


Modulaariset tietojärjestelmäkokonaisuudet ja osajärjestelmät sertifioinnissa

Täydennyksiä sertifioinnin ja olennaisten vaatimusten koulutusmateriaaliin

27.9.2022

Juha Mykkänen ja Antti-Olli Taipale

Tämä materiaali täydentää olennaisten vaatimusten ja sertifioinnin koulutusmateriaalia

- Sote-tietojärjestelmien olennaiset vaatimukset ja sertifiointi - koulutusmateriaali 15.12.2021
- Joulukuun 2021 koulutusmateriaalissa mm. määritelmät, sertifioinnin säädösperusteet, prosessi, tietojärjestelmäpalvelun tuottajaa koskevat velvoitteet, olennaisten vaatimusten eri luokat, jne.
- Järjestelmien luokittelu on muuttunut 2021 asiakastietolain ja määräysten myötä
  - Luokan A (sertifioitavat) piiriin on tullut **myös muita kuin Kanta-palveluihin liittyviä tietojärjestelmiä**
- Tässä materiaalissa
  - Perusteet järjestelmien luokittelusta ja riskitasosta
    - Pääosin sisältöä yllä mainitusta koulutuksesta
  - Modulaaristen tietojärjestelmäratkaisujen erityiskysymyksiä ja vastauksia niihin
    - Miten luokitellaan toisiinsa integroidut järjestelmät ja todennetaan niiden vaatimustenmukaisuus

Sote-tietojärjestelmien riskit ja niihin varautuminen

- Terveys- ja hyvinvointiriskit, potilasturvallisuus (safety): sovellukset ohjaavat vääränlaiseen käyttäytymiseen tai toimivat virheellisesti aiheuttaen suoraan tai välillisesti haittaa tai riskejä asiakkaille
- Tietosuojariskit (privacy): asiakkaan tiedot karkaavat sivullisille
- Tietoturvallisuusriskit (security)
- Riskit sote-palvelujen toimivuuden tai sujuvuuden näkökulmasta (mm. yhteentoimivuus)
- Varautuminen poikkeustilanteisiin
- Varautuminen väärinkäytöksiin
- Varautuminen ohjelmistovirheisiin
- Lainsäädäntöön liittyvät ja sopimukselliset.

- **Kuinka vastataan**:
  - **Ratkaisujen kehittämisessä riskien tunnistaminen ja niihin varautuminen**, testaus
  - **Huomiointi sopimuksissa** (mm. hankinnat, ylläpito, toimijoiden välisten vastuiden määrittely)
  - Kansallisten palvelujen ja tietojärjestelmien pakolliset ominaisuudet (mukaan lukien olennaiset vaatimukset)
  - Testaus- ja tietoturvallisuuden arviointikriteerit (mukaan lukien olennaiset vaatimukset)
  - **Riskitason** ja **järjestelmän luokan** huomiointi sertifioinnissa
  - **Ulkoiset todentamiset** (yhteistestaus ja tietoturvallisuuden arviointi)
  - Tietoturvasuunnitelmat ja niiden omavalvonta
  - Viranomaisvalvonta.

Järjestelmien luokittelu

Määräys 4/2021 luku 5 ja liite 1

- **Luokka A**: sertifioitavat
  - **Luokka A1**: ”tietoturvallisuuden arvioinnin suorittavat”
    - tietoturvallisuuden arviointia vaativat järjestelmät, joilta ei edellytetä yhteistestausta
    - myös muun tyyppisiä järjestelmiä aiempien teknisten Kanta-välityspalvelujen lisäksi
    - luokkaan voi kuulua sekä suppeampia että laajempia järjestelmiä
    - luokkaan voi kuulua laajasti asiakastietoja käsitteleviä / korkean riskitason järjestelmiä, jotka eivät liity Kanta-palveluihin
    - luokasta B luokkaan A siirtyminen mahdollista.
  - **Luokka A2**: ”Kanta-palveluihin liittyvät, suppeat”
    - yhteistestausta ja tietoturvallisuuden arviointia vaativat, Kanta-palveluihin liittyvät, rajattua tietosisältöä tai käyttötarkoitusta palvelevat järjestelmät.
  - **Luokka A3**: ”Kanta-palveluihin liittyvät, laajat”
    - yhteistestausta ja tietoturvallisuuden arviointia vaativat, Kanta-palveluihin liittyvät, sote-palveluja tuottavaan organisaatioon kohdistuvat vaatimukset kattavasti tai merkittävässä määrin täyttävät, laajasti hoidollisia tietoja käsittelevät tai erityisen arkaluonteista tai erityissuojattavaa tietoa sisältävät järjestelmät
    - erikseen ”kriittiset luokan A3 järjestelmät” joissa erityisiä varautumisvaatimuksia.
- **Luokka B**: ei-sertifioitavat
  - asiakas- tai potilastietojen käsittelyyn tarkoitetut järjestelmät
  - voi sisältää mm. erikoistuneita järjestelmiä, lääkinnällisiä laitteita
  - voi sisältää järjestelmiä, joissa tietoturvallisuus varmistetaan pääosin palvelunantajan suojatoimenpiteiden kautta
  - voi sisältää järjestelmiä jotka tuottavat tai käyttävät joitakin tietoja (muiden järjestelmien kautta) Kanta-palveluihin.
- Lisäksi: **luokittelemattomat** (ei asiakastietojen käsittelyyn suunniteltu tietojärjestelmä)
- Esimerkkejä järjestelmien luokittelusta: Määräys 4/2021 Liite 1

Riskitason määrittely

- Tietojärjestelmäpalvelun tuottajan on määriteltävä järjestelmän ***riskitaso***
- Riskitaso ohjaa järjestelmän **luokan** lisäksi erityisesti **tietoturvavaatimusten** kohdistumista ja niiden todentamista
- Riskitason määrittelyssä huomioitava
  - Asiakastietojen käsittelyn laajamittaisuus
    - (tavoitellun tai olemassa olevan) käyttäjäkunnan laajuus, kansalaispopulaation laajuus, eri tyyppisten asiakastietojen käsittelyn laajuus
    - järjestelmän merkitys asiakas- ja potilasturvallisuudelle ja sote-palvelujen toimivuudelle huoltovarmuus ja varautuminen huomioiden
    - käsiteltävien asiakastietojen luonne ja sensitiivisyys
    - tietojen eheyteen liittyvät riskit (mm. valtakunnallisesti kerättävän tiedon laadun ja hyödynnettävyyden näkökulmasta)
    - liitettävyys ja järjestelmän merkitys osana laajempaa tietojärjestelmäkokonaisuutta
    - tiedon säilytykseen ja käsittelyyn liittyvät ulkoistusriskit
    - Sopimukselliset riskit.
- Riskitason arvioinnin tueksi saatavilla mm. ***Riskiarviotyökalu sote-tietojärjestelmille*** (määräys 4/2021 tukimateriaalina)

Määräyksissä olevan luokittelun ja riskitason taustaa

Erityisesti THL Määräys 4/2021

- Luokittelun tarkennusten ja riskitason pohjana erityisesti
  - Kokemukset ja palaute aiemmista säädöksistä, mm. merkittävistä sertifioiduista järjestelmistä edelleen löytyneet ongelmat, kohtuullisuusvaateet ”pienten” järjestelmien sertifioinnissa
  - Tarve järjestelmän käyttötarkoituksen, laajuuden sekä riskien huomiointiin olennaisten vaatimusten kohdistamisessa ja sertifioinnissa (myös mahdollisesti vaikutukset sertifioinnin hintaan ja kuormittavuuteen)
  - Säädösten (GDPR, MDR, tiedonhallintalaki…) riskipohjaistuminen
  - Luonnoksiin saatu lausuntopalaute.

Luokittelun ja riskitason merkitys

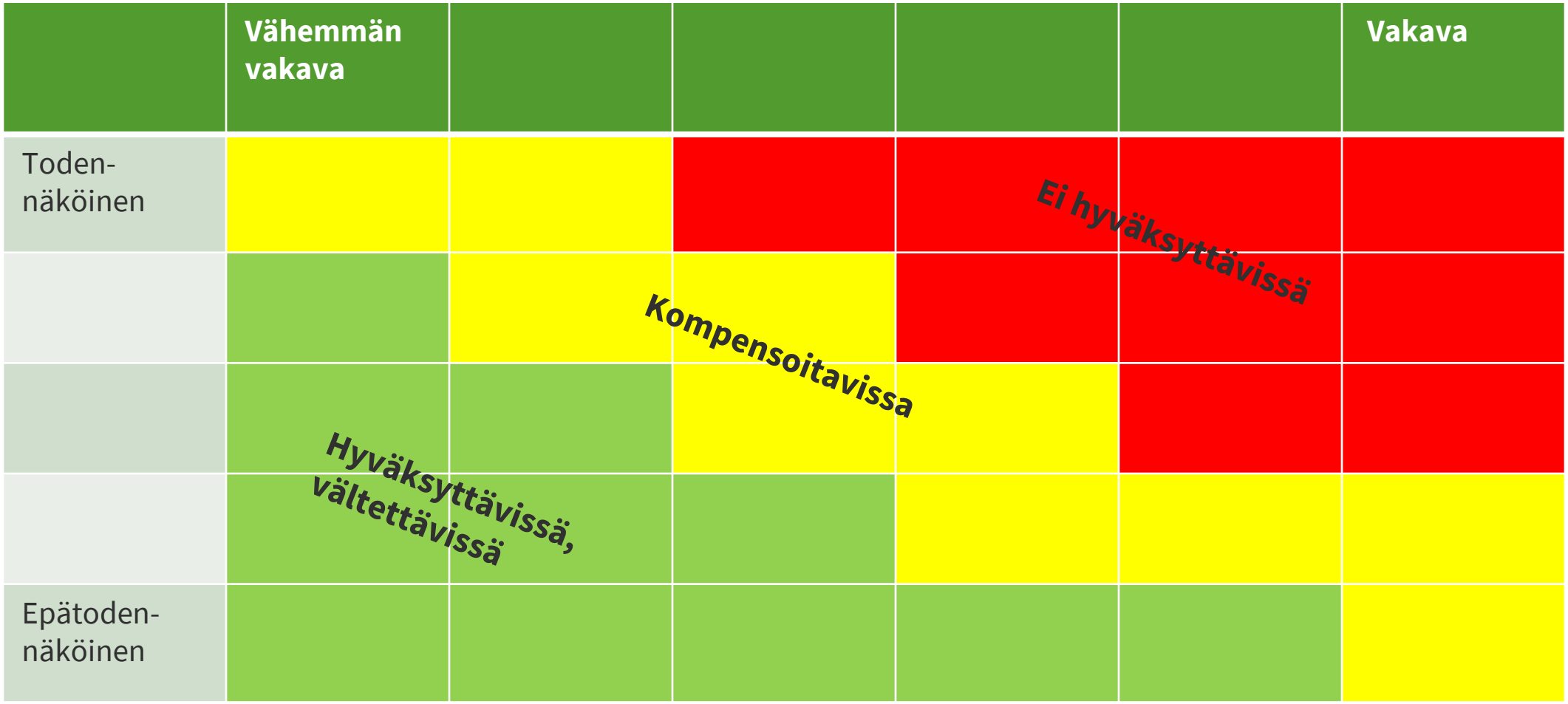
- Luokittelu ohjaa:
  - Kaikki luokkiin B, A1, A2, A3 kuuluvat:
    - Täytettävä käyttötarkoitusta vastaavat olennaiset vaatimukset, ilmoitettava Valviran tietojärjestelmärekisteriin
  - A1 lisäksi:
    - Sertifiointi / tietoturvallisuuden arviointi, tietoturvallisuustodistus
  - A2 ja A3 lisäksi:
    - Sertifiointi: yhteistestaus sekä A1 mukainen tietoturvallisuuden arviointi

- Riskitaso ohjaa:
  - Erityisesti tietoturva- ja varautumisvaatimusten kohdistumista
  - Tietoturvallisuuden arvioinnin ”syvyyttä” mm. haavoittuvuuksien etsiminen
  - Kiinnittämään huomiota riskienhallintaan…

Riski

[Ruck & Lowe]

Yksityiskohtainen riskienhallinta on kuitenkin aina järjestelmä-, organisaatio- ja tilannekohtaista!



Kuinka sertifioinnit ja luokittelut tehdään, kun järjestelmät liittyvät toisiinsa

Modulaarisuuteen liittyviä erityiskysymyksiä

Modulaarisuuden merkitys tietojärjestelmissä

[mukaillen TAPAS-projektin näkemyksiä, Suomen Kuntaliitto]

- Tietojärjestelmäkokonaisuus koostettavissa eri kokoisista osista
- Yhteisesti kuvatut ja määritellyt toiminnalliset kokonaisuudet voivat olla eri toimittajien toimittamia
- Arkkitehtuuri, rajapinnat ja tietorakenteet ovat avoimia ja yhteisesti kuvattuja
- Kokonaisuutta voidaan kehittää pienemmissä osissa ja toimittajariippuvuus vähenee
- Toiminnallisten osakokonaisuuksien kehittäminen ja käyttöönotto nopeutuu
- Kehittämistä pystytään seuraamaan ja ohjaamaan tarkemmin, jolloin riskit pienenevät
- Toimittajia voidaan tarvittaessa vaihtaa helpommin.

Modulaarisuuden huomiointi sertifioinnissa - lähtökohtia

- Viranomaisten määrittelyt ja määräykset ohjaavat joitakin (vähimmäis)vaatimuksia mutta eivät sanele tuotteiden ja organisaatioiden kaikkia arkkitehtuuriratkaisuja, integraatioita tai sopimuksia
- Kansallisten strategisten tavoitteiden mukaisesti pystyttävä tukemaan modulaarisuutta kansallisessa ohjauksessa
  - Määritykset, vaatimukset, sertifiointi, testaus jne.
  - Siirtymä monoliiteistä ja järjestelmäsiiloista ”data- ja järjestelmälukot”
  - Myös innovaatioiden ja erikoistumisen mahdollistaminen
  - Sote KA periaatteita ja strategialinjauksia kuten ”Tue modulaarisuutta ja integraatioita” ja ”Yhteentoimiva ja modulaarinen arkkitehtuuri”
- Sertifioinnissa entistä enemmän eri valmistajien osajärjestelmiä sisältäviä kokonaisuuksia
- Järjestelmän (tai osajärjestelmän) käyttötarkoituksen määrittelee ja rajaa **valmistaja**
- Käyttäjäorganisaatio vastaa omasta järjestelmäkokonaisuudestaan – tuotteen sertifiointia EI tehdä eri käyttäjäorganisaatioiden käyttöympäristöissä
- Toimijoiden välisissä sopimuksissa sovitaan toimijoiden vastuista (usein käyttöympäristökohtaisesti)
- Integraatioita vaihtelevasti osana käyttäjäorganisaation tietohallintotyötä, integraattorin työtä, toimittajan asiakassopimuksia, toimittajien välisiä tai toimittajan ja asiakkaan välisiä sopimuksia…
- Yhden järjestelmän kanssa sertifioitu järjestelmä toimii ja saa toimia myös muiden järjestelmien kanssa (myös eri käyttöympäristöissä)
- Kanta-rajapintojen lisäksi suuri joukko muita rajapintoja (sekä avoimet rajapintamäärittelyt että järjestelmä- ja toimijakohtaisia määrityksiä), ks. esim. HL7 Finland rajapintakartta

Esimerkkejä modulaarisista järjestelmäkokonaisuuksista

- Kanta-liityntäpalvelut ja järjestelmät, joiden kautta liittyy muita järjestelmiä
- Laajojen sairaaloiden järjestelmäkokonaisuudet
  - Runsas joukko ”erillisjärjestelmiä” osasto- tai erikoisalakohtaisesti, esim. laboratorio, anestesia, jne.
- Kuvantamisen järjestelmäkokonaisuudet
- Useat uudet järjestelmät ja ”käyttöliittymäkomponentit integroitavaksi laajempiin järjestelmiin”
- Integraattorin eri komponenteista koostamat portaalijärjestelmät
- Suppeasti toiminnallisesti rajatut (A-luokan) järjestelmät: esim. ostopalvelujärjestelmät yhteiskäytössä ”perusjärjestelmän” kanssa
- Omavalmistus: käyttäjäorganisaation vastuulla olevat järjestelmät / osajärjestelmät yhteiskäytössä eri valmistajien tuotteiden kanssa
- Tekniset Kanta-välityspalvelut, joiden kautta toteutetaan Kanta-liityntäpiste muiden järjestelmien Kanta-liittymistä varten
- ”Yhdellä organisaatiolla useita Kanta-liityntäpisteitä ja A-luokan järjestelmiä” tilanteet
  - Paikallisten (perusjärjestelmät) ja alueellisten järjestelmien (mm. asiointipalvelut) kombinaatiot

Asiakastietolain 784/2021 lähtökohtia

- Vaatimusten on täytyttävä käytettäessä tietojärjestelmää sekä itsenäisesti että ***yhdessä muiden siihen liitettäväksi tarkoitettujen*** tietojärjestelmien kanssa. 34 §
- Palvelunantajan käyttämien tietojärjestelmien on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset. Olennaiset vaatimukset ***voidaan täyttää yhden tai useamman tietojärjestelmän muodostaman kokonaisuuden kautta***. 34 §
- Tietojärjestelmäpalvelun tuottaja voi vastata yhden ***tai useamman*** valmistajan puolesta tietojärjestelmälle asetetuista vaatimuksista. 3 §

Modulaaristen järjestelmäratkaisujen luokittelu ja olennaiset vaatimukset - perusteet

- Myös toisiinsa liittyvien tietojärjestelmien tapauksessa
  - Kukin järjestelmä on itsenäisesti luokiteltava ja rekisteröitävä (ja tarvittaessa sertifioitava) järjestelmä
  - Toisiinsa liittyvät osajärjestelmät voivat olla eri luokissa ja niissä voi olla eri riskitaso
    - luokan A1 tai B järjestelmä voi tuottaa tietoja luokan A3 tai A2 järjestelmään, joka toimittaa ne Kanta-palveluihin
  - Olennaisia vaatimuksia on mahdollista täyttää toisen osajärjestelmän kautta
    - Järjestelmän sertifioinnissa ja ilmoittamisessa on eriteltävä ne olennaiset vaatimukset, joita täytetään toisen osajärjestelmän kautta
  - Olennaisten vaatimusten täyttäminen on pystyttävä todentamaan sertifioinnissa tai tarkastuksessa
    - Myös tilanteissa, joissa vaatimuksia täytetään toisen osajärjestelmän kautta.

Vaatimusten kohdistaminen modulaarisissa järjestelmäkokonaisuuksissa

Määräys 5/2021 Liite 1, Luku 6.3

- Vaatimukset voivat kohdistua eri tavoin koostettaviin järjestelmäkokonaisuuksiin ja niiden osajärjestelmiin
- Eri osajärjestelmillä on omat käyttötarkoituksensa
- Olennaisten vaatimusten täyttäminen on mahdollista eri tavoin koostettujen tietojärjestelmäkokonaisuuksien kautta
- Sertifioinnin toimenpiteitä voidaan kohdistaa useista osajärjestelmistä koostuviin järjestelmiin tai järjestelmäkokonaisuuksiin
- Yhteistestaukseen ja tietoturva-auditointiin hakeuduttaessa on näissä tapauksissa
  - toimitettava selkeä kuvaus kokonaisuuteen kuuluvista osajärjestelmistä ja niiden vastuutahoista
  - kustakin erikseen rekisteröitävästä osajärjestelmästä on kuvattava osajärjestelmän käyttötarkoitus sekä osajärjestelmässä täytetyt olennaiset vaatimukset
  - näiden seikkojen ilmaisemiseen kullekin osajärjestelmälle käytetään määräyksen 5/2021 mukaista **järjestelmälomaketta**
  - järjestelmälomakkeeseen merkitään myös olennaisten vaatimusten täyttäminen muiden osajärjestelmien kautta.

Järjestelmälomake

Määräys 5/2021 Liite 4 Järjestelmälomake

- Lomakepohja, **tietojärjestelmäpalvelun tuottaja** täyttää
- Käytännön työkalu tietojärjestelmän **sertifiointiin ja rekisteröintiin**
- Muodostaa **asiakastietolain edellyttämän selvityksen olennaisten vaatimusten täyttämisestä**
- Järjestelmän **perustietojen** kuvaus
- Järjestelmän **käyttötarkoituksen** tiivis kuvaus
- Tieto siitä, minkä kansallisten **profiilien** mukainen käyttötarkoitus järjestelmällä on
  - Niiden kansallisesti julkaistujen profiilien luettelo, joiden mukaiset vähimmäisvaatimukset järjestelmän kautta täytetään
- Järjestelmän käyttötarkoituksen tarkempi kuvaus suhteessa olennaisiin vaatimuksiin
  - **Toiminnot** jotka ovat osa järjestelmän käyttötarkoitusta
  - **Tietosisällöt** jotka ovat osa järjestelmän käyttötarkoitusta
  - **Tietoturvavaatimukset**, jotka täytetään järjestelmän kautta
- Yksi lomake pohjana Kelan **yhteistestaukseen** (A2 ja A3-luokka), **tietoturvallisuuden arviointiin** (A1, A2 ja A3-luokka) ja Valviran **tietojärjestelmärekisteriin tehtäviin ilmoituksiin** (A ja B-luokka)
- Ohjaa luokituksen kautta tarkempiin määrittelyihin
- **PÄIVITETTY** versio määräyksen 5/2021 yhteydessä.

”Rasti ruutuun”

Määräys 5/2021 Liite 4 Järjestelmälomake

- Lomakkeeseen merkitään järjestelmään toteutetut tai sen kautta täytetyt olennaiset vaatimukset
  - Mukaan lukien järjestelmän käyttötarkoitusta vastaavien profiilien vaatimukset
  - Merkitään myös vaatimukset, jotka täytetään toisen osajärjestelmän kautta

Ryhmä	Id	Otsikko	Selite	Toteutetaan järjestelmässä	Lisätietoja
				[täytä oikea merkintä] **X**=toteutuetaan lomakkeella ilmoitettavassa järjestelmässä **M**= muuttunut järjestelmässä verrattua aiempaan järjetelmälomakkeeseen/versioon. Lisätietoja kohdassa ilmaistava tarkemmin, miten muutettu **U**= ulkoinen, toteutetaan toisen järjestelmän tai rajapinnan kautta, lisätietoja kohdassa tämä ilmaistava tarkemmin	[täytä tarvittaessa, esim. mikäli toteutetaan erikseen sertifioidulla toisella järjestelmällä tai tietyn rajapinnan kautta, kyseisen järjestelmän tai rajapinnan nimi]
ARK			**Kanta-arkistoon liittyvän järjestelmän perustoiminnot**		
	ARK01	Asiakirjojen muodostaminen	Asiakirjan muodostus on tietojärjestelmän säännöillä ohjattu automaattinen prosessi. Asiakirja muodostetaan viimeistään, kun potilasasiakirja-asetuksessa (Sosiaali- ja terveysministeriön		
	ARK02	Lomakeasiakirjan muodostaminen	Itsenäisiä lomakkeita ja todistuksia käytetään tiedonsiirtoon eri organisaatioiden välillä. Lomakkeet ja todistukset voivat toimia täysin itsenäisinä sisältäen myös potilaan tunnistamiseen		
	ARK04	Lomakeasiakirjan välittäminen kolmannelle osapuolelle	Arkistoitu asiakirja voidaan välittää kolmannelle osapuolelle kuten eri viranomaisille. Välittäminen voidaan tehdä uuden asiakirjan muodostamisen yhteydessä tai se voi kohdistua aiemmin		

Ote järjestelmälomakkeen täyttöohjeesta

Merkitse:

1) Toiminnot-välilehdelle järjestelmässä toteutetut toiminnot

2) Tietosisällöt-välilehdelle järjestelmässä käsiteltävät tietosisällöt

3) Tietoturvavaatimukset-välilehdelle järjestelmässä toteutetut tai sen kautta täytettävät tietoturvavaatimukset seuraavasti:

X = toteutetaan lomakkeella ilmoitettavassa järjestelmässä

M = muuttunut järjestelmässä verrattua aiempaan järjestelmälomakkeeseen/versioon. Lisätietoja kohdassa ilmaistaan tarkemmin, miten muutettu

U = ulkoinen, toteutetaan toisen järjestelmän, osajärjestelmän tai rajapinnan kautta, lisätietoja -kohdassa ilmaistaan tarkemmin, mahdollista käyttää myös yhdessä M-merkinnän kanssa.

Luokkien A1 ja B rajapinta

- Luokitteluun ohjeita ja esimerkkejä määräyksessä 4/2021, esim.
  - Määräys 4 liite 1, luokan A1 (tietoturvallisuuden arviointi, ei yhteistestausta) kriteerejä:
    - b) Järjestelmät tai osajärjestelmät, joiden yhteentoimivuuden vaatimukset on todennettu toisen järjestelmän kautta, mutta joihin kohdistuu todennettavia tietoturvavaatimuksia. Esimerkiksi erikoisalakohtaista palvelua tuottavan palvelunantajan ensisijainen potilastietojärjestelmä tai asiakastietojärjestelmä X, jossa Kanta-yhteistestaus ja Kanta-rajapinnat sekä osa tietoturvavaatimuksista on toteutettu ja sertifioitu toisen järjestelmän Y kautta, mutta käyttöliittymän kautta todennettavat tai muut käyttäjäorganisaation kannalta keskeiset tietoturvavaatimukset edellyttävät kyseisten tietoturvavaatimusten todentamista järjestelmän X kautta. Kanta-palveluja hyödyntävät toisen järjestelmän kautta Kanta-palveluihin integroidut tietojärjestelmät, joita palvelunantaja voi käyttää Kanta-liittymiseen, kuuluvat vähintään luokkaan A1.
    - e) Asiakas- tai potilastietoja luokan B kriteerien mukaisesti käsittelevät järjestelmät, joissa asiakastietojen käsittelyyn kohdistuu korkea riskitaso.

- Monet järjestelmät, jotka **aiemmin olleet luokkaa B siirtyvät luokkaan A1**
  - Erityisesti käytännössä Kanta-palvelujen käyttämiseen käytettävät järjestelmät
  - Kanta-yhteentoimivuusvaatimusten / rajapintojen ja useiden tietoturvallisuusvaatimusten täyttäminen ja todentaminen voi olla osoitettavissa toisen järjestelmän kautta, mutta osa vaatimuksista (erityisesti jotkin tietoturvallisuus, usein myös muita olennaisia vaatimuksia) toteutettava käytännössä myös tai pelkästään ”loppukäyttäjän edustajärjestelmässä”.

Usein kysyttyjä kysymyksiä / modulaariset järjestelmäkokonaisuudet 1/2

- Voiko yhdessä yhteistestauksessa tai tietoturvallisuuden arvioinnissa kohteena olla (ja myös lausunnon tai todistuksen saada) useita osajärjestelmiä? **Kyllä.**
- Onko jokaisesta järjestelmästä osana sertifiointia nimettävä kaikki ne järjestelmät / tuotteet, joiden kanssa integroituna se voi toimia tuotannossa? **Ei,** mutta on osana sertifiointia nimettävä ne joiden kanssa sertifioidaan.
- Voiko tietyn profiilin vaatimukset täyttää useasta osajärjestelmästä muodostuvan kokonaisuuden kautta. **Kyllä.**
- Voiko tietojärjestelmästä ilmoittaa järjestelmälomakkeella ominaisuuksia, jotka toteutetaan ulkoisen osajärjestelmän / rajapintojen kautta? **Kyllä** (”ulkoinen järjestelmä”, pystyttävä osoittamaan); vaatimuskohtaisesti on kuitenkin tarkasteltava, onko vaatimus täytettävissä VAIN ulkoisen järjestelmän kautta.
- Voiko yhdellä tietojärjestelmäpalvelun tuottajalla olla useita kerralla sertifioitavia osajärjestelmiä osana yhtä laajempaa tietojärjestelmäkokonaisuutta? **Kyllä.**

Usein kysyttyjä kysymyksiä / modulaariset järjestelmäkokonaisuudet 2/2

- Voiko ”kerralla” sertifioida sekä järjestelmäkokonaisuuden että siihen kuuluvia osajärjestelmiä? **Kyllä.** Tällöin huolehdittava, että on alusta lähtien selvää, että kunkin osajärjestelmän tiedot (esim. nimeäminen, käyttötarkoitus, järjestelmälomake) ja vastuut ovat koko prosessin ajan erotettavissa.
- Voiko yksi järjestelmä kuulua moneen eri luokkaan? Lähtökohtaisesti **ei** (sertifiointi ja rekisteröinti ”korkeimman luokan” mukaisesti), ellei ole useita samaan pohjaan perustuvia järjestelmätuotteita, jotka on tarkoitus rekisteröidä ”erillisinä tuotteina”.
  - Case: reseptiominaisuudet suoraan järjestelmässä (ohjaisi luokkaan A3), mutta sosiaalihuollon arkiston ominaisuuksia toisen järjestelmän kautta (”aiempi luokka B”) → järjestelmä kuuluu luokkaan A3 + on tehtävä tarvittavat merkinnät siitä että sosiaalihuollon profiilit tai sosiaalihuollon arkistoon liittymisen ominaisuudet toteutetaan toisen järjestelmän kautta – luokittelun, sertifioinnin ja rekisteröinnin lähtökohta on järjestelmälähtöinen ja asiakasorganisaatiolähtöinen (mitä käyttäjät / palvelunantajat pystyvät järjestelmällä tekemään), ei Kanta-palvelulähtöinen (mihin Kanta-palveluihin yhteys on rakennettu ja testattu).
- Voiko yhdessä järjestelmäkokonaisuudessa olla eri luokkiin kuuluvia osajärjestelmiä? **Kyllä.**
- Onko sertifioinnissa aina oltava yksi ”pääintegraattori” joka vastaa järjestelmäkokonaisuudesta? **Ei,** mutta osallistujien sovittava keskenään järjestelmien ja toimijoiden väliset vastuut, integraatiot ja osallistumiset sertifiointiin. ”Yksi pääkoordinaattori järjestelmäkokonaisuuden sertifioinnissa” on hyvä ja suositeltava käytäntö.
- Voiko luokassa B edelleen toimia loppukäyttäjille tarjottavia tietojärjestelmiä? **Kyllä**, ks. luokittelun kriteerit *mukaan **lukien riskitaso***.

Voiko tietojärjestelmäpalvelun tuottaja ottaa vastuun toisen valmistajan tuotteesta?

- Lähtökohta asiakastietolaki 34 §: ”Vaatimusten on täytyttävä käytettäessä tietojärjestelmää sekä itsenäisesti että yhdessä muiden siihen liitettäviksi tarkoitettujen tietojärjestelmien kanssa.”
- Voi, jos toimijat näin ovat sopineet (esim. maahantuoja, integraattori), **mutta**
  - ottaa tällöin vastuun myös vaatimustenmukaisuuden osoittamisesta ja rekisteröinnistä
  - vastaa siitä, että Suomen säädösten mukaiset vaatimukset täyttyvät ja voidaan todentaa
  - toimijoiden välisillä sopimuksilla suuri merkitys, sopimuksia ei kuitenkaan käydä läpi sertifioinnissa tai rekisteröinnissä
- Sama periaate ainakin osin sovellettavissa myös modulaarisissa järjestelmissä
  - ”Tietojärjestelmäkokonaisuudesta vastaava taho”, ”integraattori”, ”liityntä- ja alustapalvelun tuottaja” voi vastata vaatimusten todentamisesta
    - Realistisempaa kuitenkin yleensä, että vastaa **osasta** vaatimuksia kuin että vastaa **kaikista**
  - Merkittäväkin osa vaatimuksista voi olla toisen osajärjestelmän kautta täytettäviä / todennettavia
  - Toista järjestelmää hyödyntävä järjestelmä (esim. jos ”ostaa palvelun jolla liittyy Kantaan”) vastaa myös siitä, miten ostetun palvelun kanssa toimittaessa oma järjestelmä toimii oikein
- Huom. sertifioinnin lähtökohtana EI liitäntäkomponentin vaan järjestelmän vaatimustenmukaisuus: Valviran tietojärjestelmärekisterissä ja todistuksissa vaatimukset täyttävät tietojärjestelmät ”joita sote-palvelunantaja voi hankkia ja käyttää”
  - Esim. ”jos käytän järjestelmällä Kanta-palveluja, pystyttävä osoittamaan miten järjestelmässä täytetään luokan A3 tai A2 vaatimukset”.

Kysymyksiä, toisen järjestelmän kautta / kanssa sertifioitavat tietojärjestelmät

- ”Auditoinnin sisältö epäselvä, kun Kanta-liittämiseen käytetty järjestelmä hoitaa osan tietoturvavaatimuksista”
  - Kuvattava sekä ”Kanta-liittämiseen käytetyn järjestelmän 1 osalta” että ”sen kautta liittyvän järjestelmän 2 osalta” (kunkin osajärjestelmän omalla järjestelmälomakkeella):
    - Mitkä tietoturvallisuusvaatimukset voidaan täysin todentaa ”Kanta-palveluihin yhteydessä olevan” järjestelmän 1 kautta
    - Mitä tietoturvallisuusvaatimuksia todennettava molemmissa (1 ja 2)
    - Mitä todennettava järjestelmässä 2 (toisen kautta liittyvä järjestelmä)
  - Joka tapauksessa eri osajärjestelmistä omat järjestelmälomakkeet, joissa otetaan kantaa kuhunkin vaatimukseen (täytetään tai todennetaan, täytetään toisen järjestelmän kautta, ei täytetä / ei relevantti)
  - Kanta-liittämiseen käytetyn järjestelmän tietojärjestelmäpalvelun 1 tuottaja voi tukea järjestelmäänsä hyödyntäviä muita tietojärjestelmäpalvelujen 2 tuottajia esim. ilmaisemalla selkeästi järjestelmälomakkeessa, mitkä vaatimukset voidaan täyttää ja todentaa (täysin tai alustan osalta) järjestelmän 1 kautta
  - Toimijoiden sovittava riittävän tarkasti keskenään vastuista vaatimusten täyttämisessä ja todentamisessa

Vaatimustenmukaisuus on markkinoilla toimimisen ja tuotantokäyttöönottojen edellytys

- Esitetty huolia sertifioinnin kynnyksestä ja kustannuksista
- Aiemmin realisoitunut merkittäviä tietoturvariskejä sertifioimattomissa järjestelmissä – uudistetuissa säädöksissä nähty tarpeelliseksi tuoda sertifioinnin piiriin järjestelmiä, joiden kautta voi realisoitua merkittäviä riskejä
- Regulaation tarkoitus on, että markkinoilla on vain vähimmäisvaatimukset täyttäviä järjestelmiä
  - Suomessa asetetaan lain nojalla olennaisia vaatimuksia: toiminnallisuus, yhteentoimivuus, tietoturvallisuus
  - Sertifioinnin vaatimus- ja todentamistasoa on nostettu ja nostetaan suunnitellusti (mm. uudet tietoturvauhat ja poikkeamista saadut opit, vaatimusten selkeytystarpeet, yhteiskunnan kriittisissä toiminnoissa varautuminen…)
  - Vaatimuksia voi täyttää eri tavoin ja vain kunkin järjestelmän käyttötarkoituksen mukaisessa laajuudessa, mutta vähimmäisvaatimukset on täytettävä
  - Vaatimusten täyttämisessä ja osoittamisessa saa tehdä yhteistyötä niiden kanssa, jotka vaatimuksia auttavat täyttämään (ml. osajärjestelmät, joilla hoidetaan keskeisiä tietoturvavaatimuksia tai Kanta-liitettävyyttä)
  - Huom. myös vaatimusten kohdistaminen ja sertifiointi ”modulaarista” ja suppeissa järjestelmissä suppeampaa kuin laajoissa – **todennetaan VAIN käyttötarkoituksen mukaiset vaatimukset**
  - Vaatimusten (erityisesti määräysten) valmistelussa kuulemisvelvoite – vaatimuksiin on mahdollista ehdottaa muutoksia ennen kuin ne tulevat voimaan (ks. mm. lausuntokierroksen pohjalta tehdyt muutokset / määräys 5/2021)
- Uusimmat määräykset mahdollistavat aiempaa paremmin ”eri laajuisten”, ”eritasoisten” ja ”eri käyttötarkoituksiin räätälöityjen” (eri hintaisten?) tietoturvallisuuden arviointien suorittamisen esim. järjestelmän käyttötarkoituksesta, riskitasosta, luokasta tai laajuudesta riippuen
- Vaatimustenmukaisuuden toteuttaminen ja sen osoittaminen on myös käyttäjille ja asiakkaille merkki siitä, että järjestelmä on laadukas ja turvallinen ja että vaatimustenmukaisuus on pystytty osoittamaan Suomen säädös- ja toimintaympäristössä
  - **Sertifioitu on laadukkaampi kuin sertifioimaton**

Muuta huomioitavaa

- Useissa tietoturvallisuusvaatimuksissa linkkejä niihin toiminnallisiin vaatimuksiin, joihin tietoturvavaatimus liittyy
  - Konteksti / lisätiedot / tulkinnat löytyvät usein viitattujen vaatimusten ja niissä olevien lähteiden kautta
- Nykyisen lain voimassa ollessa myönnettävät todistukset ovat nimeltään ”Tietoturvallisuustodistus” tai ”Todistus tietoturvallisuuden arvioinnista”
- Yhteistestauksen tuloksia tai yhteistestauslausuntojen otsikoita ei (enää) toisteta tietoturvallisuustodistuksessa
  - Määräys 4/2021, luku 7:
    - ”Yhteistestauksen tuloksia ei ilmaista tai kerrata tietoturvallisuustodistuksessa.”
    - ”Jos luokan A2 tai A3 tietojärjestelmä on sertifioitavana siten, että sille suoritetaan **sekä yhteistestaus että tietoturvallisuuden arviointi**, on tietojärjestelmäpalvelun tuottajan huolehdittava siitä, että yhteistestauksen ja tietoturvallisuuden arvioinnin kohteena on sama järjestelmäversio tai sellainen versio, jossa yhteistestattaviin olennaisiin vaatimuksiin liittyvät mahdolliset järjestelmämuutokset eivät vaikuta arvioitaviin tietoturvavaatimuksiin. 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**.
  - Todistuksessa saa näkyä tieto edellä kuvatusta tarkistuksesta tai tieto että järjestelmä on yhteistestattu (ilman yksityiskohtia mm. yhteistestauslausuntojen tai testattujen pakettien nimeämistä)
  - Valviran tietojärjestelmärekisteriin välittyy yhteistestauksista yksityiskohtainen tieto yhteistestauslausuntojen kautta

Kiitos!

sotetiedonhallinta@thl.fi