2025/1943

30.9.2025

KOMISJONI RAKENDUSMÄÄRUS (EL) 2025/1943,

29. september 2025,

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

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 28 lõiget 6 ja artikli 38 lõiget 6,

ning arvestades järgmist:

(1) E-allkirjade kvalifitseeritud sertifikaatidel ja e-templi kvalifitseeritud sertifikaatidel on digiettevõtluse kontekstis oluline roll, kuna need edendavad üleminekut traditsioonilistelt paberipõhistelt protsessidelt samaväärsetele elektroonilistele protsessidele. Kvalifitseeritud sertifikaadid annavad suurema kindlustunde allkirja andja või e-templi looja identiteedi suhtes tänu e-allkirja valideerimisandmete ja e-templi valideerimisandmete sidumisele vastavalt kas füüsilise või juriidilise isikuga ja tänu selle isiku nime kinnitamisele.

(2) Määruse (EL) nr 910/2014 artikli 28 lõikes 6 ja artikli 38 lõikes 6 sätestatud eeldust tingimustele vastamise kohta tuleks kohaldada üksnes siis, kui e-allkirjade kvalifitseeritud sertifikaatide väljaandmiseks kvalifitseeritud usaldusteenus ja e-templi kvalifitseeritud sertifikaatide väljaandmiseks kvalifitseeritud usaldusteenus 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 ja kvalifitseeritud sertifikaatide sisu turvalisuse ja usaldusväärsuse.

(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.

(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]).

([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).

([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).

(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

E-allkirjade ja e-templite kvalifitseeritud sertifikaatide võrdlusstandardid ja kirjeldused

1. Määruse (EL) nr 910/2014 artikli 28 lõikes 6 osutatud võrdlusstandardid ja kirjeldused on esitatud käesoleva määruse I lisas.

2. Määruse (EL) nr 910/2014 artikli 38 lõikes 6 osutatud võrdlusstandardid ja kirjeldused on esitatud käesoleva määruse II 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

([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).

I LISA

E-allkirjade kvalifitseeritud sertifikaatide võrdlusstandardite ja kirjelduste loetelu

Standardeid ETSI EN 319 411-2 V2.6.1 (ETSI EN 319 411-2), ETSI EN 319 412-1 V1.6.1 (ETSI EN 319 412-1), ETSI EN 319 412-2 V2.4.1 (ETSI EN 319 412-2) ja ETSI EN 319 412-5 V2.5.1 (ETSI EN 319 412-5) kohaldatakse järgmiste kohandustega:

1. ETSI EN 319 411-2

(1) 2.1 Viited normidele

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

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements“, järgmiste kohandustega:

Standardi ETSI EN 319 411-1 V1.5.1 jaotist 2.1 „Normative references“ („Normatiivsed viited“) muudetakse järgmiselt:

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

— [10] ETSI EN 319 412-2 V2.4.1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons“.

— [14] ETSI EN 319 412-1 V1.6.1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures“.

— [3] ETSI EN 319 412-5 V2.5.1 „Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements“.

— [5] ETSI EN 319 412-1 V1.6.1 „Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures“.

— [6] CEN/TS 419261:2015 „Security requirements for trustworthy systems managing certificates and time-stamps“.

— [7] Euroopa küberturvalisuse sertifitseerimise rühm, krüptograafia alarühm: „Agreed Cryptographic Mechanisms“, avaldanud Euroopa Liidu Küberturvalisuse Amet (ENISA) ([1]).

— [8] Komisjoni rakendusmäärus (EL) 2024/482, ([2]) millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) vastuvõtmisega,

— [9] Komisjoni rakendusmäärus (EL) 2024/3144, ([3]) millega muudetakse rakendusmäärust (EL) 2024/482 kohaldatavate rahvusvaheliste standardite osas ja parandatakse seda rakendusmäärust.

— [10] ISO/IEC 15408:2022 (1.–5. osa): „Information security, cybersecurity and privacy protection – Evaluation criteria for IT security“.

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

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

(2) 5.2 Sertifitseerimistava määrangu nõuded

— OVR-5.2-02 Kasutatavatele sertifikaadiprofiilidele esitatavad nõuded määratakse kindlaks usaldusteenuse osutaja dokumentides nimetatud sertifitseerimispoliitika(te)s.

(3) 5.3 Sertifitseerimispoliitika nimi ja identifitseerimine

— OVR-5.3-01 Kui sertifitseerimispoliitikat muudetakse punktis 4.2.2 kirjeldatud viisil ning see mõjutab kohaldatavust, tuleb muuta poliitika identifikaatorit.

(4) 6.1 Avaldamine ja hoidla kohustused

— OVR-6.1-02 Standardi ETSI EN 319 411-1 [2] nõudes DIS-6.1-04 nimetatud teave peab olema avalikult ja rahvusvaheliselt kättesaadav.

(5) 6.2.2 Identiteedi esmane valideerimine

— REG-6.2.2-01A Atribuutide ja tõendite kogumine subjekti identiteedi kohta ning nende valideerimine toimub nii, nagu on ette nähtud määruse (EL) nr 910/2014 [i.1] artikli 24 lõike 1c kohaselt vastuvõetud rakendusaktidega.

— REG-6.2.2-02 [QCP-n] ja [QCP-n-qscd] Füüsilise isiku identiteeti ja vajaduse korral selle isiku konkreetseid atribuute kontrollitakse vastavalt määruse (EL) nr 910/2014 [i.1] artikli 24 lõike 1c kohaselt vastuvõetud rakendusaktidele.

— MÄRKUS 1 kehtetu

(6) 6.3.3 Sertifikaadi väljaandmine

— GEN-6.3.3-01 Kohaldatakse standardi ETSI EN 319 411-1 [2] punktis 6.3.3 nimetatud nõudeid GEN-6.3.3-01 kuni GEN-6.3.3-10.

— GEN-6.3.3-02 [TINGIMUSLIK] Kui sertifikaat antakse välja füüsilisele isikule, kes identifitseeritakse seoses juriidilise isikuga, peavad subjektiatribuudid, millega identifitseeritakse sertifikaadis organisatsioon, esindama seda juriidilist isikut või selle juriidilise isiku allüksust ning sertifikaadi subjektiidentifikaator füüsilist isikut.

— GEN-6.3.3-03 Sertifitseerimispoliitika identifikaator on [VALIK]

(a) [QCP-n]

— nagu on ette nähtud punkti 5.3 alapunktiga a ja/või

— objekti identifikaator, mille on määranud usaldusteenuse osutaja või muu asjaomane sidusrühm, või täiendav standardimine sellise sertifitseerimispoliitika jaoks, mis täiendab vastavaid kohaldatavaid poliitikanõudeid, mis on määratletud käesolevas dokumendis.

(b) [QCP-n-qscd]

— nagu on ette nähtud punkti 5.3 alapunktiga c ja/või

— objekti identifikaator, mille on määranud usaldusteenuse osutaja või muu asjaomane sidusrühm, või täiendav standardimine sellise sertifitseerimispoliitika jaoks, mis täiendab vastavaid kohaldatavaid poliitikanõudeid, mis on määratletud käesolevas dokumendis.

(7) 6.3.5 Võtmepaari ja sertifikaadi kasutamine

— SDP-6.3.5-02A [TINGIMUSLIK] Kui usaldusteenuse osutaja haldab subjekti jaoks kvalifitseeritud e-allkirja andmise vahendit, peab usaldusteenuse osutaja olema kvalifitseeritud usaldusteenuse osutaja, kes osutab kvalifitseeritud usaldusteenust kvalifitseeritud e-allkirja kaugloomise vahendi haldamiseks kooskõlas määrusega (EL) nr 910/2014 [i.1].

— SDP-6.3.5-11A Kui abonent või subjekt genereerib subjekti võtmed, hõlmavad abonendi kohustused (vt punkt 6.3.4) järgmist:

(a) kohustus genereerida subjektivõtmed, kasutades algoritmi, mis on kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [7] sertifitseeritud võtme kasutamiseks nii, nagu sertifitseerimispoliitikas märgitud;

(b) kohustus kasutada võtmepikkust ja algoritmi, mis on kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [7] sertifitseeritud võtme kasutamiseks sertifikaadi kehtivuse jooksul nii, nagu sertifitseerimispoliitikas märgitud.

(8) 6.3.10 Sertifikaadi staatuse teenused

— CSS-6.3.10-08 [TINGIMUSLIK] Kui pakutakse tühistatud sertifikaatide loendeid, säilitab usaldusteenuse osutaja viimase tühistatud sertifikaatide loendi tervikluse ja käideldavuse vähemalt sertifitseerimistava määrangus sätestatud aja jooksul, vastavalt nõudele CSS-6.3.10-12.

(9) 6.4.4 Töötajate kontroll

— OVR-6.4.4-02 Usaldusteenuse 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-6.4.4-03 Nõude OVR-6.4.4-02 täitmine hõlmab korrapärast (vähemalt iga 12 kuu järel) ajakohastamist uute ohtude ja praeguste turvatavade kohta.

— OVR-6.4.4-04 Lisaks standardis ETSI EN 319 401 [1] (punkt 7.2-15) nimetatud usaldusrollidele toetatakse dokumendis TS 419261 [6] määratletud ülesannetega registreerimis- ja tühistamisametnike usaldusrolle. Kui kvalifitseeritud usaldusteenuse osutajat juhib otseselt liikmesriik või avaliku sektori asutus või käitatakse seda tema nimel, võib neid täiendavaid usaldusrolle täita üks või mitu ametlikku esindajat, kes tegutsevad kohalikes või piirkondlikes omavalitsustes töötavate registreerimis- ja tühistamisametnike eest või nimel.

(10) 6.4.9 Sertifitseerimisasutuse või registreerimisasutuse lõpetamine

— OVR-6.4.9-02 Usaldusteenuse osutaja lõpetamiskava peab vastama nõetele, mis on kehtestatud määruse (EL) nr 910/2014 [i.1] artikli 24 lõike 5 kohaselt vastuvõetud rakendusaktidega.

(11) 6.5.1 Võtmepaari genereerimine ja paigaldamine

— OVR-6.5.1-01A Sertifitseerimisasutuse võtmepaari genereerimiseks tuleb kasutada algoritmi, mis on kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [7] sertifitseerimisasutuse signeerimisotstarbe osas.

— OVR-6.5.1-01B Sertifitseerimisasutuse signatuurivõtme valitud võtmepikkus ja algoritm peavad olema kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [7] sertifitseerimisasutuse signeerimisotstarbe osas.

— OVR-6.5.1-01C [TINGIMUSLIK] Kui sertifitseerimisasutus genereerib subjekti võtmed, peavad sertifitseerimisasutuse genereeritud subjektivõtmed olema sertifikaadi kehtivuse jooksul kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [7] sertifitseerimispoliitikas märgitud otstarbe osas.

(12) 6.5.2 Privaatvõtme kaitsmine ja krüptomooduli tehnilised turvameetmed

— GEN-6.5.2-01 Kohaldatakse kõiki standardi ETSI EN 319 411-1 [2] punktis 6.5.2 nimetatud nõudeid, välja arvatud nõuded OVR-6.5.2-01, OVR-6.5.2-03 ja OVR-6.5.2-04.

— GEN-6.5.2-02 Usaldusteenuse osutaja võtmepaari genereerimine, kaasa arvatud selliste võtmete genereerimine, mida kasutavad tühistamis- ja registreerimisteenused, peab toimuma turvalises krüptoseadmes, mis on usaldusväärne süsteem, mis on sertifitseeritud kooskõlas järgmiste dokumentidega:

— infotehnoloogia turvalisuse hindamise ühiskriteeriumid, mis on kehtestatud standardiga ISO/IEC 15408 [10] või infotehnoloogia turvalisuse hindamise ühiskriteeriumidega, versioon CC:2002, 1.–5. osa, mille on avaldanud IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe osalised ning mis on sertifitseeritud vähemalt EAL 4. tasemel, või

— Euroopa ühiskriteeriumidel põhinev küberturvalisuse sertifitseerimise kava (EUCC) [8][9] ning mis on sertifitseeritud vähemalt EAL 4. tasemel või

— kuni 31.12.2030, FIPS PUB 140-3 [11] 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 [8][9] sertifikaat, siis konfigureeritakse see seade ja seda kasutatakse vastavalt kõnealusele sertifikaadile.

— GEN-6.5.2-03 Sertifitseerimisasutuse signeerimiseks kasutatavat privaatvõtit tuleb hoida ja kasutada turvalises krüptoseadmes, mis vastab nõuetele GEN-6.5.2-01 ja GEN-6.5.2-02.

(13) 6.5.7 Võrguturbemeetmed

— OVR-6.5.7-02 Standardi ETSI EN 319 401 [1] nõudega REQ-7.8-13 nõutav nõrkuste skaneerimine tuleb teha vähemalt üks kord kvartalis.

— OVR-6.5.7-03 Standardi ETSI EN 319 401 [1] nõudega REQ-7.8-17X nõutav läbistustest tuleb teha vähemalt üks kord aastas.

— OVR-6.5.7-04 Tulemüürid tuleb konfigureerida tõrjuma kõiki usaldusteenuse osutaja tegevuseks mittevajalikke protokolle ja juurdepääse.

(14) 6.6.1 Sertifikaadi profiil

— GEN-6.6.1-05 Sertifikaat peab sisaldama üht nõudes GEN-6.3.3-03 [VALIK] nimetatud poliitikaidentifikaatorit. Sertifikaat võib sisaldada muid usaldusteenuse osutaja määratud objekti identifikaatoreid.

2. ETSI EN 319 412-2

(1) 2.1 Viited normidele

— [2] ETSI EN 319 412-5 V2.5.1 „Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements“.

— [9] Euroopa küberturvalisuse sertifitseerimise rühm, krüptograafia alarühm „Agreed Cryptographic Mechanisms“, avaldaja ENISA.

(2) 4.2.2 Allkiri

— GEN-4.2.2-2 Signatuuri algoritm tuleb valida kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [9].

— MÄRKUS kehtetu.

(3) 4.2.3.1 Juriidilisest isikust väljaandjad

— GEN-4.2.3.1-3 Kui teadaolevalt on olemas asjakohane registreerimisnumber, peab väljaandja identiteet sisaldama atribuuti „organizationIdentifier“, milles kõnealuse registreerimisnumbri väärtus on sama nagu registreerimisnumbri kehtestanud vastavas ametlikus dokumendis märgitud.

(4) 4.2.5 Subjekti avaliku võtme teave

— GEN-4.2.5-2 Subjekti avalik võti tuleb valida kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [9].

— MÄRKUS kehtetu.

(5) 4.2.6 Seerianumber

— GEN-4.2.6-01 Igal sertifikaadil, mille usaldusteenuse osutaja välja annab, peab olema kordumatu sertifikaadi seerianumber (nagu on ette nähtud IETF RFC 5280 [1] punktiga 4.1.2.2).

II LISA

E-templite kvalifitseeritud sertifikaatide võrdlusstandardite ja kirjelduste loetelu

Standardeid ETSI EN 319 411-2 V2.6.1 (ETSI EN 319 411-2), ETSI EN 319 412-1 V1.6.1 (ETSI EN 319 412-1), ETSI EN 319 412-3 V1.3.1 (ETSI EN 319 412-3), ETSI EN 319 412-2 V2.4.1 (ETSI EN 319 412-2) ja ETSI EN 319 412-5 V2.5.1 (ETSI EN 319 412-5) kohaldatakse järgmiste kohandustega:

1. ETSI EN 319 411-2

(1) 2.1 Viited normidele

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

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements“, järgmiste kohandustega:

Standardi ETSI EN 319 411-1 V1.5.1 jaotist 2.1 „Normative references“ („Normatiivsed viited“) muudetakse järgmiselt:

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

— [10] ETSI EN 319 412-2 V2.4.1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons“.

— [14] ETSI EN 319 412-1 V1.6.1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures“.

— [3] ETSI EN 319 412-5 V2.5.1 „Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements“.

— [5] ETSI EN 319 412-1 V1.6.1 „Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures“.

— [6] CEN/TS 419261:2015 „Security requirements for trustworthy systems managing certificates and time-stamps“ (koostaja CEN).

— [7] Euroopa küberturvalisuse sertifitseerimise rühm, krüptograafia alarühm: „Agreed Cryptographic Mechanisms“ avaldanud ENISA.

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

— [9] Rakendusmäärus (EL) 2024/3144, millega muudetakse rakendusmäärust (EL) 2024/482 kohaldatavate rahvusvaheliste standardite osas ja parandatakse seda rakendusmäärust.

— [10] ISO/IEC 15408:2022 (1.–5. osa) „Information security, cybersecurity and privacy protection – Evaluation criteria for IT security“.

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

(2) 5.2 Sertifitseerimistava määrangu nõuded

— OVR-5.2-02 Kasutatavatele sertifikaadiprofiilidele esitatavad nõuded määratakse kindlaks usaldusteenuse osutaja dokumentides nimetatud sertifitseerimispoliitika(te)s.

(3) 5.3 Sertifitseerimispoliitika nimi ja identifitseerimine

— OVR-5.3-01 Kui sertifitseerimispoliitikat muudetakse punktis 4.2.2 kirjeldatud viisil ning see mõjutab kohaldatavust, tuleb muuta poliitika identifikaatorit.

(4) 6.1 Avaldamine ja hoidla kohustused

— OVR-6.1-02 Standardi ETSI EN 319 411-1 [2] nõudes DIS-6.1-04 nimetatud teave peab olema avalikult ja rahvusvaheliselt kättesaadav.

(5) 6.2.2 Identiteedi esmane valideerimine

— REG-6.2.2-01A Atribuutide ja tõendite kogumine subjekti identiteedi kohta ning nende valideerimine toimub nii, nagu on ette nähtud määruse (EL) nr 910/2014 [i.1] artikli 24 lõike 1c kohaselt vastuvõetud rakendusaktidega.

— REG-6.2.2-03 [QCP-l] ja [QCP-l-qscd] Juriidilise isiku identiteeti ja vajaduse korral selle isiku konkreetseid atribuute kontrollitakse vastavalt määruse (EL) nr 910/2014 [i.1] artikli 24 lõike 1c kohaselt vastuvõetud rakendusaktidele.

— MÄRKUS 3 Vt märkus 2.

(6) 6.3.3 Sertifikaadi väljaandmine

— GEN-6.3.3-01 Kohaldatakse standardi ETSI EN 319 411-1 [2] punktis 6.3.3 nimetatud nõudeid GEN-6.3.3-01 kuni GEN-6.3.3-10.

— GEN-6.3.3-02 Sertifitseerimispoliitika identifikaator on [VALIK]

(a) [QCP-l]

— nagu on ette nähtud punkti 5.3 alapunktiga b ja/või

— objekti identifikaator, mille on määranud usaldusteenuse osutaja või muu asjaomane sidusrühm, või täiendav standardimine sellise sertifitseerimispoliitika jaoks, mis täiendab vastavaid kohaldatavaid poliitikanõudeid, mis on määratletud käesolevas dokumendis.

(b) [QCP-l-qscd]

— nagu on ette nähtud punkti 5.3 alapunktiga d ja/või

— objekti identifikaator, mille on määranud usaldusteenuse osutaja, muu asjaomane sidusrühm või täiendav standardimine sellise sertifitseerimispoliitika jaoks, mis täiendab kohaldatavaid poliitikanõudeid, mis on määratletud käesolevas dokumendis.

(7) 6.3.5 Võtmepaari ja sertifikaadi kasutamine

— SDP-6.3.5-02A [TINGIMUSLIK] Kui usaldusteenuse osutaja haldab subjekti jaoks kvalifitseeritud e-allkirja andmise vahendit, peab usaldusteenuse osutaja olema kvalifitseeritud usaldusteenuse osutaja, kes osutab kvalifitseeritud usaldusteenust kvalifitseeritud e-templi kaugloomise vahendi haldamiseks kooskõlas määrusega (EL) nr 910/2014 [i.1].

— SDP-6.3.5-11A Kui abonent või subjekt genereerib subjekti võtmed, hõlmavad abonendi kohustused (vt punkt 6.3.4) järgmist:

(a) kohustus genereerida subjektivõtmed, kasutades algoritmi, mis on kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [7] sertifitseeritud võtme kasutamiseks nii, nagu sertifitseerimispoliitikas märgitud, ja

(b) kohustus kasutada võtmepikkust ja algoritmi, mis on kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [7] sertifitseeritud võtme kasutamiseks sertifikaadi kehtivuse jooksul nii, nagu sertifitseerimispoliitikas märgitud.

(8) 6.3.10 Sertifikaadi staatuse teenused

— CSS-6.3.10-08 [TINGIMUSLIK] Kui pakutakse tühistatud sertifikaatide loendeid, säilitab usaldusteenuse osutaja viimase tühistatud sertifikaatide loendi tervikluse ja käideldavuse vähemalt sertifitseerimistava määrangus sätestatud aja jooksul, vastavalt nõudele CSS-6.3.10-12.

(9) 6.4.4 Töötajate kontroll

— OVR-6.4.4-02 Usaldusteenuse 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-6.4.4-03 Nõude OVR-6.4.4-02 täitmine hõlmab korrapärast (vähemalt iga 12 kuu järel) ajakohastamist uute ohtude ja praeguste turvatavade kohta.

— OVR-6.4.4-04 Lisaks standardis ETSI EN 319 401 [1] (punkt 7.2-15) nimetatud usaldusrollidele toetatakse dokumendis TS 419261 [6] määratletud ülesannetega registreerimis- ja tühistamisametnike usaldusrolle. Kui kvalifitseeritud usaldusteenuse osutajat juhib otseselt liikmesriik või avaliku sektori asutus või käitatakse seda tema nimel, võib neid täiendavaid usaldusrolle täita üks või mitu ametlikku esindajat, kes tegutsevad kohalikes või piirkondlikes omavalitsustes töötavate registreerimis- ja tühistamisametnike eest või nimel.

(10) 6.4.9 Sertifitseerimisasutuse või registreerimisasutuse lõpetamine

— OVR-6.4.9-02 Usaldusteenuse osutaja tegevuse lõpetamise kava peab vastama nõetele, mis on kehtestatud määruse (EL) nr 910/2014 [i.1] artikli 24 lõike 5 kohaselt vastuvõetud rakendusaktidega.

(11) 6.5.1 Võtmepaari genereerimine ja paigaldamine

— OVR-6.5.1-01A Sertifitseerimisasutuse võtmepaari genereerimiseks kasutatakse algoritmi, mis on kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [7] sertifitseerimisasutuse signeerimisotstarbe osas.

— OVR-6.5.1-01B Sertifitseerimisasutuse signatuurivõtme valitud võtmepikkus ja algoritm peavad olema kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [7] sertifitseerimisasutuse signeerimisotstarbe osas.

— OVR-6.5.1-01C [TINGIMUSLIK] Kui sertifitseerimisasutus genereerib subjekti võtmed, peavad sertifitseerimisasutuse genereeritud subjektivõtmed olema sertifikaadi kehtivuse jooksul kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [7] sertifitseerimispoliitikas märgitud otstarbe osas.

(12) 6.5.2 Privaatvõtme kaitsmine ja krüptomooduli tehnilised turvameetmed

— GEN-6.5.2-01 Kohaldatakse kõiki standardi ETSI EN 319 411-1 [2] punktis 6.5.2 nimetatud nõudeid, välja arvatud nõuded OVR-6.5.2-01, OVR-6.5.2-03 ja OVR-6.5.2-04.

— GEN-6.5.2-02 Usaldusteenuse osutaja võtmepaari genereerimine, kaasa arvatud selliste võtmete genereerimine, mida kasutavad tühistamis- ja registreerimisteenused, peab toimuma turvalises krüptoseadmes, mis on usaldusväärne süsteem, mis on sertifitseeritud kooskõlas järgmiste dokumentidega:

  — infotehnoloogia turvalisuse hindamise ühiskriteeriumid, mis on kehtestatud standardiga ISO/IEC 15408 [10] või infotehnoloogia turvalisuse hindamise ühiskriteeriumidega, versioon CC:2002, 1.–5. osa, mille on avaldanud IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe osalised ning mis on sertifitseeritud vähemalt EAL 4. tasemel, või

  — Euroopa ühiskriteeriumidel põhinev küberturvalisuse sertifitseerimise kava (EUCC) [8][9] ning mis on sertifitseeritud vähemalt EAL 4. tasemel või

  — kuni 31.12.2030, FIPS PUB 140-3 [11] 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 [8][9] sertifikaat, siis konfigureeritakse see seade ja seda kasutatakse vastavalt kõnealusele sertifikaadile.

— GEN-6.5.2-03 Sertifitseerimisasutuse signeerimiseks kasutatavat privaatvõtit tuleb hoida ja kasutada turvalises krüptoseadmes, mis vastab nõuetele GEN-6.5.2-01 ja GEN-6.5.2-02.

(13) 6.5.7 Võrguturbemeetmed

— OVR-6.5.7-02 Standardi ETSI EN 319 401 [1] nõudega REQ-7.8-13 nõutav nõrkuste skaneerimine tuleb teha vähemalt üks kord kvartalis.

— OVR-6.5.7-03 Standardi ETSI EN 319 401 [1] nõudega REQ-7.8-17X nõutav läbistustest tuleb teha vähemalt üks kord aastas.

— OVR-6.5.7-04 Tulemüürid tuleb konfigureerida tõrjuma kõiki usaldusteenuse osutaja tegevuseks mittevajalikke protokolle ja juurdepääse.

(14) 6.6.1 Sertifikaadi profiil

— GEN-6.6.1-05 Sertifikaat peab sisaldama üht nõudes GEN-6.3.3-02 [VALIK] nimetatud poliitikaidentifikaatorit.

2. ETSI EN 319 412-3

(1) 2.1 Viited normidele

— [2] ETSI EN 319 412-2 V2.4.1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons“.

(2) 4.2.1 Subjekt

— LEG-4.2.1-6 Atribuut „organizationIdentifier“ peab sisaldama subjektorganisatsiooni identifikaatorit, mis erineb organisatsiooni nimest. Kui teadaolevalt on olemas asjakohane registreerimisnumber, peab atribuut „organizationIdentifier“ sisaldama kõnealuse registreerimisnumbri väärtust sellisena, nagu registreerimisnumbri kehtestanud vastavas ametlikus dokumendis märgitud.

3. ETSI EN 319 412-2:

(1) 2.1 Viited normidele

— [2] ETSI EN 319 412-5 V2.5.1 „Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements“.

— [9] Euroopa küberturvalisuse sertifitseerimise rühm, krüptograafia alarühm: „Agreed Cryptographic Mechanisms“ avaldanud ENISA.

(2) 2.2 Informatiivsed viited

— [i.7] kehtetu.

(3) 4.2.2 Allkiri

— GEN-4.2.2-2 Signatuuri algoritm tuleb valida kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [9].

— MÄRKUS kehtetu.

(4) 4.2.3.1 Juriidilisest isikust väljaandjad

— GEN-4.2.3.1-3 Kui teadaolevalt on olemas asjakohane registreerimisnumber, peab väljaandja identiteet sisaldama atribuuti „organizationIdentifier“, milles kõnealuse registreerimisnumbri väärtus on sama nagu registreerimisnumbri kehtestanud vastavas ametlikus dokumendis märgitud.

(5) 4.2.5 Subjekti avaliku võtme teave

— GEN-4.2.5-2 Subjekti avalik võti tuleb valida kooskõlas Euroopa küberturvalisuse sertifitseerimise rühma kinnitatud ja ENISA avaldatud dokumendiga „Agreed Cryptographic Mechanisms“ [9].

— MÄRKUS kehtetu.

(6) 4.2.6 Seerianumber

— GEN-4.2.6-01 Igal sertifikaadil, mille usaldusteenuse osutaja välja annab, peab olema kordumatu sertifikaadi seerianumber (nagu on ette nähtud IETF RFC 5280 [1] punktiga 4.1.2.2).