Tekniska anslutningsmodeller till Kanta-tjänsterna

Anvisning

Kanta-tjänsterna

11.9.2024

Kela
Kanta-palvelut
PL 450, 00056 Kela

FPA
Kanta-tjänsterna
PB 450, 00056 FPA

Kanta 381r 09 24
www.kanta.fi
kanta@kanta.fi

Ändringshistorik

Version	Ändring	Gjord 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 tagits bort 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 FPA	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	Kanta-tjänsterna FPA	9.12.2019

Version	Ändring	Gjord av	Datum
	om att det behövs ett separat systemsigneringscertifikat vid användningen av Klientdataarkivet för socialvården har strukits.		
3.8	Dokumentet har överförts till en ny mall som uppfyller tillgänglighetskraven. Hänvisningarna till Befolkningsregistercentralen (BRC) har ändrats till Myndigheten för digitalisering och befolkningsdata (MDB).	Kanta-tjänsterna FPA	1.4.2020
3.9	En modell med gemensam anslutning för den privata socialvården har fogats till kapitel 5.5. Till kapitel 2.3 har det fogats en riktlinje att en Kanta-anslutningspunkt ska vara belägen i Finland. Samma omnämnande finns även i början av kapitel 5.	Kanta-tjänsterna FPA	16.2.2021
3.10	I kapitel 1.1 Till vilka system ansluter man sig? har begränsningen av anslutningsmodellen gällande Klientdataarkivet för socialvården strukits.	Kanta-tjänsterna FPA	2.6.2021
3.11	I kapitlen 1.4 och 5.6 har det tillfogats ett omnämnande om att en permanent adressbokskoppling inte längre får användas i anslutningslösningar när nya underleverantörer anlitas, gamla tidigare överenskomna permanenta adressbokskopplingar när underleverantörer anlitas stöds fortfarande. Dessutom har socialvårdsenheterna tagits med i kapitel 1.4. Till kapitel 2.3 har det fogats text om den anslutningspunkt sjukhusapoteken använder.	Kanta-tjänsterna FPA	15.12.2021
3.12	Beskrivningen i kapitel 2.6 om hur det gemensamma systemsigneringscertifikatet används har uppdaterats.	Kanta-tjänsterna FPA	4.10.2022
3.13	Anvisningens struktur, termer och figurer har uppdaterats. Kanta-förmedlarens roll har preciserats och en beskrivning av administrativ anslutning har lagts till. Kraven i anslutning till teleförbindelser har preciserats. Länkarna och hänvisningarna till andra anvisningar och dokument har uppdaterats.	Kanta-tjänsterna FPA	13.6.2023
3.14	Beskrivningen av modellen med gemensam anslutning har preciserats. Modellen med gemensam anslutning är avsedd för privata tjänstetillhandahållare av Kanta-tjänster. I anvisningen har självständiga yrkesutövare ändrats till privata tjänsteproducenter i enlighet med lagen om tillsynen över social- och hälsovården. Kraven på teleförbindelser och certifikat har preciserats.	Kanta-tjänsterna FPA	2.1.2024

Version	Ändring	Gjord av	Datum
3.15	Hänvisningarna till THL:s föreskrifter har uppdaterats. Kraven på teleförbindelserna har preciserats i fråga om användningen av öppna internetförbindelser. Uppgifterna om teleförbindelserna till servercertifikatet har preciserats. Namnen på de Kanta-tjänster som nämns i anvisningen har uppdaterats.	Kanta-tjänsterna FPA	3.7.2024
3.16	Korrigerade hänvisningar till delarna Tjänster och införanden och Kundrelation och stöd på Kanta.fi-webbplatsen.	Kanta-tjänsterna FPA	11.9.2024

Förkortning	Term	Förklaring
CA	certification authority certifikatutfärdare	instans som beviljar certifikat
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
IP	internet protocol internetprotokoll	protokoll som blivit standard för internets nätverksskikt och vars uppgift är att sköta routningen av paket och den logiska adresseringen
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 internetstandard, 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
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

Innehåll

1 Inledning

I anvisningen beskrivs tekniska anslutningsmodeller till följande tjänster:

- Patientdatalagret
- Datalagret för bildmaterial
- Recepttjänsten
- Socialvårdens klientdatalager

Anvisningen gäller inte tjänster där

- användningen inte förutsätter någon separat anslutning (Den nationella kodtjänsten, Valideringstjänsten).
- anslutningsmodellen ännu inte har angetts eller när det finns finns en separat anvisning om användningen av tjänsten (Samtestning, Kundtesttjänsten, Informationsförmedlings- och förfrågningsservicen, Datalagret för egna uppgifter).

Följande anvisningar och föreskrifter har ett nära samband med anvisningen.

- Föreskrift 3/2024: Föreskrift om redogörelser och krav som ska tas in i informationssäkerhetsplanen (THL)
- Föreskrift 4/2024: Föreskrift om klassificering och certifiering av informationssystem och välbefinnandeapplikationer inom social- och hälsovården (THL)
- Förskrift 5/2024: Föreskrift om väsentliga krav på informationssystem och välbefinnandeapplikationer inom social- och hälsovården (THL)
- ISO OID-yksilöintitunnuksen käytön kansalliset periaatteet sosiaali- ja terveysalalla (THL)
- Certifiering, väsentliga krav och datasäkerhetsplan (Kanta.fi)

- Krav på informationssäkerhet inom data och meddelandetrafiken (Kanta.fi)
- Tjänster och införanden (Kanta.fi)
- Anslutningsmodeller (Kanta.fi)
- Kanta-ordlistor (THL)

I anvisningen beskrivs de tekniska anslutningsmodellerna till Kanta-tjänsterna. Modellerna beskriver på ett allmänt plan hur de tekniska förbindelserna mellan en aktör som anlitar tjänsterna och Kanta-tjänsterna kan upprättas. Kanta-tjänsterna reglerar emellertid inte i detalj det tekniska genomförandet av anslutningen.

Anslutningsmodellerna är förenklade. I dem beskrivs den tekniska anslutningen till Kanta-tjänsterna ur olika synvinklar. Modellerna utesluter inte varandra, och den tekniska anslutningen kan även genomföras som en kombination av flera modeller.

De befintliga miljöerna och anslutningarna hos de aktörer som använder Kanta-tjänsterna tillsammans med de olika lösningarna för utläggning ger upphov till en mångfald av tekniska anslutningar.

2 Aktörer

I det här kapitlet presenteras de aktörer som förekommer i anvisningen.

2.1 Kanta-tjänsterna

Kanta-tjänsterna (nedan i den här anvisningen ”Kanta”) producerar digitala tjänster inom social- och hälsovård för medborgarna och social- och hälsovårdens aktörer. Kantas verksamhets styrs av lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården och lagen om elektroniska recept. Kanta produceras i samarbete mellan ett flertal aktörer. I arbetet medverkar Folkpensionsanstalten (FPA), Institutet för hälsa och välfärd (THL), social- och hälsovårdsministeriet (SHM), Myndigheten för digitalisering och befolkningsdata (MDB) och Tillstånds- och tillsynsverket för social- och hälsovården (Valvira) samt aktörerna inom social- och hälsovården, apoteken, systemleverantörer och producenter av IT-tjänster.

En tjänstetillhandahållare inom social- och hälsovården eller en apotekare kan ta i bruk tjänster som hör till Kanta. I den här anvisningen behandlas den tekniska anslutningen till tjänsterna Patientdatalagret, Datalagret för bildmaterial, Recepttjänsten och Socialvårdens klientdatalager.

2.2 Aktör som ansluter sig till Kanta

Med en aktör som ansluter sig till Kanta (nedan i anvisningen ”anslutande aktör”) avses en apotekare eller en tjänstetillhandahållare inom social- och hälsovården som tar i bruk en tjänst.

Kundrelationen till Kanta börjar från att den första tjänsten tas i bruk, varvid den anslutande aktören avger en förbindelse om användningen av Kanta och godkänner de allmänna leveransvillkoren och beskrivningen av tjänsten i fråga. Den anslutande aktören kan använda sig av en eller flera tjänster.

I samband med ibruktagandet meddelar den anslutande aktören Kanta om vilket certifierat system och vilken teknisk anslutning tjänsterna används med. När Kanta godkänner den anslutande aktörens ansökan ges denne de tekniska rättigheterna att använda tjänsterna i Kantas åtkomsthantering.

Kanta får basfakta om de anslutande aktörerna från den nationella kodtjänsten som THL administrerar. Alla anslutande aktörer och aktörer som med deras förbindelser använder Kanta i enlighet med modellen med gemensam anslutning ska vara registrerade i den nationella kodtjänsten antingen i

- Apoteksregistret (Säkerhets- och utvecklingscentret för läkemedelsområdet (Fimea) – Apoteksregistret) eller
- Organisationsregistret för social- och hälsovården (THL – Organisationsregistret för social- och hälsovården) eller
- Kodverket över självständiga yrkesutövare inom hälso- och sjukvården (Valvira – Självständiga yrkesutövare inom hälso- och sjukvården). *

* Enligt lagen om tillsynen över social- och hälsovården (741/2023) blev självständiga yrkesutövare privata tjänsteproducenter med början den 1 januari 2024. Uppgifterna om

tjänsteproducenter (tjänstetillhandahållare enligt lagen om behandling av kunduppgifter inom social- och hälsovården) som 31.12.2023 fanns i Valvira - Registret över självständiga yrkesutövare inom hälso- och sjukvården flyttas fortsättningsvis från Valviras register Soteri till Kanta-tjänsterna via Valvira - Registret över självständiga yrkesutövare inom hälso- och sjukvården.

2.3 Hyresgäst (modell med gemensam anslutning)

Med hyresgäst avses i anvisningen en privat tjänstetillhandahållare som använder tjänster i enlighet med modellen med gemensam anslutning i kapitel 4 på basis av en administrativ ansökan som den anslutande aktören gör och via den anslutande aktörens tekniska anslutning. Hyresgästen avger ingen förbindelse till Kanta, men den anslutande aktören och hyresgästen ska med ett inbördes avtal avtala om ansvaren och skyldigheterna i anslutning till användningen av tjänsterna.

2.4 Kanta-förmedlare

I lagen om behandling av kunduppgifter inom social- och hälsovården benämns förmedlaren mellanhand och definieras som en tjänsteleverantör som erbjuder tjänstetillhandahållare inom social- och hälsovården informationssystemtjänster, användarmiljöer för informationssystem eller Kanta-anslutningspunkter. Förmedlaren utarbetar den informationssäkerhetsplan som beskrivs i THL:s föreskrift 3/2024 och med hjälp av vilken man planerar och säkerställer informationssäkerhet och en korrekt hantering av kunduppgifterna.

Med Kanta-förmedlare avses en förmedlare som upprättar en Kanta-anslutningspunkt. Den anslutande aktören utnyttjar Kanta-förmedlarens anslutningspunkt när en förbindelse upprättas mellan det informationssystem som används och Kanta. I den här rollen har Kanta-förmedlaren möjlighet att se okrypterade kunduppgifter till exempel i samband med underhållsåtgärder.

En Kanta-förmedlare anmäler sig till THL:s register över Kanta-förmedlare. I registret samlas uppgifter om de förmedlare som har fullmakt att fungera som förmedlare vid anslutning till Kanta, men som inte är apotek eller tjänstetillhandahållare inom social- och hälsovården.

Det ska finnas ett avtal mellan Kanta-förmedlaren och den anslutande aktör som använder sig av Kanta-förmedlarens anslutningspunkt i sin egen Kanta-anslutning. I avtalet ska ingå

ett konstaterande av att handlingsmodeller och anvisningar som gäller användningen av Kanta ska efterlevas samt hithörande ansvar och skyldigheter.

3 Grundläggande begrepp

3.1 Kanta-anslutningspunkt

Med Kanta-anslutningspunkt (nedan i den här anvisningen ”anslutningspunkt”) avses den punkt i datakommunikationen varifrån den anslutande aktörens informationssystem ansluts till Kanta via en teleförbindelse som krypterats och identifierats med ett servercertifikat för social- och hälsovården beviljat av MDB.

Den anslutande aktörens anslutningspunkt kan administreras av den anslutande aktören själv, en annan anslutande aktör eller en Kanta-förmedlare. Den som administrerar anslutningspunkten ansöker om ett servercertifikat för anslutningspunkten och meddelar uppgifterna om den (bl.a. anslutningspunktens unika identifikationskod och uppgifterna om teleförbindelserna) till Kanta.

3.1.1 Kraven på en Kanta-anslutningspunkt

Anslutningspunkten kan upprättas med ett system som Valvira har godkänt vilket kan vara en förmedlingstjänst för kunduppgifter i klass A1 i enlighet med THL:s föreskrift 4/2024 eller ett informationssystem som innehåller förmedlingstjänstens funktioner i klass A2 eller A3.

En Kanta-anslutningspunkt ska vara belägen i Finland.

3.1.2 Rekommendationer gällande en Kanta-anslutningspunkt

Rekommendationen är att ange endast en datakommunikationsadress för en anslutningspunkt. Man kan dock ange flera adresser för en anslutningspunkt om det till exempel behövs för att upprätta en reservförbindelse.

Rekommendationen är att använda olika servercertifikat för olika servrar. Om man använder samma servercertifikat i flera olika servrar (t.ex. kluster) behandlas de servrar som använder servercertifikatet som samma anslutningspunkt. Om klustret inte har en gemensam virtuell adress kan klustermedlemmarna utåt visas med sina egna datakommunikationsadresser (IP-adresser).

3.1.3 Anslutningspunktens unika identifierare

Anslutningspunkten tilldelas en unik OID-kod, som bildas i nod 13.

OID-koden för en anslutningspunkt bildas utifrån OID-koden för den anslutande aktören, apoteket eller Kanta-förmedlaren på följande sätt:

- OID-koden för en anslutningspunkt för en tillhandahållare av social- och hälsovård som är registrerad i organisationsregistret för social- och hälsovården är beroende på verksamhetsenhetens OID-kod antingen 1.2.246.10.xxx.10.y.13.n eller 1.2.246.537.10. xxx.10.y.13.n (där xxx är koden för organisationen i organisationsregistret för social- och hälsovården, y aktörens unika nummer och n anslutningspunktens unika nummer).

- OID-koden för en anslutningspunkt för en tjänstetillhandahållare 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 koden för en tjänstetillhandahållare enligt Valviras register över självständiga yrkesutövare inom hälso- och sjukvården och n den unika koden för anslutningspunkten).

- OID-koden för ett huvudapoteks och filialapoteks anslutningspunkt har formen 1.2.246.553.1.xxx.13.n (där xxx är apotekets kod enligt Fimeas Apoteksregister och n det unika numret för anslutningspunkten).

- OID-koden för en Kanta-förmedlares anslutningspunkt bildas i nod 13 under förmedlarens OID-kod i Förmedlarregistret varvid anslutningspunktens OID har formen 1.2.246.537.6.918.18.xxx.13.n (där xxx är koden för organisationen i Förmedlarregistret och n det unika numret för anslutningspunkten).

3.2 Servercertifikat

För anslutningspunkten installeras ett servercertifikat för social- och hälsovården som MDB beviljar, och utifrån vilket anslutningspunkten identifieras och en krypterad TLS-förbindelse bildas mellan Kanta-tjänsterna och anslutningspunkten. Certifikatets uppgifter används även vid identifieringen av tjänstens parter.

Servercertifikatet och anslutningspunkten kopplas till varandra med hjälp av servercertifikatets fält serialNumber i delen Subject. Fältets värde blir den unika OID-kod

som identifierar anslutningspunkten. DNS-namnet på den primära teleförbindelsen anges i fältet commonName i delen Subject samt i fältet SubjectAlternativeName. I fältet SubjectAlternativeName kan man även placera eventuella andra IP-adresser eller DNS-namn.

Servercertifikatet anskaffas av den som administrerar anslutningspunkten, antingen den anslutande aktören eller Kanta-förmedlaren.

Servercertifikatet kan även användas för att kryptera kommunikation mellan den anslutande aktören och en extern anslutningspunkt och för att identifiera kommunicerande parter.

3.3 Systemsignaturcertifikat

För Patientdatalagret och Socialvårdens klientdatalager behöver den anslutande aktören ha ett systemsignaturcertifikat för social- och hälsovården som beviljas av MDB. Med dess privata nyckel undertecknas alla handlingar som skickas till tjänsterna och som inte har undertecknats med en yrkespersons certifikat. Den anslutande aktören behöver endast ett systemsignaturcertifikat. Samma systemsignaturcertifikat kan användas i alla patient- eller klientdatasystem som den anslutande aktören har.

I princip är systemsignaturcertifikatet aktörsspecifikt. Om den anslutande aktören skaffar patient- eller klientdatasystemet som en samlad tjänst kan aktören även använda ett systemspecifikt systemsignaturcertifikat som anskaffats av den som levererar den samlade tjänsten. Då antecknas de ansvar och skyldigheter som anknyter till användningen av systemsigneringscertifikatet i avtalen mellan den tjänsteleverantör som skaffade certifikatet och den anslutande aktören. Tjänsteleverantören ska vara en Kanta-förmedlare.

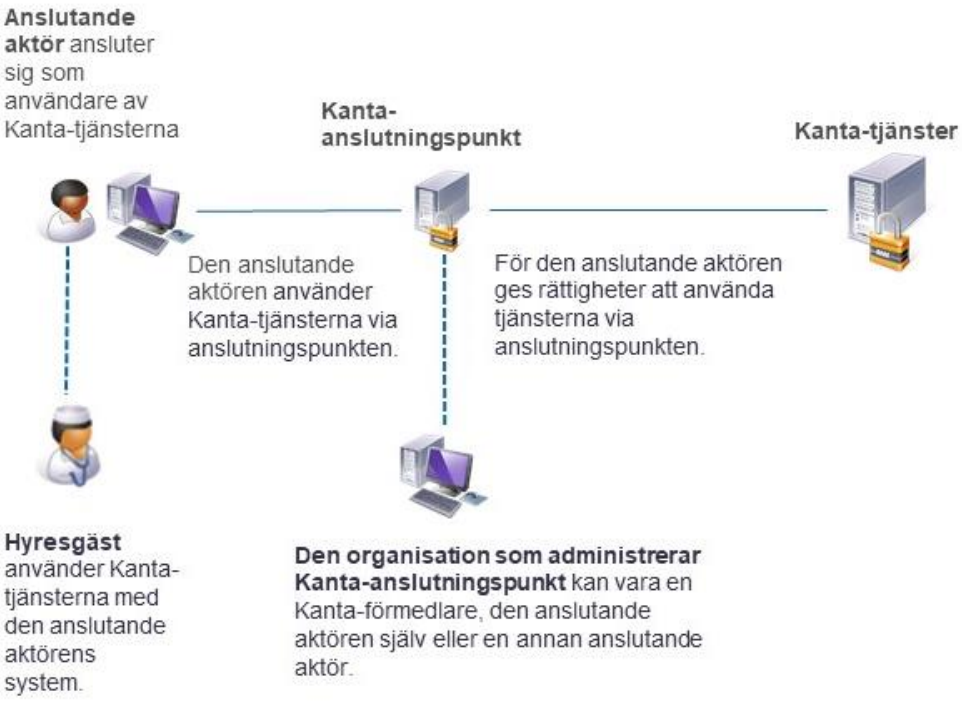
Vid anslutning enligt modellen med gemensam anslutning kan hyresgästen använda den anslutande aktörens systemsignaturcertifikat. Den anslutande aktören och hyresgästen ska avtala om detta i ett ömsesidigt avtal.

4 Anslutningsmodeller för Kanta-tjänsterna

Ibruktagandet av Kanta-tjänsterna förutsätter att den som ska ansluta sig ansluter sig administrativt, vilket beskrivs på Kanta.fi under Tjänster och införanden och Kundrelation och stöd. Den anslutande aktören kan ta i bruk en eller flera tjänster. I samband med att den första tjänsten tas i bruk ansöker den anslutande aktören om att ansluta sig som användare av tjänsten, undertecknar förbindelsen om användningen av Kanta samt godkänner de

allmänna leveransvillkoren och tjänstebeskrivningen för den tjänst som ska tas i bruk. När därpåföljande tjänster tas i bruk räcker det att ansöka om anslutning och godkänna tjänstebeskrivningen.

I samband med att tjänster tas i bruk meddelar den anslutande aktören via vilken anslutningspunkt/vilka anslutningspunkter och med vilket/vilka system denne använder tjänsten. Utifrån ansökan ges den ansökande aktören rättighet i åtkomsthanteringen i Kanta att använda tjänsterna. (Figur 1).



Figur 1: Användningen av Kanta-tjänsterna

4.1 Administrativ anslutning

4.1.1 Tjänstetillhandahållare inom social- och hälsovården

I **modellen med direkt anslutning** är den anslutande aktören en tjänstetillhandahållare inom social- och hälsovården som har anslutit sig administrativt.

I modellen med gemensam anslutning som är avsedd för privata tjänstetillhandahållare kan tjänsterna användas av en privat tjänstetillhandahållare som verkar i en privat anslutande aktörs lokaler och använder dennes datasystem. Den privata tjänstetillhandahållaren kallas i denna anvisning hyresgäst. Hyresgästen avger ingen förbindelse till Kanta och verkar

således inte som anslutande aktör. Hyresgästen och den anslutande aktören avtalar i ett ömsesidigt avtal om ansvar och skyldigheter i anslutning till användningen av tjänsterna.

I **modellen med parallell anslutning** som tillämpas av Socialvårdens klientdatalager verkar en privat tjänstetillhandahållare inom socialvården i rollen som tjänsteproducent och använder tjänsterna via kunddatasystemet hos den som ordnar tjänsterna. I modellen med parallell anslutning ansluter sig den tjänstetillhandahållare som verkar som tjänsteproducent administrativt till Kanta och är därmed anslutande aktör.

4.1.2 Apotekare

Apotekaren på huvudapotek och filialapotek ansluter sig administrativt till Kanta och är anslutande aktör. Den förbindelse apotekaren avger gäller alla de apotek som apotekaren innehar vid respektive tid.

4.1.3 Sjukhusapotek och läkemedelscentraler

Sjukhusapotek eller läkemedelscentraler avger en förbindelse om användningen av Kanta och är anslutande aktörer.

4.2 Teknisk anslutning

I samband med att tjänster tas i bruk meddelar den anslutande aktören Kanta om via vilken anslutningspunkt/vilka anslutningspunkter och med vilket/vilka system denne använder tjänsterna. Utifrån ansökan ges den ansökande aktören rättighet i åtkomsthanteringen i Kanta att använda tjänsterna.

Kanta-adressindexet fungerar som en del av Kantas åtkomsthantering och i indexet sparas uppgifterna om den anslutande aktören, de anslutningspunkter den anslutande aktören använder och tillåtna tjänster för den anslutande aktören.

4.2.1 Tjänstetillhandahållare inom social- och hälsovården

I modellen med direkt anslutning ges den anslutande aktören i Kanta-adressindexet rättigheter till de tjänster för vilka den anslutande aktören har gjort anslutningsansökan och som Kanta har godkänt att den anslutande aktören använder.

Om den anslutande aktören är en tjänstetillhandahållare inom hälso- och sjukvården som använder Recepttjänsten och som tar emot begäranden om receptförnyelse från apotek och

MittKanta ges den anslutande aktören rättigheter till att ta emot begäranden om förnyelse. För att ta emot begäranden om förnyelse krävs att den anslutande aktören har en anteckning om mottagande av begäranden om förnyelse i THL:s nationella kodtjänst. Anteckningen för tjänstetillhandahållaren görs i Valviras register över självständiga yrkesutövare inom hälso- och sjukvården eller per serviceenhet i organisationsregistret för social- och hälsovården.

I figur 2 presenteras ett förenklat exempel på teknisk anslutning för en tjänstetillhandahållare inom hälso- och sjukvården som använder sig av Kanta med modellen med direkt anslutning. Den anslutande aktören använder tjänsterna via två olika anslutningspunkter. Den första anslutningspunkten administreras av den anslutande aktören själv och via den använder den anslutande aktören Recepttjänsten och Patientdatalagret. Dessutom har den anslutande aktören två serviceenheter som tar emot begäranden om förnyelse och de går via den anslutande aktörens egen anslutningspunkt. Den anslutande aktören använder även Patientdatalagret via en Kanta-förmedlares anslutningspunkt. För den anslutande aktören läggs Recepttjänstens och Patientdatalagrets tjänster till i Kanta-adressindexet samt tjänsten att ta emot begäranden om förnyelse via den egna anslutningspunkten. För den anslutande aktören läggs det dessutom till Patientdatalagrets tjänster via en Kanta-förmedlares anslutningspunkt.

Figur 2: Teknisk anslutning av tjänstetillhandahållare inom hälso- och sjukvården

I modellen med gemensam anslutning ges en hyresgäst inte rättigheter att använda tjänster i Kantas åtkomsthantering. Hyresgästen använder tjänsterna med den anslutande aktörens rättigheter, men denne ska i fråga om meddelanden och handlingar ge tjänsten uppgifter om att tjänsten används av hyresgästen.

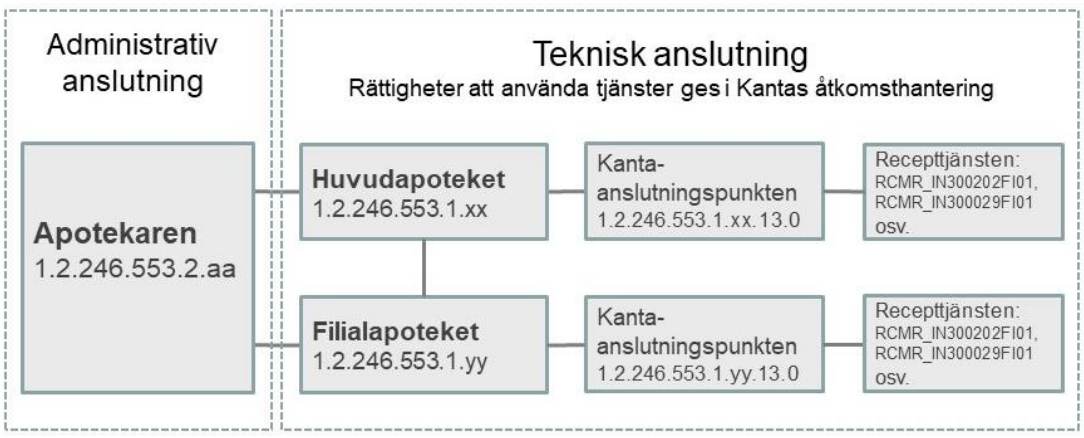
I modellen med parallell anslutning ges den anslutande aktör som fungerar som tjänstetillhandahållare rättigheter i Kanta-adressindexet att använda Socialvårdens klientdatalager via den anslutningspunkt som tjänsteanordnaren använder.

Sjukhusapotek eller läkemedelscentraler som fungerar som anslutande aktörer ges rättigheter i Kanta-adressindexet att använda Recepttjänsten. Sjukhusapotek och läkemedelscentraler kan ansluta till Kanta via en egen anslutningspunkt eller via en annan anslutande aktörs eller Kanta-förmedlarens anslutningspunkt.

4.2.2 Huvudapotek och filialapotek

Samtliga huvud- och filialapotek har egna anslutningspunkter. Huvud- och filialapotek ges i Kantas åtkomsthantering rättigheter att använda Recepttjänsten via den egna anslutningspunkten.

Figur 3 visar anslutningsmodellen för apotek. Apotekaren gör den administrativa anslutningen till Kanta. Apotekaren innehar huvudapoteket och dess filialapotek. Både huvudapoteket och filialapoteket har egna anslutningspunkter. I Kanta-adressindexet ges huvudapoteket och filialapoteket de rättigheter som apoteket behöver till Recepttjänsten via apotekens egna anslutningspunkter.



Figur 3: Teknisk anslutning för apotek

5 Datakommunikation

Samtidigt med uppgifterna om anslutningspunkten meddelar den aktör som administrerar anslutningspunkten även Kanta om anslutningspunktens teleförbindelser till vilka den behövliga routningen görs i Kanta. När en ny anslutningspunkt i produktionsmiljö inrättas kan den aktör som administrerar anslutningspunkten begära adresserna till Kantas produktionsmiljöer och partsinformation i Kanta-meddelandetrafiken hos Kantas kundtjänst.

Den anslutande aktören ansvarar för att beställa teleförbindelserna mellan den anslutande aktören och Kanta i enlighet med egna kapacitets-, kvalitets- och servicenivåkrav. För teleförbindelsernas del är det viktigt att beakta även reservförbindelserna för att trygga förbindelser både i störningssituationer och undantagsförhållanden. FPA ansvarar för Kantas interna datakommunikation fram till datakommunikationsoperatörens gränssnitt.

I det här avsnittet presenteras de centrala kraven på och rekommendationerna för teleförbindelserna på en allmän nivå.

5.1 Anslutningens typ

Teleförbindelserna mellan den anslutande aktören och Kanta ska genomföras som en förbindelse via ett privat nät för att säkerställa tillgängligheten till tjänsten och dess kvalitet. Förbindelse via ett privat nät kan skyddas bättre mot det öppna internets hot, bland annat överbelastningsattacker.

För anslutning via ett privat nät garanterar datakommunikationsoperatören en viss kapacitet hela vägen. Anslutning via ett privat nät (MPLS eller motsvarande) beställs hos en datakommunikationsoperatör mellan den anslutande aktören, anslutningspunkten eller anslutningsnoden och Kantas serverhallar. Man bör i samband med att förbindelser tas i bruk vara beredd på att det kan ta flera veckor att upprätta förbindelsen. Förbindelsen bör vara klar när den anslutande aktör som använder förbindelsen gör ansökan om anslutning till Kanta.

En öppen internetförbindelse kan användas endast i motiverade undantagsfall. Som förbindelse för Datalagret för bildmaterial eller primär förbindelse för apotekens Recepttjänst är en öppen internetförbindelse inte tillåten ens i undantagsfall.

I Tabell 1 preciseras användningen av öppen internetförbindelse i olika fall.

Användning av förbindelse	**Öppen internetförbindelse**
Apotekssystem, anslutningspunkt som apoteket administrerar	En öppen internetförbindelse får endast användas som reservförbindelse.
Patientdatasystem, om en anslutningspunkt som den anslutande aktören administrerar används	Det är tillåtet att använda öppen internetförbindelse om den anslutningspunkt som den anslutande aktören administrerar används endast av den anslutande aktören själv och meddelandetrafiken är liten.
Kunddatasystem, om en anslutningspunkt som den anslutande aktören administrerar används	Det är tillåtet att använda öppen internetförbindelse om den anslutningspunkt som den anslutande aktören administrerar används endast av den anslutande aktören själv och meddelandetrafiken är liten.
Samlingspunkt för datakommunikation eller anslutningspunkt som tillhandahålls av en Kanta-förmedlare	Det är tillåtet att använda öppen internetförbindelse endast som reservförbindelse.

Tabell 1. Exempel på användning av öppen internetförbindelse

När en öppen internetförbindelse används bör man särskilt uppmärksamma de risker som hänför sig till förbindelsesättet, som överbelastningsattacker och andra datasäkerhetshot mot internetgränssnittet.

5.2 Krav på datakommunikationen

Anslutningspunkternas IP-adresser ska vara fasta och höra till den offentliga IP-adressrymden. IP-adressen ska i det offentliga indexet kunna specificeras tillhöra den aktör som administrerar anslutningspunkten.

Teleförbindelserna mellan anslutningspunkten och Kanta ska genomföras som en förbindelse via ett privat nät, till exempel med hjälp av MPLS-metoden. Förbindelserna via

privata nät gör det möjligt att överföra datakommunikationen till Kanta-tjänsternas olika lokationer (Kanta A-, B- och C-hallar). Användning av förbindelser via det öppna internet är tillåtet endast i de undantagsfall som anges i kapitel 5.1.

Teleförbindelserna mellan anslutningspunkten och Kanta ska genomföras så att de är krypterade. Den som beställer anslutningen ska hos datakommunikationsoperatören försäkra sig om att den primära förbindelsen och reservförbindelsen faktiskt hela vägen löper via olika rutter. Det kan bli omöjligt att försäkra sig om detta om anslutningarna skaffas hos olika operatörer, eftersom operatörerna vanligtvis inte avslöjar sina anslutningars fysiska förbindelser. Om det inte är möjligt att genomföra en helt dubbelriktad förbindelse är rekommendationen att den dubbelriktas i den utsträckning som det är ekonomiskt förnuftigt.

Den tekniska lösningen för anslutning till Kanta ska uppfylla kraven i anvisningen Kanta-tjänsterna: Krav på informationssäkerhet inom data- och meddelandetrafiken.

5.3 Rekommendationer angående datakommunikationen

Det rekommenderas att man använder en till hastigheten symmetrisk teleförbindelse. Det innebär att överföringskapaciteten är lika stor i båda riktningarna.

5.4 Anslutningens dataöverföringskapacitet

Den anslutande aktören ansvarar för att definiera anslutningens överföringskapacitetsbehov. När kapacitetsbehovet uppskattas är det viktigt att ta hänsyn till mängden kommunikation och hur kritisk verksamheten är. Den anslutande aktören ska försäkra sig om att anslutningen är skalbar.

5.5 Teleförbindelsernas dimensionering

I förteckningen nedan räknas det upp exempel på minimikravet för kapacitet som behövs

- Litet apotek 10 Mbit/s
- Stort apotek 30 Mbit/s
- En anslutande aktör som arkiverar färre än 10 000 handlingar om dagen 30 Mbit/s
- En anslutande aktör som arkiverar fler än 100 000 handlingar om dagen 500 Mbit/s

- En anslutande aktör som använder Datalagret för bildmaterial minst 300 Mbit/s

5.6 Samlingspunkt för datakommunikation

En samlingspunkt för datakommunikation är en lösning där datakommunikationen från olika anslutningspunkter till Kanta sammanförs och routras till Kanta längs en gemensam teleförbindelse och där trafiken från Kanta routras till olika anslutningspunkter från Kanta. Routningen av datakommunikationen påverkar inte TLS-krypteringen: kryptering varken dekrypteras eller bildas i samlingspunkten, och inga uppgifter som ska skyddas visas okrypterade.

6 Sammandrag över rekommendationer och krav angående teknisk anslutning

Anvisningen Kanta-tjänsterna: Krav på informationssäkerhet inom data- och meddelandetrafiken ska beaktas vid teknisk anslutning, samt även följande krav:

- Teleförbindelserna genomförs i princip som en förbindelse via privata nät, till exempel med hjälp av MPLS-metoden. Förbindelse via ett privat nät ska kopplas till Kanta-tjänsternas olika lokationer (Kanta A-, B- och C-hallarna). Användning av förbindelser via det öppna internet är tillåtet endast i de undantagsfall som anges i kapitel 5.1 i den här anvisningen.

- IP-adresserna ska vara fasta och offentliga. IP-adressen ska i det offentliga indexet kunna specificeras tillhöra den aktör som administrerar anslutningspunkten.

- Den tekniska lösningen ska uppfylla informationssäkerhetskraven för data- och meddelandetrafik. Till kraven hör bland annat tillståndsstyrd brandvägg och virusbekämpning.

- För anslutningspunkten installeras ett servercertifikat som MDB beviljar, och utifrån vilket anslutningspunkten identifieras och en krypterad TLS-förbindelse bildas mellan Kanta och anslutningspunkten. Certifikaten ska motsvara minst de nationella kryptografiska kraven enligt Cybersäkerhetscentralens nivå TL IV.

- När Patientdatalagrets eller Socialvårdens klientdatalagers tjänster används ska den anslutande aktören ha ett systemsigneringscertifikat.

- Teleförbindelserna ska mångdubblas.

Det rekommenderas att man använder en till hastigheten symmetrisk teleförbindelse.

7 Exempel på teknisk anslutning

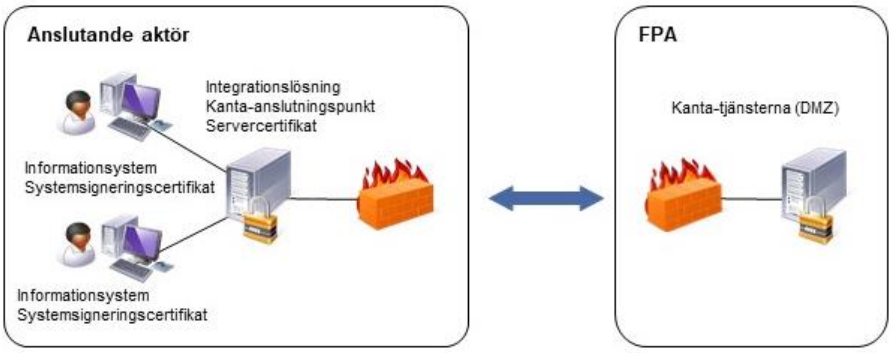
De tekniska anslutningsmodeller som beskrivs här utesluter inte varandra, och vid anslutning kan olika modeller kombineras. I fråga om alla de tekniska anslutningsmodeller som beskrivs här bör man beakta att anslutningspunkterna ska vara belägna i Finland.

7.1 Anslutning via den anslutande aktörens egen anslutningspunkt

7.1.1 Anslutning via en egen integrationslösning

I det här exemplet har den anslutande aktören en egen integrationslösning via vilken tjänsterna används med hjälp av flera olika informationssystem som den anslutande aktören har. Det servercertifikat som MDB beviljar installeras i anslutning till integrationslösningen. Med certifikatlösningen bildas en identifierad och krypterad förbindelse till Kanta. Det kan behövas ett servercertifikat även mellan integrationslösningen och de informationssystem som ska anslutas för att säkerställa parternas identitet och kryptera dataöverföringen.

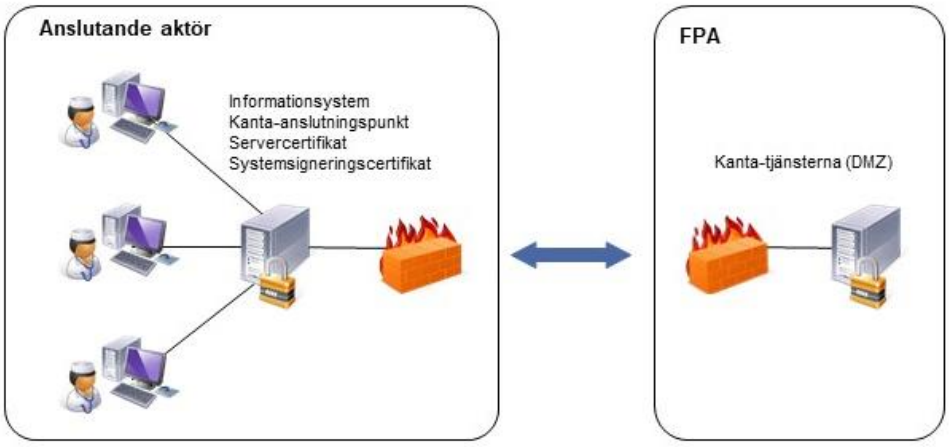
Att använda en integrationslösning möjliggör trafik från flera system till Kanta längs samma teleförbindelse. (Figur 4).



Figur 4: Anslutning via den anslutande aktörens egen integrationslösning

7.1.2 Anslutning direkt från ett informationssystem man själv administrerar

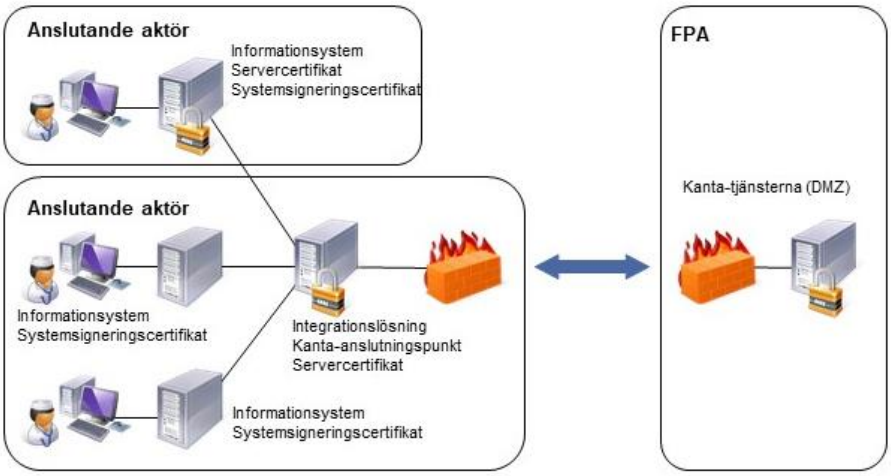
I exemplet administrerar den anslutande aktören själv det informationssystem som ska anslutas till Kanta och anslutningspunkten. Servercertifikatet installeras direkt på programservern eller en separat aktiv enhet i anslutning till informationssystemet. (Figur 5).



Figur 5: Anslutning från ett informationssystem som den anslutande aktören själv administrerar

7.2 Anslutning via en annan anslutande aktörs anslutningspunkt

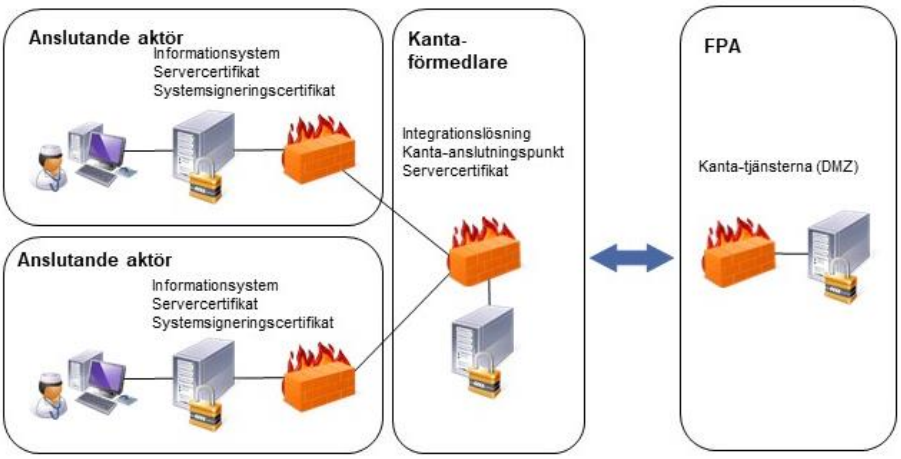
I det här exemplet använder den anslutande aktören en anslutningspunkt som en annan anslutande aktör har upprättat. Servercertifikatet är utfärdat i den anslutande aktörs namn som administrerar anslutningspunkten och installeras i anslutning till anslutningspunkten. Kommunikationen mellan den anslutande aktören och den anslutande aktör som administrerar anslutningspunkten är krypterad och identifierad med hjälp av det servercertifikat som MDB beviljar. (Figur 6).



Figur 6: Anslutning via en anslutningspunkt som en annan anslutande aktör administrerar

7.3 Anslutning via en Kanta-förmedlares anslutningspunkt

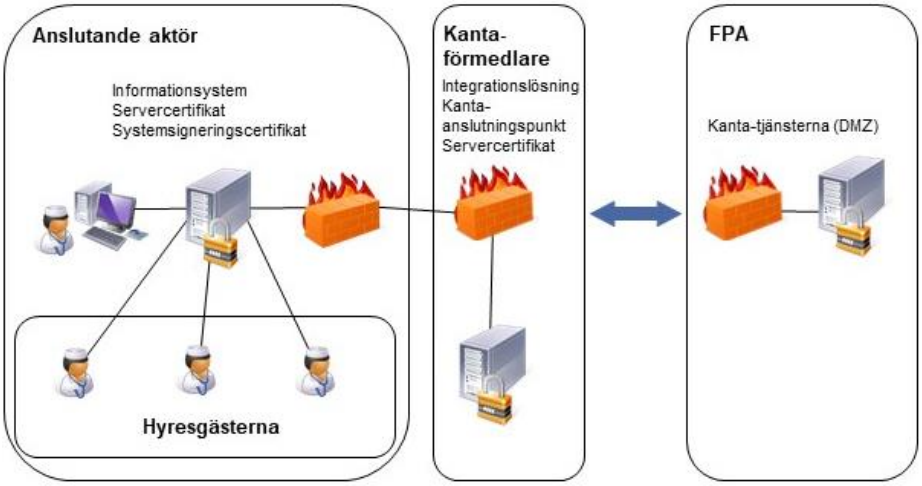
I det här exemplet använder den anslutande aktören tjänster via en anslutningspunkt som en Kanta-förmedlare har upprättat. Servercertifikatet är utfärdat i Kanta-förmedlarens namn och installeras i anslutning till anslutningspunkten. Trafiken mellan den anslutande aktören och Kanta-förmedlarens anslutningspunkt är krypterad och de kommunicerande parterna identifieras med hjälp av ett servercertifikat som MDB beviljar. Anslutande aktörer har aktörsspecifika systemsigneringscertifikat. (Figur 7).



Figur 7: Anslutning via en anslutningspunkt som administreras av en Kanta-förmedlare

7.4 Anslutning enligt modellen med gemensam anslutning

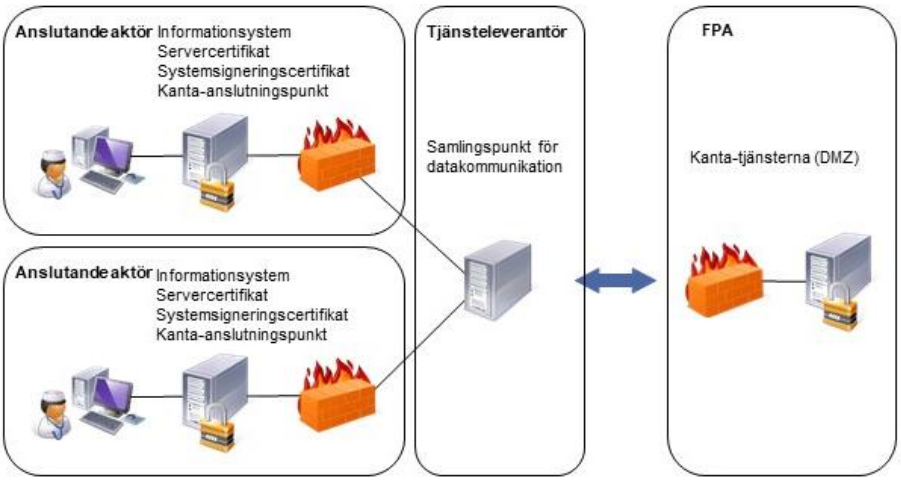
I det här exemplet använder hyresgästen (en tjänstetillhandahållare inom hälso- och sjukvården) tjänster via den anslutande aktörens informationssystem och tekniska förbindelse. Hyresgästen ingår ett avtal med den anslutande aktören om ansvar och skyldigheter i anslutning till användningen av Kanta. Informationssystemet lägger till hyresgästens identifieringsuppgifter i de handlingar och meddelande som lagras i Kanta. (Figur 8).



Figur 8: Anslutning enligt modellen med gemensam anslutning

7.5 Anslutning med hjälp av en samlingspunkt för datakommunikation

I det här exemplet använder den anslutande aktören tjänsterna med sitt eget informationssystem via sin egen anslutningspunkt. Den anslutande aktörens datakommunikation från anslutningspunkten till Kanta samlas i en samlingspunkt för datakommunikation och dirigeras till Kanta med hjälp av en gemensam teleförbindelse. På motsvarande sätt routras trafiken från Kanta i samlingspunkten för datakommunikation till olika anslutande aktörers anslutningspunkter. (Figur 9).



Figur 9: Anslutning med hjälp av samlingspunkt för datakommunikation