Kanta-sertifiointi ja omavalvonta – yleiskuva ja prosessit

Versio 09, 7.7.2015

Sisällys

1 Dokumentin tarkoitus 2
2 Yleiskuva 2
3 Toimijat 3
4 Prosessit 4
4.1 Prosessi: Asiakasorganisaation omavalvonta, välittäjän valinta ja Kantaan liittyminen – yleiskuva 4
4.2 Prosessi: Tietojärjestelmän olennaisten vaatimusten sertifiointi: Kanta-yhteistestaus ja tietoturvallisuuden auditointi 5
4.3 Prosessi: Kanta-välityspalvelun sertifiominen 6
4.4 Prosessi: Vaatimustenmukaisuustodistuksen uudistaminen 7
4 Lisätietoja 9

1 Dokumentin tarkoitus

Tämä dokumentti on tukimateriaalia, jossa kuvataan yleiskuva, osallistujat ja prosessit Kanta-palveluihin liittyvien tietojärjestelmien ja välittäjäpalvelujen sertifioinnissa sekä sertifioinnin liittyminen toimijoiden omavalvontaan. Lain säädökset ja aihepiirin määräykset ovat noudatettavia dokumentteja, joita tämä dokumentti ja erilliset ohjeet tukevat.

Dokumentti on tarkoitettu tietojärjestelmien valmistajille ja tietojärjestelmäpalvelujen tuottajille sekä niille Kanta-palveluihin liittyville tahoille, joita omavalvontasuunnitelmien laatiminen koskee. Dokumentissa kuvataan myös sertifiointiin ja valvontaan osallistuvien toimijoiden ja viranomaisten työnjakoa.

2 Yleiskuva

Omavalvonta

Sote-palveluntuottajien on lain ja määräysten mukaisesti huolehdittava tietoturvallisuuden toteutumisesta toiminnassaan. Omavalvonta on keino tämän tavoitteen toteuttamiseen. Omavalvontaa toteutetaan omavalvontasuunnitelman laatimisen ja sen toteuttamisen kautta. Suunnitelmassa on otettava kantaa siihen, miten asiakas- ja potilastietojen käsittelyssä ja tietojärjestelmien käytössä huolehditaan keskeisistä tietoturvallisuuteen vaikuttavista asioista. Tässä dokumentissa ei käsitellä omavalvontaa yksityiskohtaisesti, mutta yleiskuvassa on mukana omavalvonnan suhde sertifiointiin sekä sote-palvelutuottajien että välityspalvelujen osalta. Osana omavalvontaa kuuluu varmistua siitä, että käytettävillä Kanta-palveluihin liittyvillä järjestelmillä ja Kanta-välityspalveluilla on asianmukaiset vaatimustenmukaisuustodistukset.

Sertifiointi

Kanta-palveluihin liittyvien tietojärjestelmien sertifioinnin säädösten ja määräysten mukaisesti A-luokkaan kuuluvien tietojärjestelmien ja tietojärjestelmäpalvelujen on oltava sertifioituja. Sertifiointi sisältää seuraavat pääosat tai -vaiheet:

- Toiminnallisten vaatimusten kuvaaminen ja järjestelmän luokittelu (valmistaja tai tietojärjestelmäpalvelun tuottaja)
- Kanta-yhteistestaus (Kela, tietojärjestelmän valmistaja tai tietojärjestelmäpalvelun tuottaja)
- Kanta-tietoturva-auditointi (hyväksytty tietoturvallisuuden arviointilaitos, valmistaja tai tietojärjestelmäpalvelun tuottaja)
- Muutosilmoitusten teko ja käsitteleminen tietojärjestelmiin tehdyistä olennaisista muutoksista tai olennaisten vaatimusten muuttuessa

Tietojärjestelmän valmistaja tai tietojärjestelmäpalvelun tuottaja vastaa yllä kuvatun sertifiointikokonaisuuden läpiviennistä omien tuotteidensa tai palvelujensa osalta.

Tietojärjestelmien vaatimustenmukaisuuteen linkittyy keskeisesti myös palvelun antajien (tietojärjestelmien käyttäjäorganisaatiot) tai Kanta-välittäjänä toimivien tahojen tekemä omavalvontasuunnitelma, jonka yhtenä osana on sen varmistaminen, että käytettävät tietojärjestelmät ovat säädösten ja määräysten mukaisesti sertifioituja.

Sertifioinnin ja auditoinnin perusteena Kanta-palveluihin liittyen ovat kulloinkin voimassa olevat määrittelyt.

Kokonaisuuden keskeisimpien prosessien yleiskuva on luvussa 4.1. Prosessikuvauksissa näkyvät lakiviittaukset ovat viittauksia lakiin 250/2014 (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain muuttamisesta).

3 Toimijat

Dokumentissa ja prosessikuvauksissa käytetään seuraavia sidosryhmäkuvauksia, joiden merkitykset ja päävastuut suhteessa omavalvontaan ja sertifiointiin ovat seuraavat:

- **Asiakasorganisaatio / palvelun antaja:** terveydenhuollon toimintayksikkö, sosiaalihuollon palvelujen antaja (järjestävä viranomainen, julkinen tai yksityinen palvelun tuottaja), työterveydenhuollosta vastaava työnantaja, apteekki, itsenäisenä ammatinharjoittajana toimivaa terveydenhuollon ammattihenkilö
    - vastaa omavalvontasuunnitelmasta ja asiakas- ja potilastietojen käsittelystä toiminnassaan
- **Järjestelmän valmistaja:** taho, joka on vastuussa sosiaali- ja terveydenhuollon tietojärjestelmän suunnittelusta ja valmistuksesta, riippumatta siitä toimiiko tämä taho myös tietojärjestelmäpalvelun tuottajana
    - vastaa järjestelmään kohdistuvien vaatimusten toteuttamisesta järjestelmässä
- **Tietojärjestelmäpalvelun tuottaja:** taho, joka tarjoaa palvelun antajalle tietojärjestelmäpalvelua, jossa käsitellään asiakas- ja potilastietoja, ja joka vastaa tietojärjestelmän valmistajalle asetettuihin vaatimuksiin valmistajana, valmistajan lukuun tai valmistajan puolesta
    - vastaa järjestelmään kohdistuvien vaatimusten todentamisesta sekä sertifioinnista (mukaan lukien yhteistestaus ja tietoturvallisuuden auditointi), tietojärjestelmäpalvelun tuottamisesta palvelun antajille sekä tietojärjestelmiin liittyvistä ilmoituksista
- **Kanta-välityspalvelun toteuttaja:** Tietojärjestelmäpalvelun tuottaja, joka toteuttaa teknisen Kanta-välityspalvelun, jonka avulla toinen tietojärjestelmä liittyy Kanta-palveluun, vastaa Kanta-välityspalvelun tietoturva-auditoinnista sekä Kanta-välittäjäpalvelulta vaadittavista ilmoituksista. Samaa sertifioitua Kanta-välityspalvelua on mahdollista käyttää useissa Kanta-liityntäpisteissä tai useiden eri välittäjien toiminnassa.
- **Välittäjä:** palvelun antajan Kanta-liityntäpisteen toteuttamisessa käyttämä palveluntarjoaja, jolla on tässä roolissa mahdollisuus nähdä salaamattomia potilastietoja, esimerkiksi ylläpitotoimien yhteydessä. Välittäjä vastaa välityspalvelun tuottajan omavalvonnan toteuttamisesta sekä siitä, että liityntäpisteen toteuttamisessa täytetään Kanta-välityspalvelua koskevat olennaiset vaatimukset. Välittäjä voi vastata Kanta-liityntäpisteen varmenteen hakemisesta ja hallinnoinnista ja siitä, että liityntäpisteessä käytettävään Kanta-välityspalveluun kohdistuvat sertifiointivaatimukset täyttyvät. Välittäjä voi joissakin tapauksissa olla myös Kanta-välityspalvelun toteuttaja.
- **Tietoturvallisuuden arviointilaitos:** viestintäviraston hyväksymä taho, joka suorittaa sertifiointiprosessin osana olevan tietoturvallisuuden auditoinnin, tuottaa vaatimustenmukaisuustodistuksen ja ottaa vastaan ilmoituksia järjestelmiin tehtävistä muutoksista
- **Kanta-palvelut:** Kelan palvelu, jonka vastuulla on Kanta-palveluiden (Sähköinen resepti-, Potilastiedon arkisto- ja Omakanta –palvelut sekä Lääketietokanta) toteuttaminen, ylläpito ja kehittäminen
- **Kanta-yhteistestausvastaava:** suunnittelee ja koordinoi yhteistestauksen, ottaa vastaan ilmoituksia järjestelmiin tehtävistä muutoksista
- **Kanta-asiakastuki:** tarjoaa tukipalveluja Kanta-palveluiden asiakkaille
- **THL/OPER:** viranomainen, joka antaa määräykset olennaisista vaatimuksista ja omavalvontasuunnitelmasta

- **Valvira:** valvontaviranomainen, joka ylläpitää rekisteriä tietojärjestelmistä ja valvoo ja edistää tietojärjestelmien vaatimustenmukaisuutta
- **Viestintävirasto:** valvontaviranomainen, joka hyväksyy tietoturvallisuuden arviointilaitokset ja valvoo niitä

4 Prosessit

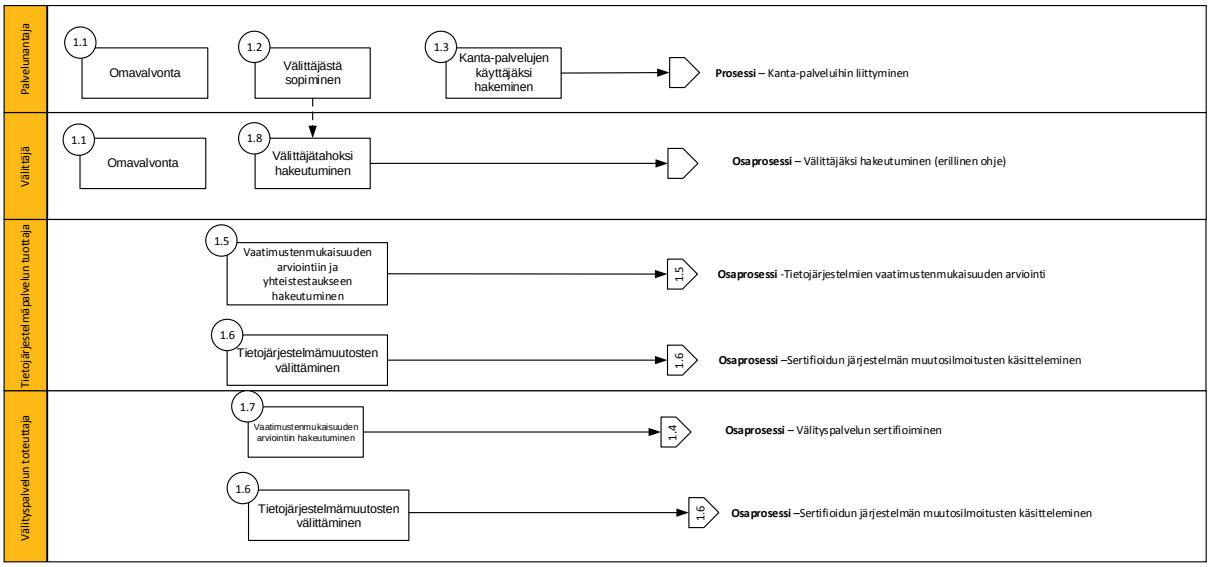
4.1 Prosessi: Asiakasorganisaation omavalvonta, välittäjän valinta ja Kantaan liittyminen – yleiskuva

Prosessin tavoite: Palveluntantajien ja välityspalvelujen tuottajien omavalvonnan ja Kanta-palveluihin liittymisen tietoturvallisuuden varmistaminen, tietojärjestelmien ja Kanta-välityspalvelujen sertifiointi

Prosessin käynnistymisehto tai -tapahtuma:
- säädösten voimaantulo (kaikki)
- omavalvonnan toteuttamisen aloittaminen, välittäjätahon valinta, Kanta-palveluihin liittyminen (palvelunantaja)
- välittäjäksi hakeutuminen (välittäjä)
- sertifiointiprosessiin hakeutuminen (tietojärjestelmäpalvelun tuottaja)
- olennaiset tietojärjestelmämuutokset (tietojärjestelmäpalvelun tuottaja)

Prosessin lopputulos:
- palvelunantajalla on omavalvontasuunnitelma jonka mukaisesti se toimii
- palvelunantaja voi olla hakeutunut Kanta-palvelujen käyttäjäksi ja huomioinut toiminnassaan tällöin vaadittavat olennaiset vaatimukset ja riittävän omavalvonnan tason
- palvelunantajan ja mahdollisen välittäjän käyttämien välityspalveluiden osalta on varmistettu omavalvonnan ja sertifioinnin vaatimusten toteutuminen
- Kanta-palveluihin liittyvät tietojärjestelmät ja Kanta-välityspalvelut (luokka A) on sertifioitu olennaisten vaatimusten osalta, niiden olennaisten tietoturvavaatimusten täyttyminen on todennettu ulkoisella auditoinnilla ja järjestelmien yhteentoimivuus on varmistettu Kanta-yhteistestauksen kautta
    - sekä ennen järjestelmien käyttöönottoa että silloin, kun järjestelmiin tehdään olennaisia muutoksia

Prosessikuvaus:



4.2 Prosessi: Tietojärjestelmän olennaisten vaatimusten sertifiointi: Kanta-yhteistestaus ja tietoturvallisuuden auditointi

Prosessin tavoite: Kanta-palveluihin liittyvä tietojärjestelmä tai tietojärjestelmäpalvelu täyttää olennaiset toiminnallisuuteen, yhteentoimivuuteen ja tietoturvallisuuteen liittyvät vaatimukset ja on läpäissyt sertifiointiprosessin

Prosessin käynnistymisehto tai -tapahtuma: tietojärjestelmäpalvelun tuottaja hakeutuu sertifiointiprosessiin

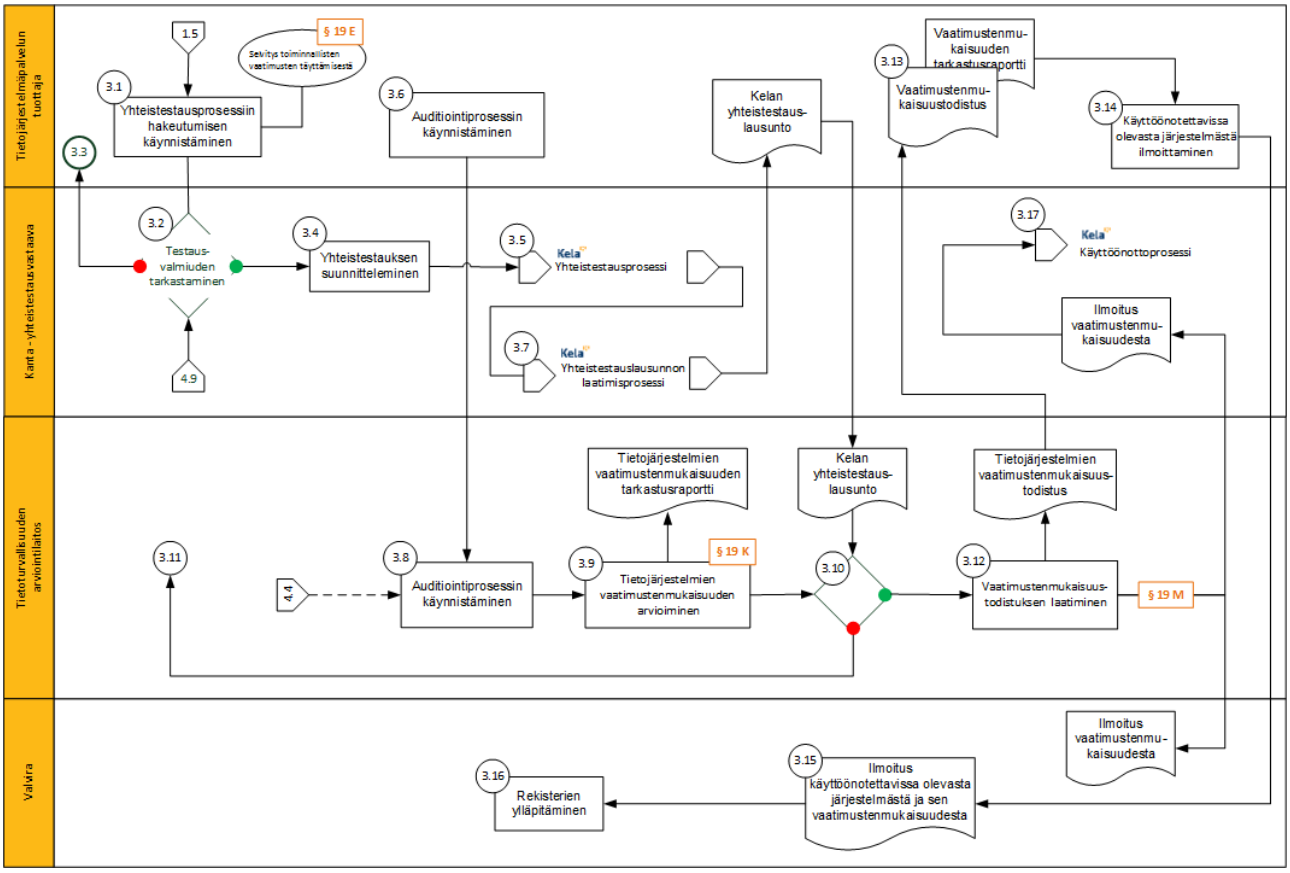
Prosessin lopputulos:

- tietojärjestelmästä tai tietojärjestelmäpalvelusta on kuvattu sen käyttötarkoitus ja ne toiminnalliset vaatimukset jotka se täyttää
- tietojärjestelmä tai tietojärjestelmäpalvelu on läpäissyt hyväksytysti Kanta-yhteistestauksen
- tietojärjestelmä tai tietojärjestelmäpalvelu on läpäissyt hyväksytysti olennaisten tietoturvavaatimusten auditoinnin
- tietojärjestelmällä tai tietojärjestelmäpalvelulla on vaatimustenmukaisuustodistus ja vaatimustenmukaisuusraportti
- tietojärjestelmästä tai tietojärjestelmäpalvelusta on asianmukaiset tiedot Valviran rekisterissä

Lisätietoja:

- sertifiointiprosessia ei suoriteta kaikkien käyttöympäristöjen osalta erikseen, vaan riittää, että eri käyttöympäristöissä käytettävä Kanta-palveluihin liittyvä tietojärjestelmä tai tietojärjestelmäpalvelu (tai sen versio) läpäisee sertifiointiprosessin vain kerran (ennen ensimmäistä tuotantokäyttöön ottoa tai Kanta-palveluihin liittymistä palvelun antajan käyttöympäristössä) suhteessa kulloinkin voimassa oleviin olennaisiin vaatimuksiin ja voimassaolosäädösten mukaisesti
- tietojärjestelmän tai tietojärjestelmäpalvelun tuottaja tai valmistaja vastaa siitä, että Valviralle toimitetaan ilmoitus tuotantokäyttöön otettavasta tietojärjestelmästä tai tuotantokäytön päättymisestä
- Valviralle toimitettavan ilmoituksen mukana on toimitettava selvitys vaatimustenmukaisuuden toteutumisesta (vaatimustenmukaisuustodistus) ja tuotantokäytön aloittamisajankohdasta

Prosessikuvaus:



4.3 Prosessi: Kanta-välityspalvelun sertifiominen

Prosessin tavoite: välityspalvelun sertifioinnin toteuttaminen

Prosessin käynnistymisehto tai -tapahtuma: välityspalvelun toteuttaja hakeutuu auditointiprosessiin

Prosessin lopputulos:

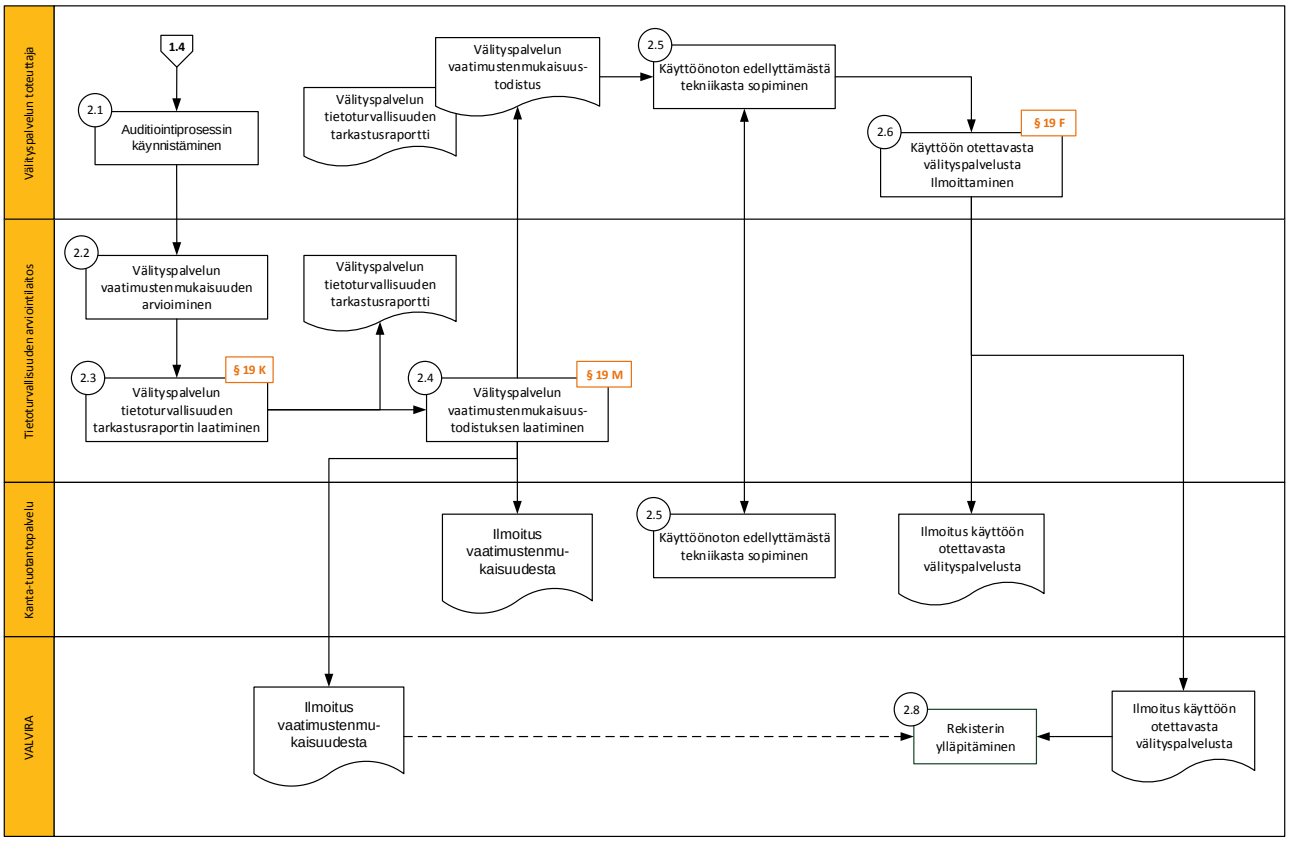
- Kanta-välityspalvelusta on kuvattu sen käyttötarkoitus ja ne toiminnalliset vaatimukset jotka se täyttää
- Kanta-välityspalvelu on läpäissyt hyväksytysti olennaisten tietoturvavaatimusten auditoinnin
- Kanta-välityspalvelulla on vaatimustenmukaisuustodistus ja vaatimustenmukaisuusraportti
- Kanta-välityspalvelusta on asianmukaiset tiedot Valviran rekisterissä

Lisätietoja:

- välityspalvelun toteuttaja voi olla sama taho tai eri taho kuin Kanta-liityntäpistettä hallinnoiva välittäjä; välittäjien on hakeuduttava välittäjäksi THL:n välittäjärekisteriohjeen mukaisesti: http://www.thl.fi/tilastoliite/koodistopalvelu/OHJE_KanTa_V%E4litt%E4j%E4rekisteri.pdf
- sertifiointiprosessia ei suoriteta kaikkien käyttöympäristöjen osalta erikseen, vaan riittää, että eri käyttöympäristöissä käytettävä Kanta-palveluihin liittyvä välityspalvelu (tai sen versio) läpäisee

auditointiprosessin vain kerran (ennen ensimmäistä tuotantokäyttöön ottoa tai Kanta-palveluihin liittymistä palvelun antajan käyttöympäristössä) suhteessa kulloinkin voimassa oleviin olennaisiin vaatimuksiin ja voimassaolosäädösten mukaisesti
- välityspalvelun toteuttaja vastaa siitä, että Valviralle toimitetaan ilmoitus tuotantokäyttöön otettavasta Kanta-välityspalvelusta tai tuotantokäytön päättymisestä; Valviralle toimitettavan ilmoituksen mukana on toimitettava selvitys vaatimustenmukaisuuden toteutumisesta (vaatimustenmukaisuustodistus) ja tuotantokäytön aloittamisajankohdasta

Prosessikuvaus:



4.4 Prosessi: Vaatimustenmukaisuustodistuksen uudistaminen

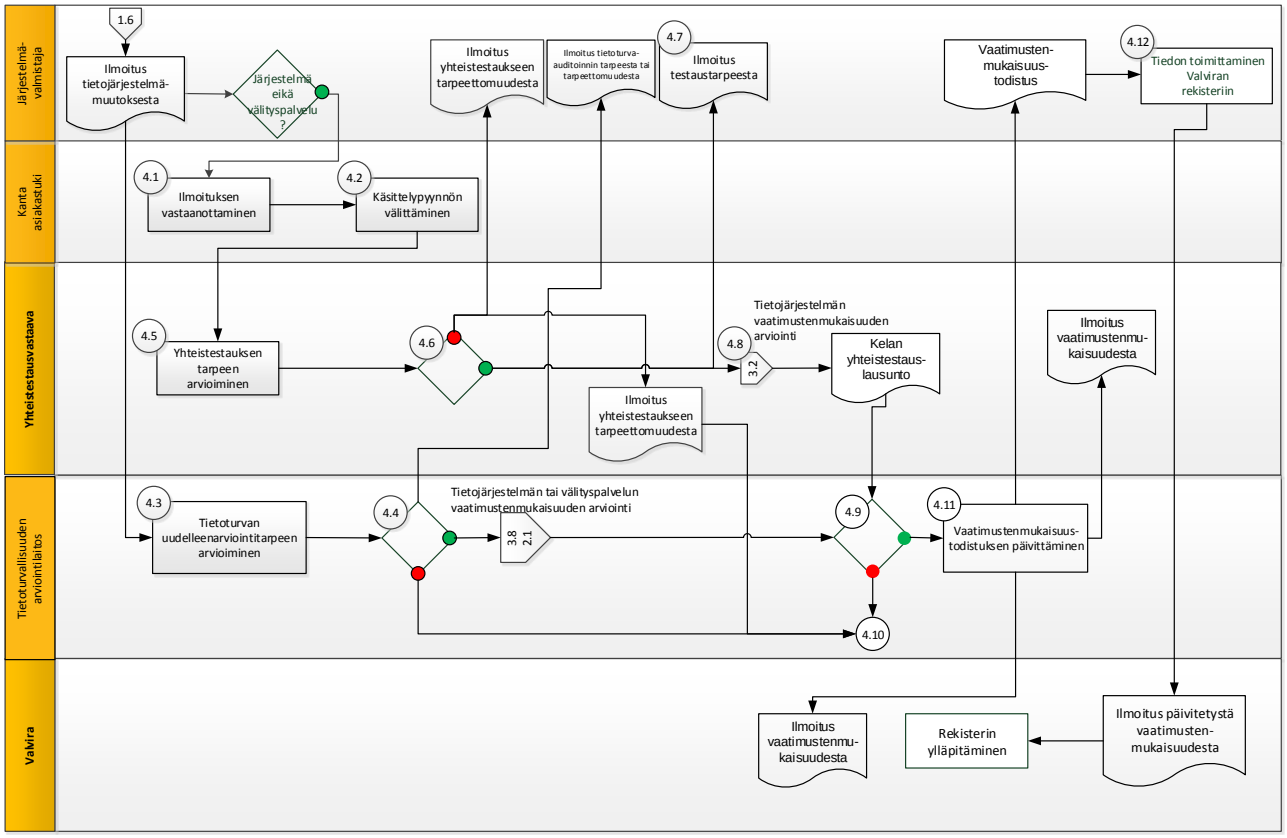
Prosessin tavoite: Kanta-palveluihin liittyvien tietojärjestelmien tai Kanta-välityspalvelun olennaisten muutosten edellyttämät sertifiointiprosessin osat (tarvittaessa yhteistestaus ja tietoturvallisuuden uudelleen auditointi) on suoritettu siten että muutokset sisältävä versio täyttää olennaiset toiminnallisuuteen, yhteentoimivuuteen ja tietoturvallisuuteen liittyvät vaatimukset ja on läpäissyt sertifiointiprosessin.

Prosessin käynnistymisehto tai -tapahtuma: merkittävä tietojärjestelmämuutos (esim. uusi versio), joka edellyttää tai voi edellyttää uudelleen sertifiointia, tai sellaiset muutokset olennaisissa vaatimuksissa jotka edellyttävät vaatimustenmukaisuustodistuksen uudistamista.

Prosessin lopputulos:

- tietojärjestelmän tai tietojärjestelmäpalvelun olennaisten muutosten edellyttämällä tasolla on tarvittaessa suoritettu uudelleen Kanta-yhteistestaus tai tietoturvallisuuden auditointi tai sellaiset osat niistä, joilla olennaisten vaatimusten toteutuminen voidaan todentaa
- tietojärjestelmästä tai tietojärjestelmäpalvelusta on tarvittaessa päivitetty sen käyttötarkoitus ja ne toiminnalliset vaatimukset jotka se täyttää
- tietojärjestelmän tai tietojärjestelmäpalvelun uusi versio täyttää Kanta-yhteistestauksessa edellytettävät yhteentoimivuuden vaatimukset
- tietojärjestelmän tai tietojärjestelmäpalvelun uusi versio täyttää olennaiset tietoturvavaatimukset
- tietojärjestelmällä tai tietojärjestelmäpalvelulla on tarvittaessa uusi tai päivitetty vaatimustenmukaisuustodistus ja vaatimustenmukaisuusraportti
- tietojärjestelmästä tai tietojärjestelmäpalvelusta tai sen uudesta versiosta on asianmukaiset ja ajantasaiset tiedot Valviran rekisterissä

Prosessikuvaus:



4 Lisätietoja

http://www.kanta.fi/web/ammattilaisille/sertifiointi

https://www.thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/tiedon-ja-vaatimusten-yhdenmukaistaminen

Ilmoitukset tai lisätietoja niiden toimittamisesta:

Kelalle lähetettävät ilmoitukset vaatimustenmukaisuudesta:
kanta@kanta.fi

Valviralle tehtävät ilmoitukset, lisätietoja:
http://www.valvira.fi/terveydenhuolto/terveysteknologia/valviralle-tehtavat-ilmoitukset

Sertifiointiin tai omavalvontasuunnitelmaan liittyvät kysymykset:
kantapalvelut@thl.fi

Yhteistestaukseen liittyvät kysymykset:
kantakehitys@kanta.fi

Terveyden ja hyvinvoinnin laitos • Institutet för hälsa och välfärd • National Institute for Health and Welfare
Mannerheimintie 166, Helsinki, Finland PL/PB/P.O. Box 30, FI-00271 Helsinki, puh/tel +358 20 610 6000