# Salattu sähköposti

Opas asiakasviestinnän suojaamiseen

# Johdanto

Viestinnän tietosuojan tarve on laajentunut sekä säätelyn lisääntymisen että uhkakuvien realisoitumisen vuoksi. Siinä missä ennen lähetettiin vain salaisuuksia kuten salasanoja suojattua kanavaa pitkin, nyt suojatun kanavan käyttö on yleistymässä kaikkeen luottamukselliseen viestintään. Odotukset ovat muuttuneet. Kysymys ei enää ole siitä, pitäisikö viestintä suojata, vaan siitä miten se parhaiten suojattaisiin.

Perinteinen sähköposti on edelleen merkittävin tapa viestiä organisaatioissa [1], ja siksi sen suojaaminen kuuluu digitaaliseen perussivistykseen. Käytännössä kuitenkin sähköposti on viestintävälineistä kaikkein hankalin turvata. Mitään de facto -ratkaisua ei ole, jonka voisi vain kytkeä päälle, on vaan joukko tekniikkoja ja tuotteita. Sähköpostin käyttäjät ovat tilanteessa, jossa esimerkiksi henkilötietojen välittämiseen on vähintäänkin kiusallista käyttää tavallista sähköpostia, mutta osapuolten kesken ei ole selvää yhteistä suojattua vaihtoehtoa. Jokaisen vastaanottajan kanssa on sovittava erikseen mitä tehdään, tai sitten lähettäjä vain päättää yksipuolisesti mitä kanavaa käytetään. Ajankäyttö per viesti kasvaa sekä lähettäjän että vastaanottajan päässä. Vastaavasti työn tuottavuus laskee.

Epätietoisuus ja vaihtoehtojen kirjavuus tarkoittavat toisaalta myös sitä, että lopputulokseen voi itse vaikuttaa. Siirtyminen pois suojaamattomasta sähköpostista on pitkälti organisaation itsensä hallittavissa. Jokainen voi löytää parhaan ratkaisun omiin tarpeisiinsa.

Tämän oppaan tarkoitus on esitellä ratkaisuja - tavallisen sähköpostin tietosuojaltaan parannettuja vaihtoehtoja asiakasviestinnässä. Asiakasviestinnällä tarkoitetaan tässä laajasti organisaation ja sen asiakkaiden välistä viestintää, jossa asiakkaat ovat kuluttajia tai toisia organisaatioita, tai näiden yhteistyökumppaneita. Olennaista on, että viestintää tehdään organisaation edustajana ja että viestintäjärjestelmä on organisaation hallinnoima. Henkilökohtaisia viestintävälineitä kuten erilaisia sosiaalisen median palveluja ja pikaviestimiä ei käsitellä, paitsi jos näitä voi hyödyntää asiakasrajapinnassa. Liian tarkkaa rajanvetoa ei kannata tehdä koska käytännöt muuttuvat. Esimerkiksi henkilökohtaiseen matkapuhelinnumeroon lähetettäviä SMS-viestejä on aina hyödynnetty tavallista sähköpostia turvallisempana kanavana.

## Sähköpostin heikot kohdat

### 1 Lähettäjä

**Ongelma**

- Kuka tahansa voi käyttää lähettäjän nimeä ja sähköpostiosoitetta.

**Ratkaisut**

- Lähettäjän nimipalvelussa määritellään luotetut SMTP-palvelimet.
- Lähettäjä allekirjoittaa viestin digitaalisella allekirjoituksella.
- Lähettäjä käyttää hallinnassaan olevaa suojattua verkkopalvelua, esim. tietosi.fi -palvelua viestintään.

### 2 Lähettäjän postilaatikko

**Ongelma**

- Viestit säilytetään työasemalla ja/tai postipalvelimella salaamattomina.

**Ratkaisut**

- Postilaatikko salataan levyn salauksella.
- Käytetään postilaatikon viestit salaavaa sähköpostia tai suojattua verkkopalvelua.

Lähdetään liikkeelle sähköpostin salauksen nykytilasta ja kerrotaan, miten siihen on päädytty. Käydään läpi suojaamattoman sähköpostin ongelmia ja teknisiä ratkaisuja niihin. Hahmotellaan, mikä käytännössä voisi toimia ja mikä ei. Tarkoitus on esittää perusteltu näkemys siitä, mihin suuntaan kehitys on kulkemassa.

## Mitä on suojattu sähköposti?

Sähköpostin suojaamisella tarkoitetaan toimenpiteitä, joilla sähköpostiviestinnän luottamuksellisuus pyritään turvaamaan. Vähintään tavoitellaan yksityisyyttä, eli sitä etteivät ulkopuoliset pääse lukemaan viestejä. Salaus on menetelmä yksityisyyden turvaamiseksi [2]. Toiseksi, luottamuksellisen viestinnän osapuolet haluavat tunnistaa toisensa luotettavasti. Tunnistaminen perustuu osapuolten itsensä hankkimaan tietoon ja ulkopuolisiin auktoriteetteihin. Kolmanneksi, suojausmenetelmillä pyritään seurantaan ja auditoitavuuteen. Halutaan pystyä osoittamaan, että vastaanottaja on nähnyt viestin. Halutaan osoittaa viestien eheys eli koskemattomuus, se ettei viestiä ole muutettu matkan varrella. Vastakohtana suojatulle sähköpostille täysin suojaamaton sähköposti on verrattavissa postikorttiin: sisältö on avoin kaikille korttia käsitteleville, lähettäjä ja vastaanottaja eivät tunnista toisiaan, eikä toimituksen perillemenoa seurata.

Suojatussa sähköpostissa on kyse ennen kaikkea viestien sisällön yksityisyydestä. Viestinvälityksen metatietoa kuten lähettäjää, vastaanottajaa, postipalvelimien nimiä ja IP-osoitteita tai välitysajankohtia ei tavallisilla menetelmillä ole tarkoitus, eikä mahdollistakaan piilottaa kokonaan. Myöskään sähköpostin tietoturvaan olennaisesti kuuluva sähköpostin kautta kulkevien haittaohjelmien torjunta ja roskapostin suodatus eivät ole sähköpostin suojaamisen tarkoituksena.

## Miksi sähköposti pitää suojata?

Osa viestinnästä pitää suojata, jotta organisaatio täyttää velvoitteensa.

Vaatimukset tietojen suojaamiselle määritellään yleisimmin lainsäädännössä ja täsmällisemmin sopimuksissa. Tuoreena esimerkkinä ovat EU:n tietosuoja-asetus (GDPR) ja tämän voimaantulon yhteydessä

## Sähköpostin heikot kohdat

**3**

### Lähetettävän viestin sisältö

- **Ongelma**
- Sisältö luettavissa ja muutettavissa sähköpostia välittävillä palvelimilla.

**Ratkaisut**

- Salataan ja digitaalisesti allekirjoitetaan viesti.
- Käytetään viestin sisällön salaavaa turvapostia tai suojattua verkkopalvelua.

**4**

### Viestiliikenne

**Ongelma**

- Tietoliikenne salakuunneltavissa

**Ratkaisut**

- Salataan tietoliikenne TLS-protokollalla.
- Lähetetään sähköpostitse ainoastaan ilmoitusviestejä, ei salattavaa sisältöä. Luetaan viestit https-yhteydellä turvapostissa tai suojatussa verkkopalvelussa.

rekisterinpitäjien ja käsittelijöiden välillä solmitut tietosuojasopimukset [3]. Varsinkin tietosuojasopimuksissa ja tietoturvaliitteissä käsittelijöiltä voidaan vaatia, että henkilötietoja sisältävät aineistot siirretään aina suojatusti.

Myös pitkään maalaillut uhkakuvat ovat osoittautuneet todellisiksi. Organisaatioiden sähköpostiviestinnän kansainvälisestä vakoilusta on jo useita korkean profiilin esimerkkitapauksia, mm. hakkerointi Yhdysvaltojen Demokraattisen puolueen sähköpostipalvelimelle, josta vuodetut viestit ovat nyt kaikkien luettavissa. Suojautuminen kansainväliseltä vakoilulta on teknisesti vaativaa, mutta useimpien organisaatioiden helpotuksena on, ettei tällaista suojautumistarvetta ole. Organisaation tiedoilla ei yksinkertaisesti ole merkitystä kansallisen turvallisuuden näkökulmasta, eikä vakoilusta aiheudu vastuita.

Merkittävämpänä uhkakuvana ovat tietovuodoista langetettavat viranomaissanktiot ja vastuut alihankintaketjuissa, sekä ennen kaikkea tietovuotojen aiheuttama maineen ja liiketoiminnan menetys. Tietovuotoihin myös puututaan aikaisempaa systemaattisemmin, sillä GDPR:n voimaantulon myötä tietoturvaloukkauksista on ilmoitettava valvontaviranomaiselle ja rikkomuksista voidaan määrätä hallinnollisia sakkoja [4].

Organisaatioissa tietosuojavaatimusten edellyttämät käytännöt on monissa yrityksissä kirjattu sisäiseen ohjeistukseen. Taustalla on joko muodollinen tai arkijärkeen perustuva käyttöoikeuspolitiikka, joka määrittelee tietojen luokittelun ja suojaustarpeen. Esimerkiksi tietojen arkaluonteisuuteen perustuva nelitasoinen luokitus voisi olla seuraava [5]:

- **Kategoria I** – Julkinen
- **Kategoria II** – Sisäiseen käyttöön
- **Kategoria III** – Arkaluonteinen
- **Kategoria IV** – Erittäin arkaluonteinen

Eri tietokategorioita varten vaaditaan erilaisia suojaustapoja. Esimerkiksi tavallinen sähköposti voidaan kieltää kategorian III arkaluonteisen tiedon välittämiseen organisaatiosta ulospäin. On myös mahdollista, että sääntelyn ja sopimusten muutokset muuttavat tietojen luokitusta. Ennen GDPR-aikaa kategorian II sisäiseen käyttöön luokiteltu henkilötieto on nyt monesti kategoriaan III kuuluvaa arkaluonteista tietoa.

## Sähköpostin heikot kohdat

**5**

### Vastaanottajan postilaatikko

**Ongelma**

- Lähettäjä ei voi vaikuttaa vastaanottajan postilaatikon suojaukseen.

**Ratkaisut**

- Käytetään lähettäjän hallinnoimaa turvapostia tai suojattua verkkopalvelua.

**6**

### Vastaanotettu viesti

**Ongelma**

- Lähettäjä ei saa kuittausta viestin vastaanottamisesta tai avaamisesta

**Ratkaisut**

- Automaattinen kuittaus viestin avaamisesta turvapostissa tai suojatussa verkkopalvelussa.

# Sähköpostin suojaustekniikat

Sähköpostin välittäminen sähköpostipalvelimien kesken perustuu SMTP-protokollaan, jonka ensimmäinen määrittely on peräisin vuodelta 1982 (RFC 821). Legendaarisen Jon Postelin alkuaan kehittämä protokolla on yksi internetin menestystarinoita. Sen toimintalogiikka on kuitenkin hyvin avoin, protokollaa ei ole suunniteltu luottamukselliseen viestintään.

Alkuperäisessä SMTP-protokollassa ja sen toteutuksissa viestit kulkevat selväkielisenä postipalvelimien välillä, ja tallennetaan ainakin lyhyeksi aikaa salaamattomina postipalvelimien levylle. Kuljettuaan reitittävien välityspalvelinten kautta, viestit lopulta päätyvät vastaanottavalle palvelimelle, jossa ne niin ikään oletuksena säilytetään salaamattomana. Loppukäyttäjä lataa viestit palvelimelta omalle koneelleen erillisellä protokollalla (POP, IMAP tai valmistajakohtainen protokolla), jälleen selväkielisenä, ja säilyttää ne salaamattomina. Tämä suojauksen taso oli arkipäivää vielä 90-luvun loppupuolella. On selvää, ettei lähettäjä voi taata viestin yksityisyyttä, jos järjestelmän jokaisessa vaiheessa välitys perustuu selväkielisiin kopioihin.

Koska potentiaalisesti turvattomia tietoliikenneprotokollia tarvitaan viestien välittämiseen ja noutamiseen, sähköpostin suojaustaso on korkeampi, jos viestejä ei välitetä julkisen internetin kautta. Kaksi käyttötapausta on hyvä nostaa esiin:

1. Sähköpostia lähetetään organisaation sisällä. Tarve SMTP-protokollan suojaamiselle koskee eri sähköpostipalvelimien välistä sähköpostiviestintää. Sisäinen sähköpostiviestintä on olennaisesti suojatumpaa kuin talosta ulos lähtevät sähköpostit, jos ja kun viestejä ei välitetä sähköpostipalvelimelta eteenpäin.
2. Posteja luetaan webmail-sovelluksella. Webmail-sovellukset kommunikoivat tavallisesti suoraan sähköpostipalvelimen kanssa sisäverkossa ilman POP/IMAP-liikennettä julkisessa internetissä. (Pitää kuitenkin huolehtia, ettei salaamattomia http-yhteyksiä käytetä liikennöinnissä selaimen ja webmail-sovelluksen välillä.)

## Sähköpostin heikot kohdat

7

### Vastaanottaja

#### Ongelma

- Lähettäjä ei tunnista vastaanottajaa kuin sähköpostiosoitteella.

#### Ratkaisut

- Tunnistetaan turvapostin vastaanottaja matkapuhelinnumerolla ja SMS-kertakäyttösalasanalla.
- Tunnistetaan suojatun verkkopalvelun käyttäjä vahvasti pankkitunnuksilla tai mobiilivarmenteella.

Perinteinen fyysinen menetelmä suojata viestiliikennettä ja viestinnän osapuolia, on sopia salainen sijainti, johon viesti toimitaan ja josta viesti noudetaan. Sähköpostiviestinnässä tämän *dead drop* -menetelmän vastine on jakaa webmail-laatikko osapuolten kesken ja käyttää pelkästään tallennettuja luonnoksia viestintään. Tämä ei kuitenkaan estä ulkopuolisten pääsyä viesteihin, jos webmail-järjestelmä on turvaton. Tunnetuin tapaus lienee, kun CIA:n pääjohtaja, kaikista maailman ihmisistä, kompastui tähän yksityiselämässään vuonna 2012.

## Tietoliikenteen salaaminen

SMTP-protokollan ja client-protokollien laajennuksissa (RFC 3207, RFC 2595) on määritelty sähköpostin tietoliikenteen suojaaminen Transport Layer Security-protokollan (TLS) avulla. SMTP-protokollan STARTTLS -laajennus vaatii kuitenkin tuen sekä lähettävältä että vastaanottavalta osapuolelta, ja jos jompikumpi puuttuu niin tiedonsiirtoa ei voi salata. Googlen Transparency Reportin mukaan Googlen sähköpostipalveluissa tällä hetkellä yli 90 % vastaanotetuista viesteistä kulkee salattuna ja lähtevistä viesteistä yli 85 % voidaan välittää TLS-salattuna. Viestien sisällön lisäksi suuri osa metatietoa pystytään salaamaan postipalvelimien välillä [6].

Tietoliikenteen salaamisesta seuraa, että heikkoja kohtia on nyt vähemmän kuin aikaisemmin. Sähköpostiliikenne on suojattua, mutta sähköpostien säilytys potentiaalisesti suojaamatonta. Sähköposteja säilytetään lähettäjän ja vastaanottajan postilaatikoissa ja SMTP-palvelimien postijonoissa. Sähköpostin osapuolten tunnistamiseen tietoliikenteen TLS-suojaus ei tuo apua kuin postipalvelimien tasolla, jotka voidaan tunnistaa aikaisempaa luotettavammin aidoiksi, palvelimelle myönnetyn varmenteen perusteella.

## Sisällön salaaminen

Turvattomassa kanavassa välitettävien viestien sisällön salaamisella on pitkä ja perinteikäs historia [7], jota voi jäljittää tuhansien vuosien taakse. Elektronisen viestinnän salaaminen perustuu kryptografisten algoritmien laskennalliseen kovuuteen, jolla tarkoitetaan sitä, että salauksen purkamiseen vaadittavaa avainta ei pysty yrityksen ja erehdyksen kautta löytämään järkevässä ajassa. Ensimmäinen NSA:n julkiseen viranomaiskäyttöön hyväksymä salausalgoritmi DES julkaistiin vuonna

1975. Salauksen pitkää taustaa vasten ei ole yllättävää, että sähköpostien salaamista varten kehitettiin teknologiaa ja määriteltiin standardeja pian internetin yleistyttyä.

### *Pretty Good Privacy (PGP)*

Ehkä tunnetuin salausjärjestelmä on julkisen avaimen infrastruktuuriin perustuva PGP, jonka ensimmäisen version kehitti ja julkaisi Phil Zimmermann vuonna 1991, alun alkaen uutisryhmien viestien ja tiedostojen salaamista varten.

PGP törmäsi kuitenkin välittömästi laillisiin esteisiin. Kylmän sodan aikaiset vientirajoitukset kielsivät kryptografisen teknologian viennin Yhdysvalloista ilman vientilupaa. PGP:n ollessa vapaasti kopioitava freeware-ohjelmisto Yhdysvaltojen liittovaltio nosti syytteen ja aloitti rikostutkinnan Zimmermania vastaan. Syytteestä luovuttiin ilman tuomiota vuonna 1996, jolloin salausteknologian vientirajoitusten purkaminen oli jo edennyt pitkälle kylmän sodan päätyttyä. Zimmermannin aloitteesta PGP:n standardointi keskitettiin sittemmin IETF:n OpenPGP-työryhmän alle (RFC 4880). Tunnetuin OpenPGP-standardin mukainen toteutus on avoimen lähdekoodin GNU Privacy Guard (GPG).

Edistyksellinen ja yleiskäyttöinen PGP kohtasi kuitenkin Yhdysvaltojen liittovaltiotakin sitkeämmän vastuksen, loppukäyttäjän, joka oli tottunut helppokäyttöisempään salaamattomaan sähköpostiin. PGP:n käytettävyysongelma salaamattomaan sähköpostiin verrattuna on ilmeinen. Jotta sähköpostin voi salata, lähettäjä tarvitsee vastaanottajan sähköpostiosoitteen lisäksi tämän julkisen avaimen. Julkinen avain on pitkä merkkijono, joka on tavalla tai toisella hankittava vastaanottajalta. Käyttäjille, jotka ovat tottuneet vapaamielisesti lisäämään vastaanottajia sähköpostiviesteihinsä, avainten etsiminen ja ylläpito on osoittautunut ylitsepääsemättömäksi kynnykseksi, pientä määrää käyttötapauksia lukuun ottamatta. PGP:n sujuvaa käyttöä varten sähköpostiohjelmaan tarvitaan salausta, salauksen purkamista ja avainten hallintaa varten laajennuksia, joita esimerkiksi webmail-clienteissa ei tavallisesti löydy. Sama ongelma on hidastanut PGP:n kanssa osittain kilpailevan S/MIME -standardin yleistymistä.

### *S/MIME*

S/MIME määrittelee, kuinka sähköpostin sisältönä kulkeva MIME-data salataan. Siinä missä PGP on yleiskäyttöinen salausjärjestelmä, S/MIME

on tarkoitettu pelkästään sähköpostiviestien sisällön salaamiseen ja digitaaliseen allekirjoittamiseen [8]. Julkisen avaimen salaukseen perustuva menetelmä edellyttää lähettäjien ja vastaanottajien X.509-varmenteita, joiden ylläpitotyön vaiva ulottuu loppukäyttäjään asti. Prosessi on kuvattu hyvin esim. Helsingin yliopiston ohjeessa. S/MIME on kuitenkin huomattavasti paremmin tuettu nykyisissä sähköpostijärjestelmissä kuin PGP. Esimerkiksi Microsoft Outlookissa on jo pitkään ollut ominaisuutena varmenteiden hallinta sekä sähköpostien digitaalinen allekirjoitus ja salaus S/MIME-tekniikalla, Googlen G Suite Enterprise sisältää hosted S/MIME -ominaisuuden, jossa vastaavat toiminnot hallinnoidaan Googlen alustalla.

### *Liitetiedostojen salaaminen*

Kolmas, PGP ja S/MIME -tekniikkoja vaatimattomampi, mutta käytännössä hyvin suosittu menetelmä sähköpostin liitetiedostojen suojaamiseen on ollut salata lähetettävät tiedostot jollakin salausohjelmalla, esim. salattuna zip-pakettina, ja avata nämä kryptaamisen yhteydessä syötetyllä jaetulla salasanalla. Tässä menetelmässä ongelmana on käytettävästä salausohjelmasta sopiminen osapuolten välillä sekä salasanan turvallinen toimittaminen vastaanottajalle, tyypillisimmin SMS-viestinä.

### *Standardien tulevaisuus*

Kokemus on osoittanut, että helppokäyttöisyys on salausteknologian yleistymisen tärkeä edellytys. Loppukäyttäjälle vaivattomasti toteutettu julkisen avaimen kryptografia on kiistatta yksi 2010-luvun menestystarinoita. Tähän perustuu niin nettiselailun, pikaviestimien kuin matkapuhelinten ja tietokoneiden massamuistien salauksen suosio. Vakioennuste viimeiset 20 vuotta on ollut, että on vain ajan kysymys, koska sähköpostin salaus yleistyy. Odottavan aika on kuitenkin käynyt pitkäksi [9] [10]. Mahdollisesti varmenteiden hankkiminen ja ylläpito on joskus tulevaisuudessa niin helppoa, että olemassa olevien standardien käytettävyysongelmat poistuvat. Esimerkiksi helppokäyttöinen Let's Encrypt on jo saavuttanut kriittisen massan www-palvelimien varmenteissa. Toisaalta on päivä päivältä todennäköisempää, että muiden ominaisuuksien, kuten osapuolten vahvan tunnistamisen ja auditoitavuuden vuoksi salattu viestintä siirtyy kokonaan sähköpostin ulkopuolelle erilaisiin yksityisiin verkkopalveluihin ja viestintäsovelluksiin.

Avointen standardien, kuten PGP:n ja S/MIME:n etuna on, että näiden tietoturvaa valvoo yksityisiä verkkopalveluja suurempi yhteisö. Toisaalta standardien toteutusten runsaudesta seuraa, että löytyneet tietoturvahaavoittuvuudet johtavat laajamittaisiin korjaustoimiin, joista viimeisenä esimerkkinä on toukokuussa 2018 julkaistun EFAIL-haavoittuvuuden vaatimat korjauspäivitykset.

## Osapuolten tunnistaminen

Sähköpostin salaaminen huolehtii viestinnän yksityisyydestä ja eheydestä viestintäkanavassa, niin että viestien tietoturva perustuu salausalgoritmin kovuuteen. Jos salaamaton sähköpostiviesti on kuin postikortti, salattua viestiä voi verrata salakirjoitettuun postikorttiin. Sähköpostin suojaamisessa tarvitaan kuitenkin muitakin ominaisuuksia, erityisesti osapuolten pitää pystyä tunnistamaan toisensa riittävän luotettavasti ja saada tietoa viestien perillemenosta.

Viestin lähettäjä päättää millä osoitteella ja nimellä viesti lähetetään. Verkkotunnuksen eli domainin haltija voi kuitenkin määritellä luotetut sähköpostipalvelimet DNS-nimipalveluun SPF- ja DKIM -tietueiksi. Tällöin vastaanottaja voi tarkastaa, onko viesti todella lähtenyt organisaation luottamalta palvelimelta. Lähettäjän henkilöllisyyttä tai pääsyä postilaatikkoon tämä ei takaa, esimerkiksi tämän oppaan latauksessa vastaanottamasi kuittausviesti oli automaattiviesti, joka läpäisee SPF-tarkistuksen.

Fyysisen postin osapuolet tunnistavat toisensa allekirjoituksilla, leimoilla ja sineteillä. Lähettäjä allekirjoittaa viestinsä, ja vastaanottajalta vaaditaan kirjatuissa lähetyksissä vastaanottokuittaus. Sähköpostissa vastaavasti käytetään digitaalisia allekirjoituksia ja kuittauksia, esimerkiksi Outlookissa voi lähettää viestin S/MIME-allekirjoitettuna ja pyytää tähän S/MIME-kuittausta.

Valitettavasti S/MIME-allekirjoituksiin liittyy sama ongelma kuin salaukseen: julkisen avaimen salauksen vaatimien varmenteiden ylläpitäminen loppukäyttäjän toimesta on kohtuuton vaatimus. Toiseksi allekirjoituksen luotettavuus riippuu varmenteen myöntäjästä, joka päättää prosessista, jolla varmenteen hakija verifioidaan. Validi allekirjoitus takaa, että sähköposti on peräisin lähettäjän osoitteen omistajalta, mutta lähettäjän henkilöllisyyttä ei varsinaisesti tunnisteta. Tämä on ongelma erityisesti asiointipalveluissa, joissa suuri joukko

kuluttajia viestii organisaation suuntaan. Yksityishenkilöiden tunnistautuminen S/MIME-allekirjoituksella ei ole riittävän luotettavaa verrattuna yleisessä käytössä oleviin vaihtoehtoihin. Tällaisia ovat, suojaustarpeen mukaan, organisaation itse hallinnoimat käyttäjätunnukset mahdollisesti kaksivaiheisella tunnistautumistavalla täydennettynä, kolmansien osapuolten kuten kansainvälisten internetjättien käyttäjätunnukset, sekä vahvat kansalliset tunnistautumistavat kuten TUPAS-pankkitunnistautuminen ja mobiilivarmenne.

Vastaanottajan tunnistamiseen sähköposti ei tarjoa juuri mitään välineitä. Vastaanottajalta pyydettävään kuittaukseen vastaaminen on vapaaehtoista, jolloin sähköpostien vastaanotto ja avaaminen ei ole auditoitavissa.

## Kokonaisratkaisut

Koska PGP tai S/MIME-suojattua sähköpostia on hankala hyödyntää kahden henkilön välisessä viestinnässä, ja vielä hankalampaa organisaatioviestinnässä, on ymmärrettävää, että organisaatiot ovat etsineet keskitettyjä yksityisiä kokonaisratkaisuja avoimien standardien sijaan. Tuotteista ei ole pulaa, Bruce Schneierin ja kumppaneiden katsaus vuodelta 2016 listaa noin 90 sähköpostin salaustuotetta ja noin 200 muun viestinnän salaustuotetta [11].

Perinteinen, jo 90-luvulta käytössä ollut ratkaisu on ollut jättää salaus sähköpostiyhdyskäytävän (gateway) tehtäväksi. Sähköpostit, jotka reititetään salaavan yhdyskäytävän, eli ”turvapostin” kautta, välitetään salattuna vastaanottajalle. Jos vastaanottajan julkisia avaimia ei ole tiedossa, eikä viestiä voi siksi välittää standardimenetelmillä, lähetetään saapumisilmoitus vastaanottajalle, joka voi lukea viestin turvapostin webmailin kautta. Webmail-käyttöä voidaan rajata IP-osoitteen perusteella ja sähköpostin säilytysaikaa webmailissa voidaan rajoittaa. Sähköpostien avaamisesta webmailissa jää varma tieto. Esimerkkejä sähköposti-gateway-ratkaisuista ovat Symantecin ja Deltagonin tuotteet. Gateway-tuotteiden etuna on, ettei loppukäyttäjille tarvitse asentaa uusia ohjelmia. Tietohallinnon tulee kuitenkin konfiguroida turvaposti organisaation käyttöön, eikä sitä voi helposti hyödyntää sähköpostien lähettämiseen älypuhelimilla tai muilla laitteilla organisaation verkon ulkopuolelta. Lisäksi turvapostien webmail-käyttöliittymät ovat usein vanhanaikaisia kuluttajille tuttuihin webmail-palveluihin verrattuna.

Esimerkiksi Helsingin yliopisto suosittelee turvapostia satunnaiseen käyttöön ja S/MIME-salausta jatkuvaan käyttöön [12]. Loppukäyttäjän tietosuojan kannalta ongelmallista on myös, että suojaus on viime kädessä yhdyskäytävän eikä käyttäjän hallinnassa. Nykyaikaisempi pilvipalveluna tarjottava versio turvapostista on Microsoftin Office 365 Message Encryption (OME), jota Office 365 -asiakkaat voivat käyttää sähköpostien suojaamiseen. Vastaanottaja voi lukea viestin kertakäyttösalasanalla tai Microsoft-tunnuksilla.

Suojatun sähköpostin voi hankkia myös erillisenä SaaS-palveluna. Tällöin kyse on Office 365:n tai Gmailin kaltaisesta hostatusta sähköpostista, jossa kuitenkin on tavanomaista enemmän tietosuoja- ja tietoturvaominaisuuksia. Vähintäänkin sähköpostilaatikko on salattu niin, ettei edes palveluntarjoaja pääse käsiksi viesteihin, ja yleensä palvelun halutaan sijaitsevan valtiossa, jossa on vahva yksityisyyden suoja. Näiden ominaisuuksien merkitys käy ilmi Yhdysvalloissa sijainneen Lavabit-sähköpostipalvelun tapauksessa. Edward Snowdenin paljastuttua Lavabit-sähköpostin käyttäjäksi, palveluntarjoan oli ensin asennettava viestiliikenteen salauksen ohittava valvontalaite sisäverkkoon, ja tämän jälkeen oikeuden päätöksellä vaadittiin salausavain, joka mahdollisti palvelussa säilytettävien viestien lukemisen. Lopulta palvelu oli suljettava. [13]

Sveitsiläinen ProtonMail on yksi esimerkki suojatusta sähköpostipalvelusta. Lähetettävien viestien suojaamiseen voi käyttää PGP-salausta tai vastaanottaja voi avata salasanasuojatun viestin selaimella. Sähköpostiyhdyskäytävään verrattuna SaaS-palveluna tarjottavan turvatun sähköpostin etuna on periaatteessa käyttöönoton helppous, mutta käytännössä käyttöönotto tarkoittaa joko siirtymistä uuteen sähköpostijärjestelmään tai kahden rinnakkaisen sähköpostin käyttöä. Toistaiseksi korkean turvallisuuden sähköpostipalvelut eivät ole saaneet merkittävää jalansijaa, esimerkiksi ProtonMail-palvelun käyttäjämääräksi vuonna 2017 kerrotaan yli 2 miljoonaa, joka on 0,2 % Gmailin yli miljardista käyttäjästä tai vajaa 2% Microsoft Office 365:n 120 miljoonasta yrityskäyttäjästä.

# Pikaviestintäsovellukset

Sähköpostin puutteita voi paikata asiakasrajapinnassa erilaisilla pikaviestintäsovelluksilla. Kukapa ei olisi asioinut operaattorin tai pankin kanssa chat-palvelua käyttäen. Sisäisessä käytössä ja keskeisten yhteistyökumppanien välisessä viestinnässä pikaviestimet kuten Slack ovat syrjäyttäneet sähköpostia siinä missä etäpalaverit tapaamisia.

Useimmat nykyaikaiset pikaviestintäsovellukset (eivät kaikki) salaavat sekä tietoliikenteen että säilytettävän tiedon, ja ovat myös viestintäprotokollaltaan sähköpostia suojatumpia. Pikaviestimet on voitu suunnitella turvallisemmiksi alusta alkaen. Toki pikaviestintäpalvelua ylläpitävän valtion viranomaisilla on oikeus seurata viestintää paikallisen lain mukaan, ja käyttöjärjestelmäalustaan voi kohdistua vakoilua.

Paremmasta tietosuojasta huolimatta on kuitenkin merkittävä määrä käyttötapauksia, joihin pikaviestimet eivät sovellu. Sähköpostiin verrattuna uuden vastaanottajan tavoittaminen on hankalaa, koska organisaatioiden käyttämillä pikaviestintäsovelluksilla ei ole samanlaista kattavuutta ja statusta kuin sähköpostilla tai puhelinnumerolla. Esimerkiksi Slack ilmoittaa päivittäiseksi käyttäjämääräkseen vain 8 miljoonaa toukokuussa 2018. Kaikkia ei myöskään haluta ottaa organisaation chat-järjestelmään mukaan, jatkuva välitön tavoitettavuus tai odotus siitä eivät sovellu kaikkeen asiakasviestintään. On epätodennäköistä, että asiakasviestintää voitaisiin kokonaan siirtää sähköpostin tai sen kaltaisen järjestelmän ulkopuolelle. Voidaan kuitenkin erottaa vastaanottajan tavoittaminen ilmoitusviesteillä suojaamattomalla sähköpostilla ja varsinainen viestintä suojatussa kanavassa, kuten turvapostissa ja web-pohjaisissa viestintäpalveluissa on tehty.

# Suojatut verkkopalvelut

Organisaatioiden käyttöön on kehitetty myös suojattuja viestintäpalveluja ja portaaleja, jotka eivät varsinaisesti ole sähköpostiviestintää tai pikaviestimiä vaan erikoistuneempia web-sovelluksia, mutta jotka käyttökokemukseltaan ovat ainakin osittain verrattavissa webin kautta käytettävään turvapostiin. Web-sovellusten etu yleiskäyttöiseen sähköpostiin nähden on, että sovellus on yleensä optimoitu johonkin tiettyyn tehtävään, esimerkiksi tiedostojen välittämiseen suojatusti.

Toinen, periaatteellisesti merkittävämpi etu on, että web-sovellus voi tunnistaa vastaanottajan vahvemmin kuin pelkällä sähköpostiosoitteella. Suojatut web-sovellukset tyypillisesti käyttävät perinteistä sähköpostia vain ilmoitusviesteihin, kun jotain huomioitavaa on tapahtunut. Tällaiset SaaS-sovellukset ovat verrattavissa pankkien ja vakuutusyhtiöiden verkkopalveluihin, jotka ovat hyvin suojattuja, viestintäominaisuuksilla varustettuja web-sovelluksia. Mutta toisin kuin yksittäisten finanssitalojen verkkopalveluja, SaaS-sovelluksen voi mikä tahansa organisaatio ottaa oman viestintänsä osaksi. Korkean turvallisuuden verkkopalveluille on olennaista vaatimus, ettei palveluntarjoaja pääse varsinaiseen viestisisältöön käsiksi. Tietosi.fi-palvelu on yksi esimerkki tällaisesta sovelluksesta. Palvelu on kehitetty GDPR-tietopyyntöjen käsittelyyn ja tiedostojen lähettämiseen vahvasti (pankkitunnuksilla tai mobiilivarmenteella) tunnistetuille vastaanottajille.

Viestintäpalvelujen ongelmana on, että tavallisen sähköpostin kautta ei voi lähettää suojattua viestiä mitenkään suoraviivaisella tavalla. Mahdollinen sähköposti-integraatio pitää rakentaa ja suojata erikseen, jolloin käytännössä palataan turvapostiin. Kuten turvapostien webmailit, viestintäsovelluksien käyttöliittymät ovat tasoltaan vaihtelevia, mikä tuskin on jäänyt huomaamatta finanssitalojen verkkopalveluja käyttäviltä kuluttajilta. Toisaalta viestintäsovellus voidaan turvapostia paremmin suunnitella ja optimoida kapeaa niche-käyttötarkoitusta tai maantieteellistä aluetta varten, jolloin myös käyttökokemus voi olla parempi.

## Lopuksi

Sähköpostin suojaaminen ei ole internetin vahvoja kohtia. Uutiset sähköpostijärjestelmien murroista, urkinnasta tai valtiollisesta vakoilusta ovat arkipäiväistyneet. Sähköpostin käyttäjät voivat kuitenkin omalla toiminnallaan vaikuttaa siihen, ettei arkaluontoista aineistoa jää suojaamattomana maailmalle määrittelemättömäksi ajaksi. Tämä kuitenkin edellyttää vähintään muutosta totutuissa käytännöissä ja sen hyväksymistä, että suojattu sähköposti on käytettävyydeltään tavallista sähköpostia huonompi. Tavoiteltaessa korkeinta turvallisuutta, perinteisestä sähköpostista pitää luopua kokonaan vastaanottoilmoituksia lukuun ottamatta.

## Kirjoittaja

**Mika Kukkonen** on osakas ja operatiivinen johtaja Tietosi.fi -palvelua kehittävässä eTaika Oy:ssä. Mikalla on pitkä kokemus ohjelmistoalalla HR-sovellusten kehittämisestä ja henkilötietojen käsittelystä B2B-asiakasrajapinnassa.

## Viitteet


[1] Adobe, "Adobe Consumer Email Survey Report 2017," 25 Elokuu 2017. [Online]. Available: https://www.slideshare.net/adobe/adobe-consumer-email-survey-report-2017.

[2] H. Orman, "Encrypted email : the history and technology of message privacy," 2015. [Online]. Available: https://www.worldcat.org/title/encrypted-email-the-history-and-technology-of-message-privacy/oclc/917888709.

[3] "GDPR. Artikla 28. Henkilötietojen käsittelijä," [Online]. Available: https://fakta.tietosuojamalli.fi/gdpr-asetus/28-henkilotietojen-kasittelija.

[4] "GDPR. Artikla 83. Hallinnollisten sakkojen määräämisen yleiset edellytykset," [Online]. Available: https://fakta.tietosuojamalli.fi/gdpr-asetus/83-hallinnollisten-sakkojen-maaraamisen-yleiset-edellytykset.

[5] Georgia Tech, "Data Categorization," [Online]. Available: https://security.gatech.edu/DataCategorization.

[6] E. Kangas, "What Is Really Protected by SSL and TLS?," 8 April 2017. [Online]. Available: https://luxsci.com/blog/what-is-really-protected-by-ssl-and-tls.html.

[7] D. Kahn, "The codebreakers : the story of secret writing," 1996. [Online]. Available: https://www.worldcat.org/title/codebreakers-the-story-of-secret-writing/oclc/35159231.

[8] Stack Exchange, "How PGP differs from S/MIME," [Online]. Available: https://security.stackexchange.com/questions/7874/how-does-pgp-differ-from-s-mime.

[9] H.-T. G. Chris Hoffman, "Why No One Uses Encrypted Email Messages," 30 4 2014. [Online]. Available: https://www.howtogeek.com/187961/why-no-one-uses-encrypted-email-messages/.

[10] C. David Roe, "Why Email Encryption Still Has A Long Way To Go," 19 4 2018. [Online]. Available: https://www.cmswire.com/information-management/why-email-encryption-still-has-a-long-way-to-go/.

[11] B. Schneier, K. Seidel ja S. Vijayakumar, "A Worldwide Survey of Encryption Products," 11 2 2016. [Online]. Available: https://www.wired.com/wp-content/uploads/2016/02/A-Worldwide-Survey-of-Encryption-Products.pdf.

[12] Helsingin yliopisto, "Sähköpostin suojausmenetelmät," [Online]. Available: https://helpdesk.it.helsinki.fi/ohjeet/yhteydenpito-ja-julkaiseminen/sahkoposti/sahkopostin-suojausmenetelmat.

[13] L. Levison, "Secrets, lies and Snowden's email: why I was forced to shut down Lavabit," 20 5 2014. [Online]. Available: https://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email.