

Case VYVI-Turvaposti – miten huolehditaan turvallisesta viestinnästä eri sidosryhmien kesken?

Tommi Simula

Tietoturvapäällikkö

Valtori

Valtori

Valtion tieto- ja
viestintätekniikkakeskus



Agenda

- Sähköpostin turvallisuus
- Yleiset käyttötapaukset
- VYVI Turvaposti
- Turvallinen viestintä jatkossa

Sähköpostin turvallisuus

- Salassa pidettävän tiedon lähettäminen organisaation hallinnassa olevan ympäristön ulkopuolelle edellyttää aina tiedon suojaamista
- Kun viestintä tapahtuu käsittelyvaatimukset täyttävän viranomaisverkon sisällä (esim. kahden VYVI-Postin käyttäjän välillä) erillistä salausta ei kansallisen ST IV- ja ST III –tiedon osalta tarvita
- Sähköpostin salaus voidaan toteuttaa joko tietoliikenteen salauksella tai viestin ja/tai sen liitetiedostojen salauksella

Tietoliikenteen sala

- Tietoliikenteen TLS-salaus edellyttää sertifikaattien vaihtoa ja sekä lähettävän että vastaanottavan sähköpostipalvelimen konfigurointia
- Salaus kattaa vain siirtotien, eli viestit tallentuvat selkokielistä sekä päätelaitteisiin että sähköpostipalvelimiin
- VYVI-Postin osalta lista organisaatioista, joiden kanssa määritelty TLA-salaus käyttöön saatavilla Valtorin palveluvastaavien kautta
 - HUOM! TLS-salaus ei ota kantaa esim. siihen minkä reitityspalvelinten tai maiden läpi viesti kulkee ennen päätymistä vastaanottajalle

Sähköpostiviestien salaus

- Viesti on salattuna ”end-to-end” lähettäjältä vastaanottajalle, myös sähköpostipalvelimilla ja päätelaitteissa
- Käyttöönotto edellyttää, että viestin lähettäjällä ja vastaanottajalla käytössään sama salausohjelmisto, esim.
 - PGP (Pretty Good Privacy, nyk. Symantec Desktop Encryption)
 - GPG (Gnu Privacy Guard, open source PGP-toteutus)
 - S/MIME (Secure/Multipurpose Internet Mail Extensions, julkiseen avaimeen pohjautuva salausmekanismi)
- Vaihtoehtoisesti voidaan käyttää erillistä tiedostosalausta liitetiedostojen salaukseen, kuten-TrueCrypt jne.

Yleiset käyttötapaukset

- Salassa pidettävän tiedon lähetys organisaation sisällä
 - Tyypillisesti ei tarvita erillissalausta (jos käytössä esim. VYVI-Posti)
- Salassa pidettävän tiedon lähetys yhteistyökumppanille, asiakkaalle tai toimittajalle
 - Salaus pakollista
 - Sovittava ennen yhteistyön alkamista joko sähköpostipalvelinten välisen liikenteen salauksesta tai yhteisen salausmenetelmän käyttöönotosta
- Salassa pidettävän tiedon lähetys muulle taholle, esim. kansalaiset, loppukäyttäjät
 - Salaus pakollista, mutta tyypillisesti ei voida sopia turvakäytännöistä etukäteen tai vaikuttaa niihin

- Palvelu perustuu Deltagon Oy:n Sec@GW –tuotteeseen, jolla NCSA-FI:n hyväksyntä ST IV –tiedolle
- Hyväksyntä koskee tuotteen versiota 3.3.0 käytettäessä Viestintäviraston hyväksymää käyttöpolitiikkaa, jota ei toistaiseksi ole käytössä VYVI-Turvassa
- Mahdollistaa turvallisen suojausluokitellun (ST III –IV) aineiston lähettämisen ja vastaanottamisen sähköpostina
- Viestejä voidaan käsitellä selaimella
- Suojausluokitellun tiedon lähettäminen on helppoa ja nopeaa, samalla yksinkertaisen turvallista
- Palvelun käyttö ei vaadi lisäsovellusten käyttöönottoa tai ylimääräisiä käyttäjäkoulutuksia

VYVI-Turva

- Tukee kahta toimintamallia:
 1. "Kirje-toiminto"
 - Lähettäjä lisää vastaanottajan osoitteen loppuun ".s"
 - Posti kulkee salattuna turvaposti-palvelimelle
 - Vastaanottaja saa linkin postiin, josta pääsee avaamaan viestin
 - Katsotaan riittäväksi kansalliselle ST IV -tiedolle
 2. "Kirjattu kirje –toiminto"
 - Lähettäjä lisää vastaanottajan osoitteen loppuun myös vastaanottajan matkapuhelinnumeron ".GSM-numero.s"
 - Toimii muuten kuten Kirje-toiminto, mutta postia avattaessa vastaanottajan matkapuhelimeen tulee pin-koodi, joka vaaditaan viestin avaamiseksi
 - Katsotaan riittäväksi kansalliselle ST III -tiedolle

VYVI-Turva muut ominaisuudet

- Sisäänpäin tuleva suojattu viestintä (D-Compose)
 - Turvapostiportaalin kautta, esim. <https://turvaposti.valtori.fi>
- Salauksen automatisointi ja tilastointi (D-Control)
 - Analysoi lähtevää sähköpostia ja salaa viestit esim. avainsanojen perusteella
- Tietoturvalliset lomakkeet (D-forms)
 - Mahdollistaa tietoturvallisesti lähetettävien lomakkeiden luomisen ja linkittämisen esim. web-sivuille
 - Samat tunnistusratkaisut kuin D-Compose -optiossa
 - Mahdollisuus integroida muihin järjestelmiin

Turvallinen viestintä jatkossa

- Jatkossa valtionhallinnon sisäisessä viestinnässä tavoitteena oletussalaus
- Valtti-työasemaympäristön mukana virkavarmenteeseen pohjautuva S/MIME-salaus
- VYVI-Turva jatkossa niissä käyttötapauksissa, joissa S/MIME:n käyttö ei mahdollista

Nyrkkisääntö: Jos et tiedä pitäisikö viesti salata, salaa se!

Kysymyksiä?

- Lisätietoa VYVI-Turvasta ja sen käyttöönotosta omilta Valtorin asiakasvastaaviltanne tai viestintaratkaisu@valtori.fi