Úradný vestník
Európskej únie

SK
Séria L

2025/1946

30.9.2025

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2025/1946

z 29. septembra 2025,

ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o kvalifikované služby uchovávania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí

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 34 ods. 2 a článok 40,

keďže:

(1) Kvalifikované služby uchovávania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí zabezpečujú dlhodobú integritu, pravosť, dôkaz o existencii a prístupnosť evidencie o uchovávaní týchto elektronických podpisov a elektronických pečatí. To umožňuje preukázať ich právnu platnosť počas dlhšieho obdobia a zaručuje ich validáciu bez ohľadu na budúce technologické zmeny. Tieto služby sa poskytujú nezávisle alebo ako súčasť inej kvalifikovanej dôveryhodnej služby, ako sú kvalifikované elektronické archivačné služby.

(2) Domnienka súladu s požiadavkami stanovená v článku 34 ods. 1a a článku 40 nariadenia (EÚ) č. 910/2014 by sa mala uplatňovať len vtedy, ak kvalifikované služby uchovávania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí spĺňajú 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, ako aj schopnosť overiť kvalifikovaný štatút a technickú platnosť podpisov a pečatí v priebehu času.

(3) 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.

(4) Komisia pravidelne posudzuje nové technológie, postupy, normy alebo technické špecifikácie. V súlade s odôvodnením 75 nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1183 ([2]) by Komisia mala toto nariadenie podľa potreby preskúmať a aktualizovať, aby bolo v súlade s globálnym vývojom, novými technológiami, 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).

(5) 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]).

(6) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([5]) sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 6. júna 2025 svoje stanovisko.

(7) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom výboru uvedeného v článku 48 nariadenia (EÚ) č. 910/2014,

PRIJALA TOTO NARIADENIE:

Článok 1

Referenčné normy a špecifikácie

Referenčné normy a špecifikácie uvedené v článku 34 ods. 2 a článku 40 nariadenia (EÚ) č. 910/2014 sú 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 29. septembra 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]) 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).

PRÍLOHA

Zoznam referenčných noriem a špecifikácií uvedených v článku 2

Uplatňujú sa normy ETSI TS 119 511 V1.1.1 (2019-06) (ďalej len „ETSI TS 119 511“) a ETSI TS 119 172-4 V1.1.1 (2021-05) (ďalej len „ETSI TS 119 172-4“) s týmito úpravami:

1. Pokiaľ ide o normu ETSI TS 119 511:

   1. 2.1. Normatívne odkazy:

      — [1] ETSI EN 319 401 V3.1.1 (2024-06) „Elektronické podpisy a infraštruktúry (ESI); všeobecné požiadavky týkajúce sa politiky pre poskytovateľov dôveryhodných služieb“,

      — [2] ETSI TS 119 612 (V2.3.1) „Elektronické podpisy a infraštruktúry (ESI); dôveryhodné zoznamy“,

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

      — [6] vykonávacie nariadenie Komisie (EÚ) 2024/482 ([1]), 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),

      — [7] vykonávacie nariadenie Komisie (EÚ) 2024/3144 ([2]), ktorým sa mení vykonávacie nariadenie (EÚ) 2024/482, pokiaľ ide o uplatniteľné medzinárodné normy, a ktorým sa opravuje uvedené vykonávacie nariadenie,

      — [8] európska skupina pre certifikáciu kybernetickej bezpečnosti, podskupina pre kryptografiu: *Agreed Cryptographic Mechanisms* (Dohodnuté kryptografické mechanizmy), uverejnené Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA) ([3]),

      — [9] ETSI TS 119 172-4 V1.1.1 (2021-05) „Elektronické podpisy a infraštruktúry (ESI); podpisové politiky; časť 4: pravidlá uplatniteľnosti podpisov (politika validácie) pre európske kvalifikované elektronické podpisy/pečate s použitím dôveryhodných zoznamov“,

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

   2. 3.1. Termíny

      — zabezpečené kryptografické zariadenie: zariadenie, v ktorom sa uchováva súkromný kľúč používateľa, ktoré tento kľúč chráni pred kompromitáciou a ktoré vykonáva funkcie podpisovania alebo dešifrovania v mene používateľa.

   3. 6.4. Profily uchovávania

      — OVR-6.4-08A [WTS][WOS] Očakávané trvanie evidencie je v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [8].

      — POZNÁMKA č. 3: neplatné.

   4. 6.5. Politika evidencie o uchovávaní

      — OVR-6.5-04A Použité kryptografické algoritmy sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [8].

      — POZNÁMKA č. 1: neplatné.

([1]) Ú. v. EÚ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([2]) Ú. v. EÚ 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. Ľudské zdroje

— OVR-7.2-02 Personál poskytovateľa služieb uchovávania (ďalej len „PSP“) v dôveryhodných rolách a prípadne jeho subdodávatelia 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.

— OVR-7.2-03 Splnenie požiadavky OVR-7.2-02 zahŕňa pravidelné aktuálne informácie (aspoň každých 12 mesiacov) o nových hrozbách a súčasných bezpečnostných postupoch.

6. 7.5. Kryptografické kontroly

— OVR-7.5-05 [PODMIENEČNÉ] Keď PSP podpisuje evidenciu o uchovávaní (alebo jej časť), súkromný podpisový kľúč PSP sa uschováva a používa 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 [10] alebo v časti 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) so schémou EUCC [6][7] a certifikovaným na úrovni EAL 4 alebo vyššej, alebo

c) do 31. 12. 2030 s normou FIPS PUB 140-3 [5] 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 [6][7], potom sa toto zariadenie nakonfiguruje a používa v súlade s uvedenou certifikáciou.

— OVR-7.5-06 [PODMIENEČNÉ] neplatné.

— OVR-7.5-07 [PODMIENEČNÉ] Keď PSP podpisuje evidenciu o uchovávaní (alebo jej časť), všetky záložné kópie súkromných podpisových kľúčov PSP sú chránené, aby sa zabezpečila ich integrita a dôvernosť zabezpečeným kryptografickým zariadením predtým, ako sa uložia mimo tohto zariadenia.

— OVR-7.5-08 Súkromný podpisový kľúč PSP sa exportuje zo zabezpečeného kryptografického zariadenia a importuje do iného takéhoto zariadenia len vtedy, ak sa uvedené exportovanie a importovanie vykonávajú zabezpečene a v súlade s certifikáciou týchto zariadení.

7. 7.8. Bezpečnosť siete

— OVR-7.8-03 Skenovanie zraniteľnosti požadované v rámci požiadavky REQ-7.8-13 normy ETSI EN 319 401 [1] sa vykonáva aspoň raz za štvrťrok.

— OVR-7.8-04 Penetračný test požadovaný v rámci požiadavky REQ-7.8-17X normy ETSI EN 319 401 [1] sa vykonáva aspoň raz za rok.

— OVR-7.8-05 Firewally sú konfigurované tak, aby sa zabránilo všetkým protokolom a prístupom, ktoré nie sú potrebné na prevádzku PSP.

8. 7.14. Kryptografické monitorovanie

— OVR-7.14-03A Hodnotenie kryptografických algoritmov uvedené v požiadavkách OVR-7.14.01 a OVR-7.14.02 je v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [8].

— POZNÁMKA: neplatné.

9. 7.12. Ukončenie činnosti a plány ukončenia činnosti poskytovateľa dôveryhodných služieb

— OVR-7.12-01A Plán ukončenia činnosti poskytovateľa dôveryhodných služieb (TSP) spĺňa požiadavky stanovené vo vykonávacích aktoch prijatých podľa článku 24 ods. 5 nariadenia (EÚ) č. 910/2014 [i.2].

10. 7.17. Dodávateľský reťazec

— OVR-7.17-01 Uplatňujú sa požiadavky stanovené v bode 7.14 normy ETSI EN 319 401 [1].

11. Príloha A (normatívna): Kvalifikovaná služba uchovávania QES v zmysle článku 34 nariadenia (EÚ) č. 910/2014

— OVR-A-02 [PDS][PDS+PGD]

a) služba uchovávania uchováva všetky informácie potrebné na kontrolu kvalifikovaného štatútu elektronického podpisu alebo pečate, ktoré by neboli verejne dostupné, do konca obdobia uchovávania;

b) služba uchovávania zabezpečí, aby sa kedykoľvek počas obdobia uchovávania uchovávali také informácie, že ak sa poskytnú ako vstupné údaje v procese uvedenom v bode 4.4 normy ETSI TS 119 172-4 [9], vo výstupe z tohto procesu sa jasne určí, či digitálny podpis alebo pečať boli v čase ich uchovania technicky vhodné na implementáciu kvalifikovaného elektronického podpisu EÚ alebo kvalifikovanej elektronickej pečate EÚ.

— OVR-A-03 [PDS][PDS+PGD] Časové pečiatky použité v rámci evidencie o uchovávaní sú kvalifikované časové pečiatky v súlade s nariadením (EÚ) č. 910/2014 [i.2].

2. Pokiaľ ide o normu ETSI TS 119 172-4:

1. 2.1. Normatívne odkazy:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) „Elektronické podpisy a infraštruktúry dôvery (ESI); postupy vyhotovovania a validácie digitálnych podpisov AdES (zdokonalený elektronický podpis); časť 1: vyhotovovanie a validácia“,

— všetky odkazy na normu „ETSI TS 119 102-1 [1]“ sa chápu ako odkazy na normu „ETSI EN 319 102-1 [1]“,

— [2] ETSI TS 119 612 (V2.3.1) „Elektronické podpisy a infraštruktúry (ESI); dôveryhodné zoznamy“,

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Elektronické podpisy a infraštruktúry (ESI); požiadavky týkajúce sa politiky a bezpečnosti na aplikácie na vyhotovenie podpisu a jeho validáciu“.

2. 4.2. Obmedzenia validácie a postupy validácie, bod „X.509 obmedzenia validácie“ písmeno c) požiadavky REQ-4.2-03:

— i) ak certifikát koncového subjektu predstavuje dôveryhodný bod, obmedzenie RevocationCheckingConstraints sa nepoužije;

— ii) ak certifikát koncového subjektu nepredstavuje dôveryhodný bod, obmedzenie RevocationCheckingConstraints sa nastaví na hodnotu „eitherCheck“ v zmysle bodu A.4.2.1 tabuľky A.2 riadkov m)2.1 normy ETSI TS 119 172-1 [3];

— iii) ak certifikát koncového subjektu predstavuje dôveryhodný bod, obmedzenie RevocationFreshnessConstraints v zmysle bodu A.4.2.1 tabuľky A.2 riadkov m)2.2 normy ETSI TS 119 172-1 [3] sa nepoužije;

— iv) ak certifikát koncového subjektu nepredstavuje dôveryhodný bod, obmedzenie RevocationFreshnessConstraints v zmysle bodu A.4.2.1 tabuľky A.2 riadkov m)2.2 normy ETSI TS 119 172-1 [3] sa pre podpisový certifikát použije s maximálnou hodnotou 0, čím sa zabezpečí, že informácie o zrušení sa akceptujú len vtedy, ak boli vydané po najlepšom čase podpisu. Pre iné certifikáty ako podpisový certifikát vrátane certifikátov podporujúcich časové pečiatky sa nenastaví žiadna hodnota obmedzenia RevocationFreshnessConstraints.

3. 4.3. Požiadavky na validáciu podpisov a postupy kontroly pravidiel uplatniteľnosti

— REQ-4.3-02 Aplikácie na validáciu podpisu sú v súlade s normou ETSI TS 119 101 [13].

4. 4.4. Proces kontroly (pravidiel) technickej uplatniteľnosti

— REQ-4.4.2-03 Ak niektorá z kontrol uvedených v požiadavke REQ-4.4.2-01 zlyhá, tak:

— sa proces zastaví,

— podpis sa technicky určí ako neurčitý, t. j. ani ako kvalifikovaný elektronický podpis EÚ, ani ako kvalifikovaná elektronická pečať EÚ,

— uvedený výsledok a výsledky procesov všetkých medziprocesov sa zohľadnia v správe o kontrole pravidiel uplatniteľnosti podpisov.