20.12.2018

Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista

Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

www.ficora.fi

Erik Palménin aukio 1
PL 313
00561 Helsinki
Puhelin 0295 390 100
Y-tunnus 0709019-2

Erik Palménin aukio 1
PB 313, FI-00561
Helsingfors, Finland
Telefon +358 295 390 100
FO-nummer 0709019-2

Erik Palménin aukio 1
P.O. Box 313, FI-00561
Helsinki, Finland
Telephone +358 295 390 100
Business ID 0709019-2

Muutoshistoria

Päivämäärä	Kuvaus
4.11.2013	Ensimmäinen julkaisuversio.
23.9.2015	Täsmennetty sisältösuodatusratkaisun kuvausta taulukossa 3.
27.6.2016	Pieniä täsmennyksiä lukuun 3. Täsmennyksiä ja täydennyksiä lukuihin 4 ja 5.
20.12.2018	Pieniä täsmennyksiä kuvauksiin. Lisätty luvut 5.3, 5.4 ja 5.5.

Sisällys

1 Johdanto

Kansainvälisistä tietoturvallisuusvelvoitteista sekä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annettujen lakien[1] mukaan Viestintäviraston tehtäviin kuuluvat erilaiset turvallisuustarkastukset ja -hyväksynnät. Viestintäviraston suorittamissa tietojärjestelmätarkastuksissa eräs tarkastettava kohde on yhdyskäytäväratkaisut eri suojaustason ympäristöjen välillä. Tässä ohjeessa kuvataan yleisimmät edellytykset hyväksyttävissä oleville yhdyskäytäväratkaisuille sekä esitetään esimerkkejä ratkaisumalleista.

2 Määritelmät

"Hyväksyttävällä yhdyskäytäväratkaisulla" tarkoitetaan tässä ohjeessa toteutusta, joka mahdollistaa eri suojaustason ympäristöjen[2] liittämisen siten, että luotettavasti estetään ylemmän suojaustason tiedon kulkeutuminen matalamman suojaustason ympäristöön.

"Yksisuuntaisella suodatusratkaisulla" tarkoitetaan tässä ohjeessa toteutusta, joka rajaa liikennöinnin yksisuuntaiseksi.

"Datadiodilla" tarkoitetaan tässä ohjeessa yksisuuntaista suodatusratkaisua, joka rajaa liikennöinnin yksisuuntaiseksi OSI-mallin[3] fyysisellä kerroksella.

3 Yhdyskäytäväratkaisujen yleiset suunnitteluperiaatteet

Hyväksyttävien yhdyskäytäväratkaisujen yleisenä suunnitteluperiaatteena on toteuttaa Bell-LaPadula-mallin[4] säännöt "No Read Up" ja "No Write Down". Hyväksyttävän yhdyskäytäväratkaisun tulee toisin sanoen luotettavasti estää ylemmän suojaustason tiedon kulkeutuminen[5] matalamman suojaustason ympäristöön.

Bell-LaPadula -mallin toteuttamiseksi käytetään usein menetelminä

- yksisuuntaisia suodatusratkaisuja, joissa sallitaan yksisuuntainen liikennöinti matalamman tason ympäristöstä ylemmän tason ympäristöön, sekä
- sisältösuodatusratkaisuja, joissa tieto tunnistetaan ylemmän tason ympäristössä, ja sallitaan vain matalamman tason tiedon siirtyminen ylemmän tason ympäristöstä matalamman tason ympäristöön.

Hyväksyttävältä toteutukselta edellytetään yleisesti myös monikerrossuojaamisen[6], vikaturvallisuuden[7], vähimpien oikeuksien ja haavoittuvuusavaruuden minimoinnin periaatteiden täyttämistä. Keskeiset suodatustoiminnallisuudet tulee toteuttaa luotetun ohjelmisto- ja rauta-alustan päällä. On myös huomioitava, että yhdyskäytäväratkaisun tulee pystyä suojaamaan itseään käyttöympäristönsä uhkia vastaan, ja että turvallisuustoteutuksen oikeellisen toiminnan tulee olla luotettavasti todennettavissa. Yhdyskäytäväratkaisulle edellytetään luotettavaa toteutusta myös turvallisuuden hallinnoinnille sekä valvonnalle, mukaan lukien hyökkäysten havainnointikyky yhdyskäytäväratkaisua ja/tai sen suojaamaa ympäristöä vastaan. Yhdyskäytäväratkaisuun ja sen komponentteihin liittyvät lokitiedot tulee suojata lähtökohtaisesti yhdyskäytäväratkaisun ylemmän puolen luokituksen mukaisesti[8].

---

[1] Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004). Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011).

[2] Ympäristöjen oletetaan lähtökohtaisesti olevan toisilleen ei-luotettuja myös tilanteissa, joissa yhdistetään eri organisaatioiden hallinnoimia ympäristöjä toisiinsa.

[3] International Organization for Standardization. 1994. ISO/IEC 7498-1:1994. Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model.

[4] Bell, D & LaPadula, L. 1973. Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, Volume I & II.

[5] Kattaen kaikki tiedon välitystavat, sisältäen esimerkiksi tiedon kopioimisen, tiedon näyttämisen ja tiedon soittamisen.

[6] Engl. ”defence in depth”.

[7] Engl. ”fail secure” ja ”fail safe”. Huomioitava muun muassa virtualisoinnissa, jossa isäntäkoneen (host) vikaantuminen voi vaikuttaa useamman virtuaalikoneen (guest) toiminnallisuuteen. Toisaalta esimerkiksi yhdyskäytäväratkaisun tietoliikennelaitteiden tulee vikatilanteessa päätyä lähtökohtaisesti liikennöinnin estävään (fail closed) tilaan.

[8] Luokittelun perusteena hyökkäystyypit, joissa yhdyskäytäväratkaisun lokitietoja käytetään piilokanavana (engl. "covert channel") ylemmän suojaustason tietojen siirtämiseen matalamman suojaustason ympäristöön.

4 Yleisimmät yhdyskäytäväratkaisutyypit

Yleisimmät hyväksyttävät yhdyskäytäväratkaisut jakautuvat yksisuuntaisiin suodatusratkaisuihin ja alkiotunnistuksen sisältösuodatusratkaisuihin. Yksisuuntaiset suodatusratkaisut jakautuvat edelleen datadiodiratkaisuihin ja muihin yksisuuntaisiin suodatusratkaisuihin. Tässä luvussa kuvataan eri yhdyskäytäväratkaisutyyppien keskeiset ominaispiirteet sekä esitetään viitteellisiä esimerkkitoteutuksia.

4.1 Yksisuuntaiset suodatusratkaisut

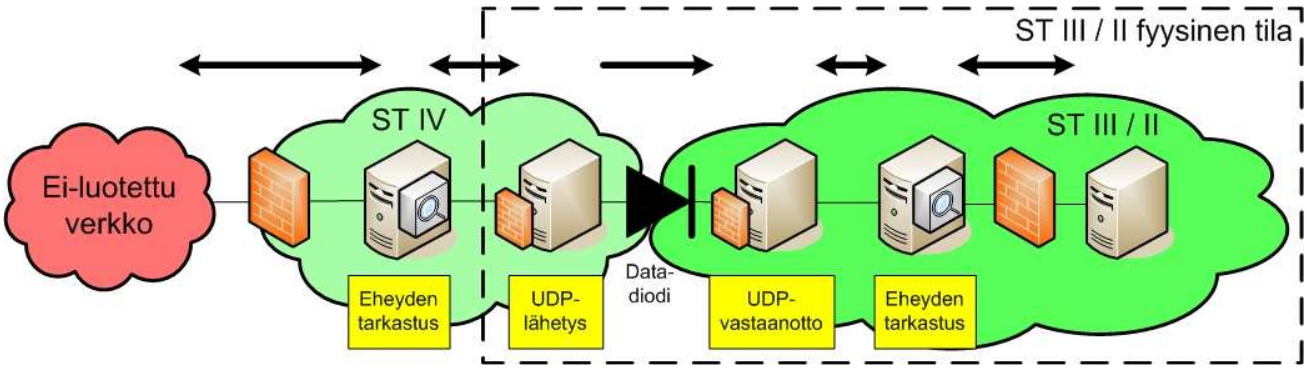
4.1.1 Datadiodiratkaisut

Datadiodiratkaisujen keskeiset ominaispiirteet on kuvattu taulukossa 1.

Taulukko 1. Datadiodiratkaisujen ominaispiirteitä.

Tiedonsiirron suunta	Matalamman tason ympäristöstä ylemmän tason ympäristöön.
Kuvaus	OSI-mallin fyysisen kerroksen tasolla tapahtuva vain yhteen suuntaan tiedonsiirron mahdollistava toteutus[9]. Hyväksyttävä toteutus edellyttää tyypillisesti kovennetuille käyttöjärjestelmäalustoille rakennettuja UDP-liikennettä välittäviä lähetys- ja vastaanottopalvelimia, sekä siirretyn aineiston eheyden tarkastavaa menettelyä[10].
Sovelluskohteita	Turvapäivitysten tuonti suojaustason III tai II ympäristöihin. Matalamman tason tiedon tuonti tilannekuvatiedon tarkkuuden parantamiseksi (esimerkiksi paikkatiedon, hälytysten, sensoritiedon tai kameravalvontatiedon välittäminen keskusvalvomoon / tilannekeskukseen).
Soveltuvuus suojaus-tasoittain	Hyväksyttävissä yhden tai useamman suojaustason ylittävänä yhdyskäytäväratkaisuna välillä ST IV → ST III, ST III → ST II ja ST IV → ST II.

Viitteellinen esimerkkitoteutus on esitetty kuvassa 1.



Kuva 1. Viitteellinen esimerkkitoteutus datadiodiratkaisusta.

4.1.2 Muut yksisuuntaiset suodatusratkaisut

Muiden yksisuuntaisten suodatusratkaisujen keskeiset ominaispiirteet on kuvattu taulukossa 2.

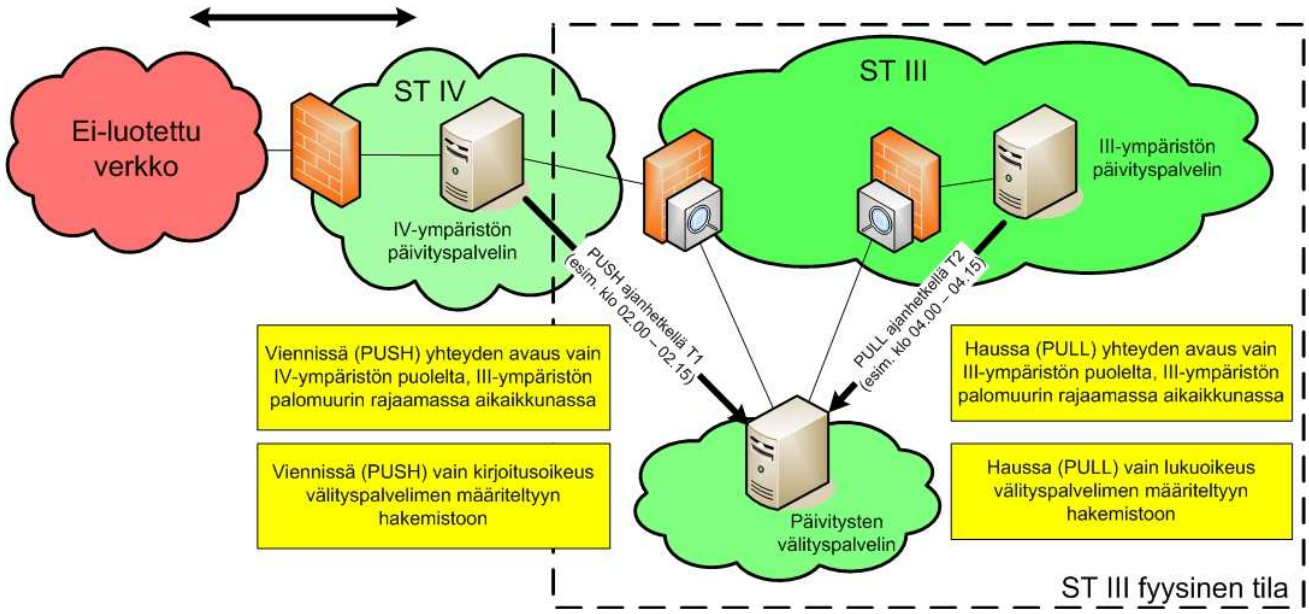
Taulukko 2. Muiden yksisuuntaisten suodatusratkaisujen ominaispiirteitä.

Tiedonsiirron suunta	Matalamman tason ympäristöstä ylemmän tason ympäristöön.
Kuvaus	Tyypillisesti OSI-mallin verkko- ja sovelluskerroksen tasoilla toteutettava vain yhteen suuntaan tiedonsiirron mahdollistava ratkaisu. Ratkaisu voi

[9] Esimerkiksi yksisuuntainen valokuituyhteys.
[10] Sisältäen esimerkiksi päivitysten tuonnissa vähintään siirrettyjen tiedostojen tarkistussummien ja allekirjoitusten tarkistamisen, sekä haittaohjelmaskannauksen.

	sisältää ajastettujen palomuurisääntöjen avulla eristetyn vyöhykkeen eri suojaustasojen välillä, mikä rajaa tiedonsiirron vyöhykkeiden välillä tapahtuvaksi vain yhteen suuntaan kerrallaan, ja sallii vain tunnistetut liikennetyypit. Toteutuksissa tulee huomioida erityisesti, että määritetyn aikaikkunan aikana avattujen yhteyksien päättymisestä varmistutaan[11] aikaikkunan sulkeutuessa. Suojaustasojen välisen vyöhykkeen hallinnoinnin eriyttäminen ympäröivien suojaustasojen hallintaratkaisuista tuo lisäsuojaa erityisesti tilanteisiin, joissa hyökkääjällä on pääsy[12] ylemmän tai alemman suojaustason ympäristön hallintaratkaisuihin. Erityisesti tulee huomioida, että välityspalvelimen lokitietoja ei tule siirtää matalamman suojaustason ympäristöön (piilokanava, vrt. alaviite 8).
Sovelluskohteita	Turvapäivitysten tuonti suojaustason III ympäristöihin. Matalamman tason tiedon tuonti tilannekuvatiedon tarkkuuden parantamiseksi.
Soveltuvuus suojaus-tasoittain	Hyväksyttävissä yhden suojaustason ylittävänä yhdyskäytäväratkaisuna välillä ST IV → ST III.

Viitteellinen esimerkkitoteutus on esitetty kuvassa 2.



Kuva 2. Viitteellinen esimerkkitoteutus yksisuuntaisesta suodatusratkaisusta.

4.2 Alkiotunnistuksen sisältösuodatusratkaisut

Alkiotunnistuksen sisältösuodatusratkaisujen keskeiset ominaispiirteet on kuvattu taulukossa 3.

Taulukko 3. Alkiotunnistuksen sisältösuodatusratkaisujen ominaispiirteitä.

Tiedonsiirron suunta	Ylemmän tason ympäristöstä matalamman tason ympäristöön, matalamman tason ympäristöstä ylemmän tason ympäristöön, edellisten yhdistelmä tai/ja saman suojaustason ympäristöstä toiseen saman suojaustason ympäristöön.
Kuvaus	Toteutukset, joilla mahdollistetaan yksi tai useampi seuraavista käyttötapauksista: A. Ylemmän tason ympäristöstä matalamman luokan tiedon siirto matalamman luokan ympäristöön. B. Matalamman tason ympäristöstä ylemmän tason ympäristöön suuntautuva tiedonsiirto.

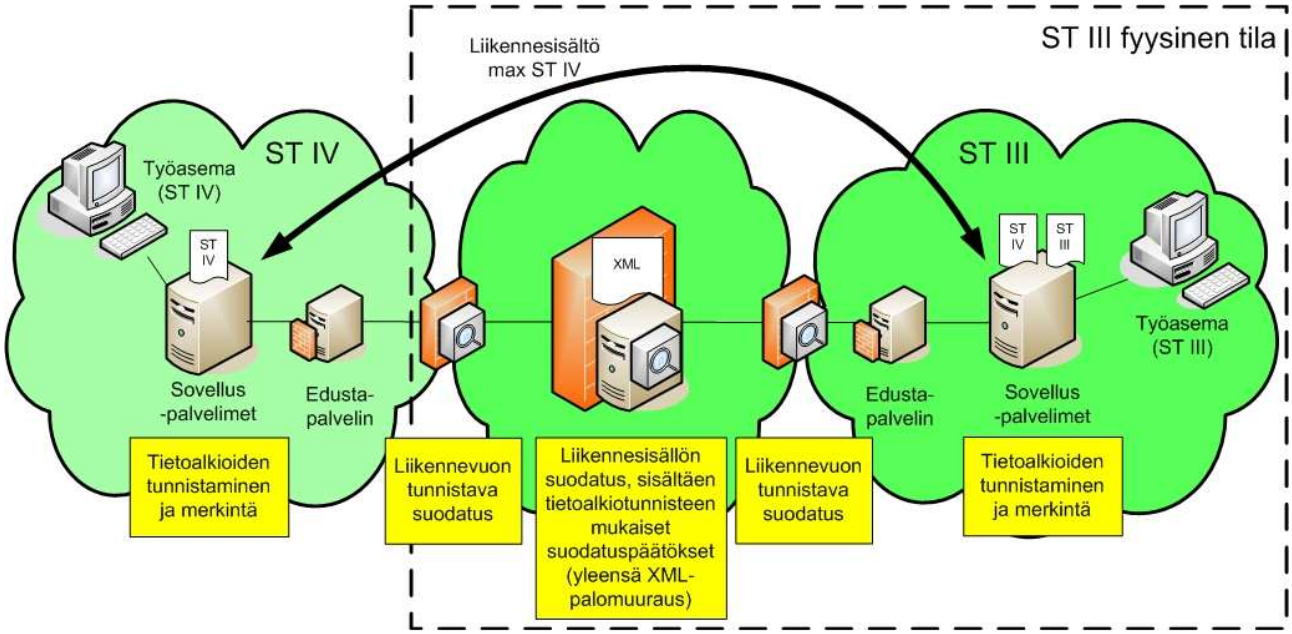
[11] Varmistumisessa voidaan hyödyntää esimerkiksi tilataulun tyhjennystä (flush) tai vastaavaa menetelmää.
[12] Esimerkiksi haittaohjelman avulla.

	C. Tietojen siirto kahden järjestelmän välillä siten, että siirto rajataan vain tarkasti määriteltyihin tietoihin (esimerkiksi kahden eri organisaation hallinnoimien suojaustason III järjestelmien välinen tiedonvaihto[13]). Käyttötapauksiin A, B ja C hyväksyttäviltä toteutuksilta edellytetään seuraavien ehtojen täyttymistä: 1) Tieto tunnistetaan ja merkitään[14] oikeellisesti. 2) Sovellustason sanomamuoto on täsmällisesti määritetty. 3) Määritetyn sanomamuodon noudattaminen tarkistetaan. 4) Sovellustason suodatus toimii luotettavasti oikein merkittyjen, sekä myös virheellisten syötteiden tapauksessa. 5) Sovellustason suodatustoiminnallisuus on eriytetty muusta sovellustoiminnallisuudesta. 6) Suodatustoiminnallisuuden haavoittuvuusavaruus on minimoitu[15] ja suodatus toteutetaan useassa kerroksessa[16]. Liikennesisällön suodatus on toteutettava sekä verkkoteknisesti (IP-portti-rajaukset) että sovelluskerroksen tasolla (esimerkiksi tietotyyppien, pituuksien ja syntaksin tarkastaminen ennen käsittelyä). Useissa hyväksyttävissä olevissa toteutuksissa suodatusta tuetaan lisäksi liikennevuon tunnistavalla suodatuksella (vrt. luku 5.1). Erityisesti sovelluskerroksen tason suodatuksessa tarkastuksen kohteen on pystyttävä osoittamaan, miten suodatusalustan haavoittuvuuksilta on pyritty suojautumaan ja miten suodatusratkaisussa (esimerkiksi XML-palomuurissa) varmistutaan siitä, että datan (esimerkiksi XML-dokumentin) jossain kentässä ei kuljeteta ylemmän suojaustason tietoa matalamman suojaustason ympäristöön. Suodatusalustan eheydestä on myös pystyttävä varmistumaan (huomioitava erityisesti sitominen luotettuun rauta-alustaan ja eheystarkastukset). Liikennesisällön koneellinen suodatus voi joissain yksisuuntaista suodatusratkaisua hyödyntävissä käyttötapauksissa olla osin korvattavissa suppeammilla, esimerkiksi henkilöstön toteuttamaan dokumenttisuodatukseen pohjautuvilla menetelmillä. Tällainen käyttötapaus voi ilmetä esimerkiksi tilanteissa, joissa suojaustason III ympäristössä laaditaan suojaustason IV dokumentti, joka siirretään datadiodin läpi suojaustason IV ympäristöön (vrt. kuva 5). Alkiotunnistuksen sisältösuodatusratkaisuja käytetään usein myös täydentävinä suojauksina osana muita yhdyskäytäväratkaisuja[17].
Sovelluskohteita	Suojaustason III järjestelmät, joista tarve siirtää suojaustason IV tietoa suojaustason IV järjestelmään (esimerkiksi suojaustason III tilannekuvajärjestelmistä siirrettävä suojaustason IV paikkatieto). Suojaustason IV järjestelmät, joista tarve siirtää suojaustason IV tietoa suojaustason III järjestelmään. Organisaation hallinnoima järjestelmä, josta tarve siirtää ja johon tarve vastaanottaa määriteltyjä tietoja (esimerkiksi vain paikkatietoa) toisen organisaation järjestelmään/järjestelmästä.

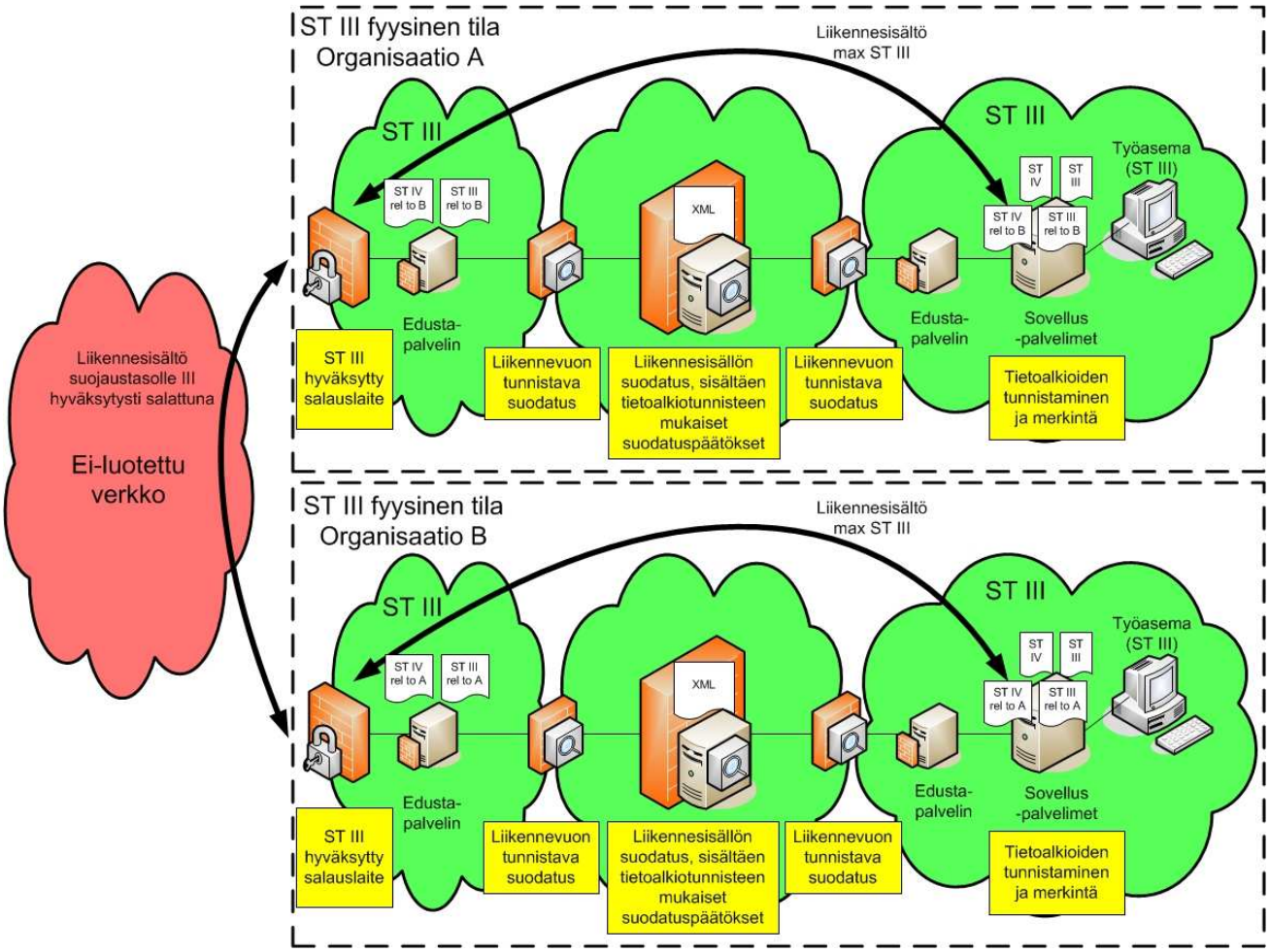
[13] Tässä ohjeessa ei käsitellä eri organisaatioiden välisiä luottosuhteita tai menetelmiä, joilla organisaatiot varmistuvat toistensa tiedonsuojauskyvyn riittävyydestä ennen tietojen luovuttamis-/vaihtopäätöksiä.
[14] Merkinnät voivat sisältää suojaustason lisäksi tiedot esimerkiksi omistajasta, salassapitoajasta ja jakelusta.
[15] Kattaen muun muassa käyttöjärjestelmä-, sovellusohjelmisto- ja verkkokerroksen. Sovellusohjelmistotason käytännön toteutukset edellyttävät usein haavoittuvuusavaruuden rajaamista vain tiukasti määriteltyä toiminnallisuutta tarjoavan edustapalvelimen avulla. Joissain järjestelmissä yhdyskäytävän suuntaan tarjottava sovellustoiminnallisuus saattaa olla rajattavissa myös suoraan taustajärjestelmässä.
[16] Esimerkiksi suodatus palomuurein ja IPS-järjestelmin IP-osoitteen ja portin, ja sovellussuodattimilla esimerkiksi XML-skeeman ja XML-kenttien sisällön osalta. Lisäksi usein IPS-järjestelmin myös liikennöintiprotokollan osalta.
[17] Esimerkiksi datadiodin tai muun yksisuuntaisen suodatusratkaisun läpi siirretyn aineiston validointi.

Soveltuvuus suojaus-tasoittain	Hyväksyttävissä yhden suojaustason ylittävänä yhdyskäytäväratkaisuna välillä ST IV ←→ ST III. Käyttötapauksen A toteutus datadiodiin yhdistettynä (vrt. kuva 5) hyväksyttävissä myös välillä ST II → ST III ja ST II → ST IV.

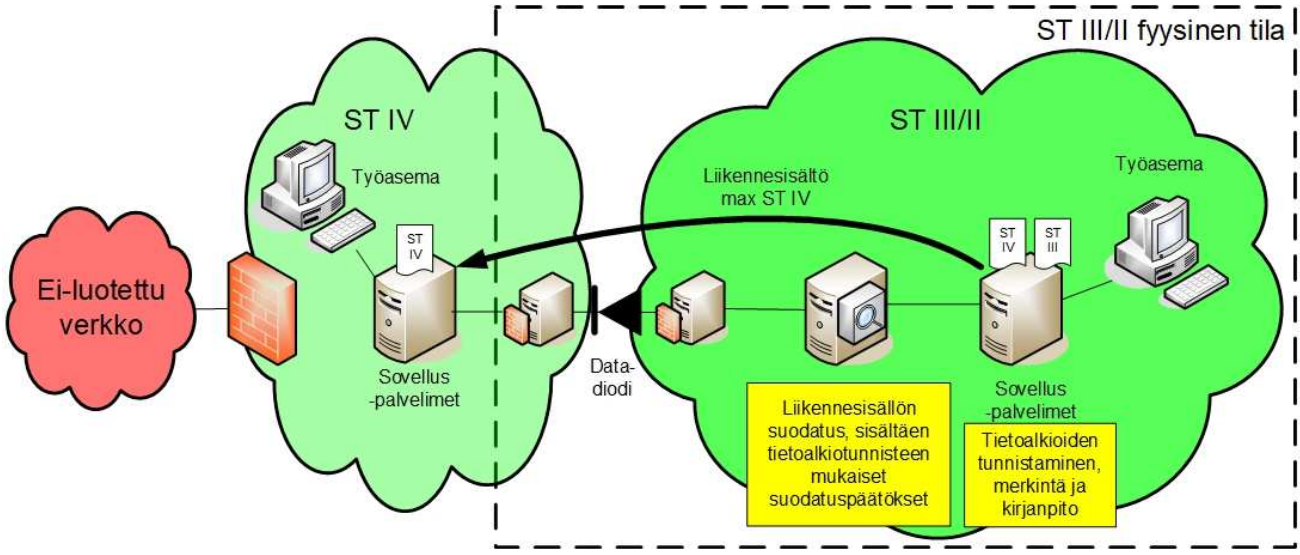
Viitteellisiä esimerkkitoteutuksia on esitetty kuvissa 3, 4 ja 5.



Kuva 3: Viitteellinen esimerkkitoteutus alkiotunnistuksen sisältösuodatusratkaisusta.



Kuva 4. Viitteellinen esimerkkitoteutus alkiotunnistuksen sisältösuodatusratkaisusta.



Kuva 5. Viitteellinen esimerkkitoteutus alkiotunnistuksen sisältösuodatusratkaisusta.

5 Muita ratkaisumalleja

Tässä luvussa kuvattavien ratkaisumallien turvallisuudessa on tiettyjä tunnistettuja heikkouksia, mistä johtuen ne eivät lähtökohtaisesti ole NCSA:n yleisesti hyväksyttävissä. Tietyissä järjestelmissä ei ole kuitenkaan mahdollista käyttää luvun 4 malleja esimerkiksi käyttöympäristön poikkeavasta luonteesta johtuen[18]. Tiedon omistaja voi tällaisissa tilanteissa riskienarviointinsa perusteella mahdollisesti hyväksyä näitä ratkaisumalleja omien tietojensa suojaamiseen.

5.1 Liikennevuon sisältösuodatusratkaisut

Liikennevuon sisältösuodatusratkaisujen keskeiset ominaispiirteet on kuvattu taulukossa 4.

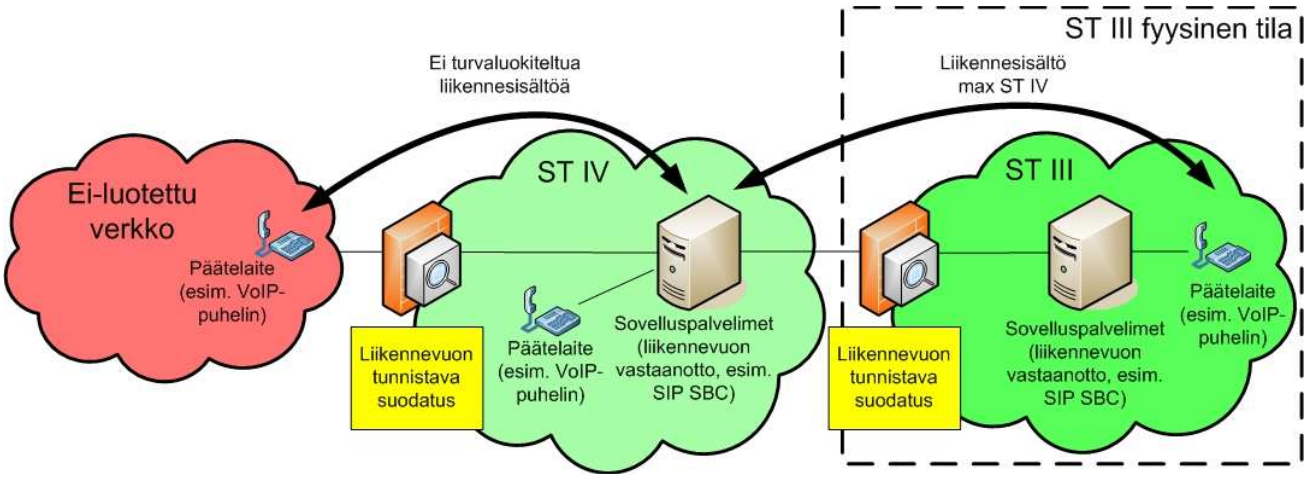
Taulukko 4. Liikennevuon sisältösuodatusratkaisujen keskeiset ominaispiirteet.

Tiedonsiirron suunta	Matalamman tason ympäristöstä ylemmän tason ympäristöön tai/ja ylemmän tason ympäristöstä matalamman tason ympäristöön tai/ja saman suojaustason ympäristöstä toiseen saman suojaustason ympäristöön.
Kuvaus	Toteutukset, joilla mahdollistetaan yksi tai useampi seuraavista käyttötapauksista: A. Matalamman tason ympäristöstä ylemmän tason ympäristöön suuntautuva tiedonsiirto. B. Ylemmän tason ympäristöstä matalamman luokan tiedon siirto matalamman luokan ympäristöön. Toteutuksissa täyttyvät tyypillisesti seuraavat yleisperiaatteet: 1) Liikennevuo on täsmällisesti määritetty. 2) Liikennevuomäärityksen noudattaminen tarkistetaan. 3) Suodatus toimii luotettavasti oikeiden, sekä myös virheellisten syötteiden tapauksessa. 4) Suodatustoiminnallisuus on eriytetty sovelluspalvelun toiminnallisuudesta. 5) Suodatustoiminnallisuuden haavoittuvuusavaruus on minimoitu[19] ja suodatus toteutetaan useassa kerroksessa[20]. Liikennevuon sisältösuodatus toteutetaan sekä verkkoteknisesti (IP-portti-rajaukset), että liikennevuon tunnistavalla suodatuksella (esimerkiksi sallimalla kyseisestä portista liikennöinnin vain tunnistetun ja hyväksytyn protokollan avulla). Liikennevuon suodatuksella tarkastetaan esimerkiksi pakettien kehystyksen oikeellisuus (täsmääkö määrityksiin, onko muodollisesti oikeaa liikennettä), pakettien kehysten kenttien maksimi-/minimipituudet (tiettyjen puskuriylivuotohyökkäysten suodatus) sekä pakettien kehysten kenttien sisällön muodollinen kelpoisuus (onko esimerkiksi sekvenssinumeroa kuvaavan kentän sisältö numeerinen). Liikennevuon sisältösuodatus sallii vain muodollisesti oikeelliseksi tunnistetut liikennevuot (whitelisting). Liikennevuon sisältösuodatuksen suodatusalustan eheydestä pyritään varmistumaan (erityisesti sitominen luotettuun rauta-alustaan ja eheystarkastukset). Yhteyksien avaaminen rajataan yleensä mahdolliseksi vain ylemmän suojaustason ympäristöstä käsin. Liikennevuon sisältösuodatusratkaisuja käytetään usein täydentävinä suojauksina osana muita yhdyskäytäväratkaisuja[21].

[18] Esimerkiksi tietyt viranomaisoperaatiot, joissa käsiteltävän suojaustason III tiedon salassapitoaika on lyhyt, ja joissa käytettävien kulkuneuvojen fyysiset ominaisuudet eivät mahdollista useamman päätelaitteen asennusta.
[19] Kattaen muun muassa käyttöjärjestelmä-, sovellusohjelmisto- ja verkkokerroksen.
[20] Esimerkiksi suodatus palomuurein IP-osoitteen ja portin, sekä IPS-järjestelmin liikennöintiprotokollan osalta.
[21] Esimerkiksi alkiotunnistuksen sisältösuodatusratkaisun tukeminen liikennevuon sisältösuodatuksella.

Sovelluskohteita	Suojaustason IV tai III järjestelmä, johon on tarve tuoda matalamman suojaustason tietosisältöä siirtävä liikennevuo (esimerkiksi VoIP-puheluliikenne) matalamman suojaustason ympäristöstä.
Soveltuvuus suojaus-tasoittain	Tiedon omistaja voi mahdollisesti oman riskienarviointinsa perusteella hyväksyä omistamiensa tietojensa suojaamiseen, lähtökohtaisesti välillä Internet → ST IV tai/ja Internet → ST III.

Viitteellinen esimerkkitoteutus on esitetty kuvassa 6.



Kuva 6. Viitteellinen esimerkkitoteutus liikennevuon sisältösuodatusratkaisusta.

5.2 Virtualisointiratkaisut

Virtualisointiratkaisujen keskeiset ominaispiirteet on kuvattu taulukossa 5.

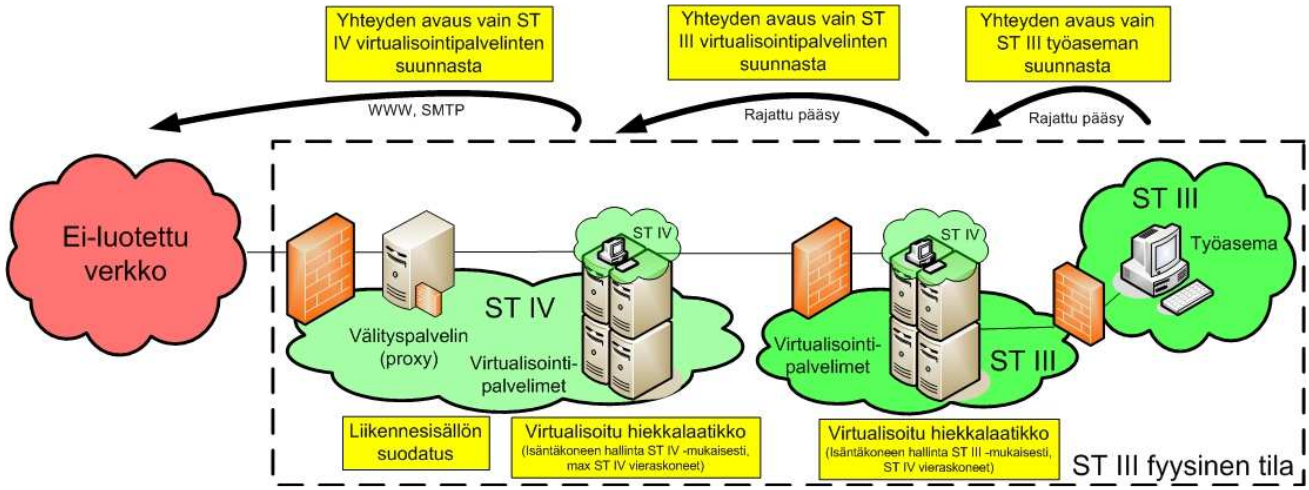
Taulukko 5. Virtualisointiratkaisujen ominaispiirteitä.

Tiedonsiirron suunta	Matalamman tason ympäristöstä ylemmän tason ympäristöön.
Kuvaus	Toteutukset, joilla mahdollistetaan matalamman tason ympäristön käyttö ylemmän tason ympäristöstä käsin. Tyypillisiä toteutusmalleja ovat esimerkiksi web-selailun ja sähköpostipalvelujen virtualisointiratkaisut. Virtualisointiratkaisuissa suojaustasojen erottelussa nojataan usein käytettyjen virtualisointiohjelmistojen tarjoamaan suojaukseen isäntäkoneen ("host") ja vieraskoneen ("guest") erottelussa[22]. Joidenkin hyökkäysmenetelmien riskejä voidaan pienentää käyttämällä ketjutettuna useampaa eri virtualisointiratkaisutuotetta. Useissa ratkaisuissa suojaustasojen erottelua tuetaan erillisellä ohjelmistoratkaisulla, jolla ylemmän tason ympäristöön tarjotaan matalamman suojaustason vieraskoneesta vain peruskäsittelyrajapinta (näyttö, näppäimistö, hiiri) ilman esimerkiksi leikepöytä- tai levykäyttörajapintoja. Tässä mallissa isäntäkoneen hallinta- ja valvontaratkaisut tulee toteuttaa aina ylemmän suojaustason mukaisesti, ja yhteyksien avaaminen rajataan mahdolliseksi vain ylemmän suojaustason ympäristöstä käsin. Esimerkiksi web-selailun virtualisointiratkaisuissa huomioidaan tyypillisesti myös vieraskoneiden säännöllinen uudelleenalustus luotettavasta lähteestä, vieraskoneiden looginen erottelu toisistaan (esimerkiksi VLAN-erottelu) sekä vieraskoneiden ja ei-luotetun verkon välisen liikenteen suodatus tunnettujen haitallisten sisältöjen osalta välityspalvelimen ("proxy") avulla.
Sovelluskohteita	Web-selailun tai Internetissä reitittyvän sähköpostipalvelun käyttö suojaustason III ympäristöstä.

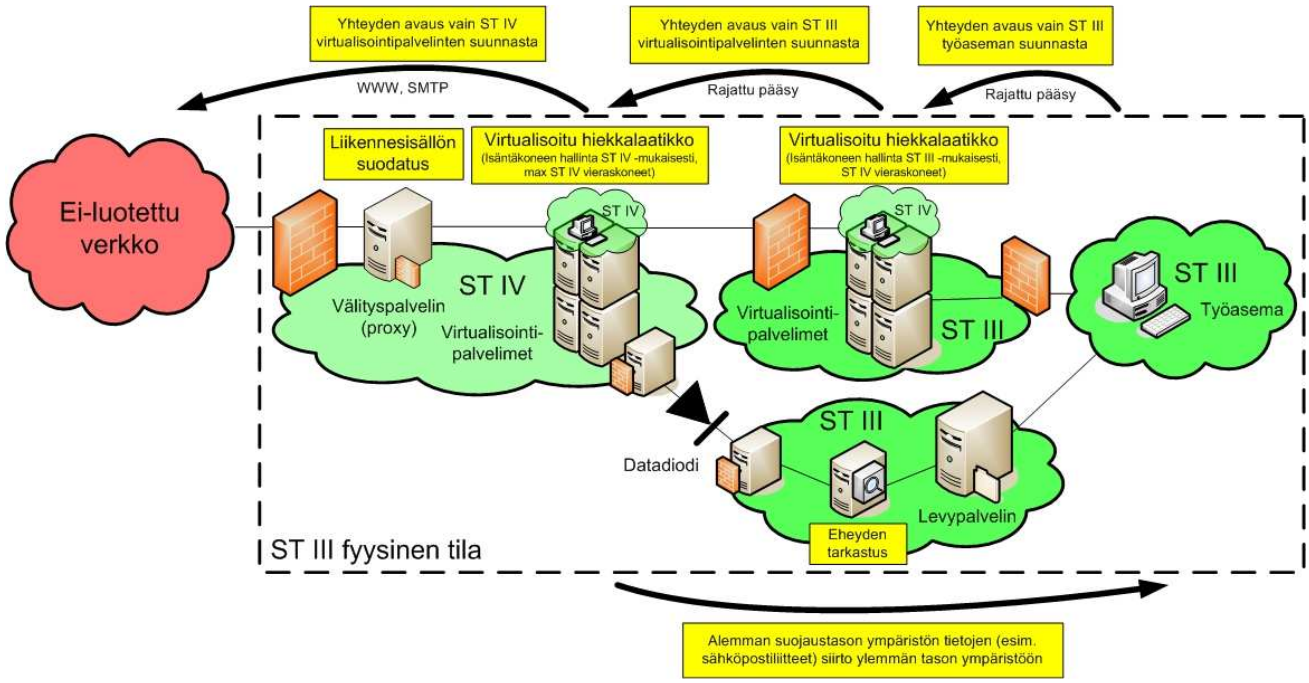
[22] Erottelusta käytetään usein käsitettä "hiekkalaatikointi" (sandboxing).

Soveltuvuus suojaus-tasoittain	Tiedon omistaja voi mahdollisesti oman riskienarviointinsa perusteella hyväksyä omistamiensa tietojensa suojaamiseen, lähtökohtaisesti välillä Internet → ST IV tai/ja Internet → ST III.

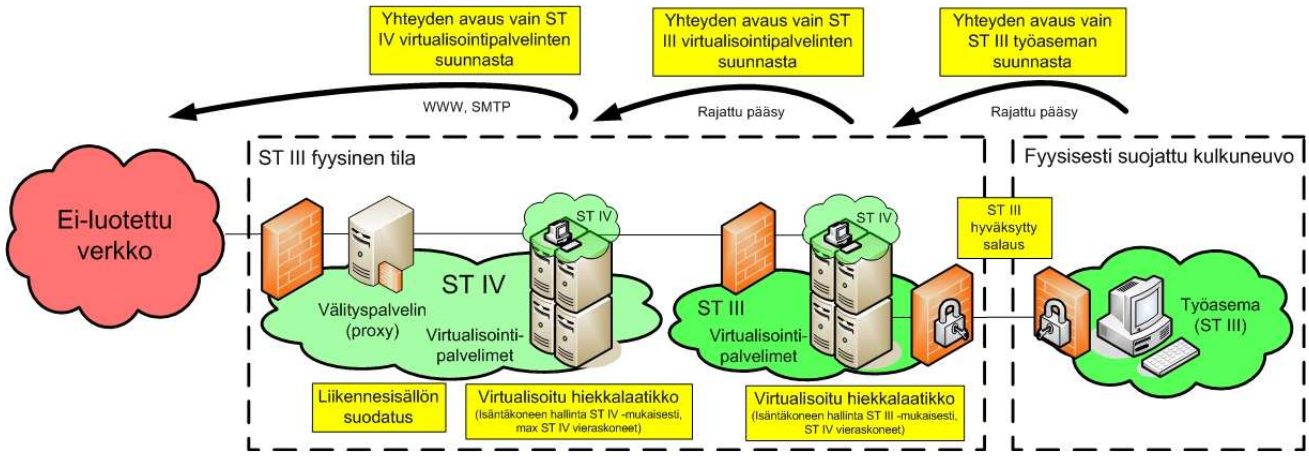
Viitteellisiä esimerkkitoteutuksia on esitetty kuvissa 7, 8 ja 9.



Kuva 7. Viitteellinen esimerkkitoteutus virtualisointiratkaisusta.



Kuva 8. Viitteellinen esimerkkitoteutus virtualisointiratkaisusta.



Kuva 9. Viitteellinen esimerkkitoteutus virtualisointiratkaisusta.

5.3 KVM-ratkaisut

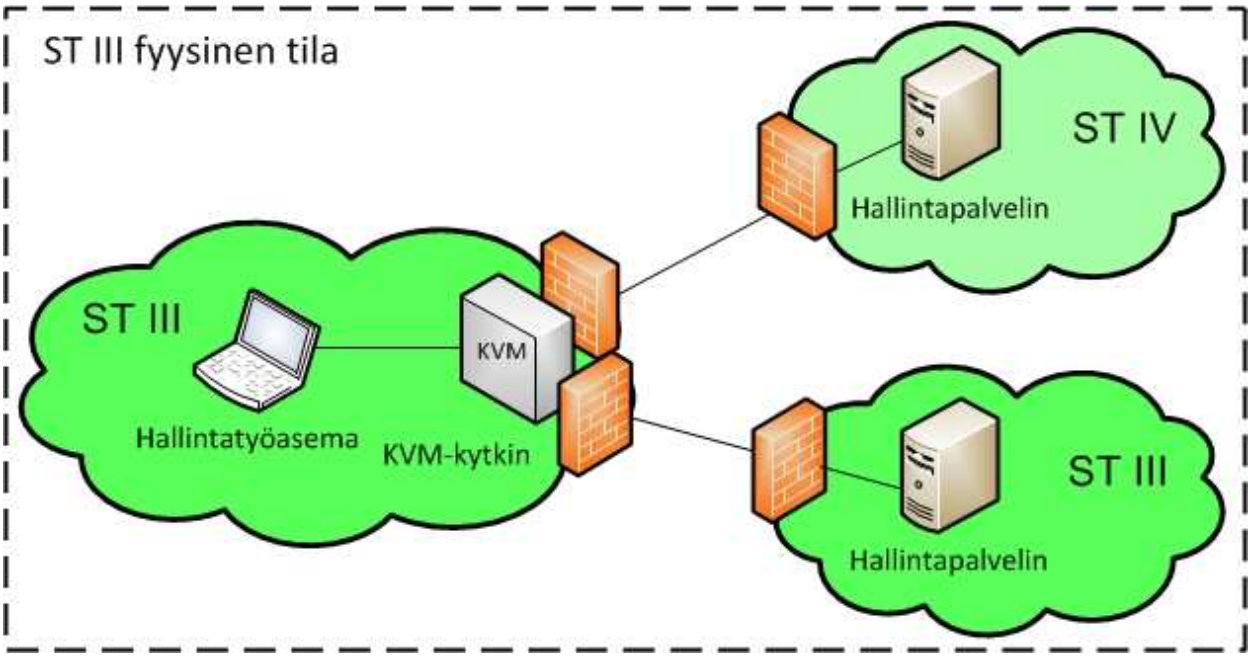
KVM-ratkaisujen (engl. "Keyboard, Video, Mouse") keskeiset ominaispiirteet on kuvattu taulukossa 6.

Taulukko 6. KVM-ratkaisujen ominaispiirteitä.

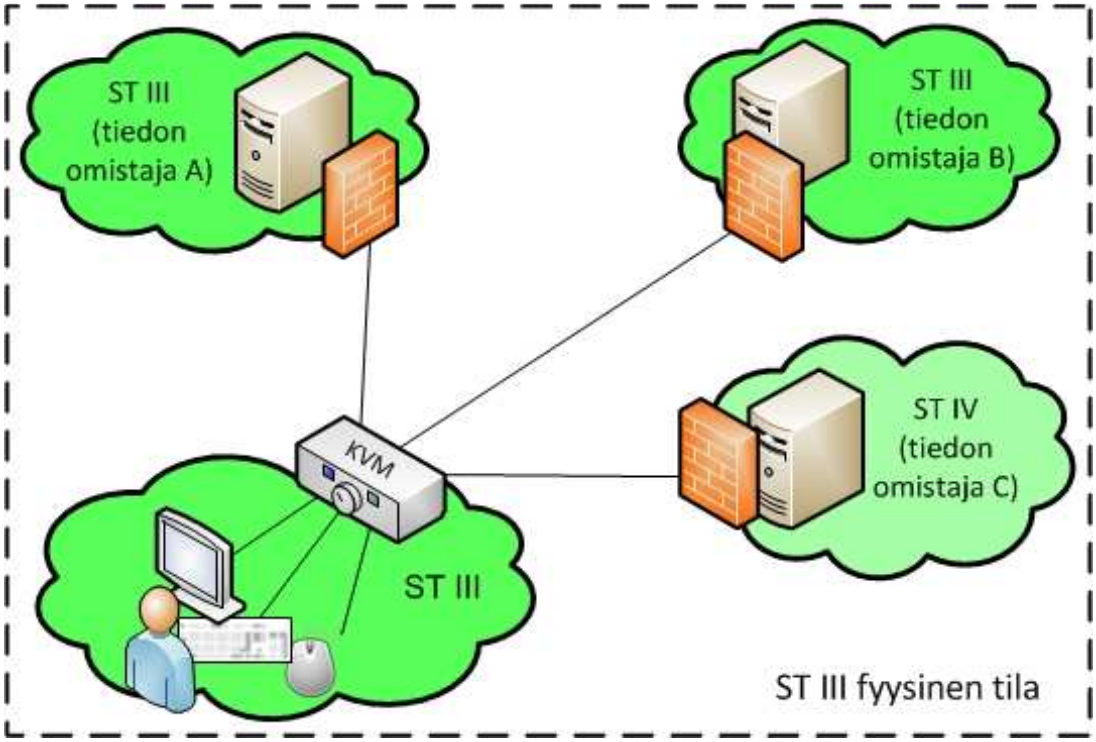
Tiedonsiirron suunta	Matalamman tason ympäristöstä ylemmän tason ympäristöön, ylemmän tason ympäristöstä matalamman tason ympäristöön, tai/ja saman suojaustason ympäristöstä toiseen saman suojaustason ympäristöön.
Kuvaus	Toteutukset, joilla mahdollistetaan yksi tai useampi seuraavista käyttötapauksista: A. Matalamman tason ympäristön hallinta ylemmän tason ympäristöstä käsin. B. Yhden näppäimistön, näytön ja hiiren sisältävän työpisteen liittäminen eri suojaustasojen tai eri tiedon omistajien ympäristöihin. Yleisimpien KVM-ratkaisujen turvallisuus perustuu KVM-kytkimen kykyyn rajata liikennöinti vain näppäimistön, näytön ja hiiren toiminnallisuuksiin. Toteutustavat vaihtelevat fyysisestä (mekaanisesta) eriytyksestä monitasoiseen loogiseen (ohjelmistopohjaiseen) eriyttämiseen. KVM-ratkaisujen turvallisuutta yhdistää tuotekohtaisuus. Tällä tarkoitetaan sitä, että eri valmistajien tuotteet ja tuotemallit, kuten myös saman valmistajan eri tuotteet, voivat erota merkittävästi luotettavuudeltaan. Useat tuotevalmistajat pyrkivät osoittamaan tuotteensa luotettavuutta esimerkiksi eri maiden viranomaisten tuotehyväksymisprosessien kautta[23]. KVM-ratkaisuja yhdistää tyypillisesti myös se, että ne eivät pysty estämään ylemmän suojaustason tiedon kulkeutumista matalamman suojaustason ympäristöön tilanteissa, joissa esimerkiksi haittaohjelma pystyy käyttämään ylemmän suojaustason ympäristön näppäimistöä.
Sovelluskohteita	Suojaustason III hallintatyöasemalta käsin tapahtuva suojaustason IV ympäristön ylläpito/hallinta. Käyttäjän pääsy työpisteeltään, samaa näppäimistöä, näyttöä ja hiirtä käyttäen, eri suojaustasojen tai eri tiedon omistajien ympäristöihin.
Soveltuvuus suojaus-tasoittain	Tiedon omistaja tai sen valtuuttama taho voi mahdollisesti hyväksyä täydentävillä suojauksilla varustettuja tuotteita riskienarviointinsa perusteella, lähtökohtaisesti välillä ST IV → ST III, Internet → ST IV tai/ja saman suojaustason sisällä (eri tiedon omistajat).

Viitteellisiä esimerkkitoteutuksia on esitetty kuvissa 10 ja 11.

[23] Joidenkin maiden joihinkin käyttötapauksiin hyväksymiä tuotteita on listattu osoitteessa http://www.ia.nato.int/niapc.



Kuva 10. Viitteellinen esimerkkitoteutus KVM-ratkaisusta.



Kuva 11. Viitteellinen esimerkkitoteutus KVM-ratkaisusta.

5.4 Ohutpääteratkaisut

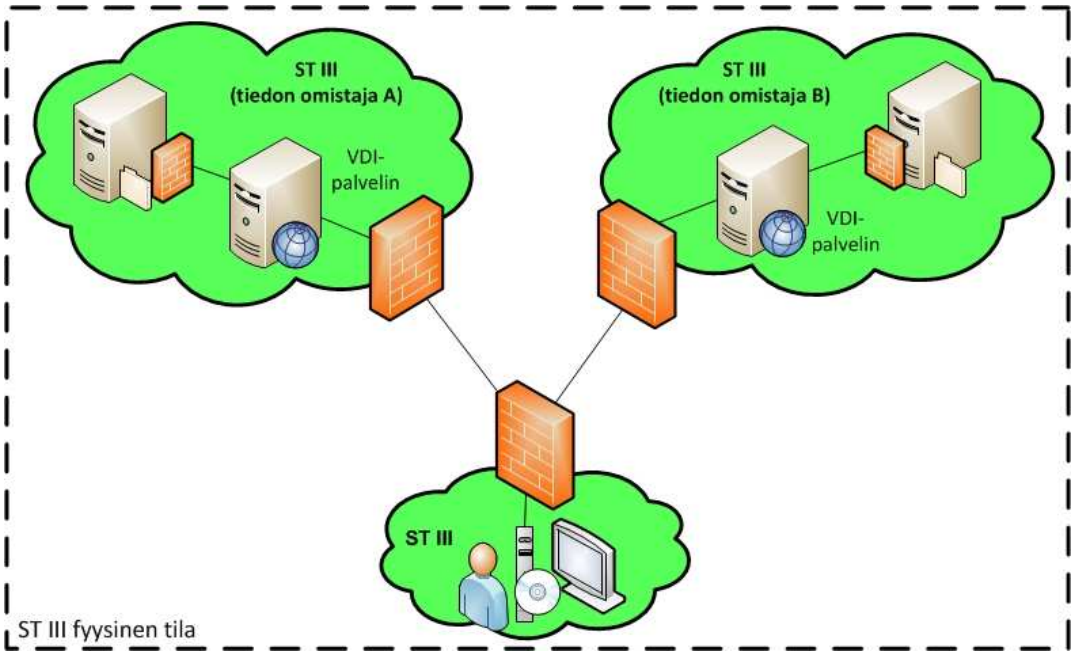
Ohutpääteratkaisujen (engl. "thin/zero client") keskeiset ominaispiirteet on kuvattu taulukossa 7.

Taulukko 7. Ohutpääteratkaisujen ominaispiirteitä.

Tiedonsiirron suunta	Matalamman tason ympäristöstä ylemmän tason ympäristöön, ylemmän tason ympäristöstä matalamman tason ympäristöön, tai/ja saman suojaustason ympäristöstä toiseen saman suojaustason ympäristöön.
Kuvaus	Toteutukset, joilla mahdollistetaan yksi tai useampi seuraavista käyttötapauksista:

	A. Eri suojaustasojen ympäristöjen käyttö yhdellä päätelaitteella. B. Eri tiedon omistajien ympäristöjen käyttö yhdellä päätelaitteella. Yleisimpien ohutpääteratkaisujen turvallisuus perustuu siihen, että päätelaite alustetaan jokaisen käyttökerran alussa luotetusta lähteestä ja tyhjennetään aina käyttökerran päätyttyä. Tyypillisiä alustamiseen käytettyjä menetelmiä ovat käynnistäminen kirjoitussuojatulta medialta[24] tai fyysisesti suojatusta verkkokytkennästä. Erityisesti luotettava tyhjentäminen on haaste, johon tyypillisesti pyritään vastaamaan minimoimalla päätelaitteen ohjelmallisesti muokattavat laitteisto-osat ja toiminnallisuudet[25], sekä tarjoamalla päätelaitteelle suojattavat tiedot vain virtuaalityöpöytäratkaisuilla[26]. Ohutpääteratkaisut eivät tyypillisesti kykene estämään suojattavan tiedon kulkeutumista[27] päätelaitteelle. Päätelaite tuleekin suojata aina korkeimman sillä käsiteltävän tiedon suojaustason mukaisesti. Erityisiä riskejä liittyy tilanteisiin, joissa päätelaitteelle tarjotaan samanaikaisesti eri suojaustasojen tai eri tiedon omistajien tietoja. Useimmissa ratkaisuissa on mahdollisuus pyrkiä ohjelmallisesti estämään tiedon välittyminen, esimerkiksi leikepöydän kautta, eri virtuaalityöpöytäistuntojen välillä. Näissä tilanteissa tietojen erottelu nojaa usein vain virtuaalityöpöytäratkaisun ohjelmistototeutuksen luotettavuuteen.
Sovelluskohteita	Samalla päätelaitteella tapahtuva eri suojaustason tai/ja eri tiedon omistajien ympäristöjen käyttö.
Soveltuvuus suojaus-tasoittain	Tiedon omistaja tai sen valtuuttama taho voi mahdollisesti hyväksyä ratkaisuja riskienarviointinsa perusteella, lähtökohtaisesti välillä ST IV → ST III, Internet → ST IV tai/ja saman suojaustason sisällä (eri tiedon omistajat).

Viitteellinen esimerkkitoteutus on esitetty kuvassa 12.



Kuva 12. Viitteellinen esimerkki ohutpääteratkaisusta.

[24] Esimerkiksi CD-ROM-levy.
[25] Esimerkiksi käyttämällä päätelaitetta, jossa ainoa pysyvämmän tiedontallennuksen mahdollistava muistialue (tyypillisesti laiteohjelmisto, engl. firmware) on laitteistotasolla lukittu.
[26] Engl. Virtual desktop infrastructure, VDI.
[27] Tieto välittyy tyypillisesti ainakin kuvana.

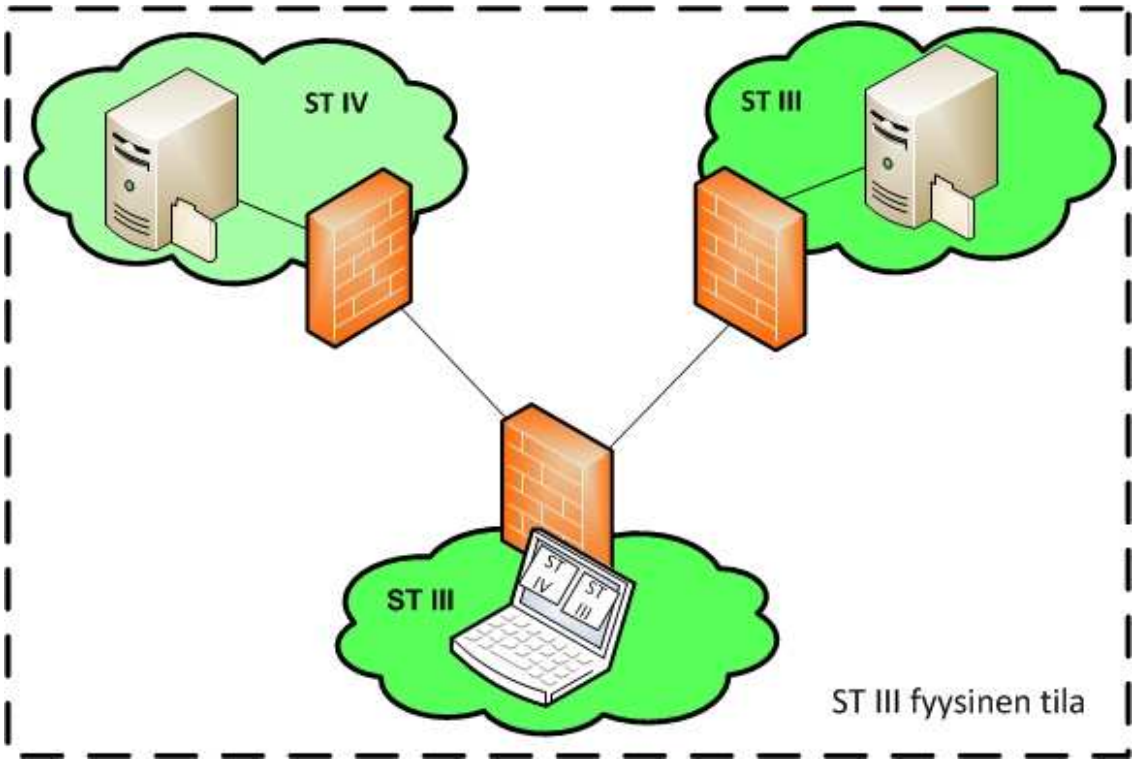
5.5 Monitasopääteratkaisut

Monitasopääteratkaisujen keskeiset ominaispiirteet on kuvattu taulukossa 8.

Tiedonsiirron suunta	Matalamman tason ympäristöstä ylemmän tason ympäristöön, ylemmän tason ympäristöstä matalamman tason ympäristöön, tai/ja saman suojaustason ympäristöstä toiseen saman suojaustason ympäristöön.
Kuvaus	Toteutukset, joilla mahdollistetaan eri suojaustasojen ympäristöjen käyttö yhdellä erikoisvalmisteisella päätelaitteella. Monitasopääteratkaisujen turvallisuus perustuu päätelaitteen laitteisto- tai/ja ohjelmistotasolla toteutettavaan suojaustasojen erotteluun. Erottelu on tuotteesta riippuen toteutettu joko A) täysin ohjelmistolla, B) osin ohjelmistolla ja osin laitteistolla, tai C) täysin laitteistolla. Mallin A ratkaisuissa laitteistoalustan päällä ajetaan räätälöityä käyttöjärjestelmäalustaa, jonka pääasialliset tehtävät ovat tarjota laitteistoalustan käyttämiseen välttämättömät rajapinnat, sekä virtualisointiratkaisu, jonka päällä varsinaiset eri suojaustasojen tietoa sisältävät virtuaalikoneet ajetaan. Tällaisille ratkaisuille on tyypillistä, että räätälöity käyttöjärjestelmäalusta on huomattavasti suppeampi kuin yleiset saatavilla olevat käyttöjärjestelmät, ja suppeampi koodimäärä on pyritty toteuttamaan mahdollisimman virheettömästi. Tällaisten ratkaisujen tarjoama suojaustasojen erottelu nojaa erityisesti räätälöidyn käyttöjärjestelmäalustan luotettavuuteen. Mallin B ratkaisuissa suojaus nojaa osin ohjelmisto- ja osin laitteistotason erotteluun. Tyypillinen ratkaisumalli on, että eri suojaustason ympäristöt asennetaan fyysisesti erillisille kiintolevyille, mutta hyödyntävät esimerkiksi samoja fyysisiä verkkoportteja. Mallin C ratkaisuissa erottelu on pyritty toteuttamaan mahdollisimman pitkälti fyysisellä tasolla. Tyypillinen ratkaisumalli on, että keskeinen eri suojaustasoille yhteinen laitteisto on näyttö, mutta että lähes kaikki muut laitteistot on kahdennettu päätelaitteen ulkokuoren sisällä. Monitasopäätelaitteiden turvallisuutta yhdistää tuotekohtaisuus. Tällä tarkoitetaan sitä, että eri valmistajien tuotteet, kuten myös saman valmistajan eri tuotteet, voivat olla luotettavuudeltaan merkittävästi eroavia. Useat tuotevalmistajat pyrkivät osoittamaan tuotteensa luotettavuutta esimerkiksi eri maiden viranomaisten tuotehyväksymisprosessien kautta[28]. Monitasopäätelaitteita yhdistää myös se, että niitä ei ole tyypillisesti suunniteltu tilanteisiin, joissa eri tiedon omistajat varaavat teknisen tarkastusoikeuden tietojensa käsittely-ympäristöihin.
Sovelluskohteita	Samalla päätelaitteella tapahtuva eri suojaustason ympäristöjen käyttö.
Soveltuvuus suojaus-tasoittain	Tiedon omistajalle tai sen valtuuttamalle taholle saattaa olla mahdollista hyväksyä ratkaisuja riskienarviointinsa perusteella, lähtökohtaisesti välillä ST IV → ST III tai Internet → ST IV.

Viitteellinen esimerkkitoteutus on esitetty kuvassa 13.

[28] Joidenkin maiden joihinkin käyttötapauksiin hyväksymiä tuotteita on listattu osoitteessa http://www.ia.nato.int/niapc.



Kuva 13. Viitteellinen esimerkki monitasopääteratkaisusta.

6 Lisätietoa

1. Bell, D & LaPadula, L. 1973. Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, Volume I & II.
2. Euroopan unionin neuvosto. 2013. Neuvoston päätös turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi (2013/488/EU). URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:274:0001:0050:FI:PDF.
3. International Organization for Standardization. 1994. ISO/IEC 7498-1:1994. Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model.
4. Jones, D & Bowersox, T. 2006. Secure data export and auditing using data diodes. In Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop (EVT'06). URL: http://homepage.cs.uiowa.edu/~jones/voting/diode/evt06paper.pdf.
5. Kang, M, Moskowitz, I & Chincheck, S. 2005. The Pump: A Decade of Covert Fun. In Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC '05). URL: http://www.acsac.org/2005/papers/Kang.pdf.
6. NIST. 2004. NIST Special Publication 800-27 Rev A: Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A. URL: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
7. Okhravi, H & Sheldon, F. 2010. Data Diodes in Support of Trustworthy Cyber Infrastructure. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '10). URL: http://info.ornl.gov/sites/publications/files/Pub24025.pdf.
8. Puolustusministeriö. 2015. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. URL: http://www.defmin.fi/katakri.
9. Stevens, M. 1995. An Implementation of an Optical Data Diode. DSTO-TR-0785. URL: http://www.dsto.defence.gov.au/publications/2110/DSTO-TR-0785.pdf.
10. Valtiovarainministeriö. 2012. Teknisen ICT-ympäristön tietoturvataso-ohje (VAHTI 3/2012). URL: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20121122Teknis/ICT_taitto.pdf.

7 Ohjeen ylläpito

Tämän ohjeen ylläpidosta vastaa Viestintävirasto. Mahdollisista puutteista pyydetään olemaan yhteydessä Viestintävirastoon.