomocí klíče 65530.

— EAA-6.2.10.1-10: Struktura IdentifierList je strukturou CBOR s následujícím CDDL:

```
IdentifierList = {

    „identifiers“: { * Identifier => IdentifierInfo },

    ? „aggregation_uri“: Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: Pokud je identifikátor přítomen v IdentifierList, je MSO, který obsahuje identifikátor v prvku stavu, zneplatněn.

— EAA-6.2.10.1-10.2: Tvrzení Aggregation_uri je specifikováno v oddíle 9.2 specifikace seznamu stavů tokenů.

— EAA-6.2.10.1-10.3: Typ obsahu seznamu identifikátorů je „application/identifierlist+cwt“ podle požadavků uvedených v oddíle 8.2 specifikace seznamu stavů tokenů.

— EAA-6.2.10.1-11: Na prvek identifier_list v MSO se vztahují následující požadavky (viz EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: Prvek identifier_list je strukturou CBOR s následujícím CDDL:

```
IdentifierListInfo = {

    „id“: Identifier,

    „uri“: URI,

    ? „certificate“: Certificate

    * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: Aby se zabránilo použití identifikátoru jako korelace napříč prezentacemi, musí být jedinečný pro každý MSO.

— EAA-6.2.10.1-12: Na seznam stavů se vztahují následující požadavky:

  — EAA-6.2.10.1-12.1: Prvek bits ve struktuře StatusList se nastaví na 1.

— EAA-6.2.10.1-13: Na prvek status_list v MSO se vztahují následující požadavky (viz EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: Prvek status_list se řídí požadavky na strukturu StatusListInfo uvedenými ve specifikaci seznamu stavů tokenů a je doplněn nepovinný prvek certifikátu definovaný v EAA-6.2.10.1-06.

  — EAA-6.2.10.1-13.2: Aby se zabránilo tomu, že index stavu bude korelovat napříč prezentacemi, musí být kombinace indexu stavu a URI jedinečná pro každý MSO.

— EAA-6.2.10.1-14: Poskytovatel peněženky použije pro zneplatnění potvrzení instance peněženky a pro zneplatnění potvrzení klíče druhou (EAA-6.2.10.1-02.2) nebo třetí (EAA-6.2.10.1-02.3) z metod uvedených v EAA-6.2.10.1-02.

— EAA-6.2.10.1-15: Poskytovatel peněženky implementuje v řešení peněženky mechanismy zneplatnění potvrzení uvedené v EAA-6.2.10.1-02.

— EAA-6.2.10.1-16: Poskytovatel osobních identifikačních údajů a poskytovatel elektronických potvrzení atributů podporuje mechanismus seznamu stavů potvrzení i mechanismus seznamu zneplatnění potvrzení uvedený v EAA-6.2.10.1-02 pro ověření stavu zneplatnění potvrzení instance peněženky a potvrzení klíče.

— EAA-6.2.10.1-17: Struktura stavů v MSO je strukturou CBOR s následujícím CDDL:

Status = {

? „identifier_list“: IdentifierListInfo,

? „status_list“: StatusListInfo,

* tstr => RFU

}“

PŘÍLOHA V

„PŘÍLOHA III

Technické specifikace podle článku 10

— Technické specifikace:

  — bod 4.2.5 normy ETSI TS 119 472-3 V1.1.1 (2026-03).“

PŘÍLOHA VI

Příloha IV se mění takto:

1) bod 1 se nahrazuje tímto:

„1. Povinný formát podpisu nebo pečeti:

a) PAdES (zaručený elektronický podpis PDF), jak je specifikováno v normě ETSI EN 319 142-1 V1.2.1 (2024-01); Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures.“;

2) bod 3 se nahrazuje tímto:

„3. Aplikační programovací rozhraní:
body 6.4.3, A.6, A.7 a A.8 normy ETSI TS 119 432 v1.3.1 (2026-03).“

PŘÍLOHA VII

„PŘÍLOHA VI

Barevná značka důvěry EU pro peněženku digitální identity



“

PŘÍLOHA VIII

„PŘÍLOHA VII

Černobílá značka důvěry EU pro peněženku digitální identity



“

PŘÍLOHA IX

„PŘÍLOHA VIII

Údaje týkající se značky důvěry EU pro peněženku digitální identity

Údaje	Popis	Kódování	Stav
TrustMarkResourceURL	URL grafických zdrojů a zdrojů uživatelských informací značky důvěry EU pro peněženku digitální identity v uživatelském rozhraní peněženky.	URL	Povinné
ListOfCertifiedWalletsURL	URL veřejného seznamu certifikovaných řešení peněženky v EU, jak je stanoveno v prováděcím nařízení Komise (EU) 2025/849 ([1]).	URL	Povinné
ListOfCertifiedWalletsQRCode	QR kód obsahující informace o ListOfCertifiedWalletsURL.	ISO-8859-1 Byte mode QR code	Nepovinné
WalletSolutionInfoPageURL	URL na informační stránku certifikovaného řešení peněženky v seznamu stránky certifikovaných řešení peněženky z ListOfCertifiedWalletsURL URL doplněné o „?“ a identifikátor řešení peněženky WalletSolutionID.	URL	Povinné
WalletSolutionInfoPageQRCode	QR kód obsahující informace o WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	Nepovinné
WalletVerifierToolURL*	URL směřující na koncový bod nástroje pro ověření peněženky */.well-known/ openid-credential-issuer* používaný pro vyhledání metadat poskytovatele potvrzení.	URL	Nepovinné

([1]) Prováděcí nařízení Komise (EU) 2025/849 ze dne 6. května 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o předkládání informací pro seznam certifikovaných evropských peněženek digitální identity Komisi a skupině pro spolupráci (Úř. věst. L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).“

PŘÍLOHA X

Příloha II prováděcího nařízení (EU) 2024/2980 se mění takto:

1) v příloze II oddíle 1 bodě 1 se písmeno i) nahrazuje tímto:

„i) jeden nebo více certifikátů v souladu s normou ETSI EN 319 412-2 V2.4.1 (2025-06) nebo normou ETSI EN 319 412-3 V1.3.1 (2023-09), které lze použít k ověření podpisu nebo pečeti vytvořených registrátorem na údajích v registru a u nichž certifikované identifikační údaje obsahují jméno registrátora a případně registrační číslo registrátora, jak je stanoveno v písmenu c) a d).“;

2) v příloze II oddíle 2 bodě 1 se písmeno h) nahrazuje tímto:

„h) jeden nebo více certifikátů v souladu s normou ETSI EN 319 412-2 V2.4.1 (2025-06) nebo normou ETSI EN 319 412-3 V1.3.1 (2023-09), které lze použít k autentizaci a ověření platnosti potvrzení jednotky peněženky, jež poskytovatel peněženky vydal, a u nichž certifikované identifikační údaje obsahují jméno a v příslušných případech registrační číslo poskytovatele peněženky, jak je uvedeno v písmenu a) a b);“

3) v příloze II oddíle 3 bodě 1 se písmeno h) nahrazuje tímto:

„h) jeden nebo více certifikátů v souladu s normou ETSI EN 319 412-2 V2.4.1 (2025-06) nebo normou ETSI EN 319 412-3 V1.3.1 (2023-09), které lze použít k ověření podpisu nebo pečeti vytvořených poskytovatelem osobních identifikačních údajů na jím poskytovaných osobních identifikačních údajích a u nichž certifikované identifikační údaje obsahují jméno a v příslušných případech registrační číslo poskytovatele osobních identifikačních údajů, jak je uvedeno v písmenu a) a b).“;

4) v příloze II oddíle 4 bodě 1 se písmeno g) nahrazuje tímto:

„g) jeden nebo více certifikátů v souladu s normou ETSI EN 319 412-2 V2.4.1 (2025-06) nebo normou ETSI EN 319 412-3 V1.3.1 (2023-09), které lze použít k ověření podpisu nebo pečeti vytvořených poskytovatelem přístupových certifikátů stran spoléhajících se na peněženku na přístupovém certifikátu, který poskytuje stranám spoléhajícím se na peněženku, s případnými informacemi potřebnými pro rozlišení přístupových certifikátů stran spoléhajících se na peněženku od jiných certifikátů.“;

5) v příloze II se doplňuje nový oddíl 5, který zní:

„5. Oznámení informací o poskytovatelích registračních certifikátů stran spoléhajících se na peněženku

1. Členské státy poskytnou Komisi tyto informace o poskytovatelích registračních certifikátů stran spoléhajících se na peněženku:

a) jméno poskytovatele registračních certifikátů stran spoléhajících se na peněženku;

b) v příslušných případech registrační číslo poskytovatele registračních certifikátů stran spoléhajících se na peněženku;

c) členský stát, ve kterém je poskytovatel registračních certifikátů stran spoléhajících se na peněženku usazen;

d) kontaktní e-mail a kontaktní telefonní číslo poskytovatele registračních certifikátů stran spoléhajících se na peněženku pro záležitosti týkající se registračních certifikátů, které poskytuje stranám spoléhajícím se na peněženku;

e) v příslušných případech adresu URL internetové stránky poskytovatele registračních certifikátů stran spoléhajících se na peněženku, která obsahuje další informace o poskytovateli a registračních certifikátech, které poskytuje stranám spoléhajícím se na peněženku;

f) adresu URL internetové stránky, která obsahuje zásady a obchodní podmínky, které se vztahují na poskytování a používání registračních certifikátů, které poskytuje stranám spoléhajícím se na peněženku;

g) jeden nebo více certifikátů v souladu s normou ETSI EN 319 412-2 V2.4.1 (2025-06) nebo normou ETSI EN 319 412-3 V1.3.1 (2023-09), které lze použít k ověření podpisu nebo pečeti vytvořených poskytovatelem registračních certifikátů stran spoléhajících se na peněženku na registračních certifikátech, které poskytuje stranám spoléhajícím se na peněženku, v příslušných případech s informacemi potřebnými pro rozlišení registračních certifikátů stran spoléhajících se na peněženku od jiných certifikátů.

2. Informace uvedené v bodě 1 se poskytují pro každého poskytovatele registračních certifikátů stran spoléhajících se na peněženku.“

PŘÍLOHA XI

„PŘÍLOHA I

Protokoly a rozhraní podle článku 4

Technická specifikace ETSI TS 119 472-3 V1.1.1 (2026-03) se použije s následujícími úpravami:

1) 4.1 General requirements

— GEN-REQ-4.1-05: neplatné

— POZNÁMKA: neplatné

2) 4.2.3 Provision of registration certificates of PID/EAA Provider to EUDI Wallet

— 1ISS-MDATA-REG_CERT-4.2.3-04: Jeden z prvků parametru pole issuer_info obsahuje registrační certifikát poskytovatele PID/EAA.

— ISS-MDATA-REG_CERT-4.2.3-07: neplatné

— ISS-MDATA-REG_CERT-4.2.3-08: neplatné

— ISS-MDATA-REG_CERT-4.2.3-09: neplatné

— ISS-MDATA-REG_CERT-4.2.3-10: neplatné

— ISS-MDATA-REG_CERT-4.2.3-11: neplatné

— ISS-MDATA-REG_CERT-4.2.3-12: neplatné

— ISS-MDATA-REG_CERT-4.2.3-13: neplatné

3) 4.2.4.2 ARF pre-defined PID/EAA reuse policy

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Pokud má člen id hodnotu „arf_annex_ii“ a pole mapované na štítek „details“ obsahuje hodnotu „once_only“ nebo hodnotu „per-relying-party“, pak objekt JSON, který obsahuje toto pole mapované na štítek „details“, obsahuje také číslo JSON mapované na štítek „reissue_trigger_unused“;

4) příloha A se nepoužije.“

PŘÍLOHA XII

„PŘÍLOHA II

Technické specifikace podle článku 5

Platí technická specifikace uvedená v příloze C normy ISO/IEC 18013-7:2025.

Technické specifikace v bodech 4.1, 4.2, 5 a 6 normy ETSI TS 119 472-2 V1.2.1 (2026-03) se použijí s následujícími úpravami, včetně vložení nového bodu 4.3:

1) 1 Scope

— Tento dokument specifikuje dva profily protokolů, které umožňují, aby spoléhající se strany (dále jen„RP“) požádaly evropskou peněženku digitální identity o EAAP nebo osobní identifikační údaje (dále jen „PID“) a aby evropská peněženka digitální identity zaslala požadované EAAP/PID těmto RP. Každý z profilů podporuje dva přenosové mechanismy, a to: zprostředkovaný API a nezprostředkovaný API, jak je uvedeno níže:

a) Profil je založen na:

— ISO/IEC 18013-5 [10] pouze pro přenosový mechanismus nezprostředkovaný API a

— příloze C normy ISO/IEC 18013-7 [16] pro přenosový mechanismus zprostředkovaný API.

Tento profil se nazývá profil ISO/IEC-mdoc a je definován v bodě 5 tohoto dokumentu.

b) Profil je založen na:

OpenID4VC-HAIP [11] pro přenosové mechanismy zprostředkované API i nezprostředkované API, a to takto:

— oddíly 5, 5.1, 5.3, 7 a 8 dokumentu [11] pro přenos prostřednictvím přesměrování nebo přenosový mechanismus nezprostředkovaný API a

— oddíly 5, 5.2, 5.3, 7 a 8 dokumentu [11] pro přenosový mechanismus zprostředkovaný API.

Tento profil se nazývá profil OpenID4VC-HAIP a je definován v bodě 6 tohoto dokumentu.

2) 2.1 Normative references

— [15] ISO 639: „Language code“.

— [16] ISO/IEC 18013-7:2025 „Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions“.

3) 4.1 EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: neplatné.

4) 4.2 EAAP implementation based on ISO/IEC-mdoc

— EAAP-ISO/IEC-mdoc-01: neplatné.

— Note2: neplatné.

— EAAP-ISO/IEC-mdoc-02: neplatné.

5) 4.3 EAAP implementation with mediating API

— EAAP-API-GEN-01: Evropská peněženka digitální identity musí podporovat zprostředkující rozhraní API, které podporuje oba protokoly definované v bodě 5.2 [11] a v příloze C [16].

— POZNÁMKA: Pokud zařízení, na kterém je evropská peněženka digitální identity nainstalována, nepodporuje oba protokoly, nelze tento požadavek splnit a vzniká nesoulad z důvodu, že příslušné operační systémy a prohlížeče nemají implementovány nezbytné funkce interoperability.

— EAAP-API-GEN-02: Evropská peněženka digitální identity musí podporovat zprostředkující rozhraní API alespoň pro typy PID a EAA zapsané v katalogu schémat definovaném v prováděcím nařízení (EU) 2025/1569 a alespoň pro všechny formáty definované v příloze II prováděcího nařízení (EU) 2024/2979.

— POZNÁMKA 1: Pokud příslušný operační systém, prohlížeč, zprostředkující rozhraní API nebo jakákoli jiná technická vrstva mimo kontrolu evropské peněženky digitální identity omezuje, filtruje, předem vybírá nebo jinak omezuje formáty pověření a typy PID a EAA registrované v katalogu schémat, nelze tento požadavek splnit. Pokud takové omezení brání evropské peněžence digitální identity podporovat registrovaný typ nebo formát pověření, je výsledný nesoulad způsoben tím, že tyto příslušné operační systémy, prohlížeče, zprostředkující rozhraní API nebo jiná příslušná technická vrstva neposkytuje nezbytné funkce interoperability.

6) 4.4 Wallet-relying party validation and overasking checks

— WRP-VALIDATION-01: Evropská peněženka digitální identity ověří platnost registračního certifikátu strany spoléhající se na peněženku, který obdržela v žádosti, dříve než předloží uživateli peněženky ke schválení jakýkoli požadovaný PID nebo elektronické potvrzení atributů.

— WRP-VALIDATION-02: Pokud se ověření platnosti registračního certifikátu strany spoléhající se na peněženku nezdaří, včetně případů, kdy platnost certifikátu vypršela, certifikát byl zneplatněn, nebyl vydán platným důvěryhodným poskytovatelem registračních certifikátů stran spoléhajících se na peněženku, byl chybně vytvořen nebo jej nelze kryptograficky ověřit, evropská peněženka digitální identity uživatele peněženky upozorní, že strana spoléhající se na peněženku nemohla být ověřena, a uvede, že platnost nebyla na žádost úspěšně ověřena. Uživatel peněženky musí žádost spoléhající se strany výslovně schválit. Tichý souhlas nebo předem zaškrtnutá políčka k udělení výslovného souhlasu nepostačují.

— WRP-VALIDATION-03: Poskytovatel peněženky na základě své analýzy rizik a bezpečnostní politiky určí, zda a za jakých podmínek může uživatel peněženky konkrétní neúspěšné kontroly ověření platnosti obejít.

— WRP-OVERASKING-01: Evropská peněženka digitální identity porovná potvrzení a atributy požadované stranou spoléhající se na peněženku s registrovanými potvrzeními a atributy v registračním certifikátu strany spoléhající se na peněženku.

— WRP-OVERASKING-02: Pokud strana spoléhající se na peněženku požaduje PID nebo elektronická potvrzení atributů nebo tvrzení, které nejsou zahrnuty v registračním certifikátu strany spoléhající se na peněženku, evropská peněženka digitální identity uživatele peněženky před jakýmkoli zpřístupněním jasně upozorní. V upozornění musí být uvedeno, že strana spoléhající se na peněženku žádá o více informací, než kolik jich registrovala. Uživatel peněženky musí žádost spoléhající se strany výslovně schválit. Tichý souhlas nebo předem zaškrtnutá políčka k udělení výslovného souhlasu nepostačují.

— WRP-OVERASKING-03: Poskytovatel peněženky na základě své analýzy rizik, bezpečnostní politiky a platných právních předpisů rozhodne, zda uživatel peněženky může i přes toto upozornění pokračovat, zda může být zpřístupněn pouze dílčí soubor požadovaných údajů, na které se vztahuje registrační certifikát, nebo zda bude žádost zamítnuta.

7) 5.1 Introduction

— Bod 5 a jeho podbody definují profil protokolu, který umožňuje, aby RP požádaly evropskou peněženku digitální identity o EAAP nebo PID a aby evropská peněženka digitální identity zaslala těmto RP požadované EAAP/PID buď pomocí přenosového mechanismu nezprostředkovaného API, který je založen na normě ISO/IEC 18013-5 [10], nebo pomocí přenosového mechanismu zprostředkovaného API, který je založen na příloze C normy ISO/IEC 18013-7 [16], pro přenos datových struktur definovaných v normě ISO/IEC 18013-5 [10], které jsou vhodně zapouzdřeny.

— Zbytek bodu 5 je uspořádán takto:

  — bod 5.2 definuje požadavky na podporu profilu a přenosových mechanismů ze strany RP a evropské peněženky digitální identity,

  — bod 5.3 upřesňuje požadavky, které jsou specifické pro přenosový mechanismus nezprostředkovaný API,

  — bod 5.4 a jeho podbody upřesňují požadavky, které jsou specifické pro přenosový mechanismus zprostředkovaný API.

8) 5.2 Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: Jednotky peněženky, poskytovatelé PID, poskytovatelé potvrzení, poskytovatelé peněženky a spoléhající se strany nepodporují vyhledávání na serveru, jak je uvedeno v normě ISO/IEC 18013-5 [10], pro vyžádání a předložení atributů PID nebo potvrzení.

— ISO/IEC 18013-SUPPORT-02: Evropská peněženka digitální identity splňuje požadavky definované v bodech 5.3 a 5.4 tohoto dokumentu.

— ISO/IEC 18013-SUPPORT-04: Spoléhající se strana by měla implementovat profil definovaný v bodě 5.4 tohoto dokumentu.

9) 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: Žádosti zařízení zaslané evropské peněžence digitální identity obsahují pár klíč-hodnota „requestInfo“, jak je uvedeno v bodě 8.3.2.1.2.1 dokumentu [10]. Hodnota tohoto páru musí být typu RequestInfo.

— ISO/IEC 18013-5-REQ-05: Typ RequestInfo odpovídá definici CDDL uvedené níže.

RequestInfo = {

„euWrprc“: bstr; obsahuje registrační certifikát (viz požadavky níže)

}

— ISO/IEC 18013-5-REQ-06: Uvedený člen requestInfo obsahuje člen s označením „euWrprc“.

— ISO/IEC 18013-5-REQ-07: Hodnotou „euWrprc“ je registrační certifikát kódovaný pomocí CBOR.

— ISO/IEC 18013-5-REQ-08: neplatné.

— POZNÁMKA 3: neplatné.

— ISO/IEC 18013-5-REQ-09: neplatné.

— ISO/IEC 18013-5-REQ-10: neplatné.

— ISO/IEC 18013-5-REQ-11: neplatné.

10) 5.3.3 ISO/IEC-mdoc EAAP Response profile

— Tento bod definuje požadavky na typ zprávy DeviceResponse, který je společný pro oba typy přenosových mechanismů (zprostředkovaný API a nezprostředkovaný API).

— POZNÁMKA 1: Pokud je použit mechanismus nezprostředkovaný API, který je založen na normě ISO/IEC 18013-5 [10], je odpověď EAAP přesně instancí DeviceResponse, jak je uvedeno v tomto bodě. Pokud je použit mechanismus zprostředkovaný API, který je založen na příloze C normy ISO/IEC 18013-7 [16], je instance DeviceRequest zapouzdřena, jak je uvedeno v příloze C normy [16].

— ISO/IEC 18013-5-RESP-02: Poskytovatel osobních identifikačních údajů a elektronických potvrzení atributů nesmí do mapy KeyAuthorizations v mobilním bezpečnostním objektu jím vydávaných osobních identifikačních údajů a elektronických potvrzení atributů zahrnout žádné datové prvky, s výjimkou datových prvků, které poskytuje strana spoléhající se na peněženku v transakčních údajích v žádosti mdoc, které má jednotka peněženky podepsat nebo opatřit pečetí pomocí soukromého klíče osobních identifikačních údajů nebo elektronických potvrzení atributů.

— POZNÁMKA 2: V důsledku toho nemohou jednotky peněženky předkládat stranám spoléhajícím se na peněženku žádné datové prvky podepsané zařízením, s výjimkou podepisování dat, která poskytla strana spoléhající se na peněženku, například v případech použití pro bezpečné ověřování uživatele.

— POZNÁMKA 3: Norma ISO/IEC 18013-5:2021 nespecifikuje, jakým způsobem mohou strany spoléhající se na peněženku zahrnout transakční údaje do žádosti mdoc. Zahrnutí transakčních údajů do žádosti mdoc se provádí s doplněním technických specifikací.

— ISO/IEC 18013-5-RESP-03: Poskytovatelé osobních identifikačních údajů neumožní, aby soukromý klíč osobních identifikačních údajů podepisoval datové prvky, které poskytuje strana spoléhající se na peněženku v transakčních údajích v žádosti mdoc.

11) 5.4 Requirements for API mediated mechanism

5.4.1 ISO/IEC 18013-7-related requirements

Tento bod definuje požadavky na přenosový mechanismus zprostředkovaný API související s požadavky definovanými v příloze C dokumentu [16].

— ISO/IEC 18013-7-API-01: Profil podporující prezentace zprostředkované API splňuje požadavky přílohy C normy ISO/IEC 18013-7 [16], jak je dále uvedeno v bodech 5.3 a 5.4 tohoto dokumentu.

— ISO/IEC 18013-7-API-02: Použijí se všechny povinné požadavky definované v příloze C dokumentu [16], jak je dále uvedeno v bodech 5.3 a 5.4 tohoto dokumentu.

— ISO/IEC 18013-7-API-03: Všechny volitelné požadavky definované v příloze C dokumentu [16] zůstávají volitelné, pokud není v tomto dokumentu uvedeno jinak.

12) 5.4.2 Additional requirements

— Tento bod specifikuje další požadavky na přenosový mechanismus zprostředkovaný API.

— ISO/IEC 18013-ADD-API-01: Evropská peněženka digitální identity automaticky informuje zprostředkující rozhraní API, které funguje v souladu s přílohou C dokumentu [16], o přítomnosti všech uložených typů elektronických potvrzení atributů, ale nezveřejňuje atributy a jejich hodnoty v těchto elektronických potvrzeních atributů.

  — POZNÁMKA 1: Omezení týkající se hodnoty atributu platí i v případě, že by takové zveřejnění zlepšilo služby poskytované operačním systémem evropské peněženky digitální identity, například výběr potvrzení v kontextu zprostředkujícího rozhraní API.

— Existují úvahy týkající se operačních systémů a prohlížečů, které jsou mimo kontrolu implementátorů a které lze zohlednit, jak je uvedeno v následujících poznámkách 2 až 4:

  — POZNÁMKA 2: Požadavek na prezentaci od spoléhající se strany podporující přílohu C dokumentu [16] může být zpracován prohlížečem a/nebo operačním systémem pro vyhledávání dostupných EAA, pro prevenci podvodů zaměřených na uživatele nebo pro účely řešení problémů.

  — POZNÁMKA 3: Očekává se, že požadavek na prezentaci od spoléhající se strany podporující přílohu C dokumentu [16] bude zpracován prohlížečem a/nebo operačním systémem pro účely bezpečnosti uživatele.

— POZNÁMKA 4: Očekává se, že požadavek na prezentaci od spoléhající se strany podporující přílohu C dokumentu [16] nebude zpracován prohlížečem a/nebo operačním systémem pro účely analýzy trhu (včetně sekundárního účelu) nebo pro interní účely prohlížeče a/nebo operačního systému.

— ISO/IEC 18013-ADD-API-02: Pokud evropská peněženka digitální identity na žádost uživatele vymaže PID nebo EAA, jež byly dříve zpřístupněny zprostředkujícímu rozhraní API, které funguje v souladu s přílohou C dokumentu [16], sdělí zprostředkujícímu rozhraní API skutečnost, že tyto PID nebo EAA již neuchovává.

— ISO/IEC 18013-ADD-API-03: Pokud si uživatel odinstaluje evropskou peněženku digitální identity, sdělí peněženka zprostředkujícímu rozhraní API, které funguje v souladu s přílohou C dokumentu [16], skutečnost, že již neuchovává žádné dříve zveřejněné PID nebo EAA.

— ISO/IEC 18013-ADD-API-04: Evropská peněženka digitální identity poskytuje globální uživatelské nastavení, které znemožňuje zveřejnění uložených EAA prostřednictvím zprostředkujícího rozhraní API, které funguje v souladu s normou ISO/IEC 18013-ADD-API-01. Pokud je toto nastavení nastaveno na „znemožněno“, evropská peněženka digitální identity nezobrazuje žádosti o prezentaci nebo vydání zprostředkované API ani na ně neodpovídá.

— ISO/IEC 18013-ADD-API-05: Evropská peněženka digitální identity ověřuje v tocích mezi zařízeními pomocí zprostředkujícího rozhraní API, zda se komunikující zařízení nachází v těsné fyzické blízkosti evropské peněženky digitální identity, a to pomocí bezpečného, přímého a uživatelem zprostředkovaného místního komunikačního kanálu, například bezdrátové komunikační technologie krátkého dosahu, která provádí kontrolu fyzické blízkosti.

— POZNÁMKA: CTAP 2.3 umožňuje využívat BLE k provádění kontroly těsné fyzické blízkosti, a pokud je implementován oběma zařízeními, umožňuje také přenášet data mezi zařízeními prostřednictvím technologií přenosu s krátkým dosahem. Provádění kontroly fyzické blízkosti i přenosu dat mezi oběma zařízeními pomocí místního komunikačního kanálu, jež umožňuje CTAP 2.3, by měly příslušné operační systémy, prohlížeče, zprostředkující rozhraní API nebo jakákoli jiná technická vrstva mimo kontrolu evropské peněženky digitální identity upřednostnit před použitím služeb tunelu CTAP Hybrid.

13) 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: Evropská peněženka digitální identity splňuje požadavky uvedené v bodě 6.5 této přílohy.

— OIDFVP-HAIP-SUPPORT-03: Evropská peněženka digitální identity by neměla podporovat mechanismus založený na přesměrování specifikovaný v bodě 6.4 pro prezentační toky mezi zařízeními.

— POZNÁMKA 3: Použití tohoto mechanismu je náchylné k útokům, jako je například fixace relace. Zmírnění takových útoků je na spoléhajících se stranách. Zavedení tohoto mechanismu by nemělo vést k nedodržování předpisů.

— OIDFVP-HAIP-SUPPORT-05: Spoléhající se strana splňuje požadavky uvedené v bodě 6.5 této přílohy.

— POZNÁMKA 5: neplatné.

14) 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: Použijí se všechny povinné požadavky uvedené v bodech 5, 5.3, 7 a 8 HAIP [11].

— POZNÁMKA 1: „HAIP [11] oddíl 5“ se vztahuje pouze na požadavky přímo pod nadpisem oddílu 5. To nezahrnuje oddíly 5.1, 5.2 a 5.3.

— OIDFVP-HAIP-GEN-03: Pokud tato příloha mění požadavek v OpenID4VC-HAIP [11], má přednost upravený požadavek specifikovaný v této příloze.

— POZNÁMKA 2: To by například umožnilo převést nepovinný požadavek z OpenID4VC-HAIP [11] na povinný nebo rozšířit povinné požadavky.

— OIDFVP-HAIP-GEN-04: Pokud je formát požadovaného potvrzení v souladu s dokumentem [10], musí spoléhající se strany a evropské peněženky digitální identity dodržovat profil „ISO mdocs“ v dokumentu [11] oddíle 6.

— POZNÁMKA 3: Pro upřesnění: „profil ISO mdocs“ v HAIP znamená, že spoléhající se strany a evropské peněženky digitální identity musí splňovat příslušné požadavky v dokumentu [7] příloze B.2.

— OIDFVP-HAIP-GEN-05: Pokud je formát požadovaného potvrzení v souladu s dokumentem [2], spoléhající se strany a evropské peněženky digitální identity dodržují profil „IETF SD-JWT VC“ v dokumentu [11] oddíle 6.

— POZNÁMKA 4: Pro upřesnění: „profil IETF SD-JWT VCs“ znamená, že spoléhající se strany a evropské peněženky digitální identity musí splňovat požadavky uvedené v dokumentu [7] příloze B.3, jakož i požadavky uvedené v dokumentu [11] oddíle 6.1.

15) 6.3.2.1 General requirements

— OIDFVP-HAIP-COMMON-REQ-01: neplatné.

16) 6.3.2.2 Requirements for the Request Object

— OIDFVP-HAIP-COMMON-REQ-RO-02: neplatné

— OIDFVP-HAIP-COMMON-REQ-RO-03: neplatné

— OIDFVP-HAIP-COMMON-REQ-RO-04: neplatné

— OIDFVP-HAIP-COMMON-REQ-RO-05: neplatné

— OIDFVP-HAIP-COMMON-REQ-RO-06: neplatné.

— OIDFVP-HAIP-COMMON-REQ-RO-07: neplatné

— OIDFVP-HAIP-COMMON-REQ-RO-08: neplatné

— OIDFVP-HAIP-COMMON-REQ-RO-09: neplatné

— OIDFVP-HAIP-COMMON-REQ-RO-10: neplatné

— OIDFVP-HAIP-COMMON-REQ-RO-11: neplatné

— OIDFVP-HAIP-COMMON-REQ-RO-12: neplatné

— Poznámka 2: neplatné

— OIDFVP-HAIP-COMMON-REQ-RO-13: Jeden z prvků parametru verifier_info musí obsahovat registrační certifikát.

— OIDFVP-HAIP-COMMON-REQ-RO-23: Listový certifikát uvedený v oddíle 5.9.3 OpenID4VP pro použití s x509_hash Client Identifier Prefix je přístupový certifikát RP, jak je uvedeno v ETSI TS 119 475 [14].

17) 6.3.3 Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: neplatné.

18) 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: neplatné.

— POZNÁMKA: neplatné.

19) 6.5.2 Additional requirements

— OIDFVP-HAIP-ADD-API-01: Evropská peněženka digitální identity automaticky informuje zprostředkující rozhraní API, které funguje v souladu s bodem 5.2 dokumentu [11], o přítomnosti všech uložených typů EAA, ale nezveřejňuje atributy a jejich hodnoty v těchto EAA.

— OIDFVP-HAIP-ADD-API-04: Pokud evropská peněženka digitální identity podporuje zprostředkující rozhraní API, které funguje v souladu s OIDFVP-HAIP-ADD-API-01, poskytuje globální uživatelské nastavení, které znemožňuje zveřejnění uložených EAA prostřednictvím zprostředkujícího rozhraní API. Pokud je toto nastavení nastaveno na „zveřejnění znemožněno“, měla by evropská peněženka digitální identity následně umožnit uživateli vybrat jednotlivá potvrzení, která mají být zpřístupněna zprostředkujícímu rozhraní API.

— OIDFVP-HAIP-ADD-API-05: Evropská peněženka digitální identity ověřuje v tocích mezi zařízeními pomocí zprostředkujícího rozhraní API, zda se komunikující zařízení nachází v těsné fyzické blízkosti evropské peněženky digitální identity, a to pomocí bezpečného, přímého a uživatelem zprostředkovaného místního komunikačního kanálu, například bezdrátové komunikační technologie krátkého dosahu, která provádí kontrolu fyzické blízkosti.

— POZNÁMKA 5: CTAP 2.3 umožňuje využívat BLE k provádění kontroly těsné fyzické blízkosti, a pokud je implementován oběma zařízeními, umožňuje také přenášet data mezi zařízeními prostřednictvím technologií přenosu s krátkým dosahem. Provádění kontroly fyzické blízkosti i přenosu dat mezi oběma zařízeními pomocí místního komunikačního kanálu, jež umožňuje CTAP 2.3, by měly příslušné operační systémy, prohlížeče, zprostředkující rozhraní API nebo jakákoli jiná technická vrstva mimo kontrolu evropské peněženky digitální identity upřednostnit před použitím služeb tunelu CTAP Hybrid.

20) 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Všechny požadavky uvedené v tomto dokumentu, které se vztahují na struktury žádosti zařízení a odpovědi zařízení uvedené v normě ISO/IEC 18013-5, platí také v případě, že evropská peněženka digitální identity obdrží žádost o prezentaci ISO/IEC mdoc prostřednictvím mechanismu přenosu pomocí API podle bodu C.1 dokumentu [16].“