Laki julkisen hallinnon tiedonhallinnasta (906/2019) **Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa** **Suosituskortti**	
Tiedonhallintalain 14§ Tietojen siirtäminen tietoverkoissa Turvallisuusluokitusasetuksen 11§ Salausratkaisut	versio 0.9/27.11.2019

Tiedonhallintalain 14 § Tietojen siirtäminen tietoverkossa

Viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja.

Käyttäjän tunnistamisesta yleisölle tarjottavissa digitaalisissa palveluissa säädetään digitaalisten palvelujen tarjoamisesta annetussa laissa (306/2019).

Turvallisuusluokitusasetuksen 12 § Asiakirjan siirtäminen tietoverkon kautta

Salassa pidettävien tietojen siirtämisestä yleisessä tietoverkossa säädetään tiedonhallintalain 14 §:ssä. Turvallisuusluokiteltuja asiakirjoja saa siirtää muussa kuin yleisessä tietoverkossa viranomaisen turvallisuusalueiden ulkopuolelle tai kyseistä turvallisuusluokkaa alemman turvallisuustason tietojärjestelmän tai tietoliikennejärjestelyn kautta vain salatussa muodossa. Jos turvallisuusluokiteltujen asiakirjojen siirtäminen tapahtuu turvallisuusalueella muussa kuin yleisessä tietoverkossa ja tietojen riittävä suojaus voidaan toteuttaa fyysisen suojaamisen menetelmin, voidaan käyttää salaamatonta siirtoa tai alemman turvallisuustason salausta.

Turvallisuusluokitusasetuksen 11.1 § kohta 7 Salausratkaisut

Turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyt tietojärjestelmät ja tietoliikennejärjestelyt on toteutettava siten, että:

7) käytetyt salausratkaisut ovat tietojärjestelmässä tai tietoliikennejärjestelyssä käsiteltyjen asiakirjojen turvallisuusluokka huomioon ottaen riittävän turvallisia.

Erityisesti liikennöitäessä julkisen tai matalamman turvallisuusluokan verkon kautta, salausratkaisut ovat usein ainoita suojauksia salassa pidettävän tiedon luottamuksellisuuden, ja tyypillisesti myös eheyden suojaamisessa. Koska salausratkaisujen mahdollisia puutteita on usein äärimmäisen haastavaa korvata muilla suojauksilla, salausratkaisun valintaan ja turvalliseen käyttötapaan suositellaan kiinnitettävän erityistä huomiota.

Siirrettäessä salassa pidettävää tietoa fyysisesti suojattujen alueiden ulkopuolella, tai julkisen verkon kautta, aineisto/liikenne tulee suojata riittävän turvallisella salauksella. Julkiseksi verkoksi tulkitaan esimerkiksi Internet ja operaattorien tarjoamat MPLS-verkot. Käytännön toteutustapoina esimerkiksi käyttäjien päätelaitteiden ja viranomaisen tietojärjestelmien väliset VPN-ratkaisut, organisaatioiden verkkojen välinen IPSec-salaus, sekä loppukäyttäjille tarjottavat turvaposti- ja tiedostosalausratkaisut. Siirrettäessä salassa pidettävää tietoa fyysisesti suojattujen alueiden ja vähintään vastaavalla tasolla suojatun verkon sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella.

Viranomaisen tulee käyttää salausratkaisuja, joiden riittävästä turvallisuudesta on luotettavaa näyttöä. Salausratkaisujen arvioinnissa huomioidaan useita eri tekijöitä. Salausvahvuuden ja salaustuotteen oikeellisesta toiminnasta varmistumisen lisäksi tulee huomioida

muun muassa salaustuotteen käyttöympäristön uhkataso. Esimerkiksi Internetin yli liikennöitäessä uhkataso eroaa tilanteesta, jossa salausta käytetään liikennöintiin hallitun fyysisesti suojatun alueen sisällä (esimerkiksi kahden turva-alueen välinen liikennöinti hallinnollisen alueen kautta). Muihin salaustuotteiden arvioinnissa huomioitaviin tekijöihin kuuluvat esimerkiksi kyseisen käyttötapauksen vaatimukset tiedon salassapitoajalle ja eheydelle.

Erilaisiin tietotyyppeihin kohdistuu erilaisia riskejä. Esimerkiksi viranomaisten turvallisuusluokitellut tiedot ovat yleensä miellettävissä valtion turvallisuuden (yleisen edun) näkökulmasta suojattaviksi. Turvallisuusluokiteltuihin tietoihin voidaan toisaalta usein olettaa kohdistuvan eriävien tahojen kiinnostus, kuin esimerkiksi turvallisuusluokittelemattomiin henkilötietoihin. Riskien eroavaisuus tulee huomioida myös salausratkaisujen valinnassa.

Salausratkaisujen valinnassa suositellaan nojautumaan ensisijaisesti kansallisen tietoturvallisuusviranomaisen (Kyberturvallisuuskeskuksen NCSA-toiminto) arvioimiin ja hyväksymiin salausratkaisuihin. Salausratkaisujen hyväksyntään liittyy oleellisesti käyttöpolitiikka ja -asetukset, joiden mukaan toimimalla kyseisen salausratkaisun on arvioitu tuottavan riittävän suojan kyseisen turvallisuusluokan tiedolle.

Salauksen suojausvaikutus voidaan menettää osin tai täysin tilanteissa, joissa avainhallinnan heikkouksia pystytään valtuuttamattomasti hyödyntämään. Salausratkaisun salausavainten hallinnointiprosessien tuleekin olla suunniteltuja, toteutettuja ja kuvattuja/ohjeistettuja. Salaisten avainten tulee olla vain valtuutettujen käyttäjien ja prosessien käytössä. Prosessien tulee edellyttää vähintään a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, ja f) valtuuttamattomien avaintenvaihtojen estämisen.

Erityisesti salausratkaisujen osalta viranomaisen tulee huomioida myös toimitusketjujen turvallisuus riskienarvioinnissaan. Vaikka salausratkaisu olisi riittävän turvallinen esimerkiksi salausratkaisun valmistajalta lähtiessään, toimitusketjun suojaamispuutteet voivat mahdollistaa salausratkaisun peukaloinnin, ja siten johtaa turvattoman salausratkaisun käyttöönottoon viranomaisen tietojärjestelmän tai tietoliikennejärjestelyn osana.

Lisätietoa turvaluokitellun tiedon suojaamiseen soveltuvasta salauksesta:

- Vahvuustaulukot:
  https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf
- Ohje salaustuotteiden arvioinneista ja hyväksynnistä:
  https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-salaustuotearvioinnit-ja-hyvaksynnat.pdf
- Hyväksyttyjä salausratkaisuja:
  https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf

Lisätietoa turvallisen salausratkaisun kehittämisen tueksi:

Laki julkisen hallinnon tiedonhallinnasta (906/2019) **Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa** **Suosituskortti**	
Tiedonhallintalain 14§ Tietojen siirtäminen tietoverkoissa Turvallisuusluokitusasetuksen 11§ Salausratkaisut	versio 0.9/27.11.2019

- Turvallinen tuotekehitys - kohti hyväksyntää: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Turvallinen_tuotekehitys_Suomi_J003_2018.pdf