VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Haukka: digitaalisen turvallisuuden arvioinnin kehitystarpeet

Tuija Kuusisto, Eeva Lantto, Niko Mäkilä
12.2.2021

Selvityksen toteutustapa

Digiturvan arvioinnin kehitystarpeiden selvitys

- Tarkastelemme lähinnä seuraavia lakeja
  - Laki tietoturvallisuuden arviointilaitoksista (1405/2011)
  - Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)
- Liittymäpintaa on muihinkin säädöksiin
  - Laki julkisen hallinnon tiedonhallinnasta (906/2019)
  - Yleinen tietosuoja-asetus (EU 2016/679)
  - Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019)
  - Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
  - Valmiuslaki (1552/2011)

Selvityksen toteutustapa

- Haastattelut
  - Arviointeja teettävät julkisen hallinnon edustajat
  - Arviointien kohteena olevat palveluntarjoajat
  - Liikenne- ja viestintävirasto Traficom
  - Kaupalliset arviointilaitokset
- Selvityksen koordinaatioryhmän työpajat ja kokoukset
- Rajaudutaan digitaaliseen turvallisuuteen: tietoturvallisuus, tietosuoja, varautuminen, kyberturvallisuus, riskienhallinta

Selvityksen havaintoja

Tarkasteltavien lakien soveltamisala

Selvityksen antia

- Arviointilaitoslaki on rajattu elinkeinonharjoittajiin ja palvelutehtäviä julkishallinnolle tarjoaviin yksiköihin, jotka
  - toimeksiannosta arvioivat tietoturvallisuustason
  - haluavat toiminnalleen Traficomin hyväksynnän
- Arviointilaki on rajattu viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuteen
- Traficomin ja arviointilaitosten velvollisuudet ja vastuut ovat tulkinnanvaraisia
  - Linjauksia ja tulkintoja haetaan Traficomilta

Toimivalta ja vastuut

Selvityksen antia

- Arviointitoiminnan toimivaltainen viranomainen on valtiovarainministeriö ja Traficom
- Traficomin tehtäviä ovat mm.
  - Tietoturvallisuuden arviointilaitosten hyväksyminen
  - Tietoturvallisuuden arviointi ja hyväksymistodistukset
  - Yleistä tietoturvallisuuden tasoa koskevat selvitykset
- Tietosuojan arviointielimen hyväksynnän tekee tietosuojavaltuutettu
- Traficomin vasteaikoja pidetään laajasti pitkinä

Arviointilaitokset

Selvityksen antia

- Tietoturvallisuuden arviointilaitos tarvitsee sekä FINASin että Traficomin hyväksynnän ja prosessi koetaan monimutkaiseksi
- Traficom on tulkinnut, että kaupalliset arviointilaitokset eivät voi tehdä turvaluokkien I ja II järjestelmiin liittyviä tietoturva-arviointeja
  - Sekä Traficom että kaupalliset arviointilaitokset voivat tehdä muita arviointeja
  - Salassa pidettävää tietoa koskevaa arviointikriteeristöä ei ole

Arviointimenettelyt

Selvityksen antia

- Vaatimukset koetaan tulkinnanvaraisiksi
  - Tulkintoja haetaan Traficomilta. Niitä saadaan usein hitaasti ja arvioinnin tulokset riippuvat tulkinnan tekijän näkemyksestä
  - Tilanne hidastaa järjestelmien käyttöönottoja ja saattaa nostaa kustannuksia
- Tiedonhallintalautakunta edistää tiedonhallintalaissa säädettyjen menettelytapojen ja vaatimusten toteuttamista
  - Tämä rooli ei näy arviointilaeissa eikä Traficomin ohjeissa
- Arvioinnit ovat kertaluonteisia ja seuranta-arvioinnit jäävät arvioitavan kohteen vastuulle
- Arvioinneissa löydetään usein poikkeamia ja arvioinnista on mahdollista saada todistus
  - Vaatimuksenmukaisen järjestelmän poikkeamien laadulle ja määrälle ei ole kriteereitä
  - Poikkeamien korjausmekanismia ja muita velvoitteita ei ole säädetty

Digitaalisen turvallisuuden vaatimukset

Selvityksen antia

- Arviointilakien vaatimukset koskevat vain tietoturvallisuutta
- Tietoturvallisuuden vaatimukset tulevat mm. tiedonhallintalaista
- Tietosuojan vaatimukset tulevat EU:n tietosuojadirektiivistä
- Varautumiselle ja jatkuvuudelle ei ole vaatimuksia

Tietoturvallisuuden arviointikriteeristöt

Selvityksen antia

- Lain mukaan tietoturvallisuuden arviointiperusteina voidaan käyttää kansallisia ja kansainvälisiä säännöksiä, ohjeita tai vahvistettuja standardeja
- Katakri on tietoturvallisuuden auditointityökalu viranomaisille
  - Soveltuu yritysturvallisuusselvityksiin ja tietojärjestelmien arviointiin
  - Tarkoituksena turvata turvallisuusluokitellun tiedon käsittely
  - Katakria ei aseta ehdottomia vaatimuksia
  - Katakria käytetään ehdottomina vaatimuksina
- Pitukri on pilvipalvelujen turvallisuuden arviointikriteeristö
- ISO-standardit ovat laajasti käytössä maailmanlaajuisesti

Kehitysehdotukset

Keskeiset kehitysehdotukset (1/3)

1) Säädetään, että kansallinen akkreditointiyksikkö FINAS arvioi tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden arviointilaitosten pätevyyden määrävälein. FINAS voi käyttää muita viranomaisia akkreditointiprosessissa käytettävien toimialakohtaisten vaatimusten määrityksessä. Määritystyöhön näissä viranomaisissa osallistuvat virkamiehet eivät saa osallistua arviointilaitoksen toimintaan arvioijina.
2) Tiedonhallintalautakunta antaa yleiset tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden arviointilaitoksen akkreditointiin liittyvät vaatimukset. Digi- ja väestötietovirasto tukee FINASia em. vaatimustenmukaisuuden arvioinnissa.
3) Traficomille säädetään tehtäviksi toimiminen tietoturvallisuuden lisäksi myös varautumisen ja toiminnan jatkuvuuden arviointilaitoksena sille säädetyillä pätevyysalueilla. FINAS arvioi myös näiden ns. viranomaisarviointilaitosten pätevyyden määrävälein. Näiden arviointilaitosten pätevyysalueita ovat tiedonhallintalain tarkoittamia turvallisuusluokkien III, II ja I tarkoittamia tietoja käsittelevät palvelut sekä niiden hallintajärjestelmät. Nämä viranomaisarviointilaitokset eivät arvioi fyysistä turvallisuutta, vaan tiedonhallintayksikön ja sen tilaaman fyysisen turvallisuuden arvioinnista säädetään kansallisellakin tasolla, esimerkiksi Suojelupoliisin tehtäväksi.

Keskeiset kehitysehdotukset (2/3)

4) FINAS akkreditoi kaupallisia tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden arviointilaitoksia hakijan hakemuksessa esittämille pätevyysalueille. Mahdolliset kilpailuoikeudelliset syyt erottaa kaupallisten arviointilaitosten ja viranomaisarviointilaitosten pätevyysalueet selvitetään. FINAS ylläpitää kuvausta mahdollisista pätevyysalueista. Pätevyysalueet voivat kattaa tiedonhallintalain turvallisuusluokan IV ja III ja salassa pidettäviä ja julkisia tietoja käsittelevät palvelut sekä niiden hallintajärjestelmät. Arviointitoimeksiannot voivat koskea kuten nykyisinkin tiedonhallintalain tarkoittamia tiedonhallintayksiköitä sekä yksityistä sektoria. Arviointitoimeksiannot voivat sisältää myös arvioinnin kohteeseen liittyvän fyysisen turvallisuuden arvioinnin.
5) Tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden akkreditoitu arviointilaitos antaa arvioinnin tuloksiin perustuvan raportin. Jos arvioinnin kohde täyttää asetetut vaatimukset, niin arviointilaitos antaa erillisen todistuksen vaatimustenmukaisuudesta eli hyväksynnän. Kansallisella tasolla hyväksynnän voisivat siten antaa muutkin kuin viranomaisarviointilaitokset.

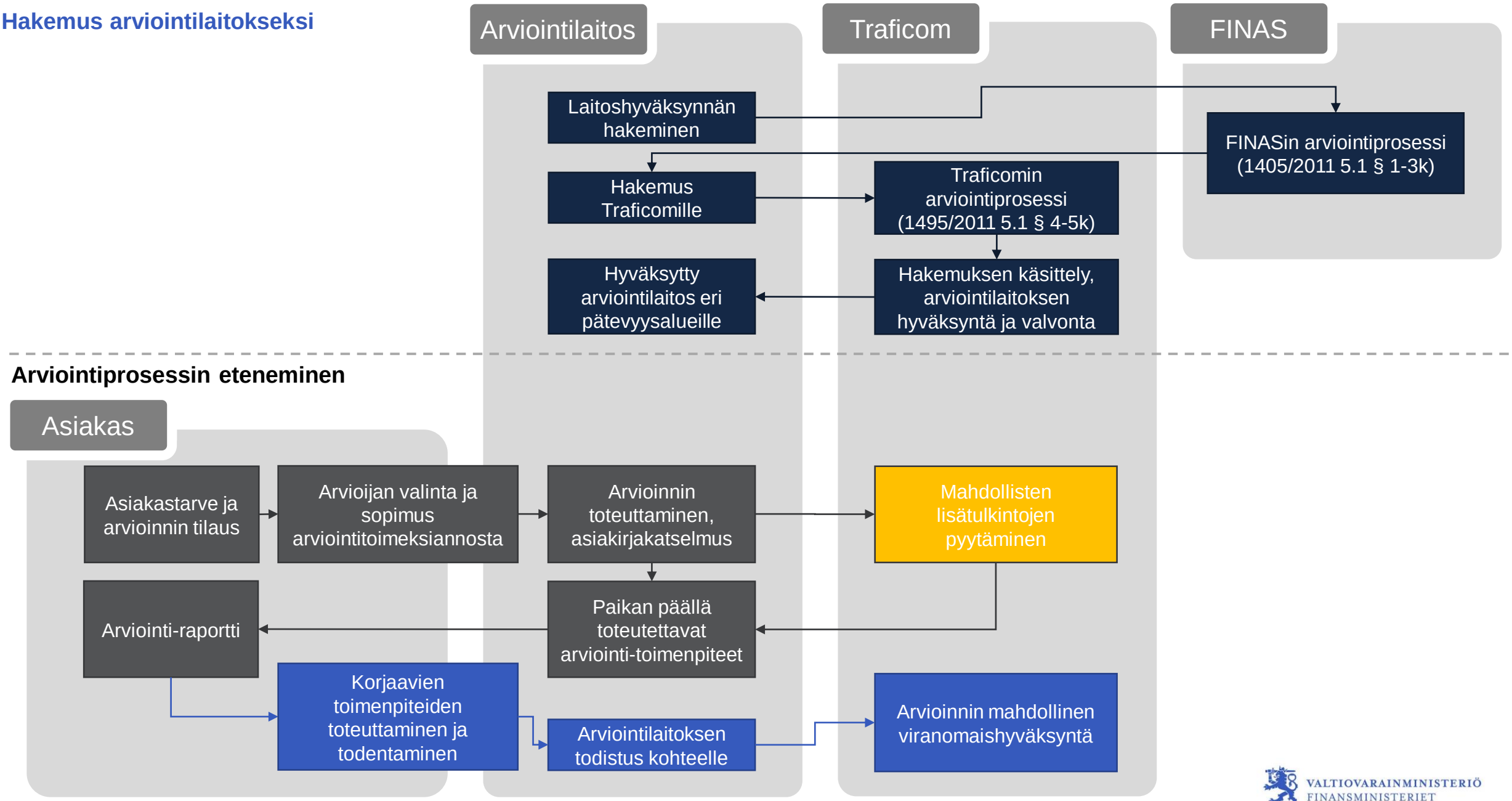
Keskeiset kehitysehdotukset (3/3)

6) Viranomaiset ja yhteisöt voivat tilata arviointeja tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden akkreditoiduilta arviointilaitoksilta niiden pätevyysalueilta ja niiden määrittämillä kustannuksilla. Toimeksiannon yhteydessä tilaaja määrittää arvioinnin kohteen ja arviointiperustan tai arviointiperusta määräytyy säädösten perusteella, esimerkiksi lain kansainvälisistä tietoturvavelvoitteista tarkoittamissa tilanteissa. Vaatimustenmukaisuustodistus voidaan myöntää ainoastaan käytettäessä pätevyysalueen mukaista arviointiperustaa (esimerkiksi tiedonhallintalautakunnan antama kriteeristö tai Katakri).
7) Tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden vaatimustenmukaisuuden arvioinnin tilaajan on osoitettava säännöllisillä seuranta-arvioinneilla palvelun turvallisuuden tason parantaminen. Säädetään tähän liittyvä valvonta.
8) Arvioidaan valtion yhteisten tieto- ja viestintäteknisten palveluiden tuottajien tietoturvallisuutta, varautumista ja toiminnan jatkuvuutta koskevia vastuita ja velvoitteita. Lähtökohtana on, että yhteisille palveluille asetetaan palvelukohtaisesti tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden vaatimukset.
9) Velvoitetaan suurimpia kuntien digitaalisten palvelujen tuottajia arvioimaan tuottamiensa palveluiden tietoturvallisuutta, varautumista sekä toiminnan jatkuvuutta säännöllisesti.

Toimintamallit nyky- ja tavoitetilassa: arviointilaitoshakemus ja tietoturvallisuusarviointi

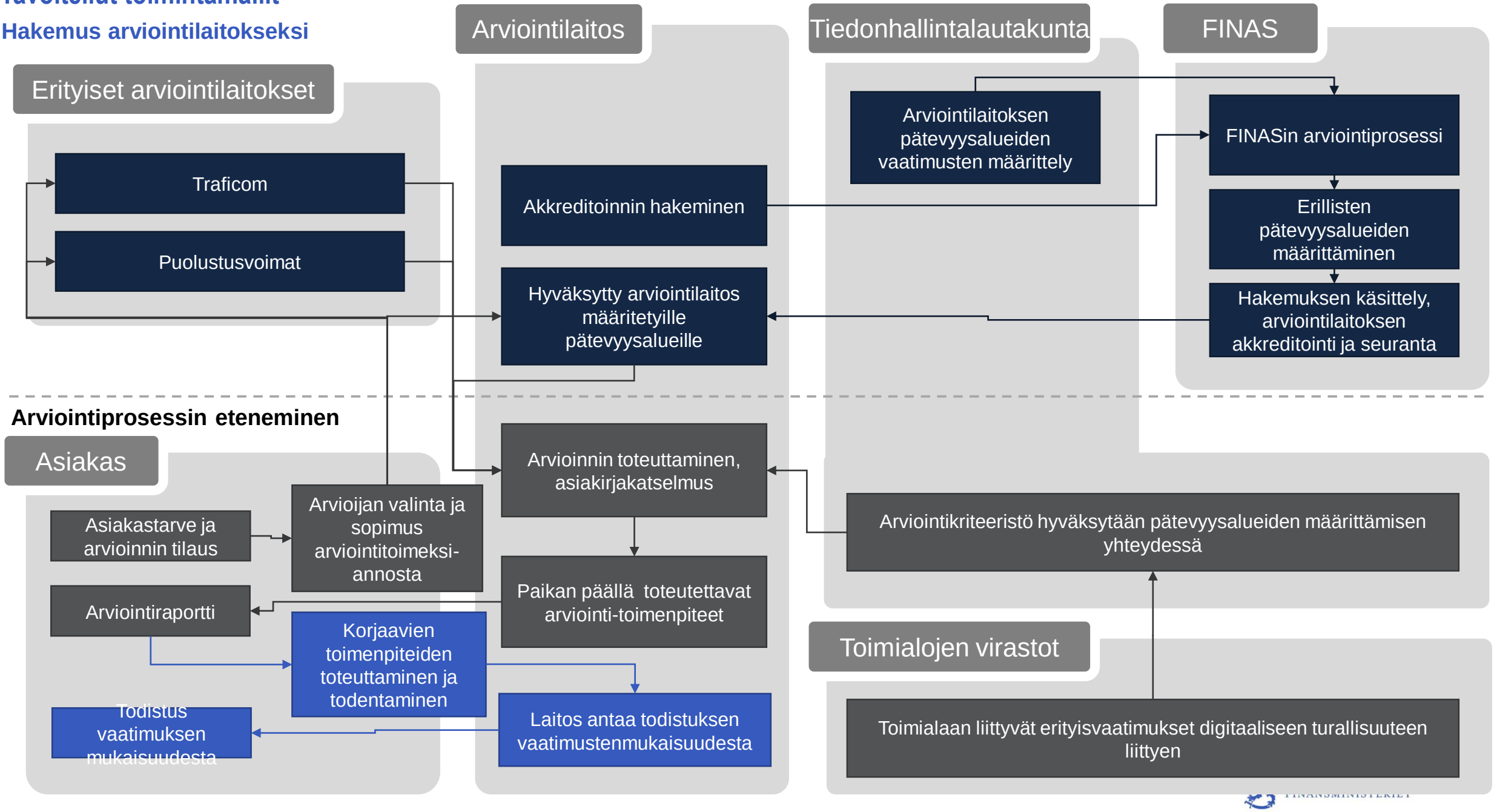
Nykyiset toimintamallit

Hakemus arviointilaitokseksi



Tavoitellut toimintamallit

Hakemus arviointilaitokseksi



Jatkotoimenpiteet

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Kuinka työ jatkuu?

- Selvitysraporttiluonnos on lausuntopalvelussa lausuttavana 9.3. saakka
  - PLM, UM, OM, TEM, LVM ja Traficom palaute on osin jo huomioitu tässä esityksessä ja huomioidaan raportin jatkotyöstössä
- Raporttiluonnos työstetään valmiiksi jo saadun ja saatavan palautteen perusteella maalis-huhtikuussa
- Mahdollinen säädöstyö vuosien 2021-2022 aikana
  - Ainakin tekniset muutokset tarpeellisia
- Päätösehdotus: Valmis loppuraportti esitellään tässä johtoryhmässä huhtikuun kokouksessa. Sen valmistelussa huomioidaan tässä kokouksessa esitetyt näkemykset.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Kiitos

Etunimi.Sukunimi@vm.fi
Niko Mäkilä