Avdelningen för informationstjänster
Enheten för styrning av den operativa
Verksamheten (OPER)

3.6.2015

CERTIFIERING AV KANTA-FÖRMEDLINGSSERVICE SAMT KANTA-FÖRMEDLARE

Målgrupper: Verksamhetsenheter för hälso- och sjukvård
Tillverkare/leverantörer av informationssystem
Bedömningsorgan för informationssäkerhet
Kanta-förmedlare
Upprättare av Kanta-förmedlingsservice

Giltighetstid: Anvisningen träder i kraft genast och gäller tills vidare

Avdelningen för informationstjänster
Enheten för styrning av den operativa
Verksamheten (OPER)

3.6.2015

CERTIFIERING AV KANTA-FÖRMEDLINGSSERVICE SAMT KANTA-FÖRMEDLARE

I samband med certifiering av de riksomfattande Kanta-tjänsterna har det framkommit behov av att precisera hur certifieringen av Kanta-förmedlartjänster går till liksom förhållandet mellan den Kanta-förmedlingsservice som avses i klientuppgiftslagen och de förmedlarorganisationer som administrerar Kanta-anslutningspunkterna.

Folkpensionsanstalten (FPA) har beskrivit allmänna modeller för hur man kan ansluta sig till Kanta-tjänsterna (Tekniska anslutningsmodeller till Kanta-tjänsterna[1]). I FPAs anvisningar beskrivs följande anslutningsmodeller till Kanta-tjänsterna för producenter av social- och hälsovårdstjänster:

1. anslutning via en egen integrationslösning (meddelandeförmedlingslösning)
2. direkt anslutning från ett patientdata- eller apotekssystem i den egna maskinsalen
3. anslutning via en externaliserad anslutningspunkt
    a. externaliserat informationssystem (t.ex. externaliserad maskinsal, Software as a Service-tjänst)
    b. externaliserad integrationslösning (meddelandeförmedlingslösning)
    c. externaliserad datakommunikation (samlingspunkt för datakommunikationen)
4. en liten organisations anslutning via internet.

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. Dessa anvisningar har utarbetats innan bestämmelser om certifiering av Kanta-förmedlingsservice togs in i lagstiftningen.

Följande frågor har lyfts fram i anslutning till saken:

- Situationen i Kanta-anslutningspunkterna är ofta den att det övergripande ansvaret för förmedlingsservicen vilar på informationsförvaltningsaktören (till exempel sjukvårdsdistriktets förmedlaraktör), som anlitar en tredje parts förmedlingsservice för att upprätta anslutningspunkten rent tekniskt. Hur ska de olika aktörernas ansvar för att kraven på informationssäkerhet uppfylls och verifieras fastställas i sådana situationer?

[1] Handbok för införandet av Patientdataarkivet: http://www.kanta.fi/sv/web/ammattilaisille/potilastiedon-arkiston-kayttoonoton-kasikirja

Avdelningen för informationstjänster
Enheten för styrning av den operativa
Verksamheten (OPER)

3.6.2015

- Är det nödvändigt att utföra samma verifiering av förmedlingsservicens informationssäkerhet flera gånger i olika anslutningspunkter och för olika Kanta-anslutare, som det är fråga om samma produkt som används i förmedlingsservicen?
- I vilken mån berörs produktionen av maskinsalstjänster eller tillämpningar som baserar sig på molntjänster av kraven på certifiering och extern auditering av Kanta-förmedlingsservice?

Denna anvisning preciserar THL:s föreskrifter 1/2015 (föreskrift om väsentliga krav på informationssäkerhet hos informationssystem av klass A) och 2/2015 (föreskrift om plan för egenkontroll). Anvisningen inverkar inte på tidsfristerna enligt föreskrifterna och bestämmelserna. Anvisningen ligger också till grund för framtida preciseringar av föreskrifterna.

BAKGRUND

Lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) ändrades och preciserades 2014. Med stöd av lagen har föreskrifter om krav på certifiering av informationssystem av klass A utarbetats. Enligt lagen är Kanta-förmedlingsservice informationssystem av klass A (som ska anslutas till Kanta-tjänsterna). Även informationssystem som anslutning till Kanta-tjänsterna via en förmedlingstjänst hör till klass A. Alla krav som riktas mot informationssystem av klass A är ändå inte relevanta med tanke på förmedlingsservice. Produktionen av förmedlingsservice berörs också av skyldighet att utarbeta en plan för egenkontroll och följa att den genomförs. Eftersom förmedlingsservice är informationssystem av klass A ska de också anmälas till Valvira. Informationssystem av klass A (och sålunda också Kanta-förmedlingsservice) berörs av det lagstadgade kravet på auditering av informationssäkerheten. Certifieringsprocessen för Kanta-förmedlingsservice har beskrivits i bl.a. dokumentet ”Kanta-certifiering och egenkontroll – överblick och processer”[2].

Varje organisation som ansluter sig till Kanta-tjänsterna har minst en *Kanta-anslutningspunkt*. Den kan upprättats som organisationens egen verksamhet eller av en annan organisation. När olika Kanta-anslutningar upprättas iakttas flera av de ovan beskrivna modellerna i olika användningsmiljöer och organisationer. De tidigare riktlinjerna för säkerställande och verifiering av informationssäkerhet har i huvudsak baserat sig på *förmedlaraktörens* Kanta-självauditeringar.

DEFINITIONER OCH PRECISERINGAR AV DEM

- **Kanta-anslutare** är en organisation som producerar social- och hälsovårdstjänster eller ett apotek som ansluter eller har anslutit sig till Kanta-tjänsterna som användare.

[2] Kanta-tjänsternas certifieringssidor: http://www.kanta.fi/sv/web/ammattilaisille/sertifiointi

- **Kanta-förmedlingsservice** är en teknisk lösning som ska utnyttjas när ett informationssystem ansluts till Kanta-tjänsterna och anslutningspunkten upprättas och för vilken överensstämmelseintyg kan skaffas genom en certifieringsprocess och som kan genomgå extern informationssäkerhetsauditering som ett led i denna process.
- **Anslutningspunkt** avser den punkt 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 eller Valviras servercertifikat finns installerat i Kanta-anslutningspunkten. Förbindelsen från producenten av social- och hälsovårdstjänster eller apoteket till Kanta-tjänsterna byggs upp via anslutningspunkten.
- **Upprättare av förmedlingsservice** är den aktör som svarar för det tekniska genomförandet av förmedlingsservicen. Definitionen motsvarar lagens ”tillverkare av informationssystem”. Upprättaren av förmedlingsservice är den aktör för vars förmedlingsservice överensstämmelseintyg ska skaffas. Tillverkaren får inte överensstämmelseintyg ”som organisation”. Upprättaren av förmedlingsservice kan i vissa situationer också vara förmedlare. Med upprättare av förmedlingsservice avses inte tillverkaren av en teknisk plattform för allmän användning, t.ex. en integrationsplattform, utan den aktör som svarar för att förmedlingsservicen tekniska helhet genomförs, t.ex. i anslutning till meddelandeförmedling eller certifikathantering, eventuellt genom att utnyttja en plattform för allmän användning. Upprättaren av förmedlingsservice kan dessutom ofta ansvara för installation, underhåll och tillsyn utöver genomförandet.
- **Förmedlare** är en serviceproducent som en hälso- och sjukvårdsorganisation eller ett apotek anlitar för att upprätta Kanta-anslutningspunkten, och som i denna roll har möjlighet att läsa icke-krypterade patientuppgifter, t.ex. i samband med underhållsåtgärder. Förmedlaren ansvarar för egenkontrollen hos producenten av förmedlingsservice samt för att de väsentliga kraven på Kanta-förmedlingsservice uppfylls då anslutningspunkten upprättas. Förmedlaren kan ansvara för ansökan om och administrering av Kanta-anslutningspunkten certifikat.

ANSVAR FÖR CERTIFIERING OCH SJÄLVKONTROLL AV FÖRMEDLINGSSERVICE

De väsentliga kraven på informationssäkerhet och kraven på egenkontroll bildar ett kontinuum, där det är möjligt att verifiera en del av kraven med produktcertifiering av förmedlingsservicen och en del med egenkontroll i användningsmiljön. Då måste man precisera och vara på det klara med vilka krav som a) Kanta-anslutaren (så som producenten av social- och hälsovårdstjänster), b) förmedlaren och c) upprättaren av förmedlingsservice ansvarar för.

När Kanta-förmedlingsservice produceras måste ansvarsförhållanden och lösningar fastställas så att planerna för egenkontroll och certifieringskraven bildar en enhetlig helhet, där man kan uppfylla alla krav som riktar sig mot förmedlingsservicen och egenkontrollen för förmedlingsservicens del.

Avdelningen för informationstjänster
Enheten för styrning av den operativa
Verksamheten (OPER)

3.6.2015

Producenten av social- och hälsovårdstjänster ansvarar i sista hand för att den Kanta-anslutningslösning som utnyttjas i användningsmiljön (inklusive en eventuell förmedlaraktörs verksamhet och Kanta-förmedlingsservice som eventuellt utnyttjas) uppfyller de väsentliga kraven på informationssäkerhet och att kraven på användningsmiljö uppfylls. Kanta-anslutarens avtal med externa förmedlare och upprättare av förmedlingsservice är viktiga sätt att uppfylla kraven.

Kanta-anslutaren ska utarbeta en plan för egenkontroll i enlighet med THL:s föreskrift 2/2015. Genom planen för egenkontroll ska det gå att verifiera att kraven är uppfyllda på ovan beskrivet sätt. I planen för egenkontroll är det också möjligt att hänvisa till planer för egenkontroll eller överensstämmelseintyg för aktörer som står i avtalsförhållande till Kanta-anslutaren, om en del av kraven riktar sig mot dessa aktörer.

Upprättaren av förmedlingsservice kan vara en annan aktör än *förmedlaren* i Kanta-anslutningspunkten. Förmedlaren ska utarbeta en lagenlig plan för egenkontroll för upprättaren av förmedlingsservice.

CERTIFIERING AV FÖRMEDLINGSSERVICE

Certifiering och auditering av informationssäkerheten som riktar sig mot Kanta-förmedlingsservice är *produktcertifiering.* Certifieringen riktar sig mot *förmedlingsservicen "*som system". Samma Kanta-förmedlingsservice kan användas i flera olika Kanta-förmedlingspunkter och i flera olika kundmiljöer. Flera olika förmedlare kan också anlita samma förmedlingsservice.

Det är inte nödvändigt att utföra extern auditering av informationssäkerheten som riktar sig mot förmedlingsservice separat i alla olika anslutningspunkter eller användningsmiljöer. För förmedlingsservicens del måste det dock beskrivas vilka omständigheter som ska preciseras i användningsmiljöerna och vilka krav ombesörjs direkt via förmedlingsservicen.

Om en del av de krav på informationssäkerhet som riktar sig mot förmedlingsservicen ska uppfyllas med åtgärder i användningsmiljön, ska upprättaren av förmedlingsservicen beskriva och ge anvisningar om hur användningsmiljöspecifika omständigheter ska preciseras i användningsmiljön. Sättet att genomföra dessa användningsmiljöspecifika preciseringar ska beskrivas i den plan för egenkontroll som hänför sig till användningsmiljön och för vilken även förmedlaren eller Kanta-anslutaren kan ansvara. Det sätt på vilket kraven uppfylls eller anvisningar om uppfyllandet av kraven har getts i användningsmiljön är en del av informationssäkerhetsauditeringen av förmedlingsservicen.

Det förutsätts inte att förmedlingsservice ska rapportera om *samtestning* som utförts tillsammans med FPA som ett led i verifieringen av överensstämmelse med kraven, men liksom i fråga om andra informationssystem av klass A förutsätts att förmedlingsservice som är i produktionsanvändning har ett gällande överensstämmelseintyg.

Avdelningen för informationstjänster
Enheten för styrning av den operativa
Verksamheten (OPER)

3.6.2015

Anmälan om certifierad förmedlingsservice ska göras till Tillstånds- och tillsynsverket för social- och hälsovården (Valvira) i enlighet med bestämmelserna.

FÖRMEDLARES EGENKONTROLL OCH REGISTRERING

Tjänsteproducenters och förmedlares självauditering har i enlighet med ändringarna i klientuppgiftslagen ersatts med *egenkontroll.* Detta är utgångspunkt också i fråga om sådana aktörer som tidigare har utfört självauditering i egenskap av Kanta-förmedlare.

Förmedlare ska i enlighet med befintliga anvisningar[3] registrera sig i THL:s förmedlarregister, om inte förmedlaren är en enhet för social- och hälsovårdstjänster som själv hör till registret över social- och hälsovårdsorganisationer. Registrering behövs bland annat för ansökan om de servercertifikat som behövs i anslutningspunkten. Om inte förmedlaren själv är en Kanta-anslutare, ska ansökan enligt anvisningarna för förmedlarregistret omfatta ett bemyndigande från Kanta-anslutaren att fungera som förmedlare. I samband med ansökan ska förmedlarens plan för egenkontroll lämnas in. En plan för egenkontroll ska också lämnas in om den inte har lämnats in tidigare i samband med ansökan om att fungera som förmedlare. Om en producent av social- och hälsovårdstjänster fungerar som förmedlare för en annan producent av social- och hälsovårdstjänster förutsätter detta inte registrering i förmedlarregistret.

Förmedlaren ska utarbeta en plan för egenkontroll, men behöver inte utföra extern auditering av informationssäkerheten om förmedlaren anlitar en certifierad förmedlingstjänst i den miljö där förmedlaren fungerar som förmedlare. Genom egenkontrollen ska även då uppfyllas de väsentliga krav på informationssäkerhet som riktar sig mot informationssystem av klass A i systemets användningsmiljö och som det vid certifieringen har konstaterats att uppfylls genom användningsmiljön.

Förmedlaren ska i sin plan för egenkontroll beskriva hur det ombesörjs att den förmedlingstjänst som anlitas är certifierad.

Förmedlaren kan också skaffa en del av anslutningspunktens tjänster från underleverantörer. Den förmedlare som administrerar anslutningspunkten, dvs. i vars namn servercertifikatet står, ska stå i avtalsförhållande till den social- och hälsovårdsorganisation eller det apotek som ansluter sig (se Tekniska Kanta-anslutningsmodeller).

I anslutningspunkten bör en certifierad förmedlingstjänst anlitas, om anslutningsmodellen innebär att en externaliserad anslutningspunkt utnyttjas. Samma certifierade

[3] Anvisning om anslutning till Kanta-förmedlarregistret:
http://www.thl.f/tilastoliite/koodistopalvelu/OHJE_KanTa_V%E4litt%E4j%E4rekisteri.pdf

förmedlingstjänst kan användas av flera anslutningspunkter, också i olika förmedlares verksamhet.

I förmedlarens egenkontroll beskrivs de saker i anslutning till kraven på användningsmiljö som förmedlaren själv ansvarar för och sådana omständigheter i anslutning till kraven på användningsmiljö beträffande vilket ansvaret bestäms utifrån ingångna avtal för någon annan part och som inte beskrivs som en del av andra aktörers planer för egenkontroll. Det ska gå att verifiera att kraven är uppfyllda.

I förmedlarens plan för egenkontroll ska det också tas ställning till sådana väsentliga krav på informationssystem av klass A som är väsentliga för förmedlarens verksamhet (allmänna krav på användningsmiljön), framför allt om till dem hänför sig användningsmiljöspecifik konfigurering eller anvisningar som förmedlaren ansvarar för i den anlitade Kanta-förmedlingstjänsten.

FÖRHÅLLANDET MELLAN KANTA-ANSLUTARENS EGENKONTROLL OCH FÖRMEDLARE OCH FÖRMEDLINGSSERVICE

Producenten av social- och hälsovårdstjänster ansvarar i sista hand för att verksamheten överensstämmer med bestämmelserna. I producentens egenkontroll beskrivs vid behov hur de krav uppfylls i användningsmiljön som inte får något svar i förmedlarens egenkontroll eller förmedlingsservicens certifiering.

Kanta-anslutaren ska anlita en certifierad förmedlingstjänst, om Kanta-anslutningsmodellen är modell 3 (externaliserad anslutningspunkt) och för att upprätta anslutningspunkten anlitat en förmedlingstjänst där man hanterar icke-krypterade klient- och patientuppgifter. Förmedlaren kan administrera anslutningspunkten.

Om modell 1,2 eller 4 används som Kanta-anslutningsmodell, ska det system som används eller den egna integrationslösningen uppfylla de certifieringskrav som riktas mot förmedlingsservicen och ha genomgått extern auditering.

I Kanta-anslutningspunkten ska användas certifiering enligt vad som beskrivs ovan och en informationssäkerhetsauditerad förmedlingstjänst eller ett system som uppfyller dessa krav.

Om en aktör som ansluter sig till tjänsterna själv ansvarar för hela sin förmedlingsservice helhet, så ansvarar denna aktör också för certifiering och informationssäkerhetsauditering av förmedlingsservicen. Ingen extern förmedlare eller separat plan för egenkontroll för förmedlaren krävs.

En extern förmedlare som används för att upprätta Kanta-anslutningspunken ska uppfylla kraven i punkten ”förmedlares egenkontroll och registrering”. Genom förmedlarens eller Kanta-anslutarens planer för egenkontroll är det möjligt att beskriva och verifiera även krav som uppfylls genom avtal med tredje parter.

Avdelningen för informationstjänster
Enheten för styrning av den operativa
Verksamheten (OPER)

3.6.2015

OMSTÄNDIGHETER SOM SKA BEAKTAS I FÖRMEDLINGSSERVICE OCH ANSLUTNINGSPUNKTER

Den certifierade förmedlingstjänst som en producent av social- och hälsovårdstjänster anlitar kan tillhandahållas av en aktör medan en annan aktör kan vara förmedlare. Då, om inte något annat överenskoms,

- ansvarar upprättaren av förmedlingsservice för auditeringen av informationssäkerheten/certifieringen samt eventuellt, om upprättaren är förmedlare, för de krav på förmedlarens egenkontroll som då är relevanta
- ansvarar förmedlaren genom egenkontrollen för att det säkerställs att kraven på användningsmiljö uppfylls och i allmänhet för till exempel ansökan om certifikat
- ansvara för helheten i sista hand producenten av social- och hälsovårdstjänster, som genom avtal och sin egen egenkontroll ska säkerställa att alla krav uppfylls.

Det är till exempel möjligt att avtala om följande omständigheter på olika sätt i olika användningsmiljöer, också i fråga om en enskild Kanta-förmedlingstjänst kan det finns olika praktiska modeller för olika användningsmiljöer:

- den aktör som ansvarar för ansökan om och administrering av certifikat och chiffernycklar (som ofta fungerar som förmedlare, men också kan vara Kanta-anslutaren)
- den aktör som i sin plan för egenkontroll beskriver den egenkontroll som hör till anslutningspunkten och dess förhållande till producenterna av social- och hälsovårdstjänsters planer för egenkontroll samt till certifieringen av förmedlingsservicen (förmedlaren eller Kanta-anslutaren)
- hur det säkerställs att informationssäkerhet och konfidentialitet för klientuppgifter säkerställs till exempel i samband med underhållsåtgärder
- på vilka sätt konfigureringen av den lokala användningsmiljön och maskinsalstjänster har ordnats.

Det servercertifikat som certifikatutfärdaren för hälso- och sjukvården utfärdar kan vara i antingen Kanta-anslutarens eller förmedlarens namn. Om förmedlaren upprättar en gemensam anslutningspunkt och tjänster i anslutning till den för flera Kanta-anslutare skaffas servercertifikatet i förmedlarens namn (se Tekniska Kanta-anslutningsmodeller).

Om flera olika producenter av social- och hälsovårdstjänster ansluter sig till Kanta-tjänsterna via samma förmedlare ska de med förmedlaren komma överens om även ansvaret för verifiering av att förmedlingsservicen stämmer överens med kraven, för produktion och utnyttjande av förmedlingsservicen samt kraven på användningsmiljöns egenkontroll i anslutning till anslutningspunkten och förmedlingsservicen.

Om Kanta-anslutningspunkten upprättas direkt via informationssystemet, ska systemet uppfylla kraven på förmedlingsservice och dessa krav ska verifieras som en del av certifieringen av informationssystemet och auditeringen av informationssäkerheten. Apotek och andra som använder servicen med egen anslutningspunkt svarar själva för sina certifikat,

om de inte har ingått avtal med en extern förmedlare. Anslutningen kan då ske till exempel direkt från ett certifierat informationssystem som man förfogar över själv via internet eller ett slutet kundnät. Eventuell förmedling av datakommunikationen via en extern samlingspunkt förutsätter inte extern auditering av samlingspunkten. Om det tekniska upprättandet av anslutningspunkten är en del av det använda systemet (till exempet apotekets informationssystem), verifieras certifieringskraven på förmedlingsservicen i tillämpliga delar som en del av certifieringen av systemet.

Om det är möjligt att kryptera klient- och patientuppgifter som personer (så som upprätthållare) som är verksamma i informationssystem som är anslutna till Kanta-tjänsterna kan läsa, bör man i första hand eftersträva detta. Om kryptering inte är möjlig, bör man särskilt ombesörja kraven på hantering och begränsning av behörigheter, uppföljning av användningen och stark autentisering och hur det garanteras att klientuppgifterna är konfidentiella.

Som förmedlare definieras inte en organisation som endast fungerar som routare eller samlingspunkt för SSL/TLS-krypterad datakommunikation och som inte kan se icke-krypterade patientuppgifter. På motsvarande sätt är en tjänst eller ett program som enbart används vid routning av krypterad datakommunikation eller som samlingspunkt för datakommunikation inte Kanta-förmedlingsservice.

Om producenten av en informationssystemtjänst (till exempel som tillhandahåller ett molnbaserat informationssystem eller en SaaS-informationssystemtjänst) upprättar en Kanta-anslutningspunkt och dess verksamhet uppfyller kriterierna på förmedlare, ska producenten registera sig som *förmedlare* och utarbeta en plan för egenkontroll. Dessutom är det möjligt att verifiera att kraven på certifiering av *förmedlingsservicen* är uppfyllda i samband med certifiering av krav på andra informationssystem av klass A. Det är emellertid också möjligt att utföra certifieringen separat från ansökan om att fungera som förmedlare.

Om kriterierna på förmedlare uppfylls i samband med att maskinsalstjänster tillhandahålls ska det beskrivas hur kraven på maskinsalstjänstens egenkontroll och användningsmiljö har uppfyllts och de ska kunna verifieras i enlighet med beskrivningen ovan (genom registrering av en befintlig förmedlare eller en ny förmedlare eller genom egenkontroll för producenten av social- och hälsovårdstjänster). Av den som producerar maskinsalstjänsten förutsätts inte extern auditering av informationssäkerheten, om det går att beskriva och verifiera att kraven på egenkontroll och användningsmiljö uppfylls genom ovannämnda aktörers planer för egenkontroll. Om produktionen av maskinsalstjänster är en del av en informationssystems- eller förmedlingsservicehelhet som ska certifieras är verifieringen av väsentliga informationssäkerhetskrav ett led i certifieringsprocessen och auditeringen av informationssäkerheten.

Vesa Jormainen
Enhetschef

Avdelningen för informationstjänster
Enheten för styrning av den operativa
Verksamheten (OPER)

3.6.2015

Juha Mykkänen
Utvecklingschef

Sändlista	Tillhandahållare av hälso- och sjukvårdstjänster Apotek Tillverkare av patientdatasystem Upprättare av Kanta-förmedlingsservice Kanta-förmedlare Bedömningsorgan för informationssäkerhet FPA/Enheten för Kanta-tjänster
För kännedom	SHM / registratorskontoret, Teemupekka Virtanen Valvira / registratorskontoret, Heikki Mattlar, Maijaliisa Aho Kommunikationsverket Finlands Kommunförbund rf / registratorskontoret