Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/1943

30.9.2025.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/1943

(2025. gada 29. septembris),

kas nosaka Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 piemērošanu kvalificētu elektronisko parakstu sertifikātu un kvalificētu elektronisko zīmogu sertifikātu atsauces standartiem

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 28. panta 6. punktu un 38. panta 6. punktu,

tā kā:

(1) Kvalificētiem elektronisko parakstu sertifikātiem un kvalificētiem elektronisko zīmogu sertifikātiem ir izšķiroša nozīme digitālajā uzņēmējdarbības vidē, jo tie veicina pāreju no tradicionāliem papīra formāta procesiem uz līdzvērtīgiem elektroniskiem procesiem. Sasaistot elektroniskā paraksta validācijas datus vai elektroniskā zīmoga validācijas datus attiecīgi ar fizisku vai juridisku personu un apstiprinot minētās personas vārdu un uzvārdu, kvalificēti sertifikāti uzlabo noteiktību attiecībā uz parakstītāja un zīmoga radītāja identitāti.

(2) Regulas (ES) Nr. 910/2014 28. panta 6. punktā un 38. panta 6. punktā paredzētais pieņēmums par noteikumu ievērošanu būtu jāpiemēro tikai tad, ja kvalificēti uzticamības pakalpojumi kvalificētu elektronisko parakstu sertifikātu izdošanai un kvalificēti uzticamības pakalpojumi kvalificētu elektronisko zīmogu sertifikātu izdošanai atbilst šajā regulā noteiktajiem standartiem. Šiem standartiem būtu jāatspoguļo iedibinātā prakse un jābūt plaši atzītiem attiecīgajās nozarēs. Tie būtu jāpielāgo, lai iekļautu papildu kontroles, kas nodrošina kvalificēto uzticamības pakalpojumu un kvalificēto sertifikātu satura drošību un uzticamību.

(3) Ja uzticamības pakalpojumu sniedzējs ievēro šīs regulas pielikumā noteiktās prasības, uzraudzības iestādēm būtu jāpieņem, ka ir ievērotas attiecīgās Regulas (ES) Nr. 910/2014 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 vai 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 vai tehniskajām specifikācijām un tajā būtu ņemta vērā paraugprakse iekšējā tirgū.

(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]).

([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).
([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).

(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 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

Kvalificētu elektronisko parakstu un elektronisko zīmogu sertifikātu atsauces standarti un specifikācijas

1. Regulas (ES) Nr. 910/2014 28. panta 6. punktā minētie atsauces standarti un specifikācijas ir izklāstītas šīs regulas I pielikumā.

2. Regulas (ES) Nr. 910/2014 38. panta 6. punktā minētie atsauces standarti un specifikācijas ir izklāstītas šīs regulas II 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

([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).

I PIELIKUMS

Kvalificētu elektronisko parakstu sertifikātu atsauces standartu un specifikāciju saraksts

Standartus 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”) un ETSI EN 319 412-5 V2.5.1 (“ETSI EN 319 412-5”) piemēro ar šādiem pielāgojumiem:

1. ETSI EN 319 411-2

1) 2.1. Normatīvās atsauces

— [1] ETSI EN 319 401 V3.1.1 (2024-06) “Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*); vispārējās politikas prasības uzticamības pakalpojumu sniedzējiem”.

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) “Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*)”; politikas un drošības prasības uzticamības pakalpojumu sniedzējiem, kas izdod sertifikātus; 1. daļa. Vispārīgas prasības” ar šādiem pielāgojumiem:

Standarta ETSI EN 319 411-1 V1.5.1 2.1. punktu “Normatīvās atsauces” groza šādi:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) “Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*); vispārējās politikas prasības uzticamības pakalpojumu sniedzējiem”.

— [10] ETSI EN 319 412-2 V2.4.1 “Elektroniskie paraksti un infrastruktūras (ESI)”; sertifikātu profili; 2. daļa. Sertifikātu profils fiziskām personām izdotiem sertifikātiem”.

— [14] ETSI EN 319 412-1 V1.6.1 “Elektroniskie paraksti un infrastruktūras (*ESI*)”; sertifikātu profili; 1. daļa. Pārskats un kopīgas datu struktūras”.

— [3] ETSI EN 319 412-5 V2.5.1 “Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*)”; sertifikātu profili; 5. daļa. QCStatements”.

— [5] ETSI EN 319 412-1 V1.6.1 “Elektroniskie paraksti un uzticamības infrastruktūras (ESI)”; sertifikātu profili; 1. daļa. Pārskats un kopīgas datu struktūras”.

— [6] CEN/TS 419261:2015 “Drošības prasības uzticamām sistēmām, kas pārvalda sertifikātus un laika zīmogus”.

— [7] Eiropas Kiberdrošības sertifikācijas grupas apakšgrupa kriptogrāfijas jautājumos: “Saskaņoti kriptogrāfijas mehānismi”, ko publicējusi Eiropas Savienības Kiberdrošības aģentūra (“ENISA”) ([1]).

— [8] Komisijas Īstenošanas regula (ES) 2024/482 ([2]) par to, kā vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) pieņemšanas sakarā piemērojama Eiropas Parlamenta un Padomes Regula (ES) 2019/881.

— [9] Komisijas Īstenošanas regula (ES) 2024/3144 ([3]) par Īstenošanas regulas (ES) 2024/482 grozījumiem attiecībā uz piemērojamajiem starptautiskajiem standartiem un par tās labojumiem.

— [10] ISO/IEC 15408:2022 (1.–5. daļa): “Informācijas drošība, kiberdrošība un privātuma aizsardzība. Kritēriji informācijas tehnoloģiju drošības novērtēšanai”.

— [11] FIPS PUB 140-3 (2019) “Drošības prasības kriptogrāfijas moduļiem”.

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

2) 5.2. Sertifikācijas prakses paziņojuma prasības

— OVR-5.2-02 *TSP* dokumentācijā norādītās SP nosaka prasības attiecībā uz izmantojamo sertifikātu profiliem.

3) 5.3. Sertifikāta politikas nosaukums un identifikācija

— OVR-5.3-01 Ja SP tiek izdarītas izmaiņas, kā aprakstīts 4.2.2. punktā, un tās ietekmē politikas piemērojamību, tad jāmaina politikas identifikators.

4) 6.1. Publicēšanas un repozitorija pienākumi

— OVR-6.1-02 ETSI EN 319 411-1 [2] DIS-6.1-04 norādītā informācija ir publiski un starptautiski pieejama.

5) 6.2.2. Sākotnējā identitātes validācija

— REG-6.2.2-01A Pazīmju un pierādījumu apkopošanu, kā arī to validāciju veic atbilstoši īstenošanas aktiem, kas pieņemti saskaņā ar Regulas (ES) Nr. 910/2014 [i.1] 24. panta 1.c punkta noteikumiem.

— REG-6.2.2-02 [QCP-n] un[QCP-n-qscd] Fiziskās personas identitāti un attiecīgā gadījumā personas raksturīgās pazīmes pārbauda saskaņā ar īstenošanas aktiem, kas pieņemti saskaņā ar Regulas (ES) Nr. 910/2014 [i.1] 24. panta 1.c punktu.

— 1. PIEZĪME nav spēkā.

6) 6.3.3. Sertifikāta izdošana

— GEN-6.3.3-01 Piemēro ETSI EN 319 411-1 [2] 6.3.3. punktā noteiktās GEN-6.3.3-01.– GEN-6.3.3.-10. punkta prasības.

— GEN-6.3.3-02 [AR NOSACĪJUMIEM] Ja sertifikāts tiek izsniegts fiziskai personai, kas ir identificēta saistībā ar juridisku personu, tad sertifikātā norādītās subjekta iezīmes, kas identificē organizāciju, attiecas uz šo juridisko personu vai tās apakšstruktūru un sertifikātā norādītais subjekta identifikators ir fiziskā persona.

— GEN-6.3.3-03 SP identifikators ir [IZVĒLE]:

a) [QCP-n]:

— kā noteikts 5.3. punkta a) apakšpunktā, un/vai

— *OID*, ko piešķīris *TSP*, cita attiecīgā ieinteresētā puse vai kas noteikts turpmākā standartizācijā, attiecībā uz sertifikāta politiku, kas papildina attiecīgās piemērojamās politikas prasības, kādas noteiktas šajā dokumentā;

b) [QCP-n-QSCD]:

— kā noteikts 5.3. punkta c) apakšpunktā, un/vai

— *OID*, ko piešķīris *TSP*, ita attiecīgā ieinteresētā puse vai kas noteikts turpmākā standartizācijā, attiecībā uz sertifikāta politiku, kas papildina attiecīgās piemērojamās politikas prasības, kādas noteiktas šajā dokumentā.

7) 6.3.5. Atslēgu pāris un sertifikāta izmantošana

— SDP-6.3.5-02A [AR NOSACĪJUMIEM] Ja *TSP* pārvalda attiecīgā subjekta QSCD, *TSP* ir kvalificēts uzticamības pakalpojumu sniedzējs, kas sniedz kvalificētu uzticamības pakalpojumu attālinātas kvalificēta elektroniskā paraksta radīšanas ierīces pārvaldībai saskaņā ar Regulu (ES) Nr. 910/2014 [i.1].

— SDP-6.3.5-11A Abonenta pienākumi (sk. 6.3.4. punktu), ja abonents vai subjekts ģenerē subjekta atslēgas, ietver:

a) pienākumu attiecībā uz sertificētās atslēgas izmantojumiem, kā noteikts SP, ģenerēt subjekta atslēgas, izmantojot algoritmu, kas atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa [7] un publicējusi *ENISA*;

b) pienākumu attiecībā uz sertificētās atslēgas izmantojumiem, kas norādīti SP, sertifikāta derīguma laikā izmantot atslēgas garumu un algoritmu, kas atbilst dokumentam saskaņotajiem kriptogrāfijas mehānismiem, kurus apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa [7] un publicējusi *ENISA*.

8) 6.3.10. Sertifikāta statusa pakalpojumi

— CSS-6.3.10-08 [AR NOSACĪJUMIEM] Ja ir nodrošināti *CRL*, *TSP* saglabā pēdējā *CRL* integritāti un pieejamību vismaz *CPS* norādītajā laikposmā, kā prasīts CSS-6.3.10-12.

9) 6.4.4. Personāla kontroles

— OVR-6.4.4-02 *TSP* darbinieki uzticamās lomās un attiecīgā gadījumā tā apakšuzņēmēji uzticamās lomās spēj izpildīt prasību par "ekspertu zināšanām, pieredzi un kvalifikāciju", izmantojot oficiālu apmācību un apliecinājumus vai faktisku pieredzi, vai abu kombināciju.

— OVR-6.4.4-03 Atbilstība OVR-6.4.4-02 ietver regulārus (vismaz reizi 12 mēnešos) atjauninājumus par jauniem apdraudējumiem un pašreizējo drošības praksi.

— OVR-6.4.4-04 Papildus uzticamām lomām, kas noteiktas ETSI EN 319 401 [1] (7.2-15 punktā), atbalsta reģistrācijas un atsaukšanas amatpersonu uzticamās lomas, kas noteiktas TS 419261 [6]. Gadījumos, kad *QTSP* tieši pārvalda dalībvalsts vai publiskā sektora struktūra vai tas darbojas dalībvalsts vai publiskā sektora struktūras vārdā, minētās papildu uzticamās lomas var pildīt viens vai vairāki oficiālie pārstāvji, kas darbojas reģistrācijas un atsaukšanas amatpersonu vārdā un uzdevumā vietējās vai reģionālās pārvaldes iestādēs.

10) 6.4.9. *CA* vai *RA* izbeigšana

— OVR-6.4,9-02: *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].

11) 6.5.1. Atslēgu pāra ģenerēšana un instalēšana

— OVR-6.5.1-01A *CA* atslēgu pāra ģenerēšanu *CA* parakstīšanas vajadzībām veic, izmantojot algoritmu, kas atbilst Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un ENISA publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [7].

— OVR-6.5.1-01B Izraudzītais *CA* parakstīšanas atslēgas garums un algoritms *CA* parakstīšanas nolūkiem atbilst Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [7].

— OVR-6.5.1-01C [AR NOSACĪJUMIEM] Ja CA ģenerē subjekta atslēgas, *CA* ģenerētās subjekta atslēgas SP norādītajos nolūkos sertifikāta derīguma laikā atbilst Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un ENISA publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [7].

12) 6.5.2. Privāto atslēgu aizsardzības un kriptogrāfijas moduļu inženiertehniskās vadības ierīces

— GEN-6.5.2-01 Piemēro visas ETSI EN 319 411-1 [2] 6.5.2. punktā noteiktās prasības, izņemot prasības OVR-6.5.2-01, OVR-6.5.2.-03 un OVR-6.5.2.-04.

— GEN-6.5.2-02 *TSP* atslēgu pāra ģenerēšanu, ieskaitot atslēgas, ko izmanto atsaukšanas un reģistrācijas dienesti, veic drošā kriptogrāfiskā ierīcē, kas ir uzticama sistēma, kura sertificēta saskaņā ar:

— vienotajiem informācijas tehnoloģiju drošības izvērtēšanas kritērijiem, kā izklāstīts ISO/IEC 15408 [10], vai vienoto informācijas tehnoloģiju drošības izvērtēšanas metodiku (versija CC:2002, 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

— vienotos kritērijos balstītu Eiropas kiberdrošības sertifikācijas shēmu (*EUCC*) [8][9], kas sertificēta atbilstoši *EAL* 4 vai augstāka līmeņa *EAL*; vai

— līdz 31.12.2030. FIPS PUB 140-3 [11] 3. līmeni.

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* [8][9] sertifikāciju, šo ierīci konfigurē un izmanto saskaņā ar minēto sertifikāciju.

— GEN-6.5.2-03 *CA* privāto parakstīšanas atslēgu tur un izmanto drošā kriptogrāfiskā ierīcē, kas atbilst GEN-6.5.2-01 un GEN-6.5.2-02 prasībām.

13) 6.5.7. Tīkla drošības kontroles

— OVR-6.5.7-02 Ievainojamības skenēšanu, kas prasīta ETSI EN 319 401 [1] REQ-7.8-13, veic vismaz reizi ceturksnī.

— OVR-6.5.7-03 Ielaušanās testu, kas prasīts ETSI EN 319 401 [1] REQ-7.8-17X, veic vismaz reizi gadā.

— OVR-6.5.7-04 Ugunsmūri ir konfigurēti tā, lai novērstu visus tos protokolus un piekļuves, kas nav vajadzīgas uzticamības pakalpojuma sniedzēja darbībai.

14) 6.6.1. Sertifikāta profils

— GEN-6.6.1-05 Sertifikātā iekļauj vienu no politikas identifikatoriem, kas norādīti GEN-6.3.3-03 [IZVĒLE]. Sertifikātā var iekļaut citus *TPS* piešķirtos *OID*.

2. ETSI EN 319 412-2:

1) 2.1. Normatīvās atsauces

— [2] ETSI EN 319 412-5 V2.5.1 "Elektroniskie paraksti un uzticamības infrastruktūras (ESI)"; sertifikātu profili; 5. daļa. QCStatements".

— [9] Eiropas Kiberdrošības sertifikācijas grupas Kriptogrāfijas apakšgrupas "Saskaņotie kriptogrāfijas mehānismi", ko publicējusi *ENISA*.

2) 4.2.2. Paraksts

— GEN-4.2.2-2 Paraksta algoritmu izraugās saskaņā ar Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [9].

— PIEZĪME nav spēkā.

3) 4.2.3.1. Izsniedzēji, kas ir juridiskās personas

— GEN-4.2.3.1-3 Ja zināms, ka pastāv atbilstošs reģistrācijas numurs, tad izsniedzēja identitāte ietver “organizationIdentifier” ar šā reģistrācijas numura vērtību, kā norādīts attiecīgajā oficiālajā ierakstā, ar ko izveido minēto reģistrācijas numuru.

4) 4.2.5. Informācija par subjekta publisko atslēgu

— GEN-4.2.5-2 Subjekta publisko atslēgu izraugās saskaņā ar Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un ENISA publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [9].

— PIEZĪME nav spēkā.

5) 4.2.6. Sērijas numurs

— GEN-4.2.6-01 Sertifikāta “serialNumber” (kā norādīts IETF RFC 5280 [1] 4.1.2.2. punktā) ir unikāls katram *TSP* izdotajam sertifikātam.

II PIELIKUMS

Kvalificētu elektronisko zīmogu sertifikātu atsauces standartu un specifikāciju saraksts

Standartus 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”) un ETSI EN 319 412-5 V2.5.1 (“ETSI EN 319 412-5”) piemēro ar šādiem pielāgojumiem:

1. ETSI EN 319 411-2

1) 2.1. Normatīvās atsauces

— [1] ETSI EN 319 401 V3.1.1 (2024-06) “Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*); vispārējās politikas prasības uzticamības pakalpojumu sniedzējiem”.

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) “Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*)”; politikas un drošības prasības uzticamības pakalpojumu sniedzējiem, kas izdod sertifikātus; 1. daļa. Vispārīgas prasības” ar šādiem pielāgojumiem:

Standarta ETSI EN 319 411-1 V1.5.1 2.1. punktu “Normatīvās atsauces” groza šādi:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) “Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*); vispārējās politikas prasības uzticamības pakalpojumu sniedzējiem”.

— [10] ETSI EN 319 412-2 V2.4.1 “Elektroniskie paraksti un infrastruktūras (*ESI*)”; sertifikātu profili; 2. daļa. Sertifikātu profils fiziskām personām izdotiem sertifikātiem”.

— [14] ETSI EN 319 412-1 V1.6.1 “Elektroniskie paraksti un infrastruktūras (*ESI*)”; sertifikātu profili; 1. daļa. Pārskats un kopīgas datu struktūras”.

— [3] ETSI EN 319 412-5 V2.5.1 “Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*)”; sertifikātu profili; 5. daļa. QCStatements”.

— [5] ETSI EN 319 412-1 V1.6.1 “Elektroniskie paraksti un uzticamības infrastruktūras (ESI)”; sertifikātu profili; 1. daļa. Pārskats un kopīgas datu struktūras”.

— [6] CEN/TS 419261:2015 “Drošības prasības uzticamām sistēmām, kas pārvalda sertifikātus un laika zīmogus” (sagatavojusi *CEN*).

— [7] Eiropas Kiberdrošības sertifikācijas grupas apakšgrupa kriptogrāfijas jautājumos: “Saskaņotie kriptogrāfijas mehānismi”, ko publicējusi *ENISA*.

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

— [9] Īstenošanas regula (ES) 2024/3144 par Īstenošanas regulas (ES) 2024/482 grozījumiem attiecībā uz piemērojamajiem starptautiskajiem standartiem un par tās labojumiem.

— [10] ISO/IEC 15408:2022 (1.–5. daļa) “Informācijas drošība, kiberdrošība un privātuma aizsardzība. IT drošības vērtēšanas kritēriji”.

— [11] FIPS PUB 140-3 (2019) “Drošības prasības kriptogrāfijas moduļiem”.

2) 5.2. Sertifikācijas prakses paziņojuma prasības

— OVR-5.2-02 *TSP* dokumentācijā norādītās SP nosaka prasības attiecībā uz izmantojamo sertifikātu profiliem.

3) 5.3. Sertifikāta politikas nosaukums un identifikācija

— OVR-5.3-01 Ja SP tiek izdarītas izmaiņas, kā aprakstīts 4.2.2. punktā, un tās ietekmē politikas piemērojamību, tad jāmaina politikas identifikators.

4) 6.1. Publicēšanas un repozitorija pienākumi

— OVR-6.1-02 ETSI EN 319 411-1 [2] DIS-6.1-04 norādītā informācija ir publiski un starptautiski pieejama.

5) 6.2.2. Sākotnējā identitātes validācija

— REG-6.2.2-01A Pazīmju un pierādījumu apkopošanu, kā arī to validāciju veic atbilstoši īstenošanas aktiem, kas pieņemti saskaņā ar Regulas (ES) Nr. 910/2014 [i.1] 24. panta 1.c punkta noteikumiem.

— REG-6.2.2-03 [QCP-n] un [QCP-n-qscd] Juridiskās personas identitāti un attiecīgā gadījumā personas raksturīgās pazīmes pārbauda saskaņā ar īstenošanas aktiem, kas pieņemti saskaņā ar Regulas (ES) Nr. 910/2014 [i.1] 24. panta 1.c punktu.

— 3. PIEZĪME. Sk. 2. piezīmi.

6) 6.3.3. Sertifikāta izdošana

— GEN-6.3.3-01 Piemēro ETSI EN 319 411-1 [2] 6.3.3. punktā noteiktās GEN-6.3.3-01.– GEN-6.3.3.-10. punkta prasības.

— GEN-6.3.3-02 SP identifikators ir [IZVĒLE]:

a) [QCP-l]

— kā noteikts 5.3. punkta b) apakšpunktā, un/vai

— OID, ko piešķīris TSP, cita attiecīgā ieinteresētā puse vai kas noteikts turpmākā standartizācijā, attiecībā uz sertifikāta politiku, kas papildina attiecīgās piemērojamās politikas prasības, kādas noteiktas šajā dokumentā;

b) [QCP-l-qscd]

— kā noteikts 5.3. punkta d) apakšpunktā, un/vai

— *OID*, ko piešķīris *TSP*, cita attiecīgā ieinteresētā puse vai kas noteikts turpmākā standartizācijā, attiecībā uz sertifikāta politiku, kas papildina attiecīgās piemērojamās politikas prasības, kādas noteiktas šajā dokumentā.

7) 6.3.5. Atslēgu pāris un sertifikāta izmantošana

— SDP-6.3.5-02A [AR NOSACĪJUMIEM] Ja *TSP* pārvalda attiecīgā subjekta *QSCD*, *TSP* ir kvalificēts uzticamības pakalpojumu sniedzējs, kas sniedz kvalificētu uzticamības pakalpojumu attālinātas kvalificēta elektroniskā zīmoga radīšanas ierīces pārvaldībai saskaņā ar Regulu (ES) Nr. 910/2014 [i.1].

— SDP-6.3.5-11A Abonenta pienākumi (sk. 6.3.4. punktu), ja abonents vai subjekts ģenerē subjekta atslēgas, ietver:

a) pienākumu ģenerēt subjekta atslēgas, izmantojot algoritmu, kas atbilst Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [7], lai izmantotu sertificēto atslēgu tā, kā noteikts SP; un

b) pienākumu izmantot atslēgas garumu un algoritmu, kas atbilst Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [7], lai sertifikāta derīguma laikā izmantotu sertificēto atslēgu tā, kā noteikts SP.

8) 6.3.10. Sertifikāta statusa pakalpojumi

— CSS-6.3.10-08 [AR NOSACĪJUMIEM] Ja ir nodrošināti *CRL*, *TSP* saglabā pēdējā *CRL* integritāti un pieejamību vismaz *CPS* norādītajā laikposmā, kā prasīts CSS-6.3.10-12.

9) 6.4.4. Personāla kontroles

— OVR-6.4.4-02 *TSP* darbinieki uzticamās lomās un attiecīgā gadījumā tā apakšuzņēmēji uzticamās lomās spēj izpildīt prasību par "ekspertu zināšanām, pieredzi un kvalifikāciju", izmantojot oficiālu apmācību un apliecinājumus vai faktisku pieredzi, vai abu kombināciju.

— OVR-6.4.4-03 Atbilstība OVR-6.4.4-02 ietver regulārus (vismaz reizi 12 mēnešos) atjauninājumus par jauniem apdraudējumiem un pašreizējo drošības praksi.

— OVR-6.4.4-04 Papildus uzticamām lomām, kas noteiktas ETSI EN 319 401 [1] (7.2-15 punktā), atbalsta reģistrācijas un atsaukšanas amatpersonu uzticamās lomas, kas noteiktas TS 419261 [6]. Gadījumos, kad *QTSP* tieši pārvalda dalībvalsts vai publiskā sektora struktūra vai tas darbojas dalībvalsts vai publiskā sektora struktūras vārdā, minētās papildu uzticamās lomas var pildīt viens vai vairāki oficiālie pārstāvji, kas darbojas reģistrācijas un atsaukšanas amatpersonu vārdā un uzdevumā vietējās vai reģionālās pārvaldes iestādēs.

10) 6.4.9. *CA* vai *RA* izbeigšana

— OVR-6.4.9-02 *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].

11) 6.5.1. Atslēgu pāra ģenerēšana un instalēšana

— OVR-6.5.1-01A *CA* atslēgu pāra ģenerēšanu *CA* parakstīšanas vajadzībām veic, izmantojot algoritmu, kas atbilst Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [7].

— OVR-6.5.1-01B Izraudzītais *CA* parakstīšanas atslēgas garums un algoritms *CA* parakstīšanas nolūkiem atbilst Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [7].

— OVR-6.5.1-01C [AR NOSACĪJUMIEM] Ja *CA* ģenerē subjekta atslēgas, *CA* ģenerētās subjekta atslēgas SP norādītajos nolūkos sertifikāta derīguma laikā atbilst Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [7].

12) 6.5.2. Privāto atslēgu aizsardzības un kriptogrāfijas moduļu inženiertehniskās vadības ierīces

— GEN-6.5.2-01 Piemēro visas ETSI EN 319 411-1 [2] 6.5.2. punktā noteiktās prasības, izņemot prasības OVR-6.5.2-01, OVR-6.5.2.-03 un OVR-6.5.2.-04.

— GEN-6.5.2-02 *TSP* atslēgu pāra ģenerēšanu, ieskaitot atslēgas, ko izmanto atsaukšanas un reģistrācijas dienesti, veic drošā kriptogrāfiskā ierīcē, kas ir uzticama sistēma, kura sertificēta saskaņā ar:

  — vienotajiem informācijas tehnoloģiju drošības izvērtēšanas kritērijiem, kā izklāstīts ISO/IEC 15408 [10], vai vienoto informācijas tehnoloģiju drošības izvērtēšanas metodiku (versija CC:2002, 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

  — vienotos kritērijos balstītu Eiropas kiberdrošības sertifikācijas shēmu (*EUCC*) [8][9], kas sertificēta atbilstoši *EAL* 4 vai augstāka līmeņa *EAL*; vai

  — līdz 31.12.2030. FIPS PUB 140-3 [11] 3. līmeni.

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* [8][9] sertifikāciju, šo ierīci konfigurē un izmanto saskaņā ar minēto sertifikāciju.

— GEN-6.5.2-03 *CA* privāto parakstīšanas atslēgu tur un izmanto drošā kriptogrāfiskā ierīcē, kas atbilst GEN-6.5.2-01 un GEN-6.5.2-02 prasībām.

13) 6.5.7. Tīkla drošības kontroles

— OVR-6.5.7-02 Ievainojamības skenēšanu, kas prasīta ETSI EN 319 401 [1] REQ-7.8-13, veic vismaz reizi ceturksnī.

— OVR-6.5.7-03 Ielaušanās testu, kas prasīts ETSI EN 319 401 [1] REQ-7.8-17X, veic vismaz reizi gadā.

— OVR-6.5.7-04 Ugunsmūri ir konfigurēti tā, lai novērstu visus tos protokolus un piekļuves, kas nav vajadzīgas uzticamības pakalpojuma sniedzēja darbībai.

14) 6.6.1. Sertifikāta profils

— GEN-6.6.1-05 Sertifikātā iekļauj vienu no politikas identifikatoriem, kas norādīti GEN-6.3.3-02 [IZVĒLE].

2. ETSI EN 319 412-3:

1) 2.1. Normatīvās atsauces

— [2] ETSI EN 319 412-2 V2.4.1 "Elektroniskie paraksti un infrastruktūras (*ESI*)"; sertifikātu profili; 2. daļa. Sertifikāta profils fiziskām personām izdotiem sertifikātiem".

2) 4.2.1. Subjekts

— LEG-4.2.1-6 Atribūts "OrganizationIdentifier" ietver subjekta organizācijas identifikāciju, kas atšķiras no organizācijas nosaukuma. Ja zināms, ka pastāv atbilstošs reģistrācijas numurs, tad atribūts "organizationIdentifier" ietver šā reģistrācijas numura vērtību, kā norādīts attiecīgajā oficiālajā ierakstā, ar ko nosaka šo reģistrācijas numuru.

3. ETSI EN 319 412-2:

1) 2.1. Normatīvās atsauces

— [2] ETSI EN 319 412-5 V2.5.1 "Elektroniskie paraksti un uzticamības infrastruktūras (*ESI*)"; sertifikātu profili; 5. daļa. QCStatements".

— [9] Eiropas Kiberdrošības sertifikācijas grupas apakšgrupa kriptogrāfijas jautājumos: "Saskaņotie kriptogrāfijas mehānismi", ko publicējusi *ENISA*.

2) 2.2. Informatīvas atsauces

— [i.7] nav spēkā.

3) 4.2.2. Paraksts

— GEN-4.2.2-2 Paraksta algoritmu izraugās saskaņā ar Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un *ENISA* publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [9].

— PIEZĪME nav spēkā.

4) 4.2.3.1. Izsniedzēji, kas ir juridiskās personas

— GEN-4.2.3.1-3 Ja zināms, ka pastāv atbilstošs reģistrācijas numurs, tad izsniedzēja identitāte ietver "organizationIdentifier" ar šā reģistrācijas numura vērtību, kā norādīts attiecīgajā oficiālajā ierakstā, ar ko izveido minēto reģistrācijas numuru.

5) 4.2.5. Informācija par subjekta publisko atslēgu

— GEN-4.2.5-2 Subjekta publisko atslēgu izraugās saskaņā ar Eiropas Kiberdrošības sertifikācijas grupas apstiprinātajiem un ENISA publicētajiem saskaņotajiem kriptogrāfijas mehānismiem [9].

— PIEZĪME nav spēkā.

6) 4.2.6. Sērijas numurs

— GEN-4.2.6-01 Sertifikāta "serialNumber" (kā norādīts IETF RFC 5280 [1] 4.1.2.2. punktā) ir unikāls katram *TSP* izdotajam sertifikātam.