VALTIOVARAINMINISTERIÖ
JulkICT-toiminto

LAUSUNTOVERSIO

21.4.2015

Valtionhallinnon salauskäytäntöjen tietoturvaohje

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä

LUONNOS

x/2015

Saatesivu

Sisällys

Esipuhe

Kyber- ja tietoturvallisuuden merkitys sekä näihin liittyvien ongelmien uutisointi on kasvanut lähes eksponentiaalisesti viimeisten kolmen vuoden aikana. Uutisissa nostetaan esille lähinnä toteutuneita uhkakuvia, jotka ovat heijastuneet esimerkiksi:

- erilaisina salassa pidettävää tai taloudellista tietoa koskevina tietomurtoina, esimerkiksi mittavina hyökkäyksinä kauppojen sähköisiä maksujärjestelmiä vastaan
- organisaation liiketoimintaa haittaavina palvelunestohyökkäyksinä, joissa usein on taustalla taloudellisen edun tavoittelu esimerkiksi kohdeorganisaatiota kiristämällä
- tiedusteluorganisaatioiden toimina, joissa yritetään keräten hyökkääjää kiinnostavaa tietoa pysyen mahdollisimman pitkään salassa
- yksityishenkilöihin kohdistuvina kampanjoina, joilla yritetään saavuttaa taloudellista hyötyä, esimerkiksi pankki- tai muiden järjestelmien käyttäjätunnuksia ja salasanoja kalastelemalla

Yksi tämän ohjeen aihepiiriä sivuava esimerkki ovat lunnashaittaohjelmat (”ransomware”), joilla käyttäjän päätelaite kaapataan rikollisen käyttöön asentamalla siihen haittaohjelma, joka salaa kaiken päätelaitteella olevan tiedon ja estää laitteen käytön; rikollinen lupaa poistaa haittaohjelman jos käyttäjä maksaa vaaditun lunnassumman. Valitettava kehityssuunta saattaa olla se, että lunnashaittaohjelmat voivat kaapata yksittäisen päätelaitteen sijaan koko organisaation tai ainakin osan organisaation keskeisistä palvelimista, tietojärjestelmistä tai palveluista.

Suojaus, sen puute tai huono toteutus päätyvät myös säännöllisesti uutisiin. Kenties yleisin esimerkki on tietomurto verkkopalveluun, jonka käyttäjätietokannassa olevat salasanat ovat vuotaneet murtautujalle; väärällä tavalla salatut salasanat puretaan ja murtautuja julkaisee ne selväkielisinä.

Tiedon salaaminen liittyy joko osittain tai hyvin vahvasti kaikkiin edellä mainittuihin seikkoihin. Eräs tämän vuosikymmenen loppupuolen keskeisiä suuntauksia tulee olemaan tiedon salauksen merkityksen kasvu ja käytön laajentuminen. Tästä hyvä esimerkki on erilaiset pilvipalvelut, joissa salassa pidettävät tiedot sijaitsevat organisaation ulkopuolella jopa ulkomailla ja niitä käytetään internet-verkon ylitse. Niiden käyttöä voidaan laajentaa siinä vaiheessa kun niissä on mahdollista käyttää asiakkaan tarkastamaa ja hyväksymää tiedon salausratkaisua. Lisäksi niihin liittyvä avaintenhallinta tulee toteuttaa siten, että myös se täyttää kaikki asiakkaan salausratkaisulta edellyttämät vaatimukset.

Kuten kaikessa toiminnassa, myös salauksen suunnittelussa, toteutuksessa, käyttöönotossa ja ylläpidossa tulee hyödyntää riskienhallintaa sekä ottaa huomioon organisaation liike- tai ydintoiminnan vaatimukset sekä mahdolliset haasteet, joita käytettävä salaus saattaa sille asettaa. Tietojen salaus tulee huomioida myös organisaation arkkitehtuurisuunnittelussa ja toteutuksessa siten, että organisaatio kehittää ja hyödyntää salausteknologiaa suunnitelmallisesti osana sen arkkitehtuurin kehittämistä.

Termiä **tiedon salaus** käytetään hyvin laajassa merkityksessä. Tässä ohjeessa on pyritty nostamaan esille niitä asioita, joita oikealla tavalla toteutettu salausratkaisu edellyttää. On olemassa sekä huonosti toteutettuja salauksia että sellaisia salausratkaisuja, jotka ovat laadukkaita ja joissa on pyritty huomioimaan käsiteltävänä olevan tiedon salauksen koko elinkaari.
Tämän ohjeen on laatinut Valtion tieto- ja kyberturvallisuuden johtoryhmän (Vahti) asettama tekninen jaosto.

1 Tausta ja tavoite

1.1 Ohjeistuksen tausta

Tietoturvallisuuden merkitys on jatkanut kasvuaan viimeisten vuosien aikana. Keskeisiä muutostekijöitä ovat olleet:

- digitalisoinnin kasvava tarve; yhä useampi toiminto on sähköistetty ja kehitys tulee tältä osin vielä kiihtymään laajamittaisen koko toimintaketjua koskevan digitalisoinnin osalta
- ajasta ja paikasta riippumaton työskentely sekä julkishallinnossa että julkishallinnon palveluita käyttävien asiakkaiden ja kansalaisten keskuudessa
- uusien päätelaitteiden ja langattomien tietoliikenneyhteyksien kehittyminen sekä uudenlaisten käyttötapojen tarve

Edellä kuvatut muutostekijät aiheuttavat myös sen, että eri tasolle luokiteltuja, sekä julkisia että salassa pidettäviä tietoja käsitellään yhä moninaisemmilla tavoilla – mahdollistaen myös tietojen salaamisen.

Laskentatehon nopea kehittyminen heikentää salausta

Tiedon salaaminen pohjautuu matemaattisiin algoritmeihin. Erilaisten laskenta-alustojen suorituskyvyn kehittyminen Mooren lain mukaisesti vaikuttaa käytettävissä olevien salausteknologioiden luotettavuuteen. 1980- tai 1990-luvulla kuviteltu avaimen pituus ei ole enää turvallinen, koska käytettävät teknologiat ovat kehittyneet ja avainten aukipurkamiseen kuluva aika on oleellisesti lyhentynyt purkamiseen käytettyjen tekniikoiden huomattavan kehittymisen myötä. Mitä kriittisemmästä ja pitkäaikaisemmasta säilytyksessä on kyse, sitä tärkeämpää on huolehtia käytettävien avainten pituudesta siten, että ne turvaavat tiedot niiden salassapidolta edellytettävän ajan. Ota yhteys kyberturvallisuuskeskukseen (ncsa@ficora.fi), jos haluat saada lisätietoa tiedon salaamisesta viranomaiskäytössä.

Tietoturvallisuusasetus toi mukanaan salausvaatimuksen

Valtaosa julkishallinnossa käsiteltävästä tiedosta on julkista. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) säätää valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvavaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturva-toimenpiteistä. Asetuksessa määritetään salassa pidettävien asiakirjojen luokittelussa käytettävät suojaustasot sekä eri suojaustasoilla edellytettävät tietoturvatasovaatimukset. Osa vaatimuksista edellyttää, että asiakirja pitää salata tai muulla tavoin suojata. Asetuksessa tai sitä täydentävissä Vahti-ohjeissa (esimerkiksi Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010 tai Sisäverkko-ohje, VAHTI 3/2010) ei ole yksityiskohtaisemmin määritetty miten tiedot pitää salata.

Tiedon salaamista on käsitelty ennen tietoturvallisuusasetuksen voimaantuloa julkaistussa Valtionhallinnon salauskäytäntöjen tietoturvaohjeessa, VAHTI 3/2008. Tämä ohje korvaa Vahti 3/2008 -ohjeen.

1.2 Ohjeen tavoitteet

Tietoturvallisuudessa korostetaan usein sen ensimmäisen osa-alueen, luottamuksellisuuden, toteuttamista samalla kun eheyttä ja saatavuutta pidetään enemmänkin vakioina.

Kuva 1. Luottamuksellisuus, eheys ja saatavuus; tietoturvallisuuden osa-alueiden merkitys vaihtelee eniten salassapidon osalta. Kuitenkaan ne eivät ole koskaan vakioita vaan ne pitää aina arvioida tapauskohtaisesti. Luottamuksellisuuden arvioimiseen käytetään tietoturvallisuusasetuksessa määritettyä tietoaineistojen luokittelua, joka pohjautuu neljään suojaustasoon. Tiedon eheydelle ja saatavuudelle ei ole olemassa vastaavanlaista määritystä, mutta ne arvioidaan yleensä kyseisen kohteen kriittisyyden mukaan organisaation toiminnalle. Tietojärjestelmien osalta saatavuus pyritään varmistamaan palvelukohtaisilla palvelutasosopimuksilla (SLA, service level agreement).

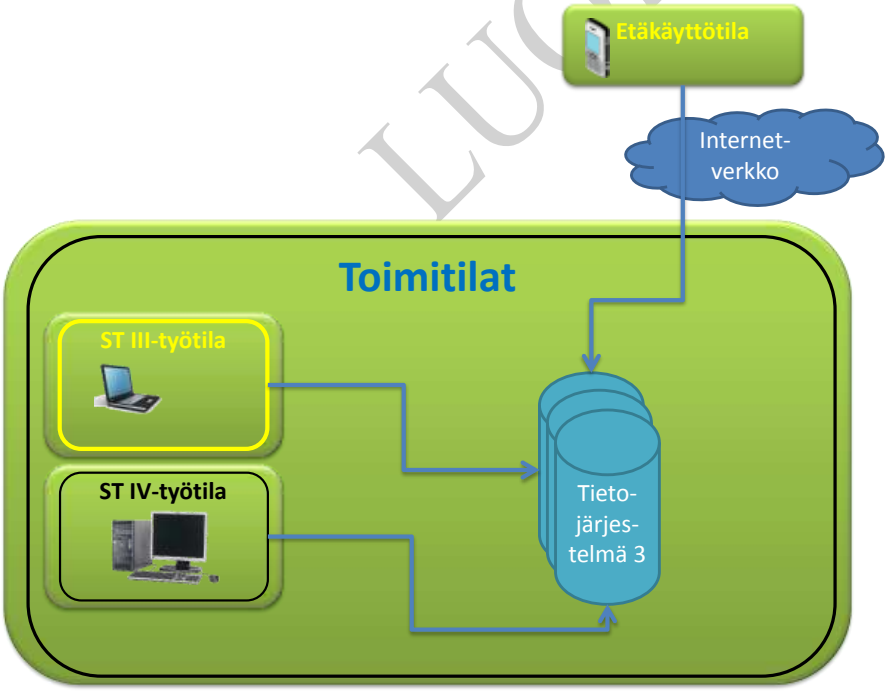
Kuva 2. Julkisen tiedon käsittelyssä korostuvat tietoturvallisuuden kaksi muuta osa-aluetta, tiedon eheyden ja saatavuuden turvaaminen. Organisaatiossa saattaa olla käytössä tietojärjestelmiä, jotka sisältävät salassa pidettävää tietoa, mutta ne eivät ole kovin kriittisiä sen toiminnan kannalta. Toisaalta julkista tietoa sisältävä tietojärjestelmä voi edellyttää, että siinä käsiteltävät tieto ei saa hallitsemattomasti muuttua tai sen saatavuus pitää olla korkein mahdollinen (esim. 99,999%).

Tietoaineiston luokituksen noustessa myös sen luottamuksellisuuden turvaamisen merkitys kasvaa. Keskeiseksi tekijäksi nousee, kuinka tiedon salaaminen tietoaineiston elinkaaren ja tietojenkäsittelyn eri vaiheissa toteutetaan.

Tietoaineiston salauksen tarve riippuu siitä, miten ja millaisissa tietojärjestelmissä salassa pidettävää tietoa käsitellään. Jopa suojaustasojen I ja II tieto voi olla tietojenkäsittely-ympäristössä salaamattomana, mikäli se sijaitsee kaikista verkoista irrotetussa työasemassa, johon pääsy on rajattu sekä tilaturvallisuuden että työaseman käyttöoikeuksien keinoin.

Toisaalta, salaamista edellytetään aina kun salassa pidettävää tietoa käytetään suojaamattomien tietoverkkojen yli esimerkiksi internetin kautta. Internetissä työskenneltäessä päätelaitteen, käytettävien palveluiden ja tietoaineistojen turvallisuus riippuu siitä, että tiedon salaus on toteutettu kaikissa vaiheissa.

Kuva 3. Yksittäisen, kaikista verkoista irrotetun työaseman suojaaminen on mahdollista toteuttaa tilaturvallisuuden keinoin ilman salausta.



Kuva 4. Mitä monimutkaisemmasta tietojenkäsittely-ympäristöstä on kyse, sitä useammassa vaiheessa tarvitaan tiedon salaamista. Pääsääntöisesti tietoliikenneyhteys pitää salata aina kun organisaation verkkoon otetaan yhteys sen omassa hallinnassa olevien tietoliikenneverkkojen ulkopuolelta.

Tietoaineiston eheyden osalta voidaan edellyttää, että viranomaisen hallinnassa oleva tieto ei saa muuttua hallitsemattomasti. Mitä kriittisemmästä tai laajuudeltaan kattavammasta tietoaineistokokonaisuudesta on kyse, sitä tärkeämmäksi eheyden säilyttäminen nousee. Yksittäisen asiakirjan eheys on tärkeä, mutta laajan tietokannan, tietovarannon tai esimerkiksi perusrekisterin eheys on perusedellytys myös koko yhteiskunnan toiminnalle.

Myös tiedon saatavuuden merkitys vaihtelee huomattavasti. Koska tietoturvallisuusasetuksessa määritellyt suojaustasot koskevat vain tiedon salassapitoa, organisaation tulee itse arvioida tiedon eheyden ja saatavuuden merkitys. Tämä on syytä tehdä osana tietojenkäsittelykokonaisuuden priorisointi- tai tärkeysluokitusta, jossa arvioidaan kunkin palvelun merkitys organisaation toiminnalle.

Tässä ohjeessa on kuvattu myös kyberturvallisuuskeskuksen tekemä salaustuotteiden hyväksyntäprosessi.

Jatkossa valtionhallinnon perustietotekniikkapalveluiden tuottaminen keskittyy Valtion tieto- ja viestintätekniikkakeskus Valtoriin, jonka tulee toteuttaa tässä ohjeessa kuvattuja asioita tuottamissaan palveluissa. Valtorin ohella kullekin valtionhallinnon organisaatiolle jää vastuu ohjeen noudattamisesta omissa substanssi-, ydin- tai liiketoimintaan liittyvissä järjestelmissä. Vastuu vaatimustenmukaisen salauksen toteuttamisesta säilyy organisaatiolla, vaikka se olisi ulkoistanut palvelun tuottamisen.

Valtion yhteishankintayksikkö Hansel Oy kilpailuttaa yhteisiä palveluita ja tuotteita valtionhallinnon käyttöön. Tiedon salaamista koskevat vaatimukset tulee huomioida myös näissä kilpailutuksissa mikäli palvelussa, tuotteessa tai osana sitä tarvitaan tiedon salaamista.

1.3 Ohjeen kohderyhmä

Tämä ohje on tarkoitettu kaikille, joiden tehtävänä on vastata organisaation tietoturvallisuudesta tai ICT-palveluista. Lisäksi ohje tulee ottaa huomioon suunniteltaessa tietojärjestelmiä ja muita tiedon salausta edellyttäviä kohteita.

1.4 Ohjeen rakenne

Tämä ohje jakautuu kuuteen lukuun ja x kpl liitteisiin. Lukujen keskeinen sisältö on seuraava:

1. Tausta ja tavoite; kertoo mikä salauksen merkitys on osana tietojen luottamuksellisuuden takaamista, joka on yksi kolmesta tietoturvallisuuden kulmakivestä
2. Tiivistelmä – tarkistuslistat; kuvaa ohjeen näkökulmasta tärkeimmät asiat valtionhallinnon organisaatiolle sekä henkilöstölle, ja sisältää huoneentaulut
3. Tietoturvallisuusasetus, tietoturvatasot ja muut viitekehykset; keskeisimmät aihepiiriin liittyvät valtionhallinnon viitekehykset kuvaa miten tietojen salausta on käsitelty ja millaisia vaatimuksia on erityisesti tietoturvallisuusasetuksessa sekä sen täytäntöönpanoa tukevissa Vahti-ohjeissa
4. Tiedon salaaminen – tekninen viitekehys; teknologiset asiat ja termit, jotka jokaisen salausasioiden kanssa säännöllisemmin työskentelevän henkilön tulisi hallita

5. Avaintenhallinta; osa-alue, joka on keskeinen koska jopa hyvin, vaatimustenmukaisesti toteutettu kokonaisuus voi sortua huonosti tai virheellisesti toteutetun avaintenhallinnan vuoksi
6. Salausratkaisun valinta ja käyttöönotto; kuvaa mihin asioihin salausratkaisun valinnassa ja käyttöönotossa tulee kiinnittää huomiota sekä erilaisia käyttötapauksia salausten toteuttamisesta

2 Tiivistelmä - tarkistuslistat

Olemme koonneet tähän lukuun kaksi tiivistä tarkistuslistaa, jotka kuvaavat tärkeimmät asiat tiedon salauksessa. Ensimmäinen on laadittu organisaatioille ja toista voidaan käyttää jalkautettaessa tätä ohjetta henkilöstölle. Ne kuvaavat mitä asioita tulee huomioida organisaatiotasolla sekä mitkä ovat tärkeimmät henkilöstön ja organisaation loppukäyttäjän huomioitavat asiat.

2.1 Huoneentaulu – organisaatio

1. Tietoaineistojen oikeaoppinen luokittelu; mikäli luokittelu tehdään väärin tai tarpeettoman laajasti tietojärjestelmän ympäristöihin (esim. kehitys-, testiympäristöt tai muut tietojärjestelmän osat), se aiheuttaa joko ylimääräisiä kustannuksia tai vaarantaa salassa pidettävän tiedon luottamuksellisuuden

2. Tarve-analyysi; kartoittakaa mihin tietojen salausta tarvitaan ja mitkä ovat ne vaatimukset, johon tiedon salaaminen perustuu

3. Kansainvälisten salassa pidettävien tietojen käsittelyvaatimukset poikkeavat vastaavista kansallisista vaatimuksista

4. Käytettävien salaustuotteiden määrittely ja valinta; usein toteutuksia tai palveluita hankittaessa hyväksytään, että siinä on jokin salaus. Tässä ohjeessa pyritään tuomaan esille se seikka, että on olemassa erilaisia salauksia, joita ei ole aina toteutettu huolellisesti ja vaatimusten mukaisesti

5. Salaustuote sellaisenaan ei riitä, vaan tulee myös selvittää kyseisen tuotteen käyttötarkoitukseen soveltuvat ominaisuudet, asetukset ja muu konfiguraatio (esim. että ei vahingossa sallita vanhentuneita tai heikommin turvattuja ominaisuuksia, protokollia tai vastaavia)

6. Avaintenhallinnan suunnittelu; vaikka salaus olisi muuten toteutettu oikeaoppisesti, kaikki vaatimukset huomioiden ja täyttäen, ratkaisu voidaan pilata puutteellisesti suunnitellulla avaintenhallinnalla

7. Avaintenhallinnan toteuttaminen; vaikka kaikki olisi suunniteltu oikeaoppisesti, erityisesti avaintenhallinnan osalta pitää esimerkiksi auditointien ja tarkastusten avulla varmistua siitä, että suunnitelmat on myös toteutettu sovitulla tavalla ja vaatimustenmukaisesti.

8. Salausjärjestelmiin liittyy usein varmenteita, joilla on voimassaoloaika. Organisaatioiden tulee huolehtia varmenteiden uusimisesta hyvissä ajoin ennen niiden vanhenemista.

9. Organisaation on syytä salata kaikkien työasemien kovalevyt. Internetistä löytyy helposti lukuisia helppokäyttöisiä ohjeita, joiden avulla päästään kiinni salaamattoman työaseman tietoihin. Mikä tahansa käytössä oleva kiintolevyn salaustuote pienentää tätä riskiä.

10. Kokonaisuuden auditoiminen; kaikkia palveluita tai tietojärjestelmiä ei ole tarkoituksenmukaista tai järkevää auditoida. Oleellista on se, että organisaatiolla on suunnitelma, joka kuvaa mitkä ovat auditointia edellyttäviä palveluita tai tietojärjestelmiä, ja kuinka ne toteutetaan. Käytännössä auditoinnit voidaan kuvata esimerkiksi osana palvelun tietoturvallisuuden vuosikelloa.

11. Salaus on vain yksi osa organisaation monikerroksista suojautumista. Salaus ei yksinään riitä, vaan se on tärkeä osa-alue ns. sipulimaisessa tietoturva-arkkitehtuurissa. Sen avulla varaudutaan siihen, että yksittäisen osa-alueen pettäessä tai murtautujan päästessä siitä läpi, seuraavat kerrokset suojaavat edelleen tietoa. Salaus on siinä mielessä haasteellinen, että normaalisti tietoa ei salata useilla salauksilla; salassa pidettävä tieto saattaa paljastua salauksen pettäessä tai puuttuessa.

12. Omistajan vastuu; organisaatio on aina itse vastuussa omistamistaan tiedoista ja käytössä olevista tietojärjestelmistään, vaikka niiden tuottamisesta vastaisi jokin ulkopuolinen taho, joko valtionhallinnon organisaatio tai kaupallinen toimittaja. Vastuuta ei ole mahdollista ulkoistaa.

2.2 Huoneentaulu – käyttäjä

1. Tietoaineistojen oikeaoppinen luokittelu; vaikka organisaatio olisi toteuttanut tietojärjestelmät ja niiden salausratkaisut oikeaoppisesti, se ei auta mikäli henkilöstö ei osaa luokitella tietoa ja käyttää luokituksen mukaisia tietojärjestelmiä oikein läpi tiedon koko elinkaaren.

2. Henkilöstön tulee käyttää ohjeistetulla tavalla määrättyjä työvälineitä, mukaan luettuna tiedon salausratkaisut sähköpostin käsittely, päätelaitteiden käyttö sekä tiedon kuljettaminen ulkoisilla apumuisteilla (usb- ja muut muistit).

3. Valtionhallintoon kohdistuu usein tiukemmat turvallisuusvaatimukset kuin yksityisiin yrityksiin. Tämän takia tulee huomata, että kaikkia yksityisellä puolella käytössä palveluita tai toimintatapoja ei ole välttämättä mahdollista käyttää valtionhallinnossa, johtuen esimerkiksi tiedon salassapitoon tai salaukseen liittyvistä vaatimuksista.

4. Vaikka digitalisoimme toimintojamme kiihtyvällä tahdilla, tietoaineistoja käsitellään jatkossakin usein tavoin, jotka eivät kaikki ole sähköisiä. Esimerkiksi keskusteluissa tai käsiteltäessä paperimuotoisia aineistoja, tietojen salaaminen ei ole mahdollista samalla

tavoin kuin tietojärjestelmissä tai tietoliikenteessä. Noudata organisaatiosi antamia ohjeita turvallisesta työskentelystä.

5. Henkilöstön velvoitteena on kysyä ja kyseenalaistaa asioita silloin kun herää epäilys, että jokin asia ei ole niin kuin sen pitäisi olla tai että asiassa vaikuttaisi olevan jotain outoa. Esimerkiksi jos käyttäjä saa sähköpostitse salassa pidettävää tietoa, jota ei ole millään lailla salattu. Samoin jos www-sivusto huomauttaa siitä, että sen käyttämä varmenne ei ole toimiva, tästä tulee ottaa yhteyttä joko palvelua tuottavan organisaation tai oman organisaation palvelupisteeseen ja pyytää korjaamaan tai muuten selvittämään asia.

   Henkilöstön tulee kaikissa turvallisuuteen liittyvissä epäselvissä tai muuten epäilyttävissä tilanteissa ottaa yhteyttä, organisaation ohjeistuksen mukaan, yleensä omaan esimieheen ja/tai organisaation turvallisuuden vastuuhenkilöihin tai palvelupisteeseen.

3 Tietoturvallisuusasetus, tietoturvatasot ja muut viitekehykset

Tässä luvussa käsitellään keskeisiä säädöksiä ja ohjeita, jotka tulee ottaa huomioon tiedon salaamista suunniteltaessa ja toteutettaessa.

3.1 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)

Tietoturvallisuusasetuksessa salausta käsitellään 16 § Sähköisen asiakirjan laatiminen, tallettaminen ja muokkaaminen, jossa todetaan

”Valtionhallinnon viranomainen voi sallia, että suojaustasoon I tai II kuuluva asiakirja talletetaan sähköisesti tietovälineelle tai muulle laitteelle, joka:
*1) ei ole liitetty tietoverkkoon, jos asiakirja talletetaan **vahvasti salattuna** tai jos se on muutoin vahvasti suojattu; tai*

2) on liitetty vain sellaiseen viranomaisen tietoverkkoon, joka yhdistää asiakirjan tallettamiseen ja säilyttämiseen käytetyn laitteen samassa viranomaisen hallinnassa olevassa erityisvalvotussa tilassa oleviin muihin laitteisiin, jos laitteet yhdistävään tietoverkkoon ei ole luotu yhteyttä muista tietoverkoista ja asiakirjan käsittely on muutoin vahvasti suojattua.

*Valtionhallinnon viranomainen voi sallia, että suojaustasoon II kuuluva asiakirja talletetaan sähköisesti viranomaisen sellaiseen tietoverkkoon liitetylle tietovälineelle tai muulle laitteelle, jonka käyttö on rajoitettu, jos asiakirja talletetaan **vahvasti salattuna** tai se on muutoin vahvasti suojattu ja viranomainen on muutoinkin varmistanut, että tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät tavanomaisesti sovellettavan korkean tietoturvallisuustason vaatimukset.*

*Valtionhallinnon viranomainen voi sallia, että suojaustasoon III kuuluva asiakirja talletetaan viranomaisen tietoverkkoon liitetylle laitteelle, jos verkon käyttö on rajoitettu ja asiakirja talletetaan **salattuna** tai muutoin suojattuna siten, että tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät tavanomaisesti sovellettavan korotetun tietoturvallisuustason*

vaatimukset. Sama koskee suojaustasoon IV kuuluvaa arkaluonteisia henkilötietoja tai biometrisiä tunnistetietoja sisältävää henkilörekisteriin talletettua asiakirjaa."

Vastaava kohta löytyy asetuksen §19, jossa käsitellään asiakirjan siirtämistä tietoverkossa:

*"Suojaustasoon II kuuluvan asiakirjan saa lisäksi siirtää sellaisessa viranomaisen tietoverkossa, jonka käyttö on rajoitettu, jos asiakirja on **vahvasti salattu** tai se on muutoin vahvasti suojattu ja valtionhallinnon viranomainen on muutoinkin varmistanut, että tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät tavanomaisesti sovellettavan korkean tietoturvallisuustason vaatimukset."*

Kuten huomataan, asetuksessa ei ole tarkemmin määritelty, miten (vahvasti) salaaminen tai muutoin (vahvasti) suojaaminen tulee toteuttaa. Salaustarpeita on kuvattu hieman tarkemmalla tasolla VAHTI 2/2010-ohjeessa.

"Vahva salaus" (strong encryption) tarkoittaa salakirjoitusta, joka ei ole millään tunnetulla hyökkäysmenetelmällä murrettavissa, tai vaarassa tulla murretuksi, sinä aikana, jolloin tiedon on pysyttävä salassa. On huomattava, että salauksen vahvuus riippuu sekä salausalgoritmin parametreistä ja teknisistä ominaisuuksista, että salausavaimen pituudesta. JulkL:n säätelemää salassapidettävää tietoa koskevat lisäksi erityissäädökset, jotka luokittelevat myös salaustoteutukset suojaustasojen mukaisiin luokkiin. Tällöin puhutaan /suojaustason mukaisesta salauksesta, esimerkiksi "STII-tason mukainen salaus", tai lyhyemmin "STII-salaus".

"Muutoin suojaaminen" tarkoittaa muilla tavoilla kuin salaamalla tapahtuvaa suojausta, joka voi käsittää yhtä tai useampaa esimerkiksi seuraavista vaihtoehdoista:

- tilaratkaisut, tietoa käsitellään sellaisessa tilassa, joka mahdollistaa kyseisen suojaustason salassa pidettävän tiedon käsittelyn ilman salausta
- käyttö- ja pääsyoikeuksien hallinta; tietoon voivat päästä käsiksi vain sellaiset henkilöt, joilla on siihen työtehtäviin liittyvä tarve,

Nämä keinot eivät välttämättä yksinään riitä, jos kohteeseen pääsy tapahtuu muuten kuin kaikista tietoliikenneverkoista irrotetulla työasemalla. Käyttötapauksesta riippuen salausta voidaan tarvita tietoliikenneverkoissa.

3.2 VAHTI 2/2010

Salauksen käyttötarvetta eri tilanteissa on ohjeistettu VAHTI 2/2010 –ohjeessa (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta). Sen luvussa 8.1 Perusvaatimuksia sivulla 64 on esitetty muun muassa seuraavat vaatimukset:

	ST IV	ST III	ST II	ST I
Siirto avoimissa verkoissa	Salattuna tai muutoin suojattuna	Salattuna tai muutoin suojattuna	Ei sallittu	Ei sallittu
Siirto viranomaisen verkoissa	Selväkielisenä perus- ja sitä korkeamman tietoturvallisuustason verkoissa	Selväkielisenä korotetun tai korkean tietoturvallisuustason verkoissa	Selväkielisenä valvotuissa korkean tietoturvallisuustason verkoissa	Vahvasti salattuna tai muutoin vahvasti suojattuna valvotuissa erillisverkoissa

Taulukko 1. Perusvaatimuksia koskien salaamista tietoa siirrettäessä. [taulukot tulevat sähköiseen www.vahtiohje.fi myös tekstimuotoisena, jolloin niihin voidaan kohdistaa hakutoimintoja]
Liitteen 3 kohdassa 5.2 Tietopalvelujen toteuttaminen sivu 80 todetaan:

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(5)	Salassa pidettävän tietoaineiston käsittely avoimissa tietoverkossa.	salattuna tai suojattuna avoimissa tietoverkoissa	salattuna tai suojattuna avoimissa tietoverkoissa	vahvasti salattuna tai vahvasti suojattuna avoimissa tietoverkoissa	käsittely ei sallittu avoimissa tietoverkoissa.
(6)	Salassa pidettävän tietoaineiston käsittely viranomaisen tietoverkossa.	selväkielisenä käyttövaltuuden tarkistavassa, perustietoturvallisuustason tietoverkossa	selväkielisenä korotetun tai korkean tietoturvallisuustason tietoverkoissa	selväkielisenä valvotuissa korkean tietoturvallisuustason vaatimukset täyttävissä tietoverkoissa	sallittu vahvasti suojattuna erillisverkossa, joka täyttää korkean tietoturvallisuustason vaatimukset ja johon ei ole yhteyttä muista tietoverkoista
(7)	Salassa pidettävän tietoaineiston tallentaminen viranomaisen tietoverkoissa	perustietoturvallisuustason palvelemilla voidaan tallentaa selväkielisenä suojattuna käyttäjätunnuksilla, suositellaan salausta,	perustietoturvallisuustason palvelimilla salattuna tai suojattuna; korotetun ja korkean tietoturvallisuustason palvelimilla sallitaan selväkielisenä	vahvasti salattuna tai vahvasti suojattuna, jos järjestelmä täyttää korkean tietoturvallisuuden tason vaatimukset.	sallittu vahvasti suojattuna valvotussa erillisverkossa joka täyttää korkean tietoturvallisuustason vaatimukset.
(8)	Salassa pidettävän tietoaineiston käsittely sähköisessä muodossa työpaikan ulkopuolella Käsittely edellyttää kaikissa luokissa viranomaisen päätöstä (vrt TTA 16 §)	sallittu, tieto tulee suojata, esimerkiksi salausta käyttäen	sallittu, tieto tulee tallentaa salattuna	erillishyväksyntä, tieto tulee tallentaa vahvaa salausta käyttäen	ei sallittu ilman tapauskohtaista viranomaispäätöstä

Taulukko 2. Taulukossa määritellään useita kohteita, joissa salausta tulee käyttää, mutta ohjeessa ei anneta yksityiskohtaisempia ohjeita salauksen toteuttamisesta.

Lisäksi liitteen 3 kohdassa 6 Tietoaineistojen siirto sivulla 89 todetaan:

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(6)	Salassa pidettävän turvallisuusluokitellun tiedon käsittely puhelimessa (ilman salauslaitetta)	kyllä, harkiten	ei sallittu	ei sallittu	ei sallittu
(7)	Salassa pidettävän tiedon käsittely puhelimessa (ilman salauslaitetta)	kyllä, harkiten	kyllä, harkiten	ei sallittu	ei sallittu
(8)	Salassa pidettävän tiedon käsittely salauslaitteella varustetulla puhelimella (päästä päähän salaava puhelinyhteys; salauslaitteelta edellytetään viranomaisen hyväksyntää kyseiseen suojaustasoon kuuluvan tiedon käsittelyyn)	selväkielisenä	selväkielisenä	selväkielisenä	ei sallittu
(9)	Salassa pidettävän tiedon siirto tekstiviestipalveluna	ei sallittu ilman salausta	ei sallittu ilman salausta	ei sallittu ilman vahvaa salausta	ei sallittu

Taulukko 3. Tiedon salaaminen pitää huomioida muussakin kuin teknisessä toiminnassa, esimerkiksi puhelimessa puhuttaessa.

(12)	Sähköisen asiakirjan siirto avoimissa tietoverkoissa	salattuna tai muutoin viranomaisen päättämällä tavalla suojattuna	salattuna tai muutoin suojattuna	ei sallittu	ei sallittu
(13)	Sähköisen asiakirjan siirto viranomaisen sisäverkoissa Salassa pidettäviä tietoaineistoja ja tietoja saa siirtää vain sellaisissa tietojärjestelmien ja tietoverkkojen osissa, jotka täyttävät kyseisen suojaustason edellyttämät vaatimukset tietovarantojen siirrolle.	selväkielisenä perustietoturvallisuustason ympäristössä	suositellaan salausta, selväkielisenä korotetun tietoturvallisuustason ympäristössä	vahvasti salattuna selväkielisenä korkean tietoturvallisuustason ympäristössä	rajoitetusti *
(14)	Sähköisen asiakirjan siirto muistivälinettä käyttäen Muistivälineet, joita käytetään kiinteän työhuoneen ulkopuolella, tulee varustaa koko tietovarannon salaavilla menetelmillä. Lisäksi luokkakohtaisesti edellytetään: (Katso myös taulukko 8, kohta 5) Sisältäessään tietoa muistivälineitä (kiintolevyt, muistivälineet) on käsiteltävä niiden sisältämän korkeimman suojaustasoa edellyttävän tiedon mukaisesti.	kyllä	kyllä	kyllä Kaikki tietojen siirto työvälineestä toiseen tulee kirjata lokiin. Samoin hävittämiset. Tiedon talletiointi on sallittu vain erikseen valvottaviin muistivälineisiin	kyllä Sallittu vain nimetyissä työasemissa. Tiedon kopiointi sallittu vain laatijan kirjallisella luvalla.

Taulukko 4. Tiedon salaaminen koskee kaikkea työskentelyä. Sen huomioiminen on usein hankalaa eikä ole mahdollista toteuttaa keskitetysti tai kokonaisvaltaisesti yhdenmukaisilla tuotteilla ja menetelmillä.

Sivulla 91 liitteen 3 kohdassa 8 Tietoaineistojen säilytys ja tallennus todetaan:

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(4)	Tietoverkon palvelimille talletetun tietovarannon salaaminen tai muu vahva suojaaminen	perustietoturvallisuustason ympäristössä voidaan tallentaa selväkielisenä, suositellaan salausta	perustietoturvallisuustason palvelimilla salattuna, korotetun ja korkean tietoturvallisuustason palvelimilla sallitaan selväkielisenä	korkean ja korotetun tietoturvallisuustason palvelimilla salattuna	rajoitetusti *
(5)	Sisältäessään tietoa tietovälineitä on käsiteltävä niiden sisältämän korkeimman suojaustasoa edellyttävän tiedon mukaisesti. Laitteet tulee varustaa koko tietovarannon salaavilla menetelmillä.	suositellaan salausta	kyllä	kyllä, vahvaa salausta käyttäen	rajoitetusti *

Taulukko 5. Sellaiset vaatimukset, joissa suositellaan salausta, kannattaa arvioida riskilähtöisesti ja tehdä päätös mahdollisesti tarvittavasta salauksesta.

Liitteen 3 kappaleessa 9 Pääsy tietoon (tiedon käyttö) sivulla 92 todetaan:

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Tietoverkon palvelimilla olevan tietovarannon lukeminen	selväkielisenä perustietoturvatason verkoista alkaen	selväkielisenä korotetun tietoturvallisuustason verkoista alkaen	selväkielisenä korkean tietoturvallisuustason verkoissa	rajoitetusti *
(2)	Etäkäyttö työnantajan tähän käyttöön antamilla välineillä ja yhteydellä edellyttäen, että käyttöympäristö täyttää tiedon suojaukselle asetetut vaatimukset	sallittu suojattua yhteyttä käyttäen	sallittu suojattua yhteyttä käyttäen, käyttäjän vahva todentaminen	sallittu vahvasti salattua tai suojattua yhteyttä käyttäen korkean tietoturvallisuustason valvotussa verkossa, käyttäjän vahva todentaminen	ei sallittu
(3)	Käyttäjän tietoverkkoon liitetyn työaseman vähimmäisvaatimukset	perustietoturvallisuustason työasema	korotetun tietoturvallisuustason työasema	korkean tietoturvallisuustason työasema	ei sallittu

Taulukko 6. Tiedon salaaminen ja käyttäjän (vahva) tunnistaminen nousevat keskeiseen asemaan myös etäkäytössä ja etätyöskentelyssä.

3.3 *VAHTI 3/2010*

Salauksen käyttöä eri tilanteissa on ohjeistettu myös VAHTI 3/2010 Sisäverkko-ohjeessa. Ohjeen luvussa 12.2 on esitetty muun muassa seuraavat vaatimukset:

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
12.4	Kansallisen salassa pidettävän tiedon siirrossa käytetään salausta, kun verkko menee viranomaisen valvoman tilan ulkopuolelle.	suositus	suositus	pakollinen vaatimus
12.5	Kansallisen ja kansainvälisen turvallisuusluokitellun tiedon siirrossa käytetään salausta aina, kun verkko menee viranomaisen valvoman tilan ulkopuolelle.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
12.6	Salaukseen tulee käyttää vähintään siirrettävän aineiston suojaustasolle hyväksyttyjä salausratkaisuja	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

Taulukko 7. Tiedon salaaminen viranomaisen valvoman tilan ulkopuolella.

3.4 *Laki kansainvälisistä tietoturvallisuusvelvoitteista*

Kansainvälisiä tietoturvallisuusvelvoitteita koskevassa laissa (588/2004) säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi. Laissa säädetään turvallisuusviranomaisten tehtävistä ja erityissuojattavan aineiston suojaamista koskevista tietoturvatoimenpiteistä.

Keskeisimmissä Suomea sitovissa kansainvälisissä velvoitteissa, kuten EU:n neuvoston turvallisuussäännöissä (2013/488/EU), edellytetään turvallisuusluokitellun tiedon salaamista esimerkiksi tilanteissa, joissa tieto liikkuu verkossa fyysisesti suojattujen alueiden ulkopuolella. Esimerkiksi EU:n turvaluokitellulle tiedolle salaustuotteen tulee lisäksi olla kansallisen viranomaisen (CAA, Crypto Approval Authority, Suomessa Viestintäviraston NCSA-toiminto) hyväksymä.

3.5 Katakri

Katakri on kansallisen turvallisuusviranomaisen (NSA, National Security Authority) julkaisema auditointityökalu viranomaisten salassa pidettävien tietoaineistojen käsittelykyvyn arvioimiseksi. Katakriin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset sekä esimerkkejä mahdollisista toteutusmalleista. Katakri ei siis itsessään aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. Katakri on tarkoitettu käytettäväksi silloin kun arvioidaan velvoittaviin sitoumuksiin perustuvien tietoturvallisuusvaatimusten toteutumista. Katakrin keskeisin kansalliseen lainsäädäntöön kuuluva vaatimuslähde on valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010). Kansainvälisenä lähteenä on käytetty ensisijaisesti EU:n neuvoston turvallisuussääntöjä

(2013/488/EU). Katakrin vaatimukset on koottu niin, että niistä muodostuu riittäväksi arvioitu kokonaisuus kansallisten tai kansainvälisten salassa pidettävien tietojen suojaamiseksi oikeudettomalta paljastumiselta ja käsittelyltä.

Katakria voidaan käyttää auditointityökaluna silloin, kun tarkoituksena on todentaa, täyttävätkö viranomaisten tai yritysten tietojärjestelmät ja toiminta niiltä edellytettävät kansalliset tai kansainväliset tietoturvavaatimukset. Salausta edellyttäviä käyttötapauksia on kuvattu yksityiskohtaisemmin luvussa 6.2 Tarveanalyysi.

4 Tiedon salaaminen – tekninen viitekehys

Yksi keskeinen keino tiedon suojaamiseen on sen salaaminen. Salaamisella tavoitellaan tiedon luottamuksellisuutta; sitä, että ulkopuoliset tahot eivät pysty lukemaan tai muuten käsittelemään tietoa. Luottamuksellisuus on kuitenkin vain yksi tietoturvallisuuden tekijöistä. Muita usein tavoiteltuja tekijöitä ovat tiedon eheys, saatavuus ja autenttisuus. Eheydellä tarkoitetaan mm. sitä, että kaikki tietoon tehtävät muutokset ovat havaittavissa. Saatavuus tarkoittaa sitä, että oikeutetuilla tahoilla on tarvittaessa pääsy tietoon. Autenttisuudella taas viitataan varmuuteen tiedon alkuperästä.

Kryptologia on tieteenala, jossa tutkitaan pääasiassa luottamuksellisuuden, eheyden ja autenttisuuden takaamiseksi tarkoitettuja menetelmiä. Kryptoanalyysillä tarkoitetaan heikkouksien etsimistä edellä mainituista menetelmistä ja kryptografialla näiden menetelmien suunnittelua. Tiedon autenttisuuden takaamiseksi on kehitetty sähköiset allekirjoitukset, jotka eivät itsessään salaa tietoa. Eheyden varmistamiseen voidaan taas käyttää tiivistefunktioita. Tiedon saatavuutta ei sen sijaan voida taata suoraan kryptologisilla menetelmillä.

Seuraavissa luvuissa käsitellään luottamuksellisuuden, eheyden ja autenttisuuden takaamiseksi käytettyjä kryptologisia menetelmiä. Puhekielessä salausmenetelmillä tarkoitetaan välillä tiedon luottamuksellisuuden takaamiseksi suunniteltujen menetelmien lisäksi myös eheyden ja autenttisuuden takaamiseksi suunniteltuja menetelmiä. Oheisessa tekstissä salausmenetelmillä tarkoitetaan kuitenkin ainoastaan tiedon salaamiseen käytettäviä menetelmiä.

4.1 Algoritmi ja avain

Tiedon suojaamiseen käytetään erilaisia algoritmeiksi kutsuttuja laskennallisia menetelmiä. Luottamuksellisuuden ja autenttisuuden takaamiseksi tarkoitetut menetelmät käyttävät avainta tai avainparia algoritmin parametreina. Pelkästään virheenkorjaukseen eli eheyden varmistamiseen tarkoitetuissa menetelmissä avaimia ei yleensä tarvita. Salausmenetelmät voidaan jakaa symmetrisiin ja epäsymmetrisiin sen mukaan, käytetäänkö avainta vai avainparia. Symmetrisissä menetelmissä hyödynnetään yhtä salaista avainta ja epäsymmetrisissä avainparia, jonka toinen avain on yksityinen ja toinen julkinen.

Menetelmän turvallisuus riippuu vahvasti käytettyjen avaimien pituudesta, jolla tarkoitetaan avaimen esittämiseen tarvittavien bittien lukumäärää. Eri menetelmien avainpituuksia ei voi käyttää suoraan niiden turvallisuuden vertailuun; esimerkiksi epäsymmetrisen RSA-salausmenetelmän

turvallisuus 3072-bittisillä avaimilla vastaa suurin piirtein symmetristä AES-salausmenetelmää 128-bittisellä avaimella.

4.2 Tiedon salaaminen

4.2.1 Symmetrinen salaus

Symmetriset salausmenetelmät käyttävät samaa avainta tiedon salaamiseen ja sen purkamiseen. Symmetriset menetelmät toimivat usein moninkertaisesti nopeammin kuin epäsymmetriset. Siksi niitä käytetään tyypillisesti suurien datamäärien salaamiseen, esimerkiksi kun tietoa siirretään avoimessa verkossa tai kun tietoa halutaan säilyttää salattuna massamuistilla.

Symmetristen menetelmien heikkous on se, että käytetty avain tulee siirtää turvallisesti kaikille osapuolille. Avain pitää myös pysyä ainoastaan näiden tahojen tiedossa, sillä sen paljastuminen tarkoittaa kaikkien sillä salattujen viestien paljastumista. Avaintenhallinta-luvussa on kuvattu tarkemmin avainten muodostamiseen ja käsittelyyn liittyviä seikkoja.

4.2.2 Epäsymmetrinen salaus

Epäsymmetriset salausmenetelmät käyttävät tiedon salaamiseen ja purkamiseen eri avainta. Avaimet muodostavat avainparin; salaamiseen käytetty avain on julkinen ja purkamiseen käytetty avain ainoastaan viestin vastaanottajan tiedossa. Kuka tahansa voi lähettää salatun viestin epäsymmetrisen avainparin omistajalle hänen julkista avaintaan käyttäen. Tällä tavalla salatun viestin voi purkaa ainoastaan viestin vastaanottaja yksityisellä avaimellaan. Avainparin avaimet tulee muodostaa yhdessä, sillä ne ovat kytköksissä toisiinsa salausmenetelmästä riippuvalla tavalla. Epäsymmetristen menetelmien etuna on se, että viestinnän osapuolet voivat lähettää toisilleen salattuja viestejä, jos he tietävät toistensa julkiset avaimet. Salauksen purkamiseen käytettyä avainta ei tarvitse välittää eri osapuolille kuten symmetrisissä menetelmissä. On kuitenkin huolehdittava, että julkiset avaimet ovat autenttisia, esim. välittämällä ne luotettavasti eri osapuolille.

Epäsymmetristen menetelmien heikkous on se, että ne ovat hitaampia kuin symmetriset menetelmät ja niiden toteutukset ovat tyypillisesti monimutkaisempia. Ne saattavat myös olla alttiimpia tietyille hyökkäystyypeille. Huolellisella toteutuksella ja tarkoin mietityllä käyttöpolitiikalla voidaan kuitenkin välttää hyökkäysten muodostamaa uhkaa. Myös käytetyt avainpituudet eroavat; epäsymmetrisessä menetelmässä on yleensä käytettävä huomattavasti pidempiä avaimia jotta saavutettaisiin sama turvallisuustaso kuin symmetrisissä menetelmissä.

4.2.3 Symmetristen ja epäsymmetristen menetelmien yhteiskäyttö

Symmetristen ja epäsymmetristen menetelmien ominaisuuksien takia useat salausjärjestelmät käyttävät niitä yhdessä viestien salaamiseen. Tyypillinen tapa on käyttää epäsymmetristä salausta symmetrisen menetelmän avaimen salaamiseen. Näin muodostettua salausjärjestelmää kutsutaan hybridisalaukseksi. Symmetrisen avaimen muodostava osapuoli voi lähettää sen vastaanottajalle käyttäen salaamiseen julkista avainta. Vastaanottaja voi purkaa salauksen oman avainparinsa salaisella avaimella. Näin symmetrinen avain voidaan välittää turvallisesti viestinnän osapuolille, jonka jälkeen muun viestinnän salaamiseen voidaan käyttää symmetristä salausta.

Symmetrisen menetelmän avaimen sopimista kutsutaan avaintenvaihdoksi. Sen tekemiseen on myös muita tapoja, joita käsitellään Avaintenhallinta-luvussa.

4.3 Tiedon eheyden varmistaminen

Tiedon eheys voidaan varmistaa esimerkiksi kryptografisen tiivisteen avulla. Se on lyhyt, viestistä muodostettu bittijono, joka lasketaan niin sanotun tiivistefunktion avulla. Tiivisteitä voidaan käyttää eheyden varmistamisen lisäksi myös tiedon autentikointiin.

Tiivistefunktioilta vaaditaan seuraavia ominaisuuksia:

- Se tulisi olla nopea laskea mistä tahansa viestistä.
- Pelkästään tiivisteen perusteella ei tulisi olla käytännössä mahdollista selvittää viestiä, josta tiiviste on laskettu.
- Viestiä ei tulisi olla mahdollista muuttaa ilman siitä lasketun tiivisteen muuttumista.
- Ei tulisi olla mahdollista löytää kahta erilaista viestiä, joiden tiivisteet ovat samoja. Tätä ominaisuutta kutsutaan myös törmäyksettömyydeksi.

Jos viestiä muutetaan, niin siitä lasketun tiivisteen tulisi muuttua edellä mainitun ominaisuuden takia. Näin tiivisteen avulla voidaan tarkistaa viestin eheys. Jos tiivisteen laskemiseen käytetään viestin lisäksi avainta, joka on vain lähettäjän ja vastaanottajan tiedossa, voidaan varmistua myös viestin alkuperästä eli viestin autenttisuudesta. Näin muodostetusta tiivisteestä käytetään nimeä Hash-Based Message Authentication Code (HMAC). Jos kuitenkin avaimen tietää useampi taho, ei viestin lähettäjästä voida olla varmoja toisin kuin käytettäessä sähköisiä allekirjoituksia.

4.4 Tiedon autentikointi

Tiedon autentikointiin eli alkuperän osoittamiseen käytetään usein sähköisten allekirjoitusten menetelmiä. Vaikka niitä ei käytetäkään viestinnän salaamiseen, ne luokitellaan epäsymmetrisiksi menetelmiksi, sillä ne perustuvat samaan matemaattiseen teoriaan kuin epäsymmetriset salausmenetelmät. Allekirjoitus on viestistä laskettu bittijono, jonka viestin lähettäjä tekee käyttäen yksityistäavaintaan. Vastaanottaja voi tarkastaa viestin autenttisuuden lähettäjän julkisen avaimen avulla.

Jotta viestit voidaan autentikoida, tulee vastaanottajan olla varma siitä, että käytetty julkinen avain todellakin kuuluu viestin lähettäjälle. Tätä varten lähettäjän identiteetin ja hänen julkisen avaimensa muodostama kokonaisuus yleensä allekirjoitetaan sähköisesti. Allekirjoituksen tekee taho, johon molemmat viestinnän osapuolet luottavat. Tätä tahoa kutsutaan nimellä varmentaja (engl. Certificate Authority, CA). Allekirjoitettua identiteetin ja julkisen avaimen muodostamaa kokonaisuutta kutsutaan varmenteeksi. Kun vastaanottaja saa viestin, hän tarkastaa varmenteen avulla, että julkinen avain kuuluu lähettäjälle, jonka jälkeen myös viesti voidaan autentikoida. Käyttäjien muodostamat luottamussuhteet muodostavat julkisen avaimen infrastruktuurin (engl. Public Key Infrastructure, PKI), jota käsitellään tarkemmin Avaintenhallinta-luvussa.

4.5 Suosituksia

Luottamuksellisuuden, eheyden ja autenttisuuden takaamiseksi on olemassa useita standardoituja

menetelmiä. Yleensä tiedon suojaamisessa luotetaan standardoituihin menetelmiin, joiden turvallisuutta on tutkittu laajasti. On suositeltavaa valita kryptografiset menetelmät standardoitujen menetelmien joukosta. Valinnan yhteydessä tulee myös valita käytettävät parametrit, kuten avaimien pituudet.

Tiedon suojaamiseen käytetään yleisesti seuraavia standardoituja menetelmiä:

- Diffie-Hellman- tai Elliptic Curve Diffie-Hellman -protokollaa avaintenvaihtoon,
- Advanced Encryption Standard -menetelmää tiedon salaamiseen,
- Secure Hash Algorithm 2 -menetelmää tiivisteiden muodostamiseen, ja
- RSA- tai Elliptic Curve Digital Signature Algorithm -menetelmää sähköiseen allekirjoittamiseen.

Käytännössä luottamuksellisuuden, eheyden ja autenttisuuden takaavaa ratkaisua ei kuitenkaan nykyään rakenneta valikoiden menetelmiä yksi kerrallaan, vaan tiedonsiirtoon käytetään standardoituja tietoturvaprotokollia, kuten Transport Layer Security (TLS) tai Internet Protocol Security (IPsec), joita käsitellään tarkemmin Tietoliikenneprotokollat-luvussa. Niiden tarjoamaa turvallisuustasoa valituilla parametreilla on kuvattu tarkemmin liitteessä 1.

Kryptografisten tuotteiden turvallisuuden arviointia varten on laadittu kriteeristöjä, joissa määritellään vaatimuksia tuotteissa käytettäville menetelmille ja toteutuksille eri turvallisuustasoilla. Esimerkki tällaisista kriteeristöistä on FIPS 140-2, joka käsittelee sekä ohjelmisto- että laitteistopuolta. Edellä mainittu kriteeristö koostuu Yhdysvaltojen standardointilaitoksen NIST:n validointisäännöksistä, jotka eivät sellaisinaan sovellu kansallisiksi ohjeiksi, mutta niitä voi käyttää viitemateriaalina. Kriteeristöjä vasten hyväksyttyjen tuotteiden käytössä on huomioitava, että hyväksynnät koskevat tiettyjä laitteistojen ja ohjelmistojen muodostaman kokonaisuuden versioita. Laitteiston tai ohjelmiston jonkin osan version muuttuessa hyväksyntä ei siis välttämättä ole enää voimassa.

4.6 Tietoliikenneprotokollat

Edellä kuvattujen menetelmien yhdistäminen toimivaksi ratkaisuksi vaatii niiden ominaisuuksien tuntemista ja syvällistä osaamista. On esimerkiksi tiedettävä mikä osa viestistä on tarpeen autentikoida ja kuinka viestin osat sidotaan toisiinsa niin, ettei niitä voi käyttää myöhemmin ns. "leikkaa ja liimaa" -tyyppisiin tai toistohyökkäyksiin (engl. replay attack). Eri tyyppisten viestintäjärjestelmien suojaamiseen on olemassa standardoituja käytäntöjä. Salauslaitteet ja -ohjelmistot toteutetaan käyttäen tiedonsiirtoon standardoituja, tietoturvallisia yhteyskäytäntöjä eli tietoliikenneprotokollia, kuten TLS ja IPsec. Niissä on yhdistetty viestinnän suojaamiseen käytettäviä menetelmiä siten, että mahdollisuudet järjestelmän murtamiseen saadaan minimoitua. Protokollat mahdollistavat usein laajennokset, jotka parantavat esimerkiksi yhteyden uudelleen muodostamiseen kuluvaa aikaa tai sallivat erilaisten autentikointimenetelmien käytön. Laajennokset saattavat kuitenkin vaarantaa turvallisuuden, ja siksi niitä ei saa käyttää tarkastamatta.

4.6.1 TLS

TLS-protokolla mahdollistaa useita erilaisia menetelmiä ja niiden parametreja tietoliikenteen luottamuksellisuuden, eheyden ja autenttisuuden takaamiseen. Käytetyt menetelmät sovitaan osapuolten kesken heidän suositustensa perusteella.

TLS-protokollasta on olemassa useita erilaisia toteutuksia, yksi käytetyimmistä on avoimen lähdekoodin sovellus OpenSSL. Turvallisuuden kannalta on oleellista käyttää uusinta versiota TLS-toteutuksesta. Järjestelmiä suunniteltaessa on tärkeää valita tarpeeksi vahvat menetelmät myös eheyden ja autentikoinnin varmistamiseen – vahva salaus ei yksinään riitä.
TLS-protokollaan on määritelty valmiiksi erilaisia yhdistelmiä salausmenetelmistä ja niiden avainpituuksista. Niiden huolellisella valinnalla voidaan suojata yhteys siten, että sen turvallisuus on taattu. Menetelmien tietoturvallisuutta on kuvattu tarkemmin liitteessä 1.
TLS-protokollalla on esimerkiksi suojattu yhteydet moniin tunnistautumista ja salaamista vaativiin palveluihin, kuten verkkokauppohin ja -pankkeihin.

4.6.2 IPsec

IPsec on standardoitu protokolla, jota käytetään tietoliikenteessä Internet Protocol (IP) -tason pakettien salaamiseen ja autentikointiin. IPsec suojaa siis alemman tason tietoliikennepaketteja kuin esimerkiksi TLS, joka toimii sovellustasolla suojaten sovellusten välisiä yhteyksiä. IPsec-protokollalla voidaan suojata kaikki IP-tason liikenne riippumatta ylempien tietoliikennetasojen suojauksista.

IPsec takaa siirretyn tiedon luottamuksellisuuden, eheyden ja autenttisuuden. Lisäksi siinä on suojaus toistohyökkäyksiä vastaan. IPsecillä voidaan luoda koneiden välille niin sanottu virtuaalinen yksityisverkko (engl. Virtual Private Network, VPN), jonka sisällä kaikki liikenne on suojattua. Tarkemmin VPN-ratkaisua kuvataan luvussa 5.9.

4.7 Tulevaisuuden näkymiä

Kryptografia on käytäntönä satoja vuosia vanha. Tieteenalana kryptografia on nuori, mutta on paljon tarkemmin määritelty kuin esim. kyberturvallisuus. Kryptografisen tutkimuksen tulosten käyttöönotto voi viedä jopa kymmeniä vuosia. Näiden seikkojen vuoksi salausteknisten ilmiöiden ennakointi on jonkin verran helpompaa kuin laajemmalla kyberturvallisuuden alueella.Tässä kappaleessa käsitellään muutamia yleisimpiä ja merkittävimpinä pidettyjä kryptografiaan liittyviä ilmiöitä ja niiden vaikutusta loppukäyttäjiin.

Salaustekniikoiden politisoituminen. Salaustekniikat ovat aina näytelleet tärkeää roolia politiikassa toimimalla valtion ylimmän johdon viestien turvaamisessa ja sotilastiedustelun välineinä. Internetin laajentumisen ja pilvilaskennan myötä tietoisuus salausteknologioista on levinnyt yhä enemmän myös suurelle yleisölle. Yleinen reagointi esim. paljastuksiin suurten tiedusteluorganisaatioiden massavalvonnasta[1] osoittaa, että valtiotason tiedustelulle on olemassa yksityisyyden suojaa kannattava vastavoima. Tällä on pienten valtioiden kannalta se hyvä puoli, että salainten heikkouksia tuodaan esiin julkisesti kansainvälisellä tasolla, kansallisen viranomaisen kannalta ”ilmaiseksi”. Toisaalta poliittinen keskustelu voi viedä asiaa tekniseltä kannalta myös huonompaan suuntaan, kun mukana olevista keskustelijoista enemmistö ei tunne asiaa tarkemmin.

Kryptoanalyysi ja kryptografia käyvät jatkuvaa kilpajuoksua keskenään. Viime vuosina on kuitenkin ollut huomattavissa se seikka, että edes tiedusteluorganisaatiot eivät ilmeisesti enää pysty

[1] Kts. esim. http://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)

murtamaan salausta algoritmitasolla, vaan niiden on ollut pakko hyökätä salaustoteutuksia vastaan. Valtiot vastaavat tähän haasteeseen tarkastustoiminnalla, ja teollisuus siirtämällä toteutuksia entistä enemmän laitteistoihin. Erilaiset formaalit verifioinnit, sivukanavahyökkäyksille immuunit algoritmitoteutukset ja peukaloinnin kestävät (”tamperproof”) piirit ovat yksittäisiä teknologioita, joilla toteutustason hyökkäyksiä pyritään estämään.Tämän hetken tunnetuimmista algoritmeista RSA:n julkisen avaimen menetelmän käyttö on laskevalla trendillä, ja korvaajaksi on tulossa järjestelmien päivityssyklin myötä elliptisten käyrien kryptografia. Pienellä prosenttiosuudella odotetaan myös nk. ”kvanttiturvallisten” algoritmien, kuten NTRU:n esiinmarssia.

Muista algoritmityypeistä AES puolustaa edelleen vakaasti paikkaansa hyvänä lohkosalaimena.Verrattuna esim. DES:in yli kaksikymmenvuotiseen taipaleeseen, AES on arviolta matkansa puolivälissä. Mikäli lohkosalaimille ei esitetä täysin uusia kryptoanalyysityyppejä tai perinteisten kryptoanalyysimenetelmien laajennukset eivät tarjoa suuria yllätyksiä, AES ehtii vanhenemaan standardisyklinsä loppuun asti rauhassa.

Tiivistefunktiot, kuten MD5 ja SHA1, ovat olleet tätä kirjoitettaessa tutkimuksen kohteena kymmenen vuotta, jonka aikana niistä on opittu paljon uutta. Oppien mukaisesti on kehitetty uusia, paljon tehokkaampia, turvallisempia ja joustavampia tiivistealgoritmeja. Näistä, kuten myös AES:stä, käytiin viisivuotinen kisa NIST:in seuraavaksi tiivistestandardiversioksi SHA-3. Sen käyttöönotto kestää kuitenkin suunniteltua pidempään johtuen pääasiassa standardoinnin hitaudesta, SHA-2:n oletettua kestävämmästä rakenteesta sekä epäilyistä NIST:in muutoksille kisan voittaja-algoritmiin, Keccakiin. SHA-2 on todennäköisesti eräs lähitulevaisuuden eniten käytetyistä tiivistefunktioista, kunhan SHA-1 on poistettu tuotteista vaiheittain.

Laskentateho on kryptoanalyysin peruskiviä, mutta jo nyt ollaan perinteisen laskennan osalta niin pitkissä avaintenpituuksissa (esim. 192 bittiä), että ideaalitapauksissakin kaikkien avainten luettelointi vaatisi auringon tuottaman energian valjastamisen n. 16000 vuodeksi[2]. Algoritmisella tasolla laskentatehon lisääminen ei ole kannattavaa kuin tiettyyn rajaan asti, mikäli muut menetelmät onnistuvat pudottamaan jonkin algoritmin turvallisuutta riittävän alas. Myös kvanttilaskennassa tunnetaan luonnontieteellisiä ylärajoja kvanttialgoritmien kellotaajuudelle[3], jotka rajoittavat tunnettujen kvanttialgoritmien pätevyyttä esimerkiksi lohkosalaimille.

Salausteknologian sijainti on perinteisesti ollut salauslaitteissa tietoturvadomainin rajalla (”security perimeter”). Yleisenä trendinä on, että tietoturvadomainien rajat fraktalisoituvat pilvilaskennan ja ”Internet of Things”-ajattelun myötä. Tällöin myös salausteknologiaa täytyy sovittaa toisaalta aivan pienimpiin laitteisiin, ja toisaalta tietoalkiotasolle asti. Salaustuotteista tulee entistä enemmän integroituja tuotteita, jossa salaustekniikka on vain yhtenä moduulina. Lisäksi näitä moduuleja sijaitsee useammalla abstraktiotasolla laitteistoista aina tekstinkäsittelyohjelmiin asti.

Salaustekniikoiden luotettavuuden arviointi pelkästään OpenSource/Closed-source -akselilla ei tule jatkossa olemaan niin suoraviivaista kuin tähän asti. Nk. Heartbleed-haavoittuvuus[4] ja Truecrypt-

[2]Landauerin rajan mukaiset laskelmat (http://en.wikipedia.org/wiki/Brute-force_attack) sovellettuna auringon ytimen energiantuottoon (http://en.wikipedia.org/wiki/Sun#Core)
[3] raja on noin 10^{26} Hz (L.Levitin, T. Toffoli: “The Fundamental Limit on the Rate of Quantum Dynamics: the Unified Bound is Tight”, Physical Review Letters 103, 13.10.2009.
[4] http://heartbleed.com; http://en.wikipedia.com/wiki/Heartbleed

tuotteen[5] tuen päättyminen osoittivat, että salaustoteutusten ylläpitäminen vaatii jatkuvaa kehitystyötä ja olemassa olevia CERT-prosesseja, johon OpenSource-puolella ei välttämättä ole varaa. Toisaalta Closed-source puolella tapahtuu avautumista erityisesti hyväksyntäviranomaisten suuntaan.

Salausteknologioiden käyttötavat laajenevat kryptografisten menetelmien laajentuessa ja tietoisuuden lisääntyessä. Eräs mielenkiintoisimmista aluevaltauksista ovat nk. kryptovaluutat, kuten bitcoin ja livecoin. Niiden perustana eivät ole harvinaiset metallit tai obligaatiot, vaan laskentateho, kun louhijat varmentavat kryptografisesti suojattuja transaktioita saaden palkkioksi lisää kryptovaluuttaa. Varmentaminen vaikeutuu sitä mukaa kuin kokonaislaskentatehoa on olemassa ja valuuttaa on tuotettu. Näitä valuuttoja ei voi hallita keskitetysti, eikä niihin sellaisenaan liity identifioivia tekijöitä. Valtiot eivät vielä tue kryptovaluuttoja, mutta joillekin niistä on jo olemassa vaihtokursseja ja jopa vaihtopörssejä. Koska kryptovaluutat ovat suureksi osaksi anonyymejä, myös rikollinen maailma käyttää niitä laajamittaisesti.

Erilaisia yrityksiä sähköiseksi valuutaksi on ollut jo vuosikymmeniä, mutta muun sähköisen pankkitoiminnan kehityksen myötä ne ovat jääneet marginaalisiksi. Kryptovaluutat edustavat tässä radikaalia ajattelutavan muutosta[6], Kyseessä on voimistuva ilmiö, johon valtioiden ja/tai rahoituslaitosten on otettava voimakkaasti kantaa vähintään keskipitkällä aikavälillä.

Kryptografia on nykyisin yleisessä käytössä myös haittaohjelmissa, erityisesti tunnistepohjaisten järjestelmien harhauttamisessa sekä varastetun datan viemisessä kohteesta hyökkääjälle. Jälkimmäisessä tapauksessa myös steganografia (datan piilottaminen toisen datan sekaan) on kokenut uuden tulemisen kryptografisten tekniikoiden ansiosta. Tämä trendi voi viimein pakottaa uusien valvontatekniikoiden käyttöönottoon ja anomaliapohjaisten IDS-järjestelmien tulon valtavirtaan.

Kvanttilaskenta on eräs teknologioista, joilla on laajamittaisesti toteutuessaan merkittävä vaikutus salausalgoritmeihin. Sen seurauksena lähestulkoon kaikki diskreetteihin logaritmeihin ja tekijöihin jakoon perustuvat järjestelmät, kuten RSA, Diffie-Hellman avaintenvaihto ja elliptisten käyrien kryptografia tulisi hylätä; symmetristen salainten avaintenpituudet tulisi kaksinkertaistaa, ym. Kvanttilaskennan laajamittainen tuleminen nimenomaan salaustekniikoita uhkaavana paradigmana näyttää yhä edelleen joko epätodennäköiseltä, hyvin pitkän aikavälin uhalta, tai se on molempia. Toisaalta, mikäli vaikutus on suuri, myös pienten todennäköisyyksien uhkiin tulisi varautua jollakin tavalla. ETSI (European Telecommunications Standards Institute) on teettänyt selvityksen[7] protokolla-/sovellustason haavoittuvuuksien vaikutuksista loppukäyttäjille sekä mahdollisuuksista korvata haavoittuvat osat muilla menetelmillä.

Koska kvanttilaskennalle haavoittuvia menetelmiä käytetään protokollissa lähinnä avainten vaihtoon, ei välttämättä ole tarvetta hylätä koko protokollaa, vaan riittää kun korvataan avaintenhallinta jollakin ”kvanttiturvallisella” menetelmällä. Kaikkia toteutuksia on joka tapauksessa muokattava, mutta kaikki protokollat eivät tarvitse muutoksia. Helposti muokattavia

[5] http://truecrypt.sourceforge.net/; http://www.darkreading.com/endpoint/the-mystery-of-the-truecrypt-encryption-software-shutdown-/d/d-id/1269323
[6] *Laskentateho* on kybertilassa verrattavissa harvinaisiin metalleihin.
[7] (mm.) Institute for Quantum Computing, University of Waterloo: Quantum Safe Cryptography, White Paper: Quantum Safe Cryptography and Secuirty; An Introduction, benefits, enablers an challenges, 10/2014

protokollia ja standardeja ovat mm. X.509(v3), S/MIME, ja SSH. Standardimuutoksia vaadittaisiin ainakin TLS:ään ja IPSeciin.

ETSI:n selvityksen mukaan ”kvanttiturvallisia” menetelmiä ovat sellaiset, joille ei vielä tunneta tehokasta kvanttilaskenta-algoritmia, tai ne ovat muuten turvallisia. Näitä ovat hilapohjaisiin ongelmiin perustuvat systeemit, kuten NTRU ja kvanttiavaintenvaihto (QKD). Kummatkin ovat jo olemassa olevia tuotteita, mutta NTRU ei ole kovin tehokas edes RSA:han verrattuna, koska sen avaimet ovat pitkiä ja prosessointi hidasta. QKD taas on kehittyvä teknologia, ja mikäli sen integrointi- ja yhteysvälihaasteet saadaan ratkottua, on se varteenotettava vaihtoehto avaintenvaihdossa - mikäli etsitään juuri kvanttiturvallisia toteutuksia.

Seuraavan sukupolven julkisen avaimen järjestelmät ovat siirtyneet akateemisesta tutkimuksesta jo teollisuuden T&K-osastoille. Nämä funktionaalisina salaustekniikoina (FE) tunnetut menetelmät[8] perustuvat siihen, että julkinen avain voidaan luoda ennen yksityistä avainta mielivaltaiseksi, ja palastella se tarvittaessa attribuuteiksi. FE-tekniikat tuovat mukanaan suuria odotuksia, kuten kevyemmän PKI-arkkitehtuurin, turvallisen ja järkevän pilvisalauksen, aidosti toimivia IPR-ratkaisuja, secure boot-mekanismeja sekä sovellusten autentikoinnin (ajettavalla sovelluksella voi olla sen toimintaan perustuva digitaalinen allekirjoitus ja olisi mahdollista tietää, käyttäytyikö sovellus niinkuin sen piti riippumatta ajoalustaan asennetuista mahdollisista tietoturva-aukoista). Valtionhallinnossa tulisivat mahdollisiksi nk. monitasotietoturvaympäristöt (MLS, multi-layer security), joissa eri tasoiset käyttäjät voivat turvallisesti käsitellä eri suojaustasojen tietoja samalla alustalla.

FE-tekniikat ovat vielä hyvin monimutkaisia ja toisiinsa integroitumattomia, mutta eri ennustusten mukaan laajamittaisia toteutuksia tullaan näkemään noin kymmenen vuoden ajanjaksolla.

[8] Esim. D. Boneh, A. Sahai, B.Waters: Functional Encryption: Definitions and Challenges. Proc. of Theory of Cryptography 2011, LNCS 6597, pp. 253-273, Springer, 2011.

5 Avaintenhallinta

Avaintenhallinta on kaikkein kriittisin osa luottamuksellisuuden takaamisessa. Tärkeän kryptografian periaatteen mukaan salauksen on kestettävä, vaikka hyökkääjällä olisi käytössään kaikki lähetetty salakielinen teksti ja kaikki tieto käytetystä menetelmästä, mutta ei salaista avainta. Vuotanut avain tekee mitättömäksi parhaatkin salausmenetelmät, mutta valitettavan usein avaintenhallinta toteutetaan puutteellisesti ja suunnittelematta. Nykyaikaiset salausmenetelmät kestävät murtoyrityksiä niin hyvin, että onnistuneiden tietomurtojen taustalla on useammin salausavaimen vuotaminen joko käyttöjärjestelmän, tietoturvaprotokollan tai käyttäjän virheen vuoksi kuin jokin salausalgoritmin heikkous.

Avaintenhallinnan asianmukaisen toteutuksen varmistamiseksi sen prosessien ja käytäntöjen tulee olla dokumentoituja. On suositeltavaa, että laaditaan järjestelmäkohtainen avaintenhallintasuunnitelma, josta tulee selvitä avainten koko elinkaari niiden luonnista asianmukaiseen tuhoamiseen.

Avaintenhallintasuunnitelman suositellaan kattavan ainakin seuraavat toiminnot:

- avainten ja satunnaislukujen luonti,
- avainten käyttötarkoitus
- avainten suojaaminen,
- avainten jakelu,
- avaimen sulkulistaaminen eli revokointi,
- avainten uusimis- ja vaihtomenetelmät,
- avainten palauttaminen,
- avainten tuhoaminen,
- avainten voimassaoloajat
- varmenteiden tyypit ja niissä käytetyt parametrit

Seuraavat toiminnot kuuluvat lähinnä tiettyjen avaintyyppien (joiden käsittelyä tyypillisesti vielä säädellään erilaisin sopimuksin) vaatimaan COMSEC-prosessiin (communication security), mutta ne voivat sisältyä myös avaintenhallintasuunnitelmaan:

- Avainten tilaus,
- avainten rekisteröinti,
- avainten säilytys ja arkistointi,
- kirjanpito

COMSEC-prosessiin liittyy myös esimerkiksi avainten suojaaminen, avainten jakelu, avainten tuhoaminen. Lisätietoa COMSEC-prosessista on Viestintäviraston kansallisen salausteknisen materiaalin käsittelyohjeessa.

Seuraavissa kappaleissa kuvataan avaintenhallintatoimintoja tarkemmin.

5.1 Avainten luonti ja jakelu

Salauksessa ja autentikoinnissa tarvitaan useita erityyppisiä avaimia eri käyttötarkoituksiin. Menetelmän mukaan voidaan puhua symmetrisistä ja epäsymmetrisista avaimista, tai salaisista,

yksityisistä ja julkisista avaimista. Avaimilla voi olla keskinäinen hierarkia ja ne jaetaan käyttötavan mukaan pitkä- ja lyhytaikaisiin avaimiin. On myös tarpeen erotella järjestelmässä sähköisesti jaettavat avaimet niistä, jotka kuljetetaan käyttöpaikalle siirrettävällä medialla.

Käsittelyn kannalta salainten tarvitsemat avaimet voidaan jakaa karkeasti kahteen luokkaan:

1. Pitkäaikaiset avaimet, joiden avulla salataan tai verifioidaan lyhytaikaisia avaimia.. Näiden avainten vaihtoväli on pidempi, tyypillisesti 3kk-1v. Pitkäaikaiset avaimet voivat olla myös ns. fyysisiä avaimia, jotka kuljetetaan käyttöpaikalle siirrettävällä medialla henkilökohtaisesti tai käyttäen tehtävään hyväksyttyä kuriiria (ns. COMSEC-toiminta). Tietyt kansainväliset sopimukset, esim. (EU:n turvallisuussäännöt) edellyttävät, että korkean suojaustason järjestelmien avaintenhallintaan on käytettävissä henkilöstöä kuljettamaan, pitämään kirjaa ja revokoimaan avaimia tarpeen mukaan.
2. Lyhytaikaiset avaimet, joiden avulla salataan dataa tai suojataan eheyttä. Näiden käyttöikä on lyhyt, tyypillisesti avaimet ovat istuntokohtaisia. Ne generoidaan ja siirretään automaattisesti järjestelmässä, jolloin ne salataan tai verifioidaan pitkäaikaisella avaimella siirron ajaksi.

5.1.1 Avainten luonti

Jotta salaus olisi vahva, on salausavaimen oltava kryptografisesti vahva. Avaimen luontiin käytetään yleensä jotain (pseudo-)satunnaislukugeneraattoria, jotta avaimet eivät olisi helposti ennustettavissa eikä niiden välillä olisi merkittävää tilastollista yhteyttä. Satunnaisluku ei itsessään riitä avaimeksi, vaan yleensä sitä käytetään syötteenä jollekin avaimenluomismenetelmälle. Sillä varmistetaan, että avaimella on toivotut ominaisuudet, kuten tasajakautuneisuus ja tuoreus, ja että se on sopiva käytettyyn salausmenetelmään.

Avainten sopiminen tai avaintenvaihto tarkoittaa, että avain sovitaan osapuolten välillä yhdistäen heidän luomaansa satunnaista avainmateriaalia. Yksi hyvin yleinen menetelmä on niin sanottu Diffie-Hellman -avaintenvaihto, jossa symmetrinen avain sovitaan epäsymmetrisen protokollan avulla. Diffie-Hellman -avaintenvaihtoprotokolla ei itsessään sisällä viestinnän osapuolten autentikointia, joten siihen on aina lisättävä jokin autentikointiratkaisu, esimerkiksi protokollan viestien sähköinen allekirjoittaminen. Avainten sopimisessa luodut avaimet ovat lyhytaikaisia, esimerkiksi istuntokohtaisia. Avainten sopiminen toteutetaan sähköisesti, ja se on osana mm. IPSec- ja TLS -protokollissa.

5.1.2 Salausavainten tyyppejä ja käyttötarkoituksia

Salausteknisiä avaimia voidaan käyttää myös muunkaltaisiin toimintoihin kuin salaukseen. Yleisesti ottaen on tärkeää olla sekoittamatta tai yhdistämättä avaimia mielivaltaisesti eri käyttötarkoituksista. Yhteen käyttötarkoitukseen tehty avaintenhallintaohjeisto ei välttämättä ole sellaisenaan siirrettävissä toiseen tarkoitukseen. Erilaisia käyttötarkoituksia salauksen lisäksi ovat esimerkiksi:

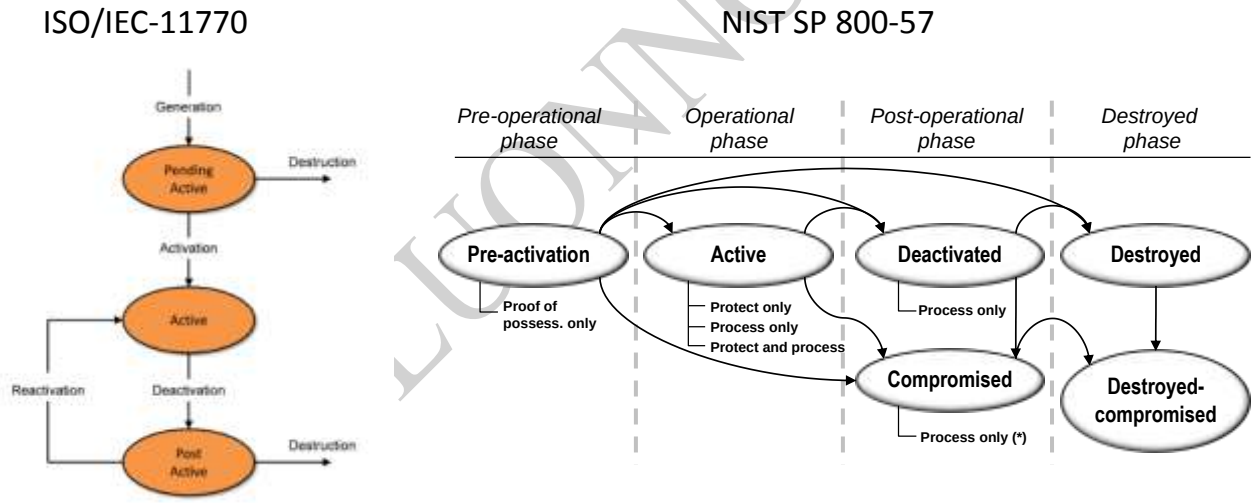
- Eheyden takaamiseen liittyvät avaimet: yksityiset asymmetriset avaimet digitaalisiin allekirjoituksiin, symmetriset avaimet MAC:ien (Message Authentication Code) tuottamiseen. Usein luottamuksellisuuden lisäksi halutaan varmistaa myös eheyttä , jolloin

on tärkeää tiedostaa milloin näihin varatut avaimet on syytä eriyttää. Esimerkiksi digitaaliseen allekirjoittamiseen käytettävä avainpari on turvallisempaa olla eri kuin salaamiseen käytettävä avainpari.

- Pääsynhallintaan liittyvät avaimet; erilaiset sertifikaatit ja tokenien, kuten sirukorttien, sisältämät avaimet. Nämä eivät vaikuta suoraan luottamuksellisuuteen, mutta toimivat kontrollina yleisessä resurssien suojaamisessa.
- Avaintenhallinnan infrastruktuurin ylläpitoon tarvittavat avaimet, kuten edellämainitut pitkäaikaiset avaimet, mutta myös avainten vanhenemisen ja katoamisen varalle muodostetut ”vara-avaimet”, kolmannen osapuolen toiminnan mahdollistavat sivu- ja yleisavaimet sekä avainten luonnissa ja salaustuotteiden käynnistyksessä tarvittavat alustusavaimet.
- Hallinnolliseen tai tietoturvatasojen eriyttämiseen liittyvät avaimet; joissain tapauksissa salauksella on sivutarkoituksena eriyttää verkkoja loogisella tasolla, joko hallinnollisista tai suojaustasoon liittyvistä syistä. Tämä luo avaintenhallintaan lisäkompleksisuutta.

5.2 Avainten elinkaari ja siihen liittyvät toiminnot

Kansainvälisissä avaintenhallinnan standardeissa ja suosituksissa (esim. ISO/IEC-11770[9] ja NIST SP 800-57[10]) keskeisessä osassa on avainten elinkaari. Kuvassa 5 on esimerkkejä näiden standardien mukaisista avainten elinkaarista.



Kuva 5. Avainten elinkaari eräiden standardointiorganisaatioiden mukaan.

5.3 *Avainten jakelu*

Avainten jakelulla tarkoitetaan sitä, että luotettu osapuoli itsenäisesti luo käytetyn avaimen ja lähettää sen muille osapuolille sähköisesti tai siirrettävällä medialla. Avain jaetaan aina joko kryptografisin menetelmin tai fyysisen turvallisuuden keinoin suojattuna. Tästä kerrotaan lisää kappaleessa Avainten suojaaminen.

[9] ISO/IEC 11770, Information Technology – Security Techniques – Key Management Part 1-5 (2006-2011)
[10] NIST Special Publication 800-57, Recommendation for Key Management – General (Rev.3), 2012.

Avainhierarkioiden, infrastruktuurin yms. järjestelmien tarkoituksena on pyrkiä minimoimaan fyysisesti jaettavien avainten määrä. Huolimatta siitä, että käytettävissä on sähköisiä avaimenjakelumenetelmiä eli etäavainnusta, järjestelmän turvallisuus pohjautuu aina yhteen tai useampaan pääavaimeen ("master key") tai jaettuun pitkäaikaiseen salaisuuteen, joka suojaa sähköisesti lähetettäviä avaimia. Se voi olla myös epäsymmetrinen avainpari, esimerkiksi juurivarmentajan avainpari.

Julkisten avainten infrastruktuuria (PKI) käytetään tarjoamaan varmennepalveluita käyttäjien ja laitteiden autentikointiin. Tunnettu ja luotettu juurivarmentaja takaa sähköisellä allekirjoituksellaan, että varmenteen sisältämä julkinen avain todella kuuluu sille taholle, jonka nimi on varmenteessa. Varmenteita ketjuttamalla päädytään viestinnän osapuolten julkisten avainten varmentamiseen. Julkisen avaimen avulla voidaan salata viestinnässä käytetty istuntokohtainen salausavain, joten julkisen avaimen infrastruktuuria voidaan käyttää avaintenjakeluun.

PKI pohjautuu luottamukseen juurivarmenteen oikeellisuudesta. Jos PKI:ta käytetään avaintenjakeluun, on kiinnitettävä huomiota siihen, että juurivarmentajiksi hyväksytään vain luotettuja tahoja. Yksittäisellä organisaatiolla voi olla myös oma juurivarmentaja. Kummassakin tapauksessa juurivarmenteen tarkastamiseen on kiinnitettävä erityistä huomiota. Sen sijaan, että oletetaan luotetuksi sellainen juurivarmentaja, jonka toimintaa ei pystytä tarkastamaan, tarvittavien palveluiden varmistamiseen olisi parempi soveltaa muita tapoja. Näitä ovat esimerkiksi loppukäyttäjävarmenteiden korvaaminen luotettavammilla, asettamalla luotetuiksi ainoastaan yksittäiset varmenteet tai asettamalla juurivarmenteen käytölle rajoitteita, mikäli varmennetyyppi tai järjestelmä sen mahdollistaa.

Varmenteisiin voidaan usein lisätä tieto käyttörajoituksista. PKI-järjestelmässä yleisenä sääntönä on rajoittaa myönnettävän avaimen käyttö mahdollisimman sopivaksi esimerkiksi asettamalla alivarmentajalle voimaan rajoitus, että se voi myöntää varmenteita vain *.esimerkki.fi-tyyppisille www-palveluille. Rajoitusten oikea käyttö on tärkeää myös RSA-pohjaisten varmenteiden kanssa, sillä samaa RSA-avainta ei tule käyttää erinäisistä hyökkäyksistä johtuen sekä mielivaltaisen tiedon allekirjoittamiseen että salaukseen.

PKI:n lisäksi toinen yleinen tapa hallita avaimia on hierarkkinen järjestelmä, jossa lyhytaikaiset avaimet suojataan pitempiaikaisilla. Toisten avainten salaamiseen käytettäviä erityyppisiä avaimia voi olla useita kerroksia. Jos pääavain hierarkian juuressa on avainparin sijasta symmetrinen avain, se pitää toimittaa käyttäjille fyysisesti.

5.4 Avainten suojaaminen

Pääperiaate on, että kaikkia salausavaimia ja niiden luontiin tarvittavaa materiaalia on suojattava vähintään yhtä hyvin kuin vastaavan tason tietoa. Järjestelmän salaisten avainten on oltava vain valtuutettujen käyttäjien ja prosessien käytössä niiden koko elinkaaren ajan. Kaikilla, joilla on pääsy suojaamattomiin avaimiin, tulisi olla valtuutus niillä salattavaan aineistoon. Tämä unohdetaan helposti järjestelmien ylläpitoa ulkoistettaessa. Jos pääavain tai muut avaimet ovat vieraan tahon, kuten ulkomaalaisen palveluntarjoajan tai juurivarmentajan, luomia tai niiden hallussa, näillä tahoilla on periaatteessa mahdollisuus purkaa salaus tai luvattomasti muuttaa tietoa.
Avainten suojaamista käsitellään tarkemmin seuraavissa kappaleissa jaoteltuna siirtotapojen mukaan.

5.4.1 Fyysisesti siirrettävät avaimet

Avaimet luodaan turvallisessa, verkosta irti olevassa laitteessa, josta ne kopioidaan siirtomedialle. Jos median fyysiset suojaamisjärjestelyt eivät ole kattavia, on suositeltavaa suojata siirrettävät avaimet jollain toisella salauksella. Samoin kuin sähköisesti siirrettäviin, myös fyysisiin avaimiin pätee, että niitä käsitellään vähintään yhtä huolellisesti kuin vastaavan tason aineistoa. Kansainvälisissä velvoitteissa ja ohjeissa avainten suojaamiseen liittyy usein lisäsäännöksiä. Järjestelmäkohtaiset käytännön toimenpiteet on syytä ohjeistaa ja dokumentoida esimerkiksi avaintenhallintasuunnitelmassa tai käyttöpolitiikassa.

Fyysisten avainten käsittely, tilaus, kuljettaminen, kirjanpito, uusiminen, revokointi ja tuhoaminen kuuluvat ns. COMSEC-toimintaan, jonka toimivaltainen viranomainen ohjeistaa erikseen. Esimerkiksi EU:n turvallisuussäännöt edellyttävät, että jokaisella maalla on fyysisten avainten hallintaa varten nimetty asianmukainen toimivaltainen viranomainen (salausteknisen aineiston jakelusta vastaava viranomainen, Crypto Distribution Authority, CDA).

5.4.2 Sähköisesti siirrettävät avaimet

Sähköisesti siirrettävien ja käsiteltävien avainten riittävän suojauksen varmistaminen ja avainten generointi kuuluvat salaustuotteiden tarkastusprosessiin. Pitkäaikaiset avaimet, kuten juurivarmenteet, luodaan turvallisessa, verkosta irti olevassa laitteessa.

Käyttäjä ei yleensä suoraan käsittele salausavaimia, vaan ne suojataan useimmiten salasanalla tai fraasilla, jonka käyttäjä naputtaa koneelle. Sähköisten avainten tai niitä suojaavien salasanojen jakelua ei saa koskaan tehdä salaamatta samalla kanavalla jolla salakielistä tekstiä lähetetään. Jos viestintäkanava on suojaamaton, eli sillä kulkevat viestit pitää salata, mahdollinen hyökkääjä pystyy kuuntelemaan myös salasanoja tai avaimia kuljettavat viestit.

Pitkät ja monimutkaiset salasanat voi olla tarpeen kirjoittaa muistiin, jolloin niiden säilyttämiseen on kiinnitettävä erityistä huomiota. Jos salasana on ainut pääsytapa tietoon, sen luokittelu- ja käsittelysäännöt periytyvät tiedolta. Jos avaimet tai niitä suojaavat salasanat säilytetään laitteella, on pääsy laitteelle suojattava samantasoisesti kuin suojattava aineisto.

Jos avaimet säilytetään laitteen muistissa, on tärkeää suojata kyseinen muistin osa, ja avainten muistista pyyhkiminen on toteutettava luotettavalla menetelmällä. PKI-järjestelmää käytettäessä varmenteiden allekirjoitusten ja revokoinnin tarkastaminen kuuluvat salauslaitteen oikeaan toimintaan.

5.5 Avainten vaihto ja käytöstä poisto

Ajan myötä avaimen luvattoman paljastumisen riski kasvaa, joten avaimia on syytä vaihtaa säännöllisin väliajoin. Useimmissa tietoliikenneprotokollissa (esim. IPSec) salausavaimet vaihdetaan automaattisesti vähintään istuntokohtaisesti. Myös järjestelmien ulkopuolella on huolehdittava pitkäaikaisten avainten säännöllisestä vaihtamisesta.

Käyttämällä tiedon suojaamiseen lyhytaikaisia avaimia, jotka ovat riippumattomia toisistaan ja pitkäaikaisista avaimista, rajoitetaan avaimen paljastumisesta aiheutuvaa vahinkoa. Tällä tavoin istuntokohtaisen avaimen paljastuminen paljastaa viestinnän vain edelliseen avaimenvaihtoon asti. Jälkeenpäin paljastunut pitkäaikainenkaan salausavain ei paljasta aiempaa viestintää. Tämä ominaisuus on nimeltään forward secrecy. Muita tärkeitä periaatteita ovat ne, että istuntokohtaisia avaimia ei käytetä materiaalina muille avaimille, ja että seuraavaa istuntoavainta ei salata edellisen istunnon avaimilla.

Avainten turvallisten vaihtovälien määrittäminen ei ole suoraviivaista. Siihen voi vaikuttaa avaimella salatun datan määrä, avaimen tyyppi ja todennäköisyys, että avain paljastuu pidemmällä aikavälillä. Jos käytettävissä oleva salausmenetelmä on turvallinen, voidaan datan määrä jättää huomiotta. Hyvä nyrkkisääntö on, että pitkäaikaiset avaimet vaihdetaan vähintään vuoden välein ja lyhytaikaiset istuntokohtaisesti.

Poikkeus vaihtosääntöön on, jos avainten epäillään paljastuneen. Epäilystä on raportoitava mahdollisimman nopeasti avaintenhallintasuunnitelman mukaan sekä viestinnän osapuolille että tiedon omistajalle. Tällaisessa tilanteessa avaimilla salattu viestintä on voinut paljastua. Paljastuneet avaimet on poistettava käytöstä ja vaihdettava heti. Samoin on vaihdettava niistä mahdollisesti riippuvat avaimet. Jos paljastunutta avainta on käytetty muiden avainten salaamiseen, on nekin avaimet vaihdettava. On huomattava, että uusien avainten jakeluun ei saa käyttää paljastuneella avaimella salattua kanavaa. Avaintenhallintasuunnitelmaan tulisi kirjata toimenpiteet epäiltäessä avainten paljastumista sekä yhteydenottotahot.

Käytöstä poiston jälkeen avaimet on tuhottava luotettavalla menetelmällä. Sähköiset avaimet pyyhitään laitteen muistista käyttäen esimerkiksi tehokkaita ylikirjoitusmenetelmiä.[11]

Fyysisten avainten (käytettyjen siirtomedioiden) tuhoaminen kuuluu ns. COMSEC-toimintaan, jonka toimivaltainen viranomainen ohjeistaa erikseen.

6 Salausratkaisun valinta ja käyttöönotto

6.1 Johdanto

Salausratkaisun valintaan ja käyttöönottoon tulee suhtautua samalla tavalla kuin minkä tahansa muun tietojärjestelmän tai sen komponentin valintaan ja käyttöönottoon. Kuten yleensä tietojärjestelmähankkeissa, ratkaisun korjaaminen tai muuttaminen sen jälkeen kun se on otettu käyttöön, on hyvin haastavaa ja voi aiheuttaa merkittäviä lisäkustannuksia.

6.2 Tarveanalyysi

Salausratkaisun valinnan ja käyttöönoton tulee perustua tarveanalyysiin. Siinä kartoitetaan käyttötilanteet, joissa salausratkaisua tarvitaan sekä määritetään yleiset reunaehdot käyttötilanteiden salaustarpeiden täyttämiseksi.

[11] Viestintäviraston ohje "Kiintolevyjen elinkaaren hallinta - Ylikirjoitus ja uusiokäyttö". URL: https://www.viestintavirasto.fi/attachments/Ylikirjoitusohje.pdf

Salausratkaisut tarjoavat joustavia menetelmiä tietojen luvattoman paljastumisen ja muuntelun estämiseen. Niitä voidaan hyödyntää myös pääsynhallintamenetelmänä tietojen suojaamiseksi esimerkiksi etätyössä. Usein on tarve pystyä siirtämään suojattavaa tietoa ei-luotetun verkon yli, jolloin tietoa voidaan suojata salausratkaisulla. Yleensä etätyöhön liittyy tarve myös säilyttää suojattavaa tietoa päätelaitteilla ja muilla muistivälineillä, jolloin salausratkaisulla pystytään tarjoamaan luotettava pääsynhallintamenetelmä tiedolle esimerkiksi laitevarkauksien varalta. Salausratkaisut tukevat ja täydentävät myös muita tiedon suojausmenetelmiä. Esimerkiksi kiintolevyjen salauksella pystytään pienentämään muun muassa sisäpiiriuhkia myös organisaation fyysisesti suojatun toimitilan sisällä, mahdollistamaan kiintolevyjen ja muiden muistivälineiden laajempi uudelleenkäyttö[12] (kustannussäästö) sekä pienentämään ulkoisia uhkia myös tilanteissa, joissa fyysisen turvallisuuden suojaukset pettävät.

Salausratkaisut tarjoavat menetelmiä suojattavan tiedon käsittelyyn tai säilytykseen myös yhteiskäyttöisissä tai muuten heikommin suojatuissa palveluissa tai mahdollistavat sähköisen asioinnin toteuttamiseen. Esimerkiksi tiedon eheyden ja kiistämättömyyden takaavilla menetelmillä pystytään vähentämään paperimuotoisen aineiston käsittelyä sekä edistämään tehokkaampien ja käyttäjäystävällisempien palvelujen käyttöönottoa.

Tarveanalyysissä tulee aina arvioida myös sitä, mitkä käyttötapaukset ovat organisaation hyväksymiä ja mitä on ylipäänsä edes perusteltua lähteä toteuttamaan salaustekniikalla. Esimerkiksi järjestelmän vaatiman suojaustason määrittäminen tarpeettoman korkealle saattaa heikentää sen käytettävyyttä. Tarveanalyysissä suositellaankin käyttötapausten kuvausta ja tarvittaessa erillisten ratkaisujen toteuttamista eri suojaustasojen ja käytettävyystarpeiden käyttötapauksille. Esimerkki tarveanalyysistä on kuvattu luvussa 6.7.1.

Viranomaisten tiedon näkökulmasta salausta edellytetään, kun on tarve suojata tietoa luvattomalta paljastumiselta tai muuntelulta ja riittävää suojausta ei ole muilla menetelmillä perusteltua toteuttaa. Esimerkiksi EU:n turvaluokitellun aineiston käsittelyssä salausta edellytetään,

a) kun suojattava aineisto liikkuu tietoverkossa fyysisesti suojattujen alueiden välillä (esimerkiksi sähköpostin salaus, VPN-ratkaisut toimipisteiden välillä, sekä VPN-ratkaisut toimipisteen ja etätyölaitteiston välillä),
b) kun suojattavaa aineistoa kuljetetaan muuten fyysisesti suojattujen alueiden välillä (tietovälineiden kuten kiintolevyt, CD-levyt, USB-muistit ja vastaavat salaus), ellei aineisto ole jatkuvasti kuljettajansa hallussa/valvonnassa,
c) salausta käytetään pääsynhallintamenetelmänä muissa tilanteissa (esimerkiksi vähimpien oikeuksien periaatteiden toteuttaminen tai vaikka tarkastusoikeuden varaavien tiedon omistajien tietojen erottelu yhteiskäyttöisissä tietojärjestelmässä),
d) järjestelmään tehdyn riskienarvioinnin pohjalta muissa tilanteissa tai käyttötapauksissa (esimerkiksi osana monikerrossuojausta[13] fyysisesti suojatun alueen sisällä).

Käsiteltäessä vain kansallista suojattavaa aineistoa, salauksen käyttämiselle ja valitun salauksen vahvuudelle on tietoturva-asetuksessa[14] jätetty riskienhallinnan pohjalta enemmän liikkumavaraa.

[12] Uudelleenkäyttömahdollisuuksia on kuvattu yksityiskohtaisemmin Viestintäviraston ohjeessa "Kiintolevyjen elinkaaren hallinta - Ylikirjoitus ja uusiokäyttö".
[13] Engl. Defence in depth.

Käytännössä salauksen poisjättämistä edellä mainituissa käyttötapauksissa on kuitenkin nykymaailman uhkiin nähden erittäin haastavaa perustella myöskään kansallisen tiedon osalta. Lisäksi on huomioitava, että käsiteltäessä esimerkiksi EU:n turvallisuussäännösten tai muiden vastaavien sopimusten piiriin kuuluvaa kansainvälistä turvaluokiteltua aineistoa, salausratkaisun suojausvaikutuksen riittävyys kyseiseen käyttöympäristöön ja suojaustasolle tulee olla kansallisen salaustuotteiden hyväksyntäviranomaisen (CAA, Crypto Approval Authority, Suomessa Viestintäviraston NCSA-toiminto) hyväksymä. Tällä tavoitellaan riittävää varmuutta siitä, että valittu salaustuote toteuttaa kyseiselle suojaustasolle riittävän vahvan suojauksen, ja että salaustuotteessa ei ole yleisiä salaustoteutuksiin liittyviä virheitä.

6.3 Riskianalyysi

Tietoturva-asetus edellyttää, että tietoturvallisuuden suunnittelu on hyvän tiedonhallintatavan mukaista, ja tietoturvallisuustoimenpiteet mitoitetaan ottamalla huomioon suojattavien tietojen merkitys. Lisäksi tietojen käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät on kartoitettu.

Salausratkaisuiden käyttöönottoon liittyvällä riskien arvioinnilla pyritään määrittämään suojattava kohde ja tunnistamaan uhkat, jotka voivat vaikuttaa salassa pidettävän tai muuten suojattavan tietoaineiston tai -järjestelmän luottamuksellisuuteen ja eheyteen. Lisäksi salausratkaisun suunnittelussa tulee ottaa huomioon olemassa olevat, havaittuja riskejä pienentävät kontrollit, määrittää riskien potentiaaliset seuraukset sekä priorisoida niiden tärkeysjärjestys.

Riskien tunnistamisen tulee olla kohdeorganisaation tavoitteisiin ja toimintaan perustuvaa. Niiden aiheuttajat ja seuraukset, todennäköisyydet, omistajat ja sietokyky pitää arvioida toimintaympäristön näkökulmasta.

Salausmenetelmän kestävyyttä kryptonanalyysia vastaan kuvataan käsitteellä kryptografinen vahvuus. Sen määrityksessä huomioidaan mm. algoritmin matemaattinen kompleksisuus ja ajanmukaiset hyökkäysmenetelmät.

Viestintäviraston vetämä kryptologian asiantuntijoista koostuva työryhmä on laatinut CAA-viranomaisen hyväksyntätyötä varten taulukon luotettavista algoritmeista ja kryptografisista vahvuus-vaatimuksista, joita noudatetaan suojaustasojen IV - II tiedon salaamisessa (Liite 1). Yleistettävyyden vuoksi vahvuusvaatimuksissa on oletettu, että tiedon on pysyttävä salassa useita kymmeniä vuosia, ja että ympäristö, jossa salattava tietoliikenne kulkee, muodostaa korkean uhkan salaukselle.

Kryptografisen vahvuuden skaalaaminen alaspäin ei ole yksinkertaista, sillä teoreettisetkin heikkoudet voivat muuttua toteutuskelpoisiksi lähestyttäessä menetelmän rajoja. Ammattilaisten laatimia vahvuusvaatimuksia noudattamalla riski luottamuksellisuuden tai autenttisuuden menetyksestä pitkälläkin salassapitoajalla on vähäinen.

[14] Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010). URL: http://www.finlex.fi/fi/laki/ajantasa/2010/20100681.

6.3.1 Kryptografiset vahvuudet suhteessa uhkaan ja vaikuttavuuteen

Ympäristöstä, hyökkäyksen vaikuttavuudesta ja suojausajasta riippuvat tekijät voivat lieventää salaukselle asetettavia vaatimuksia. Kun CAA-viranomainen soveltaa kryptovahvuusvaatimuksia lieventävästi, se voi käyttää työryhmässä tai kansainvälisissä foorumeissa sovittuja käytäntöjä. Salaukseen kohdistuvan uhkan katsotaan olevan korkein seuraavissa tapauksissa:

- suojaamattomat avoimet tietoverkot joihin pääsyä ei valvota,
- alemmalle suojaustasolle hyväksytyt järjestelmät,
- viestintä ilmarajapinnan yli
- kontrolloitujen alueiden ulkopuolelle vietävät ja muut fyysisten suojauksien ulkopuolella sijaitsevat tietokoneet ja tallennuslaitteet yms. tietovarannot.

Uhkaaja on henkilö tai taho, joita vastaan tietoa suojataan. Fyysinen ympäristö lieventää uhkaa, jos se suojaa tietoa niin, ettei ryhmän ulkopuolinen henkilö mitenkään voi saada salatussa muodossa olevaa tietoa haltuunsa. Ryhmät luokitellaan henkilöille tehdyn turvallisuusselvityksen ja tarpeellisuusperiaatteen perusteella. Korkean uhkan muodostavassa ympäristössä täysin ulkopuoliset, siis henkilöt joilla ei ole turvallisuusselvitystä, voivat saada salatussa muodossa olevan tiedon käsiinsä kryptoanalyysiä varten. Tällainen tilanne on esimerkiksi silloin, kun salattu tieto lähetetään Internetin yli.

Vahvuusvaatimusten soveltamisessa on mahdollista huomioida myös luottamuksellisuuden tai eheyden menetyksen aiheuttama vahinko. Luottamuksellisuuden menetyksestä, siis tiedon paljastumisesta aiheutunut vahinko on suoraan verrannollinen turvallisuusluokkaan.. Sen sijaan eheyden menetyksen (tiedon alkuperä, kiistämättömyys, muuttamattomuus, jne) asia ei ole näin suoraviivainen. Vaikutusta voi arvioida tiedon omistaja, järjestelmätarkastajat ja järjestelmän käyttäjät.

On kuitenkin olemassa järjestelmiä ja tilanteita, joissa tiedon eheys on tärkeämpää kuin sen luottamuksellisuus. Näin on esimerkiksi rahaliikenteessä ja sähköisesti allekirjoitetuissa todistuksissa. Mikäli organisaation käyttämä tietosisältö sisältää eheydeltään sen toiminnan kannalta kriittisiä elementtejä, on suositeltavaa luokitella tietosisältö sisäisesti myös eheyden mukaan.

6.3.2 Salausajan vaikutus avainpituuksiin ja algoritmeihin

On mahdollista, että suunnitellaan järjestelmiä, joissa välitetään tietoa, jonka salassapitoaika on hyvin lyhyt, esimerkiksi yksi päivä. Silloin ei olisi kohtuullista vaatia salausmenetelmältä vahvuutta, jolla saavutetaan vuosien salassapitoaika.

Jos järjestelmä, joka ei toteuta suojaustasoa vastaavaa salausta, hyväksytään lyhytaikaisen suojaustarpeen perusteella, sen käyttö ja ohjeistus on kuitenkin monimutkaisempaa, ja heikomman salauksen riskit tulee ymmärtää ja mahdollisuuksien mukaan kompensoida. Järjestelmän tulee muuten täyttää suojattavan aineiston vaatimukset. Käyttäjällä on syytä olla käytettävissä toinen tapa, jolla käsitellä pidempään salassapidettävää tietoa tai tulee ennaltaehkäistä tilanne, jossa sellaista tietoa on tarve lähettää samalla järjestelmällä.

Salausavaimet tulee vaihtaa salausajan vaatimusten mukaisesti. Salausajan kuluminen alkaa siitä hetkestä kun epäsymmetrisen avainparin julkinen avain tai symmetrisellä avaimella salattu tieto altistuu hyökkääjälle ensi kertaa, esim. kun varmenne lähetetään tai kun symmetristä avainta käytetään.

On syytä ottaa huomioon myös aika-muisti-vaihtokauppahyökkäys (time-memory-tradeoff attack), jossa hyökkääjä pystyy valmistelemaan salauksen murtamista ennakkoon, ja varsinainen salauksen purkamiseen kuluva aika pienenee.

Perusteet järjestelmän turvalliselta käytöltä saattavat uusien kryptologisten hyökkäystapojen tai laskentatehon kasvun myötä pudota pois nopeasti, ja siksi järjestelmän korvaamiseen tulee varautua. Tilanteen seuraamista ja järjestelmän käytön ohjaamista varten olisi hyvä nimetä vastuuhenkilö.

Minimissäänkin salausmenetelmän on kestettävä hyökkäyksiä niin, ettei mikään hyökkääjä kykene avaamaan liikennettä ajantasaisesti (on-line). Suositellaan, että tätä ehtoa täyttämättömiä salauksia ei käytettäisi lainkaan. On huomioitava myös salausmenetelmien kestävyys suhteessa käytettävissä olevaan laskentatehoon, joka kasvaa ns. Mooren lain mukaisesti. Vaikka jokin menetelmä tänä päivänä antaisi riittävän suojan, se voi vuosien kuluttua olla helposti murrettavissa. On huomioitava myös hyöty, jonka hyökkääjä saa salauksen murtamisesta – se vaikuttaa siihen, kuinka paljon resursseja ja aikaa hyökkääjä on valmis uhraamaan murtamiseen. Tästä syystä vahvuusvaatimuksista poikkeamista ei suositella lainkaan korkeille suojaustasoille.

6.4 Vaatimusmäärittely

Salausratkaisua hankittaessa tulee vaatimusmäärittelyssä huomioida erityisesti

1. toiminnallisten vaatimusten (käytettävyys)tarpeiden täyttyminen,
2. tiedon suojaustaso,
3. edellisestä johdetut mahdollisen tuotejoukon rajoitukset, sekä
4. tiedon omistajan (kansallinen, EU, NATO, jne.) erityisvaatimukset.

Vaatimusmäärittelyssä suositellaan vahvasti huomioitavaksi myös salausratkaisun tuen jatkuvuus ja saatavuus. Aina kun salausratkaisua suunnitellaan osaksi kansainvälistä suojattavaa tietoa käsittelevää järjestelmää, suositellaan ennen hankintapäätöksen tekemistä olemaan yhteydessä Viestintäviraston NCSA-toimintoon[15].

6.5 Jatkuva palvelu ja kehittäminen

Salausratkaisun koko elinkaarta on hallittava. Tämä korostuu erityisesti fyysisesti erillisissä salaustuotteissa, joiden kirjanpidon on oltava ajantasainen, luotettava ja jäljitettävissä oleva. Valinnassa on huomioitava erityisesti, että hankitaan vain kyseessä olevaan käyttötapaukseen hyväksytty salausratkaisu ja varmistetaan, että kyseessä on todellakin hyväksytty laitemalli ja/tai ohjelmistoversio.

[15] www.ncsa.fi

Salausratkaisuista, kuten muistakin ohjelmistoista löytyy ajoittain haavoittuvuuksia. Salausratkaisu tulee pitää päivitysten piirissä siten, että kyseiseen käyttötapaukseen liittyvät turvapuutteet korjataan välittömästi. Erityisesti tilanteissa, joissa käytetään kansallisen salaustuotteiden hyväksyntäviranomaisen hyväksymää salausratkaisua, tulee päivitysversion hyväksyntästatus varmistaa ennen päivityksen asentamista.

6.6 Ratkaisun tarkastaminen ja hyväksyminen

Kun käsitellään tietojärjestelmässä esimerkiksi EU:n kansainvälistä turvaluokiteltua aineistoa, sen tulee olla kansallisen turvallisuusjärjestelyjen hyväksyntäviranomaisen (SAA, Security Accreditation Authority, Suomessa Viestintäviraston NCSA-toiminto) tarkastama ja hyväksymä. Osa hyväksymisprosessia on sen tarkastaminen, onko käytetyillä salausratkaisuilla voimassaoleva hyväksyntä kansalliselta salaustuotteiden hyväksyntäviranomaiselta (CAA, Crypto Approval Authority).

Vastaava tarve voi ilmetä myös vain kansallista suojattavaa tietoa käsittelevissä tietojärjestelmissä esimerkiksi silloin kun niissä halutaan käsitellä useamman suomalaisen viranomaisen turvaluokiteltua tietoa ja käytön ehdoksi on asetettu kansallisen tietoturvallisuusviranomaisen todistus vaatimustenmukaisuudesta. Järjestelmähyväksynnän hakeminen ja hyväksyttyjen tuotteiden käyttö on suositeltavaa aina kun on tietojärjestelmissä tarkoitus käsitellä suojattavaa tietoa.

Sekä kansainvälisen että kansallisen tiedon suojaamisessa tiedon omistajalla on aina mahdollisuus hyväksyä suojaukset omistamansa tiedon osalta. Omistajalla voi olla perustellut syyt tapauskohtaisesti poiketa yleisistä salausvahvuusvaatimuksista, ja hyväksyä tiettyihin erityistapauksiin vahvuudeltaan heikompitasoinen salausratkaisu. Omistajan riskienarvioinnissa hyväksymä syy poikkeavalle suojaukselle voi perustua esimerkiksi tarpeeseen välttää ihmishenkien menetys onnettomuustilanteiden selvittelyissä tai muissa viranomaisen operatiiviseen toimintaan liittyvissä tehtävissä.

6.7 Esimerkkejä

6.7.1 Tarveanalyysi

Organisaatiossa suunnitellaan sähköisen viestintäjärjestelmän rakentamista luokitellun tiedon välittämiseksi kahden eri paikkakunnalla sijaitsevan toimipisteen välille. Organisaatio on luokitellut tietonsa suojaustasoille IV, III ja II. Alustavasti on hahmoteltu järjestelmää suojaustasolle II.

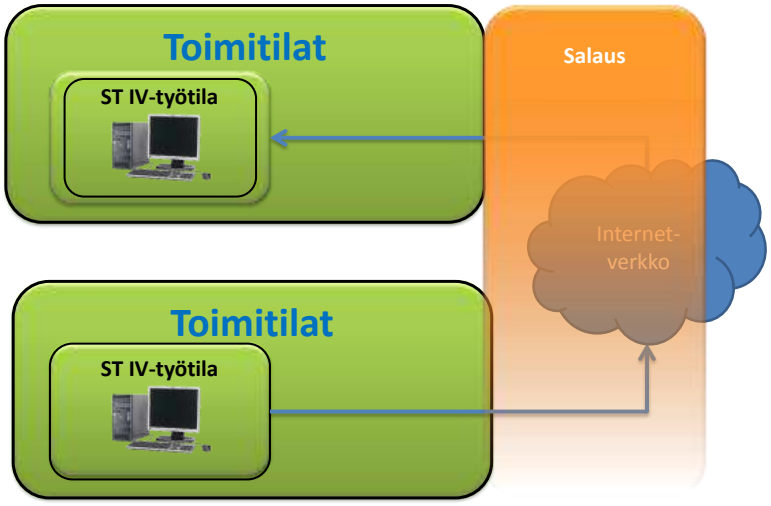
Tarkemmassa selvityksessä havaitaan välitettävän tiedon jakautuvan siten, että tiedosta 50 % on julkista, 40 % suojaustasoa IV, 8 % suojaustasoa III ja 2 % suojaustasoa II. Havaitaan, että suojaustason II tietoa tarvitsee välittää vain yksittäisiä kertoja vuodessa. Toisaalta suojaustason II järjestelmän rakentaminen aiheuttaisi kohtuuttomia kustannuksia toiminnallisiin tarpeisiin nähden. Havaitaan myös, että suojaustasojen III ja II tietoa käsittelee vain pieni osa organisaation henkilöstöstä.

Päätetään toteuttaa koko organisaation kattava etäkäyttöratkaisu suojaustason IV tietojen käsittelyyn. Suojaustason III tietojen käsittelijöille toteutetaan erillinen toimipisteet yhdistävä ratkaisu, sekä rajataan suojaustasojen III ja II käsittely erillisiin, kyseisten suojaustasojen mukaisiin työasemiin. Suojaustason II tiedot päädytään toimittamaan jatkossakin henkilökuriiria käyttäen.

6.7.2 VPN-ratkaisu organisaation kahden toimipisteen välillä

Organisaatiolla on muista ympäristöistä eristetty suojaustason III käsittely-ympäristö, joka on ulotettu kahteen tai useampaan fyysisesti suojattuun toimipisteeseen. Verkkotason rajapinta voi tällöin olla muotoa [eristetty käsittely-ympäristö] - [palomuurilaitteisto/-ohjelmisto] – [ko. suojaustasolle hyväksytty salauslaite] - [palomuurilaitteisto/-ohjelmisto] - [Internet] – [palomuurilaitteisto/-ohjelmisto] - [ko. suojaustasolle hyväksytty salauslaite] - [palomuurilaitteisto/-ohjelmisto] - [eristetty käsittely-ympäristö].

Toisin sanoen salausta käytetään tilanteessa, jossa suojattava tieto liikkuu fyysisesti suojattujen alueiden ulkopuolella. Salaus toteutetaan OSI-mallin verkkokerroksella (L3, salaus esim. IPsec:llä).



Kuva 6. Salaus tulee ottaa käyttöön organisaation fyysisesti suojattujen alueiden ulkopuolella, kun sitä käytetään salassa pidettävän tiedon välittämiseen.

6.7.3 VPN-ratkaisu organisaation toimipisteen ja työntekijän etäkäyttölaitteiston välillä

Organisaatiossa on etätyömahdollisuus, joka mahdollistaa suojaustason IV tietojen käsittelyn. Organisaation tarjoama suojaustason IV kannettava tietokone muodostaa ko. suojaustasolle hyväksytyn client-VPN -salausratkaisun kautta yhteyden organisaation suojaustason IV asianhallintajärjestelmään.

6.7.4 VPN-ratkaisu palvelinsalien välillä

Organisaation palvelimet on kahdennettu eri palvelinsaleihin. Palvelimet synkronoivat tietonsa säännöllisesti palvelinsalien välillä. Suuresta liikennemäärästä johtuen L3-salaimet eivät sovellu, joten palvelinsalien välinen salaus on toteutettu L2-salaimilla.

6.7.5 Sähköpostin salausratkaisu

Organisaatiossa käytetään sähköpostit liitteineen salaavaa ohjelmistoa (esim. GnuPG). Vaihtoehtoisesti organisaatiossa voidaan käyttää tiedostosalausohjelmistoa, jolla suojattavat tiedot salataan ja salatussa muodossa oleva tieto voidaan välittää sähköpostitse.

6.7.6 Etäkäyttölaitteiston sekä muiden päätelaitteiden kiintolevyn ja apumuistien salaus

Organisaation etäkäyttöön tarjottavissa kannettavissa tietokoneissa käytetään koko kiintolevyn salaavaa ohjelmistosalausratkaisua. Tämä sama on käytännössä suositeltavaa toteuttaa kaikissa niissä päätelaitteissa (kannettavat tietokoneet, tabletit, älypuhelimet), joissa se riskiperusteisesti pitää toteuttaa ja se voidaan kustannustehokkaasti laitteen käytettävyys taaten mahdollistaa.

6.7.7 USB-muistien salaus

Organisaatiossa käytetään "rautasalauksella" automaattisesti kaiken sisältönsä salaavia USB-muisteja. Vaihtoehtoisesti organisaatiossa käytetään tavallisia USB-muisteja, mutta niille ei saa viedä kuin toisessa ympäristössä hyväksytysti salattua aineistoa. Toisin sanoen USB-muistia käytetään vain salatussa muodossa olevan aineiston käsittelyyn/siirtämiseen fyysisesti suojattujen alueiden välillä.

6.7.8 Eri omistajien tietojen erottelu yhteiskäyttöisellä palvelimella

Organisaatio tekee tuotekehitystyötä usealle tarkastusoikeuden varaavalle tiedon omistajalle. Organisaatio käyttää varmistusratkaisua, joka tallentaa samalle fyysiselle levylle eri omistajien tiedot omilla avaimillaan salattuina tiedostoina. Toisin sanoen yhteiskäyttöisillä levyillä tarkastusoikeuden varaavien omistajien tiedot säilytetään ainoastaan eri avaimilla salatussa muodossa. Tällöin kukaan tiedon omistaja ei tarkastusoikeuden varjolla pysty saamaan selväkielisessä muodossa kuin vain omistamansa tiedot.

6.7.9 Salasanojen tallentaminen tietojärjestelmissä

Salasanoja käyttävissä palveluissa ja järjestelmissä on syytä kiinnittää erityistä huomiota salasanojen turvalliseen suojaamiseen. Ne eivät saa löytyä palvelusta selväkielisinä, vaan ne pitää tallentaa oikeaoppisesti tiivisteiden ja suolauksen avulla.

Hyvin toteutetussa palvelussa salasanoja ei varastoida järjestelmään, vaan niistä lasketaan tiiviste yksisuuntaisen tiivistefunktion avulla. Tiivisteiden ja suolaamisen avulla suojattujen salasanojen väärinkäyttöriski pienenee tietomurtojen yhteydessä. Salasanojen murtaminen edellyttää yleensä sen, että murtaja saa haltuunsa tiivisteen, minkä jälkeen oikeaa salasanaa voi yrittää arvailla palvelun ulkopuolella sitä varten kehitetyillä ohjelmistoilla.

Salasanatiivisteiden luomiseen on käytettävissä useita vaihtoehtoisia salasanatiivistealgoritmeja. Osa salasanatiivistealgoritmeistä hyödyntää tiivisteen muodostamisessa jotain standardoitua kryptografista tiivistefunktioita. Ei ole kuitenkaan suositeltavaa luoda salasanatiivisteitä yksinään tällaisella tiivistefunktioilla, vaan käyttää sitä varten kehitettyä algoritmia.

Merkittävä tekijä salasanatiivistealgoritmien turvallisuudessa on niin sanotun suolan käyttö. Suola on satunnaisesti muodostettu, yleensä julkinen, uniikki käyttäjäkohtainen merkkijono, jota käytetään algoritmin parametrina salasanan lisäksi. Suolan muuttaminen muuttaa myös tiivistettä, vaikka salasana pysyisi samana. Tämä vaikeuttaa merkittävästi salasanojen selvittämistä tiivisteiden perusteella, eikä muutaman salasanan murtaminen helpota muiden salasanojen murtamista.

Toinen tärkeä tekijä turvallisuudessa on algoritmien nopeus; salasanatiivistealgoritmit ovat huomattavasti hitaampia kuin esimerkiksi standardoidut kryptografiset tiivistefunktiot, mikä hankaloittaa salasanojen murtamista väsytysmenetelmällä.

6.7.10 Aineiston tallentaminen pilveen turvallisesti

Käsiteltävän datan määrä ja uusien teknologioiden käyttö saa monet organisaatiot harkitsemaan tiedon tallentamisen ulkoistamista pilvipalveluihin. Näissä palveluissa saatetaan tarjota erityyppisiä tietoturvallisuutta parantavia ratkaisuja, kuten tiedon automaattista salausta. On tärkeää muistaa, että myös pilvipalveluihin tulee soveltaa tiedon salaamisen perusperiaatteita; salausmenetelmän tulee olla turvallinen ja asiaankuuluvan viranomaisen hyväksymä, mutta on myös otettava huomioon autentikointi ja avaintenhallintakysymykset.

Avaintenhallinnan osalta kynnyskysymykseksi saattaa muodostua avaimia luova ja säilyttävä taho. Jos palvelun tarjoaa ulkopuolinen yritys, tuo yritys usein myös hallinnoi salausavaimia. Tällöin salaus ei tarjoa suojaa pilvipalvelun tarjoajaa vastaan, vaan sinne talletettavan tiedon tulee olla sellaista, johon palveluntarjoajalla on valtuutus. Usein on myös hyvin hankala tarkastaa avaintenhallintasuunnitelmaa, avainten suojaamista ja vaihtamista. Selaimella käytettävien pilvipalvelujen turvallisuus riippuu palvelujen omien varmenteiden lisäksi kaikkien selaimiin luotettaviksi asetettujen juurivarmentajien luotettavuudesta ja turvallisuudesta.

Jos aineiston salaus toteutetaan ennen palveluun viemistä hyväksytyillä menetelmillä, voidaan pilvipalvelua käsitellä kuten mitä tahansa ei-luotettua tiedon säilytyspaikkaa. Tällöinkin on muistettava, että pääsyä tietoon hallinnoi se, jolla on avaimet hallussaan. Avaimia, tai mitään muutakaan suojaamatonta materiaalia ei tule säilyttää pilvipalvelussa. On olemassa myös organisaatioiden omia pilvipalveluita, (ns. private cloud). Tällaisia käytettäessä avaintenhallinta voidaan pystyä toteuttamaan siten, että avaimet pysyvät vain valtuutettujen tahojen hallussa.

Pilvipalveluissa ei periaatteessa ole eroa muihin tiedon käsittelyn ulkoistusratkaisuihin, kunhan muistetaan soveltaa samoja periaatteita ja sääntöjä kuin perinteisissä ulkoistusympäristöissä.

Liite 1. Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset suojaustasot

Liitettä ylläpidetään ja säilytetään viestintäviraston sivustolla osoitteessa http://www.ficora.fi/xxx

Liite 2. Keskeinen sanasto

Epäsymmetrinen salaus, asymmetrical encyption
Salaus, jossa viestin avaaminen tapahtuu eri avaimella kuin sen salakirjoitus. Menetelmä käyttää kahta toisistaan riippuvaa avainta, joista toinen on julkinen ja toinen on salainen. Viesti salataan viestin vastaanottajan julkisella avaimella, joka on jossakin turvallisessa paikassa kaikkien nähtävillä ja saatavilla. Kun viesti on salattu, se saadaan auki ainoastaan vastaanottajan salaisella avaimella, joka on pelkästään vastaanottajan tiedossa.

CA (certificate authority)
Varmenteita myöntävä taho. Varmentajan tehtävä on selvittää, onko varmenteen hakija todella se, joka väittää olevansa. Suomen valtion virallisena juurivarmentajana toimii Väestörekisterikeskus.

COMSEC (communications security)
Viestinnän suojaamiseen liittyvät menettelyt, sisältäen salausteknisten menetelmien lisäksi mm. salausteknisen materiaalin oikean käsittelyn ja fyysisen turvallisuuden käytäntöjä.

Kryptologia (cryptology)
Kryptologia on tiede, joka tutkii salakirjoitusmenetelmiä eli kryptografiaa ja sen purkamista eli kryptoanalyysiä.

Kryptografia (cryptography)
Kryptografia on salakirjoitusten matemaattista teoriaa tutkiva tieteenala.

Kryptoanalyysi (cryptanalysis)
Kryptoanalyysi on tieteenala, joka kehittää keinoja murtaa salakirjoituksia (ilman salausavainta). Sen vastakohta on kryptografia, joka tutkii ja pyrkii kehittämään salakirjoituskeinoja.

Salaus (encryption)
1) tiedon, esimerkiksi toiselle henkilölle lähetettävän viestin käsittely niin, että ulkopuolinen ei saisi haltuunsa tietoa tai viestiä tai sen sisältämää informaatiota
2) salakirjoitus

Salauksen avaaminen / purkaminen (decryption)
Salakirjoitetun tekstin muuntaminen takaisin selväkieliseen muotoon salausalgoritmin kuvauksen mukaisesti, purku-/salausavainta käyttämällä.

Salauksen murtaminen (breaking encryption)
Tekniset ja hallinnolliset menetelmät, joiden avulla pyritään purkamaan salattuna olevaa tietoa

selväkieliseen, ymmärrettävään muotoon ilman tietoa salausavaimesta. Murtaminen voi tapahtua esim. ns. raakaa voimaa (brute force) käyttämällä, eli käyttäen hyväksi tietokoneiden laskentatehoa, matemaattisen kryptoanalyysin paljastamia salausalgoritmin heikkouksia, salaintoteutuksen heikkouksia tai näiden yhdistelmiä. On huomattava, että puhekielessä myös teoreettinen murtaminen (mikä tahansa tekninen menetelmä, jolla saavutetaan algoritmikuvauksen antamia rajoja hiukankin nopeampi avaintenhaku) saatetaan samaistaa murtamiseen yleensä ja sitä kautta käytännölliseen murtamiseen.

Salausavain (encryption key)
Salakirjoitusalgoritmin parametrinä toimiva merkki- tai bittijono, jota salausalgoritmin mukaisesti käytetään tiedon salaamiseksi. Salausavain pidetään salassa, ja ilman sitä purkamisen tulisi olla liian työlästä.

Salausavainten hallinta (encryption key management)
Salauksesta vastaava taho huolehtii salauksessa käytettävien tietojen hallitsemisesta mukaan luettuna niin hallinta, varmistaminen sekä kaikki muu hallinta ja organisointi.

Symmetrinen salaus (symmetrical encryption)
Tarkoittaa menetelmää, jossa viesti salataan samalla avaimella jolla salaus puretaan.

Tiedon omistaja
Tiedon omistajalla tarkoitetaan tässä yhteydessä sitä tahoa, joka luo alkuperäisen tiedon ja laittaa sen tarvittaessa jakeluun. Vastaanottajalla ei ole oikeutta muuttaa ilman erillistä sopimista salassa pidettävän tietoaineiston luokitusta, vastaavasti vastaanottajan tulee käsitellä tietoa sen omistajan vaatimilla tavoilla, myös käytettävien salausvaatimusten osalta.

Tiiviste (hash)
Olemassa olevasta tiedosta tiivistysfunktiota käyttäen muodostettu lyhyempi uusi tieto esimerkiksi varmenteen muodostamiseksi.

Varmenne (certificate)
Varmenne voi sisältää muun muassa käyttäjän julkisen avaimen, henkilötiedot, varmenteen voimassaoloajan sekä varmenteen myöntäjän sähköisen allekirjoituksen. Varmenteilla on keskeinen rooli salauksen käytännön laajamittaisessa toteuttamisessa.

Liite 3 Voimassa olevat VAHTI –julkaisut

VAHTI 2/2014 Tietoturvallisuuden arviointiohje
VAHTI 1/2014 VAHTIn toimintakertomus vuodelta 2013
VAHTI 5/2013 Päätelaitteiden tietoturvaohje
VAHTI 4/2013 Henkilöstön tietoturvaohje
VAHTI 2/2013 Toimitilojen tietoturvaohje
VAHTI 1/2013 Sovelluskehityksen tietoturvaohje
VAHTI 3/2012 ICT-teknisen ympäristön tietoturvataso-ohje
VAHTI 2/2012 ICT-varautumisen vaatimukset
VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohje
VAHTI 2/2011 Johdon tietoturvaopas
VAHTI 4/2010 Sosiaalisen median tietoturvaohje
VAHTI 3/2010 Sisäverkko-ohje
VAHTI 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta
VAHTI 7/2009 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä
VAHTI 6/2009 Kohdistetut hyökkäykset
VAHTI 3/2009 Lokiohje
VAHTI 9/2008 Hankkeen tietoturvaohje
VAHTI 8/2008 Valtionhallinnon tietoturvasanasto
VAHTI 7/2008 Informationssäkerhetsanvisningar för personalen
VAHTI 3/2008 Valtionhallinnon salauskäytäntöjen tietoturvaohje
VAHTI 2/2008 Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta
VAHTI 3/2007 Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 1/2007 Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä
VAHTI 12/2006 Tunnistaminen julkishallinnon verkkopalveluissa
VAHTI 11/2006 Tietoturvakouluttajan opas
VAHTI 9/2006 Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 7/2006 Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi
VAHTI 6/2006 Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006 Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 2/2006 Electronic-mail Handling Instruction for State Government
VAHTI 3/2005 Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005 Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005 Information Security and Management by Results
VAHTI 5/2004 Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004 Datasäkerhet och resultatstyrning
VAHTI 3/2004 Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004 Tietoturvallisuus ja tulosohjaus
VAHTI 7/2003 Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 2/2003 Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003 Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 3/2002 Valtionhallinnon etätyön tietoturvaohje

VAHTI 4/2001 Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje

Ohjeisto löytyy VAHTIn Internet-sivuilta www.vm.fi/vahti sekä www.vahtiohje.fi