Laki julkisen hallinnon tiedonhallinnasta, luonnos 13.10.2020 Suosituskortti	B
14 § 1 mom Tietojen siirtäminen yleisessä tietoverkossa	versio 0.9

14 § 1 mom kohta 1 Tietojen siirto

Viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä.

Perustelumuistio
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx

Yleinen tietoverkko tarkoittaa organisaation oman hallinnan ulkopuolisia verkkoalueita, esimerkiksi internetiä tai operaattorien tarjoamia MPLS-verkkoyhteyksiä. Koska yleiset tietoverkot ovat lähtökohtaisesti turvattomia, tulee niissä siirrettävä tieto olla salattua.

Salassa pidettävät viranomaisen asiakirjat määritellään viranomaisen toiminnan julkisuudesta annetussa lain (621/1999, julkisuuslaki) 24 §:ssä. Joissain erityislaeissa voi myös olla salassapitosäännöksiä. Salassa pidettävä asiakirja voi olla myös turvallisuusluokiteltu, mikäli se täyttää tiedonhallintalain (906/2019) 18 §:ssä määritellyt turvallisuusluokittelun edellytykset.

Tietoliikenteen salaus

Ensisijaisesti salaus toteutetaan tietoliikenteen vahvalla salauksella. Vahvalla salauksella tarkoitetaan yleisesti hyväksyttyä ja laajalti käytettyä salausratkaisua, jossa ei ole tunnettuja haavoittuvuuksia. Esimerkiksi kirjoitushetkellä HTTPS-protokolla TLS-salausprotokollan versiolla 1.2 tai uudempi täyttää tämän vahvan salauksen määritelmän, vanhemmilla TLS- tai SSL-versioilla ei.

Tietoliikenne tulisi ideaalitilanteessa salata päästä päähän, eli esimerkiksi käyttäjältä tietojärjestelmään tai kahden tietojärjestelmän välillä esimerkiksi HTTPS- tai SFTP-protokollilla. Mikäli tämä ei ole mahdollista, voidaan organisaatioiden verkkojen välinen yleisen tietoverkon osuus salata esimerkiksi VPN-ratkaisuilla, jolloin organisaatioiden sisäisten verkkojen osuus jää salaamatta.

Lakitekstissä puhutaan salassa pidettävästä tiedosta ja yleisestä tietoverkosta. Nykymaailmassa kannattaa kuitenkin lähtökohtaisesti teknisesti käsitellä kaikkea tietoa kuin se olisi salassa pidettävää, ja salata tietoliikenneyhteydet oletusarvoisesti aina. Vastaavasti organisaatioiden omia verkkoja kannattaa käsitellä turvattomina verkkoina ja salata samojen periaatteiden mukaan liikenne myös siellä. Esimerkiksi avoimen HTTP-protokollan käyttöä sisäverkon julkistakin tietoa käsittelevissä järjestelmissä tulisi ehdottomasti välttää.

Tietojen salaus ilman tietoliikenteen salausta

Mikäli tietoliikennettä ei kyetä salaamaan, siirrettävien tietojen salaus voidaan toteuttaa siirrettävien tietojen/tiedostojen tasolla. Esimerkiksi sähköpostiviestin tai sen liitetiedostojen salaaminen mahdollistaa viestinvälityksen myös salaamattomien verkkojen yli. Tällöin salatun viestin tai tiedoston saa auki erillisellä salasanalla (toteutuksesta riippuen mahdollisesti PIN-koodi tai kertakäyttösalasana). Tämän salasanan toimittaminen vastaanottajalle ei saa tapahtua samaa reittiä kuin itse salattu tieto kulkee.

Viittaus, lisätietoja:

Laki julkisen hallinnon tiedonhallinnasta, luonnos 13.10.2020 Suosituskortti	B
14 § 1 mom Tietojen siirtäminen yleisessä tietoverkossa	versio 0.9

	• Tiedonhallintalautakunnan suositus salassa pidettävästä tiedosta syksyllä 2020 (ei vielä julkaistu) • Tiedonhallintalautakunnan suositus turvallisuusluokiteltavien asiakirjojen käsittelystä, 2.4.2020 tai sen päivitetty versio syksyllä 2020 (ei vielä julkaistu).
V	Lisätietoa turvaluokitellun tiedon suojaamiseen soveltuvasta salauksesta: • Kyberturvallisuuskeskus, Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset suojaustasot, 28.11.2018: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf • Kyberturvallisuuskeskus, Liikenne- ja viestintävirasto Traficomin suorittamat salaustuotearvioinnit ja -hyväksynnät, 6.3.2020 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-salaustuotearvioinnit-ja-hyvaksynnat.pdf • Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut, 1.7.2020: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf