Tekniset liittymismallit Kanta-palveluihin

Kanta-palvelut

Kela
Kanta-palvelut
PL 450, 00056 Kela

FPA
Kanta tjänsterna
PB 450, 00056 FPA

Kanta 381 06.19
www.kanta.fi
kanta@kanta.fi

Muutoshistoria

Versio	Muutos	Tekijä	PVM
2.6	Lisätty viittaus liitteeseen 1, korvattu viestinvälitys termillä integraatioratkaisu, tarkennettu Kanta-liityntäpisteen kuvausta, lisätty esimerkki apteekin tiedoista osoitehakemistossa	Kanta-palveluryhmä, Kela	29.4.2010
2.7	Kpl 1.3 tarkennettu: suositeltu liityntäpisteiden lkm on 1, vaikka organisaatiolla olisi vastaanottopalveluita. Korjattu kuvia 5 ja 7.	Kanta-palveluryhmä, Kela	3.6.2010
2.8	Lisätty vastaanottopalveluiden portti 443.	Kanta-palveluryhmä, Kela	24.6.2010
2.9	Tarkennettu Kanta-liityntäpisteen määritelmää. Terveydenhuollon varmentaja vaihtunut 1.12.2010 alkaen.	Kanta-palveluryhmä, Kela	3.2.2011
3.0	Lisätty yksityisen terveydenhuollon liityntämalliin liittyvät erityispiirteet sekä pysyvä osoitteistokytkentä alihankintatilanteissa.	Kanta-palvelut Kela	18.6.2015
3.1	Tarkennettu ohjeistusta suljetun asiakasverkon käyttämiseksi liittymismallina.	Kanta-palvelut Kela	24.10.2016
3.2	Muokattu ohjeistusta uusien järjestelmien tarpeisiin. Liite 1 poistettu ja korvattu viittauksella JHS-suosituksiin.	Kanta-palvelut Kela	23.11.2017
3.3	Korjattu luvun 5.5 käsitteitä	Kanta-palvelut Kela	4.1.2018
3.4	Korjattu termi suljettu asiakasverkko termiin yksityinen verkko. Lisätty esimerkki liityntäpisteen OID-yksilöintitunnuksen muodostamisesta. Tarkennettu ohjetta julkisen internetin yhteyden käyttämisestä Kanta-liittymisissä.	Kanta-palvelut Kela	31.1.2019
3.5	Poistettu mainina Kanta-palvelujen tekemästä kirjallisesta hyväksymisestä luvussa 4.2 Julkinen internet-yhteys poikkeustapauksissa	Kanta-palvelut Kela	10.6.2019

Sisällysluettelo

Lyhenteet

CA	certification authority varmentaja	taho, joka myöntää varmenteen Lähde: Tiivis tietoturvasanasto (TSK 31, 2004)
DMZ	demilitarized zone demilitaroitu alue	organisaation lähiverkon fyysinen tai looginen aliverkko, joka yhdistää lähiverkon internetiin
DNS	domain name system nimipalvelujärjestelmä	järjestelmä, joka muuntaa tekstimuotoiset verkkotunnukset IP-osoitteiksi ja päinvastoin Lähde: Internetpuhelusanasto (TSK 37, 2007)
IP	internet protocol internet-yhteyskäytäntö	standardiksi muodostunut internetin verkkokerroksen yhteyskäytäntö, joka hoitaa pakettien reitityksen ja loogisen osoitteistuksen Lähde: Matkaviestinsanasto (TSK 29, 2001)
ISO	International Organization for Standardiza-tion	kansainvälinen standardisoimisjärjestö
MPLS	multiprotocol label switching	menetelmä, jolla kuljetetaan esimerkiksi IP-paketteja ennalta määriteltyjen yhteyksien ylitse nopean runkoverkon solmujen kautta ilman, että solmujen tarvitsee tehdä reititystä
NAT	network address translation IP-osoitteen muunnos	internetstandardin mukainen menettely, jossa IP-osoitteet muunnetaan toisiksi IP-osoitteiksi
OID	object identifier yksilöintitunnus	yksikäsitteinen tunnus, jolla kohde, esim. esine tai asia, voidaan erottaa muista vastaavista
SSL	secure sockets layer	salauskäytäntö, jolla voidaan suojata internetsovellusten tietoliikenne IP-verkkojen yli
TCP	transmission control protocol	kuljetusyhteyskäytäntö, joka huolehtii tiedonsiirrosta ja varmistaa tiedon perillemenon lähettämällä tiedon tarvittaessa uudelleen Lähde: Internetpuhelusanasto (TSK 37, 2007)
TLS	transport layer security	salauskäytäntö, jolla voidaan suojata internet-sovellusten tietoliikenne IP-verkkojen yli, käytössä versio 1.2.
URL	uniform resource locator URL-osoite	internetissä olevan tiedoston, hakemiston tai muun tiedon sekä näiden käyttöön tarvittavan yhteyskäytännön yksilöivä tunnus Lähde: Tietotekniikan termitalkoot, 2007-12-14

1 Johdanto

Tässä dokumentissa kuvataan teknisiä liittymismalleja Kanta-palveluihin. Tähän ohjeeseen liittyvät keskeisesti seuraavat dokumentit:

- Ketkä liittyvät Kanta-palveluihin – Kanta-liittyjän ohje
- Miten liitytään Kanta-palveluihin – Kanta-liittyjän ohje
- Määräys omavalvontasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista (THL:n määräys 2/2015)
- Kanta-sertifiointi ja omavalvonta – yleiskuva ja prosessit
- Määräys A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista tietoturvavaatimuksista (THL:n määräys 1/2015)
- Kanta-välityspalvelujen sertifiointi ja Kanta-välittäjätahot (THL:n ohje 3/2015)
- ISO OID-yksilöintitunnuksen käytön kansalliset periaatteet sosiaali- ja terveysalalla

Kanta-palveluihin liittyviä organisaatioita on sekä kooltaan että teknisiltä valmiuksiltaan hyvin erilaisia pienistä toimijoista suuriin toimijoihin. Kela kuvaa yleiset mallit, joilla Kanta-palveluihin voi liittyä, mutta ei säätele organisaation liittymisen teknistä toteutusta yksityiskohtaisesti.

Tässä ohjeessa esitellään erilaisia liittymismalleja Kanta-palveluihin. Malleista kuvataan yleisellä tasolla, miten tietoliikenne- ja sanomaliikenneyhteydet organisaation tietojärjestelmien ja Kanta-palvelujen välille voidaan toteuttaa. Liittymisessä on eroteltavissa seuraavat roolit, joista kukin voi olla keskenään sama tai eri taho: palvelua käyttävä organisaatio, Kanta-liittyjäorganisaatio sekä Kanta-liityntäpisteen omistaja (Kuva 1).

Kuva 1 Yleiskuva Kanta-liittymisestä

1.1 Mihin järjestelmiin liitytään?

Tämä liittymisohje koskee asiakasjärjestelmiä, jotka liittyvät johonkin seuraavista Kanta-palvelujen järjestelmistä:

1. Reseptikeskus
2. Potilastiedon arkisto
3. Sosiaalihuollon asiakastiedon arkisto

4. Omatietovaranto

5. Kuva-arkisto

Tämä liittymisohje ei koske Kansallista koodistopalvelua eikä validointipalvelua, sillä niihin ei tarvitse erikseen liittyä.

Liittymismallien valintaa koskevat seuraava rajoitus: Sosiaalihuollon asiakastiedon arkiston käyttöönotossa ei voida toistaiseksi soveltaa yhteisliittymismallia.

1.2 Itsenäinen liittyminen

(palvelua käyttävä organisaatio = Kanta-liittyjäorganisaatio = liityntäpisteen omistaja)

1. liittyminen oman integraatioratkaisun (viestinvälitysratkaisun) kautta
2. liittyminen suoraan omassa konesalissa olevasta tietojärjestelmästä
3. pienen organisaation liittyminen internetin kautta

1.3 Liittyminen ulkoistetun liityntäpisteen kautta

(Kanta-liittyjäorganisaatio ≠ liityntäpisteen omistaja)

1. liittyminen ulkoistetun liityntäpisteen kautta
2. ulkoistettu tietojärjestelmä (esim. ulkoistettu konesali, Software as a Service -palvelu, pilvipalvelut, sosiaali- tai terveydenhuollon ammattilaisten web-käyttöliittymät)
3. ulkoistettu integraatioratkaisu (viestinvälitysratkaisu)
4. ulkoistettu tietoliikenne (tietoliikenteen koontipiste)

1.4 Liittyminen toisen organisaation sitoumuksella

(palvelua käyttävä organisaatio ≠ Kanta-liittyjäorganisaatio)

1. yksityisen terveydenhuollon yksiköiden liittyminen vuokralaisena toisen palvelujen antajan sitoumuksella
2. Potilastiedon arkiston pysyvä osoitteistokytkentä alihankintatilanteessa ilman ostopalvelun valtuutusta eli potilastietoja arkistoivan organisaation liittyminen rekisterinpitäjän nimissä

Liittymismalli ohjaa organisaatiota varmenteiden ja tietoliikenneyhteyksien hankkimisessa. Jokaisessa mallissa on suosituksia ja vaatimuksia hankittaville tietoliikenne- ja sanomaliikenneyhteyksille.

Liittymismallit ovat pelkistyksiä. Niissä kuvataan Kanta-liityntää eri näkökulmista. Mallit eivät sulje pois toisiaan, ja organisaation Kanta-liityntä voidaan toteuttaa myös usean mallin yhdistelmänä.

Moninaisuutta Kanta-liityntöihin aiheuttavat organisaatioiden olemassa olevat ympäristöt ja yhteydet sekä niiden käyttämät erilaiset ulkoistusratkaisut. Periaatteessa organisaatio on voinut ulkoistaa minkä tahansa osan Kanta-liitynnästään kolmannen osapuolen eli ns. välittäjän, (ks. 2.4), toteutettavaksi.

2 Peruskäsitteet

2.1 Kanta-palveluun liittyjät

Kanta-palvelujen käytöstä on säädetty sähköistä lääkemääräystä (61/2007, muutoksineen) ja sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä (159/2007, muutoksineen) koskevissa laeissa ja näihin liittyvissä asetuksissa.

Kanta-palveluihin liittyvät tahot sekä liittymisen säädöstaustat on määritelty tarkemmin Kanta-liittyjät-ohjeissa.

Kaikkien Kanta-palveluihin liittyvien organisaatioiden ja näiden mukana Kanta-palveluita käyttöönottavien palveluyksiköiden ja sivuapteekkien pitää olla rekisteröitynä Terveyden ja hyvinvoinnin laitoksen (THL) ylläpitämään valtakunnalliseen koodistopalveluun joko

- Apteekkirekisteriin (Fimea – Apteekkirekisteri) tai
- Sosiaali- ja terveydenhuollon organisaatiorekisteriin (THL – SOTE-organisaatiorekisteri) tai
- Terveydenhuollon itsenäisten ammatinharjoittajien koodistoon (Valvira - Terveydenhuollon itsenäiset ammatinharjoittajat).

Tätä kautta niiden ISO OID -yksilöintitunnukset ja muut rekisteröidyt tiedot tulevat Kanta-palvelujen käyttöön.

2.2 Vastaanottopalvelut

Vastaanottopalveluilla tarkoitetaan Web Service -palveluja, joita organisaation järjestelmät tarjoavat Kanta-palveluille. Tällainen palvelu on sähköisen lääkemääräyksen uusimispyyntöjen vastaanotto PUSH-mallilla.

Vastaanottopalveluissa kutsuvana osapuolena on Kanta-palvelut ja palvelun tarjoajana organisaatio. Vastaanottopalvelun tarjoaminen uusimispyyntöjen vastaanottoa varten ei ole välttämätöntä, jos asiakkaan tietojärjestelmä käyttää PUSH-mallin sijasta PULL-mallia. Suosituksena on käyttää PULL-mallia aina kun se on teknisesti mahdollista.

Vastaanottopalveluiden tulee toimia https-portissa 443.

2.3 Kanta-liityntäpiste

Kanta-liityntäpisteellä tarkoitetaan sitä tietoliikenteen pistettä, josta organisaation tietojärjestelmä liittyy Kanta-palveluihin sosiaali- ja terveydenhuollon varmentajan palvelinvarmenteella salattua ja tunnistettua tietoliikenneyhteyttä pitkin. Kanta-liityntäpisteeseen on asennettu VRK:n myöntämä palvelinvarmenne.

Jokaisella Kanta-palveluihin liittyvällä organisaatiolla on käytössään vähintään yksi Kanta-liityntäpiste. Se voi olla joko organisaation omana toimintana toteutettu tai toisen organisaation toteuttama. Liityntäpisteitä (ja palvelinvarmenteita) voi olla useita, esim. jos

- organisaation yksiköt liittyvät Kanta-palveluihin suoraan eri tietojärjestelmistä ilman keskitettyä integraatioratkaisua (viestinvälitysratkaisua).
- organisaation vastaanottopalvelut (esim. uusimispyyntöjen vastaanotto) sijaitsevat eri palvelimessa kuin siinä, josta sen järjestelmät kutsuvat Kanta-palveluja.

Kanta-liityntäpisteelle annetaan yksilöivä OID-tunnus. Sitä käytetään myös liityntäpisteeseen asennettavan palvelinvarmenteen yksilöivänä tunnuksena (palvelinvarmenteen Subject-osion serialNumber-kenttä). Tunnus muodostetaan liityntäpisteen toteuttamisesta vastaavan organisaation tai organisaatioyksikön OID-tunnuksen alle solmuun 13 seuraavasti:

- Sosiaali- ja terveydenhuollon palvelujen antajan liityntäpisteen OID-tunnus on muotoa 1.2.246.10.xxx.10.y.13.n (missä xxx on Sote-organisaatiorekisterin tai Valvira – Terveydenhuollon itsenäiset ammatinharjoittajat –rekisterin mukainen organisaation tunnus, y on yksikön yksilöivä numero ja n on liityntäpisteen yksilöivä numero).
- Apteekin liityntäpisteen OID-tunnus on muotoa 1.2.246.553.1.xxx.13.n (missä xxx on Fimean Apteekkirekisterin mukainen apteekin tunnus ja n on liityntäpisteen yksilöivä numero).

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.

Suosituksena on määritellä yhdelle liityntäpisteelle yksi tietoliikenneosoite (IP-osoite tai julkisesta nimipalvelusta löytyvä DNS-nimi, ks. kohta 4.3 Tietoliikenneosoitteet). 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.

2.4 Kanta-välittäjä

Kanta-välittäjä ja Kanta-välityspalvelun tuottaja sekä niiden roolit ja vastuut on kuvattu ohjeessa Kanta-välityspalvelujen sertifiointi ja Kanta-välittäjätahot (THL:n ohje 3/2015).

Välittäjällä tarkoitetaan Kanta-palveluihin liittyvän organisaation Kanta-liityntäpisteen toteuttamisessa käyttämää palveluntarjoajaa, jolla on tässä roolissa mahdollisuus nähdä salaamattomia sosiaali- tai terveydenhuollon asiakastietoja esim. ylläpitotoimien yhteydessä. Sosiaali- ja terveydenhuollon varmentajan palvelinvarmenteella toteutettava TLS-salattu yhteys muo-

dostetaan yleensä välittäjän liityntäpisteen ja Kanta-palvelujen välille. Välittäjäksi ei määritellä organisaatiota, joka toimii ainoastaan TLS-salatun tietoliikenteen reitittäjänä eikä voi nähdä salaamattomia asiakas- ja potilastietoja.

Sosiaali- ja terveydenhuollon varmentajan (VRK) palvelinvarmenne voi olla joko liittyjän tai välittäjän nimissä. Jos välittäjä toteuttaa yhteisen liityntäpisteen ja siihen liittyvät palvelut usealle Kanta-liittyjälle, hankitaan palvelinvarmenne välittäjän nimiin.

Välittäjä voi toteuttaa osan liityntäpisteen palveluista myös alihankintana. Sen välittäjän, joka hallinnoi liityntäpistettä eli jonka nimissä palvelinvarmenne on, pitää olla sopimussuhteessa sosiaali-/terveydenhuollon organisaation tai apteekin kanssa.

Välittäjän toteuttaman liityntäpisteen OID-tunnus muodostetaan välittäjän Välittäjärekisterin mukaisen OID-tunnuksen alle solmuun 13, jolloin liityntäpisteen OID on muotoa 1.2.246.537.6.918.18.xxx.13.n (missä xxx on Välittäjärekisterin mukainen organisaation tunnus ja n on liityntäpisteen yksilöivä numero).

2.5 Palvelinvarmenne

Palvelinvarmennetta tarvitaan, jotta voidaan muodostaa salattu TLS-yhteys Kanta-palvelujen ja Kanta-liityntäpisteen välille, sekä tunnistaa Kanta-liityntäpiste. Jokaista Kanta-liityntäpistettä varten pitää hankkia oma palvelinvarmenne VRK:sta.

Palvelinvarmenne ja Kanta-liityntäpiste kytketään toisiinsa palvelinvarmenteen Subject-osion serialNumber-kentän välityksellä. Sen arvoksi tulee Kanta-liityntäpisteen OID-tunnuksen arvo. Palvelinvarmenteen Subject-osion commonName-kenttään tulee arvoksi liityntäpisteen ensisijaisen tietoliikenneyhteyden (ks. kohta 2.3 Kanta-liityntäpiste) tietoliikenneosoite.

Palvelinvarmennetta voidaan käyttää myös organisaation ja ulkoistetun Kanta-liityntäpisteen välisen liikenteen salaamisessa ja liikennöivien osapuolien tunnistamisessa.

2.6 Järjestelmäallekirjoitusvarmenne

Potilastiedon arkiston palveluja käytettäessä tarvitaan terveydenhuollon varmentajan myöntämä järjestelmäallekirjoitusvarmenne. Siihen liittyvällä yksityisellä avaimella allekirjoitetaan kaikki Kantaan lähetettävät asiakirjat, joita ei ole allekirjoitettu ammattihenkilön varmenteella.

Järjestelmäallekirjoitusvarmenne on organisaatio- ja järjestelmäkohtainen[1]. Tämä tarkoittaa, että esimerkiksi Potilastiedon arkistoon liittyvä palvelujen antaja tarvitsee ainoastaan yhden järjestelmäallekirjoitusvarmenteen. Jos

[1] Poikkeuksena yhteiset järjestelmäallekirjoitusvarmenteet erillisten määräysten mukaisesti (PTJ käyttötapaukset): Järjestelmäallekirjoitusvarmenteella allekirjoitetaan Kantaan arkistoitavat asiakirjat, joita käyttäjän ei tarvitse henkilökohtaisesti sähköisesti allekirjoittaa. Lähtökohtaisesti järjestelmävarmenne on organisaatiokohtainen, eli kukin palvelunantaja hankkii oman järjestelmävarmenteen. Lääkäriasemilla voidaan kuitenkin käyttää yhteistä järjestelmäallekirjoitusvarmennetta. Asiasta tulee sopia lääkäriaseman ja sen tiloissa toimivien keskinäisessä sopimuksessa. Myös niissä tilanteissa, joissa potilastietojärjestelmä on hankittu palveluna, eli järjestelmätoimittaja vastaa järjestelmän teknisestä ylläpidosta, voidaan käyttää yhtä varmennetta. Kukin palvelua käyttävä organisaatio valtuuttaa järjestelmätoimittajaa hankkimaan varmenteen puolestaan. Valtuutus kirjataan toimittajan ja organisaation väliseen sopimukseen.

organisaatiolla on useita potilastietojärjestelmiä, se voi käyttää kaikissa samaa järjestelmäallekirjoitusvarmennetta. Jos samalla organisaatiolla on kuitenkin yhteys myös Sosiaalihuollon asiakastiedon arkistoon, tarvitaan siihen oma järjestelmäallekirjoitusvarmenne.

2.7 Kanta-osoitehakemisto

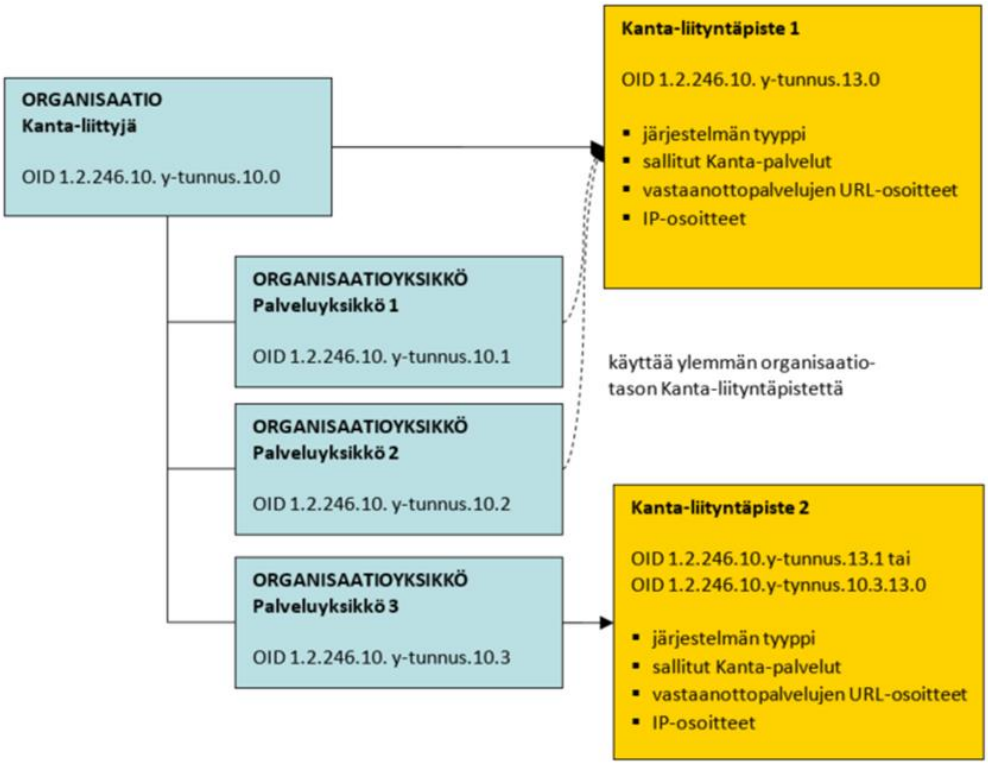
Kela ylläpitää tietoja Kanta-liittyjien liityntäpisteistä osoitehakemistossaan. Organisaatio ilmoittaa käyttämiensä omien tai ulkoisten Kanta-liityntäpisteiden tiedot Kanta-palvelujen liittymishakemuksessa.

Osoitehakemisto toimii osoitteistona ja on osa Kanta-palvelujen pääsynhallintaa. Sinne tallennetaan organisaation vastaanottopalvelujen tietoliikenneosoitteet ja organisaation käytettävissä olevat Kanta-palvelut. Jokaisesta Kanta-liityntäpisteestä tallennetaan seuraavat tiedot:

- liityntäpistettä käyttävän organisaation tai organisaatioyksikön OID-tunnus
- liityntäpisteen OID-tunnus (solmu 13)
- järjestelmän tyyppi (esimerkiksi potilastietojärjestelmä, asiakastietojärjestelmä tai apteekkijärjestelmä)
- sallitut Kanta-palvelut (Kela määrittelee hakemuksen perusteella)
- vastaanottopalvelujen URL-osoitteet.
- tietoliikenneosoitteet (IP-osoitteet).

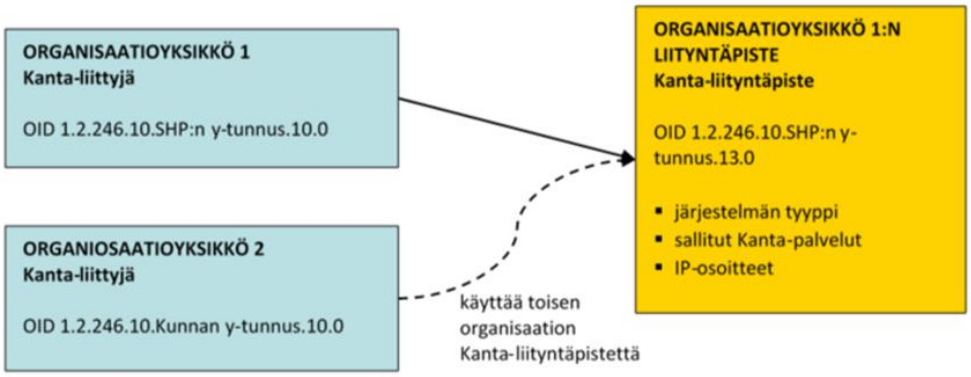
Osoitehakemistossa ylläpidetään tietoa siitä, mikä organisaatioyksikkö käyttää mitäkin liityntäpistettä. Organisaatioyksikkö, jolle ei ole määritelty omaa liityntäpistettä, perii ylemmällä tasolla olevan organisaatioyksikön liityntäpisteen eli on liittynyt Kanta-palveluihin sen kautta.

Kuvassa 2 organisaation yksi organisaatioyksikkö on liittynyt Kanta-palveluihin oman liityntäpisteen kautta ja muut organisaatioyksiköt organisaation ylimmälle tasolle määritellyn liityntäpisteen kautta.



Kuva 2 Organisaatiolla on kaksi omaa Kanta-liityntäpistettä

Organisaation tietoihin tallennetaan sen käyttämän Kanta-liityntäpisteen tiedot myös silloin, kun liityntäpiste on toisen organisaation hallussa. Kuvassa 3 organisaatioyksikkö 2 on liittynyt Kanta-palveluihin organisaatioyksikkö 1:en hallinnoiman Kanta-liityntäpisteen kautta.



Kuva 3 Organisaatio käyttää ulkoista Kanta-liityntäpistettä

2.8 Tietoliikenteen koontipiste

Tietoliikenteen koontipisteellä tarkoitetaan palvelua, jossa eri organisaatioista Kanta-palveluihin kulkeva TCP/IP-tietoliikenne kootaan yhteen ja reititetään Kanta-palveluihin yhteistä tietoliikenneyhteyttä pitkin ja jossa vastaavasti Kanta-palveluista tuleva liikenne reititetään vastaanottajan IP-osoitteen perusteella eri organisaatioihin. Tietoliikenteen reitityksellä ei ole vaikutusta yhteyksien TLS-salaukseen: salausta ei pureta eikä muodosteta koontipisteessä, eivätkä resepti- sekä asiakas- ja potilastiedot näy salaamattomina.

Tietoliikenteen koontipisteessä voidaan tarvittaessa tehdä osoitteenmuunnos niin, että kaikki koontipisteen kautta kulkeva liikenne näyttää tulevan samasta osoitteesta. Näissä tapauksissa Kanta-liityntäpisteen palvelinvarmenne ja tietoliikenneosoite sijaitsevat eri organisaatioissa, palvelinvarmenne liittyvässä organisaatiossa tai välittäjällä, ja tietoliikenneosoite koontipistettä hallinnoivassa organisaatiossa.

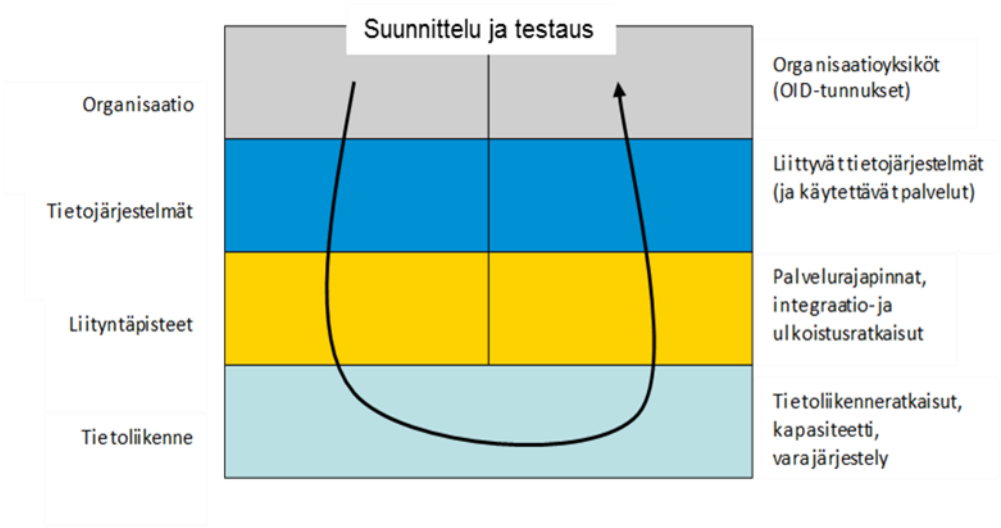
3 Liittymismallin valinta ja testaus

Liittymismallin valinta edellyttää, että organisaatio määrittelee organisaatioyksikköhierarkiansa (vaatimus ei koske yksityisiä organisaatioita, joiden organisaatiohierarkiatiedot on tallennettu Valveri-/Soteri-rekisteriin), selvittää Kanta-palveluihin liitettävät tietojärjestelmänsä sekä näiden käyttämät liityntäpisteet ja tietoliikenneyhteydet. Määrittelyssä on suositeltavaa edetä ylhäältä alas, organisaation tasolta tietoliikenneratkaisuihin seuraavasti:

1. organisaation OID-tunnusten ja organisaatioyksiköiden välisen hierarkian määrittely
2. Kanta-palveluihin liittyvien tietojärjestelmien määrittely/kuvaaminen
3. Kanta-palveluille tarjottavien palvelujen, integraatio- (viestinvälitys-) ja ulkoistusratkaisujen määrittely
4. tietoliikenneratkaisujen (mm. kapasiteetti, varayhteydet) määrittely.

Liitynnän toteutuksen jälkeen testauksessa edetään päinvastaiseen suuntaan, tietoliikenteen tasolta organisaation tasolle. Testauksen vaiheet ovat

1. TCP/IP-yhteyden testaus
2. TLS-yhteyden testaus (palvelinvarmenteet, molempiin suuntiin vastaanottopalveluiden osalta)
3. viestinvälityksen testaus (myös vastaanottopalvelusanomien)
4. OID-tunnusten oikeellisuuden testaus sanomissa (sovellustaso).



Kuva 4 Liittymismallin suunnittelu ja testaus

4 Tietoliikenneyhteys

Liittyvä organisaatio vastaa tietoliikenneoperaattorilta hankkimastaan tietoliikenteestä ja määrittelee käyttämiensä yhteyksien ominaisuudet omien kapasiteetti-, laatu- ja palvelutasovaatimustensa mukaisiksi. Kela vastaa palvelun sisäisestä tietoliikenteestä tietoliikenneoperaattorin rajapintaan asti.

Ensisijaisesti tulee käyttää yksityisen verkon yhteyttä takaamaan palvelun saatavuus ja laatu. Julkista internet-yhteyttä voi käyttää vain perustelluissa poikkeustapauksissa. Poikkeustapauksissa on huomioitava, että vastaanottopalveluja tarjoava organisaatio joutuu avaamaan palomuurissaan portin ulkoverkosta sisäverkkoonsa, mikä altistaa organisaation mm. palvelunestohyökkäyksille ja muille tietoturvauhille.

Tässä kappaleessa on esitetty tietoliikenneyhteydelle asetetut keskeiset vaatimukset ja suositukset yleisellä tasolla. Tarkempaa ohjeistusta tietoliikenneyhteyksien määrittelemisen ja hankkimisen tueksi löytyy kappaleesta 6.

4.1 Yksityisen verkon yhteys

Yksityisen verkon liittymälle tietoliikenneoperaattori takaa tietyn kapasiteetin koko liittymän matkalle. Yksityisen verkon liittymä (MPLS tai vastaava) tilataan tietoliikenneoperaattorilta yhden organisaation, organisaatioiden yhteisen Kanta-liityntäpisteen tai tietoliikennesolmun ja Kanta-palvelujen välille. Organisaatiossa on varauduttava siihen, että yhteyden toteuttaminen voi kestää useita viikkoja. Yhteyden pitää olla valmis silloin, kun organisaatio tekee liittymishakemuksen Kanta-palveluihin.

Yksityisen verkon yhteydet pystytään paremmin suojaamaan julkisen internetin uhilta, mm. palvelunestohyökkäyksiltä.

4.2 Julkinen internet-yhteys poikkeustapauksissa

Kanta-palveluihin voi liittyä julkisen internetin kautta vain perustelluissa poikkeustapauksissa. Vaihtoehto on tarkoitettu organisaatioille, joilla ei ole mahdollisuutta liittyä yksityiseen verkkoon. Julkista internet-yhteyttä käyttävälle organisaatiolle ei voida taata yksityisen verkon tasoista palvelun saatavuutta ja laatua.

4.3 Tietoliikenneosoitteet

Kanta-liityntäpisteelle määriteltyjen IP-osoitteiden pitää olla kiinteitä ja julkisia. Ylläpidon helpottamiseksi ja virhemahdollisuuksien minimoimiseksi varmenteissa on parempi käyttää DNS-nimiä kuin IP-osoitteita.

4.4 Tietoturva

Kanta-liityntäratkaisun tulee täyttää tieto- ja sanomaliikenteen tietoturvavaatimukset (ks. Kanta-palvelut: tieto- ja sanomaliikenteen tietoturvavaatimukset) sekä tietoturvavaatimukset A-luokkaan kuuluville järjestelmille ja järjestelmien käyttöympäristöille. Näihin kuuluu mm. tilallinen palomuuri ja virustorjunnasta huolehtiminen.

4.5 Varayhteys

Organisaation ja Kanta-palvelujen välisen tietoliikenneyhteyden kahdentaminen on suositeltavaa. Liittymän tilaajan kannattaa varmistaa tietoliikenneoperaattoriltaan, että ensisijainen yhteys ja varayhteys kulkevat aidosti eri reittejä koko matkan. Varmistaminen voi olla mahdotonta, jos liittymät ostetaan eri operaattoreilta, koska operaattorit eivät yleensä paljasta liittymiensä fyysisiä yhteyksiä. Jos yhteyden toteuttaminen täysin kahdennettuna ei ole mahdollista, on suositeltavaa kahdentaa yhteys niin pitkälle kuin on taloudellisesti järkevää.

Yhteyksien kahdentamisessa on muistettava, että organisaation vastaanottopalveluilla (esim. uusimispyynnön vastaanotto) pitää olla yksikäsitteiset osoitteet. Yhteyksien kahdennus pitää toteuttaa siten, että varayhteyden ja ensisijaisen yhteyden tietoliikenneosoitteet ovat samat niissä liityntäpisteissä, joissa vastaanottopalvelut sijaitsevat.

4.6 Symmetrinen yhteys

Suositeltavaa on käyttää nopeudeltaan symmetristä tietoliikenneyhteyttä. Tämä tarkoittaa sitä, että siirtokapasiteetti on kumpaankin suuntaan yhtä suuri.

4.7 Liittymän tiedonsiirtokapasiteetti

Liittymän tiedonsiirtokapasiteettitarpeen määrittely on Kanta-liittyjän vastuulla. Kapasiteettitarpeen arvioinnissa tulee huomioida liikennöintimäärä ja toiminnan kriittisyys. Tarkempaa ohjeistusta tiedonsiirtokapasiteetin arviointiin löytyy kappaleesta 6.

Organisaatioiden tulee varmistua myös liittymän skaalautuvuudesta, koska liikenteen määrät kasvavat arkiston palveluiden käyttöönoton yhteydessä.

5 Liittymismallit

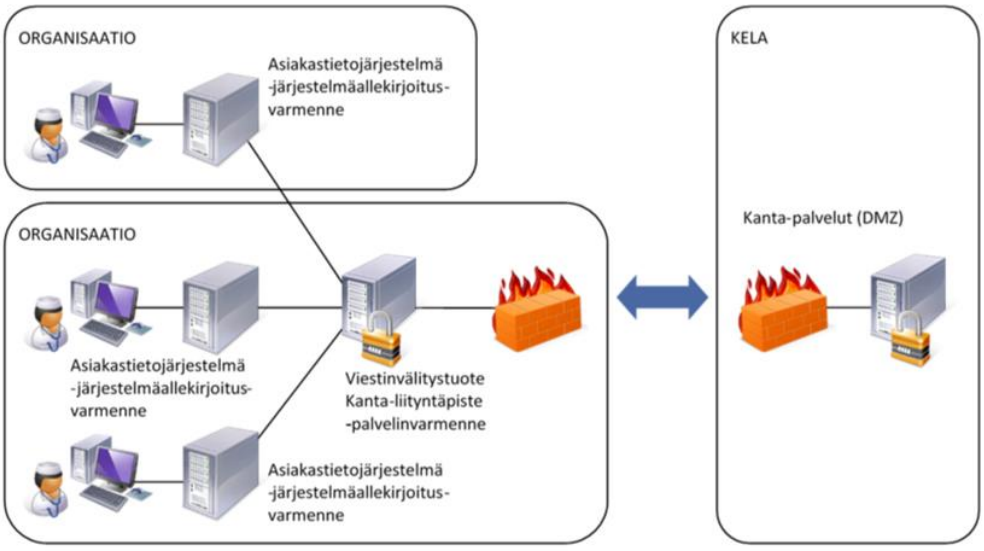
Tässä esitellyt liittymismallit eivät sulje pois toisiaan, ja organisaation Kanta-liityntä voi olla yhdistelmä eri malleja.

5.1 Liittyminen oman integraatioratkaisun kautta

Tässä mallissa Kanta-liittyjällä tai Kanta-välittäjällä on integraatioratkaisu (viestinvälitysratkaisu), jonka kautta Kanta-palveluihin liittyy useita järjestelmiä, organisaatioyksiköitä tai organisaatioita. Integraatioratkaisun tehtävänä on reitittää sanomat sovelluspalvelimille, jotka voivat sijaita eri organisaatioyksiköissä tai organisaatioissa.

Sosiaali- ja terveydenhuollon varmentajan (VRK) myöntämä palvelinvarmenne asennetaan integraatioratkaisun yhteyteen. Tällä palvelinvarmenteella muodostetaan tunnistettu ja salattu yhteys Kanta-palveluihin. Palvelinvarmennetta voidaan tarvita myös integraatioratkaisun ja liitettävien tietojärjestelmien välillä osapuolten identiteetin varmistamisessa ja tiedonsiirron salaamisessa.

Integraatioratkaisun käyttö mahdollistaa useiden järjestelmien, organisaatioyksiköiden tai organisaatioiden liittymisen Kantaan samaa tietoliikenneyhteyttä pitkin. Tapausesimerkkinä alueellinen IT-palveluntuottaja, jolla on tai joka hallinnoi useita järjestelmiä ja tarjoaa alueensa organisaatioille välityspalvelun Kanta-palveluihin (Kuva 5).



Kuva 5 Organisaatiolla on useita tietojärjestelmiä, ja se tarjoaa liityntäpisteen Kanta-palveluihin toiselle organisaatiolle

Malli soveltuu organisaatiolle,

- jolla on useita Kantaan liitettäviä tietojärjestelmiä

- jonka kautta Kantaan liittyy myös muita organisaatioita.

Vaatimukset liittymälle:

- yksityisen verkon yhteys, esim. MPLS
- kiinteät ja julkiset tietoliikenneosoitteet
- tilallinen palomuuri ja muu tietoturva
- palvelinvarmenne integraatioratkaisun yhteydessä tai erillisessä aktiivilaitteessa
- järjestelmäallekirjoitusvarmenne asiakas- tai potilastietojärjestelmän yhteydessä (arkistoon liityttäessä)
- integraatioratkaisun ja tietojärjestelmien välillä osapuolten identiteetin varmistaminen, esim. terveydenhuollon varmentajan palvelinvarmenteella
- TLS-salattu suojattu yhteys organisaatioiden välillä, toteutettu esim. sosiaali- ja terveydenhuollon varmentajan (VRK) palvelinvarmenteella.

Suositukset liittymälle:

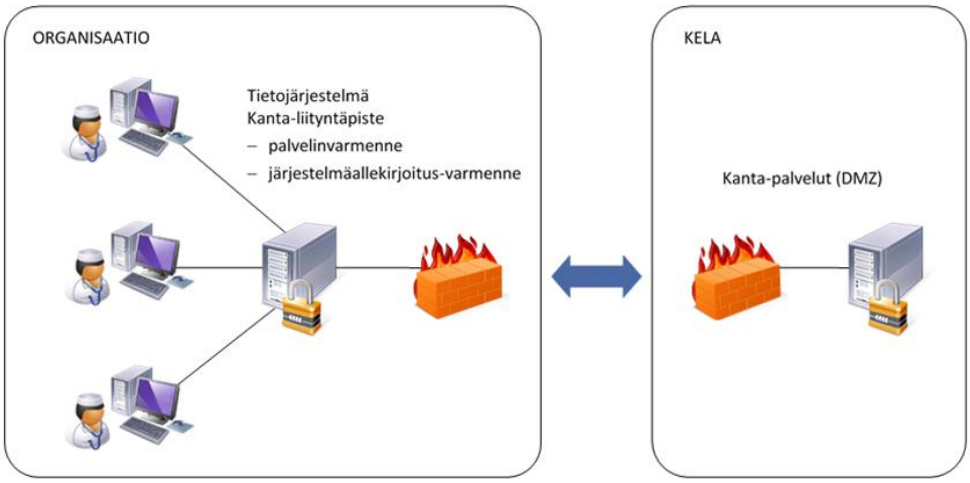
- kahdennettu, nopeudeltaan symmetrinen liittymä
- kapasiteettitarpeen ja toiminnan kriittisyyden mukaiset tekniset ja ylläpidolliset laatuvaatimukset.

5.2 Liittyminen suoraan omassa hallinnassa olevasta tietojärjestelmästä

Tässä mallissa organisaation Kantaan liitettävä järjestelmä ja Kanta-liityntäpiste ovat organisaation omassa hallinnassa. Palvelinvarmenne asennetaan suoraan sovelluspalvelimelle tai erilliseen aktiivilaitteeseen tietojärjestelmän yhteyteen.

Organisaatiolla voi olla useita Kanta-liityntäpisteitä, jos sillä on useita liitettäviä tietojärjestelmiä eikä niille ole mahdollista toteuttaa yhteistä liityntäpistettä tai jos organisaatio vastaanottaa sähköisen lääkemääräyksen uusimispyynnöt tai käyttää Valviran rooli- ja attribuuttipalvelua eri osoitteessa kuin siinä, josta se kutsuu Kanta-palveluja.

Tapausesimerkkinä mallista on organisaatio, joka liittyy Kanta-palveluihin suoraan omassa hallinnassa olevasta tietojärjestelmästä (Kuva 6).



Kuva 6 Suoraan omassa hallinnassa olevasta tietojärjestelmästä Kantaan liittynyt organisaatio

Malli soveltuu organisaatiolle, jolla on yksi omassa hallinnassa oleva liittyvä tietojärjestelmä.

Vaatimukset liittymälle:

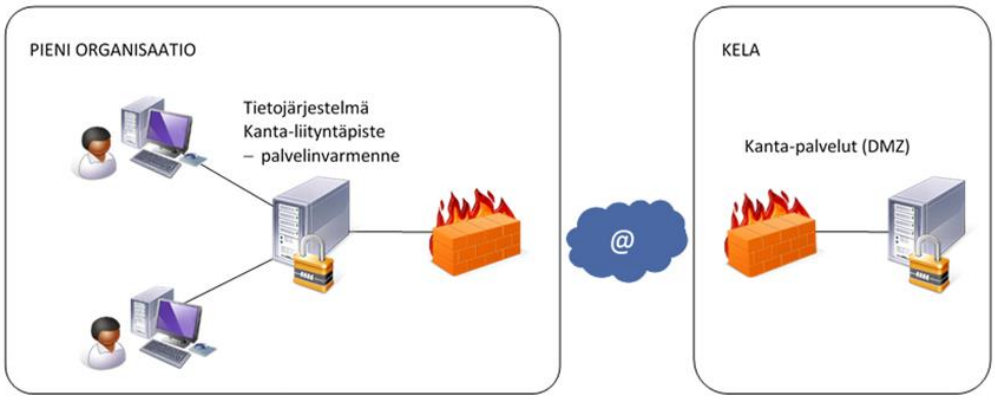
- yksityisen verkon yhteys, esim. MPLS
- kiinteät ja julkiset tietoliikenneosoitteet
- tilallinen palomuuri ja muu tietoturva
- palvelinvarmenne/liityntäpiste
- järjestelmäallekirjoitusvarmenne asiakas- tai potilastietojärjestelmän yhteydessä (arkistoon liityttäessä).

Suositukset liittymälle:

- kahdennettu, nopeudeltaan symmetrinen liittymä
- kapasiteettitarpeen ja toiminnan kriittisyyden mukaiset tekniset ja ylläpidolliset laatuvaatimukset.

5.3 Pienen organisaation liittyminen internetin kautta

Tässä mallissa organisaatio liittyy Kanta-palveluihin julkisen internetin kautta. Palvelinvarmenne asennetaan joko suoraan sovelluspalvelimelle tai verkon DMZ-alueelle (demilitarisoitu alue). Tapausesimerkkinä liittymismallista on pieni organisaatio, esimerkiksi apteekki (Kuva 7).



Kuva 7 Internetin kautta Kanta-palveluihin liittynyt pieni organisaatio

Vaatimukset liittymälle:

- kiinteät ja julkiset tietoliikenneosoitteet
- tilallinen palomuuri ja muu tietoturva
- palvelinvarmenne/liityntäpiste
- järjestelmäallekirjoitusvarmenne liittyvän tietojärjestelmän yhteydessä.

Suositukset liittymälle:

- kahdennettu, nopeudeltaan symmetrinen liittymä
- toiminnan kriittisyyden mukainen SLA-taso.

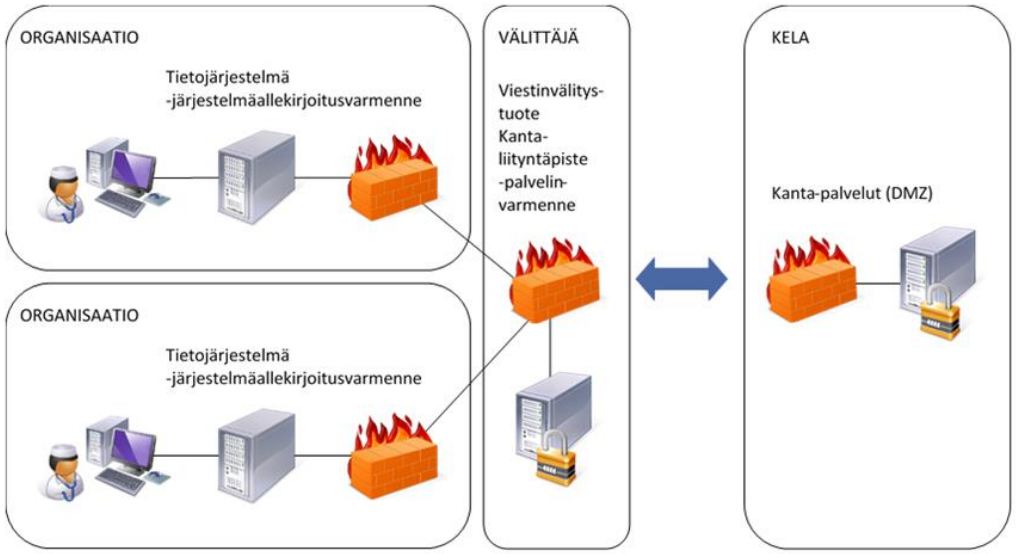
5.4 Liittyminen ulkoistetun liityntäpisteen kautta

Tässä mallissa organisaatio on liittynyt Kanta-palveluihin välittäjän toteuttaman Kanta-liityntäpisteen kautta. Organisaatio on voinut ulkoistaa välittäjälle

- tietojärjestelmän (esim. jaettu tietojärjestelmä SaaS-palveluna)
- viestinvälityksen ja/tai
- tietoliikenteen.

Palvelinvarmenne on yleensä välittäjän nimissä, ja se asennetaan liityntäpisteen yhteyteen.

Tapausesimerkkejä tietojärjestelmän tai viestinvälityksen ulkoistamisesta ovat alueellisen IT-palveluntuottajan kautta Kanta-palveluihin liittynyt organisaatioyksikkö (Kuva 8).



Kuva 8 Kaksi alueellisen IT-palveluntuottajan välityksellä Kanta-palveluihin liittynyttä organisaatiota

Vaatimukset liittymälle:

- TLS-salaus liittyvän organisaation ja välittäjäorganisaation välillä, sosiaali- ja terveydenhuollon varmentajan (VRK) myöntämällä palvelinvarmenteella
- integraatioratkaisun (viestinvälitysratkaisun) ja tietojärjestelmien välillä osapuolten identiteetin varmistaminen sosiaali- ja terveydenhuollon varmentajan (VRK) palvelinvarmenteella
- yksityisen verkon yhteys, esim. MPLS, välittäjäorganisaation ja Kanta-palvelujen välillä
- palvelinvarmenne välittäjäorganisaation nimissä
- järjestelmäallekirjoitusvarmenne tietojärjestelmän yhteydessä joko liittyjällä tai välittäjäorganisaatiolla, kuitenkin liittyvän organisaation nimissä tai sopimusperustaisesti välittäjälle valtuutettuna.

Suositukset liittymälle:

- kahdennettu, nopeudeltaan symmetrinen liittymä
- kapasiteettitarpeen ja toiminnan kriittisyyden mukaiset tekniset ja ylläpidolliset laatuvaatimukset.

Ulkoistettu tietoliikenne

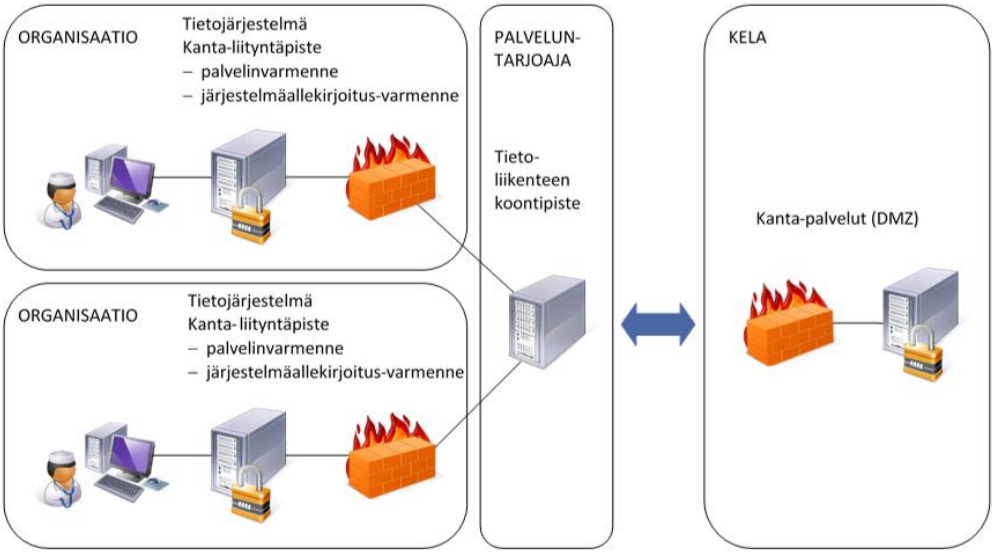
Tietoliikenteen koontipisteellä tarkoitetaan palvelua, jossa eri organisaatioista Kanta-palveluihin kulkeva tietoliikenne kootaan yhteen ja ohjataan Kanta-

palveluihin yhteistä tietoliikenneyhteyttä pitkin ja jossa vastaavasti Kanta-palveluista tuleva liikenne reititetään eri organisaatioihin. Tietoliikenteen reititys ei vaikuta yhteyksien TLS-salaukseen: salausta ei pureta eikä muodosteta koontipisteessä, eivätkä suojattavat tiedot näy salaamattomina. Kanta-välittäjäksi ei määritellä organisaatiota, joka toimii pelkästään TLS-salatun tietoliikenteen reitittäjänä tai koontipisteenä ja joka ei voi nähdä salaamattomia tietoja.

Koontipisteellä on vaikutusta Kanta-palveluihin liittymiseen ainoastaan, jos liityntäpisteen tietoliikenneosoite määräytyy koontipisteessä. Välittäjän tai liittyvän organisaation pitää silloin ilmoittaa palvelinvarmennehakemuksessa koontipisteen tietoliikenneosoite.

Vaatimukset koontipisteelle:

- Vastaanottopalvelujen (esim. uusimispyyntöjen vastaanotto) osoitteiden pitää olla yksikäsitteiset myös koontipisteen kautta liikennöitäessä.
- Palvelinvarmenne on liittyvällä organisaatiolla tai välittäjällä.



Kuva 9 Ulkoisen koontipisteen kautta Kanta-palveluihin liittyneitä organisaatioita

5.5 Yksityisen terveydenhuollon yhteisliittymismalli

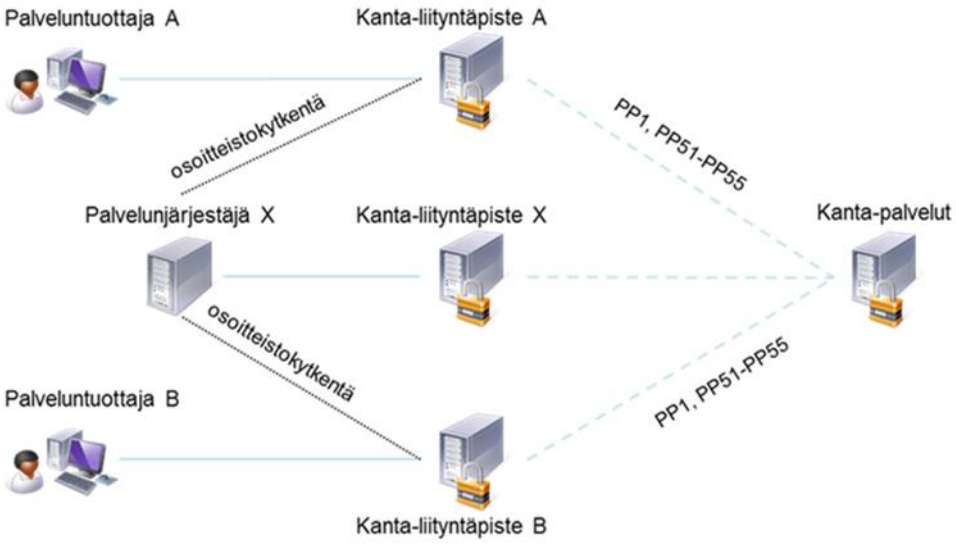
Tässä yhteisliittymismallissa palvelujen antaja (mukana liittyvä/vuokralainen) liittyy Kanta-palveluihin varsinaisen liittyjän (pääliittyjä) mukana. Pääliittyjä järjestää sanomaliikenteen ja tietoliikenteen siten, että palveluita käyttävälle vuokralaiselle tarjotaan tarvittavat tietojärjestelmäpalvelut pääliittyjän toimesta. Pääliittyjän ja mukana liittyvien välillä tulee olla Kanta-sopimusmallin mukainen sopimus.

Yhteisliittymismalliin liittyvän sanomaliikenneratkaisun erityispiirteet on kuvattu erillisissä määrittelyissä sekä Resepti-palvelun että Potilastiedon arkiston osalta. Tärkeää on, että liittyjän lisäksi näissä tilanteissa myös vuokralaisen tiedot välittyvät Kanta-palveluiden lokeille.

5.6 Potilastiedon arkiston pysyvä osoitteistokytkentä alihankintatilanteessa

Potilastiedon arkiston pysyvä osoitteistokytkentä alihankintatilanteessa on suunniteltu sellaisiin tilanteisiin, joissa esimerkiksi alueellisesti toimiva diagnostisia tutkimuksia tuottava organisaatio tuottaa asiakirjat suoraan Potilastiedon arkistoon. Koska ostopalvelutoiminta on näissä tapauksissa hyvin staattista tai jopa pysyväisluonteista, tarjoaa Kanta-palvelu mahdollisuuden arkistoida asiakirjoja (palvelupyyntö PP1) ja käyttää tiettyjä muita rajattuja palvelupyyntöjä (kevyet rajapinnat; PP51-PP53, PP55) palvelunjärjestäjän nimissä ilman ostopalvelun valtuutusta. Muiden palvelupyyntöjen käyttö on sallittua vain ostopalvelun valtuutuksella.

Koska mallissa palveluntuottaja toimii Kanta-palvelun suuntaan palvelunjärjestäjän nimissä, vaaditaan riittävien lokitietojen varmistamiseksi, että palvelunjärjestäjään kytketään dedikoitu liityntäpiste kutakin pysyvän ostopalvelujärjestelyn kautta Kanta-palveluita käyttävää tahoa varten. Tämä liityntäpiste yksilöi palvelunjärjestäjän nimissä Kanta-palveluita käyttävän palveluntuottajan.



Kuva 10 Pysyvä osoitteistokytkentä

6 Tietoliikenneyhteyksien mitoitus, laatuvaatimukset ja suositukset

Seuraavassa listassa on lueteltu esimerkkejä tarvittavan kapasiteetin minimivaatimuksista

- Pieni apteekki 10 Mbit/s
- Iso apteekki 30 Mbit/s
- Organisaatio, joka arkistoi alle 10 000 asiakirjaa päivässä 30 Mbit/s
- Organisaatio, joka arkistoi yli 100 000 asiakirjaa päivässä 500 Mbit/s
- Kuva-arkistoa käyttävä organisaatio, vähintään 300 Mbit/s

Vaaditut palvelutasomääreet ja tekniset laatuluokitukset perustuvat alalla yleisesti hyväksyttyihin raja-arvoihin. Tietoliikenteen mitoituksessa pyydetään noudattamaan JHS suosituksessa 174 ”Liite 1, palvelutasoluokat” -dokumentissa kuvattuja määrityksiä.

JHS-suositus 174 kokonaisuudessaan löytyy Internetistä osoitteesta: http://www.jhs-suositukset.fi/web/guest/jhs/recommendations/174.