# Kanta-palvelut: tieto- ja sanomaliikenteen tietoturvavaatimukset

## 1. Yleistä

Tässä dokumentissa kuvataan keskeisimmät Kanta-palveluissa käytössä olevat tietoturvaan liittyvät vaatimukset ja suositukset kommunikoitaessa Kanta-palveluihin. Tietoturvavaatimukset rajaavat Kanta-palvelujen yhteydessä olevien tahojen hyödyntämien laitteiden ja ohjelmistojen konfiguraatioita esimerkiksi käytettyjen standardien ja profiilien, avainpituuksien sekä tiivistefunktioiden osalta. Osittain näistä varmistutaan sertifiointimenettelyllä (lähinnä Kantaan liittyvien järjestelmien käytäntöjen osalta) ja osa tarkistuksista on ohjelmallisia kunkin yhteydenoton yhteydessä (siltä osin kuin tarkistus voidaan tehdä Kanta-rajapinnassa). Tarkkojen hyväksyttävien tiivistefunktioiden, avainpituuksien ym. osalta nojataan Viestintäviraston suosituksiin sekä VRK:n linjauksiin ja keskeisimpien osalta ne toistetaan tässä dokumentissa.

## 2. Määritelmät

Keskeiset Kanta-liittymän järjestämiseen liittyvät käsitteet on seuraavia tarkennuksia lukuun ottamatta kuvattu Liittymismallit Kanta-palveluihin -dokumentissa.

### 2.1 Päästä päähän -yhteys

Päästä päähän -yhteydellä tarkoitetaan apteekki- tai potilastietojärjestelmän ja Kanta-palvelujen välistä sanoma- ja tietoliikenneyhteyttä. Tämä yhteys voi kulkea välittäjäpalvelimien kautta ja muodostua useista erillisistä tietoliikenneyhteyksistä. Liityntäpisteen ja Kanta-palvelujen väliselle tietoliikenneyhteydelle asetetut sanomaliikenteen salausta ja sen osapuolten tunnistamista koskevat vaatimukset koskevat myös kaikkia muita päästä päähän -yhteyteen sisältyviä tietoliikenneyhteyksiä. Esim. organisaation tietojärjestelmän ja Kanta-välittäjän välinen tietoliikenneyhteys pitää salata ja sen osapuolet tunnistaa samantasoisella menettelyllä kuin liityntäpisteen ja Kanta-palvelujen välinen yhteys.

### 2.2 Sisäverkon yhteys

Sisäverkon yhteydellä tarkoitetaan tässä yhteydessä asiakkaan reunareitittimien sisäpuolella olevaa lähiverkkoa. Operaattorin runkoverkon kautta kulkevat yhteydet eivät ole sisäverkon yhteyksiä, vaikka ne olisi toteutettu suljettuna asiakasverkkona.

## 3. Sanomaliikenteen tietoturvavaatimukset

1. *Vaatimuksena on*, että liikenne liityntäpisteen ja Kanta-palvelun välillä salataan ja osapuolet tunnistetaan TLS-tekniikalla (tuotantoympäristössä[1] 1.3.2016 alkaen vähintään TLS-versio 1.2) käyttäen VRK:n myöntämiä palvelinvarmenteita (mutual authentication). Palvelinvarmenteissa on käytettävä Viestintäviraston TLS-salausvahvuussuosituksen mukaisesti vähintään 2048-bittisiä RSA-avaimia. Tällä hetkellä voimassa olevat salausalgoritmikombinaatiot (cipher suites) saa tarvittaessa Kanta-palveluista pyytämällä[2].
2. *Vaatimuksena on*, että sähköisen allekirjoituksen osalta noudatetaan Kanta-allekirjoitusmäärityksessä[3] esitettyjä vaatimuksia käytettävien salausalgoritmien ja tiivistefunktioiden osalta.

---

[1] Asiakastestiympäristössä 15.10.2015 alkaen vähintään TLS versio 1.2

[2] Osoitteesta tekninentuki@kanta.fi. Kela pidättää oikeuden päivittää listausta tarpeen mukaan esimerkiksi Viestintäviraston tietoturvaohjeisiin pohjautuen. Näistä muutoksista informoidaan tarpeen ilmetessä välittömästi. Normaalin muutosmenettelyn mukaisia etukäteisilmoitusaikoja ei kuitenkaan välttämättä noudateta.

[3] Kanta.fi – Ammattilaisille – Tietotekniikan ja yhteyksien toteuttajille – Kanta-arkkitehtuuri: Sähköisen allekirjoituksen määritys ja soveltamisopas

3. *Vaatimuksena on*, että aina varmennepohjaisesti tunnistauduttaessa tai allekirjoituksia tarkistettaessa tarkistetaan varmenteen voimassaolo varmentajan sulkulistaa vasten.
4. *Vaatimuksena on*, että Kanta-osoitehakemistossa on olemassa määritelty yhteys (oman tai ulkoistetun) liityntäpisteen ja Kanta-liittyjäorganisaation välillä (syntyy liittymishakemuksen täyttämisen yhteydessä)
5. *Vaatimuksena on,* että Kanta-osoitehakemistossa on määriteltynä riittävät käyttöoikeudet kullekin Kanta-palvelua käyttävälle liityntäpisteen ja liittyjäorganisaation yhdistelmälle (syntyy liittymishakemuksen täyttämisen yhteydessä)
6. *Vaatimuksena Potilastiedon arkistoon liikennöitäessä on*, että Kanta-organisaatiorekisterissä on olemassa määritelty yhteys liittyjäorganisaation ja rekisterinpitäjän välillä (vain Potilastiedon arkiston käyttöä varten, syntyy liittymishakemuksen täyttämisen yhteydessä). Poikkeuksena ovat erikseen määriteltävät yksityisen terveydenhuollon vuokralaisjärjestelyt.
7. *Vaatimuksena on*, että palvelinvarmenteen subject/serialNumber-kentän OID-koodi yksilöi liityntäpisteen ja vastaa Kanta-osoitehakemiston tietoja.
8. Mikäli liityntäpisteen toteuttaa joku muu kuin Kanta-liittyjä (eli käytetään välittäjää) *on vaatimuksena*, että
    a. Liikenne liittyjän potilastieto- tai apteekkijärjestelmältä ulkoistetulle liityntäpisteelle tulee salata vähintään vastaavan tasoisella menetelmällä kuin TLS siltä osin kuin se kulkee muualla kuin organisaation sisäverkossa (esimerkiksi operaattorin runkoverkko, vaikka käytössä olisi operaattorin suljettu yhteys).
    b. Sanomaliikenteen kaikkien osapuolten identiteetti tulee varmentaa. Varmentaminen on pakollista organisaatioiden välisessä tiedonsiirrossa, jossa käytetään muita kuin sisäverkon yhteyksiä. Tapauksissa, joissa potilastietojärjestelmien- tai apteekkijärjestelmien palvelimet sijaitsevat samassa konesaliympäristössä tiedonsiirtoon hyödynnettävien erillisten laitteistojen kanssa (kuormantasaajat, SSL-kiihdyttimet tms.) sekä mahdollisen välityspalvelun kanssa, ei varmennepohjainen tunnistaminen näiden välillä ole pakollista. Tämä kuitenkin edellyttäen että konesalin- ja käyttöympäristön sisäisestä tietoturvasta on huolehdittu auditointikriteereissä esitettyjen vaatimusten mukaisesti.
    c. Liityntäpisteen toteuttajan tulee varmistaa, että sanoma on lähetetty oikean tahon nimissä (eli HL7-sanoman controlActProcess / authorOrPerformer / assignedPerson / assignedPerson / representedOrganization / id vastaa edellisen kohdan mukaisesti varmennettua identiteettiä).
    *d.* Välittäjältä vaaditun tietoturvatason toteutuminen tulee varmistaa auditointi-/sertifiointimenettelyllä. *KANTA-määrittelyistä (2007) poiketen WS-Security-standardin mukainen sanomatason allekirjoitus ja/tai salaus eivät ole käytössä (VVAR019)*
9. *Vaatimuksena on*, että kaikkien Kanta-sanomaliikenteeseen liittyvien tahojen tulee suojata liityntäpistesijaintinsa ja tietojärjestelmien käyttöympäristöt tilallisella palomuurilla tai sovelluspalomuurilla.
10. Vastaanottopalveluissa (Kanta → liittyjä -suuntaisissa yhteysavauksissa) *on vaatimuksena*, että
    a. Liityntäpisteen toteuttaja tarkistaa Kelan Kanta-liityntäpisteen palvelinvarmenteen (ns. mutual authentication).
    b. Kullekin palvelulle (esimerkiksi lääkemääräyksen uudistamispyynnön vastaanotto) on yksi Kanta-palvelulle päin näkyvä organisaatioyksikkökohtainen liityntäpiste. Kanta ei suorita IP-failoveria liittyjän suuntaan
11. *Vaatimuksena on*, että Kanta-palveluun suoraan tai välillisesti yhteydessä olevien palvelinten aika synkronoidaan Mittatekniikan keskuksen toimittaman Suomen virallisen ajan kanssa. Julkisen NTP-palvelun käyttö on riittävää.
12. *Suosituksena on määritellä yhdelle liityntäpisteelle yksi tietoliikenneosoite* (IP-osoite). Yhdelle liityntäpisteelle voidaan kuitenkin määritellä useampi osoite, jos se on tarpeen esimerkiksi varayhteyden järjestämiseksi. Tällöinkin yksi osoitteista on ensisijainen tietoliikenneosoite. Vastaanottopalveluita tarjoava liityntäpiste ei voi myöskään sijaita kuin yhdessä tietoliikenneosoitteessa.
13. *Suosituksena on käyttää eri palvelimilla eri palvelinvarmenteita.* Jos kuitenkin on välttämätöntä käyttää samaa palvelinvarmennetta useassa eri palvelimessa (esimerkiksi klusteritoteutuksesta seuraavien rajoitusten vuoksi), kysymyksessä on sama Kanta-liityntäpiste. Näin on, vaikka kaikki klusterin jäsenet näkyisivät ulospäin omilla tietoliikenneosoitteillaan (IP-osoite), ts. klusterille ei ole yhteistä virtuaaliosoitetta.