2024/482

7.2.2024

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2024/482,

annettu 31 päivänä tammikuuta 2024,

Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC) hyväksymisestä

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta 17 päivänä huhtikuuta 2019 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 (kyberturvallisuusasetus) ([1]) ja erityisesti sen 49 artiklan 7 kohdan,

sekä katsoo seuraavaa:

(1) Tässä asetuksessa vahvistetaan yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (European Common Criteria-based cybersecurity certification scheme), jäljempänä 'EUCC', tehtävät, säännöt ja velvoitteet sekä rakenne asetuksessa (EU) 2019/881 vahvistetun eurooppalaisen kyberturvallisuuden sertifiointikehyksen mukaisesti. EUCC perustuu johtavien virkamiesten tietoturvallisuusryhmän (SOG-IS) tietotekniikan tuotteiden turvallisuusarviointitodistusten vastavuoroista tunnustamista koskevaan sopimukseen ([2]) soveltamalla Common Criteria -kriteerejä, jäljempänä 'yhteiset kriteerit', mukaan lukien kyseisen ryhmän menettelyt ja asiakirjat.

(2) Järjestelmän olisi perustuttava vakiintuneisiin kansainvälisiin standardeihin. Yhteiset kriteerit ovat tietojärjestelmäkehityksen tietoturvallisuuden kansainvälinen arviointistandardi, joka on julkaistu esimerkiksi standardina ISO/IEC 15408 *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security* (tietoturvallisuus, kyberturvallisuus ja yksityisyyden suoja – tietotekniikan turvallisuuden arviointikriteerit). Se perustuu kolmannen osapuolen arviointiin ja käsittää seitsemän varmuustasoa (Evaluation Assurance Level, EAL). Yhteisiin kriteereihin liittyvät *Common Evaluation Methodology* -menetelmät, jäljempänä 'yhteiset arviointimenetelmät', jotka on julkaistu esimerkiksi standardissa ISO/IEC 18045 *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Methodology for IT security evaluation* (tietoturvallisuus, kyberturvallisuus ja yksityisyyden suoja – tietotekniikan turvallisuuden arviointikriteerit – tietotekniikan turvallisuuden arviointimenetelmät). Eritelmät ja asiakirjat, joissa sovelletaan tämän asetuksen säännöksiä, voivat liittyä julkisesti saatavilla olevaan standardiin, joka vastaa tämän asetuksen mukaisessa sertifioinnissa käytettyä standardia, mukaan lukien tietoteknologian turvallisuuden arviointia koskevat yhteiset kriteerit ja tietotekniikan turvallisuuden yhteiset arviointimenetelmät.

(3) EUCC-kehys perustuu yhteisten kriteerien haavoittuvuusarvioinnin perheen (AVA_VAN) komponentteihin 1–5. Nämä viisi komponenttia käsittävät kaikki tärkeimmät tieto- ja viestintätekniikan tuotteiden haavoittuvuuksien analysointiin vaikuttavat tekijät ja riippuvuudet. Koska komponentit vastaavat tämän asetuksen mukaisia varmuustasoja, niiden pohjalta voidaan tehdä perusteltu valinta varmuudesta perustuen arviointeihin, jotka on tehty turvallisuusvaatimuksista ja tieto- ja viestintätekniikan tuotteen käyttötarkoitukseen liittyvistä riskeistä. EUCC-sertifikaatin hakijan olisi toimitettava tieto- ja viestintätekniikan tuotteen aiottuun käyttöön liittyvä dokumentaatio sekä analyysi tähän käyttöön liittyvistä riskitasoista, jotta vaatimustenmukaisuuden arviointilaitos voi arvioida valitun varmuustason sopivuuden. Jos arviointi- ja sertifiointitoimet suorittaa sama vaatimustenmukaisuuden arviointilaitos, hakijan olisi toimitettava pyydetyt tiedot vain kerran.

(4) Yksittäinen tekniikan osa-alue muodostaa viitekehyksen yksittäiselle joukolle tieto- ja viestintätekniikan tuotteita, joilla on erityisiä ja samankaltaisia turvallisuustoimintoja hyökkäysten lieventämiseksi ja joiden ominaisuudet vastaavat tiettyä varmuustasoa. Tekniikan osa-alue kuvaa viimeisintä kehitystä edustavissa asiakirjoissa erityiset turvallisuusvaatimukset sekä muut arviointimenetelmät, -tekniikat ja -välineet, joita sovelletaan kyseisen tekniikan osa-alueen tieto- ja viestintätekniikan tuotteiden sertifiointiin. Tekniikan osa-alue tukee näin ollen myös kattamiensa

([1]) EUVL L 151, 7.6.2019, s. 15.

([2]) Tietotekniikan tuotteiden turvallisuusarviointitodistusten vastavuoroista tunnustamista koskeva sopimus (Mutual Recognition Agreement of Information Technology Security Evaluation Certificates) (versio 3.0, tammikuu 2010, saatavilla sogis.eu -sivustolla), jonka Euroopan komission johtavien virkamiesten tietoturvallisuusryhmä (Senior Officials Group Information Systems Security) on hyväksynyt vastauksena yleisistä tietotekniikan turvallisuuden arviointiperusteista 7 päivänä huhtikuuta 1995 annetun neuvoston suosituksen 95/144/EY (EYVL L 93, 26.4.1995, s. 27) 3 kohtaan.

tieto- ja viestintätekniikan tuotteiden arvioinnin yhdenmukaistamista. Kahta tekniikan osa-aluetta käytetään nykyisin laajalti sertifioinnissa tasoilla AVA_VAN.4 ja AVA_VAN.5. Ensimmäinen näistä on älykortit ja vastaavat laitteet (”Smart cards and similar devices”), joissa vaaditut turvallisuustoiminnot riippuvat merkittäviltä osin erityisistä, räätälöidyistä ja usein irrotettavissa olevista laite-elementeistä (esim. älykorttilaitteet, integroidut piirit, yhdistetyt älykorttituotteet, luotettujen suoritusympäristöjen tekniikat eli TPM:t (Trusted Platform Modules) tai digitaaliset ajopiirturikortit). Toinen niistä on tietoturvaboksilla varustetut laitteet (”Hardware devices with security boxes”), joissa vaaditut turvallisuustoiminnot riippuvat merkittäviltä osin fyysisestä turvavaipasta (”security box”), joka on suunniteltu suojaamaan suoralta tietoturvauhalta esimerkiksi maksupäätteissä, ajopiirturin ajoneuvoyksiköissä, älykkäissä mittareissa, kulunvalvontapäätteissä ja laitteistojen tietoturvamoduuleissa (HSM-moduuleissa).

(5) Hakijan tulee sertifiointia hakiessaan perustella varmuustason valinta suhteessa asetuksen (EU) 2019/881 51 artiklassa asetettuihin tavoitteisiin ja suhteessa komponenttien valintaan yhteisten kriteerien sisältämien toiminnallisten turvallisuusvaatimusten ja turvallisuusvarmistusvaatimusten luettelosta. Sertifiointielinten olisi arvioitava valitun varmuustason asianmukaisuus ja varmistettava, että valittu taso vastaa tieto- ja viestintätekniikan tuotteen käyttötarkoitukseen liittyvää riskitasoa.

(6) Yhteisten kriteerien mukaan sertifiointi suoritetaan suhteessa turvatavoitteeseen (*security target*, ST), joka käsittää tieto- ja viestintätekniikan tuotteen turvallisuusongelman määrittelyn sekä turvallisuusongelmaan liittyvät yksittäiset turvallisuustavoitteet. Turvallisuusongelma käsittää yksityiskohtaiset tiedot tieto- ja viestintätekniikan tuotteen käyttötarkoituksesta ja siihen liittyvistä riskeistä. Valikoiduilla turvallisuusvaatimuksilla vastataan sekä tieto- ja viestintätekniikan tuotteen turvallisuusongelmaan että turvallisuustavoitteisiin.

(7) Suojausprofiilit ovat tehokas keino määritellä ennalta tiettyyn tieto- ja viestintätekniikan tuotteiden luokkaan sovellettavat yhteiset kriteerit ja siksi myös olennainen osa suojausprofiilin kattamien tieto- ja viestintätekniikan tuotteiden sertifiointiprosessia. Suojausprofiilia käytetään arvioitaessa tulevia turvatavoitteita, jotka liittyvät kulloiseenkin kyseisen suojausprofiilin kattamaan tieto- ja viestintätekniikan tuoteluokkaan. Ne yksinkertaistavat ja tehostavat tieto- ja viestintätekniikan tuotteiden sertifiointiprosessia ja auttavat käyttäjiä täsmentämään tieto- ja viestintätekniikan tuotteen toimivuuden oikein ja tehokkaasti. Suojausprofiileja tulisi näin ollen pitää erottamattomana osana tieto- ja viestintätekniikan tuotteiden sertifiointiin johtavaa tieto- ja viestintätekniikan prosessia.

(8) Jotta suojausprofiilit voisivat täyttää tehtävänsä sertifioidun tieto- ja viestintätekniikan tuotteen kehittämistä ja toimittamista tukevassa tieto- ja viestintätekniikan prosessissa, myös itse suojausprofiilit olisi voitava sertifioida erillään suojausprofiilin piiriin kuuluvan yksittäisen tieto- ja viestintätekniikan tuotteen sertifioinnista. Sen vuoksi on olennaisen tärkeää, että suojausprofiileihin sovelletaan vähintään samantasoista valvontaa kuin turvatavoitteisiin, jotta voidaan varmistaa kyberturvallisuuden korkea taso. Suojausprofiilit olisi arvioitava ja sertifioitava erillään kulloisestakin tieto- ja viestintätekniikan tuotteesta ja ainoastaan soveltamalla yhteisten kriteerien ja yhteisten arviointimenetelmien varmuusluokkaa suojausprofiileille (APE) ja tarvittaessa suojausprofiilien konfiguraatioille (ACE). Koska suojausprofiileilla on tärkeä ja arkaluonteinen rooli vertailukohteina tieto- ja viestintätekniikan tuotteiden sertifioinnissa, niitä saisivat sertifioida vain julkiset elimet tai sertifiointielimet, jotka ovat saaneet kansalliselta kyberturvallisuussertifiointiviranomaiselta etukäteen hyväksynnän kunkin yksittäisen suojausprofiilin osalta. Koska suojausprofiileilla on keskeinen rooli varmuustason ”korkea” sertifioinnissa erityisesti tekniikan osa-alueiden ulkopuolella, ne olisi laadittava viimeisintä kehitystä edustavina asiakirjoina, jotka Euroopan kyberturvallisuuden sertifiointiryhmän olisi hyväksyttävä.

(9) Kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten tulisi ottaa sertifioidut suojausprofiilit mukaan seurantaan, joka koskee vaatimustenmukaisuutta ja velvoitteiden noudattamista suhteessa EUCC:hen. Jos yksittäisiä sertifioituja suojausprofiileja varten on saatavilla tieto- ja viestintätekniikan tuotteiden arvioinnin lähestymistapoihin sovellettavia menetelmiä, välineitä ja taitoja, tekniikan osa-alueet voivat perustua kyseisiin erityisiin suojausprofiileihin.

(10) Jotta voidaan saavuttaa korkea luottamuksen ja varmuuden taso sertifioiduissa tieto- ja viestintätekniikan tuotteissa, itsearviointia ei pitäisi sallia tämän asetuksen nojalla. Ainoastaan ITSEFin ja sertifiointielinten suorittama ulkopuolinen vaatimustenmukaisuuden arviointi tulisi sallia.

(11) SOG-IS-yhteisö on tarjonnut yhteisiä tulkintoja ja lähestymistapoja yhteisten kriteerien ja yhteisten arviointimenetelmien soveltamiselle sertifioinnissa, erityisesti varmuustason ”korkea” saavuttamiseksi teknisillä osa-alueilla ”älykortit ja vastaavat laitteet” ja ”tietoturvaboksilla varustetut laitteet”. Tällaisen asiakirja-aineiston uudelleenkäyttö EUCC-järjestelmässä varmistaa sujuvan siirtymisen kansallisesti toteutetuista SOG-IS-järjestelmistä yhdenmukaistettuun EUCC-järjestelmään. Sen vuoksi tähän asetukseen olisi sisällytettävä yhdenmukaistettuja arviointimenetelmiä, joilla on yleistä merkitystä kaikkien sertifiointitoimien kannalta. Lisäksi komission olisi voitava pyytää Euroopan kyberturvallisuuden sertifiointiryhmältä lausunto, jossa hyväksytään viimeisintä kehitystä edustavissa asiakirjoissa täsmennettyjen arviointimenetelmien soveltaminen ja suositellaan sitä tieto- ja viestintätekniikan tuotteen tai suojausprofiilin sertifiointiin EUCC-järjestelmässä. Tämän asetuksen liitteessä I luetellaan viimeisintä kehitystä edustavat asiakirjat vaatimustenmukaisuuden arviointilaitosten suorittamia arviointitoimia varten. Euroopan kyberturvallisuuden sertifiointiryhmän olisi hyväksyttävä viimeisintä kehitystä edustavat asiakirjat ja pidettävä niitä yllä. Viimeisintä kehitystä edustavia asiakirjoja olisi käytettävä sertifioinnissa. Vain asianmukaisesti perustelluissa poikkeustapauksissa ja tietyin edellytyksin, erityisesti vain kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen suostumuksella, vaatimustenmukaisuuden arviointilaitos voi olla käyttämättä niitä.

(12) Tieto- ja viestintätekniikan tuotteiden sertifioinnin AVA_VAN-tasolla 4 tai 5 pitäisi olla mahdollista vain tietyin edellytyksin ja jos käytettävissä on erityiset arviointimenetelmät. Erityiset arviointimenetelmät voidaan sisällyttää kulloisenkin tekniikan osa-alueen kannalta merkityksellisiin viimeisintä kehitystä edustaviin asiakirjoihin tai yksittäisiin suojausprofiileihin, jotka on hyväksytty viimeisintä kehitystä edustavina asiakirjoina ja jotka ovat merkityksellisiä kyseisen tuoteluokan kannalta. Sertifioinnin näillä varmuustasoilla pitäisi olla mahdollista vain asianmukaisesti perustelluissa poikkeustapauksissa ja tietyin edellytyksin, erityisesti vain kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen suostumuksella, mukaan lukien sovellettavat arviointimenetelmät. Tällaisia asianmukaisesti perusteltuja poikkeustapauksia voi esiintyä, jos unionin tai kansallisessa lainsäädännössä edellytetään tieto- ja viestintätekniikan tuotteen sertifiointia AVA_VAN-tasolla 4 tai 5. Samoin asianmukaisesti perustelluissa poikkeustapauksissa suojausprofiilit voidaan sertifioida soveltamatta asiaankuuluvia viimeisintä kehitystä edustavia asiakirjoja tietyin edellytyksin, erityisesti vain kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen suostumuksella, mukaan lukien sovellettavat arviointimenetelmät.

(13) EUCC:n puitteissa käytettävien merkkien ja merkintöjen on tarkoitus näkyvästi osoittaa sertifioidun tieto- ja viestintätekniikan tuotteen luotettavuus käyttäjille ja antaa käyttäjille mahdollisuus tehdä tietoon perustuvia valintoja tieto- ja viestintätekniikan tuotteita ostaessaan. Merkkien ja merkintöjen käyttöön olisi sovellettava myös standardissa ISO/IEC 17065 ja soveltuvin osin standardissa ISO/IEC 17030 vahvistettuja sääntöjä ja ehtoja sekä sovellettavia ohjeita.

(14) Sertifiointielinten olisi päätettävä sertifikaattien voimassaolon kestosta ottaen huomioon kulloisenkin tieto- ja viestintätekniikan tuotteen elinkaari. Voimassaoloaika saa olla enintään viisi vuotta. Kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten tulisi pyrkiä yhdenmukaistamaan voimassaoloaika unionissa.

(15) Jos voimassa olevan EUCC-sertifikaatin kattavuutta supistetaan, sertifikaatti olisi peruutettava ja olisi myönnettävä uusi sertifikaatti uudella kattavuudella, jotta voidaan antaa käyttäjille selkeä tieto yksittäisen tieto- ja viestintätekniikan tuotteen sertifikaatin kattavuudesta ja varmuustasosta.

(16) Suojausprofiilien sertifiointi eroaa tieto- ja viestintätekniikan tuotteiden sertifioinnista, koska kyse on tieto- ja viestintätekniikan prosessista. Koska suojausprofiili kattaa yksittäisen tieto- ja viestintätekniikan tuotteiden luokan, sen arviointia ja sertifiointia ei voida tehdä yksittäisen tieto- ja viestintätekniikan tuotteen perusteella. Koska suojausprofiili yhdistää yksittäiseen tieto- ja viestintätekniikan tuotteiden luokkaan liittyvät yleiset turvallisuusvaatimukset ja on riippumaton siitä, miten myyjä panee tieto- ja viestintätekniikan tuotteen esille, suojausprofiilin EUCC-sertifikaatin voimassaoloajan tulisi periaatteessa olla vähintään viisi vuotta ja se voi kestää suojausprofiilin koko käyttöiän.

(17) Vaatimustenmukaisuuden arviointilaitos määritellään elimeksi, joka suorittaa vaatimustenmukaisuuden arviointitoimia, kuten kalibrointia, testausta, sertifiointia ja tarkastuksia. Palvelujen korkean laadun varmistamiseksi tässä asetuksessa täsmennetään, että yhtäältä testauksesta ja toisaalta sertifioinnista ja tarkastuksista vastaavat toisistaan riippumattomat tahot, jolloin testauksesta vastaisivat tietotekniikan turvallisuuden arviointilaitokset (Information Technology Security Evaluation Facilities), jäljempänä ’ITSEF’, ja sertifioinnista ja tarkastuksista sertifiointielimet. Kummankin tyyppiset vaatimustenmukaisuuden arviointilaitokset olisi akkreditoitava ja tietyissä tapauksissa valtuutettava.

(18) Kansallisen akkreditointielimen olisi akkreditoitava sertifiointielin standardin ISO/IEC 17065 mukaisesti varmuustasojen ”korotettu” ja ”korkea” osalta. Akkreditointia koskevien vaatimusten lisäksi, joista säädetään asetuksessa (EU) 2019/881 yhdessä asetuksen (EY) N:o 765/2008 kanssa, vaatimustenmukaisuuden arviointilaitosten olisi täytettävä erityisvaatimukset niiden teknisen pätevyyden takaamiseksi kyberturvallisuusvaatimusten arvioinnissa EUCC:n varmuustasolla ”korkea”, minkä vahvistuksena on ”valtuutus”. Valtuutusmenettelyn tukemiseksi olisi laadittava asiaankuuluvia viimeisintä kehitystä edustavia asiakirjoja, jotka ENISAn olisi julkaistava sen jälkeen, kun Euroopan kyberturvallisuuden sertifiointiryhmä on antanut hyväksyntänsä.

(19) ITSEF:n tekninen pätevyys tulisi arvioida testauslaboratorion akkreditoinnilla standardin ISO/IEC 17025 mukaisesti täydennettynä standardilla ISO/IEC 23532-1 kaikille arviointitoimille, joilla on merkitystä varmuustason kannalta ja jotka täsmennetään standardissa ISO/IEC 18045 luettuna yhdessä standardin ISO/IEC 15408 kanssa. Sekä sertifiointielimen että ITSEFin olisi perustettava henkilöstölleen asianmukainen pätevyydenhallintajärjestelmä, joka pätevyystekijöiden ja -tasojen sekä pätevyyden arvioinnin osalta perustuu standardiin ISO/IEC 19896–1, ja pidettävä sitä yllä. Tietämystä, osaamista, kokemusta ja koulutusta koskevat arvioijiin sovellettavat vaatimukset olisi otettava standardista ISO/IEC 19896–3. Säännösten ja toimenpiteiden vastaavuus tapauksissa, joissa tällaisista pätevyydenhallintajärjestelmistä poiketaan, olisi osoitettava järjestelmän tavoitteiden mukaisesti.

(20) Jotta ITSEF voidaan valtuuttaa, sen tulee osoittaa kykynsä määrittää, ettei tunnettuja haavoittuvuuksia ole, että viimeisintä kehitystä edustavat turvallisuustoiminnot pannaan asianmukaisesti ja johdonmukaisesti täytäntöön kyseessä olevan erityisen teknologian osalta ja että kohteena olevalla tieto- ja viestintätekniikan tuotteella on kyky vastustaa kyvykkäitä hyökkääjiä. Mitä tulee valtuutuksiin tekniikan osa-alueella ”älykortit ja vastaavat laitteet”, ITSEFin olisi myös osoitettava tekniset valmiudet, joita tarvitaan arviointitoimiin ja niihin liittyviin tehtäviin sellaisina kuin ne määritellään yhteisten kriteerien asiakirjassa, joka koskee älykorttien ja vastaavien laitteiden turvallisuusarviointien vähimmäisvaatimuksia ([3]). Mitä tulee valtuutuksiin tekniikan osa-alueella ”tietoturvaboksilla varustetut laitteet”, ITSEFin olisi lisäksi osoitettava tarvittavat tekniset vähimmäisvaatimukset arviointitoimien ja niihin liittyvien tehtävien suorittamiseksi tietoturvaboksilla varustetuille laitteille siten kuin Euroopan kyberturvallisuuden sertifiointiryhmä on suositellut. Näiden vähimmäisvaatimusten yhteydessä ITSEFin olisi kyettävä suorittamaan erityyppisiä hyökkäyksiä, jotka on esitetty yhteisten kriteerien asiakirjassa hyökkäyspotentiaalin soveltamisesta tietoturvaboksilla varustettuihin laitteisiin (*Application of Attack Potential to Hardware Devices with Security Boxes*). Näihin valmiuksiin kuuluvat arvioijan tiedot ja taidot sekä välineet ja arviointimenetelmät, joita tarvitaan erityyppisten hyökkäysten määrittämiseen ja arviointiin.

(21) Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen olisi seurattava, että sertifiointielimet, ITSEF ja sertifikaattien haltijat noudattavat tästä asetuksesta ja asetuksesta (EU) 2019/881 johtuvia velvoitteitaan. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen olisi käytettävä kaikkia tähän tarkoitukseen soveltuvia tietolähteitä, mukaan lukien sertifiointiprosessin osallistujilta saatavat tiedot ja omat selvitykset.

(22) Sertifiointielinten olisi tehtävä yhteistyötä asianomaisten markkinavalvontaviranomaisten kanssa ja otettava huomioon mahdolliset haavoittuvuustiedot, joilla voi olla merkitystä tieto- ja viestintätekniikan tuotteille, joille ne ovat myöntäneet sertifikaatteja. Sertifiointielinten olisi seurattava sertifioimiaan suojausprofiileja selvittääkseen, vastaavatko tieto- ja viestintätekniikan tuoteluokalle asetetut turvallisuusvaatimukset edelleen uhkaympäristön viimeaikaista kehitystä.

(23) Kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten olisi velvoitteiden noudattamisen seuraamisessa tehtävä yhteistyötä asianomaisten markkinavalvontaviranomaisten kanssa Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 58 artiklan ja Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/1020 ([4]) mukaisesti. Unionin talouden toimijoilla on velvollisuus jakaa tietoja ja tehdä yhteistyötä markkinavalvontaviranomaisten kanssa asetuksen 2019/1020 4 artiklan 3 kohdan nojalla.

([3]) *Joint Interpretation Library: Minimum ITSEF Requirements for Security Evaluations of Smart cards and similar devices*, versio 2.1, helmikuu 2020, saatavilla sogis.eu -sivustolla.

([4]) Euroopan parlamentin ja neuvoston asetus (EU) 2019/1020, annettu 20 päivänä kesäkuuta 2019, markkinavalvonnasta ja tuotteiden vaatimustenmukaisuudesta sekä direktiivin 2004/42/EY ja asetusten (EY) N:o 765/2008 ja (EU) N:o 305/2011 muuttamisesta (EUVL L 169, 25.6.2019, s. 1).

(24) Sertifiointielinten olisi seurattava, että sertifikaatin haltijat noudattavat velvoitteita ja että kaikki EUCC:n nojalla myönnetyt sertifikaatit ovat vaatimusten mukaisia. Seurannalla olisi varmistettava, että kaikkia ITSEFin laatimia arviointiraportteja ja niissä tehtyjä päätelmiä sekä arviointiperusteita ja -menetelmiä sovelletaan johdonmukaisesti ja oikein kaikissa sertifiointitoimissa.

(25) Jos havaitaan mahdollisia velvoitteiden noudattamatta jättämisiä, jotka vaikuttavat sertifioituun tieto- ja viestintätekniikan tuotteeseen, on tärkeää varmistaa oikeasuhteinen reagointi. Sertifikaattien voimassaolo voidaan tästä syystä keskeyttää. Keskeyttämisestä tulisi seurata tiettyjä rajoituksia kyseessä olevan tieto- ja viestintätekniikan tuotteen markkinoinnille ja käytölle, mutta se ei saisi vaikuttaa sertifikaatin voimassaoloon. EU-sertifikaatin haltijan olisi ilmoitettava keskeyttämisestä kulloistenkin tieto- ja viestintätekniikan tuotteiden ostajille, ja toimivaltaisen kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen olisi ilmoitettava siitä asianomaisille markkinavalvontaviranomaisille. Yleisölle tiedottamiseksi ENISAn olisi julkaistava tiedot keskeyttämisestä erityisellä verkkosivustolla.

(26) EUCC-sertifikaatin haltijan olisi pantava täytäntöön tarvittavat haavoittuvuuksien hallintamenettelyt ja varmistettava, että nämä menettelyt on sisällytetty sen organisaatioon. Kun EUCC-sertifikaatin haltija saa tiedon mahdollisesta haavoittuvuudesta, sen olisi tehtävä haavoittuvuutta koskeva vaikutusanalyysi. Jos haavoittuvuutta koskeva vaikutusanalyysi vahvistaa, että haavoittuvuutta voidaan käyttää hyväksi, sertifikaatin haltijan tulisi lähettää arvioinnista raportti sertifiointielimelle, jonka tulisi puolestaan ilmoittaa asiasta kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle. Raportissa tulee antaa tietoa haavoittuvuuden vaikutuksista, tarvittavista muutoksista tai tarvittavista korjaavista ratkaisuista, mukaan lukien haavoittuvuuden mahdolliset laajemmat vaikutukset samoin kuin korjaavat ratkaisut muille tuotteille. Haavoittuvuuden julkistamismenettelyä olisi tarvittaessa täydennettävä standardilla EN ISO/IEC 29147.

(27) Vaatimustenmukaisuuden arviointilaitokset ja kansalliset kyberturvallisuussertifioinnin myöntävät viranomaiset saavat sertifiointia varten käyttöönsä luottamuksellisia ja arkaluonteisia tietoja ja liikesalaisuuksia, jotka liittyvät myös immateriaalioikeuksiin tai velvoitteiden noudattamisen valvontaan ja jotka vaativat asianmukaista suojaamista. Niillä tulisi sen vuoksi olla tarvittava tekninen osaaminen ja tietämys, ja niiden tulisi ottaa käyttöön järjestelmät tietojen suojaamiseksi. Tietojen suojaamista koskevien vaatimusten ja edellytysten olisi täytyttävä sekä akkreditoinnin että valtuutuksen osalta.

(28) ENISAn tulisi antaa luettelo sertifioiduista suojausprofiileista kyberturvallisuussertifioinnin verkkosivustollaan ja ilmoitettava niiden tila asetuksen (EU) 2019/881 mukaisesti.

(29) Tässä asetuksessa vahvistetaan edellytykset kolmansien maiden kanssa tehtäville vastavuoroista tunnustamista koskeville sopimuksille. Tällaiset vastavuoroista tunnustamista koskevat sopimukset voivat olla kahden- tai monenvälisiä ja niiden olisi korvattava nykyisin voimassa olevat vastaavat sopimukset. Jotta voidaan helpottaa sujuvaa siirtymistä tällaisiin vastavuoroista tunnustamista koskeviin sopimuksiin, jäsenvaltiot voivat jatkaa nykyisiä yhteistyöjärjestelyjä kolmansien maiden kanssa rajoitetun ajan.

(30) EUCC-sertifikaatteja varmuustasolla ”korkea” myöntäville sertifiointielimille ja tässä yhteydessä kyseeseen tuleville ITSEFeille olisi tehtävä vertaisarviointeja. Vertaisarviointien tavoitteena tulisi olla määrittää, vastaavatko vertaisarvioitavan sertifiointielimen perussääntö ja menettelytavat edelleen EUCC-järjestelmän vaatimuksia. Vertaisarvioinnit eroavat asetuksen (EU) 2019/881 59 artiklassa säädetyistä kansallisille kyberturvallisuussertifioinnin myöntäville viranomaisille tehtävistä vertaisarvioinneista. Vertaisarvioinneissa olisi varmistettava, että sertifiointielimet toimivat johdonmukaisesti ja sertifikaatit ovat yhtä laadukkaita, ja tunnistettava mahdolliset vahvuudet tai heikkoudet sertifiointielinten toiminnassa, myös parhaiden käytäntöjen jakamista silmällä pitäen. Koska sertifiointielimiä on erityyppisiä, olisi sallittava erityyppisiä vertaisarviointeja. Monimutkaisemmissa tapauksissa, esimerkiksi kun sertifiointielimet myöntävät sertifikaatteja eri AVA_VAN-tasoilla, voidaan käyttää erityyppisiä vertaisarviointeja edellyttäen, että kaikki vaatimukset täyttyvät.

(31) Euroopan kyberturvallisuuden sertifiointiryhmällä olisi oltava tärkeä rooli järjestelmän ylläpidossa. Sen olisi toimittava tässä roolissa muun muassa tekemällä yhteistyötä yksityisen sektorin kanssa, perustamalla erikoistuneita alaryhmiä sekä huolehtimalla asiaankuuluvasta valmistelutyöstä ja avusta komission pyynnöstä. Euroopan kyberturvallisuuden sertifiointiryhmällä on tärkeä rooli viimeisintä kehitystä edustavien asiakirjojen hyväksymisessä. Viimeisintä kehitystä edustavien asiakirjojen hyväksymisessä ja vahvistamisessa olisi otettava asianmukaisesti huomioon asetuksen (EU) 2019/881 54 artiklan 1 kohdan c alakohdassa tarkoitetut seikat. Tekniikan osa-alueet ja viimeisintä kehitystä edustavat asiakirjat olisi julkaistava tämän asetuksen liitteessä I.

Viimeisintä kehitystä edustavina asiakirjoina hyväksytyt suojausprofiilit olisi julkaistava liitteessä II. Sen varmistamiseksi, että nämä liitteet ovat dynaamisia, komissio voi muuttaa niitä asetuksen (EU) 2019/881 66 artiklan 2 kohdassa säädettyä menettelyä noudattaen ja ottaen huomioon Euroopan kyberturvallisuuden sertifiointiryhmän lausunnon. Liite III sisältää suositellut suojausprofiilit, jotka eivät tämän asetuksen tullessa voimaan ole viimeisintä kehitystä edustavia asiakirjoja. Ne olisi julkaistava asetuksen (EU) 2019/881 50 artiklan 1 kohdassa tarkoitetulla ENISAn verkkosivustolla.

(32) Tätä asetusta olisi alettava soveltaa 12 kuukauden kuluttua sen voimaantulosta. Tämän asetuksen IV luvun ja liitteen V vaatimukset eivät edellytä siirtymäkautta, minkä vuoksi niitä olisi sovellettava tämän asetuksen voimaantulosta alkaen.

(33) Tässä asetuksessa säädetyt toimenpiteet ovat asetuksen (EY) N:o 2019/881 66 artiklalla perustetun Euroopan kyberturvallisuuden sertifiointikomitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

I LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde ja soveltamisala

Tässä asetuksessa vahvistetaan yhteisiin kriteereihin perustuva eurooppalainen kyberturvallisuuden sertifiointijärjestelmä (European Common Criteria-based cybersecurity certification scheme), jäljempänä ’EUCC’

Tätä asetusta sovelletaan kaikkiin tieto- ja viestintätekniikan tuotteisiin, niiden dokumentaatio mukaan lukien, jotka toimitetaan sertifioitavaksi EUCC:n mukaisesti, sekä kaikkiin suojausprofiileihin, jotka toimitetaan sertifioitavaksi osana tieto- ja viestintätekniikan tuotteiden sertifiointiin johtavaa tieto- ja viestintätekniikan prosessia.

2 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

1) ’yhteisillä kriteereillä’ (Common Criteria) tietoteknologian turvallisuuden arviointia koskevia yhteisiä kriteerejä (Common Criteria for Information Technology Security Evaluation), jotka on vahvistettu ISO-standardissa ISO/IEC 15408;

2) ’yhteisillä arviointimenetelmillä’ (Common Evaluation Methodology) tietoteknologian turvallisuuden arviointia koskevia yhteisiä menetelmiä (Common Methodology for Information Technology Security Evaluation), jotka on vahvistettu ISO/IEC-standardissa ISO/IEC 18045;

3) ’arvioinnin kohteella’ (*target of evaluation*, TOE) tieto- ja viestintätekniikan tuotetta tai sen osaa taikka osana tieto- ja viestintätekniikan prosessia suojausprofiilia, jolle tehdään kyberturvallisuusarviointi EUCC-sertifioinnin saamiseksi;

4) ’turvatavoitteella’ (*security target*, ST) toteutuksesta riippuvaisten turvallisuusvaatimusten kuvausta tietylle tieto- ja viestintätekniikan tuotteelle;

5) ’suojausprofiililla’ (*protection profile*, PP) tieto- ja viestintätekniikan prosessia, jossa vahvistetaan turvallisuusvaatimukset yksittäiselle tieto- ja viestintätekniikan tuotteiden luokalle ja joka vastaa toteutuksesta riippumattomiin turvallisuustarpeisiin ja jota voidaan käyttää arvioitaessa kyseiseen luokkaan kuuluvia tieto- ja viestintätekniikan tuotteita niiden sertifioimiseksi;

6) ’teknisellä arviointiraportilla’ ITSEFin laatimaa asiakirjaa, jossa esitetään tieto- ja viestintätekniikan tuotteen tai suojausprofiilin arvioinnin aikana saadut havainnot, päätelmät ja perustelut tässä asetuksessa vahvistettujen sääntöjen ja velvoitteiden mukaisesti;

7) ’ITSEFillä’ tietotekniikan turvallisuuden arviointilaitosta (Information Technology Security Evaluation Facility), joka on asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa määritelty vaatimustenmukaisuuden arviointilaitos ja joka suorittaa arviointitehtäviä;

8) ’AVA_VAN-tasolla’ haavoittuvuusanalyysin tasoa, joka ilmaisee, minkä asteisesti kyberturvallisuuden arviointitoimia on suoritettu sen määrittämiseksi, minkä tasoinen on kyky vastustaa virheiden tai heikkouksien potentiaalista hyväksikäyttöä arvioinnin kohteessa sen toimintaympäristössä siten kuin yhteisissä kriteereissä on määritelty;

9) ’EUCC-sertifikaatilla’ kyberturvallisuussertifikaattia, joka myönnetään EUCC:n mukaisesti tieto- ja viestintätekniikan tuotteille tai suojausprofiileille, joita voidaan käyttää yksinomaan tieto- ja viestintätekniikan tuotteiden sertifiointiin liittyvässä tieto- ja viestintätekniikan prosessissa;

10) ’yhdistetyllä tuotteella’ tieto- ja viestintätekniikan tuotetta, joka arvioidaan yhdessä toisen sen perustana olevan tieto- ja viestintätekniikan tuotteen kanssa, joka on jo saanut EUCC-sertifikaatin ja jonka turvallisuustoiminnoista yhdistetty tuote on riippuvainen;

11) ’kansallisella kyberturvallisuussertifioinnin myöntävällä viranomaisella’ jäsenvaltion asetuksen (EU) 2019/881 58 artiklan 1 kohdan nojalla nimeämää viranomaista;

12) ’sertifiointielimellä’ asetuksen (EY) N:o 765/2008 2 artiklan 13 alakohdassa määriteltyä vaatimustenmukaisuuden arviointilaitosta, joka toteuttaa sertifiointitoimia;

13) ’tekniikan osa-alueella’ tiettyyn teknologiaan liittyvää yhteistä teknistä kehystä yhdenmukaistettua sertifiointia varten, mihin sisältyvät ominaiset turvallisuusvaatimukset;

14) ’viimeisintä kehitystä edustavalla asiakirjalla’ asiakirjaa, jossa täsmennetään arviointimenetelmät, -tekniikat ja -välineet, joita sovelletaan tieto- ja viestintätekniikan tuotteiden sertifiointiin tai turvallisuusvaatimuksiin yleiselle tieto- ja viestintätekniikan tuoteluokalle, taikka muut sertifiointiin tarvittavat vaatimukset arvioinnin yhdenmukaistamiseksi yksittäisillä tekniikan osa-alueilla tai yksittäisille suojausprofiileille;

15) ’markkinavalvontaviranomaisella’ asetuksen (EU) 2019/1020 3 artiklan 4 alakohdassa määriteltyä viranomaista.

3 artikla

Arviointistandardit

EUCC-järjestelmässä suoritettaviin arviointeihin sovelletaan seuraavia standardeja:

a) yhteiset perusteet (Common Criteria);

b) yhteiset arviointimenetelmät (Common Evaluation Methodology).

4 artikla

Varmuustasot

1. Sertifiointielimet myöntävät EUCC-sertifikaatteja varmuustasolla ”korotettu” tai ”korkea”.

2. EUCC-sertifikaatit vastaavat varmuustasolla ”korotettu” sertifikaatteja tasolla AVA_VAN 1 tai 2.

3. EUCC-sertifikaatit vastaavat varmuustasolla ”korkea” sertifikaatteja tasolla AVA_VAN 3, 4 tai 5.

4. EUCC-sertifikaatissa vahvistetussa varmuustasossa on tehtävä ero turvallisuuden varmistuksen komponenttien vaatimustenmukaisen ja laajennetun käytön välillä siten kuin yhteisissä kriteereissä liitteen VIII mukaisesti täsmennetään.

5. Vaatimustenmukaisuuden arviointilaitosten on sovellettava niitä turvallisuuden varmistuksen komponentteja, joista valittu AVA_VAN-taso riippuu 3 artiklassa tarkoitettujen standardien mukaisesti.

5 artikla

Tieto- ja viestintätekniikan tuotteiden sertifiointimenetelmät

1. Tieto- ja viestintätekniikan tuotteen sertifiointi on suoritettava suhteessa sen turvatavoitteeseen,

a) jonka hakija on määritellyt; tai

b) johon sisältyy sertifioitu suojausprofiili osana tieto- ja viestintätekniikan prosessia, jos tieto- ja viestintätekniikan tuote kuuluu kyseisen suojausprofiilin kattamaan tieto- ja viestintätekniikan tuotteiden luokkaan.

2. Suojausprofiilit on sertifioitava yksinomaan sellaisten tieto- ja viestintätekniikan tuotteiden sertifiointia varten, jotka kuuluvat erityiseen suojausprofiilin kattamien tieto- ja viestintätekniikan tuotteiden luokkaan.

6 artikla

Vaatimustenmukaisuuden itsearviointi

Asetuksen (EU) 2019/881 53 artiklassa tarkoitettua vaatimustenmukaisuuden itsearviointia ei sallita.

II LUKU

TIETO- JA VIESTINTÄTEKNIIKAN TUOTTEIDEN SERTIFIOINTI

I JAKSO

ERITYISET STANDARDIT JA VAATIMUKSET ARVIOINTIA VARTEN

7 artikla

Tieto- ja viestintätekniikan tuotteiden arviointiperusteet ja -menetelmät

1. Sertifioitavaksi toimitettu tieto- ja viestintätekniikan tuote on arvioitava vähintään seuraavien mukaisesti:

a) 3 artiklassa tarkoitetut standardit soveltuvin osin;

b) turvallisuusvarmistusvaatimusten luokat haavoittuvuusarviointia ja riippumatonta toiminnallista testausta varten siten kuin määritellään 3 artiklassa tarkoitetuissa arviointistandardeissa;

c) kyseessä olevien tieto- ja viestintätekniikan tuotteiden käyttötarkoitukseen liittyvän riskin taso asetuksen (EU) 2019/881 52 artiklan mukaisesti ja niiden turvallisuustoiminnot, jotka tukevat asetuksen (EU) 2019/881 51 artiklassa vahvistettuja turvallisuustavoitteita;

d) liitteessä I luetellut sovellettavat viimeisintä kehitystä edustavat asiakirjat; ja

e) liitteessä II luetellut sovellettavat sertifioidut suojausprofiilit.

2. Asianmukaisesti perustelluissa poikkeustapauksissa vaatimustenmukaisuuden arviointilaitos voi pyytää, että se jättää soveltamatta asiaankuuluvaa viimeisintä kehitystä edustavaa asiakirjaa. Tällaisissa tapauksissa vaatimustenmukaisuuden arviointilaitoksen on ilmoitettava asiasta kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle ja perusteltava pyyntönsä asianmukaisesti. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on arvioitava

poikkeuksen perustelut ja hyväksyttävä se, mikäli se katsotaan perustelluksi. Vaatimustenmukaisuuden arviointilaitos ei saa myöntää sertifikaattia ennen kuin kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen on tehnyt päätöksensä. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilmoitettava hyväksytystä poikkeuksesta ilman aiheetonta viivytystä Euroopan kyberturvallisuuden sertifiointiryhmälle, joka voi antaa lausunnon. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on otettava Euroopan kyberturvallisuuden sertifiointiryhmän lausunto mahdollisimman tarkasti huomioon.

3. Tieto- ja viestintätekniikan tuotteiden sertifiointi AVA_VAN-tasolla 4 tai 5 on mahdollista vain seuraavissa skenaarioissa:

a) jos tieto- ja viestintätekniikan tuote kuuluu johonkin liitteessä I lueteltuun tekniikan osa-alueeseen, se on arvioitava kyseisten teknisten alojen sovellettavien viimeisintä kehitystä edustavien asiakirjojen mukaisesti,

b) jos tieto- ja viestintätekniikan tuote kuuluu tieto- ja viestintätekniikan tuoteluokkaan, jota koskee AVA_VAN-tasot 4 tai 5 käsittävä ja liitteessä II viimeisintä kehitystä edustavana suojausprofiilina mainittu sertifioitu suojausprofiili, se on arvioitava kyseiselle suojausprofiilille määritettyjen arviointimenetelmien mukaisesti,

c) jos tämän kohdan a ja b alakohtaa ei voida soveltaa ja jos tekniikan osa-alueen sisällyttäminen liitteeseen I tai sertifioidun suojaprofiilin sisällyttäminen liitteeseen II on epätodennäköistä lähitulevaisuudessa ja ainoastaan asianmukaisesti perustelluissa poikkeustapauksissa 4 kohdassa säädetyin edellytyksin.

4. Jos vaatimustenmukaisuuden arviointilaitos katsoo, että sitä koskee 3 kohdan c alakohdassa tarkoitettu asianmukaisesti perusteltu poikkeustapaus, sen on ilmoitettava suunnitellusta sertifioinnista kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle perusteluineen ja ilmoitettava ehdotetut arviointimenetelmät. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on arvioitava poikkeuksen perustelut ja, jos se katsotaan perustelluksi, hyväksyttävä arviointimenetelmät tai muutettava arviointimenetelmiä, joita vaatimustenmukaisuuden arviointilaitos aikoo soveltaa. Vaatimustenmukaisuuden arviointilaitos ei saa myöntää sertifikaattia ennen kuin kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen on tehnyt päätöksensä. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on raportoitava suunnitellusta sertifioinnista ilman aiheetonta viivytystä Euroopan kyberturvallisuuden sertifiointiryhmälle, joka voi antaa lausunnon. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on otettava Euroopan kyberturvallisuuden sertifiointiryhmän lausunto mahdollisimman tarkasti huomioon.

5. Jos on kyse tieto- ja viestintätekniikan tuotteesta, joka arvioidaan yhdistettynä tuotteena asiaankuuluvien viimeisintä kehitystä edustavien asiakirjojen mukaisesti, sen perustana olevan tieto- ja viestintätekniikan tuotteen arvioinnin suorittaneen ITSEFin on jaettava tarvittavat tiedot yhdistetyn tuotteen arvioinnin suorittavan ITSEFin kanssa.

II JAKSO

EUCC-SERTIFIKAATTIEN MYÖNTÄMINEN, UUSIMINEN JA PERUUTTAMINEN

8 artikla

Sertifiointiin tarvittavat tiedot

1. EUCC:n mukaista sertifiointia hakevan on toimitettava sertifiointielimelle tai ITSEFille tai muulla tavoin asetettava niiden saataville kaikki sertifiointitoimia varten tarvittavat tiedot.

2. Edellä 1 kohdassa tarkoitettujen tietojen on sisällettävä yhteisten kriteerien ja yhteisten arviointimenetelmien jaksojen ”Kehittäjän toiminnan elementit” (”Developer action elements”) mukaisesti ja jaksoissa ”Evidenssin sisällön ja esittämisen elementti” (”Content and presentation of evidence element”) esitetyssä muodossa kaikki asiaankuuluva evidenssi valitulle varmuustasolle ja siihen liittyville turvallisuusvarmistusvaatimuksille. Evidenssin on tarvittaessa sisällettävä yksityiskohtaiset tiedot tieto- ja viestintätekniikan tuotteesta ja sen lähdekoodista tämän asetuksen mukaisesti sillä edellytyksellä, että sovelletaan suojatoimia luvattoman ilmitulon estämiseksi.

3. Sertifioinnin hakijat voivat toimittaa sertifiointielimelle ja ITSEFille tarvittavat arviointitulokset aikaisemmasta sertifioinnista seuraavien mukaisesti:

a) tämä asetus;

b) jokin muu asetuksen (EU) 2019/881 49 artiklan nojalla hyväksytty eurooppalainen kyberturvallisuuden sertifiointijärjestelmä;

c) tämän asetuksen 49 artiklassa tarkoitettu kansallinen järjestelmä.

4. Jos arviointitulokset ovat ITSEFin tehtävien kannalta merkityksellisiä, se voi käyttää arviointituloksia uudelleen edellyttäen, että ne vastaavat sovellettavia vaatimuksia ja että niiden aitous vahvistetaan.

5. Jos sertifiointielin sallii, että tuote voidaan sertifioida yhdistettynä tuotteena, sertifioinnin hakijan on asetettava sertifiointielimen ja ITSEFin saataville kaikki tarvittavat tiedot viimeisintä kehitystä edustavien asiakirjojen mukaisesti.

6. Sertifioinnin hakijoiden on myös toimitettava sertifiointielimelle ja ITSEFille seuraavat tiedot:

a) linkki hakijan verkkosivustolle, joka sisältää asetuksen (EU) 2019/881 55 artiklassa tarkoitetut täydentävät kyberturvallisuustiedot;

b) kuvaus hakijan käyttämistä haavoittuvuuksien hallinta- ja julkistamismenettelyistä.

7. Sertifiointielimen, ITSEFin ja hakijan on säilytettävä kaikki asiaankuuluva tässä artiklassa tarkoitettu dokumentaatio viiden vuoden ajan sertifikaatin voimassaolon päättymisestä.

9 artikla

EUCC-sertifikaatin myöntämisedellytykset

1. Sertifiointielinten on myönnettävä EUCC-sertifikaatti, jos kaikki seuraavat edellytykset täyttyvät:

a) tieto- ja viestintätekniikan tuotteen luokka kuuluu sertifiointiin osallistuvan sertifiointielimen ja ITSEFin akkreditoinnin ja tapauksen mukaan valtuutuksen piiriin;

b) sertifioinnin hakija on allekirjoittanut vakuutuksen, jossa sitoudutaan kaikkiin 2 kohdassa lueteltuihin sitoumuksiin;

c) ITSEF on saattanut arvioinnin päätökseen ilman vastalauseita 3 ja 7 artiklassa tarkoitettujen arviointistandardien, -perusteiden ja -menetelmien mukaisesti;

d) sertifiointielin on saattanut arvioinnin tulosten tarkastelun päätökseen ilman vastalauseita;

e) sertifiointielin on varmistanut, että ITSEFin toimittamat tekniset arviointiraportit vastaavat toimitettua evidenssiä ja että 3 ja 7 artiklassa tarkoitettuja arviointistandardeja, -perusteita ja -menetelmiä on sovellettu oikein.

2. Sertifioinnin hakijan on annettava sitoumukset

a) toimittaa sertifiointielimelle ja ITSEFille kaikki tarvittavat täydelliset ja paikkansapitävät tiedot ja antaa pyynnöstä tarvittavat lisätiedot;

b) olla markkinoimatta tieto- ja viestintätekniikan tuotetta EUCC:n mukaisesti sertifioituna ennen EUCC-sertifikaatin myöntämistä;

c) markkinoida tieto- ja viestintätekniikan tuotetta sertifioituna ainoastaan EUCC-sertifikaatin mukaisessa laajuudessa;

d) lopettaa välittömästi tieto- ja viestintätekniikan tuotteen markkinoiminen sertifioituna, jos EUCC-sertifikaatti peruutetaan tai jos sen voimassaolo keskeytyy tai päättyy;

e) varmistaa, että EUCC-sertifikaattiin viitaten myytävät tieto- ja viestintätekniikan tuotteet ovat täysin vastaavia kuin sertifioinnin kohteena oleva tieto- ja viestintätekniikan tuote;

f) noudattaa 11 artiklan mukaisesti EUCC-sertifikaattia varten vahvistettuja sääntöjä merkin ja merkinnän käytöstä.

3. Jos on kyse tieto- ja viestintätekniikan tuotteesta, joka sertifioidaan yhdistettynä tuotteena asiaankuuluvien viimeisintä kehitystä edustavien asiakirjojen mukaisesti, sen perustana olevan tieto- ja viestintätekniikan tuotteen sertifioinnin suorittaneen sertifiointielimen on jaettava tarvittavat tiedot yhdistetyn tuotteen sertifioinnin suorittavan sertifiointielimen kanssa.

10 artikla

EUCC-sertifikaatin sisältö ja muoto

1. EUCC-sertifikaatissa on oltava vähintään liitteessä VII esitetyt tiedot.

2. EUCC-sertifikaatissa tai sertifiointiraportissa on yksiselitteisesti täsmennettävä sertifioidun tieto- ja viestintätekniikan tuotteen soveltamisala ja rajoitukset ja ilmoitettava, onko koko tieto- ja viestintätekniikan tuote sertifioitu vaiko pelkästään osia siitä.

3. Sertifiointielimen on toimitettava hakijalle EUCC-sertifikaatti vähintään sähköisessä muodossa.

4. Sertifiointielimen on laadittava liitteen V mukainen sertifiointiraportti jokaisesta antamastaan EUCC-sertifikaatista. Sertifiointiraportin on perustuttava ITSEFin antamaan tekniseen arviointiraporttiin. Teknisessä arviointiraportissa ja sertifiointiraportissa on ilmoitettava 7 artiklassa tarkoitetut arvioinnissa käytetyt erityiset arviointiperusteet ja -menetelmät.

5. Sertifiointielimen on toimitettava kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle ja ENISAlle kaikki EUCC-sertifikaatit ja kaikki sertifiointiraportit sähköisessä muodossa.

11 artikla

Merkki ja merkintä

1. Sertifikaatin haltija voi kiinnittää merkin ja merkinnän sertifioituun tieto- ja viestintätekniikan tuotteeseen. Merkki ja merkintä osoittavat, että tieto- ja viestintätekniikan tuote on sertifioitu tämän asetuksen mukaisesti. Merkki ja merkintä on kiinnitettävä tämän artiklan ja liitteen IX mukaisesti.

2. Merkki ja merkintä on kiinnitettävä tieto- ja viestintätekniikan tuotteeseen tai sen arvokilpeen näkyvästi, helposti luettavasti ja pysyvästi. Jos tämä ei tuotteen luonteen vuoksi ole mahdollista tai perusteltua, se on kiinnitettävä pakkaukseen ja tuotteen mukana oleviin asiakirjoihin. Jos sertifioitu tieto- ja viestintätekniikan tuote toimitetaan ohjelmistona, merkin ja merkinnän on oltava näkyvästi, helposti luettavasti ja pysyvästi sen mukana seuraavissa asiakirjoissa tai nämä asiakirjat on asetettava helposti ja suoraan käyttäjien saataville verkkosivuston kautta.

3. Merkki ja merkintä on esitettävä liitteen IX mukaisesti, ja niissä on oltava:

a) sertifioidun tieto- ja viestintätekniikan tuotteen varmuustaso ja AVA_VAN-taso;

b) sertifikaatin yksilöllinen tunniste, joka muodostuu seuraavista:

   1) järjestelmän nimi;

   2) sertifikaatin myöntäneen sertifiointielimen nimi ja akkreditoinnin viitenumero.

   3) myöntämisvuosi ja -kuukausi;

   4) sertifikaatin myöntäneen sertifiointielimen antama tunnistenumero.

4. Merkin ja merkinnän mukana on oltava QR-koodi, josta on linkki vähintään seuraavat tiedot sisältävälle verkkosivustolle:

a) tiedot sertifikaatin voimassaolosta;

b) tarvittavat sertifiointitiedot liitteiden V ja VII mukaisesti;

c) tiedot, jotka sertifikaatin haltijan on asetettava julkisesti saataville asetuksen (EU) 2019/881 55 artiklan mukaisesti; ja

d) tarvittaessa aikaisemmat tiedot liittyen tieto- ja viestintätekniikan tuotteen yksittäiseen sertifiointiin tai sertifiointeihin jäljitettävyyden mahdollistamiseksi.

12 artikla

EUCC-sertifikaatin voimassaoloaika

1. Sertifiointielimen on vahvistettava kunkin myönnetyn EUCC-sertifikaatin voimassaoloaika ottaen huomioon sertifioidun tieto- ja viestintätekniikan tuotteen ominaisuudet.

2. EUCC-sertifikaatti on voimassa enintään viisi vuotta.

3. Poiketen siitä, mitä 2 kohdassa säädetään, voimassaoloaika voi olla pidempi kuin viisi vuotta, jos kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen antaa siihen ennakkohyväksynnän. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilmoitettava myönnetystä hyväksynnästä Euroopan kyberturvallisuuden sertifiointiryhmälle ilman aiheetonta viivytystä.

13 artikla

EUCC-sertifikaatin tarkastaminen

1. Sertifiointielin voi sertifikaatin haltijan pyynnöstä tai muista perustelluista syistä päättää tarkastaa tieto- ja viestintätekniikan tuotteen EUCC-sertifikaatin. Tarkastus tapahtuu liitteen IV mukaisesti. Sertifiointielin määrittää tarkastuksen laajuuden. Jos tarkastus sitä edellyttää, sertifiointielimen on pyydettävä ITSEFiä suorittamaan uudelleenarviointi sertifioidusta tieto- ja viestintätekniikan tuotteesta.

2. Tarkastuksen ja tapauksen mukaan uudelleenarvioinnin tulosten perusteella sertifiointielin:

a) vahvistaa EUCC-sertifikaatin;

b) peruuttaa EUCC-sertifikaatin 14 artiklan mukaisesti;

c) peruuttaa EUCC-sertifikaatin 14 artiklan mukaisesti ja myöntää uuden EUCC-sertifikaatin samassa laajuudessa ja pidemmälle voimassaoloajalle; tai

d) peruuttaa EUCC-sertifikaatin 14 artiklan mukaisesti ja myöntää uuden EUCC-sertifikaatin eri laajuudessa.

3. Sertifiointielin voi päättää keskeyttää EUCC-sertifikaatin voimassaolon ilman aiheetonta viivytystä 30 artiklan mukaisesti, kunnes EUCC-sertifikaatin haltija toteuttaa korjaavia toimia.

14 artikla

EUCC-sertifikaatin peruuttaminen

1. EUCC-sertifikaatin peruuttaa sen myöntänyt sertifiointielin, sanotun kuitenkaan rajoittamatta asetuksen (EU) 2019/881 58 artiklan 8 kohdan e alakohdan soveltamista.

2. Edellä 1 kohdassa tarkoitetun sertifiointielimen on ilmoitettava kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle sertifikaatin peruuttamisesta. Sen on myös ilmoitettava ENISAlle tällaisesta peruuttamisesta, jotta se voi helpommin suorittaa asetuksen (EU) 2019/881 50 artiklan mukaisen tehtävänsä. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilmoitettava asiasta muille asianomaisille markkinavalvontaviranomaisille.

3. EUCC-sertifikaatin haltija voi pyytää sertifikaatin peruuttamista.

III LUKU

SUOJAUSPROFIILIEN SERTIFIOINTI

I JAKSO

ERITYISET STANDARDIT JA VAATIMUKSET ARVIOINTIA VARTEN

15 artikla

Arviointiperusteet ja -menetelmät

1. Suojausprofiili on arvioitava vähintään seuraavien mukaisesti:

a) 3 artiklassa tarkoitetut standardit soveltuvin osin;

b) kyseessä olevien tieto- ja viestintätekniikan tuotteiden käyttötarkoitukseen liittyvän riskin taso asetuksen (EU) 2019/881 52 artiklan mukaisesti ja niiden turvallisuustoiminnot, jotka tukevat mainitun asetuksen 51 artiklassa vahvistettuja turvallisuustavoitteita; ja

c) liitteessä I luetellut sovellettavat viimeisintä kehitystä edustavat asiakirjat. Yksittäisen tekniikan osa-alueen kattama suojausprofiili on sertifioitava kyseisen tekniikan osa-alueen vaatimusten mukaisesti.

2. Asianmukaisesti perustelluissa poikkeustapauksissa vaatimustenmukaisuuden arviointilaitos voi sertifioida suojausprofiilin soveltamatta asiaankuuluvia viimeisintä kehitystä edustavia asiakirjoja. Tällaisissa tapauksissa sen on ilmoitettava asiasta toimivaltaiselle kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle ja esitettävä perustelut suunnitellulle sertifioinnille, jossa ei sovelleta asiaankuuluvia viimeisintä kehitystä edustavia asiakirjoja, sekä ilmoitettava ehdotetut arviointimenetelmät. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on arvioitava perustelut ja, jos se katsotaan perustelluksi, hyväksyttävä asiaankuuluvien viimeisintä kehitystä edustavien asiakirjojen soveltamatta jättäminen sekä hyväksyttävä arviointimenetelmät tai tarvittaessa muutettava arviointimenetelmiä, joita vaatimustenmukaisuuden arviointilaitos aikoo soveltaa. Vaatimustenmukaisuuden arviointilaitos ei saa myöntää sertifikaattia suojausprofiilille ennen kuin kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen on tehnyt päätöksensä. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilmoitettava hyväksytystä viimeisintä kehitystä edustavien asiakirjojen soveltamatta jättämisestä ilman aiheetonta viivytystä Euroopan kyberturvallisuuden sertifiointiryhmälle, joka voi antaa lausunnon. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on otettava Euroopan kyberturvallisuuden sertifiointiryhmän lausunto mahdollisimman tarkasti huomioon.

II JAKSO

SUOJAUSPROFIILEJA KOSKEVIEN EUCC-SERTIFIKAATTIEN MYÖNTÄMINEN, UUSIMINEN JA PERUUTTAMINEN

16 artikla

Suojausprofiilien sertifiointiin tarvittavat tiedot

Suojausprofiilin sertifiointia hakevan on toimitettava sertifiointielimelle tai ITSEFille tai muulla tavoin asetettava niiden saataville kaikki sertifiointitoimia varten tarvittavat tiedot. Edellä olevan 8 artiklan 2, 3, 4 ja 7 kohtaa sovelletaan soveltuvin osin.

17 artikla

EUCC-sertifikaattien myöntäminen suojausprofiileille

1. Sertifiointia hakevan on toimitettava sertifiointielimelle ja ITSEFille kaikki tarvittavat täydelliset ja paikkansapitävät tiedot.

2. Edellä olevaa 9 ja 10 artiklaa sovelletaan soveltuvin osin.

3. ITSEFin on arvioitava, onko suojausprofiili täydellinen, johdonmukainen, teknisesti luotettava ja tehokas kyseisen suojausprofiilin kattaman tieto- ja viestintätekniikan tuotteen luokan käyttötarkoitukseen ja turvallisuustavoitteisiin nähden.

4. Suojausprofiilin sertifioi ainoastaan:

a) kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen tai muu sertifiointielimeksi akkreditoitu julkinen elin; tai

b) sertifiointielin, joka on saanut kansalliselta kyberturvallisuussertifioinnin myöntävältä viranomaiselta etukäteen hyväksynnän kunkin yksittäisen suojausprofiilin osalta.

18 artikla

EUCC-sertifikaatin voimassaoloaika suojausprofiileille

1. Sertifiointielimen on vahvistettava voimassaoloaika kullekin EUCC-sertifikaatille.

2. Voimassaoloaika voi olla enintään kyseisen suojausprofiilin käyttöikä.

19 artikla

Suojausprofiilien EUCC-sertifikaatin tarkastaminen

1. Sertifiointielin voi sertifikaatin haltijan pyynnöstä tai muista perustelluista syistä päättää tarkastaa suojausprofiilin EUCC-sertifikaatin. Tarkastus suoritetaan 15 artiklassa säädettyjen edellytysten mukaisesti. Sertifiointielin määrittää tarkastuksen laajuuden. Jos tarkastus sitä edellyttää, sertifiointielimen on pyydettävä ITSEFiä suorittamaan uudelleenarviointi sertifioidusta suojausprofiilista.

2. Tarkastuksen tulosten ja tapauksen mukaan uudelleenarvioinnin tulosten perusteella sertifiointielin toteuttaa jonkin seuraavista toimista:

a) vahvistaa EUCC-sertifikaatin;

b) peruuttaa EUCC-sertifikaatin 20 artiklan mukaisesti;

c) peruuttaa EUCC-sertifikaatin 20 artiklan mukaisesti ja myöntää uuden EUCC-sertifikaatin samassa laajuudessa ja pidemmälle voimassaoloajalle;

d) peruuttaa EUCC-sertifikaatin 20 artiklan mukaisesti ja myöntää uuden EUCC-sertifikaatin eri laajuudessa.

20 artikla

Suojausprofiilin EUCC-sertifikaatin peruuttaminen

1. Suojausprofiilin EUCC-sertifikaatin peruuttaa sen myöntänyt sertifiointielin, sanotun kuitenkaan rajoittamatta asetuksen (EU) 2019/881 58 artiklan 8 kohdan e alakohdan soveltamista. Edellä olevaa 14 artiklaa sovelletaan soveltuvin osin.

2. Suojausprofiilille 17 artiklan 4 kohdan b alakohdan mukaisesti myönnetyn sertifikaatin peruuttaa kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen, joka hyväksyi kyseisen sertifikaatin.

IV LUKU

VAATIMUSTENMUKAISUUDEN ARVIOINTILAITOKSET

21 artikla

Sertifiointielintä koskevat lisä- tai erityisvaatimukset

1. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on valtuutettava sertifiointielin myöntämään EUCC-sertifikaatteja varmuustasolla ”korkea”, jos kyseinen elin osoittaa asetuksen (EU) 2019/881 60 artiklan 1 kohdassa ja liitteessä säädettyjen vaatimustenmukaisuuden arviointilaitosten akkreditointia koskevien vaatimusten täyttämisen lisäksi täyttävänsä seuraavat edellytykset:

a) sillä on tarvittava asiantuntemus ja pätevyys sertifiointipäätöksen tekemiseksi varmuustasolla ”korkea”;

b) se suorittaa sertifiointitoimensa yhteistyössä 22 artiklan mukaisesti valtuutetun ITSEFin kanssa; ja

c) sillä on tarvittava pätevyys ja käytössä asianmukaiset tekniset ja operatiiviset toimenpiteet luottamuksellisten ja arkaluonteisten tietojen suojaamiseksi tehokkaasti varmuustasolla ”korkea” sen lisäksi, että sovelletaan 43 artiklassa säädettyjä vaatimuksia.

2. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on arvioitava, täyttääkö sertifiointielin kaikki 1 kohdassa säädetyt vaatimukset. Arviointiin on sisällyttävä vähintään jäsennellyt haastattelut ja sertifiointielimen tämän asetuksen mukaisesti suorittaman vähintään yhden pilottisertifioinnin tarkastelu.

Kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen voi arvioinnissaan käyttää uudelleen mitä tahansa tarvittavaa evidenssiä, joka on saatu seuraavien nojalla myönnettyjen ennakkolupien tai vastaavien pohjalta:

a) tämä asetus;

b) jokin muu asetuksen (EU) 2019/881 49 artiklan nojalla hyväksytty eurooppalainen kyberturvallisuuden sertifiointijärjestelmä;

c) tämän asetuksen 49 artiklassa tarkoitettu kansallinen järjestelmä.

3. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on laadittava valtuutusraportti, josta tehdään vertaisarviointi asetuksen (EU) 2019/881 59 artiklan 3 kohdan d alakohdan mukaisesti.

4. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on täsmennettävä tieto- ja viestintätekniikan tuoteluokat ja suojausprofiilit, joita valtuutus koskee. Valtuutus on voimassa enintään akkreditoinnin voimassaoloajan. Se voidaan uusia pyynnöstä edellyttäen, että sertifiointielin täyttää edelleen tässä artiklassa säädetyt vaatimukset. Valtuutuksen uusiminen ei edellytä pilottiarviointeja.

5. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on peruutettava sertifiointielimen valtuutus, jos se ei enää täytä tässä artiklassa säädettyjä edellytyksiä. Kun valtuutus peruutetaan, sertifiointielimen on lopetettava välittömästi toimintansa markkinointi valtuutettuna sertifiointielimenä.

22 artikla

ITSEFiä koskevat lisä- tai erityisvaatimukset

1. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on valtuutettava ITSEF suorittamaan arviointi tieto- ja viestintätekniikan tuotteista, joihin sovelletaan sertifiointia varmuustasolla ”korkea”, jos ITSEF osoittaa asetuksen (EU) 2019/881 60 artiklan 1 kohdassa ja liitteessä säädettyjen vaatimustenmukaisuuden arviointilaitosten akkreditointia koskevien vaatimusten täyttämisen lisäksi täyttävänsä kaikki seuraavat edellytykset:

a) sillä on tarvittava asiantuntemus arviointitoimien suorittamiseksi, jotta voidaan määrittää kyky vastustaa sellaisten tahojen, joilla on merkittävät kyvyt ja resurssit, tekemiä uusinta tekniikkaa hyödyntäviä kyberhyökkäyksiä;

b) liittyen tekniikan osa-alueisiin ja suojausprofiileihin, jotka ovat osa tieto- ja viestintätekniikan prosessia kyseessä oleville tieto- ja viestintätekniikan tuotteille, sillä on

1) asiantuntemus tarvittavien erityisten arviointitoimien suorittamiseksi, jotta voidaan määrittää järjestelmällisesti arvioinnin kohteen kyky vastustaa kyvykkäitä hyökkääjiä sen toimintaympäristössä olettaen, että hyökkäyspotentiaali on ”kohtalainen” (”moderate”) tai ”korkea” (”high”) siten kuin 3 artiklassa tarkoitetuissa standardeissa esitetään;

2) tekninen pätevyys liitteessä I mainittujen viimeisintä kehitystä edustavien asiakirjojen mukaisesti;

c) sillä on tarvittava pätevyys ja käytössä asianmukaiset tekniset ja operatiiviset toimenpiteet luottamuksellisten ja arkaluonteisten tietojen suojaamiseksi tehokkaasti varmuustasolla ”korkea” sen lisäksi, että sovelletaan 43 artiklassa säädettyjä vaatimuksia.

2. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on arvioitava, täyttääkö ITSEF kaikki 1 kohdassa säädetyt vaatimukset. Arviointiin on sisällyttävä vähintään jäsennellyt haastattelut ja ITSEFin tämän asetuksen mukaisesti suorittaman vähintään yhden pilottiarvioinnin tarkastelu.

3. Kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen voi arvioinnissaan käyttää uudelleen mitä tahansa tarvittavaa evidenssiä, joka on saatu seuraavien nojalla myönnettyjen ennakkolupien tai vastaavien pohjalta:

a) tämä asetus;

b) jokin muu asetuksen (EU) 2019/881 49 artiklan nojalla hyväksytty eurooppalainen kyberturvallisuuden sertifiointijärjestelmä;

c) tämän asetuksen 49 artiklassa tarkoitettu kansallinen järjestelmä.

4. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on laadittava valtuutusraportti, josta tehdään vertaisarviointi asetuksen (EU) 2019/881 59 artiklan 3 kohdan d alakohdan mukaisesti.

5. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on täsmennettävä tieto- ja viestintätekniikan tuoteluokat ja suojausprofiilit, joita valtuutus koskee. Valtuutus on voimassa enintään akkreditoinnin voimassaoloajan. Se voidaan uusia pyynnöstä edellyttäen, että ITSEF täyttää edelleen tässä artiklassa säädetyt vaatimukset. Valtuutuksen uusiminen ei edellytä pilottiarviointeja.

6. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on peruutettava ITSEFin valtuutus, jos se ei enää täytä tässä artiklassa säädettyjä edellytyksiä. Kun valtuutus peruutetaan, ITSEFin on lopetettava toimintansa markkinointi valtuutettuna ITSEFinä.

23 artikla

Sertifiointielinten ilmoittaminen

1. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilmoitettava komissiolle alueellaan toimivat sertifiointielimet, joilla on akkreditointinsa perusteella pätevyys sertifiointiin varmuustasolla ”korotettu”.

2. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilmoitettava komissiolle alueellaan toimivat sertifiointielimet, joilla on akkreditointinsa ja valtuutuspäätöksen perusteella pätevyys sertifiointiin varmuustasolla ”korkea”.

3. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on annettava vähintään seuraavat tiedot ilmoittaessaan komissiolle sertifiointielimistä:

a) varmuustaso tai -tasot, joiden osalta sertifiointielin on pätevä myöntämään EUCC-sertifikaatteja;

b) seuraavat akkreditointiin liittyvät tiedot:

1) akkreditoinnin päivämäärä;

2) sertifiointielimen nimi ja osoite;

3) sertifiointielimen rekisteröintimaa;

4) akkreditoinnin viitenumero;

5) akkreditoinnin pätevyysalue ja voimassaoloaika;

6) kansallisen akkreditointielimen osoite, sijainti ja linkki asiaankuuluvalle verkkosivustolle; ja

c) seuraavat tiedot liittyen valtuutukseen tasolla ”korkea”:

1) valtuutuksen myöntämispäivä;

2) valtuutuksen viitenumero;

3) valtuutuksen voimassaoloaika;

4) valtuutuksen soveltamisala, mukaan lukien korkein AVA_VAN-taso ja soveltuvin osa valtuutuksen kattama tekniikan osa-alue.

4. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on lähetettävä jäljennös 1 ja 2 kohdassa tarkoitetusta ilmoituksesta ENISAlle, jotta kyberturvallisuussertifioinnin verkkosivustolla voidaan julkaista paikkansapitävät tiedot sertifiointielinten kelpoisuudesta.

5. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilman aiheetonta viivytystä tutkittava mahdolliset kansallisen akkreditointielimen toimittamat tiedot akkreditointistatuksen muuttumisesta. Jos akkreditointi tai valtuutus on peruutettu, kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilmoitettava siitä komissiolle ja se voi toimittaa komissiolle pyynnön asetuksen (EU) 2019/881 61 artiklan 4 kohdan mukaisesti.

24 artikla

ITSEFin ilmoittaminen

Edellä 23 artiklassa säädettyjä kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten ilmoitusvelvollisuuksia sovelletaan myös ITSEFiin. Ilmoitukseen on sisällyttävä ITSEFin osoite, voimassa oleva akkreditointi ja tapauksen mukaan sen voimassa oleva valtuutus.

V LUKU

SEURANTA, VAATIMUSTENVASTAISUUS JA VELVOITTEIDEN NOUDATTAMATTA JÄTTÄMINEN

I JAKSO

VELVOITTEIDEN NOUDATTAMISEN SEURANTA

25 artikla

Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen seurantatoimet

1. Rajoittamatta asetuksen (EU) 2019/881 58 artiklan 7 kohdan soveltamista kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on seurattava, että

a) sertifiointielin ja ITSEF noudattavat tämän asetuksen ja asetuksen (EU) 2019/881 mukaisia velvoitteitaan;

b) EUCC-sertifikaatin haltijat noudattavat tämän asetuksen ja asetuksen (EU) 2019/881 mukaisia velvoitteitaan;

c) sertifioidut tieto- ja viestintätekniikan tuotteet täyttävät EUCC:n mukaiset vaatimukset;

d) EUCC-sertifikaatissa ilmaistu varmuus vastaa muuttuvaa uhkaympäristöä.

2. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on suoritettava seurantatoimensa erityisesti seuraavien perusteella:

a) sertifiointielimiltä, kansallisilta akkreditointielimiltä ja asianomaisilta markkinavalvontaviranomaisilta saatavat tiedot;

b) tiedot, jotka perustuvat sen omiin tai toisen viranomaisen suorittamiin tarkastuksiin ja tutkimuksiin;

c) jäljempänä olevan 3 kohdan mukaisesti suoritettava otanta;

d) vastaanotetut valitukset.

3. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on yhteistyössä muiden markkinavalvontaviranomaisten kanssa tarkastettava vuosittain riskiarvioinnin perusteella määritetty otos, joka on vähintään 4 prosenttia EUCC-sertifikaateista. Toimivaltaisen kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen pyynnöstä ja sen lukuun sertifiointielinten ja tarvittaessa ITSEFin on avustettava kyseistä viranomaista velvoitteiden noudattamisen seurannassa.

4. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on valittava tarkastettavaksi otos sertifioiduista tieto- ja viestintätekniikan tuotteista objektiivisten kriteerien perusteella, mukaan lukien seuraavat:

a) tuoteluokka;

b) tuotteiden varmuustasot;

c) sertifikaatin haltija;

d) sertifiointielin ja tapauksen mukaan alihankkijana toimiva ITSEF;

e) muut viranomaisen tietoon saatetut tiedot.

5. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilmoitettava EUCC-sertifikaatin haltijoille valituista tieto- ja viestintätekniikan tuotteista ja valintaperusteista.

6. Otokseen valitun tieto- ja viestintätekniikan tuotteen sertifioineen sertifiointielimen on kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen pyynnöstä ja vastaavan ITSEFin avustuksella suoritettava lisätarkastelu liitteessä IV olevassa IV.2 jaksossa vahvistetun menettelyn mukaisesti ja ilmoitettava tuloksista kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle.

7. Jos kansallisella kyberturvallisuussertifioinnin myöntävällä viranomaisella on riittävä syy uskoa, että sertifioitu tieto- ja viestintätekniikan tuote ei enää ole tämän asetuksen tai asetuksen (EU) 2019/881 mukainen, se voi suorittaa tutkimuksia tai käyttää muita asetuksen (EU) 2019/881 58 artiklan 8 kohdassa säädettyjä seurantavaltuuksia.

8. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilmoitettava sertifiointielimelle ja asianomaiselle ITSEFille käynnissä olevista tutkimuksista, jotka koskevat valittuja tieto- ja viestintätekniikan tuotteita.

9. Jos kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen toteaa, että meneillään oleva tutkimus koskee muihin jäsenvaltioihin sijoittautuneiden sertifiointielinten sertifioimia tieto- ja viestintätekniikan tuotteita, sen on ilmoitettava asiasta kyseisten jäsenvaltioiden kansallisille kyberturvallisuussertifioinnin myöntäville viranomaisille, jotta ne voivat tarvittaessa tehdä yhteistyötä tutkimuksissa. Kyseisen kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilmoitettava rajat ylittävistä tutkimuksista ja niiden tuloksista myös Euroopan kyberturvallisuuden sertifiointiryhmälle.

26 artikla

Sertifiointielimen seurantatoimet

1. Sertifiointielimen on seurattava seuraavia:

a) se, että sertifikaatin haltijat noudattavat tämän asetuksen ja asetuksen (EU) 2019/881 mukaisia velvoitteitaan suhteessa sertifiointielimen myöntämään EUCC-sertifikaattiin;

b) se, että sen sertifioimat tieto- ja viestintätekniikan tuotteet ovat niihin sovellettavien turvallisuusvaatimusten mukaisia;

c) sertifioiduissa suojausprofiileissa ilmaistu varmuus.

2. Sertifiointielimen on suoritettava seurantatoimensa seuraavien perusteella:

a) 9 artiklan 2 kohdassa tarkoitettujen sertifioinnin hakijan sitoumusten perusteella annetut tiedot;

b) muiden asianomaisten markkinavalvontaviranomaisten toimista saatavat tiedot;

c) vastaanotetut valitukset;

d) haavoittuvuustiedot, jotka voivat vaikuttaa sen sertifioimiin tieto- ja viestintätekniikan tuotteisiin.

3. Kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen voi laatia sääntöjä sertifiointielinten ja EUCC-sertifikaattien haltijoiden välistä säännöllistä vuoropuhelua varten, jotta voidaan todentaa 9 artiklan 2 kohdan nojalla tehtyjen sitoumusten noudattaminen ja raportoida siitä, sanotun kuitenkaan rajoittamatta toimintaa suhteessa muihin asianomaisiin markkinavalvontaviranomaisiin.

27 artikla

Sertifikaatin haltijan seurantatoimet

1. EUCC-sertifikaatin haltijan on suoritettava seuraavat tehtävät seuratakseen, että sertifioitu tieto- ja viestintätekniikan tuote on siihen sovellettavien turvallisuusvaatimusten mukainen:

a) seurattava sertifioidun tieto- ja viestintätekniikan tuotteen haavoittuvuustietoja, mukaan lukien tunnetut riippuvuudet, omin keinoin ja myös ottaen huomioon seuraavat:

   1) haavoittuvuustietojen julkaiseminen tai toimittaminen käyttäjien tai tietoturvatutkijoiden taholta asetuksen (EU) 2019/881 55 artiklan 1 kohdan c alakohdassa tarkoitetulla tavalla;

   2) tiedot mistä tahansa muusta lähteestä;

b) seurattava EUCC-sertifikaatissa ilmaistua varmuutta.

2. EUCC-sertifikaatin haltijan on tehtävä yhteistyötä sertifiointielimen, ITSEFin ja tapauksen mukaan kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen kanssa niiden seurantatoimien tukemiseksi.

II JAKSO

VAATIMUSTENMUKAISUUS JA VELVOITTEIDEN NOUDATTAMINEN

28 artikla

Sertifioidun tieto- ja viestintätekniikan tuotteen tai suojausprofiilin vaatimustenvastaisuuden seuraukset

1. Jos sertifioitu tieto- ja viestintätekniikan tuote tai suojausprofiili ei ole tässä asetuksessa ja asetuksessa (EU) 2019/881 säädettyjen vaatimusten mukainen, sertifiointielimen on ilmoitettava EUCC-sertifikaatin haltijalle havaitusta vaatimustenvastaisuudesta ja pyydettävä korjaavia toimia.

2. Jos tämän asetuksen säännösten vastaisuus saattaa vaikuttaa sellaisen muun sovellettavan unionin lainsäädännön noudattamiseen, jossa säädetään mahdollisuudesta osoittaa käyttämällä EUCC-sertifikaattia, että kyseisen säädöksen vaatimusten suhteen vallitsee vaatimustenmukaisuusolettama, sertifiointielimen on ilmoitettava asiasta viipymättä kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on välittömästi ilmoitettava havaitusta vaatimustenvastaisuudesta markkinavalvontaviranomaiselle, joka vastaa kyseisestä muusta sovellettavasta unionin lainsäädännöstä.

3. Saatuaan 1 kohdassa tarkoitetut tiedot EUCC-sertifikaatin haltijan on sertifiointielimen asettamassa määräajassa, joka saa olla enintään 30 päivää, ehdotettava sertifiointielimelle korjaavia toimia, jotka ovat tarpeen vaatimustenvastaisuuden korjaamiseksi.

4. Sertifiointielin voi ilman aiheetonta viivytystä keskeyttää EUCC-sertifikaatin voimassaolon 30 artiklan mukaisesti hätätilanteessa tai jos EUCC-sertifikaatin haltija ei tee asianmukaista yhteistyötä sertifiointielimen kanssa.

5. Sertifiointielimen on suoritettava tarkastus 13 ja 19 artiklan mukaisesti ja arvioitava, korjataanko vaatimustenvastaisuus korjaavalla toimella.

6. Jos EUCC-sertifikaatin haltija ei ehdota asianmukaisia korjaavia toimia 3 kohdassa tarkoitetun määräajan kuluessa, sertifikaatin voimassaolo keskeytetään 30 artiklan mukaisesti tai sertifikaatti peruutetaan 14 tai 20 artiklan mukaisesti.

7. Tätä artiklaa ei sovelleta haavoittuvuuksiin, jotka vaikuttavat sertifioituun tieto- ja viestintätekniikan tuotteeseen ja joita käsitellään VI luvun mukaisesti.

29 artikla

Seuraukset sertifikaatin haltijan velvoitteiden noudattamatta jättämisestä

1. Jos sertifiointielin toteaa, että

a) EUCC-sertifikaatin haltija tai sertifiointia hakeva ei noudata 9 artiklan 2 kohdassa, 17 artiklan 2 kohdassa, 27 artiklassa ja 41 artiklassa säädettyjä sitoumuksiaan ja velvollisuuksiaan; tai

b) EUCC-sertifikaatin haltija ei noudata asetuksen (EU) 2019/881 56 artiklan 8 kohtaa tai tämän asetuksen VI lukua;

sen on asetettava enintään 30 päivän määräaika, jonka kuluessa EUCC-sertifikaatin haltijan on toteutettava korjaavia toimia.

2. Jos EUCC-sertifikaatin haltija ei ehdota asianmukaisia korjaavia toimia 1 kohdassa tarkoitetun määräajan kuluessa, sertifikaatin voimassaolo keskeytetään 30 artiklan mukaisesti tai sertifikaatti peruutetaan 14 ja 20 artiklan mukaisesti.

3. Jos EUCC-sertifikaatin haltija rikkoo jatkuvasti tai toistuvasti 1 kohdassa tarkoitettuja velvoitteita, EUCC-sertifikaatti peruutetaan 14 tai 20 artiklan mukaisesti.

4. Sertifiointielimen on ilmoitettava kansalliselle kyberturvallisuussertifioinnin myöntävällä viranomaiselle 1 kohdassa tarkoitetuista havainnoista. Jos velvoitteiden noudattamatta jättäminen vaikuttaa muun sovellettavan unionin lainsäädännön noudattamiseen, kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on välittömästi ilmoitettava havaitusta velvoitteiden noudattamatta jättämisestä markkinavalvontaviranomaiselle, joka vastaa kyseisestä muusta sovellettavasta unionin lainsäädännöstä.

30 artikla

EUCC-sertifikaatin voimassaolon keskeyttäminen

1. Silloin kun tässä asetuksessa viitataan EUCC-sertifikaatin voimassaolon keskeyttämiseen, sertifiointielimen on keskeytettävä kyseisen EUCC-sertifikaatin voimassaolo keskeytyksen käynnistävien olosuhteiden edellyttämäksi ajaksi, joka saa olla enintään 42 päivää. Keskeytysaika alkaa sertifiointielimen päätöksen tekopäivää seuraavana päivänä. Keskeytys ei vaikuta sertifikaatin voimassaoloon.

2. Sertifiointielimen on ilmoitettava keskeytyksestä ilman aiheetonta viivytystä sertifikaatin haltijalle ja kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle sekä ilmoitettava keskeytyksen syyt, pyydetyt toimet ja keskeytyksen kesto.

3. Sertifioinnin haltijoiden on ilmoitettava kyseessä olevien tieto- ja viestintätekniikan tuotteiden ostajille keskeytyksestä ja sertifiointielimen keskeytykselle esittämistä syistä, paitsi niiltä osin kuin syiden ilmoittaminen muodostaisi turvallisuusriskin tai ne sisältävät arkaluonteisia tietoja. Sertifikaatin haltijan on myös asetettava nämä tiedot julkisesti saataville.

4. Jos muussa sovellettavassa unionin lainsäädännössä säädetään tämän asetuksen säännösten nojalla myönnettyihin sertifikaatteihin perustuvasta vaatimustenmukaisuusolettamasta, kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilmoitettava keskeyttämisestä markkinavalvontaviranomaiselle, joka vastaa kyseisestä muusta sovellettavasta unionin lainsäädännöstä.

5. Sertifikaatin voimassaolon keskeyttämisestä on ilmoitettava ENISAlle 42 artiklan 3 kohdan mukaisesti.

6. Asianmukaisesti perustelluissa tapauksissa kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen voi antaa luvan jatkaa EUCC-sertifikaatin voimassaolon keskeyttämistä. Keskeytyksen kokonaiskesto saa olla enintään yksi vuosi.

31 artikla

Seuraukset vaatimustenmukaisuuden arviointilaitoksen velvoitteiden noudattamatta jättämisestä

1. Jos sertifiointielin ei täytä velvoitteitaan tai tapauksissa, joissa ITSEFin havaitaan laiminlyöneen velvoitteitaan, vastaava sertifiointielin ei täytä velvoitteitaan, kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on ilman aiheetonta viivytystä

a) yksilöitävä kyseessä olevan ITSEFin tuella ne EUCC-sertifikaatit, joita asia mahdollisesti koskee;

b) tarvittaessa pyydettävä, että joko se ITSEF, joka suoritti arvioinnin, tai mikä tahansa muu akkreditoitu ja tarvittaessa valtuutettu ITSEF, jolla on siihen teknisesti paremmat edellytykset, suorittaa yhdelle tai useammalle tieto- ja viestintätekniikan tuotteelle tai suojausprofiilille arviointitoimia kyseisen yksilöinnin tukemiseksi;

c) analysoitava velvoitteiden noudattamatta jättämisen vaikutuksia;

d) ilmoitettava velvoitteiden noudattamatta jättämisestä kyseessä olevan EUCC-sertifikaatin haltijalle.

2. Sertifiointielimen on 1 kohdassa tarkoitettujen toimenpiteiden perusteella tehtävä jompikumpi seuraavista päätöksistä kunkin asianomaisen EUCC-sertifikaatin osalta:

a) pidettävä EUCC-sertifikaatti voimassa muutoksitta;

b) peruutettava EUCC-sertifikaatti 14 tai 20 artiklan mukaisesti ja myönnettävä tarvittaessa uusi EUCC-sertifikaatti.

3. Edellä 1 kohdassa tarkoitettujen toimenpiteiden pohjalta kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on

a) tarvittaessa raportoitava sertifiointielimen tai vastaavan ITSEFin velvoitteiden laiminlyönnistä kansalliselle akkreditointielimelle;

b) tarvittaessa arvioitava mahdollinen vaikutus valtuutukseen.

VI LUKU

HAAVOITTUVUUKSIEN HALLINTA JA JULKISTAMINEN

32 artikla

Haavoittuvuuksien hallinnan laajuus

Tätä lukua sovelletaan tieto- ja viestintätekniikan tuotteisiin, joille on myönnetty EUCC-sertifikaatti.

I JAKSO

HAAVOITTUVUUKSIEN HALLINTA

33 artikla

Haavoittuvuuksien hallintamenettelyt

1. EUCC-sertifikaatin haltijan on otettava käyttöön kaikki tarvittavat haavoittuvuuksien hallintamenettelyt ja pidettävä niitä yllä tässä jaksossa vahvistettujen sääntöjen mukaisesti ja tarvittaessa täydennettynä standardissa EN ISO/IEC 30111 esitetyillä menettelyillä.

2. EUCC-sertifikaatin haltijan on pidettävä käytössä asianmukaisia menetelmiä tuotteisiinsa liittyviä haavoittuvuuksia koskevan tiedon vastaanottamiseksi ulkoisista lähteistä, kuten käyttäjiltä, sertifiointielimiltä ja tietoturvatutkijoilta, ja julkaistava kyseiset menetelmät.

3. Jos EUCC-sertifikaatin haltija havaitsee tai vastaanottaa tietoa mahdollisesta sertifioituun tieto- ja viestintätekniikan tuotteeseen vaikuttavasta haavoittuvuudesta, sen on kirjattava nämä tiedot ja tehtävä haavoittuvuutta koskeva vaikutusanalyysi.

4. Jos mahdollinen haavoittuvuus vaikuttaa yhdistettyyn tuotteeseen, EUCC-sertifikaatin haltijan on ilmoitettava mahdollisesta haavoittuvuudesta tuotteeseen kytkeytyvien EUCC-sertifikaattien haltijalle.

5. EUCC-sertifikaatin haltijan on sertifikaatin myöntäneen sertifiointielimen perustellusta pyynnöstä toimitettava kyseiselle sertifiointielimelle kaikki asiaankuuluvat tiedot mahdollisista haavoittuvuuksista.

34 artikla

Haavoittuvuutta koskeva vaikutusanalyysi

1. Haavoittuvuutta koskevassa vaikutusanalyysissä on viitattava arvioinnin kohteeseen ja sertifikaatissa oleviin varmennuslausumiin. Haavoittuvuutta koskeva vaikutusanalyysi on tehtävä määräajassa, joka on sertifioidun tieto- ja viestintätekniikan tuotteen mahdollisen haavoittuvuuden hyödynnettävyyden ja kriittisyyden kannalta asianmukainen.

2. Tarvittaessa on tehtävä laskelma hyökkäyspotentiaalista noudattaen sovellettavia menetelmiä, jotka sisältyvät 3 artiklassa tarkoitettuihin standardeihin ja asiaankuuluviin liitteessä I mainittuihin viimeisintä kehitystä edustaviin asiakirjoihin, jotta voidaan määrittää haavoittuvuuden hyväksikäytettävyys. Tällöin otetaan huomioon EUCC-sertifikaatin AVA_VAN-taso.

35 artikla

Haavoittuvuutta koskeva vaikutusanalyysiraportti

1. Haltijan on laadittava haavoittuvuutta koskeva vaikutusanalyysiraportti, jos vaikutusanalyysi osoittaa, että haavoittuvuudella on todennäköinen vaikutus tieto- ja viestintätekniikan tuotteen vaatimustenmukaisuuteen suhteessa sen sertifikaattiin.

2. Haavoittuvuuden vaikutusanalyysiraporttiin on sisällyttävä arvio seuraavista:

a) haavoittuvuuden vaikutus sertifioituun tieto- ja viestintätekniikan tuotteeseen;

b) hyökkäyksen läheisyyteen tai toimintakelpoisuuteen liittyvät mahdolliset riskit;

c) se, voidaanko haavoittuvuus korjata;

d) jos haavoittuvuus voidaan korjata, mahdolliset ratkaisut haavoittuvuuden korjaamiseksi.

3. Haavoittuvuuden vaikutusanalyysiraportissa on tarvittaessa oltava yksityiskohtaiset tiedot mahdollisista keinoista käyttää haavoittuvuutta hyväksi. Tietoja mahdollisista keinoista käyttää haavoittuvuutta hyväksi on käsiteltävä asianmukaisia turvatoimenpiteitä noudattaen niiden luottamuksellisuuden suojaamiseksi ja tarvittaessa niiden leviämisen rajoittamiseksi.

4. EUCC-sertifikaatin haltijan on toimitettava haavoittuvuutta koskeva vaikutusanalyysiraportti sertifiointielimelle tai kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle asetuksen (EU) 2019/881 56 artiklan 8 kohdan mukaisesti ilman aiheetonta viivytystä.

5. Jos haavoittuvuutta koskevassa vaikutusanalyysiraportissa todetaan, että haavoittuvuudessa ei ole kyse 3 artiklassa mainituissa standardeissa tarkoitetusta jäännösriskistä ja että se voidaan poistaa, sovelletaan 36 artiklaa.

6. Jos haavoittuvuutta koskevassa vaikutusanalyysiraportissa todetaan, että haavoittuvuudessa ei ole kyse jäännösriskistä ja että sitä ei voida poistaa, EUCC-sertifikaatti peruutetaan 14 artiklan mukaisesti.

7. EUCC-sertifikaatin haltijan on seurattava mahdollisia jäännösriskejä sen varmistamiseksi, että haavoittuvuutta ei voida hyödyntää toimintaympäristön muuttuessa.

36 artikla

Haavoittuvuuden korjaaminen

EUCC-sertifikaatin haltijan on toimitettava sertifiointielimelle ehdotus tarvittaviksi korjaaviksi toimiksi. Sertifiointielimen on tarkastettava sertifikaatti 13 artiklan mukaisesti. Tarkastamisen laajuus määräytyy sen mukaan, mitä toimenpiteitä ehdotetaan haavoittuvuuden poistamiseksi.

II JAKSO

HAAVOITTUVUUDEN JULKISTAMINEN

37 artikla

Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen kanssa jaettavat tiedot

1. Tietoihin, jotka sertifiointielin toimittaa kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle, sisältyvät kaikki osatekijät, jotka kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen tarvitsee ymmärtääkseen haavoittuvuuden vaikutuksen, tiedot tieto- ja viestintätekniikan tuotteeseen tehtävistä muutoksista sekä sertifiointielimeltä saadut tiedot haavoittuvuuden laajemmista vaikutuksista muiden sertifioitujen tieto- ja viestintätekniikan tuotteiden kannalta, jos viimeksi mainitut tiedot ovat saatavilla.

2. Edellä olevan 1 kohdan mukaisesti toimitettavat tiedot eivät saa sisältää yksityiskohtaisia tietoja haavoittuvuuden hyväksikäyttökeinoista. Tämä säännös ei rajoita kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen tutkintavaltuuksia.

38 artikla

Yhteistyö muiden kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisen kanssa

1. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on jaettava asiaankuuluvat 37 artiklan mukaisesti saadut tiedot muiden kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten ja ENISAn kanssa.

2. Muut kansalliset kyberturvallisuussertifioinnin myöntävät viranomaiset voivat päättää analysoida haavoittuvuutta tarkemmin tai, sen jälkeen kun asiasta on ilmoitettu EUCC-sertifikaatin haltijalle, pyytää asianomaisia sertifiointielimiä arvioimaan, voiko haavoittuvuus vaikuttaa muihin sertifioituihin tieto- ja viestintätekniikan tuotteisiin.

39 artikla

Haavoittuvuuden julkaiseminen

Sen jälkeen, kun sertifikaatti on peruutettu, EUCC-sertifikaatin haltijan on julkistettava tieto- ja viestintätekniikan tuotteen julkisesti tiedossa olevat ja korjatut haavoittuvuudet rekisteröimällä ne Euroopan parlamentin ja neuvoston direktiivin

(EU) 2022/2555 ([5]) 12 artiklan mukaisesti perustettuun Euroopan haavoittuvuustietokantaan tai muihin asetuksen (EU) 2019/881 55 artiklan 1 kohdan d alakohdassa tarkoitettuihin verkkotietolähteisiin.

VII LUKU

TIETOJEN SÄILYTTÄMINEN, LUOVUTTAMINEN JA SUOJAAMINEN

40 artikla

Tietojen säilyttäminen sertifiointielinten ja ITSEFin toimesta

1. ITSEFin ja sertifiointielinten on ylläpidettävä kirjanpitojärjestelmää, joka sisältää kaikki kunkin niiden suorittaman arvioinnin ja sertifioinnin yhteydessä laaditut asiakirjat.

2. Sertifiointielinten ja ITSEFin on tallennettava ja säilytettävä nämä tiedot suojatusti tämän asetuksen soveltamiseksi tarvittavan ajan ja vähintään viiden vuoden ajan kulloisenkin EUCC-sertifikaatin peruuttamisen jälkeen. Jos sertifiointielin on myöntänyt uuden EUCC-sertifikaatin 13 artiklan 2 kohdan c alakohdan mukaisesti, sen on säilytettävä peruutettua EUCC-sertifikaattia koskevat asiakirjat yhdessä uuden EUCC-sertifikaatin kanssa ja yhtä kauan.

41 artikla

Sertifikaatin haltijan antamat tiedot

1. Asetuksen (EU) 2019/881 55 artiklassa tarkoitettujen tietojen on oltava saatavilla kielellä, jota käyttäjät helposti ymmärtävät.

2. EUCC-sertifikaatin haltijan on säilytettävä seuraavat tiedot suojatusti tämän asetuksen soveltamiseksi tarvittavan ajan ja vähintään viiden vuoden ajan EUCC-sertifikaatin peruuttamisen jälkeen:

a) sertifiointielimelle ja ITSEFille sertifiointiprosessin aikana toimitetut tiedot;

b) sertifioidun tieto- ja viestintätekniikan tuotteen näytekappale.

3. Jos sertifiointielin on myöntänyt uuden EUCC-sertifikaatin 13 artiklan 2 kohdan c alakohdan mukaisesti, haltijan on säilytettävä peruutettua EUCC-sertifikaattia koskevat asiakirjat yhdessä uuden EUCC-sertifikaatin kanssa ja yhtä kauan.

4. EUCC:n sertifikaatin haltijan on sertifiointielimen tai kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen pyynnöstä asetettava saataville 2 kohdassa tarkoitetut tiedot ja näytekappaleet.

42 artikla

ENISAn antamat tiedot

1. ENISA julkaisee seuraavat tiedot asetuksen (EU) 2019/881 50 artiklan 1 kohdassa tarkoitetulla verkkosivustolla:

a) kaikki EUCC-sertifikaatit;

b) tiedot EUCC-sertifikaatin tilasta, erityisesti siitä, onko sertifikaatti voimassa, onko se peruutettu määräajaksi tai kokonaan tai onko sen voimassaolo päättynyt;

c) kutakin EUCC-sertifikaattia vastaavat sertifiointiraportit;

([5]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (EUVL L 333, 27.12.2022, s. 80).

d) luettelo akkreditoiduista vaatimustenmukaisuuden arviointilaitoksista;

e) luettelo valtuutetuista vaatimustenmukaisuuden arviointilaitoksista;

f) liitteessä I luetellut viimeisintä kehitystä edustavat asiakirjat;

g) asetuksen (EU) 2019/881 62 artiklan 4 kohdan c alakohdassa tarkoitetut Euroopan kyberturvallisuuden sertifiointiryhmän lausunnot;

h) 47 artiklan mukaisesti laaditut vertaisarviointiraportit.

2. Edellä 1 kohdassa tarkoitetut tiedot on annettava saataville ainakin englannin kielellä.

3. Sertifiointielinten ja tapauksen mukaan kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten on ilmoitettava ENISAlle viipymättä päätöksistään, jotka vaikuttavat 1 kohdan b alakohdassa tarkoitettuun EUCC-sertifikaatin sisältöön tai tilaan.

4. ENISA varmistaa, että 1 kohdan a, b ja c alakohdan mukaisesti julkaistuissa tiedoissa yksilöidään selkeästi sertifioidun tieto- ja viestintätekniikan tuotteen versiot, jotka kuuluvat EUCC-sertifikaatin piiriin.

43 artikla

Tietosuoja

Vaatimustenmukaisuuden arviointilaitosten, kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten, Euroopan kyberturvallisuuden sertifiointiryhmän, ENISAn, komission ja kaikkien muiden osapuolten on varmistettava liikesalaisuuksien ja muiden luottamuksellisten tietojen, mukaan lukien valmistussalaisuudet, turvallisuus ja suojaaminen sekä immateriaalioikeuksien säilyttäminen ja toteutettava tarvittavat ja asianmukaiset tekniset ja organisatoriset toimenpiteet.

VII LUKU

VASTAVUOROISTA TUNNUSTAMISTA KOSKEVAT SOPIMUKSET KOLMANSIEN MAIDEN KANSSA

44 artikla

Edellytykset

1. Kolmansien maiden, jotka haluavat sertifioida tuotteensa tämän asetuksen mukaisesti ja jotka haluavat saada tällaisen sertifioinnin tunnustetuksi unionissa, on tehtävä vastavuoroista tunnustamista koskeva sopimus unionin kanssa.

2. Vastavuoroista tunnustamista koskevan sopimuksen on katettava sertifioituihin tieto- ja viestintätekniikan tuotteisiin sovellettavat varmuustasot ja tarvittaessa suojausprofiileihin sovellettavat varmuustasot.

3. Edellä 1 kohdassa tarkoitettuja vastavuoroista tunnustamista koskevia sopimuksia voidaan tehdä ainoastaan sellaisten kolmansien maiden kanssa,

a) joilla on viranomainen,

   1) joka on julkinen elin, joka on riippumaton niistä yhteisöistä, joiden toimintaa se valvoo ja seuraa, organisaatio- ja oikeudellisen rakenteen, rahoituksen ja päätöksenteon suhteen;

   2) jolla on asianmukaiset seuranta- ja valvontavaltuudet suorittaa tutkimuksia ja valtuudet asianmukaisiin korjaaviin toimenpiteisiin velvoitteiden noudattamisen varmistamiseksi;

   3) jolla on käytössä tehokas, oikeasuhteinen ja varoittava seuraamusjärjestelmä velvoitteiden noudattamisen varmistamiseksi;

   4) joka sopii tekevänsä yhteistyötä Euroopan kyberturvallisuuden sertifiointiryhmän ja ENISAn kanssa vaihtaakseen tietoja parhaista käytännöistä ja kehityksestä kyberturvallisuussertifioinnin alalla ja pyrkiäkseen tulkitsemaan yhdenmukaisesti tällä hetkellä sovellettavia arviointiperusteita ja -menetelmiä muun muassa soveltamalla yhdenmukaistettua dokumentaatiota, joka vastaa liitteessä I lueteltuja viimeisintä kehitystä edustavia asiakirjoja;

b) joilla on riippumaton akkreditointielin, joka suorittaa akkreditointeja käyttäen asetuksessa (EY) N:o 765/2008 tarkoitettuja standardeja vastaavia standardeja;

c) jotka sitoutuvat siihen, että arviointi- ja sertifiointiprosessit ja -menettelyt toteutetaan asianmukaisesti ja ammattimaisesti ottaen huomioon tässä asetuksessa ja erityisesti sen 3 artiklassa tarkoitettujen kansainvälisten standardien noudattaminen;

d) joilla on valmiudet ilmoittaa aiemmin havaitsemattomista haavoittuvuuksista ja käytössään vakiintunut ja asianmukainen haavoittuvuuksien hallinta- ja julkistamismenettely;

e) joilla on käytössään vakiintuneet menettelyt, jotka mahdollistavat valitusten tehokkaan jättämisen ja käsittelyn ja tarjoavat valituksen tekijälle tehokkaat oikeussuojakeinot;

f) jotka ottavat käyttöön mekanismin muiden unionin ja jäsenvaltioiden elinten kanssa tehtävää yhteistyötä varten kysymyksissä, joilla on merkitystä tämän asetuksen mukaisen kyberturvallisuussertifioinnin kannalta, mukaan lukien tietojen jakaminen sertifikaattien mahdollisesta vaatimustenvastaisuudesta, kehityksen seuraaminen sertifioinnin alalla ja yhteisen lähestymistavan varmistaminen sertifioinnin ylläpitämistä ja uudelleentarkastelua varten.

4. Sen lisäksi, että sovelletaan edellä 3 kohdassa säädettyjä edellytyksiä, 1 kohdassa tarkoitettu vastavuoroista tunnustamista koskeva sopimus, joka kattaa varmuustason ”korkea”, voidaan tehdä kolmansien maiden kanssa ainoastaan, jos myös seuraavat edellytykset täyttyvät:

a) kolmannella maalla on riippumaton ja julkinen kyberturvallisuussertifiointiviranomainen, joka suorittaa tai delegoi tarvittavat arviointitoimet sertifioinnin mahdollistamiseksi varmuustasolla ”korkea” siten, että se vastaa kansallisille kyberturvallisuusviranomaisille tässä asetuksessa ja asetuksessa (EU) 2019/881 säädettyjä vaatimuksia ja menettelyjä;

b) vastavuoroista tunnustamista koskevalla sopimuksella perustetaan yhteinen mekanismi, joka vastaa vertaisarviointia EUCC-sertifioinnin puitteissa, jotta voidaan tehostaa käytäntöjen vaihtoa ja ratkaista yhdessä arviointiin ja sertifiointiin liittyviä kysymyksiä.

IX LUKU

SERTIFIOINTIELINTEN VERTAISARVIOINTI

45 artikla

Vertaisarviointimenettely

1. Sertifiointielimelle, joka myöntää EUCC-sertifikaatteja varmuustasolla ”korkea”, on tehtävä vertaisarviointi säännöllisesti ja vähintään viiden vuoden välein. Erityyppiset vertaisarvioinnit luetellaan liitteessä VI.

2. Euroopan kyberturvallisuuden sertifiointiryhmä laatii aikataulun vertaisarvioinneille ja pitää sitä yllä varmistaen, että kyseistä jaksotusta noudatetaan. Asianmukaisesti perusteltuja tapauksia lukuun ottamatta vertaisarvioinnit suoritetaan paikan päällä.

3. Vertaisarviointi voi perustua vertaisarvioidun sertifiointielimen tai kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen aikaisempien vertaisarviointien tai vastaavien menettelyjen aikana kerättyyn evidenssiin, edellyttäen että

a) tulokset ovat enintään viisi vuotta vanhoja;

b) tulosten mukana on kuvaus kyseessä olevalle järjestelmälle perustetusta vertaisarviointiprosessista, jos tulokset liittyvät jonkin toisen sertifiointijärjestelmän puitteissa suoritettuun vertaisarviointiin;

c) jäljempänä 47 artiklassa tarkoitetussa vertaisarviointiraportissa täsmennetään, mitä tuloksia on käytetty uudelleen joko tekemällä lisäarviointia tai ilman lisäarviointia.

4. Jos vertaisarviointi kattaa yksittäisen tekniikan osa-alueen, arviointi on tehtävä myös kyseessä olevasta ITSEFistä.

5. Vertaisarvioidun sertifiointielimen ja tarvittaessa kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on varmistettava, että kaikki asiaankuuluvat tiedot asetetaan vertaisarviointiryhmän saataville.

6. Vertaisarvioinnin suorittaa liitteen VI mukaisesti perustettu vertaisarviointiryhmä.

46 artikla

Vertaisarvioinnin vaiheet

1. Valmisteluvaiheessa vertaisarviointiryhmän jäsennet tarkastelevat sertifiointielimen asiakirjoja, jotka koskevat sen toimintaperiaatteita ja menettelyjä, mukaan lukien viimeisintä kehitystä edustavien asiakirjojen käyttö.

2. Tarkastuskäyntivaiheessa vertaisarviointiryhmä arvioi elimen teknistä pätevyyttä ja tarvittaessa sellaisen ITSEFin pätevyyttä, joka on suorittanut vähintään yhden tieto- ja viestintätekniikan tuotteen arvioinnin, joka kuuluu vertaisarvioinnin piiriin.

3. Tarkastuskäyntivaihetta voidaan pidentää tai lyhentää riippuen sellaisista tekijöistä kuin mahdollisuudesta käyttää uudelleen olemassa olevaa vertaisarviointievidenssiä ja -tuloksia tai ITSEFien lukumäärästä ja niiden tekniikan osa-alueiden lukumäärästä, joiden osalta sertifiointielin myöntää sertifikaatteja.

4. Vertaisarviointiryhmä määrittää tarvittaessa kunkin ITSEFin teknisen pätevyyden vierailemalla sen teknisessä laboratoriossa tai teknisissä laboratorioissa ja haastattelemalla sen arvioijia tekniikan osa-alueista ja niihin liittyvistä erityisistä hyökkäysmenetelmistä.

5. Raportointivaiheessa arviointiryhmä dokumentoi havaintonsa vertaisarviointiraportissa, joka sisältää päätelmät ja tarvittaessa luettelon havaituista vaatimustenvastaisuuksista luokiteltuina kriittisyystason mukaan.

6. Vertaisarviointiraportista on ensin keskusteltava vertaisarvioidun sertifiointielimen kanssa. Näiden keskustelujen jälkeen vertaisarvioidun sertifiointielimen on laadittava aikataulu toimenpiteistä, jotka on toteutettava havaintoihin puuttumiseksi.

47 artikla

Vertaisarviointiraportti

1. Vertaisarviointiryhmä toimittaa vertaisarviointiraportin luonnoksen vertaisarvioidulle sertifiointielimelle.

2. Vertaisarvioidun sertifiointielimen on toimitettava vertaisarviointiryhmälle huomautuksensa havainnoista ja luettelo sitoumuksistaan vertaisarviointiraportin luonnoksessa yksilöityjen puutteiden korjaamiseksi.

3. Vertaisarviointiryhmä toimittaa Euroopan kyberturvallisuuden sertifiointiryhmälle lopullisen vertaisarviointiraportin, joka sisältää myös vertaisarvioidun sertifiointielimen tekemät huomautukset ja sitoumukset. Vertaisarviointiryhmä ottaa siinä myös kantaa huomautuksiin ja siihen, ovatko sitoumukset riittäviä havaittujen puutteiden korjaamiseksi.

4. Jos vertaisarviointiraportissa todetaan vaatimustenvastaisuuksia, Euroopan kyberturvallisuuden sertifiointiryhmä voi asettaa vertaisarvioidulle sertifiointielimelle asianmukaisen määräajan vaatimustenvastaisuuksien korjaamiseksi.

5. Euroopan kyberturvallisuuden sertifiointiryhmä antaa lausunnon vertaisarviointiraportista:

a) jos vertaisarviointiraportissa ei todeta vaatimustenvastaisuuksia tai jos vertaisarvioitu sertifiointielin on puuttunut vaatimustenvastaisuuksiin asianmukaisesti, Euroopan kyberturvallisuuden sertifiointiryhmä voi antaa myönteisen lausunnon ja kaikki asiaankuuluvat asiakirjat julkaistaan ENISAn sertifiointiverkkosivustolla;

b) jos vertaisarvioitu sertifiointielin ei puutu asianmukaisesti vaatimustenvastaisuuksiin asetetussa määräajassa, Euroopan kyberturvallisuuden sertifiointiryhmä voi antaa kielteisen lausunnon, joka julkaistaan ENISAn sertifiointiverkkosivustolla yhdessä vertaisarviointiraportin ja kaikkien asiaankuuluvien asiakirjojen kanssa.

6. Ennen lausunnon julkaisemista kaikki arkaluonteiset, henkilökohtaiset tai omistusoikeuden suojaamat tiedot on poistettava julkaistavista asiakirjoista.

X LUKU

JÄRJESTELMÄN YLLÄPITÄMINEN

48 artikla

EUCC:n ylläpitäminen

1. Komissio voi pyytää Euroopan kyberturvallisuuden sertifiointiryhmää antamaan lausunnon EUCC:n ylläpitämistä silmällä pitäen ja tarvittavien valmistelutöiden suorittamiseksi.

2. Euroopan kyberturvallisuuden sertifiointiryhmä voi antaa lausunnon, jossa se hyväksyy viimeisintä kehitystä edustavat asiakirjat.

3. ENISA julkaisee viimeisintä kehitystä edustavat asiakirjat, jotka Euroopan kyberturvallisuuden sertifiointiryhmä on hyväksynyt.

XI LUKU

LOPPUSÄÄNNÖKSET

49 artikla

EUCC:n soveltamisalaan kuuluvat kansalliset järjestelmät

1. Asetuksen (EU) 2019/881 57 artiklan 1 kohdan mukaisesti ja rajoittamatta kyseisen asetuksen 57 artiklan 3 kohdan soveltamista kaikki tieto- ja viestintätekniikan tuotteiden ja tieto- ja viestintätekniikan prosessien kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, jotka kuuluvat EUCC:n soveltamisalaan, lakkaavat tuottamasta oikeusvaikutuksia 12 kuukauden kuluttua tämän asetuksen voimaantulosta.

2. Poiketen siitä, mitä 50 artiklassa säädetään, kansallisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan käynnistää sertifiointiprosessi 12 kuukauden kuluessa tämän asetuksen voimaantulosta edellyttäen, että se saatetaan päätökseen 24 kuukauden kuluessa tämän asetuksen voimaantulosta.

3. Kansallisissa kyberturvallisuuden sertifiointijärjestelmissä myönnetyt sertifikaatit voidaan tarkastaa. Uudet sertifikaatit, joilla korvataan tarkastetut sertifikaatit, on myönnettävä tämän asetuksen mukaisesti.

50 artikla

Voimaantulo

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Sitä sovelletaan 27 päivästä helmikuuta 2025.

Tämän asetuksen IV lukua ja liitettä V sovelletaan tämän asetuksen voimaantulopäivästä.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 31 päivänä tammikuuta 2024.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN

LIITE I

Tekniikan osa-alueet ja viimeisintä kehitystä edustavat asiakirjat

1. Tekniikan osa-alueet AVA_VAN-tasolla 4 tai 5:

   a) tekniikan osa-alueen ”älykortit ja vastaavat laitteet” yhdenmukaistettuun arviointiin liittyvät asiakirjat ja erityisesti seuraavat asiakirjat versioina, jotka ovat voimassa [voimaantulopäivä]:

      1) ”Minimum ITSEF requirements for security evaluations of smart cards and similar devices” (älykorttien ja vastaavien laitteiden turvallisuusarviointien vähimmäisvaatimukset), Euroopan kyberturvallisuuden sertifiointiryhmä alun perin hyväksynyt 20. lokakuuta 2023;

      2) ”Minimum Site Security Requirements” (paikkakohtaista turvallisuutta koskevat vähimmäisvaatimukset), Euroopan kyberturvallisuuden sertifiointiryhmä alun perin hyväksynyt 20. lokakuuta 2023;

      3) ”Application of Common Criteria to integrated circuits” (yhteisten kriteerien soveltaminen integroituihin piireihin), Euroopan kyberturvallisuuden sertifiointiryhmä alun perin hyväksynyt 20. lokakuuta 2023;

      4) ”Security Architecture requirements (ADV_ARC) for smart cards and similar devices” (älykorttien ja vastaavien laitteiden turvallisuusarkkitehtuurivaatimukset (ADV_ARC)), Euroopan kyberturvallisuuden sertifiointiryhmä alun perin hyväksynyt 20. lokakuuta 2023;

      5) ”Certification of ’open’ smart card products” (”avoimien” älykorttituotteiden sertifiointi), Euroopan kyberturvallisuuden sertifiointiryhmä alun perin hyväksynyt 20. lokakuuta 2023;

      6) ”Composite product evaluation for smart cards and similar devices” (yhdistettyjen tuotteiden arviointi älykorteille ja vastaaville laitteille), Euroopan kyberturvallisuuden sertifiointiryhmä alun perin hyväksynyt 20. lokakuuta 2023;

      7) ”Application of Attack Potential to Smartcards” (hyökkäyspotentiaalin soveltaminen älykortteihin), Euroopan kyberturvallisuuden sertifiointiryhmä alun perin hyväksynyt 20. lokakuuta 2023;

   b) tekniikan osa-alueen ”tietoturvaboksilla varustetut laitteet” yhdenmukaistettuun arviointiin liittyvät asiakirjat ja erityisesti seuraavat asiakirjat versioina, jotka ovat voimassa [voimaantulopäivä]:

      1) ”Minimum ITSEF requirements for security evaluations of hardware devices with security boxes” (tietoturvaboksilla varustettujen laitteiden turvallisuusarviointien vähimmäisvaatimukset), Euroopan kyberturvallisuuden sertifiointiryhmä alun perin hyväksynyt 20. lokakuuta 2023;

      2) ”Minimum Site Security Requirements” (paikkakohtaista turvallisuutta koskevat vähimmäisvaatimukset), Euroopan kyberturvallisuuden sertifiointiryhmä alun perin hyväksynyt 20. lokakuuta 2023;

      3) ”Application of Attack Potential to hardware devices with security boxes” (hyökkäyspotentiaalin soveltaminen tietoturvaboksilla varustettuihin laitteisiin), Euroopan kyberturvallisuuden sertifiointiryhmä alun perin hyväksynyt 20. lokakuuta 2023.

2. viimeisintä kehitystä edustavat asiakirjat versioissaan, jotka ovat voimassa [voimaantulopäivä]:

   a) vaatimustenmukaisuuden arviointilaitosten yhdenmukaistettuun akkreditointiin liittyvä asiakirja: ”Accreditation of ITSEFs for the EUCC” (ITSEFien akkreditointi EUCC:ia varten), Euroopan kyberturvallisuuden sertifiointiryhmä alun perin hyväksynyt 20. lokakuuta 2023.

LIITE II

AVA_VAN -tasolla 4 tai 5 sertifioidut suojausprofiilit

1. Hyväksyttyjen sähköisen allekirjoituksen ja sähköisen leiman etäluontivälineiden luokka:

1) EN 419241-2:2019 – Trustworthy Systems Supporting Server Signing – Part 2: Protection Profile for QSCD for Server Signing ;

2) EN 419221-5:2018 – Protection profiles for Trust Service Provider Cryptographic modules – Part 5: Cryptographic Module for Trust Services

2. Suojausprofiilit, jotka on hyväksytty viimeisintä kehitystä edustavina asiakirjoina:

[TYHJÄ]

LIITE III

Suositellut suojausprofiilit (tekniikan osa-alueille liitteestä I)

Seuraavassa mainittuihin tieto- ja viestintätekniikan tuoteluokkiin kuuluvien tieto- ja viestintätekniikan tuotteiden sertifioinnissa käytettävät suojausprofiilit:

a) koneluettavien matkustusasiakirjojen luokka:

1) PP Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01;

2) PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control, BSI-CC-PP-0056-2009;

3) PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012-MA-02;

4) PP for a Machine Readable Travel Document with "ICAO Application" Basic Access Control, BSI-CC-PP-0055-2009;

b) turvallisten allekirjoitusten luomismenetelmien luokka:

1) EN 419211-1:2014 – Protection profiles for secure signature creation device – Part 1: Overview

2) EN 419211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation;

3) EN 419211-3:2013 – Protection profiles for secure signature creation device – Part 3: Device with key import;

4) EN 419211-4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application

5) EN 419211-5:2013 – Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application;

6) EN 419211-6:2014 – Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application;

c) digitaalisten ajopiirtureiden luokka:

1) *Tachograph – Tachograph Card* asetuksen (EU) N:o 165/2014 täytäntöönpanemisesta 18 päivänä maaliskuuta 2016 annetun komission täytäntöönpanoasetuksen (EU) 2016/799 (liite 1 C) mukaisesti;

2) *Digital Tachograph – Vehicle Unit* komission asetuksen (EY) N:o 1360/2002 liitteen I B mukaisesti, tarkoitettu asennettavaksi tieliikenteen ajoneuvoihin;

3) *Digital Tachograph – External GNSS Facility (EGF PP)* Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 165/2014 täytäntöönpanemisesta 18 päivänä maaliskuuta 2016 annetun komission täytäntöönpanoasetuksen (EU) 2016/799 liitteen 1 C mukaisesti;

4) *Digital Tachograph – Motion Sensor (MS PP)* Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 165/2014 täytäntöönpanemisesta 18 päivänä maaliskuuta 2016 annetun komission täytäntöönpanoasetuksen (EU) 2016/799 liitteen 1 C mukaisesti;

d) suojattujen integroitujen piirien, älykorttien ja niihin liittyvien laitteiden luokka:

1) Security IC Platform PP, BSI-CC-PP-0084-2014;

2) Java Card System – Open Configuration, V3.0.5 BSI-CC-PP-0099-2017;

3) Java Card System – Closed Configuration, BSI-CC-PP-0101-2017;

4) PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16, ANSSI-CC-PP-2015/07;

5) Universal SIM card, PU-2009-RT-79, ANSSI-CC-PP-2010/04;

6) Embedded UICC (eUICC) for Machine-to-Machine Devices, BSI-CC-PP-0089-2015;

e) maksupäätteiden ja (vastaavien) vuorovaikutuspisteiden luokka:

1) Point of Interaction "POI-CHIP-ONLY", ANSSI-CC-PP-2015/01;

2) Point of Interaction "POI-CHIP-ONLY and Open Protocol Package", ANSSI-CC-PP-2015/02;

3) Point of Interaction "POI-COMPREHENSIVE", ANSSI-CC-PP-2015/03;

4) Point of Interaction "POI-COMPREHENSIVE and Open Protocol Package", ANSSI-CC-PP-2015/04;

5) Point of Interaction "POI-PED-ONLY", ANSSI-CC-PP-2015/05;

6) Point of Interaction "POI-PED-ONLY and Open Protocol Package", ANSSI-CC-PP-2015/06;

f) tietoturvaboksilla varustettujen laitteiden luokka:

1) Cryptographic Module for CSP Signing Operations with Backup – PP CMCSOB, PP HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08;

2) Cryptographic Module for CSP key generation services – PP CMCKG, PP HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09;

3) Cryptographic Module for CSP Signing Operations without Backup – PP CMCSO, PP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

LIITE IV

Varmistuksen jatkuvuus ja sertifikaattien tarkastus

IV.1 **Varmistuksen jatkuvuus: soveltamisala**

1. Seuraavia varmistuksen jatkuvuutta koskevia vaatimuksia sovelletaan ylläpitotoimiin, jotka liittyvät seuraaviin:

   a) uudelleenarviointi siitä, täyttääkö muuttamaton sertifioitu tieto- ja viestintätekniikan tuote edelleen siihen sovellettavat turvallisuusvaatimukset;

   b) arviointi sertifioidun tieto- ja viestintätekniikan tuotteen muutosten vaikutuksista sen sertifiointiin;

   c) korjauspäivitysten soveltaminen arvioidun korjauspäivitysten hallintaprosessin mukaisesti, jos se sisältyy sertifiointiin;

   d) soveltuvin osin sertifikaatin haltijan elinkaarihallinnan tai tuotantoprosessien tarkastelu.

2. EUCC-sertifikaatin haltija voi pyytää sertifikaatin tarkastusta seuraavissa tapauksissa:

   a) EUCC-sertifikaatin voimassaolon on määrä päättyä yhdeksän kuukauden kuluessa;

   b) sertifioidussa tieto- ja viestintätekniikan tuotteessa tai muussa tekijässä on tapahtunut muutos, joka voi vaikuttaa tuotteen turvallisuustoimintoihin;

   c) todistuksen haltija vaatii, että haavoittuvuusarviointi tehdään uudelleen, jotta voidaan vahvistaa uudelleen EUCC-sertifikaatin varmistus liittyen tieto- ja viestintätekniikan tuotteen kykyyn vastustaa nykyisiä kyberhyökkäyksiä.

IV.2 **Uudelleenarviointi**

1. Jos on tarpeen arvioida muuttamattoman sertifioidun tieto- ja viestintätekniikan tuotteen uhkaympäristössä tapahtuvien muutosten vaikutusta, sertifiointielimelle on esitettävä uudelleenarviointipyyntö.

2. Uudelleenarvioinnin suorittaa sama ITSEF, joka osallistui aiempaan arviointiin, käyttämällä uudelleen kaikkia sen tuloksia, jotka ovat vielä voimassa. Arvioinnissa keskitytään varmistustoimiin, joihin sertifioidun tieto- ja viestintätekniikan tuotteen muuttunut uhkaympäristö saattaa vaikuttaa, erityisesti asianomaiseen AVA_VAN-perheeseen ja lisäksi varmistuksen elinkaaren (*assurance lifecycle*, ALC) perheeseen, jolloin kerätään uudelleen riittävästi evidenssiä kehitysympäristön ylläpidosta.

3. ITSEF kuvaa muutokset ja esittää yksityiskohtaisesti uudelleenarvioinnin tulokset sekä päivittää aiemman teknisen arviointiraportin.

4. Sertifiointielin tarkastelee päivitettyä teknistä arviointiraporttia ja laatii uudelleenarviointiraportin. Alkuperäisen sertifikaatin tilaa muutetaan sen jälkeen 13 artiklan mukaisesti.

5. Uudelleenarviointiraportti ja päivitetty sertifikaatti toimitetaan kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle ja ENISAlle julkaistavaksi sen kyberturvallisuussertifioinnin verkkosivustolla.

IV.3 **Sertifioidun tieto- ja viestintätekniikan tuotteen muutokset**

1. Jos sertifioituun tieto- ja viestintätekniikan tuotteeseen on tehty muutoksia, sertifikaatin haltijan, joka haluaa säilyttää sertifikaatin, on toimitettava sertifiointielimelle vaikutusanalyysiraportti.

2. Vaikutusanalyysiraportissa on oltava seuraavat:

   a) johdanto, jossa on tarvittavat tiedot vaikutusanalyysiraportista ja arvioinnin kohteesta (*target of evaluation*, TOE), jota on muutettu;

b) kuvaus tuotteen muutoksista;

c) määrittely kyseeseen tulevasta kehittäjän evidenssiaineistosta (*developer evidence*);

d) kuvaus kehittäjän evidenssiaineiston muutoksista;

e) havainnot ja päätelmät kunkin muutoksen vaikutuksesta turvallisuuden varmistukseen.

3. Sertifiointielin tutkii vaikutusanalyysiraportissa kuvatut muutokset, jotta voidaan validoida niiden vaikutus sertifioidun arvioinnin kohteen varmistukseen siten kuin vaikutusanalyysiraportin päätelmissä esitetään.

4. Tarkastelun jälkeen sertifiointielin määrittää yksittäisen muutoksen laajuuden vähäiseksi tai merkittäväksi sen vaikutuksen mukaan.

5. Jos sertifiointielin on vahvistanut, että muutokset ovat vähäisiä, muutetulle tieto- ja viestintätekniikan tuotteelle myönnetään uusi sertifikaatti ja alkuperäiseen sertifiointiraporttiin lisätään ylläpitoraportti seuraavin edellytyksin:

a) ylläpitoraportti liitetään osaksi vaikutusanalyysiraporttia, ja siinä on seuraavat osat:

1) johdanto;

2) kuvaus muutoksista;

3) kyseeseen tuleva kehittäjän evidenssiaineisto;

b) uuden sertifikaatin voimassaoloaika ei saa ylittää alkuperäisen sertifikaatin päivämäärää.

6. Uusi sertifikaatti toimitetaan ylläpitoraportin kanssa ENISAlle julkaistavaksi sen kyberturvallisuussertifioinnin verkkosivustolla.

7. Jos muutokset on vahvistettu merkittäviksi, tehdään uudelleenarviointi edellisen arvioinnin pohjalta ja käyttämällä uudelleen edellisen arvioinnin tuloksia, jotka ovat vielä voimassa.

8. Muutettua arvioinnin kohdetta koskevan arvioinnin päätteeksi ITSEF laatii uuden teknisen arviointiraportin. Sertifiointielin tarkastelee päivitettyä teknistä arviointiraporttia ja tarvittaessa myöntää uuden sertifikaatin ja laatii uuden sertifiointiraportin.

9. Uusi sertifikaatti ja sertifiointiraportti toimitetaan ENISAlle julkaisemista varten.

IV.4 **Päivitystenhallinta**

1. Korjauspäivitysten hallintamenettely on jäsennelty prosessi sertifioidun tieto- ja viestintätekniikan tuotteen päivittämiseksi. Korjauspäivitysten hallintamenettelyä, mukaan lukien sertifioinnin hakijan tieto- ja viestintätekniikan tuotteeseen toteuttama mekanismi, voidaan käyttää tieto- ja viestintätekniikan tuotteen sertifioinnin jälkeen vaatimustenmukaisuuden arviointilaitoksen vastuulla.

2. Sertifioinnin hakija voi sisällyttää tieto- ja viestintätekniikan tuotteen sertifiointiin päivitysmekanismin osana tuotteeseen toteutettua sertifioitua hallintamenettelyä, jos jokin seuraavista edellytyksistä täyttyy:

a) toiminnot, joihin korjauspäivitys vaikuttaa, jäävät sertifioidun tieto- ja viestintätekniikan tuotteen arvioinnin kohteen ulkopuolelle;

b) korjauspäivitys liittyy ennalta määritettyyn vähäiseen muutokseen tieto- ja viestintätekniikan tuotteessa;

c) korjauspäivitys liittyy vahvistettuun haavoittuvuuteen, jolla on kriittisiä vaikutuksia sertifioidun tieto- ja viestintätekniikan tuotteen turvallisuuden kannalta.

3. Jos korjauspäivitys liittyy merkittävään muutokseen sertifioidun tieto- ja viestintätekniikan tuotteen arvioinnin kohteessa liittyen aiemmin havaitsemattomaan haavoittuvuuteen, jolla ei ole kriittisiä vaikutuksia tieto- ja viestintätekniikan tuotteen turvallisuuteen, sovelletaan 13 artiklan säännöksiä.

4. Tieto- ja viestintätekniikan tuotteen korjauspäivitysten hallintamenettely koostuu seuraavista:

   a) prosessi tieto- ja viestintätekniikan tuotteen korjauspäivitysten kehittämistä ja julkaisua varten;

   b) tekninen mekanismi ja toiminnot korjauspäivityksen ottamiseksi käyttöön tieto- ja viestintätekniikan tuotteessa;

   c) teknisen mekanismin tehokkuuteen ja tuloksellisuuteen liittyvät arviointitoimet.

5. Tieto- ja viestintätekniikan tuotteen sertifioinnin aikana:

   a) tieto- ja viestintätekniikan tuotteen sertifiointia hakevan on toimitettava kuvaus korjauspäivitysten hallintamenettelystä;

   b) ITSEF tarkistaa seuraavat seikat:

      1) kehittäjä on toteuttanut tieto- ja viestintätekniikan tuotteen päivitysmekanismit noudattaen sertifioitavaksi toimitettua korjauspäivitysten hallintamenettelyä;

      2) arvioinnin kohde on rajattu siten, että erotettuihin prosesseihin tehdyt muutokset eivät vaikuta arvioinnin kohteen turvallisuuteen;

      3) tekninen päivitysmekanismi toimii tämän jakson säännösten ja hakijan väitteiden mukaisesti;

   c) sertifiointielin sisällyttää sertifiointiraporttiin tulokset korjauspäivitysten hallintamenettelyn arvioinnista.

6. Sertifikaatin haltija voi sen jälkeen soveltaa sertifioidun korjauspäivitysten hallintamenettelyn mukaista korjauspäivitystä kyseiseen sertifioituun tieto- ja viestintätekniikan tuotteeseen, ja sen on toteutettava seuraavat toimenpiteet viiden työpäivän kuluessa seuraavissa tapauksissa:

   a) edellä 2 kohdan a alakohdassa tarkoitetussa tapauksessa ilmoitettava kyseisestä korjauspäivityksestä sertifiointielimelle, joka ei saa muuttaa vastaavaa EUCC-sertifikaattia;

   b) edellä 2 kohdan b alakohdassa tarkoitetussa tapauksessa toimitettava kyseinen korjauspäivitys ITSEFille tarkastettavaksi. ITSEFin on korjauspäivityksen vastaanotettuaan ilmoitettava asiasta sertifiointielimelle, minkä perusteella sertifiointielin ryhtyy tarvittaviin toimiin vastaavan EUCC-sertifikaatin uuden version myöntämiseksi ja sertifiointiraportin päivittämiseksi;

   c) edellä 2 kohdan c alakohdassa tarkoitetussa tapauksessa toimitettava kyseinen korjauspäivitys ITSEFille tarvittavaa uudelleenarviointia varten, jolloin korjauspäivitys voidaan kuitenkin ottaa käyttöön samanaikaisesti. ITSEF ilmoittaa asiasta sertifiointielimelle, jotta sertifiointielin voi aloittaa asiaan liittyvät sertifiointitoimet.

LIITE V

Sertifiointiraportin sisältö

V.1 **Sertifiointiraportti**

1. Sertifiointiviranomainen laatii ITSEFin toimittamien teknisten arviointiraporttien perusteella sertifiointiraportin, joka julkaistaan yhdessä vastaavan EUCC-sertifikaatin kanssa.

2. Sertifiointiraportti sisältää yksityiskohtaiset käytännön tiedot tieto- ja viestintätekniikan tuotteesta tai tieto- ja viestintätekniikan tuotteiden luokasta sekä tuotteen turvallisesta käytöstä, minkä vuoksi siinä on oltava kaikki julkisesti saatavilla olevat ja jaettavissa olevat tiedot, joilla on merkitystä käyttäjille ja asianomaisille osapuolille. Sertifiointiraportissa voidaan viitata julkisesti saatavilla oleviin ja jaettavissa oleviin tietoihin.

3. Sertifiointiraportti sisältää ainakin seuraavat tiedot:

   a) tiivistelmä;

   b) tunnistetiedot tieto- ja viestintätekniikan tuotteesta tai tieto- ja viestintätekniikan tuoteluokasta suojausprofiilien osalta;

   c) turvallisuuspalvelut;

   d) oletukset ja soveltamisalan selventäminen;

   e) arkkitehtuuritiedot;

   f) täydentävät kyberturvallisuustiedot soveltuvin osin;

   g) tieto- ja viestintätekniikan tuotteen testaus, jos se on suoritettu;

   h) soveltuvin osin tiedot sertifikaatin haltijan elinkaarihallintaprosesseista ja tuotantolaitoksista;

   i) arvioinnin tulokset ja sertifikaattia koskevat tiedot;

   j) yhteenveto sertifioitavaksi toimitetun tieto- ja viestintätekniikan tuotteen turvatavoitteesta (*security target*, ST);

   k) järjestelmään liitetty merkki tai merkintä, jos sellainen on saatavilla;

   l) lähdeluettelo.

4. Tiivistelmä on lyhyt yhteenveto koko sertifiointiraportista. Tiivistelmässä esitetään selkeä ja tiivis yleiskatsaus arvioinnin tuloksista, ja siinä on seuraavat tiedot:

   a) arvioidun tieto- ja viestintätekniikan tuotteen nimi, arviointiin kuuluvien tuotteen komponenttien luettelo ja tuoteversio;

   b) arvioinnin suorittaneen ITSEFin nimi ja tarvittaessa luettelo alihankkijoista;

   c) arvioinnin valmistumispäivä;

   d) viittaus ITSEFin laatimaan tekniseen arviointiraporttiin;

   e) lyhyt kuvaus sertifiointiraportin tuloksista, mukaan lukien seuraavat:

      1) arviointiin sovellettavien yhteisten kriteerien (Common Criteria) versio ja tarvittaessa julkaisu;

      2) yhteisten kriteerien varmennuspaketti ja turvallisuuden varmistuksen komponentit, mukaan lukien arvioinnissa sovellettu AVA_VAN-taso ja vastaava asetuksen (EU) 2019/881 52 artiklassa säädetty varmuustaso, johon EUCC-sertifikaatissa viitataan;

      3) arvioidun tieto- ja viestintätekniikan tuotteen turvallisuustoiminnot;

      4) yhteenveto arvioituun tieto- ja viestintätekniikan tuotteeseen liittyvistä uhista ja organisatorisista turvallisuusperiaatteista;

5) erityiset konfiguraatiovaatimukset;

6) toimintaympäristöä koskevat oletukset;

7) soveltuvin osin liitteessä IV olevan IV.4 jakson mukaisen hyväksytyn korjauspäivitysten hallintamenettelyn olemassaolo;

8) vastuuvapauslausek(k)e(et).

5. Arvioitu tieto- ja viestintätekniikan tuote on yksilöitävä selkeästi, mukaan lukien seuraavat tiedot:

a) arvioidun tieto- ja viestintätekniikan tuotteen nimi;

b) luettelo arvioinnin piiriin kuuluvista tieto- ja viestintätekniikan tuotteen komponenteista;

c) tieto- ja viestintätekniikan tuotteen komponenttien versionumero;

d) sertifioidun tieto- ja viestintätekniikan tuotteen toimintaympäristöä koskevat lisävaatimukset;

e) EUCC-sertifikaatin haltijan nimi ja yhteystiedot;

f) tarvittaessa sertifikaattiin merkitty korjauspäivitysten hallintamenettely;

g) linkki EUCC-sertifikaatin haltijan verkkosivustolle, jolta saa täydentävät kyberturvallisuustiedot sertifioidusta tieto- ja viestintätekniikan tuotteesta asetuksen (EU) 2019/881 55 artiklan mukaisesti.

6. Tähän osioon sisältyvien tietojen on oltava mahdollisimman tarkkoja, jotta voidaan varmistaa, että tieto- ja viestintätekniikan tuotteesta annetaan täydellinen ja tarkka esitys, jota voidaan käyttää uudelleen tulevissa arvioinneissa.

7. Turvallisuusperiaatteita koskevassa osiossa on oltava kuvaus tieto- ja viestintätekniikan tuotteen turvallisuusperiaatteista sekä toimintaperiaatteista tai säännöistä, jotka arvioidussa tuotteessa on pantava täytäntöön tai joita siinä on noudatettava. Siinä on oltava kuvaus seuraavista toimintaperiaatteista:

a) sertifikaatin haltijan soveltamat haavoittuvuuksien käsittelyperiaatteet;

b) sertifikaatin haltijan varmistuksen jatkuvuuteen soveltamat periaatteet.

8. Tarvittaessa toimintaperiaatteisiin voi sisältyä ehtoja liittyen korjauspäivitysten hallintamenettelyn käyttöön sertifikaatin voimassaoloaikana.

9. Oletuksia ja soveltamisalan selventämistä koskevassa osiossa on oltava kattavat tiedot 7 artiklan 1 kohdan c alakohdassa tarkoitettuun tuotteen käyttötarkoitukseen liittyvistä olosuhteista ja tavoitteista. Tiedoissa on ilmoitettava seuraavat:

a) tieto- ja viestintätekniikan tuotteen käyttöä ja käyttöönottoa koskevat oletukset vähimmäisvaatimusten muodossa, kuten asianmukainen asennus ja konfigurointi sekä laitteistovaatimusten täyttyminen;

b) tieto- ja viestintätekniikan tuotteen vaatimustenmukaisen toiminnan ympäristöä koskevat oletukset;

10. Edellä 9 kohdassa lueteltujen tietojen on oltava mahdollisimman ymmärrettäviä, jotta sertifioidun tieto- ja viestintätekniikan tuotteen käyttäjät voivat tehdä tietoon perustuvia päätöksiä sen käyttöön liittyvistä riskeistä.

11. Arkkitehtuuritietoja koskevassa osiossa on oltava ylätason kuvaus tieto- ja viestintätekniikan tuotteesta ja sen tärkeimmistä komponenteista yhteisten kriteerien (Common Criteria) ADV_TDS-osajärjestelmäsuunnittelun mukaisesti.

12. Asetuksen (EU) 2019/881 55 artiklan mukaisesti on annettava täydellinen luettelo tieto- ja viestintätekniikan tuotteen täydentävistä kyberturvallisuustiedoista. Kaikki asiakirjat on merkittävä versionumeroilla.

13. Tieto- ja viestintätekniikan tuotteen testausta koskevassa osiossa on oltava seuraavat tiedot:

    a) sertifikaatin myöntäneen viranomaisen tai elimen nimi ja yhteyspiste, mukaan lukien toimivaltainen kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen;

    b) arvioinnin suorittaneen ITSEFin nimi, jos se on eri kuin sertifiointielin;

    c) käytettyjen turvallisuuden varmistuksen komponenttien yksilöinti 3 artiklassa tarkoitettujen standardien mukaisesti;

    d) viimeisintä kehitystä edustavan asiakirjan versio ja arvioinnissa käytetyt muut turvallisuuden arviointiperusteet;

    e) tieto- ja viestintätekniikan tuotteen täydelliset ja täsmälliset asetukset ja konfiguraatio arvioinnin aikana, mukaan lukien operatiiviset huomiot ja havainnot, jos niitä on;

    f) kaikki käytetyt suojausprofiilit, mukaan lukien seuraavat tiedot:

        1) suojausprofiilin laatija;

        2) suojausprofiilin nimi ja tunniste;

        3) suojausprofiilin sertifikaatin tunniste;

        4) suojausprofiilin arviointiin osallistuneen sertifiointielimen ja ITSEFin nimi ja yhteystiedot;

        5) suojausprofiilin mukaiselle tuotteelle vaadittava varmennuspaketti tai -paketit.

14. Arvioinnin tuloksia ja sertifikaattitietoja koskevassa osiossa on oltava seuraavat tiedot:

    a) vahvistus saavutetusta tämän asetuksen 4 artiklassa ja asetuksen (EU) 2019/881 52 artiklassa tarkoitetusta varmuustasosta;

    b) tämän asetuksen 3 artiklassa tarkoitettujen standardien mukaiset varmistusvaatimukset, jotka tieto- ja viestintätekniikan tuote tai suojausprofiili tosiasiallisesti täyttää, mukaan lukien AVA_VAN-taso;

    c) yksityiskohtainen kuvaus varmistusvaatimuksista sekä yksityiskohtaiset tiedot siitä, miten tuote täyttää kunkin näistä vaatimuksista;

    d) sertifikaatin myöntämispäivä ja voimassaoloaika;

    e) sertifikaatin yksilöivä tunniste.

15. Turvatavoite (*security target*, ST) on sisällytettävä sertifiointiraporttiin tai siihen on viitattava ja siitä on esitettävä yhteenveto sertifiointiraportissa, ja se on toimitettava yhdessä sertifiointiraportin kanssa julkaisemista varten.

16. Turvatavoite voidaan sanitoida eli puhdistaa tietyistä tiedoista VI.2 jakson mukaisesti.

17. EUCC:hen liitetty merkki tai merkintä voidaan lisätä sertifiointiraporttiin 11 artiklassa säädettyjen sääntöjen ja menettelyjen mukaisesti.

18. Lähdeluettelo sisältää viittaukset kaikkiin sertifiointiraportin laadinnassa käytettyihin asiakirjoihin. Näihin tietoihin on sisällyttävä ainakin seuraavat tiedot:

    a) turvallisuuden arviointiperusteet, viimeisintä kehitystä edustavat asiakirjat ja käytetyt muut eritelmät ja niiden versiot;

    b) tekninen arviointiraportti;

    c) tapauksen mukaan tekninen arviointiraportti yhdistetystä tuotteesta;

    d) tekniset viiteasiakirjat;

    e) arvioinnissa käytetty kehittäjän dokumentaatio.

19. Jotta voidaan taata arvioinnin uusittavuus, kaikki viitatut asiakirjat on yksilöitävä yksilöllisesti käyttäen oikeaa julkaisupäivää ja vastaavaa versionumeroa.

V.2 **Turvatavoitteen sanitointi eli puhdistaminen tietyistä tiedoista julkaisemista varten**

1. Turvatavoite (*security target*, ST), joka on sisällytettävä sertifiointiraporttiin tai johon on viitattava siinä VI.1 jakson 1 kohdan mukaisesti, voidaan sanitoida poistamalla omistusoikeuden suojaamat tekniset tiedot tai muotoilemalla ne uudelleen.

2. Tuloksena olevan sanitoidun turvatavoitteen on oltava oikea ja täydellinen esitys alkuperäisestä versiosta. Tämä tarkoittaa, että sanitoidusta turvatavoitteesta ei voi jättää pois tietoja, jotka ovat tarpeen arvioinnin kohteen turvallisuusominaisuuksien ja arvioinnin laajuuden ymmärtämiseksi.

3. Sanitoidun turvatavoitteen sisällön on täytettävä seuraavat vähimmäisvaatimukset:

   a) johdantoa ei sanitoida, koska se ei yleensä sisällä omistusoikeuden suojaamia tietoja;

   b) sanitoidulla turvatavoitteella on yksilöllinen tunniste, joka eri kuin sen täydellisellä alkuperäisellä versiolla;

   c) arvioinnin kohteen kuvausta voidaan supistaa, koska se voi sisältää omistusoikeuden suojaamia ja yksityiskohtaisia tietoja arvioinnin kohteen suunnittelusta, joita ei pitäisi julkaista;

   d) arvioinnin kohteen turvallisuusympäristön kuvausta (oletukset, uhat, organisatoriset turvallisuusperiaatteet) ei saa supistaa, jos nämä tiedot ovat tarpeen arvioinnin laajuuden ymmärtämiseksi;

   e) tietoja turvallisuustavoitteista ei saa supistaa, koska kaikki tiedot on julkistettava, jotta voidaan ymmärtää turvatavoitteen ja arvioinnin kohteen tarkoitus;

   f) kaikki turvallisuusvaatimukset on julkistettava. Soveltamista koskevissa huomautuksissa voidaan antaa tietoa siitä, miten 3 artiklassa tarkoitettujen yhteisten kriteerien toiminnallisia vaatimuksia on käytetty turvatavoitteen ymmärtämiseksi;

   g) arvioinnin kohteen tiivistetyn eritelmän on sisällettävä kaikki arvioinnin kohteen turvallisuustoiminnot, mutta siitä voidaan sanitoida pois muut omistusoikeudella suojatut tiedot;

   h) mukaan on sisällytettävä viittaukset suojausprofiileihin, joita sovelletaan arvioinnin kohteeseen;

   i) perustelut voidaan sanitoida omistusoikeudella suojattujen tietojen poistamiseksi.

4. Vaikka sanitoitua turvatavoitetta ei arvioida virallisesti 3 artiklassa tarkoitettujen arviointistandardien mukaisesti, sertifiointielimen on varmistettava, että se on täydellisen ja arvioidun turvatavoitteen mukainen, ja viitattava sertifiointiraportissa sekä täydelliseen että sanitoituun turvatavoitteeseen.

LIITE VI

Vertaisarviointien laajuus ja vertaisarviointiryhmien kokoonpano

VI.1 **Vertaisarvioinnin laajuus**

1. Vertaisarviointien tyypit ovat seuraavat:

   a) tyyppi 1: kun sertifiointielin suorittaa sertifiointitoimia AVA_VAN.3-tasolla;

   b) tyyppi 2: kun sertifiointielin suorittaa sertifiointitoimia liittyen tekniikan osa-alueeseen, joka on mainittu liitteessä I viimeisintä kehitystä edustavana asiakirjana;

   c) tyyppi 3: kun sertifiointielin suorittaa sertifiointitoimia AVA_VAN.3-tasoa ylemmällä tasolla käyttäen suojausprofiilia, joka on mainittu liitteessä II tai III viimeisintä kehitystä edustavana asiakirjana.

2. Vertaisarvioitava sertifiointielin toimittaa luettelon sertifioiduista tieto- ja viestintätekniikan tuotteista, jotka ovat ehdolla vertaisarviointiryhmän suorittamaa arviointia varten, seuraavien sääntöjen mukaisesti:

   a) ehdolla olevien tuotteiden on kuuluttava sertifiointielimen valtuutuksen tekniseen soveltamisalaan, ja vertaisarvioinnissa analysoidaan vähintään kaksi eri arviointia näistä tuotteista varmuustasolla ”korkea” ja yksi suojausprofiili, jos sertifiointielin on myöntänyt sertifikaatin varmuustasolla ”korkea”;

   b) tyypin 2 vertaisarviointia varten sertifiointielin toimittaa vähintään yhden tuotteen tekniikan osa-aluetta kohden ja asianomaista ITSEFIä kohden;

   c) tyypin 3 vertaisarvioinnissa arvioidaan vähintään yksi ehdolla oleva tuote sovellettavan ja asiaankuuluvan suojausprofiilin mukaisesti.

VI.2 **Vertaisarviointiryhmä**

1. Arviointiryhmässä on oltava vähintään kaksi asiantuntijaa, jotka kukin valitaan eri sertifiointielimestä, joka myöntää sertifikaatteja varmuustasolla ”korkea”, ja jotka tulevat eri jäsenvaltioista. Asiantuntijoiden tulisi osoittaa tarvittava asiantuntemus 3 artiklassa tarkoitetuista standardeista ja viimeisintä kehitystä edustavista asiakirjoista, jotka kuuluvat vertaisarvioinnin piiriin.

2. Jos sertifikaattien myöntäminen on delegoitu tai jos sertifikaatit on hyväksyttävä ennalta asetuksen (EU) 2019/881 56 artiklan 6 kohdassa tarkoitetusti, tämän jakson 1 kohdan mukaisesti valittuun asiantuntijaryhmään on lisäksi osallistuttava asiantuntija kansallisesta kyberturvallisuussertifioinnin myöntävästä viranomaisesta, joka vastaa kyseessä olevasta sertifiointielimestä.

3. Tyypin 2 vertaisarviointia varten ryhmän jäsenet valitaan sertifiointielimistä, jotka on valtuutettu kyseessä olevalle tekniikan osa-alueelle.

4. Kullakin arviointiryhmän jäsenellä on oltava vähintään kahden vuoden kokemus sertifiointitoimien suorittamisesta sertifiointielimessä.

5. Tyypin 2 tai 3 vertaisarvioinnissa kullakin arviointiryhmän jäsenellä on oltava vähintään kahden vuoden kokemus sertifiointitoimien suorittamisesta kyseisellä tekniikan osa-alueella tai kyseiseen suojausprofiiliin liittyen sekä todistettu asiantuntemus ja osallistumiskokemus ITSEFin hyväksymisestä.

6. Vertaisarvioitavan sertifiointielimen seurannasta ja valvonnasta vastaava kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen ja vähintään yksi toinen kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen, jonka sertifiointielimelle kyseistä vertaisarviointia ei tehdä, osallistuvat vertaisarviointiin tarkkailijana. Myös ENISA voi osallistua vertaisarviointiin tarkkailijana.

7. Vertaisarviointiryhmän kokoonpano ilmoitetaan vertaisarvioitavalle sertifiointielimelle. Perustelluissa tapauksissa se voi kyseenalaistaa vertaisarviointiryhmän kokoonpanon ja pyytää sen uudelleenarviointia.

LIITE VII

EUCC-sertifikaatin sisältö

EUCC-sertifikaatissa on oltava vähintään seuraavat tiedot:

a) sertifikaatin myöntäneen sertifiointielimen antama yksilöllinen tunniste;

b) sertifioitua tieto- ja viestintätekniikan tuotetta tai suojausprofiilia ja sertifikaatin haltijaa koskevat tiedot, mukaan lukien seuraavat:

   1) tieto- ja viestintätekniikan tuotteen tai suojausprofiilin ja tarvittaessa arvioinnin kohteen nimi;

   2) tieto- ja viestintätekniikan tuotteen tai suojausprofiilin ja tarvittaessa arvioinnin kohteen tyyppi;

   3) tieto- ja viestintätekniikan tuotteen tai suojausprofiilin versio;

   4) sertifikaatin haltijan nimi, osoite ja yhteystiedot;

   5) linkki sertifikaatin haltijan verkkosivustolle, jolta saa asetuksen (EU) 2019/881 55 artiklassa tarkoitetut täydentävät kyberturvallisuustiedot;

c) tieto- ja viestintätekniikan tuotteen tai suojausprofiilin arviointiin ja sertifiointiin liittyvät tiedot, mukaan lukien seuraavat:

   1) sertifikaatin myöntäneen sertifiointielimen nimi, osoite ja yhteystiedot;

   2) arvioinnin suorittaneen ITSEFin nimi, jos eri kuin sertifiointielin;

   3) toimivaltaisen kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen nimi;

   4) viittaus tähän asetukseen;

   5) viittaus liitteessä V tarkoitettuun sertifikaattia vastaavaan sertifiointiraporttiin;

   6) tämän asetuksen 4 artiklan mukaisesti sovellettava varmuustaso;

   7) viittaus 3 artiklassa tarkoitettujen arvioinnissa käytettyjen standardien versioon;

   8) varmuustason tai varmennuspaketin yksilöinti 3 artiklassa tarkoitettujen standardien pohjalta ja liitteen VIII mukaisesti, mukaan lukien käytetyt turvallisuuden varmistuksen komponentit ja asianomainen AVA_VAN-taso;

   9) tarvittaessa viittaus yhteen tai useampaan suojausprofiiliin, jota tieto- ja viestintätekniikan tuote tai suojausprofiili vastaa;

   10) myöntämispäivä;

   11) sertifikaatin voimassaoloaika;

d) sertifikaattiin 11 artiklan mukaisesti liitetty merkki ja merkintä

LIITE VIII

Varmennuspakettia koskeva ilmoitus

1. Yhteisissä kriteereissä (Common Criteria) olevista määritelmistä poiketen korotusta (*augmentation*) koskevat seuraavat säännöt:

a) sitä ei merkitä lyhenteellä ”+”;

b) se täsmennetään antamalla luettelo kaikista kyseeseen tulevista komponenteista;

c) se esitetään yksityiskohtaisesti sertifiointiraportissa.

2. EUCC-sertifikaatissa vahvistettua varmuustasoa voidaan täydentää arvioinnin vakuuttavuustasolla (*evaluation assurance level*, EAL) siten kuin täsmennetään tämän asetuksen 3 artiklassa.

3. Jos EUCC-sertifikaatissa vahvistetussa varmuustasossa ei viitata korotukseen, EUCC-sertifikaatissa ilmoitetaan jompikumpi seuraavista paketeista:

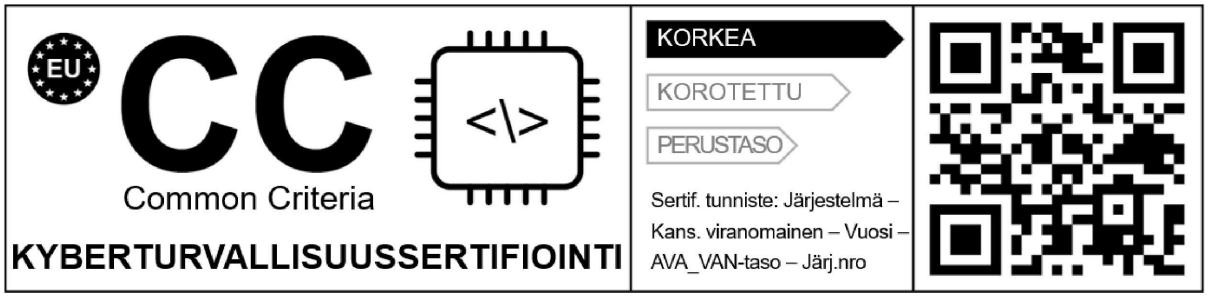
a) ”erityinen varmennuspaketti” (*specific assurance package*);

b) ”suojausprofiilia vastaava varmennuspaketti” (*assurance package conformant to a protection profile*), jos viitataan suojausprofiiliin ilman arvioinnin vakuuttavuustasoa (EAL).

LIITE IX

Merkki ja merkintä

1. Merkin ja merkinnän muoto:



2. Jos merkkiä ja merkintää pienennetään tai suurennetaan, on noudatettava yllä olevan kuvan mukaisia mittasuhteita.

3. Fyysisen merkin ja merkinnän on oltava vähintään 5 mm korkeita.