Tekniset liittymismallit Kanta-palveluihin

Ohje

Kanta-palvelut

3.7.2024

Kela
Kanta-palvelut
PL 450, 00056 Kela

FPA
Kanta tjänsterma
PB 450, 00056 FPA

Kanta 381 07 24
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
3.6	Tarkennettu liityntäpisteen OID-tunnuksen muodostamista luvussa 2.3. Lisätty lukuun 4.2 maininta, että Kuvaaineistojen arkiston yhteytenä julkinen internet ei ole sallittu.	Kanta-palvelut Kela	8.11.2019
3.7	Tarkennettu luvussa 2.6 olevaa mainintaa sosiaali- ja terveydenhuollon järjestelmävarmenteista. Poistettu mainina Sosiaalihuollon asiakastiedon arkiston käytössä tarvittavasta erillisestä järjestelmäallekirjoitusvarmenteesta.	Kanta-palvelut Kela	9.12.2019
3.8	Viety dokumentti uudelle saavutettavuusvaatimukset täyttävälle mallipohjalle.	Kanta-palvelut Kela	1.4.2020

Versio	Muutos	Tekijä	PVM
	Muutettu viittaukset Väestörekisterikeskuksesta (VRK) Digi- ja väestötietovirastoksi (DVV)		
3.9	Lisätty lukuun 5.5 yksityisen sosiaalihuollon yhteisliittymismalli Lisätty lukuun 2.3 linjaus, että Kanta-liityntäpisteen on sijaittava Suomessa. Sama maininta myös luvun 5 alkuun.	Kanta-palvelut Kela	16.2.2021
3.10	Poistettu luvusta 1.1 Mihin järjestelmiin liitytään Sosiaalihuollon asiakastiedon arkiston liittymismallia koskeva rajoitus.	Kanta-palvelut Kela	2.6.2021
3.11	Lisätty lukuihin 1.4 ja 5.6 maininta, että pysyvää osoitteistokytkentää ei saa enää käyttää uusissa alihankintatilanteiden liittymisratkaisuissa, vanhoja aiemmin sovittuja alihankintatilanteiden pysyviä osoitteistokytkentöjä tuetaan edelleen. Lisäksi lukuun 1.4 otettu mukaan sosiaalihuollon yksiköt. Lukuun 2.3 lisätty teksti sairaala-apteekkien käyttämästä liityntäpisteestä.	Kanta-palvelut Kela	15.12.2021
3.12	Päivitetty luvun 2.6 kuvausta yhteisen järjestelmäallekirjoitusvarmenteen käyttötavoista.	Kanta-palvelut Kela	4.10.2022
3.13	Ohjeen rakennetta, termejä ja kuvia uudistettu. Tarkennettu Kanta-välittäjän roolia ja lisätty hallinnollisen liittymisen kuvausta. Tietoliikenneyhteyksiin liittyviä vaatimuksia tarkennettu. Päivitetty linkit ja viittaukset muihin ohjeisiin ja dokumentteihin.	Kanta-palvelut Kela	13.6.2023
3.14	Tarkennettu yhteisliittymismallin kuvausta. Yhteisliittymismalli on tarkoitettu yksityisten palvelunantajien Kanta-palvelujen käyttöön. Päivitetty ohjeeseen itsenäisten ammatinharjoittajien muuttuminen yksityisiksi palveluntuottajiksi Sote-valvontalain mukaisesti. Tarkennettu tietoliikenneyhteyksille ja varmenteille asetettuja vaatimuksia.	Kanta-palvelut Kela	2.1.2024

Versio	Muutos	Tekijä	PVM
3.15	Päivitetty viittaukset THL:n määräyksiin. Tietoliikenneyhteyksiin liittyviä vaatimuksia on tarkennettu julkisen internetin yhteyksien käytön osalta. Palvelinvarmenteelle tulevien tietoliikenneyhteyden tietoja on tarkennettu. Päivitetty ohjeessa mainittujen Kanta-palvelujen nimet.	Kanta-palvelut Kela	3.7.2024

Lyhenne	Termi	Selite
CA	certification authority varmentaja	taho, joka myöntää varmenteen
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
IP	internet protocol internet-yhteyskäytäntö	standardiksi muodostunut internetin verkkokerroksen yhteyskäytäntö, joka hoitaa pakettien reitityksen ja loogisen osoitteistuksen
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 KANIP-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
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

Sisällys

1 Johdanto

Ohjeessa kuvataan teknisiä liittymismalleja seuraaviin palveluihin:

- Potilastietovaranto
- Kuva-aineistojen tietovaranto
- Resepti-palvelu
- Sosiaalihuollon asiakastietovaranto.

Ohje ei koske ei koske palveluja, joiden

- käyttäminen ei edellytä erillistä liittymistä (Kansallinen koodistopalvelu, Validointipalvelu).
- liittymismallia ei ole vielä määritelty tai palvelun käytöstä on olemassa erillinen ohjeistus (Yhteistestaus, Asiakastestipalvelut, Kysely- ja välityspalvelu, Omatietovaranto).

Ohjeeseen liittyy keskeisesti seuraavat ohjeet ja määräykset:

- Määräys 3/2024: Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista (THL)
- Määräys 4/2024: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista (THL)
- Määräys 5/2024: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisista vaatimuksista (THL)
- ISO OID-yksilöintitunnuksen käytön kansalliset periaatteet sosiaali- ja terveysalalla (THL)
- Sertifiointi, olennaiset vaatimukset ja tietoturvasuunnitelma (Kanta.fi)

- Tieto- ja sanomaliikenteen tietoturvavaatimukset (Kanta.fi)
- Kanta-palvelujen käyttöönoton ohjeet (Kanta.fi)
- Kanta-palvelujen liittymismallit (Kanta.fi)
- Kanta-sanasto (THL)

Ohjeessa kuvataan Kanta-palvelujen tekniset liittymismallit. Malleista kuvataan yleisellä tasolla se, miten tekniset yhteydet palveluja käyttävän toimijan ja Kanta-palvelujen välille voidaan toteuttaa. Kanta-palvelut ei kuitenkaan säätele teknisen liittymisen toteutusta yksityiskohtaisesti.

Liittymismallit ovat pelkistyksiä. Niissä kuvataan teknistä liittymistä Kanta-palveluihin eri näkökulmista. Mallit eivät sulje pois toisiaan, ja tekninen liittyminen voidaan toteuttaa myös usean mallin yhdistelmänä.

Moninaisuutta teknisiin liittymisiin aiheuttavat Kanta-palveluja käyttävien toimijoiden olemassa olevat ympäristöt ja yhteydet, sekä käytössä olevat erilaiset ulkoistusratkaisut.

2 Toimijat

Tässä luvussa on esitelty ohjeessa esiintyvät toimijat.

2.1 Kanta-palvelut

Kanta-palvelut (myöhemmin tässä ohjeessa ”Kanta”) tuottaa sosiaali- ja terveydenhuollon digitaalisia palveluja kansalaisille ja sosiaali- ja terveydenhuollon toimijoille. Kannan toimintaa ohjaavia lakeja ovat Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä ja Laki sähköisestä lääkemääräyksestä. Kantaa tuotetaan yhteistyössä usean toimijan kanssa. Työssä ovat mukana Kansaneläkelaitos (Kela), Terveyden ja hyvinvoinnin laitos (THL), sosiaali- ja terveysministeriö (STM), Digi- ja väestötietovirasto (DVV) ja Valvira, sekä sote-toimijat, apteekit, järjestelmätoimittajat ja IT-palveluntuottajat.

Sosiaali- tai terveydenhuollon palvelunantaja tai apteekkari voi ottaa käyttöön Kantaan kuuluvia palveluja. Tässä ohjeessa käsitellään teknistä liittymistä palveluihin

Potilastietovaranto, Kuva-aineistojen tietovaranto, Resepti-palvelu ja Sosiaalihuollon asiakastietovaranto.

2.2 Kanta-liittyjä

Kanta-liittyjällä (myöhemmin tässä ohjeessa ”liittyjä”) tarkoitetaan palvelun käyttöön ottavaa apteekkaria tai sosiaali- tai terveydenhuollon palvelunantajaa.

Liittyjän Kanta-asiakkuus alkaa ensimmäisen palvelun käyttöönoton yhteydessä, jolloin liittyjä tekee sitoumuksen Kannan käytöstä ja hyväksyy yleiset toimitusehdot sekä palvelukohtaisen palvelukuvauksen. Liittyjällä voi olla käytössään yksi tai useampi palvelu.

Palvelun käyttöönoton yhteydessä liittyjä ilmoittaa Kantaan tiedon siitä, millä sertifioidulla järjestelmällä ja teknisellä yhteydellä käyttää palveluja. Kun Kanta hyväksyy liittyjän hakemuksen, liittyjälle avataan Kannan pääsynhallintaan tekniset oikeudet käyttää palveluja.

Kanta saa liittyjien perustiedot THL:n ylläpitämän Kansallisen koodistopalvelun koodistoista. Kaikkien liittyjien ja näiden sitoumuksella yhteisliittymismallin mukaisesti Kantaa käyttävien toimijoiden pitää olla rekisteröitynä Kansalliseen koodistopalveluun joko

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

* Sote-valvontalain (laki sosiaali- ja terveydenhuollon valvonnasta 741/2023) mukaisesti itsenäiset ammatinharjoittajat muuttuvat yksityisiksi palveluntuottajiksi 1.1.2024 alkaen. 31.12.2023 Valvira - Terveydenhuollon itsenäiset ammatinharjoittajat -koodistossa olevien palveluntuottajien (asiakastietolain mukaisesti palvelunantajien) tiedot siirtyvät Valviran Soteri-rekisteristä Kanta-palveluihin edelleen Kansallisen koodistopalvelun Valvira - Terveydenhuollon itsenäiset ammatinharjoittajat -koodiston kautta.

2.3 Vuokralainen (yhteisliittymismalli)

Vuokralaisella tarkoitetaan tässä ohjeessa yksityistä palvelunantajaa, joka käyttää palveluja luvussa 4 esitellyn yhteisliittymismallin mukaisesti liittyjän tekemän hallinnollisen hakemuksen perustella ja teknisen liittymisen kautta. Vuokralainen ei tee sitoumusta Kantaan, mutta liittyjän ja vuokralaisen tulee sopia keskinäisellä sopimuksella palvelujen käyttöön liittyvistä vastuista ja velvoitteista.

2.4 Kanta-välittäjä

Välittäjä on asiakastietolaissa (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä) määritelty palveluntarjoaja, joka tarjoaa sosiaali- ja terveydenhuollon palvelunantajalle tietojärjestelmäpalveluja, tietojärjestelmien käyttöympäristöjä tai Kanta-liityntäpisteitä. Välittäjä laatii THL:n määräyksessä 3/2024 kuvatun tietoturvasuunnitelman, jonka avulla suunnitellaan ja varmistetaan tietoturvan ja asianmukaisen asiakastietojen hallinnan toteutuminen.

Kanta-välittäjällä tarkoitetaan Kanta-liityntäpisteen toteuttavaa välittäjää. Liittyjä hyödyntää Kanta-välittäjän liityntäpistettä yhteyden muodostamisessa käytössään olevan tietojärjestelmän ja Kannan välille. Kanta-välittäjällä on tässä roolissa mahdollisuus nähdä salaamattomia asiakastietoja esimerkiksi ylläpitotoimien yhteydessä.

Kanta-välittäjä ilmoittautuu THL:n Kanta-Välittäjärekisteriin. Rekisteriin kootaan tiedot niistä välittäjistä, joilla on valtuutus toimia välittäjänä Kantaan liityttäessä, mutta jotka eivät ole apteekkeja tai sosiaali- tai terveydenhuollon palvelunantajia.

Kanta-välittäjän ja tämän liityntäpistettä omassa Kanta-liitynnässään hyödyntävän liittyjän väillä pitää olla sopimus, jossa todetaan Kannan käyttöön liittyvien toimintamallien ja ohjeiden noudattaminen, sekä tähän liittyvät vastuut ja velvoitteet.

3 Peruskäsitteet

3.1 Kanta-liityntäpiste

Kanta-liityntäpisteellä (myöhemmin tässä ohjeessa ”liityntäpiste”) tarkoitetaan sitä tietoliikenteen pistettä, josta liittyjän tietojärjestelmä liittyy Kantaan DVV:n myöntämällä sosiaali- ja terveydenhuollon palvelinvarmenteella salattua ja tunnistettua tietoliikenneyhteyttä pitkin.

Liittyjän käyttämä liityntäpiste voi olla liittyjän itsensä, toisen liittyjän tai Kanta-välittäjän hallinnoima. Liityntäpistettä hallinnoiva taho hakee liityntäpisteelle palvelinvarmenteen ja ilmoittaa Kannalle liityntäpisteen tiedot (mm. liityntäpisteen yksilöivän tunnisteen ja tietoliikenneyhteyksien tiedot).

3.1.1 Vaatimukset Kanta-liityntäpisteelle

Liityntäpiste pitää toteuttaa Valviran hyväksymällä järjestelmällä, joka voi olla THL:n määräyksen 4/2024 mukaisesti luokkaan A1 kuuluva asiakastietojen välityspalvelu tai välityspalvelun toiminnallisuudet sisältävä A2- tai A3-luokkaan kuuluva tietojärjestelmä.

Kanta-liityntäpisteen pitää sijaita Suomessa.

3.1.2 Suositukset Kanta-liityntäpisteelle

Suosituksena on määritellä yhdelle liityntäpisteelle yksi tietoliikenneosoite. Yhdelle liityntäpisteelle voidaan kuitenkin määritellä useampi osoite, jos se on tarpeen esimerkiksi varayhteyden järjestämiseksi.

Suosituksena on käyttää eri palvelimilla eri palvelinvarmenteita. Jos samaa palvelinvarmennetta käytetään useassa eri palvelimessa (esimerkiksi klusteritoteutuksessa), käsitellään palvelinvarmennetta käyttäviä palvelimia samana liityntäpisteenä. Jos klusterille ei ole yhteistä virtuaaliosoitetta, voivat klusterin jäsenet näkyä ulospäin omilla tietoliikenneosoitteillaan (IP-osoite).

3.1.3 Liityntäpisteen yksilöivä tunniste

Liityntäpisteelle annetaan yksilöivä OID-tunnus, joka muodostetaan solmuluokkaan 13.

Liityntäpisteen OID-tunnus muodostetaan liityntäpistettä hallinnoivan liittyjän, apteekin tai Kanta-välittäjän OID-tunnukseen perustuen seuraavasti:

- Sote-organisaatiorekisteriin rekisteröidyn sosiaali- ja terveydenhuollon palvelunantajan liityntäpisteen OID-tunnus on toimintayksikön OID-tunnuksesta riippuen joko 1.2.246.10.xxx.10.y.13.n tai 1.2.246.537.10. xxx.10.y.13.n (missä xxx on Sote-organisaatiorekisterin mukainen organisaation tunnus, y on toimijan yksilöivä numero ja n on liityntäpisteen yksilöivä numero).

- Valvira – Terveydenhuollon itsenäiset ammatinharjoittajat –rekisteriin rekisteröidyn palvelunantajan liityntäpisteen OID-tunnus on 1.2.246.537.28.xxx.13.n (missä xxx on Valvira – Terveydenhuollon itsenäiset ammatinharjoittajat –rekisterin mukainen palvelunantajan tunnus ja n on liityntäpisteen yksilöivä numero).

- Pää- ja sivuapteekin 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).

- Kanta-välittäjän 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).

3.2 Palvelinvarmenne

Liityntäpisteelle asennetaan DVV:n myöntämä sosiaali- ja terveydenhuollon palvelinvarmenne, jonka avulla tunnistetaan liityntäpiste ja muodostetaan salattu TLS-yhteys Kanta-palvelujen ja liityntäpisteen välille. Varmenteen tietoja käytetään myös palvelun osapuolten tunnistamisessa.

Palvelinvarmenne ja liityntäpiste kytketään toisiinsa palvelinvarmenteen Subject-osion serialNumber-kentän välityksellä. Kentän arvoksi tulee liityntäpisteen yksilöivä OID-tunnus. Ensisijaisen tietoliikenneyhteyden DNS-nimi tulee palvelinvarmenteen Subject-osion commonName-kenttään sekä SubjectAlternativeName-kenttään. SubjectAlternativeName-kenttään voi sijoittaa myös mahdolliset muut IP-osoitteet tai DNS-nimet.

Palvelinvarmenteen hankkii liityntäpistettä hallinnoiva toimija, joko liittyjä tai Kanta-välittäjä.

Palvelinvarmennetta voidaan käyttää myös liittyjän ja ulkoistetun liityntäpisteen välisen liikenteen salaamisessa ja liikennöivien osapuolien tunnistamisessa.

3.3 Järjestelmäallekirjoitusvarmenne

Potilastietovarantoa ja Sosiaalihuollon asiakastietovarantoa varten liittyjä tarvitsee käyttöönsä DVV:n myöntämän sosiaali- ja terveydenhuollon järjestelmäallekirjoitusvarmenteen. Sen yksityisellä avaimella allekirjoitetaan kaikki palveluihin lähetettävät asiakirjat, joita ei ole allekirjoitettu ammattihenkilön varmenteella.

Liittyjä tarvitsee ainoastaan yhden järjestelmäallekirjoitusvarmenteen. Samaa järjestelmäallekirjoitusvarmennetta voi käyttää kaikissa liittyjän potilas- tai asiakastietojärjestelmissä.

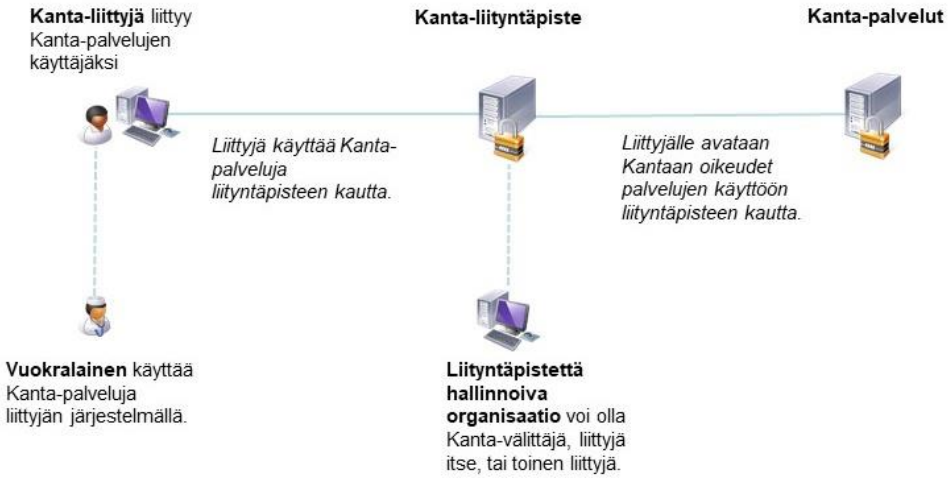
Järjestelmäallekirjoitusvarmenne on lähtökohtaisesti liittyjäkohtainen. Jos liittyjä hankkii potilastieto- tai asiakastietojärjestelmän kokonaispalveluna, voi liittyjä käyttää myös kokonaispalvelun palveluntoimittajan hankkimaa järjestelmäkohtaista järjestelmäallekirjoitusvarmennetta. Tuolloin järjestelmäallekirjoitusvarmenteen käyttöön liittyvät vastuut ja velvoitteet kirjataan varmenteen hankkineen palveluntoimittajan ja liittyjän välisiin sopimuksiin. Palveluntoimittajan tulee olla Kanta-välittäjä.

Yhteisliittymismallin mukaisessa liittymisessä vuokralainen voi käyttää liittyjän järjestelmäallekirjoitusvarmennetta. Asiasta tulee sopia liittyjän ja vuokralaisen keskinäisessä sopimuksessa.

4 Kanta-palvelujen liittymismallit

Kanta-palvelujen käyttöönotto edellyttää liittyjältä hallinnollista liittymistä, jota on kuvattu Kanta.fi-sivustolla Käyttöönotot- ja Asiakkuus-osioissa. Liittyjä voi ottaa käyttöön yhden tai useamman palvelun. Ensimmäisen palvelun käyttöönoton yhteydessä liittyjä tekee hakemuksen palvelun käyttäjäksi liittymisestä, allekirjoittaa sitoumuksen Kannan käytöstä, sekä hyväksyy yleiset toimitusehdot ja käyttöön otettavan palvelun palvelukuvauksen. Seuraavia palveluja käyttöön otettaessa riittää liittymishakemuksen tekeminen ja palvelukuvauksen hyväksyminen.

Palveluja käyttöön ottaessaan liittyjä ilmoittaa, minkä liityntäpisteen/liityntäpisteiden kautta ja millä järjestelmällä/järjestelmillä käyttää palvelua. Hakemuksen perusteella liittyjälle avataan Kannan pääsynhallintaan oikeudet käyttää palveluja. (Kuva 1).



Kuva 1: Kanta-palvelujen käyttö

4.1 Hallinnollinen liittyminen

4.1.1 Sosiaali- tai terveydenhuollon palvelunantajat

Suoraliittymismallissa liittyjä on hallinnollisen liittymisen tehnyt sosiaali- ja terveydenhuollon palvelunantaja.

Yksityisille palvelunantajille tarkoitetussa **yhteisliittymismallissa** palveluja voi käyttää yksityisen liittyjän tiloissa toimiva ja tietojärjestelmää käyttävä yksityinen palvelunantaja, jota tässä ohjeessa kutsutaan vuokralaiseksi. Vuokralainen ei tee sitoumusta Kantaan eikä siten toimi liittyjänä. Vuokralainen ja liittyjä sopivat keskinäisellä sopimuksella palvelujen käyttöön liittyvistä vastuista ja velvoitteista.

Sosiaalihuollon asiakastietovarannon **rinnakkaisliittymismallissa** yksityisen sosiaalihuollon palvelunantaja toimii palveluntuottajan roolissa ja käyttää palveluja palvelunjärjestäjän asiakastietojärjestelmän kautta. Rinnakkaisliittymismallissa palveluntuottajana toimiva palvelunantaja tekee hallinnollisen liittymisen Kantaan ja on siten liittyjä.

4.1.2 Apteekkarit

Pää- ja sivuapteekin apteekkari tekee hallinnollisen liittymisen Kantaan ja on liittyjä. Apteekkarin tekemä sitoumus koskee kaikkia apteekkarin kulloinkin hallussa olevia apteekkeja.

4.1.3 Sairaala-apteekit ja lääkekeskukset

Sairaala-apteekki tai lääkekeskus tekee sitoumuksen Kannan käytöstä ja on liittyjä.

4.2 Tekninen liittyminen

Palveluja käyttöön ottaessaan liittyjä ilmoittaa Kantaan, minkä liityntäpisteen/liityntäpisteiden kautta ja millä järjestelmällä/järjestelmillä käyttää palveluja. Hakemuksen perusteella liittyjälle avataan Kannan pääsynhallintaan oikeudet käyttää palveluja.

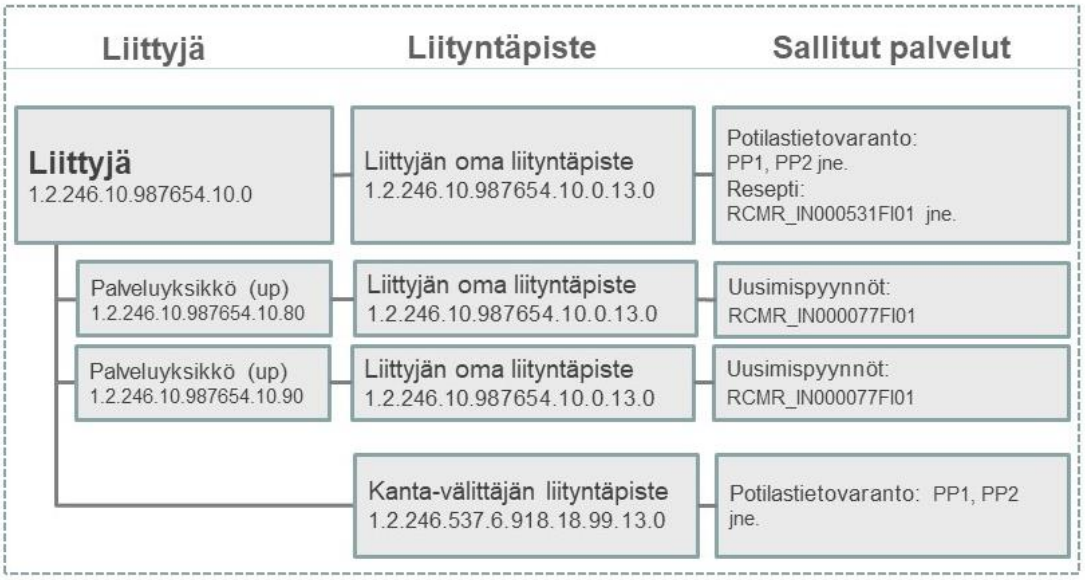
Osana Kannan pääsynhallintaa toimii Kanta-osoitehakemisto, johon tallennetaan liittyjän, liittyjän käyttämien liityntäpisteiden ja liittyjälle sallittujen palvelujen tiedot.

4.2.1 Sosiaali- tai terveydenhuollon palvelunantajat

Suoraliittymismallissa liittyjälle avataan Kanta-osoitehakemistoon oikeudet niihin palveluihin, joihin liittyjä on tehnyt liittymishakemuksen ja joiden käyttäjäksi Kanta on liittyjän hyväksynyt.

Jos liittyjä on Resepti-palvelua käyttävä uusimispyyntöjä apteekeista ja OmaKannasta vastaanottava terveydenhuollon palvelunantaja, avataan liittyjälle oikeudet uusimispyyntöjen vastaanottoon. Uusimispyyntöjen vastaanottaminen edellyttää, että liittyjällä on merkintä uusimispyyntöjen vastaanottamisesta THL:n Kansallissa koodistopalvelussa. Merkintä tehdään palvelunantajalle Valviran Terveydenhuollon itsenäiset ammatinharjoittajat –koodistoon tai palveluyksikkökohtaisesti SOTE-organisaatiorekisteriin.

Kuvassa 2 on esitelty yksinkertaistettu esimerkki Kantaa suoraliittymismallilla käyttävän terveydenhuollon palvelunantajan teknisestä liittymisestä. Liittyjä käyttää palveluja kahden eri liityntäpisteen kautta. Ensimmäinen liityntäpiste on liittyjän omassa hallinnassa, ja sen kautta liittyjä käyttää Resepti-palvelua ja Potilastietovarantoa. Lisäksi liittyjällä on kaksi uusimispyyntöjä vastaanottavaa palveluyksikköä, joiden uusimispyynnöt kulkevat liittyjän oman liityntäpisteen kautta. Liittyjä käyttää Potilastietovarantoa myös Kanta-välittäjän liityntäpisteen kautta. Kanta–osoitehakemistoon lisätään liittyjälle Reseptin ja Potilastietovarannon palvelut sekä uusimispyyntöjen vastaanoton palvelu oman liityntäpisteen kautta. Lisäksi liittyjälle lisätään Potilastietovarannon palvelut Kanta-välittäjän liityntäpisteen kautta.



Kuva 2: Terveydenhuollon palvelunantajan tekninen liittyminen

Yhteisliittymismallissa vuokralaiselle ei avata Kannan pääsynhallintaan oikeuksia palvelun käyttöön. Vuokralainen käyttää palveluja liittyjän oikeuksilla, mutta liittyjän pitää tuoda palveluun tuleville sanomille ja asiakirjoille tieto siitä, että palvelun käyttäjä on vuokralainen.

Rinnakkaisliittymismallissa palveluntuottajana toimivalle liittyjälle avataan Kanta-osoitehakemistoon oikeudet käyttää Sosiaalihuollon asiakastietovarantoa palvelunjärjestäjän käyttämän liityntäpisteen kautta.

Liittyjänä toimivalle sairaala-apteekille tai lääkekeskukselle avataan Kanta-osoitehakemistoon oikeudet käyttää Resepti-palvelua. Sairaala-apteekit ja lääkekeskukset voivat liittyä Kantaan toisen liittyjän, Kanta-välittäjän tai oman liityntäpisteen kautta.

4.2.2 Pää- ja sivuapteekit

Jokaisella pää- ja sivuapteekilla on oma liityntäpiste. Pää- ja sivuapteekeille avataan Kannan pääsynhallinnassa oikeudet käyttää Resepti-palvelua oman liityntäpisteensä kautta.

Kuvassa 3 on esitelty apteekin liittymismalli. Apteekkari tekee hallinnollisen liittymisen Kantaan. Apteekkarin hallussa on pääapteekki ja sen sivuapteekki. Sekä pää- että sivuapteekilla on omat liityntäpisteet. Kanta-osoitehakemistossa pää- ja sivuapteekeille

avataan apteekin tarvitsemat oikeudet Resepti-palveluun apteekkien omien liityntäpisteiden kautta.

Kuva 3: Apteekin tekninen liittyminen

5 Tietoliikenne

Liityntäpistettä hallinnoiva toimija ilmoittaa Kantaan liityntäpisteen tietojen ohessa liityntäpisteen tietoliikenneyhteydet, joille tehdään Kannassa tarvittavat reitit ykset. Uutta tuotantoympäristön liityntäpistettä perustettaessa liityntäpistettä hallinnoiva toimija voi pyytää Kannan tuotantoympäristöjen osoitteet ja sanomaliikenteen osapuolitunnisteet Kannan asiakaspalvelusta.

Liittyjän vastuulla on liittyjän ja Kannan välisten tietoliikenneyhteyksien tilaaminen liittyjän omien kapasiteetti-, laatu- ja palvelutasovaatimuksien mukaisesti. Tietoliikenneyhteyksissä on huomioitava myös varayhteydet häiriötilanteiden sekä poikkeusolojen yhteyksien turvaamiseksi. Kela vastaa Kannan sisäisestä tietoliikenteestä tietoliikenneoperaattorin rajapintaan asti.

Tässä kappaleessa on esitetty tietoliikenneyhteydelle asetetut keskeiset vaatimukset ja suositukset yleisellä tasolla.

5.1 Liittymän tyyppi

Liittyjän ja Kannan väliset tietoliikenneyhteydet pitää toteuttaa yksityisen verkon yhteytenä palvelun saatavuuden ja laadun varmistamiseksi. Yksityisen verkon yhteydet pystytään paremmin suojaamaan julkisen internetin uhilta, mm. palvelunestohyökkäyksiltä.

Yksityisen verkon liittymälle tietoliikenneoperaattori takaa tietyn kapasiteetin koko liittymän matkalle. Yksityisen verkon liittymä (MPLS tai vastaava) tilataan tietoliikenneoperaattorilta liittyjän, liityntäpisteen tai tietoliikennesolmun ja Kannan palvelinsalien välille. Yhteyksien käyttöönottovaiheessa on varauduttava siihen, että yhteyden toteuttaminen voi kestää useita viikkoja. Yhteyden pitää olla valmiina silloin, kun yhteyttä käyttävä liittyjä tekee liittymishakemuksen Kantaan.

Julkista internet-yhteyttä voi käyttää vain perustelluissa poikkeustapauksissa. Kuva-aineistojen tietovarannon yhteytenä tai apteekkien Reseptin ensisijaisena yhteytenä julkinen internet-yhteys ei ole sallittu edes poikkeustapauksissa.

Taulukossa 1 on kuvattu julkisen internet-yhteyden käyttöä eri tilanteissa.

Yhteyden käyttö	**Julkinen internet-yhteys**
Apteekkijärjestelmät, apteekin hallinnassa oleva liityntäpiste	Julkiksen internet-yhteyden käyttö on sallittua vain varayhteytenä.
Potilastietojärjestelmät, jos käytössä on liittyjän omassa hallinnassa oleva liityntäpiste	Julkisen internet-yhteyden käyttö on sallittua, jos liittyjän itse hallinnoimaa liityntäpistettä käyttää vain liittyjä itse ja sanomaliikenteen määrä on pieni.
Asiakastietojärjestelmät, jos käytössä on liittyjän omassa hallinnassa oleva liityntäpiste	Julkisen internet-yhteyden käyttö on sallittua, jos liittyjän itse hallinnoimaa liityntäpistettä käyttää vain liittyjä itse ja sanomaliikenteen määrä on pieni.
Tietoliikenteen koontipiste tai Kanta-välittäjän tarjoama liityntäpiste	Julkisen internet-yhteyden käyttö on sallittua vain varayhteytenä.

Taulukko 1: Esimerkkejä julkisen internet-yhteyden käytöstä

Julkisen internetin yhteyttä käytettäessä on huomioitava erityisesti yhteystavasta johtuvat riskit, kuten palvelunestohyökkäykset ja internet-rajapintaan kohdistuvat muut tietoturvauhat.

5.2 Vaatimukset tietoliikenteelle

Liityntäpisteelle määriteltyjen IP-osoitteiden pitää olla kiinteitä ja kuulua julkiseen IP-osoiteavaruuteen. IP-osoite tulee pystyä yksilöimään julkisessa hakemistossa liityntäpistettä hallinnoivalle toimijalle kuuluvaksi.

Liityntäpisteen ja Kannan väliset tietoliikenneyhteydet tulee toteuttaa yksityisen verkon yhteytenä esim. MPLS-menetelmän avulla. Yksityisen verkon yhteyksien tulee mahdollistaa tietoliikenteen siirtyminen Kanta-palveluiden eri lokaatioihin (Kanta A-, B- ja C-saleihin). Julkisen internetin kautta tulevien yhteyksien käyttö on sallittua vain luvussa 5.1 esitellyissä poikkeustapauksissa.

Liityntäpisteen ja Kannan väliset tietoliikenneyhteydet tulee toteuttaa varmennettuina. Liittymän tilaajan kannattaa varmistaa tietoliikenneoperaattoriltaan, että ensisijainen yhteys ja varayhteys kulkevat aidosti eri reittejä koko matkan. Varmistaminen voi olla mahdotonta, jos liittymät hankitaan 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 se on taloudellisesti järkevää.

Kantaan liittymisen teknisen ratkaisun tulee täyttää ohjeessa Kanta-palvelut: tieto- ja sanomaliikenteen tietoturvavaatimukset tieto- ja sanomaliikenteen tietoturvavaatimukset esitetyt vaatimukset.

5.3 Suositukset tietoliikenteelle

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

5.4 Liittymän tiedonsiirtokapasiteetti

Liittymän tiedonsiirtokapasiteettitarpeen määrittely on liittyjän vastuulla. Kapasiteettitarpeen arvioinnissa tulee huomioida liikennöintimäärä ja toiminnan kriittisyys. Liittyjän tulee varmistua liittymän skaalautuvuudesta.

5.5 Tietoliikenneyhteyksien mitoitus

Seuraavassa listassa on lueteltu esimerkkejä tarvittavan kapasiteetin minimivaatimuksista

- Pieni apteekki 10 Mbit/s
- Iso apteekki 30 Mbit/s
- Liittyjä, joka arkistoi alle 10 000 asiakirjaa päivässä 30 Mbit/s
- Liittyjä, joka arkistoi yli 100 000 asiakirjaa päivässä 500 Mbit/s
- Kuva-aineistojen tietovarantoa käyttävä liittyjä, vähintään 300 Mbit/s

5.6 Tietoliikenteen koontipiste

Tietoliikenteen koontipiste on ratkaisu, jossa eri liityntäpisteistä Kantaan kulkeva tietoliikenne kootaan yhteen ja ohjataan Kantaan yhteistä tietoliikenneyhteyttä pitkin ja jossa vastaavasti Kannasta tuleva liikenne reititetään eri liityntäpisteisiin. Tietoliikenteen reititys ei vaikuta yhteyksien TLS-salaukseen: salausta ei pureta eikä muodosteta koontipisteessä, eivätkä suojattavat tiedot näy salaamattomina.

6 Yhteenveto teknisen liittymisen suosituksista ja vaatimuksista

Teknisessä liittymisessä tulee huomioida ohje Kanta-palvelut: tieto- ja sanomaliikenteen tietoturvavaatimukset tieto- ja sanomaliikenteen tietoturvavaatimukset, sekä seuraavat vaatimukset:

- Tietoliikenneyhteydet toteutetaan lähtökohtaisesti yksityisen verkon yhteytenä esim. MPLS-menetelmän avulla. Yksityisen verkon yhteys tulee yhdistää Kanta-palveluiden eri lokaatioihin (Kanta A-, B- ja C-saleihin). Julkisen internetin kautta tulevien yhteyksien käyttö on sallittua vain tamän ohjeen luvussa 5.1 esitetyissä poikkeustapauksissa.
- IP-osoitteiden pitää olla kiinteitä ja julkisia. IP-osoite tulee pystyä yksilöimään julkisessa hakemistossa liityntäpistettä hallinnoivalle toimijalle kuuluvaksi.

- Teknisen ratkaisun pitää täyttää tieto- ja sanomaliikenteen tietoturvavaatimukset, joihin kuuluu mm. tilallinen palomuuri ja virustorjunnasta huolehtiminen.

- Liityntäpisteelle asennetaan DVV:n myöntämä palvelinvarmenne, jonka avulla tunnistetaan liityntäpiste ja muodostetaan salattu TLS-yhteys Kannan ja liityntäpisteen välille. Varmenteiden tulee olla vähintään kyberturvallisuuskeskuksen TL IV -tason mukaisesti määritettyjen kansallisten kryptografisten vaatimusten mukaisia.

- Potilastietovarannon tai Sosiaalihuollon asiakastietovarannon palveluja käytettäessä liittyjällä pitää olla käytössään järjestelmäallekirjoitusvarmenne.

- Tietoliikenneyhteydet tulee monentaa.

Suosituksena on käyttää nopeudeltaan symmetristä tietoliikenneyhteyttä.

7 Teknisen liittymisen esimerkit

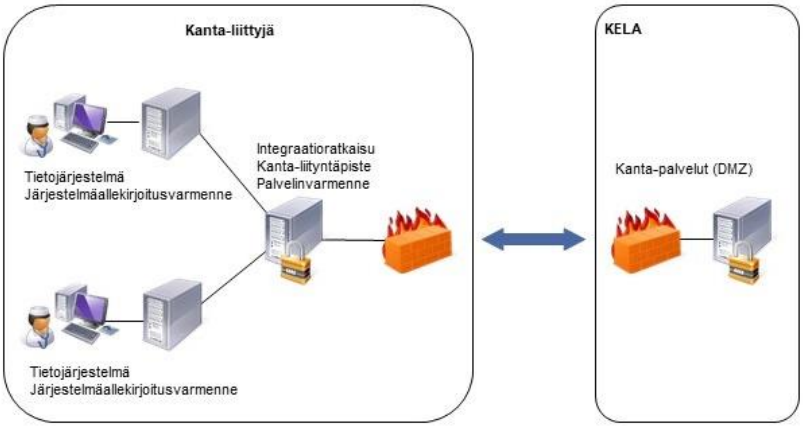
Tässä esitellyt tekniset liittymismallit eivät sulje pois toisiaan, ja liittymisessä voidaan yhdistää eri malleja. Kaikissa tässä luvussa kuvattujen teknisten liittymismallien osalta on huomioitava, että liityntäpisteiden on sijaittava Suomessa.

7.1 Liittyminen liittyjän oman liityntäpisteen kautta

7.1.1 Liittyminen oman integraatioratkaisun kautta

Tässä esimerkissä liittyjällä on oma integraatioratkaisu, jonka kautta palveluja käytetään useilla liittyjän käytössä olevilla eri tietojärjestelmillä. DVV:n myöntämä palvelinvarmenne asennetaan integraatioratkaisun yhteyteen. Palvelinvarmenteella muodostetaan tunnistettu ja salattu yhteys Kantaan. Palvelinvarmennetta voidaan tarvita myös integraatioratkaisun ja liitettävien tietojärjestelmien välillä osapuolten identiteetin varmistamisessa ja tiedonsiirron salaamisessa.

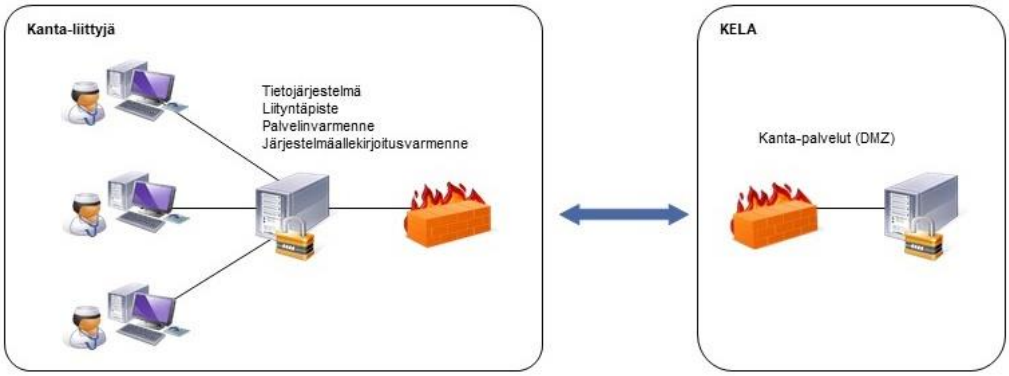
Integraatioratkaisun käyttö mahdollistaa useiden järjestelmien liikenteen Kantaan samaa tietoliikenneyhteyttä pitkin. (Kuva 4).



Kuva 4: Liittyminen liittyjän oman integraatioratkaisun kautta

7.1.2 Liittyminen suoraan omassa hallinnassa olevasta tietojärjestelmästä

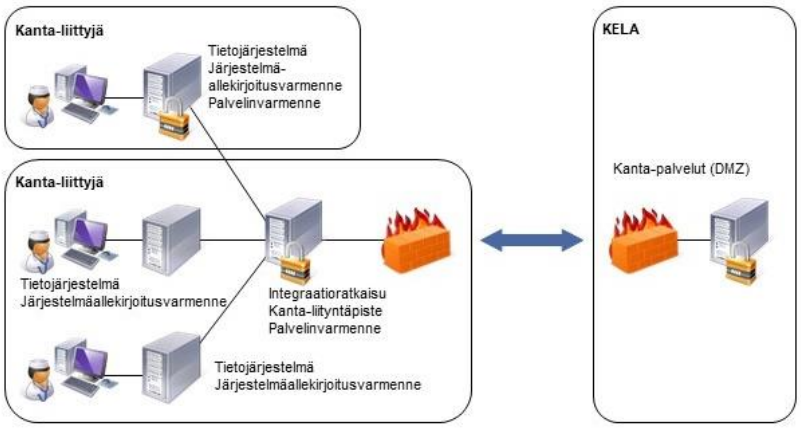
Esimerkissä Kantaan liitettävä tietojärjestelmä ja liityntäpiste ovat liittyjän omassa hallinnassa. Palvelinvarmenne asennetaan suoraan sovelluspalvelimelle tai erilliseen aktiivilaitteeseen tietojärjestelmän yhteyteen. (Kuva 5).



Kuva 5: Liittyminen liittyjän omassa hallinnassa olevasta tietojärjestelmästä

7.2 Liittyminen toisen liittyjän liityntäpisteen kautta

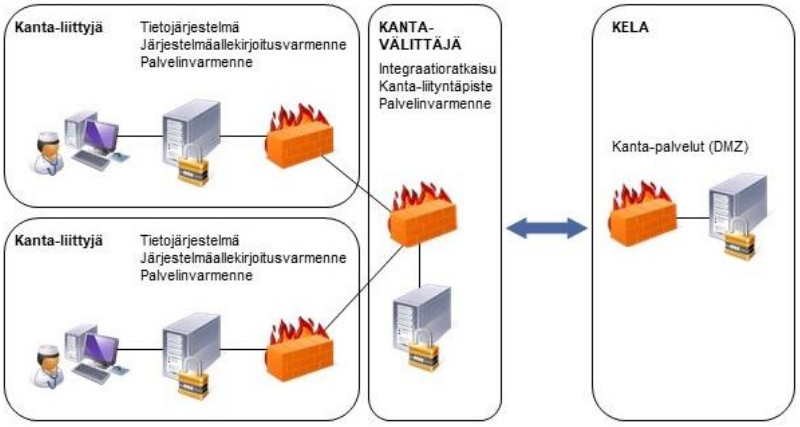
Tässä esimerkissä liittyjä käyttää Kantaa toisen liittyjän toteuttaman liityntäpisteen kautta. Palvelinvarmenne on liityntäpistettä hallinnoivan liittyjän nimissä ja se asennetaan liityntäpisteen yhteyteen. Liittyjän ja liityntäpistettä hallinnoivan liittyjän välinen liikenne on salattu ja liikennöivät osapuolet on tunnistettu DVV:n myöntämän palvelinvarmenteen avulla. (Kuva 6).



Kuva 6: Liittyminen toisen liittyjän hallinnoiman liityntäpisteen kautta

7.3 Liittyminen Kanta-välittäjän liityntäpisteen kautta

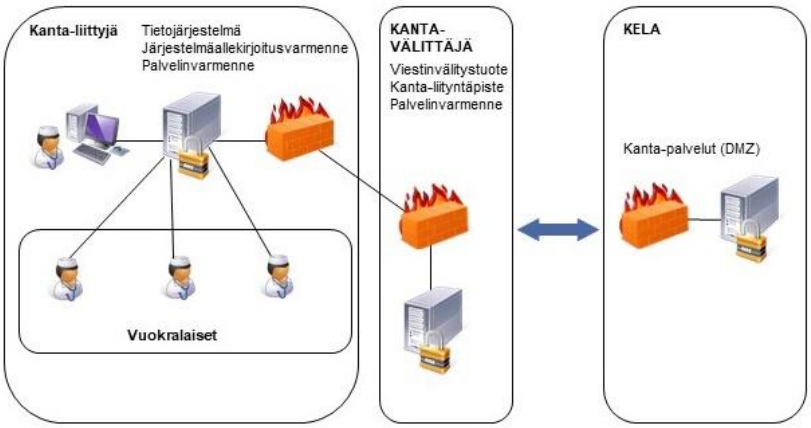
Tässä esimerkissä liittyjä käyttää palveluja Kanta-välittäjän toteuttaman liityntäpisteen kautta. Palvelinvarmenne on Kanta-välittäjän nimissä ja se asennetaan liityntäpisteen yhteyteen. Liittyjän ja Kanta-välittäjän liityntäpisteen välinen liikenne salataan ja liikennöivät osapuolet tunnistetaan DVV:n myöntämän palvelinvarmenteen avulla. Liittyjillä on liittyjäkohtaiset järjestelmäallekirjoitusvarmenteet. (Kuva 7).



Kuva 7: Liittyminen Kanta-välittäjän hallinnoiman liityntäpisteen kautta

7.4 Yhteisliittymismallin mukainen liittyminen

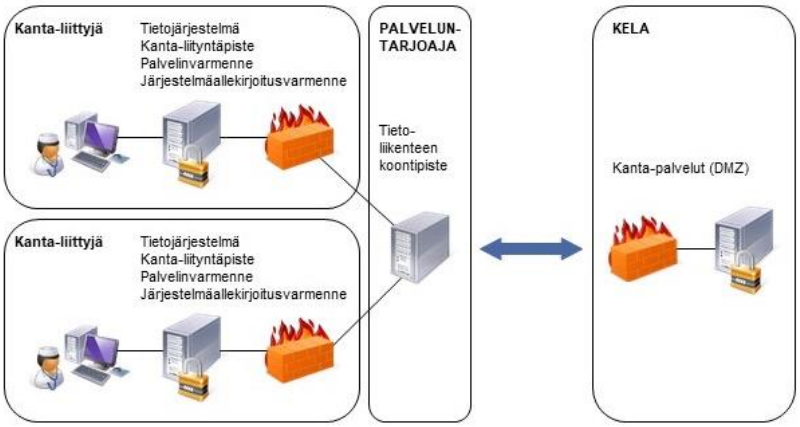
Tässä esimerkissä vuokralainen (terveydenhuollon palvelunantaja) käyttää palveluja liittyjän tietojärjestelmän ja teknisen yhteyden kautta. Vuokralainen tekee liittyjän kanssa sopimuksen Kannan käyttöön liittyvistä vastuista ja velvoitteista. Tietojärjestelmä lisää Kantaan tallennettaville asiakirjoille ja sanomille vuokralaisen tunnistetiedot. (Kuva 8).



Kuva 8: Yhteisliittymismallin mukainen liittyminen

7.5 Liittyminen tietoliikenteen koontipistettä hyödyntäen

Tässä esimerkissä liittyjä käyttää palveluja omalla tietojärjestelmällään oman liityntäpisteensä kautta. Liittyjän liityntäpisteeltä Kantaan kulkeva tietoliikenne kootaan yhteen tietoliikenteen koontipisteessä ja ohjataan Kantaan yhteistä tietoliikenneyhteyttä käyttäen. Vastaavasti Kannasta tuleva liikenne reititetään tietoliikenteen koontipisteessä eri liittyjien liityntäpisteisiin. (Kuva 9).



Kuva 9: Liittyminen tietoliikenteen koontipistettä hyödyntäen