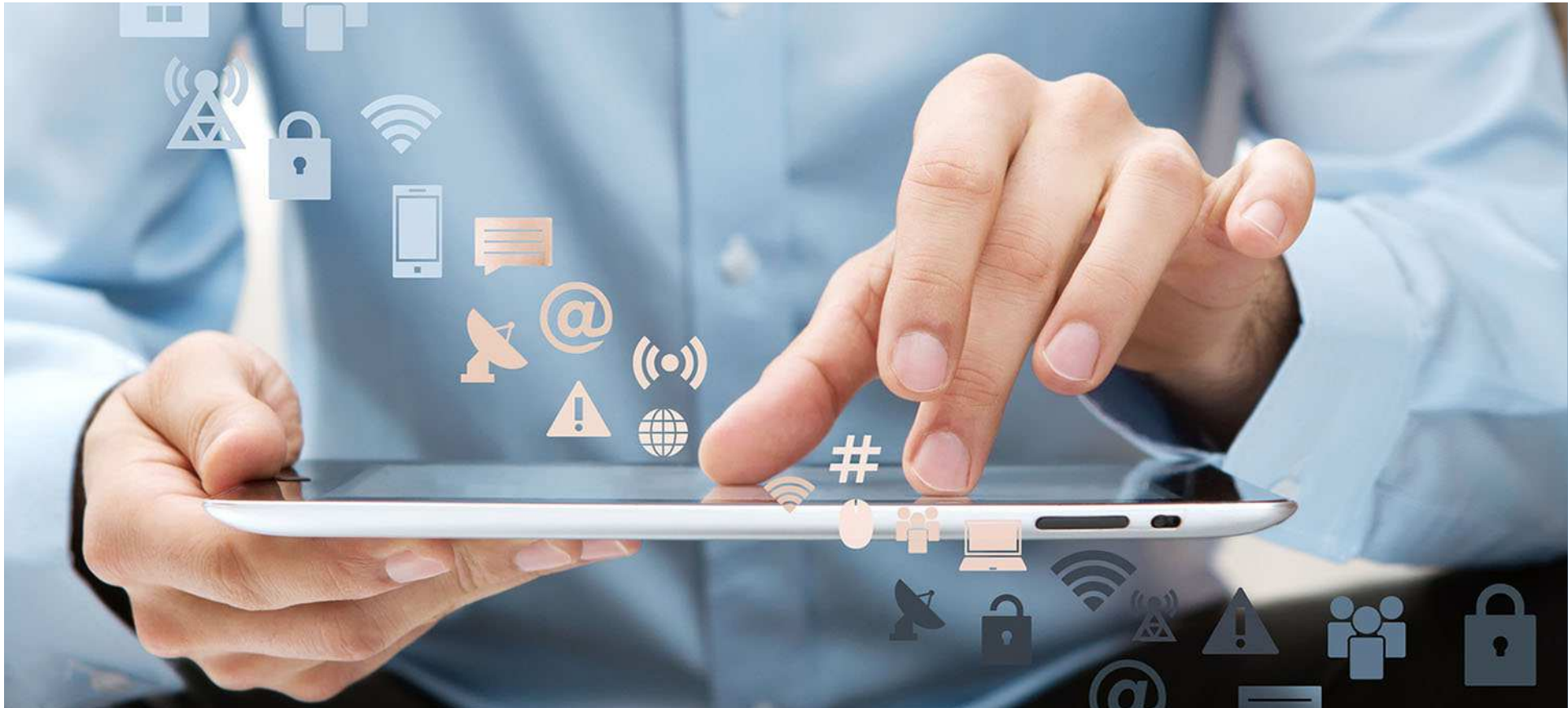




Tietojen salaus ja keskeiset haasteet

Viestintäviraston ohjeet ja suositukset

Viestintävirasto

Kyberturvallisuuskeskus

Tehtävinä mm.

- Järjestelmätarkastukset (arvioinnit ja/tai hyväksynnät), SAA
 - » Kansalliset (arviointi/hyväksyntä), laki 1406/2011, TUVE-laki, Laki 1405/2011
 - » Kansainväliset
- Salaustuotehyväksynnät, CAA
 - » Kansalliset
 - » Kansainväliset
- Avaimistojen hallinta, NDA/CDA
- Tempest-viranomaisen tehtävät, NTA
- Arviointilaitosten valvonta ja tekninen ohjaus
- Muut tuotearvioinnit ja -hyväksynnät

Luottamuksen teoriaa – C, I ja A

- Eri toimijoilla turvallisuuden eri osa-alueiden tarpeet vaihtelevat, esimerkiksi:
- Puolustushallinto: luottamuksellisuus (confidentiality)
- Lainsäädäntötyö: eheys (integrity)
- Häätäkeskus: saatavuus (availability)

Salaus on ainoa varma keino taata luottamuksellisuutta tai eheyttä

Viestintäverkkojen- ja palveluiden toimivuus



Salausratkaisun valinta ja käyttöönotto

- Luokittele tietosi oikein
- Määrittele ympäristösi missä salassa pidettävää aineistoa käsittelet (käyttötapaukset), **tarveanalyysi**
- Tee uhka-arvio omaan käsittely-ympäristöösi, **riskianalyysi**
- Valitse oikea salaustuote omaa ympäristöäsi ja käyttötapausiasi varten, **vaatimusmäärittely**
- Testaa itse ja pyydä arvio omalle valinnallesi ennen käyttöönottoa, **tarkastaminen ja hyväksyminen**

Salausratkaisun valinta ja käyttöönotto

- Käytä valitsemaasi ja arvioitua tuotetta OIKEIN, **jatkuva palvelu ja kehittäminen**
 - » Huolehdi tuotteesta sen käyttöönotosta sen elinkaaren loppuun asti
 - » **Huolehdi erityisesti avainhallinnasta koko sen elinkaaren ajan**
 - » Tee tarvittavat ohjeet kehitykselle, ylläpidolle ja **loppukäyttäjille**

Salausratkaisun valinta käytännössä

1. Valitse hyväksytty tuote

IF NO THEN GO TO 2 or IF YES THEN GO TO 3

2. Määrittele yhteistyössä asiakkaan kanssa salaustuote ja sen tarve (oikea suojaustaso)

- Käytä referenssinä:
 - o Kryptologisia vahvuusvaatimuksia
 - o Muita julkisia referenssejä
 - o Käytä viranomaisneuvontaa (suunnitteluvaihe)

IF YES THEN GO TO 3

3. Arvioita valittu tuote osana tietojärjestelmän arviointi- tai hyväksyntäpyyntöä (Viestintävirasto tai arviointilaitos)

"Kysyvä ei tieltä eksy"

- Hyväksytyt salaustuotteet:
 - » https://www.viestintavirasto.fi/attachments/tietoturva/NCSA_salausratkaisut.pdf
- Tietojärjestelmän tai tietoliikennejärjestelmän arviointi- ja hyväksyntäpyyntö:
 - » <https://www.viestintavirasto.fi/attachments/lomakkeet/NCSA-tarkastuspyyntolomake.doc>
- Kryptologiset vahvuusvaatimukset:
 - » https://www.viestintavirasto.fi/kyberturvallisuus/viestintaviraston_tietoturvapalvelut/ncsa-fi.html
 - Asiakirjat (päivittyvä dokumentti)
- Kansallinen salausteknisen materiaalin käsittelyohje (tulossa)
- Kysymykset: ncsa@viestintavirasto.fi tai caa@viestintavirasto.fi



Viestintävirasto

Kyberturvallisuuskeskus, palveluksessasi