Tekniska anslutningsmodeller till Kanta-tjänsterna

Kanta-tjänster

Kela
Kanta-palvelut
PL 450, 00056 Kela

FPA
Kanta tjänsterna
PL 450, 00056 FPA

Kanta 381r 12.19
www.kanta.fi
kanta@kanta.fi

Dokumenthistorik

Version	Beskrivning	Utarbetad / godkänd av	Datum
2.6	Hänvisning till bilaga 1 tillfogad, meddelandeförmedling ersatt med termen integrationslösning, beskrivningen av Kanta-anslutningspunkten preciserad, ett exempel på uppgifter om apotek tillfogat i adressindexet	Kanta-servicegruppen, FPA	29.4.2010
2.7	Avsnitt 1.3 preciserat: rekommenderat antal anslutningspunkter är 1, även om organisationen har mottagningstjänster. Figurerna 5 och 7 rättade.	Kanta-servicegruppen, FPA	3.6.2010
2.8	Port 443 för mottagningstjänster tillfogad.	Kanta-servicegruppen, FPA	24.6.2010
2.9	Definitionen av Kanta-anslutningspunkt preciserad. Hälso- och sjukvårdens certifikatutfärdare har bytts ut fr.o.m. 1.12.2010.	Kanta-servicegruppen, FPA	3.2.2011
3.0	De särdrag som hänför sig till anslutningsmodellen för den privata hälso- och sjukvården samt permanent adressbokskoppling när underleverantörer anlitas har tillfogats.	Kanta-tjänsterna, FPA	18.6.2015
3.1	Anvisningarna om användning av slutet kundnät som anslutningsmodell har preciserats.	Kanta-tjänsterna, FPA	24.10.2016
3.2	Anvisningarna har bearbetats med tanke på de nya systemens behov. Bilaga 1 har strukits och ersatts med en hänvisning till JHS-rekommendationerna.	Kanta-tjänsterna, FPA	23.11.2017
3.3	Begreppen i kapitel 5.5 har rättats	Kanta-tjänsterna, FPA	4.1.2018
3.4	Termen slutet kundnät har rättats till termen privat nät. Ett exempel på hur OID-koden bildas har tillfogats. Anvisningen om när öppen internetförbindelse används för Kanta-anslutningar har preciserats.	Kanta-tjänsterna, FPA	31.1.2019
3.5	Omnämnandet av ett separat skriftligt godkännande från Kanta-tjänsterna i kapitel 4.2 (Öppen internetförbindelse i undantagsfall) har tagits bort.	Kanta-tjänsterna, FBA	10.6.2019
3.6	Anvisningarna om hur OID-koden bildas har preciserats i kapitel 2.3. I kapitel 4.2 har lagts till ett omnämnande att en öppen internetförbindelse inte är tillåten som förbindelse till Arkivet över bildmaterial.	Kanta-tjänsterna FPA	8.11.2019

3.7	Omnämnandet om systemcertifikat för social- och hälsovården har preciserats i kapitel 2.6. Omnämnandet om att det behövs ett separat systemsigneringscertifikat vid användningen av Klientdataarkivet för socialvården har strukits. .	Kanta-tjänsterna FPA	9.12.2019

Innehåll

Förkortningar

CA	certification authority certifikatutfärdare	instans som beviljar certifikat Källa: Koncis informationssäkerhetsordlista (TSK 31, 2004)
DMZ	demilitarized zone demilitariserad zon	fysiskt eller logiskt delnät av en organisations lokala nät, som ansluter det lokala nätet till internet
DNS	domain name system domännamnssystem	system som konverterar domännamn i textform till IP-adresser och tvärtom Källa: Internettelefoniordlista (TSK 37, 2007)
IP	internet protocol internetprotokoll	protokoll som blivit standard för internets nätverksskikt och vars uppgift är att sköta routningen av paket och den logiska adresseringen Källa: Mobilordlista (TSK 29, 2001)
ISO	International Organization for Standardization	internationella standardiseringsorganisationen
MPLS	multiprotocol label switching	metod för att dirigera t.ex. IP-paket över på förhand definierade förbindelser via noder i ett snabbt stamnät utan att noderna behöver sköta routningen
NAT	network address translation konvertering av IP-adress	en metod enligt en internet-standard, där IP-adresser konverteras till andra IP-adresser
OID	object identifier objektidentifierare	en unik teckensträng med vars hjälp ett objekt, t.ex. ett föremål eller en sak kan särskiljas från andra motsvarande
SSL	secure sockets layer	en krypteringsmetod som kan användas för att skydda internetprograms kommunikation över IP-nät
TCP	transmission control protocol	protokoll som sköter dataöverföring och säkerställer att informationen går fram genom att vid behov skicka den på nytt Källa: Internettelefoniordlista (TSK 37, 2007)

TLS	transport layer security	en krypteringsmetod som kan användas för att skydda internetprograms kommunikation över IP-nät, version 1.2 används
URL	uniform resource locator URL-adress	en teckensträng som identifierar en fil, ett index eller någon annan resurs som finns på internet samt det protokoll som behövs för att använda dessa Källa: Tietotekniikan termitalkoot, 2007-12-14

1 Inledning

I detta dokument beskrivs tekniska anslutningsmodeller till Kanta-tjänsterna. Till denna anvisning hänför sig följande dokument:

- Vem ansluter sig till Kanta-tjänsterna Anvisning för aktörer som ansluter sig till Kanta
- Hur ansluter man sig till Kanta-tjänsterna Anvisning för aktörer som ansluter sig till Kanta
- Föreskrift om utredningar och krav som ska tas in i planen för egenkontroll (THL:s föreskrift 2/2015)
- Kanta-certifiering och egenkontroll – överblick och processer
- Föreskrift om väsentliga krav på informationssäkerhet hos informationssystem av klass A inom social- och hälsovården (THL:s föreskrift 1/2015)
- Certifiering av Kanta-förmedlingsservice samt Kanta-förmedlare (THL:s anvisning 3/2015)
- ISO OID -yksilöintitunnuksen käytön kansalliset periaatteet sosiaali- ja terveysalalla

De organisationer som ansluter sig till Kanta-tjänsterna är av mycket varierande storlek och har varierande teknisk beredskap, eftersom det handlar om allt från små till stora aktörer av mycket varierande art. FPA beskriver de allmänna modellerna för anslutning till Kanta-tjänsterna, men reglerar inte i detalj hur organisationens anslutning genomförs tekniskt.

I denna anvisning presenteras olika anslutningsmodeller till Kanta-tjänsterna. Det beskrivs allmänt hur tele- och meddelandetrafikförbindelserna mellan organisationens informationssystem och Kanta-tjänsterna kan genomföras. Vid anslutningen ska det göras skillnad mellan följande roller, som kan innehas av samma eller olika aktörer: den organisation som använder tjänsten, den organisation som ansluter sig till Kanta samt Kanta-anslutningspunktens ägare.

Figur 1 Överblick över anslutningen till Kanta

1.1 Till vilka system ansluter man sig?

Denna anslutningsanvisning gäller kundsystem som ansluter sig till något av Kanta-tjänsternas följande system:

1. Receptcentret
2. Patientdataarkivet
3. Klientdataarkivet för socialvården
4. Datalagret för egna uppgifter
5. Arkivet för bildmaterial

Den anslutningsanvisning gäller inte den nationella kodtjänsten och inte heller valideringstjänsten, eftersom man inte behöver ansluta sig separat till dem.

Valet av anslutningsmodeller berörs av följande begränsning: Vid införande av klientdataarkivet för socialvården kan modellen för gemensam anslutning tills vidare inte tillämpas.

Anvisningen tillämpas inte på organisationer utanför social- och hälsovården som utnyttjar Förfrågnings- och förmedlingstjänsten. Anslutning till Förfrågnings- och förmedlingstjänsten sker via den Nationella informationsleden.

1.2 Självständig anslutning

(den organisation som använder tjänsten = den organisation som ansluter sig till Kanta = anslutningspunktens ägare)

1. anslutning via en egen integrationslösning (meddelandeförmedlingslösning)
2. direkt anslutning från ett informationssystem i den egna maskinsalen
3. en liten organisations anslutning via internet

1.3 Anslutning via en externaliserad anslutningspunkt

(den organisation som ansluter sig till Kanta ≠ anslutningspunkten ägare)

1. anslutning via en externaliserad anslutningspunkt
2. externaliserat informationssystem (t.ex. externaliserad maskinsal, Software as a Service-tjänst, molntjänster, webbanvändargränssnitt för yrkesutbildade personer inom hälso- och sjukvården)
3. externaliserad integrationslösning (meddelandeförmedlingslösning)
4. externaliserad datakommunikation (samlingspunkt för datakommunikationen)

1.4 Anslutning med förbindelse som avgetts av en annan organisation

(den organisation som använder tjänster ≠ den organisation som ansluter sig till Kanta)

1. privata hälso- och sjukvårdsenheter ansluter sig som hyresgäster med en förbindelse som avgetts av en annan hälso- och sjukvårdsenhet

2. permanent adressbokskoppling till Patientdataarkivet när underleverantörer anlitas utan fullmakt för köpta tjänster, dvs. den organisation som arkiverar patientuppgifter ansluter sig i den personuppgiftsansvariges namn

Anslutningsmodellen styr organisationen när den skaffar certifikat och teleförbindelser. Varje modell är förenad med rekommendationer och krav på de tele- och meddelandetrafikförbindelser som ska skaffas.

Anslutningsmodellerna är förenklade. De beskriver Kanta-anslutningen ur olika synvinklar. Modellerna utesluter inte varandra, och en organisation kan också genomföra Kanta-anslutningen som en kombination av flera modeller.

Mångfalden av Kanta-anslutningar beror på organisationernas befintliga miljöer och förbindelser samt de olika externaliseringslösningar som de använder. I princip har en organisation kunnat externalisera vilken del som helst av sin Kanta-anslutning så att den genomförts av en tredje part, en s.k. förmedlare, (se 2.4).

2 Grundläggande begrepp

2.1 Aktörer som ansluter sig till Kanta-tjänsterna

Bestämmelser om användningen av Kanta-tjänsterna ingår i lagarna om elektroniska recept (61/2007, jämte ändringar) och om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007, jämte ändringar) och i de förordningar som hänför sig till dem.

De aktörer som ska ansluta sig till Kanta-tjänsterna samt författningsbakgrunden till anslutningen definieras närmare i anvisningarna om aktörer som ansluter sig till Kanta-tjänsterna.

Alla organisationer som ansluter sig till Kanta-tjänsterna och de enheter och filialapotek som tar i bruk Kanta-tjänsterna tillsammans med dem ska vara registrerade i den riksomfattande kodtjänst som upprätthålls av Institutet för hälsa och välfärd (THL), i antingen

- apoteksregistret (Fimea – apoteksregister) eller
- registret över hälso- och sjukvårdsorganisationer (THL – SOTE-organisationsregister) eller
- registret över självständiga yrkesutövare inom hälso- och sjukvården (Valvira – Självständiga yrkesutövare inom hälso- och sjukvården).

Härigenom blir deras ISO OID-koder och andra registrerade uppgifter tillgängliga för Kanta-tjänsterna.

2.2 Mottagningstjänster

Med mottagningstjänster avses Web Service-tjänster som organisationens system tillhandahåller för Kanta-tjänsterna. En sådan tjänst är mottagning av begäran om förnyelse av elektroniska recept med PUSH-modellen.

Vid mottagningstjänster är Kanta-tjänsterna den anropande parten medan organisationen tillhandahåller tjänsten. Det är inte nödvändigt att tillhandahålla en mottagningstjänst för förnyelsebegäran, om kundens informationssystem använder PULL-modellen i stället för PUSH-modellen. PULL-modellen rekommenderas alltid när det är tekniskt möjligt.

Mottagningstjänster ska finnas i https-port 443.

2.3 Kanta-anslutningspunkt

Med Kanta-anslutningspunkt avses den punkt i datakommunikationen där organisationens informationssystem ansluts till Kanta-tjänsterna längs en teleförbindelse som är krypterad och autentiserad med ett servercertifikat från hälso- och sjukvårdens certifikatutfärdare. BRC:s servercertifikat finns installerat i Kanta-anslutningspunkten.

Varje organisation som ansluter sig till Kanta-tjänsterna använder minst en Kanta-anslutningspunkt. Den kan ha upprättats av organisationen själv eller en annan organisation. Det kan finnas flera anslutningspunkter (och servercertifikat), t.ex. om

- organisationens enheter ansluter sig direkt till Kanta-tjänsterna från olika informationssystem utan centraliserad integrationslösning (meddelandeförmedlingslösning).
- organisationens mottagningstjänster (t.ex. mottagning av förnyelsebegäran) finns på en annan server än den där systemen anropar Kanta-tjänsterna.

Kanta-anslutningspunkten ges en OID-kod som identifierar den. Koden används också för att identifiera det servercertifikat som installeras i anslutningspunkten (servercertifikatets Subject-dels serialNumber-fält). Koden bildas i nod 13 under OID-koden för den organisation eller organisationsenhet som svarar för upprättandet av anslutningspunkten som följer:

- OID-koden för en anslutningspunkt hos en tillhandahållare av social- och hälsovård som är registrerad i SOTE-organisationsregistret har antingen formen 1.2.246.10.xxx.10.y.13.n eller 1.2.246.537.10. xxx.10.y.13.n (där xxx är organisationens kod enligt SOTE-organisationsregistret, y är en siffra som identifierar enheten och n är en siffra som identifierar anslutningspunkten).
- OID-koden för en självständig yrkesutövare som är registrerad i Valviras register över självständiga yrkesutövare inom hälso- och sjukvården är 1.2.246.537.28.xxx.13.n (där xxx är yrkesutövarens kod enligt Valviras register över självständiga yrkesutövare inom hälso- och sjukvården och n är en siffra som identifierar anslutningspunkten).

- OID-koden för ett apoteks anslutningspunkt har formen 1.2.246.553.1.xxx.13.n (där xxx är apotekets kod enligt Fimeas Apoteksregister och n är en siffra som identifierar anslutningspunkten).

Det rekommenderas att olika servercertifikat används på olika servrar. Om det ändå är nödvändigt att använda samma servercertifikat på flera olika servrar (exempelvis på grund av de begränsningar som följer av klusteranvändning), är det fråga om samma Kanta-anslutningspunkt. Så är fallet fast alla klustermedlemmarna skulle synas utåt med egna datakommunikationsadresser (IP-adress), m.a.o. det finns ingen gemensam virtuell adress till klustret.

Det rekommenderas att för en anslutningspunkt definieras en datakommunikationsadress (IP-adress eller DNS-namn från den offentliga namntjänsten, se punkt 4.3 Datakommunikationsadresser). Flera adresser kan dock definieras för en anslutningspunkt, om det är nödvändigt till exempel för att ordna en reservförbindelse. Även då är en av adresserna primär datakommunikationsadress. En anslutningspunkt som tillhandahåller mottagningstjänster kan inte heller ha flera än en datakommunikationsadress.

2.4 Kanta-förmedlare

Kanta-förmedlare och producenter av Kanta-förmedlingsservice samt deras roller och ansvar beskrivs i anvisningen Certifiering av Kanta-förmedlingsserive samt Kanta-förmedlare (THL:s anvisning 3/2015).

Med förmedlare avses en serviceproducent som en organisation som ansluter sig till Kanta-tjänsterna anlitar för att upprätta Kanta-anslutningspunkten, och som i denna roll har möjlighet att läsa icke-krypterade klientuppgifter inom social- och hälsovården, t.ex. i samband med underhållsåtgärder. En TLS-krypterad förbindelse som upprättas med certifikat från hälso- och sjukvårdens certifikatutfärdare upprättas i allmänhet mellan anslutningspunkten och Kanta-tjänsterna. Som förmedlare definieras inte en organisation som enbart routar TLS-krypterad datakommunikation och inte kan läsa icke-krypterade patientuppgifter.

Certifikatet från hälso- och sjukvårdens certifikatutfärdare (BRC) kan vara antingen i anslutarens eller förmedlarens namn. Om förmedlaren upprättar den gemensamma anslutningspunkten och tillhandahåller tjänster som kopplas till den för flera som ansluter sig till Kanta skaffas servercertifikatet i förmedlarens namn.

Förmedlaren kan skaffa en del av tjänsterna i anslutningspunkten även från underleverantörer. Den förmedlare som administrerar anslutningspunkten, dvs. i vars namn servercertifikatet är, ska stå i avtalsförhållande till hälso- och sjukvårdsorganisationen eller apoteket.

OID-koden för en anslutningspunkt som upprättas av en förmedlare bildas i nod 13 under förmedlarens OID-kod enligt förmedlarregistret, varvid anslutningspunktens OID har formen 1.2.246.537.6.918.18.xxx.13 (där xxx är organisationens kod enligt förmedlarregistret och n den siffra som identifierar anslutningspunkten).

2.5 Servercertifikat

Ett servercertifikat behövs för att en krypterad TLS-förbindelse ska kunna upprättas mellan Kanta-tjänsterna och Kanta-anslutningspunkten samt för att Kanta-anslutningspunkten ska kunna identifieras. För varje Kanta-anslutningspunkt ska ett eget servercertifikat skaffas från BRC.

Servercertifikatet och Kanta-anslutningspunkten kopplas till varandra via servercertifikatets Subject-dels serialNumber-fält. Dess värde blir värdet av Kanta-anslutningspunktens OID-kod. Värdet i servercertifikatets Subject-dels common-Name-fält blir datakommunikationsadressen till anslutningspunktens primära teleförbindelse (se punkt 2.3 Kanta-anslutningspunkt).

Servercertifikatet kan också användas för att kryptera trafik mellan organisationen och en externaliserad Kanta-anslutningspunkt och för att identifiera parterna i trafiken.

2.6 Systemsigneringscertifikat

För att använda Patientdataarkivets eller Klientdataarkivet för socialvårdens tjänster behövs ett systemcertifieringscertifikat som beviljats av hälso- och sjukvårdens certifikatutfärdare. Med den privata nyckel som hänför sig till det signeras alla handlingar som skickas till Kanta, och som inte har signerats med en yrkesutbildad persons certifikat.

Systemsigneringscertifikatet är organisations- och systemspecifikt[1]. Detta betyder att t.ex. en serviceproducent som ansluter sig till Patientdataarkivet eller Klientdataarkivet för socialvården behöver endast ett systemsigneringscertifikat. Om organisationen har flera patient- eller klientdatasystem kan den använda samma systemsigneringscertifikat i alla.

2.7 Kanta-adressindex

I sitt adressindex upprätthåller FPA uppgifter om anslutningspunkterna för dem som ansluter sig till Kanta. Organisationen lämnar uppgifter om egna eller externa Kanta-anslutningspunkter som den använder i ansökan om anslutning till Kanta-tjänsterna.

Adressindexet fungerar som adressbok och är en del av Kanta-tjänsternas behörighetskontroll. Där lagras datakommunikationsadresserna till organisationens mottagningstjänster och de Kanta-tjänster som organisationen har tillgång till. I fråga om varje Kanta-anslutningspunkt lagras följande uppgifter:

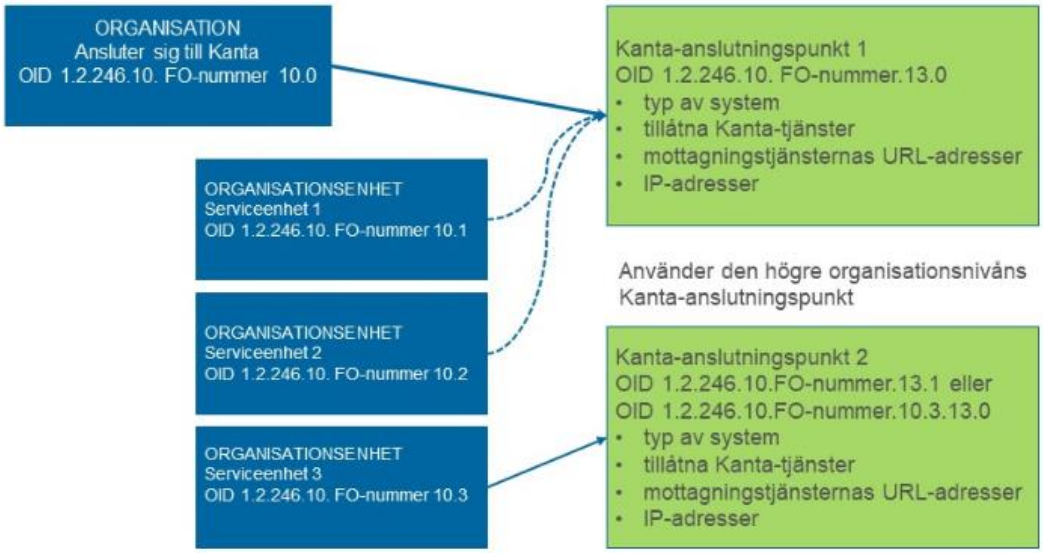
- OID-kod för den organisation eller organisationsenhet som använder anslutningspunkten

[1] Undantaget är gemensamma systemsigneringscertifikat enligt separata föreskrifter (patientdatasystemets användningsfall): Med systemsigneringscertifikat signeras handlingar som arkiveras i Kanta, och som användaren inte personligen behöver signera elektroniskt. I princip är systemcertifikatet organisationsspecifikt, dvs. varje serviceproducent skaffar ett eget systemcertifikat. På läkarstationer kan dock ett gemensamt systemsigneringscertifikat användas. Saken bör överenskommas i ett avtal mellan läkarstationen och de aktörer som verkar i dess lokaler. Även då patientdatasystemet har skaffats som en tjänst, dvs. systemleve-rantören svarar för det tekniska underhållet av systemet, kan man använda ett certifikat. Varje organisation som använder tjänsten befullmäktigar systemleverantören att skaffa certifikatet på dess vägnar. Fullmakten skrivs in i avtalet mellan leverantören och organisationen.

- anslutningspunktens OID-kod (nod 13)
- typ av system (t.ex. patientdatasystem, klientdatasystem eller apotekssystem)
- tillåtna Kanta-tjänster (FPA definierar på grund av ansökan)
- mottagningstjänsternas URL-adresser
- datakommunikationsadresser (IP-adresser).

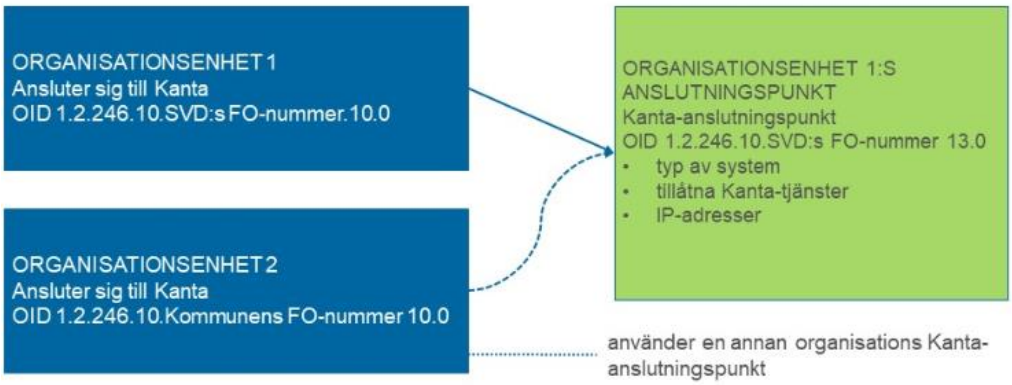
I adressindexet upprätthålls information om vilken organisationsenhet som använder vilken anslutningspunkt. En organisationsenhet för vilken ingen egen anslutningspunkt har definierats, ärver anslutningspunkten från en organisationsenhet på högre nivå, dvs. har anslutit sig till Kanta-tjänsterna via den.

I figur 2 har en enhet inom organisationen anslutit sig till Kanta-tjänsterna via en egen anslutningspunkt och de andra enheterna via en anslutningspunkt som definierats på högre nivå inom organisationen.



Figur 2 Organisationen har två egna Kanta-anslutningspunkter

Bland uppgifterna om organisationen lagras uppgifter om den Kanta-anslutningspunkt som den använder även då anslutningspunkten innehas av en annan organisation. I figur 3 har organisationsenhet 2 anslutit sig till Kanta-tjänsterna via den Kanta-anslutningspunkt som administreras av organisationsenhet 1.



Figur 3 Organisationen använder en extrem Kanta-anslutningspunkt

2.8 Samlingspunkt för datakommunikationen

Med datakommunikationens samlingspunkt avses en tjänst där TCP/IP-kommunikationen från olika organisationer till Kanta-tjänsterna samlas och routas till Kanta-tjänsterna längs en gemensam teleförbindelse och där på motsvarande sätt trafiken från Kanta-tjänsterna routas till olika organisationer utifrån mottagarens IP-adress. Routningen av datakommunikationen påverkar inte TLS-krypteringen av förbindelserna: krypteringen varken bryts eller bildas i samlingspunkten och inga icke-krypterade recept- eller patientuppgifter syns.

I datakommunikationens samlingspunkt kan adressen vid behov konverteras så att all trafik via samlingspunkten ser ut att komma från samma adress. I dessa fall finns Kanta-anslutningspunktens servercertifikat och datakommunikationsadress inom olika organisationer, servercertifikatet inom den organisation som ansluter sig eller hos förmedlaren och datakommunikationsadressen inom den organisation som administrerar samlingspunkten.

3 Val och testning av anslutningsmodell

Valet av anslutningsmodell förutsätter att organisationen definierar sin organisationsenhetshierarki (kravet gäller inte privata organisationer, vilkas organisationshierarkier finns lagrade i Valveri-/Soteri-registret), utreder vilka informationssystem som ska kopplas till Kanta-tjänsterna samt de anslutningspunkter och teleförbindelser som de använder. Vid definitionen rekommenderas att man går uppifrån neråt, från organisationsnivå till datakommunikationslösningar:

1. definition av hierarkin mellan organisationens OID-koder och organisationsenheterna

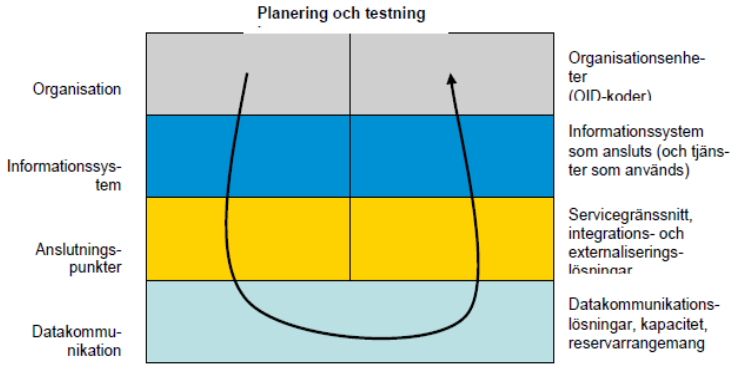
2. definition/beskrivning av de informationssystem som ska kopplas till Kanta-tjänsterna

3. definition av de tjänster, integrations- (meddelandeförmedlings-) och externaliseringslösningar som tillhandahålls för Kanta-tjänsterna

4. definition av datakommunikationslösningarna (bl.a. kapacitet, reservförbindelser).

Vid testningen efter att anslutningen upprättats går man i motsatt riktning, från datakommunikationsnivå till organisationsnivå. Testfaserna är

1. testning av TCP/IP-förbindelsen
2. testning av TLS-förbindelsen (servercertifikat, i bägge riktningarna för mottagningstjänster)
3. testning av meddelandeförmedlingen (även mottagningstjänstemeddelanden)
4. testning av OID-kodernas korrekthet i meddelanden (programnivå).



Figur 4. Planering och testning av anslutningsmodellen.

4 Teleförbindelse

Den organisation som ansluter sig svarar för de datakommunikationer den skaffar från datakommunikationsoperatören och definierar egenskaperna hos de förbindelser den använder i överensstämmelse med de egna kapacitets-, kvalitets- och servicenivåkraven. FPA svarar för den interna datakommunikationen fram till datakommunikationsoperatörens gränssnitt.

I första hand ska man använda förbindelse via ett privat nät för att garantera tjänstens tillgänglighet och kvalitet. Öppen internetförbindelse får användas endast i motiverade undantagsfall. När det gäller undantagsfall bör man lägga märke till att den organisation som tillhandahåller mottagningstjänster måste öppna en port från det externa nätet till sitt interna nät i brandväggen, vilket utsätter organisationen för bl.a. överbelastningsattacker och andra informationssäkerhetshot.

I detta avsnitt presenteras på ett allmänt plan de centrala kraven och rekommendationerna för teleförbindelsen. Närmare anvisningar som stöder definitionen och anskaffningen av teleförbindelser finns i avsnitt 6.

4.1 Förbindelse via privat nät

För ett privat näts anslutning garanterar datakommunikationsoperatören en viss kapacitet hela vägen. Ett privat näts anslutning (MPLS eller motsvarande) beställs från en datakommunikationsoperatör mellan en organisation, flera organisationers gemensamma Kanta-anslutningspunkt eller datakommunikationsnod och Kanta-tjänsterna. Inom organisationen måste man förbereda sig på att det kan ta flera veckor att upprätta förbindelsen. Förbindelsen måste vara klar när organisation gör ansökan om anslutning till Kanta-tjänsterna.

Förbindelser via ett privat nät kan skyddas bättre mot hoten mot öppna internet, bl.a. överbelastningsattacker.

4.2 Öppen internetförbindelse i undantagsfall

Man kan ansluta sig till Kanta-tjänsterna via ett öppet internet endast i motiverade undantagsfall. Alternativet är avsett för organisationer som inte har möjlighet att ansluta sig till ett privat nät. En organisation som använder en öppen internetförbindelse kan inte garanteras att tjänstens tillgänglighet och kvalitet är av samma standard som med ett privat nät. En öppen internetförbindelse är inte tillåten som förbindelse till Arkivet över bildmaterial.

4.3 Datakommunikationsadresser

De IP-adresser som definierats för Kanta-anslutningspunkten ska vara fasta och offentliga. För att underlätta underhållet och minimera felmöjligheterna är det bättre att använda DNS-namn än IP-adresser i certifikaten.

4.4 Informationssäkerhet

Kanta-anslutningslösningen ska uppfylla informationssäkerhetskraven på datakommunikation och meddelandetrafik (se dokumentet Kanta-palvelut: tieto- ja sanomaliikenteen tietoturvavaatimukset) samt informationssäkerhetskraven på system som hör till klass A och på systemens användningsmiljö. Till dessa hör bland annat tillståndsstyrd brandvägg och virusbekämpning.

4.5 Reservförbindelse

Det rekommenderas att teleförbindelsen mellan organisationen och Kanta-tjänsterna dubbelriktas. Den som beställer anslutningen bör säkerställa med sin datakommunikationsoperatör att den primära förbindelsen och reservförbindelsen faktiskt går skilda rutter hela vägen. Det kan vara omöjligt att säkerställa detta om anslutningarna köps från olika operatörer, eftersom operatörerna i allmänhet inte avslöjar de fysiska förbindelserna för sina anslutningar. Om det inte är möjligt att genomföra en helt dubbelriktad förbindelse, rekommenderas att man dubbelriktar förbindelsen så långt som det är ekonomiskt förnuftigt.

När man dubbelriktar förbindelser bör man också komma ihåg att organisationens mottagningstjänster (t.ex. mottagning av förnyelsebegäran) bör ha unika adresser. Dubbelriktningen av förbindelser bör alltså genomföras så att reservförbindelsens och den primära förbindelsens datakommunikationsadresser är desamma i de anslutningspunkter där mottagningstjänsterna finns.

4.6 Symmetrisk förbindelse

Med tanke på snabbheten rekommenderas att man använder en symmetrisk teleförbindelse. Detta betyder att överföringskapaciteten är lika stor i vardera riktningen.

4.7 Anslutningens dataöverföringskapacitet

Den som ansluter sig till Kanta ansvarar för att anslutningens överföringskapacitetsbehov definieras. När kapacitetsbehovet uppskattas ska man beakta trafikmängden och verksamhetens kritiskhet. Närmare anvisningar om uppskattning av dataöverföringskapaciteten finns i avsnitt 6.

Organisationerna ska också försäkra sig om att anslutningen är skalbar, eftersom trafiken ökar i samband med att arkivtjänsterna tas i bruk.

5 Anslutningsmodeller

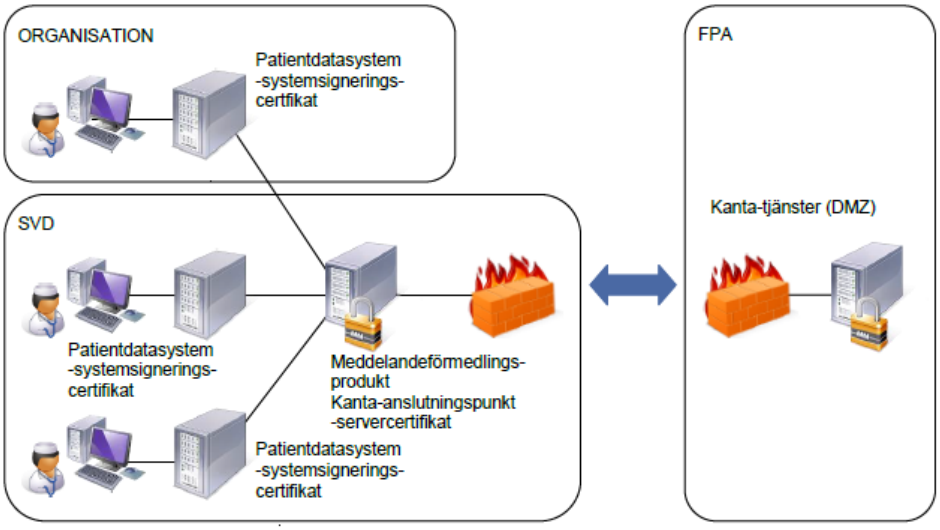
De anslutningsmodeller som presenteras här utesluter inte varandra och organisationens Kanta-anslutning kan vara en kombination av olika modeller.

5.1 Anslutning via egen integrationslösning

I denna modell har den som ansluter sig till Kanta eller Kanta-förmedlaren en integrationslösning (meddelandeförmedlingslösning), via vilken flera system, organisationsenheter eller organisationer ansluter sig till Kanta-tjänsterna. Integrationslösningens uppgift är att routa meddelandena till programservrar, som kan finnas i olika organisationsenheter eller organisationer.

Det servercertifikat som hälso- och sjukvårdens certifikatutfärdare (BRC) beviljar installeras i samband med integrationslösningen. Med hjälp av detta servercertifikat upprättas en autentiserad och krypterad förbindelse till Kanta-tjänsterna. Ett servercertifikat kan behövas även mellan integrationslösningen och de anslutande informationssystemen för att säkerställa parternas identitet och kryptera dataöverföringen.

En integrationslösning gör det möjligt att ansluta flera system, organisationsenheter eller organisationer till Kanta längs samma teleförbindelse. Exemplet är en regional IT-serviceproducent, som har eller som administrerar flera system och tillhandahåller organisationerna i området förmedlingsservice till Kanta-tjänsterna (figur 5).



Figur 5. Organisationen har flera informationssystem, och den tillhandahåller en annan organisation en anslutningspunkt till Kanta-tjänsterna.

Modellen lämpar sig för en organisation,

- som har flera informationssystem som ska anslutas till Kanta
- via vilken även andra organisationer ansluter sig till Kanta.

Krav på anslutningen:

- förbindelse via ett privat nät, t.ex. MPLS
- fasta och offentliga datakommunikationsadresser
- tillståndsstyrd brandvägg och annan informationssäkerhet
- servercertifikat i samband med integrationslösningen eller i en separat aktiv enhet
- systemsigneringscertifikat i samband med klient- eller patientdatasystemet (vid anslutning till ett arkiv)
- parternas identitet säkerställs mellan integrationslösningen och informationssystemen, t.ex. med servercertifikat från hälso- och sjukvårdens certifikatutfärdare
- TLS-krypterad skyddad förbindelse mellan organisationerna, t.ex. med servercertifikat från hälso- och sjukvårdens certifikatutfärdare (BRC).

Rekommendationer för anslutningen:

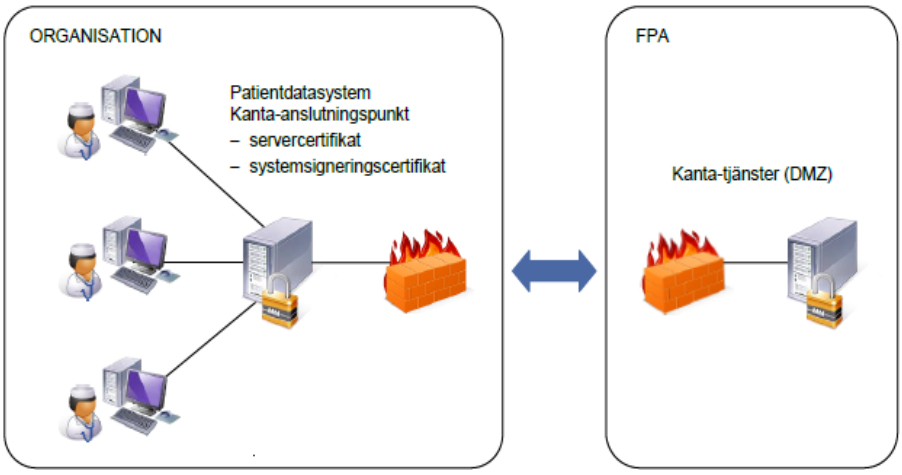
- dubbelriktad, snabb symmetrisk anslutning
- kvalitetskrav på teknik och underhåll som överensstämmer med kapacitetsbehovet och verksamhetens kritiskhet.

5.2 Direkt anslutning från ett eget informationssystem

I denna modell innehar organisationen det system som ansluts till Kanta och Kanta-anslutningspunkten. Servercertifikatet installeras direkt på programservern eller i en separat aktiv enhet i anslutning till informationssystemet.

En organisation kan ha flera Kanta-anslutningspunkter, om den har flera informationssystem som ska anslutas och det inte är möjligt att upprätta en gemensam anslutningspunkt för dem eller om organisationen tar emot begäran om förnyelse av elektroniska recept eller använder Valviras roll- och attributtjänst på en annan adress än där den anropar Kanta-tjänsterna.

Exemplet är en organisation som ansluter sig till Kanta-tjänsterna direkt från ett informationssystem som den innehar (figur 6).



Figur 6. En organisation som anslutit sig till Kanta direkt från ett informationssystem som den innehar.

Modellen lämpar sig för en organisation som har ett eget informationssystem.

Krav på anslutningen:

- förbindelse via ett privat nät, t.ex. MPLS
- fasta och offentliga datakommunikationsadresser
- tillståndsstyrd brandvägg och annan informationssäkerhet

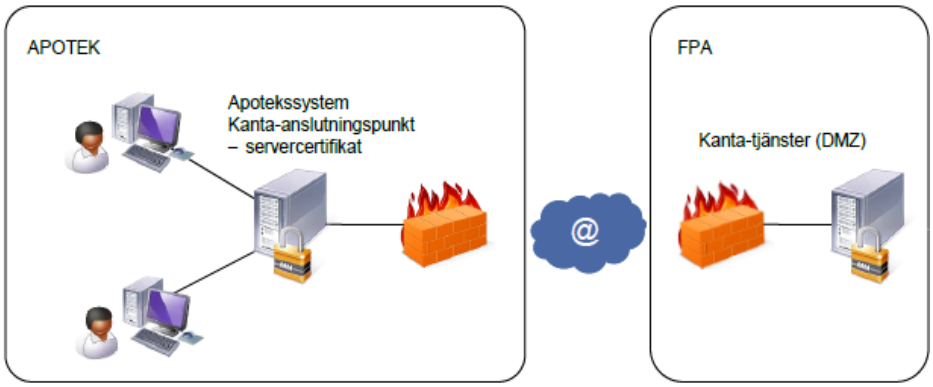
- servercertifikat/anslutningspunkt
- systemsigneringscertifikat i samband med klient- eller patientdatasystemet (vid anslutning till ett arkiv).

Rekommendationer för anslutningen:

- dubbelriktad, snabb symmetrisk anslutning
- valitetskrav på teknik och underhåll som överensstämmer med kapacitetsbehovet och verksamhetens kritiskhet.

5.3 En liten organisations anslutning via internet

I denna modell ansluter sig organisationen till Kanta-tjänsterna via ett öppet internet. Servercertifikatet installeras antingen direkt på programservern eller i nätets DMZ-zon (demilitariserade zon). Exemplet är en liten organisation, t.ex.ett apotek (figur 7).



Figur 7. En liten organisation som anslutit sig till Kanta-tjänsterna via internet

Krav på anslutningen:

- fasta och offentliga datakommunikationsadresser
- tillståndsstyrd brandvägg och annan informationssäkerhet
- servercertifikat/anslutningspunkt
- systemsigneringscertifikat i samband med informationssystemet.

Rekommendationer för anslutningen:

- dubbelriktad, snabb symmetrisk anslutning
- SLA-nivå enligt verksamhetens kritiskhet.

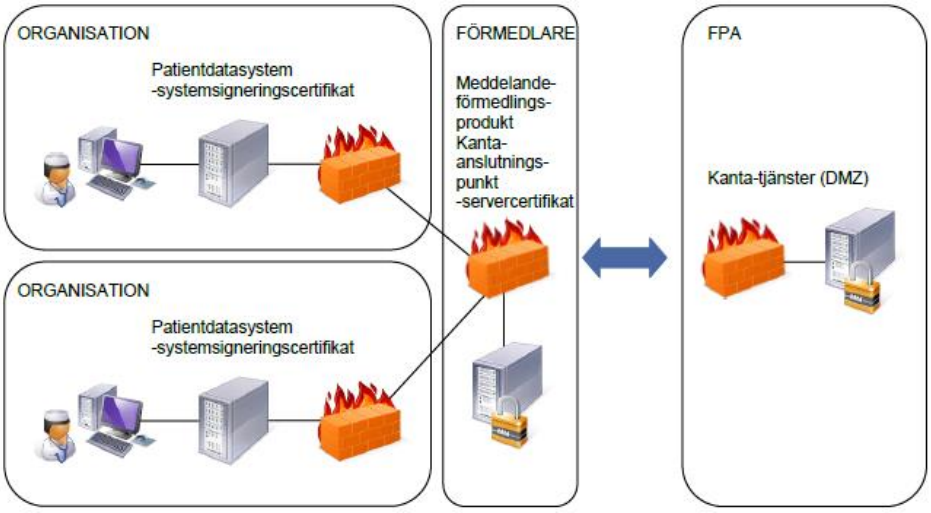
5.4 Anslutning via en externaliserad anslutningspunkt

I denna modell har organisationen anslutit sig till Kanta-tjänsterna via en Kanta-anslutningspunkt som upprättats av förmedlaren. Organisationen har till förmedlaren kunnat externalisera

- informationssystemet (t.ex. ett delat informationssystem som SaaS-tjänst)
- meddelandeförmedlingen och/eller
- datakommunikationen.

Servercertifikatet är i allmänhet i förmedlarens namn, och det installeras i samband med anslutningspunkten.

Exemplen på externalisering av informationssystemet eller meddelandeförmedlingen är en organisationsenhet som anslutit sig till Kanta-tjänsterna via en regional IT-serviceproducent (figur 8).



Figur 8. Två organisationer som anslutit sig till Kanta-tjänsterna via en regional IT-serviceproducent.

Krav på anslutningen:

- TLS-kryptering mellan den organisation som ansluter sig och förmedlarorganisationen, med servercertifikat från hälso- och sjukvårdens certifikatutfärdare (BRC)
- säkerställande av parternas identitet mellan integrationslösningen (meddelandeförmedlingslösningen) och informationssystemen, med servercertifikat från hälso- och sjukvårdens certifikatutfärdare (BRC)

- förbindelse via privat nät, t.ex. MPLS, mellan förmedlarorganisationen och Kanta-tjänsterna
- servercertifikatet är i förmedlarorganisationens namn
- systemsigneringscertifikat i samband med informationssystemet hos antingen den som ansluter sig eller förmedlarorganisationen, dock i den anslutande organisationens namn eller avtalsbaserat med fullmakt för förmedlaren.

Rekommendationer för anslutningen:

- dubbelriktad, snabb symmetrisk anslutning
- kvalitetskrav på teknik och underhåll som överensstämmer med kapacitetsbehovet och verksamhetens kritiskhet.

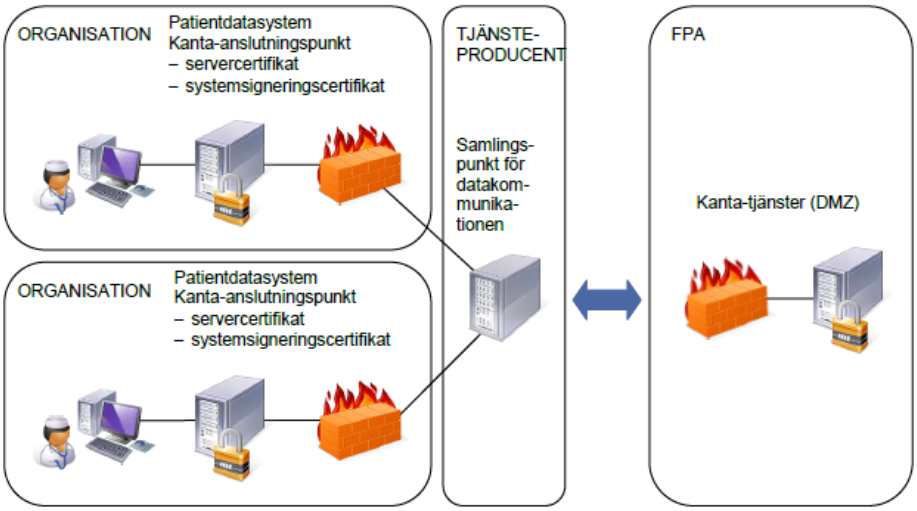
Externaliserad datakommunikation

Med datakommunikationens samlingspunkt avses en tjänst där datakommunikationen från olika organisationer till Kanta-tjänsterna samlas och styrs till Kanta-tjänsterna längs en gemensam teleförbindelse och där trafiken från Kanta-tjänsterna på motsvarande sätt routas till de olika organisationerna. Routningen av datakommunikationen påverkar inte förbindelsernas TLS-kryptering: krypteringen varken bryts eller bildas i samlingspunkten, och inga icke-krypterade uppgifter syns. Som Kanta-förmedlare definieras inte en organisation som enbart routar eller fungerar som samlingspunkt för TLS-krypterad datakommunikation och som inte kan läsa icke-krypterade uppgifter.

Samlingspunkten inverkar på anslutningen till Kanta-tjänsterna endast om anslutningspunktens datakommunikationsadress bestäms i samlingspunkten. Förmedlaren eller den anslutande organisationen ska då uppge samlingspunktens adress i ansökan om servercertifikat.

Krav på samlingspunkten:

- Mottagningstjänsternas (t.ex. mottagning av förnyelsebegäran) adresser ska vara unika också när trafiken går via samlingspunkten.
- Servercertifikatet finns hos den organisation som ansluter sig eller förmedlaren.



Figur 9. Organisationer som anslutit sig till Kanta-tjänsterna via en extern samlingspunkt.

5.5 Modell med gemensam anslutning för privat hälso- och sjukvård

I denna modell med gemensam anslutning ansluter sig en privat serviceproducent (den som ansluter sig via någon annan/hyresgästen) till Kanta-tjänsterna tillsammans med den egentliga anslutaren (huvudsanslutaren). Huvudanslutaren ordnar meddelandetrafiken och datakommunikationen så att denne tillhandahåller den hyresgäst som använder tjänsterna nödvändiga informationssystemtjänster. Ett avtal enligt Kanta-avtalsmodellen ska ha upprättats mellan huvudanslutaren och dem som ansluter sig via denne.

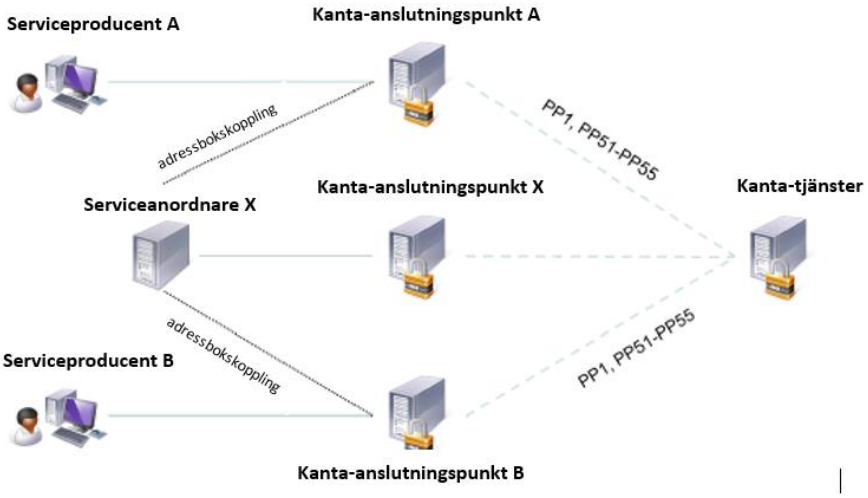
Särdragen hos den meddelandetrafiklösning som hänför sig till modellen med gemensam anslutning har beskrivits i de separata specifikationerna för såväl Recepttjänsten som Patientdataarkivet. I dessa situationer är det viktigt att även uppgifter om hyresgästen förmedlas till Kanta-tjänsternas loggar.

5.6 Patientdataarkivets permanenta adressbokskoppling när en underleverantör anlitas

Patientdataarkivets permanenta adressbokskoppling när en underleverantör anlitas är planerad för sådana situationer där till exempel en organisation som producerar diagnostiska undersökningar i ett område producerar handlingar som går direkt till Patientdataarkivet. Eftersom arrangemanget med köpta tjänster i dessa fall är mycket statisk eller rent av permanent, erbjuder Kanta-tjänsten möjlighet att arkivera handlingarna (servicebegäran PP1) och använda vissa andra begränsade typer av servicebegäran (lätta gränssnitt; PP51-PP53, PP55) i tjänsteanordnarens namn utan fullmakt för köpta tjänster. Andra typer av servicebegäran får användas endast med fullmakt för köpta tjänster.

Eftersom modellen innebär att serviceproducenten agerar i serviceanordnarens namn mot Kanta-tjänsterna, krävs för att säkerställa tillräckliga logguppgifter att till serviceanordnaren kopplas en dedikerad anslutningspunkt för varje aktör

som använder Kanta-tjänsterna via det permanent arrangemanget med köpta tjänster. Denna anslutningspunkt identifierar den serviceproducent som använder Kanta-tjänsterna i serviceanordnarens namn.



Figur 10. Permanent adressbokskoppling

6 Dimensionering, kvalitetskrav och rekommendationer för teleförbindelserna

I följande förteckning uppräknas exempel på minimikraven på behövlig kapacitet

- Litet apotek 10 Mbit/s
- Stort apotek 30 Mbit/s
- En organisation som arkiverar färre än 10 000 handlingar per dag 30 Mbit/s
- En organisation som arkiverar över 100 000 handlingar per dag 500 Mbit/s
- En organisation som använder arkivet för bildmaterial, minst 300 Mbit/s

De erforderliga servicenivåattributen och tekniska kvalitetsklassificeringarna baserar sig på de allmänt godkända gränsvärdena på området. Vid dimensioneringen av datakommunikationen bör de specifikationer som beskrivs i dokumentet ”Liite 1, palvelutasoluokat” i JHS rekommendation 174 iakttas.

JHS-rekommendation 174 finns i sin helhet på internet, adress: http://www.jhs-suositukset.fi/web/guest/jhs/recommendations/174.