Úradný vestník
Európskej únie

SK
Séria L

2025/1929

30.9.2025

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2025/1929

z 29. septembra 2025,

ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o spájanie dátumu a času s údajmi a stanovovanie presnosti zdrojov času na poskytovanie kvalifikovaných elektronických časových pečiatok

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 42 ods. 2,

keďže:

(1) Kvalifikované elektronické časové pečiatky zohrávajú kľúčovú úlohu v digitálnom prostredí tým, že podporujú prechod od tradičných procesov využívajúcich papierové dokumenty k ich elektronickým ekvivalentom. Spájaním informácií o dátume a čase s elektronickými údajmi pomáhajú kvalifikované elektronické časové pečiatky zabezpečiť správnosť dátumu a času, ktoré uvádzajú, a integritu digitálnych dokumentov, s ktorými sú dátum a čas spojené.

(2) Domnienka súladu s požiadavkami stanovená v článku 42 ods. 1a nariadenia (EÚ) č. 910/2014 by sa mala uplatňovať len vtedy, ak kvalifikované dôveryhodné služby na vydávanie kvalifikovaných časových pečiatok spĺňajú normy stanovené v tomto nariadení. Tieto normy by mali odrážať zavedené postupy a mali by byť všeobecne uznávané v príslušných odvetviach. Tieto normy by sa mali upraviť tak, aby zahŕňali dodatočné kontroly, ktoré zaistia bezpečnosť a dôveryhodnosť kvalifikovanej dôveryhodnej služby a spájania dátumu a času s údajmi a presnosť zdroja 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 vykonávacie 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.

(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]).

([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).

([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).

(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 uvedené v článku 42 ods. 2 nariadenia (EÚ) č. 910/2014 sú stanovené v prílohe k tomuto nariadeniu.

Článok 2

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

([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 pre služby súvisiace s kvalifikovanými časovými pečiatkami

Uplatňujú sa normy ETSI EN 319 421 V1.3.1 ([1]) (ďalej len „ETSI EN 319 421“) a ETSI EN 319 422 V1.1.1 ([2]) (ďalej len „ETSI EN 319 422“) s týmito úpravami:

1. Pokiaľ ide o normu ETSI EN 319 421:

   1. 2.1. Normatívne odkazy:

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

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

      — [5] ETSI EN 319 422 V1.1.1 (2016-03) „Elektronické podpisy a infraštruktúry (ESI); protokol časových pečiatok a profily tokenov časových pečiatok“,

      — [6] neplatné,

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

      — [10] vykonávacie nariadenie Komisie (EÚ) 2024/482 ([4]) 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),

      — [11] vykonávacie nariadenie Komisie (EÚ) 2024/3144 ([5]) 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.

   2. 3.1. Termíny

      — obdobie platnosti certifikátu: časový interval od dátumu notBefore do dátumu notAfter vrátane, počas ktorého certifikačný orgán (CA) zaručuje, že bude udržiavať informácie o stave certifikátu.

   3. 3.3. Skratky

      — EUCC: európska schéma certifikácie kybernetickej bezpečnosti založená na spoločných kritériách.

   4. 6.2. Vyhlásenie o postupoch týkajúcich sa dôveryhodných služieb

      — OVR-6.2-03 Orgán poskytujúci služby časovej pečiatky (ďalej len „TSA“) zahrnie do svojho vyhlásenia o zverejňovaní informácií vyhlásenia o dostupnosti svojej služby časovej pečiatky.

   5. 7.3. Personálna bezpečnosť

      — OVR-7.3-02 Personál TSA 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-7.3-03 Splnenie požiadavky OVR-7.3-02 zahŕňa pravidelné aktuálne informácie (aspoň každých 12 mesiacov) o nových hrozbách a súčasných bezpečnostných postupoch.

([1]) EN 319 421 – Elektronické podpisy a infraštruktúry (ESI) – požiadavky týkajúce sa politiky a bezpečnosti pre poskytovateľov dôveryhodných služieb vydávajúcich časové pečiatky, V1.3.1.
([2]) EN 319 422 – Elektronické podpisy a infraštruktúry (ESI) – protokol časových pečiatok a profily tokenov časových pečiatok, V1.1.1 (2016-03), https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([4]) Ú. v. EÚ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) Ú. v. EÚ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6. 7.6.2. Generovanie kľúča jednotky časovej pečiatky

— TIS-7.6.2-03 Generovanie kľúča (kľúčov) jednotky časovej pečiatky (ďalej len „TSU“) sa vykonáva 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 [3] 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 [10][11] a certifikovaným na úrovni EAL 4 alebo vyššej, alebo

c) do 31. 12. 2030 s normou FIPS PUB 140-3 [7] 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 [10][11], potom sa toto zariadenie nakonfiguruje a používa v súlade s uvedenou certifikáciou.

— TIS-7.6.2-04 neplatné.

— POZNÁMKA č. 3: neplatné.

— TIS-7.6.2-05A Algoritmus generovania kľúča TSU, výsledná dĺžka podpisového kľúča a podpisový algoritmus používané na podpisovanie časových pečiatok a na podpisovanie certifikátov verejného kľúča TSU sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti [9] a uverejnenými agentúrou ENISA.

— POZNÁMKA č. 4: neplatné.

— TIS-7.6.2-06 Podpisový kľúč TSU 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. 7.6.3. Ochrana súkromného kľúča TSU

— TIS-7.6.3-02 Súkromný kľúč TSU 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 [3] alebo v časti 1 až 5 spoločných kritérií hodnotenia bezpečnosti informačných technológií, verzii CC:2002, 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) [10][11], a certifikovaným na úrovni EAL 4 alebo vyššej, alebo

c) do 31. 12. 2030 s normou FIPS PUB 140-3 [7] 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 [10][11], potom sa toto zariadenie nakonfiguruje a používa v súlade s uvedenou certifikáciou.

— TIS-7.6.3-03 neplatné.

— POZNÁMKA č. 2: neplatné.

8. 7.6.7. Koniec životného cyklu kľúča TSU

— TIS-7.6.7-03A Dátum skončenia platnosti súkromných kľúčov TSU je v súlade s dohodnutými kryptografickými mechanizmami [9].

— POZNÁMKA č. 1: neplatné.

9. 7.10. Bezpečnosť siete

— OVR-7.10-05 Skenovanie zraniteľnosti požadované v rámci požiadavky REQ-7.8-13 normy ETSI EN 319 401 [1] sa vykonáva aspoň raz za štvrťrok.

— OVR-7.10-06 Penetračný test požadovaný v rámci požiadavky REQ-7.8-17X normy ETSI EN 319 401 [1] sa vykonáva aspoň raz za rok.

— OVR-7.10-07 Firewally sú konfigurované tak, aby sa zabránilo všetkým protokolom a prístupom, ktoré nie sú potrebné na prevádzku TSA.

10. 7.14. Ukončenie činnosti a plány ukončenia činnosti TSA

— OVR-7.14-01A 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.4].

2. Pokiaľ ide o normu ETSI EN 319 422:

1. 2.1. Normatívne odkazy

— [5] neplatné,

— [6] neplatné,

— [8] európska skupina pre certifikáciu kybernetickej bezpečnosti, podskupina pre kryptografiu: „dohodnuté kryptografické mechanizmy“,

— [9] RFC 9110 Sémantika HTTP.

2. 4.1.3. Hašovacie algoritmy, ktoré sa majú použiť

— Uplatňuje sa tento bod:

Hašovacie algoritmy používané na hašovanie informácií, ktoré sa majú opatriť časovou pečiatkou, očakávané trvanie časovej pečiatky a zvolené hašovacie funkcie verzus čas sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [8].

— POZNÁMKA: neplatné.

3. 4.2.3. Algoritmy, ktoré majú byť podporované

— Uplatňuje sa tento bod:

Podpisové algoritmy tokenov časových pečiatok, ktoré majú byť podporované, sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [8].

— POZNÁMKA: neplatné.

4. 4.2.4. Dĺžky kľúča, ktoré majú byť podporované

— Uplatňuje sa tento bod:

Dĺžky kľúča podpisového algoritmu pre zvolený podpisový algoritmus sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA.

— POZNÁMKA: neplatné.

5. 5.1.3. Algoritmy, ktoré majú byť podporované

— Uplatňuje sa tento bod:

Hašovacie algoritmy pre údaje časovej pečiatky, ktoré majú byť podporované, očakávané trvanie časovej pečiatky a zvolené hašovacie funkcie verzus čas sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [8].

— POZNÁMKA: neplatné.

6. 5.2.3. Algoritmy, ktoré sa majú použiť

— Uplatňuje sa tento bod:

Hašovacie algoritmy používané na hašovanie informácií, ktoré sa majú opatriť časovou pečiatkou, a podpisové algoritmy tokenov časových pečiatok sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [8].

— POZNÁMKA: neplatné.

7. 6.3. Požiadavky na dĺžku kľúča

— Uplatňuje sa tento bod:

Dĺžka kľúča pre zvolený podpisový algoritmus certifikátu TSU sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [8].

— POZNÁMKA: neplatné.

8. 6.5. Požiadavky na algoritmus

— Uplatňuje sa tento bod:

Verejný kľúč TSUa podpis certifikátu TSU používajú algoritmy, ktoré sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [8].

— POZNÁMKA: neplatné.

9. 7. Profily prenosových protokolov, ktoré majú byť podporované

— Klient časovej pečiatky a server časových pečiatok podporujú protokol časových pečiatok prostredníctvom HTTPS [9] v zmysle bodu 3.4 normy IETF RFC 3161 [1].

10. 8. Objektové identifikátory kryptografických algoritmov

— Uplatňuje sa tento bod:

Verejný kľúč TSU a podpis certifikátu TSU používajú algoritmy v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [8].

11. 9.1. Vyhlásenie o súlade s nariadením

— Ak TSA vyhlási token časovej pečiatky za kvalifikovanú elektronickú časovú pečiatku v súlade s nariadením (EÚ) č. 910/2014 [i.2], token obsahuje jednu inštanciu rozšírenia qcStatements v poli rozšírenia tokenu časovej pečiatky so syntaxou v zmysle bodu 3.2.6 normy IETF RFC 3739 [i.3].

— Rozšírenie qcStatements obsahuje jednu inštanciu vyhlásenia „esi4-qtstStatement-1“ v zmysle prílohy B.

— Rozšírenie qcStatements sa neoznačí ako kritické.