Úradný vestník
Európskej únie

SK
Séria L

2025/1943

30.9.2025

# VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2025/1943

## z 29. septembra 2025,

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

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 28 ods. 6 a článok 38 ods. 6,

keďže:

(1) Kvalifikované certifikáty pre elektronické podpisy a kvalifikované certifikáty pre elektronické pečate zohrávajú kľúčovú úlohu v digitálnom podnikateľskom prostredí tým, že podporujú prechod od tradičných procesov využívajúcich papierové dokumenty k ich elektronickým ekvivalentom. Prepojením validačných údajov elektronického podpisu s fyzickou osobou alebo validačných údajov elektronickej pečate s právnickou osobou a potvrdením mena alebo názvu tejto osoby zvyšujú kvalifikované certifikáty istotu, pokiaľ ide o totožnosť podpisovateľa a pôvodcu pečate.

(2) Domnienka súladu s požiadavkami stanovená v článku 28 ods. 6 a článku 38 ods. 6 nariadenia (EÚ) č. 910/2014 by sa mala uplatňovať len vtedy, ak kvalifikované dôveryhodné služby na vydávanie kvalifikovaných certifikátov pre elektronické podpisy a kvalifikované dôveryhodné služby na vydávanie kvalifikovaných certifikátov pre elektronické pečate 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 kvalifikovaných dôveryhodných služieb a obsahu kvalifikovaných certifikátov.

(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.

(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 pre kvalifikované certifikáty pre elektronické podpisy a elektronické pečate**

1. Referenčné normy a špecifikácie uvedené v článku 28 ods. 6 nariadenia (EÚ) č. 910/2014 sú stanovené v prílohe I k tomuto nariadeniu.

2. Referenčné normy a špecifikácie uvedené v článku 38 ods. 6 nariadenia (EÚ) č. 910/2014 sú stanovené v prílohe II 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

([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 I*

**Zoznam referenčných noriem a špecifikácií pre kvalifikované certifikáty pre elektronické podpisy**

Uplatňujú sa normy ETSI EN 319 411-2 V2.6.1 (ďalej len „ETSI EN 319 411-2“), ETSI EN 319 412-1 V1.6.1 (ďalej len „ETSI EN 319 412-1“), ETSI EN 319 412-2 V2.4.1 (ďalej len „ETSI EN 319 412-2“) a ETSI EN 319 412-5 V2.5.1 (ďalej len „ETSI EN 319 412-5“) s týmito úpravami:

1. Pokiaľ ide o normu ETSI EN 319 411-2:

1. 2.1. Normatívne odkazy

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

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Elektronické podpisy a infraštruktúry dôvery (ESI); požiadavky týkajúce sa politiky a bezpečnosti pre poskytovateľov dôveryhodných služieb vydávajúcich certifikáty; časť 1: všeobecné požiadavky“ s týmito úpravami:

bod 2.1. Normatívne odkazy normy ETSI EN 319 411-1 V1.5.1 sa mení takto:

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

— [10] ETSI EN 319 412-2 V2.4.1 „Elektronické podpisy a infraštruktúry (ESI); profily certifikátov; časť 2: profil certifikátu pre certifikáty vydávané fyzickým osobám“,

— [14] ETSI EN 319 412-1 V1.6.1 „Elektronické podpisy a infraštruktúry (ESI); profily certifikátov; časť 1: prehľad a spoločné štruktúry údajov“,

— [3] ETSI EN 319 412-5 V2.5.1 „Elektronické podpisy a infraštruktúry dôvery (ESI); profily certifikátov; časť 5: QCStatements“,

— [5] ETSI EN 319 412-1 V1.6.1 „Elektronické podpisy a infraštruktúry dôvery (ESI); profily certifikátov; časť 1: prehľad a spoločné štruktúry údajov“,

— [6] CEN/TS 419261:2015 „Bezpečnostné požiadavky na dôveryhodné systémy spravujúce certifikáty a časové pečiatky“,

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

— [8] vykonávacie nariadenie Komisie (EÚ) 2024/482 ([2]), 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),

— [9] vykonávacie nariadenie Komisie (EÚ) 2024/3144 ([3]), ktorým sa mení vykonávacie nariadenie (EÚ) 2024/482, pokiaľ ide o uplatniteľné medzinárodné normy, a ktorým sa opravuje uvedené vykonávacie nariadenie,

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

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

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

2. 5.2. Požiadavky na vyhlásenie o postupoch týkajúcich sa certifikátov

— OVR-5.2-02 V politike (politikách) v oblasti certifikátov [ďalej len „CP(s)“] identifikovanej (identifikovaných) v dokumentácii poskytovateľa dôveryhodných služieb (ďalej len „TSP“) sa uvádzajú požiadavky na profily certifikátov, ktoré sa majú použiť.

3. 5.3. Názov a identifikácia politiky v oblasti certifikátov

— OVR-5.3-01 Ak sa v politike v oblasti certifikátov (ďalej len „CP“) vykonajú akékoľvek zmeny opísané v bode 4.2.2, ktoré ovplyvňujú uplatniteľnosť, zmení sa identifikátor politiky.

4. 6.1. Zodpovednosti v oblasti uverejňovania a uchovávania informácií

— OVR-6.1-02 Informácie identifikované v požiadavke DIS-6.1-04 normy ETSI EN 319 411-1 [2] sú verejne a medzinárodne dostupné.

5. 6.2.2. Prvotná validácia totožnosti

— REG-6.2.2-01A Zhromažďovanie atribútov a evidencie o totožnosti subjektu, ako aj ich validácia sa vykonávajú v súlade s vykonávacími aktmi prijatými podľa článku 24 ods. 1c nariadenia (EÚ) č. 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] a [QCP-n-qscd] Totožnosť fyzickej osoby a prípadne akékoľvek osobitné atribúty osoby sa overujú v súlade s vykonávacími aktmi prijatými podľa článku 24 ods. 1c nariadenia (EÚ) č. 910/2014 [i.1].

— POZNÁMKA č. 1: neplatné.

6. 6.3.3. Vydávanie certifikátov

— GEN-6.3.3-01 Uplatňujú sa požiadavky GEN-6.3.3-01 až GEN-6.3.3-10 určené v bode 6.3.3 normy ETSI EN 319 411-1 [2].

— GEN-6.3.3-02 [PODMIENEČNÉ] Ak sa certifikát vydá fyzickej osobe identifikovanej v spojení s právnickou osobou, potom atribúty subjektu identifikujúce organizáciu v certifikáte predstavujú právnickú osobu alebo podsubjekt tejto právnickej osoby a identifikátorom subjektu v certifikáte je daná fyzická osoba.

— GEN-6.3.3-03 Identifikátor CP [VÝBER]:

a) [QCP-n]

— zodpovedá špecifikácii v bode 5.3 písm. a) a/alebo

— je objektový identifikátor (ďalej len „OID“), ktorý pridelil TSP, iná príslušná zainteresovaná strana alebo ďalšia normalizácia pre politiku v oblasti certifikátov posilňujúcu zodpovedajúce platné požiadavky týkajúce sa politiky vymedzené v tomto dokumente;

b) [QCP-n-qscd]

— zodpovedá špecifikácii v bode 5.3 písm. c) a/alebo

— je OID, ktorý pridelil TSP, iná príslušná zainteresovaná strana alebo ďalšia normalizácia pre politiku v oblasti certifikátov posilňujúcu zodpovedajúce platné požiadavky týkajúce sa politiky vymedzené v tomto dokumente.

7. 6.3.5. Používanie kľúčového páru a certifikátu

— SDP-6.3.5-02A [PODMIENEČNÉ] Ak TSP spravuje zariadenie na vyhotovenie kvalifikovaného elektronického podpisu/pečate (ďalej len „QSCD“) pre daný subjekt, TSP je kvalifikovaný poskytovateľ dôveryhodných služieb poskytujúci kvalifikovanú dôveryhodnú službu na správu zariadenia na vyhotovenie kvalifikovaného elektronického podpisu na diaľku v súlade s nariadením (EÚ) č. 910/2014 [i.1].

— SDP-6.3.5-11A Ak žiadateľ alebo subjekt generuje kľúče subjektu, medzi povinnosti žiadateľa (pozri bod 6.3.4) patrí:

a) povinnosť generovať kľúče subjektu pomocou algoritmu v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti [7] a uverejnenými agentúrou ENISA na účely použitia certifikovaného kľúča identifikované v CP;

b) povinnosť používať dĺžku kľúča a algoritmus v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti [7] a uverejnenými agentúrou ENISA na účely použitia certifikovaného kľúča identifikované v CP počas platnosti certifikátu.

8. 6.3.10. Služby súvisiace so štatútom certifikátu

— CSS-6.3.10-08 [PODMIENEČNÉ] Ak sú k dispozícii zoznamy zrušených certifikátov (ďalej len „CRL“), TSP zachová integritu a dostupnosť posledného CRL aspoň počas obdobia uvedeného vo vyhlásení o postupoch týkajúcich sa certifikátov (ďalej len „CPS“), ako sa požaduje v požiadavke CSS-6.3.10-12.

9. 6.4.4. Personálne opatrenia

— OVR-6.4.4-02 Personál TSP 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-6.4.4-03 Splnenie požiadavky OVR-6.4.4-02 zahŕňa pravidelné (aspoň každých 12 mesiacov) aktuálne informácie o nových hrozbách a súčasných bezpečnostných postupoch.

— OVR-6.4.4-04 Okrem dôveryhodných rolí identifikovaných v norme ETSI EN 319 401 [1] (body 7.2 až 15) sú podporované dôveryhodné roly pracovníkov zodpovedných za registráciu a zrušenie so zodpovednosťami podľa vymedzenia v norme TS 419261 [6]. V prípadoch, keď je kvalifikovaný poskytovateľ dôveryhodných služieb (ďalej len „QTSP“) priamo riadený alebo prevádzkovaný v mene členského štátu alebo subjektu verejného sektora, tieto dodatočné dôveryhodné roly môže plniť jeden alebo viacero formálnych zástupcov konajúcich v mene pracovníkov zodpovedných za registráciu a zrušenie, ktorí vykonávajú činnosť v miestnej alebo regionálnej správe.

10. 6.4.9. Ukončenie činnosti certifikačného orgánu (ďalej len „CA“) alebo registračného orgánu (ďalej len „RA“)

— OVR-6.4.9-02 Plán ukončenia činnosti TSP spĺňa požiadavky stanovené vo vykonávacích aktoch prijatých podľa článku 24 ods. 5 nariadenia (EÚ) č. 910/2014 [i.1].

11. 6.5.1. Generovanie a inštalácia kľúčových párov

— OVR-6.5.1-01A CA generuje kľúčové páry pomocou algoritmu v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [7] na účely podpisovania CA.

— OVR-6.5.1-01B Zvolená dĺžka kľúča a algoritmus pre podpisový kľúč CA sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [7] na účely podpisovania CA.

— OVR-6.5.1-01C [PODMIENEČNÉ] Ak CA vygeneruje kľúče subjektu, kľúče subjektu vygenerované CA sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [7] na účely uvedené v CP počas platnosti certifikátu.

12. 6.5.2. Ochrana súkromného kľúča a technické kontroly kryptografických modulov

— GEN-6.5.2-01 Platia všetky požiadavky určené v bode 6.5.2 normy ETSI EN 319 411-1 [2] okrem požiadaviek OVR-6.5.2-01, OVR-6.5.2-03 a OVR-6.5.2-04.

— GEN-6.5.2-02 Generovanie kľúčových párov TSP vrátane kľúčov používaných službami zrušenia a registrácie sa vykonáva v rámci zabezpečeného kryptografického zariadenia, ktoré je dôveryhodným systémom certifikovaným v súlade:

— 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: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

— s európskou schémou certifikácie kybernetickej bezpečnosti založenou na spoločných kritériách (EUCC) [8][9], a certifikovaným na úrovni EAL 4 alebo vyššej, alebo

— do 31. 12. 2030 s normou FIPS PUB 140-3 [11] 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 [8][9], potom sa toto zariadenie nakonfiguruje a používa v súlade s uvedenou certifikáciou.

— GEN-6.5.2-03 Súkromný podpisový kľúč CA sa uschováva a používa v rámci zabezpečeného kryptografického zariadenia, ktoré spĺňa požiadavky GEN-6.5.2-01 a GEN-6.5.2-02.

13. 6.5.7. Kontroly sieťovej bezpečnosti

— OVR-6.5.7-02 Skenovanie zraniteľnosti požadované v rámci požiadavky REQ-7.8-13 normy ETSI EN 319 401 [1] sa vykonáva aspoň raz za štvrťrok.

— OVR-6.5.7-03 Penetračný test požadovaný v rámci požiadavky REQ-7.8-17X normy ETSI EN 319 401 [1] sa vykonáva aspoň raz za rok.

— OVR-6.5.7-04 Firewally sú konfigurované tak, aby sa zabránilo všetkým protokolom a prístupom, ktoré nie sú potrebné na prevádzku TSP.

14. 6.6.1. Profil certifikátu

— GEN-6.6.1-05 Certifikát obsahuje jeden z identifikátorov politiky identifikovaných v požiadavke GEN-6.3.3-03 [VÝBER]. Certifikát môže obsahovať aj iné OID pridelené TSP.

2. Pokiaľ ide o normu ETSI EN 319 412-2:

1. 2.1. Normatívne odkazy

— [2] ETSI EN 319 412-5 V2.5.1 „Elektronické podpisy a infraštruktúry dôvery (ESI); profily certifikátov; časť 5: QCStatements“,

— [9] európska skupina pre certifikáciu kybernetickej bezpečnosti, podskupina pre kryptografiu: *Agreed Cryptographic Mechanisms* (Dohodnuté kryptografické mechanizmy), uverejnené agentúrou ENISA.

2. 4.2.2. Podpis

— GEN-4.2.2-2 Podpisový algoritmus sa vyberá v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [9].

— POZNÁMKA: neplatné.

3. 4.2.3.1. Vydavatelia-právnické osoby

— GEN-4.2.3.1-3 Ak je známe, že existuje príslušné registračné číslo, totožnosť vydavateľa obsahuje atribút organizationIdentifier s hodnotou tohto registračného čísla, ako sa uvádza v príslušnom úradnom zázname stanovujúcom toto registračné číslo.

4. 4.2.5. Informácie o verejnom kľúči subjektu

— GEN-4.2.5-2 Verejný kľúč subjektu sa vyberá v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [9].

— POZNÁMKA: neplatné.

5. 4.2.6. Sériové číslo

— GEN-4.2.6-01 Atribút serialNumber certifikátu (ako sa uvádza v bode 4.1.2.2 normy IETF RFC 5280 [1]) je jedinečný pre každý certifikát vydaný TSP.

*PRÍLOHA II*

**Zoznam referenčných noriem a špecifikácií pre kvalifikované certifikáty pre elektronické pečate**

Uplatňujú sa normy ETSI EN 319 411-2 V2.6.1 (ďalej len „ETSI EN 319 411-2“), ETSI EN 319 412-1 V1.6.1 (ďalej len „ETSI EN 319 412-1“), ETSI EN 319 412-3 V1.3.1 (ďalej len „ETSI EN 319 412-3“), ETSI EN 319 412-2 V2.4.1 (ďalej len „ETSI EN 319 412-2“) a ETSI EN 319 412-5 V2.5.1 (ďalej len „ETSI EN 319 412-5“) s týmito úpravami:

1. Pokiaľ ide o normu ETSI EN 319 411-2:

1. 2.1. Normatívne odkazy

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

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Elektronické podpisy a infraštruktúry dôvery (ESI); požiadavky týkajúce sa politiky a bezpečnosti pre poskytovateľov dôveryhodných služieb vydávajúcich certifikáty; časť 1: všeobecné požiadavky“ s týmito úpravami:

bod 2.1. Normatívne odkazy normy ETSI EN 319 411-1 V1.5.1 sa mení takto:

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

— [10] ETSI EN 319 412-2 V2.4.1 „Elektronické podpisy a infraštruktúry (ESI); profily certifikátov; časť 2: profil certifikátu pre certifikáty vydávané fyzickým osobám“,

— [14] ETSI EN 319 412-1 V1.6.1 „Elektronické podpisy a infraštruktúry (ESI); profily certifikátov; časť 1: prehľad a spoločné štruktúry údajov“,

— [3] ETSI EN 319 412-5 V2.5.1 „Elektronické podpisy a infraštruktúry dôvery (ESI); profily certifikátov; časť 5: QCStatements“,

— [5] ETSI EN 319 412-1 V1.6.1 „Elektronické podpisy a infraštruktúry dôvery (ESI); profily certifikátov; časť 1: prehľad a spoločné štruktúry údajov“,

— [6] CEN/TS 419261:2015 „Bezpečnostné požiadavky na dôveryhodné systémy spravujúce certifikáty a časové pečiatky“ (vypracovaná výborom CEN),

— [7] európska skupina pre certifikáciu kybernetickej bezpečnosti, podskupina pre kryptografiu: *Agreed Cryptographic Mechanisms* (Dohodnuté kryptografické mechanizmy), uverejnené agentúrou ENISA,

— [8] vykonávacie nariadenie (EÚ) 2024/482, 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),

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

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

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

2. 5.2. Požiadavky na vyhlásenie o postupoch týkajúcich sa certifikátov

— OVR-5.2-02 V CP(s) v oblasti certifikátov identifikovanej (identifikovaných) v dokumentácii TSP sa uvádzajú požiadavky na profily certifikátov, ktoré sa majú použiť.

3. 5.3. Názov a identifikácia politiky v oblasti certifikátov

— OVR-5.3-01 Ak sa v CP vykonajú akékoľvek zmeny opísané v bode 4.2.2, ktoré ovplyvňujú uplatniteľnosť, zmení sa identifikátor politiky.

4. 6.1. Zodpovednosti v oblasti uverejňovania a uchovávania informácií

— OVR-6.1-02 Informácie identifikované v požiadavke DIS-6.1-04 normy ETSI EN 319 411-1 [2] sú verejne a medzinárodne dostupné.

5. 6.2.2. Prvotná validácia totožnosti

— REG-6.2.2-01A Zhromažďovanie atribútov a evidencie o totožnosti subjektu, ako aj ich validácia sa vykonávajú v súlade s vykonávacími aktmi prijatými podľa článku 24 ods. 1c nariadenia (EÚ) č. 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] a [QCP-l-qscd] Totožnosť právnickej osoby a prípadne akékoľvek osobitné atribúty osoby sa overujú v súlade s vykonávacími aktmi prijatými podľa článku 24 ods. 1c nariadenia (EÚ) č. 910/2014 [i.1].

— POZNÁMKA č. 3: Pozri poznámku č. 2.

6. 6.3.3. Vydávanie certifikátov

— GEN-6.3.3-01 Uplatňujú sa požiadavky GEN-6.3.3-01 až GEN-6.3.3-10 určené v bode 6.3.3 normy ETSI EN 319 411-1 [2].

— GEN-6.3.3-02 Identifikátor CP [VÝBER]:

a) [QCP-l]

— zodpovedá špecifikácii v bode 5.3 písm. b) a/alebo

— je OID, ktorý pridelil TSP, iná príslušná zainteresovaná strana alebo ďalšia normalizácia pre politiku v oblasti certifikátov posilňujúcu zodpovedajúce platné požiadavky týkajúce sa politiky vymedzené v tomto dokumente;

b) [QCP-l-qscd]

— zodpovedá špecifikácii v bode 5.3 písm. d) a/alebo

— je OID, ktorý pridelil TSP, iná príslušná zainteresovaná strana alebo ďalšia normalizácia pre politiku v oblasti certifikátov posilňujúcu platné požiadavky týkajúce sa politiky vymedzené v tomto dokumente.

7. 6.3.5. Používanie kľúčového páru a certifikátu

— SDP-6.3.5-02A [PODMIENEČNÉ] Ak TSP spravuje QSCD pre daný subjekt, TSP je kvalifikovaný poskytovateľ dôveryhodných služieb poskytujúci kvalifikovanú dôveryhodnú službu na správu zariadenia na vyhotovenie kvalifikovanej elektronickej pečate na diaľku v súlade s nariadením (EÚ) č. 910/2014 [i.1].

— SDP-6.3.5-11A Ak žiadateľ alebo subjekt generuje kľúče subjektu, medzi povinnosti žiadateľa (pozri bod 6.3.4) patrí:

a) povinnosť generovať kľúče subjektu pomocou algoritmu v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [7] na účely použitia certifikovaného kľúča identifikované v CP a takisto

b) povinnosť používať dĺžku kľúča a algoritmus v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [7] na účely použitia certifikovaného kľúča identifikované v CP počas platnosti certifikátu.

8. 6.3.10. Služby súvisiace so štatútom certifikátu

— CSS-6.3.10-08 [PODMIENEČNÉ] Ak sú k dispozícii CRL, TSP zachová integritu a dostupnosť posledného CRL aspoň počas obdobia uvedeného v CPS, ako sa požaduje v požiadavke CSS-6.3.10-12.

9. 6.4.4. Personálne opatrenia

— OVR-6.4.4-02 Personál TSP 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-6.4.4-03 Splnenie požiadavky OVR-6.4.4-02 zahŕňa pravidelné (aspoň každých 12 mesiacov) aktuálne informácie o nových hrozbách a súčasných bezpečnostných postupoch.

— OVR-6.4.4-04 Okrem dôveryhodných rolí identifikovaných v norme ETSI EN 319 401 [1] (body 7.2 až 15) sú podporované dôveryhodné roly pracovníkov zodpovedných za registráciu a zrušenie so zodpovednosťami podľa vymedzenia v norme TS 419261 [6]. V prípadoch, keď je QTSP priamo riadený alebo prevádzkovaný v mene členského štátu alebo subjektu verejného sektora, tieto dodatočné dôveryhodné roly môže plniť jeden alebo viacero formálnych zástupcov konajúcich v mene pracovníkov zodpovedných za registráciu a zrušenie, ktorí vykonávajú činnosť v miestnej alebo regionálnej správe.

10. 6.4.9. Ukončenie činnosti CA alebo RA

— OVR-6.4.9-02 Plán ukončenia činnosti TSP spĺňa požiadavky stanovené vo vykonávacích aktoch prijatých podľa článku 24 ods. 5 nariadenia (EÚ) č. 910/2014 [i.1].

11. 6.5.1. Generovanie a inštalácia kľúčových párov

— OVR-6.5.1-01A CA generuje kľúčové páry pomocou algoritmu v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [7] na účely podpisovania CA.

— OVR-6.5.1-01B Zvolená dĺžka kľúča a algoritmus pre podpisový kľúč CA sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [7] na účely podpisovania CA.

— OVR-6.5.1-01C [PODMIENEČNÉ] Ak CA vygeneruje kľúče subjektu, kľúče subjektu vygenerované CA sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [7] na účely uvedené v CP počas platnosti certifikátu.

12. 6.5.2. Ochrana súkromného kľúča a technické kontroly kryptografických modulov

— GEN-6.5.2-01 Platia všetky požiadavky určené v bode 6.5.2 normy ETSI EN 319 411-1 [2] okrem požiadaviek OVR-6.5.2-01, OVR-6.5.2-03 a OVR-6.5.2-04.

— GEN-6.5.2-02 Generovanie kľúčových párov TSP vrátane kľúčov používaných službami zrušenia a registrácie sa vykonáva v rámci zabezpečeného kryptografického zariadenia, ktoré je dôveryhodným systémom certifikovaným v súlade:

  — 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: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

  — s európskou schémou certifikácie kybernetickej bezpečnosti založenou na spoločných kritériách (EUCC) [8][9], a certifikovaným na úrovni EAL 4 alebo vyššej, alebo

  — do 31. 12. 2030 s normou FIPS PUB 140-3 [11] 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 [8][9], potom sa toto zariadenie nakonfiguruje a používa v súlade s uvedenou certifikáciou.

— GEN-6.5.2-03 Súkromný podpisový kľúč CA sa uschováva a používa v rámci zabezpečeného kryptografického zariadenia, ktoré spĺňa požiadavky GEN-6.5.2-01 a GEN-6.5.2-02.

13. 6.5.7. Kontroly sieťovej bezpečnosti

— OVR-6.5.7-02 Skenovanie zraniteľnosti požadované v rámci požiadavky REQ-7.8-13 normy ETSI EN 319 401 [1] sa vykonáva aspoň raz za štvrťrok.

— OVR-6.5.7-03 Penetračný test požadovaný v rámci požiadavky REQ-7.8-17X normy ETSI EN 319 401 [1] sa vykonáva aspoň raz za rok.

— OVR-6.5.7-04 Firewally sú konfigurované tak, aby sa zabránilo všetkým protokolom a prístupom, ktoré nie sú potrebné na prevádzku TSP.

14. 6.6.1. Profil certifikátu

— GEN-6.6.1-05 Certifikát obsahuje jeden z identifikátorov politiky identifikovaných v požiadavke GEN-6.3.3-02 [VÝBER].

2. Pokiaľ ide o normu ETSI EN 319 412-3:

1. 2.1. Normatívne odkazy

— [2] ETSI EN 319 412-2 V2.4.1 „Elektronické podpisy a infraštruktúry (ESI); profily certifikátov; časť 2: profil certifikátu pre certifikáty vydávané fyzickým osobám“.

2. 4.2.1. Subjekt

— LEG-4.2.1-6 Atribút organizationIdentifier obsahuje inú identifikáciu organizácie, ktorá je subjektom, než je názov organizácie. Ak je známe, že existuje príslušné registračné číslo, atribút organizationIdentifier obsahuje hodnotu tohto registračného čísla, ako sa uvádza v príslušnom úradnom zázname stanovujúcom toto registračné číslo.

3. Pokiaľ ide o normu ETSI EN 319 412-2:

1. 2.1. Normatívne odkazy

— [2] ETSI EN 319 412-5 V2.5.1 „Elektronické podpisy a infraštruktúry dôvery (ESI); profily certifikátov; časť 5: QCStatements“,

— [9] európska skupina pre certifikáciu kybernetickej bezpečnosti, podskupina pre kryptografiu: *Agreed Cryptographic Mechanisms* (Dohodnuté kryptografické mechanizmy), uverejnené agentúrou ENISA,

2. 2.2. Informatívne odkazy

— [i.7] neplatné.

3. 4.2.2. Podpis

— GEN-4.2.2-2 Podpisový algoritmus sa vyberá v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [9].

— POZNÁMKA: neplatné.

4. 4.2.3.1. Vydavatelia-právnické osoby

— GEN-4.2.3.1-3 Ak je známe, že existuje príslušné registračné číslo, totožnosť vydavateľa obsahuje atribút organizationIdentifier s hodnotou tohto registračného čísla, ako sa uvádza v príslušnom úradnom zázname stanovujúcom toto registračné číslo.

5. 4.2.5. Informácie o verejnom kľúči subjektu

— GEN-4.2.5-2 Verejný kľúč subjektu sa vyberá v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [9].

— POZNÁMKA: neplatné.

6. 4.2.6. Sériové číslo

— GEN-4.2.6-01 Atribút serialNumber certifikátu (ako sa uvádza v bode 4.1.2.2 normy IETF RFC 5280 [1]) je jedinečný pre každý certifikát vydaný TSP.