Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/1942

30.9.2025.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/1942

(2025. gada 29. septembris),

ar ko paredz noteikumus Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 piemērošanai attiecībā uz kvalificētu elektronisko parakstu kvalificētiem validēšanas pakalpojumiem un kvalificētu elektronisko zīmogu kvalificētiem validēšanas pakalpojumiem

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK ([1]), un jo īpaši tās 33. panta 2. punktu un 40. pantu,

tā kā:

(1) Kvalificēti validēšanas pakalpojumi kvalificētiem elektroniskajiem parakstiem un kvalificētiem elektroniskajiem zīmogiem nodrošina attiecīgi kvalificēto elektronisko parakstu un kvalificētu elektronisko zīmogu validēšanas procesa un rezultātu integritāti, autentiskumu un pareizību. Šādiem kvalificētiem uzticamības pakalpojumiem ir izšķiroša nozīme digitālajā uzņēmējdarbības vidē, jo tie veicina pāreju no tradicionāliem procesiem papīra formātā uz elektroniskiem ekvivalentiem.

(2) Regulas (ES) Nr. 910/2014 33. panta 2. punktā un 40. pantā noteiktais pieņēmums par atbilstību būtu jāpiemēro tikai tad, ja kvalificētu elektronisko zīmogu kvalificētie validēšanas pakalpojumi atbilst šajā regulā noteiktajiem tehniskajiem standartiem. Šiem standartiem būtu jāatspoguļo iedibinātā prakse un jābūt plaši atzītiem attiecīgajās nozarēs. Tie būtu jāpielāgo nolūkā iekļaut papildu kontroles, kas nodrošina kvalificēto uzticamības pakalpojumu drošību un uzticamību, kā arī spēju laika gaitā pārbaudīt kvalificēto elektronisko parakstu un kvalificēto elektronisko zīmogu kvalificēto statusu un tehnisko derīgumu.

(3) Ja uzticamības pakalpojumu sniedzējs ievēro šīs regulas pielikumā noteiktās prasības, uzraudzības iestādēm būtu jāpieņem, ka ir ievērotas Regulas (ES) Nr. 910/2014 attiecīgās prasības, un šāds pieņēmums pienācīgi jāņem vērā, piešķirot vai apstiprinot uzticamības pakalpojuma kvalificēto statusu. Tomēr kvalificētu uzticamības pakalpojumu sniedzējs joprojām var paļauties uz citu praksi, lai pierādītu atbilstību Regulas (ES) Nr. 910/2014 prasībām.

(4) Komisija regulāri novērtē jaunās tehnoloģijas, praksi, standartus un tehniskās specifikācijas. Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2024/1183 ([2]) 75. apsvērumu Komisijai šī regula vajadzības gadījumā būtu jāpārskata un jāatjaunina, lai tā atbilstu globālajām norisēm, jaunām tehnoloģijām, standartiem un tehniskajām specifikācijām un lai ņemtu vērā paraugpraksi iekšējā tirgū.

([1]) OV L 257, 28.8.2014., 73. lpp., ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Eiropas Parlamenta un Padomes Regula (ES) 2024/1183 (2024. gada 11. aprīlis), ar ko groza Regulu (ES) Nr. 910/2014 attiecībā uz Eiropas digitālās identitātes satvara izveidi (OV L, 2024/1183, 30.4.2024., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(5) Šajā regulā noteiktajām personas datu apstrādes darbībām piemēro Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([3]) un, attiecīgā gadījumā, Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([4]).

(6) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([5]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2025. gada 6. jūnijā sniedza savu atzinumu.

(7) Šajā regulā noteiktie pasākumi saskan ar atzinumu, ko sniegusi ar Regulas (ES) Nr. 910/2014 48. pantu izveidotā komiteja,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Atsauces standarti un specifikācijas

Regulas (ES) Nr. 910/2014 33. panta 2. punktā un 40. pantā minētie atsauces standarti un specifikācijas ir izklāstītas šīs regulas pielikumā.

2. pants

Stāšanās spēkā

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2025. gada 29. septembrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

([3]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp., ELI:. http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

PIELIKUMS

Atsauces standartu un specifikāciju saraksts kvalificētu elektronisko parakstu kvalificētiem validēšanas pakalpojumiem un kvalificētu elektronisko zīmogu kvalificētiem validēšanas pakalpojumiem

Standartus ETSI TS 119 441 V1.2.1 (2023-10) ([1]) ("ETSI TS 119 441") un ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) ("ETSI TS 119 172-4") piemēro ar šādiem pielāgojumiem:

1. Attiecībā uz ETSI TS 119 441

1) 2.1. Normatīvās atsauces

— [1] ETSI TS 119 101 V1.1.1 (2016-03) "Elektroniskie paraksti un infrastruktūras (*ESI*); Politikas un drošības prasības attiecībā uz paraksta radīšanas un paraksta validēšanas pieteikumiem".

— [2] ETSI EN 319 401 V3.1.1 (2024-06) "Elektroniskie paraksti un infrastruktūras (*ESI*); Vispārējās politikas prasības uzticamības pakalpojumu sniedzējiem".

— [3] ETSI EN 319 102-1 V1.4.1 (2024-06) "Elektroniskie paraksti un infrastruktūras (*ESI*); Procedūras *AdES* digitālo parakstu izveidei un validēšanai. 1. daļa: Izveide un validēšana".

— [4] ISO/IEC 15408-1:2022 "Informācijas drošība, kiberdrošība un privātuma aizsardzība – IT drošības vērtēšanas kritēriji".

— [5] Nav spēkā.

— [6] FIPS PUB 140-3 (2019) "Drošības prasības kriptogrāfijas moduļiem".

— [7] Komisijas Īstenošanas regula (ES) 2024/482 ([3]) par to, kā vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) pieņemšanas sakarā piemērojama Eiropas Parlamenta un Padomes Regula (ES) 2019/881.

— [8] ETSI TS 119 172-4 V1.1.1 (2021-05) "Elektroniskie paraksti un infrastruktūras (*ESI*); uzticamības saraksti. Parakstu politika; 4. daļa: Noteikumi par paraksta piemērojamību (validēšana politika) kvalificētiem Eiropas elektroniskajiem parakstiem/zīmogiem, kas izmanto uzticamības sarakstus".

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) "Elektroniskie paraksti un infrastruktūras (*ESI*); Procedūras *AdES* digitālo parakstu izveidei un validēšanai. 2. daļa: Paraksta validēšanas ziņojums".

— [10] Eiropas Kiberdrošības sertifikācijas grupas kriptogrāfijas jautājumu apakšgrupa: "Saskaņoti kriptogrāfijas mehānismi", ko publicējusi Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) ([4]).

— [11] Komisijas Īstenošanas regula (ES) 2024/3144 ([5]) par Īstenošanas regulas (ES) 2024/4822 grozījumiem attiecībā uz piemērojamajiem starptautiskajiem standartiem un par tās labojumiem.

— [12] ETSI EN 319 411-1 "Elektroniskie paraksti un infrastruktūras (*ESI*); politikas un drošības prasības uzticamības pakalpojumu sniedzējiem, kas izdod sertifikātus. 1. daļa: Vispārīgas prasības".

([1]) ETSI TS 119 441 "Elektroniskie paraksti un infrastruktūras (*ESI*); Politikas prasības *TSP*, kas sniedz paraksta validēšanas pakalpojumus, V1.2.1 (2023-10).

([2]) ETSI TS 119 172-4 "Elektroniskie paraksti un infrastruktūra (*ESI*)"; Parakstu politika; 4. daļa: Noteikumi par paraksta piemērojamību (validēšanas politika) kvalificētiem Eiropas elektroniskajiem parakstiem/zīmogiem, kas izmanto uzticamības sarakstus, V1.1.1 (2021-05).

([3]) OV 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]) OV L, 2024/3144, 19.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2. Informatīvas atsauces

— [i.11] Nav spēkā.

3) 3.3. Saīsinājumi

— *EUCC*: vienotos kritērijos balstītā Eiropas kiberdrošības sertifikācijas shēma

4) 4.3.3. Process

— 10. PIEZĪME. Norādījumus sk. ETSI EN 319 102-1 [3] un papildu norādījumus attiecībā uz ES kvalificētu parakstu vai zīmogu sk. ETSI TS 119 172-4 [8].

5) 6.1. Parakstu validēšanas pakalpojuma prakses paziņojums

— OVR-6.1-02 *SVS* prakses paziņojums ir strukturēts saskaņā ar A pielikumu.

— OVR-6.1-03 *SVS* prakses paziņojumā uzskaita atbalstīto *SVS* politiku vai atsaucas uz to (piemēram, izmantojot *OID*) un to īsi apraksta.

6) 6.3. Informācijas drošības politika

— OVR-6.3-02 Drošības politika dokumentē drošības un privātuma kontroli, kas īstenota, lai aizsargātu personas datus.

7) 7.2. Cilvēkresursi

— OVR-7.2-02 *SVSP* darbinieki uzticamās lomās un attiecīgā gadījumā tā apakšuzņēmēji uzticamās lomās spēj izpildīt prasību par "ekspertu zināšanām, pieredzi un kvalifikāciju", ko apstiprina formāla apmācība un akreditācija vai pieredze, vai abi minētie.

— OVR-7.2-03 Atbilstība OVR-7.2-02 ietver regulārus (vismaz reizi 12 mēnešos) atjauninājumus par jauniem apdraudējumiem un pašreizējo drošības praksi.

8) 7.5. Kriptogrāfijas kontroles

— OVR-7.5-02 [AR NOSACĪJUMIEM] Kad tiek parakstīti validēšanas ziņojumi, *SVSP* publiskās parakstīšanas sertifikātu, kas atbilst *SVSP* privātajai parakstīšanas atslēgai, izdod uzticama *CA* saskaņā ar *NCP+* sertifikātu politiku, kā noteikts ETSI EN 319 411-1 [12]. Tas jāizdod saskaņā ar attiecīgu sertifikātu politiku, kas noteikta ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [AR NOSACĪJUMIEM] Kad tiek parakstīti validēšanas ziņojumi, *SVSP* privāto atslēgu glabā un izmanto drošas kriptogrāfijas ierīcē, kas ir uzticama sistēma, kura sertificēta saskaņā ar:

a) vienotajiem informācijas tehnoloģiju drošības izvērtēšanas kritērijiem, kā izklāstīts ISO/IEC 15408 [4], vai vienoto informācijas tehnoloģiju drošības izvērtēšanas metodiku (versija CC:2022, 1.–5. daļa), ko publicējuši Vienošanos par kopējo kritēriju sertifikātu atzīšanu IT drošības jomā dalībnieki un kas sertificēti saskaņā ar *EAL* 4 vai augstāka līmeņa *EAL*; vai

b) *EUCC* [7][11] un sertificēta saskaņā ar *EAL* 4 vai augstāku standartu; vai

c) līdz 31.12.2030. FIPS PUB 140-3 [6] 3. līmenis.

Šī sertifikācija attiecas uz drošības mērķi vai aizsardzības profilu, vai moduļa dizainu un drošības dokumentāciju, kas atbilst šā dokumenta prasībām, pamatojoties uz riska analīzi un ņemot vērā fiziskos un citus netehniskos drošības pasākumus.

Ja drošajai kriptogrāfiskajai ierīcei piemēro *EUCC* [7][11] sertifikāciju, šo ierīci konfigurē un izmanto saskaņā ar minēto sertifikāciju.

— OVR-7.5-04 Nav spēkā.

— OVR-7.5-06 *SVSP* parakstīšanas atslēgu eksportē un importē citā drošas kriptogrāfijas ierīcē tikai tad, ja šo eksportu un importu veic droši un saskaņā ar minēto ierīču sertifikāciju.

9) 7.7. Darbības drošība

— OVR-7.7-02 Lai nodrošinātu, ka sistēmas, kurās lietotne ir izstrādāta, piemēro atbilstīgus drošības pasākumus un pielāgojas konkrētām lietojuma vidēm, *SVA* izmanto lietošanas vidi, kas tiek uzturēta ar atjauninātiem drošības labojumiem.

— OVR-7.7-03 Uz *SVA* attiecas šādas prasības, kas noteiktas ETSI TS 119 101 [1] 5.2. punktā: *GSM* 1.3.

10) 7.8. Tīkla drošība

— OVR-7.8-02 Ja ir atļauta attālināta piekļuve sistēmām, kas glabā vai apstrādā konfidenciālus datus, kā daļu no OVR-6.3-02 prasītajiem elementiem pieņem un apraksta oficiālu politiku.

— OVR-7.8-04 Ievainojamības skenēšanu, kas prasīta ETSI EN 319 401 [1] REQ-7.8-13, veic vismaz reizi ceturksnī.

— OVR-7.8-05 Ielaušanās testu, kas prasīts ETSI EN 319 401 [1] REQ-7.8-17X, veic vismaz reizi gadā.

— OVR-7.8-06 Ugunsmūri ir konfigurēti tā, lai novērstu visus tos protokolus un piekļuves, kas nav vajadzīgas *SVSP* darbībai.

11) 7.12. Parakstu validēšanas pakalpojums, kas paredz darbības izbeigšanu un darbības izbeigšanas plānu

— OVR-7.12-02: *TSP* darbības izbeigšanas plāns atbilst prasībām, kas noteiktas īstenošanas aktos, kuri pieņemti saskaņā ar Regulas (ES) Nr. 910/2014 24. panta 5. punktu [i.1].

12) 7.14. Piegādes ķēde

— OVR-7.14-01 Piemēro ETSI EN 319 401 [2] 7.14. punktā noteiktās prasības.

13) 8.1. Paraksta validēšanas process

— VPR-8.1-07 Validēšanas lietojumprogramma (*SVA*) atbilst ETSI TS 119 101 [1], *SIA* 1 līdz *SIA* 4 7.4. punkta prasībām.

— VPR-8.1-11 [AR NOSACĪJUMIEM] Ja *SVS* mērķis ir validēt kvalificētus elektroniskos parakstus vai kvalificētus elektroniskos zīmogus saskaņā ar Regulas (ES) Nr. 910/2014 [i.1] 32. panta 1. punktu (vai attiecīgi 40. pantu), validēšanas procesā ievēro ETSI TS 119 172-4 [8] prasības.

14) 8.2. Paraksta validēšanas protokols

— SVP-8.2-03 Paraksta validēšanas atbildē ir *SVS* politikas *OID*.

15) 8.4. Paraksta validēšanas ziņojums

— SVR-8.4-02 Validēšanas ziņojums atbilst ETSI TS 119 102-2 [9].

— SVR-8.4-07 [AR NOSACĪJUMIEM] Ja *SVS* nav pilnībā apstrādājis paraksta validēšanas politiku, ziņojumā papildus ziņošanai par validētajiem ierobežojumiem ziņo arī par ierobežojumiem, kas nav ņemti vērā vai ir atcelti.

— SVR-8.4-15 Validēšanas ziņojumā skaidri norāda katras *PoE* izcelsmi (no paraksta, klienta, servera).

— SVR-8.4-16 Validēšanas ziņojums ir parakstīts ar validēšanas ziņojuma parakstu, kas ir *SVSP* digitālais paraksts.

— SVR-8.4-17 [AR NOSACĪJUMIEM] Kad tiek parakstīti validēšanas ziņojumi, paraksta formāts un mērķis atbilst ETSI TS 119 102-2 [9].

16) 9. Satvars validēšanas pakalpojumu politikas definēšanai, pamatojoties uz uzticamības pakalpojumu politiku, kas noteikta šajā dokumentā

— OVR-9-05 [AR NOSACĪJUMIEM] Izstrādājot *SVS* politiku uz šajā dokumentā noteiktā uzticamības pakalpojumu politikas pamata, veic riska novērtējumu, lai novērtētu uzņēmējdarbības prasības un noteiktu drošības prasības, kas jāiekļauj politikā attiecībā uz norādīto kopienu un piemērojamību.

— OVR-9-06 [AR NOSACĪJUMIEM] Izstrādājot *SVS* politiku uz šajā dokumentā noteiktā uzticamības pakalpojumu politikas pamata, politiku apstiprina un groza saskaņā ar noteiktu pārskatīšanas procesu, arī atbildību par politikas uzturēšanu.

— OVR-9-07 [AR NOSACĪJUMIEM] Izstrādājot *SVS* politiku uz šajā dokumentā noteiktā uzticamības pakalpojumu politikas pamata, ir jābūt noteiktam pārskatīšanas procesam, lai nodrošinātu, ka politiku atbalsta paziņojumi par praksi.

— OVR-9-08 [AR NOSACĪJUMIEM] Izstrādājot *SVS* politiku uz šajā dokumentā noteiktā uzticamības pakalpojumu politikas pamata, *TPS* dara *TSP* atbalstītās politikas pieejamas savai lietotāju kopienai.

— OVR-9-09 [AR NOSACĪJUMIEM] Izstrādājot *SVS* politiku uz šajā dokumentā noteiktā uzticamības pakalpojumu politikas pamata, abonentiem dara pieejamas *TSP* atbalstītās politikas izmaiņas.

17) B pielikums (normatīvs) *QES* kvalificētais validēšanas pakalpojums, kā noteikts Regulas (ES) Nr. 910/2014 33. pantā

— VPR-B-02 [AR NOSACĪJUMIEM] Ja *SVSP* ir *QSVSP*, izpilde atbilst ETSI TS 119 172-4 [8].

— 2. PIEZĪME. Nav spēkā.

— OVR-B-04 [AR NOSACĪJUMIEM] Ja *SVSP* ir *QSVSP*, OVR-B-03 testos pārbauda dažādus lietošanas gadījumus – pozitīvus un negatīvus.

— VPR-B-11 [AR NOSACĪJUMIEM] Ja *SVSP* ir *QSVSP*, *SVSP* kontrolē jaucējskaitīšanu (vai nu veic skaitīšanu servera pusē, vai kontrolē klientu, ja tas ir atļauts klienta pusē).

— 5. PIEZĪME. Nav spēkā.

— 6. PIEZĪME. Nav spēkā.

— VPR-B-15 [AR NOSACĪJUMIEM] Ja *SVSP* ir *QSVSP*, lai izpildītu VPR-B-13 līdz VPR-B-14 prasības, validēšanas ziņojums atbilst ETSI TS 119 102-2 [9].

— VPR-B-16 [AR NOSACĪJUMIEM] Ja *SVSP* ir *QSVSP*, izpilde atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* [10] piemērotu kriptogrāfijas paņēmienu izmantošanai, sniedzot kvalificētus validēšanas pakalpojumus *QES*.

18) C pielikums (informatīvs) Regulas (ES) Nr. 910/2014 prasību kartēšana, iedaļa "Validēšana saskaņā ar 32. panta 1. punktu", otrā daļa

— Lai nodrošinātu, ka tiek pārbaudīti visi Regulas (ES) Nr. 910/2014 [i.1] 32. panta 1. punktā un 40. pantā paredzētie nosacījumi, ir vajadzīgs pareizs validēšanas algoritms. Tas nodrošina tādu pašu determinētu rezultātu attiecībā uz validēšanai iesniegto parakstu vai zīmogu. Šajā nolūkā izšķiroša nozīme ir parakstu validēšanas politikai. ETSI TS 119 172-4 [8], pamatojoties uz ETSI EN 319 102-1 [3] norādīto validēšanas algoritmu, ir izdots ar šādu perspektīvu.

2. Attiecībā uz ETSI EN 119 172-4

1) 2.1. Normatīvās atsauces

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) "Elektroniskie paraksti un Uzticamības infrastruktūras (*ESI*). Procedūras *AdES* digitālo parakstu izveidei un validēšanai. 1. daļa: Izveide un validēšana".

— Visas atsauces uz "ETSI TS 119 102-1 [1]" saprot kā atsauces uz "ETSI EN 319 102-1 [1]".

— [2] ETSI TS 119 612 V2.3.1 (2024-11) "Elektroniskie paraksti un infrastruktūras (*ESI*); uzticamības saraksti".

— [13] ETSI TS 119 101 V1.1.1 (2016-03) "Elektroniskie paraksti un infrastruktūras (*ESI*); Politikas un drošības prasības attiecībā uz paraksta radīšanas un paraksta validēšanas pieteikumiem".

2) 4.2. Validēšanas ierobežojumi un validēšanas procedūras, REQ-4.2-03 prasība, iedaļa "X.509 validēšanas ierobežojumi", c) punkts:

— i) ja gala subjekta sertifikāts ir uzticamības enkurs, *RevocationCheckingConstraints* neizmanto;

— ii) ja gala subjekta sertifikāts nav uzticamības enkurs, *RevocationCheckingConstraints* iestata uz "*either*Check", kā definēts ETSI TS 119 172-1 [3] A.4.2.1. punkta A.2. tabulas m)2.1. rindā;

— iii) ja gala subjekta sertifikāts ir uzticamības enkurs, ETSI TS 119 172-1 [3] A.4.2.1. punkta A.2. tabulas m)2.2. rindā definēto *RevocationFreshnessConstraints* neizmanto;

— iv) ja gala subjekta sertifikāts nav uzticamības enkurs, ETSI TS 119 172-1 [3] A.4.2.1. punkta A.2. tabulas m)2.2. rindā definēto *RevocationFreshnessConstraints* izmanto ar maksimālo vērtību 24 stundas parakstīšanas sertifikātam. *RevocationFreshnessConstraints* vērtību nenosaka sertifikātiem, kas nav parakstīšanas sertifikāti, ieskaitot sertifikātiem, kas apliecina laika zīmogus.

3) 4.4. Tehniskās piemērojamības (noteikumu) pārbaudes process

— REQ-4.4.2-03 Ja kāda no REQ-4.4.2-01 norādītajām pārbaudēm ir nesekmīga, tad:

a) procesu aptur;

b) parakstu tehniski nosaka kā nenoteiktu, t. i., ne kā ES kvalificētu elektronisko parakstu, ne kā kvalificētu ES elektronisko zīmogu;

c) iepriekš minēto rezultātu un visu starpprocesu procesu rezultātus atspoguļo paraksta piemērojamības noteikumu pārbaudes ziņojumā.