VALTIOVARAINMINISTERIÖ

VAHTI

Ohje salauskäytännöistä

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä
– VAHTI 2/2015

Julkisen hallinnon ICT

VALTIOVARAINMINISTERIÖ

Ohje salauskäytännöistä

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä
– VAHTI 2/2015

Julkisen hallinnon ICT

4041 0017
Painotuote

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 0295 16001 (vaihde)
Internet: www.vm.fi
Taitto: Valtioneuvoston hallintoyksikkö/Tietotuki- ja julkaisuyksikkö/Pirkko Ala-Marttila

ISSN 1459-3394 (nid.)
ISBN 978-952-251-725-8 (nid.)
ISSN 1797-9714 (pdf)
ISBN 978-952-251-726-5 (pdf)

Lönnberg Print & Promo, 2015

VALTIOVARAINMINISTERIÖ

Ohje

VM/2204/00.00.00/2015

4.11.2015

Ministeriöille, virastoille ja laitoksille

Ohje salauskäytännöistä

Valtiovarainministeriön antaman Ohjeen salauskäytännöistä (VAHTI 2/2015) tavoitteena on kehittää viranomaisten salassa pidettävän tiedon suojaamista. Kansainvälisten tietoturvavelvoitteiden piirissä olevien tietoaineistojen salauksessa noudatetaan kansallisen turvallisuusviranomaisen antamia määräyksiä.

Ohje on laadittu valtionhallinnon ja julkisen hallinnon organisaatioille, mutta sitä voidaan käyttää myös laajemmin kehitettäessä yksityisten organisaatioiden tiedon salausta.

Ohje tukee tiedon salaamisen suunnittelua, käyttöönottoa, toteuttamista ja ylläpitoa julkisen hallinnon hankkimissa ja käyttämissä ICT-palveluissa ja – ratkaisuissa.

Ohje edistää osaltaan Suomen kyberturvallisuusstrategian täytäntöönpanoa ja ohjeen julkaiseminen on osa Suomen osallistumista Euroopan unionin kyberturvallisuuskuukauteen.

Ohjeen on valmistellut Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän alaisuudessa toimiva tekninen jaosto.

Lisätietoja ohjeesta antavat:

Kimmo Rousku, VAHTI-pääsihteeri, teknisen jaoston puheenjohtaja
Aarne Hummelholm, teknisen jaoston varapuheenjohtaja
(etunimi.sukunimi@vm.fi)

Kunta- ja uudistusministeri — Anu Vehviläinen

Yksikön päällikkö,
VAHTIn puheenjohtaja — Aku Hilve

Liite — Ohje salauskäytännöistä (VAHTI 2/2015)

Tiedoksi — Kunnat

Valtiovarainministeriö Snellmaninkatu 1 A, Helsinki PL 28, 00023 Valtioneuvosto Puh 0295 16001 (Vaihde) Faksi 09 160 33123 valtiovarainministerio@vm.fi www.vm.fi Y-tunnus 0245439-9

Sisältö

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, kuten mittavina hyökkäyksinä kauppojen sähköisiä maksujärjestelmiä vastaan
- organisaation liiketoimintaa haittaavina palvelunestohyökkäyksinä, joissa usein on taustalla taloudellisen edun tavoittelu esimerkiksi kohdeorganisaatiota kiristämällä
- tiedusteluorganisaatioiden toimina, joissa yritetään kerätä hyökkääjää kiinnostavaa tietoa pysyen mahdollisimman pitkään salassa
- yksityishenkilöihin kohdistuvina kampanjoina, joilla yritetään saavuttaa taloudellista hyötyä, esimerkiksi kalastelemalla pankki- tai muiden järjestelmien käyttäjätunnuksia ja salasanoja
- lunnashaittaohjelmina (”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 on 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 säännöllisesti myös uutisiin. Kenties yleisin esimerkki on tietomurto verkkopalveluun, jonka käyttäjätietokannassa olevat salasanat ovat vuotaneet murtautujalle; väärällä tavalla salatut salasanat puretaan ja murtautuja julkaisee ne selväkielisinä.

Edellisten lisäksi nopeasti kasvava uhka on yritysten maksuliikenne- tai muihin talousjärjestelmiin murtautuminen ja asiakas- tai luottokorttitietojen varastaminen sekä niiden hyödyntäminen rikollisesti.

Kaikki edellä olevat esimerkit ovat sellaisia, jotka uhkaavat myös julkishallinnon toimintaa ja tietoja. Tiedon salaaminen liittyy osittain kaikkiin edellä mainittuihin esimerkkeihin. Eräs tämän vuosikymmenen loppupuolen keskeisiä suuntauksia tuleekin olemaan tiedon salauksen merkityksen kasvu ja sen käytön laajentuminen.

Hyvä esimerkki salaustarpeesta on pilvipalvelu, jossa salassa pidettävät tiedot sijaitsevat organisaation ulkopuolella, mahdollisesti ulkomailla, ja niitä käytetään internet-verkon ylitse. Pilvipalveluiden käyttöä voidaan laajentaa siinä vaiheessa kun niissä on mahdollista käyttää asiakkaan tarkastamaa ja hyväksymää tiedon salausratkaisua. Lisäksi salaukseen liittyvä avaintenhallinta tulee toteuttaa siten, että myös se täyttää kaikki asiakkaan edellyttämät vaatimukset.

Kuten kaikessa toiminnassa, myös salauksen suunnittelussa, toteutuksessa, käyttöönotossa ja ylläpidossa tulee hyödyntää riskienhallintaa sekä ottaa huomioon lakisääteiset ja 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 arkkitehtuurinsa kehittämistä.

Termiä **tiedon salaus** käytetään hyvin laajassa merkityksessä. Tässä ohjeessa on pyritty nostamaan esille niitä asioita, joita oikealla tavalla toteutettu salausratkaisu edellyttää. On olemassa huonosti toteutettuja salauksia, mutta myös sellaisia salausratkaisuja, jotka ovat laadukkaita ja joissa on pyritty huomioimaan käsiteltävänä olevan tiedon koko elinkaari. Elinkaari voi olla hyvinkin lyhyt tai vastaavasti kymmeniä vuosia.

Tämän ohjeen on laatinut Valtion tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) asettama tekninen jaosto. Ohje on hyväksytty VAHTI-johtoryhmän kokouksessa 18.8.2015.

1 Tausta ja tavoite

1.1 Ohjeistuksen tausta

Tietoturvallisuuden merkitys on jatkanut kasvuaan viimeisten vuosien aikana. Keskeisiä muutostekijöitä ovat esipuheessa mainitun uhkakuvien muuttumisen ohella nopeasti muuttuva yhteiskunta sekä ICT-palveluiden käyttämiseen ja tuottamiseen liittyvät tekijät kuten

- digitalisoinnin kasvava tarve; yhä useampi toiminto on sähköistetty ja kehitys tulee tältä osin vielä kiihtymään laajamittaisen, kokonaisia toimintaketjuja koskevan digitalisoinnin myötä
- ajasta ja paikasta riippumaton työskentely sekä julkishallinnossa että julkishallinnon palveluita käyttävien asiakkaiden ja kansalaisten keskuudessa
- uusien päätelaitteiden ja langattomien tietoliikenneyhteyksien kehittyminen
- uudenlaiset palveluiden tuotantotavat, palveluiden virtualisoiminen, jaetut kapasiteettipalvelut sekä pilvipalvelut

Nämä kaikki ovat luoneet uusia tapoja käyttää palveluita, joka edellyttää myös tietoturvallisuuden ja jatkuvuuden hallinnan sekä varautumisen uudelleenarviointia.

Edellä kuvatut muutostekijät aiheuttavat myös sen, että eri tasoille luokiteltuja, sekä julkisia että salassa pidettäviä tietoja käsitellään yhä moninaisemmilla tavoilla. Myös tämä edellyttää tietojen salaamisen kehittämistä.

Laskentatehon nopea kehittyminen heikentää salausta

Tiedon salaaminen pohjautuu matemaattisiin algoritmeihin. Erilaisten laskenta-alustojen suorituskyvyn kehittyminen Mooren lain mukaisesti vaikuttaa käytettävissä olevien salausteknologioiden luotettavuuteen. Esimerkiksi 1980- tai 1990-luvulla kuviteltu avaimen pituus ei ole enää turvallinen, koska käytettävät teknologiat ovat kehittyneet ja sitä myötä avainten auki purkamiseen kuluva aika on oleellisesti lyhentynyt. Myös pilviteknologia tuo uusia ja helpommin saatavilla olevia hyökkäystapoja esimerkiksi salasanojen murtamiseen. Mitä kriittisemmästä ja pitkäaikaisemmasta säilytyksestä on kyse, sitä tärkeämpää on huolehtia käytettävien avainten pituudesta siten, että ne turvaavat tiedot koko niiden salassapidolta edellytettävän ajan. Lisätietoa tiedon salaamisesta viranomaiskäytössä antaa kyberturvallisuuskeskus (ncsa@viestintavirasto.fi).

Tietoturvallisuusasetus toi mukanaan salausvaatimuksen

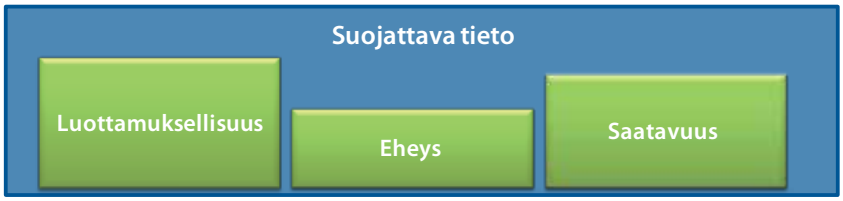
Valtaosa julkishallinnossa käsiteltävästä tiedosta on julkista. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) säätää valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvavaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua 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 (mm. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010 ja Sisäverkko-ohje, VAHTI 3/2010) ei ole kuitenkaan määritetty, miten tiedot pitää salata.

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

1.2 Salaus osana tietoturvallisuuden kolmijakoa

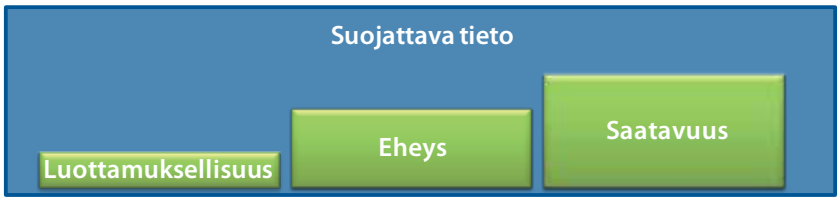
Tietoturvallisuudessa korostetaan usein sen ensimmäisen osa-alueen, luottamuksellisuuden, turvaamista samalla kun eheyttä ja saatavuutta pidetään enemmänkin vakioina.

Kuvio 1. Luottamuksellisuus, eheys ja saatavuus; tietoturvallisuuden osa-alueiden merkitys vaihtelee suojattavan kohteen mukaan.



Ne eivät kuitenkaan koskaan ole vakioita, vaan ne pitää arvioida tapauskohtaisesti. Luottamuksellisuuden arvioimiseen käytetään tietoturvallisuusasetuksessa määritettyä tietoaineistojen luokittelua, joka pohjautuu neljään suojaustasoon (ST IV – ST I). Tiedon eheydelle ja saatavuudelle ei ole olemassa vastaavanlaista määritystä, mutta ne arvioidaan yleensä sen mukaan kuinka kriittisiä tiedot ovat organisaation ydin- tai liiketoiminnalle. Tietojärjestelmissä saatavuus pyritään varmistamaan palvelukohtaisilla palvelutasosopimuksilla (SLA, service level agreement).

Kuvio 2. Julkisen tiedon käsittelyssä korostuvat tietoturvallisuuden kaksi muuta osa-aluetta, tiedon eheyden ja saatavuuden turvaaminen.



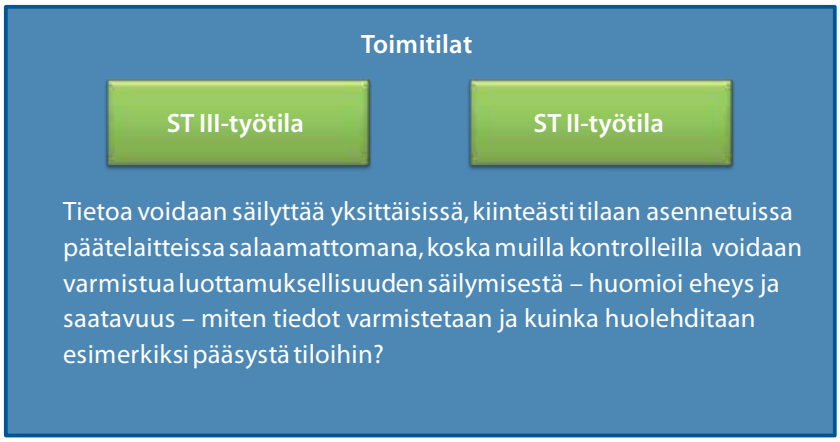
Organisaatiolla voi olla käytössä tietojärjestelmiä, jotka sisältävät salassa pidettävää tietoa mutta jotka eivät ole kovin kriittisiä sen ydin- tai liiketoiminnan kannalta. Toisaalta julkista tietoa sisältävä tietojärjestelmä voi edellyttää, että siinä käsiteltävä tieto ei saa hallitsemattomasti muuttua tai sen saatavuus pitää olla erittäin korkea (esim. 99,999%).

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

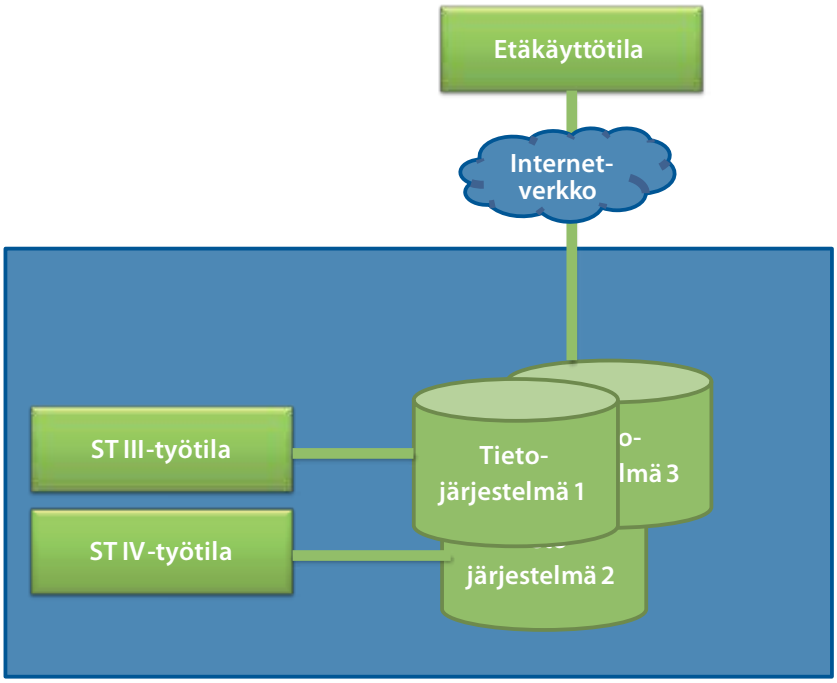
Tietojen salaustarve riippuu siitä, miten ja millaisissa tietojärjestelmissä salassa pidettävää tietoa käsitellään. Jopa suojaustasojen I ja II tietoa voidaan säilyttää tietojenkäsittelyympäristössä salaamattomana, mikäli tiedot sijaitsevat verkoista irrotetussa työasemassa, johon pääsy on rajattu sekä tilaturvallisuuden että työaseman käyttöoikeuksien keinoin.

Toisaalta, salaamista edellytetään aina silloin kun salassa pidettävää tietoa käytetään suojaamattomien tietoverkkojen yli esimerkiksi internetin kautta. Internetissä työskenneltäessä päätelaitteen, käytettävien palveluiden ja tietoaineistojen turvallisuus toteutuu vain silloin kun tiedon salaus on toteutettu kaikissa käsittelyvaiheissa.

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



Kuvio 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 tietojen eheys on perusedellytys myös koko yhteiskunnan toiminnalle. Eheyden turvaamisessa tulee huomata, että pelkkä tiedon salaaminen ei välttämättä riitä; myös salattua tietoa voi olla mahdollista muuttaa ja siten vaikuttaa tiedon eheyteen.

Myös tiedon saatavuuden merkitys vaihtelee tapauskohtaisesti. 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.

Jatkossa valtionhallinnon perustietotekniikkapalveluiden tuottaminen keskittyy Valtion tieto- ja viestintätekniikkakeskus Valtoriin, jonka tulee ottaa huomioon tässä ohjeessa kuvatut toimenpiteet tuottamissaan ja kehittämissään palveluissa sekä palvelutuotannossaan. Kullekin valtionhallinnon organisaatiolle jää vastuu ohjeen noudattamisesta omissa substanssi-, ydin- tai liiketoimintaan liittyvissä järjestelmissä. Vastuu vaatimusten toteut-

tamisesta säilyy toiminnasta vastaavalla organisaatiolla, jolloin sen tulee huolehtia salauksen vaatimustenmukaisuudesta, vaikka se olisi ulkoistanut palvelun tuottamisen valtionhallinnon organisaatiolle tai kaupalliselle toimittajalle.

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

Lisätietoa kyberturvallisuuskeskuksen salaustuotteiden hyväksyntäprosessista löytyy asiakirjasta ”Viestintäviraston suorittamat salaustuotearvioinnit ja hyväksynnät”. Ajantasainen linkki asiakirjaan löytyy tämän ohjeen www.sivulta www.vahtiohje.fi.

1.3 Ohjeen tavoite

Tämän ohjeen tavoitteena on:

- kertoa tiedon salauksesta yleisellä tasolla siten, että lukija saa käsityksen myös aihekokonaisuuteen liittyvistä haasteista ja salauksen tulevaisuudennäkymistä
- ohjeistaa, kuinka salaus tulisi ottaa huomioon organisaatioiden eri toiminnoissa
- antaa ohjeita ja tietoa siitä, miten ja mistä salaukseen liittyvää lisätietoa on saatavilla
- päivitettävien, verkossa sijaitsevien liitetiedostojen avulla määrittää valtionhallinnossa käytettäviä teknisiä salaukseen liittyviä vaatimuksia

1.4 Ohjeen kohderyhmä

Tämä ohje on tarkoitettu organisaatiossa kaikille niille tahoille, joiden tehtävänä on vastata organisaation

- ICT-arkkitehtuurista
- ICT-palveluista
- järjestelmien suunnittelusta ja kehittämisestä
- järjestelmien operatiivisesta palvelutuotannosta
- tietoturvallisuudesta

Ohje ei ole tarkoitettu sellaisenaan jaettavaksi organisaation henkilöstölle. Ohje tulee ottaa huomioon suunniteltaessa ja kehitettäessä tietojärjestelmiä tai muita tiedon salausta edellyttäviä kohteita.

1.5 Ohjeen rakenne

Tämä ohje jakautuu kuuteen lukuun ja kahteen (2) liitteeseen. Lukujen keskeinen sisältö on seuraava:

1. Tausta ja tavoite; kertoo mikä on salauksen merkitys osana tietojen luottamuksellisuuden takaamista, joka on yksi kolmesta tietoturvallisuuden kulmakivestä
2. Tiivistelmä – tarkistuslistat; kuvaa salauksen näkökulmasta tärkeimmät asiat organisaatiolle ja henkilöstölle sekä sisältää huoneentaulut em. ryhmille
3. Tietoturvallisuusasetus, tietoturvatasot ja muut viitekehykset; listaa keskeisimmät aihepiiriin liittyvät valtionhallinnon viitekehykset sekä 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 työskentelevän henkilön tulisi hallita
5. Avaintenhallinta; keskeinen osa-alue, koska jopa hyvin toteutettu salauskokonaisuus 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

Tähän lukuun on koottu 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 esimerkinomaisesti niitä asioita, joista organisaation tulisi henkilöstölle tiedottaa.

2.1 Huoneentaulu – organisaatio

1. Luokittele tiedot oikeaoppisesti! Tietoaineistojen oikeaoppinen luokittelu; mikäli luokittelu tehdään väärin tai tarpeettoman laajasti tietojärjestelmän eri ympäristöihin (esim. kehitys-, testiympäristöt tai muut tietojärjestelmän osat), se aiheuttaa joko ylimääräisiä kustannuksia (yliluokiteltu) tai vaarantaa salassa pidettävän tiedon luottamuksellisuuden (aliluokittelu).
2. Salaa tarpeen mukaan! Tarve-analyysi; kartoittakaa mihin tietojen salausta tarvitaan ja mitkä ovat ne vaatimukset, joihin tiedon salaaminen perustuu.
3. Ole erityisen huolellinen kansainvälisiä salassa pidettävien tietojen käsittelyä suunniteltaessa ja toteutettaessa! Kansainvälisten salassa pidettävien tietojen käsittelyvaatimukset poikkeavat vastaavista kansallisista vaatimuksista.
4. Määritä tarpeet ja vaatimukset! Käytettävien salaustuotteiden määrittely ja valinta; usein toteutuksia tai palveluita hankittaessa todetaan riittäväksi, että siinä on jokin salaus. Tässä ohjeessa pyritään tuomaan esille se, että on olemassa myös salauksia, joita ei ole aina toteutettu huolellisesti ja vaatimusten mukaisesti.
5. Ota tuote käyttöön oikeaoppisesti! Salaustuote sellaisenaan ei riitä, vaan tulee myös selvittää tuotteen kyseiseen käyttötarkoitukseen soveltuvat ominaisuudet, asetukset ja konfiguraatio (esim. että vahingossa ei sallita käyttöön vanhentuneita tai heikommin turvattuja ominaisuuksia, protokollia tai vastaavia asetuksia tai toimintoja).
6. Suunnittele avaintenhallinta! Vaikka salaus olisi muuten toteutettu huolellisesti ja oikeaoppisesti, kaikki vaatimukset huomioiden ja täyttäen, ratkaisu voidaan pilata puutteellisesti suunnitellulla avaintenhallinnalla.

7. Toteuta avaintenhallinta suunnitelman mukaisesti! Vaikka kaikki olisi suunniteltu huolellisesti, erityisesti avaintenhallinnan osalta pitää esimerkiksi auditointien ja tarkastusten avulla varmistua siitä, että suunnitelmat on myös toteutettu sovitulla tavalla ja vaatimustenmukaisesti.
8. Hallitse varmenteita! Salausjärjestelmiin liittyy yleensä varmenteita, joilla on voimassaoloaika. Organisaatioiden tulee huolehtia varmenteiden uusimisesta hyvissä ajoin ennen niiden vanhenemista. Tämä pitää vastuuttaa ja keskittää siten, että käytettävistä varmenteista on olemassa ajantasainen tieto ja prosessi niiden hallitsemiseksi.
9. Salaa kiintolevyt! Organisaation on syytä salata kaikkien työasemien kovalevyt. Internetistä löytyy helposti lukuisia helppokäyttöisiä ohjeita, joiden avulla voidaan päästä kiinni salaamattoman työaseman tietoihin. Hyvä kiintolevyn salaustuote pienentää tätä riskiä.
10. Muista auditoida! 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 auditoinnit toteutetaan. Käytännössä suunnitelma voi olla esimerkiksi osa palvelun tietoturvallisuuden vuosikelloa.
11. Toteuta monikerroksinen suojausratkaisu! Salaus on vain yksi osa organisaation monikerroksista suojautumista. Se ei yksinään riitä, mutta se on tärkeä osa ns. sipulimaisessa tietoturva-arkkitehtuurissa. Monikerroksisen rakenteen avulla varaudutaan siihen, että yksittäisen osa-alueen pettäessä tai murtautujan päästessä yhdestä kerroksesta läpi, seuraavat kerrokset suojaavat edelleen tietoa.
12. Muista vastuut! Omistajan vastuu; organisaatio on aina itse vastuussa omistamistaan tiedoista ja käytössään olevista tietojärjestelmistä, vaikka niiden toteuttamisesta vastaisi jokin ulkopuolinen taho, joko valtionhallinnon organisaatio tai kaupallinen toimittaja. Vastuuta ei ole mahdollista ulkoistaa.

2.2 Huoneentaulu – käyttäjä

1. Opettele luokittelemaan tiedot oikein! 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. Käytä salassa pidettävän tietojen käsittelyyn niitä varten tarkoitettuja ohjelmia ja palveluita! Henkilöstön tulee käyttää määrättyjä työvälineitä ohjeistetulla tavalla, mukaan luettuna tiedon salausratkaisut sähköpostin käsittelyssä, päätelaitteiden käytössä sekä tiedon kuljettamisessa ulkoisilla apumuisteilla (usb- ja muut muistit). Nämä tulee huomioida toimittaessa työpaikalla, työmatkalla tai etätöissä.

3. Toimimme vaatimustenmukaisesti! Valtionhallintoon kohdistuu usein tiukemmat turvallisuusvaatimukset kuin yksityisiin yrityksiin. Tämän takia tulee huomata, että kaikkia yksityisellä puolella käytössä olevia palveluita tai toimintatapoja ei ole välttämättä mahdollista käyttää valtionhallinnossa, johtuen esimerkiksi tietojen salassapitoon tai salaukseen liittyvistä vaatimuksista.
4. Noudata annettuja ohjeita! Vaikka digitalisoimme toimintojamme kiihtyvällä tahdilla, tietoaineistoja käsitellään jatkossakin usein tavoin, jotka eivät kaikki ole sähköisiä. Esimerkiksi keskusteluissa tai paperimuotoisissa aineistoissa tietojen salaaminen ei ole mahdollista samalla tavoin kuin tietojärjestelmissä tai tietoliikenteessä. Tietojen käsittelyssä on noudatettava organisaation antamia ohjeita turvallisesta työskentelystä.
5. Ole aktiivinen, ilmoita poikkeamista! 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, tulee ottaa yhteyttä joko palvelua tuottavan tai oman organisaation palvelupisteeseen ja pyytää korjaamaan asia tai muuten selvittämään sitä.

Henkilöstön tulee kaikissa turvallisuuteen liittyvissä epäselvissä tai epäilyttävissä tilanteissa toimia organisaation ohjeistuksen mukaan, yleensä ottaa yhteyttä 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 talletamiseen 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§, joka koskee 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 parametreista ja teknisistä ominaisuuksista että salausavaimen pituudesta. JulkL:ssa säädettyjä salassa pidettäviä tietoja koskevat lisäksi erityissäädökset, jotka luokittelevat myös salaustoteutukset suojaustasojen mukaisiin luokkiin. Tällöin puhutaan suojaustason mukaisesta salauksesta, esimerkiksi ”ST II -tason mukainen salaus”, tai lyhyemmin ”ST II -salaus”.

”Muutoin suojaaminen” tarkoittaa muuten kuin salaamalla tapahtuvaa suojausta, joka voidaan toteuttaa yhdellä tai useammalla tavalla 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 kohde sijaitsee jossain muualla kuin kaikista tietoliikenneverkoista irrotetulla työasemalla. Käyttötapauksesta riippuen salausta voidaan tarvita myös tietoliikenneverkoissa.

3.2 VAHTI 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta

Salauksen käyttötarvetta eri tilanteissa on ohjeistettu VAHTI 2/2010 -ohjeessa (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta). Vaatimuksia on käsitelty

- Luvussa 8.1 Perusvaatimuksia - sivu 64
- Liitteen 3 kohdassa 5.2 Tietopalvelujen - sivu 80
- Liitteen 3 kohdassa 6 Tietoaineistojen siirto - sivu 89

- Liitteen 3 kohdassa 8 Tietoaineistojen säilytys ja tallennus - sivu 91
- Liitteen 3 kappaleessa 9 Pääsy tietoon (tiedon käyttö) - sivu 92

3.3 VAHTI 3/2010 sisäverkko-ohje

Salauksen käyttöä eri tilanteissa on ohjeistettu myös VAHTI 3/2010 Sisäverkko-ohjeessa. Sen luvussa 12.2 on esitetty vaatimuksia muun muassa kansallisen ja kansainvälisen turvallisuusluokitellun tiedon siirrolle.

3.4 Laki kansainvälisistä tietoturvallisuusvelvoitteista

Kansainvälisiä tietoturvallisuusvelvoitteita koskevassa laissa (588/2004) säädetään viranomaisten velvoitteista 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 käytetyn salaustuotteen tulee lisäksi olla kansallisen viranomaisen (CAA, Crypto Approval Authority, Suomessa Viestintäviraston NCSA-toiminto) hyväksymä.

Lista Viestintäviraston NCSA-toiminnon hyväksymistä salausratkaisuista asiakirjaan löytyy asiakirjasta ”Viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut”. Ajantasainen linkki asiakirjaan löytyy tämän ohjeen www-sivulta www.vahtiohje.fi.

Ohjeena on ottaa yhteyttä Kyberturvallisuuskeskukseen osoitteeseen ncsa@viestintavirasto.fi lisätietojen saamiseksi.

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 itsessään aseta vaatimuksia tietoturvallisuudelle, vaan siihen kootut kriteerit 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 val-

tionhallinnossa (681/2010). Kansainvälisenä lähteenä on käytetty ensisijaisesti EU:n neuvoston turvallisuussääntöjä (2013/488/EU). Katakri on koottu niin, että kriteereistä 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

Salaaminen on yksi keskeinen tiedon suojaamisen keino. Salaamisella tavoitellaan tiedon luottamuksellisuutta; sitä, että ulkopuoliset tahot eivät pysty lukemaan tietoa. Se on kuitenkin vain yksi salauksen tavoitteista. Muita usein tavoiteltuja asioita ovat tiedon eheys ja autenttisuus. Eheydellä tarkoitetaan tässä ohjeessa sitä, että kaikki tietoon tehtävät muutokset ovat havaittavissa. 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 esimerkiksi sähköiset allekirjoitukset, jotka eivät itsessään salaa tietoa. Eheyden varmistamiseen voidaan käyttää muun muassa tiivistefunktioita. Tiedon saatavuutta ei sen sijaan voida taata suoraan kryptologisilla menetelmillä.

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

Kryptografiassa luottamuksellisuuden suojaamisessa käytetään pääasiassa datan muuntamista salatuksi dataksi käyttäen salausavaimia. Sillä ei voi suoraan turvata datan merkitykseen (siis varsinaiseen informaatioon) liittyviä ominaisuuksia, kuten esimerkiksi tiedon paikkansapitävyyttä tai sisäistä eheyttä. Jos merkitykseen liittyvät ominaisuudet on määritelty riittävän tarkasti, kryptografialla voidaan joissain tapauksissa turvata kokonaisuuden osia. Esimerkkinä voidaan mainita digitaalisen allekirjoituksen yhdistäminen lakitekniseen kiistämättömyyden käsitteeseen.

Lisäksi kryptografia tarjoaa vain työkaluja, ei aktiivista valvontaa. Esimerkiksi dataan tehdyt muutokset voidaan havaita vain, jos eheystarkisteisiin ja niiden ilmaisemiin muutoksiin reagoidaan. Kryptografian avulla näitä muutoksia ei kuitenkaan voida estää.

Kryptografiaa käytetään moneen eri tarkoitukseen kuten tiedon salaamiseen, eheyden varmistamiseen sekä pääsynhallintaan. Sitä käytetään OSI-mallin useilla tasoilla: esimerkiksi viestiliikenteessä tietoa voidaan suojata erikseen linkkikerroksella (kuten WPA), siirtokerroksella (kuten IPSec) ja sovelluskerroksella (kuten PGP). Salausratkaisua valittaessa on tärkeää tunnistaa se taso, jolle suojausta etsitään.

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, epäsymmetrisissä avainparia, jonka toinen avain on yksityinen ja toinen julkinen.

Menetelmän turvallisuus riippuu vahvasti käytettyjen avaimien pituudesta, jolla tarkoitetaan niiden esittämiseen tarvittavien bittien lukumäärää. Eri menetelmien avainpituuksia ei voi suoraan käyttää 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 salauksen purkamiseen. Ne toimivat usein monta kertaa nopeammin kuin epäsymmetriset. Siksi niitä käytetään tyypillisesti suurten 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. Avaimen pitää myös pysyä ainoastaan näiden tahojen tiedossa, sillä sen paljastuminen tarkoittaa kaikkien sillä salattujen viestien paljastumista. Avaintenhallinta-luvussa on kuvattu tarkemmin avainten muodostamisessa ja käsittelyssä huomioitavia seikkoja.

4.2.2 Epäsymmetrinen salaus

Epäsymmetriset salausmenetelmät käyttävät tiedon salaamiseen ja purkamiseen eri avainta. Ne muodostavat avainparin; salaamiseen käytetty avain on julkinen ja purkamiseen käytetty avain ainoastaan viestin vastaanottajan tiedossa. Kuka tahansa voi lähettää salatun viestin epäsymmetrisen avainparin omistajalle käyttäen hänen julkista avaintaan. Sen voi purkaa ainoastaan viestin vastaanottajan yksityisellä avaimella. Avainparin avaimet muodostetaan samalla kertaa, 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, esimerkiksi 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 olla myös alttiimpia tietyille hyökkäystyypeille, kuten sivukanavahyökkäyksille. Huolellisella toteutuksella ja tarkoin mietityllä käyttöpolitiikalla voidaan kuitenkin pienentää hyökkäysten muodostamaa uhkaa. Epäsymmetrisissä menetelmissä myös käytetään tyypillisesti pidempiä avaimia, jotta saavutettaisiin sama turvallisuustaso kuin symmetrisissä menetelmissä.

4.2.3 Symmetristen ja epäsymmetristen menetelmien yhteiskäyttö

Useat salausjärjestelmät hyödyntävät sekä symmetristä että epäsymmetristä menetelmää tiedon salaamisessa. Esimerkiksi hybridisalauksissa käytetään epäsymmetristä menetelmää salaamaan symmetrisessä menetelmässä käytetty avain: yksi viestinnän kahdesta osapuolesta muodostaa aluksi symmetrisen avaimen, salaa sen toisen osapuolen julkisella avaimella ja lähettää sen hänelle. Tämän jälkeen osapuolet voivat käyttää symmetristä avainta keskinäisen viestinnän salaamiseen. Näin saadaan hyödynnettyä symmetristen ja epäsymmetristen menetelmien vahvuuksia.

Symmetrisen menetelmän avaimen sopimista kutsutaan avaintenvaihdoksi. Sen tekemiseen on useita tapoja, joita käsitellään 5. Avaintenhallinta-luvussa.

4.3 Tiedon eheyden varmistaminen

Tiedon eheys voidaan varmistaa esimerkiksi kryptografisen tiivisteen avulla. Se on lyhyt, käsiteltävästä tiedosta muodostettu bittijono, joka lasketaan tiivistefunktion avulla. Eheyden varmistamisen lisäksi tiivisteitä voidaan käyttää myös tiedon autentikoinnissa.

Tiivistefunktioilta vaaditaan seuraavia ominaisuuksia:

- Tulisi olla vaivatonta laskea tiiviste mistä tahansa viestistä.
- Pelkästään tiivisteen perusteella ei tulisi olla mahdollista selvittää viestiä, josta se 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.

Tiivisteen avulla voidaan tarkistaa viestin eheys. Jos viestiä muutetaan, niin siitä lasketun tiivisteen tulee muuttua. 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. Tietyissä käyttötapauksissa tiivisteen laskemisessa on tarpeellista käyttää suolaa, joka tarkoittaa syötteen yhteyteen lisättävää satunnaista dataa. Näin tehdään esimerkiksi salasanatiivisteissä, joita käsitellään luvussa 6.7.9 Salasanojen tallentaminen tietojärjestelmissä.

Tiivistefunktioilla ja muilla samankaltaisilla funktioilla on myös muita käyttötarkoituksia esimerkiksi salasanalla tapahtuvassa autentikoinnissa, jota on kuvattu myös luvussa 6.7.9.

4.4 Tiedon autentikointi

Tiedon autentikointiin eli sen 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 muodostaa käyttäen yksityistä avaintaan. 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 voi 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.

Samaa tekniikkaa voidaan hyödyntää tietojärjestelmissä asiakirjan sähköisen allekirjoituksen toteuttamiseen. Tällöin asiakirjasta lasketaan tiiviste-bittijono ja asiakirjan laatija vahvistaa sen yksityisellä avaimellaan sähköisesti allekirjoittaen.

4.5 Suosituksia

Luottamuksellisuuden, eheyden ja autenttisuuden takaamiseksi on olemassa useita standardoituja menetelmiä. On suositeltavaa valita kryptografiset menetelmät standardoitujen menetelmien joukosta, joiden turvallisuutta on tutkittu laajasti. Valinnan yhteydessä tulee valita myös 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 salausratkaisuja 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 seuraavassa luvussa. Menetelmien parametrien vaikutus protokollan kokonaisturvallisuustasoon on kuvattu tarkemmin liitteessä 1.

Kryptografisten tuotteiden turvallisuuden arviointia varten on laadittu kriteeristöjä, joissa määritellään vaatimuksia tuotteissa käytettäville menetelmille ja toteutuksille eri turvallisuustasoilla. Esimerkki näistä 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 joita voi käyttää viitemateriaalina. Kriteeristöjen mukaan hyväksyttyjen tuotteiden käytössä on huomioitava, että ne koskevat tiettyjä versioita laitteistojen ja ohjelmistojen muodostamasta kokonaisuudesta. Jonkin osuuden version muuttuessa hyväksyntä ei siis välttämättä ole enää voimassa.

4.6 Tietoliikenneprotokollat

Edellä kuvattujen menetelmien yhdistäminen toimivaksi ratkaisuksi vaatii niiden ominaisuuksien tuntemista sekä syvällistä osaamista. On esimerkiksi tiedettävä, mikä osa viestistä on tarpeen autentikoida ja kuinka viestin osat sidotaan toisiinsa niin, ettei niitä voi myöhemmin käyttää ns. ”leikkaa ja liimaa” -tyyppisiin tai toistohyökkäyksiin (engl. replay attack). Erityyppisten 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 laajennukset, jotka parantavat esimerkiksi yhteyden uudelleen muodostamiseen kuluvaa aikaa tai sallivat erilaisten autentikointimenetelmien käytön. Ne saattavat kuitenkin vaarantaa ratkaisun turvallisuuden, joten siksi niitä ei saa käyttää tarkastamatta. Vaikka protokollissa on yhdistetty tiedon suojaamiseen käytettyjä menetelmiä, tulee niiden parametreihin kiinnittää edelleen huomiota, sillä ne vaihtelevat yhdistelmästä riippuen.

Tietoturvallisuuteen liittyvän protokollan käyttöönotossa tulee huolehtia kyseisen protokollan turvallisista, parhaisiin käytäntöihin perustuvista periaatteista.

4.6.1 Transport Layer Security (TLS)

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

TLS-protokollasta on olemassa useita erilaisia toteutuksia. Turvallisuuden kannalta on oleellista käyttää uusinta versiota valitusta TLS-toteutuksesta. Järjestelmiä suunniteltaessa vahva salaus ei yksinään riitä, vaan on tärkeää valita tarpeeksi vahvat menetelmät myös eheyden ja autentikoinnin varmistamiseen.

TLS-protokollaan on määritelty valmiiksi erilaisia yhdistelmiä salausmenetelmistä ja niiden avainpituuksista. Niiden huolellisella valinnalla yhteys voidaan suojata siten, että sen turvallisuus on taattu. TLS-protokollalla on suojattu yhteydet esimerkiksi moniin tunnistautumista ja salaamista vaativiin palveluihin, kuten verkkokauppoihin ja -pankkeihin.

4.6.2 Internet Protocol Security (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 suojaa sovellusten välisiä yhteyksiä ja toimii sovellustasolla. 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. VPN-ratkaisua kuvataan tarkemmin luvussa 6.7.3.

4.7 Tulevaisuuden näkymiä

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

Salaustekniikoiden politisoituminen. Salaustekniikat ovat aina näytelleet tärkeää roolia politiikassa, esim. valtion ylimmän johdon viestien turvaamisessa ja sotilastiedustelussa. Internetin laajentumisen ja pilvilaskennan myötä tietoisuus salausteknologioista on levinnyt yhä enemmän myös suurelle yleisölle. Yleinen reagointi esimerkiksi paljastuksiin suurten tiedusteluorganisaatioiden massavalvonnasta[1] osoittaa, että valtiotason tiedustelulle on olemassa yksityisyyden suojaa kannattava vastavoima. Tällä on pienten valtioiden

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

kannalta se hyvä puoli, että salainten heikkouksia tuodaan esiin julkisesti kansainvälisellä tasolla, kansallisen viranomaisen kannalta ”ilmaiseksi”. Toisaalta poliittinen keskustelu voi viedä asiaa myös huonompaan suuntaan tekniseltä kannalta, kun keskustelijoiden enemmistö ei tunne asiaa tarkemmin.

Kryptoanalyysi ja kryptografia käyvät jatkuvaa kilpajuoksua keskenään. Viime vuosina on kuitenkin ollut huomattavissa se, että edes tiedusteluorganisaatiot eivät ilmeisesti enää pysty 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 (engl. tamperproof) piirit ovat yksittäisiä teknologioita, joilla toteutuksia vastaan tehtäviä hyökkäyksiä pyritään estämään.

Tämän hetken tunnetuimmista algoritmeista RSA:n julkisen avaimen menetelmän käyttö on vähenemässä, ja korvaajaksi on tulossa järjestelmien päivitysten myötä elliptisten käyrien kryptografia. Merkittävällä osuudella odotetaan myös nk. ”kvanttiturvallisten” algoritmien, kuten NTRU:n[2] esiinmarssia.

Muista algoritmityypeistä AES[3] puolustaa edelleen vakaasti paikkaansa hyvänä lohkosalaimena. Verrattuna esim. DES:in[4] yli kaksikymmenvuotiseen taipaleeseen, AES on arviolta matkansa puolivälissä. Mikäli lohkosalaimille ei esitetä täysin uusia analyysityyppejä tai perinteisten analyysimenetelmien laajennukset eivät tarjoa suuria yllätyksiä, AES ehtii vanhenemaan elinkaarensa loppuun asti rauhassa.

Tiivistefunktiot, kuten MD5 ja SHA-1, 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, järjestettiin viisivuotinen kilpailu NIST:in seuraavaksi tiivistestandardiksi (versio SHA-3). Sen käyttöönotto kestää kuitenkin suunniteltua pidempään johtuen pääasiassa standardoinnin hitaudesta ja SHA-2:n oletettua kestävämmästä rakenteesta.[5] SHA-2 on todennäköisesti eräs lähitulevaisuuden eniten käytetyistä tiivistefunktioista, kunhan SHA-1 poistetaan tuotteista vaiheittain.

Laskentateho on kryptoanalyysin peruskiviä, mutta jo nyt ollaan perinteisen laskennan osalta niin pitkissä avaintenpituuksissa (esim. 192 bittiä), että ideaalitapauksissakin kaikkien avainten läpikäynti vaatisi kaiken auringon tuottaman energian valjastamisen n. 16000 vuodeksi[6]. Laskentatehon lisääminen ei siis ole hyökkääjän näkökulmasta kannattavaa kuin tiettyyn rajaan asti. Myös kvanttilaskennassa tunnetaan kvanttialgoritmien kello-

---

2 NTRU, joidenkin lähteiden mukaan johdettu suunnittelijoidensa ryhmän nimestä (”Number Theory Research Unit”), on nk. hilaongelmiin perustuva julkisen avaimen salausmenetelmä.

3 AES, Advanced Encryption Standard, USA:n NIST-standardointiorganisaation lohkosalainstandardi

4 DES, Data Encryption Standard, AES:n edeltäjä

5 On myös esitetty epäilyjä NISTin Keccakiin (kisan voittaja-algoritmi) tekemien muutosten turvallisuudesta.

6 Landauerin periaatteen (R. Landauer: “Irreversibility and heat generation in the computing process”, IBM Journal of Research and Development 5, p.183-191, 1961) mukaiset laskelmat sovellettuna auringon ytimen energiantuottoon (NASA: “Sun Fact Sheet”, http://nssdc.gsfc.nasa.gov/planetary/factsheet/sunfact.html)

taajuudelle[7] luonnontieteellisiä ylärajoja, jotka rajoittavat tunnettujen kvanttialgoritmien käyttöä esimerkiksi lohkosalaimille.

Pilvilaskenta tuo myös kryptoanalyysiin uuden elementin lähinnä laskentatehon saatavuudella. Eräänlaista hajautettua laskentaa Internetiin kytkettyjen koneiden avulla on sinänsä käytetty jo 1990-luvun lopulta yksittäisissä projekteissa, mutta pilvilaskenta tuo yleiskäyttöisen laskennan yhä useampien ulottuville. Kryptoanalyyttisten algoritmien erikoisominaisuuksien vuoksi pilvilaskenta ei todennäköisesti tuo uusia uhkavektoreita yleisesti tunnettuihin algoritmeihin ja toteutuksiin (koska suhteellisen monella taholla on kuitenkin kykyä ja resursseja tuottaa spesifistä laitteistoa, jossa laskennan kustannustehokkuus juuri yhteen tiettyyn ongelmaan on eri kertaluokkaa kuin pilvilaskennassa). Erilaisiin pistemäisiin sovelluksiin pilvilaskenta tulee kuitenkin tarjoamaan uusia mahdollisuuksia, ja esimerkiksi salasananmurskaus ad-hoc-tarpeeseen on kustannustehokkaampaa pilvilaskennalla kuin erityislaitteistolla.

Salausteknologian sijainti on perinteisesti ollut salauslaitteissa tietoturvan hallinnollisen alueen rajalla (security perimeter). Yleisenä trendinä on, että nämä rajat lähenevät kohti tietosisältöä, muuttuen samalla monimutkaisemmiksi pilvilaskennan ja ”Internet of Things”-ajattelun (”esineiden internet”) myötä. 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 avoimen / suljetun lähdekoodin OpenSource/Closed-source -akselilla ei tule jatkossa olemaan niin suoraviivaista kuin tähän asti. Salaustoteutusten ylläpitäminen vaatii jatkuvaa kehitystyötä ja haavoittuvuuksien hallintaprosesseja, mihin avoimen lähdekoodin puolella ei välttämättä ole varaa. Esimerkkejä siitä, mitä pahimmillaan voi käydä, jos avoimen lähdekoodin tuotteiden ylläpitoon ei ole riittäviä resursseja, on jo olemassa.[8,9] Toisaalta suljetun lähdekoodin puolella tapahtuu tapahtuu avautumista erityisesti hyväksyntäviranomaisten suuntaan.

Salausteknologioiden käyttötavat laajenevat kryptografisten menetelmien yleistyessä 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 kauppatapahtumia (transaktioita) saaden palkkioksi lisää kryptovaluuttaa. Varmentaminen vaikeutuu

---

7 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.

8 Nk. Heartbleed (http://heartbleed.com; http://en.wikipedia.com/wiki/Heartbleed) paljasti huhtikuussa 2014 haavoittuvuuden OpenSSL-salauskirjastossa (OpenSource), joka johti TLS-protokollan väärinkäyttömahdollisuuteen, ja esim. yksityisten avainten paljastumiseen palvelinten muistiavaruudesta. Syyksi esitettiin ylläpitäjien resurssien puutetta suorittaa vaadittuja auditointeja ja testauksia eri versioille.

9 Truecrypt-salaustuotteelta (OpenSource) lopetettiin äkkinäisesti tuki 28.5.2014. Syitä spekuloitiin, ja näistä yhtenä mainittiin kehittäjien kiinnostuksen loppuminen (http://www.darkreading.com/endpoint/the-mystery-of-the-truecrypt-encryption-software-shutdown-/d/d-id/1269323). Huhut Truecryptissä olleista mahdollisista aukoista vähenivät 2.4.2015 julkaistun toiseen vaiheen auditoinnin jälkeen, joka ei löytänyt tahallisia takaportteja Truecryptin lähdekoodista. Truecryptin rinnakkaisversioita (CipherShed, VeraCrypt) kehitetään myös edelleen.

sitä mukaa kuin kokonaislaskentatehoa on olemassa ja valuuttaa on tuotettu. Näitä valuuttoja ei voi hallita keskitetysti, eikä niihin sellaisenaan liity tekijöitä, joiden avulla valuutan omistajan tai käyttäjän voisi jäljittää. Valtiot eivät vielä tue kryptovaluuttoja, mutta joillekin niistä on jo olemassa vaihtokursseja ja jopa vaihtopörssejä. Koska kryptovaluutat ovat suureksi osaksi anonyymejä, myös rikollinen maailma hyödyntää 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[10]. Kyseessä on voimistuva ilmiö, johon valtioiden ja rahoituslaitosten on otettava voimakkaasti kantaa vähintään keskipitkällä aikavälillä.

Kryptografia on nykyisin yleisessä käytössä myös haittaohjelmissa, erityisesti tunnistepohjaisten järjestelmien harhauttamisessa sekä varastetun datan siirtämisessä kohteesta hyökkääjälle. Jälkimmäisessä tapauksessa myös steganografia (datan piilottaminen muun datan sekaan) on kokenut uuden tulemisen kryptografisten tekniikoiden ansiosta. Tämä trendi voi viimein pakottaa uusien valvontatekniikoiden käyttöönottoon ja oppivien tilannekuvajärjestelmien yleistymiseen.

Kvanttilaskenta on teknologia, jolla on laajamittaisesti toteutuessaan merkittävä vaikutus salausalgoritmeihin. Sen suuren laskentatehon seurauksena lähestulkoon kaikki diskreetteihin logaritmeihin ja tekijöihinjakoon perustuvat järjestelmät, kuten RSA, Diffie-Hellman avaintenvaihto ja elliptisten käyrien kryptografia tulisi hylätä, symmetristen salainten avaintenpituudet tulisi kaksinkertaistaa, jne. Kvanttilaskennan laajamittainen tuleminen nimenomaan salaustekniikoita uhkaavana paradigmana näyttää yhä edelleen joko epätodennäköiseltä tai pitkän aikavälin uhalta[11], 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[12] protokolla-/sovellustason haavoittuvuuksien vaikutuksista loppukäyttäjille sekä mahdollisuuksista korvata haavoittuvat osat muilla menetelmillä.

Koska kvanttilaskennalle haavoittuvia menetelmiä käytetään protokollissa pääasiassa vain avaintenvaihtoon, 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 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 jotka ovat muuten turvallisia. Näitä ovat

---

[10] *Laskentateho* on kybertilassa verrattavissa harvinaisiin metalleihin.

[11] Esim. Alankomaiden kvanttiturvallisuusstrategia on asettanut valtion “kvanttiturvallisuudelle” tavoitteeksi 2020, ja perustelee tätä laajamittaisen kvanttilaskennan toteutumisella 2030 mennessä. Myös USAn salausturvallisuusviranomainen, NSA, on elokuussa 2015 muuttanut salaussuosituksiaan ilmoituksen mukaan kvanttilaskennan aiheuttaman uhan vuoksi (https://www.nsa.gov/ia/programs/suiteb_cryptography/)

[12] (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

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, se on varteenotettava vaihtoehto avaintenvaihtoon – mikäli etsitään juuri kvanttiturvallisia toteutuksia.

Seuraavan sukupolven julkisen avaimen järjestelmät ovat siirtyneet akateemisesta tutkimuksesta jo teollisuuden tutkimus- ja tuotekehitysosastoille. Nämä funktionaalisina salaustekniikoina (FE) tunnetut menetelmät[13] perustuvat siihen, että julkinen avain voidaan luoda ennen yksityistä avainta mielivaltaiseksi, ja palastella se tarvittaessa attribuuteiksi. FE-tekniikat tuovat mukanaan suuria odotuksia, kuten kevyemmän julkisen avaimen arkkitehtuurin, turvallisen ja järkevän pilvisalauksen, aidosti toimivia IPR-ratkaisuja[14], secure boot-mekanismeja sekä sovellusten autentikoinnin (ajettavalla sovelluksella voi olla sen toimintaan perustuva digitaalinen allekirjoitus, ja olisi mahdollista varmentaa, käyttäytyikö sovellus kuten sen piti riippumatta ajoalustaan asennetuista mahdollisista tietoturva-aukoista). Valtionhallinnossa tulisivat mahdollisiksi nk. monitasotietoturvan ympäristöt (MLS, multi-level security), joissa eritasoiset 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 sisällä.

---

[13] 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.

[14] IPR, Intellectual Property Rights, esim. median sisällöntuottajien tapa salata media kulutettavaksi vain siitä maksaneille tahoille.

5 Avaintenhallinta

Avaintenhallinta on kaikkein kriittisin osa salauksen luotettavuuden takaamisessa. Kryptografian tärkeän 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 salausalgoritmin heikkouden sijaan useammin salausavaimen vuotaminen joko käyttöjärjestelmän, tietoturva-protokollan tai käyttäjän virheen vuoksi.

Avaintenhallinnan asianmukaisen toteutuksen varmistamiseksi sen prosessien ja käytäntöjen tulee olla dokumentoituja. On suositeltavaa laatia 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
- avainten 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 sekä muunkin salausteknisen materiaalin, kuten salauslaitteiden käsittely. Lisätietoa COMSEC-prosessista on Viestintäviraston kansallisen salausteknisen materiaalin käsittelyohjeessa. Seuraavissa kappaleissa avaintenhallintatoimintoja kuvataan 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 voidaan jakaa 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 vaihtoväli on tyypillisesti 3 kk – 1 v. Pitkäaikaiset avaimet voivat olla myös ns. fyysisiä avaimia, jotka kuljetetaan käyttöpaikalle siirrettävällä medialla henkilökohtaisesti tai käyttäen tehtävään hyväksyttyä kuriiria (kuuluu COMSEC-toimintaan). 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 järjestelmissä automaattisesti, jolloin ne salataan tai verifioidaan siirron ajaksi pitkäaikaisella avaimella.

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. Avaimen hyvyys on pääasiassa kunnollisen satunnaislukugeneraattorin ja sen käyttämän entropialähteen varassa. Satunnaisluku ei itsessään riitä avaimeksi, vaan yleensä sitä käytetään syötteenä jollekin avaimenluomismenetelmälle. Sillä varmistetaan, että avaimella on toi-

votut ominaisuudet, kuten tasajakautuneisuus ja tuoreus, ja että se on sopiva käytettyyn salausmenetelmään.

Avaimista sopiminen tai avaintenvaihto tarkoittaa, että avain sovitaan osapuolten välillä yhdistämällä 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 sisältyy mm. IPSec- ja TLS -protokolliin.

5.1.2 Salausavainten tyyppejä ja käyttötarkoituksia

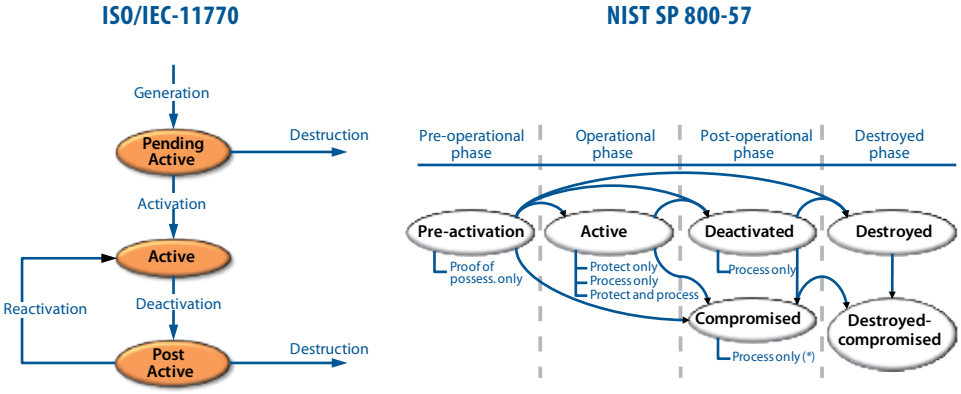
Salausteknisiä avaimia voidaan käyttää myös muihin toimintoihin kuin salaukseen. Yleisesti ottaen on tärkeää olla sekoittamatta tai yhdistämättä mielivaltaisesti eri käyttötarkoituksiin tarkoitettuja avaimia. Yhteen käyttötarkoitukseen tehty avaintenhallintaohjeisto ei välttämättä ole sellaisenaan siirrettävissä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

- Eheyden takaamiseen liittyvät avaimet: yksityiset epäsymmetriset 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 on turvallisempaa käyttää eri avainparia kuin salaamiseen.
- Pääsynhallintaan liittyvät avaimet; erilaiset sertifikaatit sekä sirukorttien ja muiden tokenien sisältämät avaimet. Nämä eivät vaikuta suoraan tiedon luottamuksellisuuteen, mutta ne toimivat lisäkontrollina resurssien suojaamisessa.
- Avaintenhallinnan infrastruktuurin ylläpitoon tarvittavat avaimet; edellä mainitut pitkäaikaiset avaimet, avainten vanhenemisen ja katoamisen varalle muodostetut ”vara-avaimet”, luotetun 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 tuo lisää monimutkaisuutta avaintenhallintaan.

5.2 Avainten elinkaari ja siihen liittyvät toiminnot

Kansainvälisissä avaintenhallinnan standardeissa ja suosituksissa (esim. ISO/IEC-11770[15] ja NIST SP 800-57[16]) avainten elinkaarella on keskeinen rooli. Kuvassa 5 on esimerkkejä näiden standardien mukaisista avainten elinkaarista.

Kuvio 5. Avainten elinkaari eräiden standardointiorganisaatioiden mukaan.



5.3 Avainten jakelu

Avainten jakelulla tarkoitetaan sitä, että luotettu osapuoli luo käytetyn avaimen itsenäisesti 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.

Avainhierarkioiden, infrastruktuurin ja vastaavien 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.

---

15 ISO/IEC 11770, Information Technology – Security Techniques – Key Management Part 1-5 (2006-2011)

16 NIST Special Publication 800-57, Recommendation for Key Management – General (Rev.3), 2012.

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

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

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

5.4 Avainten suojaaminen

Pääperiaate on, että 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 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. Kuten 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, jotka pitää erikseen selvittää ja ottaa huomioon. Järjestelmäkohtai-

set 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 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 käsiteltävä aineisto suojataan useimmiten salasanalla tai fraasilla, jonka käyttäjä näppäilee koneelle. Sähköisten avainten tai niitä suojaavien salasanojen jakelua ei saa koskaan tehdä salaamatta samalla kanavalla, jolla salakielistä tekstiä lähetetään. Jos viestintäkanava on suojaamaton, mahdollinen hyökkääjä pystyy kuuntelemaan 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 tapa päästä 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 voimassaolon 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. 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 luodessa muita avaimia, 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 huomioimatta. 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 kyseisillä 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 yhteydenottotahot sekä toimenpiteet epäiltäessä avainten paljastumista.

Käytöstä poiston jälkeen avaimet on tuhottava luotettavalla menetelmällä. Sähköiset avaimet pyyhitään laitteen muistista käyttäen esimerkiksi tehokkaita ylikirjoitusmenetelmiä.[17]

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

[17] Viestintäviraston ohje "Kiintolevyjen elinkaaren hallinta - Ylikirjoitus ja uusiokäyttö". Linkki ohjeeseen löytyy tämän ohjeen sivulta osoitteesta www.vahtiohje.fi.

6 Salausratkaisun valinta ja käyttöönotto

6.1 Johdanto

Salausratkaisun valintaan ja käyttöönottoon tulee suhtautua samalla tavalla kuin minkä tahansa tietojärjestelmän tai sen komponentin valintaan ja käyttöönottoon. Kuten yleensä tietojärjestelmähankkeissa, ratkaisun korjaaminen tai muuttaminen käyttöönoton jälkeen 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 niiden salaustarpeiden täyttämiseksi.

Salausratkaisut tarjoavat joustavia menetelmiä tietojen luvattoman paljastumisen ja muuntelun estämiseen. Niitä voidaan hyödyntää myös tietojen suojaamiseen esimerkiksi etätyössä. Usein on tarve pystyä siirtämään salassa pidettävää tietoa ei-luotetun verkon yli, jolloin tietoa voidaan suojata salausratkaisulla. Yleensä etätyöhön liittyy tarve myös säilyttää tietoa päätelaitteilla tai muilla muistivälineillä, jolloin salausratkaisulla pystytään tarjoamaan luotettava pääsynhallintamenetelmä tiedolle esimerkiksi laitevarkauksien varalta.

Salausratkaisut myös tukevat ja täydentävät muita tiedon suojausmenetelmiä. Esimerkiksi kiintolevyjen salauksella pystytään pienentämään uhkia myös organisaation fyysisesti suojatun toimitilan sisällä, mahdollistamaan kiintolevyjen ja muiden muistivälineiden laajempi uudelleenkäyttö[18] sekä pienentämään ulkoisia riskejä 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 toteuttamisen. Esimerkiksi tiedon eheyden ja kiistämättömyyden takaavilla menetelmillä pystytään vähentämään paperimuotoisen aineiston käsittelyä sekä edistämään tehokkaampien ja käyttäjäystävällisempien palvelujen käyttöönottoa.

[18] Uudelleenkäyttömahdollisuuksia on kuvattu yksityiskohtaisemmin Viestintäviraston ohjeessa "Kiintolevyjen elinkaaren hallinta - Ylikirjoitus ja uusiokäyttö".

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

Viranomaisten tiedon salausta edellytetään silloin, 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 salassa pidettävää aineistoa kuljetetaan muuten fyysisesti suojattujen alueiden välillä (kiintolevyjen, CD-levyjen, USB-muistien ja vastaavien tietovälineiden salaus), ellei aineisto ole jatkuvasti sitä kuljettavan tahon hallussa/valvonnassa,

c) kun salausta käytetään pääsynhallintamenetelmänä muissa tilanteissa (esimerkiksi vähimpien oikeuksien periaatteiden toteuttaminen tai tarkastusoikeuden varaavien tiedon omistajien tietojen erottelu yhteiskäyttöisissä tietojärjestelmissä),

d) järjestelmään tehdyn riskienarvioinnin pohjalta muissa tilanteissa tai käyttötapauksissa (esimerkiksi osana monikerrossuojausta[19] fyysisesti suojatun alueen sisällä).

Käsiteltäessä vain kansallista salassa pidettävää aineistoa salauksen käyttämiselle ja valitun salauksen vahvuudelle on tietoturva-asetuksessa jätetty riskienhallinnan pohjalta enemmän liikkumavaraa. 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 turvallisuussäännöstön 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.

[19] Engl. Defence in depth.

6.3 Riskianalyysi

Tietoturvallisuus-asetus edellyttää, että tietoturvallisuuden suunnittelu on hyvän tiedonhallintatavan mukaista, tietoturvallisuustoimenpiteet mitoitetaan ottamalla huomioon suojattavien tietojen merkitys ja 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 riskien 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 muun muassa algoritmin matemaattinen kompleksisuus ja ajanmukaiset hyökkäysmenetelmät.

Viestintäviraston johtama kryptologian asiantuntijoista koostuva työryhmä on laatinut CAA-viranomaisen hyväksyntätyötä varten taulukon luotettavista algoritmeista ja kryptografisista vahvuusvaatimuksista, 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.

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 ympäristöissä:

- 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, jota vastaan tietoa suojataan. Fyysinen ympäristö lieventää uhkaa, jos se suojaa tietoa niin, ettei ryhmän ulkopuolinen henkilö tai taho voi mitenkään saada haltuunsa salatussa muodossa olevaa tietoa. Ryhmät luokitellaan henkilöille tehdyn tarpeellisuusperiaatteen ja sen perusteella tehtävän turvallisuusselvityksen perusteella. Korkean uhkan muodostavassa ympäristössä täysin ulkopuoliset, siis henkilöt joilla ei ole turvallisuusselvitystä, voivat saada salatussa muodossa olevan tiedon käsiinsä kryptoanalyysiä (heikkouksien etsimistä) 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 sen turvallisuusluokkaan. Sen sijaan eheyden menetyksen (tiedon alkuperä, kiistämättömyys, muuttamattomuus, jne.) vaikutus ei ole näin suoraviivainen. Sitä voi arvioida erityisesti tiedon tai järjestelmän omistaja. On kuitenkin olemassa järjestelmiä ja tilanteita, joissa tiedon eheys on tärkeämpää kuin sen luottamuksellisuus. Näin on esimerkiksi rahaliikenteessä ja sähköisesti allekirjoitetuissa todistuksissa. Mikäli organisaation tietosisällön eheys on sen toiminnalle kriittistä, on suositeltavaa luokitella tietosisältö myös eheyden mukaan.

6.3.2 Salausajan vaikutus avainpituuksiin ja algoritmeihin

Joissain järjestelmissä voidaan välittää tietoa, jonka salassapitoaika on hyvin lyhyt, esimerkiksi yksi päivä. Silloin ei olisi kohtuullista vaatia salausmenetelmältä vahvuutta, jolla turvataan vuosien salassapitoaika.

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

Salausavainten vaihto tulee toteuttaa salausajan vaatimusten mukaisesti. Sen kuluminen alkaa siitä hetkestä, kun joko epäsymmetrisen avainparin julkinen avain tai symmetrisellä avaimella salattu tieto altistuu hyökkääjälle ensi kertaa, esimerkiksi kun varmenne lähetetään tai kun symmetristä avainta käytetään.

Avaintenpituuksia valittaessa on syytä ottaa huomioon myös aika-muisti-vaihtokauppahyökkäys (time-memory-tradeoff attack) sellaisissa tilanteissa, joissa uhkamalli ei ole täysin tunnettu. Tämä sen takia, että hyökkääjä pystyy mahdollisesti valmistelemaan salauksen murtamista ennakkoon esimerkiksi laskemalla Rainbow- tai Diffie-Hellman-tauluja, joita käyttäen salauksen purkamiseen kuluva aika lyhenee. On jopa esitetty arvioita, joiden mukaan valtiolliset tahot pystyisivät tekemään samalla alkulukuparametrilla muodostetuille 1024-bittisille Diffie-Hellman-avaimille valmistelevia laskutoimituksia, joiden avulla niitä voisi murtaa lähes reaaliajassa. Tällaisesta hyökkäyksestä voi suojautua käyttämällä pidempää avainpituutta tai vaihtuvaa alkulukuparametria.

Perusteet järjestelmän turvalliselta käytöltä saattavat pudota pois nopeasti uusien kryptologisten hyökkäystapojen tai laskentatehon kasvun myötä, ja siksi järjestelmän korvaamiseen tulee varautua. Tilanteen seuraamista ja järjestelmän käytön ohjaamista varten olisi hyvä nimetä vastuuhenkilö, jonka tulisi yleisestikin toimia organisaatiossa vastuuhenkilönä salaukseen liittyvissä asioissa.

Minimissäänkin salausmenetelmän on kestettävä hyökkäyksiä niin, ettei mikään hyökkääjä kykene avaamaan liikennettä ajantasaisesti (on-line). Tätä ehtoa täyttämättömiä salauksia ei pitäisi käyttää lainkaan. Lisäksi on huomioitava 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 vaatimusmäärittelyssä tulee 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 huomioitavan myös salausratkaisun tuen jatkuvuus ja saatavuus. Aina kun salausratkaisua suunnitellaan osaksi kansainvälistä luokiteltua tietoa käsittelevää järjestelmää, suositellaan ennen hankintapäätöksen tekoa olemaan yhteydessä Viestintäviraston NCSA-toimintoon[20] .

6.5 Jatkuva palvelu ja kehittäminen

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

Salausratkaisuista, kuten muistakin ohjelmistoista löytyy ajoittain haavoittuvuuksia. Ratkaisu tulee pitää päivitysten piirissä siten, että käyttötapaukseen liittyvät turvapuutteet

[20] www.viestintavirasto.fi, ncsa@viestintavirasto.fi

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 voimassa oleva hyväksyntä kansalliselta salaustuotteiden hyväksyntäviranomaiselta (CAA, Crypto Approval Authority).

Vastaava tarve voi ilmetä myös kansallista salattavaa 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 silloin kun tietojärjestelmissä on tarkoitus käsitellä suojattavaa tietoa.

Sekä kansainvälisen että kansallisen tiedon suojaamisessa tiedon omistajalla on mahdollisuus hyväksyä omistamansa tiedon suojaus. 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 paikkakunnilla sijaitsevan toimipisteen välillä. Organisaatio on luokitellut tietonsa suojaustasoille IV, III ja II. Järjestelmää on alustavasti hahmoteltu 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 muutamia 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.

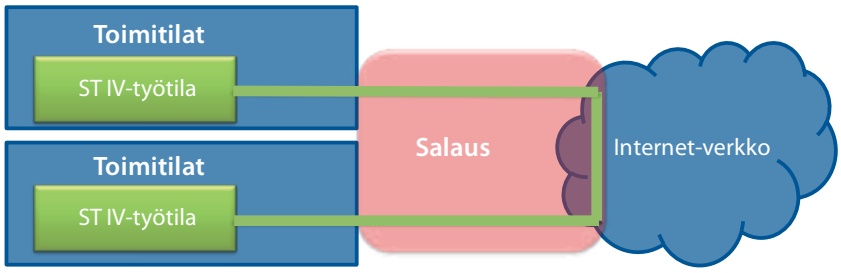
6.7.2 VPN-ratkaisu organisaation kahden toimipisteen välillä

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).

Kuvio 6. Salaus tulee ottaa käyttöön organisaation fyysisesti suojattujen alueiden ulkopuolella, kun sitä käytetään salassa pidettävän tiedon välittämiseen – niin etäyhteydessä kuin



toimitilojen tietoliikenneyhteyksiä toteutettaessa.

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 palvelua esimerkiksi Valtorin tarjoamaa VYVI-turvapostiratkaisua. 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. Salaus on suositeltavaa toteuttaa kaikissa niissä päätelaitteissa (kannettavat tietokoneet, tabletit, älypuhelimet), joissa se riskiperusteisesti pitää toteuttaa ja voidaan kustannustehokkaasti laitteen käytettävyys taaten mahdollistaa.

6.7.7 USB-muistien ja muiden ulkoisten muistien salaus

Organisaatiossa käytetään ”rautasalauksella” automaattisesti kaiken sisältönsä salaavia USB-muisteja. Vaihtoehtoisesti organisaatiossa voidaan käyttää tavallisia USB-muisteja, mutta niille ei saa tallettaa 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 eri omistajien tiedot samalle

fyysiselle levylle omilla avaimillaan salattuina tiedostoina. Toisin sanoen yhteiskäyttöisillä levyillä tarkastusoikeuden varaavien omistajien tietoja säilytetään ainoastaan eri avaimilla salatussa muodossa. Tällöin kukaan tiedon omistaja ei tarkastusoikeuden varjolla pysty saamaan selväkielisessä muodossa muuta kuin omistamaansa tietoa.

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 sellaisenaan järjestelmään, vaan niistä lasketaan tiiviste yksisuuntaisen tiivistefunktion tai vastaavan 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 niistä hyödyntää tiivisteen muodostamisessa jotain standardoitua kryptografista tiivistefunktioita. Ei ole kuitenkaan suositeltavaa luoda salasanatiivisteitä yksinään tällaisilla funktioilla, jotka ovat käyttötarkoitukseensa liian nopeita, vaan käyttää sitä varten kehitettyä algoritmia.

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

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

Suositeltavia salasanatiivistealgoritmeja on listattu liitteessä 1.

6.7.10 Aineiston tallentaminen pilveen turvallisesti

Käsiteltävän datan määrä ja uusien teknologioiden käyttö saa monet organisaatiot harkitsemaan tiedon tallentamista ulkoisiin pilvipalveluihin. Niissä saatetaan tarjota erityyppisiä tietoturvallisuutta parantavia ratkaisuja, kuten tiedon automaattista salausta.

Lähtökohtana pilvipalveluiden käytölle on pidettävä sitä, ei ole tiedossa mitä reittiä tieto liikkuu, mihin tieto tallennetaan ja mitkä kaikki tahot tietoon pääsevät käsiksi – ellei toisin pitävästi osoiteta. Tämä sisältää mahdollisten tietomurtautujien, palveluntarjoajan ja sen alihankkijoiden sekä tietoliikennepalveluntarjoajien lisäksi myös maansa lakien puitteissa toimivat viranomaistahot. Jos tieto pilvipalvelussa kulkee valtion läpi tai tallennetaan valtioon, jossa viranomaisilla on mahdollista esimerkiksi maan lakien perusteella tai oikeu-

den määräyksellä pyytää palvelun asiakkaiden tietoja, niin he myös tiedot saavat. Tiedon eheyden vaarantumisen riski on myös otettava huomioon. Pilvipalveluja käytettäessä uhkilta on mahdollista luotettavasti suojautua vain turvallisilla salausratkaisuilla ja pitämällä niiden avaintenhallinta luotettavan tahon hallussa.

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. Avaintenhallinnassa kynnyskysymykseksi saattaa muodostua avaimia luova ja säilyttävä taho. Jos palvelun tarjoaa ulkopuolinen yritys, se myös usein 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 palvelun omien varmenteiden lisäksi kaikkien selaimiin luotettaviksi asetettujen juurivarmentajien luotettavuudesta ja turvallisuudesta.

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

Liite 1. Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset suojaustasot

Liitettä ylläpidetään ja säilytetään viestintäviraston sivustolla osoitteessa https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/ncsa-fi.html

Kohdasta asiakirjat:

Kryptografiset vahvuusvaatimukset - kansalliset suojaustasot.pdf. Lisäksi linkki asiakirjaan löytyy tämän ohjeen www-sivulta osoitteesta www.vahtiohje.fi.

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. Murtami-

nen 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.

Suola (salt)
Salasanoja käyttävissä palveluissa ja järjestelmissä pitää kiinnittää erityistä huomiota salasanojen turvalliseen suojaamiseen. Ne eivät saa löytyä palvelusta selväkielisinä, vaan ne pitää tallentaa oikeaoppisesti tiivisteiden ja suolauksen avulla. Suola on satunnaisesti muodostettu, yleensä julkinen, uniikki käyttäjäkohtainen merkkijono, jota käytetään salasanan lisäksi algoritmin parametrina. Suolan muuttaminen muuttaa myös tiivistettä, vaikka salasana pysyisi samana. Tämä vaikeuttaa merkittävästi salasanojen selvittämistä tiivisteistä, eikä muutaman salasanan murtaminen helpota muiden salasanojen selvittämistä.

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.

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
Telefaksi 09 160 33123
www.vm.fi

ISSN 1459-3394 (nid.)
ISBN 978-952-251-725-8 (nid.)
ISSN 1797-9714 (pdf)
ISBN 978-952-251-726-5 (pdf)

Lokakuu 2015