Liikenne- ja viestintäviraston salaus- ja turvallisuuskriittisten tuotteiden arviointiohje

Versiohistoria

Päiväys	Kuvaus/muutos
23.4.2025	Korjattu lauserakenne kpl 8.8, liitteen nimi ja liitteen 2 taulukon otsikot.
7.2.2025	Yhdistetään ohjeet - *Liikenne- ja viestintävirasto Traficomin suorittamat salaustuotearvioinnit ja -hyväksynnät - Tilaajan näkökulma* (1487/651/2017, 6.3.2020) ja - *Liikenne- ja viestintävirasto Traficomin suorittamat turvallisuuskriittisten tuotteiden arvioinnit ja -hyväksynnät - Tilaajan näkökulma* (1487/651/2017, 4.1.2022) Lisätään ja päivitetään seuraavia - valmistajan alkuperän edellytykset - arvioinnin varmuustasojen määrittely - arviointimenettelyt/menetelmät - arviointiprosessin kuvaus - arviointiin tarvittava dokumentaatio (liite) - EU:n ja Naton (salaus)tuotehyväksynnät - viraston arvioinnin tuloksena antamat lausunnot ja päätökset ja milloin tieto arvioinnin tuloksesta voi olla julkinen - asiakirjojen ja aineiston käsittely julkisuuslain mukaan

Sisällys

1. Johdanto

1.1 Ohjeen tarkoitus

Tässä ohjeessa kuvataan salaustuotteiden ja muiden turvallisuuskriittisten tuotteiden arviointi- ja hyväksyntäprosessien pääperiaatteet ja eri tilanteet, joissa Liikenne- ja viestintävirasto (Traficom) voi tehdä arviointeja. Ohje koskee turvallisuusluokitellun tiedon sähköisen käsittelyn suojaamiseen tarkoitettuja tuotteita.

Ohje on tarkoitettu tietojärjestelmiensä turvallisuudesta vastaaville viranomaisille ja yrityksille, jotka valmistavat salaus- ja turvallisuuskriittisiä tuotteita. Ohjeen tarkoitus on kuvata tuotteiden arviointiprosesseja ja sitä, millaisia lausuntoja tai hyväksyntöjä Traficom voi antaa arvioinnin perusteella. Traficomin arvioinnin tavoitteena on tukea viranomaisten mahdollisuuksia hankkia turvallisuusluokitellun tiedon suojaamiseen riittävän turvallisia tuotteita, ja siten tukea viranomaisten riskienhallintatyötä turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmiensä suojaamisessa. Arviointityö edistää välillisesti myös valmistajien kilpailukykyä ja mahdollisuuksia osallistua esimerkiksi EU:n tai Naton turvallisuusluokitellun tiedon suojaamiseen liittyviin tietojärjestelmähankkeisiin tuotetoimittajan roolissa.

Tuotteen suunniteltu käyttötarkoitus vaikuttaa arviointiin. Keskeinen ero liittyy siihen, onko kysymyksessä kansallisen turvallisuusluokitellun tiedon suojaamiseen vai kansainväliseen tietoturvallisuusvelvoitteeseen liittyvä arviointi. Arviointiin vaikuttaa myös se, tehdäänkö arviointi itsenäisenä tuotearviointina vai osana tietojärjestelmän arviointia.

Kansallisen turvallisuusluokitellun tiedon suojaamisessa tietojärjestelmän vastuuviranomainen voi päättää tietojärjestelmissään käytettävistä tuotteista riskienarviointiinsa pohjautuen ja tuotearviointien hyödyntäminen on vapaaehtoista. Kansainvälisissä tietoturvallisuusvelvoitteissa sen sijaan edellytetään tyypillisesti, että turvallisuusluokitellun tiedon suojaamiseen käytetään vain toimivaltaisen tietoturvallisuusviranomaisen arvioimia ja hyväksymiä turvallisuuskriittisiä tuotteita.

Tämän ohjeen lisäksi Traficom ohjaa ja neuvoo arvioinnin yksityiskohdista tapauskohtaisesti.

1.2 Säännökset, joihin ohje perustuu

Ohje perustuu Traficomin arviointitehtäviin, joista säädetään viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011, arviointilaki) 4 §:ssä, turvallisuusselvityslain (726/2014) 9 §:n 3 momentissa ja kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004, kv-titulaki) 4 §:ssä.

Traficom toimii kv-titulain 4 §:n perusteella kansallisena salaustuotteiden hyväksyntäviranomaisena (CAA, Crypto Approval Authority), josta säädetään EU:n neuvoston turvallisuussääntöjen EU/488/2013 artiklassa 10.6 ja liitteessä IV.

Traficom toimii myös kansallisena viestintä- ja tietojärjestelmien turvallisuusviranomaisena (NCSA, National CIS Security Authority), josta säädetään Naton turvallisuussäännöstön C-M(2002)49-REV1 liitteen F kohdissa 11 ja 13 (ks. Laki tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdystä sopimuksesta ja turvallisuussäännöistä (907/2023), SopS 55/2023, asetus SopS 56/2023).

Traficomin tehtävät on määritelty laissa Liikenne- ja viestintävirastosta (23.11.2018/935). Sen mukaisesti Liikenne- ja viestintäviraston kyberturvallisuuskeskus - - tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä. Se ylläpitää kansallisen kyberturvallisuuden

tilannekuvaa. Kyberturvallisuuskeskuksen toiminta edistää ja varmistaa tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuutta.

Säännöksiä käsitellään tarkemmin jäljempänä.

1.3 Ohjeen suhde muuhun tuotesääntelyyn ja arviointiin

1.3.1 CRA

Tämä ohje ei koske EU:n kyberkestävyyssäädöksen (EU) 2024/2847 (nk. CRA, Cyber Resilience Act) mukaisia tuoteturvallisuusarviointeja. Asetusta ei 2 artiklan 7 alakohdan mukaan sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, jotka on kehitetty tai joita on muutettu yksinomaan kansalliseen turvallisuuteen tai puolustukseen liittyviin tarkoituksiin, eikä tuotteisiin, jotka on erityisesti suunniteltu turvallisuusluokiteltujen tietojen käsittelyä varten. Asetus ei toisaalta kuitenkaan estä markkinoilla tarjottavan tuotteen arvioimista viranomaisen turvallisuusluokitellun tiedon suojaamisen tarkoituksiin. CRA koskee EU:n sisämarkkinoilla tarjottavia digitaalisen elementin sisältäviä laitteita ja ohjelmistoja, jotka ovat suoraan tai epäsuorasti liitettävissä toiseen laitteeseen tai verkkoon.

1.3.2 Arviointilaitokset tai muut arviointitahot

Kansainvälisiin tietoturvallisuusvelvoitteisiin liittyvät arviointitehtävät on säädetty kv-titulaissa Traficomille. Tehtävien ulkoistaminen sopimuksella tai pätevyyden mahdollistaminen tietoturvallisuuden arviointilaitokselle edellyttäisi sääntelyn kehittämistä.

Myös **kansallisen turvallisuusluokitellun** tiedon suojaamiseksi arviointilain nojalla tehtävissä Traficomin tuotearvioinneissa arvioinnin ulkoistaminen kokonaan tai osittain edellyttäisi sääntelypohjan täydentämistä.

Kansallisen turvallisuusluokitellun tiedon käsittelyyn käytettävien tuotteiden arviointiin olisi periaatteessa mahdollista hakea pätevyyttä tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011, arviointilaitoslaki) nojalla. Tämä edellyttäisi muun muassa pätevyyden osoittamisessa sovellettavien kriteerien kehittämistä sekä tarvittavan osaamisen rakentamista tietoturvallisuuden arviointilaitoksille. Traficom tukee tarvittaessa arviointilaitosten tekemiä arviointeja salausratkaisujen ja muiden turvallisuuskriittisten tuotteiden osalta.

Traficom tekee virastolain perusteella arviointeja valmistajien pyynnöstä sopimusperusteisesti. Tässä yhteydessä Traficom on tehnyt pilottiluonteisen yksittäisen sopimuksen ulkoisen arviointitahon kanssa. Osapuolten niin sopiessa tapauskohtaisesti kyseinen arviointitaho voi tehdä tietyn turvallisuuskriittisen tuotetyypin testauksen ja tarkastuksen Traficomin ohjauksessa ja Traficom hyödyntää tarkastuksen tulosta omassa lausunnossaan. Menettely edellyttää, että valmistaja tekee sopimuksen kyseisen arviointitahon kanssa. Liikenne- ja viestintävirasto ei ole valmistajan ja arviointitahon välisen sopimuksen osapuoli eikä arviointitaho valmistajan ja Liikenne- ja viestintäviraston välisen sopimuksen osapuoli. Traficom katselmoi tuotteen arviointisuunnitelman. Arviointitaho noudattaa Traficomin määrittelemiä kriteerejä, antaa Traficomille kaikki arviointia koskevat tiedot ja noudattaa Traficomin ohjausta ja linjauksia kaikissa arviointiprosessin vaiheissa. Traficom arvioi, onko lausunnon antamiselle edellytykset ja antaa lausunnon.

1.3.3 Hajasäteily ja salausteknisen aineiston hallinta

Tässä ohjeessa ei käsitellä salaustuotteiden tai turvallisuuskriittisten tuotteiden suojauskyvyn arvioimista hajasäteilyn aiheuttamia uhkia vastaan (TEMPEST-suojaustoimet). Ne arvioidaan tarvittaessa omien säännöstensä ja ohjeiden mukaisesti.

Tässä ohjeessa ei käsitellä salauslaitteiden ja muun salausteknisen aineiston kuten salausavainten hallintaa (COMSEC-menettelyt).

1.4 Ohjeen voimaantulo ja lisätiedot

Tämä ohje tulee voimaan 7.2.2025. Ohje on voimassa toistaiseksi.

Tällä ohjeella yhdistetään ja päivitetään aikaisemmat ohjeet Liikenne- ja viestintävirasto Traficomin suorittamat salaustuotearvioinnit ja -hyväksynnät - Tilaajan näkökulma (1487/651/2017, 6.3.2020) ja Liikenne- ja viestintävirasto Traficomin suorittamat turvallisuuskriittisten tuotteiden arvioinnit ja -hyväksynnät - Tilaajan näkökulma (1487/651/2017, 4.1.2022)

Ohjetta täydennetään ja muutetaan tarvittaessa. Ohjeen muutetut versiot löytyvät listattuna versiohistoriasta sivulta 2.

Lisätietoja voi pyytää osoitteesta ncsa@traficom.fi.

2. Määritelmät

Tässä luvussa määritellään ohjeessa käytettävät termit. Määritelmien tarkoitus on helpottaa ohjeen lukemista. Määritelmissä on pyritty huomioimaan eri säädösten terminologia, mutta sääntelyn terminologia ei ole yhdenmukaista. Kansallisessa sääntelyssä ei käsitellä tuotteita nimenomaisesti ja EU:n ja Naton turvallisuussäännöjen yksityiskohdissa on eroja. Kutakin säädöstä tulkittaessa on aina tarkasteltava säädöksen määritelmiä.

Salaustuote tarkoittaa tuotetta tai ratkaisua, jonka ensisijainen ja pääasiallinen tarkoitus on suojata tiedon luottamuksellisuus, eheys, käytettävyys, aitous ja/tai kiistämättömyys yhden tai useamman salausmenetelmän avulla.

Turvallisuuskriittinen tuote tarkoittaa tuotetta, jolla on tietojärjestelmässä kriittinen rooli turvallisuusluokitellun tiedon suojaamisessa. Kriittinen rooli muodostuu tyypillisesti siitä, että tuote toimii turvallisuusluokitellun tiedon suojauksena ulkoisia toimijoita vastaan, jolloin tuotteen mahdollisia turvallisuuspuutteita ei tyypillisesti pystytä kompensoimaan muilla suojauksilla. Tyypillisiä esimerkkejä ovat eri turvallisuusluokkien ympäristöjen erotteluun käytettävät yhdyskäytäväratkaisut.

Kansainvälinen tietoturvallisuusvelvoite tarkoittaa, mitä siitä on säädetty laissa kansainvälisistä tietoturvallisuusvelvoitteista. Esimerkiksi EU:n ja Naton turvallisuusluokitellun tiedon suojaamiseen liittyy velvoitteita salaus- ja eräiden muiden tuotteiden hyväksynnästä ja sääntelyä tuotteiden ja niiden valmistuksen vaatimuksista.

Valmistaja tarkoittaa yritystä, joka kehittää, suunnittelee, valmistaa, kokoaa ja ylläpitää tuotteen.

Olennainen alihankkija tarkoittaa yritystä, jonka tarjoama tuotteen osaksi tuleva komponentti tai muu osa on olennainen tuotteen arvioitavien ominaisuuksien kannalta.

Asiakasviranomainen tarkoittaa viranomaista, jolla on tarve saada tuote osaksi tietojärjestelmäänsä ja joka siksi puoltaa tuotteen arviointia. Määritelmässä ei edellytetä hankintasopimuksen olemassaoloa.

Vaatimus tarkoittaa joko säädettyjä vaatimuksia tai arvioinnissa käytettäviä kriteereitä.

Kriteerit tarkoittavat ennalta vahvistettuja turvallisuusluokitellun tiedon suojaamisessa sovellettavia yleisesti käytössä olevia tai Traficomin viranomaistehtävissään

tarkentamia ja määrittelemiä sääntöjä, joihin tuotetta verrataan. Kansainvälisissä tietoturvallisuusvelvoitteissa kriteerit määräytyvät kulloinkin kansainvälisissä velvoitteissa säädettyjen vaatimusten mukaan. Kansallisen turvallisuusluokitellun tiedon suojaamisessa käytetään tiedonhallintalain ja turvallisuusluokitteluasetuksen yleisluonteisten vaatimusten puitteissa Traficomin määrittelemää yleistä teknistä hyvää käytäntöä, jossa on huomioitu kansainväliset käytännöt.

Tarkastus tarkoittaa tuotteen ja sen valmistuksen teknisten, toiminnallisten ja loogisten komponenttien kuten laitteen, algoritmien ja ohjelmistokoodin konkreettista havainnointia ja testaamista eri menetelmillä

Arviointi tarkoittaa tarkastamista ja valmistajaan ja tuotteeseen liittyvän dokumentaation, selvityksen ja tarkastushavaintojen analysointia ja vertaamista kriteereihin ja vaatimuksiin.

Varmuustaso tarkoittaa arvioinnissa käytettävien arviointimenetelmien yhdistelmän vaikutusta siihen, kuinka luotettava käsitys tuotteen turvallisuudesta voidaan muodostaa. Varmuustaso ei siten tarkoita tuotteen turvallisuuden luokittelua vaan sitä, missä määrin sitä on voitu arvioida. Varmuustasoluokittelulla ei ole sellaisenaan suoraa vastinetta muussa sääntelyssä, mutta termiä käytetään yleisesti alalla. Tässä ohjeessa luokittelun tarkoitus on lisätä viranomaisten ja valmistajien tietoa arvioinnin antamasta vaatimuksenmukaisuuden varmuudesta ja toimia työkaluna arvioinnin määrittelyssä.

Vaatimustenmukaisuus tarkoittaa tuotteen ominaisuuksien ja sen valmistuksen ja ylläpidon suojaamiseen liittyvien olosuhteiden vastaavuutta arvioinnissa käytettyjen kriteereiden kanssa. Salaustuotteiden ja turvallisuuskriittisten tuotteiden vaatimuksenmukaisuus määritellään aina jonkin turvallisuusluokan mukaisesti. Vaatimustenmukaisuus voidaan määritellä suhteessa kansallisiin turvallisuusluokkiin (TL I - TL IV) tai/ja kansainvälisiin luokkiin (esimerkiksi EU-R tai NR).

Lausunto tarkoittaa Traficomin kirjallista arviota siitä, täyttääkö tuote arvioinnissa sovelletun tietyn turvallisuusluokan mukaiset vaatimukset tiedon suojaamisessa.

Hyväksyntä tarkoittaa Traficomin kirjallista hallintopäätöstä siitä, että arvioitu tuote täyttää kansainväliseen tietoturvallisuusvelvoitteeseen perustuvat arvioinnissa sovelletut kyseisen tuotteen vaatimukset tietyn turvallisuusluokan tiedon suojaamisessa.

Käyttöpolitiikka tarkoittaa lausuntoon tai hyväksyntään liittyvää Traficomin selostetta niistä käyttötavoista, joita turvallisuusluokan mukainen suojaaminen edellyttää.

3. Säännökset

Seuraavissa luvuissa kuvataan säännökset, joiden perusteella Traficom tekee tuotearviointeja ja joihin tämä ohje perustuu.

3.1 Tuotearvioinnit kansallisen turvallisuusluokitellun tiedon suojaamisessa

3.1.1 Viranomaisten pyynnöt

Traficom tekee tuotteiden arviointeja osana viranomaisen tietojärjestelmän tai tietoliikennejärjestelyn tietoturvallisuuden arviointia viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011, arviointilaki) 4 §:n nojalla. Laki mahdollistaa vain viranomaisten pyynnöt, joten Traficom ei voi tämän lain perusteella tehdä arviointeja valmistajien pyynnöstä. Arviointiperusteista säädetään lain 7 §:ssä.

Arviointilaki *4 § Viestintäviraston tehtävät*

Viestintäviraston tehtävänä on viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden edistämiseksi ja varmistamiseksi:
1) arvioida viranomaisen pyynnöstä tämän määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tai tietoliikennejärjestelyjen tietoturvallisuuden vaatimuksenmukaisuutta;
[…]

Arviointilaki *7 § Tietoturvallisuuden arviointiperusteet*

Viestintävirasto voi käyttää viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointiperusteina:
1) lailla tai asetuksella säädettyjä viranomaisten toimintaa koskevia tietoturvallisuusvaatimuksia ja valtiovarainministeriön tietoturvallisuutta koskevia ohjeita;
2) kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun kansallisen turvallisuusviranomaisen antamia kansainvälisten tietoturvallisuusvelvoitteiden toteuttamista koskevia ohjeita;
3) Euroopan unionin tai muun kansainvälisen toimielimen antamia tietoturvallisuutta koskevia säännöksiä ja ohjeita;
4) julkaistuja ja yleisesti tai alueellisesti sovellettuja tietototurvallisuutta koskevia säännöksiä, määräyksiä tai ohjeita;
5) vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia.

Viestintävirasto selvittää, täyttääkö tietojärjestelmä tai tietoliikennejärjestely ne tietoturvallisuutta koskevat vaatimukset, jotka on otettu arviointiperusteeksi. Arviointi voidaan tehdä myös osittaisena.

Traficom tekee tuotteiden arviointia myös yritysturvallisuusselvityksen osana laatiessaan suojelupoliisin tai pääesikunnan pyynnöstä turvallisuusselvityslain 9 §:n 3 momentin mukaisen tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen.

Turvallisuusselvityslaki *9 § Toimivaltaiset viranomaiset*

[…]

Liikenne- ja viestintävirasto laatii yritysturvallisuusselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen.

[…]

3.1.2 Valmistajien pyynnöt

Traficom tekee tuotteiden arviointia myös valmistajien pyynnöstä. Tällöinkin taustalla on oltava jonkin viranomaisen tarve tuotteelle. Valmistajien arviointipyyntöjen käsittely edellyttää sopimusta valmistajan kanssa. Traficomin mahdollisuus sopimusten tekemiseen perustuu lakiin Liikenne- ja viestintävirastosta (935/2018, virastolaki). Laissa säädetty tietoturvallisuuden edistämistehtävä liittyy muun muassa valtioneuvoston asetukseen asiakirjojen turvallisuusluokittelusta. Arviointien maksuista säädetään erikseen.

Virastolaki *3 § Viraston kyberturvallisuuskeskuksen tehtävät*

Liikenne- ja viestintäviraston kyberturvallisuuskeskus, jäljempänä Kyberturvallisuuskeskus, tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä. Se ylläpitää kansallisen kyberturvallisuuden tilannekuvaa. Kyberturvallisuuskeskuksen toiminta edistää ja varmistaa tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuutta. Kyberturvallisuuskeskus toimii julkisesti säännellyn satelliittipalvelun vastuuviranomaisena ja Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2021/887 6 artiklan mukaisena kansallisena koordinointikeskuksena. Lisäksi Kyberturvallisuuskeskus huolehtii viestintätoimialan varautumisesta normaaliolojen häiriötilanteisiin ja poikkeusoloihin, edistää ja valvoo

sähköisen viestinnän toimintavarmuutta sekä tukee toimialallaan yhteiskunnan yleistä varautumista normaaliolojen häiriötilanteisiin ja poikkeusoloihin. (19.11.2021/1002)

[…]

Liikenne- ja viestintävirasto voi tuottaa Kyberturvallisuuskeskuksen 1 momentissa tarkoitettuihin tehtäviin perustuvia julkisoikeudellisia tai liiketaloudellisin perustein hinnoiteltavia suoritteita ja tehdä niiden tuottamista koskevia sopimuksia.

3.2 Kansainvälisten tietoturvallisuusvelvoitteiden tuotehyväksynnät

Kansainväliset tietoturvallisuusvelvoitteet koskevat toisesta valtiosta tai kansainväliseltä järjestöltä tai toimielimeltä saadun turvallisuusluokitellun tiedon suojaamista Suomessa. Tällaiseen *erityissuojattavaan tietoaineistoon* liittyvistä velvoitteista säädetään laissa kansainvälisistä tietoturvallisuusvelvoitteista (588/2004, kv-titulaki). Velvollisuudet koskevat kaikkia organisaatioita ja henkilöitä, jotka käsittelevät turvallisuusluokiteltua tietoa.

Kansainväliset tietoturvallisuusvelvoitteet perustuvat Suomea sitovaan kansainväliseen sopimukseen tai muuhun Suomea koskevaan velvoitteeseen. Suomen kansainväliset tietoturvallisuussopimukset (GSA, General Security Agreement) löytyvät ulkoministeriön kansallisen turvallisuusviranomaisen (NSA, National Security Authority) verkkosivulta[1]. EU:n ja Naton turvallisuusluokitellun tiedon suojaamista koskevat velvoitteet perustuvat EU:n neuvoston turvallisuussääntöön EU/488/2013[2] ja Naton turvallisuussäännöstöön C-M(2002)49-REV1[3].

Traficomin tuotearviointitehtävä perustuu kv-titulain 4 §:ssä säädettyyn tehtävään määrättynä turvallisuusviranomaisena tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa. EU:n ja Naton turvallisuussäännöissä ja kansainvälisissä tietoturvallisuussopimuksissa määritellään tarkemmin salaustuotteiden tai muiden turvallisuuskriittisten tuotteiden arviointi -ja hyväksyntävelvoitteista. Näissä tilanteissa arviointi ja hyväksyntä on siis pakollista toisin kuin kansallisen turvallisuusluokitellun tiedon suojaamisessa.

Kv-titulaki 4 *§ Turvallisuusviranomaiset ja niiden tehtävät*

Ulkoasiainministeriö toimii kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa Suomen kansallisena turvallisuusviranomaisena. Puolustusministeriö, pääesikunta, suojelupoliisi ja Viestintävirasto toimivat kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitettuina määrättyinä turvallisuusviranomaisina.

Kansallisen turvallisuusviranomaisen tehtävänä on erityisesti ohjata ja valvoa, että tässä laissa tarkoitetut erityissuojattavat tietoaineistot suojataan ja niitä käsitellään asianmukaisesti.

Määrätyt turvallisuusviranomaiset huolehtivat niille tässä laissa säädetyistä ja muista niille kansainvälisistä tietoturvallisuusvelvoitteista johtuvista tehtävistä. Puolustusministeriö, pääesikunta ja suojelupoliisi toimivat kansallisen turvallisuusviranomaisen asiantuntijoina henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa sekä Viestintävirasto tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa. (19.9.2014/731)

Traficomin kv-titulain 4 §:n mukaisiin kansainvälisistä tietoturvallisuusvelvoitteista johtuviin tehtäviin kuuluvat EU:n neuvoston turvallisuussäännön salauslaitteiden hyväksyntäviranomaisen tehtävä (CAA, Crypto Approval Authority)

[1] https://um.fi/voimassa-olevat-tietoturvallisuussopimukset
[2] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32013D0488
[3] Ks. Laki tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdystä sopimuksesta ja turvallisuussäännöistä (907/2023), SopS 55/2023, asetus SopS 56/2023. Asiakirja C-M(2002)49-REV1 ja käännös suomeksi löytyy HE 4/2023 vp https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_4+2023.pdf

EU/488/2013 *10 artikla Viestintä- ja tietojärjestelmissä käsiteltävien EU:n turvallisuusluokiteltujen tietojen suojaaminen*

6. Jos EU:n turvallisuusluokiteltujen tietojen suojaamiseen käytetään salaustuotteita, tällaiset tuotteet on hyväksyttävä seuraavasti:

a) SECRET UE/EU SECRET- tai sitä korkeamman turvallisuusluokan tietojen luottamuksellisuus on suojattava salaustuotteilla, jotka salauslaitteiden hyväksyntäviranomaisena toimiva neuvosto on hyväksynyt turvallisuuskomitean suosituksesta;

b) CONFIDENTIEL UE/EU CONFIDENTIAL- tai RESTREINT UE/EU RESTRICTED -turvallisuusluokan tietojen luottamuksellisuus on suojattava salaustuotteilla, jotka salauslaitteiden hyväksyntäviranomaisena toimiva neuvoston pääsihteeri, jäljempänä 'pääsihteeri', on hyväksynyt turvallisuuskomitean suosituksesta.

Sen estämättä, mitä b alakohdassa säädetään, EU:n CONFIDENTIEL UE/EU CONFIDENTIAL- tai RESTREINT UE/EU RESTRICTED -turvallisuusluokiteltujen tietojen luottamuksellisuus voidaan suojata jäsenvaltioiden kansallisissa järjestelmissä salaustuotteilla, jotka on hyväksynyt jäsenvaltion salauslaitteiden hyväksyntäviranomainen.

Liite IV *25. Jäsenvaltion salauslaitteiden hyväksyntäviranomaisen on arvioitava ja hyväksyttävä EU:n turvallisuusluokiteltujen tietojen suojaamisessa käytettävät salaustuotteet.*

Liite IV *46. Salauslaitteiden hyväksyntäviranomainen vastaa sen varmistamisesta, että salaustuotteet ovat kansallisten tai neuvoston salausperiaatteiden mukaisia. Se hyväksyy salaustuotteen, jolla EU:n turvallisuusluokitellut tiedot suojataan määrättyyn turvallisuusluokkaan asti tuotteen käyttöympäristössä. Jäsenvaltioiden osalta salauslaitteiden hyväksyntäviranomainen vastaa lisäksi salaustuotteiden arvioinnista.*

Vrt. Liite IV 48. Turvallisuusjärjestelyjen hyväksyntäviranomainen; Security Accreditation Authority: g) viestintä- ja tietojärjestelmän turvallisuuden varmistamiseen käytettyjen hyväksyttyjen salaus- ja TEMPEST-tuotteiden valinnan vahvistamisesta.

Traficomin kv-titulain 4 §:n mukaisiin kansainvälisistä tietoturvallisuusvelvoitteista johtuviin tehtäviin kuuluvat Naton turvallisuussäännöstön viestintä- ja tietojärjestelmien turvallisuusviranomaisen tehtävä (NCSA, National CIS Security Authority, CIS eli Communications and Information Systems)

C-M(2002)49-REV1 Liite F *11. SALAUKSEEN PERUSTUVA TURVALLISUUS*
11.1. Kun luottamuksellisuuden ja muun kuin luottamuksellisuuden suojaamiseksi tarvitaan salaustuotteita tai -menetelmiä tiedon siirtämisen, käsittelyn tai säilyttämisen (data at rest) aikana, nämä tuotteet tai menetelmät on erikseen hyväksytettävä tätä tarkoitusta varten ja fyysisten, menettelyllisten ja teknisten toimenpiteiden on täytettävä erityiset salausta koskevat vaatimukset, jotta vaadittavat turvallisuustavoitteet saavutetaan.

11.3. Turvallisuusluokkaan NATO SECRET ja sitä ylempiin luokkiin luokitellun tiedon luottamuksellisuus on tietoa siirrettäessä suojattava Naton sotilaskomitean (NAVMILCOM) hyväksymillä salaustuotteilla tai -menetelmillä.

11.4. Turvallisuusluokkaan NATO CONFIDENTIAL tai NATO RESTRICTED luokitellun tiedon luottamuksellisuus on tietoa siirrettäessä suojattava joko Naton sotilaskomitean tai Naton jäsenvaltion hyväksymillä salaustuotteilla tai -menetelmillä.

13.4. Kansallinen viestintä- ja tietojärjestelmien turvallisuusviranomainen

13.4.1. Kukin Naton jäsenvaltio ja tapauksen mukaan Naton ulkopuolinen valtio määrää kansallisen viestintä- ja tietojärjestelmien turvallisuusviranomaisen, joka voidaan perustaa virastoksi kansalliseen turvallisuusinfrastruktuuriin. Kansallisen viestintä- ja tietojärjestelmien turvallisuusviranomaisen vastuulla on
(a) valvoa teknistä salaustietoa, joka liittyy Naton tiedon suojaamiseen kyseisessä valtiossa;
(b) varmistaa, että Naton tiedon suojaamiseen käytettävät salausjärjestelmät, tuotteet ja menetelmät valitaan asianmukaisesti ja niitä käytetään ja ylläpidetään asianmukaisesti;

(c) varmistaa, että Naton tiedon suojaamiseen käytettävät viestintä- ja tietojärjestelmien turvallisuustuotteet valitaan asianmukaisesti ja niitä käytetään ja ylläpidetään asianmukaisesti kyseisessä valtiossa;
[…]

Tarkentavassa sääntelyssä (AC/35-D/2005-REV3) otetaan kantaa myös muiden turvallisuuskriittisten tuotteiden (SEP, Security Enforcing Products) arviointi- ja hyväksyntämenettelyyn.

9.3.5 The approval of a security enforcing product is a formal statement, by a National CIS Security Authority (NCSA), supported by an independent review of the conduct and results of an evaluation and/or a certification, approving the use of a product for a specific purpose and under specific conditions. The approval of a security enforcing product for a CIS is a two-step process: while the approval by an NCSA is required to declare the product suitable for the protection of NATO information, the approval by an SAA is related to its use in the context of a specific CIS, as part of the security accreditation process.

4. Arviointiin liittyvien tietojen julkisuus

4.1 Asiakirjojen julkisuus ja salassapito

Traficom arvioi ja ratkaisee aina tapauskohtaisesti, ovatko viraston arviointitehtävässä saadut aineistot ja tiedot sekä viraston arvioinnin perusteella laatimat asiakirjat julkisia vai kokonaan tai osittain salassa pidettäviä tai myös turvallisuusluokiteltuja.

4.1.1 Traficomin saamat aineistot

Traficomille arvioinnin yhteydessä toimitetut aineistot ja tiedot ovat viranomaisen asiakirjoja, joita Traficom käsittelee viranomaisen toiminnan julkisuudesta annetun lain (621/1999, julkisuuslaki), tiedonhallintalain ja turvallisuusluokitteluasetuksen mukaisesti.

Traficom arvioi aina tietojen julkisuuden tai salassapito- tai turvallisuusluokitteluperusteet viran puolesta ja kuulee tarvittaessa valmistajaa tai asiakasviranomaista. Julkisuuslain 24 §:ssä säädetään viranomaisen tietojen salassapidon perusteista. Säännöksen perusteella elinkeinonharjoittajan liikesalaisuudet ovat salassa pidettäviä. Salassa pidettäviä voivat olla myös esimerkiksi tieto- ja viestintäjärjestelmien turvajärjestelyjä tai maanpuolustusta koskevat tiedot.

Traficomin tuotearvioinnit liittyvät aina turvallisuusluokitellun tiedon suojaamistarpeisiin. Valmistajan tuotteisiin liittyvät yksityiskohtaiset aineistot voivat sisältää sekä liikesalaisuutena suojattavia tietoja että tieto- ja viestintäjärjestelmien turvajärjestelyihin vaikuttavia tietoja. Esimerkiksi tuotteen lähdekoodi on tyypillisesti tietoa, jota tulee julkisuuslain valossa suojata sekä liikesalaisuutena että tieto- ja viestintäjärjestelmien turvajärjestelyihin vaikuttavana tietona. Liikesalaisuuselementin vuoksi Traficom voisi julkisuuslain mukaan luovuttaa tietoa esimerkiksi asiakasviranomaiselle vain valmistajan suostumuksella ja turvajärjestelyihin liittyvän elementin vuoksi tieto tulee turvallisuusluokitella ja suojata tietojärjestelmissä käsittelyssä turvallisuusluokan edellyttämällä tavalla.

4.1.2 Traficomin laatimat asiakirjat

Traficomin arvioinnin aikana laatimien asiakirjojen ja arvioinnin lopputuloksena antamien asiakirjojen julkisuus tai salassapito kokonaan tai osittain arvioidaan julkisuuslain mukaisesti asiakirjan sisältämien tietojen perusteella. Traficomin arvioinnin lopputuloksen julkisuudessa täytyy erottaa tieto arvioinnin lopputuloksesta ja asiaan liittyvät eri asiakirjat, joita voivat olla muun muassa itse lausunto tai päätös ja lausuntoon tai päätökseen liittyvä käyttöpolitiikka, arviointiraportti tai kryptologinen lausunto.

Tieto Traficomin arvioinnin lopputuloksesta voi olla julkinen tai salassa pidettävä. Tähän vaikuttaa muun muassa arvioinnin varmuustaso.

- Varmuustasoltaan korkean (A) arvioinnin lopputulos voi olla lähtökohtaisesti julkinen. Tällöin Traficom julkaisee verkkosivuillaan tiedon siitä, että tuotteelle on annettu lausunto tai hyväksyntä, ellei perustellusta viranomaisen toimintaan liittyvästä syystä toisin sovita. Koko asiakirjaa ei julkaista verkkosivuilla, mutta siltä osin, kun se on julkinen, kenellä tahansa on julkisuuslain mukaisesti oikeus saada se pyynnöstä.

- Varmuustasoltaan keskitason (B) tai matalan (C) arvioinnin lopputulos on oletusarvoisesti salassa pidettävä ja se annetaan arviointia pyytäneelle viranomaiselle ja tiedoksi tuotteen valmistajalle.

- Traficomin lausunnon tai hyväksynnän yhteydessä laatima käyttöpolitiikka tai vaatimuksiin liittyvä ohjeistus voi tyypillisesti olla salassa pidettävä tai turvallisuusluokiteltu. Sama koskee arviointiraporttia ja kryptologista lausuntoa, sillä ne sisältävät poikkeuksetta turvajärjestelyihin vaikuttavia yksityiskohtia.

Kuten edellä oli todettu, Traficom voi tehdä tuotteen arvioinnin valmistajan pyynnöstä, jos valmistajan ja Traficomin välillä on ollut edellytykset tehdä sopimus tuotearvioinnista. Tällöin sopimusmallin yleiset ehdot ovat lähtökohtaisesti julkisia. Yrityksen nimi ja arvioitavana olevat tuotteet sen sijaan voivat olla salassa pidettävää tietoa ennen arvioinnin valmistumista. Sopimus ja tuotteen arviointi voivat olla salassa pidettävää tietoa myös arvioinnin jälkeen, mikäli salassapidolle on edellä kuvatut perusteet. Sopimusperusteisesti tehdään kuitenkin pääsääntöisesti vain varmuustasoltaan laajoja arviointeja, jolloin yleensä on edellytykset lopputuloksen julkisuudelle.

4.2 Salassa pidettävien ja turvallisuusluokiteltujen asiakirjojen luovuttaminen

Traficom voi tarvittaessa julkisuuslain mukaisesti luovuttaa tuotteen arviointiin liittyvää tietoa tuotteen hankinnasta kiinnostuneelle viranomaiselle tai muulle tietylle kolmannelle osapuolelle. Liikesalaisuuksia sisältävien tietojen luovuttaminen edellyttää julkisuuslain mukaan valmistajan suostumusta. Eräillä muilla julkisuuslain 24 §:ssä säädetyillä perusteilla salassa pidettävien tietojen luovuttamisen Traficom voi ilman valmistajan suostumusta arvioida tapauskohtaisesti kullekin salassapitoperusteelle pykälässä säädetyn vahinkoedellytyslausekkeen mukaisesti. Harkinnassa Traficom arvioi, voiko tiedon luovutus aiheuttaa haittaa suojattavalle intressille. Salassa pidettävän tiedon saajaa koskevat julkisuuslain salassapito- ja vaitiolovelvollisuudet.

Traficom voi luovuttaa arvioinnin yhteydessä salaus- ja turvallisuuskriittisten tuotteiden valmistajalle salassa pidettäviä ja turvallisuusluokiteltuja asiakirjoja.

Kun asiakirjat ovat turvallisuusluokiteltuja ja Traficom luovuttaa asiakirjoja eteenpäin, Traficomin on huolehdittava, että luovutettavia turvallisuusluokiteltuja asiakirjoja ja tietoja käsitellään vaatimusten mukaisesti.

Turvallisuusluokitteluasetus *6 § Turvallisuusluokitellun asiakirjan antamisen edellytykset*

Valtionhallinnon viranomaisen on ennakolta varmistuttava siitä, että turvallisuusluokitellun asiakirjan suojaamisesta huolehditaan asianmukaisesti, jos se antaa turvallisuusluokitellun asiakirjan muulle kuin valtionhallinnon viranomaiselle. Vaatimus ei koske asianosaisen tiedonsaantioikeuteen perustuvaa tiedon antamista asiakirjan sisällöstä.
[…]

Valmistajan on sitouduttava pitämään salassa Traficomilta saamansa asiakirjan tai tieto, jonka virasto on merkinnyt tai ilmoittanut salassa pidettäväksi tai joka on

turvallisuusluokiteltu. Valmistaja voi luovuttaa tuotteeseen liittyvät salassa pidettävät asiakirjat viranomaiselle, joka tarvitsee niitä tuotteen mahdollista hankintaa tai käyttöä varten. Valmistajan on ennalta informoitava asiakirjan salassa pidosta ja mahdollisesta turvallisuusluokituksesta, jotta viranomainen voi harkita käsittelytavan. Asiakirjojen ja tietojen luovuttaminen toiselle yritykselle tulee selvittää tapauskohtaisesti Traficomin kanssa.

Jos valmistajalle on perusteltu tarve (need-to-know) luovuttaa kansainvälisen tietoturvallisuusvelvoitteen perusteella erityissuojattavia eli turvallisuusluokiteltuja asiakirjoja, Traficom sitouttaa valmistajan käsittelemään ja suojaamaan tietoja niitä koskevien vaatimusten mukaisesti ja käyttämään tietoja ainoastaan arviointia ja siihen liittyvää tuotekehitystä varten. Käytännössä ennen tietojen luovuttamista Traficom laatii yrityksen allekirjoitettavaksi sitoumuksen, jossa yksilöidään turvallisuusluokan perusteella määräytyvät vaatimukset ja perehdyttää yrityksen tiedon suojaamisen vaatimuksiin. Sitoumuksessa vaaditaan valmistajaa suojaamaan ja käsittelemään luovutettua tietoa kansallisten säännösten sekä kansallisen turvallisuusviranomaisen *Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje -ohjeen*[4] ajantasaisen version mukaisesti. Tarvittaessa valmistajalta edellytetään luovutettavien tietojen mukaista kansainvälistä yritysturvallisuusselvitystä (FSC, Facility Security Clearance).

Kv-titulaki *6 § Salassapitovelvollisuus ja tietojen käyttö*

Erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. (22.10.2010/885)

Erityissuojattavaa tietoaineistoa saa käyttää ja luovuttaa vain siihen tarkoitukseen, jota varten se on annettu, jollei se, joka on määritellyt aineiston turvallisuusluokan, ole antanut muuhun suostumustaan.

Erityissuojattavaa tietoaineistoa käsittelevän viranomaisen on pidettävä huolta siitä, että tietoaineistoon on pääsy vain niillä, jotka tarvitsevat tietoja tehtävänsä hoitamisessa. Nämä henkilöt on nimettävä etukäteen kansainvälisessä tietoturvallisuusvelvoitteessa edellytetyissä tapauksissa. Sama koskee myös 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajaa.

5. Arvioinnin yleiset edellytykset

5.1 Tuotteen edellytykset

Tuotteen arvioitavaksi ottamisen edellytyksenä on tuotteen tekninen rajattavuus ja soveltuvuus tiedon salaamiseen tai muuhun suojaamiseen tieto- tai tietoliikennejärjestelmissä. Tuotetyypin arviointikelpoisuuden tulkinnassa nojaudutaan kansainvälisten tietoturvallisuusvelvoitteiden mukaisiin periaatteisiin ja soveltamiskäytäntöön.

Salaustuotteiden ja muiden turvallisuuskriittisten tuotteiden valmistuksen on täytettävä soveltuvin osin seuraavat edellytykset, joita tulkitaan suhteessa arvioitavaan turvallisuusluokkaan:

Traficomin täytyy saada tiedot salaustuotteen tuotekehityksestä ja Traficomilla täytyy olla mahdollisuus ottaa kantaa ja vaikuttaa tuotekehitykseen. Traficom pyrkii tarkastelemaan tuotekehitystä myös muissa kuin salaustuotteissa ja tuottamaan siitä tarvittaessa tietoa osana lausuntoa tai päätöstä.

- Traficomilla tulee olla pääsy tuotteen kaikkeen olennaiseen lähdekoodiin Traficomin tiloissa tai erikseen sovittaessa muussa kohtuullisesti järjesteltävissä olevassa turvallisuusvaatimukset täyttävässä tilassa.

[4] Turvallisuusluokitellun tiedon käsittelyohje - Ulkoministeriö

- Vaatimukset koskevat teknistä kokonaisuutta mukaan lukien laitealusta ja Traficomin täytyy saada tekninen kokonaisuus tarkastettavaksi sekä riittävät tiedot alustasta.
- Tuotteen kehitystyön, immateriaalioikeuksien ja tuotteen ylläpidon tulee olla koko elinkaaren ajan valmistajan tai luotetun alihankkijan oikeudellisessa, taloudellisessa ja tosiasiallisessa hallinnassa.
- Yleisesti saatavilla olevia avoimen lähdekoodin komponentteja ja muita yleisesti saatavilla olevia yleiskäyttöisiä komponentteja voi käyttää, vaikka ne eivät olisikaan valmistajan tai luotetun alihankkijan omaa tuotantoa.

5.2 Valmistajan edellytykset ja asiakasviranomaisen vaatimus eri varmuustasoilla

5.2.1 Yhteenveto

Tässä luvussa kuvataan kaikkia arviointeja koskevat edellytykset, joiden on täytyttävä tuotearvioinnin aloittamiseksi.

Valmistuksen sekä toimitusketjun alkuperämaihin liittyy vaatimuksia, jotka riippuvat tuotteen käyttötarkoituksesta sekä suojattavan tiedon turvallisuusluokasta ja alkuperäisestä luovuttajasta (*originator,* esimerkiksi EU tai Nato).

Valmistuksen alkuperään liittyviä riskejä arvioidaan aina. Vaatimukset riskien hallitsemiseksi riippuvat turvallisuusluokasta sekä tiedon alkuperäisestä luovuttajasta. Hallintakeinojen toteuman arvioinnin syvällisyys riippuu puolestaan arvioinnin varmuustasosta. Korkean varmuustason arvioinneissa Traficom selvittää sen tarvittavassa laajuudessa. Matalampien varmuustasojen arvioinneissa valmistuksen alkuperämaan selvittäminen ja merkityksen arviointi voi jäädä tapauskohtaisesti asiakasviranomaisen vastuulle.

Traficomin arviointi edellyttää aina myös tietoa jonkin asiakasviranomaisen tarpeesta tuotteelle turvallisuusluokitellun tiedon suojaamisessa ja puollosta arvioinnin tekemiselle.

Myös valmistusympäristön turvallisuuteen kohdistuvat vaatimukset riippuvat turvallisuusluokasta, ja niiden täyttymisen arvioinnin luotettavuus arvioinnin varmuustasosta.

5.2.2 Valmistajan edellytykset

Tässä luvussa käsitellään korkean varmuustason arviointien edellytyksiä. Tällaista voidaan edellyttää esimerkiksi tilanteessa, jossa tavoitteena saada salaustuote julkiselle EU:n tai Naton turvallisuusluokitellun tiedon suojaamiseen hyväksyttyjen tuotteiden listalle.

Kansallisen turvallisuusluokitellun tiedon salausratkaisujen tai muiden turvallisuuskriittisten tuotteiden arvioinnista tai valmistajien tai valmistuksen vaatimuksista ei ole säädetty nimenomaisesti. Turvallisuusluokitteluasetuksen mukaan ratkaisujen on oltava *riittävän* luotettavia. Traficomin soveltamiskäytännön periaatteena on antaa julkisia lausuntoja vain tuotteista, joiden valmistuksesta ja elinkaaren hallinnasta Traficom pystyy itse riittävästi varmistumaan.

Tuotteen arvioinnin edellytyksenä on, että Traficom voi selvittää tuotteen valmistukseen liittyvät riskit muiden valtioiden vaikutuksesta (FOCI, Foreign Ownership and Control Influence). Selvityksen laajuuteen vaikuttaa tuotteen arvioinnin laajuus ja suojattavan tiedon turvallisuusluokka. Lisäksi selvitykseen vaikuttaa, onko

kyseessä tuotteen arviointi kansallisen turvallisuusluokitellun tiedon suojaamisen vai kansainvälisen tietoturvallisuusvelvoitteen takia.

Kansallisen turvallisuusluokitellun tiedon suojaamisen korkean varmuustason arvioinnin edellytyksenä on, että tuotteen valmistajana on suomalainen yritys, joka harjoittaa toimintaa Suomessa. Edellytyksenä on, että tuotteen valmistus ja tuotekehitys tapahtuu olennaisilta osin Suomessa. Asiaan voivat vaikuttaa tuotteen valmistajan omistuspohja ja päätösvalta ja olennaisten tuotekohtaisten turvallisuuskomponenttien toimittajien (olennaiset alihankkijat) alkuperä.

Valmistajaan ja olennaisiin alihankkijoihin liittyvät seikat voi tarvittaessa osoittaa esimerkiksi yritysturvallisuusselvitystodistuksella tai jos sellaista ei ole käytettävissä, muulla luotettavalla selvityksellä, jonka Traficom voi arvionsa mukaan hyväksyä. Kun Traficom solmii yrityksen kanssa sopimuksen tuotteen arvioinnista, selvitys arvioidaan ennen sopimuksen tekemistä ja liitetään sopimukseen. Valmistaja sitoutuu ilmoittamaan Traficomille viivytyksettä selvityksen sisältöön tulevista muutoksista.

Traficom arvioi saamansa selvityksen riittävyyden tapauskohtaisesti ottaen huomioon Suomen tavanomaiset luottamusviitekehykset esimerkiksi Pohjoismaiden, EU:n tai Naton jäsenvaltioiden kanssa. Selvitys arvioidaan suhteessa turvallisuusluokkaan.

Viranomainen voi pyytää tapauskohtaista arviota tai hyväksyntää myös alkuperältään ulkomaisesta tuotteesta. Kansallisen turvallisuusluokitellun tiedon suojaamisessa Traficomin ja asiakasviranomaisen täytyy sopia, miten ulkomaisen vaikutuksen riski arvioidaan. Riskipäätös kuuluu asiakasviranomaisen vastuulle. Kansainvälisten tietoturvallisuusvelvoitteiden täyttämisen arvioinnissa Traficom arvioi asian ja toteaa sen hyväksyntäpäätöksessä tai osana tietojärjestelmän hyväksyntää koskevaa hyväksyntälausuntoa. Traficom voi myös selvittää, miten mahdollinen toisessa valtiossa annettu EU:n tai Naton turvallisuussääntöjen puitteissa olemassa oleva hyväksyntä sekä saatavissa olevat tiedot tuotteesta huomioidaan.

Kansainväliseen tietoturvallisuusvelvoitteeseen liittyvän arvioinnin edellytyksenä on, että riskit muiden valtioiden vaikutuksesta on arvioitava EU:n tai Naton turvallisuussääntöjen mukaisesti. Valmistajan ja asiakasviranomaisen on tiedostettava, että jos syntyy tarve saada Traficomilta kansainväliseen tietoturvallisuusvelvoitteeseen liittyvä hyväksyntä tuotteen käytölle EU:n tai Naton turvallisuusluokitellun tiedon suojaamisessa, valmistuksen riippuvuudella eri valtioista tai Traficomin kontrollimahdollisuuksilla voi olla vaikutusta hyväksyntäedellytyksiin.

5.2.3 Viranomaistarve tuotteen arvioinnille

Arviointilain ja virastolain mukaan Traficomin tehtävä on tehdä arviointeja viranomaisen pyynnöstä ja edistää tietojärjestelmien ja tietoliikennejärjestelyjen turvallisuutta.

Arvioitavaksi ottaminen edellyttää siten sitä, että tuotteen arvioinnille on olemassa viranomaisen tarve. Jos arvioinnin hakija/pyytäjä on viranomainen, tarve tulee selvitetyksi pyynnössä/hakemuksessa. Jos arvioinnin pyytäjä on valmistaja, Traficomille täytyy toimittaa kirjallinen selvitys yhden tai useamman viranomaisen tarpeesta tuotteelle tietojärjestelmiinsä liittyvissä hankinnoissa. Tarkoitus on selvittää, että tuotteella on mahdollisuuksia vastata viranomaisten tiedossa oleviin tarpeisiin, mutta varsinaista hankintasopimusta ei edellytetä.

Viranomaisen tarpeen varmistamisella voi olla yhteys myös Traficomin arvioinnista perimiin maksuihin. Arvioinnin suunnittelussa on tärkeää määritellä selkeästi ennalta, vastaako maksuista valmistaja vai viranomainen.

5.2.4 Valmistusympäristön arviointi

Tuotteiden valmistusympäristö ja alihankittujen komponenttien valmistus vaikuttavat tuotteen luotettavuuteen. Valmistusympäristön asianmukaisuudesta voidaan varmistua eri menettelyillä, esimerkiksi seuraavilla:

- Valmistajan itsearviointi, jolloin Traficom edellyttää yleensä käytettäväksi Katakri-kriteeristöä,
- asiakasviranomaisen ja valmistajan turvallisuussopimus
- Traficomin katselmointi tai tarkastus
- toimintaympäristön kattava yritysturvallisuusselvitystodistus.

Traficom määrittelee tarkoituksenmukaiset menettelyt tapauskohtaisesti.

5.2.5 Yleisiä neuvoja viranomaiselle

Viranomaisen tietojärjestelmiin ja tietoliikennejärjestelyihin tarvittavien salaustuotteiden tai muiden turvallisuuskriittisten tuotteiden valinnassa tulevat pohdittavaksi ainakin seuraavat seikat

- Suojataanko tuotteella kansallista turvallisuusluokiteltua tietoa vai jonkin kansainvälisen tietoturvallisuusvelvoitteen mukaista tietoa.
- Soveltuuko tarpeeseen jokin tuote, jonka Traficom on jo aikaisemmin arvioinut ja josta löytyy tieto Traficomin verkkosivun luettelosta.[5] Tällöin on tarpeen selvittää arvioinnin tarkka sisältö, mahdolliset rajaukset sekä käyttöpolitiikan sisältö.
- On hyvä muistaa, että riskienarviointi ja päätös tuotteen käyttöönotosta on tiedonhallintayksikön eli viranomaisen vastuulla, ja että Traficomin mahdollinen lausunto on tarkoitettu tiedonhallintayksikön oman riskienarvioinnin ja mahdollisen käyttöönottopäätöksen tueksi.
- EU:n ja Naton turvallisuusluokitellun tiedon sähköisessä käsittelyssä tiedon suojaaminen salausratkaisulla edellyttää Traficomin hyväksyntää (*approval*) eli hyväksyntäpäätöstä tuotteelle tai hyväksyntää järjestelmäkohtaisesti osana tietojärjestelmäakkreditointia (*accreditation*). Tällöinkin varsinaisen päätöksen tuotteen käytöstä tietojärjestelmässä tekee järjestelmän vastuuviranomainen.
- Valtioiden kahdenvälisessä tietoturvallisuussopimuksiin perustuvassa sähköisen tiedonsiiron suojaustarpeessa voi tulla kysymykseen jommankumman osapuolen hyväksymä tuote tai hankkeen perusteella yhteisesti sovittava EU:n tai Naton puitteissa hyväksytty tuote.
- Soveltuuko tarpeeseen jokin tuote, joka löytyy EU:n tai Naton julkiselta tuotelistalta.[6] Tällöin on tarpeen selvittää hyväksynnän kohteen sisältö ja mahdollinen rajaus sekä se, onko hyväksynnästä saatavissa tarkempaa tietoa. Traficom tukee mahdollisuuksiensa mukaan toisten maiden tekemien hyväksyntäpäätösten ja käyttöpolitiikoiden (SecOps) saamisessa Suomen

[5] https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat-salausratkaisut
https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat

[6] EU:n LAPC: Yleistä: https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/ ja List of Approved Cryptographic Products https://www.consilium.europa.eu/media/x0ebv5jn/st09931en24.pdf
Naton NIAPC, Nato Indformation Assurance Product Catalogue: https://www.ia.nato.int/NIAPC

viranomaisen käyttöön. On hyvä huomata, että EU:n ja Naton turvallisuusluokiteltuja tietoja tulee suojata toiselta organisaatiolta kuten muiltakin ulkopuolisilta tahoilta ja kolmansilta osapuolilta, mikä vaikuttaa erityisesti salausratkaisuihin.

6. Arviointivaatimukset ja kriteerit

6.1 Kansalliset vaatimukset viranomaisille: tiedonhallintalaki ja turvallisuusluokitteluasetus

Viranomaisten tarpeet tuotteiden arviointiin perustuvat viranomaisten velvollisuuksiin turvallisuusluokitellun tiedon sähköisen käsittelyn suojaamisessa. Velvoitteista säädetään julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019, tiedonhallintalaki) 13 §:ssä ja 14 §:ssä sekä valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019, turvallisuusluokitteluasetus). Näissä säädöksissä asetetaan vaatimuksia tiedon suojaamiselle ja tiedon sähköisessä suojaamisessa käytettäville salaustuotteille. Arviointivelvollisuutta ei säädetä.

Tiedonhallintalaki *13 § Tietoaineistojen ja tietojärjestelmien tietoturvallisuus*

Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.

Viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti.

Viranomaisen on suunniteltava tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa.

Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään erikseen.

Tiedonhallintalaki *14 § Tietojen siirtäminen tietoverkossa*

Viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja.

[…]

Tiedonhallintalaki *15 § Tietoaineistojen turvallisuuden varmistaminen*

…

Turvallisuusluokitteluasetus *11 § Tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vaatimukset*

Turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyt tietojärjestelmät ja tietoliikennejärjestelyt on toteutettava siten, että:

1) ne erotetaan niissä käsiteltyjen asiakirjojen turvallisuusluokka huomioon ottaen riittävän luotettavasti alemman turvallisuustason tietojärjestelmistä ja tietoliikennejärjestelyistä;

[…]

7) käytetyt salausratkaisut ovat tietojärjestelmässä tai tietoliikennejärjestelyssä käsiteltyjen asiakirjojen turvallisuusluokka huomioon ottaen riittävän turvallisia.

[…]

Turvallisuusluokitteluasetus *12 § Asiakirjan siirtäminen tietoverkon kautta*

Salassa pidettävien tietojen siirtämisestä yleisessä tietoverkossa säädetään tiedonhallintalain 14 §:ssä.

Turvallisuusluokiteltuja asiakirjoja saa siirtää muussa kuin yleisessä tietoverkossa viranomaisen turvallisuusalueiden ulkopuolelle tai kyseistä turvallisuusluokkaa alemman turvallisuustason tietojärjestelmän tai tietoliikennejärjestelyn kautta vain salatussa muodossa. Jos turvallisuusluokiteltujen asiakirjojen siirtäminen tapahtuu turvallisuusalueella muussa kuin yleisessä tietoverkossa ja tietojen riittävä suojaus voidaan toteuttaa fyysisen suojaamisen menetelmin, voidaan käyttää salaamatonta siirtoa tai alemman turvallisuustason salausta.

Turvallisuusluokitteluasetus *13 § Asiakirjan kuljettaminen*

Turvallisuusluokiteltuja asiakirjoja saa kuljettaa turvallisuusalueiden ulkopuolelle suojaamalla sähköiset tietovälineet riittävällä salauksella.

[…]

Turvallisuusluokitteluasetus *15 § Asiakirjan tuhoaminen*

Tarpeettomaksi käynyt turvallisuusluokiteltu asiakirja on tuhottava tavalla, jolla kyseiselle turvallisuusluokalle riittävän luotettavasti estetään tietojen palauttaminen sekä kokoaminen uudelleen kokonaan tai osittain.

[…]

6.2 Kriteerit kansallisen turvallisuusluokitellun tiedon suojaamisessa

Tässä luvussa kuvataan, miten Traficom määrittelee tuotteen arvioinnissa käyttämänsä kriteerit.

Traficom on julkaissut osan arvioinnissa sovellettavista kriteereistä. Lisäksi Traficom soveltaa laatimiaan salassa pidettäviä tai turvallisuusluokiteltavia kriteereitä. Kriteerit liittyvät turvallisuusluokkiin, käsittely- tai säilytysympäristön tyypillisiin riskeihin ja niissä seurataan olennaisia yleisesti hyväksi havaittuja kansainvälisiä kriteerejä. Periaatteena arvioinnissa on, että mitä vakavampia riskejä on nähtävissä, sitä tiukemmat turvallisuusmekanismit ovat tarpeen. Alla on listattu keskeisimmät julkiset arvioinnissa sovellettavat kriteerit:

Kryptografiset ohjeet

- *Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat* (Ohje 190/651/2015, 9.12.2024)[7]
- *Hyväksytyt TLS-cipher suitet turvallisuusluokille IV-III* (kalvomuodossa laadittu muistio 13.10.2022)[8]

Salauslaitteiden ja turvallisuuskriittisten tuotteiden arvioinnissa sovelletaan teknisesti soveltuvin osin Katakria

- *Katakri – tietoturvallisuuden auditointityökalu viranomaisille* (kansallisen turvallisuusviranomaisen ohje)[9]

[7] Kryptografiset_vahvuusvaatimukset_-_kansalliset_turvallisuusluokat_1.pdf
[8] TLS cipher suitet suojaustasoille IV-III
[9] https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

Tietyistä turvallisuuskriittisten tuotteiden tyypeistä Traficom on julkaissut ohjeet, joita sovelletaan myös Traficomin tekemissä arvioinneissa

- *Tallennusvälineiden tyhjennys ja uusiokäyttö* (28.6.2024)[10]
- *Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista* (2.12.2021)[11]

Useisiin tuotteisiin ja niiden arviointeihin sovellettava ohje turvallisesta tuotekehityksestä ja turvallisuuskriittisten tuotteiden arvioinneista

- Turvallinen tuotekehitys: Kohti hyväksyntää (Ohje 2018)[12]

Kansallisen turvallisuusluokitellun tiedon suojaamiseksi tehtävän arvioinnin kriteerit on pyritty määrittelemään mahdollisimman yhdenmukaisesti kansainvälisten käytäntöjen kanssa.

Tavoitteena on, että kansallisen turvallisuusluokitellun tiedon suojaamiseksi tehdyn tuotekohtaisen arvioinnin tuloksia on mahdollista hyödyntää ja käyttää pohjana, mikäli asiakasviranomainen tai valmistaja hakee samalle tuotteelle hyväksyntää myös EU:n tai Naton turvallisuusluokitellun tiedon suojaamiseen. Käytännössä kansallisen turvallisuusluokitellun tiedon suojaamisen ja kansainvälisen tietoturvallisuusvelvoitteen arviointi voidaan toteuttaa myös rinnakkain.

6.3 Kansainväliset tietoturvallisuusvaatimukset

6.3.1 Kahdenväliset tietoturvallisuussopimukset

Valtioiden kahdenvälisissä tietoturvallisuussopimuksissa pääsääntö on vastavuoroisuusperiaate, jolloin toisesta valtiosta saatua turvallisuusluokiteltua tietoa suojataan kuten kansallista vastaavan turvallisuusluokan tietoa. Valtioiden välisessä tiedonsiirrossa käytettävistä salausratkaisuista sopivat keskenään jäsenvaltioiden asianomaiset viranomaiset, Suomessa Traficom. Salausratkaisuihin voi liittyä sopimus- tai hankekohtaisia vaatimuksia.

Esimerkki sopimusmääräyksistä

Sopimus Suomen tasavallan ja Belgian kuningaskunnan välillä turvallisuusluokitelluntiedon vastavuoroisesta suojaamisesta (SopS 8 ja 9/2022)[13]

5 artikla Turvallisuusluokitellun tiedon suojaaminen
1. Osapuolet toteuttavat kaikki asianmukaiset kansallisten säädöstensä ja määräystensä mukaiset toimet suojatakseen tässä sopimuksessa tarkoitetun turvallisuusluokitellun tiedon. Osapuolet antavat tälle tiedolle samantasoisen suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolleen.
[…]

7 artikla Turvallisuusluokitellun tiedon välittäminen
[…]
2. Luovuttava osapuoli ja vastaanottava osapuoli välittävät turvallisuusluokiteltua tietoa toisilleen sähköisesti ainoastaan toimivaltaisten turvallisuusviranomaisten keskenään sopimilla turvallisilla keinoilla.

[10] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tallennusv%C3%A4lineiden%20tyhjennys%20ja%20uusiok%C3%A4ytt%C3%B6.PDF
[11] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Yhdyskaytavaratkaisuohje.pdf
[12] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Turvallinen_tuotekehitys_Suomi_J003_2018.pdf
[13] https://www.finlex.fi/fi/sopimukset/sopsteksti/2022/20220009/20220009_2

6.3.2 EU ja Nato

EU:n neuvoston turvallisuussäännön EU/488/2013 6 artiklan nojalla annetuissa periaatteissa (policy) ja suuntaviivoissa (guidelines) ja Naton turvallisuussäännöstöön sisältyvissä direktiiveissä ja ohjeissa tarkennetaan eri tavoin salausratkaisujen ja muiden turvallisuuskriittisten tuotteiden ja niiden arvioinnin vaatimuksia. Asiakirjat ovat pääsääntöisesti salassa pidettäviä tai turvallisuusluokiteltuja. Tiedon luovuttamista näistä käsitellään ohjeen luvussa 4.2.

EU:n tai Naton edellä mainittujen asiakirjojen lisäksi Traficom voi käyttää tarvittaessa täydentävästi kansallisen tiedon suojaamisessa määriteltyjä kriteerejä.

6.4 Arvioinneissa käytettävien vaatimusten koonti

Arvioinneissa käytettäviä vaatimuksia on havainnollistettu taulukossa 1.

Taulukko 1. Arvioinneissa käytettäviä vaatimuksia.

Tuotteeseen ja sen elinkaareen kohdistuvia vaatimuksia	Esimerkkejä
Tuotteen teknisiin ominaisuuksiin kohdistuvat julkiset vaatimukset	Salauksen kryptografinen vahvuus yhdyskäytäväratkaisun turvallisuustoiminnallisuudet
Tuotteen teknisiin ominaisuuksiin kohdistuvat salassa pidettävät vaatimukset	Yksityiskohtaisemmat tekniset vaatimukset Tuotekohtaiseen uhkamallinnukseen perustuvat vaatimukset
Tuotteen valmistamiseen ja kehittämiseen kohdistuvat vaatimukset	Tuotekehitysympäristön pääsynhallinnan ja eheyden suojaaminen Valmistuksen kontrollointi
Tuotteen valmistukseen ja toimitusketjuihin liittyvien riskien hallinta muiden valtioiden vaikutuksesta (FOCI, Foreign Ownership and Control Influence)	Joidenkin turvallisuusluokkien tai/ja tiedon luovuttavien viranomaisten (originator) tietojen käsittelyyn liittyvät rajoitukset
Asiakasviranomaisen tarve ja puolto	Viranomaisen ilmaisema tarve ko. tuotteen käytölle sekä puolto ko. tuotteen arvioinnille

7. Arviointimenettelyt ja arvioinnin varmuustasot

7.1 Arviointien sisältö

Arvioinnin sisältö riippuu turvallisuusluokasta siten, että ylempien turvallisuusluokkien tietojen suojaamiseen tarkoitettuihin tuotteisiin sekä tuotteiden elinkaaren kattavaan suojaamiseen kohdistuu laajemmat ja tiukemmat vaatimukset ja korkeampi uhkaympäristö. Myös tuotteen rakenne ja uhka-arvio vaikuttaa testauksen sisältöön.

Turvallisuusluokan vaikutusta arvioinnin sisältöön tapauksessa, jossa tuotteesta tehdään korkean varmuustason tuotearviointi, on havainnollistettu korkealla tasolla

taulukossa 2. Käytettävät yksityiskohtaiset arviointimenetelmät valitaan kuitenkin tapauskohtaisesti arviointityön suunnitteluvaiheessa.

Taulukko 2. Turvallisuusluokan vaikutus korkean varmuustason arvioinnin vähimmäissisältöön.

Arviointimenettely	TL II	TL III	TL IV
Yleisen ja teknisen dokumentaation tarkastus	X	X	X
Asetusten ja elinkaarenhallinnan tarkastus	X	X	X
Yksityiskohtainen yleisen ja teknisen dokumentaation tarkastus	X	X	
Lähdekoodin suppea katselmointi (salauskoodi)	X	X	X
Lähdekoodin turvallisuuteen vaikuttavien osien katselmointi	X	X	
Lähdekoodin kokonaiskatselmointi	X		
Ratkaisun suppea testaus	X	X	X
Ratkaisun perusmuotoinen testaus	X	X	
Ratkaisun laaja testaus	X		
Kehitysprosessin kontrollointi CAA:n toimesta	X	X	

Testauksen tasot määrittävät yleisimmät arviointimenetelmät. Arvioinnin laajuuteen vaikuttaa myös käyttötapaus, uhkaympäristö ja tuotteen rakenne.

Suppean testauksen tarkoituksena on ymmärtää laitteen toiminta ja asetukset, jotta voidaan arvioida mahdollisia riskejä ja todentaa turvalliseen käyttöön liittyvät keskeiset seikat. Tavoitteena on testata, ettei tuotteessa ole ilmeisiä ongelmia tavanomaisessa käytössä.

Suppeassa testauksessa arvioidaan tuotteen oikeellinen toiminta käyttöliittymän ja ulkoisten rajapintojen kautta tehtävällä pintapuolisella testauksella ja toiminnan seuraamisella. Lisäksi varmistetaan, ettei tuotteen sisäisissä tai ulkoisissa rajapinnoissa ja turvakontrolleissa ole tunnettuja ja helposti hyödynnettäviä heikkouksia.

Perusmuotoisen testauksen tarkoituksena on varmistaa suppean testauksen lisäksi laitteen sisäisen toteutuksen turvallisuus. Testauksessa varmistetaan asetukset ja toiminnat tarkemmalla tasolla kuin millä ne näkyvät esimerkiksi laitteen ylläpitäjille, esimerkiksi käyttöjärjestelmän kovennukset. Tuotteelle tehdään kehittyneiden hyökkäysten riskien kartoitus ja testauksessa myös tarkastetaan, miten laite reagoi kehittyneisiin hyökkäyksiin. Testaukseen voi kuulua yksittäisten kriittisten komponenttien erillistä testausta.

Laajan testauksen tarkoituksena on arvioida syvällisesti tuotteen teknistä toimintaa. Yksittäisiä komponentteja testataan yksittäisinä osina. Testauksessa toteutetaan yksittäisten komponenttien kattava testaus ilman tuotteen komponenttien ympäröiviä suojausmekanismeja. Testausmenetelminä on myös käytössä erityisen kehittyneet hyökkäykset.

7.2 Arvioinnin varmuustasot

Mitä kattavammin turvallisuusluokittain laajentuvien ja tiukentuvien vaatimusten täyttymisen arviointi tehdään, sitä suurempi varmuus tuotteen toiminnasta ja luotettavuudesta voidaan saada. Tätä kuvataan käsitteellä varmuustaso. Varmuustaso ei ilmaise tuotteen vaatimuksenmukaisuutta, vaan nimenomaan tuotteeseen kohdistuvien vaatimusten täyttymisen arvioinnin luotettavuutta.

Arvioinnin varmuustasoja on havainnollistettu taulukossa 3. Tuotearvioinnin korkea varmuustaso (A) on arviointityön lähtökohta. Se on myös edellytys kansainvälisille tuotehyväksynnöille ja julkisille lausunnoille kansallisten tuotteiden osalta. Alemman varmuustason arvioinnit on tarkoitettu tukemaan viranomaisen riskiarviointia ja päätöksentekoa. Niitä tehdään viranomaisten tarpeista silloin, kun käyttötapauksessa ei ole olemassa tai muuten mahdollista hyödyntää korkealla tasolla arvioitua tuotetta.

Taulukko 3. Arvioinnin varmuustasot.

Varmuustaso	Arvioinnin syvyys (luotettavuus)
Matala (C)	Matala
Keskitaso (B)	Perusmuotoinen
Korkea (A)	Syvällinen

Eri varmuustasojen arvioinnit edellyttävät erilaisia tietoja ja aineistoja tuotteen valmistajalta. C-tason arvioinneissa tuotetta arvioidaan pääasiassa siihen liittyvän dokumentaation perusteella. B-tason arvioinneissa tuotteesta on toimitettava toimiva kappale arviointia varten. A-tason arviointeja varten tuotteesta on toimitettava kattavimmat tiedot ja aineistot mukaan lukien lähdekoodi.

7.3 Arviointimenettelyiden valinta

Traficom määrittelee ja valitsee arvioinnissa käytettävät menettelyt turvallisuusluokan mukaisten tuotteen vaatimusten, uhka-arvion ja tavoiteltavan varmuustason mukaisesti. Tuotteen arvioinnissa käytettävät menettelyt sovitaan arvioinnin suunnitteluvaiheessa.

7.4 Varmuustason vaikutus lausunnon tai päätöksen julkisuuteen

Lähtökohtaisesti tuotearvioinnit tehdään korkealla varmuustasolla. Tällöin lausunto on julkinen, jos viranomaisen tarve ei edellytä sen pitämistä salassa. Matalampien varmuustasojen arvioinneista kirjoitetut lausunnot ovat taas yleensä salassa pidettäviä.

Traficom päättää tapauskohtaisesti, onko lausunto tai päätös julkinen. Julkisuuden arvioinnissa otetaan huomioon asiakasviranomaisen ja valmistajan perustellut tarpeet.

Tämä menettely johtuu siitä, ettei tuotteen käyttäjien haluta erehtyvän arvioinnin sisällöstä, kun ne tekevät omia valintojaan järjestelmiinsä. Traficomin julkista arviota voitaisiin sen rajoituksista riippumatta helposti erehtyä pitämään yleispätevänä ja arvioinnin rajoituksiin liittyvät vaikutukset voisivat jäädä tuotteen viranomaiskäyttäjältä huomioimatta. Traficomin antaa siis julkisen lausunnon vaatimusten täyttymisestä vain sellaisissa tilanteissa, joissa Traficomilla on riittävät tiedot tuotteen valmistuksesta ja teknisestä toteutuksesta sekä mahdollisuus saada pääsy tarkastuksen ja arvioinnin kannalta olennaisiin resursseihin ja tietoon.

Tämä yhdistettynä valmistuksen kontrollointitarpeeseen tarkoittaa sitä, että lähtökohtaisesti ulkomaisille tuotteille voidaan tehdä korkeiden varmuustasojen arviointeja vain turvallisuusluokille IV/NR/EU-R.

7.5 Muiden hyväksyntöjen tai sertifikaattien hyväksi lukeminen

Traficom voi harkintansa mukaan ottaa huomioon osana arviointiin liittyvää selvitystä jonkin toisen valtion viranomaisen tai sertifiointiorganisaation tuotteelle tekemän arvioinnin. Arvioinnin hyödyntäminen riippuu siitä, mihin tarkoitukseen ja millä perusteella arviointi on tehty ja mitä tietoja sen sisällöstä on saatavilla.

Tuotearvioinnit turvallisuusluokitellun tiedon suojaamiseen liittyvät aina kansallisesti turvallisuusluokitellun tiedon suojaamiseen tai kansainvälisten tietoturvallisuusvelvoitteiden täyttämiseen. Näihin velvoitteisiin ei liity säädettyjä velvoitteita arviointien vastavuoroisesta tunnustamisesta tai hyväksi lukemisesta (lukuun ottamatta kahdenvälisiä kansainvälisiä tietoturvallisuussopimuksia), joten Traficom punnitsee tapauskohtaisesti muiden arviointien hyödynnettävyyden omassa arvioinnissaan.

8. Arviointiprosessi

Tässä luvussa kuvataan arviointiprosessin keskeiset vaiheet. Arviointiprosessi on havainnollistettu liitteessä 1.

8.1 Traficomin, asiakasviranomaisen ja valmistajan kolmikanta

Tuotteen arviointi tulee Traficomissa vireille asiakasviranomaisen tai valmistajan pyynnöllä, jota kuvataan seuraavassa luvussa. Käynnistyipä arviointiprosessi muodollisesti kumman tahansa pyynnöllä, on yleensä tärkeää selvittää arviointiprosessin tavoitteet ja pääpiirteet kaikkien osapuolten kesken.

Kaikilla osapuolilla täytyy olla sama käsitys siitä, minkä varmuustason arviointi on mahdollista tehdä ja onko lopputuloksena tarkoitus tai mahdollista syntyä julkinen tieto arvioinnin tuloksesta vai viranomaiskohtainen tieto tiettyä järjestelmää varten. Itse tekninen arviointiprosessi on yleensä pääasiassa Traficomin ja valmistajan välistä vuoropuhelua ja toimia, mutta on hyvä tunnistaa raportoinnin ja tiedonvaihdon tarpeet kaikkien osapuolten välillä. On myös tärkeää muodostaa yhteinen käsitys arviointiin liittyvistä maksuista.

8.2 Arviointi- tai hyväksyntäpyyntö

Jotta tuote voidaan ottaa arvioitavaksi Traficomissa, viranomaisen tai valmistajan täytyy tehdä arviointipyyntö.

Arvioinnin tarpeesta on hyvä olla yhteydessä Traficomiin jo tuotteen suunnitteluvaiheessa, jotta Traficom voi antaa neuvontaa asiassa, huomioida eri tarpeet

priorisoinnissa, suunnitella arviointien resursointia ja osallistua tarvittaessa tuotekehitykseen alusta alkaen (ks. yllä, koskee turvallisuusluokkia II ja III).

Valmistajan pyynnöstä tehtävä arviointi edellyttää Traficomin ja valmistajan sopimusta tuotearvioinnista ja selvitystä viranomaisen tarpeesta.

Viranomainen voi pyytää arviointilain perusteella tietojärjestelmän arviointia ja arviointi voi koskea myös tietojärjestelmän osaa. Viranomainen voi pyytää arviointia tuotteesta kansallisen turvallisuusluokitellun tiedon suojaamisessa tai hyväksyntää EU:n tai Naton turvallisuusluokitellun tiedon suojaamisessa. Pyyntö voi koskea tuotteen arvioimista siten, että arvioinnin tulos voidaan yleispätevänä julkaista (ottaen huomioon valmistuksen alkuperään liittyvät edellytykset) tai siten, että tuote arvioidaan tai hyväksytään vain tapauskohtaisesti viranomaisen tietojärjestelmässä.

Tarvittaessa Traficom arvioi siis tuotteen **osana viranomaisen järjestelmäkokonaisuutta.** Viranomaisen pyynnöstä voidaan arvioida myös pelkkä hankittavaksi suunniteltu salausratkaisu tai tuote.

Viranomainen voi pyytää tapauskohtaista arviota tai hyväksyntää myös alkuperältään ulkomaisesta tuotteesta. Kansallisen turvallisuusluokitellun tiedon suojaamisessa Traficomin ja asiakasviranomaisen täytyy sopia, miten ulkomaisen vaikutuksen riski arvioidaan. Riskipäätös kuuluu asiakasviranomaisen vastuulle. Kansainvälisten tietoturvallisuusvelvoitteiden täyttämisen arvioinnissa Traficom arvioi asian ja toteaa sen hyväksyntäpäätöksessä tai osana tietojärjestelmän hyväksyntää koskevaa hyväksyntälausuntoa. Traficom voi myös selvittää, miten mahdollinen toisessa valtiossa annettu EU:n tai Naton turvallisuusääntöjen puitteissa olemassa oleva hyväksyntä sekä saatavissa olevat tiedot tuotteesta huomioidaan.

Arviointipyynnöstä täytyy ilmetä, millaisesta tuotteesta on kyse, missä vaiheessa tuotteen kehitys on (suunnitteilla, valmisteilla, tuotannossa) ja mikä on tuotteelle tavoiteltu turvallisuusluokka.

Traficom voi pyytää täydennystä arvioinnin edellytysten selvittämiseksi. Tarvittaessa Traficom ilmoittaa kirjallisesti sekä valmistajalle että asiakasviranomaiselle arviointiprosessin luonteesta ja pääpiirteistä (esim. varmuustasosta ja voiko tulos olla julkinen). Traficom ilmoittaa myös, jos tuotetta ei voi ottaa arvioitavaksi ja perustelut tälle.

Arvioinnin pyytäjältä edellytetään, että tämä toimittaa riittävät tiedot arviointisuunnitelman tekemistä varten, nimeää vähintään yhden soveltuvan teknisen yhteyshenkilön vastaamaan arvioinnissa esiin tuleviin kysymyksiin ja sitoutuu arviointiprojektin aikatauluun. Pyytäjältä edellytetään myös, että se omalta osaltaan mahdollistaa arviointiprojektin kannalta tarvittavat resurssit, joihin tyypillisesti sisältyy testattavan tuotteen ja pyydetyn dokumentaation toimittaminen, tuotteeseen liittyvä koulutus sekä soveltuvat henkilöstö- ja tilavaraukset.

Hyväksytyn tietoturvallisuuden arviointilaitoksen lausuntopyyntöä Traficomille arviointilaitoksen toimeksiannoissa käsitellään arviointilaitosohjeessa.

8.3 EU- ja Natohyväksynnät

8.3.1 Salaustuotehyväksyntä EU-tiedon suojaamiseen

Traficom on toimivaltainen tekemään salaustuotehyväksynnän EU:n turvallisuusluokitellun tiedon käsittelyssä kansallisissa järjestelmissä turvallisuusluokissa EU-R ja EU-C. Korkeammissa turvallisuusluokissa edellytetään aina lisäksi nk. AQUA[14]-

[14] AQUA = Approriately Qualified Authority

maan tekemää toista arviointia (SPE, Second Party Evaluation) ja neuvoston hyväksyntää.

Salaustuotteiden vieminen EU:n hyväksyttyjen salaustuotteiden listalle (LACP[15]) edellyttää aina AQUA-maan SPE-arviointia kansallisen CAA-viranomaisen arvioinnin ja hyväksynnän lisäksi koskien kaikkia turvallisuusluokkia.

Taulukossa 5 kuvataan Traficomin (CAA-toiminnon) toimivalta EU-salaustuotehyväksynnöissä.

Taulukko 4. Toimivalta EU-salaustuotehyväksynnöissä.

EU-turvallisuusluokka (SopS 77/2015 artikla 2)	**vastaava kansallinen turvallisuusluokka** (SopS 77/2015 liite)	**Traficomin CAA-tehtävä salaustuotteiden hyväksynnässä** EU/488/2013 EU:n neuvoston turvallisuussääntö artikla 10.6
TRES SECRET UE / EU TOP SECRET (TS-UE/EU-TS)	ERITTÄIN SALAINEN YTTERST HEMLIG (TL I)	• **hyväksyntätoimivalta neuvostolla** turvallisuuskomitean suosituksesta • hyväksyntä perustuu AQUA-maan tekemään toiseen arviointiin (SPE, Second Party Evaluation) ja suositukseen • kansallinen CAA tekee ensimmäisen arvioinnin (FPE, First Party Evaluation)
SECRET UE / EU SECRET (S-UE/EU-S)	SALAINEN HEMLIG (TL II)	• **hyväksyntätoimivalta neuvostolla** turvallisuuskomitean suosituksesta • hyväksyntä perustuu AQUA-maan tekemään toiseen arviointiin (SPE, Second Party Evaluation) ja suositukseen • kansallinen CAA tekee ensimmäisen arvioinnin (FPE, First Party Evaluation)
CONFIDENTIEL UE / EU CONFIDENTIAL (C-UE/EU-C)	LUOTTAMUKSELLINEN KONFIDENTIELL (TL III)	• **kansallinen CAA voi hyväksyä salausratkaisun kansallisessa järjestelmässä** • kansallisessa järjestelmässä voi käyttää myös neuvoston hyväksymää salausratkaisua
RESTREINT UE / EU RESTRICTED (R-UE/EU-R)	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG (TL IV)	• **kansallinen CAA voi hyväksyä salausratkaisun kansallisessa järjestelmässä** • kansallisessa järjestelmässä voi käyttää myös neuvoston hyväksymää salausratkaisua

8.3.2 Salaustuotehyväksyntä Naton turvallisuusluokitellun tiedon hyväksyntään

Traficom on toimivaltainen tekemään salaustuotehyväksynnän Naton turvallisuusluokitellun tiedon käsittelyssä turvallisuusluokissa NR (Nato Restricted) ja NC (Nato Confidential). Korkeammissa turvallisuusluokissa edellytetään aina lisäksi SECAN-viraston tekemää toista arviointia (SPE, Second Party Evaluation) ja Naton sotilaskomitean hyväksyntää.

[15] LACP = List of Approved Cryptographic Products

Yritys voi hakea salaustuotteensa lisäämistä NIAPC[16]-listalle, mutta tuotteen hyväksyntätietojen lisäämiseksi tarvitaan kansallisen NCSA-viranomaisen tuki. NIAPC sivuilta löytyy lomakkeet listauksen hakemiseksi.

Taulukossa 6 kuvataan Traficomin (NCSA-toiminnon) toimivalta Naton salaustuotehyväksynnöissä.

Taulukko 5. Toimivalta Nato-salaustuotehyväksynnöissä.

Naton turvallisuusluokka	**vastaava kansallinen turvallisuusluokka**	**Traficomin NCSA-tehtävä salaustuotteiden hyväksynnässä** **C-M(2002)49-REV1 Liite F artikla 11**
COSMIC TOP SECRET (CTS)	ERITTÄIN SALAINEN YTTERST HEMLIG (TL I)	• **hyväksyntätoimivalta sotilaskomitealla (NAMILCOM)** • hyväksyntä perustuu Naton elimen tekemään toiseen arviointiin (SPE, Second Party Evaluation) • kansallinen NCSA tekee ensimmäisen arvioinnin (FPE, First Party Evaluation)
NATO SECRET (NS)	SALAINEN HEMLIG (TL II)	• **hyväksyntätoimivalta sotilaskomitealla (NAMILCOM)** • hyväksyntä perustuu Naton elimen tekemään toiseen arviointiin (SPE, Second Party Evaluation) • kansallinen NCSA tekee ensimmäisen arvioinnin (FPE, First Party Evaluation)
NATO CONFIDENTIAL (NC)	LUOTTAMUKSELLINEN KONFIDENTIELL (TL III)	• **kansallinen NCSA voi hyväksyä salausratkaisun kansallisessa järjestelmässä** • kansallisessa järjestelmässä voi käyttää myös sotilaskomitean (NS:lle tai CTS:lle) hyväksymää salausratkaisua
NATO RESTRICTED (NR)	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG (TL IV)	• **kansallinen NCSA voi hyväksyä salausratkaisun kansallisessa järjestelmässä** • kansallisessa järjestelmässä voi käyttää myös sotilaskomitean (NS:lle tai CTS:lle) hyväksymää salausratkaisua

8.3.3 Security Enforcing Products Naton turvallisuussäännöstössä

Naton turvallisuussäännöstön useissa asiakirjoissa mainitaan turvallisuuskriittiset tuotteet eli Security Enforcing Products (SEP-tuotteet). Säännöissä määritellään tietyt turvallisuuskriittisten tuotteiden kategoriat, joille edellytetään aina NCSA:n hyväksyntää kansallisissa järjestelmissä. Osana järjestelmätarkastusta voidaan edellyttää NCSA:n hyväksyntää myös tuotteille näiden määriteltyjen tuotekategorioiden ulkopuolelta.

Hyväksyntä voidaan nähdä kaksiosaisena prosessina:

- Hyväksyntä tuotteen soveltuvuudesta Naton turvallisuusluokitellun tiedon käsittelyyn kansallisessa järjestelmässä (NCSA tekemä tuotehyväksyntä)
- Hyväksyntä tuotteen käytöstä osana tiettyä järjestelmää (osana SAA-toiminnon hyväksyntälausuntoa)

[16] NIAPC = Nato Information Assurance Product Catalogue

Osalle tuotteista määritellään turvallisuussäännöstössä erityisiä vaatimuksia. Muutoin sovelletaan kansallisia vaatimuksia, joita täydennetään tarvittaessa soveltuvilla Naton dokumenteilla. Tietojen luovuttamista valmistajalle käsitellään luvussa 4.2.

NIAPC-listalle voidaan viedä myös SEP-tuotteita. NIAPC sivuilta löytyy lomakkeet listauksen hakemiseksi. Yritys voi hakea tuotteensa lisäämistä NIAPC-listalle, mutta tuotteen hyväksyntätietojen lisäämiseksi tarvitaan kansallisen NCSA-viranomaisen tuki.

8.4 Traficomin priorisointiperiaatteet

Traficom noudattaa tuotteiden arviointipyyntöjen priorisoinnissa samoja arviointilaissa säädettyjä periaatteita kuin tieto- ja tietoliikennejärjestelmien arviointipyynnöissä.

Arviointilaki *4 § Viestintäviraston tehtävät*
3 mom. Viestintävirasto suorittaa tässä laissa tarkoitetut tehtävät käytettävissään olevien voimavarojen mukaisesti ottaen huomioon kansainvälisten tietoturvallisuusvelvoitteiden noudattaminen sekä pyydettyjen toimenpiteiden merkitys viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen.

Arviointi- ja hyväksyntätehtävien priorisoinnissa otetaan siis huomioon kansainvälisten tietoturvallisuusvelvoitteiden noudattaminen sekä pyydettyjen toimenpiteiden merkitys viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen eli viranomaisen tarve tuotteelle. Jotta tuote otetaan Traficomissa arvioitavaksi, tulee tuotteilla olla viranomaistarve ja tuotteilla tulee olla potentiaalia vastata viranomaisen tarpeeseen.

Etenkin kansallisen turvallisuusluokitellun tiedon suojaamiseen tarkoitettujen tuotteiden arvioinnin edellytyksenä on, että Traficomilla on siihen riittävät henkilöresurssit.

Priorisoinnissa huomioidaan arvioinnin laajuus ja tuotteilla suojattavan tiedon turvallisuusluokka. Tuotteiden arviointi- ja hyväksyntätehtävissä priorisoidaan tuotteita, joiden arviointi voidaan toteuttaa korkealla varmuustasolla. Laissa ei säädetä tuotteiden valmistuksen alkuperästä, mutta käytännössä korkean varmuustason arvioinnin edellytykset täyttyvät lähinnä kotimaisessa valmistuksessa, joka kuuluu Suomen lainkäyttövallan piiriin. Suppea arviointi on tarkoitettu toteutettavaksi vain rajatuissa tapauksissa, kuten osana tietojärjestelmän arviointia. Lähtökohtaisesti priorisointiin vaikuttaa myös vastaavien tuotteiden saatavuus. Arviointipyynnöissä on tarkasteltava, löytyykö vastaavia tuotteita esimerkiksi Traficomin hyväksyttyjen tuotteiden listalta, vai onko uuden tuotteen arvioinnille tarvetta.

Sääntelyssä ei ole otettu huomioon tilannetta, jossa valmistaja hakisi itse EU- tai Natohyväksyntää tuotteelleen. EU:n ja Naton turvallisuussäännöt eivät ota kantaa kansallisiin hallintoprosesseihin. Traficom priorisoi arviointilain mukaisesti viranomaisten tietojärjestelmiin ja tietoliikennejärjestelyihin liittyvät tarpeet.

8.5 Esipalaveri valmistajan ja Traficomin välillä

Esipalaveri pidetään valmistajan ja Traficomin arvioijien kesken. Tarvittaessa myös asiakasviranomainen voidaan ottaa mukaan, jotta tuotteen käyttötarpeista voidaan varmistua ja jotta arviointiprosessin kokonaisuus voidaan käydä läpi kaikkien osapuolten kesken. Esipalaverissa sovitaan arviointityön käytännöistä.

Esipalaverissa keskustellaan asiakkaan etukäteen toimittamista tiedoista, joita ovat soveltuvin osin muun muassa:

- Tuotteen toiminnallinen kuvaus

- Käydään läpi tuotelupaus, tuotteen suorituskyky sekä toiminnallisuus.
- Lisäksi käydään läpi tuotteen kokonaisarkkitehtuuria ja sitä ympäröiviä elementtejä sekä uhkamalleja.

- Tuotteen salaustekniikka
  - Käydään läpi tuotteen salaustekniset ominaisuudet ja ratkaisut sekä avaintenhallinta.
- Arvioinnin tavoitetaso
  - Käydään läpi tavoiteltu turvallisuusluokka ja arvioinnin varmuustaso ja näiden edellytykset tuotteen suunnitellussa käyttötarkoituksessa.
- Aikaisemmat arvioinnit ja testaukset
  - Käydään läpi mahdolliset aiemmin tehdyt arvioinnit ja testaukset.
- Yritysturvallisuuteen ja tuotekehitykseen liittyvät turvallisuusasiat
  - Katselmoidaan valmistajan tietoturvallisuusjärjestelyt ja tilaajan/viranomaisen mahdollinen tarve hakea valmistajasta yritysturvallisuusselvitystä

Esipalaverissa keskustellaan valmistajan ja asiakasviranomaisen kanssa siitä, halutaanko tuotteesta tai sen käynnissä olevasta arvioinnista antaa tietoa muille viranomaisille.

Arviointia varten tarvittava dokumentaatio kuvataan liitteessä 2. Ennen arviointisuunnitelman laatimista tulee Traficomille toimittaa vaadittava dokumentaatio riittäviltä osin. Ensimmäinen esipalaveri voidaan kuitenkin järjestää, vaikka tarkkaa dokumentaatiota kaikista kohdista ei olisi toimitettu. Mikäli arviointisuunnittelun edellyttämiä tietoja ei saada toimitettua esipalaveriin tai kohtuullisessa ajassa sen jälkeen, Traficom voi keskeyttää prosessin ja käyttää varatut resurssit muihin arviointeihin.

8.6 Työmääräarvio

Traficom laatii kunkin tuotteen ja tuoteversion arvioinnista työmääräarvion, jossa kuvataan yleisellä tasolla kyseisen tuotteen arviointiin eri osa-alueisiin kuluva aika sekä kokonaisuuden työmäärä.

Valmistajalle ja asiakasviranomaiselle annetaan mahdollisuus kommentoida työmääräarviota. Arviota päivitetään tarvittaessa arvioinnin kuluessa, jos siihen tulee olennaisia muutoksia.

Työmääräarvion tarkoitus on auttaa ennakoimaan aikataulua ja arvioinnista perittävää maksua, jota käsitellään seuraavassa luvussa.

8.7 Traficomin maksut

Traficom perii arvioinnista kulloinkin voimassa olevan maksuasetuksen mukaisesti (Liikenne- ja viestintäministeriön asetus Liikenne- ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista)[17] omakustannusarvon mukaisen maksun, joka perustuu tarkastukseen, arviointiin ja lausunnon tai hyväksynnän valmisteluun ja antamiseen käytettyyn työmäärään ja aikaan.

[17] https://finlex.fi/fi/laki/ajantasa/2018/20180935

Maksu peritään asetuksen mukaan myös muutosten tai poikkeamien käsittelyyn liittyvästä oleellisesta suoritteesta. Maksu peritään myös keskeytetyssä arvioinnista käytetystä ajasta.

Maksuvelvollisuus koskee valmistajan sopimuksen voimassaollessa tehtyjä toimenpiteitä, vaikka sopimus olisi päättynyt.

Maksusta on viime kädessä vastuussa joko valmistaja, jonka kanssa tehdyn sopimuksen puitteissa arviointipyyntö käsitellään tai viranomainen, jonka pyynnöstä (arviointilain mukaisesta hakemuksesta) arviointi on otettu vireille ja Traficomin käsiteltäväksi. Valmistaja ja asiakasviranomainen voivat kuitenkin keskenään sopia maksuvastuista ja siitä, mikä laskutusyhteystieto ilmoitetaan Traficomille.

8.8 Arviointi

Tuotteen arvioinnin tarkoituksena on tutkia täyttääkö tuote sille asetetut tietoturvavaatimukset ja toimiiko tuote kuvatulla tavalla.

Arvioinnin edetessä valmistajalle ja tarvittaessa asiakasviranomaiselle raportoidaan keskeisiä havaintoja, joiden pohjalta valmistajan on mahdollista tehdä tuotteeseen muutoksia. Mahdollisten muutosten jälkeen tarvittavat testit uusitaan ja tuotteen testaamista jatketaan suunnitelman mukaisesti. Tuotteisiin arvioinnin aikana tehtävät muutokset ja korjaukset voivat vaikuttaa sekä arvioinnin aikatauluun että kustannuksiin.

Arviointi voidaan aloittaa, kun asiakas on toimittanut tuotteen kehitysvaiheen mukaiset riittävät tiedot arvioitavasta tuotteesta.

8.9 Lausunto tai hyväksyntäpäätös ja muut asiakirjat

Kun arviointi on saatu päätökseen, Traficom antaa lausunnon tai hyväksyntäpäätöksen

- Lausunto vaatimusten täyttymisestä turvallisuusluokan [TL IV-TL II] tietojen suojaamisessa
- Lausunto vaatimusten osittaisesta täyttymisestä [TL IV-TL II] tietojen suojaamisessa
- (Lausunto siitä, että vaatimukset eivät täyty tai pelkkä arviointiraportti, josta tämä ilmenee)
- Päätös tuotteen hyväksynnästä [EU:n tai Naton yksilöidyn turvallisuusluokan] tietojen suojaamisessa
- Päätös tuotteen (tapauskohtaisesta) hyväksynnästä [EU:n tai Naton yksilöidyn turvallisuusluokan] tietojen suojaamisessa [viranomaisen X tietojärjestelmässä]
- (Tarvittaessa päätös siitä, että vaatimukset eivät täyty)

Traficomin lausuntoon tai hyväksyntäpäätökseen voivat liittyä muun muassa seuraavat liitteet

- Arviointiraportti
- Kryptologinen lausunto
- Käyttöpolitiikka (SecOps)

8.10 Tuotteen elinkaarenhallinta

8.10.1 Lausuntojen ja hyväksyntöjen määräaikaisuus ja muutosten arviointi

Traficomin lausunto tai hyväksyntäpäätös vaatimuksen täyttävälle tuotteelle on aina määräaikainen ja on pääsääntöisesti voimassa korkeintaan 3 vuotta. Tämän jälkeen arvioinnin voimassaoloa voidaan jatkaa, mikäli tuotteen turvallisuus edelleen vastaa siihen kohdistuvia vaatimuksia. Määräaika voi olla myös lyhyempi.

Valmistajan tulee aktiivisesti ylläpitää tuotteen turvallisuutta. Kriittiset ohjelmistohaavoittuvuudet tulee korjata mahdollisimman nopeasti ja asiasta tulee olla viivytyksettä yhteydessä Traficomiin.

Lausunto tai hyväksyntä koskee yleensä vain tiettyä tuoteversiota. Uudet ohjelmisto- tai tuoteversiot voivat siten edellyttää arviointia. Mikäli muutetulle tuotteelle halutaan lausuntoa tai hyväksyntää, tulee asiasta olla yhteydessä Traficomiin. Arviointiprosessin aikana voidaan kuitenkin sopia valmistajan kanssa siitä, millaisia muutoksia hyväksynnän saaneelle tuotteelle voidaan tehdä ilman erillistä yhteydenottoa.

Edellä kuvattu muutosten ylläpito koskee tilanteita, joissa tuotteelle on laadittu lausunto vaatimusten täyttymisestä kansallisen turvallisuusluokitellun tiedon suojaamisessa ja tieto lausunnosta on julkaistu. Ylläpito koskee myös tilanteita, joissa Traficom on antanut hyväksynnän tuotteen käytölle kansainvälisen turvallisuusluokitellun tiedon suojaamisessa ja tieto on julkaistu.

Niissä tilanteissa, joissa Traficom on antanut viranomaiselle lausunnon kansallisen turvallisuusluokitellun tiedon suojaamisesta tai kansainvälisen tietoturvallisuusvelvoitteen edellyttämän hyväksynnän järjestelmäkohtaisesti tuotteen käyttämisestä osana tietojärjestelmää, vastuu tuotteen tietoturvallisuudessa tapahtuvien muutosten seurannasta ja esim. päivitysten asentamisesta on tietojärjestelmän vastuuviranomaisella.

Teknisten muutosten ilmoittamista voidaan lähtökohtaisesti luokitella seuraavasti:

1) Suunniteltu muutos on aina ilmoitettava ennen sen toteuttamista Traficomin arvioitavaksi ja hyväksyttäväksi, jos muutos voi vaikuttaa tuotteen salausominaisuuksiin, käyttöturvallisuuteen, ohjelmistoarkkitehtuuriin tai muuten tuotteen turvallisuuden kannalta keskeisiin tekijöihin.

   Traficom tutkii ja todentaa muutoksen laajuudesta riippuen tuotteen turvallisuusominaisuudet osittain tai kokonaan.

2) Suunnitellusta muutoksesta ja sen yksityiskohdista on ilmoitettava Traficomille vähintään neljä viikkoa ennen muutoksen suunniteltua toteutusajankohtaa, kun hyväksyttyyn tuotteeseen on tarkoitus toteuttaa vähäisiä muutoksia, esimerkiksi konfiguraatiomuutoksia, joilla ei ole turvallisuusvaikutuksia.

   Traficom arvioi muutoksen luonteen ja tiedottaa tuotteen valmistajaa siitä, voidaanko muutos toteuttaa ja jaella ilman erillistä arviointia vai edellyttääkö muutos Traficomin tarkastusta ennen kuin se voidaan toteuttaa ja jaella.

   Tuotteen on edelleen muutoksen jälkeen oltava salausominaisuuksiltaan ja keskeisiltä tietoturvallisuusominaisuuksiltaan hyväksyntää vastaava ja käytettävissä käyttöpolitiikan mukaisesti. Jos ohjelmiston tosiasiallinen toiminnallisuus ei muutoksen seurauksena muutu, kyseessä on vähäinen muutos ja se voidaan tehdä ilman Traficomin arviointia.

3) Traficomille täytyy ilmoittaa viipymättä mahdollisimman tarkasti muutoksen jakelemisesta tuotteeseen ja muutoksen sisällöstä, kun tuotteeseen tehdään tietoturvallisuuspäivityksiä.

   Tietoturvallisuuspäivityksen laajuudesta ja sisällöstä riippuen Traficom arvio muutoksen joko ennen tai jälkeen päivityksen.

   Tietoturvallisuuspäivitykset tuotteeseen tulee tehdä ja jaella asiakkaille viipymättä.

4) Traficomille täytyy ilmoittaa viipymättä mahdollisimman tarkasti muutoksen jakelemisesta tuotteeseen ja muutoksen sisällöstä, kun tuotteeseen tehdään tuotemerkkiin liittyviä pintapuolisia muutoksia tai vastaavia muutoksia, jotka eivät liity tai vaikuta salausominaisuuksiin.

   Tällaiset muutokset voidaan tehdä ja jaella ilman Traficomin arviointia.

   Tuotteen on edelleen muutoksen jälkeen oltava salausominaisuuksiltaan ja keskeisiltä tietoturvallisuusominaisuuksiltaan alkuperäistä lausuntoa vastaava ja käytettävissä käyttöpolitiikan mukaisesti.

Liitteet

1. Arviointiprosessikuvaus
2. Arvioinnissa tarvittava dokumentaatio (Material needed for evaluation). (Tämä liite on jaettu kahteen osaan, julkiseen ja turvallisuusluokiteltuun. Turvallisuusluokiteltu osa luovutetaan erikseen tarvitsijoille.)
3. Salaustuotearvioinnin pyyntölomake
4. Turvallisuuskriittisen tuotteen arvioinnin pyyntölomake