

**HL7 Finlandin selvitys täydellisesti salatusta HL7 v2-liikenteestä**

**Versio 1.0**

**OID: 1.2.246.777.11.2025.2**

**23.6.2025**

**Työdokumentti**

Versiohistoria

|  |  |  |  |
| --- | --- | --- | --- |
| **Päiväys** | **Versio** | **Tekijä** | **Kuvaus** |
| 27.12.2024 | 0.1 | Timo Tarhonen | Tämä asia on siirretty omaan dokumenttiinsa 17.12.2024 HL7 TC-kokouksen jälkeen ja samalla sisältöä on selkeytetty. |
| 18.6.2025 | 0.2 | Timo Tarhonen | Kommenttikierrokselta ei kommentteja. Hyväksytty työdokumentiksi 10.6.2025 TC-kokouksessa. |
| 23.6.2025 | 1.0 | Timo Kaskinen | Versio julkaistavaksi, lisätty oid |

Sisällysluettelo

[1 Johdanto 4](#_Toc186527651)

[2 HL7 v2-sanoman siirto salattuna 4](#_Toc186527652)

[3 Tietojen sijoittelu OBR- ja OBX-tietoryhmiin 5](#_Toc186527653)

[4 Salauksen soveltamistapa 5](#_Toc186527654)

[5 Esimerkki 6](#_Toc186527655)

[6 Yhteenveto 6](#_Toc186527656)

# Johdanto

On tuotu esiin tarve siirtää sanoma salattuna siten, että välissä olevat integraatioalustat osaavat reitittää sanoman, mutta eivät näe varsinaista hyötykuormaa. Tällöin luottamuksellista tietoa ei jää välityspalvelimien lokeihin, tietokantoihin ja varmuuskopioille.

Lähettäjä

välittäjä

vastaanottaja

salattu

sanoma

salattu

sanoma

Tähän tarpeeseen ei ole vielä löytynyt valmista määritystä. Toisaalta tarve on tässä vaiheessa teoreettinen. Käytännössä kuitenkin hyökkäysvektorit kohdistuvat välityspalvelimiin, joissa on useita portteja avoinna.

Tämä määritys keskittyy siis varsinaisen sanoman salaamiseen. Turvallisesta tietoliikenteestä on oma dokumenttinsa. Turvallisessa tietoliikenteessä tietoliikenneyhteys salataan asiakasvarmenteen avustuksella. Tässä määrityksessä vastaanottajan varmenteen julkista avainta käytetään varsinaisen sanoman salaamiseen siten, että se ei ole nähtävissä edes välityspalvelimissa. Tämä määritys ei ota kantaa siihen, onko tietoliikenneyhteys salattu vai ei.

# HL7 v2-sanoman siirto salattuna

Alkuperäinen salattu sanoma siirretään siirtosanomalla, jonka välityspalvelimet pystyvät reitittämään MSH-segmentin avulla.

Alkuperäinen salattu sanoma siirretään siirtosanoman OBX-5 komponentissa Base64-koodattuna.

Esimerkki Base64-koodatun tiedon siirrosta HL7 v2-sanomassa on CDA R2-standardissa, siellä on käytetty TXA-sanomaa. Toinen esimerkki on HL7-Finlandin radiologian sanomien soveltamisoppaassa 1.50, kappale 3.1.6.6. Käytetty sanoma on ORM.

Tämä määritys ehdottaa, että alkuperäinen salattu sanoma voidaan siirtää käyttämällä siirtosanomana ORU^R01-sanomaa. Alkuperäinen sanoma voi olla mikä tahansa HL7 v2-sanoma.

MSH:n lisäksi siirtosanomassa on pakollinen OBR-segmentti ja salattu sanoma OBX:ssä. Tällöin sanoma menee validoinnista läpi.

Sanoma ORU^R01:

MSH

OBR

OBX

# Tietojen sijoittelu OBR- ja OBX-tietoryhmiin

OBR-tietoryhmässä on pakollinen OBR-4 service id.

OBR-4: alkuperäisen sanoman id eli MSH-9.

OBX-1: juokseva numero, yleensä vain yksi OBX-segmentti

OBX-2: tietotyyppi ED

OBX-3: Käytetyn salaussertifikaatin Subject

OBX-4: Käytetyn salaussertifikaatin Serial number

OBX-5-2: AP (ED-2)

OBX-5-4: Base64 (ED-4)

OBX-5-5: Salattu alkuperäinen sanoma Base64-koodattuna MIME-kehyksessä (ED-5)

# Salauksen soveltamistapa

Jos salatun sanoman koko on yli 65k, niin tarvitaan useampi OBX-segmentti. Numerointi aloitetaan arvosta 1. Kussakin OBX-segmentissä on vain yksi MIME-kehys. Vastaanottopäässä OBX-segmenteistä otetaan pois MIME-kehykset ja Base64-osuudet liitetään toisiinsa, Base64 koodaus puretaan ja sanoman salaus puretaan. Salauksen yksityiskohdista sovitaan alkuperäisen lähettäjän ja lopullisen vastaanottajan välillä ennen liikenteen aloittamista.

Lähettäjä salaa sanoman vastaanottajan julkisella avaimella. Vastaanottaja purkaa salauksen julkista avainta vastaavalla yksityisellä avaimella.

# Esimerkki

MSH|...

OBR|...

OBX|1|ED|474131417414WYZ|785565546221293838|

^AP^^Base64^

MIME-Version: 1.0

Content-Type: text/plain; boundary="HL7-Secret-boundary";

type="text/plain";

Content-Transfer-Encoding: BASE64

--HL7-Secret-boundary

Content-Type: text/plain; charset="ISO-8859-1"



--HL7-Secret-boundary

# Yhteenveto

Tässä dokumentissa ei ole kehitetty mitään uutta salausmenetelmää, vaan kyseessä on soveltamistapa, kuinka hyödynnetään olemassa olevia menetelmiä. Base64-koodaus, Base64-koodauksen purku, alkuperäisen sanoman salaus ja salauksen purku tehdään olemassa olevilla kirjastofunktioilla.