Dnro: 153/602/2016
22.6.2022

Ohje tietoturvallisuuden arviointilaitoksille 210/2022 O

Versiohistoria

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	Anne Lohtander/Traficom,

		ja sitä täydentäviä määräyksiä ja ohjeita. Päivitetty säädös- ja määräysviittauksia liitteessä Päivitetty Traficomin sähköpostiosoite arviointilaitosasioissa.	THL/Mykkänen, Kalliovainio, Linsamo, Valviran asiantuntijat sekä Kela/Varis.

TRAFICOM
Liikenne- ja viestintävirasto

22.6.2022

Sisältö

1 Johdanto

1.1 Ohjeen tarkoitus ja soveltamisala

Laissa tietoturvallisuuden arviointilaitoksista (Arviointilaitoslaki) säädetään arviointilaitosten hyväksymisestä, valvonnasta ja toiminnasta. Laissa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (Arviointilaki), laissa julkisen hallinnon turvallisuusverkkotoiminnasta (TUVEL), laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (Asiakastietolaki) ja laissa sosiaali- ja terveystietojen toissijaisesta käytöstä (Toisiolaki) säädetään tehtävistä, joita Liikenne- ja viestintäviraston hyväksymä tietoturvallisuuden arviointilaitos voi hoitaa.

Lain liikenne- ja viestintäministeriön hallinnonalan virastouudistuksen täytäntöönpanoa sekä virastojen tehtävien uudelleenorganisointia koskevan lainsäädännön voimaanpanosta 4 §:n mukaan "Lain 1 §:ssä mainitun Liikenne- ja viestintävirastosta annetun lain 2 ja 3 §:ssä tarkoitettuun tehtäväalaan kuuluva tehtävä, joka on muualla laissa säädetty Liikenteen turvallisuusviraston, Viestintäviraston, Liikenneviraston, Ilmailuhallinnon, Telehallintokeskuksen, Autorekisterikeskuksen, Ajoneuvohallintokeskuksen, Rautatieviraston, Merenkulkulaitoksen tai lääninhallituksen hoidettavaksi, siirtyy Liikenne- ja viestintävirastolle 1 päivänä tammikuuta 2019 tämän lain mukaisesti." Näin ollen toimivaltainen viranomainen tietoturvallisuuden arviointilaitosasioissa on 1.1.2019 lähtien Liikenne- ja viestintävirasto, Traficom.

Tässä ohjeessa kuvataan tietoturvallisuuden arviointilaitoksen rooli ja tehtävät siinä tietoturvallisuuden arviointitoiminnassa, josta säädetään edellä mainituissa laeissa. 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 kokevat 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

1.3 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.

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[1] ja ISO/IEC 27006:2015[2] vaatimuksia. Kyseisissä standardeissa yksilöidään vaatimukset tietoturvallisuuden johtamisjärjestelmiä auditoiville ja sertifioiville elimille.

[1] 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

[2] ISO/IEC 27006:2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

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.

Luottamuksellisen tiedon turvallista käsittelyä koskevat vaatimukset todennetaan Katakrin[3] 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.[4] 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 hyväksytyissä tietojärjestelmissä.

Vaatimusten täyttäminen tarkoittaa käytännössä muun muassa sitä, että laitos on määritellyt sen turvallisuustoimintaa koskevat periaatteet, turvallisuusorganisaation sekä siihen liittyvät vastuut, sillä on riittävät menetelmät riskien tunnistamiseksi, arvioimiseksi ja poikkeustilanteiden hallitsemiseksi. Laitoksen toimitilojen on puolestaan täytettävä Katakrissa luetellut vaatimukset koskien aluetta, fyysisiä rakenteita ja turvallisuusteknisiä järjestelmiä.

---

[3] Katakri - tietoturvallisuuden auditointityökalu viranomaisille 2015.

[4] 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.

Henkilöstöturvallisuusvaatimukset edellyttävät muun muassa sitä, että arviointitoiminnassa käytetään vain sellaisia henkilöitä, jotka ovat antaneet asianmukaiset salassapitositoumukset sekä läpäisseet riittävät turvallisuusselvitykset. Arviointilaitoksen on haettava toimintaan osallistuvista henkilöistä turvallisuusselvitykset sen perusteella, minkä tason turvallisuusluokiteltua tietoa arviointitoimintaan osallistuva henkilö käsittelee. Arviointilaitos voi toiminnassaan käyttää vain sellaisia henkilöitä, joiden turvallisuusselvityksessä ei ole tullut esiin mitään sen tarkoituksen kannalta merkityksellistä tietoa. Jos turvallisuusselvityksen perusteella annetaan kirjallinen ilmoitus, on arviointilaitoksen aina pyydettävä Traficomilta etukäteinen kirjallinen lausunto henkilöstövaatimusten täyttymisestä ennen kyseisen henkilön käyttämistä arviointitoiminnassa.

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 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 arviointia.

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

Tietoturvallisuuden arviointikriteeristöt:

1) valtiovarainministeriön VAHTI-ohjeet tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (yksilöity liitteessä 1), kulloinkin voimassa olevat versiot
2) Katakri, tietoturvallisuuden arviointityökalu viranomaisille, kulloinkin voimassa oleva versio
3) ISO/IEC 27001, kulloinkin voimassa oleva versio
4) muu julkaistu ja yleisesti tai alueellisesti sovellettu tietoturvallisuutta koskeva säännös, määräys tai ohje taikka vahvistettuun standardiin sisältyvät tietoturvallisuutta koskevat vaatimukset

Arviointilaitoksen on aina haettava pätevyyttä osa-alueelle 3) eli jotta laitos voidaan hyväksyä tietoturvallisuuden arviointilaitokseksi, sillä on oltava pätevyys suorittaa ISO/IEC 27001 -standardin mukaisia arviointeja.

Jos tietoturvallisuuden arviointilaitoksen pätevyysalue kattaa valtiovarainministeriön ohjeet tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (kohta 1) tai Katakrin (kohta 2), se voi tehdä myös seuraavia arviointeja:

- sosiaali- ja terveydenhuollon tietojärjestelmien arvioinnin ja antaa olennaisten vaatimusten täyttymistä koskevan todistuksen (ks. luku 3.6 Sosiaali- ja terveydenhuollon tietojärjestelmien arviointi) ja

- sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain mukaisen käyttöympäristön tietoturvallisuuden arvioinnin ja antaa vaatimusten täyttymistä koskevan todistuksen (ks. luku 3.7 Toisiolain mukaisen käyttöympäristön tietoturvallisuuden arviointi).

Jos arviointilaitos hakee pätevyysalueekseen VAHTIa tai Katakria, sen tulee hakea pätevyyttä myös turvallisuusluokan perusteella.

Kun arviointilaitos hakee ensimmäistä kertaa Traficomin hyväksymäksi tietoturvallisuuden arviointilaitokseksi, sille voidaan määritellä akkreditoitu pätevyysalue korkeintaan turvallisuusluokkaan KÄYTTÖRAJOITETTU 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 turvallisuusluokka (turvallisuusluokka vain, jos haetaan VAHTI- tai Katakri-pätevyyttä)
- 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. Tietoturvallisuuden arviointilaitoksen hyväksymistä koskevan asian käsittelystä perittävästä maksusta säädetään valtion maksuperustelaissa (150/1992) ja liikenne- ja viestintäministeriön asetuksessa Liikenne- ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista (1149/2018).

2.3 Pätevyysalueen muuttaminen

Kun arviointilaitoksen hyväksytyn pätevyysalueen kriteeristö muuttuu esimerkiksi Katakrin uuden version myötä, ei hyväksytty pätevyysalue automaattisesti muutu. Pätevyysalue säilyy hyväksyntäpäätöksen mukaisena niin kauan kuin päätös on voimassa. 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.

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, julkisuuslakia sekä kielilakia. Lain julkisen hallinnon tiedonhallinnasta (Tiedonhallintalaki) 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.[5] Hyväksytyn arviointilaitoksen onkin sopiessaan palveluidensa tarjoamisesta varmistuttava asiakkaaltaan, haluaako se Traficomin hyväksymän arviointilaitoksen palvelun vai arviointilaitosstatuksen ulkopuolisen palvelun[6]. 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[7], 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.

3.2 Arviointikriteeristöt ja niiden soveltamisohjeet

Tässä kuvataan yleiset reunaehdot vaatimusten tulkintakäytännöille. Epäselvissä tilanteissa tulee tulkintaohje pyytää Traficomilta.

3.2.1 VAHTI

Kansallista suojattavaa tietoa sisältävien järjestelmien suojausvaatimukset kuvattiin ennen valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (Tietoturvallisuusasetus). Valtiovarainministeriö on antanut sen toimeenpanon ohjauksesta ja vaatimusten täyttämisestä VAHTI-ohjeita. 1.1.2020 voimaantullut tiedonhallintalaki kumosi Tietoturvallisuusasetuksen. Tietoturvallisuusasetuksen toimeenpanon ohjaukseen tarkoitetut VAHTI-ohjeet on lueteltu liitteessä 1. Haettaessa viranomaishyväksyntää VAHTI-kriteeristöä vasten, kohteelta edellytetään tietoturvallisuusasetuksessa sekä liitteessä 1 mainituissa VAHTI-ohjeissa kuvattujen vaatimusten täyttämistä.

VAHTI 2/2014 (Tietoturvallisuuden arviointiohje) toteaa tietoturvallisuuden arvioinnista seuraavaa:

"*Tietoturvaturvallisuusasetuksen 4 §:ssä[8] säädetään kymmenen vaatimusta tietoturvallisuuden perustasolle. Näitä vaatimuksia täsmentää ja täydentää*

[5] Akkreditoinnin ja Traficomin hyväksynnän edellytyksenä on kuitenkin toiminnallinen ja taloudellinen riippumattomuus.
[6] Esimerkiksi Finasin akkreditointielimenä tehtävä ISO 27001:2013 -arviointi, jota tarjotaan yksityisen sektorin yritykselle, joka ei käsittele viranomaisen salassa pidettävää tietoa.
[7] Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 3 §.
[8] Pitäisi olla 5 §:ssä.

VAHTI-ohje 2/2010, jossa tietoturvatasojen kaikkien kolmen tason vaatimukset on kuvattu yksityiskohtaisesti. Nämä vaatimukset kohdistuvat menettelytapoihin ja prosesseihin eikä niiden perusteella voida tehdä päätöksiä teknisistä yksityiskohdista ja ratkaisuista, joiden avulla tasovaatimukset voidaan täyttää. Tämän seikan korjaamiseksi tietoturvatasot on huomioitu kaikissa asetuksen voimaantulon jälkeen julkaistuissa VAHTI-ohjeissa, joissa annetaan vaatimuksia ja suosituksia eri tietoturvatasoilla sovellettavista ratkaisuista.

Tietoturvatasovaatimuksia toteutettaessa ja arvioitaessa on huomioitava VAHTI 2/2010 -ohjeen lisäksi erityisesti seuraavat ohjeet:

VAHTI 3/2010 Sisäverkko-ohje
VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohje
VAHTI 3/2012 Teknisen ympäristön tietoturvataso-ohje
VAHTI 1/2013 Sovelluskehityksen tietoturvaohje
VAHTI 2/2013 Toimitilojen tietoturvaohje
VAHTI 4/2013 Henkilöstön tietoturvaohje
VAHTI 5/2013 Päätelaitteiden tietoturvaohje".

Traficom soveltaa edellä mainittua ohjeistusta siten, että VAHTI-kriteeristöä vasten arvioitaessa arviointi kattaa VAHTI-ohjeissa 2/2010, 3/2010, 3/2012, 1/2013, 2/2013 ja 5/2013 kuvatut vaatimukset soveltuvin osin. Tilanteissa, joissa vaatimukset ovat keskenään ristiriitaisia, tulkitaan vaatimusten täyttämisen olevan mahdollista siten, että tiukin vaatimus täyttyy.

VAHTI-julkaisuissa viitataan joidenkin vaatimusten osalta Katakriin. Näiden vaatimusten täyttymisen arviointi tulee toteuttaa Katakrissa kuvattujen määritysten mukaisesti.

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.[9]

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

[9] 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).

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

3.2.3 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.

3.2.4 PiTuKri

Traficom on julkaissut Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) keväällä 2019. Traficom tulee ilmoittamaan, kun arviointilaitoksille tulee mahdolliseksi hakea PiTuKri-pätevyyttä. Toistaiseksi PiTuKri-pätevyyden hakeminen ei ole vielä mahdollista.

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[10]. Arvioinnin lopputuloksena arviointilaitos toteaa, täyttyvätkö arvioinnin perustana olevat vaatimukset. Todistuksen voi antaa vain, jos vaatimukset täyttyvät.

Lähtökohtaisesti VAHTI- ja 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[11]. Todistuksen voimassaoloa voidaan jatkaa, jos kohde täyttää kriteerit uuden arvioinnin perusteella.

Viranomaisen tietojärjestelmää tai tietoliikennejärjestelyä koskevan arviointipyynnön tekee viranomainen, jonka määräämisvallassa tai hankittavaksi

[10] ISO 17021 liite E Kolmannen osapuolen auditointi- ja sertifiointiprosessi. Seuranta-auditoinnit ja uudelleenarvioinnit suoritetaan VAHTI- ja Katakri-arvioinneissa, mikäli tästä erikseen osapuolten välillä sovitaan.

[11] Poikkeuksena kuitenkin THL:n määräyksen mukaan tehdyt sosiaali- ja terveydenhuollon tietojärjestelmät, joille voidaan myöntää todistus viideksi vuodeksi, ks. luku 3.6.

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 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.[12] Osittaisen arvioinnin perusteella ei voi saavuttaa yleispätevää VAHTI- tai Katakri 2015 -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 säilytettävä keskeiset arviointitulokseen vaikuttavat todistusaineistot VAHTI- ja Katakri-arvioinneista 6 vuotta arviointitapahtuman päättymisen jälkeen.

Arviointilaitokset eivät voi arvioida sellaisia tietojärjestelmiä, joissa käsitellään NATO:n, EU:n tai ESA:n turvallisuusluokiteltua tietoa. Tällaisten kansainvälistä, turvallisuusluokiteltua tietoa sisältävien tietojärjestelmien tarkastamiseen on Suomessa toimivalta ainoastaan Traficomilla. Näin ollen arviointilaitokset eivät voi ottaa vastaan arviointitoimeksiantoa sellaisesta tietojärjestelmästä, jossa käsitellään kansainvälistä turvallisuusluokiteltua tietoa.

Turvallisuusselvityslain 9 §:n mukaan Traficomilla on toimivalta tehdä yritysturvallisuusselvityksiin liittyvät tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevat selvitykset. Selvityksen pohjamateriaalina on mahdollista käyttää arviointilaitoksen testijärjestelmälle tekemää arviointia.

Tällaisia arviointeja voidaan käyttää esimerkiksi tilanteissa, joissa arviointilaitos tekee arvioinnin, joka kohdistuu erilliseen tietojärjestelmään, jonka

[12] Ks. luku 3.3.5 Todistuksen antamisesta.

yritys haluaisi myöhemmin liittää yritysturvallisuusselvityksen kattamaan tietojärjestelmään/tietojenkäsittely-ympäristöön ja osaksi yritysturvallisuusselvitystä. Tällöin Traficom suorittaa kuitenkin lopullisen yritysturvallisuusselvitykseen liittyvän tarkastuksen. Tässä tulee lisäksi huomioida, etteivät arviointilaitokset voi arvioida sellaisia tietojärjestelmiä, joissa käsitellään EU:n, Naton tai ESA:n turvallisuusluokiteltua tietoa tai muuta sellaista kv-turvaluokiteltua tietoa, jonka käsittely on rajattu vain nimetyille viranomaisille. Lisäksi aina kv-datan tapauksessa on varmistettava Traficomilta ennen tarkastuksen aloitusta, voiko arviointilaitos tehdä arvioinnin, sillä lähtökohtaisesti se ei voi niitä tehdä.

3.3.2 Arvioinnin perustaksi otettujen tietoturvallisuutta koskevien vaatimusten toteutuminen

Kun arviointikriteeristönä käytetään VAHTI:a tai 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) on ne tarkastanut. Arvioinnin perusteella annettavaa todistusta ei voida antaa ilman asianmukaista toimitilojen tarkastamista.

Tietyissä tietoturvallisuutta koskevissa yksittäisissä vaatimuksissa edellytetään kansallisen tietoturvaviranomaisen antamaa hyväksyntää. Tällaista hyväksyntää voidaan edellyttää esimerkiksi salaustuotteiden, yhdyskäytäväratkaisujen ja hajasäteilyä koskevien vastatoimien (TEMPEST) osalta[13]. Arvioinnin kohteen on hankittava viranomaishyväksynnät etukäteen arviointia varten. Arvioinnissa arviointilaitos toteaa, että hyväksyntä on haettu ja että kohteen toiminta vastaa hyväksynnän vaatimuksia ja ehtoja (esim. salaustuotteen käyttöä koskevat ehdot). Arviointilaitos voi hakea salaustuotetta koskevan Traficomin arvion niin sanottuna CAA-pikaprosessina.

3.3.3 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[14].

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

[14] ISO 19011:2011 "Guidelines for auditing management systems"/ SFS-EN ISO 19011 "Johtamisjärjestelmän auditointiohjeet", ISO 27007 Guidelines for information security management systems auditing

Kuva 1. Esimerkki tietoturvallisuuden arvioinnin etenemisestä

3.3.4 Arviointiraportti ja muut arviointiin liittyvät asiakirjat

Tietoturvallisuuden arvioinnista ja suoritetuista tarkastuksista on laadittava arviointiraportti noudattaen standardien ISO/IEC 17021 ja ISO/IEC 27006 vaatimuksia. VAHTI- ja 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. Vastaavan sisältöistä raportointimallia tulee käyttää myös VAHTI-arviointeihin.

Arviointilaitoksen on dokumentoitava arviointitehtävän suorittamisen yhteydessä syntyvä asiakirja- ja todistusaineisto riittävällä tarkkuudella siten, että arvioinnissa tehdyt havainnot voidaan todentaa jälkikäteen. Arviointilaitoksen tulee myös varmistua asiakirja- ja todistusaineiston saatavuudesta havaintojen myöhempää todentamista varten.[15]

[15] Arviointilaitoksen on säilytettävä keskeiset arviointitulokseen vaikuttavat todistusaineistot 6 vuotta arviointitapahtuman päättymisen jälkeen.

3.3.5 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.[16]

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.

Todistuksessa on oltava vähintään seuraavat tiedot:

- Kenelle todistus on myönnetty
- 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.[17]

Arviointilaitoksen tulee asettaa todistuksen voimassaololle päättymispäivä. Todistus voi olla voimassa korkeintaan kolme vuotta.[18]

---

[16] Ks. myös luku 3.4.1.5 rajauksesta.

[17] Muu tieto voi olla esimerkiksi tieto siitä, että arvioinnin yhteydessä on tehty laajempaa arviointia käyttäen muitakin kuin vaatimuksenmukaisia todentamismenetelmiä. Lisäksi riippuen arvioitavasta järjestelmästä tulee todistuksessa huomioida ohjeen luvut 3.6.2 ja 3.7.2.

[18] Toisiolain (552/2019) 26 §:n 3 momentin mukaan arviointilaitoksen myöntämä todistus voi olla voimassa enintään 5 vuotta.

3.3.6 Arviointia koskevien tietojen julkaiseminen

Kun arviointikriteeristönä käytetään muuta kuin ISO/IEC 27001:tä, arviointilaitoksen on asetettava ISO/IEC 17021 -standardin kohdissa 8.1.3 ja 8.3 tarkoitetut tiedot julkisesti saataville vain, jos viranomainen, jonka pyynnöstä arviointi on tehty, on antanut tähän kirjallisen suostumuksen.

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.

3.3.7 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.

Muista seuranta- ja uudelleenarviointitehtävistä arviointilaitos vastaa toimeksiannon perusteella.

3.4 Arviointimenetelmät

3.4.1 Yleisiä arviointitoiminnassa huomioitava periaatteita

3.4.1.1 Asiakastietojen suojaaminen tarkastustoiminnassa

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

- tiedon erottelu / asiakaskohtainen dedikointi[19],
- tarkastuslaitteiston eheys ja mittaustiedon luotettavuus, sekä
- tietojen kuljettamis- ja säilyttämiskäytännöt.

[19] 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[20].

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. Vastaavasti, kun arviointikriteeristönä käytetään VAHTI:a, tulee seuraavat aihepiirit tarkastaa luokkaa korkeamman tason mukaisesti:

1) sovelluskerroksen turvallisuus,
2) jäljitettävyys ja havainnointikyky,
3) tehtävien eriyttäminen, ja
4) tietovarannon fyysinen turvallisuus.

[20] 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.

3.4.1.4 Sovellettavat uhkamallit

Turvallisuusluokan IV järjestelmät on suojattava yleisiltä matalan tai keskitason resursseilla ja/tai osaamisella varustettujen hyökkääjien uhkia vastaan. Esimerkiksi julkisesta verkosta saavutettavat etäkäyttöratkaisujen terminointipisteet on pidettävä tiukasti julkaistujen turvapäivitysten tasolla, ja julkaistujen nollapäivähaavoittuvuuksien hyödyntäminen on estettävä muilla keinoin[21].

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 todentamismenetelmät sekä turvallisuusluokat, joille kyseessä olevia menetelmiä edellytetään.

ID	Todentamismenetelmä	Tasot	Huomioitavaa
H1	Haastattelut	IV ja III	Kohteena soveltuvat henkilöt, tyypillisesti sisältäen johdon, ylläpidon/kehityksen ja loppukäyttäjien edustajat
H2	Dokumentaatioon tutustuminen	IV ja III	Kattaen verkkokuvat, järjestelmäkuvaukset, prosessikuvaukset ja vastaavat

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

Taulukko 1. Hallinnollisen todentamisen vähimmäisvaatimukset

Tässä ohjeessa ei kuvata turvallisuusluokkien II-I järjestelmien turvallisuuden hallinnolliselle todentamiselle asetettavia lisävaatimuksia.

3.4.3 Tekniselle todentamiselle asetettavat vähimmäisvaatimukset

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

ID	Todentamismenetelmä	Tasot	Huomioitavaa
T1	Passiivinen rajapinta-analyysi	IV ja III	Menetelmään sisällyttävä verkko-/järjestelmäkuvien rakentamiset sekä liikenneanalyysit.
T2	Järjestelmä-konfiguraatioiden turvallisuuden tarkastelu	IV ja III	Menetelmän katettava kaikki kohteen turvallisuuteen vaikuttavat osakokonaisuudet[22].
T3	Aktiivinen rajapinta-analyysi	IV ja III	Menetelmään sisällyttävä porttiskannaukset, haavoittuvuusskannaukset (tunnetut haavoittuvuudet) sekä toimintavarmuustestaukset[23] (tuntemattomat haavoittuvuudet).
T4	Sovellusturvallisuuden tarkastelut järjestelmätyypeittäin	IV ja III	Menetelmän katettava kohteen turvallisuuteen vaikuttavien sovelluskomponenttien tarkastelut, esimerkiksi web-sovellukset, Java-palvelin-/asiakasohjelmistot ja ERP-järjestelmien sisäiset pääsynhallintamekanismit.
T5	Salausratkaisujen turvallisuuden todentaminen	IV ja III	Kohteissa, joissa käytetään Traficomin NCSA-toiminnon hyväksymää salausratkaisua, todennettava salausasetusten ja hallintakäytäntöjen turvallisuuden riittävyys. Tilanteissa, joissa kohteessa ei ole käytössä hyväksyttyä salausratkaisua, on ratkaisun turvallisuudelle haettava NCSA:n arvio.

[22] Osakokonaisuuksia ovat tyypillisesti esimerkiksi palvelinten ja työasemien käyttöjärjestelmät sekä muut alustaan asennetut ohjelmistot, verkkolaitteiden konfiguraatiot, tietokantojen konfiguraatiot sekä muut järjestelmän turvallisuuteen vaikuttavat ohjelmistot.

[23] 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).

T6	Käytettävyystestaukset (ml. kuormitustestaukset)	IV ja III	Edellytetään vain järjestelmiin, joilla on korkeat käytettävyysvaatimukset (esim. ihmishenkiä suojaavat turvajärjestelmät). Arviointilaitoksella tulee olla kyky toteuttaa sovellusten stressitestejä, palvelunestohyökkäyksen kestokykytestauksia sekä kyky arvioida kohteen jatkuvuuden hallinnan / toimintavarmuuden menettelyjä.
T7	Fyysisen turvallisuuden suojausten todentamismenetelmät	IV ja III	
T8	Yhdyskäytäväratkaisujen turvallisuuden testaukset	III	Kohteissa, joissa Traficomin Yhdyskäytäväratkaisuohjeen[24] mukaista yhdyskäytäväratkaisua, todennettava toteutetun ratkaisun turvallisuuden riittävyys suhteessa Yhdyskäytäväratkaisuohjeessa kuvattuihin vaatimuksiin. Tilanteissa, joissa kohteessa ei ole käytössä em. ohjeen mukaista yhdyskäytäväratkaisua, on ratkaisun turvallisuudelle haettava NCSA:n arvio.
T9	Poikkeamahavainnointikyvyn testaukset	IV ja III	Menetelmään sisällyttävä erityisesti suojattavan turvallisuusluokan III ympäristön sisällä tehtävien valtuuttamattomien toimien ja niiden yritysten havainnointikyvyn testaus.
T10 (*)	Hajasäteilysuojausten todentaminen	III	Tarkastettava edellytettävä taso tiedon omistajakohtaisesti. Edellytetään esimerkiksi EU:n turvaluokitellulle Confidential-tason tiedolle.
T11 (*)	Luvattomien teknisten laitteiden olemassaolon todentaminen	III	Tarkastettava edellytettävä taso kohdekohtaisesti tiedon omistajalta tai omistajan valtuuttamalta taholta. Ei tyypillisesti edellytetä esimerkiksi palvelintiloihin, joissa ei keskustella salassa pidettävästä tiedosta.

Taulukko 2. Teknisen todentamisen vähimmäisvaatimukset

Taulukossa 2 tähdellä (*) merkityt todentamismenetelmät on mahdollista ulkoistaa DSA-viranomaiselle[25]. Tässä ohjeessa ei kuvata turvallisuusluokkien

[24] Traficomin ohje "Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista", ks. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa.
[25] DSA-viranomaisia ovat suojelupoliisi, pääesikunta, puolustusministeriö ja Traficom.

II-I järjestelmien turvallisuuden tekniselle todentamiselle asetettavia lisävaatimuksia.

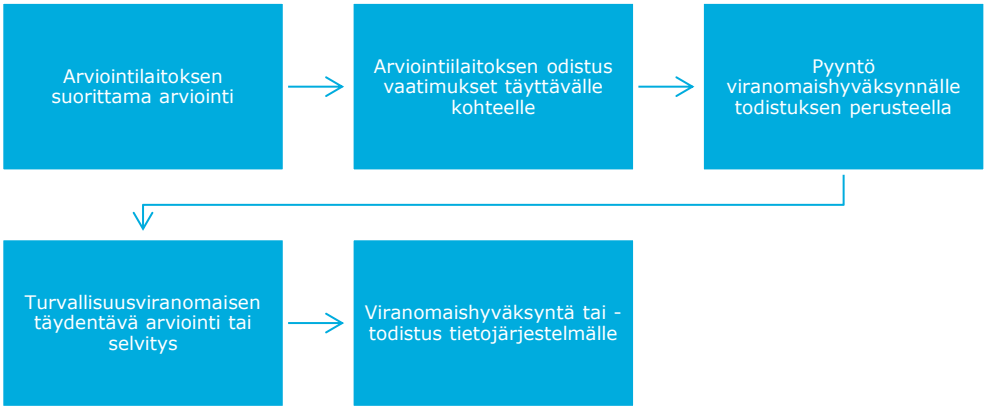
3.4.4 Todentamismenetelmät arviointikriteeristöjen käytössä

VAHTI- ja Katakri-arvioinneissa edellytetään tehtyjen havaintojen oikeellisuuden varmistamista useammasta soveltuvasta lähteestä (vrt. luku 3.4.1.2). VAHTI- tai 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 VAHTI- ja Katakri-arvioinneissaan todentaa vaatimusten täyttymisen tila vähintään Traficomilla hyväksytettyjen, kyseistä arviointikriteeristöä koskevien todennusmenetelmien mukaisesti.

3.5 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. Traficom voi myöntää em. todistuksen joko itse tekemänsä tietojärjestelmäarvioinnin perusteella tai niin, että oikein rajatun ja hyväksytysti läpäistyn tietojärjestelmäarvioinnin on tehnyt arviointilaitos ja arvioinnista on riittävä raportointi.

Jotta arvioinnin kohde saadaan määriteltyä tarkoituksenmukaisesti viranomaishyväksyntään tähtäävissä arvioinneissa, tulee Traficomiin olla yhteydessä jo arvioinnin alkuvaiheessa. Viranomaishyväksynnän saamisen edellytyksenä on aina, että kaikki käytettävän kriteeristön vaatimukset täyttyvät.



Kuva 2. Kohteen hyväksymismenettely

Viranomaishyväksynnän hakemista on kuvattu yksityiskohtaisemmin Traficomin ohjeessa "Liikenne- ja viestintäviraston suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit - Tilaajaorganisaation näkökulma".[26]

Viranomaishyväksynnästä perittävästä maksusta säädetään valtion maksuperustelaissa (150/1992) ja liikenne- ja viestintäministeriön asetuksessa Liikenne- ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista (1149/2018).

3.6 Asiakastietolain mukaisten luokan A tietojärjestelmien ja hyvinvointisovellusten sertifiointi

3.6.1 Arvioitavat tietojärjestelmät

Sosiaali- ja terveydenhuollon tietojärjestelmiä koskee laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021, asiakastietolaki[27]). Laissa määritellään tietojärjestelmien olennaiset vaatimukset ja niiden osoittaminen.

Asiakastietolaissa ja sitä tarkentavissa määräyksissä määritellään, millaisia tietojärjestelmiä luokan A olennaiset vaatimukset koskevat ja mille siten on hankittava sertifiointi. Järjestelmiä ovat esimerkiksi:

- apteekkijärjestelmät,
- Kanta-palvelut,
- asiakastietojen välityspalvelut,
- reseptijärjestelmät,
- sosiaalihuollon asiakastietojärjestelmät sekä
- terveydenhuollon potilastietojärjestelmät.

Asiakastietolaissa *tietojärjestelmällä* tarkoitetaan *tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä, jota valmistajan suunnittelemien ominaisuuksien mukaisesti on tarkoitettu käytettäväksi asiakastietojen sähköiseen käsittelyyn, asiakasasiakirjojen tallentamiseen ja ylläpitoon tai valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen tai jolla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää hyvinvointitietoja* (3 § 6 kohta).

Asiakastietolain mukaiseen arviointiin ei sisälly tietojärjestelmäpalvelun tuottajan, valmistajan eikä käyttäjän (palvelunantajan) toimitilojen arviointi eikä tarkastaminen (37 §).

Asiakastietolain mukaan tietojärjestelmät jaetaan luokkiin A ja B järjestelmän käyttötarkoituksen ja ominaisuuksien perusteella (29 §).

[26] Ks. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa.
[27] https://www.finlex.fi/fi/laki/ajantasa/2021/20210784

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.

Tietojärjestelmän luokittelu on tietojärjestelmäpalvelun tuottajan tehtävä.

Luokkaan A kuuluvat

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

2) valtakunnallisiin tietojärjestelmäpalveluihin liitettäväksi tarkoitetut sosiaalihuollon asiakastietoja ja terveydenhuollon potilastietoja käsittelevät tietojärjestelmät ja hyvinvointisovellukset ja

3) muut käyttötarkoituksensa perusteella sertifioitavat tietojärjestelmät, hyvinvointisovellukset ja välittäjien palvelut

Muut asiakastietolain mukaiset tietojärjestelmät kuuluvat luokkaan B. A-luokka jaetaan edelleen A1, A2 ja A3-luokkiin, jotka erotellaan toisistaan järjestelmän käyttötarkoituksen, järjestelmässä käsiteltyjen asiakastietojen luonteen ja laajuuden sekä järjestelmän riskitason ja kriittisyyden perusteella. THL on ohjeistanut tarkemmin tietojärjestelmien luokittelusta määräyksessä 4/2021 ja sen liitteessä 1.

THL voi päättää epäselvissä tilanteissa tietojärjestelmän luokasta.

3.6.2 Arviointihakemus ja yhteistestaus

Asiakastietolaissa s*ertifioinnilla* tarkoitetaan *menettelyä, jolla todennetaan tietojärjestelmän tai hyvinvointisovelluksen täyttävän sitä koskevat tuotantokäyttöä varten vaadittavat olennaiset vaatimukset* (3 § 20 kohta)*.*

Tietoturvallisuuden arvioinnissa kriteerinä käytettävien tietoturvavaatimusten lisäksi olennaisia vaatimuksia ovat tietojärjestelmiin kohdistuvat toiminnalliset ja yhteentoimivuuden vaatimukset. Osa tietoturvavaatimuksista linkittyy toiminnallisiin ja yhteentoimivuusvaatimuksiin.

Luokkaan A kuuluvan tietojärjestelmän tai hyvinvointisovelluksen tietoturvallisuuden arvioinnin voi suorittaa vain arviointilaitos, jonka pätevyysalueena on VAHTI tai Katakri.

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. Jos kysymyksessä on vanhenemassa olevan todistuksen uusiminen, *yhteydenotto tietoturvallisuuden arviointilaitokseen ja Kelaan tulee tehdä viimeistään kuusi kuukautta ennen aiemman todistuksen vanhenemista (*THL:n määräys 4/2021*)*.

Jos luokan A2 tai A3 -järjestelmän sertifioinnissa ollaan suorittamassa sekä yhteistestaus että tietoturvallisuuden arviointi, arviointilaitoksen on varmistettava Kelalta yhteistestauksen tarve ja tilanne.

Tietoturvallisuuden arviointi voidaan aloittaa vasta sen jälkeen, kun yhteistestaus on suoritettu tai kun Kela on arvioinut yhteistestauksen olevan riittävän pitkällä.

Jos järjestelmän yhteistestaus on vielä kesken, Kela arvioi, voidaanko tietoturvallisuuden arviointi aloittaa ja milloin tietoturvallisuuden arviointi voidaan aloittaa.

Jos kysymys on vanhenemassa olevan todistuksen uusimisesta, on hyvä huomata, että yhteistestauslausunnolla ei ole tiettyä voimassaoloaikaa.

Tietoturvallisuustodistuksen myöntäminen ei edellytä yhteistestausta, jos

1) kyseessä on luokkaan A1 kuuluva tietojärjestelmä, jolle ei suoriteta lainkaan yhteistestausta (esim. asiakastietojen välityspalvelu)
2) kyseessä on uudelleensertifiointi ja järjestelmään toteutettu ja testattu aiemmin vaaditut tietosisällöt ja toiminnallisuudet.

Ennen tietoturvallisuustodistuksen antamista luokkaan A2 tai A3 kuuluvalle järjestelmälle tietoturvallisuuden arviointilaitos varmistaa tietojärjestelmäpalvelun tuottajalta ja Kelalta, että yhteistestauksen kohteena olevaan järjestelmään ei ole tulossa muutoksia, jotka voisivat vaikuttaa tietoturvavaatimusten toteuttamiseen (THL:n määräys 4/2021 luku 7).

Luokkaan A2 tai A3 kuuluvalle järjestelmälle voidaan kirjoittaa tietoturvallisuustodistus vasta sen jälkeen, kun järjestelmä on hyväksytysti läpäissyt yhteistestauksen (THL:n määräys 4/2021 luku 7).

3.6.3 Arviointimenettely ja -kriteeristö

Luokkaan A kuuluvien järjestelmien arviointi toteutetaan arviointilaitoslain ja asiakastietolain säännösten mukaisesti. Tietoturvallisuuden arvioinnin kriteeristönä käytetään THL:n määräyksen 5/2021 mukaisia tietoturvavaatimuksia tai myöhempien määräysten ne korvaavia vaatimuksia. Arvioinnissa noudatetaan tässä ohjeessa ja THL:n määräyksissä kuvattuja menettelyjä.

Luokkaan A kuuluvan tietojärjestelmän vaatimustenmukaisuuden arviointi ja todentaminen kokonaisuutena[28]:

1. *Selvitys järjestelmälomakkeella.* Tietojärjestelmäpalvelun tuottaja antaa selvityksen (järjestelmälomake) siitä, että järjestelmä täyttää kaikki toiminnallisuutta koskevat vaatimukset (ks. THL:n määräys

[28] Asiakastietolain 35.1 § ja määräykset THL 4/2021 luku 7 sertifiointiprosessista ja M 5/2021 liite 5, luku 5 sertifiointiprosessin soveltamisesta

5/2021). Järjestelmälomakkeella tietojärjestelmäpalvelun tuottaja ilmoittaa myös sen, mitkä tietoturvavaatimukset järjestelmässä tai siihen liitettyjen muiden osajärjestelmien kautta täytetään. Lomakkeessa ilmoitetaan myös järjestelmässä toteutetut profiilit eli se, minkä kansallisesti määriteltyjen käyttötarkoitusten vähimmäisvaatimukset järjestelmä täyttää. Myös järjestelmän luokka ja riskitaso sekä luokan A3 järjestelmän mahdollinen kriittisyys ilmoitetaan järjestelmälomakkeella.

2. *Yhteistestaus.* Jos tietojärjestelmältä edellytetään yhteistestaus (järjestelmä kuuluu luokkaan A2 tai A3), se on tehtävä ennen tietoturvallisuuden arvioinnista annettavan todistuksen myöntämistä (THL:n määräyksessä 4/2021 kuvataan yhteistestauksen ja tietoturvallisuuden arvioinnin suhde, huom. yhteen järjestelmään voi kohdistua useita eri ajankohtina testattavia testauskokonaisuuksia.)

3. *Tietoturvallisuuden arviointi ja todentaminen.* 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. Osana arviointia todennetaan siis tietojärjestelmiä koskevien vähimmäisvaatimusprofiilien sisältämien tietoturvavaatimuksien toteutuminen tietojärjestelmässä. Olennaisten vaatimusten todentamisen menettelyistä tulee huomioida erityisesti THL:n määräys 5/2021 luku 10.

Vain silloin, kun tietojärjestelmä täyttää yllä mainitut vaatimukset 1-3, arviointilaitos myöntää tietojärjestelmälle tietoturvallisuustodistuksen. Tietoturvallisuustodistus osoittaa, että kyseinen tietojärjestelmä täyttää ne vaatimukset, jotka sille on asiakastietolailla ja siihen perustuvalla THL:n määräyksellä asetettu.

Luokat A1, A2 ja A3 ohjaavat sitä, millaisella tasolla ja millä menettelyillä (testaus, dokumentointi, validointi jne.) järjestelmiin kohdistuvat vaatimukset on todennettava sertifiointiin kuuluvassa yhteistestauksessa tai tietoturvallisuuden arvioinnissa määräyksen 4/2021 luvun 7 mukaisesti.

Kanta-palveluilta edellytetään aina ulkoista tietoturvallisuuden arviointia. Kanta-palveluilta, jotka sisältävät sosiaali- ja terveydenhuollon palvelunantajille tai asiakkaille tarkoitettuja käyttöliittymiä edellytetään soveltuvin osin tason A3 mukaista sertifiointia. Näitä toimenpiteitä on mahdollista yhdistää tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) mukaisiin Kelalle viranomaistoimijana suoritettaviin tietoturvallisuuden arviointeihin.

3.6.4 Tietoturvallisuustodistuksen sisältö

Yhdellä tietojärjestelmällä 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 3.3.5.

Vähimmäissisällön lisäksi sosiaali- ja terveydenhuollon tietojärjestelmille myönnettävään todistukseen tulee kirjata omina kohtinaan seuraavat asiat (suluissa myös järjestelmälomakkeen vastaavia kohtia):

- Tieto siitä, että kyseessä on asiakastietolain perusteella myönnetty tietoturvallisuustodistus ja siitä, että tietojärjestelmä täyttää THL:n määräyksen sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista vaatimuksista (5/2021) asettamat tietoturvavaatimukset
- Todistuksen yksilöivä tieto
- Tietojärjestelmäpalvelun tuottaja ja järjestelmän valmistaja (jos eri tahot)
- Järjestelmän nimi- ja versiotiedot (3-4)
- Järjestelmän luokka (A1, A2 tai A3 / kriittinen luokan A3 järjestelmä, 6a)
- A3-järjestelmissä huomioitava tarvittaessa maininta paikallisiin luovutuksiin liittyvien toimintojen toteuttamatta jättämisestä (järjestelmälomakkeen tietoturvavaatimukset -välilehti, APAKOL04 ja APAKOL11)
- Järjestelmän riskitaso (perustason tai korkean riskitason järjestelmä, 6b)
- Järjestelmän käyttötarkoitus (5), esim. järjestelmälomakkeessa tietojärjestelmäpalvelun tuottajan antamaa kuvausta (ks. THL:n määräyksen 4/2021 luku 6) hyödyntäen ja siten että käy ilmi, mikäli järjestelmä on
    - Apteekkijärjestelmä
    - Asiakastietojärjestelmä
    - Asiakastietojen välityspalvelu
    - Kanta-palvelu
    - Potilastietojärjestelmä (ja millä tavoin rajattu potilastietojärjestelmä)
- Ilmoitetut järjestelmän tukemat profiilit (7)
- Mihin Kanta-palveluihin järjestelmä liittyy (Resepti /Potilastiedon arkisto / Sosiaalihuollon asiakastiedon arkisto / Kuva-aineistojen arkisto / Omatietovaranto, (8a, 8c)
- Tieto ja kuvaus siitä, onko tietojärjestelmä osa suurempaa kokonaisuutta, ja luettelo tai tieto mahdollisista vaatimuksista, joiden todentaminen on toteutettu tai täyttäminen tapahtuu toisen järjestelmän kautta, tarvittaessa lisätiedot (8b ja järjestelmälomakkeen kohdat, joissa ilmoitettu ”u” – täytetään toisen järjestelmän / osajärjestelmä tai rajapintojen kautta).

- Mahdolliset tarkentavat havainnot, joilla on vaikutusta järjestelmän käyttöönottoihin, säädösten mukaiseen toimintaan tai tietoturvalliseen käyttöön. Erityisesti järjestelmien käyttäjäorganisaatioissa huomioitavat seikat vaatimusten täyttämiseksi. [29]

Arviointilaitos voi myöntää todistuksen A-luokan tietojärjestelmälle, joka toimii osana (osajärjestelmä) laajempaa Kanta-palveluihin liittyvää tietojärjestelmäkokonaisuutta siten, että järjestelmä hyödyntää muita järjestelmäkokonaisuuden osia Kanta-yhteyksien toteuttamiseen tai joidenkin vaatimusten (myös tietoturvallisuusvaatimusten) täyttämiseen. Tällaisista seikoista ja vaatimuksista on oltava selkeä maininta todistuksessa.

Jos todistuksessa havaitaan virhe tai sitä ei ole laadittu tässä ohjeessa kuvatulla tavalla, tulee todistus korjata.

THL:n määräyksen 4/2021 kohdan 7.2 mukaan *Tietoturvallisuustodistus tulisi 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.*

3.6.5 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, joille arviointilaitos on myöntänyt tietoturvallisuustodistuksen.[30]

Arviointilaitoksen myöntämän tietoturvallisuustodistuksen käyttökohteet ovat ainakin seuraavat:

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

[29] Seikat jotka on huomioitava järjestelmän käyttöympäristössä ja seikat jotka on huomioitava käytettäessä järjestelmää yhdessä muiden järjestelmien kanssa. Tarpeen ei ole selostaa, miten jokin ongelma on ratkaistu, vaan kertoa tarvittavat lisätiedot arviointiperusteiden soveltamisesta. Tietoturvallisuustodistukseen kirjoitettu ehto voi olla esimerkiksi se, että tietoturvallisuustodistus on myönnetty järjestelmäkokonaisuudelle ja jos kokonaisuuden järjestelmäarkkitehtuuri muuttuu, tulee vaatimustenmukaisuus arvioida uudelleen. Tietoturvallisuustodistukseen kirjoitettu rajoite voi olla esimerkiksi se, että järjestelmä toteuttaa ostopalveluvaltuutus-toiminnallisuudesta vain järjestäjän osuuden, ei tuottajan osuutta.

[30] Asiakastietolaki 38 §.

- 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

- 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 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.

3.6.6 Muutosarvioinnit, seuranta-auditoinnit ja arviointilaitoksen ilmoitusvelvollisuudet

3.6.6.1 Muutosarviointi

Asiakastietolain mukaan tietojärjestelmäpalvelun tuottajan on ilmoitettava arviointilaitokselle ja Kansaneläkelaitokselle tietojärjestelmän olennaisista muutoksista (32 §). Edelleen lain mukaan *tietoturvallisuuden arviointia koskeva todistus tai yhteentoimivuuden testaus on uudistettava, jos tietojärjestelmään […] tehdään merkittäviä muutoksia, tai olennaisia vaatimuksia on muutettu tavalla, joka edellyttää uutta sertifiointia (32 §).*

THL määräyksen 4/2021 liitteessä 2 määrätään luokkaan A kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien muutosten ilmoittamisesta ja siitä, millaisia muutoksia on ilmoitettava arviointilaitokselle.

Arviointilaitos tekee saamansa muutosilmoituksen pohjalta päätöksen siitä, onko järjestelmälle suoritettava muutosten takia uusi tietoturvallisuuden arviointi. Muutosten arvioinnissa on noudatettava THL:n määräystä 4/2021.

Lain mukaan *arviointi on suoritettava tietojärjestelmän ja hyvinvointisovelluksen käyttötarkoitusta koskevien olennaisten vaatimusten tai järjestelmään tehtyjen muutosten laajuuden mukaisesti* (37 §). Jos arviointilaitos tekee muutosten takia tietoturvallisuuden arvioinnin, muutosarvioinnissa on käytävä läpi vaatimukset, joiden toteutumiseen muutoksilla on vaikutuksia. Mikäli muut vaatimukset täyttyvät tietojärjestelmäpalvelun tuottajan mukaan aiemmin todennetun tasoisesti, voidaan tietoturvallisuustodistus päivittää siten, että aiemman todistuksen voimassaoloaika ei muutu.

Tietojärjestelmäpalvelun tuottaja voi myös päättää, että muutosten takia tarvittavassa tietoturvallisuuden arvioinnissa tähdätään kokonaan uuteen tietoturvallisuustodistukseen. Tällöin tietoturvallisuuden arvioinnissa käydään läpi

kaikki järjestelmän kautta toteutetut tai täytetyt tietoturvavaatimukset ja kirjoitetaan uusi todistus, jolla on uusi voimassaoloaika.

3.6.6.2 Seuranta-auditointi

Tietojärjestelmälle 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 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.

3.6.6.3 Poikkeamat

Jos arviointilaitos toteaa, ettei järjestelmä enää täytä sille asetettuja vaatimuksia tai vaatimustenmukaisuustodistusta ei olisi tullut myöntää, arviointilaitoksen on hyvän hallintotavan mukaisesti kehotettava tietojärjestelmän valmistajaa tai tuottajaa korjaamaan puutteet. Valvontatoimivalta asiassa on asiakastietolain nojalla Valviralla (44 §). Poikkeamailmoituksia koskevan asiakastietolain 41 §:n mukaan muu taho eli myös arviointilaitos voi ilmoittaa Valviralle tietojärjestelmässä havaitsemistaan riskeistä. Riskit voivat liittyä asiakasturvallisuuteen tai tietoturvallisuuteen. Valvira suosittelee, että arviointilaitos tekee sille poikkeamailmoituksen merkittävistä riskeistä, jotka eivät korjaannu säännönmukaisessa arviointiprosessissa.

Asiakastietolain 41 §:n mukaan tietosuojapoikkeamista on ilmoitettava tietosuojavaltuutetulle.

3.6.7 Arvioitavat hyvinvointisovellukset

Tietojärjestelmien lisäksi asiakastietolaissa määritellään hyvinvointisovellukset. Sertifiointivelvoite koskee myös Kanta-palveluihin integroitavia hyvinvointisovelluksia.

Asiakastietolain mukaan *hyvinvointisovelluksella* tarkoitetaan *yksityishenkilön käyttämää omatietovarantoon liittyvää sovellusta, jolla käsitellään hyvinvointitietoja, ja johon henkilö voi saada asiakastietonsa arkistointipalvelusta, reseptikeskuksesta ja tiedonhallintapalvelusta (3 § 13 kohta).*

Kaikki lain määritelmän mukaiset hyvinvointisovellukset kuuluvat luokkaan A ja niille suoritetaan tietoturvallisuuden arviointi. Arviointi siis ei koske sovelluksia, jotka eivät liity tai ole liittymässä Kanta-palvelujen omatietovarantoon.

Hyvinvointisovellusten sertifiointimenettelyt ja niihin kohdistuvat olennaiset vaatimukset mukaan lukien tietoturvallisuuden arvioinnissa todennettavat vaatimukset on määritelty THL:n määräyksessä 6/2021 ja sen liitteissä.

Hyvinvointisovellusten valmistajia koskevat pääosin vastaavantyyppiset velvoitteet kuin tietojärjestelmien valmistajia. Sertifioinnin näkökulmasta on kuitenkin huomioitava seuraavat keskeisimmät erot:

- Hyvinvointitiedot on määritelty erikseen asiakastiedoista. Hyvinvointitietojen ja asiakastietojen elinkaaren hallinnassa, rekisterinpitäjyyden vastuissa ja tietoihin kohdistuvissa oikeuksissa on merkittäviä eroja.
- Hyvinvointisovelluksille ei ole tarkempia luokkia A1, A2 tai A3 eikä riskitason määrittelyä.
- Hyvinvointisovelluksilla ei oleteta olevan sote-organisaatioita käyttäjinä tai vastuutahoina. Näin ollen ei ole sote-organisaatioiden tietoturvasuunnitelmia tai sote-organisaatioita vastaamassa käyttöympäristön tietoturvamenettelyistä.
- Hyvinvointisovellusten arviointikriteereinä käytetään THL:n määräyksen 6/2021 liitteessä kuvattuja kriteerejä.
- Jos hyvinvointisovellus täyttää sekä tietojärjestelmän että hyvinvointisovelluksen määritelmän, sovelletaan ensisijaisesti tietojärjestelmien kriteerejä (THL:n määräys 5/2021) ja täydentävästi hyvinvointisovellusten kriteerejä.
- Hyvinvointisovelluksilla ei ole vastaavaa järjestelmälomaketta tai tietojärjestelmäprofiileja kuin tietojärjestelmillä. Niille on käytössä Hyvinvointisovellusten olennaiset vaatimukset -lomake.
- Hyvinvointisovelluksiin kohdistuu voimassa olevan asiakastietolain mukaan sertifiointi- ja rekisteröintivelvoite, mutta ei vastaavaa Valviran viranomaisvalvontaa kuin tietojärjestelmiin.

Sote-organisaatioiden sähköiset asiointipalvelut eivät ole hyvinvointisovelluksia, jolleivät ne täytä hyvinvointisovelluksen määritelmää. Useat, esimerkiksi potilastietojärjestelmiin integroidut asiointipalvelut täyttävät sen sijaan tietojärjestelmän määritelmän.

Hyvinvointisovelluksiin ja hyvinvointitietoihin liittyviä tietojen hyödyntämisen ja luovuttamisen määräaikoja kuvataan asiakastietolain siirtymäsäännöksissä.

3.7 Toisiolain mukaisen käyttöympäristön tietoturvallisuuden arviointi

3.7.1 Vaatimustenmukaisuuden arviointi

Sosiaali- ja terveysalan tietolupaviranomainen Findata ylläpitää sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019, toisiolaki) mukaisesti tietoturvallista käyttöympäristöä.[31] 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 1/2020[32], 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.

Käytännössä käyttöympäristön tietoturvallisuus on osoitettava tietoturvallisuuden arviointilaitoksen antamalla todistuksella.[33] Tietojärjestelmän tietoturvallisuuden arviointia tulee pyytää ajoissa arviointilaitokselta. Arviointiin on varattava riittävästi aikaa. Tietoturvallisuuden arviointilaitos arvioi toisiolain mukaisesti hakemuksesta, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset. Arviointiperusteena on käytettävä Findatan määräystä 1/2020.[34]

---

[31] Toisiolaki 20 § 1 momentti.
[32] Sosiaali- ja terveysalan tietolupaviranomaisen määräys 1/2020: Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavat vaatimukset.
[33] Toisiolaki 25 § 1 momentti.
[34] Toisiolaki 26 § 1 momentti.

Jos käyttöympäristö täyttää Findatan määräyksen 1/2020 mukaiset tietoturvallisuusvaatimukset, tietoturvallisuuden arviointilaitoksen on annettava suorittamastaan arvioinnista palveluntarjoajalle todistus sekä siihen liittyvä tarkastusraportti.[35] Tämän jälkeen Findata voi harkita ja luovuttaa tietoaineistoja hakijan käsiteltäväksi muussa kuin sen omassa käyttöympäristössä.

3.7.2 Vaatimuksenmukaisuustodistuksen sisältö ja tarkastusraportti

Arviointilaitos myöntää todistuksen käyttöympäristön palveluntarjoajalle.[36] Arviointilaitoksen myöntämän vaatimustenmukaisuustodistuksen vähimmäissisältö on kerrottu luvussa 3.3.5. 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 1/2020: Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavat vaatimukset
- Yksilöintitietoina vaatimustenmukaisuustodistuksen numero/ID, palveluntarjoajan käyttöympäristön nimi[37] ja Y-tunnus/Rekisteröintitunnus
- Jos arviointi tai uudelleenarviointi koskee vain käyttöympäristön osaa, arviointilaitoksen antamaan todistukseen on selkeästi merkittävä, mikä osa käyttöympäristöstä on arvioitu. [38] Lisäksi todistuksessa tulee olla perustelut sille, miksi osaa käyttöympäristöstä ei ole arvioitu.
- Tietoturvallisuuden arviointilaitoksen käyttöympäristölle tai palveluntarjoajalle asettamat rajoitukset[39]
- 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.

---

[35] Toisiolaki 26 § 2 momentti.

[36] 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.

[37] Käyttöympäristön nimen tulee olla yksilöllinen ja siinä muodossa, jossa käyttöympäristöä tarjotaan asiakkaalle. Todistus kirjoitetaan samalle käyttöympäristölle, jonka Valvira rekisteröinti-ilmoituksen perusteella rekisteröi.

[38] Toisiolaki 26 § 2 momentti.

[39] Toisiolaki 27 ja 28 §.

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[40], 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.

3.7.3 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.
- Arviointilaitos lähettää vaatimuksenmukaisuustodistuksen tiedot sekä tarkastusraportin Valviran kirjaamoon salatulla sähköpostilla (kirjaamo[at]valvira.fi). Valvira ylläpitää julkista rekisteriä sille ilmoitetuista vaatimukset täyttävistä käyttöympäristöistä.

3.7.4 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.[41]

Palveluntarjoajan on säilytettävä vaatimustenmukaisuutta koskevat ja muut valvonnan edellytyksenä olevat tiedot vähintään viisi vuotta tietoturvallisen käyttöympäristön tuotantokäytön päättymisestä.[42]

Jos tietoturvallisuuden arviointilaitos toteaa, että käyttöympäristö ei ole täyttänyt tai ei enää täytä toisiolaissa ja Findatan määräyksessä 1/2020 säädettyjä vaatimuksia tai että todistusta ei muutoin olisi tullut myöntää, laitoksen on kehotettava palveluntarjoajaa korjaamaan puutteet ja ilmoittaa tilan-

[40] Toisiolaki 26 § 3 momentti.
[41] Toisiolaki 29 § 1 momentti.
[42] Toisiolaki 29 § 2 momentti.

teesta 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.[43]

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.[44]

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 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

4.2.1 Vuosi-ilmoitus

Osana Traficomin arviointilaitoksiin kohdistuvaa valvontaa, hyväksytyn tietoturvallisuuden arviointilaitoksen tulee toimittaa vuosi-ilmoitus Traficomin kirjaamoon (kirjaamo[at]traficom.fi) ilmoitusvuotta seuraavan vuoden maaliskuun loppuun mennessä. **Vuosi-ilmoitus koskee toimintaa, jota arviointilaitos on harjoittanut roolissaan Traficomin hyväksymänä arviointilaitoksena**.[45] Vuosi-ilmoitus tehdään Traficomin lomakkeella.

4.2.2 Etukäteen ilmoitettavat arviointitiedot ja tilannekuvatiedot

Traficomille tulee ilmoittaa etukäteen arvioinnista, jonka Traficomin hyväksymä arviointilaitos aikoo tässä roolissaan tehdä ja jossa kriteeristönä käytetään VAHTIA tai Katakria.

---

[43] Toisiolaki 27 §.
[44] Toisiolaki 28 §.
[45] Traficom ei valvo luvussa 2.1. kuvattua hyväksytyn tietoturvallisuuden arviointilaitoksen ulkopuolista toimintaa.

Ilmoitus Traficomille tehdään turvapostitse osoitteeseen arviointilaitokset[at]traficom.fi siten, että otsikko alkaa sanalla "Arviointilaitos:" tai arviointilaitoswikin kautta.

Kuukausittain, kunkin kuukauden ensimmäisen viikon aikana, tulee toimittaa excel-tiedostossa **tilannekuvataulukko** kaikista kuluvan vuoden aikana työn alla olevista arvioinneista (mukaan lukien jo aikaisempina vuosina alkaneet toimeksiannot).

Kahden viikon kuluessa uuden projektin alkamisesta tulee toimittaa kyseisen projektin tiedoilla **päivitetty tilannekuvataulukko**. Projektin alkamisajankohdaksi lasketaan asiakkaan kuittaus hyväksytystä tarjouksesta, tai jokin vastaava vahvistus kyseisen projektin alkamisesta.

Ilmoituksen tulee sisältää:

- tieto arvioitavasta kohteesta sekä käytettävä kriteeristö
- arvioinnin ajankohta
- hyväksytyn arviointilaitoksen yhteyshenkilö, jolta voidaan kysyä lisätietoja

Arviointilaitoksen tulee myös ilmoittaa toimeksiannon yhteydessä tarkastettavalle kohteelle, että:

- tarkastuksesta ilmoitetaan Traficomille,
- Traficom voi niin halutessaan osallistua arviointiin ja
- Arviointiraportti ja -todistus toimitetaan Traficomille tiedoksi ja rekisteröitäväksi.

4.2.3 Traficomille toimitettavat arviointiraportit ja todistukset

Traficomin valvontatehtävää varten arviointilaitoksen tulee toimittaa Traficomille kopio Traficomin hyväksymänä arviointilaitoksena antamistaan **arviointiraporteista** ja mahdollisista **todistuksista** kahden viikon kuluessa raportin (ja todistuksen) toimittamisesta asiakkaalle. Raportteja ei kuitenkaan edellytetä arvioinneista, joissa kriteeristönä on käytetty muuta kuin VAHTIa tai Katakria.

Toimitus tulee tehdä USB-medialla, henkilökuriirilla tai vaihtoehtoisesti Traficomin hyväksymää TC-salausta III-mukaisesti käyttäen, turvapostin lisäsuojaamana osoitteeseen arviointilaitokset[at]traficom.fi.

Samalla arviointilaitoksen tulee ilmoittaa Traficomille, saako todistuksen tiedot asiakkaan suostumuksella tallettaa turvallisuusselvitysrekisteriin Arviointilaitoslain 13 a §:n mukaisesti.[46]

[46] Ks. luku 3.3.6 Arviointia koskevien tietojen julkaiseminen

4.2.4 Muutostiedot

Traficomin hyväksymän arviointilaitoksen on ilmoitettava Traficomille sellaisesta toimintaansa koskevasta muutoksesta, jolla on merkitystä laitosta koskevien velvoitteiden kannalta. Ilmoitus tehdään sähköpostitse osoitteeseen arviointilaitokset[at]traficom.fi siten, että otsikko alkaa sanalla "Arviointilaitos:".

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

Jos arviointilaitos lopettaa toimintansa tai sen toiminta siirtyy esimerkiksi yrityskaupalla toiselle yritykselle, kyseessä olisi edellä mainitussa pykälässä mainittu muutos, josta sen tulee ilmoittaa Traficomille. Muutoksen merkittävyyden vuoksi tällainen muutos tulee ilmoittaa Traficomille viipymättä.

Muita tapauksia, joista arviointilaitoksen tulee ilmoittaa Traficomille, ovat esimerkiksi sen johdossa tai auditoijissa tapahtuva muutos sekä yrityksen toimitilojen muutos (esim. uusi toimitila tai olennainen rakenteellinen muutos vanhoissa tiloissa).

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

5 Arviointilaitoksen palveluiden käyttäminen

Arviointilain 3 §:n mukaan valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden arvioinnissa vain Traficomia tai sen hyväksymää arviointilaitosta.

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

Tämän ohjeen luvussa 3.3.1 kerrotaan arviointilaitoksen asiakkaaltaan saamasta toimeksiannosta. Luvussa 3.3.6 kerrotaan arviointia koskevien tietojen julkaisemisen edellytyksistä. Luku 3.3.7 koskee arvioinnin seurantatoimenpiteitä.

Arviointilaitoksen asiakkaan on hyvä huomioida Traficomin valvontatoiminta, jonka vuoksi arviointilaitos toimittaa hyväksyttynä arviointilaitoksena tekemistään raporteista ja myöntämistään todistuksista kopiot Traficomille (ks. luku 4.2.3). Todistuksen tiedot merkitään arviointilaitoksen asiakkaan suostumuksella myös turvallisuusselvitysrekisteriin (ks. luku 4.2.3). Traficomin virkamiehillä on lisäksi mahdollisuus seurata arviointilaitoksen arviointityötä arviointilaitoksen asiakkaan luona (ks. luku 4.2.2).

6 Ohjeen voimaantulo

Tämä ohje tulee voimaan 22.6.2022

Helsingissä 22.6.2022

Ylijohtaja	Sauli Pahlman
Johtaja	Jukka-Pekka Juutinen

7 LIITTEET

1. Tietoturvallisuuden arviointitoimintaa ohjaavat keskeiset normit

Liite 1. 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 sähköisestä käsittelystä (784/2021)**

  Laissa säädetään sosiaali- ja terveydenhuollon asiakastietojen käsittelyssä käytettävien tietojärjestelmien tietoturvallisuusvaatimuksista, niiden todentamisesta sekä hyväksytyn tietoturvallisuuden arviointilaitoksen tehtävistä

  - **Terveyden ja hyvinvoinnin laitoksen määräys 4/2021:** Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista
  - **Terveyden ja hyvinvoinnin laitoksen määräys 5/2021**: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista
  - **Terveyden ja hyvinvoinnin laitoksen määräys 6/2021**: Omatietovarantoon liittyvien hyvinvointisovellusten sertifioinnista ja 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 1/2020**: Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavat vaatimukset

- **Laki sähköisestä lääkemääräyksestä (61/2007)**

Laissa säädetään sähköisestä lääkemääräyksestä, jonka laadinnassa ja toimittamisessa käytettävät tietojärjestelmät on ennen niiden käyttöönottoa arvioitava sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain mukaisesti.

- **Tietosuojalaki (1050/2018)**

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

II Päätökset

- FINAS-akkreditointipalvelun akkreditointipäätös ehtoineen
- Traficomin hyväksymispäätös ehtoineen

III Ohjeet, suositukset tms.

- Traficomin ohje tietoturvallisuuden arviointilaitoksille
-
- Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille

- Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010)
- Sisäverkko-ohje (VAHTI 3/2010)

- Teknisen ICT-ympäristön tietoturvataso-ohje (VAHTI 3/2012)
- Sovelluskehityksen tietoturvaohje (VAHTI 1/2013)
- Valtionhallinnon toimitilojen tietoturvaohje (VAHTI 2/2013)
- Päätelaitteiden tietoturvaohje (VAHTI 5/2013)

VAHTI-julkaisuissa viitataan joidenkin vaatimusten osalta Katakriin. Näiden vaatimusten täyttymisen arviointi tulee toteuttaa Katakrissa kuvattujen määritysten mukaisesti. Tulee myös huomioida, että viranomaishyväksynnän ehtona on hallinnollisen turvallisuuden lisäksi aina myös teknisten suojausvaatimusten täyttäminen.

- Terveyden ja hyvinvoinnin laitoksen määräys sosiaali- ja terveydenhuollon järjestelmien olennaisista vaatimuksista.

- Tulkintalinjaukset ja muut ohjeistukset, jotka luetellaan Traficomin Internet-sivuilla tai jotka muuten on annettu tiedoksi arviointilaitoksille

- Sosiaali- ja terveysalan tietolupaviranomaisen määräys 1/2020: Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavat vaatimukset