

Kanta-palvelujen tieto- ja sanomaliikenteen tietoturvavaatimukset

Ohje

Kanta-palvelut

10.9.2026

Muutoshistoria

Versio	Muutos	Tekijä	PVM
1.06	Hyväksytty versio	Kanta-palvelut	14.12.2015
1.07	Dokumenttipohja uusittu. Päivitetty muuttuneet toimijat ja linkit. Tarkennettu vaatimuksia ja suosituksia	Kanta-palvelut	2.1.2024
1.08	Tarkennettu DVV:n 1.10.2026 tapahtuvan varmenneuudistuksen ohjeistusta Kanta-palveluihin liityttäessä.	Kanta-palvelut	10.9.2026

Sisällys

Muutoshistoria	1
1 Johdanto.....	3
2 Liittyvät ohjeet ja dokumentit.....	3
3 Määritelmät.....	3
3.1 Päästä päähän yhteys	4
3.2 Sisäverkon yhteys	4
3.3 Kanta-osoitehakemisto	4
3.4 SOTE- ja hyvinvointisovellusvarmenteet	4
4 Sanomaliikenteen tietoturva-vaatimukset	5

1 Johdanto

Tässä dokumentissa kuvataan keskeisimmät Kanta-palveluissa (myöhemmin tässä dokumentissa Kanta) käytössä olevat tietoturvaan liittyvät vaatimukset ja suositukset kommunikoitaessa Kantaan. Tietoturva-vaatimukset rajaavat Kantaan yhteydessä olevien tahojen hyödyntämien laitteiden ja ohjelmistojen konfiguraatioita esimerkiksi käytettyjen standardien ja profiilien, avainpituuksien sekä tiivistefunktioiden osalta. Osittain näistä varmistutaan Kanta-palveluihin liittyvien järjestelmien sertifiointimenettelyllä ja osa tarkistuksista on ohjelmallisia kunkin yhteydenoton yhteydessä (siltä osin kuin tarkistus voidaan tehdä Kanta-rajapinnassa). Tarkkojen hyväksyttävien tiivistefunktioiden, avainpituuksien ym. osalta nojataan Kyberturvallisuuskeskuksen TL IV - vähimmäisvaatimuksiin ja keskeisimpien osalta ne toistetaan tässä dokumentissa.

2 Liittyvät ohjeet ja dokumentit

[Sertifiointi, olennaiset vaatimukset ja tietoturvasuunnitelma \(Kanta.fi\)](#)

[Tekniset liittymismallit Kanta-palveluihin \(Kanta.fi\)](#)

[Sähköisen allekirjoituksen määrittäminen ja soveltamisohje \(Kanta.fi\)](#)

[Palveluvarmenteet | Digi- ja väestötietovirasto | Digi- ja väestötietovirasto](#)

[TLS cipher suites turvallisuusluokille IV-III \(kyberturvallisuuskeskus.fi\)](#)

- Kanta-palveluissa TLS-avaimistoille ja algoritmeille vähimmäisvaatimuksena on TL IV -mukaiset suositukset

[Kryptografiset vahvuusvaatimukset - kansalliset turvallisuusluokat 1.pdf](#)

- Kanta-palveluissa allekirjoitusavaimistolle vähimmäisvaatimuksena on TL IV -mukaiset suositukset.

3 Määritelmät

Keskeiset Kanta-liittymän järjestämiseen liittyvät käsitteet on seuraavia tarkennuksia lukuun ottamatta kuvattu Tekniset liittymismallit Kanta-palveluihin -dokumentissa.

3.1 Päästä päähän yhteys

Päästä päähän -yhteydellä tarkoitetaan apteekki-, asiakas- tai potilastietojärjestelmän ja Kannan välistä sanoma- ja tietoliikenneyhteyttä. Tämä yhteys voi kulkea Kanta-liityntäpisteen kautta ja muodostua useista erillisistä tietoliikenneyhteyksistä. Liityntäpisteen ja Kannan väliselle tietoliikenneyhteydelle asetetut sanomaliikenteen salausta ja sen osapuolten tunnistamista koskevat vaatimukset koskevat myös kaikkia muita päästä päähän -yhteyteen sisältyviä tietoliikenneyhteyksiä. Esim. liittyjän tietojärjestelmän ja Kanta-välittäjän liityntäpisteen välinen tietoliikenneyhteys pitää salata ja sen osapuolet tunnistaa samantasoisella menettelyllä kuin liityntäpisteen ja Kannan välinen yhteys.

3.2 Sisäverkon yhteys

Sisäverkon yhteydellä tarkoitetaan tässä yhteydessä liittyjän reunareitittimien sisäpuolella olevaa lähiverkkoa. Operaattorin runkoverkon kautta kulkevat yhteydet eivät ole sisäverkon yhteyksiä, vaikka ne olisi toteutettu yksityisen verkon yhteytenä.

3.3 Kanta-osoitehakemisto

Kanta-osoitehakemisto on osa Kanta-palvelujen pääsynhallintaa. Osoitehakemistoon tallennetaan liittyjän, liittyjän käyttämien liityntäpisteiden ja liittyjälle sallittujen palvelujen tiedot. Osoitehakemistoon lisättävät tiedot kerätään liittyjiltä liittymishakemuksella, ja tietoja muutetaan tilanteen muuttuessa esimerkiksi silloin, jos liittyjä alkaa käyttää Kanta-palveluja uuden liityntäpisteen kautta.

3.4 SOTE- ja hyvinvointisovellusvarmenteet

Kanta-palveluun liitettyssä tietoliikenneyhteydessä käytetään DVV:n tuottamia SOTE- tai hyvinvointisovelluspalveluvarmenteita. Varmennetta käytetään tietoliikenteen salaamisessa ja liityntäpisteen tunnistamisessa.

DVV myöntää 30.09.2026 saakka Kanta -liityntää varten SOTE- ja Hyvinvointisovelluspalvelinvarmenteita. Näissä varmenteissa "Extended Key Usages" -kentässä on määritetty käyttötarkoituksiksi "Server Authentication" ja "Client Authentication". Ennen 1.10.2026 myönnettyjä varmenteita voi käyttää koko varmenteen voimassaolon ajan.

1.10.2026 alkaen DVV:n varmennemuutokset luovat kaksi eri varmennetyyppiä:

- SOTE-palvelinvarmenne, jota käytetään palvelimissa, joihin muut palvelimet tai asiakkaat ottavat yhteyttä. Näissä varmenteissa "Extended Key Usages" -kentässä on määritetty käyttötarkoitukseksi "Server Authentication".
- SOTE-asiakasvarmenne, jota käytetään palvelimissa, jotka ottavat yhteyttä yllä mainittuihin palvelimiin. Näissä varmenteissa "Extended Key Usages" -kentässä on määritetty käyttötarkoitukseksi "Client Authentication".

Kanta-palveluun yhteyttä ottavan liityntäpisteen varmenne tulee olla SOTE-asiakasvarmenne.

Hyvinvointisovellukset ottavat yhteyttä Kanta-palveluihin hyvinvointisovellusasiakasvarmenteella.

SOTE- ja hyvinvointisovellusvarmenteet on kuvattu DVV:n [Palveluvarmenteiden tekniset tiedot -dokumentin](#) luvuissa 2.6, 2.8, 2.9 ja 2.10.

4 Sanomaliikenteen tietoturva-vaatimukset

Sanomaliikenteelle asetetaan seuraavat vaatimukset:

1. Liikenne liityntäpisteen ja Kannan välillä salataan ja osapuolet tunnistetaan TLS-tekniikalla (vähintään TLS-versio 1.2) käyttäen DVV:n myöntämiä varmenteita.
2. Palvelinvarmenteissa on käytettävä Traficomin TLS-salausvahvuussuositusten mukaisia avainpituuksia ja salausalgoritmikombinaatioita. Kannan ja liityntäpisteen välisessä liitynnässä käytetään vähintään Kansallisen turvallisuusluokan TL IV -vaatimusten mukaisia salausalgoritmikombinaatioita (cipher suites). Suositusten mukainen minimiavainpituus RSA-algoritmille on 3072 bittiä ja EC-algoritmille 256 bittiä. Tällä hetkellä Kannan käytössä olevat salausalgoritmikombinaatiot (cipher suites) saa tarvittaessa Kannan asiakastuesta, tekninentuki@kanta.fi. Kela pidättää oikeuden päivittää käytössä olevien algoritmien ja avainpituuksien listausta tarpeen mukaan esimerkiksi kyberturvallisuuskeskuksen tietoturvaohjeisiin pohjautuen. Näistä muutoksista informoidaan tarpeen ilmetessä välittömästi. Normaalin muutosmenettelyn mukaisia etukäteisilmoitusajkoja ei kuitenkaan välttämättä

noudateta. Tavallisesti muutokset pyritään yhdistämään varmenteiden uusimisprosessien yhteyteen.

3. Sähköisen allekirjoituksen osalta noudatetaan [Sähköisen allekirjoituksen määrittäminen ja soveltamisohjeessa](#) esitettyjä vaatimuksia käytettävien salausalgoritmien ja tiivistefunktioiden osalta. Sähköisissä allekirjoituksissa käytetään vähintään Kansallisen turvallisuusluokan TL IV -vaatimusten mukaisia tiiviste- ja allekirjoitusalgoritmeja sekä avainpituuksia. Suositusten mukainen minimiavainpituus RSA-algoritmilta on 3072 bittiä ja EC-algoritmilta 256 bittiä.
4. Varmennepohjaisesti tunnistauduttaessa tai allekirjoituksia tarkistettaessa on varmenteen voimassaolo varmentajan sulkulistaa vasten tarkistettava. Varmenteen on oltava voimassa eikä se saa olla sulkulistalla allekirjoitushetkellä.
5. Kanta-osoitehakemistoon on määriteltä liittymällä oikeudet käyttää palveluja käytössään olevien liittymäpisteiden kautta. Oikeudet lisätään Kanta-palveluissa liittymän tekemän liittymishakemuksen tai muutoilmoituksen perusteella.
6. Kanta-palveluihin liittyvät potilas-, asiakastieto- tai apteekkijärjestelmät tulee olla luvitettu Tekniset liittymismallit Kanta-palveluihin -ohjeen mukaisesti.
7. Asiakasvarmenteen subject/serialNumber-kentän OID-koodi yksilöi liittymäpisteen ja sen tulee vastata Kanta-osoitehakemiston tietoja.
8. Mikäli liittymäpiste ei ole liittymän omassa hallinnassa, on huomioitava seuraavat vaatimukset:
 - a. Liikenne liittymän asiakastieto-, potilastieto- tai apteekkijärjestelmältä liittymäpisteelle tulee salata vähintään vastaavan tasoisella menetelmällä (TLS) siltä osin kuin se kulkee muualla kuin liittymän sisäverkossa (esimerkiksi operaattorin runkoverkko, vaikka käytössä olisi operaattorin yksityisen verkon yhteys).
 - b. Sanomaliikenteen kaikkien osapuolten identiteetti tulee varmentaa. Varmennaminen on pakollista organisaatioiden välisessä tiedonsiirrossa, jossa käytetään muita kuin sisäverkon yhteyksiä. Tapauksissa, joissa potilastieto-, ja asiakastieto-tai apteekkijärjestelmien palvelimet sijaitsevat

samassa konesaliympäristössä tiedonsiirtoon hyödynnettävien erillisten laitteistojen kanssa (kuormantasaajat, SSL-kiihdyttimet tms.) sekä mahdollisen liityntäpisteen kanssa, ei varmennepohjainen tunnistaminen näiden välillä ole pakollista. Tämä kuitenkin edellyttää, että konesalin ja käyttöympäristön sisäisestä tietoturvasta on huolehdittu sosiaali- ja terveydenhuollon tietojärjestelmien olennaisten tietoturva vaatimusten mukaisesti.

- c. Liityntäpisteen toteuttajan tulee varmistaa, että sanoma on lähetetty oikean tahon nimissä (eli HL7-sanoman controlActProcess / authorOrPerformer / assignedPerson / assignedPerson / representedOrganization / id vastaa edellisen kohdan mukaisesti varmennettua identiteettiä).
 - d. Kanta-välittäjä ilmoittautuu THL:n Kanta-välittäjärekisteriin ja laatii tietoturvasuunnitelman, jonka avulla suunnitellaan ja varmistetaan tietoturvan ja asianmukaisen asiakastietojen hallinnan toteutuminen.
9. Kaikkien Kanta-sanomaliikenteeseen liittyvien tahojen tulee suojata liityntäpistesijaintinsa ja tietojärjestelmien käyttöympäristöt tilallisella palomuurilla tai sovelluspalomuurilla.
10. Kantaan suoraan tai välillisesti yhteydessä olevien palvelinten aika tulee olla synkronoitu Suomen viralliseen aikaan (VTT MIKES ylläpitää virallista [Suomen ajan NTP](#)-aikapalvelua). Julkisen NTP-palvelun käyttö katsotaan myös riittäväksi.