Úradný vestník
Európskej únie

SK
Séria L

2025/1942

30.9.2025

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2025/1942

z 29. septembra 2025,

ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o kvalifikované služby validácie kvalifikovaných elektronických podpisov a kvalifikované služby validácie 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 33 ods. 2 a článok 40,

keďže:

(1) Kvalifikované služby validácie kvalifikovaných elektronických podpisov, prípadne kvalifikovaných elektronických pečatí zabezpečujú integritu, pravosť a správnosť procesu a výsledkov validácie kvalifikovaných elektronických podpisov, prípadne kvalifikovaných elektronických pečatí. Tieto kvalifikované dôveryhodné služby zohrávajú kľúčovú úlohu v digitálnom podnikateľskom prostredí tým, že podporujú prechod od tradičných procesov využívajúcich papierové dokumenty k ich elektronickým ekvivalentom.

(2) Domnienka súladu s požiadavkami stanovená v článku 33 ods. 2 a článku 40 nariadenia (EÚ) č. 910/2014 by sa mala uplatňovať len vtedy, ak kvalifikované služby validácie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí spĺňajú technické normy stanovené v tomto nariadení. Uvedené 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, ako aj schopnosť overiť kvalifikovaný štatút a technickú platnosť kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí.

(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 33 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 pre kvalifikované služby validácie kvalifikovaných elektronických podpisov a kvalifikované služby validácie kvalifikovaných elektronických pečatí

Uplatňujú sa normy ETSI TS 119 441 V1.2.1 (2023-10) ([1]) (ďalej len „ETSI TS 119 441“) a ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) (ďalej len „ETSI TS 119 172-4“) s týmito úpravami:

1. Pokiaľ ide o normu ETSI TS 119 441:

1. 2.1. Normatívne odkazy

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

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

— [4] ISO/IEC 15408-1:2022 – Bezpečnosť informácií, kybernetická bezpečnosť a ochrana súkromia – kritériá na hodnotenie bezpečnosti IT,

— [5] neplatné,

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

— [7] vykonávacie nariadenie Komisie (EÚ) 2024/482 ([3]), 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),

— [8] 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“,

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) „Elektronické podpisy a infraštruktúry (ESI); postupy vyhotovovania a validácie digitálnych podpisov AdES (zdokonalený elektronický podpis); časť 2: správa o validácii podpisu“,

— [10] európska skupina pre certifikáciu kybernetickej bezpečnosti, podskupina pre kryptografiu: *Agreed Cryptographic Mechanisms* (Dohodnuté kryptografické mechanizmy), uverejnené Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA) ([4]),

— [11] vykonávacie nariadenie Komisie (EÚ) 2024/3144 ([5]), ktorým sa mení vykonávacie nariadenie (EÚ) 2024/4822, pokiaľ ide o uplatniteľné medzinárodné normy, a ktorým sa opravuje uvedené vykonávacie nariadenie,

— [12] ETSI EN 319 411-1 „Elektronické podpisy a infraštruktúry (ESI); požiadavky týkajúce sa politiky a bezpečnosti pre poskytovateľov dôveryhodných služieb vydávajúcich certifikáty; časť 1: všeobecné požiadavky“.

([1]) ETSI TS 119 441 – Elektronické podpisy a infraštruktúry (ESI); požiadavky týkajúce sa politiky na poskytovateľov dôveryhodných služieb (ďalej len „TSP“), ktorí poskytujú služby validácie podpisov, V1.2.1 (2023-10).

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

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

([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

([5]) Ú. v. EÚ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2. 2.2. Informatívne odkazy

— [i.11] neplatné.

3. 3.3. Skratky

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

4. 4.3.3. Proces

— POZNÁMKA č. 10: Pozri normu ETSI EN 319 102-1 [3] pre usmernenia a normu ETSI TS 119 172-4 [8] pre dodatočné usmernenia týkajúce sa prípadu kvalifikovaného podpisu alebo pečate EÚ.

5. 6.1. Vyhlásenie o postupoch týkajúcich sa služieb validácie podpisov

— OVR-6.1-02 Vyhlásenie o postupoch týkajúcich sa služieb validácie podpisov (ďalej len „SVS“) je štruktúrované podľa prílohy A.

— OVR-6.1-03 Vo vyhlásení o postupoch týkajúcich sa SVS sa uvádza zoznam podporovaných politík týkajúcich sa SVS alebo odkaz na tieto politiky [napr. prostredníctvom objektových identifikátorov (ďalej len „OID“)] a stručne sa v ňom opisujú.

6. 6.3. Politika v oblasti informačnej bezpečnosti

— OVR-6.3-02 Bezpečnostná politika dokumentuje kontroly bezpečnosti a ochrany súkromia zavedené na ochranu osobných údajov.

7. 7.2. Ľudské zdroje

— OVR-7.2-02 Personál poskytovateľa služieb validácie podpisov (ďalej len „SVSP“) 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.

8. 7.5. Kryptografické kontroly

— OVR-7.5-02 [PODMIENEČNÉ] Pri podpise správ o validácii vydá dôveryhodný certifikačný orgán (CA) verejný podpisový certifikát SVSP zodpovedajúci súkromnému podpisovému kľúču SVSP, a to v súlade s rozšírenou normalizovanou politikou v oblasti certifikátov (NCP+), ako sa uvádza v norme ETSI EN 319 411-1 [12]. Mal by sa vydať v súlade s príslušnou politikou v oblasti certifikátov uvedenou v norme ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [PODMIENEČNÉ] Pri podpise správ o validácii sa súkromný podpisový kľúč SVSP 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 [4] 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 [7][11] a certifikovaným na úrovni EAL 4 alebo vyššej, alebo

c) do 31. 12. 2030 s normou FIPS PUB 140-3 [6] 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 [7][11], potom sa toto zariadenie nakonfiguruje a používa v súlade s uvedenou certifikáciou.

— OVR-7.5-04 neplatné.

— OVR-7.5-06 Súkromný podpisový kľúč SVSP 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.

9. 7.7. Prevádzková bezpečnosť

— OVR-7.7-02 S cieľom zabezpečiť, aby systémy, v ktorých sa aplikácia vyvíja, uplatňovali primerané bezpečnostné opatrenia a prispôsobili sa špecifickému prostrediu aplikácie, aplikácia na validáciu podpisu (ďalej len „SVA“) používa prostredie aplikácie, ktoré je udržiavané aktuálnymi bezpečnostnými opravami.

— OVR-7.7-03 Na SVA sa uplatňujú nasledujúce požiadavky stanovené v bode 5.2 normy ETSI TS 119 101 [1]: GSM 1.3.

10. 7.8. Bezpečnosť siete

— OVR-7.8-02 Ak je povolený vzdialený prístup k systémom, v ktorých sa uchovávajú alebo spracúvajú dôverné údaje, prijme sa formálna politika a opíše sa ako súčasť prvkov požadovaných v rámci požiadavky OVR-6.3-02.

— OVR-7.8-04 Skenovanie zraniteľnosti požadované v rámci požiadavky REQ-7.8-13 normy ETSI EN 319 401 [1] sa vykonáva aspoň raz za štvrťrok.

— OVR-7.8-05 Penetračný test požadovaný v rámci požiadavky REQ-7.8-17X normy ETSI EN 319 401 [1] sa vykonáva aspoň raz za rok.

— OVR-7.8-06 Firewally sú konfigurované tak, aby sa zabránilo všetkým protokolom a prístupom, ktoré nie sú potrebné na prevádzku SVSP.

11. 7.12. Ukončenie činnosti a plány ukončenia činnosti poskytovania služieb validácie podpisov

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

12. 7.14. Dodávateľský reťazec

— OVR-7.14-01 Uplatňujú sa požiadavky stanovené v bode 7.14 normy ETSI EN 319 401 [2].

13. 8.1. Proces validácie podpisu

— VPR-8.1-07 Aplikácia na validáciu (SVA) spĺňa požiadavky SIA 1 až SIA 4 uvedené v bode 7.4 normy ETSI TS 119 101 [1].

— VPR-8.1-11 [PODMIENEČNÉ] Keď je cieľom SVS validovať kvalifikované elektronické podpisy alebo kvalifikované elektronické pečate v súlade s článkom 32 ods. 1 (prípadne článkom 40) nariadenia (EÚ) č. 910/2014 [i.1], proces validácie spĺňa požiadavky ETSI TS 119 172-4 [8].

14. 8.2. Protokol validácie podpisu

— SVP-8.2-03 Odpoveď na validáciu podpisu obsahuje OID politiky týkajúcej sa SVS.

15. 8.4. Správa o validácii podpisu

— SVR-8.4-02 Správa o validácii je v súlade s normou ETSI TS 119 102-2 [9].

— SVR-8.4-07 [PODMIENEČNÉ] Ak SVS úplne nespracuje politiku týkajúcu sa validácie podpisov, v správe sa okrem validovaných obmedzení uvádzajú aj obmedzenia, ktoré boli ignorované alebo potlačené.

— SVR-8.4-15 V správe o validácii sa jasne uvádza pôvod každého dôkazu o existencii (PoE) (z podpisu, z klienta, zo servera).

— SVR-8.4-16 Správa o validácii obsahuje podpis správy o validácii, ktorým je digitálny podpis SVSP.

— SVR-8.4-17 [PODMIENEČNÉ] Pri podpisovaní správ o validácii sú formát a cieľ podpisu v súlade s normou ETSI TS 119 102-2 [9].

16. 9 Rámec na vymedzenie politík týkajúcich sa služieb validácie na základe politiky týkajúcej sa dôveryhodných služieb vymedzenej v tomto dokumente:

— OVR-9-05 [PODMIENEČNÉ] Pri tvorbe politiky týkajúcej sa SVS na základe politiky týkajúcej sa dôveryhodných služieb vymedzenej v tomto dokumente sa vykoná posúdenie rizika s cieľom vyhodnotiť obchodné požiadavky a určiť bezpečnostné požiadavky, ktoré sa majú zahrnúť do politiky pre uvedenú komunitu a uplatniteľnosť.

— OVR-9-06 [PODMIENEČNÉ] Pri tvorbe politiky týkajúcej sa SVS na základe politiky týkajúcej sa dôveryhodných služieb vymedzenej v tomto dokumente sa uvedená politika schvaľuje a upravuje v súlade s vymedzeným postupom preskúmania, a to vrátane zodpovednosti za udržiavanie politiky.

— OVR-9-07 [PODMIENEČNÉ] Pri tvorbe politiky týkajúcej sa SVS na základe politiky týkajúcej sa dôveryhodných služieb vymedzenej v tomto dokumente existuje vymedzený postup preskúmania, aby sa zabezpečilo, že politiku budú podporovať vyhlásenia o postupoch.

— OVR-9-08 [PODMIENEČNÉ] Pri tvorbe politiky týkajúcej sa SVS na základe politiky týkajúcej sa dôveryhodných služieb vymedzenej v tomto dokumente TSP sprístupní politiky podporované poskytovateľom dôveryhodných služieb svojej komunite používateľov.

— OVR-9-09 [PODMIENEČNÉ] Pri tvorbe politiky týkajúcej sa SVS na základe politiky týkajúcej sa dôveryhodných služieb vymedzenej v tomto dokumente sa revízie politík podporovaných TSP sprístupnia žiadateľom.

17. Príloha B (normatívna): Kvalifikovaná služba validácie QES v zmysle článku 33 nariadenia (EÚ) č. 910/2014:

— VPR-B-02 [PODMIENEČNÉ] Ak je SVSP kvalifikovaným poskytovateľom služieb validácie podpisov (ďalej len „QSVSP“), vykonávanie je v súlade s normou ETSI TS 119 172-4 [8].

— POZNÁMKA č. 2: neplatné.

— OVR-B-04 [PODMIENEČNÉ] Ak je SVSP QSVSP, testy v rámci požiadavky OVR-B-03 kontrolujú rôzne prípady použitia, pozitívne aj negatívne.

— VPR-B-11 [PODMIENEČNÉ] Ak je SVSP QSVSP, SVSP riadi hašovací výpočet (buď vykonáva výpočet na strane servera, alebo riadi klienta, ak je povolený na strane klienta).

— POZNÁMKA č. 5: neplatné.

— POZNÁMKA č. 6: neplatné.

— VPR-B-15 [PODMIENEČNÉ] Ak je SVSP QSVSP, správa o validácii je v súlade s normou ETSI TS 119 102-2 [9], aby boli splnené požiadavky VPR-B-13 až VPR-B-14.

— VPR-B-16 [PODMIENEČNÉ] Ak je SVSP QSVSP, vykonávanie je v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [10] na používanie vhodných kryptografických techník pri poskytovaní kvalifikovaných služieb validácie kvalifikovaných elektronických podpisov (QES).

18. Príloha C (informatívna): Mapovanie požiadaviek s nariadením (EÚ) č. 910/2014, oddiel „Poskytovanie validácie v súlade s článkom 32 ods. 1“ druhý odsek:

— S cieľom zabezpečiť overenie všetkých podmienok požadovaných v článku 32 ods. 1 a článku 40 nariadenia (EÚ) č. 910/2014 [i.1] je potrebný správny validačný algoritmus. Poskytuje rovnaký deterministický výsledok pre podpis alebo pečať, ktoré boli predložené na validáciu. Na tento účel má zásadný význam politika týkajúca sa validácie podpisov. S touto perspektívou bola na základe validačného algoritmu stanoveného v norme ETSI EN 319 102-1 [3] vydaná norma ETSI TS 119 172-4 [8].

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 (2024-11) „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, ako sa vymedzuje v bode A.4.2.1 tabuľke A.2 riadkoch m)2.2 normy ETSI TS 119 172-1 [3], sa nepoužije,

— iv) ak certifikát koncového subjektu nepredstavuje dôveryhodný bod, obmedzenie RevocationFreshnessConstraints, ako sa vymedzuje v bode A.4.2.1 tabuľke A.2 riadkoch m)2.2 normy ETSI TS 119 172-1 [3], sa pre podpisový certifikát použije s maximálnou hodnotou 24. Pre iné certifikáty ako podpisový certifikát vrátane certifikátov podporujúcich časové pečiatky sa nenastaví žiadna hodnota obmedzenia RevocationFreshnessConstraints.

3. 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:

a) sa proces zastaví;

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

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