Úradný vestník
Európskej únie

SK
Séria L

2025/2531

17.12.2025

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2025/2531

zo 16. decembra 2025,

ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o referenčné normy a špecifikácie pre kvalifikované elektronické registre

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES ([1]), a najmä na jeho článok 45l ods. 3,

keďže:

(1) Nariadením Európskeho parlamentu a Rady (EÚ) 2024/1183 ([2]) sa do nariadenia (EÚ) č. 910/2014 zaviedol zoznam nových dôveryhodných služieb a kvalifikovaných dôveryhodných služieb vrátane zaznamenávania elektronických údajov v kvalifikovanom elektronickom registri. Komisia má vypracovať zoznam referenčných noriem a v prípade potreby stanoviť špecifikácie pre takéto služby.

(2) Elektronický register je postupnosť záznamov elektronických údajov, ktorá má zabezpečiť integritu týchto záznamov údajov a presnosť chronologického poradia týchto záznamov. S cieľom zabezpečiť, aby bolo zaznamenávanie údajov v kvalifikovanom elektronickom registri chronologicky zoradené, konzistentné a spoľahlivé, je potrebné stanoviť spoločný súbor špecifikácií pre zaznamenávanie elektronických údajov v kvalifikovanom elektronickom registri.

(3) Domnienka súladu s požiadavkami stanovená v článku 45l ods. 2 nariadenia (EÚ) č. 910/2014 by sa mala uplatňovať len vtedy, ak kvalifikované dôveryhodné služby na zaznamenávanie elektronických údajov v kvalifikovanom elektronickom registri spĺňa normy stanovené v tomto nariadení. Tieto normy by mali odrážať zavedené postupy a mali by byť všeobecne uznávané v príslušných odvetviach. Mali by sa upraviť tak, aby zahŕňali dodatočné kontroly, ktoré zaistia bezpečnosť a dôveryhodnosť kvalifikovanej dôveryhodnej služby.

(4) Ak poskytovateľ dôveryhodných služieb dodržiava požiadavky stanovené v prílohe k tomuto nariadeniu, orgány dohľadu by mali predpokladať súlad s príslušnými požiadavkami nariadenia (EÚ) č. 910/2014 a náležite zvážiť takúto domnienku pri udeľovaní alebo potvrdzovaní kvalifikovaného štatútu dôveryhodnej služby. Kvalifikovaný poskytovateľ dôveryhodných služieb však môže pri preukazovaní súladu s požiadavkami nariadenia (EÚ) č. 910/2014 stále využívať aj iné postupy.

(5) Komisia pravidelne posudzuje nové technológie, postupy, normy alebo technické špecifikácie. V súlade s odôvodnením 75 nariadenia (EÚ) 2024/1183 by Komisia mala toto nariadenie preskúmať a podľa potreby aktualizovať, aby bolo v súlade s globálnym vývojom, novými technológiami, postupmi, normami alebo technickými špecifikáciami a aby sa na vnútornom trhu dodržiavali najlepšie postupy.

([1]) Ú. v. EÚ L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o zriadenie európskeho rámca digitálnej identity (Ú. v. EÚ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Na činnosti spracúvania osobných údajov podľa tohto nariadenia sa vzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 ([3]) a v relevantných prípadoch smernica Európskeho parlamentu a Rady 2002/58/ES ([4]) aj s prihliadnutím na usmernenia Európskeho výboru pre ochranu údajov 02/2025 o spracúvaní osobných údajov technológiami blockchainu ([5]).

(7) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([6]) sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 21. októbra 2025 svoje stanovisko ([7]).

(8) Opatrenia prijaté v tomto nariadení sú v súlade so stanoviskom výboru zriadeného podľa článku 48 nariadenia (EÚ) č. 910/2014,

PRIJALA TOTO NARIADENIE:

Článok 1

Referenčné normy a špecifikácie

Referenčné normy a špecifikácie uvedené v článku 45l ods. 3 nariadenia (EÚ) č. 910/2014 sú pre kvalifikované elektronické registre stanovené v prílohe k tomuto nariadeniu.

Článok 2

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 16. decembra 2025

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES 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]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic ledgers [Formálne pripomienky EDPS k návrhu vykonávacieho nariadenia, ktorým sa stanovujú pravidlá uplatňovania nariadenia (EÚ) č. 910/2014, pokiaľ ide o referenčné normy a špecifikácie pre kvalifikované elektronické registre].

PRÍLOHA

Zoznam technických špecifikácií a referenčných noriem pre kvalifikované distribuované elektronické registre

1. Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

   a) „nemennosť“ je stav záznamu údajov elektronického registra, v ktorom sa záznam stal nezvratným a nemožno ho zmeniť ani odstrániť;

   b) „distribuovaný elektronický register“ je elektronický register, ktorý je zdieľaný v súbore uzlov distribuovaného elektronického registra a ktorý je medzi nimi synchronizovaný medzi pomocou mechanizmu konsenzu;

   c) „uzol distribuovaného elektronického registra“ je zariadenie alebo proces, ktorý je súčasťou siete distribuovaného elektronického registra a uchováva úplnú alebo čiastočnú kópiu záznamov údajov elektronického registra;

   d) „sieť distribuovaného elektronického registra“ je sieť uzlov distribuovaného elektronického registra, ktorá tvorí systém distribuovaného elektronického registra;

   e) „systém distribuovaného elektronického registra“ je systém, ktorým sa zavádza distribuovaný elektronický register;

   f) „konsenzus“ je dohoda medzi uzlami distribuovaného elektronického registra o platnosti transakcií a udržiavaní konzistentného a zoradeného súboru validovaných transakcií v celom systéme distribuovaného elektronického registra;

   g) „mechanizmus konsenzu“ je súbor pravidiel a postupov, ktorými sa dosahuje konsenzus;

   h) „pravidlá riadenia“ sú súbor protokolov, politík a mechanizmov, ktoré určujú, ako systém distribuovaného elektronického registra funguje, ako sa údaje validujú a pridávajú do elektronického registra a ako účastníci interagujú;

   i) „transakcia“ je najmenšia jednotka pracovného procesu v rámci elektronického registra;

   j) „pracovný proces“ je jedna alebo viacero postupností činností potrebných na dosiahnutie výsledku, ktorý je v súlade s pravidlami riadenia elektronického registra;

   k) „validovaná transakcia“ je transakcia, v prípade ktorej sa v súlade s pravidlami riadenia systému distribuovaného elektronického registra skontrolovala požadovaná integrita, pravosť a podmienky špecifické pre protokol;

   l) „kryptografické prepojenie“ je odkaz na údaje vytvorený pomocou vhodných kryptografických techník s cieľom zabezpečiť integritu, pravosť alebo vysledovateľnosť údajov, na ktoré odkazuje, a správnu postupnosť záznamov údajov;

   m) „správa z registra“ je štruktúrovaná prezentácia overiteľných informácií extrahovaných zo záznamov údajov elektronického registra, ktorá poskytuje prehľad o konkrétnych činnostiach, stavoch alebo súlade s vopred stanovenými pravidlami;

   n) „poskytovateľ kvalifikovaného elektronického registra“ je kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý poskytuje kvalifikovanú dôveryhodnú službu spočívajúcu v zaznamenávaní údajov v kvalifikovanom elektronickom registri;

   o) „kvalifikovaný distribuovaný elektronický register“ je distribuovaný elektronický register, ktorý spĺňa požiadavky kvalifikovaného elektronického registra.

2. Ak kvalifikovaný poskytovateľ dôveryhodných služieb potrebuje vypracovať správu z registra, vypracuje ju automatizovaným spôsobom.

3. Poskytovatelia kvalifikovaných elektronických registrov vytvárajú kvalifikovaný elektronický register, zaznamenávajú v ňom elektronické údaje, aktualizujú ho a spravujú ho v súlade so špecifikáciami stanovenými v týchto dokumentoch:

   a) pokiaľ ide o všetkých poskytovateľov kvalifikovaných elektronických registrov, norma ETSI EN 319 401 v3.1.1 (2024-06) s týmito úpravami:

      — 2.1. Normatívne odkazy:

        [1] európska skupina pre certifikáciu kybernetickej bezpečnosti, podskupina pre kryptografiu: *Agreed Cryptographic Mechanisms* (dohodnuté kryptografické mechanizmy), uverejnené Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA),

[2] IETF RFC 7515 (máj 2015): „Webový podpis JSON (JWS)“,

[3] FIPS PUB 140-3 (2019) „Bezpečnostné požiadavky na kryptografické moduly“,

[4] vykonávacie nariadenie Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskej schémy certifikácie kybernetickej bezpečnosti založenej na spoločných kritériách (EUCC),

[5] vykonávacie nariadenie Komisie (EÚ) 2024/3144 z 18. decembra 2024, ktorým sa mení vykonávacie nariadenie (EÚ) 2024/482, pokiaľ ide o uplatniteľné medzinárodné normy, a ktorým sa opravuje uvedené vykonávacie nariadenie,

[6] ISO/IEC 15408:2022 (časti 1 až 5): „Bezpečnosť informácií, kybernetická bezpečnosť a ochrana súkromia – kritériá na hodnotenie bezpečnosti IT“.

— 6.1. Vyhlásenie o postupoch týkajúcich sa dôveryhodných služieb:

  — REQ-6.1-12 Vyhlásenie o postupoch týkajúcich sa elektronického registra obsahuje aspoň tieto informácie:

    — funkčné a technické spôsobilosti platformy elektronického registra a jej používania počas celého poskytovania zaznamenávania údajov v kvalifikovanom elektronickom registri ako kvalifikovanej dôveryhodnej služby,

    — osobitné mechanizmy autentifikácie pôvodu údajov používané pri poskytovaní služby,

    — osobitné mechanizmy sekvenčného chronologického poradia používané pri poskytovaní služby,

    — v prípade potreby kryptografické prepojenie použité na zabezpečenie postupnosti záznamov údajov,

    — v prípade potreby mechanizmus konsenzu zabezpečujúci nemennosť a integritu záznamov údajov a transakcií uchovávaných v registri vrátane akéhokoľvek rezervného času až do dosiahnutia nemennosti a integrity,

    — osobitné mechanizmy integrity údajov používané pri poskytovaní služby.

  — 6.2. Podmienky:

    — REQ-6.2-03 Účastníci a strany spoliehajúce sa na dôveryhodnú službu sú pred uzavretím zmluvného vzťahu informovaní o presných podmienkach vrátane skôr uvedených položiek, a to jasným, komplexným a ľahko prístupným spôsobom vo verejne prístupnom priestore a individuálne.

  — 6.3. Politika v oblasti informačnej bezpečnosti:

    — REQ-6.3-04X Poskytovateľ dôveryhodných služieb (ďalej len „TSP“) stanoví postupy na oznamovanie akýchkoľvek zmien v poskytovaní dôveryhodnej služby orgánu dohľadu v súlade s obchodnými požiadavkami a príslušnými zákonmi a inými právnymi predpismi. TSP informuje orgán dohľadu aspoň:

      — jeden mesiac pred vykonaním akejkoľvek zmeny,

      — tri mesiace pred plánovaným ukončením poskytovania dôveryhodnej služby.

  — 7.2. Ľudské zdroje:

    — REQ-7.2-04X Personál TSP v dôveryhodných rolách sú schopní splniť požiadavku na „odborné znalosti, skúsenosti a kvalifikáciu“ na základe formálnej odbornej prípravy a poverení alebo reálnych skúseností, alebo kombinácie oboch možností.

— REQ-7.2-05X To zahŕňa pravidelné aktuálne informácie (aspoň každých 12 mesiacov) o nových hrozbách a súčasných bezpečnostných postupoch.

— 7.5. Kryptografické kontroly:

— REQ-7.5-01X Zavedú sa primerané bezpečnostné kontroly na správu všetkých kryptografických kľúčov, kryptografických algoritmov a kryptografických zariadení počas celého ich životného cyklu, pričom v prípade potreby sa uplatňuje prístup kryptografickej agility.

— REQ-7.5-02 TSP na účely poskytovania svojej dôveryhodnej služby vyberá a používa vhodné kryptografické techniky, ktoré sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [1].

Konkrétne:

— REQ-7.5-03 Poskytovatelia kvalifikovaných elektronických registrov stanovujú pôvod záznamov údajov v elektronickom registri. Na tento účel používajú zdokonalené elektronické podpisy založené na kvalifikovaných certifikátoch alebo zdokonalené elektronické pečate založené na kvalifikovaných certifikátoch vyhotovené používateľmi služby v súlade s týmito normami a špecifikáciami:

a) ETSI EN 319 122-1 V1.3.1 (2023-06): elektronické podpisy a infraštruktúra (ESI); digitálne podpisy CAdES; Časť 1: Základné moduly a základné podpisy CAdES;

b) ETSI EN 319 132-1 V1.3.1 (2024-07): Elektronické podpisy a infraštruktúry dôvery (ESI); digitálne podpisy XAdES; Časť 1: Základné moduly a základné podpisy XAdES;

c) ETSI TS 119 182-1 V1.2.1 (2024-07): Elektronické podpisy a infraštruktúry dôvery (ESI); digitálne podpisy JAdES; Časť 1: Základné moduly a základné podpisy JAdES s touto úpravou:

— 5.1.8. Parameter záhlavia x5c (X.509 Reťazec certifikátov)

— Parameter záhlavia x5c v zmysle bodu 4.1.6 normy IETF RFC 7515 [2] musí byť prítomný v podpise JAdES, a to buď ako podpísaný, alebo nepodpísaný parameter záhlavia.

— Parameter záhlavia x5c musí mať sémantiku uvedenú v bode 4.1.6 normy IETF RFC 7515 [2].

— Parameter záhlavia x5c musí mať syntax uvedenú v bode 4.1.6 normy IETF RFC 7515 [2].

— REQ-7.5-04: Poskytovatelia kvalifikovaných elektronických registrov zabezpečujú jedinečné sekvenčné chronologické poradie záznamov údajov v elektronickom registri. Na tento účel používajú kryptografické prepojenia založené na hašovacích zoznamoch alebo hašovacích stromoch s použitím kryptografických hašovacích funkcií v súlade s týmito špecifikáciami a normami:

a) SHA-256 alebo dlhší hašovací reťazec – v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [1];

b) SHA3-256 alebo dlhší hašovací reťazec – v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [1].

Alternatívne, ak poskytovatelia kvalifikovaných elektronických registrov používajú na zabezpečenie jedinečného sekvenčného chronologického poradia záznamov údajov v elektronickom registri zaznamenávanie času, používajú kvalifikované časové pečiatky.

— REQ-7.5-05 Poskytovatelia kvalifikovaných elektronických registrov zabezpečujú integritu záznamov údajov zaznamenaných v kvalifikovanom elektronickom registri. Na tento účel používajú zdokonalené elektronické podpisy založené na kvalifikovaných certifikátoch alebo zdokonalené elektronické pečate založené na kvalifikovaných certifikátoch v súlade s týmito normami a špecifikáciami:

  a) akékoľvek formáty podpisu alebo pečate, ktoré sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [1];

  b) SHA-256 alebo dlhší hašovací reťazec – v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [1];

  c) SHA3-256 alebo dlhší hašovací reťazec – v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [1];

  d) Poskytovatelia kvalifikovaných elektronických registrov zabezpečujú, aby bolo možné okamžite zistiť akúkoľvek následnú zmenu údajov zaznamenaných v elektronickom registri.

— REQ-7.5-06 Keď sa používajú mechanizmy digitálneho podpisu, podpisové súkromné kľúče poskytovateľa kvalifikovaného elektronického registra sa uchovávajú a používajú v rámci zabezpečeného kryptografického zariadenia, ktoré je dôveryhodným systémom certifikovaným v súlade:

  a) so spoločnými kritériami hodnotenia bezpečnosti informačných technológií, ako sa stanovuje v norme ISO/IEC 15408 ([1]) [6] alebo v častiach 1 až 5 spoločných kritérií hodnotenia bezpečnosti informačných technológií, verzii CC:2022, ktoré uverejnili účastníci dohody o uznávaní certifikátov spoločných kritérií v oblasti hodnotenia bezpečnosti informačných technológií, a certifikovaným na úrovni EAL 4 alebo vyššej alebo

  b) s európskou schémou certifikácie kybernetickej bezpečnosti založenou na spoločných kritériách (EUCC) ([2]) ([3]) [4][5] a certifikovaným na úrovni EAL 4 alebo vyššej, alebo

  c) do 31. 12. 2030 s normou FIPS PUB 140-3 ([4]) [3] na úrovni 3.

Táto certifikácia zodpovedá bezpečnostnému cieľu alebo profilu ochrany, alebo koncepcii modulu a bezpečnostnej dokumentácii, ktorá spĺňa požiadavky tohto dokumentu, a to na základe analýzy rizík a s prihliadnutím na fyzické a iné netechnické bezpečnostné opatrenia.

Ak má zabezpečené kryptografické zariadenie certifikáciu EUCC [4][5], potom sa toto zariadenie nakonfiguruje a používa v súlade s uvedenou certifikáciou.

([1]) ISO/IEC 15408:2022 (časti 1 až 5): „Bezpečnosť informácií, kybernetická bezpečnosť a ochrana súkromia – kritériá na hodnotenie bezpečnosti IT“.

([2]) Vykonávacie nariadenie Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskeho systému certifikácie kybernetickej bezpečnosti založeného na spoločných kritériách (EUCC) (Ú. v. EÚ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).

([3]) Vykonávacie nariadenie Komisie (EÚ) 2024/3144 z 18. decembra 2024, ktorým sa mení vykonávacie nariadenie (EÚ) 2024/482, pokiaľ ide o uplatniteľné medzinárodné normy, a ktorým sa opravuje uvedené vykonávacie nariadenie (Ú. v. EÚ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

([4]) FIPS PUB 140-3 (2019): „Bezpečnostné požiadavky na kryptografické moduly“.

— 7.8. Bezpečnosť siete:

— REQ-7.8-14X Skenovanie zraniteľnosti požadované v rámci požiadavky REQ-7.8-13 sa vykonáva aspoň raz za štvrťrok.

— REQ-7.8-18X Penetračný test požadovaný v rámci požiadavky REQ-7.8-17X sa vykonáva aspoň raz za rok.

— REQ-7.8-21X Firewally musia byť takisto konfigurované tak, aby sa zabránilo všetkým protokolom a prístupom, ktoré nie sú potrebné na prevádzku TSP.

— 7.9.1. Monitorovanie a logovanie:

— REQ-7.9.1-02X Monitorovacie činnosti zohľadňujú citlivosť všetkých zbieraných alebo analyzovaných informácií.

— 7.12. Ukončenie činnosti a plány ukončenia činnosti TSP:

— REQ-7.12-02A Plán ukončenia činnosti TSP spĺňa požiadavky stanovené vo vykonávacích aktoch prijatých podľa článku 24 ods. 5 nariadenia (EÚ) č. 910/2014 [i.1];

b) okrem toho pokiaľ ide o všetkých poskytovateľov kvalifikovaných elektronických registrov, ktorí využívajú technológie distribuovaných elektronických registrov:

1. ISO 23257:2022: Blockchain a technológie distribuovaného registra – referenčná architektúra, bod 9, kde sa uvádza úplný opis systému technológie distribuovaného elektronického registra, zodpovedajúcej siete technológie distribuovaného elektronického registra a uzlov technológie distribuovaného elektronického registra;

2. ISO/TS 23635:2022: Blockchain a technológie distribuovaného registra – usmernenia pre riadenie, pokiaľ ide o písomné a verejne prístupné politiky a postupy týkajúce sa štruktúry riadenia služby elektronického registra, ktorú poskytujú.