Euroopa Liidu
Teataja

ET
L-seeria

2025/1942

30.9.2025

KOMISJONI RAKENDUSMÄÄRUS (EL) 2025/1942,

29. september 2025,

millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses kvalifitseeritud e-allkirjade kvalifitseeritud valideerimisteenuste ja kvalifitseeritud e-templite kvalifitseeritud valideerimisteenustega

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ, ([1]) eriti selle artikli 33 lõiget 2 ja artiklit 40,

ning arvestades järgmist:

(1) Kvalifitseeritud e-allkirjade ja kvalifitseeritud e-templite kvalifitseeritud valideerimisteenused tagavad vastavalt kvalifitseeritud e-allkirjade ja kvalifitseeritud e-templite valideerimise protsessi ja tulemuste tervikluse, autentsuse ja õigsuse. Neil kvalifitseeritud usaldusteenustel on digitaalses ettevõtluskeskkonnas oluline roll, kuna need edendavad üleminekut traditsioonilistelt paberipõhistelt protsessidelt samaväärsetele elektroonilistele protsessidele.

(2) Määruse (EL) nr 910/2014 artikli 33 lõikes 2 ja artiklis 40 sätestatud eeldust tingimustele vastamise kohta tuleks kohaldada üksnes siis, kui kvalifitseeritud e-allkirjade ja kvalifitseeritud e-templite kvalifitseeritud valideerimisteenused täidavad käesolevas määruses sätestatud standardite nõudeid. Need standardid peaksid kajastama väljakujunenud tavasid ja olema asjaomastes sektorites laialdaselt tunnustatud. Neid tuleks kohandada, et lisada täiendavad kontrollimeetmed, mis tagavad kvalifitseeritud usaldusteenuste turvalisuse ja usaldusväärsuse ja suutlikkuse kontrollida kvalifitseeritud e-allkirjade ja kvalifitseeritud e-templite kvalifitseeritud staatust ja tehnilist kehtivust.

(3) Kui usaldusteenuse osutaja järgib käesoleva määruse lisas sätestatud nõudeid, peaksid järelevalveasutused eeldama, et määruse (EL) nr 910/2014 asjaomased nõuded on täidetud, ning võtma sellist eeldust usaldusteenuse osutajale kvalifitseeritud staatuse andmisel või selle staatuse kinnitamisel nõuetekohaselt arvesse. Kvalifitseeritud usaldusteenuste osutaja võib siiski kasutada muid võimalusi tõendada vastavust määruse (EL) nr 910/2014 nõuetele.

(4) Komisjon hindab regulaarselt uusi tehnoloogialahendusi, tavasid, standardeid ja tehnilisi kirjeldusi. Euroopa Parlamendi ja nõukogu määruse (EL) 2024/1183 ([2]) põhjenduse 75 kohaselt peaks komisjon käesoleva määruse läbi vaatama ja seda vajaduse korral ajakohastama, et tagada selle kooskõla üleilmsete arengusuundumustega ja uute tehnoloogialahenduste, standardite või tehniliste kirjeldustega ning järgida siseturu parimaid tavasid.

([1]) ELT L 257, 28.8.2014, lk 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Euroopa Parlamendi ja nõukogu 11. aprilli 2024. aasta määrus (EL) 2024/1183, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega (ELT L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(5) Isikuandmete selliste töötlemistoimingute suhtes, mis toimuvad käesoleva määruse alusel, kohaldatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2016/679 ([3]) ning vajaduse korral Euroopa Parlamendi ja nõukogu direktiivi 2002/58/EÜ ([4]).

(6) Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([5]) artikli 42 lõikele 1 on konsulteeritud Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse 6. juunil 2025.

(7) Käesoleva määrusega ette nähtud meetmed on kooskõlas määruse (EL) nr 910/2014 artikliga 48 loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Võrdlusstandardid ja kirjeldused

Määruse (EL) nr 910/2014 artikli 33 lõikes 2 ja artiklis 40 osutatud võrdlusstandardid ja kirjeldused on esitatud käesoleva määruse lisas.

Artikkel 2

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 29. september 2025

Komisjoni nimel
president
Ursula VON DER LEYEN

([3]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

LISA

Kvalifitseeritud e-allkirjade kvalifitseeritud valideerimisteenuste ja kvalifitseeritud e-templite kvalifitseeritud valideerimisteenuste võrdlusstandardite ja kirjelduste loetelu

Kohaldatakse standardeid ETSI TS 119 441 V1.2.1 (2023-10) ([1]) (ETSI TS 119 441) ja ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) (ETSI TS 119 172-4) järgmiste kohandustega:

1. ETSI TS 119 441

1) 2.1 Viited normidele

— [1] ETSI TS 119 101 V1.1.1 (2016-03) „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation“.

— [2] ETSI EN 319 401 V3.1.1 (2024-06) „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers“.

— [3] ETSI EN 319 102-1 V1.4.1 (2024-06) „Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation“.

— [4] ISO/IEC 15408-1:2022 – Information security, cybersecurity and privacy protection – Evaluation criteria for IT security.

— [5] kehtetu.

— [6] FIPS PUB 140-3 (2019) „Security Requirements for Cryptographic Modules“.

— [7] Komisjoni rakendusmäärus (EL) 2024/482, ([3]) millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) vastuvõtmisega.

— [8] ETSI TS 119 172-4 V1.1.1 (2021-05) „Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists“.

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) „Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report“.

— [10] Euroopa küberturvalisuse sertifitseerimise rühm, krüptograafia alarühm: „Agreed Cryptographic Mechanisms“, avaldanud Euroopa Liidu Küberturvalisuse Amet (ENISA) ([4]).

— [11] Komisjoni rakendusmäärus (EL) 2024/3144, ([5]) millega muudetakse rakendusmäärust (EL) 2024/4822 kohaldatavate rahvusvaheliste standardite osas ja parandatakse seda rakendusmäärust.

— [12] ETSI EN 319 411-1 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements“

([1]) ETSI TS 119 441 - Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services, V1.2.1 (2023-10).
([2]) ETSI TS 119 172-4 - Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists, V1.1.1 (2021-05).
([3]) ELT 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]) ELT L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2 Informatiivsed viited

— [i.11] kehtetu.

3) 3.3 Lühendid

— EUCC – Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava

4) 4.3.3 Protsess

— MÄRKUS 10 ELi kvalifitseeritud allkirja või templi juhtumi kohta vt suuniseid standardist ETSI EN 319 102-1 [3] ja täiendavaid suuniseid standardist ETSI TS 119 172-4 [8].

5) 6.1 Signatuuri valideerimise teenuse tavade määrang

— OVR-6.1-02 Signatuuri valideerimise teenuse tavade määrang tuleb struktureerida vastavalt lisale A.

— OVR-6.1-03 Signatuuri valideerimise teenuse tavade määrangus tuleb loetleda signatuuri valideerimise teenuse toetatud põhimõtted või esitada viited neile (nt objektiidentifikaatorite kaudu) ja neid lühidalt kirjeldada.

6) 6.3 Infoturvapoliitika

— OVR-6.3-02 Turvapoliitika peab dokumenteerima isikuandmete kaitsmiseks rakendatavad turva- ja privaatsuskontrollimeetmed.

7) 7.2 Personal

— OVR-7.2-02 Signatuuri valideerimise teenuse osutaja usaldusrolle täitvad töötajad ja kui see on asjakohane, tema usaldusrolle täitvad alltöövõtjad peavad suutma täita erialaste teadmiste, kogemuste ja kvalifikatsiooni nõude ametliku koolituse ja tõendite või tegeliku töökogemuse või nende kahe kombinatsiooni kaudu.

— OVR-7.2-03 Nõude OVR-7.2-02 täitmine hõlmab korrapärast ajakohastamist (vähemalt iga 12 kuu järel) uute ohtude ja praeguste turvatavade kohta.

8) 7.5 Krüptograafilised turvameetmed

— OVR-7.5-02 [TINGIMUSLIK] Kui valideerimisaruanded signeeritakse, peab signatuuri valideerimise teenuse osutaja avaliku signeerimissertifikaadi, mis vastab signatuuri valideerimise teenuse osutaja privaatsele signeerimisvõtmele, andma välja usaldusväärne sertifitseerimisasutus kooskõlas laiendatud normaliseeritud sertifitseerimispoliitikaga (NCP+), mis on esitatud standardis ETSI EN 319 411-1 [12]. See tuleks välja anda kooskõlas standardis ETSI EN 319 411-2 [i.17] täpsustatud asjakohase sertifikaadipoliitikaga.

— OVR-7.5-03 [TINGIMUSLIK] Kui valideerimisaruanded signeeritakse, tuleb signatuuri valideerimise teenuse osutaja privaatset signeerimisvõtit hoida ja kasutada turvalises krüptoseadmes, mis on usaldusväärne süsteem, mis on sertifitseeritud kooskõlas järgmiste dokumentidega:

(a) infotehnoloogia turvalisuse hindamise ühiskriteeriumid, mis on kehtestatud standardiga ISO/IEC 15408 [4] või infotehnoloogia turvalisuse hindamise ühiskriteeriumidega, versioon CC:2022, 1.–5. osa, mille on avaldanud IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe osalised ning mis on sertifitseeritud vähemalt EAL 4. tasemel, või

(b) EUCC [7][11] vähemalt EAL 4. tasemel või

(c) kuni 31.12.2030, FIPS PUB 140-3 [6] 3. tase.

See sertifitseerimine peab käsitlema vastavust sellisele turvasihile või kaitseprofiilile või moodulprojektile ja turvadokumentatsioonile, mis vastab käesoleva dokumendi nõuetele, tuginedes riskianalüüsile ning võttes arvesse füüsilisi ja muid mittetehnilisi turbemeetmeid.

Kui turvalisel krüptoseadmel on EUCC [7][11] sertifikaat, siis konfigureeritakse see seade ja seda kasutatakse vastavalt sellele sertifikaadile.

— OVR-7.5-04 kehtetu.

— OVR-7.5-06 Signatuuri valideerimise teenuse osutaja privaatse signeerimisvõtme võib teise turvalisse krüptoseadmesse eksportida ja importida ainult siis, kui selline eksportimine ja importimine toimub turvaliselt ja kooskõlas nende seadmete sertifikaatidega.

9) 7.7 Operatsiooniturve

— OVR-7.7-02 Tagamaks, et rakenduse arendamiseks kasutatavates süsteemides kohaldatakse asjakohaseid turvameetmeid ja et need süsteemid kohanevad konkreetse rakenduse keskkondadega, peab signatuuri valideerimise rakendus kasutama rakenduskeskkonda, mida hooldatakse ajakohaste turvaparandustega.

— OVR-7.7-03 Signatuuri valideerimise rakenduse suhtes kohaldatakse järgmisi standardi ETSI TS 119 101 [1] punktis 5.2 nimetatud nõudeid: GSM 1.3.

10) 7.8 Võrgu turvalisus

— OVR-7.8-02 Kui konfidentsiaalseid andmeid salvestavatele või töötlevatele süsteemidele on lubatud kaugjuurdepääs, tuleb võtta kasutusele ametlik poliitika ja kirjeldada seda nõude OVR-6.3-02 kohaselt nõutavate elementide osana.

— OVR-7.8-04 Standardi ETSI EN 319 401 [1] nõudega REQ-7.8-13 nõutav nõrkuste skaneerimine tuleb teha vähemalt üks kord kvartalis.

— OVR-7.8-05 Standardi ETSI EN 319 401 [1] nõudega REQ-7.8-17X nõutav läbistustest tuleb teha vähemalt üks kord aastas.

— OVR-7.8-06 Tulemüürid tuleb konfigureerida tõrjuma kõiki signatuuri valideerimise teenuse osutaja tegevuseks mittevajalikke protokolle ja juurdepääse.

11) 7.12 Signatuuri valideerimise teenuse osutamise tegevuse lõpetamine ja tegevuse lõpetamise kavad

— OVR-7.12-02 Usaldusteenuse osutaja lõpetamiskava peab vastama nõetele, mis on kehtestatud määruse (EL) nr 910/2014 [i.1] artikli 24 lõike 5 kohaselt vastuvõetud rakendusaktidega.

12) 7.14 Tarneahel

— OVR-7.14-01 Kohaldatakse standardi ETSI EN 319 401 [2] punktis 7.14 nimetatud nõudeid.

13) 8.1 Signatuuri valideerimise protsess

— VPR-8.1-07 Valideerimisrakendus (SVA) peab vastama standardi ETSI TS 119 101 [1] punkti 7.4 nõuetele SIA 1 kuni SIA 4.

— VPR-8.1-11 [TINGIMUSLIK] Kui signatuuri valideerimise teenuse eesmärk on valideerida kvalifitseeritud e-allkirju või kvalifitseeritud e-templeid vastavalt määruse (EL) nr 910/2014 [i.1] artikli 32 lõikele 1 (või artiklile 40), peab valideerimisprotsess järgima standardi ETSI TS 119 172-4 [8] nõudeid.

14) 8.2 Signatuuri valideerimise protokoll

— SVP-8.2-03 Signatuuri valideerimise vastus peab olema varustatud signatuuri valideerimise teenuse poliitika objektiidentifikaatoriga.

15) 8.4 Signatuuri valideerimise aruanne

— SVR-8.4-02 Valideerimisaruanne peab olema kooskõlas standardiga ETSI TS 119 102-2 [9].

— SVR-8.4-07 [TINGIMUSLIK] Kui signatuuri valideerimise teenus ei töötle signatuuri valideerimise poliitikat täielikult, tuleb aruandes lisaks valideeritud kitsenduste kajastamisele kajastada ka kitsendused, mis on kõrvale jäetud või sürjutatud (*overridden*).

— SVR-8.4-15 Valideerimisaruandes peab olema selgelt märgitud iga olemasolutõendi päritolu (signatuurist, kliendilt, serverist).

— SVR-8.4-16 Valideerimisaruanne peab olema varustatud valideerimisaruande signatuuriga, milleks on signatuuri valideerimise teenuse osutaja digisignatuur.

— SVR-8.4-17 [TINGIMUSLIK] Kui valideerimisaruanded signeeritakse, peab signatuuri vorming ja siht olema kooksõlas standardiga ETSI TS 119 102-2 [9].

16) 9 Käesolevas dokumendis määratletud usaldusteenusepoliitikal põhinevate valideerimisteenuse poliitikate määratlemise raamistik:

— OVR-9-05 [TINGIMUSLIK] Kui signatuuri valideerimise teenuse poliitika luuakse käesolevas dokumendis määratletud usaldusteenusepoliitika põhjal, tuleb teha riskihindamine, et hinnata ärinõudeid ja määrata kindlaks turvanõuded, mis tuleb märgitud kogukonna ja kohaldamise jaoks poliitikasse lisada.

— OVR-9-06 [TINGIMUSLIK] Kui signatuuri valideerimise teenuse poliitika luuakse käesolevas dokumendis määratletud usaldusteenusepoliitika põhjal, tuleb poliitika heaks kiita ja poliitikat muuta vastavalt kindlaksmääratud läbivaatamisprotsessile, mis sisaldab poliitika säilitamisega seotud ülesandeid.

— OVR-9-07 [TINGIMUSLIK] Kui signatuuri valideerimise teenuse poliitika luuakse käesolevas dokumendis määratletud usaldusteenusepoliitika põhjal, peab olemas olema määratletud läbivaatamisprotsess, mis tagaks et poliitikat toetavad tavade määrangud.

— OVR-9-08 [TINGIMUSLIK] Kui signatuuri valideerimise teenuse poliitika luuakse käesolevas dokumendis määratletud usaldusteenusepoliitika põhjal, peab usaldusteenuse osutaja tegema usaldusteenuse osutaja toetatavad poliitikad kättesaadavaks oma kasutajakogukonnale.

— OVR-9-09 [TINGIMUSLIK] Kui signatuuri valideerimise teenuse poliitika luuakse käesolevas dokumendis määratletud usaldusteenuse poliitika põhjal, tuleb usaldusteenuse osutaja toetatavate poliitikate läbivaadatud versioonid teha abonentidele kättesaadavaks.

17) Lisa B (normatiivne): Määruse (EL) nr 910/2014 artiklis 33 määratletud kvalifitseeritud e-allkirjade kvalifitseeritud valideerimisteenus

— VPR-B-02 [TINGIMUSLIK] Kui signatuuri valideerimise teenuse osutaja on kvalifitseeritud signatuuri valideerimise teenuse osutaja, peab rakendamine olema kooskõlas standardiga ETSI TS 119 172-4 [8].

— MÄRKUS 2 kehtetu

— OVR-B-04 [TINGIMUSLIK] Kui signatuuri valideerimise teenuse osutaja on kvalifitseeritud signatuuri valideerimise teenuse osutaja, kontrollitakse nõudes OVR-B-03 osutatud testidega erinevaid kasutusjuhte, nii positiivseid kui ka negatiivseid.

— VPR-B-11 [TINGIMUSLIK] Kui signatuuri valideerimise teenuse osutaja on kvalifitseeritud signatuuri valideerimise teenuse osutaja, peab signatuuri valideerimise teenuse osutaja kontrollima räsi arvutamist (kas teostama arvutamise serveri poolel või kontrollima klienti, kui seda on lubatud teha kliendi poolel).

— MÄRKUS 5 kehtetu

— MÄRKUS 6 kehtetu

— VPR-B-15 [TINGIMUSLIK] Kui signatuuri valideerimise teenuse osutaja on kvalifitseeritud signatuuri valideerimise teenuse osutaja, peab valideerimisauranne olema nõuete VPR-B-13 kuni VPR-B-14 täitmiseks kooskõlas standardiga ETSI TS 119 102-2 [9].

— VPR-B-16 [TINGIMUSLIK] Kui signatuuri valideerimise teenuse osutaja on kvalifitseeritud signatuuri valideerimise teenuse osutaja, peab rakendamine toimuma kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“[10] seoses sobivate krüptomeetodite kasutamisega kvalifitseeritud e-signatuuri valideerimiseks kvalifitseeritud teenuste osutamisel.

18) Lisa C (informatiivne) Nõuete vastendamine määrusega (EL) nr 910/2014, jaotis pealkirjaga „Valideerimine vastavalt artikli 32 lõikele 1“, teine lõik:

— Tagamaks, et kontrollitakse kõiki määruse (EL) nr 910/2014 [i.1] artikli 32 lõike 1 ja artikli 40 kohaselt nõutavaid tingimusi, on vaja õiget valideerimisalgoritmi. See annab valideerimiseks esitatud allkirja või pitseri kohta sama deterministliku tulemuse. Signatuuri valideerimise poliitika on sellest seisukohast otsustava tähtsusega. Standardis ETSI EN 319 102-1 [3] nimetatud valideerimisalgoritmil põhinev standard ETSI TS 119 172-4 [8] on välja antud seda silmas pidades.

2. ETSI TS 119 172-4

1) 2.1 Viited normidele

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) „Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation“.

— Kõiki viiteid standardile ETSI TS 119 102-1 [1] käsitatakse viidetena standardile „ETSI EN 319 102-1 [1]“.

— [2] ETSI TS 119 612 V2.3.1 (2024-11) „Electronic Signatures and Infrastructures (ESI); Trusted Lists“.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation“.

2) 4.2 Valideerimispiirangud ja valideerimisprotseduurid, nõue REQ-4.2-03, jaotis „X.509 valideerimispiirangud’, punkt c:

— i) Kui lõppolemi sertifikaat kujutab endast usaldusankrut, ei kasutata parameetrit RevocationChecking-Constraints.

— ii) Kui lõppolemi sertifikaat ei kujuta endast usaldusankrut, määratakse parameetri RevocationChecking-Constraints väärtuseks „eitherCheck“, mis on määratletud standardi ETSI TS 119 172-1 [3] punkti A.4.2.1 tabeli A.2 reas (m)2.1.

— iii) Kui lõppolemi sertifikaat kujutab endast usaldusankrut, ei kasutata parameetrit RevocationFreshness-Constraints, mis on määratletud standardi ETSI TS 119 172-1 [3] punkti A.4.2.1 tabeli A.2 reas (m)2.2.

— iv) Kui lõppolemi sertifikaat ei kujuta endast usaldusankrut, kasutatakse signeerimissertifikaadi jaoks standardi ETSI TS 119 172-1 [3] punkti A.4.2.1 tabeli A.2 reas (m)2.2 määratletud parameetrit RevocationFreshnessConstraints maksimumväärtusega 24 tundi. Parameetrile RevocationFreshness-Constraints ei määrata väärtust muude sertifikaatide puhul peale signeerimissertifikaadi, sealhulgas ajatempleid toetavate sertifikaatide puhul.

3) 4.4 Tehnilise kohaldatavuse (eeskirjade) kontrollimise protsess

— REQ-4.4.2-03 Kui mõni nõudes REQ-4.4.2-01 nimetatud kontrollidest ebaõnnestub, siis:

(a) protsess seiskub;

(b) loetakse signatuur tehniliselt määramatuks, st seda ei peeta ei ELi kvalifitseeritud e-allkirjaks ega ELi kvalifitseeritud e-templiks;

(c) eespool nimetatud tulemus ja kõigi vaheprotsesside protsesside tulemusi kajastatakse signatuuri kohaldatavuseeskirjade kontrollimise aruandes.