2025/2531

17.12.2025

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2025/2531

ze dne 16. prosince 2025,

kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy a specifikace pro kvalifikované elektronické knihy záznamů

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. 45 l odst. 3 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Nařízením Evropského parlamentu a Rady (EU) 2024/1183 ([2]) byl do nařízení (EU) č. 910/2014 zařazen seznam nových služeb vytvářejících důvěru a kvalifikovaných služeb vytvářejících důvěru, včetně zaznamenávání elektronických dat do kvalifikované elektronické knihy záznamů. Komise má stanovit seznam referenčních norem a v případě potřeby stanovit specifikace pro uvedené služby.

(2) Elektronická kniha záznamů je posloupnost elektronických datových záznamů, která má zajistit integritu těchto datových záznamů a přesnost chronologického řazení těchto záznamů. Aby se zajistilo, že zaznamenávání dat do kvalifikované elektronické knihy záznamů bude konzistentní, spolehlivé a chronologicky řazené, je nezbytné stanovit společný soubor specifikací pro zaznamenávání elektronických dat do kvalifikované elektronické knihy záznamů.

(3) Předpoklad shody stanovený v čl. 45 l odst. 2 nařízení (EU) č. 910/2014 by měl platit pouze tehdy, pokud kvalifikované služby vytvářející důvěru pro zaznamenávání elektronických dat do kvalifikované elektronické knihy záznamů splňují normy stanovené v tomto nařízení. Tyto normy by měly odrážet zavedené postupy a měly by být široce uznávány v příslušných odvětvích. Měly by být upraveny tak, aby zahrnovaly další opatření zajišťující bezpečnost a důvěryhodnost této kvalifikované služby vytvářející důvěru.

(4) 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 kvalifikovaného statusu 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.

(5) Komise pravidelně posuzuje nové technologie, postupy, normy nebo technické specifikace. V souladu se 75. bodem odůvodnění nařízení (EU) 2024/1183 by Komise měla toto nařízení přezkoumávat a v případě potřeby ho aktualizovat, aby bylo v souladu s globálním vývojem, novými technologiemi, postupy, normami či 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).

(6) Na 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]), též se zohledněním pokynů Evropského sboru pro ochranu osobních údajů 02/2025 o zpracování osobních údajů prostřednictvím technologií blockchain ([5]).

(7) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([6]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 21. října 2025 ([7]).

(8) 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. 45 l odst. 3 nařízení (EU) č. 910/2014 jsou pro kvalifikované elektronické knihy záznamů stanoveny 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 16. prosince 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]) edpb_guidelines_202502_blockchain_en.pdf.

([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]) Formální připomínky EIOÚ k návrhu prováděcího nařízení, kterým se stanoví prováděcí pravidla k nařízení (EU) č. 910/2014, pokud jde o referenční normy a specifikace pro kvalifikované elektronické knihy záznamů.

PŘÍLOHA

Seznam technických specifikací a referenčních norem pro kvalifikované distribuované elektronické knihy záznamů

1. Pro účely tohoto nařízení se rozumí:

   a) „neměnností“ stav datového záznamu v elektronické knize záznamů, který se stal nevratným a nelze jej změnit ani odstranit;

   b) „distribuovanou elektronickou knihou záznamů“ elektronická kniha záznamů, která je sdílena mezi sadou uzlů distribuované elektronické knihy záznamů a která je mezi uzly distribuované elektronické knihy záznamů synchronizována pomocí mechanismu konsensu;

   c) „uzlem distribuované elektronické knihy záznamů“ zařízení nebo proces, který je součástí sítě distribuované elektronické knihy záznamů a uchovává úplnou nebo částečnou kopii datových záznamů elektronické knihy záznamů;

   d) „sítí distribuované elektronické knihy záznamů“ síť uzlů distribuované elektronické knihy záznamů, která tvoří systém distribuované elektronické knihy záznamů;

   e) „systémem distribuované elektronické knihy záznamů“ systém, který implementuje distribuovanou elektronickou knihu záznamů;

   f) „konsenzem“ dohoda mezi uzly distribuované elektronické knihy záznamů o platnosti transakcí a udržování konzistentního a uspořádaného souboru ověřených transakcí v celém systému distribuované elektronické knihy záznamů;

   g) „mechanismem konsensu“ soubor pravidel a postupů, kterými se dosahuje konsensu;

   h) „pravidly správy“ soubor protokolů, politik a mechanismů, které určují, jak funguje systém distribuované elektronické knihy záznamů, jak jsou data ověřována a přidávána do elektronické knihy záznamů a jak účastníci interagují;

   i) „transakcí“ nejmenší jednotka pracovního procesu v rámci elektronické knihy záznamů;

   j) „pracovním procesem“ jedna nebo více posloupností kroků potřebných k dosažení výsledku, který je v souladu s pravidly správy elektronické knihy záznamů;

   k) „ověřenou transakcí“ transakce, u níž byly požadované podmínky integrity a pravosti a podmínky specifické pro protokol zkontrolovány v souladu s pravidly správy systému distribuované elektronické knihy záznamů;

   l) „kryptografickým propojením“ odkaz na data vytvořená pomocí vhodných kryptografických technik k zajištění integrity, pravosti nebo sledovatelnosti dat, na něž se odkazuje, a správné posloupnosti datových záznamů;

   m) „sestavou knihy záznamů“ strukturovaná podoba ověřitelných informací získaných z datových záznamů v elektronické knize záznamů, která poskytuje poznatky o konkrétních činnostech, stavech nebo souladu s předem stanovenými pravidly;

   n) „poskytovatelem kvalifikované elektronické knihy záznamů“ kvalifikovaný poskytovatel služeb vytvářejících důvěru, který poskytuje kvalifikovanou službu vytvářející důvěru spočívající v zaznamenávání dat do kvalifikované elektronické knihy záznamů;

   o) „kvalifikovanou distribuovanou elektronickou knihou záznamů“ distribuovaná elektronická kniha záznamů, která splňuje požadavky na kvalifikovanou elektronickou knihu záznamů.

2. Pokud kvalifikovaný poskytovatel služeb vytvářejících důvěru potřebuje vytvářet sestavu knihy záznamů, vytváří ji automatizovaně.

3. Poskytovatelé kvalifikovaných elektronických knih záznamů vytvářejí, aktualizují a vedou kvalifikovanou elektronickou knihu záznamů a zaznamenávají do ní elektronická data v souladu se specifikacemi stanovenými:

   a) pro všechny poskytovatele kvalifikovaných elektronických knih záznamů: v normě ETSI EN 319 401 v3.1.1 (2024-06) s těmito úpravami:

      — 2.1 Normativní odkazy:

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

[2] IETF RFC 7515 (květen 2015): „*JSON Web Signature (JWS)*“.

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

[4] 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).

[5] 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.

[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).

— 6.1 Prohlášení o postupech služeb vytvářejících důvěru:

  — REQ-6.1-12 Prohlášení o postupech elektronické knihy záznamů uvádí alespoň tyto informace:

    — funkční a technické schopnosti platformy elektronické knihy záznamů a její používání po celou dobu poskytování zaznamenávání dat do kvalifikované elektronické knihy záznamů jako kvalifikované služby vytvářející důvěru,

    — konkrétní mechanismy autentizace původu dat používané při poskytování služby,

    — konkrétní mechanismy sekvenčního chronologického řazení používané při poskytování služby,

    — v příslušných případech kryptografické propojení použité k uspořádání datových záznamů do posloupnosti,

    — v příslušných případech mechanismus konsensu zajišťující neměnnost a integritu datových záznamů a transakcí uchovávaných v knize záznamů, včetně případné bezpečnostní doby do dosažení neodvolatelnosti a integrity,

    — konkrétní mechanismy zajištění integrity dat používané při poskytování služby.

  — 6.2 Podmínky:

    — REQ-6.2-03 Účastníci a strany spoléhající se na službu vytvářející důvěru musí být před uzavřením smluvního vztahu jasným, úplným a snadno přístupným způsobem, ve veřejně přístupném prostoru a jednotlivě informováni o přesných podmínkách.

  — 6.3 Politika v oblasti bezpečnosti informací:

    — REQ-6.3-04X Poskytovatel služby vytvářející důvěru (TSP) stanoví postupy oznamování veškerých změn v poskytování služby vytvářející důvěru orgánu dohledu v souladu s obchodními požadavky a příslušnými právními předpisy. TSP informuje příslušný orgán dohledu alespoň:

      — jeden měsíc před provedením jakékoli změny,

      — tři měsíce před plánovaným ukončením poskytování služby vytvářející důvěru.

  — 7.2 Lidské zdroje:

    — REQ-7.2-04X Pracovníci TSP na důvěryhodných pozicích musí být schopni splnit požadavek na „odborné znalosti, zkušenosti a kvalifikaci“ prostřednictvím formální odborné přípravy a osvědčení, skutečných zkušeností, nebo kombinace obojího.

— REQ-7.2-05X To zahrnuje pravidelné (alespoň každých dvanáct měsíců) aktualizace pokrývající nové hrozby a aktuální bezpečnostní postupy.

— 7.5 Kryptografická opatření:

— REQ-7.5-01X 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-7.5-02 TSP musí pro účely poskytování svých služeb vytvářejících důvěru zvolit a používat vhodné kryptografické techniky, které jsou v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [1].

Konkrétně:

— REQ-7.5-03 Poskytovatelé kvalifikovaných elektronických knih záznamů stanoví původ datových záznamů v elektronické knize záznamů. Za tímto účelem používají zaručené elektronické podpisy založené na kvalifikovaných certifikátech nebo zaručené elektronické pečetě založené na kvalifikovaných certifikátech vytvořené uživateli služby v souladu s těmito normami a specifikacemi:

a) ETSI EN 319 122-1 V1.3.1 (2023-06). „*Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures*“ (Elektronické podpisy a infrastruktury (ESI); Digitální podpisy CAdES; Část 1: Stavební bloky a základní podpisy CAdES).

b) ETSI EN 319 132-1 V1.3.1 (2024-07). „*Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures*“ (Elektronické podpisy a důvěryhodné infrastruktury (ESI); Digitální podpisy XAdES; Část 1: Stavební bloky a základní podpisy XAdES).

c) ETSI TS 119 182-1 V1.2.1 (2024-07). „*Electronic Signatures and Trust Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures*“ (Elektronické podpisy a důvěryhodné infrastruktury (ESI); Digitální podpisy JAdES; Část 1: Stavební prvky a základní podpisy JAdES), s touto úpravou:

— 5.1.8 Parametr x5c hlavičky (X.509 Certificate Chain)

— Parametr x5c hlavičky definovaný v bodě 4.1.6 normy IETF RFC 7515 [2] musí být v podpisu JAdES uveden, a to buď jako podepsaný, nebo jako nepodepsaný parametr hlavičky.

— Parametr x5c hlavičky musí mít sémantiku stanovenou v bodě 4.1.6 normy IETF RFC 7515 [2].

— Parametr x5c hlavičky musí mít syntaxi stanovenou v bodě 4.1.6 normy IETF RFC 7515 [2].

— REQ-7.5-04: Poskytovatelé kvalifikovaných elektronických knih záznamů zajišťují jedinečné sekvenční chronologické řazení datových záznamů v elektronické knize záznamů. Za tímto účelem používají kryptografická propojení, která jsou založena na hašových seznamech nebo hašových stromech, využívají kryptografické hašovací funkce a jsou v souladu s těmito specifikacemi a normami:

a) SHA-256 nebo s delším výstupem hašování, v souladu s „dohodnutými kryptografickými mechanismy“ přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [1].

b) SHA3-256 nebo s delším výstupem hašování, v souladu s „dohodnutými kryptografickými mechanismy“ přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [1].

Alternativně, pokud poskytovatelé kvalifikovaných elektronických knih záznamů zajišťují jedinečné sekvenční chronologické řazení datových záznamů v elektronické knize záznamů pomocí zaznamenávání času, používají kvalifikovaná časová razítka.

— REQ-7.5-05 Poskytovatelé kvalifikovaných elektronických knih záznamů zajistí integritu datových záznamů zaznamenaných v kvalifikované elektronické knize záznamů. Za tímto účelem používají zaručené elektronické podpisy založené na kvalifikovaných certifikátech nebo zaručené elektronické pečetě založené na kvalifikovaných certifikátech v souladu s těmito normami a specifikacemi:

  a) jakékoli formáty podpisů nebo pečetí, které jsou v souladu s „dohodnutými kryptografickými mechanismy“ přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [1];

  b) SHA-256 nebo s delším výstupem hašování, v souladu s „dohodnutými kryptografickými mechanismy“ přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [1];

  c) SHA3-256 nebo s delším výstupem hašování, v souladu s „dohodnutými kryptografickými mechanismy“ přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [1].

  d) Poskytovatelé kvalifikovaných elektronických knih záznamů zajistí okamžitou zjistitelnost jakékoli následné změny dat zaznamenaných v kvalifikované elektronické knize záznamů.

— REQ-7.5-06 Pokud se používají mechanismy digitálního podpisu, musí být soukromé podpisové klíče poskytovatele kvalifikované elektronické knihy záznamů uchovávány a používány v bezpečném kryptografickém prostředku, který je důvěryhodným systémem certifikovaným v souladu:

  a) se společnými kritérii pro hodnocení bezpečnosti informačních technologií stanovenými v normě ISO/IEC 15408 ([1]) [6] nebo ve společných kritériích pro hodnocení bezpečnosti informačních technologií, verzí CC:2022, částmi 1 až 5, zveřejněnými účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT, a je certifikován na úrovni EAL 4 nebo vyšší, nebo

  b) s evropským systémem certifikace kybernetické bezpečnosti založeným na společných kritériích (EUCC) ([2]) ([3]) [4][5] a certifikovaným na úrovni EAL 4 nebo vyšší, nebo

  c) do 31.12.2030 v souladu s FIPS PUB 140-3 ([4]) [3], úrovní 3.

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.

([1]) 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]) 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/2024/482/2025-01-08).

([3]) 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).

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

— 7.8 Bezpečnost sítí:

— REQ-7.8-14X Skenování zranitelností podle požadavku REQ-7.8-13 se provádí nejméně jednou za čtvrtletí.

— REQ-7.8-18X Penetrační test podle požadavku REQ-7.8-17X se provádí nejméně jednou ročně.

— REQ-7.8-21X: Firewally musí být rovněž nakonfigurovány tak, aby blokovaly všechny protokoly a přístupy, které nejsou nutné pro provoz TSP.

— 7.9.1 Monitorování a protokolování:

— REQ-7.9.1-02X Činnosti monitorování musí zohledňovat citlivost veškerých shromažďovaných nebo analyzovaných informací.

— 7.12 Ukončení činnosti a plány ukončení činnosti TSP:

— REQ-7.12-02 A Plán ukončení činnosti TSP musí splňovat požadavky stanovené v prováděcích aktech přijatých podle čl. 24 odst. 5 nařízení (EU) č. 910/2014 [i.1].

b) Navíc pro všechny poskytovatele kvalifikovaných elektronických knih záznamů, kteří využívají technologie distribuované elektronické knihy záznamů:

1) ISO 23257:2022 „*Blockchain and distributed ledger technologies – Reference architecture*“ (Technologie blockchainu a technologie distribuovaného registru – Referenční architektura), bod 9, přičemž poskytnou úplný popis technologie systému distribuované elektronické knihy záznamů, technologie příslušné sítě distribuované elektronické knihy záznamů a technologie uzlů distribuované elektronické knihy záznamů;

2) ISO/TS 23635:2022. „*Blockchain and distributed ledger technologies – Guidelines for governance*“ (Technologie blockchain a technologie distribuovaného registru – Pokyny pro správu a řízení), pokud jde o písemné a veřejně přístupné politiky a postupy týkající se struktury správy a řízení služby elektronické knihy záznamů, kterou poskytují.