Antopäivä: 13.6.2025

Voimaantulopäivä: 13.6.2025

Voimassa: toistaiseksi

Lainsäädäntö, johon ohje perustuu:
Laki tietoturvallisuuden arviointilaitoksista (1405/2011)

Muutostiedot:
Korvaa aiemman 22.6.2022 voimaan tulleen ohjeen: Liikenne- ja viestintäviraston Ohje tietoturvallisuuden arviointilaitoksille 210/2022 O (Dnro: 153/602/2016)
ks. tarkemmat muutostiedot: Liite 1

Ohje tietoturvallisuuden arviointilaitoksille

Sisältö:

1 Johdanto

1.1 Ohjeen tarkoitus ja soveltamisala

Laissa tietoturvallisuuden arviointilaitoksista (1405/2011, Arviointilaitoslaki) säädetään arviointilaitosten hyväksymisestä, valvonnasta ja toiminnasta. Laissa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011, Arviointilaki), laissa julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015, TUVEL), laissa sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023, Asiakastietolaki) ja laissa sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019, Toisiolaki) säädetään tehtävistä, joita Liikenne- ja viestintävirasto Traficomin hyväksymä tietoturvallisuuden arviointilaitos voi hoitaa.

Lisäksi EU:n kyberturvallisuusdirektiivin (NIS2 -direktiivi) [1] kansallisen täytäntöönpanon yhteydessä annetuissa kyberturvallisuuslaissa (124/2025) sekä julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, Tiedonhallintalaki) uudessa 4 a luvussa on osoitettu arviointilaitoksille valvovia viranomaisia avustavia tehtäviä.[2]

Tässä ohjeessa kuvataan tietoturvallisuuden arviointilaitoksen rooli ja tehtävät siinä tietoturvallisuuden arviointitoiminnassa, josta säädetään varsinkin Arviointilaitoslaissa ja jonka ohjauksesta ja valvonnasta Traficom vastaa. Ohjeessa tarkoitetaan arviointilaitoksella aina tietoturvallisuuden arviointilaitosta. Ohjeessa kuvataan arviointilaitosten toimintaa koskevat vaatimukset ja arviointia koskeva menettely. Hyväksytyn arviointilaitoksen on tunnettava sen toimintaan liittyvä voimassa oleva lainsäädäntö ja muut toimintaa koskevat vaatimukset.

1.2 Määritelmät

Akkreditointi FINAS-akkreditointipalvelun suorittama arviointielimen pätevyyden toteaminen yhdenmukaisten kansainvälisten tai eurooppalaisten arviointiperusteiden mukaisesti.

Tietoturvallisuuden arviointikriteeristö vaatimuskriteeristö, jota sovelletaan tietoturvallisuuden arvioinnissa ja joihin arviointilaitos voi hakea akkreditointia ja Traficomin hyväksyntää.

[1] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555
[2] Ks. luku 5

1.3 Arviointilaitos

Arviointilaitos arvioi toimeksiannosta arvioinnin kohteen tietoturvallisuustason. Arviointilaitoksen tulee arvioinnissa selvittää, onko arvioinnin kohteen toiminnassa asianmukaisella tavalla toteutettu ne tietoturvallisuutta koskevat vaatimukset, jotka on otettu arvioinnin perustaksi. Jos vaatimukset täyttyvät, arviointilaitos voi antaa tästä arvioinnin kohteelle todistuksen.

Arviointilaitoksen tulee toiminnassaan noudattaa lainsäädännössä, akkreditoinnissa sovellettavissa standardeissa, Traficomin ohjeissa ja arviointilaitoksen hyväksymispäätöksessä asetettuja vaatimuksia.

1.4 Velvollisuus käyttää hyväksyttyä arviointilaitosta

Arviointilain 3 §:n mukaan valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden arvioinnissa vain Traficomia tai sen hyväksymää tietoturvallisuuden arviointilaitosta. Hyväksytyt arviointilaitokset hoitavat julkista hallintotehtävää ja niiden toiminta on säänneltyä ja valvottua.

Viranomaiset voivat kuitenkin osana normaalia toiminnan kehittämistä tehdä itse sisäisiä arviointeja, itsearviointeja tai tietojärjestelmien teknistä testausta. Ohjattujen sisäisten arviointien ja itsearviointien tukena voidaan myös hankkia erilaisia palveluita ulkopuolisilta palveluntuottajilta. Näissä tilanteissa on kuitenkin syytä kiinnittää riittävästi huomiota käytettävän toimijan taustoihin. Viranomaisen on ennakolta varmistuttava palveluntarjoajan luotettavuudesta toimeksiannon edellyttämässä laajuudessa ja että viranomaisen tietoja suojataan asianmukaisesti.[3]

Tiedonhallintalain 18 k §:n mukaan valvova viranomainen voi NIS2 -direktiivin noudattamisen valvomiseksi tehtäviin tarkastuksiin liittyen antaa avustavan tehtävän hyväksytylle tietoturvallisuuden arviointilaitokselle. Valvova viranomainen voi myös velvoittaa viranomaisen teettämään tietoturvallisuuden arviointilaitoksella kyberturvallisuuteen kohdistuvan riskienhallinnan arvioinnin.[4]

Arviointilaitos voi tarjota arviointilaitospalveluitaan myös muille kuin viranomaisille. Tällöin kyseeseen voi tulla arviointilaitoksen palvelu hyväksyttynä arviointilaitoksena tai sen ulkopuolelle jäävä palvelu (ks. luku 3.1).

[3] Ks. Laki viranomaisten toiminnan julkisuudesta (621/1999) 26 §:n 3 mom.
[4] Ks. kohta 5.1

Asiakastietolain ja Toisiolain mukaisia arviointivelvoitteita on kuvattu tarkemmin luvussa 6 ja liitteessä 3.

2 Arviointilaitoksen hyväksyminen

2.1 Vaatimukset tietoturvallisuuden arviointilaitokselle

Tietoturvallisuuden arviointilaitoksen hyväksymisen edellytyksenä on, että laitos täyttää Arviointilaitoslain 5 §:n mukaiset hyväksymiskriteerit eli

1) laitos on toiminnallisesti ja taloudellisesti riippumaton arvioinnin kohteesta;

2) laitoksen henkilökunnalla on hyvä tekninen ja ammatillinen koulutus sekä riittävän laaja-alainen kokemus toimintaan kuuluvissa tehtävissä;

3) laitoksella on toiminnan edellyttämät laitteet, välineet ja järjestelmät;

4) laitoksen vastuuhenkilöiden luotettavuus on varmistettu ja laitoksella on luotettavaksi arvioitu ja valvottu menetelmä, jonka avulla laitoksen toimitilojen ja tietojenkäsittelyn turvallisuus varmistetaan;

5) laitoksella on asianmukaiset ohjeet toimintaansa ja sen seurantaa varten.

2.1.1 FINAS-akkreditointipalvelun akkreditointi

Turvallisuus- ja kemikaaliviraston FINAS-akkreditointipalvelu vastaa sen selvittämisestä, että arviointilaitos täyttää edellä mainitut vaatimukset 1-3. Osoituksena vaatimusten täyttymisestä FINAS myöntää arviointilaitokselle akkreditointitodistuksen neljäksi vuodeksi, minkä jälkeen akkreditointia voidaan jatkaa uudella neljän vuoden määräajalla. FINAS myös valvoo akkreditoinnin edellytysten täyttymistä akkreditointitodistuksen voimassaoloaikana.

Arviointilaitoksen akkreditoinnissa sovelletaan standardien ISO/IEC 17021-1:2015[5] ja ISO/IEC 27006:2024[6] vaatimuksia. Kyseisissä standardeissa yksilöidään vaatimukset tietoturvallisuuden johtamisjärjestelmiä auditoiville ja sertifioiville elimille.

[5] SFS-EN ISO/IEC 17021-1:2015 Vaatimustenmukaisuuden arviointi. Vaatimukset johtamisjärjestelmiä auditoiville ja sertifioiville elimille. Conformity assessment. Requirements for bodies providing audit and certification of management systems.
[6] ISO/IEC 27006:2024 Information security, cybersecurity and privacy protection. Requirements for bodies providing audit and certification of information security management systems. Part 1: General

2.1.2 Traficomin hyväksyntä tietoturvallisuuden arviointilaitokselle

Kun FINAS on akkreditoinut arviointilaitoksen, Traficom voi myöntää arviointilaitokselle hyväksynnän, jos myös Arviointilaitoslain 5 §:n kohtien 4 ja 5 vaatimukset täyttyvät.

2.1.2.1 Vastuuhenkilöiden luotettavuus ja tietojenkäsittelyn turvallisuus

Arviointilaitoksen vastuuhenkilöiden tulee olla luotettavaksi todettuja henkilöitä. Vastuuhenkilöiksi katsotaan laitoksen kaupparekisteriotteessa ilmoitetut henkilöt ja laitoksen ylin johto.

Arviointilaitos käsittelee arviointitoiminnan yhteydessä arvioinnin kohteiden salassa pidettävää tietoa ja laitoksella tulee olla kyky käsitellä tällaista tietoa sille asetettujen suojausvaatimusten mukaisesti. Arviointilaitoksella on oltava luotettavaksi arvioitu ja valvottu menetelmä, jonka avulla laitoksen toimitilojen ja tietojenkäsittelyn turvallisuus varmistetaan.

Turvallisuusluokitellun tiedon turvallista käsittelyä koskevat vaatimukset todennetaan Katakrin[7] kulloinkin voimassa olevan version avulla. Arviointilaitoksen on täytettävä toiminnassaan Katakrin turvallisuusjohtamista, fyysistä turvallisuutta sekä teknistä tietoturvallisuutta koskevat vaatimukset. Arviointilaitoksen omaan toimintaan sovelletaan lähtökohtaisesti yhtä turvallisuusluokkaa korkeampaa vaatimustasoa, kuin mille laitos hakee hyväksyntää.[8] Tilanteissa, joissa haettavana pätevyysalueena on vain ISO/IEC 27001, tietojenkäsittelyn turvallisuus todennetaan käyttäen Katakrissa kuvattuja III-tason vaatimuksia. Arviointilaitoksena tehtävien arviointien yhteydessä saatua arvioinnin kohteiden salassa pidettävää tietoa tulee käsitellä vain arviointilaitoksen hyväksymisprosessissa tai Traficomin toimesta erikseen hyväksytyissä tietojärjestelmissä.

Vaatimusten täyttäminen tarkoittaa käytännössä muun muassa sitä, että arviointilaitos on määritellyt sen turvallisuustoimintaa koskevat periaatteet, turvallisuusorganisaation sekä siihen liittyvät vastuut, sillä on riittävät menetelmät riskien tunnistamiseksi, arvioimiseksi ja poikkeustilanteiden hallitsemiseksi. Arviointilaitoksen toimitilojen on puolestaan täytettävä

[7] Katakri - tietoturvallisuuden auditointityökalu viranomaisille.
[8] Arviointilaitoksella tulee olla kyky käsitellä loppuasiakkaansa luokittelemaa tietoa sille asetettujen suojausvaatimusten mukaisesti. Arviointilaitoksen arvioidessa esimerkiksi loppuasiakkaansa IV-tason järjestelmää, tulee arviointilaitos saamaan arviointiprosessin aikana asiakkaansa luokittelemaa ko. järjestelmää koskevaa tietoa (esimerkiksi verkkokuvat ja tiedot kytkennöistä muihin järjestelmiin). Järjestelmien turvallisuustoteutuksiin liittyvät tiedot luokitellaan eräissä tapauksissa pykälää korkeammalle, kuin mikä on korkein järjestelmässä käsiteltävä tieto. Myös eri loppuasiakkaiden tiedoista koostuvan tietovarannon turvallisuusluokka on usein tulkittavissa kasautumisvaikutuksesta johtuen yksittäisten tietojen turvallisuusluokkaa korkeammaksi.

Katakrissa luetellut vaatimukset koskien aluetta, fyysisiä rakenteita ja turvallisuusteknisiä järjestelmiä.

Henkilöstöturvallisuusvaatimukset edellyttävät muun muassa sitä, että arviointitoiminnassa käytetään vain sellaisia henkilöitä, jotka ovat antaneet asianmukaiset salassapitositoumukset, joilla on asiakkaan hyväksyntä ja voimassa riittävät turvallisuusselvitykset. Aiemmin arviointilaitosohjeessa on edellytetty, että arviointilaitos hakee toimintaan osallistuvista henkilöistä turvallisuusselvitykset. Suojelupoliisin ratkaisun (5/2024) mukaan arviointilaitoksilla ei ole edellytyksiä päästä turvallisuusselvityslain (726/2014, Turvallisuusselvityslaki) mukaiseen henkilöturvallisuusmenettelyyn arviointitoiminnan harjoittamisen perusteella. Arviointitoimintaan osallistuvien henkilöiden henkilöturvallisuusselvitysten hakemisesta vastaa suojelupoliisin tulkinnan mukaan tiedon omistaja eli arvioinnin kohde. Arviointilaitosten asiakkailla onkin useimmiten mahdollisuus hankkia arviointia suorittavista arviointilaitoksen työntekijöistä turvallisuusselvitykset. [9]

Arviointilaitoksen tulisi hyvissä ajoin informoida asiakkaitaan tarpeesta hakea turvallisuusselvitykset, sekä huolehtia että selvitykset haetaan riittävästä joukosta henkilöitä, jotta aikataulujen ja mahdollisten henkilövaihdosten osalta ei tulisi yllätyksiä.

Turvalliseen tiedonkäsittelyyn liittyen arviointilaitoksen tulee huomioida tietojenkäsittelyssään myös akkreditointistandardien vaatimukset koskien luottamuksellisuutta. Niiltä osin kuin tietojenkäsittelyn turvallisuuden vaatimukset eroavat akkreditointistandardien ja Katakrin välillä, noudatetaan Katakrissa kuvattua tietojen suojaamisen tasoa. Lisäksi arviointilaitoksen on varmistuttava siitä, että tiedonkäsittelyvaatimuksia noudatetaan riippumatta siitä, kuka arviointilaitoksen lukuun tekevä henkilö tai taho käsittelee salassa pidettävää tietoa. Vaatimukset koskevat yhtä lailla omaa henkilöstöä kuin tahoa, joka hoitaa arviointiin liittyviä tehtäviä esimerkiksi toimeksiantosopimuksen perusteella.

2.1.2.2 Asianmukaiset ohjeet toimintaa ja sen seurantaa varten

Arviointilaitoksella tulee olla ja sen tulee ylläpitää ohjeistusta koskien arviointitoimintaa ja toiminnan seurantaa. Ohjeistuksen tulee ottaa huomioon arviointilaitostoimintaan liittyvät lakisääteiset ja muut

[9] Turvallisuuselvityslaki 15 §: Henkilöturvallisuusselvitystä voi hakea, jollei kansainvälisistä tietoturvallisuusvelvoitteista muuta johdu tai laissa toisin säädetä, selvityksen kohteen työnantaja tai se, jonka antamaa toimeksiantoa tai siihen kuuluvaa tehtävää selvityksen kohteen on tarkoitus hoitaa tai jota hän hoitaa.

vaatimukset sekä tämän ohjeen sisältö. Lisäksi arviointilaitoksen tietoturvallisuusohjeistuksen on täytettävä Katakrissa kuvatut vaatimukset.

Arviointilaitoksen tulee varmistua siitä, että sen lukuun työskentelevät henkilöt ja tahot saatetaan tietoisiksi tietoturvallisuuden arviointitoimintaan liittyvistä vaatimuksista ja velvollisuuksista. Tämän varmistamiseksi arviointilaitoksen ohjeistuksessa tulee ottaa kantaa esimerkiksi siihen, miten laitos varmistuu siitä, että sen henkilöstö ja muut laitoksen lukuun työskentelevät henkilöt ovat tietoisia arviointilaitoksen yleisestä ja tietoturvallisuuteen liittyvästä ohjeistuksesta ja ymmärtävät ohjeistuksen sisällön.

2.2 Arviointilaitokseksi hakeutuminen

2.2.1 Akkreditoinnin hakeminen FINAS-akkreditointipalvelulta ja pätevyysalue

Ennen hyväksynnän hakemista Traficomilta arviointilaitoksen on haettava FINAS-akkreditointipalvelulta akkreditointia eli pätevyyden toteamista.

Arviointilaitoksen on hakiessaan pätevyyden toteamista ilmoitettava, mille pätevyysalueelle se hakee akkreditointia. Pätevyysalueet määritellään arviointikriteeristöittäin ja turvallisuusluokittain.

Tietoturvallisuuden arviointikriteeristöt:

1) ISO/IEC 27001, kulloinkin voimassa oleva versio

2) Katakri, tietoturvallisuuden arviointityökalu viranomaisille, kulloinkin voimassa oleva versio

3) muu julkaistu ja yleisesti tai alueellisesti sovellettu tietoturvallisuutta koskeva säännös, määräys tai ohje taikka vahvistettuun standardiin sisältyvät tietoturvallisuutta koskevat vaatimukset

Traficomin vakiintuneen soveltamiskäytännön mukaan arviointilaitoksen on aina haettava pätevyyttä osa-alueelle 1) eli jotta laitos voidaan hyväksyä tietoturvallisuuden arviointilaitokseksi, sillä on oltava pätevyys suorittaa ISO/IEC 27001 -standardin mukaisia arviointeja.

Jos tietoturvallisuuden arviointilaitoksen pätevyysalue kattaa Katakrin tai aiemmin käytössä olleet valtiovarainministeriön ohjeet tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI-ohjeet), se voi tehdä myös seuraavia arviointeja:

- sosiaali- ja terveydenhuollon tietojärjestelmien arvioinnin ja antaa olennaisten vaatimusten täyttymistä koskevan todistuksen

- sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain mukaisen käyttöympäristön tietoturvallisuuden arvioinnin ja antaa vaatimusten täyttymistä koskevan todistuksen

Jos arviointilaitos hakee pätevyysalueekseen Katakria, sen tulee hakea pätevyyttä myös turvallisuusluokan[10] perusteella. Turvallisuusluokan määrittely voi olla tarpeen myös muiden arviointikriteeristöjen osalta.

Kun arviointilaitos hakee ensimmäistä kertaa Traficomin hyväksymäksi tietoturvallisuuden arviointilaitokseksi, sille voidaan vakiintuneen soveltamiskäytännön mukaan hyväksyä pätevyysalue korkeintaan turvallisuusluokkaan KÄYTTÖ RAJOITETTU eli TL IV. Myöhemmin arviointilaitoksen on mahdollista hakea pätevyysalueeksi korkeintaan turvallisuusluokkaa LUOTTAMUKSELLINEN eli TL III.

2.2.2 Hyväksynnän hakeminen Traficomilta

Tietoturvallisuuden arviointilaitos voi hakea hyväksyntää toimintaansa varten Traficomille osoitetulla vapaamuotoisella hakemuksella. Hakemukseen on liitettävä tiedot, jotka ovat tarpeen asian käsittelyä varten. Hakemukseen liitteenä tulee olla FINAS-akkreditointipalvelun akkreditointipäätös, josta ilmenee arviointilaitoksen akkreditoitu pätevyysalue. Hyväksynnän antamisen edellytyksenä on, että laitos täyttää arviointilaitoslain 5 §:n hyväksymisvaatimukset.

Hakemuksen tulee sisältää seuraavat tiedot:

- Haettava pätevyysalue ja mahdollinen turvallisuusluokka
- Ilmoitus arviointilaitoksen vastuuhenkilöistä (toimitusjohtaja, hallituksen jäsenet sekä nimenkirjoitusoikeutetut)
- Selvitys arviointilaitoksen menetelmästä, jonka avulla laitoksen toimitilojen ja tietojenkäsittelyn turvallisuus varmistetaan;
- Arviointilaitoksen toimintaa koskevat ohjeet; sekä
- Tarvittaessa ilmoitus hakemukseen sisältyvistä salassa pidettävistä tiedoista.

Jos hakemus sisältää salassa pidettäviä tietoja, tulee hakemuksessa eritellä, miltä osin hakemus on salassa pidettävä ja mihin salassapito perustuu. Salassa pidettävät tiedot erotetaan mielellään hakemuksen erillisiksi liitteiksi.

[10] Ks. Laki julkisen hallinnon tiedonhallinnasta (906/2019) 18 § ja valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) 3 §.

2.3 Pätevyysalueen muuttaminen

Kun arviointilaitoksen hyväksytyn pätevyysalueen kriteeristö muuttuu esimerkiksi ISO/IEC 27001-standardin tai Katakrin uuden version myötä, ei hyväksytty pätevyysalue automaattisesti muutu. Pätevyysalue säilyy hyväksyntäpäätöksen mukaisena niin kauan kuin päätös on voimassa.[11] Traficom ei aseta määräaikaa uuden version käyttöönotolle, vaan arviointilaitos harkitsee itse, milloin se haluaa hakea pätevyyttä tarjota arviointeja uuden kriteeristön mukaan.

Jos Traficomin hyväksymä arviointilaitos haluaa muuttaa pätevyysaluettaan, sen tulee ensin hakea FINASilta pätevyysalueen muutosta tai kokonaan uutta pätevyysaluetta. FINAS arvioi muutoksen ja arvioinnin pohjalta tekee akkreditointipäätöksen muutoksen. Tämän jälkeen arviointilaitos voi hakea Traficomilta uutta hyväksyntäpäätöstä, jossa pätevyysalue on muutettu.

2.4 Maksullisuus

Tietoturvallisuuden arviointilaitoksen hyväksymistä koskevan asian käsittelystä perittävästä maksusta säädetään valtion maksuperustelaissa (150/1992) ja kulloinkin voimassa olevassa liikenne- ja viestintäministeriön asetuksessa Liikenne- ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista.[12]

Traficom perii omakustannusarvon mukaisen maksun toimenpiteistä, jotka liittyvät tietoturvallisuuden arviointilaitosten hyväksyntään. Asian vireille saattajalta peritään toimenpiteeseen käytettyyn aikaan perustuva maksu[13]. Maksu peritään myös suoritteen jälkikäteisvalvontaan liittyvästä olennaisesta suoritteesta.

---

[11] Hyväksynnän voimassaolon edellytyksenä on voimassa oleva FINAS-akkreditointi. Akkreditointi tai akkreditoinnin voimassa olon jatkaminen ei ole välttämättä mahdollista vanhentuneiden arviointikriteeristöjen osalta. Akkreditoinnin muutoksista tulee ilmoittaa Traficomille.

[12] 6/2025 voimassa on 21.12.2023 annettu Liikenne- ja viestintäministeriön asetus Liikenne- ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista (1190/2023). Ks. https://www.traficom.fi/fi/traficom/hinnat-ja-maksut

[13] 6/2025 voimassa olevan asetuksen mukaan (1190/2023) 150 euroa käytettyä työtuntia kohden (5 §).

3 Tietoturvallisuuden arviointilaitoksena toimiminen

3.1 Hyväksytyn arviointilaitoksen palvelut ja ei-hyväksytyn arviointilaitoksen palvelut

Arviointilaitoslain 2 §:n mukaan sitä sovelletaan elinkeinonharjoittajiin ja palvelutehtäviä julkishallinnolle tarjoaviin yksiköihin, jotka toimeksiannosta arvioivat tietoturvallisuustason ja jotka haluavat toiminnalleen Traficomin hyväksynnän.

Edelleen Arviointilaitoslain 13 §:n mukaan hyväksytyn tietoturvallisuuden arviointilaitoksen on Arviointilaitoslaissa tarkoitettuja tehtäviä hoitaessaan noudatettava hallintolakia (434/2003), viranomaisten toiminnan julkisuudesta annettua lakia (621/1999, Julkisuuslaki) sekä kielilakia (423/2003). Tiedonhallintalain 3 §:n 4 momentin nojalla arviointilaitosten tulee myös soveltaa Tiedonhallintalain 4 lukua (tietoturvallisuus) sekä 25-28 §:ää Arviointilaitoslaissa tarkoitettuja tehtäviä hoitaessaan.

Traficomin hyväksymä tietoturvallisuuden arviointilaitos voi hoitaa myös muita kuin Arviointilaitoslaissa tarkoitettuja arviointitehtäviä.[14] Hyväksytyn arviointilaitoksen onkin sopiessaan palveluidensa tarjoamisesta varmistuttava asiakkaaltaan, haluaako se Traficomin hyväksymän arviointilaitoksen palvelun vai arviointilaitosstatuksen ulkopuolisen palvelun[15]. Yksityisen sektorin yrityksellä on mahdollisuus valita joko Traficomin hyväksymän arviointilaitoksen palvelu tai sen ulkopuolinen palvelu. Viranomaiset saavat kuitenkin käyttää tietojärjestelmätarkastuksissaan vain Traficomia tai sen hyväksymää arviointilaitosta[16], joten kun kyseessä on viranomaisen tietojärjestelmän arviointi, tulee aina valita hyväksytyn arviointilaitoksen palvelu. Arviointilaitoksen vastuulla on tiedottaa asiakastaan asianmukaisesti niin, että asiakas tietää, onko se ostamassa Traficomin hyväksymän tietoturvallisuuden arviointilaitoksen palvelua vai jotakin muuta.

Arviointilaitoslaki samoin kuin Traficomin ohje tietoturvallisuuden arviointilaitoksille koskevat vain sellaisia palveluita, joita arviointilaitokset tuottavat Traficomin hyväksymän arviointilaitoksen roolissa.

---

[14] Akkreditoinnin ja Traficomin hyväksynnän edellytyksenä on kuitenkin toiminnallinen ja taloudellinen riippumattomuus.
[15] Esimerkiksi FINAS:in akkreditoimana sertifiointielimenä tehtävä ISO 27001 -arviointi, jota tarjotaan yksityisen sektorin yritykselle, joka ei käsittele viranomaisen salassa pidettävää tietoa.
[16] Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 3 §.

3.2 Arviointikriteeristöt

3.2.1 Vahvistettuun standardiin perustuvat tietoturvallisuusvaatimukset

ISO/IEC 27001 -standardi sisältää vaatimukset tietoturvallisuuden hallintajärjestelmille. ISO/IEC 27001 -standardin soveltamisessa ja standardiin liittyvissä arvioinneissa voidaan käyttää apuna muita ISO/IEC 27000 -sarjan standardeja.

3.2.2 Katakri - tietoturvallisuuden auditointityökalu viranomaisille

Katakri on kansallisen turvallisuusviranomaisen (NSA, National Security Authority) julkaisema auditointityökalu viranomaisten salassa pidettävien tietoaineistojen käsittelykyvyn arvioimiseksi. Katakrin vaatimukset on koottu niin, että niistä muodostuu riittäväksi arvioitu kokonaisuus kansallisten tai kansainvälisten salassa pidettävien tietojen suojaamiseksi oikeudettomalta paljastumiselta ja käsittelyltä.[17]

Katakria voidaan käyttää auditointityökaluna silloin, kun tarkoituksena on todentaa, täyttävätkö viranomaisten tai yritysten tietojärjestelmät ja toiminta niiltä edellytettävät kansalliset tai kansainväliset tietoturvavaatimukset.

Arviointilaitoksilla ei kuitenkaan ole toimivaltaa arvioida sellaisia viranomaisten tietojärjestelmiä, joissa käsitellään EU:n tai NATO:n turvallisuusluokiteltua tietoa.

3.2.3 Julkri - julkisen hallinnon tietoturvallisuuden arviointikriteeristö

Tiedonhallintolautakunnan antamassa suosituksessa kuvataan julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)[18], ja ohjeistetaan sen käytöstä. Julkria voidaan käyttää apuna arvioitaessa Tiedonhallintalaissa, turvallisuusluokitteluasetuksessa[19] sekä osin myös tietosuoja-asetuksessa[20] säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä.

Tietoturvallisuuden arviointilaitoksille ei ole toistaiseksi ollut mahdollista hakea Julkria pätevyysalueeksi, koska sen osalta ei ole selkeästi määritelty vaatimuksia täsmentävää, tulkintaohjeita ja muuta neuvontaa antavaa tahoa, joka määrittelisi kriteerien mukaisen riittävän käytännön ja

[17] Katakrin keskeisin kansalliseen lainsäädäntöön kuuluva vaatimuslähde on ollut valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010), joka on kumoutunut 1.1.2020. Kansainvälisenä lähteenä on käytetty ensisijaisesti EU:n neuvoston turvallisuussääntöjä (2013/488/EU).
[18] Valtiovarainministeriön julkaisuja 2023:46
[19] Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019)
[20] EU:n yleinen tietosuoja-asetus (EU) 2016/679

arvioinneissa todentamiseen käytettävät menetelmät, joiden avulla voitaisiin varmistaa kriteeristön yhdenmukainen, tasapuolinen ja vertailukelpoinen käyttö.

3.3 Arviointimenettelyn vaiheet

Arviointitoiminnan tarkoituksena on tuottaa arvioinnin toimeksiantajalle tieto arvioinnin kohteen vaatimustenmukaisuudesta. Arvioinnissa selvitetään, onko arvioinnin kohteen toiminnassa asianmukaisella tavalla toteutettu tietoturvallisuutta koskevat vaatimukset, jotka on otettu selvityksen perustaksi.

3.3.1 Toimeksianto

Tietoturvallisuuden arviointimenettely käynnistyy aina toimeksiannosta. Toimeksianto tarkoittaa arvioinnin suorittamista ISO/IEC 17021 standardin mukaisella menettelyllä[21]. Arvioinnin lopputuloksena arviointilaitos toteaa, täyttyvätkö arvioinnin perustana olevat vaatimukset. Todistuksen voi antaa vain, jos vaatimukset täyttyvät.

Lähtökohtaisesti Katakri-arvioinneissa arviointitoimeksiannolla tarkoitetaan yksittäisen arvioinnin suorittamista. Tällöin toimeksiantoon ei liity esimerkiksi määräaikaistarkastusta. Toisaalta toimeksiantaja ja arviointilaitos voivat sopia myös laajemmasta arviointipalvelusta esimerkiksi koskien laajempaa arviointiohjelmaa, seurantatoimia ja uudelleenarviointeja. Jos arviointilaitos myöntää arvioinnin perustella todistuksen, todistus on voimassa korkeintaan kolme vuotta[22]. Todistuksen voimassaoloa voidaan jatkaa, jos kohde täyttää kriteerit uuden arvioinnin perusteella.

Viranomaisen tietojärjestelmää tai tietoliikennejärjestelyä koskevan arviointipyynnön tekee viranomainen, jonka määräämisvallassa tai hankittavaksi suunnittelema järjestelmä on. Määräämisvallalla tarkoitetaan, että järjestelmä on viranomaisen käytettävissä esimerkiksi käyttöoikeussopimuksen perusteella ja jos viranomainen on oikeutettu määräämään sen käytöstä, tietojen luovuttamisesta ja muusta tiedonkäsittelystä. Viranomaisen tietojärjestelmää koskevan arviointipyynnön voi tehdä myös se, joka tarjoaa sellaisia

[21] ISO 17021 liite E Kolmannen osapuolen auditointi- ja sertifiointiprosessi. Seuranta-auditoinnit ja uudelleenarvioinnit suoritetaan Katakri-arvioinneissa, mikäli tästä erikseen osapuolten välillä sovitaan.
[22] Poikkeuksena Toisiolain (552/2019) 26 §:n 3 momentin mukaan arviointilaitoksen myöntämä todistus voi olla voimassa enintään 5 vuotta.

tietojenkäsittelypalveluja, joita käytetään yleisesti valtionhallinnon eri viranomaisissa, kun viranomainen antaa tähän valtuutuksen.

Arviointilaitoksen tulee laatia kirjallinen sopimus tietoturvallisuuden arviointitehtävästä arvioinnin toimeksiantajan kanssa. Sopimuksessa on sovittava ainakin arvioinnin kohteesta ja mahdollisista kohdetta koskevista rajauksista, sovellettavasta arviointiperusteesta ja arviointikriteeristöstä, turvallisuusluokasta, arvioinnin laajuudesta ja kestosta, toimeksiantajalle luovutettavasta arviointiraportista ja muusta asiakirja-aineistosta sekä arviointitehtävästä perittävästä maksusta.

Arviointilaitoslain 9 §:n 2 momentin mukaan arviointi voidaan tehdä myös osittaisena. Näin ollen on mahdollista tehdä arviointi esimerkiksi vain Katakrin F-osaa vasten. Arvioinnin osittaisuus tulee kuitenkin selkeästi ilmaista tehdyssä raportissa sekä mahdollisessa todistuksessa.[23] Osittaisen arvioinnin perusteella ei voi saavuttaa yleispätevää Katakri -kelpoisuutta.

Arviointilaitoksen on varmistuttava toimeksiantosopimuksessa siitä, että laitoksella on oikeus saada riittävät tiedot ja pääsy tarvittaviin tiloihin arviointitehtävän suorittamiseksi. Arviointilaitoksen on lisäksi varmistuttava, että arviointiin liittyvät tiedot ovat riittävässä määrin arviointilaitoksen ja Traficomin saatavilla myös arviointitehtävän päättymisen jälkeen. Arviointilaitoksen on varmistettava, että keskeiset arviointitulokseen vaikuttavat todistusaineistot ovat saatavilla Katakri-arvioinneista 6 vuotta arviointitapahtuman päättymisen jälkeen.

3.3.2 Kansainväliset tietoturvallisuusvelvoitteet ja yritysturvallisuusselvitykset

Arviointilain 3 §:n perusteella valtionhallinnon viranomaisen tulee hankkia tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arviointi Traficomilta tai hyväksytyltä tietoturvallisuuden arviointilaitokselta. Tämä soveltuu kansallisen turvallisuusluokitellun tiedon suojaamisen arviointiin.

Arviointilaitokset eivät sen sijaan voi itsenäisesti hoitaa kansainvälisten tietoturvallisuusvelvoitteiden tai yritysturvallisuusselvitysten edellyttämiä arviointitehtäviä, sillä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004, Kv-titulaki) 4 §:ssä ja Turvallisuusselvityslain 9 §:ssä tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioiminen säädetään Traficomin tehtäväksi.

Kansainväliset tietoturvallisuusvelvoitteet voidaan jakaa kahteen päätyyppiin:

[23] Ks. kohta 3.3.5 todistuksen antamisesta.

- EU:n neuvoston ja Naton turvallisuussääntöjen mukaiset tietoturvallisuusvelvoitteet ja
- valtioiden kahdenvälisten tietoturvallisuussopimusten (GSA, General Security Agreement) mukaiset velvoitteet.

Yhteistä näille on se, että ne ovat Suomessa lainsäädäntönä sovellettavia velvoitteita ja tarkentavat Kv-titulain sääntelyä.

Arviointilaitokset eivät voi arvioida sellaisia tietojärjestelmiä, joissa käsitellään Naton, EU:n tai ESA:n[24] turvallisuusluokiteltua tietoa. EU:n (ml. ESA:n) tai Naton turvallisuusluokitellun tiedon sähköinen käsittely edellyttää aina toimivaltaisen viranomaisen tekemää arviointia ja hyväksyntälausuntoa. Näihin arviointeihin liittyy yleensä myös EU:n tai Naton turvallisuussääntöihin sisältyvien turvallisuusluokiteltujen vaatimusten käsittelyä.

Arviointilaitos ei voi arvioida valtioiden välisen turvallisuusluokitellun tiedon vaihtamiseen tarkoitettua tiedonsiirtoyhteyttä. Kahdenvälisissä tietoturvallisuussopimuksissa Traficomin viranomaistehtävät liittyvät yleensä valtioiden rajat ylittävään tietojärjestelmäosuuteen, joka koostuu tyypillisesti sähköisestä tiedonsiirtoratkaisusta ja siihen liittyvästä yhdyskäytäväratkaisusta.

Sen sijaan arviointilaitos voi mahdollisesti arvioida kansallista tietojärjestelmää, joka on liitetty edellisessä kappaleessa kuvattuun valtioiden väliseen tiedonsiirtoyhteyteen tai jossa muutoin käsitellään toisen valtion turvallisuusluokiteltua tietoa. Näihin sovelletaan yleensä tietoturvallisuussopimusten perusteella vastavuoroisuusperiaatetta. Vastavuoroisuusperiaatteella tarkoitetaan sitä, että toisesta valtiosta saadut turvallisuusluokitellut tiedot on suojattava samalla tavalla kuin vastaavan kansallisen turvallisuusluokan tiedot. Arviointilaitoksen arviointi olisi tällöin tehtävä samalla tavalla kuin vastaavan turvallisuusluokitellun tiedon käsittelyn arviointi eli esimerkiksi TL IV mukaisesti Katakrin perusteella.

Kahdenvälisiin tietoturvallisuussopimuksiin ja niiden nojalla sovittuihin hankkeisiin voi kuitenkin liittyä tapauskohtaisia erityispiirteitä. Siksi tällaisissa toimeksiannoissa on tarpeen varmistua siitä, ettei arviointilaitoksen arvioinnille ole estettä. Asiasta on hyvä olla yhteydessä Traficomiin ja Traficom selvittää asian tarvittaessa yhteistyössä toimeksiantajan kanssa.

Yritysturvallisuusselvitys voidaan tehdä kansainvälisen tietoturvallisuusvelvoitteen tai kansallisen tarpeen vuoksi. Pääsääntöisesti

[24] European Space Agency

yritysturvallisuusselvitys tarvitaan TL III tai sitä vastaavan turvallisuusluokan tiedonkäsittelyyn. Sähköisen käsittelyn tietoturvallisuuden arvioinnin tekee Turvallisuusselvityslain 9 §:n mukaan Traficom. Traficom voi käyttää oman arviointinsa osana eli pohjamateriaalina arviointilaitoksen pätevyytensä puitteissa tekemää arviointia, jos kysymys on kansallisen turvallisuusluokitellun tiedon käsittelystä tai vastavuoroisiin velvoitteisiin perustuvasta toisen valtion turvallisuusluokitellun tiedon käsittelystä. Traficom vastaa arvioinnista, mutta voi parhaimmillaan merkittävästi hyödyntää arviointilaitoksen tekemää arviointia.

Traficom voi käyttää arviointilaitoksen tekemää arviointia esimerkiksi, jos yritys haluaa liittää arviointilaitoksen arvioiman erillisen tietojärjestelmän yritysturvallisuusselvityksen kattamaan tietojärjestelmään/ tietojenkäsittely-ympäristöön ja osaksi yritysturvallisuusselvitystä.

EU:n ja Naton turvallisuusluokitellun tiedon sähköisen käsittelyn arviointi on yritystenkin tapauksessa yksinomaan Traficomin tehtävä.

Arviointiprosessia kansainvälisissä tietoturvallisuusvelvoitteissa ja yritysturvallisuusselvityksissä kuvataan Liikenne- ja viestintäviraston ohjeessa tietojärjestelmien arviointi- ja hyväksyntäprosesseista.[25]

3.3.3 Arvioinnin perustaksi otettujen tietoturvallisuutta koskevien vaatimusten toteutuminen

Kun arviointikriteeristönä käytetään Katakria, arviointi suoritetaan noudattaen luvun 3.3 "Arvioinnissa sovellettava menettely" mukaisia vaatimuksia. Arviointilaitoksen on arvioinnissaan tarkastettava kohteen toimitilat tai varmistuttava, että toimivaltainen viranomainen (suojelupoliisi tai pääesikunta) tai toinen hyväksytty arviointilaitos on ne tarkastanut. Arvioinnin perusteella annettavaa todistusta ei voida antaa ilman asianmukaista toimitilojen tarkastamista.

Tietyissä tietoturvallisuutta koskevissa yksittäisissä vaatimuksissa voi olla tarpeen hyödyntää Traficomin tekemää arviointia ja lausuntoa tai hyväksyntää, koska arviointilaitoksella ei ole pätevyyttä arvioida vaatimuksen täyttymistä. Tämä koskee erityisesti salaustuotteiden, yhdyskäytäväratkaisujen ja hajasäteilyä koskevien vastatoimien (TEMPEST)

[25] Ks. Liikenne- ja viestintäviraston ohje tietojärjestelmien tietoturvallisuuden arviointi- ja hyväksyntäprosesseista (Dnro TRAFICOM/1061/09.04.00/2023, 3.4.2025), kohta 4.1 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohje-tietojarjestelmien-arviointi-ja-hyvaksyntaprosesseista-2025.pdf

osalta[26]. Arvioinnin kohteen on hyvä hankkia Traficomin arviointi etukäteen tietojärjestelmän arviointia varten. Arvioinnissa arviointilaitos toteaa, että arviointi on haettu ja että kohteen toiminta vastaa Traficomin lausunnon vaatimuksia ja ehtoja (esim. salaustuotteen käyttöä koskevat ehdot).

Salaustuotteiden kohdalla arviointilaitos arvioi ensin kohteen uhkatason. Mikäli salausratkaisu on olennaisesti tiedon turvallisuuden tuottava komponentti, on uhkataso korkea. Kun salausratkaisu ei ole olennaisesti tiedon turvallisuuden tuottava komponentti, on uhkataso matala.

Matala uhkataso

Matalan uhkatason ympäristöissä arviointilaitos voi tehdä riskiarvion perusteella arvion salausratkaisun ja fyysisen turvallisuuden kokonaisuudesta ja arvioida järjestelmäkohtaisen toteutuksen.

Korkea uhkataso

Korkean uhkatason ympäristössä salausratkaisulle on tarpeen saada erillinen lausunto.

Arviointilaitos voi arvioida salausratkaisun riittävyyden, mikäli kansallista tietoa käsiteltäessä käytetyllä salausratkaisulla on Traficomin, tai sellaisen arviointilaitoksen jolla on salaustuotearviointipätevyys[27], lausunto vaatimusten täyttymisestä ja käyttö on toteutettu käyttöpolitiikan mukaisesti.

Mikäli salausratkaisulla ei ole Traficomin, tai sellaisen arviointilaitoksen jolla on salaustuotearviointipätevyys, lausuntoa vaatimusten täyttymisestä tai ratkaisua käytetään käyttöpolitiikan vastaisesti, toimitaan toisella seuraavista tavoista:

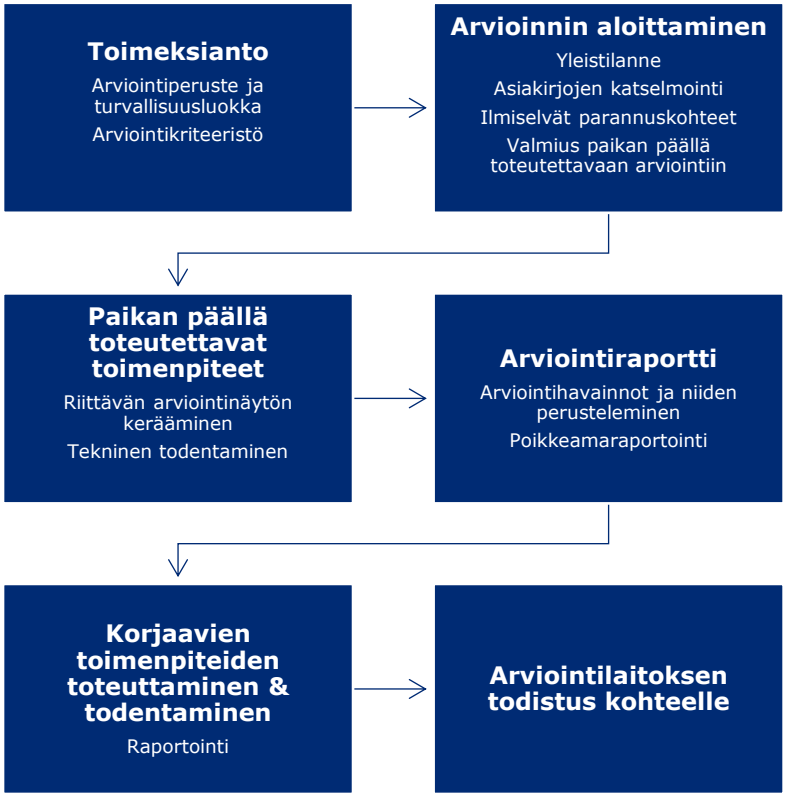
1) Mikäli suojattava tieto on korkeintaan TL IV ja arviointilaitoksella on salaustuotteiden arviointiin vaadittava pätevyys, voi se tehdä tapauskohtaisen arvioinnin itse.

2) Mikäli arviointilaitoksella ei ole salaustuotteen arviointiin vaadittavaa pätevyyttä tai suojattava tieto on vähintään TL III, arviointilaitoksen on tehtävä tapauskohtainen lausuntopyyntö (aiemmin pikapyyntö tai CAA-pikaprosessi) Traficomille.

[26] Traficomin NCSA-toiminnon hyväksymät salausratkaisut, yhdyskäytäväratkaisuohje ja sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet ks. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa.
[27] Ks. kohta 3.5.

3.3.4 Arvioinnissa sovellettava menettely

Tietoturvallisuuden arviointimenettelyssä noudatetaan standardien ISO/IEC 17021 ja ISO/IEC 27006 mukaisia prosessivaatimuksia soveltuvin osin. Arviointimenettelyssä voidaan käyttää myös standardien ISO 19011 ja ISO/IEC 27007 mukaisia menettelyitä[28].



Kuva 1. Esimerkki tietoturvallisuuden arvioinnin etenemisestä

3.3.5 Arviointiraportti ja muut arviointiin liittyvät asiakirjat

Tietoturvallisuuden arvioinnista ja suoritetuista tarkastuksista on laadittava arviointiraportti noudattaen standardien ISO/IEC 17021 ja ISO/IEC 27006 vaatimuksia. Katakri-arvioinneissa arviointiraporttiin on aina liitettävä vaatimustaulukko arviointituloksineen ja perusteluineen. Raportissa ja sen liitteenä olevassa vaatimustaulukossa on perusteltava riittävän kattavasti tehdyt havainnot sekä se, millä perusteilla yksittäinen asiakohta on hyväksytty tai hylätty. Traficom antaa arviointilaitosten käyttöön raporttipohjan Katakri-arviointeja varten.

Arviointilaitoksen on dokumentoitava arviointitehtävän suorittamisen yhteydessä syntyvä asiakirja- ja todistusaineisto riittävällä tarkkuudella

[28] ISO 19011:2018 "Guidelines for auditing management systems"/ SFS-EN ISO 19011:2018 "Johtamisjärjestelmän auditointiohjeet", ISO 27007 Guidelines for information security management systems auditing.

siten, että arvioinnissa tehdyt havainnot voidaan todentaa jälkikäteen. Arviointilaitoksen tulee myös varmistua asiakirja- ja todistusaineiston saatavuudesta havaintojen myöhempää todentamista varten.[29]

3.3.6 Todistuksen antaminen

Arviointilaitoksen tulee antaa arvioinnin kohteelle todistus, jos kohteen toimitilat ja toiminta ovat arvioinnin perustana olleiden tietoturvallisuusvaatimusten mukaiset. Jos kaikki vaatimuskriteerit eivät täyty, ei todistusta voi myöntää.

Todistuksen myöntämisen edellytyksenä on, että arviointi on suoritettu tietojärjestelmässä siten, että se on kohdistunut tietojärjestelmään tai sen osaan, joka on tietoturvallisesti erotettavissa muista tietojärjestelmistä tai niiden osista. Toisin sanoen arvioinnin kohteen rajauksen tulee olla sellainen, että kohde muodostaa kokonaisuuden, joka on kyseiselle turvallisuusluokalle riittävän luotettavilla rajapinnoilla erotettu arvioinnin ulkopuolelle jäävistä tietojärjestelmistä.[30]

Katakrin rakenteen vuoksi todistus on mahdollista myöntää osittaisesta Katakri-arvioinnista vain joko T-osiosta tai T+F -osioista. Pelkän F- tai I-osion arvioinnin perusteella ei ole mahdollista myöntää todistusta.

Todistuksen osalta tulee huomioida, että arvioinnin tilaajalla saattaa usein olla tarpeita jakaa sitä eteenpäin omille asiakkailleen tai muille sidosryhmille, jonka takia todistukseen tulevien tiettyjen tietojen osalta (esim. arvioidun tietojärjestelmän käyttöpaikan osoitetiedot) tulee sopia tapauskohtaisesti toimeksiantajan kanssa, millä tarkkuudella tiedot voi kirjata todistukseen. Salassa pidettävät asiat on syytä jättää erilliselle todistuksen liitteelle.

Traficomin viranomaisnäkökulmasta arviointilaitosten Arviointilaitoslain perusteella antamat todistukset, samoin kun tiedot niiden olemassaolosta, voivat usein olla salassa pidettävää tietoa. Todistuksen saajan tulisi omien tarpeidensa perusteella arvioida missä tapauksissa todistusta tai sen tietoja voidaan jakaa eteenpäin. Arviointilaitosten tekemien sote-arviointien osalta todistuksiin liittyy tarkempia vaatimuksia, joita laitosten tulee noudattaa.[31]

Todistuksessa on oltava vähintään seuraavat tiedot:

- Kenelle todistus on myönnetty

[29] Arviointilaitoksen on varmistettava että keskeiset arviointitulokseen vaikuttavat todistusaineistot ovat saatavilla 6 vuotta arviointitapahtuman päättymisen jälkeen.
[30] Ks. myös kohta 3.4.1.5 rajauksesta.
[31] Ks. L3.1.4., L3.1.5 ja L3.2.2 sote-arviointien osalta.

- Arvioinnin laajuus (kohteen rajaus ja yksilöinti, erilliselle liitteelle tietojärjestelmän käyttöpaikka ja muut mahdolliset salassapidettävät asiat ja pitkät kuvaukset)
- Tietoturvallisuuden arviointiperusteet eli arviointikriteeristö
- Sovellettu tietoturvallisuustaso
- Todistuksen myöntämispäivä
- Viimeinen voimassaolopäivä
- Sitoumus: "Arvioinnin kohteen tulee ilmoittaa todistuksen antajalle kaikista niistä arvioinnin kohdetta koskevista muutoksista, joilla voi olla vaikutusta tietoturvallisuusvaatimusten täyttymiseen. Arvioinnin kohde sitoutuu siihen, että tietojärjestelmän tietoturvallisuustaso säilyy samana kuin arvioinnin aikaan."
- Laki tietoturvallisuuden arviointilaitoksista 9 §
- Pääauditoijan allekirjoitus ja nimenselvennys
- Todistuksen myöntäjä (arviointilaitoksen nimi ja y-tunnus)

Lisäksi arviointilaitos voi ilmoittaa muitakin tietoja todistuksella.[32]

Arviointilaitoksen tulee asettaa todistuksen voimassaololle päättymispäivä. Todistus voi olla voimassa korkeintaan kolme vuotta.[33]

3.3.7 Arviointia koskevien tietojen julkaiseminen

ISO/IEC 17021-standardiin sisältyy vaatimuksia julkisesti saataville asetettavista tiedoista (kohta 8.1.2)[34]. Kuitenkin viranomaisasiakkaiden osalta tällaiset tiedot ovat asetettavissa julkisesti saataville vain, jos viranomainen, jonka pyynnöstä arviointi on tehty, on antanut tähän kirjallisen suostumuksen. Myös standardin em. kohdan mukaan asiakkaan pyynnöstä pääsyä tiettyihin tietoihin voidaan poikkeustapauksissa rajoittaa (esimerkiksi turvallisuussyistä).

Hyväksytyn tietoturvallisuuden arviointilaitoksen tulee noudattaa kaikessa arviointejaan koskevan tiedon luovuttamisessa tai julkistamisessa viranomaisasiakkaansa tekemää määrittelyä tiedon julkisuudesta tai salassapidosta. Julkisuuslain vaatimukset ovat hyväksytyn tietoturvallisuuden arviointilaitoksen toiminnassa etusijalla standardeihin nähden.

---

[32] Muu tieto voi olla esimerkiksi tieto siitä, että arvioinnin yhteydessä on tehty laajempaa arviointia käyttäen muitakin kuin vaatimuksenmukaisia todentamismenetelmiä. Lisäksi riippuen arvioitavasta järjestelmästä tulee tarvittaessa ottaa huomioon sote-arviointeihin liittyvät omat vaatimukset (Ks. L3.1.4., L3.1.5 ja L3.2.2).
[33] Toisiolain (552/2019) 26 §:n 3 momentin mukaan arviointilaitoksen myöntämä todistus voi olla voimassa enintään 5 vuotta.
[34] ISO/IEC 17021-1:2015, kohta 8.1.2.

Arviointilaitoslain 13 a §:n mukaan Traficom merkitsee turvallisuusselvitysrekisteriin tiedot hyväksytyistä arviointilaitoksista samoin kuin arviointilaitokselle annettuun todistukseen merkityt tiedot. Hyväksytty arviointilaitos voi ilmoittaa Traficomille turvallisuusselvitysrekisteriin merkitsemistä ja siitä edelleen luovuttamista varten tiedot arvioimastaan kohteesta ja sille annetun todistuksen sisällöstä, jollei arvioinnin kohde ole sitä kieltänyt. Arvioinnin kohteelle on ennen ilmoituksen tekemistä annettava tieto tietojenkäsittelyn tarkoituksesta ja sitä koskevasta sääntelystä.

3.3.8 Seurantatoimenpiteet

Jos arviointilaitos myöntää arvioinnin kohteelle todistuksen tietoturvallisuusvaatimusten täyttymisestä, on todistuksessa edellytettävä arvioinnin kohdetta ilmoittamaan kaikista niistä arvioinnin kohdetta koskevista muutoksista, joilla voi olla vaikutusta tietoturvallisuusvaatimusten täyttymiseen sekä sitoutumaan siihen, että tietojärjestelmän tietoturvallisuustaso säilyy samana kuin arvioinnin aikaan. Kun arviointilaitos saa ilmoituksen muutoksesta, jonka johdosta arvioinnin kohde ei enää täytä niitä vaatimuksia, jotka on otettu arvioinnin perustaksi, sen on kuultava todistuksen haltijaa ja varattava sille tilaisuus korjata puutteet. Jos puutteita ei kohtuullisessa ajassa korjata, arviointilaitoksen on peruutettava todistus. Arviointilaitoksen tulee ilmoittaa todistuksen peruuttamisesta arvioinnin toimeksiantajalle ja Traficomille.

Muista seuranta- ja uudelleenarviointitehtävistä arviointilaitos vastaa toimeksiannon perusteella.

3.4 Arviointimenetelmät

3.4.1 Yleisiä arviointitoiminnassa huomioitava periaatteita

3.4.1.1 Asiakkaan tietojen suojaaminen tarkastustoiminnassa

Asiakkaan suojattavien tietojen käsittelyssä on täytettävä Katakrissa kuvatut suojausvaatimukset koko tiedon elinkaaren ajan. Tekniseen tarkastamiseen liittyen tulee erityisesti huomioida

- tiedon erottelu / asiakaskohtainen dedikointi[35],
- tarkastuslaitteiston eheys ja mittaustiedon luotettavuus, sekä
- tietojen kuljettamis- ja säilyttämiskäytännöt.

[35] Asiakkaan verkkoon voi kytkeä vain laitteiston, joka ei sisällä muiden asiakkaiden tietoja.

3.4.1.2 Tarkastuslaitteiston eheys ja mittaustiedon luotettavuus

Tarkastuslaitteiston tuottaman mittaustiedon luotettavuudesta on pystyttävä varmistumaan. On varmistettava erityisesti, että

- laitteisto alustetaan jokaiseen tarkastuskäyntiin luotettavasta lähteestä, ja
- mittaustiedon tulosten oikeellisuus tarkastetaan useammasta lähteestä[36].

3.4.1.3 Kasautumisvaikutuksen arviointi

Kasautumisvaikutuksella tarkoitetaan ilmiötä, jossa suuresta määrästä tietyn turvallisuusluokan tietoa koostuvissa tietojärjestelmissä asiakokonaisuus nousee luokitukseltaan usein yksittäistä tietoa korkeampaan turvallisuusluokkaan. Tyypillisesti kasautumisessa on kysymys IV-tason tiedosta (esimerkiksi suuri määrä TL IV tietoa voi muodostaa yhdistettynä TL III tietovarannon).

Kun kohteen keskeisen tietovarannon turvallisuusluokka tulkitaan kasautumisvaikutuksesta johtuen yksittäisten tietoalkioiden luokkaa korkeammaksi, tulee tietovarannon määritellyt suojausmenetelmät toteuttaa korkeamman turvallisuusluokan vaatimusten mukaisesti. Määritellyillä suojausmenetelmillä tarkoitetaan menetelmiä, joilla rajataan pääsy vain tehtävässä tarvittavaan yksittäiseen tai suppeaan osaan tietosisällöstä, ja joilla yritykset päästä valtuuttamattomasti laajempaan osaan tietosisällöstä havaitaan.

Kun arviointityökaluna käytetään Katakria, tulee kasautumisvaikutus tulkita siten, että tietovarannon suojauksilta edellytetään korkeamman tason mukaisena tietovarannon fyysisen turvallisuuden lisäksi kohtia I-13 (sovelluskerroksen turvallisuus), I-10 ja I-11 (jäljitettävyys ja havainnointikyky) sekä I-06 (tehtävien eriyttäminen). Onkin huomioitava, että kasautumisvaikutuksen seurauksena yhdellä luokalla noussut tietovarannon turvallisuusluokka ei edellytä hyväksyttävää yhdyskäytäväratkaisua tietovarannon (esim. TL III) ja päätelaitteiden (esim. TL IV) välille.

3.4.1.4 Sovellettavat uhkamallit

Turvallisuusluokan IV järjestelmät on suojattava yleisiltä matalan tai keskitason resursseilla ja/tai osaamisella varustettujen hyökkääjien uhkia

[36] Esimerkiksi päivityskäytäntöjen toteutus tulee todentaa vähintään henkilöstöä haastattelemalla, prosessikuvauksiin (tai vast.) tutustumalla, päivitystason tutkinnalla järjestelmän "sisältä päin" (esim. tarkastamalla turvapäivitysten asennusaikaleimat itse järjestelmästä) sekä suorittamalla kohteeseen ulkoa päin haavoittuvuusskannaus.

vastaan. Esimerkiksi julkisesta verkosta saavutettavat etäkäyttöratkaisujen terminointipisteet on pidettävä tiukasti julkaistujen turvapäivitysten tasolla, ja julkaistujen nollapäivähaavoittuvuuksien hyödyntäminen on estettävä muilla keinoin[37].

Turvallisuusluokan III järjestelmät on suojattava merkittävimmillä resursseilla ja/tai osaamisella varustettujen hyökkääjien uhkia vastaan. Esimerkiksi turvallisuusluokan III tiedon käsittely on rajattava hyväksyttyihin vaatimukset täyttäviin fyysisiin toimitiloihin.

3.4.1.5 Rajausten määrittely

Tietoa tulee suojata vaatimusten mukaisesti koko sen elinkaaren ajan kaikissa siihen kohdistuvissa käyttötapauksissa ja käyttöympäristöissä. Esimerkiksi työaseman tarkastuksessa on huomioitava työaseman ensiasennuksen, päivitys- ja muutoshallinnan, käytöstä poiston prosessien toteutukset, sekä lisäksi käyttötapaukset eri käyttöympäristöissä (esimerkiksi etätyö). Viranomaishyväksyntään tai arviointilaitoksen myöntämään todistukseen tähtäävissä tarkastuksissa edellytetään tarkastuksen rajauksen ulottamista kaikkiin ympäristöihin, missä suojattava tieto käy elinkaarensa aikana hyväksynnän/todistuksen piiriin haettavissa käyttötapauksissa. Jos tarkastuksen kohteena on esimerkiksi viraston A tiedonhallintajärjestelmä, tarkastuksen rajaukseen on sisällyttävä tiedonhallintajärjestelmän lisäksi kaikki työasemat ja verkot, joista kyseessä olevaa tiedonhallintajärjestelmää käytetään tai joista pystytään muuten vaikuttamaan kyseessä olevan tiedon suojauksiin. Traficom ohjeistaa arviointilaitoksia yksityiskohtaisemmin rajausmäärittelyistä eri tarkastustyypeissä ja käyttötapauksissa.

3.4.2 Hallinnolliselle todentamiselle asetettavat vähimmäisvaatimukset

Hallinnolliselle todentamiselle asetettavat vähimmäisvaatimukset on kuvattu taulukossa 1. Taulukossa listataan edellytettävät todennusmenetelmät sekä turvallisuusluokat, joille kyseessä olevia menetelmiä edellytetään

ID	Todennusmenetelmä	Luokat	Huomioitavaa
H1	Haastattelut	IV ja III	Kohteena soveltuvat henkilöt, tyypillisesti sisältäen johdon, ylläpidon/kehityksen ja loppukäyttäjien edustajat

[37] Esimerkiksi poistamalla haavoittuva komponentti käytöstä ennen kuin turvapäivitys on julkaistu ja saatu asennettua.

H2	Dokumentaatioon tutustuminen	IV ja III	Kattaen verkkokuvat, järjestelmäkuvaukset, prosessikuvaukset ja vastaavat

Taulukko 1. Hallinnollisen todentamisen vähimmäisvaatimukset

3.4.3 Tekniselle todentamiselle asetettavat vähimmäisvaatimukset

Tekniselle todentamiselle asetettavat vähimmäisvaatimukset on kuvattu taulukossa 2. Taulukossa listataan edellytettävät todennusmenetelmät sekä turvallisuusluokat, joille kyseessä olevia menetelmiä edellytetään.

ID	Todennusmenetelmä	Luokat	Huomioitavaa
T1	Passiivinen rajapinta-analyysi	IV ja III	Menetelmään sisältyy verkko-/järjestelmäkuvien rakentamiset sekä liikenneanalyysit.
T2	Järjestelmä-konfiguraatioiden turvallisuuden tarkastelu	IV ja III	Menetelmä kattaa kaikki kohteen turvallisuuteen vaikuttavat osakokonaisuudet[38].
T3	Aktiivinen rajapinta-analyysi	IV ja III	Menetelmään sisältyy porttiskannaukset, haavoittuvuusskannaukset (tunnetut haavoittuvuudet) sekä toimintavarmuustestaukset[39] (tuntemattomat haavoittuvuudet).
T4	Sovellusturvallisuuden tarkastelut järjestelmätyypeittäin	IV ja III	Menetelmä kattaa kohteen turvallisuuteen vaikuttavien sovelluskomponenttien tarkastelut, esimerkiksi web-sovellukset, Java-palvelin-/asiakasohjelmistot ja ERP-järjestelmien sisäiset pääsynhallintamekanismit.
T5	Salausratkaisujen turvallisuuden todentaminen	IV	Kohteissa, joissa käytetään Traficomin NCSA-toiminnon, tai sellaisen arviointilaitoksen jolla on

[38] Osakokonaisuuksia ovat tyypillisesti esimerkiksi palvelinten ja työasemien käyttöjärjestelmät sekä muut alustaan asennetut ohjelmistot, verkkolaitteiden konfiguraatiot, tietokantojen konfiguraatiot sekä muut järjestelmän turvallisuuteen vaikuttavat ohjelmistot.
[39] Toimintavarmuustestauksella tarkoitetaan tässä ohjeessa erityisesti virheellisen syötteen lähettämiseen (fuzz testing) perustuvaa koestusta. Toimintavarmuustestausta edellytetään vain turvallisuuden kannalta kriittisiin järjestelmäosiin. Tällaisia ovat esimerkiksi turvallisuusluokan III yhdyskäytäväratkaisut, eri verkkoteknologioiden väliset liityntärajapinnat sekä suurten tietomassojen pääsynhallintamekanismit (kasautumisvaikutus).

			salaustuotearviointipätevyys[40], hyväksymää salausratkaisua[41], todennetaan salausasetusten ja hallintakäytäntöjen turvallisuuden riittävyys suhteessa hyväksynnän yhteydessä määritettyyn käyttöpolitiikkaan. Tilanteissa, joissa kohteessa ei ole käytössä hyväksyttyä salausratkaisua, Traficomin NCSA-toiminto tai sellainen arviointilaitos jolla on salaustuotearviointipätevyys voi arvioida ratkaisun turvallisuuden tapauskohtaisesti.
		III	Kohteissa, joissa käytetään Traficomin NCSA-toiminnon hyväksymää salausratkaisua, todennetaan salausasetusten ja hallintakäytäntöjen turvallisuuden riittävyys suhteessa hyväksynnän yhteydessä määritettyyn käyttöpolitiikkaan. Tilanteissa, joissa kohteessa ei ole käytössä hyväksyttyä salausratkaisua, Traficomin NCSA-toiminto arvioi ratkaisun turvallisuuden tapauskohtaisesti.
T6	Käytettävyystestaukset (ml. kuormitustestaukset)	IV ja III	Käytetään vain järjestelmiin, joilla on korkeat käytettävyysvaatimukset (esim. ihmishenkiä suojaavat turvajärjestelmät). Kattaa tyypillisesti sovellusten stressitestit, palvelunestohyökkäyksen kestokykytestaukset sekä kohteen jatkuvuuden hallinnan / toimintavarmuuden menettelyjen arvioinnin.
T7	Fyysisen turvallisuuden suojausten todentamismenetelmät	IV ja III	Toteutus kansainvälisten turvallisuusluokiteltujen tietoaineistojen osalta suojelupoliisilla tai Pääesikunnalla.

[40] Ks. kohta 3.5
[41] Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat-salausratkaisut

T8	Yhdyskäytäväratkaisujen turvallisuuden testaukset	III	Kohteissa, joissa Traficomin Yhdyskäytäväratkaisuohjeen[42] luvussa 4 kuvattua luotettavana pidettävää yhdyskäytäväratkaisua, todennetaan toteutetun ratkaisun turvallisuuden riittävyys suhteessa Yhdyskäytäväratkaisuohjeessa kuvattuihin vaatimuksiin. Tilanteissa, joissa kohteessa ei ole käytössä em. ohjeen ko. luvun mukaista yhdyskäytäväratkaisua, Traficomin NCSA-toiminto voi tiettyjen ehtojen täyttyessä arvioida ratkaisun turvallisuuden tapauskohtaisesti.
T9	Poikkeamahavainnointi-kyvyn testaukset	IV ja III	Kattaa erityisesti suojattavan ympäristön sisällä tehtävien valtuuttamattomien toimien ja niiden yritysten havainnointikyvyn testauksen, sekä tapauskohtaisesti hyökkäystoimien jäljittelyyn[43] perustuvat menetelmät.
T10 (*)	Hajasäteilysuojausten (TEMPEST) todentaminen	III	Kattaa tyypillisesti tilan, laitteiston, koteloinnin tai/ja esimerkiksi laitteiston asennustavan hajasäteilysuojauksen riittävyyden arvioinnin. Edellytettävän hajasäteilysuojauksen taso vaihtelee käsiteltävän tiedon alkuperäisestä luovuttajasta (originator) ja tiedon turvallisuusluokasta.
T11 (*)	Luvattomien teknisten laitteiden olemassaolon todentaminen[44]	III	Tapauskohtainen soveltaminen, tyypillisesti tilan käyttötarpeen mukaisesti.
T12	Uhkatietojohdannaiset menetelmät	III	Tapauskohtainen soveltaminen, tyypillisesti painottuen turvallisuusluokkien II ja I ympäristöihin.

Taulukko 2. Teknisen todentamisen vähimmäisvaatimukset

Taulukossa 2 tähdellä (*) merkityt todentamismenetelmät on mahdollista ulkoistaa DSA-viranomaiselle. Tässä ohjeessa ei kuvata turvallisuusluokkien

[42] Traficomin ohje "Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista", 2.12.2021
https://kyberturvallisuuskeskus.fi/sites/default/files/media/file/Yhdyskaytavaratkaisuohje.pdf
[43] Engl. Adversary Emulation.
[44] Engl. Technical Surveillance Counter-Measures (TSCM).

II-I järjestelmien turvallisuuden tekniselle todentamiselle asetettavia lisävaatimuksia.

3.4.4 Todentamismenetelmät arviointikriteeristöjen käytössä

Katakri-arvioinneissa edellytetään tehtyjen havaintojen oikeellisuuden varmistamista useammasta soveltuvasta lähteestä (vrt. luku 3.4.1.2). Katakri-pätevyysaluetta haettaessa hakijan tulee pystyä osoittamaan, kuinka se tulee tarkastamaan kyseessä olevan arviointikriteeristön vaatimusten täyttymisen siten, että kukin vaatimus tulee todennettua riittävän luotettavasti. Arviointilaitoksen tulee Katakri-arvioinneissaan todentaa vaatimusten täyttymisen tila vähintään Traficomilla hyväksytettyjen, kyseistä arviointikriteeristöä koskevien todennusmenetelmien mukaisesti.

3.5 Tapauskohtainen salausratkaisujen arviointi

Arviointilaitoksen on mahdollista halutessaan täydentää olemassa olevaa turvallisuusluokitellun tiedon arviointipätevyyttä (Katakri 2020, TL IV) Traficomin antaman perehdytyksen ja tulkintaopastuksen avulla, niin että se kattaa myös salausratkaisujen arvioinnin ympäristöissä, joissa käsitellään enintään TL IV tietoa.

Salausratkaisujen arviointi edellyttää arviointilaitoslain mukaisesti tehtävää erillistä Traficomin hyväksyntäpäätöstä turvallisuusluokitellun tiedon arviointipätevyyden täydentämisestä. Arviointilaitoksen hyväksyntäpäätökseen lisätään tällöin tapauskohtaista salausratkaisujen arviointia koskevat ehdot, rajoitukset sekä muut vaatimukset.

Salausratkaisujen arviointipätevyyttä voi hakea vapaamuotoisella hakemuksella, joka toimitetaan turvasähköpostilla osoitteisiin arviointilaitokset[at]traficom.fi ja caa[at]traficom.fi.

Salausratkaisun arviointipätevyyteen liittyviä vaatimuksia:

- Arviointilaitoksella tulee olla Katakri 2020 TL IV -pätevyys
- Salausratkaisujen arvioinnissa tulee noudattaa voimassa olevaa Traficomin ohjetta (*Ohje salausratkaisun valinnan ja asetusten arvioinnista TLIV-tasolla, Dnro: Traficom/8316/09.04.07/2025)*
- Tapauskohtaisten salausratkaisujen arviointeja voivat arviointilaitoksissa tehdä vain ne työntekijät, jotka ovat osallistuneet säännöllisesti Traficomin arviointiviranomaisena tarjoamaan perehdytykseen. Traficom seuraa osallistumisia.

- Arviointilaitoksen tulee kuvata toimintaansa koskevassa ohjeistuksessa, miten se toteuttaa salaustuotteiden arviointitehtävät ja varmistaa arviointitehtäviin osallistuvien henkilöiden riittävän osaamisen, sekä pitää huolen siitä, että salausratkaisujen arviointeja koskevat ohjeet ja neuvot saavuttavat kaikki näihin arviointitehtäviin osallistuvat asiantuntijat.

- Arviointilaitosten tulee myös noudattaa salausratkaisujen arviointien raportoinneista annettavaa tarkempaa ohjeistusta.

3.6 Arviointilaitoksen suorittaman arvioinnin suhde Traficomin suorittamaan arviointiin ja ns. viranomaishyväksyntä

Viranomaishyväksynnällä tarkoitetaan vakiintuneesti Traficomin Arviointilain 8 §:n nojalla myöntämää todistusta tietojärjestelmälle, erotuksena tietoturvallisuuden arviointilaitoksen myöntämästä todistuksesta.

Traficomin tekemiä arviointeja on kuvattu yksityiskohtaisemmin Traficomin ohjeessa *Liikenne- ja viestintäviraston ohje tietojärjestelmien tietoturvallisuuden arviointi- ja hyväksyntäprosesseista* (Dnro TRAFICOM/1061/09.04.00/2023, 3.4.2025)[45]. Ohjeessa todetaan, että arviointilaitoslain antama todistus on lainsäädännön näkökulmasta yhtä pätevä kuin Traficomin antama, eikä arviointilaitoksen todistuksen lisäksi yleensä pitäisi olla tarvetta hakea Traficomin todistusta.

Arviointilaitoksen tekemän arvioinnin lisäksi ei siten ole tarpeen pyytää todistusta Traficomilta ja pääsääntöisesti Traficom ei tee päällekkäistä arviointia tai anna todistusta kohteesta, jonka arviointilaitos on jo arvioinut.

4 Arviointilaitoksen valvonta ja laadunhallinta

4.1 Arviointilaitosten ohjaus ja valvonta

Traficom ohjaa ja valvoo hyväksyttyjä tietoturvallisuuden arviointilaitoksia tavoitteinaan turvata laadukas ja luotettava tietoturvallisuuden arviointitoiminta sekä varmistaa laitosten yhdenmukaiset toimintatavat. Ohjauksen ja valvonnan keinoja ovat arviointilaitosten ohjeistaminen ja viranomaisneuvonta, hyväksymiseen liittyvien ehtojen ja rajoitusten asettaminen sekä arviointilaitosten toiminnan valvonta, jota voidaan

[45] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohje-tietojarjestelmien-arviointi-ja-hyvaksyntaprosesseista-2025.pdf

toteuttaa esimerkiksi laitoksen toimintaan ja tuotoksiin kohdistuvilla tarkastuksilla. Tarkastuksia voidaan tehdä määräaikaistarkastuksina ja viranomaishyväksyntään tulevien tai muiden kohteiden pistokoemaisena arvioimisena.

Arviointilaitoslain 7 §:ssä säädetään Traficomin tarkastusoikeudesta ja 6 §:ssä arviointilaitoksen hyväksymisen peruuttamisesta.

4.2 Arviointilaitoksen tiedonanto- ja ilmoitusvelvollisuus

Traficomin valvontatehtävän mahdollistamiseksi arviointilaitoksilla on tiedonanto- ja ilmoitusvelvollisuus koskien toimintaa, jota arviointilaitos on harjoittanut roolissaan Traficomin hyväksymänä arviointilaitoksena.

4.2.1 Vuosi-ilmoitus

Arviointilaitoksen tulee toimittaa vuosi-ilmoitus Traficomille. Vuosi-ilmoitus tehdään käyttäen Traficomin lomaketta ja se toimitetaan selkokielisenä turvasähköpostilla Traficomin kirjaamoon (kirjaamo[at]traficom.fi) ilmoitusvuotta seuraavan vuoden maaliskuun loppuun mennessä. Sähköpostiviestin otsikkokentässä tulee ilmoittaa arviointilaitoskohtainen vuosittainen diaarinumero.

4.2.2 Tilannekuvatiedot

Arviointilaitoksen tulee ilmoittaa tilannekuvaa arvioinneista, jossa kriteeristönä käytetään Katakria. Ilmoitukset tehdään Traficomin tilannekuvataulukkoa käyttäen.

Tilannekuvataulukko toimitetaan selkokielisenä turvasähköpostilla Traficomin kirjaamoon (kirjaamo[at]traficom.fi) kuukausittain, kunkin kuukauden ensimmäisen kokonaisen kalenteriviikon aikana. Sähköpostiviestin otsikkokentässä tulee ilmoittaa arviointilaitoskohtainen vuosittainen diaarinumero.

4.2.3 Arviointiraportit ja todistukset

Arviointilaitoksen tulee toimittaa Traficomille kopio Traficomin hyväksymänä arviointilaitoksena antamistaan arviointiraporteista ja mahdollisista todistuksista, kun kriteeristönä on käytetty Katakria. Samalla arviointilaitoksen tulee ilmoittaa Traficomille, saako todistuksen tiedot asiakkaan suostumuksella merkitä turvallisuusselvitysrekisteriin Arviointilaitoslain 13 a §:n mukaisesti.

Mikäli arviointilaitoksella on pätevyys arvioida tapauskohtaisia salausratkaisuja ja mikäli arviointilaitos on niitä tehnyt, tulee myös

salaustuotteen arviointiin liittyvät täytetyt salaustuotteen hyväksyntäpyyntölomakkeet sekä raportit toimittaa Traficomille.

Arviointiraporttien ja todistusten nimestä tulee käydä ilmi arvioinnin kohteeseen liittyvä yksilöivä tunniste (Projekti ID), jota käytetään myös tilannekuvataulukossa.

Arviointiraportit ja todistukset toimitetaan salattuna pakettina turvasähköpostilla Traficomin kirjaamoon (kirjaamo[at]traficom.fi) kuukausittain, kunkin kuukauden ensimmäisen kokonaisen kalenteriviikon aikana. Sähköpostiviestin otsikkokentässä tulee ilmoittaa arviointilaitoskohtainen vuosittainen diaarinumero.

Tiedon salauksessa käytetään Traficomin kanssa erikseen sovittuja menettelyjä. Salattu paketti voidaan toimittaa yhdessä tilannekuvataulukon kanssa.

Arviointiraportteja voidaan toimittaa myös USB-medialla, henkilökuriirilla tai useammin kuin kerran kuukaudessa, mikäli siihen on perusteltu syy.

4.2.4 Muutostiedot

Traficomin hyväksymän arviointilaitoksen on ilmoitettava Traficomille sellaisesta toimintaansa koskevasta muutoksesta, jolla on merkitystä laitosta koskevien velvoitteiden, hyväksyttyjen toimintatapojen tai muiden hyväksyntään liittyvien ehtojen kannalta.

Suunnitelluista muutoksista tulee ilmoittaa etukäteen sen arvioimiseksi, täyttääkö arviointilaitos enää hyväksymisen vaatimukset suunnitellun muutoksen jälkeen. Samoin voidaan arvioida, tarvitseeko muutosta erikseen hyväksyä ennen sen mahdollista käyttöönottoa.

Epäselvissä tapauksissa muutoksista on syytä ilmoittaa, jolloin hyväksynnän antanut viranomainen tekee ratkaisun siitä, onko muutoksella merkitystä laitoksen velvoitteiden kannalta.

Muutostiedot tulee ilmoittaa Traficomille turvasähköpostilla osoitteeseen arviointilaitokset[at]traficom.fi

Ilmoituksen saatuaan Traficom arvioi, täyttääkö arviointilaitos enää hyväksymiselle asetettuja vaatimuksia, ja kehottaa sitä tarvittaessa korjaamaan puutteen määräajassa.

5 Arviointilaitokset ja NIS2 -direktiivi

Euroopan unionin kyberturvallisuusdirektiivin (NIS2 -direktiivin) tavoitteena on kyberturvallisuuden yhteisen tason varmistaminen kaikkialla Euroopan unionissa. Direktiivi on Suomessa pantu täytäntöön säätämällä Kyberturvallisuuslaki ja Tiedonhallintalain uusi 4 a luku.

5.1 Tiedonhallintalain 4 a luku

Tiedonhallintalain 4 a luku koskee julkishallintoa ja sen osalta toimivaltainen valvova viranomainen on Liikenne- ja viestintävirasto. Valvova viranomainen voi tehdä viranomaisiin kohdistuvia tarkastuksia NIS2 -direktiivin velvoitteiden noudattamisen valvomiseksi (18 j §) ja antaa tarkastustehtävään liittyvän avustavan tehtävän Arviointilaitoslaissa tarkoitetulle hyväksytylle tietoturvallisuuden arviointilaitokselle (18 k §). Ellei 4 a luvussa toisin säädetä, tietoturvallisuuden arviointilaitokseen sovelletaan Arviointilaitoslakia. Tiedonhallintalain osalta tarkastuksissa ei ole mahdollista käyttää apuna muita toimijoita, johtuen Arviointilain 3 §:n rajauksesta.

Valvova viranomainen voi antaa avustavan tehtävän tietoturvallisuuden arviointilaitokselle, jonka pätevyysalue on soveltuva avustavan tehtävän suorittamiseen. Lain perusteluissa todetaan, että arviointilaitoksen henkilöstön pätevyys varmistetaan lähtökohtaisesti silloin kun arviointilaitos hyväksytään arviointilaitoslain mukaisessa menettelyssä.

Viranomaisten tarkastuksissa tulee todennäköisesti vastaan salassa pidettäviä[46] tai turvallisuusluokiteltuja tietoja, joiden käsittelyyn liittyy erityisvaatimuksia[47].

Arviointilaitoksen valinnassa tulee huomioida, millaista todentamista tarkastuksen aikana tulee pystyä suorittamaan. Riittääkö hallinnollinen todentaminen (haastattelut ja dokumentaatioon tutustuminen)[48] vai tuleeko arviointilaitoksen pystyä tekemään myös teknistä todentamista[49], johon liittyy vaatimuksia todennusmenetelmien ja tarkastuksessa apuna käytettäviä laitteiden, välineiden ja järjestelmien osalta.

---

[46] Esim. Julkisuuslain 24 §: Salassa pidettäviä viranomaisen asiakirjoja ovat, jollei erikseen toisin säädetä... 7) henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat...

[47] Turvallisuusluokiteltujen asiakirjojen käsittelyyn liittyvistä tietoturvallisuustoimenpiteistä säädetään tarkemmin valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019).

[48] Ks. kohta 3.4.2.

[49] Ks. kohta 3.4.3.

Traficom on tarkastunut Katakri pätevyysalueen hyväksynnän yhteydessä arviointilaitoksen todennusmenetelmät sekä laitoksen toimitilojen ja tietojenkäsittelyn turvallisuuden, niin että ne täyttävät turvallisuusluokiteltavan tiedon käsittelyyn liittyvät vaatimukset turvallisuusluokkien TL IV tai TL III mukaisesti.

Arviointilaitoksen ISO/IEC 27001 pätevyysalueen hyväksyminen ei sisällä vastaavia tekniseen todentamiseen liittyviä vaatimuksia. Pelkästään ISO/IEC 27001 pätevyyden osalta hyväksynnän saaneet arviointilaitokset voivat tehdä hallinnollista todentamista, myös salassa pidettävän tiedon osalta.

Valvova viranomainen voi valvonnan toteuttamiseksi velvoittaa myös viranomaisen teettämään tietoturvallisuuden arviointilaitoksella kyberturvallisuuteen kohdistuvan riskienhallinnan arvioinnin, mikäli 18 k § 2. mom edellytykset täyttyvät. Itse arvioinnin tilaisi näissä tapauksissa arvioinnin kohteena oleva viranomainen, joka myös vastaisi arvioinnin kustannuksista. Valvova viranomainen voi kuitenkin asettaa arvioinnin teettämiselle ehtoja.

5.2 Kyberturvallisuuslaki

Kyberturvallisuuslailla on pantu täytäntöön NIS2 -direktiivi muilta osin, Tiedonhallintalain 4 a luvun koskiessa vain julkishallinnon toimialaa.

Kyberturvallisuuslain mukaiset valvovat viranomaisen on säädetty lain 26 §:ssä sektorikohtaisesti. Kukin viranomainen valvoo omalta osaltaan tiettyä toimijajoukkoa. Valvovia viranomaisia ovat Liikenne- ja viestintävirasto; Energiavirasto; Turvallisuus- ja kemikaalivirasto; Sosiaali- ja terveysalan lupa- ja valvontavirasto; Etelä-Savon elinkeino-, liikenne- ja ympäristökeskus; Ruokavirasto ja Lääkealan turvallisuus- ja kehittämiskeskus.

Kyberturvallisuuslain 29 §:n mukaan valvovalla viranomaisella on oikeus tehdä toimijaa koskeva tarkastus NIS2 -direktiivin velvoitteiden noudattamisen valvomiseksi ja se voi pyytää tarkastuksen suorittajaksi toisen valvovan viranomaisen tai käyttää tarkastuksessa apuna toista valvovaa viranomaista, tietoturvallisuuden arviointilaitosta ja ulkopuolista tietotekniikan asiantuntijaa. Tarkastuksesta aiheutuvasta kustannuksesta vastaisi tarkastuksen suorittamisesta päättänyt valvova viranomainen.

Kyberturvallisuuslain mukaisessa avustavassa tehtävässä voidaan käyttää muutakin toimijaa kuin tietoturvallisuuden arviointilaitosta. Valvova viranomainen ei voi siirtää tarkastustehtävää kokonaisuudessaan tietoturvallisuuden arviointilaitoksen tai ulkopuolisen asiantuntijan suoritettavaksi.

Pykälän perustelujen mukaan viranomainen voisi tietoturvallisuuden arviointilaitokselle tai ulkopuoliselle asiantuntijalle osoitetussa **toimeksiannossa** määritellä, millaista pätevyyttä arviointilaitokselta tai asiantuntijalta edellytetään ja mitä kriteeristöä arviointilaitoksen tai asiantuntijan tulee käyttää. Tarkastuksen suorittajalla ja siihen osallistuvalla olisi oltava sellainen koulutus ja kokemus, kuin tarkastuksen suorittamiseksi on tarpeen.

Arviointilaitosten osalta huomioon tulee kuitenkin ottaa arviointilaitoslain 10 §:n (tietoturvallisuuden arviointiperusteet) mukaiset käytettävissä olevat arviointikriteeristöt ja laitokselle hyväksytyt pätevyysalueet, jotka saattavat asettaa rajoituksia siihen, mitä laitokset voivat tehdä toimiessaan hyväksyttynä tietoturvallisuuden arviointilaitoksena.[50]

Perustelujen mukaan tarkastus voitaisiin tehdä toimijan tiloissa tai tietojärjestelmässä, niin että:

- **Tietojärjestelmässä tehtävä tarkastus** voisi olla esimerkiksi **teknisten riskienhallintakeinojen havainnointia** taikka tietokantojen, laitteistojen, palomuurien, salauksen ja verkkojen heikkouksien tunnistamista.

- Toimijan **tiloissa tapahtuva tarkastus** voisi kohdistua esimerkiksi pääsynhallintaan ja **tilaturvallisuutta** koskeviin seikkoihin.

- Muuta toimijan tiloissa toteutettavaa tarkastusta voisi olla myös **kirjallisen aineiston perusteella tapahtuva tarkastaminen**, kuten toimijan laatimien toimintakäsikirjojen, ohjeiden, prosessikuvausten, koulutuskirjanpidon, ulkopuolisen tarkastuksen tulosten tai muun relevantin aineiston tarkastaminen ja vaatimustenmukaisuuden arviointi.

Vastaavasti kuin Tiedonhallintalain osalta, myös 29 §:n mukaisten tarkastusten avustajaa valittaessa tulee huomioida, millaista todentamista tarkastuksen aikana tulisi pystyä suorittamaan. Missä tilanteissa riittää osaaminen hallinnollinen todentaminen osalta, vai tulisiko pystyä tekemään myös teknistä todentamista, jonka avulla voidaan varmistaa, että asiat on hoidettu dokumentoidun mukaisesti.[51]

---

[50] Ks. kohta 3.1. Kyberturvallisuuslain mukaisten tarkastusten osalta laitokset voivat toimia myös muussa roolissa kuin Traficomin hyväksymänä tietoturvallisuuden arviointilaitoksena, sillä arvioinnit eivät kohdistu valtionhallinnon viranomaisten tietojärjestelmiin ja tietoliikennejärjestelyihin. Arviointilaitoksia sitoo kuitenkin näissäkin tilanteissa FINAS-akkreditoinnin ja standardien vaatimukset.

[51] 29 §:n säännöskohtaisten perustelujen mukaan tarkastaja voisi tarkastaa yrityksen toimitilojen, tietojärjestelmien ja tietoliikennejärjestelyjen suojaamiseksi toteutetut sekä muut

On hyvä huomata, että valvovan viranomaisen on ennakolta varmistuttava arviointipalveluja hankkiessaan palveluntarjoajan luotettavuudesta toimeksiannon edellyttämässä laajuudessa ja että viranomaisen tietoja suojataan asianmukaisesti.[52] Arviointien suorittajalle asetettavien turvallisuus- ja osaamisvaatimusten määrittäminen on viranomaisen vastuulla.

Valvova viranomainen voi Kyberturvallisuuslain 30 §:n mukaan päätöksellä velvoittaa toimijaa teettämään kyberturvallisuuden riskienhallintaan kohdistuva turvallisuusauditoinnin, mikäli pykälässä mainitut edellytykset täyttyvät. Toimijan tulee tällöin omalla kustannuksellaan teettää velvoitteen mukainen turvallisuusauditointi.

6 Sote-arvioinnit

Tietoturvallisuuden arviointilaitoksille on annettu lainsäädännössä tehtäviä myös sosiaali- ja terveydenhuollon tietojärjestelmien arviointeihin liittyen. Näistä tehtävistä on säädetty laissa sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023, Asiakastietolaki) ja laissa sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019, Toisiolaki). Molempien lakien osalta, kyseisten lakien mukaisia arviointitehtäviä hoitavilta arviointilaitoksilta edellytetään, että ne täyttävät Arviointilaitoslain mukaisten vaatimusten lisäksi myös juuri näihin lakeihin liittyvät lisävaatimukset.

Asiakastietolain osalta arviointilaitoksella tulisi olla hyvä asiantuntemus sosiaali- ja terveydenhuollon tietojärjestelmiä koskevista vaatimuksista, joista säädetään asiakastietolain 84 §:ssä ja sen nojalla. Asiakastietolain 84 §:n mukaan Terveyden ja hyvinvoinnin laitos (THL) antaa tarkempia määräyksiä olennaisten vaatimusten sisällöstä, toimeenpanon määräajoista ja siitä, mitkä olennaiset vaatimukset on täytettävä eri palveluissa käytettävissä tietojärjestelmissä ja hyvinvointisovelluksissa.

Asiakastietolain 85 §:n mukaan THL voi antaa määräyksiä vaatimustenmukaisuuden osoittamisessa noudatettavista menettelyistä ja annettavan selvityksen sisällöstä. Lisäksi Kansaneläkelaitos (Kela) voi antaa määräyksiä ko. laissa tai lääkemääräyslaissa tarkoitettuihin

turvallisuusjärjestelyt. Tarkastusta suorittavalla olisi oikeus saada tutkittavakseen valvontatehtävän kannalta välttämättömät tiedot, asiakirjat, laitteet ja ohjelmistot, suorittaa tarvittavia testejä ja mittauksia sekä tarkastaa toimijan toteuttamat turvallisuusjärjestelyt. Tarkastajan olisi voitava suorittaa tarvittavia testejä ja mittauksia, kuten tunkeutumis- tai kuormitustestauksia osana tarkastusta.

[52] Ks. Julkisuuslaki 26 §:n 3 mom.

valtakunnallisiin tietojärjestelmäpalveluihin liitettävien tietojärjestelmien yhteentoimivuuden todentamisessa noudatettavista menettelyistä.

Toisiolain 26 §:n mukaan tietoturvallisuuden arviointilaitos arvioi tämän lain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti palveluntarjoajan hakemuksesta, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset. Arviointiperusteina on käytettävä Sosiaali- ja terveysalan tietolupaviranomaisen (Findata) määräyksiä turvalliselle käyttöympäristölle asetettavista vaatimuksista.

Asiakastietolain sekä Toisiolain mukaisten arviointien osalta arviointilaitosten tuleekin noudattaa kulloinkin voimassa olevia toimivaltaisten viranomaisten määräyksiä sekä muuta ohjausta ja neuvontaa. Traficomilla ei ole kyseisten lakien mukaista erityisosaamista, eikä toimivaltaa tehdä sote-arviointeihin liittyviä laintulkintoja tai antaa muuta tarkempaa ohjeistusta. Traficomin toimivaltaan kuuluu arviointilaitosten yleinen ohjaus ja valvonta.

Traficomin arviointilaitosohjeeseen on aiemmissa versioissa otettu mukaan myös sote-arviointeihin liittyvää ohjeistusta (aiemman ohjeen kohdat 3.6 ja 3.7), joka on laadittu yhteistyössä toimivaltaisten viranomaisten kanssa. Kyseisten osuuksien ajan tasalla pitäminen on aiheuttanut haasteita, sillä toimivaltaiset viranomaiset voivat päivittää antamiaan määräyksiä tai muuta ohjeistusta eri aikoihin.

Hyväksytyt tietoturvallisuuden arviointilaitokset ovat Traficomin hyväksyntäpäätöksissä velvoitettu noudattamaan Traficomin arviointilaitosohjetta, joka voi sote-arviointeja koskevien kirjausten osalta olla vanhentunut tai pahimmillaan ristiriitaista voimassa olevien määräysten suhteen.

Sote-arviointeja koskeva arviointilaitosohjeen osana aiemmin ollut tarkempi ohjeistus onkin nyt siirretty ohjeen liitteeksi (Liite 3). Liitteen kirjaukset väistävät, mikäli ne eroavat tai ovat ristiriidassa toimivaltaisen viranomaisen antamien ajantasaisten ohjeiden ja sääntelyn suhteen. Ohjeistus on yhteistyössä toimivaltaisten viranomaisten kanssa päivitetty vastaamaan tilannetta 5/2025.

Sote-arviointien osalta arviointilaitosten tulee ottaa selville kulloinkin voimassa oleva sääntely, toimivaltaisten viranomaisten antamat määräykset ja muu ohjeistus. Toimivaltaiset viranomaiset antavat tarvittaessa myös ohjausta ja neuvontaa, sekä auttavat tulkintakysymyksissä

Helsingissä 13. päivänä kesäkuuta 2025

Anssi Kärkkäinen
ylijohtaja

Heidi Kivekäs
osastopäällikkö

Liitteet 1 Muutostiedot

2 Tietoturvallisuuden arviointitoimintaa ohjaavat keskeiset normit

3 Sote-arviointeja koskevat ohjeet

Liitteet

LIITE 1 Muutostiedot

Versio	Päiväys	Kuvaus/muutos	Tekijä
1.0	7.5.2013	[Ensimmäinen versio]	Laura Kiviharju
2.0	29.1.2015	Luku 6, laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain muuttamisesta (250/2014) ja sähköisestä lääkemääräyksestä annetun lain muuttamisesta (251/2014)	Laura Kiviharju
3.0	12.8.2015	4.2.3 Pätevyysalueen muuttaminen; Katakri III:n aiheuttamat muutokset dokumenttiin.	Anna von Fieandt-Lehtonen
4.0	19.2.2016	Luvut 1.1 Ohjeen tarkoitus ja soveltamisala ja 7 Arviointilaitoksen valvonta ja laadunhallinta: täsmennyksiä ja lisäyksiä.	Anna von Fieandt-Lehtonen
5.0	19.5.2017	Lisäys: 5.4.4 Todentamismenetelmät arviointikriteeristöjen käytössä; täsmennykset: 5.5 Viranomaishyväksyntä, alaviite 20 säilytysajoista; 5.3.5 todistuksen sisältö; 6.1 todistuksen sisältö; 7.2.1 vuosi-ilmoituksen sisältö; 7.2.2 itsenäisesti ilmoitettavat arviointitiedot; 7.2.3 Viestintävirastolle toimitettavat arviointiraportit ja todistukset	Anna von Fieandt-Lehtonen
6.0	15.11.2017	Alaviitteet 27 ja 28; uusi luku 4.1 Arviointilaitoksena toimiminen; muutos: 5.3.4 Arviointiraportti ja muut arviointiin liittyvät asiakirjat	Anna von Fieandt-Lehtonen
7.0	23.4.2018	Uusi ohje	Anna von Fieandt-Lehtonen
8.0	24.9.2019	Traficomia koskevat päivitykset, täsmennyksiä ja linjauksia lukuihin 3.2, 3.3.1, 3.3.5, 3.5, 3.6, 4.2.2 ja 4.2.3	Anna von Fieandt-Lehtonen
8.1	28.1.2020	Tiedonhallintalain aiheuttamat muutokset, muutos lukuun 3.3.1	Anna von Fieandt-Lehtonen
8.2	18.12.2020	Toisiolain ja Findatan määräyksen aiheuttamat lisäykset tehty lukuihin 1.1, 2.2.1 ja alaviitteeseen 18. Lisäksi lisätty asiaa koskeva kokonaan uusi luku 3.7. Tehty myös muutoksia alaviitteeseen 17 sekä tehty sähköpostiosoitteisiin muutoksia.	Eija Alavesa ja Anna von Fieandt-Lehtonen

8.3	22.6.2022	Päivitetty ja täydennetty luku 3.6 vastaamaan voimassa olevaa asiakastietolakia ja sitä täydentäviä määräyksiä ja ohjeita. Päivitetty säädös- ja määräysviittauksia liitteessä Päivitetty Traficomin sähköpostiosoite arviointilaitosasioissa.	Anne Lohtander/Traficom THL/Mykkänen, Kalliovainio, Linsamo, Valviran asiantuntijat sekä Kela/Varis.
8.4	13.6.2025	Lisätty NIS2 -direktiivin kansallinen sääntely (luku 5) ja arviointilaitosten uusi salaustuotearviointipätevyys (kohta 3.5.). Sote-arviointien osuudet siirretty liitteeksi L3 (aiemmin ohjeen kohdat 3.6 ja 3.7), sekä päivitetty ajan tasalle. Poistettu viittaukset vanhentuneisiin VAHTI-ohjeisiin. Siirretty aiempi luku 5 (Arviointilaitoksen palveluiden käyttäminen) osittain kohdaksi 1.4. Lisätty kohta 2.4 Maksullisuus. Lisätty kohta 3.3.2 Kansainväliset tietoturvallisuusvelvoitteet ja yritysturvallisuusselvitykset. Päivitetty kohta 4.2 arviointilaitoksen tiedonanto- ja ilmoitusvelvollisuus. Täsmennetty kohta 3.3.6 (Todistuksen antaminen). Täsmennetty velvollisuutta hakea turvallisuusselvityksiä (2.1.2.1). Täsmennetty 3.3.7 Arviointia koskevien tietojen julkaiseminen. Päivitetty todennusmenetelmät (3.4.2 ja 3.4.3). Päivitetty säädökset ja standardien versiot ajan tasalle	Jussi Rissanen ja arviointilaitostiimi/ Traficom; THL/Mykkänen, Taipale; Valviran asiantuntijat sekä Kela/Varis.

LIITE 2 Tietoturvallisuuden arviointitoimintaa ohjaavat keskeiset normit

Tässä liitteessä luetellaan tietoturvallisuuden arviointilaitoksen toiminnan kannalta keskeiset normit, jotka arviointilaitoksen lukuun työskentelevien henkilöiden on tunnettava.

I Lainsäädäntö, ml. määräykset

- **Laki viranomaisten toiminnan julkisuudesta (621/1999)**
  Julkisuuslaissa säädetään viranomaisen asiakirjojen julkisuudesta ja salassapitoperusteista sekä muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista.

- **Laki julkisen hallinnon tiedonhallinnasta (906/2019)**

- **Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019)**

- **Laki tietoturvallisuuden arviointilaitoksista (1405/2011)**
  Laissa säädetään arviointilaitoksen hyväksymisvaatimuksista ja -menettelystä, tehtävistä sekä velvollisuuksista.

- **Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)**
  Laissa säädetään viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista sekä tietoturvallisuuden arviointiperusteista.

- **Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023)**
  Laissa säädetään sosiaali- ja terveydenhuollon asiakastietojen käsittelyssä käytettävien tietojärjestelmien tietoturvallisuusvaatimuksista, niiden todentamisesta sekä hyväksytyn tietoturvallisuuden arviointilaitoksen tehtävistä

  - **Terveyden ja hyvinvoinnin laitoksen määräys 4/2024:** Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista

  - **Terveyden ja hyvinvoinnin laitoksen määräys 5/2024**: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisista vaatimuksista

- **Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019)**
  Laissa säädetään sosiaali- ja terveystietojen toissijaisesta käytöstä, käyttöympäristöille asetettavista vaatimuksista ja hyväksytyn tietoturvallisuuden arviointilaitoksen tehtävistä.

  - **Sosiaali- ja terveysalan tietolupaviranomaisen määräys 1/2022**: Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavat vaatimukset

- **Tietosuojalaki (1050/2018)**

- **Euroopan parlamentin ja neuvoston asetus (EU) 2016/679**
  Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (**yleinen tietosuoja-asetus**)

- **Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)**
  Laissa säädetään toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden mukaisten erityissuojattavien tietoaineistojen suojaamiseksi tehtävistä tietoturvallisuustoimenpiteistä.

- **Turvallisuusselvityslaki (726/2014)**
  Laissa säädetään muun muassa henkilö- ja yritysturvallisuusselvitysten laatimisen edellytyksistä, selvitysten laadinnassa noudatettavasta menettelystä sekä turvallisuusselvityksen ja sen perusteella annetun todistuksen voimassaolosta ja todistuksen peruuttamisesta.

- **Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555**
  Toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (**NIS 2 -direktiivi**)

- **Kyberturvallisuuslaki (124/2025)**
  Laissa säädetään toimivaltaisten viranomaisten mahdollisuudesta käyttää NIS2 sääntelyn noudattamisen valvontaan liittyvässä tarkastuksessa apuna tietoturvallisuuden arviointilaitosta.

II Päätökset

- FINAS-akkreditointipalvelun akkreditointipäätös ehtoineen
- Traficomin hyväksymispäätös ehtoineen

III Ohjeet, suositukset tms.

- Traficomin ohje tietoturvallisuuden arviointilaitoksille
- Katakri 2020 - Tietoturvallisuuden auditointityökalu viranomaisille
- Sosiaali- ja terveysalan tietolupaviranomaisen ohje käyttöympäristön vaatimustenmukaisuuden arviointiin (THL/7064/14.00.07/2024, annettu 11.12.2024)
- Tulkintalinjaukset ja muut ohjeistukset, jotka luetellaan Traficomin Internet-sivuilla tai jotka muuten on annettu tiedoksi arviointilaitoksille.

LIITE 3 Sote-arviointeja koskevat ohjeet

L3.1 Asiakastietolain mukaisten luokan A tietojärjestelmien ja hyvinvointisovellusten sertifiointi (aiemmin luku 3.6)

L3.1.1 Arvioitavat tietojärjestelmät ja hyvinvointisovellukset

Sosiaali- ja terveydenhuollon tietojärjestelmiä ja hyvinvointisovelluksia koskee laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023, asiakastietolaki[53]).

Asiakastietolain 84 §:n 1 momentti määrittelee, että ”Asiakastietojen käsittelyssä käytettävän tietojärjestelmän ja hyvinvointisovelluksen tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset. Hyvinvointisovelluksen tulee täyttää saavutettavuusvaatimukset. Vaatimusten on täytyttävä käytettäessä tietojärjestelmää sekä itsenäisesti että yhdessä muiden siihen liitettäviksi tarkoitettujen tietojärjestelmien kanssa.”

Asiakastietolain 84 §:n 2 momentti määrittelee olennaisten vaatimusten osoittamisen: ”Palvelunantajan ja apteekin käyttämien tietojärjestelmien on vastattava käyttötarkoitukseltaan palvelunantajan ja apteekin toimintaa ja täytettävä palvelunantajan ja apteekin toimintaan liittyvät olennaiset vaatimukset. Olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän muodostaman kokonaisuuden kautta.”

Asiakastietolaissa ja sitä tarkentavissa THL:n määräyksissä 4/2024 (Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista) ja 5/2024 (Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisista vaatimuksista) määritellään millaisia tietojärjestelmiä ja hyvinvointisovelluksia luokan A olennaiset vaatimukset koskevat ja mille siten on hankittava sertifiointi.

Asiakastietolaissa *tietojärjestelmällä* tarkoitetaan *ohjelmistoa, järjestelmää tai osajärjestelmää, jota valmistajan suunnittelemien ominaisuuksien mukaisesti on tarkoitettu käytettäväksi asiakasasiakirjojen sähköiseen käsittelyyn, asiakirjojen tallentamiseen valtakunnallisiin tietojärjestelmäpalveluihin tai valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen tai jolla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää hyvinvointitietoja* (3 § 19 kohta).

Hyvinvointisovelluksella asiakastietolaissa tarkoitetaan *sovellusta, joka liittyy omatietovarantoon ja jolla käsitellään hyvinvointitietoa, sekä*

[53] https://www.finlex.fi/fi/lainsaadanto/2023/703

sovellusta, johon henkilö voi saada asiakastietonsa valtakunnallisesta asiakastietovarannosta, reseptikeskuksesta tai tiedonhallintapalvelusta (3 § 18 kohta).

Asiakastietolain mukaiseen arviointiin ei sisälly tietojärjestelmäpalvelun tuottajan, tietojärjestelmän valmistajan eikä käyttäjän (palvelunantajan) toimitilojen arviointi eikä tarkastaminen (87 §).

Asiakastietolain mukaan sosiaali- ja terveydenhuollon tietojärjestelmät sekä hyvinvointisovellukset jaetaan luokkiin A ja B niiden käyttötarkoituksen ja ominaisuuksien perusteella (79 §).

Tämä ohje ei koske luokkaan B kuuluvia järjestelmiä, sillä asiakastietolaissa ei edellytetä niiltä tietoturvallisuuden arviointia. Vapaaehtoinen tietoturvallisuuden arviointi luokan B järjestelmille on suositeltavaa, mutta niille ei myönnetä asiakastietolain tarkoittamaa tietoturvallisuustodistusta.

Tietojärjestelmäpalvelun tuottaja ja hyvinvointisovelluksen valmistaja vastaavat tietojärjestelmän ja hyvinvointisovelluksen käyttötarkoituksen määrittelemisestä ja luokittelun tekemisestä.

Luokkaan A kuuluvat

1) Kansaneläkelaitoksen ylläpitämät valtakunnalliset tietojärjestelmäpalvelut (nk. Kanta-palvelut),

2) valtakunnallisiin tietojärjestelmäpalveluihin liitettäväksi tarkoitetut tietojärjestelmät ja hyvinvointisovellukset

3) muut kuin 1 ja 2 kohdassa tarkoitetut käyttötarkoituksensa perusteella sertifioitavat tietojärjestelmät

4) välittäjien palvelut.

Muut asiakastietolain mukaiset tietojärjestelmät kuuluvat luokkaan B.

A-luokka jaetaan edelleen A1, A2 ja A3-luokkiin, jotka erotellaan toisistaan järjestelmän ja hyvinvointisovelluksen käyttötarkoituksen, käsiteltyjen tietojen luonteen ja laajuuden sekä riskitason ja kriittisyyden perusteella. Hyvinvointisovellukset kuuluvat oletusarvoisesti luokkaan A. THL on määrännyt tarkemmin tietojärjestelmien luokittelusta määräyksessä 4/2024 ja sen liitteessä 1.

THL voi päättää epäselvissä tilanteissa tietojärjestelmän luokasta. Luokittelu on kuitenkin tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan tehtävä määräyksissä annettujen kriteerien pohjalta, ja myös arviointilaitosten tulisi tarvittaessa ohjata

luokittelua, jos esimerkiksi tietojärjestelmäpalvelun tuottaja on selvästi luokitellut järjestelmänsä kriteerien vastaisesti.

L3.1.2 Arviointihakemus ja suhde yhteistestaukseen

Asiakastietolaissa *sertifioinnilla* tarkoitetaan *menettelyä, jolla todennetaan tietojärjestelmän tai hyvinvointisovelluksen täyttävän sitä koskevat tuotantokäyttöä varten vaadittavat olennaiset vaatimukset* (3 § 23 kohta).

Olennaisten vaatimusten todentamista ja vaatimustenmukaisuutta suhteessa erityyppisiin vaatimuksiin käsitellään yksityiskohtaisemmin THL:n määräyksessä 4/2024. Määräys 5/2024 liitteineen sisältää varsinaiset olennaiset vaatimukset. Määräyksen 5/2024 liite 1 sisältää lisätietoja ja havainnollistavia kuvauksia sertifiointiprosessin soveltamisesta sekä olennaisten vaatimusten täyttämisestä ja todentamisesta.

Luokkaan A kuuluva järjestelmä, osajärjestelmä tai hyvinvointisovellus on sertifioitava. Tietojärjestelmän sertifioinnin käynnistämisestä ja läpiviennistä vastaa tietojärjestelmäpalvelun tuottajana toimiva taho, joka voi olla myös järjestelmän valmistaja (asiakastietolaki 85 §). Hyvinvointisovelluksen sertifioinnin käynnistämisestä ja läpiviennistä vastaa hyvinvointisovelluksen valmistaja.

THL:n määräyksessä 4/2024 *tietoturvallisuuden arviointi on* määritelty sertifiointiprosessin osaksi, jossa hyväksytty tietoturvallisuuden arviointilaitos todentaa asiakastietolain 87 §:n perusteella tietoturvavaatimukset ja tuottaa todistuksen tietoturvallisuuden arvioinnista.

Luokkaan A kuuluvan tietojärjestelmän tai hyvinvointisovelluksen tietoturvallisuuden arvioinnin voi suorittaa vain arviointilaitos, jonka pätevyysalueena on VAHTI tai Katakri. Tietoturvallisuuden arvioinnin kriteeristönä on käytettävä THL:n määräyksen 5/2024 mukaisia tietoturvavaatimuksia ja digitaalisten palvelujen vaatimuksia.

Tietoturvallisuuden arviointi tehdään tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan hakemuksesta. Tietojärjestelmän tietoturvallisuuden arviointia tulee pyytää arviointilaitokselta hyvissä ajoin ennen suunniteltua käyttöönottoa. Arviointiin on varattava riittävästi aikaa.

Arvioinnissa on huomioitava se, onko kyseessä ensimmäinen järjestelmän sertifiointi vai vaatimustenmukaisuuden uudistaminen. Asiaa kuvataan erityisesti THL:n määräyksen 4/2024 luvuissa 10 ja 7.3.

Sertifiointiin kuuluu tietoturvallisuuden arvioinnin lisäksi yhteistestaus Kanta-palvelujen kanssa, jos järjestelmä kuuluu luokkaan A2 tai A3. Yhdellä järjestelmällä voi olla vain yksi voimassa oleva tietoturvallisuustodistus, mutta yhteen järjestelmään voi kohdistua useita eri ajankohtina testattavia testauskokonaisuuksia.

Uuden järjestelmän sertifiointi tapahtuu vaiheittain siten, että vaadittavat yhteistestaukset on suoritettava ennen tietoturvallisuuden arviointia, kun kyse on luokkiin A2 tai A3 kuuluvasta järjestelmästä. Tietoturvallisuuden arviointi on mahdollista käynnistää ennen yhteistestauslausunnon valmistumista (THL:n määräys 4/2024 luku 7). Näissä tilanteissa tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan tulee huolehtia, että yhteistestauksen ja tietoturvallisuuden arvioinnin kohteena on sama järjestelmä- tai sovellusversio tai sellainen versio, jossa yhteistestattaviin olennaisiin vaatimuksiin liittyvät mahdolliset järjestelmämuutokset eivät vaikuta arvioitaviin tietoturvavaatimuksiin. Tällöin myös tietoturvallisuuden arviointilaitos varmistaa ennen tietoturvallisuustodistuksen myöntämistä tietojärjestelmäpalvelun tuottajalta tai hyvinvointisovelluksen valmistajalta, että yhteistestauksen kohteena olevaan järjestelmään tai sovellukseen ei ole tulossa muutoksia, jotka voisivat vaikuttaa tietoturvallisuusvaatimusten toteuttamiseen. Arviointilaitoksen on varmistettava asia myös Kelalta.

Sertifioinnin uusimisen yhteydessä tietojärjestelmätoimittajan pitää olla yhteydessä Kelaan ja tietoturvallisuuden arviointilaitokseen 6 kk ennen vaatimustenmukaisuuden vanhenemista (THL:n määräys 4/2024 luku 10). Tietoturvallisuuden arviointiin voidaan edetä, vaikka järjestelmällä olisi käynnissä olevia yhteistestauksia. Valvira kuitenkin valvoo rekisteri-ilmoituksen yhteydessä, että tietojärjestelmään on toteutettu lainsäädännön vaatimat ja Kanta-palveluiden ajantasaisiin määrittelyihin perustuvat yhteistestaukset.

Tietoturvallisuustodistuksen myöntäminen ei edellytä yhteistestausta, jos kyseessä on luokkaan A1 kuuluva tietojärjestelmä, jolle ei suoriteta lainkaan yhteistestausta (esim. asiakastietojen välityspalvelu).

Lisätietoja yhteistestauksen ja tietoturvallisuuden arvioinnin suhteesta on THL:n määräyksen 4/2024 luvuissa 7.3 ja 10.

L3.1.3 Arviointimenettely ja -kriteeristö

Luokkaan A kuuluvien järjestelmien arviointi toteutetaan arviointilaitoslain ja asiakastietolain säännösten mukaisesti. Tietoturvallisuuden arvioinnin kriteeristönä käytetään THL:n määräyksen 5/2024 mukaisia

tietoturvavaatimuksia tai myöhempien määräysten ne korvaavia vaatimuksia.

Arvioinnissa todennettavat tietoturvavaatimukset on kuvattu THL:n määräyksen 5/2024 liitteen 2 (Olennaisten vaatimusten luettelo) Tietoturvavaatimukset- ja Digit.palvelujen vaatimukset -osioissa. Vaatimustenmukaisuuden arviointi edellyttää usein arviointia suhteessa olennaisten vaatimusten lähteenä oleviin määrittelyihin tai standardeihin.

Arvioinnissa noudatetaan tässä ohjeessa ja THL:n määräyksissä kuvattuja menettelyjä. Tietoturvallisuuden arvioinnin menettelyjä kuvataan tarkemmin erityisesti THL:n määräyksen 4/2024 luvuissa 7 ja 10, määräyksen 5/2024 luvuissa 7 ja 10, sekä määräyksen 5/2024 liitteen 1 luvuissa 5 ja 6.

Keskeinen arvioinnin pohjana käytettävä tietojärjestelmäpalvelun tuottajan dokumentti on THL:n määräyksen 5/2024 mukainen järjestelmälomake. Lomakkeella ilmoitetaan kaikki olennaiset vaatimukset, joita järjestelmässä täytetään. Jos järjestelmän käyttötarkoitus vastaa THL:n määräyksen 5/2024 mukaisia profiileja, kaikkien järjestelmää koskevien profiilien mukaiset vaatimukset on täytettävä järjestelmässä. Järjestelmää koskevien profiilien mukaisten tietoturvavaatimusten täyttämisen todentaminen on osa tietoturvallisuuden arviointia. Myös järjestelmän luokka ja riskitaso sekä luokan A3 järjestelmän mahdollinen kriittisyys ilmoitetaan järjestelmälomakkeella.

Arviointilaitos arvioi luokkaan A1, A2 tai A3 kuuluvan tietojärjestelmän tietoturvallisuuden ja myöntää arvioinnin hyväksytysti läpäisseelle järjestelmälle tietoturvallisuustodistuksen. Arvioinnin on katettava kaikki järjestelmälomakkeella täytetyksi ilmoitetut tietoturvavaatimukset ja tietoturvavaatimukset, jotka sisältyvät järjestelmälomakkeella ilmoitettuihin profiileihin.

L3.1.4 Tietoturvallisuustodistuksen sisältö

Yhdellä tietojärjestelmällä tai hyvinvointisovelluksella tulee olla vain yksi voimassa oleva todistus. Suomen- tai ruotsinkielisestä todistuksesta tulee käydä selkeästi ilmi, mitä on arvioitu ja milloin.

Arviointilaitoksen myöntämän todistuksen yleinen vähimmäissisältö on kerrottu luvussa 3.3.6. Mikäli asiakastietolain tai sen nojalla annettujen määräysten perusteella todistuksen vaatimukset poikkeavat tämän ohjeen luvun 3.3.6 vaatimuksista, tulee niille asiakastietolain mukaisissa arvioinneissa antaa etusija, eikä todistuksen yleiset vaatimukset tule sovellettaviksi näiltä osin.

Vähimmäissisällön lisäksi sosiaali- ja terveydenhuollon tietojärjestelmille myönnettävään todistukseen tulee kirjata tieto siitä, että kyseessä on asiakastietolain perusteella myönnetty tietoturvallisuustodistus ja tietojärjestelmä tai hyvinvointisovellus täyttää THL:n määräyksen sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista vaatimuksista (5/2024) asettamat tietoturvavaatimukset ja digitaalisten palvelujen vaatimukset.

Todistuksessa tulee ilmoittaa THL:n määräyksen 4/2024 kohdassa 7.3 (Tietoturvallisuuden arvioinnin sisältö ja tulokset) edellytetyt tiedot.

Jos todistuksessa havaitaan virhe tai sitä ei ole laadittu THL:n määräyksissä ja tässä ohjeessa kuvatulla tavalla, tulee todistus korjata.

THL:n määräyksen 4/2024 kohdan 7.3 mukaan *Tietoturvallisuustodistus tulee kirjoittaa kolme vuotta voimassa olevaksi, ellei viranomaisten määräyksistä tai ohjeista johtuen tai tiedossa olevan olennaisten vaatimusten tai muiden säännösten uudistamisen vuoksi lyhyempi voimassaolo ole välttämätön.*

L3.1.5 Tietoturvallisuustodistuksen käsittely

Asiakastietolain mukaan arviointilaitoksen on ilmoitettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle, Kansaneläkelaitokselle ja Terveyden ja hyvinvoinnin laitokselle tiedot kaikista myönnetyistä, muutetuista, täydennetyistä ja evätyistä todistuksista. Arviointilaitoksen tulee lähettää myönnetty todistus viranomaisille heti myöntämisen jälkeen.

Arviointilaitoksen on myös pyydettäessä annettava Valviralle kaikki tarvittavat lisätiedot tietojärjestelmistä ja hyvinvointisovelluksista, joille arviointilaitos on myöntänyt tietoturvallisuustodistuksen.[54]

Arviointilaitoksen myöntämän tietoturvallisuustodistuksen käyttökohteet ovat ainakin seuraavat:

- Tuotantokäyttöön otettavalla A-luokan tietojärjestelmällä tai hyvinvointisovelluksella on oltava voimassa oleva tietoturvallisuustodistus.

- Tietoturvallisuustodistuksen tiedot lähetetään Valviralle, joka päivittää tietojärjestelmärekisterin tietoja todistuksessa olevien tietojen pohjalta.

- Kela tarkistaa todistuksen tiedot Valviran rekisteristä ennen kuin järjestelmää käyttävälle palvelunantajalle avataan yhteys Kanta-palveluihin

[54] Asiakastietolaki 88 §.

- Sote-palvelunantajat ja apteekit tarkistavat todistuksen tiedot Valviran rekisteristä, kun laativat ja ylläpitävät lakisääteistä tietoturvasuunnitelmaansa ja suorittavat sen perusteella asiakastietojen käsittelyn ja tietojärjestelmien käytön omavalvontaa, tai järjestelmien hankinta- tai sopimusprosessien yhteydessä.

Tietoturvallisuustodistus kertoo, että tietojärjestelmässä tai hyvinvointisovelluksessa on todennettu sille asetetut olennaiset tietoturvavaatimukset. Palvelunantaja saa myös Valviran tietojärjestelmärekisterin kautta tiedon, jos jokin vaatimus tulee täytettäväksi esimerkiksi sen käyttöympäristössä, mikä on tärkeää, jotta tietoturvavaatimukset toteutuvat tuotannossa. Tästä syystä erityisesti käyttöympäristössä huomioitavien seikkojen ilmaiseminen todistuksessa selkeästi on tärkeää.

L3.1.6 Muutosarvioinnit, seuranta-auditoinnit ja arviointilaitoksen ilmoitusvelvollisuudet

L3.1.6.1 Muutosarviointi

Asiakastietolain mukaan tietojärjestelmäpalvelun tuottajan on ilmoitettava arviointilaitokselle ja Kansaneläkelaitokselle tietojärjestelmän ja hyvinvointisovelluksen valmistajan hyvinvointisovellusten olennaisista muutoksista (82 §). Edelleen lain mukaan *tietoturvallisuuden arviointia koskeva todistus tai yhteentoimivuuden testaus on uudistettava, jos tietojärjestelmään tai hyvinvointisovellukseen […] tehdään merkittäviä muutoksia, tai olennaisia vaatimuksia on muutettu tavalla, joka edellyttää uutta sertifiointia* (82 §).

THL määräyksen 4/2024 liitteessä 2 määrätään luokkaan A kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten muutosten ilmoittamisesta ja siitä, millaisia muutoksia on ilmoitettava arviointilaitokselle.

Arviointilaitos tekee saamansa muutosilmoituksen pohjalta päätöksen siitä, onko järjestelmälle tai hyvinvointisovellukselle suoritettava muutosten takia uusi tietoturvallisuuden arviointi. Muutosten arvioinnissa on noudatettava THL:n määräystä 4/2024.

Lain mukaan *arviointi on suoritettava tietojärjestelmän ja hyvinvointisovelluksen käyttötarkoitusta koskevien olennaisten vaatimusten tai järjestelmään tehtyjen muutosten laajuuden mukaisesti* (87 §). Jos arviointilaitos tekee muutosten takia tietoturvallisuuden arvioinnin, muutosarvioinnissa on käytävä läpi vaatimukset, joiden toteutumiseen muutoksilla on vaikutuksia. Mikäli muut vaatimukset täyttyvät

tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan mukaan aiemmin todennetun tasoisesti, voidaan tietoturvallisuustodistus päivittää siten, että aiemman todistuksen voimassaoloaika ei muutu. Tietoturvallisuustodistuksessa pitää mainita, mikä järjestelmässä tai hyvinvointisovelluksessa on muuttunut ja miksi muutosarviointi on tehty

Tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja voi myös päättää, että muutosten takia tarvittavassa tietoturvallisuuden arvioinnissa tähdätään kokonaan uuteen tietoturvallisuustodistukseen. Tällöin tietoturvallisuuden arvioinnissa käydään läpi kaikki järjestelmän tai hyvinvointisovelluksen kautta toteutetut tai täytetyt tietoturvavaatimukset ja kirjoitetaan uusi todistus, jolla on uusi voimassaoloaika.

L3.1.6.2 Seuranta-auditointi

Tietojärjestelmälle tai hyvinvointisovellukselle mahdollisesti suoritettavat tietoturvallisuuden seuranta-auditoinnit on erotettava todistuksen uusimiseen tähtäävistä tietoturvallisuuden arvioinneista.

Asiakastietolaissa ei edellytetä tietoturvallisuuden seuranta-auditointeja. Ne perustuvat tietoturvallisuuden arviointilaitoksen ja tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan väliseen sopimukseen.

THL suosittelee luokan A3 järjestelmille ja korkean riskitason järjestelmille seuranta-auditointeja, joissa vuosittain käydään läpi keskeiset tietoturvavaatimusten toteutumiseen mahdollisesti vaikuttavat tietojärjestelmän ja sen teknisen käyttöympäristön (mukaan lukien alustapalvelut ja käyttöjärjestelmät) muutokset ja riskit, olennaisten vaatimusten mahdolliset muutokset ja päivitykset sekä mahdollinen tarve muutosilmoitukselle.

Seuranta-auditoinneista ei kirjoiteta uutta tietoturvallisuustodistusta ja vanhan todistuksen voimassaoloaikaa ei jatketa seuranta-auditoinnin tuloksena. Seuranta-auditoinnissa mahdollisesti tehtävät havainnot voivat johtaa myös (muutosilmoitukseen ja) muutosten johdosta tehtävään tietoturvallisuuden arviointiin.

L3.1.6.3 Poikkeamat

Jos arviointilaitos toteaa, ettei järjestelmä tai hyvinvointisovellus enää täytä sille asetettuja vaatimuksia tai tietoturvallisuustodistusta ei olisi tullut myöntää, arviointilaitoksen on hyvän hallintotavan mukaisesti kehotettava tietojärjestelmän valmistajaa tai tuottajaa korjaamaan puutteet. Valvontatoimivalta asiassa on asiakastietolain nojalla Valviralla (89 §). Poikkeamailmoituksia koskevan asiakastietolain 90 §:n mukaan muu taho eli myös arviointilaitos voi ilmoittaa Valviralle tietojärjestelmässä tai hyvinvointisovelluksessa havaitsemistaan riskeistä. Riskit voivat liittyä

asiakas- tai potilasturvallisuuteen tai tietoturvallisuuteen. Valvira suosittelee, että arviointilaitos tekee sille poikkeamailmoituksen merkittävistä riskeistä, jotka eivät korjaannu säännönmukaisessa arviointiprosessissa.

Asiakastietolain 90 §:n mukaan tietosuojapoikkeamista on ilmoitettava tietosuojavaltuutetulle.

L3.2 Toisiolain mukaisen käyttöympäristön tietoturvallisuuden arviointi (aiemmin luku 3.7)

L3.2.1 Vaatimustenmukaisuuden arviointi

Sosiaali- ja terveysalan tietolupaviranomainen Findata ylläpitää sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019, toisiolaki) mukaisesti tietoturvallista käyttöympäristöä.[55] Ne tietoaineistot, joiden käyttöön Findata on myöntänyt luvan, luovutetaan pääsääntöisesti luvansaajan käsittelyä varten kyseiseen Findatan käyttöympäristöön. Mikäli tietoaineistoja on pyydetty käsiteltäviksi muussa kuin Findatan tietoturvallisessa käyttöympäristössä, Findata tai muu toisiolaissa tarkoitettu viranomainen saa luovuttaa tiedot hakijalle vain, jos hakijan käyttöympäristö täyttää toisiolain 20 § 2 momentissa ja 21–29 §:ssä säädetyt edellytykset. Lisäksi hakijan tulee noudattaa toisiolain 18 §:ssä vaadittuja yleisiä tietoturvavaatimuksia, joiden mukaan henkilötietoja käsiteltäessä toisiolain nojalla, käsittelyn riittävä tietoturvallisuus on varmistettava riskienhallinnalla, pääsynhallinnalla, aktiivisella valvonnalla sekä noudattamalla tietoturvallisuuden ja tietosuojan toteutuksesta ja valvonnasta vastaavan viranomaisen määräyksiä ja ohjeita. Erityistä huomiota on kiinnitettävä käyttörajoitusten sekä salassapitovelvoitteen toteuttamiseen.

Toisiolain 24 §:n 2 momentin mukaan Findata antaa tarkemmat määräykset muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista. Findata on antanut toisiolain 24 §:n 2 momentin mukaisesti määräyksen 1/2022[56], jossa on asetettu palveluntarjoajien tietoturvallisille käyttöympäristöille vaatimuksia. Toisiolain mukaisesti yksilötasoisten aineistojen analysointi on sallittua ainoastaan määräyksen vaatimukset täyttävissä käyttöympäristöissä. Vaatimukset edellyttävät vastaavaa tietoturvan tasoa kuin Findatan omassa käyttöympäristössä.

Findata on antanut lisäksi erillisen määräystä 1/2022 koskevan ohjeen käyttöympäristön vaatimustenmukaisuuden arviointiin (THL/7064/14.00.07/2024, annettu 11.12.2024).

Käytännössä käyttöympäristön tietoturvallisuus on osoitettava tietoturvallisuuden arviointilaitoksen antamalla todistuksella.[57] Tietojärjestelmän tietoturvallisuuden arviointia tulee pyytää ajoissa arviointilaitokselta. Arviointiin on varattava riittävästi aikaa.

---

[55] Toisiolaki 20 § 1 momentti.
[56] Sosiaali- ja terveysalan tietolupaviranomaisen määräys 1/2022: Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavat vaatimukset.
[57] Toisiolaki 25 § 1 momentti.

Tietoturvallisuuden arviointilaitos arvioi toisiolain mukaisesti hakemuksesta, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset. Arviointiperusteena on käytettävä Findatan määräystä 1/2022.[58]

Jos käyttöympäristö täyttää Findatan määräyksen 1/2022 mukaiset tietoturvallisuusvaatimukset, tietoturvallisuuden arviointilaitoksen on annettava suorittamastaan arvioinnista palveluntarjoajalle todistus sekä siihen liittyvä tarkastusraportti.[59] Tämän jälkeen Findata voi harkita ja luovuttaa tietoaineistoja hakijan käsiteltäväksi muussa kuin sen omassa käyttöympäristössä.

L3.2.2 Vaatimuksenmukaisuustodistuksen sisältö ja tarkastusraportti

Arviointilaitos myöntää todistuksen käyttöympäristön palveluntarjoajalle[60]. Arviointilaitoksen myöntämän vaatimustenmukaisuustodistuksen vähimmäissisältö on kerrottu luvussa 3.3.6. Mikäli toisiolain tai sen nojalla annettujen määräysten perusteella todistuksen vaatimukset poikkeavat tämän ohjeen luvun 3.3.6 vaatimuksista, tulee niille toisiolain mukaisissa arvioinneissa antaa etusija, eikä todistuksen yleiset vaatimukset tule sovellettaviksi näiltä osin.

Vähimmäissisällön lisäksi toisiolain mukaiselle käyttöympäristölle myönnettävään vaatimustenmukaisuustodistukseen tulee kirjata omina kohtinaan seuraavat asiat:

- Kyseessä on toisiolain perusteella myönnetty vaatimustenmukaisuustodistus siitä, että tietojärjestelmä täyttää Findatan määräyksen 1/2022: Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavat vaatimukset
- Yksilöintitietoina vaatimustenmukaisuustodistuksen numero/ID, palveluntarjoajan käyttöympäristön nimi ja Y-tunnus/Rekisteröintitunnus
- Jos arviointi tai uudelleenarviointi koskee vain käyttöympäristön osaa, arviointilaitoksen antamaan todistukseen on selkeästi merkittävä, mikä osa käyttöympäristöstä on arvioitu. [61] Lisäksi todistuksessa tulee olla perustelut sille, miksi osaa käyttöympäristöstä ei ole arvioitu.

---

[58] Toisiolaki 26 § 1 momentti.
[59] Toisiolaki 26 § 2 momentti.
[60] Palveluntarjoajalla tarkoitetaan sitä organisaatiota, jolle kirjoitetaan todistus ja jolta Valvira vastaanottaa käyttöympäristön rekisteri-ilmoituksen. Mikäli toiminnassa on mukana useampi organisaatio, todistus kirjoitetaan kuitenkin vain yhdelle organisaatiolle, jolla tulee olla sopimukset toiminnasta muiden organisaatioiden kanssa. Valviran rekisteriin otetaan vastaan ilmoitus vain yhdeltä toimijalta, jonka käyttöympäristöön myös viranomaisen valvontatoimet voivat kohdistua.
[61] Palveluntarjoajalla tarkoitetaan sitä organisaatiota, jolle kirjoitetaan todistus ja jolta Valvira vastaanottaa käyttöympäristön rekisteri-ilmoituksen. Mikäli toiminnassa on mukana useampi organisaatio, todistus kirjoitetaan kuitenkin vain yhdelle organisaatiolle, jolla tulee olla

- Tietoturvallisuuden arviointilaitoksen käyttöympäristölle tai palveluntarjoajalle asettamat rajoitukset [62]
- Käyttöympäristön yleiskuvaus ja sen käyttötarkoitus
- Onko kyseessä ensimmäinen arviointi vai uudelleenarviointi (mikäli uudelleen arviointi, niin vanhan ja uuden todistuksen yksilöivät tunnukset, mikäli poikkeavat toisistaan)
- Mikäli vaatimuksenmukaisuuden arvioinnissa on hyödynnetty voimassa olevia sertifikaatteja, ne tulee listata sekä mainita, miltä osin kunkin sertifikaatin tulkitaan vastaavan tietyn osa-alueen vaatimuksiin ja kuinka pitkään sertifikaatit ovat voimassa.

Arviointilaitoksen myöntämä todistus on voimassa enintään viisi vuotta. Tietoturvallisuuden arviointilaitos voi vaatia palveluntarjoajalta kaikki arvioinnin sekä todistuksen laatimisen ja ylläpitämisen edellytyksenä olevat tiedot.

Todistuksen antamiseen sovelletaan muutoin tietoturvallisuuden arviointilaitoksista annetun lain 9 §:n 3 momenttia[63], jonka mukaan hyväksytty tietoturvallisuuden arviointilaitos antaa selvitysten ja tarkastuksen perusteella todistuksen, jos arvioitavan kohteen toimitilat ja toiminta on selvityksen perustana olleiden arviointiperusteiden mukainen. Todistuksessa tulee yksilöidä arvioinnissa käytetyt tietoturvallisuuden arviointiperusteet ja arvioinnin laajuus.

L3.2.3 Vaatimustenmukaisuustodistuksen merkitys

Arviointilaitoksen myöntämän vaatimustenmukaisuustodistuksen käyttökohteet ovat ainakin seuraavat:

- Findatan ulkopuolisilla käyttöympäristöillä, joissa käsitellään toisiolain mukaisia henkilötietoja sisältäviä tietoaineistoja, on oltava voimassa oleva, toisiolaissa edellytetty vaatimuksenmukaisuustodistus.

---

sopimukset toiminnasta muiden organisaatioiden kanssa. Valviran rekisteriin otetaan vastaan ilmoitus vain yhdeltä toimijalta, jonka käyttöympäristöön myös viranomaisen valvontatoimet voivat kohdistua.

[62] Palveluntarjoajalla tarkoitetaan sitä organisaatiota, jolle kirjoitetaan todistus ja jolta Valvira vastaanottaa käyttöympäristön rekisteri-ilmoituksen. Mikäli toiminnassa on mukana useampi organisaatio, todistus kirjoitetaan kuitenkin vain yhdelle organisaatiolle, jolla tulee olla sopimukset toiminnasta muiden organisaatioiden kanssa. Valviran rekisteriin otetaan vastaan ilmoitus vain yhdeltä toimijalta, jonka käyttöympäristöön myös viranomaisen valvontatoimet voivat kohdistua.

[63] Toisiolaki 26 § 3 momentti.

- Arviointilaitos lähettää vaatimuksenmukaisuustodistuksen tiedot sekä tarkastusraportin Valviran kirjaamoon salatulla sähköpostilla (kirjaamo[at]valvira.fi). Valvira ylläpitää julkista rekisteriä sille ilmoitetuista vaatimukset täyttävistä käyttöympäristöistä.

L3.2.4 Käyttöönoton jälkeinen seuranta ja arviointilaitoksen ilmoitusvelvollisuus

Palveluntarjoajan on seurattava ja arvioitava ajantasaisella järjestelmällisellä menettelyllä tietoturvallisesta käyttöympäristöstä sen tuotantokäytön aikana saatavia kokemuksia. Palveluntarjoajan on seurattava toisiolain muutoksia ja tehtävä käyttöympäristöön muutosten edellytyksenä olevat korjaukset. Käyttöympäristön olennaisista muutoksista on ilmoitettava tietoturvallisuuden arviointilaitokselle. Arviointilaitoksen myöntämä todistus on uudistettava, jos käyttöympäristöön tehdään merkittäviä muutoksia tai jos käyttöympäristöä koskevia vähimmäisvaatimuksia on muutettu tavalla, jonka edellytyksenä on uusi arviointi.[64]

Palveluntarjoajan on säilytettävä vaatimustenmukaisuutta koskevat ja muut valvonnan edellytyksenä olevat tiedot vähintään viisi vuotta tietoturvallisen käyttöympäristön tuotantokäytön päättymisestä.[65]

Jos tietoturvallisuuden arviointilaitos toteaa, että käyttöympäristö ei ole täyttänyt tai ei enää täytä toisiolaissa ja Findatan määräyksessä 1/2022 säädettyjä vaatimuksia tai että todistusta ei muutoin olisi tullut myöntää, laitoksen on kehotettava palveluntarjoajaa korjaamaan puutteet ja ilmoittaa tilanteesta Valviralle. Arviointilaitos voi peruuttaa todistuksen määräajaksi tai kokonaan taikka myöntää sen rajoitettuna, jollei palveluntarjoaja korjaa puutteellisuuksia arviointilaitoksen asettamassa määräajassa. Määräajan pituutta määritettäessä on otettava huomioon käyttöympäristön korjaamiseksi tarvittava kohtuullinen aika.[66]

Tietoturvallisuuden arviointilaitoksen on ilmoitettava Valviralle tiedot kaikista myönnetyistä, muutetuista, täydennetyistä, määräajaksi tai kokonaan peruutetuista tai evätyistä todistuksista sekä toisiolain 27 §:n mukaisista kehotuksista ja rajoituksista. Lisäksi tietoturvallisuuden arviointilaitoksen on pyydettäessä annettava Valviralle kaikki tarvittavat lisätiedot.[67]

---

[64] Toisiolaki 29 § 1 momentti.
[65] Toisiolaki 29 § 2 momentti.
[66] Toisiolaki 27 §.
[67] Toisiolaki 28 §.