Euroopan unionin
virallinen lehti

FI
L-sarja

2025/2462

9.12.2025

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2025/2462,

annettu 8 päivänä joulukuuta 2025,

täytäntöönpanoasetuksen (EU) 2024/482 muuttamisesta määritelmien, tieto- ja viestintätekniikan tuotesarjojen sertifioinnin, varmistuksen jatkuvuuden ja viimeisintä kehitystä edustavien asiakirjojen osalta

(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) Komission täytäntöönpanoasetuksessa (EU) 2024/482 ([2]) 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.

(2) Yhteiset kriteerit (Common Criteria, CC) ovat tietojärjestelmäkehityksen tietoturvallisuuden kansainvälinen arviointistandardi, johon liittyvät yhteiset arviointimenetelmät (Common Evaluation Methodology) mahdollistavat tieto- ja viestintätekniikan tuotteiden turvallisuuden arvioinnin sertifiointitarkoituksiin. Jotkin tieto- ja viestintätekniikan tuotteet voivat rakentua samalle toiminnalliselle perustalle, jotta eri alustoilla tai laitteissa voidaan tarjota samanlaisia turvallisuustoimintoja. Tällaisia tuotteita kutsutaan myös tuotesarjaksi. Suunnittelu, laitteisto, laiteohjelmisto tai ohjelmistot voivat tällöin kuitenkin vaihdella tieto- ja viestintätekniikan tuotteesta toiseen. Sertifiointielimen tehtävänä on päättää tapauskohtaisesti, voidaanko tuotesarja sertifioida. Tuotesarjojen sertifioinnin edellytyksiä voidaan kuvata tarkemmin EUCC:n soveltamista tukevissa suuntaviivoissa.

(3) Sertifioitujen tuotteiden luotettavuuden ylläpitämiseksi on olennaisen tärkeää määritellä, mikä on merkittävä ja mikä on vähäinen muutos arvioinnin kohteessa (*target of evaluation*, TOE) tai sen ympäristössä, mukaan lukien toiminta- tai kehitysympäristöt. Näin ollen on tarpeen täsmentää kyseiset käsitteet ottaen huomioon nykyiset ja laajalti käytetyt tekniset eritelmät, jotka ovat peräisin johtavien virkamiesten tietoturvallisuusryhmältä (SOG-IS) ja yhteisten kriteerien mukaisten sertifikaattien tunnustamista tietotekniikan turvallisuuden alalla koskevaan järjestelyyn (Arrangements on the Recognition of Common Criteria Certificates in the field of IT Security), jäljempänä ’CCRA’, osallistuvilta tahoilta.

(4) Vähäisille muutoksille on usein ominaista, että niillä on vain vähäinen vaikutus myönnetyllä EUCC-sertifikaatilla annettuun tuotevarmennuslausumaan. Vähäisten muutosten käsittelyn tulisi näin ollen tapahtua ylläpitomenettelyjen yhteydessä, eivätkä ne edellytä tuotteen turvallisuustoimintojen uudelleenarviointia. Esimerkkejä vähäisistä muutoksista, jotka pitäisi käsitellä ylläpidon kautta, ovat muun muassa toimitukselliset muutokset, sellaiset arvioinnin kohteen ympäristön muutokset, jotka eivät muuta sertifioitua arvioinnin kohdetta, ja sellaiset sertifioidun arvioinnin kohteen muutokset, joilla ei ole vaikutusta turvallisuuden varmistuksen evidenssin kannalta. Myös kehitysympäristön muutoksia voidaan pitää vähäisinä edellyttäen, että niillä ei ole seurannaisvaikutuksia voimassa oleviin turvallisuuden varmistuksen toimenpiteisiin. Joissakin tapauksissa ne voivat kuitenkin edellyttää kyseeseen tulevien toimenpiteiden osittaista arviointia.

([1]) EUVL L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) 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 (EUVL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) Merkittävä muutos on mikä tahansa muutos sertifioidussa arvioinnin kohteessa tai sen ympäristössä, jos voi vaikuttaa kielteisesti EUCC-sertifikaatissa ilmaistuun varmuuteen, minkä vuoksi tällaisen muutoksen tulisi edellyttää uudelleenarviointia. Esimerkkejä merkittävistä muutoksista ovat muun muassa muutokset ilmoitettuihin varmistusvaatimuksiin, lukuun ottamatta CC ALC_FLR -perheen (puutteiden korjaaminen) varmistusvaatimuksia, muutokset kehitysympäristön luottamuksellisuuden tai eheyden valvontaan, jos tällaiset muutokset voivat vaikuttaa arvioinnin kohteen turvalliseen kehittämiseen tai tuotantoon, tai muutokset, jotka arvioinnin kohteeseen tehdään hyödynnettävissä olevan haavoittuvuuden poistamiseksi. Lisäksi myös yksittäinen joukko vähäisiä muutoksia, joilla on yhdessä merkittävä vaikutus turvallisuuteen, voidaan katsoa merkittäväksi muutokseksi. On myös tärkeää tunnustaa, että vaikka ohjelmavirheen korjaus voi vaikuttaa vain tiettyyn arvioinnin kohteen näkökohtaan, sen ennakoimattomuus ja potentiaalinen vaikutus varmuuden kannalta voivat tehdä muutoksesta merkittävän, mikäli se asettaa kyseenalaiseksi sertifioinnin antamat turvallisuusvarmistukset.

(6) Muutokset muuttamattoman sertifioidun tieto- ja viestintätekniikan tuotteen uhkaympäristössä saattavat edellyttää uudelleenarviointia. Tällaisen uudelleenarviointiprosessin mahdolliset tulokset ja erityisesti sen vaikutus EUCC-sertifikaatin kannalta olisi määriteltävä selkeästi. Jos uudelleenarviointi saatetaan päätökseen onnistuneesti, sertifiointielimen tulisi vahvistaa sertifikaatti tai myöntää uusi sertifikaatti, jonka voimassaolon päättymistä on myöhennetty. Jos uudelleenarviointiprosessi ei johda tulokseen, sertifiointielimen tulisi peruuttaa sertifikaatti ja mahdollisesti myöntää uusi sertifikaatti uudella kattavuudella. Kyseisiä säännöksiä olisi sovellettava soveltuvin osin suojausprofiilien uudelleenarviointiin.

(7) Täytäntöönpanoasetuksen (EU) 2024/482 liitteessä I luetellaan tieto- ja viestintätekniikan tuotteiden ja suojausprofiilien arvioinnissa sovellettavat viimeisintä kehitystä edustavat asiakirjat. Näitä viimeisintä kehitystä edustavia asiakirjoja olisi päivitettävä viimeisimmän kehityksen, kuten teknologian, kyberuhkaympäristön, toimialan käytäntöjen tai kansainvälisten standardien kehityksen, huomioon ottamiseksi. Päivitys on tarkoituksenmukainen viimeisintä kehitystä edustaville asiakirjoille, jotka koskevat paikkakohtaisen turvallisuuden vähimmäisvaatimuksia, hyökkäyspotentiaalin soveltamista älykortteihin, hyökkäyspotentiaalin soveltamista tietoturvaboksilla varustettuihin laitteisiin, yhteisten kriteerien soveltamista integroituihin piireihin ja yhdistettyjen tuotteiden arviointia älykorteille ja vastaaville laitteille. Mukaan eivät sisälly viimeisintä kehitystä edustavat asiakirjat, jotka koskevat yhdistettyjen tuotteiden arviointia ja sertifiointia käyttämällä yhteisten kriteerien standardien uusinta versiota, paikalla tehtävien tarkastusten arviointitulosten uudelleenkäyttöä ja selvennyksiä suojausprofiilien tulkinnasta hyväksyttyjen sähköisen allekirjoituksen luontivälineiden, ajopiirtureiden ja laitteistoturvamoduulien osalta. Jotta varmistetaan tieto- ja viestintätekniikan tuotteiden yhdenmukainen arviointi EUCC:n puitteissa, liitettä I olisi muutettava sisällyttämällä siihen kyseiset päivitetyt ja uudet viimeisintä kehitystä edustavat asiakirjat, kun Euroopan kyberturvallisuuden sertifiointiryhmä (ECCG) on hyväksynyt ne.

(8) Järjestelmään olisi myös lisättävä viimeisintä kehitystä edustava asiakirja ”ADV_SPM.1 interpretation for CC:2022 transition”, jotta spesifeihin suojausprofiileihin perustuvissa sertifiointiprosesseissa voidaan edelleen käyttää muodollista mallintamista (ADV_SPM.1), kunnes vastaavat suojausprofiilit päivitetään, esimerkiksi lisäämällä CC:2022:n vaatimukset täyttävä ADV_SPM.1:tä tukeva suojausprofiili useammalla varmuuskonfiguraatiolla. Jotta markkinoilla olisi riittävästi aikaa siirtyä päivitettyihin yhteisten kriteerien standardeihin, tarvitaan erityisiä siirtymäsääntöjä suojausprofiileille Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, tai Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020. Markkinahäiriöiden välttämiseksi olisi vahvistettava, että viimeisintä kehitystä edustava asiakirja ”ADV_SPM.1 interpretation for CC:2022 transition” on sovellettavissa sertifiointiprosesseihin, jotka on käynnistetty ennen tämän asetuksen hyväksymistä. Kyseisen asiakirjan soveltaminen olisi kuitenkin rajattava tiukasti siihen, mikä on tarpeen ottaen huomioon vastaavien suojausprofiilien päivittämiseen tarvittava aika. Tarkemmin sanottuna sertifiointiprosesseissa, joissa käytetään suojausprofiileja Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, tai Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, viimeisintä kehitystä edustavaa asiakirjaa tulisi soveltaa niihin prosesseihin, jotka on käynnistetty ennen 1 päivää lokakuuta 2026. Sertifiointiprosesseissa, joissa käytetään suojausprofiilia Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, viimeisintä kehitystä edustavaa asiakirjaa tulisi soveltaa ainoastaan ennen tämän asetuksen voimaantulopäivää käynnistettyihin prosesseihin, koska suojausprofiilista Java Card System – Open Configuration on jo saatavilla uusi versio.

(9) Viimeisintä kehitystä edustavien asiakirjojen muuttaminen sertifiointiprosessin aikana voi häiritä tuotteen arviointia ja viivästyttää sertifikaatin myöntämistä. Siksi tarvitaan asianmukaiset siirtymäsäännöt uusia tai päivitettyjä viimeisintä kehitystä edustavia asiakirjoja varten, jotta myyjät, ITSEFit, sertifiointielimet ja muut sidosryhmät voivat tehdä tarvittavat mukautukset. Sovellettavia päivitettyjä ja uusia viimeisintä kehitystä edustavia asiakirjoja tulisi soveltaa sertifiointihakemusten tapauksessa, mukaan lukien uudelleenarviointeja koskevat hakemukset, kun taas meneillään olevissa sertifiointiprosesseissa tulisi voida käyttää edelleen viimeisintä kehitystä edustavien asiakirjojen aikaisempia versioita.

(10) Täytäntöönpanoasetuksen (EU) 2024/482 liitteissä II ja III luetellaan AVA_VAN-tasolla 4 tai 5 sertifioidut suojausprofiilit ja suositellut suojausprofiilit. Monet viittauksista ovat puutteellisia tai vanhentuneita, koska suojausprofiileja on päivitetty. Viittauksia olisi täydennettävä ja uusia viittauksia lisättävä, jotta varmistetaan suojattujen integroitujen piirien, älykorttien ja niihin liittyvien laitteiden sekä luotettujen suoritusympäristöjen parempi kattavuus.

(11) Täytäntöönpanoasetuksen (EU) 2024/482 19 artiklaa on tarpeen muuttaa selventämällä, että liitettä IV sovelletaan tarvittavin muutoksin EUCC-sertifikaattien tarkastamiseen suojausprofiilien osalta.

(12) Koska turvatavoite (*security target*, ST) on keskeinen tekijä sertifiointiprosessin laajuuden ymmärtämisessä, ENISAn on myös tarpeen julkaista kutakin EUCC-sertifikaattia vastaava turvatavoite verkkosivustollaan.

(13) Lisäksi sertifiointielinten olisi toimitettava ENISAlle englanninkielinen versio turvatavoitteesta ja sertifiointiraportista, jotta ENISA voi asettaa nämä tiedot saataville englannin kielellä verkkosivustollaan täytäntöönpanoasetuksen (EU) 2024/482 42 artiklan 2 kohdan mukaisesti. Sertifioinnin hakijoiden olisi sen vuoksi pyydettäessä toimitettava sertifiointielimille englanninkielinen versio turvatavoitteesta.

(14) Sertifikaatin yksilöllisessä tunnisteessa ei ole tarpeen viitata sertifiointielimeen sen nimellä, sillä sertifiointielimen tunnusnumero riittää kyseisen elimen yksilöimiseen. Myöskään myöntämiskuukautta ei tarvitse ilmoittaa, koska sertifikaatit lasketaan vuosittain. Siksi kyseinen vaatimus olisi yksinkertaisuuden vuoksi poistettava. Koska sertifikaatin myöntämisvuosi vastaa ensimmäisen sertifikaatin myöntämistä, sama päivämäärä olisi mainittava tarkastuksen jälkeen myönnettyjen sertifikaattien yksilöllisessä tunnisteessa jäljitettävyyden varmistamiseksi.

(15) Sen vuoksi täytäntöönpanoasetusta (EU) 2024/482 olisi muutettava.

(16) Tässä asetuksessa säädetyt toimenpiteet ovat asetuksen (EU) 2019/881 66 artiklalla perustetun komitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

1 artikla

Muutetaan täytäntöönpanoasetus (EU) 2024/482 seuraavasti:

1) lisätään 2 artiklaan 16, 17 ja 18 kohta seuraavasti:

”16) ’tuotesarjalla’ hakijan tieto- ja viestintätekniikan tuotteiden kokonaisuutta, joka rakentuu samalle toiminnalliselle perustalle samojen turvallisuustarpeiden täyttämiseksi ja jossa suunnittelu, laitteisto, laiteohjelmisto tai ohjelmistot voivat vaihdella tieto- ja viestintätekniikan tuotteesta toiseen;

17) ’vähäisellä muutoksella’ mitä tahansa sertifioidun arvioinnin kohteen tai sen ympäristön muutosta, joka ei vaikuta kielteisesti EUCC-sertifikaatissa ilmaistuun varmuuteen;

18) ’merkittävällä muutoksella’ mitä tahansa sertifioidun arvioinnin kohteen tai sen ympäristön muutosta, joka voi vaikuttaa kielteisesti EUCC-sertifikaatissa ilmaistuun varmuuteen.”;

2) lisätään 5 artiklaan 3 kohta seuraavasti:

”3. Sertifiointielin voi sallia tuotesarjan sertifioinnin.”;

3) korvataan 9 artiklan 2 kohdan a alakohta seuraavasti:

”a) toimittaa sertifiointielimelle ja ITSEFille kaikki tarvittavat täydelliset ja paikkansapitävät tiedot ja antaa pyynnöstä tarvittavat lisätiedot, mukaan lukien englanninkielinen versio turvatavoitteesta;”;

4) korvataan 11 artiklan 3 kohdan b alakohta seuraavasti:

”b) sertifikaatin yksilöllinen tunniste, joka muodostuu seuraavista:

1) järjestelmän nimi;

2) täytäntöönpanoasetuksen (EU) 2024/3143 3 artiklan mukainen sertifikaatin myöntäneen sertifiointielimen tunnusnumero;

3) alkuperäisen sertifikaatin myöntämisvuosi;

4) sertifikaatin myöntäneen sertifiointielimen antama tunnistenumero.”;

5) korvataan 19 artiklan 1 kohta seuraavasti:

”1. Sertifiointielin voi sertifikaatin haltijan pyynnöstä tai muista perustelluista syistä päättää tarkastaa suojausprofiilin EUCC-sertifikaatin. Tarkastus tapahtuu liitteen IV mukaisesti. Sertifiointielin määrittää tarkastuksen laajuuden. Jos tarkastus sitä edellyttää, sertifiointielimen on pyydettävä ITSEFiä suorittamaan uudelleenarviointi sertifioidusta suojausprofiilista.”;

6) muutetaan 42 artikla seuraavasti:

a) lisätään 1 kohtaan i alakohta seuraavasti:

”i) kutakin EUCC-sertifikaattia vastaava turvatavoite;”;

b) korvataan 2 kohta seuraavasti:

”2. Edellä 1 kohdassa tarkoitetut tiedot on annettava saataville ainakin englannin kielellä. Tätä varten sertifiointielinten on toimitettava ENISAlle sertifiointiraporttien ja turvatavoitteiden alkuperäiset kielitoisinnot ja lisäksi englanninkielinen versio kyseisistä asiakirjoista ilman aiheetonta viivytystä.”;

7) korvataan 48 artiklan 4 kohta seuraavasti:

”4. Jollei liitteessä I tai II toisin säädetä, viimeisintä kehitystä edustavia asiakirjoja sovelletaan sen muutossäädöksen soveltamispäivästä lähtien käynnistettyihin sertifiointimenettelyihin, mukaan lukien uudelleenarvioinnit, jolla viimeisintä kehitystä edustavat asiakirjat on sisällytetty liitteeseen I tai II.”;

8) korvataan liite I tämän asetuksen liitteessä I olevalla tekstillä;

9) korvataan liite II tämän asetuksen liitteessä II olevalla tekstillä;

10) korvataan liite III tämän asetuksen liitteessä III olevalla tekstillä;

11) muutetaan liite IV tämän asetuksen liitteen IV mukaisesti;

12) muutetaan liite V tämän asetuksen liitteen V mukaisesti;

13) korvataan liite IX tämän asetuksen liitteessä VI olevalla tekstillä.

2 artikla

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

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

Tehty Brysselissä 8 päivänä joulukuuta 2025.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN

LIITE I

”LIITE I

Tekniikan osa-alueita tukevat viimeisintä kehitystä edustavat asiakirjat ja muut viimeisintä kehitystä edustavat asiakirjat

1. Viimeisintä kehitystä edustavat asiakirjat, jotka tukevat tekniikan osa-alueita AVA_VAN-tasolla 4 tai 5:
   a) seuraavat tekniikan osa-alueen ”älykortit ja vastaavat laitteet” yhdenmukaistettuun arviointiin liittyvät asiakirjat:
      1) ”Minimum ITSEF requirements for security evaluations of smart cards and similar devices” (älykorttien ja vastaavien laitteiden turvallisuusarviointien vähimmäisvaatimukset), versio 1.1;
      2) ”Minimum Site Security Requirements” (paikkakohtaista turvallisuutta koskevat vähimmäisvaatimukset), versio 2;
      3) ”Reusing evaluation results of site audits (STAR)” (paikalla tehtävien tarkastusten arviointitulosten uudelleenkäyttö), versio 1;
      4) ”Application of Common Criteria to integrated circuits” (yhteisten kriteerien soveltaminen integroituihin piireihin), versio 2;
      5) ”Security Architecture requirements (ADV_ARC) for smart cards and similar devices” (älykorttien ja vastaavien laitteiden turvallisuusarkkitehtuurivaatimukset (ADV_ARC)), versio 1.1;
      6) ”Certification of ’open’ smart card products” (”avoimien” älykorttituotteiden sertifiointi), versio 1.1;
      7) ”Composite product evaluation for smart cards and similar devices for CC3.1” (yhdistettyjen tuotteiden arviointi älykorteille ja vastaaville laitteille), versio 2;
      8) ”Composite product evaluation and certification for CC:2022” (yhdistettyjen tuotteiden arviointi ja sertifiointi), versio 1;
      9) ”Application of Attack Potential to Smartcards and Similar Devices” (hyökkäyspotentiaalin soveltaminen älykortteihin ja vastaaviin laitteisiin), versio 2;
      10) ”Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices” (hyväksyttyjen sähköisen allekirjoituksen/leiman luontivälineiden turvallisuuden arviointi ja sertifiointi), versio 1;
      11) ”ADV_SPM.1 interpretation for CC:2022 transition” (ADV_SPM.1:n tulkinta siirtymiselle CC:2022:een), versio 1.1, sovellettavissa sertifiointiprosesseihin, joissa käytetään
         a) suojausprofiileja Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, tai Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, ja jotka on käynnistetty ennen 1. lokakuuta 2026;
         b) suojausprofiilia Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, ja jotka on käynnistetty ennen 29 päivää joulukuuta 2025.
   b) seuraavat tekniikan osa-alueen ”tietoturvaboksilla varustetut laitteet” yhdenmukaistettuun arviointiin liittyvät asiakirjat:
      1) ”Minimum ITSEF requirements for security evaluations of hardware devices with security boxes” (tietoturvaboksilla varustettujen laitteiden turvallisuusarviointien vähimmäisvaatimukset), versio 1.1;
      2) ”Minimum Site Security Requirements” (paikkakohtaista turvallisuutta koskevat vähimmäisvaatimukset), versio 2;
      3) ”Reusing evaluation results of site audits (STAR)” (paikalla tehtävien tarkastusten arviointitulosten uudelleenkäyttö), versio 1;
      4) ”Application of Attack Potential to hardware devices with security boxes” (hyökkäyspotentiaalin soveltaminen tietoturvaboksilla varustettuihin laitteisiin), versio 2;
      5) ”Hardware assessment in EN 419221-5 (HSM PP)” (laitteiden arviointi standardissa EN 419221-5), versio 1;
      6) ”JIL Tachograph MS PP Clarification” (suojausprofiilin selvennys JIL-ajopiirturille), versio 1.
2. Vaatimustenmukaisuuden arviointilaitosten yhdenmukaistettuun akkreditointiin liittyvät viimeisintä kehitystä edustavat asiakirjat:
   a) ”Accreditation of ITSEFs for the EUCC” (ITSEFien akkreditointi EUCC:ia varten), versio 1.1, ennen 8. heinäkuuta 2025 myönnetyille akkreditoinneille;
   b) ”Accreditation of ITSEFs for the EUCC” (ITSEFien akkreditointi EUCC:ia varten), versio 1.6c, 8. heinäkuuta 2025 jälkeen ensimmäistä kertaa myönnetyille tai tarkastetuille akkreditoinneille.
   c) ”Accreditation of CBs for the EUCC” (sertifiointielinten akkreditointi EUCC:ia varten), versio 1.6b.”.

LIITE II

”LIITE II

AVA_VAN -tasolla 4 tai 5 sertifioidut suojausprofiilit

1. Hyväksytyille sähköisen allekirjoituksen ja sähköisen leiman etäluontivälineille:

   a) EN 419241-2:2019 – Trustworthy Systems Supporting Server Signing – Part 2: Protection Profile for QSCD for Server Signing (v0.16), ANSSI-CC-PP-2018/02-M01;

   b) EN 419221-5:2018 – Protection profiles for Trust Service Provider Cryptographic modules – Part 5: Cryptographic Module for Trust Services (v0.15), ANSSI-CC-PP-2016/05-M01

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

   [TYHJÄ].”

LIITE III

”LIITE III

Suositellut suojausprofiilit

Tieto- ja viestintätekniikan tuotteiden sertifioinnissa käytettävät suojausprofiilit, mukaan lukien tuotteet seuraavilla tekniikan osa-alueilla:

1. Älykortit ja vastaavat laitteet

   a) matkustusasiakirjat:

      1) PP Machine Readable Travel Document with ”ICAO Application” Basic Access Control (v1.10), BSI-CC-PP-0055-2009;

      2) PP Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP) (v1), BSI-CC-PP-0068-V2-2011-MA-01;

      3) PP Machine Readable Travel Document with ”ICAO Application” Extended Access Control with PACE (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;

   b) turvalliset allekirjoituksen luomisvälineet (SSCD):

      1) EN 419211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation (v1.03), BSI-CC-PP-0059-2009-MA-02;

      2) EN 419211-3:2013 – Protection profiles for secure signature creation device – Part 3: Device with key import (v1.0.2), BSI-CC-PP-0075-2012-MA-01;

      3) 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 (v1.0.1), BSI-CC-PP-0071-2012-MA-01;

      4) 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 (v1.0.1), BSI-CC-PP-0072-2012-MA-01;

      5) 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 (v1.0.4), BSI-CC-PP-0076-2013-MA-01;

   c) ajopiirturit: Digital Tachograph – Tachograph Card (TC PP) (v1.0), BSI-CC-PP-0091-2017;

   d) suojatut integroidut piirit, Java Card -alusta ja eUICC:

      1) Universal SIM Java Card Platform Protection Profile Basic and SCWS Configurations (v2.0.2), ANSSI-CC-PP-2010/04 (Basic), ANSSI-CC-PP-2010/05 (Basic ja SCWS);

      2) Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014;

      3) Embedded UICC (eUICC) for Machine-to-Machine Devices (v1.1), BSI-CC-PP-0089-2015;

      4) Cryptographic Service Provider – CSP (v0.9.8), BSI-CC-PP-0104-2019;

      5) Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, BSI-CC-PP-0107-2019;

      6) Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering (PPC-CSP-TS-Au-Cl) Version 0.9.4, BSI-CC-PP-0108-2019;

      7) Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020;

      8) Secure Element Protection Profile – GPC_SPE_174 (v1.0), CCN-CC-PP-5-2021;

      9) Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile (v1.8), BSI-CC-PP-0117-V2-2023;

      10) Java Card System – Open Configuration (v3.2), BSI-CC-PP-0099-V3-2024;

      11) Embedded UICC for Consumer Devices Protection Profile (v2.1), BSI-CC-PP-0100-V2-2025;

   e) TPM:t (Trusted Platform Modules): Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0; Level 0; Revision 1.59 (v1.3), ANSSI-CC-PP-2021/02.

2. Tietoturvaboksilla varustetut laitteet

a) maksupäätteet ja (vastaavat) vuorovaikutuspisteet (POI):

1) Point of Interaction ”POI-CHIP-ONLY” (v4.0), ANSSI-CC-PP-2015/01;

2) Point of Interaction ”POI-CHIP-ONLY and Open Protocol Package” (v4.0), ANSSI-CC-PP-2015/02;

3) Point of Interaction ”POI-COMPREHENSIVE” (v4.0), ANSSI-CC-PP-2015/03;

4) Point of Interaction ”POI-COMPREHENSIVE and Open Protocol Package” (v4.0), ANSSI-CC-PP-2015/04;

5) Point of Interaction ”POI-PED-ONLY” (v4.0), ANSSI-CC-PP-2015/05;

6) Point of Interaction ”POI-PED-ONLY and Open Protocol Package” (v4.0), ANSSI-CC-PP-2015/06;

b) laitteistoturvamoduulit:

1) Cryptographic Module for CSP Signing Operations with Backup – PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08;

2) Cryptographic Module for CSP Key Generation Services – PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09;

3) Cryptographic Module for CSP Signing Operations without Backup – PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10;

c) ajopiirturit:

1) Digital Tachograph – Motion Sensor (MS PP) (v1.0), BSI-CC-PP-0093-2017;

2) Digital Tachograph – Vehicle Unit (VU PP) (v1.15), BSI-CC-PP-0094-V2-2021;

3) Digital Tachograph – External GNSS Facility (EGF PP) (v1.10), BSI-CC-PP-0092-V2-2021.

3. Muut: Trusted Execution Environment Protection Profile – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.”

LIITE IV

Muutetaan täytäntöönpanoasetuksen (EU) 2024/482 liite IV seuraavasti:

1) korvataan IV.2 jakson 4 kohta seuraavasti:

”4. Sertifiointielin tarkastelee päivitettyä teknistä arviointiraporttia ja laatii uudelleenarviointiraportin. Alkuperäisen sertifikaatin tilaa muutetaan sen jälkeen 13 tai 19 artiklan mukaisesti. Jos uudelleenarviointi saatetaan päätökseen onnistuneesti, sovelletaan 13 artiklan 2 kohdan a tai c alakohtaa tuotteen sertifioinnin tapauksessa ja 19 artiklan 2 kohdan a tai c alakohtaa suojaprofiilin sertifioinnin tapauksessa. Jos uudelleenarviointiprosessi ei johda tulokseen, sovelletaan 13 artiklan 2 kohdan b tai d alakohtaa tuotteen sertifioinnin tapauksessa ja 19 artiklan 2 kohdan b tai d alakohtaa suojaprofiilin sertifioinnin tapauksessa.”;

2) muutetaan IV.3 jakso seuraavasti:

a) korvataan IV.3 jakson otsikko seuraavasti:

”IV.3 **Sertifioidun tieto- ja viestintätekniikan tuotteen muutokset – ylläpito ja uudelleenarviointi**”;

b) korvataan 4 ja 5 kohta seuraavasti:

”4. Tarkastelun jälkeen sertifiointielin määrittää yksittäisen muutoksen laajuuden vähäiseksi tai merkittäväksi sen mukaan, mikä on sen vaikutus EUCC-sertifikaatissa ilmaistuun varmuuteen.

5. Jos sertifiointielin on vahvistanut, että muutokset ovat vähäisiä, muutetulle tieto- ja viestintätekniikan tuotteelle ei 13 artiklan 2 kohdan a alakohdan tai 19 artiklan 2 kohdan a alakohdan mukaisesti myönnetä uutta sertifikaattia ja alkuperäiseen sertifiointiraporttiin lisätään ylläpitoraportti.”;

c) lisätään 5 a kohta seuraavasti:

”5 a. Jos turvallisuuden varmistuksen toimenpiteisiin tehdään muutoksia kehitysympäristössä, mukaan lukien CC ALC_FLR -perheen (puutteiden korjaaminen) varmistusvaatimusten lisääminen, sertifiointielin voi pyytää ITSEFiä tekemään osa-arvioinnin kyseeseen tulevista turvallisuuden varmistuksen toimenpiteistä. ITSEF antaa osittaisen teknisen arviointiraportin, jonka perusteella sertifiointielin vahvistaa, että muutokset ovat joko vähäisiä tai merkittäviä. Jos sertifiointielin on vahvistanut, että muutokset ovat vähäisiä, sovelletaan liitteessä IV olevan IV.3 jakson 5 kohtaa. Jos sertifiointielin on vahvistanut, että muutokset ovat merkittäviä, sovelletaan liitteessä IV olevan IV.3 jakson 7 kohtaa.”.

LIITE V

Korvataan täytäntöönpanoasetuksen (EU) 2024/482 liitteessä V oleva V.1 jakso seuraavasti:

"V.1 **Sertifiointiraportti**

1. Sertifiointiviranomainen laatii ITSEFin toimittamien teknisten arviointiraporttien perusteella sertifiointiraportin, joka julkaistaan yhdessä vastaavan EUCC-sertifikaatin ja turvatavoitteen (*security target*, ST) kanssa.

2. Sertifiointiraportti sisältää yksityiskohtaiset käytännön tiedot tieto- ja viestintätekniikan tuotteesta ja tuotteen turvallisesta käytöstä. Sen 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;
   c) tieto- ja viestintätekniikan tuotteen arviointiin liittyvät yhteystiedot;
   d) turvallisuusperiaatteet;
   e) oletukset ja soveltamisalan selventäminen;
   f) arkkitehtuuritiedot;
   g) täydentävät kyberturvallisuustiedot soveltuvin osin;
   h) yhteenveto tieto- ja viestintätekniikan tuotteen arvioinnista ja arvioitu konfiguraatio;
   i) arvioinnin tulokset ja sertifikaattia koskevat tiedot;
   j) tarvittaessa huomautukset ja suositukset;
   k) liitteet (jos on);
   l) viittaus sertifioitavaksi toimitetun tieto- ja viestintätekniikan tuotteen turvatavoitteeseen;
   m) järjestelmään liitetty merkki tai merkintä, jos sellainen on saatavilla;
   n) sanasto (jos on);
   o) lähdeluettelo.

4. Edellä 3 kohdan a alakohdassa tarkoitettu tiivistelmä on lyhyt yhteenveto koko sertifiointiraportista. Siinä esitetään selkeä ja tiivis yleiskatsaus arvioinnin tuloksista, ja siinä on seuraavat tiedot:
   a) arvioidun tieto- ja viestintätekniikan tuotteen nimi;
   b) arvioinnin suorittaneen ITSEFin nimi;
   c) arvioinnin valmistumispäivä;
   d) sertifikaatin myöntämispäivä;
   e) soveltuvin osin alkuperäisen sertifikaatin myöntämispäivä;
   f) voimassaoloaika;
   g) sertifikaatin yksilöllinen tunniste 11 artiklan mukaisesti;
   h) lyhyt kuvaus sertifiointiraportin tuloksista, mukaan lukien seuraavat:
      i) arviointiin sovellettavien yhteisten kriteerien (Common Criteria) versio ja tarvittaessa julkaisu;
      ii) yhteisten kriteerien varmennuspaketti tai lista turvallisuuden varmistuksen komponenteista, mukaan lukien arvioinnissa sovellettu AVA_VAN-taso ja vastaava asetuksen (EU) 2019/881 52 artiklassa säädetty varmuustaso, johon EUCC-sertifikaatissa viitataan;
      iii) soveltuvin osin suojausprofiilit, joiden suhteen tieto- ja viestintätekniikan tuote ilmoitetaan vaatimusten-mukaiseksi;
      iv) viittaus arvioidun tieto- ja viestintätekniikan tuotteen turvallisuusperiaateisiin;
      v) soveltuvin osin vastuuvapauslausek(k)e(et).

5. Edellä 3 kohdan b alakohdassa tarkoitetuissa tunnistetiedoissa on selkeästi yksilöitävä arvioitu tieto- ja viestintätekniikan tuote, mukaan lukien seuraavat:

   a) arvioidun tieto- ja viestintätekniikan tuotteen yksilöllinen tunniste;

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

   c) viittaus sertifioidun tieto- ja viestintätekniikan tuotteen toimintaympäristöä koskeviin lisävaatimuksiin.

6. Edellä 3 kohdan c alakohdassa tarkoitettujen yhteystietojen on sisällettävä vähintään seuraavat tiedot:

   a) kehittäjän nimi;

   b) EUCC-sertifikaatin haltijan nimi ja yhteystiedot;

   c) sertifikaatin myöntäneen sertifiointielimen nimi;

   d) toimivaltainen kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen;

   e) arvioinnin suorittaneen ITSEFin nimi ja tarvittaessa luettelo alihankkijoista.

7. Edellä 3 kohdan d alakohdassa tarkoitetuissa turvallisuusperiaatteissa on oltava kuvaus tieto- ja viestintätekniikan tuotteen turvallisuusperiaatteista kattaen kaikki turvallisuuspalvelut sekä toimintaperiaatteista tai säännöistä, jotka arvioidussa tuotteessa on pantava täytäntöön tai joita siinä on noudatettava. Niissä esitetään myös seuraavat tiedot:

   a) kuvaus sertifikaatin haltijan käyttämistä haavoittuvuuksien hallinta- ja julkistamismenettelyistä täydennettynä ainoastaan tiedoilla, jotka voidaan asettaa julkisesti saataville;

   b) sertifikaatin haltijan varmistuksen jatkuvuuteen soveltamat periaatteet, mukaan lukien tarvittaessa kuvaus sertifikaatin haltijan elinkaarihallinnasta tai tuotantoprosesseista liitteessä IV olevan IV.1 jakson mukaisesti;

   c) soveltuvin osin korjauspäivitysten hallintamenettelyn olemassaolo ja tulokset sen arvioinnista liitteessä IV olevan IV.4 jakson mukaisesti.

8. Edellä 3 kohdan e alakohdassa tarkoitetun oletusten ja soveltamisalan selventämisen on käsitettävä tietoja 7 artiklan 1 kohdan c alakohdassa tarkoitettuun tuotteen käyttötarkoitukseen liittyvistä olosuhteista ja tavoitteista, ja niihin on sisällyttävä 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;

   c) kuvaus mahdollisista tieto- ja viestintätekniikan tuotteeseen kohdistuvista uhkista, joita tuotteen arvioidut turvallisuustoiminnot eivät torju sen käyttötarkoituksesta riippuen, mikäli niitä pidetään merkityksellisinä tieto- ja viestintätekniikan tuotteen potentiaalisen käyttäjän kannalta.

   Ensimmäisessä alakohdassa tarkoitettujen tietojen on oltava mahdollisimman selkeitä ja ymmärrettäviä, jotta sertifioidun tieto- ja viestintätekniikan tuotteen potentiaaliset käyttäjät voivat tehdä tietoon perustuvia päätöksiä sen käyttöön liittyvistä riskeistä.

9. Edellä 3 kohdan f alakohdassa tarkoitettuihin arkkitehtuuritietoihin on sisällyttävä ylätason kuvaus tieto- ja viestintätekniikan tuotteesta ja sen pääkomponenteista perustuen suoritteisiin, jotka on määritelty yhteisten kriteerien perheessä Development – TOE Design (ADV_TDS).

10. Edellä 3 kohdan g alakohdassa tarkoitettujen täydentävien kyberturvallisuustietojen on asetuksen (EU) 2019/881 55 artiklan mukaisesti sisällettävä linkki EUCC-sertifikaatin haltijan verkkosivustolle.

11. Edellä 3 kohdan h alakohdassa tarkoitetussa tieto- ja viestintätekniikan tuotteen arvioinnissa ja konfiguraatiossa on kuvattava sekä kehittäjän että arvioijan suorittama testaus ja esitettävä testaustapa ja -konfiguraatio ja testauksen kattavuus. Siinä on oltava ainakin seuraavat tiedot:

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

    b) viimeisintä kehitystä edustavien asiakirjojen versio ja arvioinnissa käytetyt muut turvallisuuden arviointiperusteet;

    c) testauksessa ja haavoittuvuusanalyysissä käytetyn arvioinnin kohteen (*target of evaluation*, TOE) asetukset ja konfiguraatio;

    d) kaikki käytetyt suojausprofiilit, mukaan lukien suojausprofiilin nimi, versio, päiväys ja sertifikaatti.

12. Edellä 3 kohdan i alakohdassa tarkoitettujen arvioinnin tulosten ja sertifikaattia koskevien tietojen on sisällettävä tiedot tämän asetuksen 4 artiklassa ja asetuksen (EU) 2019/881 52 artiklassa tarkoitetusta saavutetusta varmuustasosta.

13. Edellä 3 kohdan j alakohdassa tarkoitettuja huomautuksia ja suosituksia käytetään arvioinnin tuloksista annettavan lisätiedon antamiseen. Huomautukset ja suositukset voivat koskea arvioinnin aikana havaittuja tieto- ja viestintätekniikan tuotteen puutteita tai erityisen hyödyllisiä ominaisuuksia.

14. Edellä 3 kohdan k alakohdassa tarkoitettuja liitteitä käytetään sellaisen lisätiedon esittämiseen, josta voi olla hyötyä raportin yleisölle mutta joka loogisesta näkökulmasta ei sovi raportin yksittäisiin osiin, esimerkiksi kun turvallisuusperiaatteista annetaan täydellinen kuvaus.

15. Edellä 3 kohdan l alakohdassa tarkoitetulla turvatavoitteella tarkoitetaan arvioitua turvatavoitetta. Arvioitu turvatavoite on ilmoitettava sertifiointiraportin mukana, jotta se voidaan julkaista asetuksen (EU) 2019/881 50 artiklan 1 kohdassa tarkoitetulla verkkosivustolla. Jos arvioidun turvatavoitteen sanitointi eli puhdistaminen tietyistä tiedoista on tarpeen ennen julkaisemista, se on tehtävä tämän asetuksen liitteessä V olevan V.2 jakson mukaisesti.

16. Edellä 3 kohdan m alakohdassa tarkoitetut EUCC-järjestelmään liitetyt merkit tai merkinnät on lisättävä sertifiointiraporttiin 11 artiklassa säädettyjen sääntöjen ja menettelyjen mukaisesti.

17. Edellä 3 kohdan n alakohdassa tarkoitettua sanastoa käytetään parantamaan raportin luettavuutta antamalla määritelmät lyhenteistä tai termeistä, joiden merkitys ei välttämättä ole ilmeinen.

18. Edellä 3 kohdan o alakohdassa tarkoitettu lähdeluettelo sisältää viittaukset kaikkiin sertifiointiraportin laadinnassa käytettyihin asiakirjoihin. Näihin tietoihin on sisällyttävä ainakin seuraavat:

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

    b) tekninen arviointiraportti;

    c) tapauksen mukaan tekninen arviointiraportti yhdistetystä tuotteesta;

    d) tekniset viiteasiakirjat;

    e) kehittäjän turvallisuusohjeet;

    f) kehittäjän konfiguraatioluettelo.

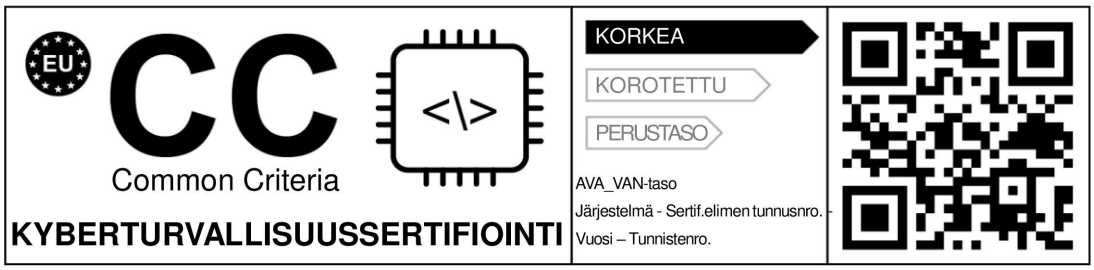
    Jotta voidaan taata arvioinnin uusittavuus, kaikki viitatut asiakirjat on yksilöitävä yksilöllisesti käyttäen oikeaa julkaisupäivää ja vastaavaa versionumeroa.”.

LIITE VI

”LIITE IX

Merkki ja merkintä

1. Merkin ja merkinnän muoto:



2. Jos merkkiä ja merkintää pienennetään tai suurennetaan, on noudatettava 1 kohdan mukaisia mittasuhteita.

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