Úřední věstník
Evropské unie

CS
Řada L

2026/1735

22.7.2026

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2026/1735

ze dne 15. července 2026,

kterým se mění prováděcí nařízení (EU) 2025/1569, 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. 45d odst. 5, čl. 45e odst. 2 a čl. 45f odst. 6 a 7 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 přijetí prováděcího nařízení Komise (EU) 2025/1569 výrazně vyvinuly, mělo by být nyní prováděcí nařízení (EU) 2025/1569 ([3]) odpovídajícím způsobem změněno, aby bylo v souladu s novými normami a specifikacemi.

(2) V souladu s cíli nařízení (EU) č. 910/2014 byla pro splnění požadavků platných pro vydávání, správu a ověřování elektronických potvrzení atributů vybrána řada norem. Tyto normy by měly odrážet zavedené postupy a měly by být široce uznávány v příslušných odvětvích. V případě potřeby by měly být tyto normy upraveny nebo doplněny, aby byla zajištěna vysoká úroveň bezpečnosti a integrity elektronických potvrzení atributů a zároveň usnadněna přeshraniční interoperabilita a účinné fungování vnitřního trhu. V souladu s tímto cílem toto nařízení aktualizuje požadavky platné pro vydávání a zneplatňování kvalifikovaných elektronických potvrzení atributů a elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem a zavádí dále požadavky pro podepisování a pečetění výsledků ověřování podle autentických zdrojů.

(3) Na všechny činnosti zpracování osobních údajů podle tohoto nařízení se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ([4]) a v příslušných případech směrnice Evropského parlamentu a Rady 2002/58/ES ([5]).

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

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

([3]) 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).

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

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

(4) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([6]) byl konzultován evropský inspektor ochrany údajů, který vydal své stanovisko dne 17. dubna 2026 ([7]).

(5) 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) 2025/1569

Prováděcí nařízení (EU) 2025/1569 se mění takto:

1) V článku 3 se odstavec 2 nahrazuje tímto:

„2. Pokud poskytovatelé kvalifikovaných elektronických potvrzení atributů a poskytovatelé elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem vydají elektronická potvrzení atributů, která jsou zahrnuta do schémat registrovaných v katalogu schémat pro potvrzování atributů, musí splňovat požadavky příslušného schématu pro potvrzování atributů. Součástí posouzení shody stanoveného v nařízení (EU) č. 910/2014 jsou politiky a postupy stanovené vydavateli potvrzení za účelem zajištění souladu s požadavky schémat pro potvrzování atributů.“;

2) článek 4 se mění takto:

a) odstavec 1 se zrušuje;

b) odstavec 3 se nahrazuje tímto:

„3. Poskytovatelé kvalifikovaných elektronických potvrzení atributů a poskytovatelé elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem zneplatní tato potvrzení, jsou-li vydána s dobou platnosti delší než 24 hodin, alespoň v těchto případech:

a) na žádost osoby, které bylo elektronické potvrzení atributů vydáno, nebo v příslušných případech subjektu potvrzení;

b) pokud poskytovatel zjistí, že došlo k narušení bezpečnosti nebo důvěryhodnosti kvalifikovaných elektronických potvrzení atributů nebo elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem;

c) v jiných situacích, kdy to vyžadují právní předpisy Unie nebo vnitrostátní právní předpisy.“;

c) odstavec 4 se nahrazuje tímto:

„4. Poskytovatelé kvalifikovaných elektronických potvrzení atributů a poskytovatelé elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem zavedou techniky zneplatnění a metody správy, které zachovávají soukromí a brání propojitelnosti nebo sledovatelnosti. Techniky zneplatnění musí splňovat požadavky stanovené v příloze II.“;

([6]) 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).

([7]) EDPS Formal comments on the draft Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties (Formální připomínky EIOÚ k návrhu prováděcího nařízení Komise, pokud jde o platné normy a specifikace pro registraci stran spoléhajících se na peněženku) | Evropský inspektor ochrany údajů.

3) článek 9 se mění takto:

a) za odstavec 2 se vkládá nový odstavec 2a, který zní:

„2a. Ověřovací mechanismus musí být v souladu se specifikacemi stanovenými v příloze IV.“;

b) odstavec 4 se nahrazuje tímto:

„4. Výsledek ověření uvádí to, zda byl atribut ověřen, či nikoli, a specifikuje subjekt veřejného sektoru odpovědný za autentický zdroj nebo v příslušných případech subjekt veřejného sektoru určený k jednání jménem autentického zdroje, podle něhož byl atribut ověřen.

Výsledek ověřování opatřuje podpisem nebo pečetí subjekt veřejného sektoru odpovědný za autentický zdroj nebo určený zprostředkovatel uznaný na vnitrostátní úrovni, přičemž používá minimálně zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronické podpisy nebo zaručenou elektronickou pečeť založenou na kvalifikovaném certifikátu pro elektronické pečetě.“;

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

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

6) znění obsažené v příloze III tohoto nařízení se doplňuje jako příloha IV.

Článek 2

Vstup v platnost

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

Ustanovení čl. 1 bodu 3 se použije ode dne 1. ledna 2027.

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 I

Seznam referenčních norem a specifikací uvedených v článku 3

Norma ETSI TS 119 471 V1.1.1 (2025-05) se použije s těmito úpravami:

1) 2.1 Normativní odkazy:

[1] ETSI EN 319 401 V3.2.1 (2026-01): „*Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers*“ (Elektronické podpisy a důvěryhodné infrastruktury (ESI); Obecné politické požadavky na poskytovatele služeb vytvářejících důvěru).

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

[3] FIPS PUB 140-3 (2019) „*Security Requirements for Cryptographic Modules*“ (Bezpečnostní požadavky na kryptografické moduly).

[4] Prováděcí nařízení Komise (EU) 2024/482 ([1]).

[5] Prováděcí nařízení Komise (EU) 2024/3144 ([2]).

[6] ISO/IEC 15408:2022 (části 1 až 5): „*Information security, cybersecurity and privacy protection – Evaluation criteria for IT security*“ (Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Kritéria hodnocení bezpečnosti IT).

2) 3.1 *Terms* (Podmínky):

Doplňuje se nový výraz, který zní:

— bezpečný kryptografický prostředek: prostředek, který uchovává soukromý klíč uživatele, chrání tento klíč před neoprávněným přístupem a provádí podepisování nebo dešifrovací funkce jménem uživatele.

3) 4. *EAA trust services* (Služby elektronického potvrzení atributů vytvářející důvěru):

— Bod 4.2.2.2 „*Verification of attributes against authentic sources*“ (Ověřování atributů podle autentických zdrojů) se nepoužije.

— REQ-EAASP-4.2.2.3-02: EAASP (poskytovatel služeb elektronického potvrzení atributů) se autentizuje instanci peněženky EUDIW (evropské peněženky digitální identity) za použití mechanismů vzájemné autentizace a pomocí platného přístupového certifikátu.

— REQ-EAASP-4.2.2.3-03: EAASP ověří jednotku peněženky EUDIW a to, *zda byla instance peněženky EUDIW zneplatněna*.

— Bod *4.3.2 „EUDIW Specific*“ (Specifické pro peněženky EUDIW) se nepoužije.

4) 6.1 *EAAS practice statement* (Prohlášení o postupech služeb elektronického potvrzení atributů):

— REQ-EAASP-6.1-02: EAASP zdokumentuje mechanismus zneplatnění v prohlášení o postupech služeb elektronického potvrzení atributů.

5) 6.3 *Information security policy* (Politika v oblasti bezpečnosti informací):

— REQ-EAASP-6.3-02: Poskytovatel služeb elektronického potvrzení atributů zavede postupy, kterými informuje orgán dohledu o veškerých změnách v poskytování služby elektronického potvrzení atributů vytvářející důvěru a o záměru ukončit tyto činnosti, a to v souladu s obchodními požadavky a příslušnými právními předpisy, a dále v souladu s požadavky prováděcích aktů přijatých podle čl. 24 odst. 5 nařízení (EU) č. 910/2014. Poskytovatel služeb elektronického potvrzení atributů informuje orgán dohledu alespoň:

— jeden měsíc před provedením jakékoli změny,

— tři měsíce před plánovaným ukončením poskytování služby vytvářející důvěru.

([1]) Prováděcí nařízení Komise (EU) 2024/482 ze dne 31. ledna 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2019/881, pokud jde o přijetí evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC) (Úř. věst. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Prováděcí nařízení Komise (EU) 2024/3144 ze dne 18. prosince 2024, kterým se mění prováděcí nařízení (EU) 2024/482, pokud jde o použitelné mezinárodní normy, a kterým se uvedené prováděcí nařízení opravuje (Úř. věst. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

6) 7.5 *Cryptographic controls* (Kryptografická opatření):

— REQ-EAASP-7.5.2-05: neplatné

— REQ-EAASP-7.5.2-06: neplatné

— REQ-EAASP-7.5.3-01A: Musí být zavedena vhodná bezpečnostní opatření pro správu veškerých kryptografických klíčů, kryptografických algoritmů a kryptografických prostředků po celou dobu jejich životního cyklu, v příslušných případech v souladu s přístupem založeným na kryptografické flexibilitě.

— REQ-EAASP-7.5.3-01B: Poskytovatel služeb elektronického potvrzení atributů si pro účely poskytování svých služeb vytvářejících důvěru zvolí a používá vhodné kryptografické techniky, které jsou v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [2].

— REQ-EAASP-7.5.3-02: Poskytovatel služeb elektronického potvrzení atributů zajistí, aby bezpečný kryptografický prostředek, který používá k vytváření digitálních podpisů nebo pečetí elektronických potvrzení atributů, byl kvalifikovaným prostředkem k vytváření podpisů nebo pečetí a aby všechny ostatní digitální podpisy nebo pečetě používané k poskytování odpovídající služby elektronického potvrzení atributů vytvářející důvěru nebo její části byly vytvořeny bezpečným kryptografickým prostředkem, jenž je důvěryhodným systémem certifikovaným v souladu:

a) se společnými kritérii pro hodnocení bezpečnosti informačních technologií, jak uvádí Společná kritéria pro hodnocení bezpečnosti informačních technologií ve verzi 3.1 (CC3.1) do data 31.8.2027, nebo ve verzi CC:2022, částech 1 až 5, zveřejněných účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT, nebo jak stanoví norma ISO/IEC 15408 [6], s certifikací na úroveň EAL 4 nebo vyšší, nebo

b) s evropským schématem certifikace kybernetické bezpečnosti založeným na společných kritériích (EUCC) [4][5] a certifikovaným na úrovni EAL 4 nebo vyšší, nebo

c) s normou FIPS-140-2 úroveň 3, jež se použije do 31. srpna 2027 pro stávající certifikované systémy, nebo normou FIPS PUB 140-3 [3] úroveň 3, která je použitelná do 31. prosince 2030.

Tato certifikace musí odpovídat bezpečnostnímu cíli nebo profilu ochrany nebo dokumentaci návrhu modulu a jeho bezpečnosti, které splňují požadavky tohoto dokumentu, vycházet z analýzy rizik a přihlížet k fyzickým a jiným netechnickým bezpečnostním opatřením.

Pokud je bezpečný kryptografický prostředek certifikován podle systému EUCC [4][5], musí být tento prostředek nakonfigurován a používán v souladu s touto certifikací.

— REQ-EAASP-7.5.5-01: neplatné

— REQ-EAASP-7.5.5-02: neplatné

— REQ-EAASP-7.5.5-04: neplatné.

7) 7.9 *Vulnerabilities and Incident management* (Řízení zranitelností a incidentů):

— REQ-EAASP-7.9-02: Činnosti monitorování musí zohledňovat citlivost veškerých shromažďovaných nebo analyzovaných informací.

8) 7.12 *EAASP and EAAS termination and termination plans* (Ukončení činnosti EAASP a EAAS a plány ukončení činnosti):

— REQ-EAASP-7.12-04: Plán ukončení činnosti EAASP musí splňovat požadavky stanovené v prováděcích aktech přijatých podle čl. 24 odst. 5 nařízení (EU) č. 910/2014 [i.1].“

PŘÍLOHA II

„PŘÍLOHA II

Technické specifikace uvedené v článcích 3 a 4

Poskytovatelé kvalifikovaných elektronických potvrzení atributů a poskytovatelé elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem vydávají svá potvrzení v souladu s alespoň jednou z norem uvedených v příloze II prováděcího nařízení Komise (EU) 2024/2979 ([1]) a uplatňují příslušné techniky zneplatnění, jež též uvádí příloha II prováděcího nařízení Komise (EU) 2024/2979.“

([1]) 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).

PŘÍLOHA III

„PŘÍLOHA IV

Seznam norem a technických specifikací uvedených v článku 9

Ověřovací mechanismy uvedené v článku 9 musí být v souladu s jedním nebo oběma následujícími soubory specifikací, a to s těmito úpravami:

a) technické specifikace stanovené v bodě 6.1.1 normy ETSI TS 119 478 V1.1.1 (2026-01) – *Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources* (Elektronické podpisy a důvěryhodné infrastruktury (ESI); Specifikace rozhraní týkajících se autentických zdrojů);

— REQ-ASIP-6.1.1.2-04-01 [PODMÍNĚNÉ]: V případě, že attributeVerificationResult je buď http://uri.etsi.org/19478/VerificationResult/Match, nebo http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, může attributeVerificationResult obsahovat element attributeValue.

— REQ-ASIP-6.1.1.2-04-02 [PODMÍNĚNÉ]: Pokud je zpět zaslaný attributeVerificationResult http://uri.etsi.org/19478/VerificationResult/Match a attributeVerificationResult obsahuje element attributeValue, pak musí element attributeValue obsahovat hodnotu jako v žádosti.

— REQ-ASIP-6.1.1.2-04-03 [PODMÍNĚNÉ]: Pokud je zpět zaslaný attributeVerificationResult http://uri.etsi.org/19478/VerificationResult/MatchWithVariation a attributeVerificationResult obsahuje element attributeValue, pak musí element attributeValue obsahovat hodnotu atributu uloženou v autentickém zdroji.

— REQ-ASIP-6.1.1.2-06-04-01 [PODMÍNĚNÉ]: Pokud je fragmentVerificationResult buď http://uri.etsi.org/19478/VerificationResult/Match, nebo http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, může attributeVerificationResult obsahovat element fragmentValue.

— REQ-ASIP-6.1.1.2-06-04-02 [PODMÍNĚNÉ]: Pokud je zpět zaslaný fragmentVerificationResult http://uri.etsi.org/19478/VerificationResult/Match a attributeVerificationResult obsahuje element fragmentValue, pak musí element fragmentValue obsahovat hodnotu, která byla v žádosti.

— REQ-ASIP-6.1.1.2-06-04-03 [PODMÍNĚNÉ]: Pokud je zpět zaslaný fragmentVerificationResult http://uri.etsi.org/19478/VerificationResult/MatchWithVariation a attributeVerificationResult obsahuje element fragmentValue, musí element fragmentValue obsahovat hodnotu fragmentu atributu uloženou v autentickém zdroji.

b) technické specifikace stanovené v bodě 6.2.3 normy ETSI TS 119 478 V1.1.1 (2026-01) – *Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources* (Elektronické podpisy a důvěryhodné infrastruktury (ESI); Specifikace rozhraní týkajících se autentických zdrojů).

— REQ-ASIP-6.2.3.2.1-08-04: Element AttributeVerificationResponse může zahrnovat přesně jeden podřízený element typu TextValue, XMLValue nebo AttributeProperties.“