

**HL7 Finlandin suositus turvallisesta HL7 v2-liikenteestä**

**Versio 1.0**

**20.12.2024**

**URN:OID: 1.2.246.777.11.2024.7**

Versiohistoria

|  |  |  |  |
| --- | --- | --- | --- |
| Päiväys | Versio | Tekijä | Kuvaus |
| 26.8.2024 | 0.1 | Timo Tarhonen | Ensimmäinen luonnos TC:tä varten. |
| 28.8.2024 | 0.2 | Timo Tarhonen | Uusi versio TC:n kommenttien perusteella |
| 2.9.2024 | 0.21 | Timo Tarhonen | Täsmennyksiä. Kommentointiversio. |
| 9.12.2024 | 0.3 | Timo Tarhonen | Varmenteiden myöntäjä-kappaleeseen muutos ja uusi kappale viestin salaus. Muokattu johdantokappaletta. |
| 20.12.2024 | 1.0 | Timo Tarhonen | Siirretty kappale 8 sanoman siirto salattuna omaksi dokumentikseen. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Sisällysluettelo

[1 Johdanto 4](#_Toc186196853)

[2 Siirtotavat 4](#_Toc186196854)

[3 TLS-salauksen versio 4](#_Toc186196855)

[4 Vähimmäisjärjestely 4](#_Toc186196856)

[5 Normaalijärjestely 4](#_Toc186196857)

[6 Varmenteiden myöntäjä 5](#_Toc186196858)

[7 HL7 Finland suositus 5](#_Toc186196859)

[8 Sanoman täydellinen salaaminen myös välityspalveluilta 5](#_Toc186196860)

# Johdanto

Virallinen HL7 v2-määritys ei ota kantaa liikenteen salaukseen ja tietoturvaan. Liikenteen salaus on kuitenkin suositeltavaa. HL7 Finlandilta on kysytty asiasta, joten asiasta on tehty suositus.

Perinteinen v2-liikenne on käytössä etenkin laboratorioliikenteessä, kuvantamisen liikenteessä ja potilaan perustietojen siirrossa. Tämä suositus soveltuu myös hoitolähete/hoitopalauteliikenteeseen (pikaxml).

Turvallisesta tietoliikenteestä löytyy kattavia määrityksiä, joten tämän dokumentin tarkoitus ei ole kuvata teknisiä mahdollisuuksia kattavasti. Tarkoitus on määritellä, kuinka HL7-liikenteen turvatason nostamisessa päästään alkuun. Oletuksena on, että tietoliikenneyhteydet ovat jo perusturvallisia eivätkä kulje yleisen internetin kautta.

# Siirtotavat

Yleisimmin HL7 v2 liikennettä siirretään TCP/IP-socketin kautta (MLLP-siirto) ja joissakin tapauksessa tiedostosiirtona.Tiedostosiirrossa kannattaa käyttää SFTP:tä ja TCP/IP-socketin tapauksessa TLS-salausta.

# TLS-salauksen versio

TLS-salauksessa pitää käyttää vähintään versiota TLS1.2. Joissakin tapauksissa TLS1.3 on jo käytössä. TLS-salauksen käyttö terveydenhuollossa on tuttua KANTA-liikenteen vuoksi.

# Vähimmäisjärjestely

Lähettävässä päässä käytetään asiakasvarmennetta ja vastaanottopäässä palvelinvarmennetta. Lähettäjä ja vastaanottaja luottavat toistensa varmenteisiin ilman tarkistuksia. Varmennetta tarvitaan kumppanin todentamiseen sekä salauksessa ja salauksen purussa tarvittavan yhteyskohtaisen symmetrisen istuntoavaimen siirtoon.

Vaikka järjestely onkin yksinkertainen, tämäkään tapa ei ole yleisesti käytössä, mutta siitä on hyvä aloittaa. Onhan liikenne sentään salattua.

# Normaalijärjestely

Vähimmäisjärjestelyn lisäksi lähettäjä tarkistaa vastaanottajan palvelinvarmenteen:

1. varmennepolun
2. voimassaolon
3. estolistalla olon

Vastaavasti vastaanottaja tarkistaa lähettäjän asiakasvarmenteen:

1. varmennepolun
2. voimassaolon
3. estolistalla olon

Varmennepolun tarkistaminen tarkoittaa sitä, että väli- (intermediate) ja juuri- (root) varmenteiden voimassaolo tarkistetaan myös ja noiden varmenteiden pitää löytyä omasta luotettujen varmenteiden varastosta. Yleensä TLS-konfiguraatioissa tämä kuuluu perustoiminnallisuuteen.

Tämä järjestely edellyttää, että (omien) varmenteiden voimassaolon valvonta on automatisoitu.

Estolistalla olon tarkistus voi vaatia räätälöintia.

(Vielä tiukemmalla tasolla voi tarkistaa myös varmenteen sarjanumeron.)

# Varmenteiden myöntäjä

Varmenteita on siis kahdentyyppisiä: asiakasvarmenne ja palvelinvarmenne.

Olisi hyvä, mutta ei pakollista, että palvelinvarmenteen myöntäjä olisi oma organisaatio. Tässä sopiva taho (CA) on hyvinvointialue tai DVV. Useassa integraatioalustassa on jo DVV:n myöntämä asiakasvarmenne KANTA-liikenteen vaatimuksien vuoksi. Kyseistä varmennetta voi käyttää myös palvelinvarmenteena.

Asiakasvarmenne pitää hakea vastaanottajan määrittelemältä myöntäjältä.

Terveydenhuollon toimijoilla on omat varmennepolitiikkansa, joten asiaa ei tässä avata syvällisemmin.

# HL7 Finland suositus

Ensimmäisessä vaiheessa otetaan käyttöön vahimmäisjärjestely (kappale 4), koska se on melko vaivaton.

Samalla aloitetaan varautuminen normaalijärjestelyn käyttöönottoon.

# Sanoman täydellinen salaaminen myös välityspalveluilta

Tästä asiasta on tehty oma erilinen määrityksensä: ”HL7 v2-liikenteen täydellinen salaaminen”.