VALTIOVARAINMINISTERIÖ

Valtion-hallinnon salaus-käytäntöjen tietoturva-ohje

Valtionhallinnon tietoturvallisuuden johtoryhmä

3/2008 VAHTI

VALTIOVARAINMINISTERIÖ

Valtionhallinnon salauskäytäntöjen tietoturvaohje

Valtionhallinnon tietoturvallisuuden johtoryhmä

3/2008

VAHTI

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 09 16001 (vaihde)
Internet: www.vm.fi
Taitto: Pirkko Ala-Marttila/VM-julkaisutiimi

ISSN 1455-2566
ISBN 978-951-804-805-6 (nid)
ISBN 978-951-804-806-3 (pdf)

Edita Prima Oy
Helsinki 2008

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 16/01/2008

OHJE
28.2.2008

Ministeriöille, virastoille ja laitoksille

VALTIONHALLINNON SALAUSKÄYTÄNTÖJEN TIETOTURVAOHJE

Valtionhallinnon salauskäytäntöjen tietoturvaohje (VAHTI 3/2008) on yleisohje salauskäytäntöjen tietoturvallisesta ja hyvien käytäntöjen mukaisesta järjestämisestä ministeriöissä, virastoissa ja laitoksissa. Ohje korvaa valtiovarainministeriön aiemman asiakirjan *Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus (VAHTI 3/2001)*.

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on ohjannut ohjeen valmistelun ja hyväksynyt ohjeen käytettäväksi valtionhallinnon tietoturvallisuuden kehittämisessä, ohjauksessa ja yhteistyössä. Ohje on osa laajaa VAHTI-ohjeistoa.

Jokaisen organisaation johto päättää ja vastaa riittävien salausmenettelyjen käytöstä ja kehittämisestä organisaatiossa. Ohje on suunnattu erityisesti ministeriöiden ja virastojen johdolle sekä teknisille asiantuntijoille. Lisäksi ohje palvelee monia valtionhallinnon sidosryhmiä sekä kansallista ja kansainvälistä yhteistyötä.

Ohjeessa käsitellään muun muassa salauskäytäntöjen liittymiä toiminnallisiin, tietohallinnollisiin ja teknisiin kokonaisuuksiin. Ohjeeseen sisältyy suositusten, käyttötarpeiden ja algoritmien sekä prosessimallin ja -vaatimusten kuvaukset.

Salausratkaisujen suunnitelmallisella ja hyvien käytäntöjen mukaisella käytöllä edistetään avoimuutta, luottamusta ja luotettavuutta. Salaus mahdollistaa osaltaan hyvien tietoturvakäytäntöjen mukaisen kontrollien toteuttamisen, turvallisen viestinnän, luotettavan tunnistamisen ja riskien hallinnan sekä vähentää paperiprosesseja. Ohje korostaa salausratkaisun käyttöönoton ja käytön prosessia, osaamisen kehittämistarpeita, ratkaisujen luotettavuuden merkitystä ja salauskäytäntöjen yhteentoimivuusvaatimuksia.

Lisätietoja antavat tietoturvallisuusasiantuntija Juhani Sillanpää ja tietoturvapäällikkö Kari Keskitalo (sähköpostit: etunimi.sukunimi@vm.fi).

Hallinto- ja kuntaministeri — Mari Kiviniemi

Neuvotteleva virkamies — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite: *Valtionhallinnon salauskäytäntöjen tietoturvaohje (VAHTI 3/2008)*

Esipuhe

Valtiovarainministeriö (VM) vastaa julkishallinnon tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.

VAHTIssa käsitellään kaikki merkittävät valtionhallinnon tietoturvalinjaukset ja tietoturvatoimenpiteiden ohjausasiat. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTIn käsittelyn kohteina ovat kaikki tietoturvallisuuden osa-alueet.

VAHTIn toiminnalla on parannettu valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä ja kansainvälisesti. Tuloksena on aikaansaatu erittäin kattava yleinen tietoturvaohjeisto (www.vm.fi/VAHTI). Valtiovarainministeriön ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita. VAHTI on valmistellut, ohjannut ja toteuttanut valtion tietoturvallisuuden kehitysohjelman, jossa on aikaansaatu merkittävää kehitystyötä yhteensä 26 kehityskohteessa yli 300 hankkeisiin nimetyn henkilön toimesta.

VAHTI edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

Valtionhallinnon lisäksi VAHTIn toiminnan tuloksia hyödynnetään laajasti myös kunnallishallinnossa, yksityisellä sektorilla, kansalaistoiminnassa ja kansainvälisessä yhteistyössä. VAHTI on saanut kolmena perättäisenä vuotena tunnustuspalkinnon esimerkillisestä toiminnasta Suomen tietoturvallisuuden parantamisessa.

Tämän ohjeen ovat yhteistyössä laatineet VAHTIn alainen salauskäytännöt- ja varmenteet- työryhmistä yhdistetty työryhmä. Ohje on viimeistelty laa-

jan lausuntokierroksen palautteen pohjalta ja hyväksytty viimeisteltäväksi ja julkaistavaksi VAHTIn kokouksessa joulukuussa 2007. Ohje korvaa aiemman VAHTI-julkaisun Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001.

Johdon tiivistelmä

Salausratkaisu on kokonaisuus, jolta vaaditaan toiminnallisuutta ja luotettavuutta.

Tähän tarvitaan prosessit, riittävä osaaminen ja tarkoituksenmukainen tekniikka.

Salaus ei ole yksittäinen teknologia vaan yksi kontrollien mahdollistaja. Kaikkia kontrolleja tulee hyödyntää aktiivisesti, ja kaikkien kontrollien tulee tukea toisiaan osana tiedon suojausta.

Vaatimukset salaukselle johdetaan seuraavista: Kansainväliset linjaukset, vaatimukset luokitellun tiedon suojaamisesta, toiminnallinen yhteensopivuus, tarve- ja tilannekohtaisuus sekä tapa työskennellä.

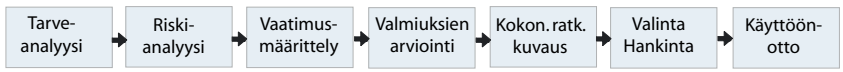
Yhteensopivuus todennusratkaisujen kanssa on aina lisäarvo. Väestörekisterikeskus katsotaan luotetuksi varmennetoimittajaksi. Virkamieskortin ja sähköisen henkilökortin käyttöä edistetään.

Osapuolet eivät aina ole henkilöitä. Laitteiden, ohjelmistojen tai muiden olioiden välinen luottamus on tärkeätä. Tätä edistetään standardien hyödyntämisellä ja ohjelmistovarmenteilla.

Algoritmi- ja avainkysymykset voivat olla kynnyskysymyksiä, mutta ohjeistettavissa tarkasti. Esimerkiksi algoritmi AES, tiivistefunktio SHA, avainpituus kaksinkertainen AES -avaimesta.

Tuotteiden kypsyys on kohtuullisen hyvä. Haasteet ovat integroinneissa ja prosesseissa. Sähköpostisuositukset ovat osin tapauskohtaisia niin kauan, kun ratkaisut ovat heterogeenisia.

Salausratkaisun käyttöönotto on prosessi, jossa painotetaan tavoitteita ja valmiuksia:



Tiedon, järjestelmän ja salausratkaisun elinkaaret ovat erimittaiset. Näiden elinkaarten hallinta edellyttää valmistautumista. Organisaatiolla on oltava riittävä kypsyys ja kyvykkyys.

Salausratkaisut edistävät avoimuutta, luottamusta ja luotettavuutta.

Sisältö

1 Tausta ja tavoite

1.1 Rajaus ja kokonaisvaltaisuus

Tämä dokumentti ohjaa erilaisten salausratkaisujen hyödyntämistä julkishallinnon tietoteknisessä ympäristössä. Salausratkaisuja ei esitetä ainoastaan yksittäiseen tarpeeseen vastaavana teknologiana vaan vaihtoehtoisena, täydentävänä ja mahdollistavana tietoaineiston kontrollina.

Salausratkaisu on kokonaisuus, jolta vaaditaan toiminnallisuutta ja luotettavuutta. Salausteknologian avulla kontrolloidaan tiedon luottamuksellisuutta ja eheyttä sekä mahdollistetaan luotettava tunnistus ja todennus.

Salausratkaisun toiminnallisuus ja luotettavuus saavutetaan, kun tiedon luonteesta ja organisaation toiminnasta johtuva tarve salaukselle ratkaistaan kontrolloitujen prosessien, riittävän osaamisen ja tarkoituksenmukaisen tekniikan avulla.

Tämän ohjeen rakenne ja sisältö ohjaavat kokonaisvaltaista lähestymistä.

1.2 Ohjeistuksen virallinen tausta

Valtiovarainministeriö asetti keväällä 2007 valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) alaisuuteen kaksi sittemmin yhdistettyä työryhmää päivittämään salauskäytäntöjä koskevaa valtionhallinnon tietoturvallisuussuositusta (VAHTI 3/2001) sekä kehittämään ja yhteen sovittamaan varmenteiden käyttöön sähköpostissa liittyvää kehitystyötä.

Yhdistetyn työryhmän puheenjohtajana toimi tietoturvapäällikkö Kari Keskitalo valtiovarainministeriöstä.

Yhdistetyn työryhmän kokoonpano:
Sirpa Astala, erikoissuunnittelija, ulkoasiainministeriö
Juhani Eronen, tietoturva-asiantuntija, Viestintävirasto
Juha-Matti Heimonen, tietoturva-asiantuntija, Tampereen yliopisto
Leena Heino, järjestelmäasiantuntija, Tampereen yliopisto
Pasi Hänninen, atk-järjestelmäpäällikkö, Viestintävirasto
Kari Keskitalo, tietoturvapäällikkö, valtiovarainministeriö, puheenjohtaja

Jukka Kumpula, erikoissuunnittelija, ulkoasiainministeriö
Raimo Mäenpää, IT-suunnittelija, oikeusministeriö
Harri Mäntylä, atk-järjestelmäpäällikkö, Pääesikunta
Ossi Ojala, erikoistutkija, Puolustusvoimien Johtamisjärjestelmäkeskus
Jan Partanen, kehityspäällikkö, Väestörekisterikeskus
Olli-Pekka Rissanen, erityisasiantuntija, valtiovarainministeriö, varapuheenjohtaja
Tarja Saari, järjestelmäasiantuntija, oikeusministeriö
Juhani Sillanpää, tietoturvallisuusasiantuntija, valtiovarainministeriö
Seppo Sundberg, turvallisuusjohtaja, Valtiokonttori
Tapio Virkkunen, kehityspäällikkö, Väestörekisterikeskus
Mervi Virtanen, järjestelmäsuunnittelija, ulkoasianministeriö
Antti Hemminki, konsultti, Secproof Finland Oy

Yhdistetty työryhmä tuotti tämän ohjeen ensimmäiselle lausuntokierrokselle lähetetyn version keväällä 2007. Dokumenttia muokattiin lausuntojen perusteella loppusyksynä 2007 ja se luovutettiin hyväksyttäväksi joulukuun 2007 VAHTI-kokoukseen.

Työryhmät halusivat dokumentille rakenteen, joka tekisi siitä edellistä versiota helpommin päivitettävän ja täydennettävän. Yhdistetyn työryhmän valitseman linjan mukaisesti ohjeeseen haettiin hallinnollista, organisatorista ja prosessisuuntautunutta näkemystä. Lisäksi haettiin liitosta hyvään hallintotapaan ja tiedonhallintaan kokonaisuutena. Näiden tavoitteiden vuoksi tämä dokumentti poikkeaa rakenteeltaan ja painotuksiltaan edellisestä suosituksesta (VAHTI 3/2001).

Lopputulos kokonaisuutena on tarkoitettu palvelemaan kaikkia työryhmien asettamiskirjeissä ja niiden liitteissä yksilöityjä sidosryhmiä.

1.3 Ohjeen tavoitteet

1.3.1 Asetetut tavoitteet ja reunaehdot

Yhdistetyltä työryhmältä edellytettiin seuraavaa näkemystä ja lähestymistapaa:

- Töissä tulee ottaa huomioon säädöskehitys, valtion tietoturvallisuuden kehitysohjelma, VAHTI-ohjeet ja -hankkeet, valtion IT-strategia, kansainvälinen ja kansallinen kehitys sekä muu ohjeen kannalta keskeinen kehitys.
- Lopputuloksen tulee olla helposti päivitettävä.

Salausohjeistuksen uusimistyön osalta määritettiin aluksi seuraavat tehtäväalueet ja tavoitteet:

- Määritellä riittävät salauskäytännöt sekä viranomaisten sisäiseen, että viranomaisen ja kansalaisen tai asiakkaan väliseen yhteydenpitoon,
- selvittää, millaisia ratkaisuja salauksen hoitamiseen on tarjolla,
- suosittaa, minkälaisia salauskäytäntöjä tulee käyttää erityyppisten tietojen, asiakirjojen ja sähköpostiviestien tietojenkäsittelyn elinkaaren aikana sekä
- laatia tietoturvaohje sekä täydentäviä tiivistelmiä, esityksiä ja muuta materiaalia, joiden avulla edesautetaan suositusten mukaista toimintaa sekä parannetaan tietoturvallisuuden tasoa yhtenäistämällä salauskäytäntöjä ja salaustekniikan käyttöä valtionhallinnossa.

Varmenteiden käyttö sähköpostissa työn osalta määritettiin aluksi seuraavaa:

- Teknisten standardien valinta ja ohjeistuksen laatiminen.
- Tukea ja ohjeistaa varmenteiden käyttöä valtionhallinnossa yleisesti käytössä olevissa sähköpostiohjelmissa.
- Varmenteiden hallintaan liittyvien hallinnollisten ratkaisujen luominen.

Lopputulos tiivistää alun perin erillisinä asetetut tavoitteet yhdistetyn työryhmän rakentaman viitekehyksen avulla. Yhdistetty työryhmä toteaa kuitenkin, että tämän ohjeen ja useiden kehityshankkeiden välinen yhteensopivuus on varmennettava säännöllisesti. Kun tätä dokumenttia laadittiin, niin kaikkia tarvittavia päätöksiä esimerkiksi arkkitehtuureista ei ollut.

1.3.2 Sidosryhmät ja odotukset

Ohje palvelee seuraavia kohderyhmiä vastaavin tavoittein.

Sidosryhmä	Sidosryhmän odotukset
Valtionhallinnon tietoturvapäälliköt, tietoturva-asiantuntijat, IT-suunnittelijat ja muut IT ammattilaiset.	Ohjeistus linjaa salausratkaisujen tarkoituksenmukaista käyttöä omassa työssä, organisaatiossa ja muiden sidosryhmien kesken. Ohjeistus auttaa määrittämään käyttöönotto- ja kehittämisprojekteja salausratkaisuille.
Valtionhallinnon tietohallintopäälliköt ja hallinnollinen johto.	Ohjeistus sisältää jäsenneltyä materiaalia oman päätöksenteon tueksi johtotehtävissä ja investointien suunnittelussa.
Hansel	Ohjeistusta ja erityisesti siihen perustuvia kulloinkin ajantasaistettuja tai erikseen tuotettuja liitteitä voidaan käyttää tuotteiden ja toimittajien vaatimustason asettamisen pohjana, esimerkiksi mahdollisissa salausratkaisujen puitesopimusneuvotteluissa.
IT-mediatahot	Ohjeistus lisää tietoisuutta ja erityisesti kokonaisvaltaista näkemystä, missä ratkaisujen toimivuus osoitetaan riippuvaksi hallinnollisista päätöksistä ja osaamisesta, prosessien tarkkuudesta ja teknologian kyvykkyydestä.
Muu julkishallinto ja yritysmaailma	Ohjeistus lisää tietoisuutta ja näkemystä sekä kykyä asettaa vaatimustasoja salausratkaisuille omassa työssä ja ympäristössä. Ohjeistus auttaa määrittämään käyttöönotto- ja kehittämisprojekteja salausratkaisuille.
Kansainvälinen yhteistyö (OECD, EU, NATO)	Ohjeistus perustuu näkemyksiin ja selvityksiin siitä, miten näissä yhteyksissä on toimittu, tulee toimia ja voitaisiin toimia. Ohjeistus tai vähintään sen keskeiset kohdat on käännetty myös englanniksi.
Tietoturvaratkaisujen toimittajat	Ohjeistus antaa näkemyksen siitä, miten omien ratkaisujen tulisi suhtautua julkishallinnon vaatimuksiin. Ohjeistus auttaa toimittajia kehittämään ja suuntaamaan toimintaansa ja tuotteitansa julkishallintoa jatkuvasti paremmin palvelevaan suuntaan.
Peruskäyttäjät	Ohjeistusta ei sellaisenaan ole suunniteltu tai suunnattu peruskäyttäjiä ajatellen. Ohjeistuksen rinnalle voidaan tuottaa täydentävää materiaalia, josta osa vastaa tähän tavoitteeseen (esimerkkinä ohjeet varmenteista ja sähköpostiohjelmista).

On syytä huomata ja vielä erikseen korostaa, että tämä ohje ei ole suunnattu käyttäjien jokapäiväisen toiminnan yksityiskohtaiseksi ohjeistukseksi, vaan salausratkaisujen valintaa, käyttöönottoa ja hallintaa yleisesti ja kokonaisvaltaisesti ohjaavaksi materiaaliksi.

2 Rakenne, sisältö ja hyödyntäminen

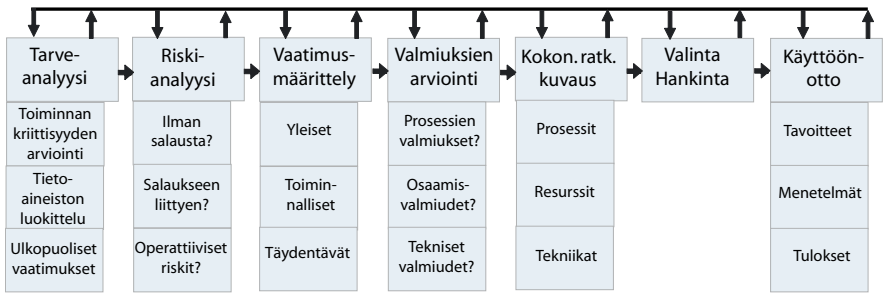
2.1 Rakenne

Dokumentin rakenne ja esitystapa perustuu linjaaviin peruskysymyksiin seuraavasti:

- Tiivistelmä suosituksista:
  - Luku 3: Visiosta toteutuksiin – tiivistelmä suosituksista
- Miksi salausratkaisuja tarvitaan? Mitä yleisiä vaatimuksia ratkaisujen tulee täyttää?
  - Luku 4: Yleiset suositukset, viitekehykset ja standardit
- Mitä teknisiä vaatimuksia salausratkaisujen tulee täyttää?
  - Luku 5: Terminologiat, teknologiat ja tekniset suositukset
- Missä salausratkaisuja voidaan hyödyntää?
  - Luku 6: Käyttötarvekuvaukset, suositukset ja tarjonnasta
- Miten salausratkaisut otetaan tuloksekkaasti käyttöön?
  - Luku 7: Prosessimalli: Suunnittelu, valinta ja käyttöönotto
- Mitä sisältyy salausratkaisun elinkaareen?
  - Luku 8: Prosessivaatimukset: Tiedon ja salausratkaisujen elinkaari (Erityisesti avainten hallinta)

Dokumentin kokonaiskuva syvenee ja tarkentuu, kun siihen perehdytään kuvatussa järjestyksessä. Yksittäiset luvut on kirjoitettu siten, että niihin voi tietyin rajoituksin perehtyä erillisinä. Kokonaisvaltaisuutta korostetaan toistuvasti.

- Dokumentin rakenne tukee seuraavaa käyttöönottoprosessia, mikä esitellään yksityiskohtaisesti luvussa 7. Dokumentti luo luku luvulta valmiuksia tämän kokonaisprosessin hallintaan:



2.2 Dokumentin sisältö ja hyödyntäminen

Seuraavassa taulukossa kuvataan lyhyesti dokumentin kunkin luvun keskeiset teemat.

Luku	Teema	Aihealueet	Lyhyesti	Hyöty lukijalle
Luku 1	Virallinen tausta ja tavoite	Kokonaisvaltaisuus Asettamispäätökset	Tavoitteiden yksilöinti ja näiden muokkaaminen yhdistetyn työryhmän näkemysten mukaisesti	Käsitys siitä, millä oletuksilla ohjeistus on tuotettu ja mitä haetaan.
Luku 2	Rakenne, sisältö ja hyödyntäminen	Dokumentin kuvaus	Osioiden suhteet ja sisällöt	Auttaa selaamista kuvaamalla kunkin luvun tarkoituksen.
Luku 3	Visiosta toteutuksiin - tiivistelmä suosituksista	Kaikki teemat	Ohjeistuksen kootut suositukset	Tiivistelmä ohjeistuksen kaikkien lukujen sisältämistä ja näissä tarkemmin perustelluista suosituksista nopeata hakua varten.
Luku 4	Yleiset suositukset, viitekehykset ja standardit	Kansainvälisyys, normiohjaus. riskienhallinta, tietoturvallisuus ja hyvä hallintotapa. Tietoaineiston hallinta ja elinkaareen liittyvät kontrollit. Liitokset arkkitehtuureihin.	Perustelut, joiden mukaan salausratkaisut pitää nähdä osana laajempaa kokonaisuutta (tiedonhallinnan kontrolleja). Näkökulmia, joista saadaan kaikkea valintaa, käyttöönottoa ja käyttöä ohjaavia peruskriteerejä. Esimerkkinä yhteensopivuus.	Tarjoaa katsauksen strategisiin, operatiivisiin ja teknisiin rajapintoihin. Antaa näkemyksiä, joiden avulla voidaan perustella linjauksia ja myös yksittäisiä ratkaisuja.
Luku 5	Terminologiat, teknologiat ja tekniset suositukset	Määritelmät. Symmetrinen salaus, epäsymmetrinen salaus, tiivistefunktiot. Käyttötapauksia ja suosituksia.	Algoritmin valinta ja avainpituus riippuvat toisistaan. Symmetrisellä ja epäsymmetrisellä salauksella on luontevat käyttötarkoituksensa. Tiivistefunktiot varmentavat eheyttä. Varmenteen luotettavuus on myös prosessikysymys. Kokonaisuus ratkaisee laadun.	Tiivistelmä teknisistä arvoista ja ratkaisuista sekä näiden perusteella annettavat suositukset.

Luku 6	Käyttötarve-kuvaukset, suositukset ja tarjonnasta	Käyttötarpeiden mallintaminen. Esimerkkejä.	Käyttötarpeen kuvaamisessa käytettäviä parametreja: Tietoaineisto, topologia, lähettäjä ja vastaanottaja sekä todennustarpeet.	Näkemyksiä yksittäisen tarpeen ratkaisemisesta. Liitoksia kokonaisuuteen topologiassa. Linjauksia ja suosituksia sekä joitain näkemyksiä markkinoiden tarjonnasta.
Luku 7	Prosessimalli: Suunnittelu, valinta ja käyttöönotto	Vaatimusmäärittely, valmiudet, hankinta- ja käyttöönotto prosessina.	Vaatimusten ja valmiuksien mallintaminen organisaation tarpeiden ja kypsyyden pohjalta. Prosessimallin korostaminen, koska salausratkaisua ei saa nähdä yksittäisenä hankintana.	Hyvää hallintotapaa tukeva ja systemaattisia hankintakäytäntöjä korostava tiivistelmä suosituksineen.
Luku 8	Prosessi-vaatimukset: Tiedon ja salausratkaisujen elinkaari	Elinkaariajattelu. Salausratkaisun ja erityisesti avainten elinkaaren hallinta, rekisteröinnistä sulkemiseen.	Ongelman asettelu: Tiedon, järjestelmän ja salausratkaisun elinkaarten huomioiminen. Salausratkaisun, avainten ja varmenteiden elinkaareen liittyviä kysymyksiä, joihin organisaation on kyettävä vastaamaan.	Tiivistelmä haasteista, joihin on vastattava ennakoivasti. Hahmottaa haasteita myös valinnan ja käyttöönoton ja ohjaa miettimään ratkaisuja.

3 Visiosta toteutuksiin – tiivistelmä suosituksista

3.1 Johdanto

Tämä luku on tiivistelmä dokumentin sisältämistä suosituksista.

Tähän lukuun kerättyjä suosituksia perustellaan, kuvataan ja täydennetään dokumentin muissa luvuissa. Luvun jäsennys ja kappaleiden numerointi vastaa koko dokumentin jäsennystä siten, että esimerkiksi kappale 3.4 perustuu luvun neljä (4) sisältöön sekä luvussa neljä tarkemmin esitettyihin taustoihin ja perusteluihin.

3.2 Mistä visio?

Suositellaan luottamuksen ja luotettavuuden korostamista kaikissa asiayhteyksissä.

- Kansainväliset suositukset salauksesta ja sähköisestä todennuksesta.
- Valtionhallinnon rooli ja vastuu kansalaisiin ja muihin sidosryhmiin nähden.
  - Salausratkaisut edistävät avoimuutta, luottamusta ja luotettavuutta.
  - Arvoina aina luottamus ja yksityisyyden kunnioitus.
  - Salausratkaisut ovat kontrollien mahdollistaja.
  - Salausratkaisut tukevat normiohjausta.

3.3 Mistä strategia?

Suositellaan toiminnallista yhteensopivuutta mahdollisimman monen sidosryhmän kesken.

- Tiedon elinkaaren vaatimat kontrollit, valtionhallinnon linjaukset ja arkkitehtuurit.

- Valtionhallinnon rooli ja vastuu kansalaisiin ja muihin sidosryhmiin nähden.
  - Julkishallinnon ratkaisuissa korostetaan yhteensopivuutta ja integroitavuutta sidosryhmien kesken, hyödyntäen yhteisiä hallinnollisia ja teknisiä rajapintoja sekä ohjaavia arkkitehtuureja.
  - Julkishallinnon sisäisten ratkaisujen valinnassa korostetaan tehokkuutta, tarkoituksenmukaisuutta ja harmonisointia, unohtamatta organisaatioiden erityispiirteiden vaatimaa vaihtoehtoisuutta.
  - Kansalaisia ja muita ulkoisia sidosryhmiä palvelevissa ratkaisuissa tuetaan myös vaihtoehtoisuutta, tavoitteena kuitenkin yleinen yhteensopivuus.

Valtionhallinnon tulisi omilla valinnoillaan ja vaatimuksillaan edesauttaa salausjärjestelmien ja ratkaisujen kehittämistä painottaen avoimuutta, yhteensopivuutta ja helppokäyttöisyyttä.

3.4 Mallit, viitekehykset ja standardit

3.4.1 Yleiset mallit, standardit ja viitekehykset

Vaaditaan normiohjaus ja sen osoittaminen kaikessa salaukseen liittyvässä päätöksenteossa.

Suositellaan hyvän hallintotavan mukaisia johtamisjärjestelmiä ja salausjärjestelmien perustelemista ja tukemista yleisesti hyväksyttyjen mallien ja standardien mukaisesti. Esimerkkejä:

- Riskinhallinnan malli COSO [www.coso.org].
- Tietohallinnon kehittämisen malli COBIT [www.itgi.org].
- Tietoturvan johtamisjärjestelmän standardi ISO27001 [www.iso.org].
- Tietohallinnon prosessien mallintaminen ITIL [www.itil.org].
- Organisaation kypsyyden ja kyvykkyyden kehittäminen: SSE-CMM.

Salausratkaisun valinnassa suositellaan painotettavaksi yhteensopivuutta sekä julkishallinnon arkkitehtuurien kanssa että tunnistettujen sidosryhmien kesken.

3.4.2 Tietoaineiston kontrollivaatimukset

Salausratkaisun on tuettava kaikkia luokitellun tiedon käsittelyvaatimuksia.

Suositellaan, että salausratkaisuja hyödynnetään aktiivisesti tietoaineiston käytön kontrollointiin: Salaustekniikat tehostavat todentamista, parantavat luo-

kitellun tiedon luottamuksen suojausta ja mahdollistavat tietoaineiston eheyden ja muuttumattomuuden varmentamisen.

Suositellaan ja ohjaavasti vaaditaan, että mitä kriittisempi tietoaineisto, sitä tiukemmaksi on myös salaustekniikan mahdollistamat kontrollit tehtävä. Korkean turvaluokan tietojen suojauksesta:

- Todennuksessa pitää suosia vahvaa varmennepohjaista todennusta, ja näiden varmenteiden tulee olla hyväksytyn tahon (esimerkiksi VRK) tuottamia.
- Salauksessa pitää suosia vahvoja algoritmeja hyödyntäviä tuotteita, joiden toiminnallisuus kyetään osoittamaan ja siihen kyetään myös vaikuttamaan.
- Eheyden varmennuksessa pyritään suosimaan vain vahvimpia algoritmeja, milloin tämä on markkinoiden rajallinen tarjonta huomioiden mahdollista.

3.5 Teknologia ja ratkaisut

Salausratkaisujen algoritmeista ja avainpituuksista annetaan seuraavat yleiset suositukset:

- Salausratkaisuissa käytettävän algoritmin tulee olla avoin, eli sen oikeellisuuden arvioinnin tulee perustua kriittiseen, avoimeen ja tieteelliseen tutkimustyöhön. Salausratkaisun luotettavuus ei saa heikentyä, jos algoritmi paljastuu.
- Avainpituuden tulee olla valittuun algoritmiin nähden riittävän pitkä käyttöhetkellä voimassa olevan käsityksen ja mahdollisesti tarkennetun ohjeistuksen mukaisesti.

Symmetristen algoritmien osalta yleisiä suosituksia tarkennetaan seuraavasti:

- Suositaan algoritmia AES ja vähintään 128 bitin avainpituutta.
- Muita hyväksyttyjä algoritmeja ovat Twofish, Blowfish ja IDEA.
- Algoritmia 3DES kolmella avaimella (3 x 56bit) voidaan suositella vain, jos 3DES algoritmin käytölle ei ole olemassa tilanteeseen sopivaa vaihtoehtoa.
- Jonosalausalgoritmia RC4 voidaan käyttää soveltuvissa tapauksissa. Näissä tapauksissa on kuitenkin huomioitava algoritmin rajoitteet. Suositellaan seuraamaan algoritmin SNOW kehittymistä ja siirtymään siihen kun toimivuus on osoitettu.
- Muita symmetrisiä algoritmeja tai alle 128 bitin avainpituuksia ei suositella.

Epäsymmetristen algoritmien ja varmenteiden osalta yleissuositusta tarkennetaan seuraavasti:

- Suositellaan, että valtionhallinto aktiivisesti edistää keskustelua epäsymmetristen algoritmien kehittämisestä ja uusien vaihtoehtojen tuonnista tuotteisiin.

- Suositellaan hyväksyttyjen tahojen (esimerkkinä VRK) tuottamia ja tukemia varmenteita (virkamieskortti, sähköinen henkilökortti).
- Pyritään edistämään varmenteiden käyttöä myös laitteiden ja ohjelmistojen välisessä todentamisessa.
- Suositellaan organisaatioiden ottavan pikaisesti käyttöönsä sähköpostijärjestelmien välinen todentaminen (SSL/TLS).
- Suhtaudutaan varauksella varmenteiden myöntäjiin, joita järjestelmät tarjoavat ”helppoina oletuksina” tai joihin järjestelmät luottavat ”esiasennettuina”.

Tiivistefunktioiden osalta annettu yleissuosituksen tarkenne:

- Suositeltavat algoritmit ovat SHA-256, SHA-384 ja SHA-512. Avainpituuden tulisi olla kaksinkertainen verrattuna tiedon salaamiseen käytetyn algoritmin avainpituuteen.
- Suhtaudutaan varauksella muihin tiivistefunktioihin, kuten MD5 tai SHA-1.

Lisäksi suositellaan kriteeristön FIPS140 ja sen uusimman version (FIPS 140-3) mukaisen hyväksynnän vaatimista tai sitä, että vastaavat kriteerit pystytään osoittamaan täytetyiksi.

3.6 Käyttötarvekohtaisia suosituksia

Käyttötarpeet eivät tuo varsinaisia lisäsuosituksia, koska muut annetut suositukset pitää täyttää jokaisessa tarpeessa ja tilanteessa. Tuotteen ja ratkaisun valinnassa korostetaan lisäarvoina esimerkiksi ratkaisun ja toimituksen avoimuutta, yhteensopivuutta ja toimittajan osaamista.

3.7 Prosessimalli ja elinkaaren hallintakysymykset

Suositellaan dokumentin luvussa seitsemän (7) kuvatun prosessimallin mukaista lähestymistä salaushankkeisiin. Malli auttaa huomioimaan kaikki näkökohdat päätöksenteossa, myös organisaation kypsyyden ja kyvykkyyden.

Suositellaan, että organisaatio varmistaa oman kyvykkyytensä selviytyä ratkaisujen elinkaaren vaatimista toimenpiteistä. Muistutetaan erityisesti niistä haastavista tilanteista, missä tietojärjestelmän, salausratkaisun, salausratkaisun komponenttien ja tiedon elinkaaret ovat erimittaisia. (Luku 8).

4 Yleiset suositukset, viitekehykset ja standardit

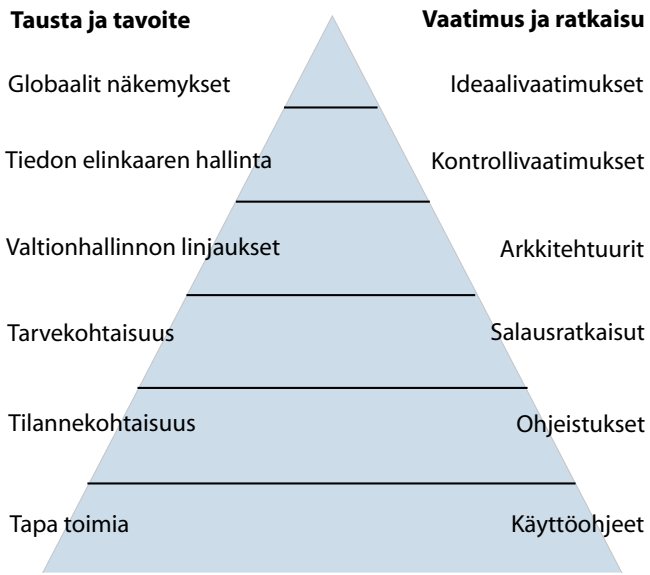
4.1 Johdanto

Salausratkaisun toiminnallisuus ja luotettavuus saavutetaan, kun tiedon luonteesta ja organisaation toiminnasta johtuva tarve salaukselle ratkaistaan kontrolloitujen prosessien, riittävän osaamisen ja tarkoituksenmukaisen tekniikan avulla.

Tämä luku on tiivis katsaus erilaisiin malleihin, joiden avulla voidaan jäsentää ja kuvata salausratkaisuihin kohdistuvia tarpeita ja vaatimuksia. Luku myös osoittaa, miten salaus liittyy muihin tiedon hallinnan kontrolleihin.

4.2 Vaatimusmäärittelyn hierarkia ja yhteensopivuus arvona

Salausratkaisun välttämättömyys tai tarpeellisuus perustuu ensisijaisesti tiedon laatuun. Julkishallinnosta on helppo löytää useita yksittäisiä tarpeita salausratkaisuille. Vaatimukset salausratkaisuille voidaan kuvata toisiinsa nähden hierarkkisesti seuraavan mallin avulla:



Salausratkaisun pitää tukea kansainvälisiä tavoitteita ja periaatteita (esimerkiksi luottamuksen rakentaminen). Tiedon elinkaaren hallinta edellyttää kontrolleja, joiden tiukkuus riippuu tietoaineiston kriittisyydestä. Kriittisimmän tiedon suojaamisen tarve lähtee julkishallintoa ohjaavasta lainsäädännöstä. Yhteensopivuus arkkitehtuurien kanssa on vaatimus salausratkaisun ja sen hallintaan liittyvien tekniikoiden ja prosessien yhteisistä rajapinnoista. Tarve- ja tilannekohtaisuus antaa lopullisen liikkumavaran, minkä puitteissa voidaan tehdä valinta vaihtoehtoisten tekniikoiden, tuotteiden ja toimittajien välillä.

4.3 Kansainvälinen yhteistyö ja vaatimustenmukaisuus

4.3.1 Kansainvälisyys

Kansainvälinen yhteistyö lisää tarpeita tiedon jakamisen ja siirron kontrollointiin. Osittain tämän vuoksi julkishallinnon salausratkaisuja ja niiden hyödyntämistä ohjataan kansainvälisillä suosituksilla.

OECD [Organisation for Economic Co-operation and Development] julkaisi suosituksia salausratkaisujen hyödyntämisestä julkishallinnossa jo vuonna 1997. (RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES FOR CRYPTOGRAPHY POLICY. 27 March 1997). Soveltavia poimintoja alkuperäisestä suosituksesta:

- Salausratkaisut edistävät osaltaan luottamusta (”trust”) sähköiseen asiointiin. Tämän vuoksi niiden valintaan ja käyttöön pitää kiinnittää huomiota.
- Yksityisyyden suojaaminen on nähtävä kaikkea toimintaa ohjaavana itseisarvona. Luottamuksen ja yksityisyyden säilymistä ei saa heikentää.
- Valtionhallinnon tulee tarjota kansalaisilleen vaihtoehtoisia mahdollisuuksia ja pyrkiä omalla toiminnallaan edistämään todellista vaihtoehtoisuutta.
- Hyödynnettävän teknologian tai ratkaisun tulee perustua avoimeen tutkimustietoon ja sen laadun jatkuvan kehittymisen tulee osaltaan perustua avoimeen kilpailuun.
- Vastuukysymykset tulee aina määrittää yksityiskohtaisesti kaikissa ratkaisun toimivuuteen ja yhtälailla ratkaisun käyttöön liittyvissä kysymyksissä.
- Julkishallinnon tulee aktiivisesti pyrkiä kansainväliseen yhteistyöhön tällä saralla. Salauksen käyttöä ei saisi missään tapauksissa rajoittaa.

Esitetyt linjaukset ovat edelleen pohja suosituksille. Vähintään EU-alueella pyritään siihen, että salausratkaisut suunnitellaan mahdollisimman yhteensopiviksi rakenteiltaan sekä kontrolloiduiksi ja osoituskelpoisiksi hallinnollisilta menetelmiltään ja vaatimuksiltaan.

OECD julkaisi kesäkuussa 2007 uuden suosituksen todennusratkaisujen hyödyntämisestä sähköisessä toimintaympäristössä (OECD Recommendation Electronic Authentication and OECD Guidance for Electronic Authentication. June 2007). Soveltavia poimintoja alkuperäisestä:

Todennusratkaisut ovat oleellinen komponentti, jota tarvitaan sähköisissä ympäristöissä identiteettien oikeellisuuden varmentamiseen ja hallintaan.

- Sähköiset todennusratkaisut auttavat järjestelmien ja verkkojen turvallisuuden vahvistamisessa ja kaikkien osapuolten yksityisyyden turvaamisessa.
- Suositellaan tukemaan teknologiamielessä neutraaleja ja yhteensopivia ratkaisuja kotimaisen ja kansainvälisen yhteistyön tehostamiseksi.
- Suositellaan kaikkialla, sekä julkisella että yksityisellä sektorilla, tukemaan ja kehittämään hyviä toimintatapoja, teknologioita ja ratkaisuja.

OECD:n linjaukset korostavat julkishallinnon roolia ja mahdollisuuksia markkinoiden ohjaajana. Suositellaan, että julkishallinnon organisaatiot aktiivisesti vaativat markkinoiden toimijoilta ja ratkaisuilta helppokäyttöisyyden, hallittavuuden ja yhteensopivuuden jatkuvaa kehittämistä.

4.3.2 Normiohjaus

Normiohjautuvuudella tarkoitetaan ohjaavien lakien, asetusten ja arvojen huomioimista päätöksenteossa. Normiohjautuvuus voidaan nähdä salausratkaisujen kannalta ainakin seuraavista näkökulmista:

- Salausratkaisujen pitää sekä täyttää ulkoiset vaatimukset että tukea niitä.
  - Esimerkki: Tietoaineiston käsittelyä ohjaa olemassa oleva normisto. [VIITE: Tietoaineistojen käsittely valtionhallinnossa, VAHTI 2/2002].
- Salausratkaisuilla voidaan ohjata toimintaa siten, että kaikkia toimintaa koskevia normeja kunnioitetaan ja samalla edistetään niiden tukemia arvoja.
  - Esimerkki: Salausratkaisuilla voidaan taata sekä julkisuuslain vaatima avoimuus, yksityisyyden suojan vaatimukset että kansalaisten luottamus sähköisen asioinnin kontrolleihin.

Salausratkaisut ja näihin läheisesti liittyvät todennusratkaisut tulee valtionhallinnossa nähdä tietoaineistoon kohdistuvan normiohjauksen mahdollistajina ja luottamuksen edistäjänä.

4.3.3 Salaus- ja todennusratkaisut: Suosituksia ja mahdollisuuksia

OECD:n suositukset ovat hyvä pohja tarkemmille suosituksille. Myös tämän VAHTI-ohjeen näkemykset ja suositusten henki perustuvat OECD:n suositusten henkeen.

Suosituksia:

- OECD:n linjauksia suositellaan noudatettaviksi organisaatioiden välisessä kanssakäymisessä sekä kotimaisessa että kansainvälisessä yhteistyössä.
- Vähintään EU-alueella linjaukset voidaan nähdä ohjaavina suosituksina.
- Kansalliset ratkaisut tulisi suunnitella ja toteuttaa siten, että suositusten mukaiset periaatteet, esimerkkinä yksityisyyden korostaminen, ovat osoitettavissa.
- Lainsäädäntö ei saisi olla ristiriidassa esitettyjen periaatteiden kanssa. Tämä toisin päin kääntäen, juridinen vaatimustenmukaisuus on suunnittelussa aina pakollista.
  - Tämä ohjeistus ei tietenkään ota kantaa lakien säätämiseen, mutta näkökulma on esitettävä: Lainsäädäntö ei saisi rajoittaa salausratkaisuja.
- Yhteensopivuutta pitää korostaa kaikissa tilanteissa.

Mahdollisuuksia:

- Salaus- ja todennusratkaisut edesauttavat tietoaineiston hallintaa ja kontrolleja.

  - Kontrolloidaan tiedon luottamuksellisuutta ja eheyttä ja mahdollistetaan luotettava tunnistus ja todennus.
- OECD:n linjaukset voidaan nähdä ohjaavina suosituksina valintatilanteissa.

Vaatimus ratkaisun yhteensopivuudesta ja kilpailun avoimuudesta voidaan ottaa ohjaavaksi arvoksi minkä tahansa salausratkaisun arviointiin.

4.4 Tiedon hallinta, riskienhallinta ja tietoturvallisuus

4.4.1 Tiedon hallinta, riskienhallinta ja tietoturvallisuus

Tiedon hallinnalla on merkittävä rooli organisaation toiminnassa ja siihen pitää kohdistaa tarkoituksenmukaiset kontrollit. Kaikki tietoturvaratkaisut ja siten myös salausratkaisut ovat osa organisaation tietoriskien ja tietopääoman hallintaa ja siten osa operatiivisten riskien hallintaa.

Päätökset salausratkaisujen käyttöönotosta pitää perustella saavutettavien operatiivisten hyötyjen ja muuten kohdattavien operatiivisten riskien perusteella. Myös ratkaisun käyttöönottoon liittyvät riskit, esimerkiksi tietoaineiston heikentynyt käytettävyys, on mietittävä kun arvioidaan ratkaisun vaatiman investoinnin hyötyjä.

Yleisesti hyväksytty viitekehys organisaation riskien hallintaan on COSO [www.coso.org]. Hyvää tiedonhallintaa ohjaa esimerkiksi COBIT [www.itgi.org]. Tietohallinnon prosessien mallintamisessa hyödynnetään usein ITIL-mallia [www.itil.org]. Kaikessa kehittämisessä on kunnioitettava hyvää hallintotapaa. Tämän vuoksi ei ole syitä siihen, että salausratkaisujen valinnassa, käyttöönotossa ja hyödyntämisessä ei tukeuduttaisi yleisesti hyväksyttyihin malleihin.

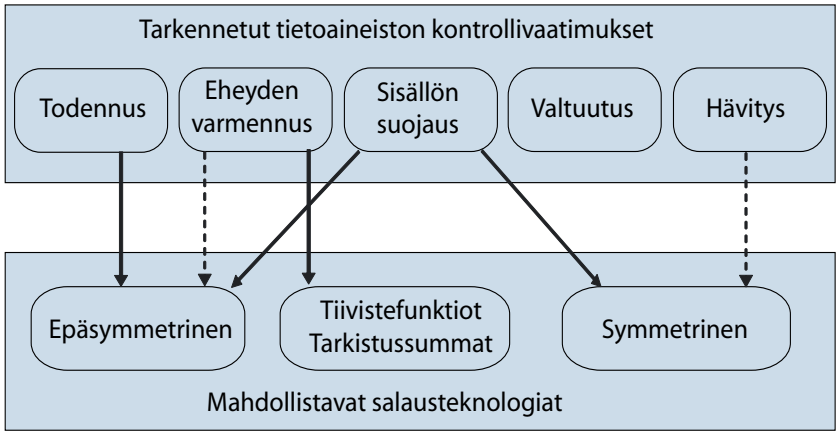
Tietoturvallisuus on osa hyvän hallintotavan edellyttämää kontrollia. Tietoturvallisuuden johtamisessa käytetään usein standardia ISO27001 [www.iso.org]. Tässä standardissa tietoturvatoiminnan tavoitteiksi asetetaan luottamuksellisuus, eheys ja käytettävyys ja osittain erikseen korostaen todennuksen kiistämättömyys.

4.4.2 Salaus- ja todennusratkaisut: Suosituksia ja mahdollisuuksia

Salausratkaisut ovat mahdollistava teknologia, jonka avulla voidaan vaikuttaa tiedon luottamuksellisuuteen, eheyteen ja tietoon kohdistuvan todennuksen kiistämättömyyteen.

Salausratkaisut mahdollistavat monet tiedon hallinnan vaatimat kontrollit, ja niiden käyttöä voi ja tulisi kehittää rinnakkaisesti muiden kontrollien (erityisesti todennus) kehittämisen kanssa.

Kontrollien ja salausteknologian tuomia mahdollisuuksia mallinnetaan seuraavan kuvan avulla. Tietoaineiston hävitysmahdollisuus on jätetty esitykseen sen vuoksi, että monet tuotteet tarjoavat tämän mahdollisuuden yhtenä ominaisuutena. Vaikka valtuutusta ei toteuteta salausteknologialla, on termi valtuutus jätetty kuvaan siksi, että kontrollien luettelo olisi kattava.

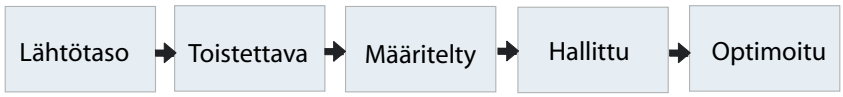


Kuvassa kokonaisella viivalla piirretyt nuolet korostavat markkinoilta saatavien ratkaisujen pääasiallisia toteutuksia. Katkoviivalla piirretyt nuolet esittävät vaihtoehtoista tapaa (”eheyden varmentaminen allekirjoituksella käyttäen epäsymmetristä salausalgoritmia”) ja erillistä ominaisuutta monissa tuotteissa (”tiedon hävitys ylikirjoittamalla”, esim. PGP -ohjelmistolla”).

4.5 Kypsyys ja kyvykkyysmallit

4.5.1 Kypsyys ja kyvykkyys

Julkishallinnon tietoturvatasoja kuvaavat Vahti-suositukset ja ohjeistukset soveltavat eri yhteyksissä mallia SSE-CMM [Capability and Maturity Model]. Tässä mallissa organisaation kyvykkyys ja kypsyys nähdään kehittyväksi ja kehitettäväksi seuraavin askelin:



Mallia voidaan hyödyntää myös salausratkaisujen käyttöönoton ohjauksessa kuvaamaan ensin organisaation nykyisiä valmiuksia yleisesti ja sitten salausratkaisun ja siihen liittyvien prosessien tavoitetilaa. Tämän ajattelun avulla organisaatio voi mallintaa, mihin sen omat rahkeet riittävät ja mitä prosesseja sen on vielä kehitettävä, kun se hyödyntää salausratkaisuja.

4.5.2 Salausratkaisut: Suositus ja mahdollisuus

Salausratkaisut vaativat käyttäjäorganisaatioilta valmiuksia ja osaamista sekä ratkaisujen hallintaan liittyvistä prosesseista että ratkaisujen teknologiasta ja yhteensovittamisesta.

Suositus ja mahdollisuus:

- Organisaation pitää ennen päätöksiä salausratkaisujen käyttöönotosta arvioida oma kyvykkyytensä tulevan ratkaisun käytössä ja hallinnassa.
- Arvioinnin tuloksia voi ja pitää käyttää myös sen hahmottamiseen, missä prosesseissa, osaamisessa tai toiminnoissa tarvitaan ulkopuolisia resursseja.

Suositus ohjaa jokaista käyttäjäorganisaatiota miettimään yhteistyön, keskittämisen ja myös ulkoistamisen mahdollisuuksia yhteensopivuuden, tehokkuuden ja turvallisuuden optimoinnissa.

4.6 Valtionhallinnon ohjeistukset tiedon hallintaan ja kontrolleihin

4.6.1 Viitedokumentit

Tiedon hallinnan ja turvaamisen tapaan liittyviä suosituksia on kirjattu eri Vahti-julkaisuihin. Tämä salauskäytäntöjä koskeva suositus liittyy läheisesti periaatteisiin tietoaineiston käsittelystä ja tietoturvatasoista.

4.6.2 Ohjeistus ja suositus tietoturvatasoista

Valtion IT-strategian toimeenpanon kärkihanke valtionhallinnon tietoturvatasoista on tuottamassa suosituksia, jotka todennäköisesti ohjaavat myös salausratkaisujen valintaa ja käyttöä. Salausratkaisut ovat tietoturvallisuuden hallintakeinoja, joihin tulee liittää arviointikriteeristö. Salausratkaisuihin liittyvän arviointikriteeristön laadintaa ja hyödyntämistä kuvataan tarkemmin tämän suosituksen luvuissa 6 ja 7.

4.6.3 Tietoaineiston käsittely ja kontrollit

Salausratkaisut voidaan nähdä tietoaineiston kontrollina, jolla on liitos muihin vaihtoehtoisiin tai täydentäviin kontrolleihin. Esimerkkejä toisiinsa läheisesti liittyvistä kontrolleista ovat salaus, todennus, valtuutus, sisällön eheyden varmennus, sekä transaktioiden varmennus ja lokitus.

Valtionhallinnossa tietoaineiston kriittisyyttä kuvaa tietoaineiston luokittelu ja käsittelyvaatimukset, joita ollaan parhaillaan kehittämässä. Tällä hetkellä voimassa olevien normien ja linjausten mukaisia suosituksia:

- Mitä kriittisempi turvaluokitus, sitä enemmän vaaditaan kaikilta kontrolleilta.
- Salauksen osalta tämä tarkoittaa sitä, että sekä teknisessä että hallinnollisessa mielessä vaatimustaso tiukentuu kun siirrytään kohti kriittisempiä turvaluokkia.
- Kriittisyyden kasvu vähentää hyväksyttävien vaihtoehtojen määrää. Mitä kriittisempi tietoaineisto on, sitä tarkemmin käytännöt tulee ohjeistaa myös tapauskohtaisesti.

Konkreettisia esimerkkejä ajattelumallin soveltamisesta näitä keskeistä periaatteita noudattaen:

- Julkiseksi luokiteltu aineisto:
  - Koska luokittelun perustana on aineiston luottamuksellisuus, niin salausteknologiaa ei oletuksena tarvita sisällön suojaamiseksi.
  - Myös julkisen aineiston alkuperäisyys ja muuttumattomuus voidaan ja tietyissä tilanteissa pitää varmentaa. Tähän voidaan käyttää esimerkiksi tiivistefunktioita, digitaalisia allekirjoituksia tai näiden yhdistelmää.

- Turvaluokat IV ja III
  - Viimeistään turvaluokassa III on suositeltava, että osapuolten identiteetti todennetaan vahvasti. Tukeutuminen vahvan todennuksen tarjoavaan todennusarkkitehtuuriin (varmenteisiin) on suositeltavaa.

  - Mikäli tiedon hyödyntäjien määrä on pieni, niin riittää yleensä se, että salausratkaisu on yhteensopiva ja sovittu kyseisen käyttäjäjoukon kesken.
  - Mikäli käyttäjien ja käyttötapojen määrä lisääntyy tai tiedon kriittisyys kasvaa, niin ratkaisujen valinnassa tulee korostaa yhteensopivuutta olemassa olevien salausratkaisujen ja todennuskäytäntöjen kanssa.
  - Sisällön muuttumattomuuden ja eheyden varmentamisen tulisi olla automaattista ja mahdollistettu valituilla ohjelmistoilla ja muilla työkaluilla.

- Turvaluokka II
  - Tällä tasolla vaaditaan mahdollisimman vahvaa todennusta ja rooli- ja tarvepohjaista valtuutusta. Integrointi vahvan todennuksen järjestelmiin on nähtävä pakolliseksi. Tämä tarkoittaa suosituksena integrointia yhteisiin todennusratkaisuihin eli valtionhallinnon tukemiin varmenneratkaisuihin.
  - Salausmenetelmän tulisi olla kaikkien tietoa käsittelevien tahojen yhteisesti hyväksymä, jotta toiminnallisuus ja turvallisuus voitaisiin taata.

- Turvaluokka I
  - Tätä turvaluokkaa koskevien käsittelysääntöjen mukaan tietoja ei saa lähettää sähköisissä tietojärjestelmissä. Integrointi yhteisiin teknisiin rajapintoihin on haasteellista tai jopa mahdotonta.
  - Jokaisen tämän turvaluokan ratkaisun on oltava erikseen hyväksytty, eikä ratkaisun prosesseissa tai tekniikassa saa tehdä kompromisseja.

Valitun ja käyttöönotetun ratkaisun toimivuus ja tarkoituksenmukaiseen pitää pystyä myös osoittamaan. Tämä voi tapahtua auditoimalla, mistä seuraavat yleiset suositukset:

- Organisaatio voi varmentaa ratkaisujensa luotettavuuden itse parhaaksi katsomallaan tavalla, mikäli tietoaineisto on luokiteltu turvaluokkaan ”julkinen” tai ”IV”.
- Viimeistään turvaluokan ”III” tietoja suojaavista ratkaisuista tulee pyytää näkemys organisaation nähden ulkopuoliselta taholta ja ne tulisi tarkistuttaa vastaavasti.
- Turvaluokkien ”II” ja ”I” tietoja suojaavat ratkaisut tulisi tarkastuttaa organisaatioon nähden riippumattomalla taholla ennen niiden hyväksymistä tai käyttöönottoa.

Mitä kriittisempi tietoaines ja mitä laajempi käyttäjäjoukko, sitä tarkemmin on varmistettava ratkaisun toimivuus.

4.7 Ohjaavat arkkitehtuurit

4.7.1 Määritelmä ja ValtIT

ICT-arkkitehtuurilla tarkoitetaan järjestelmien suunnittelua ja toteutusta ohjaavia raameja. ICT- arkkitehtuurien vertauskuvaksi sopii maankäytöllinen termi ”kaavoitus”. Molemmissa määrätään yleisilme ja raamit, mutta yksityiskohtaiselle toteutukselle jätetään liikkumatilaa.

Salausratkaisun pitää olla yhteensopiva vahvistettujen tai vahvistettavien arkkitehtuurien kanssa.

4.7.2 ValtIT kärkihankkeet ja salauskäytännöt

Monet ValtIT kärkihankkeet sisältävät liittymiä salausratkaisuihin. Esimerkkejä:

- Sähköisen asioinnin alusta ->Liitos todennukseen ja varmennukseen.
- Kansalaisten tunnistaminen ->Liitos todennukseen ja varmennukseen.
- Yritysten tunnistaminen ->Liitos todennukseen ja varmennukseen.
- Valtionhallinnon arkkitehtuuri ->Kaikkia ratkaisuja ohjaavat periaatteet.
- Integraatioratkaisu ->Liitos rajapintojen kautta.
- Virkamiehen tunnistaminen ->Liitos todennukseen ja varmennukseen.
- Dokumentinhallinta ja arkistointi ->Tarpeet kontrolleille koko elinkaaren ajalle.
- Tietoliikenneratkaisu ->Vaatimukset tietoliikenteen salaukselle.
- Sähköposti ja kalenteri ->Useita käytännönläheisiä liitoksia.
- Tietoturvatasot ->Mallit ja menetelmät monitahoisesti.

Yhteensopivuus valtionhallinnon kokonaisarkkitehtuurien ja sitä tukevien hankkeiden kanssa on aina varmistettava tapauskohtaisesti.

4.7.3 Valtionhallinnon todennuskäytännöt

Lukijaa muistutetaan aluksi termien ”tunnistus” ja ”todennus” eroista. Tunnistaminen (englanniksi identification) vastaa kysymykseen kuka tai mikä. Todennus (englanniksi authentication) vastaa väitetyn identiteetin varmentamisesta. Salausratkaisuilla ei käyttäjiä tunnisteta, mutta niiden avulla käyttäjä voidaan todentaa.

Valtionhallinnon todennus- ja tunnistuskäytäntöihin otetaan kantaa seuraavissa hankkeissa:

- Kansalaisten tunnistaminen,
- yritysten tunnistaminen ja
- virkamiehen tunnistaminen.

Nämä hankkeet tuottavat linjauksia, jotka vaikuttavat erityisesti todennuksen mahdollistaviin salausratkaisuihin. Tämän ohjeen laatimisajankohtana voidaan antaa seuraava todennäköisiin linjauksiin perustuva yleissuositus:

- Milloin henkilön todentamistarve on ilmeinen tai käyttäjäkunta laaja, tulee ratkaisun tukeutua valtionhallinnon todennusarkkitehtuureihin, esimerkkinä virkamieskortti.
  - Esimerkki: Kirjautuminen hallinnonalan järjestelmiin.
- Mikäli salausratkaisu koskee rajattua käyttäjäkuntaa tai on luonteeltaan väliaikainen, voidaan edellisestä yleissuosituksesta tinkiä tarkoituksenmukaisuuden nimissä.
  - Esimerkki: Väliaikaisen projektiryhmän dokumenttihakemisto.

Salausteknologiaan perustuvaa todennusta vaaditaan myös laitteistojen ja ohjelmistojen välillä. Näissä tilanteissa ei voida hyödyntää tavanomaista henkilön todennusmekanismia eli korttivarmennetta. Tämän vuoksi annetaan seuraava salausteknologian markkinoiden ja ratkaisujen nykytilanteen huomioiva yleissuositus:

- Kriittisten yhteyksien osalta suositellaan, että laitteistot ja ohjelmistot todentavat toisensa ennen yhteyden hyväksymistä. Tämä todennus voidaan toteuttaa ohjelmistopohjaisin varmentein. Esimerkkinä tästä protokollat, joilla mahdollistetaan sähköpostipalvelinten keskinäinen todennus.

4.7.4 Valtionhallinnon rajapinnat ja hakemistot

Rajapinnoilla ja hakemistoilla tarkoitetaan tässä yhteydessä ohjelmisto- ja tietoliikennepohjaisia ratkaisuja, jotka mahdollistavat myös salausratkaisujen liittämisen kokonaisuuteen.

Rajapintoja ja hakemistoratkaisuja määritetään esimerkiksi seuraavissa hankkeissa:

- Valtionhallinnon arkkitehtuuri.
- Integraatioratkaisu.

Salausteknologian markkinoiden ja ratkaisujen nykytilanteen perusteella voidaan antaa seuraava teknisluontoinen yleissuositus:

- Salausratkaisun avainten tai käyttäjätietojen säilytyksessä kannattaa tukeutua yleisiin hakemistoratkaisuihin ja rajapintoihin. Hyvä esimerkki tästä on LDAP.

Lisäksi kerrataan perusperiaate ja yleissuositus:

- Yhteensopivuus valtionhallinnon kokonaisarkkitehtuurien ja sitä tukevien hankkeiden kanssa on aina varmistettava tapauskohtaisesti.

4.7.5 Valtionhallinnon sähköpostiratkaisut

Julkishallinto käyttää useita erilaisia sähköpostiohjelmistoja sekä palvelimina (”server”) että näihin yhteyden mahdollistavina asiakasratkaisuina (”client”). Käytännössä on mahdotonta laatia yhteinen ja kaiken kattava yleissuositus kaikkiin yhdistelmiin ja käyttötapauksiin.

ValtIT kärkihanke sähköposti ja kalenteri ottaa kantaa linjauksiin. Syntyvä arkkitehtuuri määrää, millä tasolla ja miten erilaiset sähköpostiratkaisut ovat jatkossa tuettuja. Tätä määritystä tarvitaan, kun ohjeistetaan varmenteiden käyttöä sähköpostissa.

Valtionhallinnon yksiköt hyödyntävät kaupallisina sähköpostiratkaisuina esimerkiksi Microsoft Exchange, Lotus Notes ja Tiimiposti-ohjelmistoja. Lisäksi löytyy useita muita sähköpostiratkaisuja, joista osa perustuu kaupallisiin ja osa avoimen ohjelmistokoodin järjestelmiin.

Sähköpostijärjestelminä tulisi suosia sellaisia ratkaisuja, jotka tukevat valtionhallinnon valitsemia todennuskäytäntöjä ja erityisesti virkamies- ja kansalaisvarmenteita. Lisäksi tulisi varmistua siitä, että järjestelmät kykenevät todentamaan toisensa avoimia tietoliikenneprotokollia käyttäen.

Ulkoasiainministeriö on tuottanut salatun sähköpostin lähettämiseen ja vastaanottamiseen liittyvän ohjeistuksen Microsoft Exchange-ympäristöön. Ohjeisto ja sitä vastaavat muut materiaalit ovat Vahdin sivuilta.

4.7.6 Salausratkaisut: Suosituksia ja mahdollisuuksia

Tässä yhteydessä suositukset ja mahdollisuudet kulkevat käsi kädessä:

- Yhteensopivuus jokaisen arkkitehtuurin kanssa on aina varmistettava.
- Integrointi hakemistorakenteisiin ja yhteisiin ohjelmistorajapintoihin on aina suositeltavaa, erityisesti kun käyttäjäjoukko on laaja tai määrittämätön.

- Integrointi keskitettyihin valvonta- ja hallintajärjestelmiin on suositeltava lisäarvo.

Laajat salausratkaisut pitäisi toteuttaa keskitetysti. Jos tämä ei ole hallinnollisista tai muista syistä mahdollista, niin pitää varmistaa mahdollisimman laaja yhteensopivuus.

5 Terminologiat, teknologiat ja tekniset suositukset

5.1 Johdanto

Salausratkaisun toiminnallisuus ja luotettavuus saavutetaan, kun tiedon luonteesta ja organisaation toiminnasta johtuva tarve salaukselle ratkaistaan kontrolloitujen prosessien, riittävän osaamisen ja tarkoituksenmukaisen tekniikan avulla.

Tekniikan tarkoituksenmukaisuudella tarkoitetaan ratkaisun yhteensopivuutta, integroitavuutta, käytettävyyttä ja luotettavuutta. Näistä kriteereistä kolme ensimmäistä voidaan nähdä kaikkea valintaa ja käyttöönottoa ohjaavina arvoina, ja neljäs (tekninen luotettavuus) välttämättömänä reunaehtona. Tämä luku hahmottaa salausratkaisujen tekniikkaa ja antaa näiden perusteella suosituksia ja näkemyksiä teknisen luotettavuuden arviointiin.

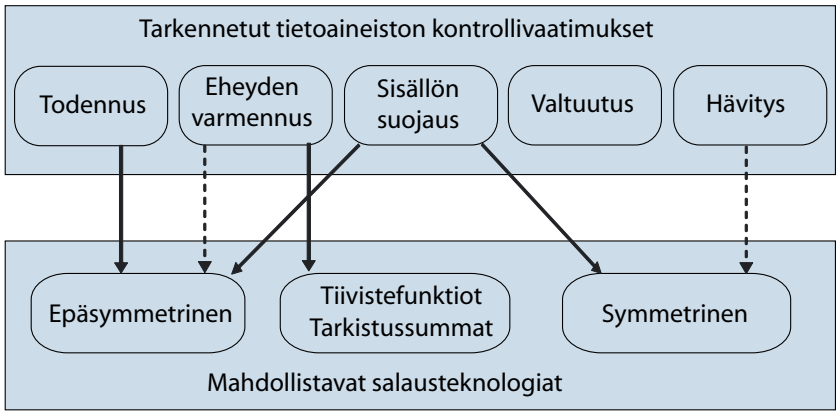
5.2 Terminologiat

Termillä salaus on suomen kielellä sivumerkityksiä, joiden painoarvo riippuu hyvinkin paljon kuulijan taustasta. Toisinaan salauksen ymmärretään tarkoittavan ainoastaan selväkielisen tiedon muuttamista suojatuksi, kun taas toisinaan termillä ymmärretään kaikkia tiedon suojaukseen liittyviä mahdollisuuksia, joiden pohjana on salausratkaisujen matemaattinen teoria. Tässä dokumentissa termillä ”salausratkaisut” tarkoitetaan tätä jälkimmäistä, laajempaa tulkintaa.

Kirjallisuudessa esiintyvät termit kryptologia, kryptografia ja kryptoanalyysi. Kryptologia on tieteenala, joka tutkii kryptografiaa eli viestien salaamista sekä kryptoanalyysia eli salausten murtamista.

Tässä ohjeessa salausratkaisuilla tarkoitetaan kaikkia kryptografian tuottamia matemaattisia menetelmiä, joiden avulla voidaan varmentaa tiedon luottamuksellisuutta ja eheyttä tai todentaa käsittelyosapuolten identiteetit. Luvun 4.4.2 mukaisesti:

- Salausratkaisut ovat mahdollistava teknologia, jonka avulla voidaan vaikuttaa tiedon luottamuksellisuuteen, eheyteen ja kohdistuvan todennuksen kiistämättömyyteen.
- Salausratkaisut mahdollistavat monet tiedon hallinnan vaatimat kontrollit, ja niiden käyttöä voi kehittää osana muiden kontrollien (erityisesti todennus) kanssa.



Tässä luvussa tai tässä dokumentissa ei avata kaikkea salaukseen liittyvää matematiikkaa. Tavoitteena on kuvaus, jonka avulla lukija ymmärtää salauksen mahdollisuudet ja rajoitukset sekä ymmärtää esityksessä annettujen suositusten taustan ja merkityksen.

5.3 Algoritmi ja avain

Salausratkaisun algoritmilla tarkoitetaan sitä matemaattista menetelmää, jonka avulla salausratkaisu ohjelmallisesti toteuttaa tietoaineiston suojauksen. Tämä algoritmi vaatii syötteekseen ainakin yhden lähtöarvon, jonka avulla matemaattinen operaatio ja laskenta toteutetaan. Tätä syötettä kutsutaan salausratkaisun avaimeksi.

Teknisesti ja matemaattisesti ajatellen, salausratkaisun luotettavuus perustuu algoritmin riittävään oikeellisuuteen ja avaimen riittävään pituuteen. Algoritmin oikeellisuuden kriteerinä voidaan pitää sitä, että sen paljastuminen ilman avaimen paljastumista ei heikennä salauksen laatua. Käytännössä tämä tarkoittaa sitä, että algoritmin tulisi olla yleisesti tunnettu.

Lähtökohtana salausratkaisujen valinnassa pidetään seuraavia suosituksia:

- Salausratkaisuissa käytettävän algoritmin tulee olla avoin, eli sen oikeellisuuden arvioinnin tulee perustua kriittiseen, avoimeen ja tieteelliseen tutkimustyöhön.
- Avainpituuden tulee olla kulloisenakin ajanhetkenä riittäväksi hyväksytty suhteessa valittuun salausalgoritmiin.

Mainitut kaksi perusperiaatetta voidaan kääntää myös toisin päin: Valtionhallinnossa tulee välttää sellaisia ratkaisuja, jotka perustuvat toimittajasidonnaisiin algoritmeihin. Edelleen, avainpituuksien riittävyys on varmistettava säännöllisesti ajantasaistettavien kriteerien mukaisiksi.

Käytännön toteutuksissa luotettavuuteen vaikuttaa myös algoritmin ohjelmoinnin oikeellisuus, sovelluksen käytön helppous ja käytön oikeellisuus, avaimen laatu ja avaimen hallintaan liittyvien prosessien tarkkuus.

5.4 Symmetrinen salaus

5.4.1 Määritelmä

Symmetrisessä (eli salaisen avaimen) salauksessa tietoaineiston salauksen purkamiseen tarvittava avain on suoraan johdettavissa salausavaimesta. Käytännössä symmetrisissä salausalgoritmeissa viesti salataan ja salaus puretaan samalla avaimella. Jos kolmas osapuoli saa tietoonsa tämän avaimen ja sitä vastaavan algoritmin, tietosisältö paljastuu. Avainten välittämiseen osapuolten välillä tarvitaan turvallinen kanava, minkä vuoksi symmetristen avainten menetelmiä kutsutaan myös salaisten avainten menetelmiksi.

Symmetrinen salausmenetelmä sopii hyvin tapauksiin, jossa salausavainta ei tarvitse siirtää, esimerkiksi käyttäjän hakemistojen tai paikallisen kovalevyn salaukseen. Symmetristen salausmenetelmien etu on salausmenetelmän nopeus. Ongelmana on avainten hallinta, käytännössä avainten välitys toiselle osapuolelle, sillä viestin lähettäjän ja vastaanottajan on etukäteen sovittava avaimesta, jota käytetään viestin salaukseen ja purkuun. Myös skaalautuvuus esimerkiksi käyttäjien lisääntyessä on hallinnollisesti ja teknisesti haastavaa.

5.4.2 Toteutukset

Symmetriset salausmenetelmät jaetaan lohko- ja jonosalausmenetelmiin. Lohkosalauksissa algoritmi käsittelee syötettä suurempina palasina eli blokkeina. Valikoituja esimerkkejä lohkosalausalgoritmeistä: AES, IDEA, Blowfish, Twofish ja 3DES.

Jonosalauksessa avaingeneraattorin tuottamaa bittivirtaa summataan jatkuvasti niin kutsutulla modulo2 menetelmällä salattavaan bittivirtaan. Valikoitu esimerkki jonosalausalgoritmista: RC4.

Edellä lyhyesti kuvatun taustamatematiikan vuoksi jonosalaus soveltuu teoriassa hieman paremmin jatkuvan tietovirran salaukseen ja lohkosalaus puolestaan paikalliseen salaukseen. Käytännössä tällä taustalla ei enää ole merkitystä, vaan tiettyjä erityistilanteita lukuun ottamatta lohkosalaukset ovat vallanneet käyttötapaukset ja niihin perustuvat myös markkinoiden tuotteet.

5.4.3 Suositukset

Salausratkaisujen luotettavuutta arvioidaan sen mukaan, miten kauan niiden avulla toteutettu luottamuksellisuuden suojaus kestää kun murtamiseen käytetään ajantasaista teknologiaa. Symmetrisissä algoritmeissa tämä aika riippuu kaikkein eniten käytetystä avainpituudesta.

Yksinkertaistettu vertailu symmetristen algoritmien vaatimista avainpituuksista suosituksineen. Taulukko perustuu seuraaviin lähteisiin: www.keylength.com, knowledge and article base. www.ecrypt.eu.org/documents/D.SPA.21-1.1.pdf.

Avainpituus (bittiä)	Yleinen esimerkki	Valtionhallinnon suositus
32	Murrettavissa reaaliaikaisesti perusvälinein.	Ei hyväksytä.
64	Murrettavissa lyhyen ajan sisällä perustietotekniikalla.	Ei hyväksytä
72	Murrettavissa lyhyen ajan sisällä perustietotekniikalla.	Ei hyväksytä.
80	Kestää teoriassa murtamisen perustietotekniikalla.	Ei hyväksytä.
96	Yleisesti katsottu ehdottomaksi minimiksi.	Ei hyväksytä.
112	Yleisesti katsottu riittäväksi minimiksi.	Ei suositella.
128	Yleisesti riittäväksi katsottu taso kaikkeen käyttöön, pois lukien erittäin kriittinen.	Hyväksytty ja suositeltava.
256	Yleisesti riittäväksi katsottu taso myös erittäin kriittiseen käyttöön.	Hyväksytty ja suositeltava

Edellisen perusteella annetaan seuraava suositus valtionhallinnossa hyväksyttävistä symmetrisistä algoritmeista avainpituuksineen:

Hyväksytyt lohkosalaukseen perustuvat symmetriset algoritmit ja vastaavat avainpituudet:

- 3DES, missä käytetään kolmea avainta (3 x 56 bittiä), voidaan hyväksyä.
- Twofish, avainpituus vähintään 128 bittiä, hyväksytty yhdistelmä.
- Blowfish, avainpituus vähintään 128 bittiä, hyväksytty yhdistelmä.
- IDEA, avainpituus vähintään 128 bittiä, hyväksytty yhdistelmä.
- AES, avainpituus 128 bittiä tai enemmän, suositeltava yleisratkaisu.
- AES, avainpituus 256 bittiä, suositeltava ratkaisu myös kriittisiin ympäristöihin.

Luettelosta kannattaa huomata, että AES on yleensä suositeltavin vaihtoehto sekä teknisistä syistä (luotettava algoritmi ja riittävät avainpituudet) että kaupallisista syistä (laajasti tuettu).

Hyväksyttyjen jonosalausten luetteloon päätyy lopulta vain yksi, ja seurantaan toinen:

- RC4, avainpituus 128 bittiä, voidaan hyväksyä sille luonteenomaisiin tilanteisiin. Lisäksi on huomioitava ongelmat ja rajoitukset. Näistä yksilöitävin on vaatimus ensimmäisten 512 bitin pudottamisesta bittivirran alkuosasta.
- SNOW, vuonna 2007 vielä tutkimusten kohteena, mutta jo lupaava vaihtoehto.

Sekä tekniset että markkinasyyt ovat johtaneet siihen, että jonosalaukset ovat jonkin verran menettäneet osuuttaan ja asemiaan. Käytännössä lohkosalauksia voidaan yleensä käyttää siellä, missä aiemmin käytettiin vain jonosalausalgoritmeja. Hyvänä esimerkkinä lohkosalauksen markkinahyväksynnän kasvamisesta on AES, mistä löytyy jopa useita piirisarjaratkaisuja.

5.4.4 Käyttötarpeita ja esimerkkejä

Symmetrinen salaus soveltuu käytännössä kaikkeen salaukseen, sillä nykyiset algoritmit ovat nopeita ja riittävillä avainpituuksilla erittäin luotettavia. Markkinoilla on useita näihin perustuvia ratkaisuja, joiden keskinäisessä vertailussa pitää kiinnittää huomioita yhteensopivuuteen, käytettävyyteen ja integrointiin. Perusluotettavuus on käytännössä yhtenevä ratkaisujen välillä.

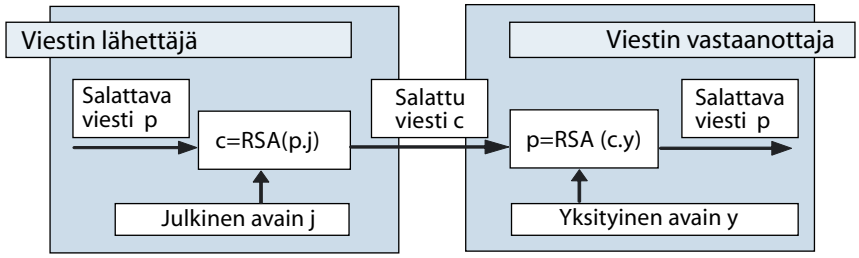
5.4.5 Tulevaisuuden näkymät

Tulevaisuus vaikuttaa hyvältä ja myös helposti ennustettavalta: Symmetristen algoritmien luotettavuus ja saatavuus on tällä hetkellä sillä tasolla, että nopeita muutoksia ei ole odotettavissa. Esimerkiksi AES-256 toimii yleensä riittävän nopeasti jo tällä hetkellä, ja salauksen katsotaan suojaavan aineistoa äärimmäisiäkin hyökkäyksiä vastaan jopa kymmeniä vuosia.

5.5 Epäsymmetrinen salaus

5.5.1 Määritelmä

Epäsymmetrisessä salauksessa käytetään avainparia, joista toinen avain on julkinen ja toinen yksityinen. Lähetettäessä tietoaineistoa (esimerkiksi sähköpostia), viesti salataan vastaanottajan julkisella avaimella ja vastaanottaja avaa viestin omalla yksityisellä avaimellaan.



Epäsymmetristä (eli julkisen avaimen salausmenetelmä) salausta käytetään yleensä varmennuksiin. Sitä voidaan käyttää todennukseen, allekirjoituksiin, avaintenhallintaan ja myös salaukseen. Epäsymmetrinen salaus on tosin hidasta, koska se edellyttää pitkiä avaimia riittävän turvallisuuden takaamiseksi. Lisäksi salatun tiedoston koko saattaa olla huomattavasti suurempi kuin alkuperäisen selväkielisen tiedon.

Epäsymmetrisen menetelmän (julkisen avaimen menetelmän) etuna on se, että suurempia määriä avaimia voidaan hallita helpommin kuin symmetristen menetelmien tapauksessa (salaisten avainten menetelmissä). Käytännössä julkinen avain voidaan aina julkistaa ja tallettaa esimerkiksi julkiseen avainhakemistoon, josta kaikki halukkaat voivat hakea sen. Yksityinen avain pidetään tallessa ja se on tarkoitettu vain haltiansa käyttöön. Julkisen avaimen käsittelyssä on voitava varmistaa, että sai oikean julkisen avaimen ja että saatu avain on voimassa.

Epäsymmetrisiä salausmenetelmiä voidaan käyttää sähköiseen asiointiin, jolloin puhutaan PKI:stä eli julkisen avaimen infrastruktuurista. Tämä on toimintamalli julkisten avainten ja varmenteiden hallinnointiin, kuten digitaaliseen allekirjoitukseen. Huomattakoon, että ”käyttäjä” voi olla paitsi luonnollinen henkilö, myös esimerkiksi yhteisö tai yritys, tai jopa tietokone, tietokoneverkko, tietokanta, tai mikä tahansa muu julkisen avaimen menetelmän laskentaan pystyvä olio, jonka haltuun yksityinen avain voidaan turvallisesti tallettaa.

5.5.2 Toteutukset

Julkisen avaimen menetelmä muodostuu algoritmista ja sitä käyttävistä avaimista. Yksi avain saattaa käyttää useita eri algoritmeja. Julkisen avaimen menetelmään perustuvat algoritmit voivat toteuttaa erityyppisiä tietoturvamekanismeja, kuten:

- allekirjoittaminen,
- avainten vaihto eli istuntokohtaisen tai sanomakohtaisen salaisen avaintiedon muodostaminen kahden käyttäjän välillä,
- käyttäjän todentaminen, ja
- kiistämättömyys.

Lähettävän tiedoston muuttumattomuus voidaan varmistaa esimerkiksi käyttämällä tiivistefunktiota ja tarkistussumman salaamista. Mikäli halutaan varmistaa myös tiedoston alkuperä, tiiviste muunnetaan lähettäjän salaista avainta käyttäen, jolloin tiedosto voidaan todennettavasti yhdistää avaimen omistajaan. Järjestelmien muuttumattomuutta voidaan seurata tekemällä eheystarkistuksia ohjelmisto- ja asetustiedostoille.

5.5.3 Yleisesti varmenteista

Epäsymmetristen algoritmien vaatima avain on bittijono, jolle on luotava samanaikaisesti mahdollisimman helppokäyttöinen, turvallinen ja luotettava säilytyspaikka. Avaimesta ja sen säilytysmuodosta käytetään usein yleisnimeä ”varmenne”.

Varmenne voi olla tiedostopohjainen tai se voidaan tallettaa jollekin laitteistolle. Tiedostoista käytettävät varmenteet ovat luontevia laitteiden ja ohjelmistojen välisen keskustelun varmentamiseksi. Henkilön varmentamiseen ja todentamiseen käytetään usein fyysistä varmenneratkaisua, tyypillisesti ratkaisua missä avaimet on talletettu nk. älykortille.

Sana ”varmenne” voi siis laajasti tarkoittaa sekä ihmisten että tietoteknisten olioiden käytettävissä olevia sekä tiedosto- että laitteistopohjaisia ratkaisuja. Liian usein käydään keskustelua varmenteista rajaten kontekstia vain ihmisten (henkilöiden) todentamiseen fyysisten ratkaisujen avulla (esimerkkinä virkamieskortti).

Varmenne toimii todisteena sille, että salausavain kuuluu tietylle oliolle, esimerkiksi ihmiselle, laitteelle tai sovellukselle. Varmenteen luotettavuus perustuu teknisten ominaisuuksien lisäksi varmenteen elinkaareen liittyvien prosessien ja toimintojen oikeellisuuteen ja tarkkuuteen. Tämän vuoksi varmenteen myöntäjä- ja ylläpitotahon toiminnan tunteminen ja sen arviointi on välttämätön osa varmenteen luotettavuuden arviointia.

5.5.4 Suositukset

Varmenteen luotettavuus perustuu tekniikan lisäksi tietoon varmenteita myöntävän ja niiden elinkaarta hallitsevan tahon toimintatavoista ja näiden tapojen oikeellisuudesta ja tarkkuudesta.

- Väestörekisterikeskus katsotaan valtionhallinnossa luotettavaksi tahoksi.
- Väestörekisterikeskuksen myöntämät varmenteet ja näiden säilytykseen käytetyt tekniset ratkaisut (esimerkiksi virkamieskortti ja kansalaisen sähköinen henkilökortti) katsotaan valtionhallinnossa luotettaviksi ja suositeltaviksi ratkaisuiksi.
- Muiden tahojen myöntämien ja hallitsemien varmenteiden käyttöön tulee suhtautua varauksella. Jokainen yksittäinen taho ja näiden tahojen hallitsemat varmenteet tulee toistaiseksi tarkistaa ja hyväksyttää luotetuiksi erikseen.
  - Varmenteita hallitsevan tahon toiminnasta ja menetelmistä täytyy löytyä yksityiskohtaiset kuvaukset.
  - Toiminta ja kuvaukset pitää pystyä auditoimaan, ja auditoinnista on saatava hyväksyttävä lausunto.
- Käyttöjärjestelmät ja monet muut laitteisto- ja ohjelmistoratkaisut antavat usein mahdollisuuden ”ottaa helposti käyttöön varmentajan”. Hyvin usein varmenteiden myöntäjiä on hyväksytty luotetuiksi järjestelmän oletusasetuksissa. Kaikkiin näihin mahdollisuuksiin ja oletusasetuksiin tulee suhtautua kriittisesti.

Luotettavuutta voidaan arvioida myös sen mukaan, miten kauan ratkaisulla toteutettu luottamuksellisuuden suojaus kestää kun murtamiseen käytetään ajantasaista teknologiaa. Usein verrataan menetelmien vaatimia avainpituuksia murtokestävyydeltään vastaavan tason antaviin symmetrisiin algoritmeihin. Seuraavassa taulukossa on tämä vertailu. Taulukko perustuu samoihin lähdemateriaaleihin kuin taulukko kappaleessa 5.4.3: (www.keylength.com, knowledge and article base. www.ecrypt.eu.org/documents/D.SPA.21-1.1.pdf). Taulukko ei ole tarkoitettu selittämään matemaattisten menetelmien eroavaisuuksia vaan ainoastaan vertaamaan eri menetelmien vaatimia avainpituuksia keskenään.

Symmetrinen salaus avain (vertailu)	Yleinen esimerkki	Alkulukuihin perustuvat menetelmät (esim. RSA)	Diskreettien logaritmien menetelmä (avain/ ryhmä)	Elliptisten käyrien menetelmät
32	Murrettavissa reaaliaikaisesti perusvälinein.	-	-	-
64	Murrettavissa lyhyen ajan sisällä perustietotekniikalla.	816	128 / 816	128
72	Murrettavissa lyhyen ajan sisällä perustietotekniikalla.	1008	144 / 1008	144
80	Kestää teoriassa murtamisen perustietotekniikalla.	1248	160 / 1248	160
96	Yleisesti katsottu ehdottomaksi minimiksi.	1776	192 / 1776	192
112	Yleisesti katsottu riittäväksi minimiksi	2432	224 / 2432	224
128	Yleisesti riittäväksi katsottu, pois lukien erittäin kriittiset.	3248	256 / 3248	256
256	Yleisesti riittäväksi katsottu myös erittäin kriittiseen käyttöön.	15424	512 / 15424	512

Taulukon mukaisesti AES-256 symmetrisen salauksen murtokestävyys saavutettaisiin yleisesti käytössä olevalla RSA-algoritmilla vasta kun avainpituudeksi otettaisiin 15424 bittiä. Näin suurten bittimäärien vaatima laskentateho olisi jo liikaa tavanomaisilla työasemille. Teoriassa olisi siis suositeltavaa siirtyä sellaisiin epäsymmetrisiin algoritmeihin, joissa vaatimukset avainpituuksille olisivat lievempiä. Pienimpiä avainpituuksia tarvitaan elliptisten käyrien matematiikassa.

Edellä kuvattu ja taulukossa esitetty vertailu koskee vain luottamuksellisuuden varmistamista salauksen murtokestävyyden avulla. Jos luottamuksellisuus menetetään heikon avainpituuden vuoksi, niin se on menetetty lopullisesti. Jos kyseessä on muu tietoturvallisuuden tavoite, kuten kiistämättömyys, käyttäjän todentaminen tai viestin todentaminen (message authentication), niin vähempikin riittää. Jos käytetty avainpituus tulee epäluotettavaksi, voidaan tietoturvatoiminnot tehdä uudelleen suuremmilla avainpituuksilla.

Mikäli edellä esitettyyn taulukkoon laitettaisiin suojatason mukaisesti vastaavat kannanotot kuin mitä annettiin symmetristen algoritmien osalta (kappale 5.4.3), niin käytännössä mitkään yleiset ratkaisut eivät olisi vastaavien suositusten mukaisesti riittävän luotettavia luottamuksellisuuden suojaamiseen.

Suosituksissa pitää painottaa menetelmien etuja ja yhteiskäyttöä.

Merkittävä ratkaisujen kokonaissuunnittelua linjaava suositus:

- Epäsymmetriset algoritmit ovat parhaimmillaan todennuksessa ja symmetriset puolestaan tehokkaita ja luotettavia tietoaineiston salauksessa. Kaikissa tilanteissa ja ratkaisuissa pitäisi pyrkiä siihen, että näitä vahvuuksia hyödynnetään juuri näin.
- Tulee siis pyrkiä ratkaisuihin, missä todentaminen pohjautuu valtionhallinnon todennusarkkitehtuurin mukaisiin epäsymmetrisiin ratkaisuihin ja luottamuksellisuuden suojaus tapahtuu symmetristen algoritmien ratkaisuilla.

Suositukset varmenteiden ja epäsymmetristen salausalgoritmien osalta:

- Suosituksena annetaan tukeutuminen valtionhallinnon yleisten rajapintaohjeiden ja arkkitehtuurien kanssa yhteensopiviin ratkaisuihin, esimerkiksi virkamieskortteihin.
- Suositellaan, että RSA-algoritmia pitää käyttää uuden standardin PKCS#1v2.1 mukaisesti.

Teorian mukainen suositus voisi olla se, että pyritään ainakin tulevaisuudessa tukeutumaan esimerkiksi elliptisten käyrien matematiikkaan perustuviin ratkaisuihin. Käytännössä tämä ei ole mahdollista, koska tuotevalikoima markkinoilla on ainakin toistaiseksi hyvin rajallinen.

5.5.5 Käyttötapausesimerkkejä

Toiminnan ja sen kehittämisen kannalta oleellisia ratkaisuja suunnitellaan ja linjataan esimerkiksi ValtIT kärkihankkeina ja muutenkin osana valtionhallinnon arkkitehtuuriuudistuksia. Näistä monissa korostetaan todennusta ja teknologisena pohjana varmenneratkaisuja.

Tiedostomuotoisia varmenteita voidaan hyödyntää miltei aina, kun halutaan varmentaa kahden rajapinnan välisen kommunikoinnin kiistämättömyys. Esimerkiksi sähköpostipalvelimet voivat todentaa toisensa ohjelmistovarmenteiden avulla.

5.5.6 Tulevaisuuden näkymät

Epäsymmetristen salausten tekniset haasteet on tiedostettu, minkä vuoksi lähitulevaisuudelta voisi olettaa merkittäviä muutoksia. Näin ei ilmeisesti kuitenkaan käy, sillä muutokset tällä alalla ovat hitaita. Nykyiset ongelmat ja haasteet on tiedostettava.

5.6 Tiivistefunktiot

5.6.1 Määritelmä

Tiivistefunktioiden avulla varmistetaan tietoaineiston muuttumattomuus tuottamalla alkuperäisestä sisällöstä periaatteessa ainutkertainen ”tarkistussumma”. Tiivistefunktio on yhdensuuntainen, eli alkuperäisestä dokumentista muodostuu samalla algoritmilla ja salausavaimella aina sama tiiviste, mutta tiivisteestä ei voida johtaa alkuperäistä.

5.6.2 Toteutukset

Tiivistefunktioiden kehittämistä ei ole historiallisesti kontrolloitu yhtä kriittisesti kuin symmetristen ja epäsymmetristen algoritmien kehitystyötä. Tästä johtuu se, että useat tiivistefunktiot ovat ajan myötä osoittautuneet epäluotettaviksi.

5.6.3 Suositukset

Tiivistefunktion laskenta ei vielä takaa alkuperäisyyttä. Mikäli ulkopuolisella taholla on pääsy sekä tiivisteeseen että alkuperäiseen tietoaineistoon, niin ulkopuolinen voi laskea uuden tiivisteen ja korvata alkuperäisen uudella. Näin tiivisteen ja alkuperäisen yhteys on matemaattisesti oikea, mutta eheys on murrettu. Tiiviste on siis salattava, jotta muuttumattomuudesta voidaan olla varmoja. Tiivisteen voi myös säilyttää erillään alkuperäisestä dokumentista.

Tiivistefunktioiden algoritmeista annetaan kaksi suositusta:

- Tiivistefunktiona tulisi käyttää seuraavia algoritmeja ja avainpituuksia: SHA-256, SHA-384 ja SHA-512.
- Valitun tiivistefunktion avainpituuden tulisi olla kaksinkertainen verrattuna siihen symmetrisen algoritmin avainpituuteen, mitä käytetään vastaavan tiedon salaukseen.

Käytännössä tämä suositus voidaan yhdistää symmetristen algoritmien kohdalla esitettyyn:

- AES-128 ja SHA-256 antavat suojatun ja sisältöeheydeltään tarkistettavissa olevan paketin. Tämä taso riittää tällä hetkellä (2008) useimmille valtionhallinnon organisaatioille.
- AES-256 ja SHA-512 antavat tämän hetkisen näkemyksen mukaan riittävän kokonaiskontrollin myös kriittiselle tietoaineistolle. Tätä yhdistelmää

on syytä käyttää, milloin se tapauskohtaisesti on mahdollista ja tarkoituksenmukaista.

Annetun bittimääräsuosituksen takana on matemaattinen teoria, josta kansanomaisesti voidaan käyttää nimeä ”syntymäpäiväefekti”: Mitä useampi henkilö on samassa huoneessa, sitä todennäköisemmin ainakin kahdella heistä on sama syntymäpäivä – ja henkilöiden määrän lisääntyminen lisää tätä todennäköisyyttä. Jotta eri tietoaineistoilla ei olisi liian usein samaa tiivistesummaa, niin tarvitaan tässä annettua kahdenkertaisen avainpituuden suositusta.

Monet sovellukset käyttävät edelleen osana toimintojaan tiivistefunktioita, joita ei enää pidetä täysin luotettavina, esimerkiksi MD5 tai SHA-1. Tästä syntyy pieni ristiriita suosituksen ja käytännön mahdollisuuksien välille. Tämä on tiedostettava.

5.6.4 Käyttötapausesimerkkejä

Näihin kuuluvat kaikki tilanteet, missä halutaan varmentaa tietoaineiston muuttumattomuus ja eheys. Tarkistus liitetään usein osaksi digitaalista allekirjoitusta, samoin sähköpostin salausta.

5.6.5 Tulevaisuuden näkymät

Tiivistefunktioiden kehittämisestä on käynnissä kansainvälinen kilpailu, jonka avulla tähän käyttötarkoitukseen toivotaan uusia, testattuja ja tutkittuja menetelmiä noin vuodeksi 2012. Tämän vuoksi voidaan sanoa, että tilanne ja tekniikka tulevat varmasti muuttumaan lähivuosina. Toistaiseksi pyritään noudattamaan kohdan 5.6.3 suosituksia.

5.7 HSM-moduulit ja muut integroidut komponentit

Kokonaisratkaisun teknisestä näkökulmasta katsoen salaus on vain yksi erityistoiminto. Esimerkiksi suojatun tietoliikenneyhteyden (VPN) toteuttamiseen tarvitaan IP-protokollan hallintaa, ei pelkästään salauksen toteuttamista.

Monissa kaupallisissa ratkaisuissa salaustoiminto toteutetaan erillisen, tätä tarkoitusta varten suunnitellun ja rakennetun moduulin (HSM – Hardware Security Module) tai ohjelmiston osaksi liitetyn, jopa erillisistä lähteistä haetun ohjelmistokirjaston avulla.

Mikäli kokonaisratkaisu perustuu integroituun ohjelmistokomponenttiin tai HSM-moduulin, pitää tämän moduulin toiminnallisuus pystyä todentamaan

erikseen. Suositukseksi annetaan FIPS-140 kriteeristön kulloinkin ajantasaisen version mukainen hyväksyntä tai osoitus siitä, että vastaavat kriteerit täytetään. (FIPS-140, Security Requirements for Cryptographic Modules. National Institute of Standards and Technology, U:S Department of Commerce).

5.8 Kriteerejä ja suosituksia

5.8.1 Kriteeristö: FIPS 140-2 ja FIPS 140-3

FIPS- (Federal Information Processing Standards Publications) julkaisu 140 esittelee ja käsittelee salausmodulien toiminnallisuuteen ja turvallisuuteen liittyviä kysymyksiä. (FIPS-140, Security Requirements for Cryptographic Modules. National Institute of Standards and Technology, U:S Department of Commerce).

Koska salausratkaisulla rakennetaan luottamusta ja turvallisuutta, pitää ratkaisun oma turvallisuus ja luotettavuus olla tiedossa. FIPS-hyväksyntää suositellaan kriteeriksi myös valtionhallinnossa. Koska kaupallisen tuotteen FIPS-hyväksynnän saaminen on suhteellisen pitkä prosessi, ei tätä suositusta voida antaa välttämättömänä. Kriteeristön mukaisia yksityiskohtia pitäisi kuitenkin pystyä varmentamaan myös tapauskohtaisesti.

FIPS140 julkaisusta ilmestyi uusi versio FIPS 140-3 syksyllä 2007. Mainittakoon, että siinä kiinnitetään edellistä versiota enemmän huomiota myös fyysiseen turvallisuuteen osana salausratkaisun turvallisuutta. Salausratkaisu itsessään pitää suojata kokonaisuutena.

5.8.2 Yksittäisiä kriteerejä ja suosituksia

Seuraavassa luetellut kriteerit ovat valikoituja esimerkkejä ratkaisujen toimittajille suunnattavista teknisesti yksityiskohtaisista kysymyksistä. Lista ei ole tarkoitettu kattavaksi, mutta jokaista esitettyä kriteeriä voidaan pitää suosituksena, kun etsitään hyvää salausratkaisua.

- Onko algoritmi avoin, yleisesti tunnettu ja hyväksytty käyttötarkoitukseen?
- Onko algoritmin ohjelmistototeutus tehty oikein? Miten tämä osoitetaan?
- Voiko ratkaisun komponentteja ja toimintoja päivittää tai korvata? Voiko esimerkiksi algoritmin toteuttavan ohjelmisto-moduulin korvata toisella toteutuksella?
- Mihin algoritmiin ja toteutukseen perustuu ratkaisun satunnaislukujen todellinen satunnaisuus? Miten tämä on osoitettavissa? Voiko satunnaislukugeneraattorin vaihtaa? (Tämä kriteeri on erittäin tärkeä, sillä avaimet ovat satunnaislukuja).

6 Käyttötarvekuvaukset, suositukset ja tarjonnasta

6.1 Käyttötarpeiden kuvaaminen ja vaatimusten hierarkia

Tietoteknisille ratkaisuille asetettavat vaatimukset jaetaan toiminnallisiin ja yleisiin vaatimuksiin. Toiminnalliset vaatimukset muotoillaan käyttötarvekuvausten avulla.

Salausratkaisuille asetettavien vaatimusten määrittely tehdään vastaavasti. Vaatimusten kuvaamisessa voidaan hyödyntää vaatimusmäärittelyn hierarkiaa (luku 4.2).

- Salausratkaisun välttämättömyys tai tarpeellisuus perustuu ensisijaisesti tiedon laatuun.
- Tietoaineiston elinkaaren vaatimat kontrollit riippuvat tiedon luokittelusta ja luokittelun vaatimasta käsittelystä. Kriittisimmän tiedon suojaamisen tarve lähtee julkishallintoa ohjaavasta lainsäädännöstä.
- Tavoiteltava yhteensopivuus arkkitehtuurien kanssa antaa vaatimuksia salausratkaisun ja sen hallintaan liittyvien tekniikoiden ja prosessien yhteisille rajapinnoille.
- Tarve- ja tilannekohtaisuus antaa lopullisen liikkumavaran, minkä puitteissa voidaan tehdä valinta vaihtoehtoisten tekniikoiden, tuotteiden ja toimittajien välillä.
- Käyttötarvekuvauksessa pitää yksilöidä myös:
  - Tiedon tallentajat ja/tai lähettäjät (henkilö, laitteisto, ohjelmisto).
  - Tiedon vastaanottajat ja/tai hyödyntäjät (henkilö, laitteisto, ohjelmisto).

Mitä tarkemmin ja kiistattomammin käyttötarve kuvataan, sitä tarkemmin voidaan ohjata ja ohjeistaa salausratkaisun valintaa, käyttöönottoa ja hyödyntämistä. Tärkeitä yksityiskohtia ovat suojattavan tiedon kriittisyys, toiminnan ja tilanteen erityispiirteet ja käytön laajuus.

6.2 Käyttötarpeiden luokittelu

6.2.1 Käyttötarpeiden luokittelun malli

Tässä ohjeessa salausratkaisujen käyttötarpeet jaetaan seuraavasti:

- Todentamista vaativat käyttötarpeet.
- Yhteyksien suojaamista vaativat käyttötarpeet.
- Tiedoston tai tietosisällön suojaamista vaativat käyttötarpeet.

Yksittäinen tilanne vaatii harvoin vain yhtä edellisistä vaan usein ainakin kahta, ja tietyissä tilanteissa kaikkia kolmea. Käytännössä miltei kaikissa tilanteissa tarvitaan todennusta.

6.2.2 Todentamista vaativat käyttötarpeet

Todennuksella tarkoitetaan sen asian varmentamista, että tiedon hyödyntäjä tai yhteyden muodostaja on identiteetiltään se joksi hänet oletetaan.

Tärkeä epäsymmetrisen salauksen käyttömahdollisuus on varmenteiden avulla tapahtuva todentaminen. Tätä hyödynnetään seuraavissa tilanteissa:

- Henkilön todentaminen varmenteen avulla useissa erilaisissa tilanteissa.
- Laitteiden tai ohjelmistojen välinen todentaminen yhteyden muodostamiseksi.

Monet käyttötarpeet perustuvat seuraavan kaltaiseen ratkaisumalliin:

- Symmetrisen salausavaimen suojaus perustuu epäsymmetrisen salausavaimen hyödyntämiseen todennuksessa. Esimerkkejä: VPN-yhteyksien avaus, sähköpostin salaus.

Kaikissa todentamista vaativissa käyttötapauksissa kannattaa aktiivisesti hyödyntää julkishallinnon tukemia ja todennusarkkitehtuurin kanssa yhteensopivia varmenneratkaisuja.

Salausratkaisun yhteensopivuus ja liitettävyys julkishallinnon tukemaan varmennearkkitehtuuriin on aina ratkaisun käyttöä ja käyttöönottoa vahvasti puoltava tekijä. Jos salausratkaisu ei mahdollista tätä yhteensovittamista, niin sen pitää tarjota muita selkeitä lisäarvoja.

Monissa kaupallisissa tai avoimen lähdekoodin ratkaisuissa tämä tavoiteltu liittäminen voidaan toteuttaa esimerkiksi hakemistointegroinnin (LDAP) avulla. Käytännössä tämä perustuu yksityiskohtaiseen suunnitteluun ja tarkkaan parametrointiin, mikä ei kaikkien tuotteiden osalta ole edes mahdollista. Myös tämän vuoksi yhteensopivuuden selvittäminen on tärkeää.

6.2.3 Yhteyksien suojaamista vaativat käyttötarpeet

Yhteyksien suojaamisella tarkoitetaan tässä kaikkia niitä tilanteita, joissa tietosisältöä siirretään kahden pisteen välillä mitä tahansa viestintäkanavaa käyttäen.

Yhteistä näille käyttötapauksille on usein se, että salauksen toteuttaa laitteisto tai ohjelmisto käyttäjän kannalta läpinäkyvästi. Yhteyksien avaamisen vaatima todennus vaatii tietyissä tianteissa toimenpiteitä käyttäjältä (henkilöltä), mutta monissa tapauksissa tämä todennus laitteiden tai ohjelmistojen välillä tapahtuu automaattisesti tietoliikenneratkaisujen avulla.

Esimerkkejä ja suosituksia tärkeimmistä yhteyksien suojaamista vaativista käyttötapauksista:

Käyttötapaus	Kuvaus tai esimerkki	Suositukset	Lisäarvot	Esimerkkejä
Lähde: IP-yhdyskäytävä Kohde: IP-yhdyskäytävä	Organisaatioiden välisen tietoliikenteen salaus.	Avoimia standardeja [esimerkiksi IPSec] tukevat ja markkinoiden kypsäksi osoittamat ratkaisut.	Yhteensopivuus ja integrointi julkishallinnon varmenneratkaisuihin. Yhteensopivuus ja integrointi hallintajärjestelmiin.	Kaupalliset ja avoimen lähdekoodin IPSEC-ratkaisut.
Lähde: Päätelaite Kohde: IP-yhdyskäytävä	Etäkäyttöyhteys, missä yhteyden ensimmäinen terminointi tapahtuu organisaation yhdyskäytävässä.	Vahvan todennuksen integroinnin mahdollistavat, avoimia standardeja tukevat ja markkinoiden kypsäksi osoittamat ratkaisut.	Yhteensopivuus ja integrointi julkishallinnon varmenneratkaisuihin. Yhteensopivuus ja integrointi hallintajärjestelmiin.	Kaupalliset ja avoimen lähdekoodin IPSEC-ratkaisut. Kaupalliset ja avoimen lähdekoodin SSL/VPN-ratkaisut.
Lähde: Päätelaite Kohde: Palvelu	Järjestelmän vastuuhenkilön muodostama etäkäyttöyhteys, missä salataan koko tietoliikenne vastuuhenkilön työasemalta kohdejärjestelmään.	Vahvan todennuksen integroinnin mahdollistavat, avoimia standardeja tukevat ja markkinoiden kypsäksi osoittamat ratkaisut.	Yhteensopivuus ja integrointi julkishallinnon varmenneratkaisuihin. Yhteensopivuus ja integrointi hallintajärjestelmiin.	Kaupalliset ja muut ratkaisut, esimerkkinä SSH ja OpenSSH.
Lähde: Ohjelmisto Kohde: Ohjelmisto	Sähköpostipalvelinten välinen todennus ja liikenteen suojaus.	Varmenteisiin perustuvat ja avointen standardien mukaiset ratkaisut	Yhteensopivuus ja integrointi julkishallinnon varmenneratkaisuihin. Yhteensopivuus ja integrointi hallintajärjestelmiin.	Sähköpostiesimerkissä TLS-suojaus. Yleisesti SOA-palveluväylän kautta tapahtuva todennus, avainten vaihto ja tietoliikenteen suojaus.
Muu kuin IP-pohjainen viestintä	Puhelin tai telekopio.	Tapauskohtaisesti tutkitut tuotteet ja ratkaisut.	Ratkaisun avoimuus.	Yksittäiset tuotteet, jotka hyväksytään tapauskohtaisesti.

Näihin käyttötarpeisiin löytyy useita kaupallisia ja avoimen lähdekoodin ratkaisuja ja markkinatilanne on ostajan kannalta hyvä. Tuotteet ja palvelut ovat kypsiä, niitä löytyy eri valmistajilta ja toimittajilta ja ne ovat yleensä myös keskenään yhteensopivia. Hyvä esimerkki kaikesta tästä on VPN-ratkaisut.

Erityisviestinnän ratkaisuissa (puhelin, gsm, telekopio, videoneuvottelu jne.) joudutaan vielä tekemään erillisiä päätöksiä, koska toimittajia ja ratkaisuja on vähän ja toiminnot perustuvat suljettuihin moduuleihin (HSM). Näiden laadun ja toiminnallisuuden tutkiminen ja takaaminen on haastavaa, ja joissakin ratkaisuissa jopa salausalgoritmit ovat suljettuja.

6.2.4 Tiedoston tai tietosisällön suojaamista vaativat käyttötarpeet

Näillä tarkoitetaan niitä tilanteita, missä suojattava tietoaines säilytetään talletettuna tiedostona joko pysyvästi tai väliaikaisesti, esimerkiksi ennen tiedon siirtämistä.

Yksittäisiä käyttötarpeita on useita. Nämä tapaukset eroavat toisistaan mm. käyttäjämäärän laajuuden (oma, jaettu) ja tiedoston topologisen sijainnin (paikallinen, verkko, mobiili) suhteen.

Esimerkkejä ja suosituksia tiedoston ja tietosisällön suojaamista vaativista käyttötapauksista:

Käyttötapaus	Kuvaus / esimerkki	Suositukset	Lisäarvot	Esimerkkejä
Yksittäisten tiedostojen suojaaminen paikallisessa mediassa.	Tiedoston tai hakemiston suojaaminen USB-muistitikulla, CD- tai DVD-mediassa tai muussa liikutettavassa mediassa.	Avoimia standardeja tukevat, markkinoiden kypsäksi osoittamat ratkaisut.	Helppokäyttöisyys. Mahdollisuus estää salaamaton / suojaamaton toiminta. Keskitetty hallinta ja integrointi todennusratkaisuihin.	Monia yksittäisiä ratkaisuvaihtoehtoja.
Yksittäisten tiedostojen suojaaminen tietoverkkoyhteyden takana olevassa mediassa.	Hakemiston ja/ tai tiedoston salaus symmetrisellä algoritmilla.	Avoimia standardeja tukevat, markkinoiden kypsäksi osoittamat ratkaisut.	Helppokäyttöisyys. Mahdollisuus estää salaamaton / suojaamaton toiminta. Keskitetty hallinta ja integrointi todennusratkaisuihin.	Monia yksittäisiä ratkaisuvaihtoehtoja.
Henkilökohtaisen työaseman tai muun laitteen [PDA] sisältämien tietojen suojaus.	Koko median salaus symmetrisellä algoritmilla.	Avoimia standardeja tukevat, markkinoiden kypsäksi osoittamat ratkaisut.	Helppokäyttöisyys. Mahdollisuus estää salaamaton / suojaamaton toiminta. Keskitetty hallinta ja integrointi todennusratkaisuihin..	Muutamia selkeitä vaihtoehtoja.
Määrätyn käyttäjäjoukon kesken jaettavan tiedon suojaaminen.	Hakemiston ja/tai tiedoston salaus symmetrisellä algoritmilla ja avaimen suojaus todennuksella (varmenteella).	Avoimia standardeja tukevat, markkinoiden kypsäksi osoittamat ratkaisut.	Helppokäyttöisyys. Mahdollisuus estää salaamaton / suojaamaton toiminta. Keskitetty hallinta ja integrointi todennusratkaisuihin.	Yksittäisiä ratkaisuvaihtoehtoja.
Yhteiskäyttöisten [työryhmä]-ohjelmistojen avulla jaettavan tiedon suojaaminen.	Plug-in ohjelmistot tai erilliset ohjelmistot, jotka mahdollistavat tiedo[sto]n talletta-misen salattuna.	Avoimia standardeja tukevat, markkinoiden kypsäksi osoittamat ratkaisut.	Helppokäyttöisyys. Mahdollisuus estää salaamaton / suojaamaton toiminta. Keskitetty hallinta ja integrointi todennusratkaisuihin.	Yksittäisiä ratkaisuvaihtoehtoja.
Yksittäisen tietoaineiston suojaaminen palvelujen sisällä [tietokantataso].	Erityisohjelmistot tietokantojen sisältämien tietoalkioiden suojaamiseen.	Tapauskohtaisesti toimiva ratkaisu.	Hallinta, integrointi.	Salausmahdollisuus tietokantaohjelmiston optiona lisääntyvä mahdollisuus. Rajallinen määrä kapean fokuksen tuoteratkaisuja.

Tiedoston tai hakemiston suojaamiseen on saatavilla useita kaupallisia ja avoimen lähdekoodin ratkaisuja, joiden perustoiminnallisuus on kunnossa. Jos käyttäjälle tai käyttävälle ryhmälle riittää se, että suojaus perustuu ratkaisun kysymään käyttäjätunnukseen ja salasanaan, niin markkinoiden valikoima on runsas alkaen yksittäisistä USB-muistitikuista päätyen projektikansioiden suojausratkaisuihin. Kun halutaan liitettävyyttä keskitettyihin todennus- ja valvontaratkaisuihin, niin vaihtoehtojen määrä putoaa. Trendi on kuitenkin selvä ja hankkijan kannalta positiivinen: Mahdollisuus integrointiin esimerkiksi MS Active Directoryn kautta on yhä useammin tuotteen ja ratkaisun ominaisuus. Tapauskohtaista selvitystä suositellaan.

Ratkaisut kaiken tietoaineiston salaamiseen kovalevyllä ovat kypsiä ja näistä löytyy ostajalle vaihtoehtoja. Markkinoiden tuotteet ja ratkaisut tarjoavat myös rajapintoja todennusratkaisuihin. Myös keskitetty hallinta alkaa olla toimiva vakio-ominaisuus näissä tuotteissa.

Yksittäisen tietoaineiston suojaaminen tietokannan sisällä on edelleen pieni haaste. Salausmahdollisuudet tietokannan optiona ovat lisääntymässä, mutta kokemukset näistä ovat edelleen rajalliset. Tapauskohtaista selvitystä suositellaan.

Salausratkaisujen yleistymisestä kertoo omaa kieltään se, että myös varmuuskopiointiohjelmistot kykenevät nykyään tiedon salaamiseen. Tätä yksityiskohtaa ei korosteta tässä ohjeessa, mutta se esitetään selvänä esimerkkinä yleisestä trendistä: Salaus integroituu ratkaisuihin.

6.3 Varmenteet ja sähköposti

6.3.1 Johdanto

Sähköposti on perusluonteeltaan haavoittuva palvelu. Ilman erityisratkaisuja ei voida taata viestinnän osapuolten kiistämättömyyttä, viestinnän luottamuksellisuutta, viestien eheyttä eikä lähetetyn viestin saapumista vastaanottajalle.

Sähköposti on kuitenkin yksi eniten käytetyistä palveluista sekä valtionhallinnon sisäisessä viestinnässä että yhteydenpidossa ulkoisten sidosryhmien kanssa. Koska sähköpostin käytön laajuus ja kriittisyys lisääntyvät jatkuvasti, pitää sähköpostin hyödyntämistä ohjata.

Tässä dokumentin osassa otetaan kantaa niihin kysymyksiin, mihin voidaan vastata epäsymmetristen salausalgoritmien ja varmenteiden tuomien mahdollisuuksien avulla. Esitys linjaa tavoitteita, mutta näiden saavuttamiseksi tarvitaan paljon erillistä taustatyötä.

6.3.2 Käyttäjälähtöinen näkökulma

Käyttäjä voi hyödyntää salausteknologiaa seuraaviin tarkoituksiin vastaavin perustekniikoin.

- Viestin allekirjoittaminen digitaalisesti -> Epäsymmetrinen salausalgoritmi.
- Viestin eheyden varmentaminen -> Tiivistefunktiot.
- Viestin luottamuksellisuuden suojaus -> Symmetriset salausalgoritmit.

Sähköpostin salaukseen tarkoitetut kaupalliset ja avoimet ratkaisut antavat yleensä mahdollisuuden näihin kaikkiin. Kokonaistoiminto toteutetaan näissä seuraavasti:

- Eheyden varmentamista varten viestistä lasketaan ”tarkistesumma” tiivistefunktiolla.
- Viesti ja tarkistesumma salataan symmetrisellä algoritmilla. Tässä toiminnossa käytettävä avain suojataan vastaanottajan julkisella avaimella, siis epäsymmetrisellä algoritmilla.
- Viesti allekirjoitetaan omalla salaisella avaimella, eli esimerkiksi varmenteen sisältämällä epäsymmetrisellä algoritmilla. Näin vastaanottaja pystyy todentamaan lähettäjän.

Käyttäjä tarvitsee tekniikan, jolle asetetaan seuraavat perusvaatimukset ja suositukset:

- Mahdollistaa edellä kuvatut toiminnot (eheystarkistus, salaus, allekirjoitus).
- Helppo käyttää ja integroitavissa omaan sähköpostiohjelmistoon.
- Yhteensopiva vastaanottajan järjestelmien ja toimintatapojen kanssa.
- Toimii halutulla tavalla erilaisissa virhe- tai huolimattomuustilanteissa.
- Täyttävät tekniset perusvaatimukset esimerkiksi algoritmitasolla.

Mikään markkinoilta löytyvä ratkaisu ei täytä kaikkia esitettyjä vaatimuksia ympäristössä, mistä löytyy useita käyttäjäohjelmistoja (client), missä käytetään sähköpostin lukemiseen myös selaimia, missä hyödynnetään useita sähköpostijärjestelmiä (”server”), ja mikä hallinnollisesti koostuu useista itsenäisistä organisaatioista ja useista erilaisista tavoista käyttää järjestelmiä.

Varmennekäytännöt selkeyttävät tilannetta, vaikka kaikkiin haasteisiin ei vastatakaan.

6.3.3 Järjestelmälähtöinen näkökulma

Sähköpostipalvelimilta (”server”) voidaan vaatia seuraavia perustoimintoja:
- Käytettävissä useilla vaihtoehtoisilla pääteohjelmistoilla (”client”).
- Tukee myös selainpohjaista käyttöä (”web based access”).
- Todentavat viestinnän osapuolet myös palvelintasolla.
- Toiminnallisesti yhteensopiva sekä järjestelmä- että käyttäjätasolla.

Ensimmäinen ja toinen vaatimus pelkistyy tietoliikennerajapintojen vakiointikysymykseksi. Käytännössä tilanne on kuitenkin sellainen, että vain tietyt yhdistelmät toimivat kaikin ominaisuuksin. Erityisesti milloin sähköpostitoimintojen lisäksi halutaan kattaa samalla teknologialla myös kalenteriratkaisut, törmätään merkittäviin epäyhteensopivuusongelmiin. Ilman järjestelmien vakiointia ei näihin tilanteisiin voida antaa kattavia suosituksia tai ratkaisuja.

Viestinnän osapuolten todentamiseen järjestelmätasolla löytyy standardit ja ratkaisut, jotka ovat kohtuullisesti hyödynnettävissä myös käytännössä. Näiden osalta voidaan esittää tarkkoja ratkaisuvaihtoehtoja ja antaa vastaavia suosituksia.

Toiminnallinen yhteensopivuus muodostuu haasteeksi, kun sähköpostijärjestelmiltä vaaditaan monitasoista tietoturvallisuutta, minkä pitää sisältää salausteknologian tarjoamien mahdollisuuksien lisäksi esimerkiksi roskapostien ja aktiivisen häirinnän suodattamista. Nämä kysymykset on rajattu kokonaan tämän ohjeen ulkopuolelle. Joka tapauksessa, teknisten tietoturvaratkaisujen integrointi alkaa topologian suunnittelusta, ja osana tätä suunnittelua on tehtävä linjaavia päätöksiä myös salausratkaisujen topologisista ulottuvuuksista.

6.3.4 Valtionhallinto, varmenteet ja sähköposti

Kohdissa 6.3.2 ja 6.3.3 tiivistetyt reaalimaailman ongelmat ja haasteet kumuloituvat valtionhallinnon kaltaisessa erityisen kirjavassa ympäristössä. Ilman järjestelmä- ja sovelluskirjon karsintaa ei ole mahdollista saavuttaa kaikkia esille nostettuja tavoitteita.

Varmenteet antavat välittömästi seuraavat kehittämis- ja kehittymismahdollisuudet:
- Mahdollisuuksien tarjoaminen, valittujen kehityslinjojen ja arkkitehtuurien vahvistaminen.
- Vakioiduissa ympäristöissä tapahtuva käyttäjien salausratkaisujen tehokas harmonisointi.
- Salauskäytäntöjen osittainen harmonisointi ja tehostaminen eri ympäristöjen välillä.

- Palvelimien välisen liikenteen todentaminen ja salaus vakioiduksi käytännöksi.
- Rajapintoja ja vaihtoehtoisia ratkaisuja sidosryhmien väliseen viestintään.

Näiden tavoitteiden saavuttamiseksi tarvitaan yhteisiä valtionhallinnon tasoisia päätöksiä.

6.3.5 Suosituksia ja mahdollisuuksia

Varmenteiden tuomiin mahdollisuuksiin liittyviä strategisia suosituksia ja linjauksia, jotka voivat ohjata kaikkien salausratkaisujen valintaa ja käyttöönottoa:

- Kaikissa vahvaa todentamista vaativissa käyttötapauksissa tulee ensisijaisesti tukeutua valtionhallinnon tukemiin ja keskitetysti hallittuihin varmenneratkaisuihin.
  - Tämä tarkoittaa tukeutumista virkamiehen, kansalaisen tai yrityksen tunnistamisen ja todennuksen mahdollistaviin arkkitehtuureihin.
  - Käytännön suositus on siis Väestörekisterikeskuksen ratkaisujen hyödyntäminen.
- Milloin edellinen ei ole suoraan mahdollista, tulisi valitun ratkaisun olla mahdollisimman helposti integroitavissa valtionhallinnon arkkitehtuureihin ja ratkaisuihin.
  - Tämä tarkoittaa omien hakemistojen perustamista ja hallinnointia mahdollisimman standardien rajapintojen, esimerkiksi LDAP, avulla.

Sähköpostijärjestelmien käyttöä tukevia operatiivisia suosituksia ja linjauksia, millä ohjataan mahdollisimman monia osallisia yhdenmukaisiin ja luotettaviin sähköpostikäytäntöihin:

- Sähköpostipalvelimien tulisi ainakin valtionhallinnon sisällä varmentaa ja salata keskinäiset yhteytensä. Tämä on mahdollista SSL/TLS käytännöin [RFC 3207].
  - Tämä suositus annetaan voimakkaasti ohjaavana ja sitä tulisi soveltaa mahdollisuuksien mukaan myös sidosryhmien suuntaan.
- Milloin kontrollivaatimusten vuoksi on tarpeen, tulisi lähettäjän ja vastaanottajan välinen viestiliikenne varmentaa ja salata ensisijaisesti S/MIME käytännöin. Varmenteina tulisi käyttää valtionhallinnon yleisesti hyväksymiä varmenteita.
  - Suositus S/MIMEstä ensisijaisena annetaan siksi, että se on todennäköisimmin integroitavissa moniin valtionhallinnon arkkitehtuureissa kuvattaviin järjestelmiin.
  - Suositus varmenteista annetaan sen vuoksi, että tavoitteena on oltava yhdenmukaiset käytännöt ja niiden takaa löytyvät yhdenmukaisesti

menetelmät. Näitä ei saavuteta, mikäli organisaatiot luovat itse omat varmenneratkaisunsa.

- Sidosryhmien suuntaan tulee jatkossakin olla käytettävissä myös muita vaihtoehtoisia menetelmiä, joista esimerkiksi annetaan PGP.
  - OECD:n suositusten mukaisesti valtionhallinto ei saa ohjata ratkaisuja vain tiettyjen markkinoiden tai tuotteiden suuntaan. Vaihtoehtoisten ratkaisujen käyttö tulisi jatkossakin mahdollistaa kansalaisille ja muille ulkoisille sidosryhmille.
  - Tämä suositus annetaan siitä huolimatta, että hanke kansalaisten tunnistuksesta ja todentamisesta tulee ohjaamaan myös sähköpostikäytäntöihin liittyviä todennus- ja salauskäytäntöjä.

Lähitulevaisuuden lisämahdollisuutena esitetään seurattavaksi:

- DKIM [www.dkim.org]. Tämä on menetelmä jossa lähettävä sähköpostipalvelin allekirjoittaa sen kautta lähtevät viestit julkisen avaimen menetelmää käyttäen.
  - Implementointimahdollisuudet eri järjestelmiin vielä epäselvät.
  - Lupaava toimintamalli, joka mahdollistaa keskitetysti sähköpostiliikenteen kiistämättömyyden hallinnan.

6.3.6 Esimerkki käyttäjän ohjeistuksesta

Ulkoasiainministeriö on tuottanut omaan käyttöönsä ohjeen virkavarmenteiden hyödyntämisestä omassa ympäristössään (Microsoft Exchange). Tämä ohje on rakenteellisesti ja sisällöllisesti kattava ja laadukas. Niinpä siihen viitataan hyvänä ja käytännön läheisenä ohjeistuksena, jota suositellaan malliksi muille organisaatio- ja tekniikkakohtaisille ohjeistuksille.

6.3.7 Nykyhetken perushaaste

Arkkitehtuurihankkeilta odotetaan uusia ja tarkennettuja linjauksia myös valtionhallinnon sähköpostiratkaisuista. Näiden linjausten perusteella voidaan suosituksia ja ohjeistuksia varmenteista ja sähköposteista viedä tapauskohtaisesti eteenpäin.

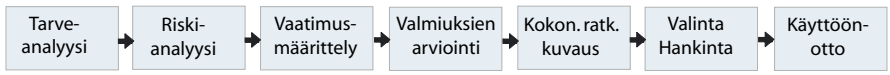
7 Prosessimalli: Suunnittelu, valinta ja käyttöönotto

7.1 Johdanto ja prosessimalli

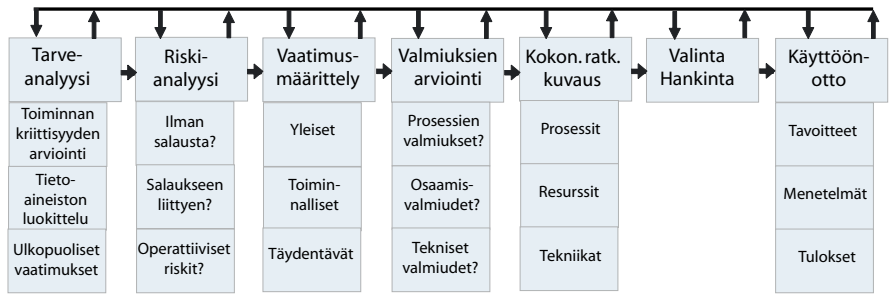
Salausratkaisun toiminnallisuus ja luotettavuus saavutetaan, kun tiedon luonteesta ja organisaation toiminnasta johtuva tarve salaukselle ratkaistaan kontrolloitujen prosessien, riittävän osaamisen ja tarkoituksenmukaisen tekniikan avulla.

Edellä kerratun tavoitteen saavuttaminen vaatii systemaattista lähestymistä. Huomiota pitää kohdistaa teknisten arvojen lisäksi oman toiminnan kriittisyyteen ja oman organisaation valmiuksiin hyödyntää salausratkaisuja tavoitellulla tavalla.

Tämän luvun ohjaavana mallina toimii seuraava yksinkertaistettu prosessikaavio:



Prosessin vaiheita ei saa nähdä puhtaasti peräkkäisinä vaan toisiansa täydentävinä. Yksittäiset vaiheet voidaan pilkkoa alatehtäviinsä. Malli kokonaisuutena näyttää seuraavalta:



Seuraavat kappaleet 7.2 – 7.8 antavat tiivistettyjä vaatimuksia ja ohjaavia esimerkkejä toteutuksesta. Luvut ovat myös eräänlainen synteesi suosituksesta, sillä kuvattu prosessimalli perustuu tässä dokumentissa aiemmin esitettyihin suosituksiin, linjauksiin ja näkemyksiin.

7.2 Tarveanalyysi

Tarveanalyysi vastaa perustellusti kysymykseen ”miksi tarvitsemme salausratkaisuja?”. Käyttötarve ja sen kuvaus syntyy hierarkisesti luvun 4.2. mallia soveltaen seuraavasti:

- Ulkoiset vaatimukset: Lait, asetukset ja muut normiohjauskriteerit.
  - Nämä on selvitettävä, tiedettävä ja tunnistettava tapauskohtaisesti.
  - Itsearviointiin soveltuvia kuvauksia: Kansainvälisyydestä ja normiohjauksesta (kappaleet 4.3.1 ja 4.3.2) sekä käyttötarvekuvausten tarkemmat analyysit.
- Muut käsiteltävänä olevaan tietoaineistoon kohdistuvat vaatimukset.
  - Mitä kriittisempi tietoaineisto, sitä tiukemmat vaatimukset kaikille kontrolleille ja tämän vuoksi myös salausratkaisujen mahdollistamille kontrolleille.
  - Itsearviointiin soveltuvia kuvauksia: Tietoaineistojen käsittelyohjeista (kappale 4.6.3) ja salausratkaisuista mahdollistajana (kappale 4.4.2).
- Organisaation toiminnan yleinen ja tapauskohtainen kriittisyys.
  - Mitä kriittisempi perustoiminta, sitä tiukemmat vaatimukset kaikille kontrolleille ja tämän vuoksi myös salausratkaisujen mahdollistamille kontrolleille.
  - Itsearviointiin soveltuvia kuvauksia: Valtionhallinnon tietoturvatasoista (kappale 4.6.2) ja kypsyys-kyvykkyys mallitus (kappale 4.5.1).

Esimerkkejä konkreettisista kysymyksistä, joita pitää esittää itsearvioinneissa:

- Mitkä ovat tärkeimmät ulkoiset vaikutteet sille, että tarvitsemme salausratkaisuja?
- Minkä tietoaineiston turvaamiseksi tarvitsemme salausratkaisun?
- Mitä muita kontrolleja tietoaineiston [tietoturva]luokittelu edellyttää?
- Miten näitä kontrolleja voidaan vahvistaa salausratkaisujen avulla?
- Mikä on toimintamme yleinen kriittisyysaste [vrt. tietoturvatasot].

Tarveanalyysin jälkeen organisaatio tietää salausratkaisuhankkeen hyödyt ja tavoitteet.

7.3 Riskianalyysi

Kappaleen 4.4.1 (Tiedon hallinta, riskinhallinta ja tietoturvallisuus) mukaisesti: Salausratkaisut ovat osa organisaation tietoriskien ja tietopääoman hallintaa ja siten osa operatiivisten riskien hallintaa.

Riskianalyysissä vastataan tarkentaen kahteen pääkysymykseen:

- Mitä riskejä toimintaamme kohdistuu, mikäli emme ota salausratkaisuja käyttöön?
- Mitä uhkia toimintaamme liittyy, jos tai kun otamme salausratkaisut käyttöön?

Näistä ensimmäinen antaa edellistä lukua 7.2. tarkentavan näkemyksen kysymykseen ”miksi salausratkaisut”. Toinen kysymys pakottaa organisaation kuvaamaan tarkemmin omat toimintatapansa ja valmiutensa. Epäonnistuneen käyttöönoton riskit voivat olla erittäin merkittäviä, esimerkiksi pääsy tietoon voidaan pahimmassa tapauksessa menettää kokonaan.

Päätöksenteon tulee perustua sille arviolle, että syyt salausratkaisujen käytölle ovat painavammat kuin käyttöönoton mukanaan tuomat riskit. Itsearviointia ohjataan seuraavin kysymyksin:

- Toimintamme ilman salausratkaisuja:
  - Lain, asetusten ja muiden normiohjausvaatimusten laiminlyönti?
  - Paljastumisen tai väärentymisen taloudelliset vaikutukset?
  - Paljastumisen tai väärentymisen operatiiviset vaikutukset?
  - Paljastumisen tai väärentymisen PR-vaikutukset (median reaktiot ym.)?
- Toimintamme epäonnistuneen tai toimintaa muuten vaikeuttavan salausratkaisun kanssa:
  - Taloudelliset vaikutukset tiedon käytettävyyden menetyksistä?
  - Operatiiviset vaikutukset ylimääräisen työn vaikutuksesta?
  - PR-menetykset toimintamme tehottomuuden vuoksi?

Tarkka analyysi edellyttää systemaattista lähestymistä. Tämän vuoksi kappaleessa 4.4.1 viitattiin myös riskinhallinnan viitekehykseen COSO [www.coso.org]. Edellä kuvatut kysymykset ovat riskinhallintaprosessissa osa vaikutusanalyysiä (”mitä tapahtuu jos”). Vaikutusanalyysin jälkeen pitää tehdä vielä riskianalyysi (”voiko näin siis tapahtua”) ja päätökset (”perustellen siis näin”).

Mikäli riskianalyysi jätetään tekemättä tai tehdään puutteellisesti, puuttuu organisaatiolta pohja päätöksenteolle (”salausratkaisut vai ei”) ja tarkennetuille vaatimuksille (”millainen”). Riskianalyysi on erittäin tärkeä osa hankintaprosessia ja siihen pitää panostaa.

7.4 Vaatimusmäärittely

7.4.1 Mitä tarkoittaa vaatimusmäärittely?

Vaatimusmäärittely on systemaattinen menetelmä, jonka avulla organisaatio kuvaa, jäsentää ja arvottaa ratkaisuun, tässä tapauksessa siis salausratkaisuun, kohdistuvat odotuksensa.

Vaatimukset jaetaan ”toiminnallisiin vaatimuksiin” ja ”yleisiin” tai ”ei-toiminnallisiin vaatimuksiin”. Toiminnalliset vaatimukset perustuvat käyttötarvekuvauksiin. Ei-toiminnalliset vaatimukset ovat määrämuotoisia, yleisteknisiä ja kohdistuvat ratkaisuun itseensä, ei sen käyttöön. Hyvä esimerkki yleisestä vaatimuksesta on vaatimus järjestelmän käytettävyysasteelle.

7.4.2 Toiminnalliset ja ei-toiminnalliset vaatimukset

Toiminnallisilla vaatimuksilla tarkoitetaan organisaation toimintaan ja tehtäviin liittyviä mahdollisimman tarkkoja kuvauksia siitä, miten salausratkaisuja aiotaan käyttää. Näiden käyttötarvekuvausten kirjoittamista käsiteltiin luvussa 6 (käyttötarvekuvaukset).

Toiminnallisten vaatimusten määritystä ohjataan seuraavan kaltaisilla kysymyksillä:

- Kuka käyttää salausta, missä tilanteessa ja miten tämän käytön halutaan tapahtuvan? (Käyttötarvekuvaukset ja näistä johdettavat vaatimukset).
- Kuka hallitsee ratkaisua, missä tilanteissa ja miten tämän halutaan tapahtuvan? (Prosessikuvaukset ja näistä johdettavat vaatimukset).

Mitä tarkemmin vaatimukset määritetään todellisten ja tavoiteltujen käyttötarvekuvausten avulla, sitä tarkemmin kokonaisratkaisun valinta ja käyttöönotto voidaan suunnitella ja toteuttaa.

Yleisillä tai ei-toiminnallisilla vaatimuksilla tarkoitetaan niitä vaatimuksia, jotka voidaan kuvata mallinnettavin ja mitattavin kriteerein irrallisina yksittäisistä käyttötapauskuvauksista: Yhteensopivuus, integroitavuus, käytettävyys, suorituskyky, hallittavuus ja skaalautuvuus.

Yleisten vaatimusten määrittämiseen käytetään seuraavan kaltaisia kysymyksiä:

- Mitä korkeamman tason yhteensopivuusvaatimuksia pitää kunnioittaa? (Kappale 4.2, vaatimusmäärittelyn hierarkiasta ja yhteensopivuudesta).
- Mitkä muut yhteensopivuusmahdollisuudet ovat arvokkaita? (Esimerkiksi valtionhallinnon sisäisten sidosryhmien jo käyttämät ratkaisut).

- Mihin rajapintoihin ratkaisun täytyy integroitua? (Esimerkkejä kappale 4.7, ohjaavista arkkitehtuureista).
- Mihin muihin teknisiin tai hallinnollisiin rajapintoihin kannattaa tukeutua?
- Mikä on ratkaisulta vaadittava perusluotettavuus ja käytettävyysaste?
- Mitä edellytetään ratkaisun skaalautuvuudelta?
- Minkälaisia muutoksia on nähtävissä, eli mitä vaaditaan ratkaisun joustavuudelta?
- Miten kaikki nämä arvotetaan yksittäin ja priorisoiden?

Jako toiminnallisiin ja ei-toiminnallisiin vaatimuksiin on yleinen esitystapa, mutta se ei ole ehdoton. Esimerkiksi yhteensopivuus ja integroitavuus voidaan nähdä molempina, ja se onkin yksi tärkeimmistä teknisistä vaatimuksista mitä salausratkaisulle esitetään.

Vaatimusmäärittelyn lopputuloksena saadaan kuvaukset siitä, miten ratkaisua käytetään ja miten ratkaisun käytettävyyttä ja yleistä laatua arvioidaan.

7.4.3 Valintakriteeristön viimeistely

Vaatimusmäärittelyn jälkeen organisaatiolla on priorisoitu luettelo vaatimuksista sekä näkemys siitä, miten vaihtoehtoisia ratkaisuja arvotetaan näihin odotuksiin nähden.

Ihannetapauksessa kaikki tämä on muokattu pisteytyslistaksi, ja jokaista kriteeriä vasten on kirjattu välttämätön minimitaso ja tavoitetaso. Tällä tavalla ohjataan kokonaisvalintaa.

7.5 Valmiuksien arviointi

7.5.1 Johdanto: Kypsyys ja kyvykkyys ratkaisevat

Salausratkaisun toiminnallisuus ja luotettavuus saavutetaan, kun tiedon luonteesta ja organisaation toiminnasta johtuva tarve salaukselle ratkaistaan kontrolloitujen prosessien, riittävän osaamisen ja tarkoituksenmukaisen tekniikan avulla.

Organisaation, joka suunnittelee salausratkaisujen käyttöönottoa ja hyödyntämistä tulee arvioida kriittisesti oma kyvykkyytensä. Arvioinnin suositellaan perustuvan kypsyys-kyvykkyys –malleihin.

Salausratkaisut edellyttävät hallinnollisia valmiuksia, resursseja, osaamista ja teknisiä valmiuksia. Hankkiva organisaatio on vastuussa kaikista näistä ja salausratkaisuihin liittyvistä prosesseista.

Organisaation on arvioitava realistisesti, mitä se voi tehdä itse ja minkä verran sen kannattaa tai pitää turvautua muihin tahoihin esimerkiksi ylläpidon tai avainhallinnan prosesseissa.

7.5.2 Hallinnolliset ja organisatoriset valmiudet

Salausratkaisujen käyttöönoton välttämätön edellytys on se, että organisaation tietohallinnon ja tietoturvallisuuden valta- ja vastuukysymykset on määritetty kiistattomasti. Näkemyksiä tämän kohdan arviointiin löytyy useista viitekehyksistä (esimerkkeinä ISO27001, COBIT, ITIL). Esimerkkejä:

- Onko tietoturvallisuuden tavoitteet määritetty kiistattomasti?
- Onko vaatimukset kontrolleille kuvattu riittävällä tarkkuudella?
- Vastaako tarveanalyysin (kappale 7.2) lopputulos edellisiä?
- Löytyykö tiedolle ja järjestelmille vastuulliset, asiansa hallitsevat omistajat?

Salausratkaisuihin liittyy vastuita, jotka ovat resursoitava hyvissä ajoin etukäteen:

- Mikä on käytettävissä oleva henkilöstön määrä ja osaaminen?
- Kykenemmekö hallitsemaan tekniset ja hallinnolliset rajapinnat?
- Mitä muita resursseja organisaatiolla on käytettävissä (sidosryhmät)?

Kärjistettynä esimerkkinä: Mikäli salausratkaisut otetaan käyttöön ilman käsitystä tiedon omistajuudesta, ja ilman riittävää sisäistä osaamista, niin riskit ovat todella suuret.

Hallinnollisten ja organisatoristen valmiuksien kartoitus on pohja käyttöönottosuunnitelmalle.

7.5.3 Prosessien ja toimintatapojen varmentaminen

Kyvykkyyttä ja kypsyyttä näiden osalta arvioidaan seuraavan kaltaisin kysymyksin, joihin kuhunkin kuuluu osaltaan näkemys osaamisesta, resursseista ja tekniikasta.

- Tietohallinnon prosessien tunnistaminen ja kuvaukset.
- Mahdollisuus liittää salausratkaisujen hallintaprosessit näihin.

Malleja tämän kohdan kysymyksiin löytyy useista lähteistä (ISO27001, COBIT, ITIL). Ohjeistus valtionhallinnon tietoturvatasoista sisältää myös käyttökelpoisia lähestymistapoja tähän kohtaan.

Prosessien varmentaminen on pohja useille linjauksille, esimerkiksi ulkoistuspäätöksille.

7.5.4 Teknisten valmiuksien varmentaminen

Välttämätön osa valmiuksien arviointia on teknisten valmiuksien varmentaminen. Koska salausratkaisut liittyvät teknisesti moniin eri järjestelmiin, pitää varmistaa, että integrointi ylipäänsä on mahdollista ilman merkittäviä lisätöitä tai kustannuksia.

Käytännön esimerkki edellisestä: Organisaation suunnitellessa varmenteiden hyödyntämistä sähköpostin allekirjoitukseen sen pitää ensin tarkistaa, miten integrointi käytössä oleviin sähköpostijärjestelmiin ja käyttömenetelmiin tapahtuu. Mikäli tätä ei selvitetä etukäteen yksityiskohtaisesti, on hyvin todennäköistä, että ongelmia syntyy.

Teknisten valmiuksien kartoittaminen tarkentaa suorien investointien tarvetta.

7.6 Kokonaisratkaisun kuvaus

Salausratkaisun toimivuus, tuottavuus ja luotettavuus syntyvät siten, että organisaation toiminnan ja sen hyödyntämän tiedon luonteesta johtuva tarve salaukselle ratkaistaan kontrolloitujen prosessien, riittävän osaamisen ja tarkoituksenmukaisen tekniikan avulla.

Suunniteltu kokonaisratkaisu pitää kuvata kaikkien johtolauseessa kerrattujen komponenttien osalta: Miten prosessit hoidetaan, miten osaaminen varmistetaan ja mitä tekniikalta odotetaan.

7.7 Ratkaisun valinta ja hankinta

Kaikki edellä kuvatut vaiheet mahdollistavat kokonaisratkaisun realistisen ja objektiivisen valinnan ja tähän valintaan tähtäävän avoimen kilpailutuksen. Hankintamenettelyissä noudatetaan valtionhallinnon ohjaavia periaatteita.

7.8 Käyttöönotto

Käyttöönottosuunnitelma laaditaan ennakkoon kaiken edellisen perusteella.

Lopullisen kokonaisratkaisun laatu tulee myös varmentaa. Mitä kriittisemmän perustarpeen täyttämisestä on kysymys, sitä tärkeämpää on käyttää varmentamiseen riippumatonta osapuolta.

7.9 Itse tehden, yhdessä hoitaen vai ulkoistaen?

Laajat salausratkaisut sitovat huomattavia määriä resursseja ratkaisujen elinkaaren ajaksi. Ohjaavana periaatteena valtionhallinnossa tulee olla tukeutuminen sellaisiin ratkaisuihin, joiden hallinta ja ylläpito voidaan keskittää ja siten jakaa mahdollisimman monen osallisen kesken. Tämä periaate ohjaa organisaatioita kohti keskitettyjä, harmonisoituja ja yhteensopivia ratkaisuja.

8 Prosessivaatimukset: Tiedon ja salausratkaisujen elinkaari

8.1 Johdanto

Tämä luku on täydentävä kuvaus, joka avaa elinkaarimallin avulla salausratkaisuihin liittyviä prosessitason haasteita. Luku on tiivis ja pääperiaatteita korostava, ei yksityiskohtiin pureutuva.

Luku antaa käytännönläheisyyttä omien valmiuksien arviointiin (kappale 7.5, valmiuksien arvioinnista) ja ohjaa julkishallinnon organisaatioita yhteneviin käytäntöihin.

8.2 Salausratkaisut ja tietohallinnon yleiset prosessit

Salausratkaisu on järjestelmä, jolla pitää olla omistaja ja nimetyt vastuulliset. Salausratkaisu on tässä mielessä vain yksi, joskin vaativa, tietoteknisen kokonaisympäristön tarjoama palvelu.

Salausratkaisun hallintaan ja ylläpitoon pitää löytyä kaikki vastaavat prosessit kuin minkä tahansa muun tietoteknisen palvelun hallintaan. Esimerkkejä ITIL-mallia [www.itil.org] soveltaen:

- Konfiguraation hallinta
- Muutosten hallinta
- Käytettävyyden hallinta
- Jatkuvuuden hallinta
- “Help Desk” ja ongelmien hallinta

Salausratkaisun hankkiva organisaatio on aina vastuussa siitä, että ratkaisun hallinnan ja ylläpidon prosessit on toteutettu siten, että ne eivät vaaranna palvelun tuomaa turvallisuutta.

8.3 Salausratkaisut ja avainten hallintaan liittyvät prosessit

8.3.1 Johdanto: Elinkaariajattelu

Suojattavan tiedon elinkaari on eri mittainen kuin tiedon hallintaan käytettävän järjestelmän elinkaari tai tiedon suojaamisen käytettävän salausratkaisun tai sen komponenttien elinkaari. Näiden elinkaarien hallintaan liittyy haasteita, joihin on varauduttava ennakolta.

Salausratkaisut vaativat elinkaaren hallintaan sellaisia prosesseja, jotka liittyvät ainoastaan näiden ratkaisujen toiminnan ja luotettavuuden varmentamiseen. Tämä luku kuvaa salausratkaisujen elinkaarta avainten hallintaan liittyvien käytäntöjen avulla.

Kun organisaatio arvioi omia valmiuksiaan (kappale 7.5, valmiuksien arvioinnista), niin valmiuksia elinkaarten ja avainten hallintaan tulee arvioida erityisen kriittisesti. Kärjistäen on pakko todeta, että hyväkin salausratkaisu muuttuu heikoksi epätarkoilla elinkaaren hallinnan prosesseilla.

Kontrolloitu avainten hallinta on välttämätöntä kaikissa salausratkaisuissa. Tämä hallinta on toki yksinkertaisempaa rajatun käyttäjäryhmän pistemäisissä salausratkaisuissa kuin laajan käyttäjäjoukon hyödyntämissä, organisaatioiden väliset rajapinnat ylittävissä ratkaisuissa. Periaatteet ovat kuitenkin saman kaltaisia tapauksesta riippumatta.

8.3.2 Rekisteröinti ja tilaus

Salausratkaisun käyttäjät pitää tunnistaa (identifioida) ja käyttäjistä on ylläpidettävä kiistatonta rekisteriä. Tunnistamisen merkitys kasvaa laajoissa järjestelmissä, koska kokonaisuuden kannalta yksi suurista uhkakuvista on se, että henkilö pystyisi rekisteröitymään väärällä identiteetillä.

Rekisteröintiä varten on luotava prosessi, joka tarkistaa identiteetit ja kiistämättömyyden. Mitä laajempi ja kriittisempi järjestelmä, sitä tiukemmat vaatimukset koko rekisteröintiprosessille. Keskistetysti ohjatuissa järjestelmissä (esimerkkinä virkamiesvarmenteet) myös vaatimukset rekisteröintiprosessille annetaan keskitetysti ja itse rekisteröintiprosessi on keskitetty.

Tilausprosessi alkaa rekisteröinnistä. Tilaus velvoittaa usein erillisen tahon tuottamaan avaimen tai avaimet rekisteröidylle käyttäjälle. Myös tilauksen kiistämättömyys pitää varmentaa. Tämän vuoksi rekisteröinti ja tilaus on linkitetty keskenään, eikä tilausta saa koskaan suorittaa ilman varmennettua rekisteröintiä. Jonon ohittava tilaus murentaa prosessin luottamuksen.

Lisähuomautuksena muistutetaan, että termi käyttäjä voi tarkoittaa henkilöä tai mitä tahansa muuta resurssia, joka pystyy käyttämään salausratkaisua

ja sen avaimia. Vaikka käyttäjä ei olisikaan henkilö, pitää prosessia noudattaa tarkoituksenmukaisesti vastaavalla tarkkuudella.

8.3.3 Luominen, toimitus ja luovutus

Tilauksen vastaanottanut taho tai tämän tahon valtuuttama erillinen instanssi luo avaimen tai avaimet rekisteröityä käyttäjää varten. Luomista kontrolloidaan vielä tarvekohtaisesti erikseen.

Kun avaimet on luotu, ne pitää toimittaa luotettavaa menetelmää ja kanavaa käyttäen käyttäjälle. Tämä menetelmä on myös tapauskohtainen, mutta varsinkin laajoissa järjestelmissä samalla tavalla toistettava ja moninkertaisesti varmennettu ja valvottu. Toimitus päättyy luovutukseen, jonka yhteydessä käyttäjän identiteetti varmennetaan vielä kertaalleen.

8.3.4 Käytön hallinta ja valvonta

Salausratkaisun ja sen avainten käyttöä on seurattava tarkoituksenmukaisin ja käytettävissä olevin hyväksytyin keinoin. Valvonnassa tulee kiinnittää huomiota poikkeavaan käyttöön.

Tärkeä osa käytön hallintaa ja valvontaa on myös käyttäjien koulutus.

8.3.5 Muutosten hallinta

Salausratkaisuja joudutaan kontrolloimaan erittäin usein osana muutostenhallintaa, koska miltei jokainen muutos toimintaympäristössä vaikuttaa potentiaalisesti salausratkaisuihin. Muutokset itse salausjärjestelmään tai sen avaimiin tulee toteuttaa erityisen kontrolloidusti.

Jokainen muutostilanne mikä liittyy suojattavan tiedon elinkaareen pitää suunnitella ennakoivasti. Organisaation on varauduttava esimerkiksi siihen, että salausratkaisun algoritmin ja avaimen elinkaari on lyhyempi kuin suojattavan tiedon elinkaari. Suojattavaan tietoon pitää olla luotettava ja turvallinen pääsy kaikista muutostilanteista huolimatta.

8.3.6 Varmenteiden ja avainten sulkeminen (revokointi) ja uusiminen

Lukijalle huomautuksena, että sulkemisesta käytetään varsinkin puhekielessä usein englannista kielestä periytettyä sanaa revokointi. Tässä ohjeessa käytetään termiä sulkeminen.

Avainten ja varmenteiden sulkemiseen ja uusimiseen liittyviin prosesseihin pitää kiinnittää erityistä huomiota. Sulkeminen voi tapahtua tiettynä ajanhetkenä suunnitelman mukaisesti, esimerkiksi kun projektiryhmä päättää työnsä. Tarve mitätöintiin voi olla myös äkillinen. Äkillinen mitätöinti on tarpeen esimerkiksi silloin, kun avaimet tai varmenteet ovat paljastuneet tai joutuneet vääriin käsiin.

Varmenneratkaisuissa suljetaan varmenne, ei siihen liittyviä avaimia. Avaimet siis toimivat teknisesti varmenteen sulkemisen jälkeen, mutta niihin ei voi enää luottaa. Niitä ei voi käyttää todentamiseen eikä luottaa niillä sulkutapahtuman jälkeen tehtyjä allekirjoituksia.

Koska varmenteen sulkeminen estää salatun tiedon avaamisen vanhoilla avaimilla, koko prosessi pitäisi perustaa tiedon – ei siis järjestelmän – elinkaaren mukaiseksi. Käytännön toteutukset tästä ovat kuitenkin osoittautuneet erittäin haastaviksi, eikä niitä pystytä ratkaisemaan pelkästään teknisin keinoin. Salatun tiedon arkistointi on tästä hyvä esimerkki.

Jotta äkillinen sulkeminen ylipäätään käynnistyy, tarvitaan tarkkoja valvonta- ja seurantajärjestelmiä. Yksi esimerkki näistä ovat ”sulkulistat” (CRL, Certificate Revocation List), joiden ylläpito vaatii myös omat prosessinsa.

Sulkemista seuraa yleensä avaimen uusiminen. Pääperiaatteiltaan tämä tarkoittaa jälleen rekisteröintiä, tilausta, luomista, toimitusta ja luovutusta. Mikäli sulkeminen tapahtui suunnitelmallisesti, pitäisi uusimisenkin tapahtua jouhevasti.

Sulkeminen ja uusiminen aiheuttavat helposti ongelmia peruskäyttäjille. Vahva suositus on, että järjestelmän käyttöönottokoulutuksessa satsataan näihin kysymyksiin. Muuten törmätään valitettavan tyypilliseen tilanteeseen, missä peruskäyttäjä on menettänyt vanhat tietonsa, koska niitä ei enää saa käyttöön uusilla salausavaimilla.

8.3.7 Huomioitava erityiskysymys: Tiedon elinkaari

Jos tiedon elinkaari on erimittainen kuin salausratkaisun tai sen avainten elinkaari, niin tästä seuraa aina prosessitason haasteita. Arkistointivaatimukset on tärkeä esimerkki: Miten arkistoida tieto, jota on säilytetty salattuna?

Lause elinkaarien pituuseroista on yksinkertainen, mutta vielä toistaiseksi ei ole löytynyt viisastenkiveä, jonka avulla haasteeseen voidaan vastata yleispätevästi. Elinkaaren hallinta vaatii aina tarkat ja osittain tapauskohtaiset prosessit ja näihin prosesseihin liitetyt kontrollit.

9 Yhteenveto

Tarve salaukseen syntyy organisaation käsittelemän tiedon kriittisyydestä ja myös organisaation toiminnan yleisestä kriittisyydestä.

Markkinoilta löytyy jo suhteellisen kypsiä ratkaisuja, jotka täyttävät tärkeimmät tekniset vaatimukset. Valtionhallinnon tulisi suosia sellaisia ratkaisuja, jotka ovat avoimia ja yhteensopivia eivätkä muodosta estettä täydentävien ja vaihtoehtoisten ratkaisujen hyödyntämiselle.

Salausratkaisun toiminnallisuus ja luotettavuus saavutetaan, kun tiedon luonteesta ja organisaation toiminnasta johtuva tarve salaukselle ratkaistaan kontrolloitujen prosessien, riittävän osaamisen ja tarkoituksenmukaisen tekniikan avulla.

Mikäli vaatimusmäärittely on puutteellinen tai salausratkaisun vaatimat prosessit ovat epätarkkoja, ratkaisusta ja jopa loppukäyttäjien toiminnasta tulee helposti tehotonta.

LIITE Valtiovarainministeriön voimassaolevat VAHTI-julkaisut:

Valtionhallinnon salauskäytäntöjen tietoturvaohje, VAHTI 3/2008

Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008

VAHTIn toimintakertomus vuodelta 2007, VAHTI 1/2008

Tietoturvallisuudella tuloksia – valtionhallinnon tietoturvallisuuden yleisohje, VAHTI 3/2007

Äypuhelimien tietoturvallisuus – hyvät käytännöt, VAHTI 2/2007

Osallistumisesta vaikuttamiseen - valtionhallinnon haasteet kansainvälisessä tietoturvatyössä, VAHTI 1/2007

Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006

Tietoturvakouluttajan opas, VAHTI 11/2006

Henkilöstön tietoturvaohje, VAHTI 10/2006

Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006

Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006

Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi, VAHTI 7/2006

Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006

Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 5/2006

Electronic Mail-handling Instructions for State Government, VAHTI 2/2006

Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005

Valtionhallinnon sähköpostien käsittelyohje, VAHTI 2/2005

Information Security and management by Results, VAHTI 1/2005

Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004

Datasäkerhet och resultatstyrning, VAHTI 4/2004

Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004

Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004

Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006, VAHTI 1/2004

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003

Valtionhallinnon tietoturvakäsitteistö, VAHTI 4/2003

Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003

Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003

Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003

Arkaluonteiset kansainväliset tietoaineistot, VAHTI 4/2002

Valtionhallinnon etätyön tietoturvallisuusohje, VAHTI 3/2002

Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002

Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista, VAHTI 6/2001

Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001

Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001

Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000

Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000

Julkisuuslain mukaisen tietojärjestelmäselosteen laadintasuositus, VM 17.2.2000

Julkisuuslain mukaisen tietojärjestelmäselosteen esimerkki

Julkisuuslain mukaisen tietojärjestelmäselosteen rtf-lomakepohja

Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje

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

3/2008
VAHTI
maaliskuu 2008

ISSN 1455-2566
ISBN 978-951-804-805-6 (nid.)
ISBN 978-951-804-806-3 (pdf)