2025/1946

30.9.2025

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2025/1946

ze dne 29. září 2025,

kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o kvalifikované služby uchovávání kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí

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. 34 odst. 2 a článek 40 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Kvalifikované služby uchovávání kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí zajišťují dlouhodobou integritu, pravost, průkaznost a dostupnost důkazů o uchovávání těchto elektronických podpisů a elektronických pečetí. To umožňuje prokázat jejich dlouhodobou platnost a zaručuje, že mohou být ověřeny bez ohledu na budoucí technologické změny. Tyto služby jsou poskytovány samostatně nebo jako součást jiné kvalifikované služby vytvářející důvěru, například kvalifikovaných služeb elektronické archivace.

(2) Předpoklad shody stanovený v čl. 34 odst. 1a a článku 40 nařízení (EU) č. 910/2014 by měl platit pouze tehdy, pokud kvalifikované služby uchovávání kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí splňují normy stanovené v tomto nařízení. Tyto normy by měly odrážet zavedené postupy a měly by být v příslušných odvětvích široce uznávány. Měly by být upraveny tak, aby zahrnovaly další kontroly zajišťující bezpečnost a důvěryhodnost kvalifikované služby vytvářející důvěru, jakož i možnost ověřovat status kvalifikovaných podpisů a kvalifikovaných pečetí a jejich technickou platnost v čase.

(3) Pokud poskytovatel služeb vytvářejících důvěru splňuje požadavky stanovené v příloze tohoto nařízení, měly by orgány dohledu předpokládat shodu s příslušnými požadavky nařízení (EU) č. 910/2014 a tento předpoklad řádně zohlednit při udělování nebo potvrzování statusu kvalifikované služby vytvářející důvěru. Kvalifikovaný poskytovatel služeb vytvářejících důvěru však může při prokazování shody s požadavky nařízení (EU) č. 910/2014 nadále využívat i jiných postupů.

(4) Komise pravidelně posuzuje nové technologie, postupy, normy nebo technické specifikace. V souladu se 75. bodem odůvodnění nařízení Evropského parlamentu a Rady (EU) 2024/1183 ([2]) by Komise měla toto nařízení přezkoumávat a v případě potřeby ho aktualizovat, aby bylo v souladu s globálním vývojem, novými technologiemi, normami nebo technickými specifikacemi a aby byly dodržovány osvědčené postupy na vnitřním trhu.

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

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

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

(6) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([5]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 6. června 2025.

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

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Referenční normy a specifikace

Referenční normy a specifikace uvedené v čl. 34 odst. 2 a článku 40 nařízení (EU) č. 910/2014 jsou uvedeny v příloze tohoto nařízení.

Článek 2

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 29. září 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

([3]) 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).

([4]) 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).

([5]) 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).

PŘÍLOHA

Seznam referenčních norem a specifikací uvedený v článku 2

Normy ETSI TS 119 511 V1.1.1 (2019-06) (dále jen „ETSI TS 119 511“) a ETSI TS 119 172-4 V1.1.1 (2021-05) (dále jen „ETSI TS 119 172-4“) se použijí s těmito úpravami:

1. Pro normu ETSI TS 119 511

1) 2.1 Normativní odkazy:

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Elektronické podpisy a infrastruktury (ESI); Obecné politické požadavky na poskytovatele služeb vytvářejících důvěru“.

— [2] ETSI TS 119 612 (V2.3.1) „Elektronické podpisy a infrastruktury (ESI); Důvěryhodné seznamy“.

— [5] FIPS PUB 140-3 (2019) „Bezpečnostní požadavky na kryptografické moduly“.

— [6] Prováděcí nařízení Komise (EU) 2024/482 ([1]), 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).

— [7] Prováděcí nařízení Komise (EU) 2024/3144 ([2]), kterým se mění prováděcí nařízení (EU) 2024/482, pokud jde o použitelné mezinárodní normy, a kterým se uvedené prováděcí nařízení opravuje.

— [8] Evropská skupina pro certifikaci kybernetické bezpečnosti, podskupina pro šifrování: „Dohodnuté kryptografické mechanismy“ zveřejněné Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) ([3]).

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) „Elektronické podpisy a infrastruktury (ESI); Podpisové politiky; Část 4: Pravidla použitelnosti podpisu (politika ověřování platnosti) pro evropské kvalifikované elektronické podpisy/pečetě používající důvěryhodné seznamy“.

— [10] ISO/IEC 15408:2022 (části 1 až 5) „Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Kritéria hodnocení bezpečnosti IT“.

2) 3.1 Podmínky

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

3) 6.4 Profily uchovávání

— OVR-6.4-08A [WTS][WOS] Očekávaná doba platnosti důkazů musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [8].

— POZNÁMKA 3 neplatné.

4) 6.5 Zásady uchovávání důkazů

— OVR-6.5-04A Používané kryptografické algoritmy musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [8].

— POZNÁMKA 1 neplatné.

([1]) Úř. věst. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([2]) Úř. věst. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

5) 7.2 Lidské zdroje

— OVR-7.2-02 Pracovníci poskytovatele služeb uchovávání na důvěryhodných pozicích a v příslušných případech jeho subdodavatelé na důvěryhodných pozicích musí být schopni splnit požadavek na „odborné znalosti, zkušenosti a kvalifikaci“ prostřednictvím formální odborné přípravy a pověření nebo skutečných zkušeností nebo kombinace obojího.

— OVR-7.2-03 Soulad s OVR-7.2-02 musí zahrnovat pravidelné aktuální informace (alespoň každých dvanáct měsíců) o nových hrozbách a stávajících bezpečnostních postupech.

6) 7.5 Kontroly šifrování

— OVR-7.5-05 [PODMÍNĚNÉ] Pokud poskytovatel služeb uchovávání podepisuje důkaz o uchovávání (nebo jeho část), musí být soukromý podpisový klíč poskytovatele služeb uchovávání uchováván a používán v rámci bezpečného kryptografického prostředku, který je důvěryhodným systémem certifikovaným v souladu s/se:

a) společnými kritérii pro hodnocení bezpečnosti informačních technologií stanovenými v normě ISO/IEC 15408 [10] nebo ve společných kritériích pro hodnocení bezpečnosti informačních technologií, verzi CC:2022, části 1 až 5, zveřejněných účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT a certifikovaných na úrovni EAL 4 nebo vyšší, nebo

b) systémem EUCC [6][7] a certifikovaným na úrovni EAL 4 nebo vyšší, nebo

c) do 31. 12. 2030 s normou FIPS PUB 140-3 [5] úrovně 3.

Tato certifikace musí odpovídat bezpečnostnímu cíli nebo profilu ochrany nebo dokumentaci návrhu modulu a jeho bezpečnosti, která splňuje požadavky tohoto dokumentu na základě analýzy rizik a s přihlédnutím k fyzickým a jiným netechnickým bezpečnostním opatřením.

Pokud je bezpečný kryptografický prostředek certifikován podle systému EUCC [6][7], musí být toto zařízení nakonfigurováno a používáno v souladu s touto certifikací.

— OVR-7.5-06 [PODMÍNĚNÉ] neplatné.

— OVR-7.5-07 [PODMÍNĚNÉ] Pokud poskytovatel služeb uchovávání podepisuje důkaz o uchovávání (nebo jeho část), musí být všechny záložní kopie soukromých podpisových klíčů poskytovatele služeb uchovávání chráněny bezpečným kryptografickým prostředkem, aby byla zajištěna jejich integrita a důvěrnost předtím, než jsou uloženy mimo tento prostředek.

— OVR-7.5-08 A Soukromý podpisový klíč poskytovatele služeb uchovávání lze exportovat a importovat do jiného bezpečného kryptografického prostředku pouze tehdy, pokud je tento export a import prováděn bezpečně a v souladu s certifikací těchto prostředků.

7) 7.8 Bezpečnost sítí

— OVR-7.8-03 Skenování zranitelnosti požadované v rámci požadavku REQ-7.8-13 normy ETSI EN 319 401 [1] se provádí nejméně jednou za čtvrtletí.

— OVR-7.8-04 Penetrační test požadovaný v rámci požadavku REQ-7.8-17X normy ETSI EN 319 401 [1] se provádí nejméně jednou ročně.

— OVR-7.8-05 Firewally musí být nakonfigurovány tak, aby zabránily veškerým protokolům a přístupům, které nejsou nezbytné pro provoz poskytovatele služeb uchovávání.

8) 7.14 Sledování šifrování

— OVR-7.14-03A Hodnocení kryptografických algoritmů v ustanoveních OVR-7.14.01 a OVR-7.14.02 musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [8].

— POZNÁMKA neplatné.

9) 7.12 Ukončení činnosti poskytovatele služeb vytvářejících důvěru a plány ukončení činnosti poskytovatele služeb vytvářejících důvěru

— OVR-7.12-01A Plán ukončení činnosti poskytovatele služeb vytvářejících důvěru musí splňovat požadavky stanovené v prováděcích aktech přijatých podle čl. 24 odst. 5 nařízení (EU) č. 910/2014 [i.2].

10) 7.17 Dodavatelský řetězec

— OVR-7.17-01 Uplatňují se požadavky uvedené v normě ETSI EN 319 401 [1], bodě 7.14.

11) Příloha A (normativní): Kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů ve smyslu článku 34 nařízení (EU) č. 910/2014

— OVR-A-02 [PDS][PDS+PGD]:

a) služba uchovávání uchovává veškeré informace potřebné ke kontrole statusu kvalifikovaného elektronického podpisu nebo pečetě, které by nebyly veřejně dostupné, a to až do konce doby uchovávání;

b) služba uchovávání zajistí, aby v daném okamžiku během doby uchovávání byly uchovávané informace takové, že výstup tohoto procesu, je-li poskytnut jako vstup do procesu uvedeného v bodě 4.4 normy ETSI TS 119 172-4 [9], jasně určuje, zda digitální podpis nebo pečeť byly v době jejich uchovávání technicky vhodné k provedení kvalifikovaného elektronického podpisu EU nebo kvalifikované elektronické pečetě EU.

— OVR-A-03 [PDS][PDS+PGD] Časová razítka použitá v rámci důkazů o uchovávání musí být kvalifikovanými časovými razítky v souladu s nařízením (EU) č. 910/2014 [i.2].

2. Pro normu ETSI TS 119 172-4

1) 2.1 Normativní odkazy:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Postupy pro vytváření a ověřování platnosti digitálních podpisů v případě zaručených elektronických podpisů; Část 1: Vytvoření a ověření platnosti“.

— Veškeré odkazy na normu „ETSI TS 119 102-1 [1]“ se považují za odkazy na normu „ETSI EN 319 102-1 [1]“;

— [2] ETSI TS 119 612 (V2.3.1) „Elektronické podpisy a infrastruktury (ESI); Důvěryhodné seznamy“.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Elektronické podpisy a infrastruktury (ESI); Politické a bezpečnostní požadavky na aplikace pro vytváření a ověřování platnosti podpisů“.

2) 4.2 Omezení ověřování a ověřovací postupy, požadavek REQ-4.2-03, oddíl „X.509 omezení ověřování“, písmeno c):

— i) pokud certifikát koncového subjektu představuje zdroj důvěry, omezení RevocationCheckingConstraints se nepoužijí;

— ii) pokud certifikát koncového subjektu nepředstavuje zdroj důvěry, nastaví se omezení RevocationCheckingConstraints na hodnotu „eitherCheck“, jak je vymezeno v normě ETSI TS 119 172-1 [3], bodě A.4.2.1, tabulce A.2 řádcích (m)2.1;

— iii) pokud certifikát koncového subjektu představuje zdroj důvěry, omezení RevocationFreshnessConstraints vymezená v normě ETSI TS 119 172-1 [3], bodě A.4.2.1, tabulce A.2 řádcích (m)2.2 se nepoužijí;

— iv) pokud certifikát koncového subjektu nepředstavuje zdroj důvěry, omezení RevocationFreshnessConstraints vymezená v normě ETSI TS 119 172-1 [3], bodě A.4.2.1, tabulce A.2 řádcích (m)2.2 se použijí s maximální hodnotou 0 pro podpisový certifikát, čímž se zajistí, že informace o zneplatnění bude přijata pouze tehdy, pokud byla vydána po nejlepším čase podpisu. Pro jiné certifikáty než podpisový certifikát, včetně certifikátů podporujících časová razítka, se hodnota omezení RevocationFreshnessConstraints nenastavuje.

3) 4.3 Požadavky na postupy ověřování platnosti podpisu a kontroly pravidel použitelnosti

— REQ-4.3-02 Aplikace pro ověřování platnosti podpisu musí být v souladu s normou ETSI TS 119 101 [13].

4) 4.4 Proces kontroly (pravidel) technické použitelnosti

— REQ-4.4.2-03 Pokud některá z kontrol uvedených v požadavku REQ-4.4.2-01 selže, pak:

— proces se zastaví,

— podpis se technicky určí jako neurčitý, tj. ani jako kvalifikovaný elektronický podpis EU, ani jako kvalifikovaná elektronická pečeť EU,

— výše uvedený výsledek a výsledky všech meziprocesů se uvedou ve zprávě o kontrole pravidel použitelnosti podpisu.