# Tietoturvallisuusvaatimukset puolustusvoimien tietohallintopäätösmenettelyn mukaisessa tietojärjestelmähankkeessa

**12. Turvallisuusjohdon koulutusohjelma**

**Tutkielma**

**Laura Liitsalo**

**Puolustusvoimat**

**Tikkakoski 20.3.2013**

**Aalto University Professional Development – Aalto PRO**

**Tiivistelmä**

Tietoturvallisuus on nykyaikaisissa tietojärjestelmissä yhä tärkeämmässä roolissa. Tietoturvallisuudelle puolustusvoimien tietojärjestelmissä on asetettu erilaisia vaatimuksia, näistä tärkeimpinä asetus tietoturvallisuudesta valtionhallinnossa (681/2010), kansallinen turvallisuusauditointikriteeristö (KATAKRI II) sekä lain kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) asettamat velvoitteet.

Tässä laadullisessa, osin vertailevassa tapaustutkimuksessa selvitettiin, kuinka tietoturvallisuusvaatimukset esiintyvät puolustusvoimien tietohallintopäätösmenettelyn mukaisissa tietojärjestelemähankkeissa ja hankkeisiin kuuluvissa sovelluskehitysprojekteissa. Tutkimuksessa tunnistettiin myös asiaan liittyviä kehittämistarpeita.

Tutkimuksessa osoitettiin, että voimassa olevassa puolustusvoimien normipohjassa on harmonisointi- ja uudistamistarpeita. Tietojärjestelmäakkreditointi tulisi sitoa paremmin osaksi tietohallintopäätösmenettelyä ja kriteerien valinnassa tulisi huomioida järjestelmään liittyvä uhka-arvio sekä riskiarviointi. Tietoturvavastuut tulisi kuvata selkeämmin jokaisessa THP-menettelyn vaiheessa. Sovelluskehityksen tietoturvaohjetta kannattaa hyödyntää myös puolustusvoimien sovelluskehityksessä. Tutkimuksen tuloksia koottiin myös liitteessä kaksi olevaan taulukkoon, jossa tietoturvallisuusvaatimusten esiintyminen sekä niiden todentaminen on esitetty vaiheittain.

Avainsanat: Akkreditointi, sovelluskehitysprojekti, tietohallintopäätösmenettely, tietojärjestelmä, tietojärjestelmähanke, tietoturva-auditointi, tietoturvallisuus, tietoturvallisuusvaatimus, tietoturvatarkastus

**Sisältö**

# 1 Johdanto

Tietoturvallisuus on yhä tärkeämmässä roolissa nykyaikaisissa tietojärjestelmissä. Tietojärjestelmien sisältämää tietoa täytyy suojata erilaisia uhkia vastaan ja toisaalta tiedon tulee olla turvallisesti ja oikea-aikaisesti käytettävissä. Tiedon luottamuksellisuuden ja eheyden tulee säilyä. Tietojärjestelmien tietoturvallisuuden toteuttaminen edellyttää sitä, että sovellukset rakennetaan tietoturvallisiksi. Parhaan ja kustannustehokkaan lopputuloksen aikaansaamiseksi tietoturvallisuus tulee ottaa huomioon sovelluskehityksessä heti alusta alkaen.

Tässä tutkimuksessa selvitetään, kuinka tietoturvallisuusvaatimukset esiintyvät puolustusvoimien tietohallintopäätösmenettelyn mukaisissa tietojärjestelmähankkeissa. Tutkimusongelmia tarkastellaan sekä tietojärjestelmähankkeiden tasolla, että hankkeisiin sisältyvien sovelluskehitysprojektien tasolla, riippuen siitä, kumpi tasoista on kyseisessä asiassa vastuullisena.

Tutkimuksessa selvitetään, mikä taho ja missä vaiheessa tai vaiheissa vaatimukset määrittelee sekä mikä tai mitkä tahot vaatimuksien täyttymisen todentavat. Tutkimuksen tavoitteena on myös esittää kehitysehdotuksia nykytilan kartoituksen pohjalta.

Tietohallintopäätösmenettelyllä (THP) tarkoitetaan prosessia, jolla puolustusvoimat tehostaa tietohallintoon osoitettujen voimavarojen käyttöä. Yksi menettelyn tavoitteista on varmistaa tietoturvavaatimusten täyttyminen elinjakson kaikissa vaiheissa. [10] Tietohallintopäätösmenettelyssä on useita toimijoita, joilla on vaihteleva rooli tietoturvavaatimusten määrittelemisen ja todentamisen suhteen. Tietohallintopäätösmenettely liittyy puolustusvoimien hanketoimintaan läheisesti, sillä menettelyssä hallitaan hankkeissa tehtävää kehitystyötä ja sen tuloksia. Menettelyyn kuuluvalla tietohallintopäätöksellä hyväksytään tai hylätään kehitystyön eteneminen, kehitystyön tuloksena syntyneiden järjestelmien tai niihin liittyvien palveluiden operoin-

tiin siirto (ns. tuotantokäyttölupa) tai olemassa oleviin järjestelmiin tai niihin liittyviin palveluihin tehtävät merkittävät muutokset [10]. Tietohallintopäätös on edellytys etenemis- tai investointipäätöksille [10]. Tietohallintopäätösmenettely on ollut voimassa nykyisenä normiasiakirjana vuodesta 2009.

Menettely itsessään on vaiheineen selkeä mutta tietoturvallisuusvaatimusten määritteleminen ja niiden täyttymisen todentaminen ja asiaan liittyvät vastuut on ohjeistettu ja kuvattu useassa eri normissa tai ohjeessa. Esimerkiksi teknisen tietoturvallisuuden tarkastustoimintaa puolustusvoimissa ohjataan omalla normillaan, samoin hanketoimintaa omilla normeillaan. Tietoturvallisuusvaatimukset myös kehittyvät koko ajan ja esimerkiksi lainsäädännöllinen viitekehys on muuttunut vuoden 2009 jälkeen (tietoturvallisuusasetus sekä esimerkiksi laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista). Edellä mainituista seikoista johtuen tutkimus on tarpeellinen selvitys, joka tulee kokoamaan yhteen eri lähteissä olevaa tietoa kokonaiskuvan muodostamiseksi ja kehittämistarpeiden tunnistamiseksi.

Tutkielman rakenne on seuraavanlainen. Ensimmäinen luku on johdatusta aihepiiriin. Toisessa luvussa on tutkimusasettelun, tutkimusmenetelmien ja tutkimuskysymysten kuvaus, sekä tutkimuksen keskeisten käsitteiden määrittelyt. Kolmannessa luvussa kuvataan tietohallintopäätösmenettelyn nykytila sekä sen tulevaisuuden näkymät. Tietohallintopäätösmenettelyn ohjeistavaa normia ollaan uudistamassa, joten on tärkeää huomioida tässä tutkimuksessa menettelyyn mahdollisesti liittyvät, näköpiirissä olevat muutokset. Neljännessä luvussa kuvataan hanketoiminta puolustusvoimissa, sisältäen elinjaksoauditointien ja elinjaksopäätösten kuvaamisen. Viidennessä luvussa esitellään puolustusvoimien arkkitehtuuriohjaus lyhyesti sekä sovelluskehitysmalli ARKKI. Kuudes luku käsittelee tietoturvallisuuden auditointia ja tarkastamista puolustusvoimissa. Luvussa kuvataan myös kansalliset toimijat sekä toimintaan liittyvä lainsäädäntö. Lukujen kolme, neljä, viisi ja kuusi lopuissa on lyhyt yhteenveto kuvatuista asioista. Seitsemännessä luvussa esitetään työn tulokset eli kootaan yhteen miten ja missä vaiheissa tietoturvallisuusvaatimukset esiintyvät puolustusvoimien THP-menettelyn mukaisissa tietojärjestelmähankkeissa ja niihin sisältyvissä sovelluskehitysprojekteissa. Luvussa tehdään myös vertailua Sovelluskehityksen tietoturvaohjeeseen (VAHTI 1/2013). Luvussa osoitetaan myös ARKKI-

sovelluskehitysmallin merkitys vaatimusten asettamisessa ja toisaalta niiden todentamisessa. Luvussa esitetään lisäksi tutkimuksen tuloksena syntyneitä kehitysehdotuksia, joilla pyritään vastaamaan kolmannen pääongelman tutkimuskysymyksiin. Kahdeksannessa luvussa on lyhyt yhteenveto.

Tutkielman lopussa olevissa liitteissä on ARKKI-sovelluskehitysmallin mukaiset dokumentit sekä niiden tekijät (liite 1) sekä edellä mainitut tietoturvallisuuteen liittyvät tehtävät THP-menettelyn vaiheissa, kuvattuna taulukkomuodossa (liite 2).

# 2 Tutkimuksen viitekehys

## 2.1 Keskeiset käsitteet

**Akkreditoinnilla** tarkoitetaan pätevyyden tai kelpoisuuden toteamista tähän oikeutetun tai muuten luotetun tahon toimesta. Akkreditointi voi sisältää tietoturva-auditoinnin tai – tarkastuksen. [9, 11]

Toisen määritelmän mukaan akkreditoinnilla tarkoitetaan prosessia, jonka päätteeksi turvallisuusjärjestelyt hyväksyvä viranomainen antaa virallisen lausunnon siitä, että järjestelmä on hyväksytty käytettäväksi määritellyssä turvaluokassa, tiettyä turvallisuuden takaavaa toimintatapaa noudattaen käyttöympäristössään ja hyväksyttävällä riskitasolla, sen pohjalta, että hyväksytyt tekniset, fyysiset, organisatoriset ja menettelyyn liittyvät turvatoimet on toteutettu. [27]

**Sovelluskehitysprojektit** tai lyhyemmin sovellusprojektit ovat tietojärjestelmähankkeiden osia. Niiden elinkaari tavoiteasettelusta käyttöönottovaiheeseen on osa pidempää elinkaarta. Varsinainen tietojärjestelmien rakentamistyö tehdään sovellusprojekteissa. [1]

**Tietohallintopäätösmenettelyllä** (THP) tarkoitetaan prosessia, jolla puolustusvoimat tehostaa tietohallintoon osoitettujen voimavarojen käyttöä. Yksi THP:n tavoitteista on varmistaa tietoturvavaatimusten täyttyminen elinjakson kaikissa vaiheissa. [10]

Tietohallintopäätösmenettely toimii siten hanketoimintaa ja hankkeisiin kuuluvia sovelluskehitysprojekteja osaltaan vaiheistavana prosessina, jossa ennalta määrätyissä tarkastelupisteissä (THP-pisteet) tarkastetaan hankkeen tai projektin tarkoituksenmukainen eteneminen. THP-pisteissä tarkastetaan myös tietoturvallisuuden toteutuminen, kuhunkin vaiheeseen soveltuvalla tavalla.

**Tietojärjestelmä** on ihmisistä, laitteista ja sovelluksista muodostuva kokonaisuus, jonka avulla pyritään kehittämään tai tehostamaan toimintaa. [34]

**Tietojärjestelmähanke** on pääesikuntatasolle muodostettu pitkäaikainen linjaorganisaation osa, jonka johdolla ja vastuulla kehitetään tiettyä tietojärjestelmää. Tietojärjestelmähanke vastaa tietojärjestelmätason vaatimusmäärittelyistä. Tietojärjestelmähankkeessa ei kuitenkaan itsenäisesti tuoteta sovellusosia eikä hankkeeseen suoraan hankita sovelluskehitystyötä. [1]

**Tietoturva-auditointi** on arviointi/testaus, jonka tarkoituksena on tarkastella tietoturvamekanismien toimivuutta havaitakseen ja/tai estääkseen tietoturvaloukkauksia. [11] **Tietoturvatarkastus** on riippumattoman tahon suorittama kohteen, sen toiminnan ja toiminnan tulosten yleensä määräajoin tapahtuva tutkiminen sen selvittämiseksi, vastaako järjestelmä siihen kohdistuvia vaatimuksia. [11, 27] Termejä tietoturva-auditointi ja tietoturvatarkastus voidaan käyttää myös toistensa synonyymeina.

**Tietoturvallisuus** tarkoittaa tietojen ja tietojärjestelmien käyttöä ja suojelua siten, että eheys, luottamuksellisuus ja käytettävyys säilyvät. [9]

**Tietoturvallisuusvaatimus** on tietoturvallisuuteen liittyvä vaatimus. Vaatimus on puolustusvoimien vaatimustenhallintaohjeen mukaan ilmaisuja, jotka kuvaavat asiakkaan tahtoa liittyen tuotteen tai suoritteen ominaisuuksiin, suorituskykyyn tai muihin parametreihin. [7]

### 2.2 Tutkimusongelmat

Tutkimus pyrkii löytämään vastauksen kolmeen pääongelmaan ja ensimmäisen pääongelman osaongelmiin.

Ensimmäinen pääongelma: Kuinka tietoturvallisuus on huomioitu THP-menettelyn mukaisissa puolustusvoimien tietojärjestelmähankkeissa, hankkeisiin kuuluvissa sovelluskehitysprojekteissa kehitettävien sovelluksien/tietojärjestelmien vast. osalta?

> Osaongelma: Missä eri THP-menettelyn vaiheissa tietoturvallisuusvaatimukset esiintyvät ja kuka vaatimukset määrittelee?
>
> Osaongelma: Kuinka, missä vaiheessa tai vaiheissa ja kenen toimesta vaatimusten täyttyminen todennetaan?

Toinen pääongelma: Minkälaisia eroavaisuuksia ja samankaltaisuuksia puolustusvoimien THP-menettelyn mukaisissa tietojärjestelmähankkeissa ja niihin sisältyvissä ARKKI-sovelluskehitysmallin mukaisissa sovelluskehitysprojekteissa on verrattuna Sovelluskehityksen tietoturvaohjeen malliin?

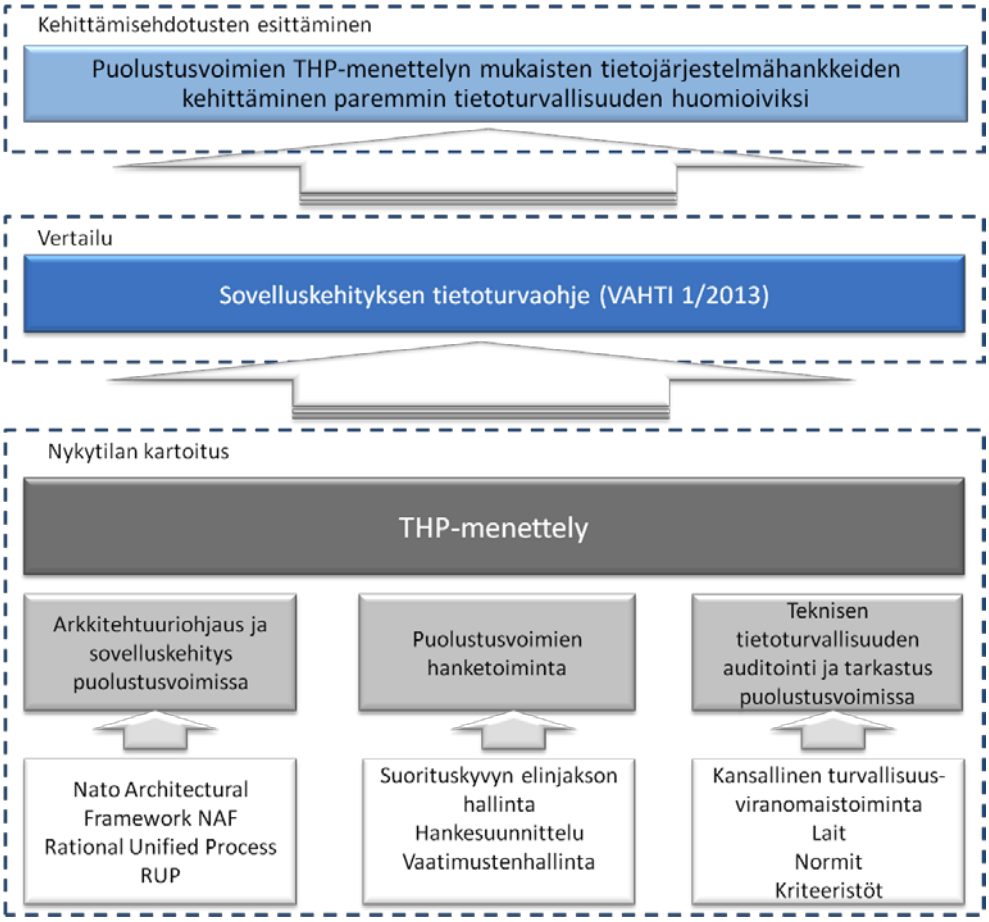
Kolmas pääongelma: Kuinka THP-menettelyn mukaisia puolustusvoimien tietojärjestelmähankkeita ja niihin sisältyviä sovelluskehitysprojekteja tulisi kehittää, jotta tietoturvallisuus tulisi niissä paremmin huomioitua?

### 2.3 Tutkimuksen rajaukset

Tutkimus keskittyy tietojärjestelmähankkeisiin kuuluvissa sovelluskehitysprojekteissa kehitettävien sovellusten tietoturvallisuusvaatimuksiin. Tutkimuksessa ei oteta kantaa hankkeen itsensä tai hankeen projektien turvallisuus- tai tietoturvallisuusvaatimuksiin. Vaatimustenhallintaa ei käsitellä tutkielmassa yleisesti. Puolustusvoimien projektiohjetta [22] ei myöskään kuvata vaan projekteja tarkastellaan sovelluskehitysmallin avulla.

### 2.4 Tutkimuksen viitekehys

Tutkimuksen viitekehys on kuvattu seuraavassa. Ensimmäistä pääongelmaa ja sen osaongelmia tarkastellaan alemmassa katkoviivoitetussa laatikossa ”Nykytilan kartoitus”, toista pääongelmaa keskimmäisessä katkoviivoitetussa laatikossa ”Vertailu” ja kolmatta pääongelmaa ylimmässä katkoviivoitetussa laatikossa ”Kehittämisehdotusten esittäminen”.




**Kuva 1** Tutkimuksen viitekehys

### 2.5 Tutkimusote ja tutkimusmenetelmät

Kyseessä on laadullinen, osin vertaileva tutkimus [26]. Tutkimus on myös tapaustutkimus [31], sillä tutkimuksen kohteena on puolustusvoimat ja tietty puolustusvoimien prosessi. Ensisijaisena tiedonkeruutapana on kirjallisuuskatsaus, mukaan lukien julkinen materiaali, lait ja asetukset, puolustusvoimien pysyväisasiakirjat, normit ja ohjeistus sekä muu puolustusvoimien materiaali. Vertailua VAHTI 1/2013 – ohjeeseen tehdään käyttäen lähinnä toteavan vertailun menetelmää [30] vaikkakin tutkimuksessa esitetään myös kehittämisehdotuksia, jolloin vertailusta tulee jossain määrin myös ohjailevaa [30]. Vaikka tutkimus onkin tapaustutkimus, käsitellään kohdetta lähinnä kirjallisuuslähteiden valossa. Tutkimuksen kohteena on siis ensisijaisesti se, miten puolustusvoimat on tutkimuksen aiheeseen liittyen ohjeistanut ja määrännyt. Käytänteet voivat poiketa ohjeistuksesta mutta tässä tutkimuksessa ei tutkita sitä.

### 2.6 Aiemmat tutkimukset

Aiheesta ei tiedetä tehdyn aiempia tutkimuksia. Tutkimuskenttä on jatkuvasti kehittyvä ja muuttuva sekä puolustusvoimien sisällä että laajemmassa kontekstissa.

VAHTI-julkaisu ”Sovelluskehityksen tietoturvaohje” vuodelta 2013 opastaa sovelluskehittäjiä ottamaan tietoturvavaatimukset huomioon kaikissa sovelluskehityksen vaiheissa, alusta alkaen. Ohje tarjoaa yhden mallin, johon THP-menettelyä ja tietoturvallisuusvaatimusten esiintymistä siinä voidaan verrata. VAHTIn tietoturvaohjeisto on yksi maailman kattavimmista yleisistä tietoturvaohjeistoista. VAHTI-ohjeita käytetään valtionhallinnon lisäksi hyväksi myös esimerkiksi kansainvälisessä tietoturva- ja yhteistyössä, yrityksissä ja kunnissa. [35] Sovelluskehitysohjeessa on mm. otettu huomioon tietoturva-asetuksen ja sen täytäntöönpanoa tukevan ohjeen (VAHTI 2/2010) käytännön vaatimuksia sekä tietohallintolaista (634/2011) ja muista VAHTI-ohjeista annettuja tietoturvavaatimuksia sovelluskehitykselle. Ohjeeseen on myös sisällytetty kansallisen turvallisuusauditointikriteeristön (KATAKRI II) sovelluskehitystä koskevat kriteerit. [34] Kansallisen turvallisuusauditointikriteeristön päätavoitteena on yhtenäistää viranomaistoimintoja silloin, kun viranomainen toteuttaa yrityksessä tai muussa yhteisössä kohteen turvallisuustason todentavan tarkastuksen eli auditoinnin. [20] Puolustusvoimat käyttää KATAKRIa myös auditoidessaan itse omaa toimintaansa [3].

Majuri Jarmo Simin 10. Turvallisuusjohdon koulutusohjelman tutkielma aiheesta ”Puolustusvoimien turvaluokiteltua tietoa sisältävien kotimaisten hankintojen turvallisuus” [32] sivuaa tutkimuksen aihealuetta. Simin tutkielma keskittyy hankinnan itsensä turvallisuuteen, kun taas tässä tutkimuksessa tarkastellaan hankinnan kohteena olevan järjestelmän (vast.) tietoturvallisuutta.

# 3 Tietohallintopäätösmenettely

## 3.1 Tietohallintopäätösmenettelyn kuvaus

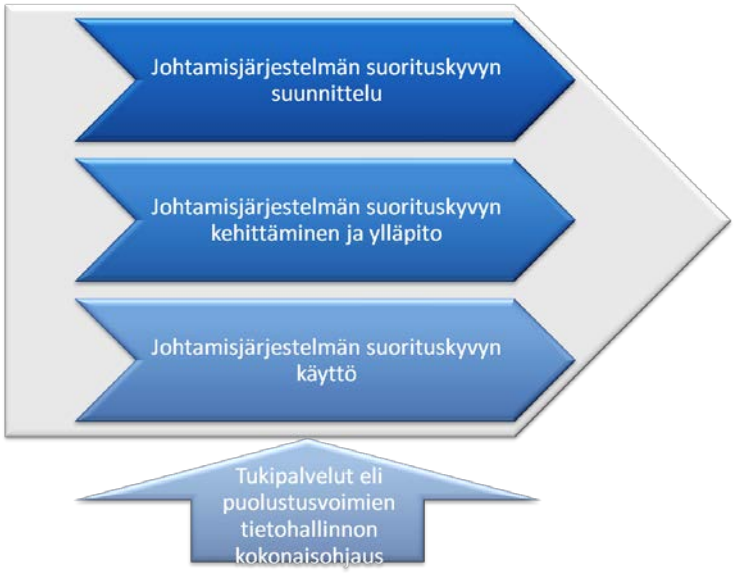
Tietohallintopäätösmenettelyllä (THP tai THP-menettely) puolustusvoimat tehostaa tietohallintoon osoitettujen voimavarojen käyttöä. Tehostaminen tapahtuu

- tunnistamalla ja vähentämällä päällekkäistä työtä
- ohjaamalla ja tukemalla tietohallinnon kehitystä ja kehitystöiden arkkitehtuurinmukaisuutta
- tunnistamalla yhteiskäyttöön soveltuvia toiminnallisuuksia ja menetelmiä
- ohjaamalla puolustushaarojen (ja vastaavien) yhteistyötä sekä yhtenäisiä menettelytapoja
- varmistamalla tietoturvavaatimusten täyttyminen elinjakson kaikissa vaiheissa
- ohjaamalla vaatimustenmukaiseen yhteensopivuuteen kansallisten ja kansainvälisten järjestelmien kanssa
- mahdollistamalla prosessin omistajalle yhtenäisen toimintamallin sekä työkalut muutostarpeiden arviointiin ja muutostenhallintaan
- tunnistamalla järjestelmien, palveluiden ja vastaavien elinjakson aikaiset kustannukset. [10]

Tietohallintopäätösmenettely on Pääesikunnan työjärjestyksen [13] mukaisesti puolustusvoimien johtamisjärjestelmäalan prosessi. Johtamisjärjestelmätoimialalla tarkoitetaan niitä puolustusvoimien toimintoja, jotka toimivat työjärjestyksensä mukaisesti puolustusvoimien johtamisjärjestelmäalan suorituskykyjen suunnittelun, rakentamisen ja ylläpidon sekä käytön osa-alueilla [14]. Toimialan tehtäviin sisältyy myös puolustusvoimien tietohallintoon liittyen puolustusvoimien tietohallinnon suunnittelu ja ohjaus, arkki-

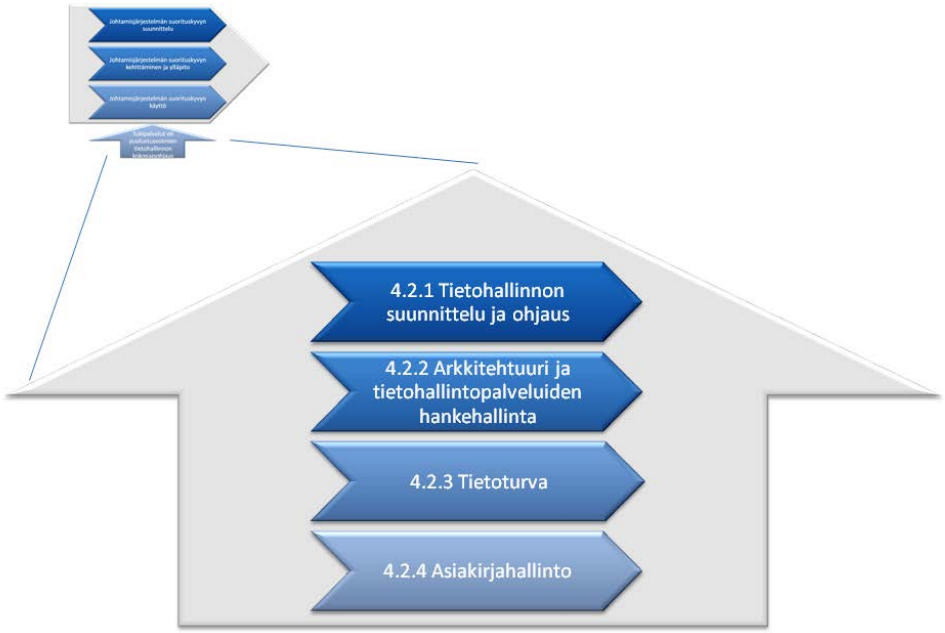
tehtuuriohjaus ja tietohallintopalveluiden elinjakson hallinta sekä tekninen tietoturva [14].

Puolustusvoimien johtamisjärjestelmäalan toimintamalli määrittelee alalle neljä pääprosessia [14, liite 1].



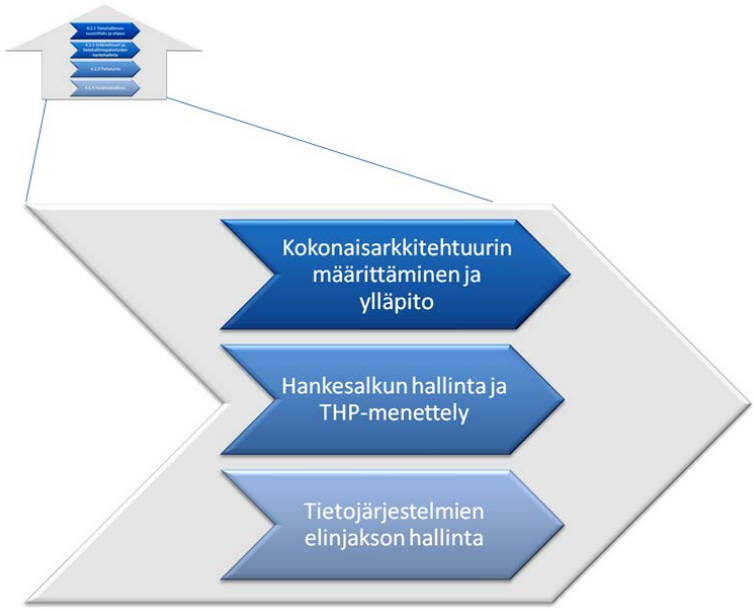

**Kuva 2** Puolustusvoimien johtamisjärjestelmäalan pääprosessit [14, liite 1]

Tukipalvelut-pääprosessi sisältää puolustusvoimien tukiprosessin 4.2 tietohallinto. Tukipalvelut-pääprosessin tehtävänä on määrittää toimintatapamallit ja ohjaus, eli se miten toimitaan. Tukipalvelut vastaa prosessina ohjauksessa käytettävien normien määrittelystä ja toimialan sisäisestä tarkastuksesta. [14, liite 1] Tietohallintopäätösmenettely kuuluu prosessikuvauksissa tietohallinnon prosesseihin. Tietohallinnon pääprosesseja on neljä, ja ne on kuvattu seuraavassa.




**Kuva 3** Puolustusvoimien tietohallinnon kokonaisohjauksen osaprosessit [14, liite 4]

Tietohallintopäätösmenettely on yksi arkkitehtuuri ja tietohallintopalveluiden hankehallinnan pääprosessin osaprosesseista [14, liite 4]. Osaprosessit ovat:




**Kuva 4** Arkkitehtuuri ja tietohallintopalveluiden hankehallinnan osaprosessit [14, liite 4]

Tietohallintopäätösmenettely kuuluu hankesalkun hallinta ja THP-menettely – osaprosessiin.

### 3.2 Tietohallintopäätösmenettelyn rakenne

Tietohallintopäätösmenettely jakautuu toiminnallisesti tietohallintoauditointeihin (THA) ja tietohallintopäätöksiin (THP). [14] Tietohallintopäätös perustuu tietohallintoauditoinnissa saatuihin ja tuotettuihin tuloksiin.

**Tietohallintoauditoinnit (THA)** liittyvät prosessitasolla puolustusvoimien hankeauditointeihin. Puolustusvoimien Johtamisjärjestelmäkeskus (PVJJK) tuottaa auditointisuunnitelman perusteella Pääesikunnan johtamisjärjestelmäosastolle hankkeisiin sisältyvistä tietoteknisistä osioista tietoteknisen auditointimateriaalin, joka sisältää

- Hankkeiden tietoteknisten osioiden tuloksellisuuden arviointiraportin, TULA-arviointi
- Tietoturva-auditoinnin arviointiraportin, TITU-arviointi ja
- Arkkitehtuuri-auditoinnin arviointiraportin, Arkki-arviointi


**Kuva 5** Tietohallintoauditoinnin osa-alueet

Kyseisen materiaalin perusteella johtamisjärjestelmäosasto laatii Pääesikunnan materiaaliosastolle hankeauditointeihin liitettävän lausunnon hankkeen tietoteknisestä kypsyydestä. [14] Tietohallintoauditoinnit ovat siis osa hankeauditointeja [16]. Hankeauditointeja käsitellään tarkemmin seuraavassa luvussa.

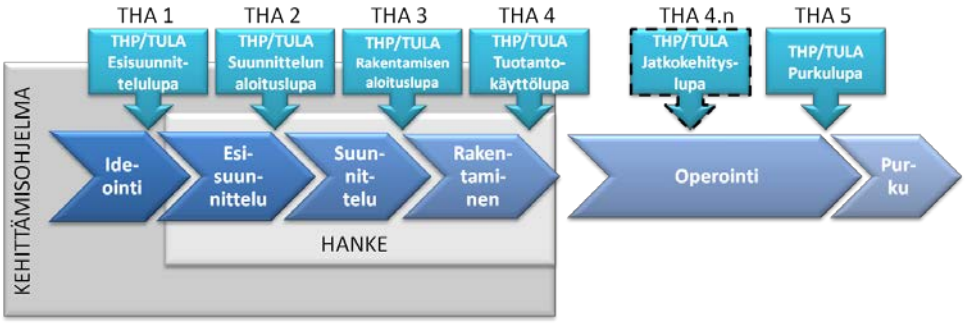
**Tietohallintopäätös (THP)** on tietoteknisiä järjestelmiä koskeva hallinnollinen elinjaksopäätös, jonka tekee Pääesikunnan johtamisjärjestelmäosaston esittelystä puolustusvoimien johtamisjärjestelmäpäällikkö. Taustamateriaalina THP:ssä käytetään joko tietoteknisten projektien auditointimateriaalia, tuotteistamisraportteja, tuotteistusdokumentaatiota tai luopumissuunnitelmia. Tausta-aineisto on sidoksissa käsiteltävään elinjakson vaiheeseen. Pää-

töksen perusteena käytettävän tausta-aineiston tuottaa PVJJK, tai teknisen tietoturvallisuuden auditoinnin ja tarkastuksen ohjeistavan normin mukaisesti joissakin tapauksissa Pääesikunnan johtamisjärjestelmäosasto tai muu hyväksytty puolustusvoimien toimija. [11, 14] THP-päätös tulee olla hyväksyttynä olemassa ennen suorituskykyvastaavien antamia elinjaksopäätöksiä niistä hankekokonaisuuksista, jotka sisältävät tietoteknisiä projekteja. [14] Elinjaksopäätöksiä käsitellään hankeauditointien lailla seuraavassa luvussa.

Tietohallintopäätöksellä puolustusvoimien johtamisjärjestelmäalan johto elinjakson eri vaiheissa joko hyväksyy tai hylkää

1. kehitystyön etenemisen
2. kehitystyön tuloksina syntyneiden järjestelmien tai niihin liittyvien palveluiden operointiin siirron
3. olemassa oleviin järjestelmiin tai niihin liittyviin palveluihin tehtävät merkittävät muutokset [10]

Seuraavassa on kuvattu THP-pisteet tietojärjestelmähankkeen eri vaiheissa.




**Kuva 6** THP-pisteet

Teknisen tietoturvan tarkastamiseen liittyvät toimenpiteet THP-pisteittäin on kuvattu luvussa 6, kappaleissa 6.3.1 Tietoturvatarkastus ja 6.3.2 Tietoturva-akkreditointi.

### 3.3 Tietohallintopäätösmenettelyn tulevaisuuden näkymät

Tietohallintopäätösmenettelyä ja sitä ohjaavaa normia ollaan uudistamassa. Uudistustyö alkoi vuonna 2012 ja on tarkoitus saada päätökseen vuonna 2013. Työstä vastaa Pääesikunnan johtamisjärjestelmäosasto. Työ liittyy laajempaan kokonaisuuteen, jossa uudistetaan myös Pääesikunnan materiaaliosaston hanketoimintaa ohjaavat kuusi normia. Tämänkin työn on arvioitu

valmistuvan vuoden 2013 aikana. Uudistuksen myötä tietohallintoauditoinnit sidotaan paremmin osaksi elinjaksoauditointeja. [18]

Siirtymävaiheessa noudatetaan erillisellä asiakirjalla [18] ohjeistettua toimintatapaa. Merkittävin muutos siirtymävaiheessa on se, ettei PVJJK tuota THA-raporttia, ellei toisin päätetä. Toinen muutos on Pääesikunnan henkilöstöosaston edustajan ottaminen mukaan THP-menettelyyn.

### 3.4 Yhteenveto

Tietohallintopäätösmenettely on tietohallintoon osoitettujen voimavarojen käytön tehostamiseen tähtäävä Pääesikunnan johtamisjärjestelmäosaston prosessi. Yksi menettelyn tavoitteista on tietoturvavaatimusten täyttymisen varmistaminen elinjakson kaikissa vaiheissa. Tietohallintopäätösmenettely jakautuu toiminnallisesti tietohallintoauditointeihin ja tietohallintopäätöksiin. Tietohallintopäätös perustuu tietohallintoauditoinnissa saatuihin ja tuotettuihin tuloksiin. Tietohallintoauditoinnit liittyvät prosessitasolla seuraavassa luvussa kuvattaviin puolustusvoimien hankeauditointeihin ja sisältävät tietoturva-auditoinnin. Tietohallintopäätös on tietoteknisiä järjestelmiä koskeva puolustusvoimien johtamisjärjestelmäpäällikön tekemä hallinnollinen elinjaksopäätös. Tietohallintopäätös tehdään kaikissa elinjakson vaiheissa. Teknisen tietoturvan tarkastamiseen liittyvät toimenpiteet THP-pisteittäin on kuvattu luvussa 6.

Tietohallintopäätösmenettely ja sitä ohjaava normi ovat uudistumassa vuoden 2013 aikana. Uudistustyö liittyy laajempaan kokonaisuuteen, jossa myös hanketoimintaa ohjeistavat normit uudistetaan.

Seuraavassa luvussa käsitellään hanketoimintaa puolustusvoimissa.

# 4 Hanketoiminta puolustusvoimissa

## 4.1 Hanketoiminta osana suorituskyvyn elinjakson hallintaa

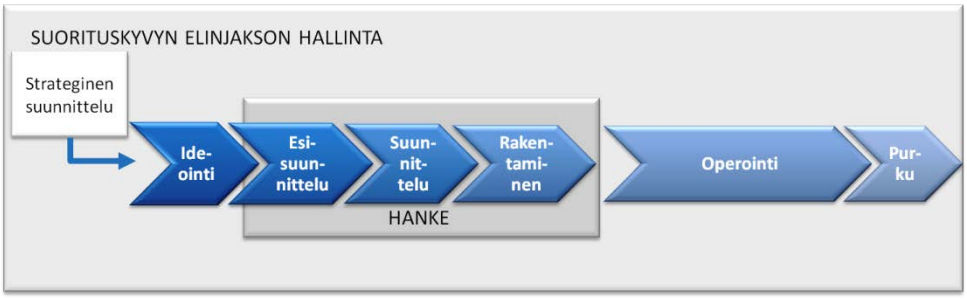
Hankkeella tarkoitetaan puolustusvoimien kehittämisohjelmassa määritellyn suorituskyvyn luomiseksi muodostettavaa sisällöltään ja tavoitteiltaan täsmällisesti määriteltyä toimintokokonaisuutta [23]. Hankkeet tulee pyrkiä toteuttamaan korkeintaan neljän vuoden mittaisina ja kullakin hankkeella tulee saada aikaan toimiva kokonaisuus. [5] Hankkeet kuuluvat kehittämisohjelmiin, sekä jakautuvat edelleen projekteiksi. Tietojärjestelmähankkeisiin liittyvä sovelluksen tai järjestelmän rakennustyö tehdään sovelluskehitysprojekteissa [1].


**Kuva 7** Kehittämisohjelmasta osaprojektiin [15, liite 5]

Osana suorituskyvyn elinjakson hallintaa hanke kattaa vaiheiden 2-4 eli esisuunnittelu, suunnittelu ja rakentaminen, ohjaamisen ja toteuttamisen. Elinjakson vaiheiden välillä tehdään elinjaksopäätös vaiheesta toiseen siirtymisestä. Elinjaksopäätöksiä edeltävät elinjakso/hankeauditoinnit. Hankkeen aikana tapahtuvia auditointeja kutsutaan hankeauditoinneiksi ja muita

elinjaksoauditoinneiksi. Hankeauditointi 1 suoritetaan ennen esisuunnitteluvaiheen käynnistämispäätöstä, hankeauditointi 2 ennen suunnitteluvaiheen käynnistämistä ja hankeauditointi 3 ennen rakentamisvaiheen käynnistämistä. [5, liite 1]

Suorituskyvyn elinjakson hallintaa ollaan uudistamassa ELJAKE-projektissa. Projektin tulosten odotetaan tulevan käyttöön vuoden 2013 aikana. [33, s. 29 ja 31]




**Kuva 8** Suorituskyvyn elinjakson hallinta [5, liite 1]

### 4.2 Hankesuunnittelu ja elinjaksoauditoinnit

Hankesuunnittelua puolustusvoimissa ohjataan Pääesikunnan materiaaliosaston pysyväisasiakirjalla PAK 8:01 Hanketoiminta puolustusvoimissa [5]. Sen ensimmäinen liite käsittelee hankesuunnittelun toteuttamista, sisältäen hankesuunnitteluun liittyvien roolien ja vastuiden kuvaamisen. Seuraavissa kappaleissa on kuvattu lyhyesti hankesuunnittelua eri vaiheissa.

#### 4.2.1 Esisuunnitteluvaihe

Esisuunnitteluvaiheessa tarkennetaan ja täydennetään ideointivaiheen tuotoksena syntyneen konseptin kuvausta. Vaiheessa tehdään sekä kokonaissuunnittelua että hankkeen osa-alueiden suunnittelua. Esimerkkinä ensin mainitusta voidaan mainita järjestelmän operatiivisen konseptin laadinta ja jälkimmäisenä mainitusta järjestelmävaatimusten ja järjestelmäarkkitehtuurin laatiminen. [5] Puolustusvoimien vaatimustenhallintaohjeen [7] mukaan tietoturvallisuusvaatimukset kuuluvat järjestelmävaatimuksiin. Vaiheessa valmistellaan ja toteutetaan hankeauditointi 2 sekä tehdään vaiheeseen liittyvä elinjaksopäätös.

#### 4.2.2 Suunnitteluvaihe

Suunnitteluvaiheen työ perustuu esisuunnitteluvaiheessa tehtyihin suunnitelmiin, hankeauditointi 2:n suosituksiin sekä elinjaksopäätöksessä käskettyihin tehtäviin ja linjauksiin. Tässä vaiheessa järjestelmäsuunnittelua tarkennetaan osajärjestelmätasolle. Vaiheessa voidaan luoda hankintavalmius kolmelle eri tasolle:

1. Hankittavaan järjestelmään liittyvät määrittelyt ja kuvaukset on laadittu
2. Tarjouspyyntö on valmisteltu lähetettäväksi
3. Tarjoukset on saatu ja on olemassa esitys hankittavasta järjestelmästä. [5, liite 1]

Vaiheessa valmistellaan ja toteutetaan hankeauditointi 3 sekä tehdään vaiheeseen liittyvä elinjaksopäätös. Elinjaksopäätöksessä päätetään, aloitetaanko rakentamisvaihe. Mikäli vaihe päätetään käynnistää, laaditaan tarvittavat toimeksiannot sekä kohdennetaan tarvittavat resurssit. [5, liite 1].

#### 4.2.3 Rakentamisvaihe

Rakentamisvaiheen työ perustuu suunnitteluvaiheessa tehtyihin suunnitelmiin, hankeauditointi 3:n suosituksiin sekä elinjaksopäätöksessä käskettyihin tehtäviin ja linjauksiin. Vaiheessa toteutetaan järjestelmähankinta tehtyjen suunnitelmien ja asetettujen vaatimusten, mukaan lukien tietoturvavaatimukset, mukaisesti [5, liite 1]. Käytännössä tämä tarkoittaa vaihetta, jossa varsinainen tietojärjestelmien rakentamistyö tehdään sovellusprojektissa tai -projekteissa.

Vaiheen lopuksi tehdään elinjaksopäätös, jossa ratkaistaan, päätetäänkö hanke ja käynnistetäänkö operointivaihe. Mikäli hanke päätetään, puretaan myös perustetut projektiorganisaatiot. [5, liite 1]

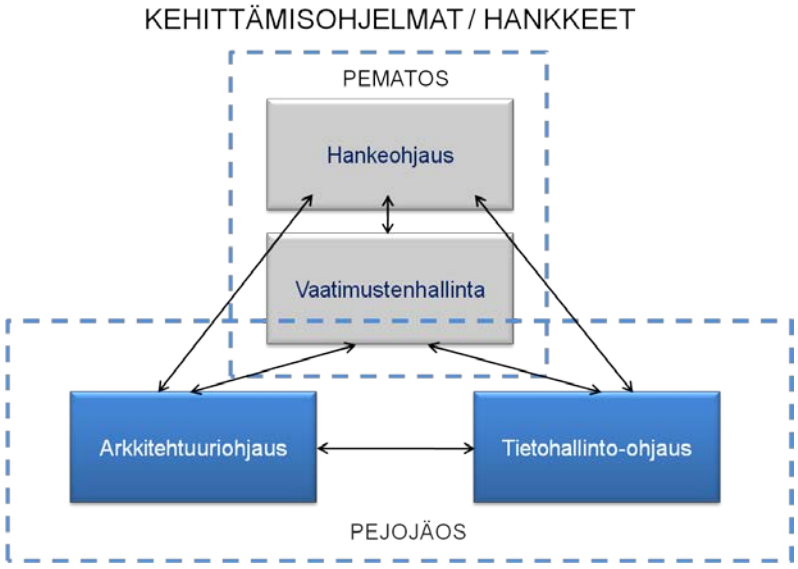
### 4.3 Organisaatioiden roolit ja vastuut

Puolustusministeriö ohjaa kehittämisohjelmien valmistelua sekä hankkeiden toteutusta materiaali-, teknologia- ja teollisuuspoliittisin linjauksin sekä käsittelemällä ja hyväksymällä merkittävien hankkeiden tieto- ja tarjouspyynnöt sekä hankintaesitykset [5, liite 1].

Pääesikunnan johtamisjärjestelmäosasto ohjaa referenssi- ja kohdearkkitehtuurien suunnittelua sekä puolustusvoimien johtamisen kehittämisohjelmaan sisältyviä hankkeita. Johtamisjärjestelmäosasto antaa myös johtamisjärjestelmäalan kehittämistä ja tietohallintoa koskevia ohjeita, käskyjä ja määräyksiä sekä tietohallinnon ohjaukseen liittyviä päätöksiä, jollainen myös tietohallintopäätös on. [16]

Pääesikunnan materiaaliosasto ohjaa puolustusvoimien hanke- ja hankintatoimintaa. Hanketoimintaan kuuluvat Pääesikunnan työjärjestyksen [11] mukaan vaatimusten-, elinjakson-, riskien- ja projektinhallinta. Näiden toimintojen lisäksi materiaaliosasto vastaa myös elinjakso/hankeauditointitoiminnasta ja sen kehittämisestä. [16]

Edellä mainitut pääesikunnan johtamisjärjestelmäosaston (PEJOJÄOS) ja pääesikunnan materiaaliosaston (PEMATOS) vastuut on kuvattu seuraavassa kuvassa.




**Kuva 9** Hankeohjauksen vastuujako [16]

Pääesikunta ohjaa hankkeita työjärjestyksensä mukaisesti sekä toiminnan ja resurssien suunnittelun ja seurannan eli TRSS-prosessin kautta. Hanke esitellään pääesikunnassa elinjaksoauditointien 1-4 jälkeen ennen seuraavaa päätöstä käynnistää esisuunnittelu-, suunnittelu-, rakentamis- ja operointivaiheet. Mikäli hanke etenee kehittämisohjelmassa asetettujen vaatimusten ja reunaehtojen mukaisesti, sitä ei tarvitse esitellä muulloin pääesikunnassa. [5, liite 1]

Pääesikunnan materiaaliosasto vastaa tärkeimpien hankkeiden auditoinnista osana elinjaksoauditointeja. Puolustushaaraesikunnat vastaavat muiden hankkeiden auditoinnista osana elinjaksoauditointeja materiaaliosaston ohjeiden mukaan. [5, liite 1]

### 4.4 Toimijoiden roolit ja vastuut

Seuraavissa kappaleissa kuvataan hanketoiminnan eri toimijoiden vastuita niiltä osin, kuin ne liittyvät tietoturvallisuusvaatimuksiin, niiden todentamiseen tai THP-menettelyyn. Toimijoilla on lisäksi paljon muita vastuita, jotka eivät liity tämän tutkimuksen aihepiiriin.

#### 4.4.1 Kehittämisohjelman omistaja

Kehittämisohjelman omistaja omistaa kehittämisohjelmansa hankkeiden tuotoksena syntyvät suorituskyvyt. Omistaja vastaa siitä, että kehittämisohjelman hankkeet on auditoitu ennen päätöksentekoesittelyä seuraavan elinjakson vaiheen aloittamisesta. Omistaja tekee suorituskykyyn liittyvät elinjaksopäätökset. [6, liite 1]

#### 4.4.2 Suorituskykyvastuullinen taho

Suorituskykyvastuullinen taho on hankevaiheessa käytännössä hankepäällikkö. Hankepäällikkö vastaa elinjaksoauditointien valmisteluista auditointikohteen osalta ja tekee esityksen hankkeensa auditoinneista. Hän vastaa myös hankkeen vaatimustenhallinnasta, siis myös tietoturvallisuusvaatimustenhallinnasta. [6, liite 1]

#### 4.4.3 Järjestelmävastuullinen taho

Järjestelmävastuullinen taho vastaa järjestelmään liittyvästä osasta elinjaksoauditointien valmistelussa. [6, liite 1] Järjestelmävastuullinen taho myös vastaa ideointivaiheessa ideoitavien konseptien teknisen toteutuskelpoisuuden arvioinnista, esisuunnitteluvaiheessa järjestelmävaatimusten laadinnasta, mukaan lukien siis tietoturvallisuusvaatimukset, suunnitteluvaiheessa järjestelmäsuunnittelun tarkentamisesta osajärjestelmätasolle sekä osajärjestelmien järjestelmävaatimusten laadinnasta (ml. tietoturvallisuusvaatimukset), testaussuunnitelmien laadinnasta ja järjestelmäsuunnittelun päivittämisestä. Rakentamisvaiheessa järjestelmävastuullinen taho ohjaa hankintaa ja vastaa järjestelmän teknisestä hyväksynnästä. Operointivaiheessa järjestelmävastuullinen taho vastaa järjestelmävaatimusten ylläpitämisestä. [5, liite

1] Purkamisvaiheessa järjestelmävastuullisella taholla ei ole selviä tietoturvallisuuteen liittyviä vastuita.

Järjestelmävastuullisella taholla on tietoturvallisuusvaatimusten määrittelemiseen liittyen selvästi selkein vastuu, vaikka suorituskykyvastuullinen taho, käytännössä hankepäällikkö, vastaakin vaatimustenhallinnasta kokonaisuutena.

#### 4.4.4 Elinjaksopäätöksen tekijä

Elinjaksopäätöksen tekijä on yleensä kehittämisohjelman omistaja. Elinjaksopäätöksen tekijä hyväksyy vaiheiden aikana tehdyn työn ja käskee suunnitteluperusteet. [5, liite 1] Elinjaksopäätöksen tekijä ratkaisee aloitetaanko seuraava elinjaksovaihe vai tarvitseeko käynnissä olevaan vaiheeseen tehdä tarkennuksia tai tarkistuksia. Elinjaksopäätöksen tekijä myös ratkaisee, suoritetaanko uusi elinjaksoauditointi kyseisten tarkastusten tai tarkennusten tekemisen jälkeen. [6, liite 1]

### 4.5 Yhteenveto

Hanke määriteltiin luvussa puolustusvoimien kehittämisohjelmassa määritellyn suorituskyvyn luomiseksi muodostettavaksi toimintokokonaisuudeksi. Hankkeet kuuluvat kehittämisohjelmiin, sekä jakautuvat edelleen projekteiksi. Tietojärjestelmähankkeisiin liittyvä sovelluksen tai järjestelmän rakennustyö tehdään sovelluskehitysprojekteissa. Tässä tutkimuksessa sekä sovelluskehitysprojekteissa tehtävä tietoturvallisuusvaatimuksiin liittyvä työ, että hanketasolle liittyvät tietoturvallisuusvastuut ovat tarkastelun kohteena. Osana suorituskyvyn elinjakson hallintaa hanke kattaa vaiheiden 2-4 eli esisuunnittelu, suunnittelu ja rakentaminen, ohjaamisen ja toteuttamisen. Elinjakson vaiheiden välillä tehdään elinjaksopäätös vaiheesta toiseen siirtymisestä.

Hankkeen vaiheista rakentamisvaihe on vaihe, jossa varsinainen tietojärjestelmien rakentamistyö tehdään sovellusprojektissa tai -projekteissa. On kuitenkin tärkeää ymmärtää, että käytännössä tietoturvallisuusvaatimukset täytyy määritellä ennen rakentamisvaihetta. Tietoturvallisuusvaatimukset, kuten muutkin vaatimukset liitetään osaksi suunnitteluvaiheen lopussa lähetettävää tarjouspyyntöä.

Luvussa kuvattiin myös organisaatioiden ja eri toimijoiden vastuita. Järjestelmävastuullisella taholla on selkeästi konkreettisin vastuu tietoturvallisuusvaatimusten määrittelemisessä vaikka hankepäällikkö/suorituskykyvastuullinen taho vastaakin vaatimustenhallinnasta kokonaisuutena.

Seuraavassa luvussa käsitellään arkkitehtuuriohjausta ja sovelluskehitystä puolustusvoimissa.

# 5 Arkkitehtuuriohjaus ja sovelluskehitys puolustusvoimissa

## 5.1 Arkkitehtuuriohjaus puolustusvoimissa

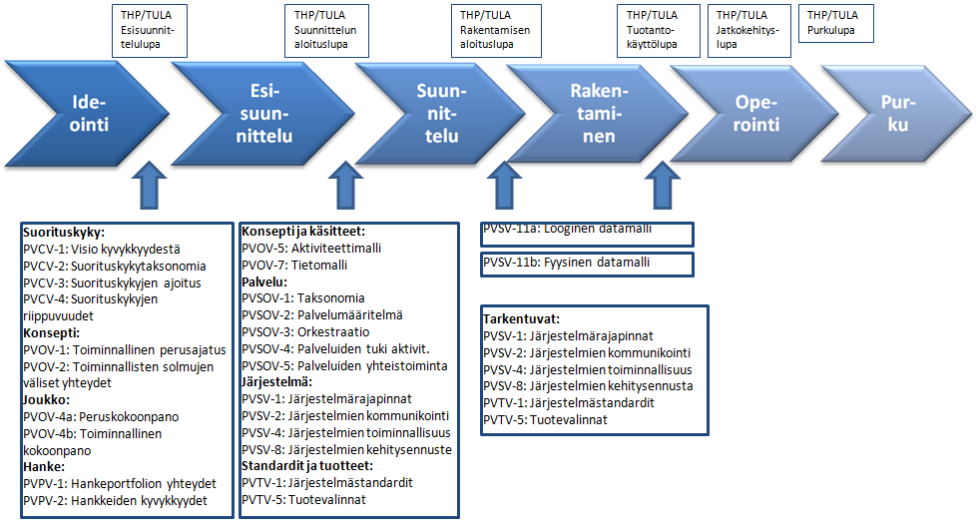
Arkkitehtuuriohjauksen tavoitteena on tuottaa perusteet puolustusvoimien johtamisjärjestelmän tietohallintopalveluiden elinjakson hallinnalle. Syötteinä arkkitehtuuriohjaukselle toimivat puolustushallinnon tietohallinnon toimintatapamalli, kehittämisohjelmien suunnitelmat sekä tietopalvelujen kehittämisen palvelukartta. [2]

Kokonaisarkkitehtuurin määrittämisessä ja arkkitehtuurin kehittämissuunnitelman laadinnassa käytetään Puolustusvoimien tietohallinnon arkkitehtuurikehikkoa (PVTAK), joka pohjautuu NATO:n arkkitehtuurikehikkoon (NAF, Nato Architectural Framework). Kokonaisarkkitehtuurikuvauksella ohjataan referenssiarkkitehtuureja ja niiden kehittämistä. Kokonaisarkkitehtuurin laadinnasta vastaa Pääesikunnan johtamisjärjestelmäosasto ja siellä puolustusvoimien pääarkkitehti. Kuvausten tuottamiseen osallistuu Puolustusvoimien Johtamisjärjestelmäkeskuksen Arkkitehtuuri-osaamiskeskus (ARKKI-OK) sekä referenssi- ja kohdearkkitehtuurien omistajat. [2]

Vuoden 2011 alusta lähtien hankkeilta on vaadittu yhteneväiset tavoitetilakuvaukset PVTAK-muodossa. Käytännössä tämä tarkoittaa vaiheittain rakennettavaa arkkitehtuurikokonaisuutta, joka esittää hankkeen tavoitetilan sekä riippuvuudet muille osa-alueille eri näkökulmista. Arkkitehtuurikuvaukset auditoidaan osana hankkeen elinjaksoauditointeja. Hankkeen alla olevat projektit voivat ”periä” hankkeen arkkitehtuurin. [4]


**Kuva 10**Kokonaisarkkitehtuurista tarkkaan suunnitteluun [1]

Hanke tai projekti tuottaa arkkitehtuurikuvaukset tietohallintoauditointeihin seuraavan kuvan mukaisesti. Kuvauksia voidaan myöhemmissä vaiheissa tarkentaa, mutta ei päivittää. [10, liite 1]



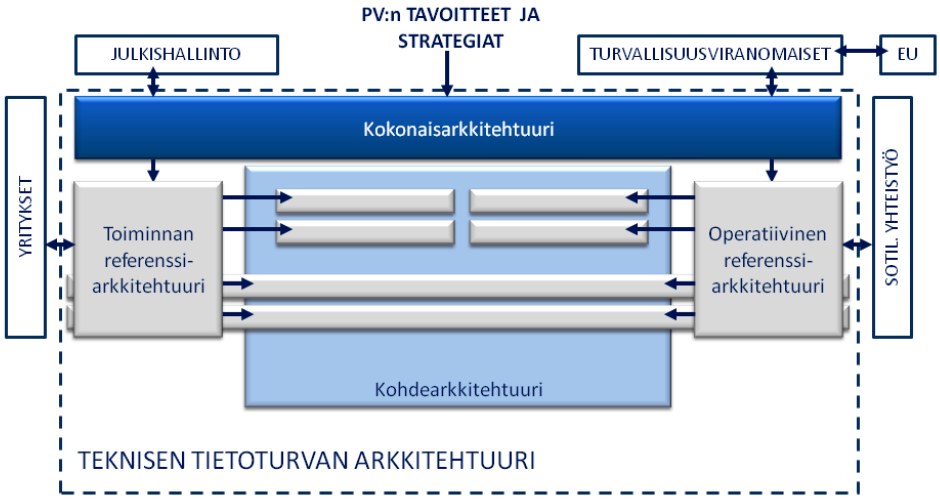

**Kuva 11** Arkkitehtuuriyhteensopivuuden määrittäminen elinjakson auditointipis-teissä [10, liite 1]

### 5.2 Puolustusvoimien johtamisjärjestelmän teknisen tietoturvallisuuden arkkitehtuuri

Puolustusvoimien johtamisjärjestelmällä on lisäksi vuodesta 2012 ollut määriteltynä teknisen tietoturvallisuuden arkkitehtuuri [8], jolla on vaikuttavuutta referenssi- ja kohdearkkitehtuureihin sekä suoraan hankkeisiin ja yksittäisten järjestelmien teknisiin ratkaisuihin. Johtamisjärjestelmä on puolustusjärjestelmän osajärjestelmä, jolla tarkoitetaan suorituskykyjen toimi-

vallan käytön ja ohjauksen johtamisen kokonaisuutta [15]. Teknisen tietoturvallisuuden arkkitehtuurin tavoitteena on muodostaa yhteinen ohjeistus puolustusvoimissa kehitettävien johtamisjärjestelmien sovellusten, tietoliikennejärjestelmien sekä niihin liittyvien palvelujen teknisten tietoturvaratkaisujen toteutukselle. Päämääränä on tietoturvallinen, kustannustehokas sekä yhteentoimiva johtamisjärjestelmäkokonaisuus. Teknisen tietoturvallisuuden arkkitehtuurinmukaisuus tarkistetaan tietohallintopäätösmenettelyn eri vaiheissa. Arkkitehtuuridokumentti perustuu puolustusvoimien hallinnollisiin normeihin, KATAKRIn toiseen versioon sekä VAHTI ohjeisiin 2/2010 (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta) sekä 3/2010 (Sisäverkko-ohje). [8]

Seuraavassa on kuvattu teknisen tietoturvan arkkitehtuurin sijoittuminen kokonais-, ja referenssi- ja kohdearkkitehtuureihin nähden. Kuva on pelkistetty.




**Kuva 12** Teknisen tietoturvan arkkitehtuuri osana kaikkia arkkitehtuureja [8 mukaillen]

### 5.3 Sovelluskehitys puolustusvoimissa

Sovelluskehitystä puolustusvoimissa käsitellään tässä ARKKI-sovelluskehitysmallia tarkastelemalla.

ARKKI-sovelluskehitysmallilla määritellään puolustusvoimissa käytettävä inkrementaalinen sovelluskehitysmalli. ARKKI-sovelluskehitysmallin avulla vaiheistetaan ja ohjeistetaan puolustusvoimien ja toimittajan tehtävät sovellusprojekteissa. Sovelluskehitysmallissa mainitut, työn tuloksena synty-

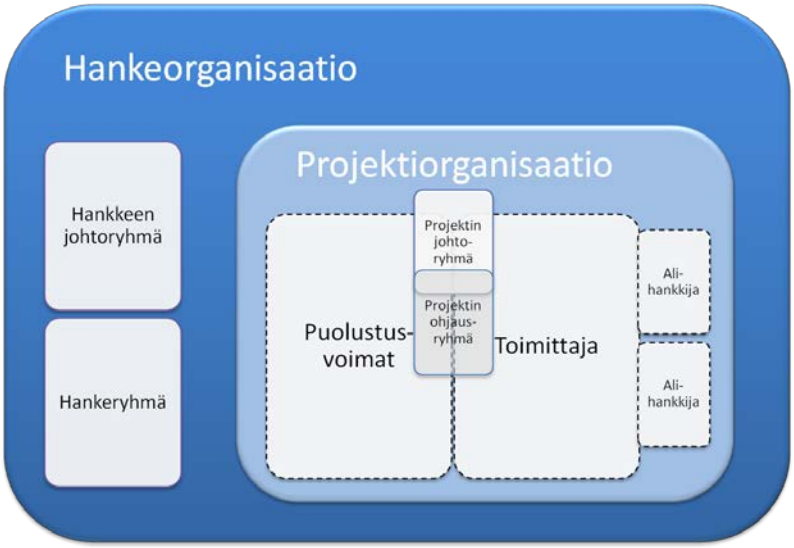
vät dokumentit ovat pakollisia. [1] Dokumentit on listattu tämän tutkimuksen liitteessä 1. Osaa ARKKI-sovelluskehitysmallin mukaisista dokumenteista tarkastellaan tietojärjestelmän akkreditointivaiheessa eli rakentamisesta operointiin – vaiheessa (THP 4). Malli kattaa sovellusprojektin tavoiteasettelun, sovelluksen vaatimusmäärittelyn, sovelluksen rakentamisen, sovelluksen luovutuksen ja käyttöönoton. Malli ei sisällä sovellusprojektin perustamista edeltäviä hanketason vaiheita eikä käyttöönoton jälkeistä käyttö- ja ylläpitovaihetta. Mallissa ei sen määrittelemien rajausten mukaan ole täsmennetty kovin tarkasti liitoksia auditointeihin ja tietohallintopäätösmenettelyyn. Mallissa ei myöskään ole määritelty täsmällisiä projektin läpivientiin tarvittavia roolituksia ja vastuita. [1]

### 5.4 Sovellusprojekti ja sen vaiheet

Sovelluskehitysprojektilla tai lyhyemmin sovellusprojektilla tarkoitetaan projektia, jossa kehitetään sovellustoiminnallisuutta ja komponentteja osaksi laajempaa tietojärjestelmää [1]. Kuten käsitemäärittelyissä luvussa kaksi todettiin, sovellusprojekti on osa tietojärjestelmähanketta. Varsinainen tietojärjestelmän kehitystyö tehdään sovellusprojekteissa.

Yksi hanke voi koostua useasta projektista, jolla kullakin on oma organisaationsa. Projektin laajuuteen, sisältöön, aikatauluun ja/tai kustannuksiin merkittävästi vaikuttavista asioista päättää projektin johtoryhmä. Johtoryhmään kuuluvat puolustusvoimien hallinnollinen projektipäällikkö ja toimittajan projektipäällikkö sekä puolustusvoimien sovelluksen omistajan edustus. Projektin käytännön toimia ohjaa projektin ohjausryhmä, johon kuuluvat ainakin toimittajan ja puolustusvoimien projektipäälliköt. Puolustusvoimien projektiorganisaatiossa projektia johtaa kolme erilaista roolia: hallinnollinen, toiminnallinen ja tekninen projektipäällikkö. Riippuen projektista nämä voivat olla saman tai eri henkilön hoitamia rooleja. Suuremmissa sovelluskehitysprojekteissa projektiorganisaatio voi jakaantua toiminnallisiin osa-alueisiin, vastaten kehitettävän sovelluksen osa-alueita. [1]

Seuraavassa kuvassa on esitetty hanke- ja projektiorganisaatio pelkistetysti.




**Kuva 13** Esimerkki hanke- ja projektiorganisaatiosta [1 mukaillen]

ARKKI-mallissa sovellusprojektit jaetaan neljään vaiheeseen, jotka kuvataan tarkemmin seuraavissa kappaleissa:

1. Tavoiteasetteluvaihe. Tälle vaiheelle ei ole esitetty aikarajaa.
2. Vaatimusmäärittelyvaihe. Vaihe saa kestää enintään 3 kuukautta.
3. Rakentamisvaihe. Vaiheen ohjeellinen kestoaika on enintään 18 kuukautta.
4. Käyttöönottovaihe. Vaiheen ohjeellinen kestoaika on enintään 6 kuukautta. [1]

### 5.4.1 Tavoiteasetteluvaihe

Kaikki sovellusprojektit tulisi aloittaa tavoiteasettelulla, jossa kuvataan perusteet sovelluksen kehittämiselle. Tavoiteasetteluvaiheessa laaditaan järjestelmän omistavan linjaorganisaation toimesta tavoiteasetteluasiakirja, ja se toteutetaan kokonaisuudessaan puolustusvoimien sisäisin toimenpitein. [1]

Tavoiteasettelussa määritellään prosessi tai sen osa, jota pyritään kehittämään ja tukemaan. Tämän jälkeen määritellään, miten tietojärjestelmää kehittämällä voidaan parantaa tätä prosessia. Lisäksi määritellään tavoitteet koko sovelluksen kehittämiselle, sovelluksen kehittävä organisaatio, tavoiteaika sekä budjetoinnin raamit. Tavoiteasettelu esitellään Pääesikunnan johtamisjärjestelmäosastolle. Johtamisjärjestelmäosasto määrittää, mitä muita vastaavia sovelluksia on tekeillä tai tehty, keiden kanssa tulee tehdä yhteistyötä, mitä materiaalia on valmiina tukemaan työtä, miten seuraava vai-

he tulee toteuttaa, millainen koulutus toteuttajalle järjestetään sekä mitä asioita tulee vielä selvittää ennen virallisen projektiehdotuksen laatimista. Tavoiteasetteluvaiheessa Pääesikunnan johtamisjärjestelmäosaston rooli on tukeva. Osasto vastaa siitä, että hankkeen toteuttajalla on kaikki tarvittava ohjeistus käytössään. [1]

Järjestelmän omistava linjaorganisaatio laatii jokaisen sovelluksen toteuttamisesta projektiehdotuksen ja esittelee sen tietohallintopäätösmenettelyn esisunnitteluvaiheessa, toisessa tietohallintoauditoinnissa (THA 2). Projektiehdotukseen liitetään tavoiteasetteluasiakirja. Projektiehdotuksen hyväksyminen käynnistää sovelluksen kehittämisen. [1]

### 5.4.2 Vaatimusmäärittelyvaihe

Vaatimusmäärittelyvaihe on tämän tutkimuksen kannalta kaikkein merkittävien sovelluskehitysprojektin vaiheista. Se on kokonaan puolustusvoimien johtamaa työtä. Vaatimusmäärittelyvaihe alkaa nykytilan kuvauksen laatimisella. Sen tarkoituksena on saavuttaa ymmärrys nykyisistä toimintaprosesseista ja sekä niihin liittyvistä parannusmahdollisuuksista [1]. Lisäksi tarkoituksena on tunnistaa projektin suunnitteluun sekä vaatimusmäärittelyyn liittyvät rajoitukset ja uudelleenkäyttömahdollisuudet [1].

Vaatimusten määrittelyssä oleellisinta on löytää ne toiminnalliset vaatimukset, jotka uuden sovelluksen tulee täyttää. Toiminnallisten vaatimusten määrittelemisestä vastaa käyttäjän edustaja, joka toimii tässä asiantuntijan roolissa. Toiminnallisten vaatimusten määrittelyllä:

- kuvataan sovelluksen halutut toiminnalliset ominaisuudet
- kuvataan, kuinka kehitettävää sovellusta käytetään osana prosessia
- kuvataan, miten sovellus liittyy käyttäjän tasolla muihin prosesseihin
- määritellään sovelluksen turvallisuustasot [1]

Toiminnalliset vaatimukset kirjataan tavoitetilan kuvauksiin sekä käyttötapauskuvauksiin. Toiminnallisten vaatimusten lisäksi määritellään tekniset, laatu- ja muut vaatimukset. Tietoturvallisuusvaatimukset kuuluvat tähän joukkoon. Vaatimusmäärittelyn hyväksyy järjestelmän omistaja ja se liitetään osaksi toimittajille lähetettävää tarjouspyyntöä. [1] Toimittajien tarjoukset – ja myöhemmin siis tilaukset, perustuvat tähän tarjouspyyntöön ja

siksi on ensiarvoisen tärkeää, että tarjouspyyntö sisältää kaikki ne vaatimukset, joita aiotaan projektin myöhemmissä vaiheissa toteuttaa.

Kun vaatimusmäärittely on valmis, tietojärjestelmän omistava organisaatio hakee sovellukselle operaatiopäälliköltä toteutusluvan (rakentamisen aloituslupa) tietohallintopäätösmenettelyn mukaisessa kolmannessa tietohallintoauditoinnissa (THA 3). Toteutuslupaesitys laaditaan tietojärjestelmähanketasolla omistajan ohjaamana, ja siinä määritellään:

- toteutustapa
- tarkennettu rahoitus
- käytettävät valmiit komponentit ja lupa niiden jatkokehittämiseen
- toteutettavat yhteiset komponentit
- sovellusprojektin turvallisuustasot ja – järjestelyt
- sovellusprojektin johtoryhmä, projektiryhmä sekä aikataulutus
- sovellusprojektin vaatima tuki [1]

Toteutuslupa toimii samalla toimeksiantona eri osapuolille. [1]

#### 5.4.3 Rakentamisvaihe

Sovelluksen rakentamisvaiheessa tehdään varsinainen rakentamistyö määrittelystä testaukseen, joka tilataan puolustusvoimien ulkopuoliselta toimittajalta. Puolustusvoimien edustajat toimivat vaiheessa asiantuntijoina. Toimittajan kannalta rakentamisvaihe sisältää projektin kaikki vaiheet ja on näin ollen rakentamisprojekti vaikka puolustusvoimien kannalta kyse onkin vain yhdestä vaiheesta. [1]

Työnjaossa puolustusvoimien ja toimittajan kesken noudatetaan seuraavia pääperiaatteita:

- toimittaja johtaa rakentamisprojektia
- puolustusvoimien projektipäällikkö arvioi syntyneitä tuloksia
- puolustusvoimien nimetyt henkilöt osallistuvat vaatimusten hallintaan, toiminnan mallintamiseen sekä sovelluksen määrittelyyn asiantuntijan roolissa

- hyväksymistestauksen suorittaa puolustusvoimat, toimittaja korjaa löydetyt virheet
- dokumentoinnista vaiheen aikana vastaa toimittaja
- ohjeistuksen laatii toimittaja, taktisen käyttöohjeen puolustusvoimat
- hyväksymistestauksen, käyttöönoton ja koulutuksen suunnittelu on puolustusvoimien suorittamaa työtä [1]

Puolustusvoimat voi halutessaan käyttää ulkopuolista toimijaa (yritystä) tekemään katselmointeja sovellusprojektille. Tällaista auditointia suositellaan esimerkiksi sovelluksille, jotka ovat tietoturvallisuuden suhteen kriittisiä. Tietoturvallisuuteen ja tietoturvallisuusvaatimuksiin liittyen ARKKI-sovelluskehitysmallissa suositellaan ulkopuolisen toimijan suoritettavaksi seuraavia katselmointikohteita:

- Esitettyjen tietoturvaratkaisujen arvioiminen tarjousten katselmoinnin yhteydessä ennen toimittajan valintaa
- Tietoturvan suunnittelun laadun arvioiminen rakennusvaiheen ensimmäisen iteraation jälkeen
- Suorituskyky-, tietoturva- ja yhteenvetokatselmoinnin suorittaminen käyttöönottovaiheen aikana. Tämä sisältää tietoturvatarkastuksen. [1]

ARKKI-mallin mukaista ulkoisen toimijan suorittamaa tietoturvatarkastusta ei ole mainittu THP-menettelyä kuvaavassa normissa. Tarkastustoiminnan ohjeistavassa normissa [11] mahdollistetaan ulkopuolisen toimijan käyttäminen korkeintaan ST II – tasoiseen kehitystyöhön liittyen.

#### 5.4.4 Käyttöönottovaihe

Käyttöönottovaihe alkaa hyväksymistestauksen jälkeen. Samalla alkaa sovelluksen takuuaika ja se siirtyy omistajaorganisaatiolle käytettäväksi osana tietojärjestelmää, johon se on rakennettu. Käyttöönottovaihe sisältää koekäytön, käyttäjien koulutuksen sekä tuotantokäyttöönoton. Tuotantokäyttöluvan saaminen edellyttää hyväksytysti suoritettua tietoturva-akkreditointia. [1] Tietoturvallisuuden tarkastamista puolustusvoimissa käsitellään seuraavassa luvussa.

### 5.5 Yhteenveto

Luvussa kuvattiin lyhyesti arkkitehtuuriohjaus puolustusvoimissa sekä puolustusvoimien johtamisjärjestelmän teknisen tietoturvallisuuden arkkitehtuuri. Kokonaisarkkitehtuurin määrittämisessä ja arkkitehtuurin kehittämissuunnitelman laadinnassa käytetään Puolustusvoimien tietohallinnon arkkitehtuurikehikkoa, joka pohjautuu NATO:n arkkitehtuurikehikkoon.

ARKKI-sovelluskehitysmalli on puolustusvoimissa käytettävä sovelluskehitysmalli. ARKKI-sovelluskehitysmallin avulla vaiheistetaan ja ohjeistetaan puolustusvoimien ja toimittajan tehtävät sovellusprojekteissa. ARKKI-mallissa sovellusprojektit jaetaan neljään vaiheeseen, jotka ovat tavoiteasetteluvaihe, vaatimusmäärittelyvaihe, rakentamisvaihe ja käyttöönottovaihe. Näistä vaatimusmäärittelyvaihe on nimensä mukaisesti tärkein tietoturvallisuusvaatimusten määrittelemisen suhteen. Malli mahdollistaa ja jossain tapauksissa jopa suosittelee ulkopuolisen toimijan käyttämistä rakentamisvaiheen aikana tietoturvallisuuskatselmointien suorittamiseen. Myös seuraavassa luvussa lähteenä käytetty ja esitelty normi tietoturvallisuuden tarkastustoiminnasta puolustusvoimissa [11] mahdollistaa ulkopuolisen toimijan käyttämisen, jos kehitystyön sisältämä työ on korkeintaan tasoa ST II.

Seuraavassa luvussa kuvataan teknisen tietoturvallisuuden auditointia ja tarkastamista puolustusvoimissa. Luvussa käsitellään myös kansallista tietoturvallisuusviranomaistoimintaa.

# 6 Teknisen tietoturvallisuuden auditointi ja tarkastaminen puolustusvoimissa

## 6.1 Yleistä

Teknisen tietoturvallisuuden auditoinnista ja tarkastamisesta puolustusvoimissa määrätään Pääesikunnan johtamisjärjestelmäosaston laatimassa normissa [11]. Normi on ollut voimassa vuodesta 2010 lähtien ja on muiden johtamisjärjestelmäalan normien tapaan uudistumassa vuoden 2013 aikana. Normissa kuvataan teknisen tietoturvallisuuden tarkastamiseen liittyvä toiminta sekä määritellään siihen liittyvät tehtävät ja vastuut. Teknisen tietoturvallisuuden suunnittelun, rakentamisen, ylläpidon ja purkamisen prosessit sekä käyttöönoton hyväksyntä ovat osa tietohallintopäätösmenettelyä [11]. Teknistä tarkastustoimintaa suoritetaan osana tietohallintopäätösmenettelyä mutta sitä voidaan tarvittaessa suorittaa myös erillään THP-menettelystä esimerkiksi osana hankintaprosessia [11]. Tietohallintopäätösmenettelyn eri vaiheissa tapahtuvaa tarkastustoimintaa kuvataan tarkemmin kappaleessa 6.3.

Teknisen tietoturvallisuuden tarkastustoiminnan tavoitteena on varmistaa, että tietojärjestelmä, tietoliikennejärjestelmä, telejärjestelmä tai muu tietohallintopalvelu vastaa sille asetettua tietoturvatasoa ja tietoturvaluokitusvaatimuksia [11]. Normi määrittelee, että tekniset tarkastusperusteet määräytyvät lakien, säädösten, tietoturvatasojen, tietoturvapolitiikan ja – strategian perusteella sekä toiminnallisista ja teknisistä vaatimuksista. [11] Tarkastuksissa käytetään seuraavia kriteeristöjä soveltuvin osin:

1. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)
2. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010)

3. Muut VAHTI:n tietoturvallisuusasetukseen perustuvat ohjeet
4. Sisäverkko-ohje (VAHTI 3/2010)
5. ICT-varautuminen
6. Kansallinen turvallisuusauditointikriteeristö (KATAKRI)
7. EU:n kriteeristö, kun soveltuu ja on tarpeen
8. NATO:n kriteeristö, kun soveltuu ja on tarpeen [11]

Myös muiden kriteeristöjen käyttäminen on mahdollista, jos esimerkiksi kahdenväliset sopimukset näin määräävät. Kansainvälisten velvoitteiden osalta noudatetaan kansallisen turvallisuusviranomaisen antamia ohjeita. [11] Kansallinen turvallisuusviranomaistoiminta on kuvattu seuraavassa kappaleessa.

Normissa määritellään myös tiettyjä vastuita eri tahoille. Kehitystyön omistaja asettaa kehitystyölle tietoturvatasotavoitteen [11]. Tämä on tärkeä tehtävä, sillä akkreditointikriteerit ovat erilaisia eri tietoturvatasoilla. Tietoturvatason tulee perustua siihen, minkä tasoista tietoa kehitystyön kohteena olevassa järjestelmässä käsitellään. Pääesikunnan operatiivinen osasto asettaa toiminnalliset ja Pääesikunnan johtamisjärjestelmäosasto tekniset tietoturvallisuusvaatimukset [11]. Normi ei kuitenkaan kuvaa, mitä tämä käytännössä tarkoittaa, ja kuinka operatiivinen osasto ja johtamisjärjestelmäosasto käytännön vaatimusmäärittelytyöhön osallistuvat.

### 6.2 Kansallinen turvallisuusviranomaistoiminta

Suomessa toimii monien muiden maiden tapaan kansallinen turvallisuusviranomaisorganisaatio. Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) säätää kansallisen turvallisuusviranomaisen tehtäväkentän hoitamisesta Suomessa [24]. Laissa määritetään vastuut tapauksissa, joissa kansainvälistä erityissuojattavaa tietoaineistoa siirtyy maiden välillä - esimerkiksi suomalaisen ja ulkomaisen yrityksen välillä. Lain mukaisesti kansallisena turvallisuusviranomaisena (NSA, National Security Authority) toimii ulkoasiainministeriö. Ulkoasiainministeriö vastaa tämän velvoitteen myötä mm. kansainvälisten turvallisuussopimusten valmistelusta. Laissa nimetään määrätyiksi turvallisuusviranomaisiksi (DSA, Designated Security Authority) Suojelupoliisi (henkilöturvallisuusselvitykset), Pääesikunta (yhteisöturvallisuus- ja henkilöturvallisuusselvitykset) sekä puolustusministeriö. [28] Tietoturvallisuusviranomaistoiminnot puolustusvoimissa määritellään Pääesikunnan johtamisjärjestelmäosaston laatimassa normissa [12].

Kansallinen turvallisuusviranomainen eli ulkoasiainministeriö on valtuuttanut Viestintäviraston toimimaan tietoliikenneturvallisuusviranomaisena niissä tapauksissa, joissa on kyse teknisestä tietoturvallisuudesta ja tietoliikenteen turvallisuudesta. Tästä viranomaistehtävästä käytetään kansainvälisesti nimitystä NCSA, National Communication Security Authority. Tehtävä käsittää mm. tietojärjestelmien hyväksynnän tietylle turvallisuustasolle. [28] Pääesikunnan johtamisjärjestelmäosasto vastaa puolustusvoimien ja Viestintäviraston yhteistoiminnasta tietoturvallisuusviranomaisasioissa [12].


**Kuva 14** Kansallinen turvallisuusviranomaistoiminta Suomessa

### 6.2.1 NCSA-FI

Viestintäviraston NCSA-FI toiminnolla on sekä kansainvälisiä että kansallisia tietoturvavelvoitteita. Yksi NCSA-FI:n tietoturvavelvoitteisiin liittyvistä tehtävistä on viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointi. NCSA-FI:n arviointimenettelyn piiriin kuuluvat

- viranomaisen määräämisvallassa olevat tai hankittavaksi suunnitellemat järjestelmät, joista viranomainen on tehnyt Viestintävirastolle arviointipyynnön, ja
- valtiovarainministeriön pyynnöstä tehtävät selvitykset valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta. [36]

Lain viranomaisen tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011) pykälässä neljä säädetään Viestintäviraston tehtävistä. Lain mukaan Viestintäviraston tehtävänä on:

> 1) arvioida viranomaisen pyynnöstä tämän määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tai tietoliikennejärjestelyjen tietoturvallisuuden vaatimuksenmukaisuutta;
>
> 2) antaa tietojärjestelmälle tai tietoliikennejärjestelylle sen hyväksymistä osoittava todistus 8 §:ssä säädetyllä tavalla;
>
> 3) tehdä valtiovarainministeriön pyynnöstä selvityksiä valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta. [25]

Tietoturvallisuuden arviointiperusteista säädetään laissa siten, että arviointiperusteina voidaan käyttää

> 1) lailla tai asetuksella säädettyjä viranomaisten toimintaa koskevia tietoturvallisuusvaatimuksia ja valtiovarainministeriön tietoturvallisuutta koskevia ohjeita;
>
> 2) kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun kansallisen turvallisuusviranomaisen antamia kansainvälisten tietoturvallisuusvelvoitteiden toteuttamista koskevia ohjeita;
>
> 3) Euroopan unionin tai muun kansainvälisen toimielimen antamia tietoturvallisuutta koskevia säännöksiä ja ohjeita;
>
> 4) julkaistuja ja yleisesti tai alueellisesti sovellettuja tietototurvallisuutta koskevia säännöksiä, määräyksiä tai ohjeita;
>
> 5) vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia. [25]

Näin ollen laki mahdollistaa lähes minkä tahansa kriteeristön tai vastaavan käyttämisen tietoturvallisuuden arvioinnissa. On selvää, että käytännön soveltamisohje tietoturvallisuuden arviointiin tarvitaan, jotta eri toimijoilla on riittävät perusteet tuottaa Viestintäviraston tietoturvallisuuden arvioinnin läpäiseviä järjestelmiä.

Kaiken kaikkiaan käytännöt tässä toiminnossa ovat vielä muotoutumassa, sillä toimintaa ohjaavat lait ovat olleet voimassa vasta vuodesta 2012. Valtiovarainministeriö on kuitenkin lain voimaantulon jälkeen linjannut [37], että se voi tarvittaessa pyytää Viestintävirastoa tarkastamaan viranomaisen, mikäli se ”huomaa puutteita tietoturvallisuusasetuksen toimeenpanossa”. Puolustusvoimat on perinteisesti huolehtinut itse omien järjestelmiensä tar-

kastamisesta mutta lain 1406/2011 myötä myös ulkopuolisen pyynnöstä tapahtuviin ja ulkopuolisen toimesta suoritettaviin tarkastuksiin on varauduttava.

### 6.2.2 SAA ja CAA

SAA ja CAA ovat kansallisia turvallisuus- ja tietoturvaviranomaisia. Puolustusvoimilla on omat SAA- ja CAA-viranomaisensa omien järjestelmiensä akkreditointia ja omassa käytössä olevien salaustuotteiden hyväksymistä varten. Molemmissa toiminnoissa tehdään yhteistyötä NSCA-FI:n kanssa. [29]

SAA, eli Security Accreditation Authority hoitaa turvallisuusjärjestelyt hyväksyvän viranomaisen tehtävät. SAA siis vastaa luokiteltua tietoa käsittelevien tieto- ja tietoliikennejärjestelmien tietoturva-akkreditoinneista. Puolustusvoimissa SAA voi akkreditoida myös vain julkista tietoa sisältäviä järjestelmiä, mikäli ne ovat laajuudeltaan, kustannuksiltaan tai julkiselta näkyvyydeltään merkittäviä [17]. CAA, eli Crypto Approval Authority hoitaa salaustuotteiden hyväksyntäviranomaisen tehtävät. CAA varmistaa, että valitut salaustuotteet ovat kryptografisesti turvallisia. [29]

## 6.3 Teknisen tietoturvallisuuden tarkastus- ja akkreditointiprosessi puolustusvoimissa

Seuraavassa kuvassa on kuvattu teknisen tietoturvallisuuden tarkastus- ja akkreditointiprosessi ja sen toimijat puolustusvoimissa siten, kuin teknisen tietoturvallisuuden tarkastamisen normi [11] prosessin määrittelee. Eri vaiheet kuvataan tarkemmin seuraavissa kappaleissa.


**Kuva 15** Teknisen tietoturvallisuuden tarkastus- ja akkreditointiprosessi puolustusvoimissa [11]

### 6.3.1 Tietoturvatarkastus

Tietoturvatarkastuksella, josta voidaan käyttää myös termejä tietoturva-arviointi tai tietoturva-auditointi, tarkoitetaan sen seikan selvittämistä, täyt-

tääkö tietty kohde sille asetetut tietoturvallisuusvaatimukset eri osiltaan [11]. Tietoturvatarkastus tulisi THP-normin [10] mukaan olla riippumattoman tahon suorittama. Riippumattomuudella tarkoitetaan esimerkiksi sitä, ettei tarkastava taho ole ollut määrittelemässä tai toteuttamassa tarkastuksen kohdetta. Tämän tutkimuksen kannalta ei ole tarpeen erotella tietoturvatarkastusta, tietoturva-auditointia ja tietoturva-arviointia toisistaan. Niillä voidaan tarkoittaa joko täysin samoja tai hieman eri asioita mutta tässä kontekstissa sillä ei ole merkitystä. Oleellista tämän tutkimuksen kannalta on erottaa tietoturva-akkreditointi muista tietoturvallisuuteen liittyvistä tarkastuksista ja auditoinneista.

Kuten luvun alussa todettiin, tietoturvatarkastustoimintaa voidaan suorittaa osana THP-menettelyä tai erillisenä, esimerkiksi osana hankintaprosessia. Osana THP-menettelyä tarkastustoimintaa suoritetaan tarkastustoiminnan ohjeistavan normin mukaan seuraavasti. Tehtävät eri vaiheissa on sisällytetty myös liitteen 2 taulukkoon.

Ideoinnista esisuunnitteluun – vaiheessa (THP 1) suoritetaan Pääesikunnan johtamisjärjestelmäosaston toimesta tietoturva-arviointi perustuen kehitystyön sen hetkiseen dokumentaatioon. Suoritettavan arvioinnin tarkoituksena on tunnistaa ne rakenteet, joita vaaditaan asetetun tietoturvatason (suojaustason) täyttämiseksi. [11]

Esisuunnittelusta suunnitteluun – vaiheessa (THP 2) suoritetaan Pääesikunnan johtamisjärjestelmäosaston toimenpitein vastaava arviointi, kuin tietohallintopäätösmenettelyn pisteessä yksi (THP 1). Arvioinnissa tarkastetaan myös, onko vaiheessa yksi mahdollisesti annetut huomautukset korjattu. Arvioinnista tiedotetaan SAA-toimijaa. [11]

Suunnittelusta rakentamiseen – vaiheessa (THP 3) suoritetaan kahden edeltävän vaiheen kaltainen tietoturva-arviointi mutta se suoritetaan tässä vaiheessa Puolustusvoimien johtamisjärjestelmäkeskuksen THP-ryhmän toimenpitein. Tästäkin arvioinnista tiedotetaan SAA-toimijaa. [11]

Vaiheessa rakentamisesta operointiin (THP 4) suoritetaan tietoturva-akkreditointi [11], joka kuvataan kappaleessa 6.3.2.

Operointivaiheessa (THP 5) suoritetaan teknisiä tietoturvatarkastuksia ja –auditointeja osana tuotantokäytön aikaista toimintaa. Tarkastus voidaan

ajoittaa esimerkiksi päivitysten yhteyteen tai suorittaa sovitusti määräajoin. Kehitystyön omistaja päättää tarkastusten ajankohdasta. Tarkastukset voi suorittaa kuka tahansa puolustusvoimissa hyväksytty tarkastustoimija. [11]

Operoinnista purkuun – vaiheessa (THP 6) arvioidaan purkamis- ja luopumissuunnitelmien vaikutus palveluympäristön tietoturvallisuuteen. Osana THP 6 – päätöstä annetaan purkamislupa teknisen tietoturvallisuuden osalta. Arviointi suoritetaan Pääesikunnan johtamisjärjestelmäosaston toimesta. [11]

Kaikkien edellä mainittujen vaiheiden (ml. luvussa 6.3.2 tarkemmin kuvattu tietoturva-akkreditointi) tarkastuksista syntyneet raportit toimitetaan tarkastuksen tilaajalle, kehitystyön omistajalle, Pääesikunnan johtamisjärjestelmäosastolle, Pääesikunnan operatiiviselle osastolle sekä SAA-toimijalle eli Pääesikunnan tutkintaosastolle. Tarkastuksen tulos voi olla hyväksytty, hyväksytty korjauksin tai hylätty. Pääesikunnan johtamisjärjestelmäosaston päällikkö hyväksyy tarkastustoiminnan raportin perusteella kehitystyön suunnittelun etenemisen, rakentamisen, käyttöönoton tai purkamisen osana tietohallintopäätöstä. [11]

### 6.3.2 Tietoturva-akkreditointi

Kuten käsitemäärittelyissä todettiin, tietoturva-akkreditoinnilla tarkoitetaan järjestelmän tietoturvallisuuden pätevyyden tai kelpoisuuden toteamista tähän oikeutetun tai muuten luotetun tahon toimesta [10]. Akkreditointi voi sisältää tietoturva-auditoinnin tai – tarkastuksen tai se voi hyödyntää niiden tuloksia [11]. Tietoturva-auditoinnin tai – tarkastuksen voi näissä tapauksissa suorittaa muu, kuin akkreditoiva taho. Akkreditointi on aina määräaikainen ja se voi lisäksi olla ehdollinen [11]. Akkreditoinnin tarkoituksena on todentaa, että tietojärjestelmä täyttää suojaustason mukaiset kriteerit. Pääkriteeristönä käytetään kansallisen turvallisuusauditointikriteeristö KATAKRI:n versiota II. [29]

Tietoturva-akkreditointi suoritetaan THP-menettelyn rakentamisesta operointiin – vaiheessa (THP 4). Akkreditointi perustuu kehitystyön dokumentaatioon ja toteutukseen. Akkreditoinnissa varmistetaan myös resursoinnin riittävyys, pisteessä THP 3 annettujen tietoturvaehtojen toteutuminen sekä toipumissuunnitelmat. [11]

Akkreditoinnissa käsitellään erityisesti seuraavia ARKKI-sovelluskehitysmallin mukaisia dokumentteja:

- PH10 Tavoiteasetteluasiakirja
- PH30 PV:n projektisuunnitelma
- PH40 Toimittajan projektisuunnitelma
- TA20 Teknisen arkkitehtuurin kuvaus
- TA30 Tuotantoympäristön kuvaus
- MS70 Tietovaraston suunnittelu
- MS40 Sovellusarkkitehtuurin kuvaus
- TU10 Ylläpitosuunnitelma
- TU20 Tukiorganisaation valmiusraportti
- VH10 Tavoitetilan kuvaukset
- VH40 Käyttötapauskuvaukset
- Toipumissuunnitelma, mikäli ei ole osana projektisuunnitelmaa
- Tietoturvadokumentaatio, mikäli ei ole osana projektisuunnitelmaa [17]

Tarkastettavat alueet jakaantuvat tietotasolle, järjestelmätasolle, sovellustasolle sekä verkkotasolle [17]. Tässä tutkimuksessa ei kuvata tarkemmin tarkastuksen kohteita tai menetelmiä, sillä ne eivät kaikilta osin ole julkisia.

Puolustusvoimien SAA-toimijan antama akkreditointilausunto pyritään antamaan kolmen vuoden määräajaksi mutta se voi vaihdella kohteesta riippuen [17]. Seuraavassa taulukossa on kuvattu tietojärjestelmän päivitystarpeita ja niiden merkitystä uudelleen akkreditoinnin tarpeeseen. Taulukko on esimerkinomainen eikä sisällä kaikkia tapauksia.

**Taulukko 1** Uudelleenakkreditoinnin tarve eri tilanteissa, esimerkkejä [17]

| Uusi akkreditointi | Ei uutta akkreditointia |
|---|---|
| • uusien kehityspiirteiden käyttöönotto<br>• liittymien käyttöönotto muihin järjestelmiin<br>• salausratkaisujen ja avaintenhallinnan käytäntöjen muuttaminen<br>• liitosten tekeminen uusiin verkkoihin | • järjestelmän toiminnallisuuteen liittyvät korjauspäivitykset<br>• tietoturvapäivitykset<br>• pienimuotoiset versionnostot |

NCSA-FI:n SAA-toimijalla on oma ohjeistuksensa [27] akkreditoinnin voimassaoloajasta sekä esimerkiksi siitä, minkälaiset muutokset edellyttävät

uutta akkreditointia. Tässä tutkimuksessa keskitytään kuitenkin kuvaamaan puolustusvoimien SAA-toimijan käytäntöjä, tutkimuksen viitekehys huomioon ottaen.

#### 6.3.3 Tuotantokäyttölupa

Pääesikunnan tutkintaosasto laatii SAA-toimijan ominaisuudessa hyväksytystä turvallisuusakkreditoinnista lausunnon, jonka perusteella Pääesikunnan johtamisjärjestelmäosasto hyväksyy tietojärjestelmän tuotantokäyttöön, eli myöntää tuotantokäyttöluvan. Mikäli järjestelmän akkreditoinnin on suorittanut NCSA-FI (esimerkiksi kansainvälisten tietoturvavelvoitteiden vuoksi), voidaan tuotantokäyttölupa myöntää myös NCSA-FI:n hyväksyntäpäätöksen perusteella. [29]

### 6.4 Yhteenveto

Teknisen tietoturvallisuuden auditointia ja tarkastamista puolustusvoimissa ohjataan omalla normillaan. Normi on ollut voimassa vuodesta 2010 ja on muiden Pääesikunnan johtamisjärjestelmäosaston normien lailla uudistumassa vuoden 2013 aikana. Normi kuvaa selkeästi THP-vaiheittain tarkastukseen liittyvät tehtävät ja vastuutahot. Normissa kuvataan myös joitakin tietoturvallisuuteen liittyviä määrittelyvastuita mutta ei tarkemmin sitä, kuinka nämä tehtävät konkretisoituvat.

Kansallinen tietoturvallisuusviranomaistoiminta Suomessa on ulkoasiainministeriön johtamaa. Ulkoasiainministeriö on valtuuttanut Viestintäviraston toimimaan tietoliikenneturvallisuusviranomaisena eli NCSA-FI:nä niissä tapauksissa, joissa on kyse teknisestä tietoturvallisuudesta ja tietoliikenteen turvallisuudesta. Tehtävä käsittää mm. tietojärjestelmien hyväksynnän tietylle turvallisuustasolle. Vaikka Viestintävirasto on Suomen NCSA-FI -viranomainen, on puolustusvoimilla on omat SAA- ja CAA-toimijansa omien järjestelmiensä arviointia varten. Molemmissa toiminnoissa tehdään yhteistyötä NCSA-FI:n kanssa. SAA-toimija on tämän tutkimuksen kannalta keskeinen, sillä SAA suorittaa tietoturvallisuusakkreditoinnin THP 4 – vaiheessa rakentamisesta operointiin.

Luvussa kuvattiin myös teknisen tietoturvallisuuden tarkastus- ja akkreditointiprosessi puolustusvoimissa. Prosessiin kuuluu tietoturvatarkastus, tietoturva-akkreditointi sekä tuotantokäyttöluvan myöntäminen.

Seuraavassa luvussa kootaan tutkimuksessa kuvattuja asioita yhteen, eli vastataan luvussa kaksi esitettyjen tutkimusongelmien kysymyksiin. Tietoturvallisuusvaatimusten asettamiseen ja todentamiseen liittyviä tehtäviä on kuvattu myös liitteessä 2, johon on koottu yhteen eri lähteistä saatu tieto. Seuraavassa luvussa esitetään myös tutkimuksen löydösten perusteella tehtyjä kehitysehdotuksia.

# 7 Tietoturvallisuusvaatimukset THP-menettelyn mukaisissa tietojärjestelmähankkeissa

## 7.1 Tietoturvallisuusvaatimukset ja hanketoiminta

Hanketoimintaa ohjaavat normit, etenkin pysyväisasiakirja Hanketoiminta puolustusvoimissa [5] sekä pysyväisasiakirja Elinjaksoauditoinnit puolustusvoimissa [6] käsittelevät hankkeita niiden vaiheiden kautta. Lähtökohtana on jonkun suorituskyvyn kehittäminen. Vaiheistus on selkeä ja tehtävät eri vaiheissa on kuvattu vastuineen melko yksiselitteisesti. Tietoturvallisuutta ei kuitenkaan vastuissa tai tehtävissä käytännössä mainita. Ottaen huomioon tietoturvallisuuden kasvavan merkityksen tietojärjestelmähankkeissa, tulisi se huomioida myös hanketason vastuissa ja tehtävissä. Tietoturvallisuuden tulisikin näkyä myös hankesuunnittelussa, eikä pelkästään elinjaksoauditoinneissa THP-menettelyn kautta.

## 7.2 Tietoturvallisuusvaatimukset ja ARKKI-sovelluskehitysmalli

ARKKI-sovelluskehitysmallissa korostuu tietoturvavaatimusten ja tietoturvallisuuden osalta todentamiseen liittyvät vastuut.

Mallissa kuvataan audit-toiminta, joka tarkoittaa ulkopuolisen toimijan käyttämistä sovellusprojektiin liittyvissä katselmoinneissa. Yksi audit-toiminnan tavoitteista on tietoturvallisuuteen liittyvien ongelmien löytäminen aikaisessa vaiheessa. Mikäli ulkopuolista toimijaa ei käytetä, tulee katselmoinnit ja muut audit-toiminnalle suunnitellut tehtävät suorittaa sisäisin toimenpitein. Ulkopuolisen toimijan käyttöä tulee harkita etenkin silloin, jos sovellus on kriittinen ja laaja, tai jos osaamista ja/tai resursseja tietoturvallisuuden arviointiin ei ole. Mikäli audit-toiminnan tuloksia halutaan hyödyntää akkreditoinnissa, tulee tulosten hyödynnettävyys varmistaa etukäteen. Käytännössä toiminnan tulee silloin olla lain 1406/2011 mukaista. ARKKI-

mallissa audit-toimintaan liittyen on kuvattu tietoturvatehtäviä selkeästi ja hyvin. Kappaletta ei tule missään nimessä sivuuttaa, vaan tehtävät tulee suorittaa joko omin tai ulkopuolisen toimijan toimenpitein. Valitettavasti vain tehtävät painottuvat tietoturvan tarkastamiseen, määrittelyyn liittyvien tehtävien ja vastuiden jäädessä käytännössä kuvaamatta. Mallissa on yksittäisiä mainintoja tietoturvallisuudesta mutta ne eivät todellisuudessa kuvaa sitä, mitä ja kenen tulisi tehdä. On vaikea sanoa, onko vastuuttaminen jätetty tarkoituksella määrittelemättä, vai eikö sitä ole osattu sisällyttää sovelluskehitysmalliin.

### 7.3 Tietoturvallisuuteen liittyvä tarkastustoiminta

Tietoturvallisuuden teknistä tarkastusta puolustusvoimissa ohjeistava normi [11] määrittelee selkeästi tarkastustoimintaan liittyvät tehtävät ja vastuut kussakin THP-vaiheessa. Normissa kuvataan, että Pääesikunnan operatiivinen osasto asettaa toiminnalliset tietoturvavaatimukset, ja Pääesikunnan johtamisjärjestelmäosasto tekniset tietoturvavaatimukset. Tekniset tietoturvavaatimukset määritellään johtamisjärjestelmien osalta Puolustusvoimien johtamisjärjestelmän teknisen tietoturvallisuuden arkkitehtuurissa [8].

Pääkriteeristönä tietoturva-akkreditoinnissa käytetään SAA-toimijan oman ilmoituksen mukaan [29] KATAKRIn toista versiota kun taas tarkastustoimintaa ohjaavassa normissa [11] ensimmäisenä mainitaan Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa [19]. KATAKRI on tässä normissa mainittuna vasta kuudentena kriteeristönä. Puolustusvoimien ohjeistuksessa on siis tältä osin ristiriitaa. Etenkin akkreditointitoiminnan ohjeistuksen tulisi olla riittävän tarkalla tasolla ja yksiselitteistä, jotta hankkeissa ja sovelluskehityksessä pystytään valmistautumaan akkreditointiin parhaalla mahdollisella tavalla. Tällä hetkellä tilanne ei näin ole. Riittämätön valmistautuminen akkreditointiin haittaa sekä SAA-toimijaa, että hidastaa hankkeita ja projekteja THP-päätösten mahdollisesti viivästyessä.

### 7.4 Vertailua Sovelluskehityksen tietoturvaohjeeseen (VAHTI 1/2013)

Sovelluskehityksen tietoturvaohjeen tavoitteena on ohjeen mukaan [34, s. 11] opastaa sovelluskehittäjiä ottamaan tietoturvavaatimukset huomioon sovelluskehityksen kaikissa vaiheissa jo alusta lähtien. Ohjeessa annetaan tietoturvavaatimukset tietoturvatasoittain sovelluskehityksen eri vaiheisiin.

Ohje soveltuu sekä lineaariseen, että iteratiiviseen sovelluskehitykseen. [34, s. 7]

Ohjeen mukaan sen tavoitteena on:

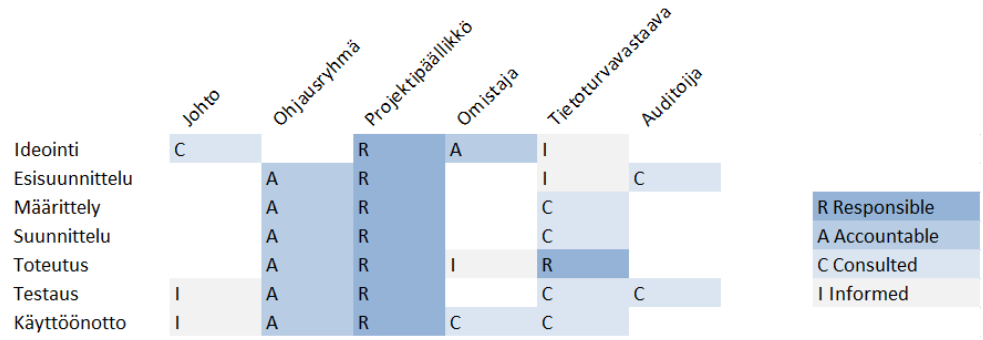
- tukea sovelluskehitystä niin, että sovellukset saavuttavat riittävän tietoturvallisuuden tason suhteessa sovelluksen käyttökohteisiin
- tukea julkishallinnon organisaatioita sovelluskehityshankkeiden läpiviennissä, valmisohjelmistojen hankinnoissa sekä ylläpitoon liittyvissä tietoturvatehtävissä
- varmistaa julkishallinnon sovellusten tietoturvallinen toteutus
- turvata organisaatioiden toiminnan jatkuvuus kaikissa olosuhteissa siltä osin, että tietojärjestelmät ovat käytettävissä
- mahdollistaa sovelluskehityksen arviointi tietoturvatasojen mukaisesti, sekä
- toimia vaatimusmäärittelyn tukena sovelluskehitystyötä hankittaessa [34, s. 12]

Ohjeen mukaan sovelluskehityksen tietoturvavaatimusten lähtökohtana tulisi olla sovelluksen kriittisyys ja sovelluksessa käsiteltävän tiedon merkitys organisaation toiminnalle [34, s. 15].

VAHTI 1/2013 sisältää sovelluskehityksen eri vaiheiden lisäksi organisaatioon liittyviä yleisiä vaatimuksia. Vertailua on kuitenkin tässä tutkimuksessa tarkoituksenmukaista tehdä keskittyen pelkästään sovelluskehityksen vaiheisiin sekä tietoturvavastuisiin liittyen.

Sovelluskehityksen tietoturvaohjeessa suositellaan ns. RACI-mallin käyttöä tietoturvavastuiden ja työnjaon kuvaamiseksi. Vastuiden ja tehtävien selkeällä määrittelyllä varmistetaan ohjeen mukaan tietoturvallisuuden toteutuminen projektin kaikissa vaiheissa. Ohjeessa on selkeästi kuvattu eri roolit ja niihin liittyvät tietoturvavastuut. Ohje muistuttaa tältä osin hankesuunnittelua ohjaavan pysyväisasiakirjan [5] kuvauksia sillä erolla, että tässä keskitytään tietoturvavastuisiin. RACI-mallia ei mainita ARKKI-sovelluskehitysohjeessa mutta sen käyttäminen olisi hyödyllistä myös puolustusvoimissa vastuunjaon selkeyttämiseksi. RACI-taulukon lisäksi tietoturvavastuut olisi syytä kuvata myös sanallisesti VAHTI-ohjeen [34, s. 21-24] tapaan. Osaamisen varmistaminen on tärkeä osa tietoturvavastuiden

määrittelemistä. Tehtäviä ei ole järkevää vastuuttaa sellaiselle taholle, jolla ei ole osaamista tehtävän suorittamiseksi. Tietoturvaosaamisen lisääminen ja kehittäminen sekä toisaalta osaamisen ja osaajien säilyttäminen tulee olemaan keskeistä puolustusvoimissa tulevaisuudessa.




**Kuva 16** Esimerkki RACI-mallin käytöstä sovelluskehitysprojektin roolien tehtävistä eri vaiheissa sovelluskehitystä [34 mukaillen]

Sovelluskehityksen tietoturvaohjeen liitteessä 1 [34, s. 72] on ohjeen sisältämät tietoturvavaatimukset koottuna taulukkomuotoon. Taulukossa on sekä aiemmin mainittuja organisaatioon liittyviä yleisiä vaatimuksia, että sovelluskehitykseen liittyvät vaatimukset kuvattuna vaiheittain. Sovelluskehitysmallin käsittely alkaa kohdasta 7 [34, s. 79]. Tämän jälkeen vaatimukset ovat lueteltuna vaiheittain. Vaiheet ovat esitutkimus, vaatimusmäärittely, suunnittelu, toteutus, testaus, käyttöönotto ja ylläpito. Vaatimukset on jokaisessa vaiheessa kuvattu tietoturvatasoittain, eli perustason, korotetun tason ja korkean tason vaatimuksiin jaoteltuina. Lisäksi on määritelty, onko vaatimus tasolla suositus, vahva suositus vai pakollinen vaatimus, ja se, tarvitseeko vaatimus liittää tarjouspyyntöön. Vaatimukset, joita ei liitetä tarjouspyyntöön, voidaan tulkita puolustusvoimien omaksi työksi.

Taulukko on erittäin hyödyntämiskelpoinen myös puolustusvoimissa, ottaen huomioon, että se perustuu tietoturvallisuusasetuksen vaatimuksiin, muihin VAHTI-ohjeisiin ja KATAKRIn keskeisiin sovelluskehitystä koskeviin kriteereihin [34, s. 7]. Puolustusvoimien johtamisjärjestelmän teknisen tietoturvallisuuden arkkitehtuuri muistuttaa vaatimuksien abstraktiotasoltaan VAHTI 1/2013 – ohjetta mutta siinä lähestymistapa on arkkitehtuurikuvaukseen perustuva. Teknisen tietoturvallisuuden arkkitehtuuri ei siten suoraan vaiheista eri vaatimuksien määrittelyä vaikka eri arkkitehtuurikuvausten tarkastelu onkin määritelty tietohallintoauditointien arkkitehtuuriarvioinneissa tehtäväksi. Vaiheet eivät dokumentissa käy kuitenkaan yhtä hyvin

selville, kuin Sovelluskehityksen tietoturvaohjeessa. Henkilölle, jolle puolustusvoimien arkkitehtuurikuvaukset ovat tuttuja, on teknisen tietoturvallisuuden arkkitehtuuri hyvin ymmärrettävä. Dokumentin etuna on luonnollisesti se, että se on kokonaan puolustusvoimien lähtökohdista ja tarpeisiin kirjoitettu, olkoonkin että kohteena on puolustusvoimien johtamisjärjestelmä. Sovelluskehityksen tietoturvaohje taas edustaa perinteisen inkrementaalisen sovelluskehitysprojektin lähestymistapaa, ja on siten ymmärrettävä myös puolustusvoimien arkkitehtuuriohjausta vähemmän tuntevalle taholle. Molemmissa ohjeissa on sama perusta, eli tietoturvallisuusasetus ja muut lakipohja, VAHTI-ohjeet sekä KATAKRI. VAHTI-ohjeen etuna on myös sen julkisuus ja saatavuus, sekä sovellettavuus myös muihin, kuin puolustusvoimien johtamisjärjestelmiin.

## 7.5 Kehitysehdotuksia

Seuraavassa kuvataan tämän tutkimuksen tuloksena syntyneitä kehitysehdotuksia.

### 7.5.1 Normipohjan harmonisointi

Kaiken kaikkiaan tässä tutkimuksessa kuvattu normipohja on uudistamisen ja harmonisoinnin tarpeessa ja tarpeellinen uudistustyö onkin käynnissä. Uudistamistarpeen aiheuttaa jo pelkästään normien ikä, sekä jatkuvasti kehittyvä sovelluskehityksen ja tietoturvallisuuden toimintaympäristö. Normeissa käytettävä sanasto tulisi yhtenäistää. Erityisesti eri toimijoista käytettävien nimitysten tulisi olla yhtenevät kaikissa normeissa yhtenäisen kokonaiskuvan muodostamiseksi. Esimerkiksi tarkastustoimintaa ohjaava normi [11] puhuu kehitystyön omistajasta, mitä termiä hanketoimintaa tai THP-menettelyä ohjeistavat normit eivät tunne. ARKKI-sovelluskehitysmallissa puhutaan järjestelmän omistajasta ja hanketoimintaa ohjaavissa normeissa suorituskykyvastuullisesta tahosta sekä järjestelmävastuullisesta tahosta. Selkeät ja yhtenevät nimitykset ovat edellytys onnistuneelle vastuutukselle.

### 7.5.2 Kokonaiskuva THP-prosessista ja sen toimivuudesta

Tämän tutkimuksen viitekehykseen sisältyvät asiat eli arkkitehtuuriohjaus ja sovelluskehitys, hanketoiminta, teknisen tietoturvallisuuden auditointi ja tarkastus sekä THP-menettely ovat vastuutettu laajasti eri puolille puolustusvoimien organisaatiota. THP-menettely on kyllä Pääesikunnan johtamis-

järjestelmäosaston omistama prosessi mutta siihen liittyy monia muita laajoja kokonaisuuksia viitekehyksen mukaisesti. Vastuuta on niin Pääesikunnan johtamisjärjestelmäosastolla, Pääesikunnan materiaaliosastolla, Pääesikunnan operatiivisella osastolla, Pääesikunnan tutkintaosastolla, Puolustusvoimien johtamisjärjestelmäkeskuksella kuin puolustushaaroillakin. Vastuun ja toimintojen jakautumisessa on vaarana se, ettei kokonaiskuvaa muodostu kenellekään eikä etenkään kehittämistarpeita tästä syystä tunnisteta. THP-prosessin omistajan tulisikin huolehtia, että myös prosessiin liittyvät asiat ja toiminnot tulevat riittävällä tarkkuudella huomioitua – ja toisaalta myös ohjeistettua.

#### 7.5.3 Riittävä valmius turvallisuusakkreditointiin ja akkreditointikriteerien tarkoituksenmukainen käyttö

SAA-toimijan suorittama tietoturvallisuusakkreditointi tulisi sitoa selvemmin osaksi tietohallintopäätösmenettelyä. Sen tulisi näkyä muutenkin kuin tietyssä pisteessä tehtävänä tarkasteluna. Yhteistyötä akkreditoivan tahon kanssa tulisi mahdollisuuksien mukaan tehdä järjestelmä- tai sovelluskehityksen alusta alkaen. SAA-toimijan tulisi antaa riittävää ohjausta projekteille. Akkreditoinnin tarkastelukohteiden ja kriteereiden tulisi, mahdollisuuksien mukaan, olla selvillä jo vaatimusmäärittelyvaiheessa. Tämä on haasteellista erityisesti hankkeissa, jotka kestävät vuosia ja joiden aikana akkreditointikriteeristöt kehittyvät ja uudistuvat. Akkreditoinnissa mahdollisesti löytyneiden puutteiden korjaaminen jälkikäteen on usein hankalaa ja kallista. Näitä puutteita ei mahdollisesti ole pystytty tunnistamaan vaatimusmäärittelyvaiheessa. Akkreditoinnissa tulisikin arvioida järjestelmää huomioiden sen kehittämisen aikaiset kriteeristöt ja mahdollisten puutteiden aiheuttamat jäännösriskit. Tässä nousee oleelliseen osaan järjestelmän riskianalyysi. THP-normin uudistustyössä on pyritty ottamaan huomioon tietoturvatasojen riskienhallintaan liittyvät vaatimukset ja se, mikä niiden merkitys on nimenomaan THP-prosessissa. Riskienhallinta on nähty ongelmallisena THP-prosessissa esimerkiksi siksi, ettei ymmärretä sen hyötyjä. Yhtenä ratkaisumallina normin uudistustyön aikana on esitetty hankkeisiin nimettävää tietoturvavastaavaa, jonka vastuulla olisi myös riskienhallinta. Päätöksiä tämän suhteen ei ole kuitenkaan vielä tehty.

Akkreditointi ei kuitenkaan saa ohjata rakentamista siten, että vain akkreditointikriteeristön tai – kriteeristöjen mukaiset vaatimukset toteutetaan. On muistettava, että kriteeristöt eivät ole yhtä kuin vaatimusmäärittely. Termejä

käytetään usein virheellisesti jopa toistensa synonyymeinä. Vaatimusten tulee lakisääteisten tai muiden normipohjaisten velvoitteiden lisäksi perustua operatiivisiin, suorituskykyyn liittyviin tarpeisiin. Vaatimuksilla tulee myös vastata uhka-arvion avulla selville saatuihin tietojärjestelmään kohdistuviin uhkiin niin, että järjestelmästä tulee ominaisuuksiltaan sekä käytöltään mahdollisimman turvallinen. Sovelluskehityksen tietoturvaohjekin korostaa, että tietoturvavaatimusten lähtökohtana tulee olla sovelluksen kriittisyys ja sovelluksessa käsiteltävien tietojen merkitys organisaatiolle [34, s. 15]. Erikoissuunnittelija Petri Kiiskilä on kirjoittanut aiheesta Insinööriupseeri 2012 – julkaisussa otsikolla ”KATAKRI – ilmavoimat lentää vieläkin” [21, s. 35–36]. Kiiskilän mukaan KATAKRIn velvoittavuutta on tulkittu siten, että auditointikriteeri on yhtä kuin vaatimus, ja että kaikkien vaatimusten tulee toteutua. Tästä seuraa se, että kaikissa tietojärjestelmähankkeissa pyritään torjumaan kaikkia tietoturvallisuusuhkia, toimintaympäristöstä riippumatta. Kiiskilä kritisoi mielestäni täysin aiheellisesti sitä, että KATAKRIn käyttöönoton jälkeen turvallisuusuhkien ja riskien tunnistaminen on jätetty tekemättä ja tekniset ja hallinnolliset ratkaisut on uhka-arvion sijaan perusteltu sillä, että KATAKRI näin vaatii. Kiiskilän mukaan ”Satojen tietoturvallisuuden toteuttamista ohjaavien lakien, asetuksien, normien ja ohjeistuksien joukosta on poimittu yksi kaksiosainen julkaisu, josta on tullut puolustusvoimien tietoturvallisuuden synonyymi?” Mielestäni tilanne puolustusvoimien tietojärjestelmäkehityksessä on hyvin pitkälle Kiiskilän kuvaaman kaltainen, ja yhdyn hänen esittämäänsä kritiikkiin. Kiiskilän mukaan KATAKRIn tehokas käyttö edellyttäisi tietoturvallisuusuhkien ja riskien tunnistamista sekä sitä, että tunnistetuille uhkille ja riskeille löydettäisiin omistaja. Omistajalla pitäisi myös olla tarvittavat resurssit uhkan tai uhkien pienentämiseksi. Vaatimustenhallinta on laajemminkin yksi iso kokonaisuus, jossa on selkeitä kehittämistarpeita. Tähänkin liittyen on käynnissä kehittämistyötä, yhtenä esimerkkinä DOORIS-projekti [33].

#### 7.5.4 Tietoturvavastuut ja niiden kuvaaminen

Tietoturvavastuut tulisi kuvata selkeämmin hankesuunnittelun ohjauksessa, THP-menettelyssä sekä sovelluskehitysmallissa. Kuten kappaleen alussa todettiin, etenkin vastuiden kuvaamisessa tulisi käyttää yhteneviä nimityksiä kaikissa ohjeistavissa dokumenteissa. Kuvaamisessa voisi hyödyntää RACI-mallia sekä Sovelluskehityksen tietoturvaohjetta. Vastuuttaminen edellyttää osaamista, sillä ei ole järkevää vastuuttaa jotakin taholle, joka ei ole sitä

kykenevä suorittamaan. Puolustusvoimien tietoturvaosaamisen varmistaminen – osaamisen kasvattaminen ja ylläpito – on siis ensiarvoisen tärkeää jo tietoturvavastuiden toteutumisenkin kannalta.

ARKKI-sovelluskehitysmallissa suositellaan myös tiettyjen katselmointien suorittamista ulkopuolisen toimijan toimesta. Tarkastustoimintaa ohjeistava normi [11] mahdollistaa ulkopuolisen toimijan käytön, jos kehitystyö sisältää korkeintaan ST II – tasoista tietoa. Ohjeistusta voisi tältä osin selkeyttää ja saatujen tulosten hyödynnettävyyttä tietohallintopäätösmenettelyssä ja erityisesti akkreditoinnissa pohtia. Ihannetapauksessa saatuja tuloksia tulisi voida hyödyntää akkreditoinnissa.

### 7.5.5 Yhteenveto kehitysehdotuksista

Tutkimuksen tuloksena syntyneet kehitysehdotukset on koottu seuraavaan kuvaan.


**Kuva 17** Tutkimuksen kehitysehdotukset

# 8 Yhteenveto

Tämän tutkimuksen tavoitteena oli selvittää, kuinka tietoturvallisuusvaatimukset esiintyvät puolustusvoimien tietohallintopäätösmenettelyn mukaisissa tietojärjestelmähankkeissa ja niihin kuuluvissa sovelluskehitysprojekteissa. Tutkimusongelmaa lähestyttiin ensisijaisesti kirjallisuuskatsauksen avulla, toisin sanoen selvittämällä, kuinka asia on puolustusvoimissa ohjeistettu ja määrätty.

Tietohallintopäätösmenettelyn ohjeistava normi on muiden johtamisjärjestelmäalan normien tavoin uudistumassa. Selkeitä uudistus- ja harmonisointitarpeita normipohjassa on havaittavissa. Tietohallintopäätösmenettelyn ohjeistava normi on ollut voimassa vuodesta 2009, hanketoiminnan ohjeistavat normit jo vuodesta 2007. Asetus tietoturvallisuudesta valtionhallinnossa on astunut voimaan vuonna 2010 ja tietoturvallisuus on kaiken kaikkiaan, esimerkiksi uhkien ja teknisten ratkaisujen osalta muuttunut merkittävästi viime vuosina. On tärkeää, että hanketoimintaa ohjaavat normit, tietohallintopäätösmenettelyn itsensä kuvaava normi, sovelluskehitysmalli ja tietoturvallisuuden tarkastustoimintaa ohjaavat normit vastaavat tämän päivän lainsäädännöllistä viitekehystä ja ovat muutenkin ajan tasalla. Keskinäinen harmonisointi on tärkeää normien välisten ristiriitojen välttämiseksi.

Ensimmäinen tutkimusongelma oli: Kuinka tietoturvallisuus on huomioitu THP-menettelyn mukaisissa puolustusvoimien tietojärjestelmähankkeissa, hankkeisiin kuuluvissa sovelluskehitysprojekteissa kehitettävien sovelluksien/tietojärjestelmien vast. osalta? Ongelmaa lähestyttiin kuvaamalla tietohallintopäätösmenettely prosessina sekä siihen kuuluvat rakenteet, tietohallintoauditointi ja tietohallintopäätös. Lisäksi kuvattiin puolustusvoimien hanketoimintaa, sovelluskehitysmalli ARKKI sekä teknisen tietoturvallisuuden tarkastustoiminta puolustusvoimissa. Lähdemateriaalista löytyneet tietoturvallisuustehtävät THP-menettelyn sekä ARKKI-mallin mukaisissa

vaiheissa kerättiin liitteen 2 taulukkoon. Taulukon avulla vastattiin ensimmäisen pääongelman osaongelmiin, jotka olivat: Missä eri THP-menettelyn vaiheissa tietoturvallisuusvaatimukset esiintyvät ja kuka vaatimukset määrittelee, sekä kuinka, missä vaiheessa tai vaiheissa ja kenen toimesta vaatimusten täyttyminen todennetaan? Tutkimuksen tuloksena voidaan todeta, että vaatimusten todentamiseen liittyvät vastuut on kuvattu kokonaisuutena selkeämmin ja konkreettisemmin, kuin vaatimusten määrittelemiseen liittyvät vastuut. Tietoturvallisuusvaatimuksiin liittyviä vastuita ei juuri ole eritelty yleisistä vaatimuksiin liittyvistä vastuista. Erittely ei toki ole välttämätöntä mutta usein tietoturvallisuuteen liittyvissä tehtävissä halutaan käyttää tietoturvallisuuden asiantuntijaa. Tämän vuoksi olisi hyvä kuvata tietoturvallisuusvaatimusten määritteleminen omana tehtävänään.

Tutkimuksen toinen pääongelma oli: Minkälaisia eroavaisuuksia ja samankaltaisuuksia puolustusvoimien THP-menettelyn mukaisissa tietojärjestelmähankkeissa ja niihin sisältyvissä ARKKI-sovelluskehitysmallin mukaisissa sovelluskehitysprojekteissa on verrattuna Sovelluskehityksen tietoturvaohjeen (VAHTI 1/2013) malliin? Ongelmaa lähestyttiin luvussa seitsemän kuvaamalla lyhyesti Sovelluskehityksen tietoturvaohjetta ja tekemällä vertailua sen sisältöön ja rakenteeseen. Sovelluskehityksen tietoturvaohje lähestyy vaatimusasettelua sovellusprojektin vaiheittain ja tietoturvatasoittain. Malli on tästä syystä helposti ymmärrettävä kenelle tahansa sovelluskehitystyötä ymmärtävälle. Puolustusvoimien teknisen tietoturvallisuuden arkkitehtuuri lähestyy vaatimusten asettamista laadittavien arkkitehtuurikuvausten kautta. Tässä mallissa vaatimusten asettaminen vaiheittain ei käy yhtä selvästi ilmi vaikkakin arkkitehtuurikuvausten käyttäminen lähestymistapana on muutoin perusteltua. Sovelluskehityksen tietoturvaohje esittelee RACI-mallin käytön tietoturvatehtävien vastuuttamiseksi. Mallia voi suositella käytettävän myös puolustusvoimissa. Kuten ohjeessa todetaan, vastuiden ja tehtävien määrittelyllä varmistetaan tietoturvallisuuden toteutuminen projektin kaikissa vaiheissa. Tietoturvavastuiden selkeämpi määrittely on yksi tutkimuksessa tunnistetuista kehittämiskohteista. Vastuuttamiseen liittyen on kuitenkin aina tärkeää varmistaa riittävä osaaminen.

Tutkimuksen kolmas ja viimeinen pääongelma oli: Kuinka THP-menettelyn mukaisia puolustusvoimien tietojärjestelmähankkeita ja niihin sisältyviä sovelluskehitysprojekteja tulisi kehittää, jotta tietoturvallisuus tulisi niissä paremmin huomioitua? Tunnistettuja kehittämiskohteita kuvattiin kootusti

luvussa seitsemän. Tietoturvallisuusakkreditointi tulisi sitoa paremmin osaksi THP-menettelyä ja sovelluskehitystä. SAA-toimijan tulisi mahdollisuuksien mukaan antaa ohjausta jo hankkeen tai projektin alkuvaiheisiin. SAA-toimijan tulee kuitenkin ehdottomasti säilyttää riippumattomuutensa, eli varsinaiseen määrittely- tai rakentamistyöhön SAA-toimija ei voi osallistua. Akkreditoinnin tulisi perustua järjestelmän uhka-arvioon siten, ettei kaikissa järjestelmissä suojauduta kaikkia uhkia vastaan, täyttämällä kaikki mahdolliset kriteerit. Tämä lisää myös kustannustehokkuutta. Tietoturvakatselmointien järjestämistä ulkopuolisen auditoijan toimesta kannattaa pohtia, etenkin jos on osaamis- tai resurssivajetta. Resurssien vähäisyyden ja tarkastustarpeiden suuren määrän vuoksi on hyvin mahdollista, ettei tarkastus- ja akkreditointitoimintaa pystytä jatkossa suorittamaan pelkästään puolustusvoimien oman henkilöstön voimin. Yksi tärkeä kehittämiskohde on jo aiemmin mainittu tietoturvavastuiden selkeämpi vastuuttaminen ja siihen liittyvä osaamisen varmistaminen.

Hanketoimintaa ohjaavien ja johtamisjärjestelmäalan normien uudistustyön on tarkoitus valmistua tänä vuonna. On mielenkiintoista nähdä, minkälainen lopputulos uudistustyössä saadaan aikaan. Päätöksiä tietoturvallisuuteen liittyvän tarkastustoiminnan kehittämiseksi on myös luvassa vuoden 2013 aikana. Tähän liittyy yhteistoiminta Viestintäviraston kanssa. Näiden muutosten vaikutukset näkyvät hankkeissa laajemmin vasta joidenkin vuosien kuluessa. Aika näyttää, miten tilanne tulee kehittymään.

# Lähteet

**JULKAISEMATTOMAT LÄHTEET**

**Puolustusvoimien materiaali**

[1] ARKKI-sovelluskehitysmalli. 2005. Pääesikunnan johtamisjärjestelmäosaston ohje.

[2] Arkkitehtuuriohjaus. Puolustusvoimien intranet Torni. Viitattu 9.8.2012.

[3] Kansallisen turvallisuusauditointikriteeristön käyttöönotto puolustusvoimissa. 2011. Pääesikunnan johtamisjärjestelmäosaston käsky, AH11938.

[4] Korkka, Mikko. 2011. PVTAK hankkeille, ohje hankkeiden arkkitehtuurityöhön. Sisäinen ohje.

[5] PAK 8:01 Hanketoiminta puolustusvoimissa. 2007. Pääesikunnan materiaaliosaston pysyväisasiakirja, HD590.

[6] PAK 8:03 Elinjaksoauditoinnit puolustusvoimissa. 2007. Pääesikunnan materiaaliosaston pysyväisasiakirja, HD596.

[7] PAK 8:06 Vaatimustenhallinta puolustusvoimissa. 2007. Pääesikunnan materiaaliosaston pysyväisasiakirja, HD603.

[8] Puolustusvoimien johtamisjärjestelmän teknisen tietoturvallisuuden arkkitehtuuri. 2012. Teknisen tietoturvallisuuden arkkitehtuurikuvaus, AI12843 (ST IV).

[9] Puolustusvoimien määritelmärekisteri. Puolustusvoimien asianhallintajärjestelmä. Viitattu 20.2.2013.

[10] PVHSM 4.2.2.2 Tietohallinto 022 – Tietohallintopäätösmenettely. 2009. Pääesikunnan johtamisjärjestelmäosaston normi, HF1500.

[11] PVHSM 4.2.3.3 Tietohallinto 017 PEJOJÄOS Teknisen tietoturvallisuuden auditointi ja tarkastus. 2010. Pääesikunnan johtamisjärjestelmäosaston normi, HG1231.

[12] PVHSMK 4.2.3 Tietohallinto 012 PEJOJÄOS - Tietoturvallisuusviranomaistoiminnot puolustusvoimissa. 2010. Pääesikunnan johtamisjärjestelmäosaston normi, HG537.

[13] PVHSM Hallinto 001 – PEKANSLIA Pääesikunnan työjärjestys 2012. 2012. Pääesikunnan kanslian määräys, HI650 (ST IV Käyttö rajoitettu).

[14] PVHSM johtamisjärjestelmä 001 Puolustusvoimien johtamisjärjestelmäalan toimintamalli. 2009. Pääesikunnan johtamisjärjestelmäosaston määräys, HF1547.

[15] PVOHJEK-PE Puolustusvoimien strateginen suunnittelu. 2012. Pääesikunnan suunnitteluosaston normi, HI1152.

[16] THP-uudistus 2012. 2012. Pääesikunnan johtamisjärjestelmäosaston muistio 10.5.2012. Muistio esitetty THP-kehityskokouksessa 10.5.2012.

[17] Turvallisuusakkreditoinnin usein kysytyt kysymykset (SAA FAQ). 2011. Pääesikunnan tutkintaosaston ohje (ST IV Käyttö rajoitettu).

[18] Täsmennykset tietohallintopäätösmenettelyä ohjaavan PEJO-JÄOS:n normin PVHSM 022 soveltamiseen. 2012. Pääesikunnan johtamisjärjestelmäosaston ohje, AI17978.

**JULKAISTUT LÄHTEET**

[19] A 1.7.2010/681. Asetus tietoturvallisuudesta valtionhallinnossa

[20] Kansallinen turvallisuusauditointikriteeristö versio II. 2011. Puolustusministeriö. Viitattu 28.2.2013. < http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf >

[21] Kiiskilä, Petri. 2012. KATAKRI – ilmavoimat lentää vieläkin. Insinööriupseeri 2012 sivut 35-36. Verkkoversion osoite < http://iul-fi-bin.directo.fi/@Bin/a51d652639ef2d557317c80916b7c563/1362302147/application/pdf/135130/Insin%C3%B6%C3%B6riupseeri%202012%20verkkoversio.pdf > .

[22] Kosola, Jyri. 2012. Puolustusvoimien projektiohje. Maanpuolustuskorkeakoulun julkaisuja. Verkkoversion osoite <http://urn.fi/URN:ISBN:978-951-25-2327-6>

[23] Kosola, Jyri. 2007. Suorituskyvyn elinjakson hallinta. Maanpuolustuskorkeakoulun julkaisusarja nro 7/2007 sivu 398

[24] L 24.6.2004/588. Laki kansainvälisistä tietoturvallisuusvelvoitteista

[25] L 22.12.2011/1406. Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista

[26] Menetelmäpolkuja humanisteille. Jyväskylän yliopisto, Humanistinen tiedekunta. Viitattu 23.2.2013. <https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja>.

[27] NCSA-FI:n suorittama tietojärjestelmien tietoturvallisuushyväksyntä, tilaajaorganisaation näkökulma. 2013. Viestintäviraston ohje. Viitattu 23.2.2013. < http://www.ficora.fi/attachments/suomimq/6DWADTJfp/NCSA-FI-hyvaksynta_ja_-arviointiprosessi_-_Tilaajaorganisaation_nakokulma.pdf >

[28] Puolustusministeriön www-sivusto. Viitattu 13.3.2012. < http://www.defmin.fi/hallinnonala/puolustushallinnon_turvallisuustoiminta/kansainvalinen_yhteistyo_turvallisuustoiminnan_alalla>.

[29] Puolustusvoimien www-sivusto. Viitattu 15.8.2012. < http://www.puolustusvoimat.fi/ >.

[30] Routio, Pentti. 2005. Vertailu. Tuotetiede. Taideteollisen korkeakoulun virtuaaliyliopisto. Viitattu 23.2.2013 <http://www.uiah.fi/virtu/materiaalit/tuotetiede/html_files/14112_totea.html>

[31] Saaranen-Kauppinen, Anita & Puusniekka, Anna. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. Viitattu 23.2.2013. <http://www.fsd.uta.fi/menetelmaopetus/>.

[32] Simi, Jarmo. 2010. Puolustusvoimien turvaluokiteltua tietoa sisältävien kotimaisten hankintojen turvallisuus. Turvallisuusjohdon koulutusohjelma, Teknillinen korkeakoulu. Tutkielma.

[33] Solante, Tero. 2012. Elinjakson hallinta kehittyy. Insinööriupseeri 2012 sivut 29–31. Verkkoversion osoite < http://iul-fi-bin.directo.fi/@Bin/a51d652639ef2d557317c80916b7c563/1362302147/application/pdf/135130/Insin%C3%B6%C3%B6riupseeri%202012%20verkkoversio.pdf > .

[34] Sovelluskehityksen tietoturvaohje, VAHTI 1/2013. 2013. Juvenes Print – Suomen Yliopistopaino Oy.

[35] VAHTIn rakenteisen verkkosivuston ensimmäinen versio. Viitattu 28.2.2013. <https://www.vahtiohje.fi/>.

[36] Viestintäviraston www-sivusto. Viitattu 15.8.2012. < http://www.ficora.fi/ >.

[37] VM uutiskirje 24/2012, 30.08.2012. 2012. Viitattu 3.3.2013. < http://www.vm.fi/vm/fi/03_tiedotteet_ja_puheet/03_uutiskirjeet/2412_ict.jsp >

# Liitteet

**Liite 1 ARKKI-sovelluskehitysmallin mukaiset dokumentit sekä niiden tekijät**

| Dokumentti | Tekijä | Räät./valm. |
|---|---|---|
| ***PH10 Tavoiteasetteluasiakirja** | **PV** | **RV** |
| PH20 Projektiehdotus | PV | RV |
| ***PH30 PV:n projektisuunnitelma** | **PV** | **RV** |
| ***PH40 Toimittajan projektisuunnitelma** | **Toimittaja** | **RV** |
| PH50 Iteraatiosuunnitelma | Toimittaja | RV |
| PH60 Kokoonpanonhallintasuunnitelma | Toimittaja | RV |
| PH70 Muutostenhallintasuunnitelma | Toimittaja | RV |
| PH80 Muutospyyntö pv | PV | RV |
| PH81 Muutospyyntö toimittaja | Toimittaja | RV |
| TA10 Kehitys- ja testausympäristön infrastruktuurikuvaus | Toimittaja | RV |
| ***TA20 Teknisen arkkitehtuurin kuvaus** | **Toimittaja** | **RV** |
| ***TA30 Tuotantoympäristön infrastruktuurikuvaus** | **Toimittaja** | **RV** |
| OR10 Organisaatiomuutokset | PV | RV |
| KO10 Koulutussuunnitelma | PV | RV |
| KO20 Työtehtävätuen ylläpitosuunnitelma | PV | RV |
| KO30 Koulutusmateriaali | PV | RV |
| KO40 Sovelluksen taktinen käyttöohje | PV | RV |
| VI10 Viestintäsuunnitelma | PV | RV |
| ***TU10 Ylläpitosuunnitelma** | **PV** | **RV** |
| ***TU20 Tukiorganisaation valmiusraportti** | **PV** | **RV** |
| TM10 Käsitemalli peruskäsitteistä (RUP Business Analysis Model) | PV/Toimittaja | RV |
| ***VH10 Tavoitetilan kuvaus (RUP Vision)** | **PV/Toimittaja** | **RV** |
| VH20 Toiminnallisia vaatimuksia täydentävät vaatimuk- | PV | RV |

| | | |
|---|---|---|
| set ja reunaehdot (RUP Supplementary Specifications) | | |
| VH30 Käyttötapausmalli (RUP Use Case Model) | PV/Toimittaja | RV |
| ***VH40 Käyttötapauskuvaukset (RUP Use Case Specifications)** | **PV/Toimittaja** | **RV** |
| VH50 Sanasto (RUP Glossary) | PV/Toimittaja | RV |
| MS10 Nykytilan kuvaus | PV/Toimittaja | RV |
| MS20 Määritelymalli (RUP Analysis Model) | Toimittaja | R |
| MS30 Suunnittelumalli (RUP Design Model) | Toimittaja | R |
| ***MS40 Sovellusarkkitehtuurin kuvaus (RUP Software Architecture Document)** | **Toimittaja** | **R** |
| MS50 Käyttötapausten toteutuskuvaukset (RUP Use Case Realization) | Toimittaja | R |
| MS60 Näyttöjen toteutuskuvaus | Toimittaja | R |
| ***MS70 Tietomalli (RUP Data Model)** | **Toimittaja** | **R** |
| MS80 Valmisohjelmiston valinta | PV/Toimittaja | V |
| MS90 Sovellussuunnitelma | PV/Toimittaja | V |
| TO10 Komponenttimalli (Implementation Model) | Toimittaja | R |
| TO20 Komponenttien kuvaukset | Toimittaja | R |
| TO30 Valmisohjelmiston kattavuusanalyysi | Toimittaja | V |
| TO40 Räätälöitävät toiminnot | Toimittaja | V |
| TO50 Sovelluksen käsitteellinen kuvaus | Toimittaja | V |
| TO60 Räätälöinnin toiminnallinen kuvaus | Toimittaja | V |
| TO70 Sovelluksen toiminnallinen kuvaus | Toimittaja | V |
| TO80 Valmisohjelmiston konfiguraation kuvaus | Toimittaja | V |
| TO90 Räätälöinnin tekninen kuvaus | Toimittaja | V |
| TO100 Sovelluksen tekninen kuvaus | Toimittaja | V |
| TO110 Rajapintojen määrittely | Toimittaja | V |
| TE10 Testaussuunnitelma (RUP Test Plan) | Toimittaja | RV |
| TE20 Testitapausten kuvaukset (RUP Test Case) | Toimittaja | RV |
| TE30 Hyväksymistestaussuunnitelma | PV | RV |
| TE40 Luovutuskokeen hyväksymiskriteerit | PV | RV |
| AS10 Tietojen konversiosuunnitelma | Toimittaja | RV |
| AS20 Käyttöönottosuunnitelma | PV | RV |
| AS30 Asennusohjeet (RUP Installation Artifacts) | Toimittaja | RV |
| AS40 Käyttäjän ohjeet (RUP End-User Support Material) | Toimittaja | RV |

Sarakkeiden selitykset:

Tekijä:

- PV: Puolustusvoimat tuottaa dokumentin
- Toimittaja: Toimittaja tuottaa dokumentin
- PV/Toimittaja: Puolustusvoimat tuottaa dokumentin, jonka toimittaja ottaa oman työnsä pohjaksi ja tarkentaa lopulliseen muotoon joko yksin tai yhdessä puolustusvoimien kanssa.

Räät./valm.

R: Dokumentti tuotetaan räätälöidyssä sovelluskehityksessä

V: Dokumentti tuotetaan valmisohjelmistopohjaisessa sovelluskehityksessä

RV: Dokumentti tuotetaan sekä räätälöidyssä että valmisohjelmistopohjaisessa sovelluskehityksessä.

Taulukossa on lihavoituna sekä tähdellä (*) merkittynä dokumentit, joita tietoturva-akkreditoinnissa tietohallintopäätösmenettelyn vaiheessa 4 rakentamisesta tuotantoon (THP4) erityisesti tarkastellaan. Dokumenttien sisältö on kuvattu tarkemmin ARKKI-sovelluskehitysohjeessa.

**Liite 2 Tietoturvallisuuteen liittyvät tehtävät THP-menettelyn vaiheissa**

| THP-menettelyn vaihe | ARKKI-sovelluskehitys-mallin vaihe | Tietoturvallisuusvaatimuksiin liittyvät tehtävät hanketoimintaa ohjeistavien normien, THP-menettelyn sekä ARKKI-sovelluskehitysmallin mukaan | Vaadittavat ARKKI-dokumentit | Arviointiin tai akkredi-tointiin liittyvät tehtävät (tarkastuksen suoritta-va taho) |
|---|---|---|---|---|
| **Ideointi /THA 1** | Ei sisälly | • Ei selkeitä tietoturvallisuuteen liittyviä tehtäviä [2]<br>• Hahmotelma sovelluksen tietoturvallisuustasosta [4]<br>• Vaihe ei sisälly ARKKI-sovelluskehitysmalliin. | Ei sisälly | Tietoturva-arviointi (PE-JOJÄOS) [5] |
| **Esisuunnittelu / THA 2** | Tavoiteasetteluvai-he | • Järjestelmävaatimukset sisältäen tietoturvallisuusvaatimukset laaditaan ohjeistuksen mukaisesti [2], [3]<br>• Alustava versio sovelluksen tietoturvallisuustasosta [4]<br>• ARKKI-sovelluskehitysmalli ei kuvaa selkeitä tietoturvallisuuteen liittyviä kokonaisuuksia tai tehtäviä tässä vaiheessa | PH10, PH20, PH30 | Tietoturva-arviointi (PE-JOJÄOS) -> Tiedotus SAA-toimijalle [5] |
| **Suunnittelu / THA 3** | Vaatimusmäärittely-vaihe | • Järjestelmän suunnittelun tarkentaminen osajärjestelmätasolle [2], [3]<br>• Testauksen, evaluoinnin ja hyväksyntöjen suunnitelmien laadinta [2],[3]<br>• Järjestelmään liittyvien määrittelyjen ja kuvausten laadinta [2], [3]<br>• Tarjouspyynnön valmisteleminen lähetettäväksi [2], [3]<br>• Kuvataan sovellukselle asetettavat tekniset-, laatu- ja muut vaatimukset [1]<br>• Kuvataan sovelluksen halutut toiminnalliset ominaisuudet [1]<br>• Kuvataan, kuinka kehitettävää sovellusta käytetään osana prosessia [1]<br>• Kuvataan, miten sovellus liittyy käyttäjän tasolla muihin prosesseihin [1]<br>• Määritellään sovelluksen turvallisuustasot [1], hyväksytty versio sovelluksen turvallisuustasosta [5] | PH10, PH20, PH30, TM10, VH10, VH20, VH30, VH40, VH50, MS10, sekä MS80, MS90 (valmisohjelmisto-jen osalta) | Tietoturva-arviointi (THP-ryhmä) -> Tiedotus SAA-toimijalle [5] |
| **Rakentaminen / THA 4** | Rakentamisvaihe | • Järjestelmävaatimusten verifioinnin toteuttaminen [2], [3]<br>• ARKKI-mallissa suositellaan ulkopuolista auditoijaa seuraaviin toimenpitei-siin: | PH30, PH40, PH50, PH60, PH70, PH80, PH81, TA10, TA20, TA30, OR10, KO10, | SAA-akkreditointi [5] (SAA-toimija. Tarvittavat ARKKI-dokumentit: PH10, PH30 PH40, |

| THP-menettelyn vaihe | ARKKI-sovelluskehitys-mallin vaihe | Tietoturvallisuusvaatimuksiin liittyvät tehtävät hanketoimintaa ohjeistavien normien, THP-menettelyn sekä ARKKI-sovelluskehitysmallin mukaan | Vaadittavat ARKKI-dokumentit | Arviointiin tai akkredi-tointiin liittyvät tehtävät (tarkastuksen suoritta-va taho) |
|---|---|---|---|---|
| | | ✓ Esitettyjen tietoturvaratkaisujen arvioiminen tarjousten katselmoinnin yhtey-dessä, ennen toimittajan valintaa<br>✓ Tietoturvan suunnittelun laadun arvioiminen rakennusvaiheen ensimmäisen iteraation jälkeen [1] | KO20, KO40, KO30, VI10, TU10, TU20 | TA20, TA30, MS70, MS40, TU10, TU20, VH10, VH40) [6] |
| **Operointi / THA 4n** | Ei varsinaisesti sisälly. Käyttöönot-tovaihe (operointi-vaiheen 6 ensim-mäistä kuukautta) | • Järjestelmävaatimusten sisältäen tietoturvallisuusvaatimukset ylläpito [2]<br>• ARKKI-mallissa suositellaan ulkopuolista auditoijaa seuraavaan toimenpi-teeseen:<br>✓ Suorituskyky, tietoturva- ja yhteenvetokatselmointi käyttöönottovaiheen aikana. Tämä sisältää tietoturvatarkastuksen[1] | Ei sisälly. | Teknisiä tietoturvatarkas-tuksia ja –auditointeja osana kehityskohteen tuotantokäytön aikaista toimintaa. (Hyväksytty tarkastustoimija) [5]<br><br>Suorituskyky, tietoturva-ja yhteenvetokatselmointi käyttöönottovaiheen aikana. Tämä sisältää tietoturvatarkastuksen (Ulkopuolisen toimijan toimesta ) [1] |
| **Purku / THA 5** | Ei sisälly | • Ei tunnistettuja tehtäviä yhdessäkään lähteessä | Ei sisälly | Arvio kehitystyön purka-mis- ja luopumissuunni-telmien vaikutuksesta palveluympäristön tieto-turvaan. Annetaan pur-kamislupa teknisen tieto-turvan osalta. (PEJOJÄ-OS) [5] |

Taulukossa käytetyt lähteet:

[1] ARKKI-sovelluskehitysmalli. 2005. Pääesikunnan johtamisjärjestelmäosaston ohje.
[2] PAK 8:01 Hanketoiminta puolustusvoimissa, liite 1. 2007. Pääesikunnan materiaaliosaston pysyväisasiakirja , HD590
[3] PAK 8:03 Elinjaksoauditoinnit puolustusvoimissa, liite 1. 2007. Pääesikunnan materiaaliosaston pysyväisasiakirja, HD596
[4] PVHSM 4.2.2.2 Tietohallinto 022 – Tietohallintopäätösmenettely, liite 3. 2009. Pääesikunnan johtamisjärjestelmäosaston normi, HF1500.
[5] PVHSM 4.2.3.3 Tietohallinto 017 PEJOJÄOS Teknisen tietoturvallisuuden auditointi ja tarkastus. 2010. Pääesikunnan johtamisjärjestelmäosaston normi, HG1231
[6] Pääesikunnan tutkintaosaston ohje, Turvallisuusakkreditoinnin usein kysytyt kysymykset (SAA FAQ), 16.5.2011. Sisäinen ohje.