Turvallisuusluokitellun verkkoympäristön parantaminen

Vesa Hartonen

Opinnäytetyö, AMK
Joulukuu 2021
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Hartonen Vesa

Turvallisuusluokitellun verkkoympäristön parantaminen

Jyväskylä: Jyväskylän ammattikorkeakoulu. **Joulukuu 2021**, 77 sivua

Tekniikan ala. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Tietoturvallinen toimintaympäristö on yhä tärkeämpää. Tämä korostuu erityisesti valtioiden tärkeänä pitämän tiedon käytössä, siten että niihin on pääsy ainoastaan tähän etukäteen hyväksytyillä henkilöillä. Enenevässä määrin onkin tärkeää, että valtiot voivat luoda ja ylläpitää kustannustehokkaita ja moderneihin tietoturvavaatimuksiin vastaavia verkkoympäristöjä, joissa kansallisen turvallisuuden kannalta kriittinen tieto pysyy aina turvassa. Tähän haasteeseen Yhdysvaltain kansallisen turvallisuuden virasto (National Security Agency, NSA) on kehittänyt CSfC-ohjelman.

Opinnäytteen tarkoituksena oli tutkia tätä NSA:n kehittelemää ohjelmaa tietoturvallisten ympäristöjen luomiseen. CSfC-ohjelman tarkoituksena on ollut asettaa moderneihin tietoturvavaatimuksiin vastaavat puitteet, jonka pohjalta avoimilla markkinoilla toimivat yritykset voivat kehittää valmiita toteutuksia, joita valtion virastot puolestaan voivat hankkia ja odottaa, että hankitut ratkaisut ovat riittävän tietoturvallisia. Lisäetua saadaan myös sillä, että julkisilla varoilla tehdyt hankinnat pysyvät kustannuksiltaan kohtuullisina.

Selvityksen perusteella CSfC-ohjelman toteuttaminen sellaisenaan Suomessa, tai ylipäätään Yhdysvaltain ulkopuolella, on hankalaa. Markkinoilla tarjolla olevat toteutukset ovat järjestään vain Yhdysvaltojen viranomaisille suunnattuja. Opinnäytteessä päädyttiinkin ehdotukseen ottaa CSfC-ohjelma vertailukohteeksi, jonka perusteella voidaan tulevaisuudessa kehittää tietoturvallisempia ympäristöjä.

Avainsanat (asiasanat)

tietoliikenne, tietoturva

jamk

Description

Hartonen Vesa

Improving classified network

Jyväskylä: JAMK University of Applied Sciences, December 2021, 77 pages

Engineering and technology. Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for web publication: Yes

Language of publication: Finnish

Abstract

Safety of information networks is increasingly important. This can be seen in the usage of information held important to nations, so that only those with suffiecient clearance can access said information. It could be argued that it is increasingly important for nations to be able to create and manage cost-effective and secure information networks, that are able to hold classified information securely. This is a challenge the National Security Agency of the United States has tried to solve by creating CSfC-program.

The purpose of this thesis was to study the CSfC-program. This program aims to set the framework for modern information security, from which commercially available products are able to be created. These products can in turn then be bought cost-effectively by govenrment agencies with the expectation that the bought solutions are able to meet the standards for modern classified information networks.

Based on the results, it seems unlikely that CSfC-program could be implemented in Finland, or anywhere outside of the United States, as it is. Solutions available commercially are aimed solely for the various organizations under united States government. For this reason this thesis ended up recommending that the CSfC-program used as a reference for future projects regarding information networks of the Finnish government.

Keywords/tags (subjects)

information network, information security

Sisältö

Kuviot

Taulukot

Työssä käytetyt termit ja lyhenteet

CSfC

Commercial Solutions for Classifieds.

CP

Capability Package. Opinnäytteessä käytetään suomenkielisenä terminä ominaisuuspaketti.

EUD

End-user device. Loppukäyttäjän käyttämä työnantajaorganisaation hallinnoima laite. Tällaisia ovat esimerkiksi matkapuhelin ja kannettava tietokone.

IDS/IPS

Intrusion Detection System ja Intrusion Prevention System. Järjestelmiä, joiden tarkoitus on joko havainnoida tai havainnoida ja reagoida tietoturvapoikkeamiin

IPsec

IP Security Architecture. IPsec on kokoelma erilaisia protokollia, joilla voidaan luoda turvallinen VPN-yhteys.

MACsec

Media Access Control Security. IPsec vastaava tapa luoda VPN-yhteys. Toimii OSI-mallin siirtoyhteyskerroksella

SIEM

Security Information and Event Management. Useiden eri järjestelmien tietoturvan valvontajärjestelmä

VPN

Virtual Private Network. Virtuaalinen erillisverkko on yleisnimitys menetelmille, joilla voidaan kaksi tai useampaa erillistä verkkoa yhdistää virtuaalisesti yhdeksi kokonaisuudeksi.

WLAN

Wireless Local Area Network, langaton lähiverkko

1 Johdanto

1.1 Tausta ja toimeksiantaja

Turvallisuusluokitelluissa ympäristöissä on tarpeen olla perillä uusista tavoista suojata tietoverkkoja. Nämä menetelmät ja teknologiat ovat yleensä kaupallisia ratkaisuja, joten on tärkeää, että niistä ei muodostu tietoturvariskiä käyttäjille. Koska kaupalliset ratkaisut ovat helposti saatavilla ja yleensä kustannuksiltaan kohtuullisia, on julkisten tahojen etuna myös jatkossa pystyä käyttämään tällaisia ratkaisuja. Tähän tähtää CSfC-ohjelma. (Commercial Solutions for Classified (CSfC))

CSfC on ensisijaisesti kehitelty Yhdysvaltain valtion virastojen tarpeisiin. Tämä opinnäyte käy läpi mikä CSfC-ohjelma on, sekä sen yleistä soveltuvuutta eri valtioiden virastoille, erityisesti Suomelle.

Opinnäytteen toimeksiantajana oli valtion toimialariippumattomia ICT-palveluja tuottava Valtori. Valtori on perustettu vuonna 2014 tarkoituksena koota yhteen eri valtion virastojen silloiset varsin erilaiset ICT-toteutukset, joita virastot olivat toteuttaneet omiin tarpeisiinsa. Valtorin alaisuudessa toimii lisäksi korotettua turvallisuutta vaativien viranomaisten ympäristöjä ylläpitävä turvallisuusverkkopalvelut.

1.2 Opinnäytteen tavoite ja tutkimuskysymykset

Opinnäytteen tavoitteena oli selvittää Yhdysvaltain kansallisesta turvallisuudesta vastaavan viraston NSA:n kehittelemää CSfC-ratkaisua, jolla voidaan toteuttaa moderneja ja tietoturvallisia turvallisuusluokiteltuja verkkoympäristöjä

Opinnäytteelle asetettiin tutkimuskysymykseksi:

Voidaanko CSfC ottaa käyttöön Suomessa turvallisuusluokitelluissa verkoissa?

Tämän lisäksi kysymykselle asetettiin kaksi apukysymystä, jotka ovat:

- Mikä CSfC on ja miten se toimii?
- Mikäli toteutus on mahdollista, kuinka se tapahtuisi tai mitä lisätutkimusta käyttöönotto vaatisi?

2 Tutkimusmenetelmä

Työssä käytetään kvalitatiivista, eli laadullista tutkimusotetta. Tavoitteena oli tutkia ja ymmärtää tiettyä ilmiötä ja johtaa sen perusteella jatkoehdotuksia, tässä tapauksessa selvittää mitä CSfC on ja kuinka sitä voisi toteuttaa Suomessa. Tämän tyyppiseen selvitystyöhön laadullinen tutkimus on hyvä valinta.

Hanna Vilkka (2021, 121) toteaa teoksessaan Tutki ja Kehitä, että laadullisessa tutkimuksessa ei ole niinkään oleellista, että saadaan kasaan mahdollisimman laajalti tutkimusaineistoa. Tärkeämpää on, että tutkimusaineisto on mielekästä ja palvelee tutkimuksen tarkoitusta. Tästä näkökulmasta laadullinen tutkimus on myös sovelias valinta.

Tutkimusmenetelmäksi valikoitui soveltava tutkimus. Tämän tutkimusmenetelmän painopisteenä on ratkaisun löytäminen johonkin, erityisesti työelämän, olemassa olevaan käytännön ongelmaan. Tämän saavuttamiseksi käytetään usein jo olevan tiedon soveltamista (Kunnela, Latvala & Tuomi).

Soveltava tutkimusmenetelmä vastaa juuri siihen tarpeeseen, mihin opinnäyte pyrkii vastaamaan. Suomenkin valtion on pysyttävä tietotekniikan ja erityisesti tietoturvan kehityksen mukana. Erityisen tärkeää tämä on, kun kehitettävänä kohteena on valtion ylläpitämät turvallisuusluokitellut verkkoympäristöt. Tämän opinnäytteen tavoitteena on tutustua yhteen tapaan luoda tietoturvallisia turvallisuusluokiteltuja verkkoympäristöjä ja pohtia, onko tämä sovellettavissa Suomeen.

3 Ohjelman kuvaus

3.1 Yleiskuvaus

CSfC-ohjelma on lähtenyt liikkeelle Yhdysvaltain valtionhallinnon eri organisaatioiden tarpeesta saada käyttöön tuoreimpia kaupallisia tietoteknisiä tuotteita. Koska näiden tuotteiden on tarjottava myös riittävä suojaus valtion arkaluontoisimmillekin tiedoille, on Yhdysvaltain kansallisesta turvallisuudesta vastaava virasto NSA halunnut tarjota tähän ratkaisun. (Commercial Solutions for Classified (CSfC))

Aiempaa tutkimusta aiheesta ei ole julkisesti saatavilla. CSfC-ohjelma on sen verran tarkasti sidoksissa Yhdysvaltoihin, että sitä ei ole yleensä ottaen juuri käsitelty Yhdysvaltojen ulkopuolella. Tämän lisäksi aihetta on melko hankala käsitellä julkisesti, koska tutkimuksessa kohteena on salaiseksi luokiteltua materiaalia.

3.2 Kryptografinen perusta

CSfC-ohjelman teknisiä vaatimuksia on kehitetty pohjana oletus, että kvanttitietokoneet tulevat olemaan yhä tärkeämmässä roolissa tietoteknisten suojausten murtamisessa. Tämän johdosta NSA on halunnut korostaa erityisesti elliptisten käyrien käyttöä. Tätä varten NSA on ottanut CSfC-ohjelman kryptografiseksi perustaksi Yhdysvaltain kansallisen standardointiorganisaation NIST:n standardeja sisältävän kryptografisten algoritmien kokoelman CNSA suite B:n. (Commercial National Security Algorithm (CNSA) Suite)

3.3 Ominaisuuspaketti

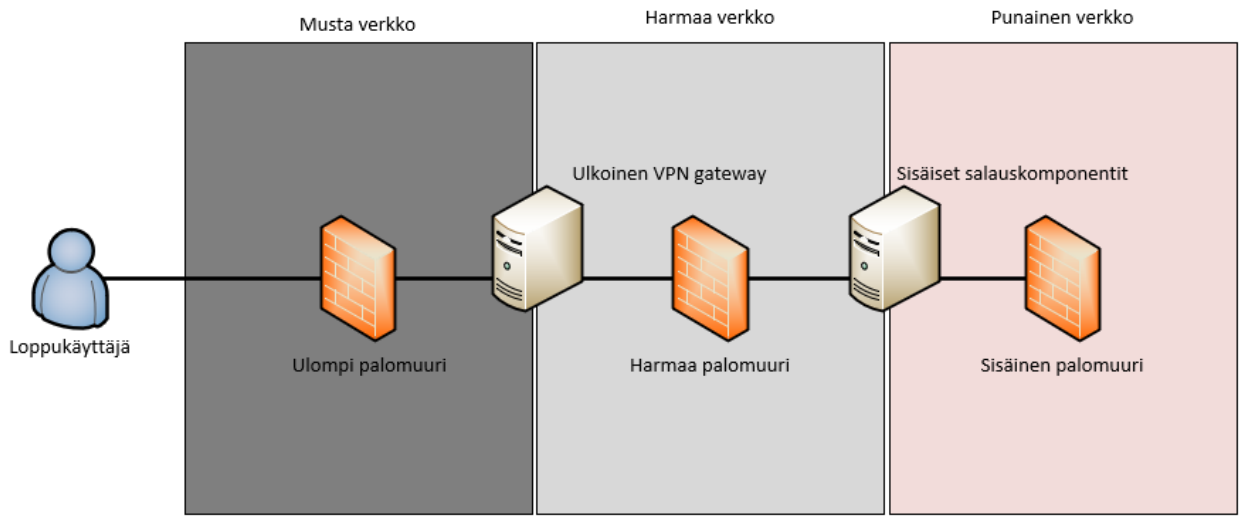
CSfC:n oleellisena osana ovat niin kutsutut ominaisuuspaketit eli Capability Packaget, CP:t. Jokainen ominaisuuspaketti keskittyy yhteen osaan tietoverkossa. ominaisuuspaketit eivät ota kantaa käytettäviin tekniikoihin tai ole tuoteriippuvaisia. Sen sijaan ominaisuuspaketit pyrkivät tarjoamaan selvityksen kuinka tietty osa tietoverkkoa toteutetaan modernien tietoturvavaatimusten mukaisesti. Ominaisuuspaketteja voikin verrata idealtaan esim. OSI-malliin.

Seuraavissa kappaleissa käydään läpi tämänhetkiset ominaisuuspaketit ja niiden keskeiset sisällöt. Tällä hetkellä ominaisuuspaketteja on tarjolla neljä kappaletta.

3.4 Etäyhteys ominaisuuspaketti

Ominaisuuspaketti etäyhteyden luomiseen eli Mobile Access CP tarjoaa yleisluontoisen ratkaisun, jonka avulla voidaan loppukäyttäjien mobiililaitteet yhdistää turvallisuusluokiteltuun verkkoon, sekä turvata turvallisuusluokiteltua dataa, jonka on kuljettava ei-luotetun verkon kautta, tai verkossa, joka sisältää useita eri turvallisuusluokiteltuja vyöhykkeitä. Tämä tapahtuu käyttäen kaksinkertaista tunnelointia. Ulompi tunneli toteutetaan IPsec:n avulla ja sisempi tunneli voidaan toteuttaa joko IPsec:n tai vaihtoehtoisesti TLS:n avulla. (Mobile Access Capability Package V2.1. 2018, 10)

Kuviossa 1 on kuvattuna yksinkertaisesti tunneloinnin periaate ja niiden terminointipisteet. Kuviossa esiintyvät väriluokitellut alueet kuvaavat verkkoja, joiden läpi liikenne tunneloidaan. Alueiden välisillä rajoilla ovat tunneleiden terminointipisteet. Seuraavissa kappaleissa kuvataan tarkemmin alueet.



Kuvio 1 Etäyhteyden luomisen periaate

3.4.1 Musta verkko

Musta verkko on uloin ja turvattomin vyöhyke mobiilidatan kuljetuksessa loppukäyttäjän laitteen ja turvallisuusluokitellun verkon välillä. Sekä ulompi, että sisempi tunneli kulkee mustan verkon kautta. (Mobile Access Capability Package V2.1. 2018, 14)

Uloimman tunnelin muodostamiseen etäyhteys ominaisuuspaketti hyväksyy joko erillisen VPN-sovelluksen tai Government-owned Retransmission Devicen (RD). RD on tässä tapauksessa erillinen laite, joka voi toimia sekä Wi-Fi tukiasemana, että mobiilireititttimenä. Loppukäyttäjä yhdistää oman laitteensa RD:hen joko ethernetillä tai langattomasti. Wi-Fiä käytettäessä vaatimuksena on WPA2-salaus. RD puolestaan muodostaa VPN-tunnelin julkisen verkon kautta. (Mobile Access Capability Package V2.1. 2018, 14)

Edellä mainituista vaatimuksista voidaan poiketa, mikäli käytettävissä on valtion itsenäisesti ylläpitämä matkapuhelinverkko tai langaton verkko (Mobile Access Capability Package V2.1. 2018, 14).

3.4.2 Harmaa verkko

Harmaa verkko on turvallisuusluokitellun verkon ulompi vyöhyke, joka sisältää ulomman salauslaitteen, sekä Harmaan palomuurin. Harmaa verkko päättyy kuviossa 1 esiintyvän Harmaan palomuurin jälkeiseen sisempään salauslaitteeseen, jossa sisempi tunneli puretaan.

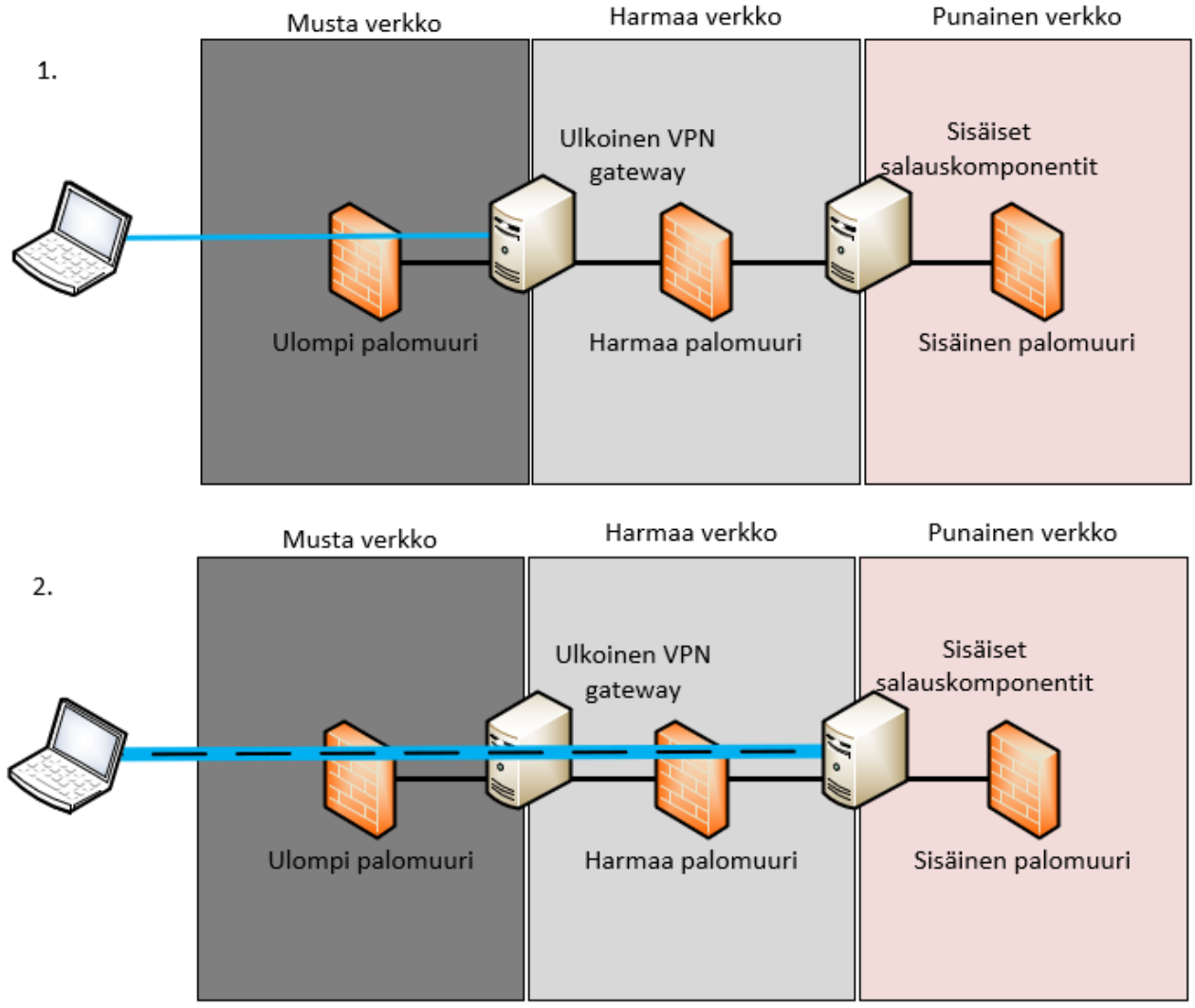
Harmaalle verkolle sijoittuvat Harmaan palomuurin lisäksi myös SIEM sekä IDS- ja IPS-järjestelmät. Lisäksi tänne voidaan sijoittaa tälle alueelle rajoittuvat varmennepalvelut (CA, CRL, CDP). Mikäli harmaan verkon tarpeisiin halutaan käyttää omaa juurivarmennepalvelua, täytyy harmaalle verkolle luoda oma juuri-CA:n alainen CA.

3.4.3 Punainen verkko

Punainen verkko on sisäinen, turvallisuusluokiteltu verkko, jossa data kulkee salaamattomana. Punainen verkko alkaa kuvion 1 mukaisesti sisemmän salauslaitteen sisärajapinnalta, josta puretun sisäisen tunnelin liikenne lähtee salaamattomana kohti sisäistä palomuuria.

3.4.4 Etäyhteys ominaisuuspaketin toiminta

Kaikki punaisesta verkosta ei-luotetun verkon yli, kohti loppukäyttäjää, kulkeva liikenne salataan kahdesti, kuvion 2 mukaisesti. Ensin Sisäisellä salauslaitteella, joka muodostaa sisemmän tunnelin ja sen jälkeen ulkoisella VPN-yhdyskäytävällä, jossa muodostetaan ulompi tunneli. (Mobile Access Capability Package V2.1. 2018, 16)



Kuvio 2 salatun yhteyden muodostus

Etäyhteys ominaisuuspaketti hyväksyy kaksi erilaista tapaa luoda suojattu yhteys loppukäyttäjän laitteen ja punaisen verkon välille. Nämä ovat VPN EUD ja TLS EUD. VPN EUD käyttää kahta IPsec-kerrosta suojatun VPN-yhteyden muodostamiseen. Sisempi IPsec muodostetaan laitteessa olevalla IPsec:iä käyttävällä VPN-sovelluksella ja ulomman muodostamiseen voidaan käyttää toista IPsec VPN-sovellusta tai erillistä VPN-laitetta. TLS EUD-laitteessa sisempi VPN muodostetaan TLS:n avulla ja ulompi VPN muodostetaan, kuten VPN EUD:n tapauksessa, VPN-sovelluksella tai erillisellä VPN-laitteella. Huomionarvoista on, että mikäli käytetään erillistä VPN-laitetta, loppukäyttäjän laitteen ja VPN-laitteen väliseen yhteyteen on käytettävä joko kiinteää liityntää tai langattomasti WPA2-salauksella. Huomioitavaa on myös EUD:n fyysinen turvallisuus. Laitetta on käytettävä niin, ettei ulkopuolinen taho pääse vahingossa tai tarkoituksella laitteeseen käsiksi. (Mobile Access Capability Package V2.1. 2018, 16)

Etäyhteys ominaisuuspaketin liikenne jaetaan käyttötarkoituksen mukaan kolmeen kategoriaan: data, management ja control plane. Data plane-liikenne on varsinaista käyttäjän ja järjestelmien tuottamaa dataa, joka on turvallisuusluokiteltua. Tällaista on esimerkiksi sähköpostiliikenne. Management planen liikenne on etäyhteys ominaisuuspaketin komponentteihin liittyvää hallinta- ja valvontaliikennettä. Esimerkiksi SIEM-järjestelmään lähetettävät lokit, tai palvelimen hallinta on tällaista liikennettä. Control plane-liikenteeseen kuuluu kaikki toiminnan kannalta välttämättömien protokollien liikenne, kuten DNS-kyselyt, NTP tai reititystiedot. (Mobile Access Capability Package V2.1. 2018, 17)

Etäyhteys ominaisuuspaketti vaatii, että data plane- ja management plane-liikenne erotetaan toisistaan joko fyysisesti omiin yhteyksiin tai loogisesti eri toteutuksiin salauksesta. Pelkkä VLANien käyttö erottamaan data ja hallinta, ei riitä. Vastaavasti control planen liikenne saa kulkea salaamattomana ainoastaan VPN-yhteyden muodostamiseen välttämättömin osin. Muutoin control planen liikennettä ei tarvitse erotella kuten datan ja hallinnan tapauksessa. (Mobile Access Capability Package V2.1. 2018, 17)

3.4.5 Etäyhteys ominaisuuspaketin komponentit

Ulompi palomuuri on uloin komponentti ja se on yhteydessä mustaan verkkoon. Ulomman palomuurin, kohti mustaa verkkoa oleva, ulkorajapinta päästää eteenpäin ainoastaan ulkoiselle VPN-yhdyskäytävälle suuntaavan, VPN-yhteyden muodostamiseen välttämättömän liikenteen. Sisärajapinta puolestaan päästää läpi ainoastaan ulkoiselta VPN-yhdyskäytävältä tulevan IPsec-liikenteen, sekä välttämättömän control plane-liikenteen. Ulomman palomuurin on lisäksi oltava fyysisesti ulkoisesta VPN-yhdyskäytävästä erillään oleva laite. Virtualisointia samalla alustalla ei täten sallita. (Mobile Access Capability Package V2.1. 2018, 27)

Ulkoinen VPN-yhdyskäytävä on laite, jossa EUD:t muodostavat ulomman VPN-yhteyden. Ulkoinen VPN-yhdyskäytävä ei saa reitittää liikennettä harmaan ja mustan verkon välillä, vaan liikenteen on aina kuljettava VPN-tunneleissa. Ulkoinen VPN-yhdyskäytävä ei myöskään saa osallistua reititysprotokollien toteutukseen. (Mobile Access Capability Package V2.1. 2018, 28)

Harmaan palomuuri sijaitsee ulkoisen VPN-yhdyskäytävän ja sisäisen salauslaitteen välillä. Harmaan palomuurin ulkorajapinta laskee läpi ainoastaan liikennettä, jonka lähteenä on joku ulkoisen

VPN-yhdyskäytävän EUD:ille varaama IP. Sisärajapinta puolestaan hyväksyy vain sisäiseltä salauslaitteelta tulevan liikenteen. Kuten aiemmatkin komponentit, harmaan palomuurin on oltava fyysisesti erillinen laite. (Mobile Access Capability Package V2.1. 2018, 28)

Sisäinen palomuuri sijaitsee sisäisen salauslaitteen ja punaisen verkon välillä. Sisäisen palomuurin ulkorajapinta hyväksyy vain sisäiseltä salauslaitteelta tulevan liikenteen ja sisäinen rajapinta puolestaan päästää läpi vain kohti sisäistä salauslaitetta suuntaavan liikenteen. (Mobile Access Capability Package V2.1. 2018, 29)

Sisäisen salauskomponentin toteutus riippuu, käytetäänkö sisemmässä VPN-tunnelissa IPsec- vai TLS-salausta. Kummassakin tapauksessa tässä kohdassa muodostetaan sisempi VPN-tunneli joko sisemmän VPN-yhdyskäytävän tai TLS-palvelimen kanssa. Sisäinen salauskomponentti on ulkoisesta rajapinnastaan yhteydessä harmaaseen palomuurin ja sisäisestä rajapinnastaan sisäisessä palomuurissa. Taulukkoon 1 on listattu komponenteille ja muodostettaville VPN-yhteyksille asetetut minimivaatimukset (Mobile Access Capability Package V2.1. 2018, 55).

Taulukko 1 Etäkäyttö ominaisuuspaketin kryptografiset minimivaatimukset

kryptografinen osa	**minimivaatimus**
salaus	AES-256
digitaalinen allekirjoitus	RSA 3072 ECDSA over the curve P-384 with SHA-384
avaintenvaihto	ECDH over the curve P-384 (DH Group 20) Diffie-Hellman 3072
tarkistussumma	SHA-384
TLS Cipher Suite (mikäli käytössä TLS EUD)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

3.5 Kampus WLAN ominaisuuspaketti

Kampus WLAN ominaisuuspaketti kuvaa, kuinka turvallisuusluokitellussa ympäristössä voidaan luoda tietoturvallinen langaton verkko. Tämän saavuttamiseksi käytetään kaksikerroksista salausta. Ensimmäisessä vaiheessa laitteet muodostavat yhteyden langattomaan liityntäpisteeseen WPA2:n avulla, käyttäen vähintään AES-128 salausta. Toisen kerroksen muodostaa IPsec-tunneli AES-256 salauksella. (Wireless Local Area Network Capability Package V2.2 2018, 3)

Kampus WLAN ominaisuuspaketti sisältää samat ympäristöt kuin etäyhteys ominaisuuspaketti. Nämä ovat musta verkko, harmaa verkko ja punainen verkko. Punainen verkko on turvallisuusluokiteltu ympäristö, jossa liikenne kulkee salaamattomana. Kampus WLAN ominaisuuspaketin tarkoitus on kuvata turvallinen tapa päästä käsiksi punaiseen verkkoon ei-luotetun, mustan verkon, yli. (Wireless Local Area Network Capability Package V2.2 2018, 4)

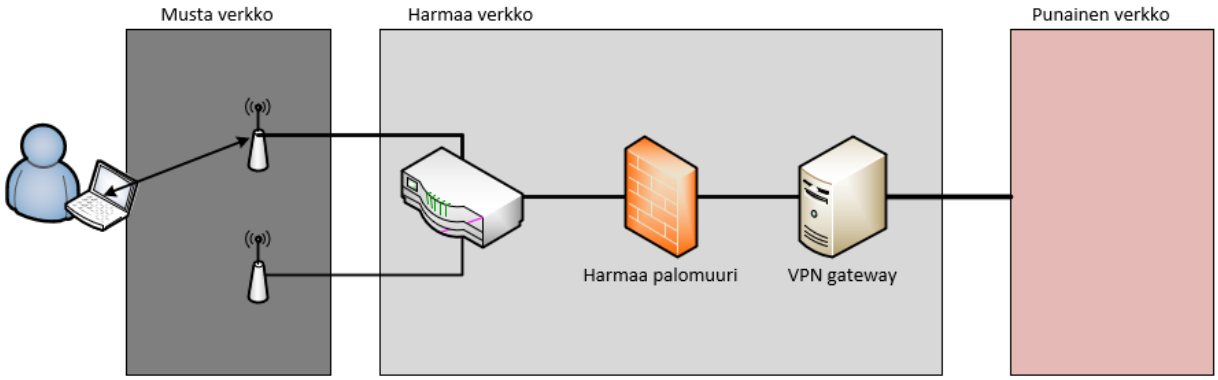
Harmaa verkko on turvallisuusluokiteltua punaista verkkoa hallinnoivan organisaation ylläpitämä ympäristö, jonka lävitse kulkeva liikenne on kertaalleen salattua. Huomionarvoista on, että tämä koskee myös fyysisten laitteiden lisäksi tietoliikenteen siirtoteitä, kuten kupari- ja kuituyhteyksiä. Harmaan verkon kautta salattu liikenne päästetään punaiseen verkkoon. Harmaa verkko voidaan vielä jakaa kahteen aliverkkoon, jotka ovat hallinta- ja dataverkot. Harmaassa hallintaverkossa kulkeva liikenne on tarkoitettu kohti punaista verkkoa kulkevan liikenteen salaukseen tarvittavien komponenttien hallinnointiin. Lisäksi tähän kuuluvat valvonta- ja auditointijärjestelmien, kuten IDS/IPS ja SIEM:n liikenne. Harmaa dataverkko käsittää varsinaiset VPN-tunnelit, kohti punaista verkkoa. (Wireless Local Area Network Capability Package V2.2 2018, 5)

Musta verkko on ympäristö, jonka kautta loppukäyttäjän laite ottaa yhteyttä harmaaseen verkkoon IPsec VPN-tunnelin muodostamiseksi. Tunnelin muodostamisen jälkeen varsinainen dataliikenne on täten kahdesti salattua, ensin WLAN-tukiasemaan WPA2-salauksella ja lopulta IPsec VPN-tunnelissa. Vaikka sekä loppukäyttäjän laitteet, että WLAN-tukiasemat ovat turvallisuusluokitellun ympäristön omistavan organisaation hallinnassa, kulkee liikenne kuitenkin langattomasti loppukäyttäjän laitteelta WLAN-tukiasemaan. Tätä väliä ei voida pitää luotettavana, joten se luokitellaan mustaksi verkoksi, vaikka onkin laajuudeltaan huomattavasti pienempi kuin kappaleessa etäyhteys ominaisuuspaketti, kuvattu musta verkko. (Wireless Local Area Network Capability Package V2.2 2018, 5)

edellä mainittujen verkkojen lisäksi Kampus WLAN ominaisuuspaketti sisältää samat liikenteen luokittelut kuin etäyhteys ominaisuuspaketti, jotka ovat data plane, management plane ja control plane. Näiden tarkoitus on sama, joten niitä ei käydä läpi uudelleen.

3.5.1 Kampus WLAN ominaisuuspaketin toiminta

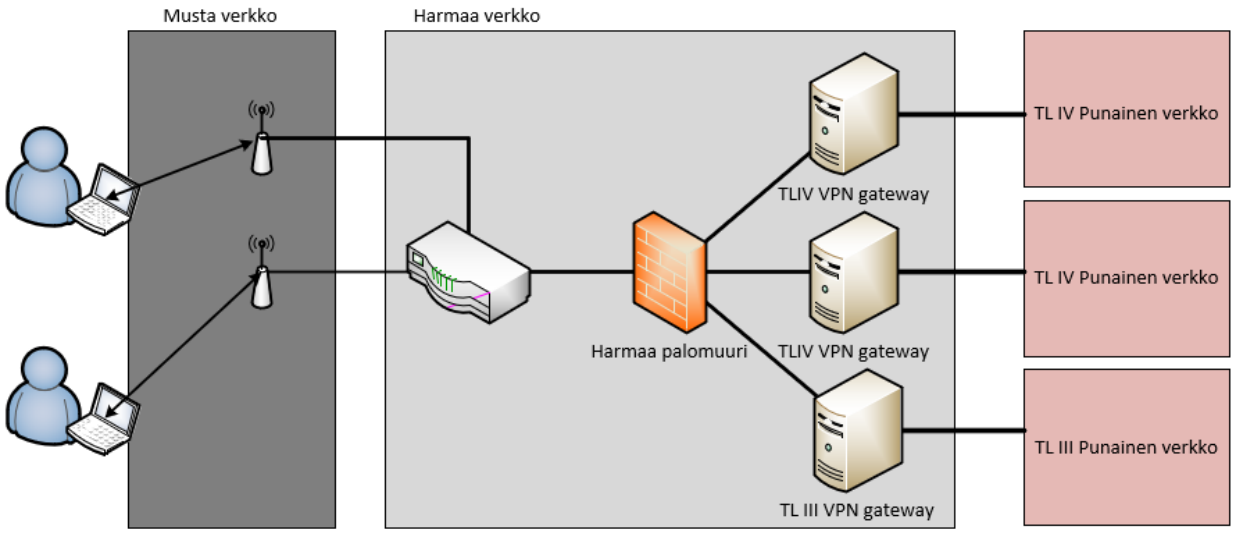
Kampus WLAN ominaisuuspaketin yleisidea on kuvattu kuviossa 3. Loppukäyttäjän laite, EUD, muodostaa yhteyden mustassa verkossa olevaan tukiasemaan WPA2-protokollalla. Tämän jälkeen EUD:ssä oleva VPN-sovellus ottaa tukiaseman kautta yhteyden harmaassa verkossa olevaan VPN-yhdyskäytävään. Mikäli EUD tunnistaa itsensä VPN yhdyskäytävällä onnistuneesti, muodostetaan IPsec VPN-tunneli EUD:n ja VPN yhdyskäytävän välillä. Tämän jälkeen EUD voi liikennöidä punaiseen verkkoon ja kaikki liikenne EUD:n ja punaisen verkon välillä kulkee salatussa IPsec VPN-tunnelissa.



Kuvio 3 Kampus WLAN ominaisuuspaketin yleiskuvaus

Kampus WLAN ominaisuuspaketti tukee myös toteutusta, jossa saman mustan / harmaan verkon kautta on pääsy useampaan eri punaiseen verkkoon. Nämä verkot voivat kuulua saman tai eri turvallisuusluokituksen alle, tai yhdistelmään edellisistä. Kuten kuviosta 4 nähdään, tällaisessa toteutuksessa jokaiseen punaiseen verkkoon pääsyn edellytyksenä on oma VPN-yhdyskäytävä. Nämä VPN-yhdyskäytävät ovat fyysisesti ja loogisesti erotettuja toisistaan, eivätkä ne saa esim. luottaa toistensa varmenteisiin. Näin voidaan ehkäistä tilanteet, joissa loppukäyttäjä yrittää tahallisesti tai

tahattomasti yhteyttä väärään punaiseen verkkoon. (Wireless Local Area Network Capability Package V2.2 2018, 7)



Kuvio 4 Usean punaisen verkon Kampus WLAN toteutus

3.5.2 Kampus WLAN ominaisuuspaketin komponentit

Loppukäyttäjän laite, eli EUD on turvallisuusluokitellun ympäristön omistavan organisaation hallinnoima laite, jolla loppukäyttäjä pääsee punaisen verkon resursseihin kiinni. Tämä voi olla mikä tahansa WLAN-yhteyteen kykenevä laite kuten matkapuhelin tai kannettava tietokone. EUD:n on kyettävä muodostamaan WPA2-protokollaa käyttäen yhteys WLAN-tukiasemaan. WLAN-adapterin lisäksi, EUD:ltä vaaditaan erillinen VPN-sovellus, joka muodostaa IPsec-tunnelin VPN-yhdyskäytävän kanssa. (Wireless Local Area Network Capability Package V2.2 2018, 9)

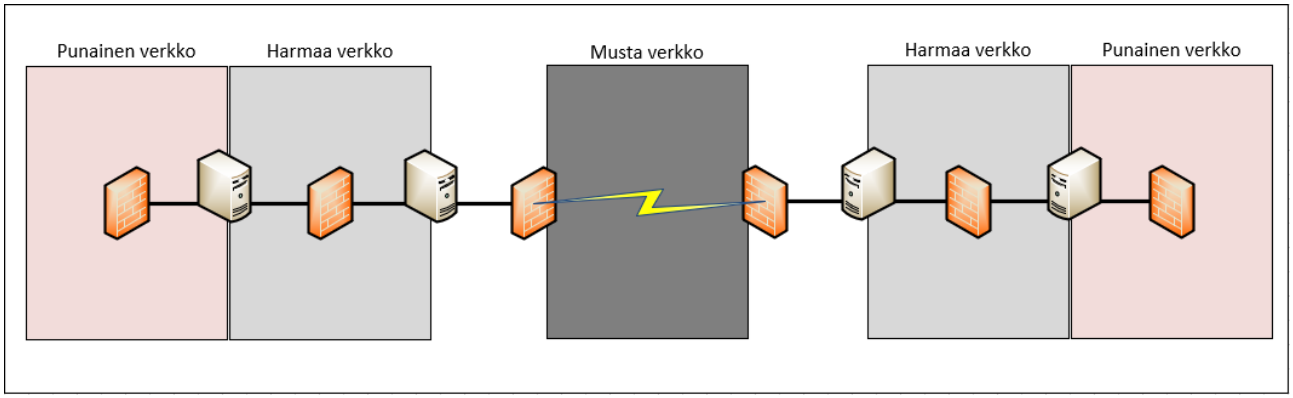
WLAN-tukiasemat, eli AP:t ja näiden hallintalaitteet toimivat liityntäpisteenä EUD:lle, kohti punaista verkkoa. Kampus WLAN ominaisuuspaketti hyväksyy toteutukset, joissa WPA2-yhteys muodostetaan joko AP:lle suoraan tai AP-hallintajärjestelmään. Mikäli AP:t toimivat vain linkkinä hallintajärjestelmään, lasketaan AP:t osaksi harmaata verkkoa. Mikäli WPA2-yhteys muodostetaan suoraan tukiasemaan, kuuluvat AP:t mustaan verkkoon ja tällöin on varmistettava, että ulkopuolisen tahon pääsy esim. tukiaseman konsoliporttiin on fyysisesti tai loogisesti estetty. (Wireless Local Area Network Capability Package V2.2 2018, 12)

WLAN-tukiasemien ja hallintajärjestelmän osana on lisäksi erillinen autentikointipalvelin. Tämän tehtävänä on varmistaa, että tukiasemiin voivat muodostaa yhteyden vain hyväksytyt laitteet. Varmentaminen tapahtuu IEEE 802.1X-pohjaisilla laitevarmenteilla. (Wireless Local Area Network Capability Package V2.2 2018, 13)

Harmaa palomuuri suodattaa liikennettä kohti VPN-yhdyskäytävää. Sen tehtävänä on varmistaa, että vain hyväksytty liikenne WLAN-tukiasemilta ja hallintajärjestelmältä päästetään eteenpäin ja ainoastaan kohti VPN-yhdyskäytävää. Mikäli käytössä on useampi punainen verkko ja samalla useampi VPN-yhdyskäytävä, harmaan palomuurin tehtäviin kuuluu myös varmistaa, että EUD:t eivät pääse väärälle VPN-yhdyskäytävälle. (Wireless Local Area Network Capability Package V2.2 2018, 13)

3.6 Moni-toimipiste ominaisuuspaketti

Monitoimipiste, eli Multi-Site Connectivity (MSC) ominaisuuspaketti tarjoaa ratkaisun yhdistää, kuvion 5 mukaisesti, kaksi tai useamman maantieteellisesti tai loogisesti eri paikoissa sijaitsevaa saman turvallisuusluokituksen verkkoa toisiinsa tietoturvallisesti. Yhdistettävät verkot voivat käyttää siirtoväylänään ei-luotettua, tai luotettua mutta eri turvallisuusluokituksen omaavaa verkkoa. Tämä toteutetaan, kuten etäyhteys ominaisuuspaketin tapauksessa kahdella sisäkkäisellä VPN-tunnelilla. Nämä tunnelit voidaan toteuttaa joko IPsec- tai MACsec-menetelmillä. (Multi-Site Connectivity Capability Package V.1.1.8 2021, 7)



Kuvio 5 Moni-toimipiste ominaisuuspaketin toimintaperiaate

3.6.1 Moni-toimipiste ominaisuuspaketin verkot

Punainen verkko on kaksi tai useampi turvallisuusluokiteltu ympäristö, joiden välille luodaan turvallinen kahdesti suojattu VPN-yhteys. (Multi-Site Connectivity Capability Package V.1.1.8 2021, 8)

Harmaa verkko, kuten punainenkin on turvallisuusluokitellun ympäristön omistavan organisaation täysin hallitsema ympäristö. Erona punaiseen verkkoon on, että harmaassa verkossa kulkee pelkästään salattua dataa, tai salauksen muodostamiseen tarvittavaa dataa. Täällä sijaitsevat ulomman VPN-tunnelin muodostamiseen käytettävät VPN-yhdyskäytävät, liikenteen suodattamiseen välttämätön harmaa palomuuri, sekä tietoturvallisen toimintaympäristön kannalta oleelliset taustapalvelut, kuten varmennepalvelut ja hallinta- ja valvontapalvelut. (Multi-Site Connectivity Capability Package V.1.1.8 2021, 9)

Kuten harmaassa verkossa, myös mustassa verkossa kulkeva data on salattua tai salauksen muodostavaa. Erona punaiseen ja harmaaseen verkkoon on, että musta verkko on joko täysin tai osittain turvallisuusluokitellun ympäristön omistavan organisaation hallinnan ulkopuolella. Mikäli musta verkko on täysin kolmannen osapuolen hallinnoima, kulkee kaikki liikenne mustassa verkossa, punaisten verkkojen välillä, harmaan verkon viimeiseksi komponentiksi sijoitettavan ulkoisten palomuurien kautta. (Multi-Site Connectivity Capability Package V.1.1.8 2021, 9)

edellä mainittujen verkkojen lisäksi moni-toimipiste ominaisuuspaketti sisältää samat liikenteen luokittelut kuin etäyhteys ominaisuuspaketti ja Kampus WLAN ominaisuuspaketti. Nämä luokittelut ovat data plane, management plane ja control plane. Näiden tarkoitus on sama, joten niitä ei käydä läpi uudelleen.

3.6.2 Moni-toimipiste ominaisuuspaketin komponentit

Mikäli turvallisuusluokiteltujen verkkojen välinen yhteys luodaan mustan verkon kautta, on viimeiseksi komponentiksi ennen mustaa verkkoa sijoitettava ulkoinen palomuuri. Tämä palomuuri päästää läpi toiminnan kannalta välttämättömän control plane-liikenteen lisäksi ainoastaan IPsec- tai MACsec-liikennettä, jonka kohteena tai lähteenä on ulkoinen salauskomponentti.

Ulkoinen salauskomponentti voi olla joko IPsec VPN-yhdyskäytävä tai MACsec-laite. Riippuen valitusta vaihtoehdosta, ulkoisen salauskomponentin kanssa luodaan ulkoinen VPN-tunneli. Mikäli käytössä on useampi saman turvallisuusluokituksen punainen verkko, on ulkoisella salauskomponentilla myös vastuulla liikenteen suodatus, joka estää punaisia verkkoja keskustelemasta keskenään. Ulkoisen salauskomponentin on lisäksi oltava fyysisesti erillisellä laitteella kuin ulkoinen ja harmaa palomuuri.

Harmaan palomuuri sijaitsee sisäisen ja ulkoisen salauskomponentin välillä. Sen tärkein tehtävä on suodattaa liikennettä ja estää liikenne eri turvallisuusluokituksen omaavien sisäisten salauskomponenttien välillä. Mikäli käytössä on vain yhden turvallisuusluokituksen sisäisiä salauskomponentteja, harmaa palomuuri ei ole pakollinen komponentti. Mikäli harmaata palomuuria käytetään, on sen oltava fyysisesti erillisellä laitteella kuin ulkoinen ja sisäinen salauskomponentti.

Sisäinen salauskomponentti voi olla, kuten ulkoinenkin, joko IPsec VPN-yhdyskäytävä tai MACsec-laite. Sen tehtävänä on muodostaa sisempi VPN-tunneli saman turvallisuusluokituksen omaavien punaisten verkkojen välillä. Sisäinen salauskomponentti ei saa reitittää suoraan liikennettä harmaan ja punaisen verkon välillä, vaan kaiken liikenteen on kuljettava VPN-tunneleissa. Kuten muutkin komponentit, myös sisäisen salauskomponentin on oltava fyysisesti omalla laitteellaan.

3.6.3 Moni-toimipiste ominaisuuspaketin toiminta

Kuten mustan verkon kohdalla todettiin, ulkoinen palomuuri on pakollinen komponentti, mikäli musta verkko on täysin kolmannen osapuolen hallinnoima. Ulkoisen palomuurin ulkorajapinta on kohti mustaa verkkoa ja sisärajapinta harmaassa verkossa. Ulkorajapinta päästää läpi vain IPsec- tai MACsec-salattua liikennettä kohti ulompaa salauskomponenttia. Sisärajapinta puolestaan sallii vain IPsec- tai MACsec-salatun liikenteen, jonka lähde on ulompi salauskomponentti. Huomionarvoista on, että ulkoisen palomuurin on oltava fyysisesti erillinen laite tai virtualisoituna erillisellä laitteella, kuin ulompi salauskomponentti. (Multi-Site Connectivity Capability Package V.1.1.8 2021, 21)

3.7 Data levossa ominaisuuspaketti

Data levossa, eli Data at Rest (DAR) ominaisuuspaketti tähtää CSfC:n oleellisena osana olevan loppukäyttäjän laitteen, eli EUD:n suojaamiseen silloin kun laite on sammutettuna tai kun siihen ei ole kirjautuneena ketään. Data levossa ominaisuuspaketti toteuttaa tämän vaatimalla kaksikerroksisen salauksen suojattavalle tiedolle. Yksikerroksinen salaus on sinällään riittävä turvaamaan turvallisuusluokiteltu tieto. Data levossa ominaisuuspaketin vaatimukselle kaksikerroksisesta salauksesta on pohjalla toisiaan varmistavat salaukset. Mikäli toinen kerroksista pettää vahingossa tai tahallisen toiminnan seurauksena, on toinen salauskerros edelleen suojaamassa turvallisuusluokiteltua tietoa.

Taulukkoon 2 on listattu data levossa ominaisuuspaketin asettamat minimivaatimukset kryptografisille komponenteille (Data at Rest Capability Package 2020, 11).

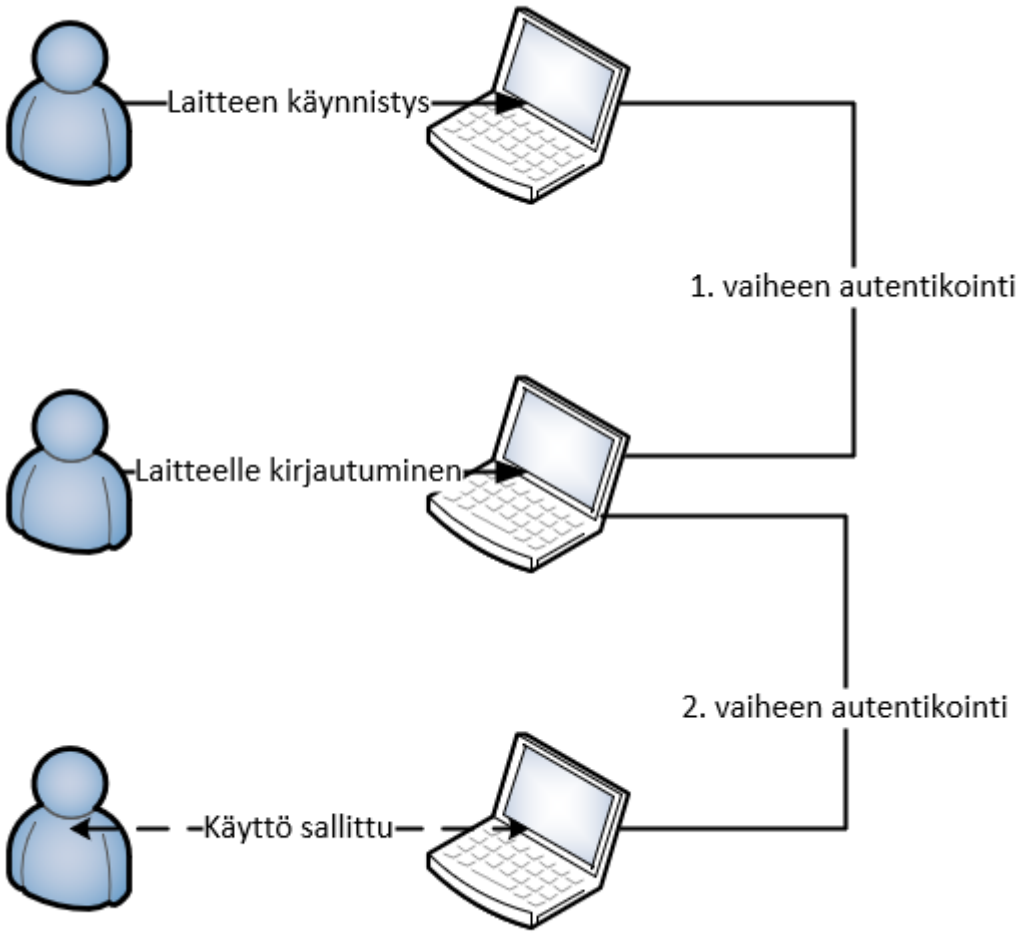
Taulukko 2 Data levossa ominaisuuspaketin kryptografiset vaatimukset

Kryptografinen komponentti	Minimivaatimus
Salaus	AES-256
Autentikointi (digitaalinen allekirjoitus)	Elliptic Curve Digital Signature Algorithm over the curve P-384 with SHA-384 RSA-3072
Tarkistussumma	SHA-384
Salaustaso	Nato Top Secret / Erittäin salainen

3.7.1 Data levossa ominaisuuspaketin toiminta

Kuviossa 6 on käyty läpi esimerkki Data levossa ominaisuuspaketin toiminnasta. Ensimmäisessä vaiheessa loppukäyttäjä käynnistää kannettavan tietokoneensa ja ulompana salauskerroksena toi-

miva sovelluspohjainen laitesalaus vaatii käyttäjää autentikoitumaan antamalla salasanan. Kun salasana on onnistuneesti syötetty sovelluspohjainen laitesalaus poistaa sisemmän salauksen ja antaa työaseman käyttöjärjestelmän hallintaan. Toisessa vaiheessa käyttäjä autentikoi itsensä sisemmän kerroksen salauksesta vastaavalle tiedostonsalaussovellukselle ja pääsee käyttämään kannettavaa tietokonettaan.



Kuvio 6 Data levossa ominaisuuspaketin autentikointiprosessi

Aikaisempien lukujen ominaisuuspaketit ovat käsitelleet luotettavan yhteyden luomista päätepisteiden välille. Tähän on käytetty erillisiä komponentteja, jotka ovat todentaneet osapuolet ja varmistaneet yhteyden luotettavuuden. Data levossa ominaisuuspaketin tapauksessa luotettavuus varmistetaan, sillä että laitteen käyttöä yrittävällä taholla on hallussaan aiemmin määritelty salaisuus, jolla salaus poistetaan ja laitteeseen annetaan pääsy. Tällaiset salaisuudet voivat olla esim.

salasana, PIN-koodi tai varmennekortti + PIN-koodi yhdistelmä. (Data at Rest Capability Package 2020, 12)

Loppukäyttäjien laitteet (EUD) ovat usein omistavan organisaation valvonnan ulkopuolisissa tiloissa ja data levossa ominaisuuspaketti pystyy antamaan puitteet vain laitteen sisältämän datan suojaamiseen. Tästä johtuen ottaa data levossa ominaisuuspaketti kantaa myös laitteen fyysiseen suojaamiseen. Vaatimuksena on, että EUD:n on oltava jatkuvasti loppukäyttäjän hallinnassa. Lisäksi EUD:n omistavan organisaation on laadittava suunnitelma ja ohjeistus siitä, missä tilanteissa hallinnan katsotaan lakanneen, eli EUD määritellään kadonneeksi. Mikäli EUD, joka on määritelty kadonneeksi, myöhemmin löydetään, on siihen kohdistettava myös asianmukainen tutkintaoperaatio sen selvittämiseksi, onko laitteeseen onnistuttu kajoamaan. Joissain tapauksissa EUD on myös hävitettävä tämän jälkeen asianmukaisesti. Data levossa ominaisuuspaketti vaatii, että EUD:n omistava organisaatio määrittelee ne raja-arvot, joiden ylityttyä EUD:n uudelleen käyttöönotto ei ole enää tietoturvallista. (Data at Rest Capability Package 2020, 14)

Aiempien lukujen kohdalla käytettiin paljon termejä punainen, harmaa ja musta verkko, kuvaamaan datan suojausastetta. Myös data levossa ominaisuuspaketti käyttää samaa väriluokitusta, mutta kuvaamaan kuinka vahvasti EUD:ssa oleva tieto on suojattua. Punainen data on suojaamatonta turvallisuusluokiteltua tietoa, johon päästään käsiksi, kun sisempi suojauskerros on purettu. Harmaa data on kertaalleen suojattua, ulommasta suojauskerroksesta purettua tietoa. Musta data puolestaan on kahteen kertaan salattua tietoa. EUD:lla oleva turvallisuusluokiteltu aineisto on mustassa datatilassa, kun käyttäjä ei ole vielä aloittanut autentikointiprosessia tai kun laite on virrattomassa tilassa. (Data at Rest Capability Package 2020, 14)

3.7.2 Data levossa ominaisuuspaketin komponentit

Data levossa ominaisuuspaketti hyväksyy käyttöön sovelluspohjaisen laitesalauksen (Software full disk encryption, SWFDE) toisena salauskerroksena. Sovelluspohjaisen laitesalauksen tehtävä on salata koko EUD:n käyttämä kiintolevy käyttöjärjestelmää myöten. Sovelluspohjainen laitesalaus sijoittuu käynnistysprosessin alkuun, ennen käyttöjärjestelmän latausta. Kun käyttäjä on onnistuneesti autentikoinut itsensä esim. salasanalla, poistaa sovelluspohjaisen laitesalauksen ja luovuttaa käynnistymisprosessin käyttöjärjestelmälle. (Data at Rest Capability Package 2020, 17)

Data levossa ominaisuuspaketti hyväksyy sisempään salaukseen tiedostojen salausohjelmien (File Encryption, FE) käytön. Tällaisten ohjelmien käytössä on huomioitava, että laitteessa käytettävät ohjelmat eivät kirjoita tietoa sellaisille alueille kiintolevyä, joita tiedostonsalaus ei suojaa. Mikäli käytetty tiedostonsalaussovellus ei pysty automaattisesti salaamaan lisämuistin käyttämiä alueita kiintolevyltä, on käyttöjärjestelmältä kiellettävä lisämuistin käyttö. Vastaavasti käyttöjärjestelmän ominaisuudet, joilla voidaan palauttaa tiedostoja, on estettävä, mikäli tiedostonsalaus ei pysty automaattisesti suojaamaan myös tällaisia palautettuja tiedostoja. Tiedostonsalauksen parina voidaan käyttää alustansalausta (Platform Encryptionia, PE). Tämä on paljolti tiedostonsalausta vastaava, käyttöjärjestelmän mukana tuleva, ulomman salauskerroksen toteuttava menetelmä. (Data at Rest Capability Package 2020, 19)

Kuten sovelluspohjaista laitesalausta, laitteistopohjaista levysalausta (Hardware Full Disk Encryption, HWFDE) voidaan käyttää ulompana tai sisempänä salauskerroksena. laitteistopohjainen levynsalaus salaa automaattisesti kaiken tiedon, joka levylle kirjoitetaan ja purkaa salauksen, kun sitä luetaan. Samoin kuin sovelluspohjaisen laitesalauksen tapauksessa, myös laitteistopohjainen levynsalaus vaatii autentikoinnin, esim. salasanan syöttämisen ennen kuin käyttäjä pääsee laitteelle. (Data at Rest Capability Package 2020, 21)

Taulukkoon 3 on listattu data levossa ominaisuuspaketin suosittelemat yhdistelmät salauskomponenteista (Data at Rest Capability Package 2020, 23). Kuten taulukosta voidaan nähdä, edellä kuvattuja menetelmiä voidaan yhdistellä varsin vapaasti ja silti saavuttaa riittävä turvallisuuden taso.

Taulukko 3 Data levossa ominaisuuspaketin salauskomponenttiyhdistelmät

Yhdistelmä
sovelluspohjainen laitesalaus: ulompi salaus tiedostonsalaus: sisempi salaus
alustan salaus: ulompi salaus tiedostonsalaus: sisempi salaus
laitteistopohjainen levynsalaus: ulompi salaus tiedostonsalaus: sisempi salaus
laitteistopohjainen levynsalaus: ulompi salaus sovelluspohjainen laitesalaus: sisempi salaus
laitteistopohjainen levynsalaus: ulompi salaus laitteistopohjainen levynsalaus: sisempi salaus

4 Toteutukset ja tarkastelu

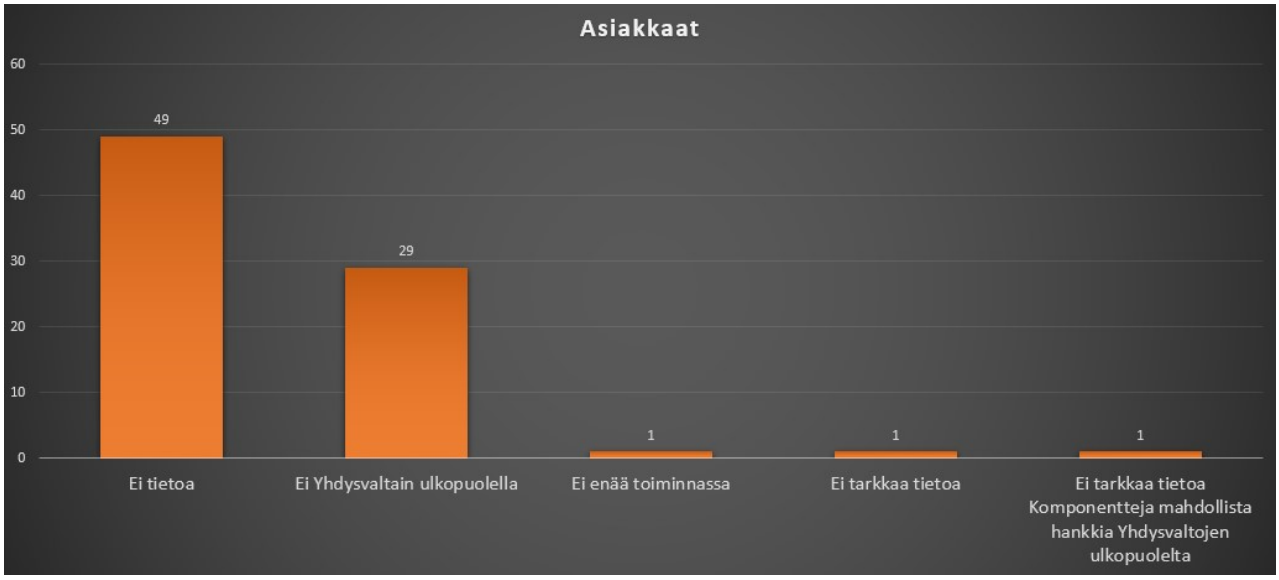
Kuten NSA itse toteaa, CSfC-ohjelma on kehitetty Yhdysvaltain viranomaistarpeisiin (Who are the typical CSfC clients?). Itse turvallisuuden suhteen tämä ei ole ongelma. CSfC:tä voidaan käyttää aina top secret-tasolle luokitelluissa verkoissa. Suomessa tämä vastaa ylintä, erittäin salainen, turvallisuusluokitusta (Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje 2016, 17).

Koska CSfC ei myöskään ole teknologia itsessään vaan kokoelma kriteerejä, joiden toteutus pohjautuu avoimiin standardeihin, ei sen käyttöönotto herätä huolta toisen valtion turvallisuusviranomaisen pääsystä turvallisuusluokiteltuun tietoon. CSfC:n käyttöönotossa suurin kysymys onkin sen saatavuudessa Yhdysvaltain ulkopuolella. CSfC-toteutuksia tarjoavat, NSA:n kumppaneiksi hyväksymät yritykset ovat Yhdysvaltalaisia, eivätkä välttämättä edes tarjoa tuotteitaan kuin Yhdysvaltain viranomaisille.

4.1 CSfC-toteutukset

Seuraavassa on käyty läpi CSfC-toteutuksia tarjoavat yritykset. Yritykset on valittu NSA:n yhteistyökumppaneiksi hyväksyttyjen CSfC-toteutusten tarjoajien listalta (Trusted Integrator List). Tarkempi katsaus yrityksiin löytyy liitteestä 1.

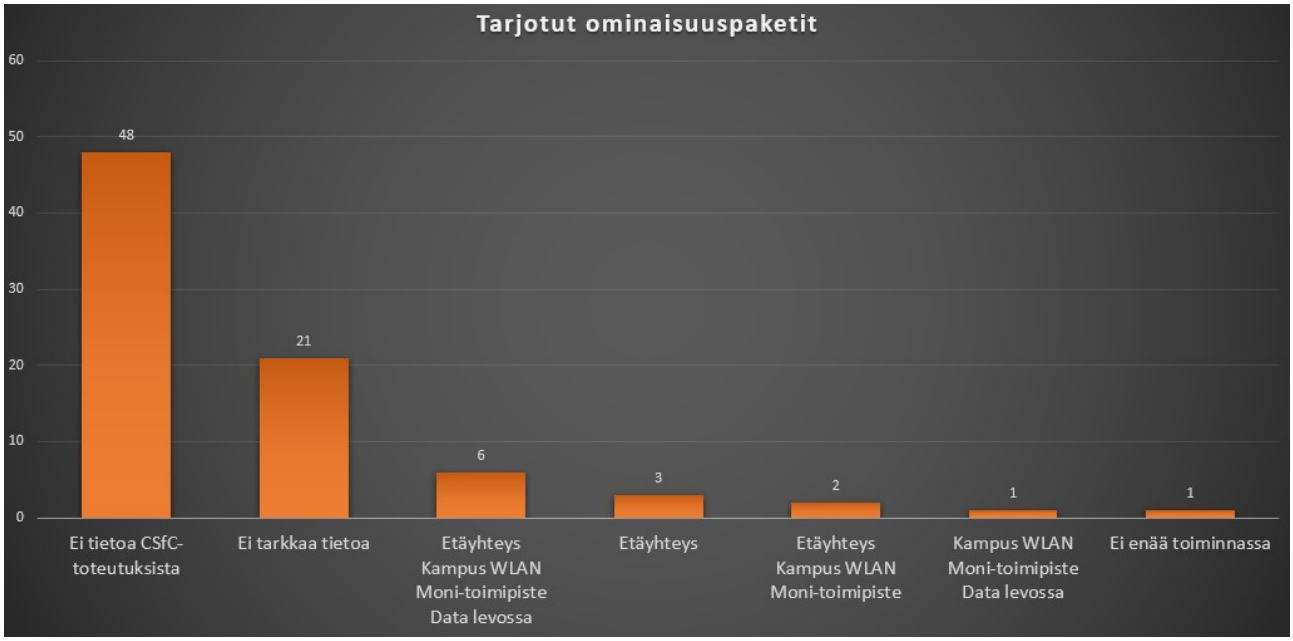
Kaiken kaikkiaan eri CSfC-toteutusten tarjoajia tarkastellessa huomaa, että jopa yksityisen sektorin toimijat ovat tarttuneet ideaan, että CSfC on tarkoitettu Yhdysvaltojen viranomaisille. Kuviosta 7 voidaan huomata, että 81:stä yhteistyökumppanista 29 tarjoaa CSfC-toteutuksia vain Yhdysvaltain viranomaisille ja vain yhdessä tapauksessa on olemassa selvästi jonkinlainen mahdollisuus hankkia CSfC-yhteensopivia komponentteja. Koska NSA pitää listaa CSfC-yhteensopivista komponenteista, on tämäkin tieto melko tarpeeton. Näitä komponentteja voidaan hankkia helposti muualtakin, mukaan lukien suoraan Suomesta.



Kuvio 7 CSfC-asiakkaat

Ylipäätään tietoa siitä, mitenkä yritykset toteuttavat CSfC:tä on vaikea löytää. 49 yritystä 81:stä ei ilmoita mitään asiakkaistaan tai ylipäätään olevansa NSA:n yhteistyökumppani. Täten sen varmistaminen tekevätkö nämä yritykset ylipäätään toteutuksia ominaisuuspaketeille, on vaikea varmistaa. Suurimpien yhteistyökumppaneiden, kuten Boeing tai IBM tapauksessa, asiakkaita on maailmanlaajuisesti, mutta CSfC-toteutusten kohdalla tietoa ei joko ole ollenkaan tai se on liian epäselvästi ilmoitettu, ollakseen hyödyllistä.

Kuten yhteistyökumppaneiden asiakkaiden tapauksessa, myös itse ominaisuuspaketeista on vaikeaa löytää tietoa. Kuviosta 8 voidaan huomata, että 48 NSA:n yhteistyökumppaneiksi ilmoittamaa yritystä 81:stä, ei ilmoita millään lailla olevansa NSA:n yhteistyökumppani. Tällöin myös tarjolla olevista ominaisuuspaketeista on vaikeaa löytää tietoa. 21 yritystä ilmoittaa olevansa mukana CSfC-ohjelmassa ja olevansa NSA:n yhteistyökumppani. Näissä tapauksissa yritykset ovat kuitenkin hyvin epämääräisiä siitä, mitä ominaisuuspaketteja he tarjoavat. Joissain tapauksissa ylipäätään tieto siitä tarjoavatko he ylipäätään mitään toteutuksia, on puutteellista.



Kuvio 8 Tarjotut ominaisuuspaketit

12:sta yrityksestä, joilta löytyy tieto tarjotuista ominaisuuspaketeista, 6 tarjoaa toteutuksen jokaiseen neljään ominaisuuspakettiin. Kolme yritystä tarjoaa toteutuksen kolmeen ominaisuuspakettiin ja kolme yritystä myy etäyhteys ominaisuuspaketille toteutuksen. Ilmeistä on, että etäyhteys ominaisuuspakettia pidetään tärkeänä, koska vain yhdeltä yritykseltä puuttuu toteutus sille.

Kuten kuviosta 8 nähdään, usealla toimittajalla on tarjolla toteutukset kaikkiin ominaisuuspaketteihin. Tällä voidaan päästä CSfC-ohjelman yhteen tavoitteista, eli helppouteen hankinnoissa, kun voidaan käyttää yhtä toimittajaa. Etuna tästä on, että voidaan todennäköisemmin välttää ongelmat, joita tavallisesti syntyy, kun käytetään useaa toimittajaa. Jokaisen komponentin on toimittava keskenään, mistä monesti ei ole takeita enne kuin ympäristö on pystyssä. Vianselvitys ja ylläpito voivat myös helpottua, kun toimittaja ymmärtää koko ympäristön toiminnan.

4.2 Tulosten tarkastelu

Yhden toimittajan käytössä on kuitenkin riskinsä, jotka olisi hyvä ottaa huomioon. Kun yksi toimittaja tarjoaa kaikki komponentit ympäristöön, joka voi olla hyvinkin laaja, on tilaajaorganisaatio vaarassa joutua liian riippuvaiseksi toimittajasta. Mikäli komponenteista löytyy vikoja tai häiriöitä,

voi näiden eristäminen olla hankalampaa, kuin jos käytettäisiin useampaa toimittajaa. Yhden toimittajan käytössä on lisäksi riskinä joutua riippuvaiseksi ko. toimittajasta. Ympäristön tai sen osien muuttaminen voi olla liian hankalaa, jotta tähän voidaan ryhtyä.

Mikäli CSfC-ohjelman ominaisuuspaketteja olisi joskus mahdollista hankkia Yhdysvaltain ulkopuolelta, toiminnan jatkuvuuden kannalta voisi olla turvallisempaa käyttää esim. eri toimittajia jokaiselle hankittavalle ominaisuuspaketille.

Eräs ongelma on, että CSfC ei varsinaisesti tarjoa mitään uutta. Ominaisuuspaketeissa esitellyt vaatimukset voidaan jo nykyisellään pitkälti toteuttaa Suomen turvallisuusluokitelluissa verkoissa. Erona on ainoastaan, että nykyiset ratkaisut ovat kokoelma eri palveluntarjoajien tuotteita. CSfC-ohjelman käyttöönoton tapauksessa olisi mahdollista saada käyttöön yksi toteutus. Tämä lisäisi verkkoympäristön toimintavarmuutta, kun toteutus on yhdeltä toimittajalta, ja monen toimittajan, eli multi-vendor ympäristön mukanaan tuomaa teknistä epävarmuutta pystytään minimoimaan.

Lisäetuna, erityisesti kyseen ollessa julkisen hankkijan, on toki myös mahdolliset kustannussäästöt. Useamman toimittajan verkkoympäristöissä, jokaisella toimittajalla on luonnollisesti omat katteensa mukana hinnassa. Näitä kustannuksia olisi mahdollista hallita helpommin yhdeltä toimittajalta hankituissa ratkaisuissa.

Yksi CSfC-ohjelman lähtökohdista on ollut kustannusten hallinta ottamalla käyttöön valmiita ratkaisuja täyttämään eri ominaisuuspakettien kuvaamat tarpeet. Tästä puolesta toteutusten tarjoajat eivät juuri mainitse mitään, lukuun ottamatta melko yleisellä tasolla olevia lupauksia helposta ja edullisesta käyttöönotosta. Jollakin palveluntarjoajalla olisi voinut olla esim. vertailu kustannuksista oman tuotteen ja muutoin tehdyn ominaisuuspaketin vaatimusten toteutuksen välillä. Tällöin olisi ollut helpompi nähdä, toteutuuko CSfC-ohjelman lupaus edullisuudesta.

Taulukkoon 4 on koottu yhteen edellä läpikäytyjä huomioita NSA:n CSfC-ohjelman eduista ja haitoista, sekä mahdollisista riskeistä. Näkökulmana yhteenvedossa on Suomen valtion hallinnassa olevat turvallisuusluokitellut tietoliikenneverkot ja verkkoympäristöt.

Taulukko 4 Kooste CSfC-ominaisuuksista

Etu	Haitta / riski
Helppous	Kehitetty Yhdysvaltain valtionhallinnolle, saatavuus Yhdysvaltain ulkopuolella voi olla ongelma
kustannukset Yksi CSfC-ohjelman lupauksista on edullisuus	kustannukset Edullisuudesta ei ole varmuutta. Toimittajat eivät ole ilmoittaneet kustannuksia, joten vertailua ei voi toteuttaa
Yhdellä toimittajalla voidaan välttää monen toimittajan ympäristön luomisesta ja ylläpidosta seuraavat ongelmat	Yhden toimittajan käytöllä on omat riskinsä
Suomen turvallisuusluokitelluissa verkkoympäristöissä voidaan saavuttaa riittävä luotettavuus tietoturvan suhteen	
Koska vaatimukset komponenteille on listattu, ei CSfC:tä tarvitse hankkia valmiina toteutuksena, vaan voidaan tarkistaa täyttäisikö tarjolla olevat ei-CSfC-sertifioidut tuotteet tarvittavaa tietoturvaa	

Saatujen tulosten valossa, opinnäytteelle asetettuun tutkimuskysymykseen, voidaanko CSfC-ohjelma ottaa käyttöön Suomessa, saadaan kieltävä vastaus. Yritykset, jotka NSA on hyväksynyt ominaisuuspakettien toimittajiksi, eivät vaikuta tarjoavan toteutuksia Yhdysvaltain ulkopuolelle.

4.3 Komponenttikatsaus

NSA pitää listaa komponenteista, jotka täyttävät CSfC:n vaatimukset, mistä on hyötyä myös Suomen turvallisuusluokiteltujen verkkojen näkökulmasta. Vaikka valmiiksi suunniteltua toteutusta ei olisikaan tarjolla, voidaan tarkistaa, löytyykö tarjottu tuote komponenttilistalta.

Tutkimuskysymykselle asetetusta apukysymyksestä, kuinka CSfC-ohjelman käyttöönotto tapahtuisi tai mitä lisätutkimusta tämä vaatisi, voidaan antaa ehdotuksia jatkoa ajatellen. Varteenotettavin huomio CSfC-ohjelmasta on NSA:n ylläpitämä komponenttilista. Tällä listalla olevat tuotteet tarjoavat riittävät turvallisuusominaisuudet, jotta niitä voidaan käyttää turvallisuusluokitelluissa ympäristöissä.

Taulukkoon 5 on listattu CSfC-ohjelmaan yhteensopiviksi hyväksyttyjä komponentteja. Näissäkin on huomattavissa CSfC-ohjelman keskittyminen Yhdysvaltoihin. Yhtenä kriteerinä komponenttilistalle pääsyn epäämiseen on riittävä ulkomainen omistuspohja. Toisena huomiona on kuitenkin avoimen koodin ratkaisujen hyväksyminen esim. Red Hatin tapauksessa. Tarkempi listaus komponenteista löytyy liitteestä 2 (Components List Index).

Taulukko 5 Komponenttivertailu

Komponentti	**Ominaisuuspaketti**	**Toimittaja**
Autentikointipalvelin	Etäyhteys Kampus WLAN Moni-toimipiste	Aruba Cisco
Varmennepalvelu	Etäyhteys Kampus WLAN Moni-toimipiste	Information Security Corporation Red Hat Inc

Komponentti	**Ominaisuuspaketti**	**Toimittaja**
Loppukäyttäjän laite / Mobiili-laite	Etäyhteys	Motorola Samsung
Tiedostonsalaus	Data levossa	Jacobs Samsung
Laitteistopohjainen levynsa-laus	Data levossa	Curtiss-Wright Defense Soluti-ons KLC Group Mercury Systems NetApp
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco Juniper McAfee SonicWall
IPsec VPN-sovellus	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco Samsung
Mobiililaitehallinta	Etäyhteys	Blackberry Samsung VMware

Komponentti	**Ominaisuuspaketti**	**Toimittaja**
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Apriva Aruba Attila Security Checkpoint Cisco CommScope Technologies Extreme Networks Juniper PacStar Palo Alto SonicWall WatchGuard Technologies
MACsec salauslaite	Moni-toimipiste	Cisco Juniper
Sovelluspohjainen laitesalaus	Data levossa	Curtiss-Wright Defense Solutions NetApp
WLAN-järjestelmä	Kampus WLAN	Aruba Cisco CommScope Ruckus Wireless Ultra Electronics-3eTI

Komponentti	**Ominaisuuspaketti**	**Toimittaja**
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Aruba Attila Security CheckPoint Cisco F5 Networks Forcepoint Juniper PacStar Palo Alto SonicWall WatchGuard Technologies

Taulukkoon 5 koostetun komponenttilistauksen perusteella CSfC-ohjelman ominaisuuspakettien vaatimukset pystyttäisiin toteuttamaan ilman erillistä kokonaisuutta. Tämä vaatii hankkijalta enemmän vaivaa ja perehtyneisyyttä, kun kasataan ympäristö erillisistä komponenteista, jotka täyttävät CSfC-ohjelman vaatimukset, mutta eivät kuulu valmiiseen ominaisuuspakettiratkaisuun.

Taulukossa 6 on käyty läpi esimerkin omaisena toteutusehdotuksena NSA:n hyväksymistä komponenteista koostettu ratkaisu eri ominaisuuspaketeille. Tietosuojasyistä komponentit on valittu sattumanvaraisesti, eivätkä välttämättä vastaa oikeiden hankintojen vaatimuksia muuten kuin ominaisuuspaketin vaatimusten osalta. Komponentit on kuitenkin valittu siten, että ne ovat hankittavissa Suomesta.

Taulukko 6 Esimerkki ominaisuuspakettien toteutuksesta komponenteilla

Ominaisuuspaketti	Komponenttiesimerkki
Etäyhteys	Mobiililaite: Android 10 käyttöjärjestelmällä varustettu Samsung Palomuurit: Watchguard M5600IPS: Cisco FMC2600 VPN-komponentit: Juniper SRX4600 Tarvittavat palvelimet: RHEL-pohjaisia
Kampus WLAN	IPS: Cisco FMC2600 Palomuurit: Watchguard M5600 WLAN: Cisco 8540 hallintajärjestelmä ja Aironet tukiasemat Tarvittavat palvelimet: RHEL-pohjaisia
Moni-toimipiste	IPS: Cisco FMC2600 MACsec: Cisco ESS-3300-NCP Palomuurit: Watchguard M5600 Tarvittavat palvelimet: RHEL-pohjaisia
Data levossa	Tiedostonsalaus: Knox File Encryption Laitteistopohjainen levynsalaus: NetApp Storage Encryption Ohjelmistopohjainen levynsalaus: NetApp Storage Encryption Tarvittavat palvelimet: RHEL-pohjaisia

Kuten taulukoista 5 ja 6, sekä liitteestä 2 voidaan huomata, on komponenteissa melko laaja valikoima ja niistä pystytään koostamaan ominaisuuspakettien vaatimusten mukaisia ratkaisuja. Jatkoehdotuksena on käydä läpi komponenttilistausta tarkemmin ja selvittää onko näissä mukana komponentteja, joita voidaan käyttää Suomen turvallisuusluokitelluissa verkoissa. Tämä kuitenkin olisi salassapitosyistä suoritettava täysin Valtorin sisäisenä selvityksenä, eikä näin ollen sovellu opinnäytetyön kaltaiseen tutkimukseen.

5 Pohdinta

Opinnäyte lähti liikkeelle kysymyksestä, onko NSA:n CSfC-ohjelma mahdollista ottaa Suomessa käyttöön. Tämän avuksi asetettiin kysymykset siitä mikä CSfC-ohjelma on ja miten sen toteutus tapahtuisi, sekä tarpeen vaatiessa mitä lisätutkimusta tarvitaan.

CSfC-ohjelma ja sen toiminta saatiin selvitettyä riittävällä tarkkuudella sen käyttöönoton mahdollisuuden selvittämiseksi. Tämän ja yhteistyökumppaneiden ominaisuuspakettien toteutusten tarjontaa tarkastellessa saatiin myös vastaus varsinaiseen tutkimuskysymykseen. CSfC-ohjelman käyttöönotto sellaisenaan ei onnistu Suomessa

Tulosten perusteella CSfC-ohjelma on liian sidoksissa Yhdysvaltojen hallinnon tarpeisiin ollakseen suoraan käytettävissä Suomessa. Ohjelman itsensä jatkotutkimuksella tuskin saataisiin lisäarvoa. Mahdollisen jatkon kannalta olisikin järkevämpää keskittyä ominaisuuspakettien listaamiin vaatimukseen, sekä komponenttilistalla oleviin tuotteisiin ja ottaa nämä vertailukohteeksi. Yleisluontoisessa katsauksessa komponentteihin saatiin tulokseksi, että listatuista komponenteista olisi mahdollista luoda CSfC-ohjelman vaatimuksia kasaavia ratkaisuja. Tältä pohjalta komponentteja voisi lähteä tarkastelemaan tarkemmin oikeaan tuotantoympäristöön. Tämä kuitenkin vaatisi syvällisempää avaamista Suomen turvallisuusverkkoympäristöistä, mikä ei sovellu opinnäytteen kaltaiselle tutkimukselle.

Huomionarvoiseksi ongelmaksi kirjoittamisen aikana muodostui, kuinka käsitellä tällaista aihetta ottamatta esille turvallisuusluokiteltua tietoa. Kerätyn aineiston analysointi piti tehdä hyvin yleiseltä pohjalta, mikä luonnollisesti vähentää työstä saatua arvoa.

Lähteet

Commercial National Security Algorithm (CNSA) Suite. N.d. NSA:n julkaisu. Viitattu 23.10.2021. CNSS WORKSHEET.PDF (defense.gov)

Commercial Solutions for Classified (CSfC). N.d. Ohjelman kuvaus NSA:n sivuilla. Viitattu 3.10.2021. https://www.nsa.gov/Portals/75/documents/resources/everyone/csfc/handout-trifold.pdf

Components List Index. N.d. Komponenttilistaus NSA:n sivuilla. Viitattu 01.12.2021. https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Components-List/#components-list-index

Data at Rest Capability Package. 2020. NSA:n julkaisu. Viitattu 3.10.2021. https://www.nsa.gov/Portals/75/documents/resources/everyone/csfc/capability-packages/(U)%20DAR%20CP%20v5_0%20Final.pdf

Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje. 2016. Ulkoasiainministeriön julkaisu. Viitattu 3.10.2021. https://um.fi/documents/35732/48132/kansainv%C3%A4lisen_turvallisuusluokitellun_tietoaineiston_k%C3%A4sittelyohje/

Kunnela, A., Latvala, E. & Tuomi, S. Soveltavasta tutkimuksesta. Jyväskylän ammattikorkeakoulu. Viitattu 19.10.2021. https://oppimateriaalit.jamk.fi/yamk-kasikirja/soveltavat-tutkimusmenetelmat/

Mobile Access Capability Package V2.1. 2018. NSA:n julkaisu. Viitattu 3.10.2021. https://www.nsa.gov/portals/75/documents/resources/everyone/csfc/capability-packages/MACPv2_1.pdf7. MACP.pdf 5.1 outer firewall

Multi-Site Connectivity Capability Package V.1.1.8. 2021. NSA:n julkaisu. Viitattu 3.10.2021. https://www.nsa.gov/portals/75/documents/resources/everyone/csfc/capability-packages/(U)%20Multi-Site%20Connectivity%20Capability%20Package%20v1_1_8.pdf?ver=Oju5P225bTNqYIouuFunlw%3d%3d

Vilkka, H. 2021. Tutki ja kehitä. 5. painos. Jyväskylä: PS-kustannus

Who are the typical CSfC clients?. N.d. FAQ-osio NSA:n sivuilla. Viitattu 3.10.2021. https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/faq/

Wireless Local Area Network Capability Package V2.2. 2018. NSA:n julkaisu. Viitattu 3.10.2021. https://www.nsa.gov/portals/75/documents/resources/everyone/csfc/capability-packages/WLANCPv2.2_20180626.pdf

Liitteet

Liite 1 NSA:n hyväksytyt CSfC-palveluntarjoajat

Kumppani	Tarjotut ominaisuuspaketit	CSfC-asiakkaat
4n2n Solutions LLC https://4n2nsolutions.com/csfc	Etäyhteys Kampus WLAN Moni-toimipiste	Ei Yhdysvaltain ulkopuolella
Agile Defense Inc https://agile-defense.com/	Ei tietoa CSfC-toteutuksista	Ei Yhdysvaltain ulkopuolella
American Systems https://www.americansystems.com/	Ei tietoa CSfC-toteutuksista	Ei Yhdysvaltain ulkopuolella
Apriva ISS LLC https://www.apriva.com/	Ei tarkkaa tietoa Mukana etäkäyttöratkaisuissa	Ei Yhdysvaltain ulkopuolella
Assured Information Security Inc https://www.ainfosec.com/	Ei tarkkaa tietoa Tarjoaa CSfC-yhteensopivaa etäkäyttöratkaisua	Ei Yhdysvaltain ulkopuolella
AT&T CORP., Government Solutions https://www.business.att.com/industries/public-sector.html	Ei tarkkaa tietoa	Ei Yhdysvaltain ulkopuolella
Augustine Consulting Inc	Ei tietoa	Ei tietoa

https://www.aciedge.com/		
B&D Consulting Inc	Ei tietoa	Ei tietoa
BAE Systems Technology Solutions & Services Inc https://www.baesystems.com	Ei tietoa	Ei tietoa
The Boeing Company https://www.boeing.com/	Ei tietoa	Ei tietoa
Booz Allen Hamilton https://www.boozallen.com/	Ei tarkkaa tietoa	Ei tarkkaa tietoa
By Light Professional IT Services https://www.bylight.com/	Ei tietoa	Ei Yhdysvaltain ulkopuolella
CACI Technologies Inc https://www.caci.com/	Ei tarkkaa tietoa	Ei Yhdysvaltain ulkopuolella
Cambridge International https://www.cambridgeinternati-onal.org/	Ei tietoa	Ei tietoa
CDW Government https://www.cdwg.com/	Ei tietoa	Ei Yhdysvaltain ulkopuolella
CIS Secure Computing Inc https://cissecure.com	Etäyhteys Kampus WLAN Moni-toimipiste	Ei tarkkaa tietoa Komponentteja mahdollista hankkia Yhdysvaltojen ulko-puolelta

	Data levossa	
Collins Aerospace https://www.collinsaeros-pace.com/	Ei tietoa	Ei tietoa
Crystal Clear Technologies Inc https://www.crystalcleartec.com	Etäyhteys Kampus WLAN Moni-toimipiste Data levossa	Ei tietoa
CSRA LLC Ei enää toiminnassa	Ei enää toiminnassa	Ei enää toiminnassa
CyberIP Services https://cyberipservices.com/	Ei tietoa	Ei tietoa
Deloitte LLP https://www2.deloitte.com	Ei tietoa	Ei tietoa
Enterprise Services LLC	Ei tietoa	Ei tietoa
Envistacom LLC https://www.envistacom.com/	Ei tietoa	Ei Yhdysvaltain ulkopuolella
Futron Inc https://futroninc.com/	Ei tarkkaa tietoa	Ei tietoa

General Dynamics Mission Systems https://gdmissionsystems.com/	Ei tarkkaa tietoa	Ei tietoa
General Dynamics/Electric Boat Corporation http://www.gdeb.com/	Ei tietoa	Ei tietoa
General Dynamics Information Technology https://www.gdit.com/	Ei tietoa	Ei tietoa
Global Technical Systems https://gts.us.com/	Etäyhteys Kampus WLAN Moni-toimipiste Data levossa	Ei Yhdysvaltain ulkopuolella
GuROO LLC https://gurooit.com/	Etäyhteys Kampus WLAN Moni-toimipiste	Ei Yhdysvaltain ulkopuolella
IAP Worldwide Services Inc https://www.iapws.com/	Ei tarkkaa tietoa	Ei Yhdysvaltain ulkopuolella
IBM https://www.ibm.com	Ei tietoa	Ei tietoa
ID Technologies https://www.idtec.com/	Etäyhteys Kampus WLAN	Ei Yhdysvaltain ulkopuolella

	Moni-toimipiste Data levossa	
iGov Technologies Inc https://www.igov.com/	Ei tietoa	Ei Yhdysvaltain ulkopuolella
Integrio Technologies http://integrio.com/	Ei tarkkaa tietoa	Ei tietoa
Intelligent Waves LLC https://intelligentwaves.com/	Ei tarkkaa tietoa	Ei Yhdysvaltain ulkopuolella
Iron Bow Technologies https://ironbow.com/	Etäyhteys Kampus WLAN Moni-toimipiste Data levossa	Ei Yhdysvaltain ulkopuolella
IT Veterans, LLC	Ei tietoa	Ei tietoa
Key Management Solutions	Ei tietoa	Ei tietoa
Kord Technologies Inc https://kordtechnologies.com/	Ei tietoa	Ei tietoa
Leidos Innovations Corporation https://www.leidos.com/	Ei tarkkaa tietoa	Ei tietoa
Life Cycle Engineering https://www.lce.com/	Ei tarkkaa tietoa	Ei tietoa

LinQuest Corporation https://www.linquest.com/	Ei tietoa	Ei tietoa
L3 Harris Technologies https://www.l3harris.com/	Ei tietoa	Ei tietoa
Lockheed Martin Corporation https://www.lockheedmartin.com	Ei tietoa	Ei tietoa
Lumen Technologies Government Solutions https://www.lumen.com/public-sector.html	Ei tietoa	Ei tietoa
MAG DS Corp	Ei tietoa	Ei tietoa
M.C. Dean Inc https://www.mcdean.com/	Ei tietoa	Ei tietoa
The Mil Corporation https://www.milcorp.com/	Ei tarkkaa tietoa	Ei Yhdysvaltain ulkopuolella
Mission 1st Group Inc https://www.mission1st.com/	Ei tarkkaa tietoa	Ei Yhdysvaltain ulkopuolella
Motorola Solutions Inc https://www.motorolasoluti-ons.com/en_us.html	Ei tarkkaa tietoa	Ei Yhdysvaltain ulkopuolella

NAVAIR Naval Air Warfare Center - Aircraft Division https://www.na-vair.navy.mil/nawcad/	Ei tietoa	Ei tietoa
NCI Information Systems Inc https://www.nciinc.com/	Ei tietoa	Ei tietoa
Network Designs Inc	Ei tarkkaa tietoa	Ei Yhdysvaltain ulkopuolella
NexTech Solutions LLC https://nextechsol.com/	Ei tietoa	Ei tietoa
Northrop Grumman Mission Sys-tems https://www.northropgrum-man.com/who-we-are/business-sectors/mission-systems/	Ei tietoa	Ei tietoa
Oceus Networks https://www.oceusnet-works.com/	Ei tarkkaa tietoa	Ei Yhdysvaltain ulkopuolella
Ortman Consulting LLC https://ortmanconsulting.com/	EtäyhteysKampus WLAN Moni-toimipiste Data levossa	Ei Yhdysvaltain ulkopuolella
OSC Edge LLC https://oscedge.com/	Etäyhteys	Ei Yhdysvaltain ulkopuolella

Peraton	Ei tarkkaa tietoa	Ei Yhdysvaltain ulkopuolella
Perfecta Federal https://www.perfecta.com/	Ei tietoa	Ei tietoa
Perspecta Labs Inc	Ei tietoa	Ei tietoa
Progeny Systems Corp https://www.progeny.net/	Ei tietoa	Ei Yhdysvaltain ulkopuolella
Raytheon Technologies https://www.rtx.com/	Ei tietoa	Ei tietoa
Red River Technology https://redriver.com/	Ei tarkkaa tietoa	Ei tietoa
Referentia Systems https://www.referentia.com/	Ei tietoa	Ei tietoa
SAIC https://www.saic.com/	Ei tietoa	Ei tietoa
Scientific Research Corporation https://www.scires.com/	Ei tietoa	Ei tietoa
Seakr Engineering https://www.seakr.com/	Ei tietoa	Ei tietoa
Solers Inc		

SOS International https://www.sosi.com	Ei tarkkaa tietoa	Ei Yhdysvaltain ulkopuolella
Technica Corp https://technicacorp.com/	Etäyhteys	Ei Yhdysvaltain ulkopuolella
Trace Systems Inc https://www.tracesystems.com/	Ei tietoa	Ei tietoa
Tribalco LLC https://www.tribalco.com/	Etäyhteys Kampus WLAN Moni-toimipiste Data levossa	Ei tietoa
Unisys Corporation https://www.unisys.com/	Ei tarkkaa tietoa	Ei Yhdysvaltain ulkopuolella
U.S. Air Force Research Laboratory https://www.afrl.af.mil/	Ei tietoa	Ei tietoa
U.S. Army C5ISR Center	Ei tietoa	Ei tietoa
US Naval Information Warfare Systems Command – Atlantic https://www.niwcatlantic.navy.mil	Ei tietoa	Ei tietoa
US Naval Information Warfare Systems Command – Pacific	Ei tietoa	Ei tietoa

https://www.niwcpaci-fic.navy.mil/		
VAE Inc https://www.vaeit.com/	Ei tietoa	Ei tietoa
Verizon https://www.verizon.com/	Ei tietoa	Ei tietoa
ViaSat Inc https://www.viasat.com/	Ei tietoa	Ei tietoa
World Wide Technology Inc https://www.wwt.com/	Ei tietoa	Ei tietoa

Liite 2 Komponenttilistaus

Komponentti	Ominaisuuspaketti	Toimittaja	Tuote	Hyväksytyt versiot
Autentikaatiopalvelin	Etäyhteys Kampus WLAN Moni-toimipiste	Aruba	ClearPass Policy Manager	6.9
Autentikaatiopalvelin	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	Identity Services Engine	2.6
Varmennepalvelu	Etäyhteys Kampus WLAN Moni-toimipiste	Information Security Corporation	CertAgent	7.0
Varmennepalvelu	Etäyhteys Kampus WLAN Moni-toimipiste	Red Hat Inc	Red Hat Certificate System	RHEL 7.6
Loppukäyttäjän laite / Mobiililaite	Etäyhteys	Samsung	Galaxy Tab S6, Galaxy S9, Galaxy S9+, Galaxy Note9, Galaxy S10, Galaxy S10 5G, Galaxy Note S10+ 5G, Galaxy Note S10+, Galaxy S10E, Galaxy Fold, Galaxy Fold 5G, Galaxy S20 Ultra 5G, Galaxy S20+ 5G, Galaxy S20 5G, Galaxy S20 LTE, Galaxy S20+ LTE, Galaxy Z Flip, Galaxy XCover	Android 10

			Pro, Galaxy XCover FieldPro, Galaxy A51, Galaxy Note 10, Galaxy S10+, Galaxy Note 20 Ultra 5G, Galaxy Note 20 Ultra LTE, Galaxy Note 20 5G, Galaxy Note 20 LTE, Galaxy Tab S7+, Galaxy Tab S7, Galaxy Note 10 5G, Galaxy Z Fold 2 5G, Galaxy Tab S6 5G, Galaxy S20 FE, Galaxy Tab S7+ 5G, Galaxy Tab S7 5G, Galaxy Z Flip 5G, Galaxy S20 TE, Galaxy A71 5G, Galaxy A51 5G, Galaxy Tab Active 3, Galaxy Tab S4	
Loppukäyttäjän laite / Mobiililaite	Etäyhteys	Samsung	Galaxy S21 Ultra 5G, Galaxy S21+ 5G, Galaxy S21 5G, Galaxy Z Fold2 5G, Galaxy Note20 Ultra 5G, Galaxy Note20 Ultra LTE, Galaxy Note20 5G, Galaxy Note20 LTE, Galaxy Tab S7+ 5G, Galaxy Tab S7+, Galaxy Tab S7 5G, Galaxy Tab S7, Galaxy Z Flip 5G, Galaxy S20 Ultra 5G, Galaxy S20+ 5G, Galaxy S20+ LTE, Galaxy S20 5G, Galaxy S20 TE, Galaxy S20 LTE, Galaxy S20 FE, Galaxy	Android 11

			XCover Pro, Galaxy A51, Galaxy Note10+ 5G, Galaxy Note10+, Galaxy Note10 5G, Galaxy Note10, Galaxy Tab S6 5G, Galaxy Tab S6, Galaxy S10 5G, Galaxy S10+, Galaxy S10, Galaxy S10e, Galaxy Fold 5G, Galaxy Fold, Galaxy Z Flip, Galaxy A71 5G, Galaxy A51 5G, Galaxy Tab Active3, Galaxy A52 5G, Galaxy A42 5G	
Loppukäyttäjän laite / Mobiililaite	Etäyhteys	Motorola	Motorola Lex L11	Android 9
Tiedostonsalaus	Data levossa	Jacobs	KeyW Protect for Samsung	1.2.1.0
Tiedostonsalaus	Data levossa	Samsung	Knox File Encryptiont	1.0, 1.2, 1.3
Laitteistopohjainen levynsalaus	Data levossa	Curtiss-Wright Defense Solutions	Compact Network Storage 4-Slot (CNS4) Hardware Encryption Layer	A1
Laitteistopohjainen levynsalaus	Data levossa	Curtiss-Wright Defense Solutions	Data Transport System 1-Slot (DTS1) Hardware Encryption Layer	5.1
Laitteistopohjainen levynsalaus	Data levossa	KLC Group	CipherDrive	1.2.2

Laitteistopohjainen levynsalaus	Data levossa	Mercury Systems	ASURRE-Stor Solid State Self-Encrypting Drive	3.0
Laitteistopohjainen levynsalaus	Data levossa	NetApp	Storage Encryption	ONTAP 9.7P13
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	Cisco FirePOWER 7000 Series, 8000 Series & Cisco AMP, Cisco UCS B200-M4, B200-M5, C220-M4S, C220-M5, C240-M5, C240-M4SX, C240-M4L, C460-M4, C480-M5, EN120S-M2/K9, EN120E-208/KP, E140S-M2/k9, E160S-M3 & E180D-M2/K9 Cisco FireSIGHT FS750, FS1000, FS2000, FS2500, FS4000, FS4500	6.2
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	FP8350, FP8360, FP8370, FP8390, AMP8350, AMP8360, AMP8370,	6.4

			AMP8390, FMC1000, FMC2500, FMC4500, FMC1600, FMC2600, FMC4600 Cisco UCS-B & C-series	
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	ASA 5508, ASA 5516, ISA 3000, FMC1000, FMC2500, FMC4500, FMC1600, FMC2600, FMC4600	FTD 6.4
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	Firepower 1000 & 2100-series FPR 1010, FPR 1120, FPR 1140, FPR2110, FPR 2120, FPR2130, FPR 2140, FMC1000, FMC2500, FMC4500, FMC1600, FMC2600, FMC4600	FTD 6.4
IPS	Etäyhteys	Cisco	FPR 4110, FPR 4120, FPR 4140,	FX-OS 2.6 & FTD 6.4

	Kampus WLAN Moni-toimipiste		FPR 4150, FPR 4115, FPR 4125, FPR 4145, FPR 9300 SM-24, FPR 9300 SM-36, FPR 9300 SM-44, FPR 9300 SM-40, FPR 9300 SM-48, FPR 9300 SM-56, FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9, FMC4600-K9	
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600, SRX5800, SRX1500, SRX4100, SRX4200	JUNOS 17.4R1
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX 4600 Series	Junos OS 18.1R1
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX550M	Junos OS 19.2R1

			SRX1500, SRX4100, SRX4200, SRX4600	
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	vSRX 3.0	Junos OS 19.2R1-S3
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	NFX 150	Junos OS 19.2R1-S2
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX5400, SRX5600 & SRX5800 Series	Junos OS 19.2R1-S2
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX345, SRX345-DUAL-AC, SRX380, SRX1500	Junos OS 20.2R1
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	McAfee	NS9300S, NS9300P, NS9200, NS9100, NS7350, NS7250, NS7150, NS7300, NS7200, NS7100, NS5200, NS5100, NS3200, NS3100	9.1.x
IPS	Etäyhteys Kampus WLAN	McAfee	NS3100, NS3200, NS5100, NS5200, NS3500, NS7100,	10.1x

	Moni-toimipiste		NS7200, NS7300, NS7150, NS7250, NS7350, NS7500, NS9100, NS9200, NS9300S, NS9300P, NS9500	
IPS	Etäyhteys Kampus WLAN Moni-toimipiste	SonicWall	TZ 300P, TZ 350, TZ 350W, TZ 600P, SOHO 250, SOHO 250W, TZ300, TZ300W, TZ400, TZ400W, TZ500, TZ500W, TZ600, NSa2650, NSA3600, NSa3650, NSA4600, NSa4650, NSA5600, NSa5650, NSA6600, NSa6650, NSa9250, NSa9450, NSa9650, SM9200, SM9400, SM9600, SM9800	6.5.4
IPsec VPN-sovellus	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	AnyConnect Se-cure Mobility Client for iOS 13	4.9

IPsec VPN-sovellus	Etäyhteys Kampus WLAN Moni-toimipiste	Samsung	Galaxy Tab S6, Galaxy S9, Galaxy S9+, Galaxy Note9, Galaxy S10, Galaxy S10 5G, Galaxy Note S10+ 5G, Galaxy Note S10+, Galaxy S10E, Galaxy Fold, Galaxy Fold 5G, Galaxy S20 Ultra 5G, Galaxy S20 5G, Galaxy S20 LTE, Galaxy S20+ 5G, Galaxy S20+ LTE, Galaxy Z Flip, Galaxy XCover Pro, Galaxy XCo-ver FieldPro, Ga-laxy A51, Galaxy Note 10, Galaxy S10+, Galaxy Note 20 Ultra 5G, Ga-laxy Note 20 Ultra LTE, Galaxy Note 20 5G, Galaxy Note 20 LTE, Ga-laxy Tab S7+, Ga-laxy Tab S7, Ga-laxy Note 10 5G, Galaxy Z Fold 2, Galaxy Tab S6 5G,	Android 10

			Galaxy S20 FE, Galaxy Tab S7+ 5G, Galaxy Tab S7 5G, Galaxy Z Flip 5g, Galaxy S20 TE	
IPsec VPN-sovellus	Etäyhteys Kampus WLAN Moni-toimipiste	Samsung	Galaxy A71 5G, Galaxy A51 5G, Galaxy Tab Active 3, Galaxy Tab S4	Android 10
IPsec VPN-sovellus	Etäyhteys Kampus WLAN Moni-toimipiste	Samsung	Galaxy S21 Ultra 5G, Galaxy S21+ 5G, Galaxy S21 5G, Galaxy Z Fold2 5G, Galaxy Note20 Ultra 5G, Galaxy Note20 Ultra LTE, Galaxy Note20 5G, Galaxy Note20 LTE, Galaxy Tab S7+ 5G, Galaxy Tab S7+, Galaxy Tab S7 5G, Galaxy Tab S7, Galaxy Z Flip 5G, Galaxy S20 Ultra 5G, Galaxy S20+ 5G, Galaxy S20+ LTE, Galaxy S20 5G, Galaxy S20 TE, Galaxy S20 LTE, Galaxy	Android 11

			S20 FE, Galaxy XCover Pro, Galaxy A51, Galaxy Note10+ 5G, Galaxy Note10+, Galaxy Note10 5G, Galaxy Note10, Galaxy Tab S6 5G, Galaxy Tab S6, Galaxy S10 5G, Galaxy S10+, Galaxy S10, Galaxy S10e, Galaxy Fold 5G, Galaxy Fold, Galaxy Z Flip)	
IPsec VPN-sovellus	Etäyhteys Kampus WLAN Moni-toimipiste	Samsung	Galaxy A71 5G, Galaxy A51 5G, Galaxy Tab Active3, Galaxy A52 5G, Galaxy A42 5G	Android 11
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Apriva	Apriva MESA VPN	2.0
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Aruba	Virtual Mobility Controller	
IPsec VPN-yhdyskäytävä	Etäyhteys	Aruba	AP-203R, AP-203RP, AP-205H,	Aruba OS 8.2

	Kampus WLAN Moni-toimipiste		AP-303H, 7205, 7210, 7220, 7240, 7240XM	
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Aruba	7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280, 9004	Aruba OS 8.6
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Attila Security	SilentEdge Enterprise Server & GoSilent Client	Debian 9
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Checkpoint	Security Gateway Appliances	R80.30
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	ISR 1101	IOS-XE 16.12
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	4351, 4331, 4321	IOS XE 3.13.2
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	ISR 1101, ISR 1109, ISR 1111, ISR 1112, ISR 1113, ISR 1116, ISR 1117, ISR 1118, ISR 1121, ISR 1126, ISR	IOS-XE 17.3

			1127, ISR 1128, ISR 1161	
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	FPR 2110, FPR 2120, FPR 2130, FPR 2140, FPR 4110, FPR 4115, FPR 4120, FPR 4125, FPR 4140, FPR 4145, FPR 4150, FPR 9300 SM-24, FPR 9300 SM-36, FPR 9300 SM-44, FPR 9300 SM-40, FPR 9300 SM-48, FPR 9300 SM-56	ASA v9.12 & FX-OS 2.6
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASAv5, ASAv10, ASAv30	ASA 9.12
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	Cisco Cloud Services Router 1000V	IOS-XE 17.3

IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	ESR-6300-CON-K9, ESR-6300-NCP-K9	IOS-XE 17.3
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	FPR 4110, FPR 4120, FPR 4140, FPR 4150, FPR 4115, FPR 4125, FPR 4145, FPR 9300 SM-24, FPR 9300 SM-36, FPR 9300 SM-44, FPR 9300 SM-40, FPR 9300 SM-48, FPR 9300 SM-56, FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9, FMC4600-K9	FX-OS 2.6 & FTD 6.4
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	FPR 1010, FPR 1120, FPR 1140, FPR2110, FPR 2120, FPR2130, FPR 2140, FMC1000, FMC2500, FMC4500, FMC1600,	FTD 6.4

			FMC2600, FMC4600	
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	CommScope Technologies	ICX 7450-24, ICX 7450-24P, ICX 7450-48, ICX 7450-48P, ICX 7450-48F	8.0.70
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Extreme Networks	BR-MLXE-4-AC, BR-MLXE-8-AC, BR-MLXE-16-AC & Management Card BR-MLX-MR2-X / BR-MLX-10GX4-IPSEC-M Card / BR-MLXE-32-AC & Management Card BR-MLX-MR2-32X / BR-MLX-10GX4-IPSEC-M Card)	R06.3.0aa
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600, SRX5800, SRX1500, SRX4100, SRX4200	JUNOS 17.4R1

IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX 4600 Series	Junos OS 18.1R1
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX550M	Junos OS 19.2R1
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	vSRX 3.0	Junos OS 19.2R1-S3
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX1500, SRX4100, SRX4200, SRX4600	Junos OS 19.2R1
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX5400, SRX5600 & SRX5800 Series	Junos OS 19.2R1-S2
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	NFX150	Junos OS 19.2R1-S2
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX345, SRX345-DUAL-AC, SRX380, SRX1500	Junos OS 20.2R1

IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	PacStar	PacStar 451/453/455 Series	v9.12
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	Palo Alto	PA-220, PA-800, PA-3000, PA-3200, PA-5200, PA-7000 & VM Series NGFW PA-220, PA-220R, PA-820, PA-850, PA-3020, PA-3050, PA-3060, PA-3220, PA-3250, PA-3260, PA-5220, PA-5250, PA-5260, PA-5280, PA-7050, PA-7080 & VM-50, VM-100, VM-200, VM-300, VM-500, VM-700 & VM-1000-HV	PAN-OS 9.0, PAN-OS 9.1.8 & PAN-OS 10.0.5
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	SonicWall	TZ 300P, TZ 350, TZ 350W, TZ 600P, SOHO 250, SOHO 250W, TZ300, TZ300W, TZ400, TZ400W, TZ500, TZ500W, TZ600, NSa2650,	Version 6.5.4

			NSA3600, NSa3650, NSA4600, NSa4650, NSA5600, NSa5650, NSA6600, NSa6650, NSa9250, NSa9450, NSa9650, SM9200, SM9400, SM9600, SM9800	
IPsec VPN-yhdyskäytävä	Etäyhteys Kampus WLAN Moni-toimipiste	WatchGuard Tech-nologies	T20, T20-W, T35, T35-W, T40, T40-W, T55, T55-W, T70, T80, M270, M370, M470, M570, M670, M4600, M5600	OS v12.6.2
MACsec salauslaite	Moni-toimipiste	Cisco	C9606R Chassis, C9600-SUP-1, C9600-LC-24C and C9600-LC-48YL	IOS-XE 16.12
MACsec salauslaite	Moni-toimipiste	Cisco	C9200-24T, C9200-48T, C9200-24P, C9200-48P, C9200-24P8X, C9200-48P8X, C9200L-24P-4G,	IOS-XE 16.12

			C9200L-24P-4X, C9200L-24T-4G, C9200L-24T-4X, C9200L-48P-4G, C9200L-48P-4X, C9200L-48T-4G, C9200L-48T-4X, C9200L-24P8X-2Y, C9200L-24P8X-4X, C9200L-48P12X-4X, C9200L-48P8X-2Y, C9300-24S, C9300-48S, C9300L-24T-4G, C9300L-24P-4G, C9300L-48T-4G, C9300L-48P-4G, C9300L-24T-4X, C9300L-24P-4X, C9300L-48T-4X, C9300L-48P-4X, C9300L-24UX-4X, C9300L-48UX-4X, C9300L-24UX-2Q, C9300L-48UX-2Q, Chassis C9404R, C9407R, C9410R; Supervisor C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y	

MACsec salauslaite	Moni-toimipiste	Cisco	ESS-3300-NCP, ESS-3300-24T-CON, ESS-3300-24T-NCP, ESS-3300-CON	IOS-XE 16.12
MACsec salauslaite	Moni-toimipiste	Juniper	MX80, MX104, MX240, MX480, MX960 & MICMACSEC-20G	Junos OS 18.3R1-S1
Mobiililaitehallinta	Etäyhteys	Blackberry	Blackberry Enterprise Service	12.5
Mobiililaitehallinta	Etäyhteys	Samsung	Unified Endpoint Management (UEM) Server & Android Client	12
Mobiililaitehallinta	Etäyhteys	VMware	Enterprise Mobility Management (EMM)	2.2.5
Sovelluspohjainen laitesalaus	Data levossa	Curtiss-Wright Defense Solutions	Compact Network Storage 4-Slot Software Encryption Layer	A1
Sovelluspohjainen laitesalaus	Data levossa	Curtiss-Wright Defense Solutions	Data Transport System 1-Slot (DTS1) Software Encryption Layer	5.1
Sovelluspohjainen laitesalaus	Data levossa	NetApp	Volume Encryption Appliances	ONTAP 9.7P13

Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Aruba	Virtual Mobility Controller	6.5.0
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Aruba	7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280, 9004	Aruba OS 8.6
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Attila Security	SilentEdge Enterprise Server GoSilent Client	Debian 9
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	CheckPoint	Security Gateway Appliances	R80.30
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	FPR 2110, FPR 2120, FPR 2130, FPR 2140	ASA v9.12 & FX-OS 2.6
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	FPR 4110, FPR 4115, FPR 4120, FPR 4125, FPR 4140, FPR 4145, FPR 4150, FPR 9300 SM-24, FPR 9300 SM-36, FPR 9300 SM-44, FPR 9300 SM-40, FPR	ASA v9.12 & FX-OS 2.6

			9300 SM-48, FPR 9300 SM-56	
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	FPR 1010, FPR 1120, FPR 1140, FPR2110, FPR 2120, FPR2130, FPR 2140, FMC1000, FMC2500, FMC4500, FMC1600, FMC2600, FMC4600	FTD 6.4
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	FPR 4110, FPR 4120, FPR 4140, FPR 4150, FPR 4115, FPR 4125, FPR 4145, FPR 9300 SM-24, FPR 9300 SM-36, FPR 9300 SM-44, FPR 9300 SM-40, FPR 9300 SM-48, FPR 9300 SM-56, FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9, FMC4600-K9	FX-OS 2.6 & FTD 6.4

Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Cisco	ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASAv5, ASAv10, ASAv30, ASAv50	ASA 9.12
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	F5 Networks	BIG-IP	12.1.3.4
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Forcepoint	Next Generation Firewall	LINUX 6.5
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600, SRX5800, SRX1500, SRX4100 and SRX4200	JUNOS 17.4R1
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX 4600 Series	Junos OS 18.1R1

Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX550M, SRX1500, SRX4100, SRX4200, SRX4600	Junos OS 19.2R1
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	vSRX 3.0	Junos OS 19.2R1-S3
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	NFX 150	Junos OS 19.2R1-S2
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX5400, SRX5600 & SRX5800 Series	Junos OS 19.2R1-S2
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	Juniper	SRX345, SRX345-DUAL-AC, SRX380, SRX1500	Junos OS 20.2R1
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	PacStar	PacStar 451/453/455 Series	v9.12
Palomuuri	Etäyhteys Kampus WLAN	Palo Alto	PA-220, PA-800, PA-3000, PA-3200, PA-5200,	PAN-OS 9.0, PAN-OS 9.1.8

	Moni-toimipiste		PA-7000 VM Series NGFW PA-220, PA-220R, PA-820, PA-850, PA-3020, PA-3050, PA-3060, PA-3220, PA-3250, PA-3260, PA-5220, PA-5250, PA-5260, PA-5280, PA-7050, PA-7080, VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000-HV	& PAN-OS 10.0.5
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	SonicWall	TZ 300P, TZ 350, TZ 350W, TZ 600P, SOHO 250, SOHO 250W, TZ300, TZ300W, TZ400, TZ400W, TZ500, TZ500W, TZ600, NSa2650, NSA3600, NSa3650, NSA4600, NSa4650, NSA5600, NSa5650, NSA6600,	6.5.4

			NSa6650, NSa9250, NSa9450, NSa9650, SM9200, SM9400, SM9600, SM9800	
Palomuuri	Etäyhteys Kampus WLAN Moni-toimipiste	WatchGuard Technologies	T20, T20-W, T35, T35-W, T40, T40-W, T55, T55-W, T70, T80, M270, M370, M470, M570, M670, M4600, M5600	12.6.2
WLAN-järjestelmä	Kampus WLAN	Aruba	7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280, 9004	Aruba OS 8.6
WLAN-järjestelmä	Kampus WLAN	Cisco	Catalyst 9800, Catalyst 9800-40, Cloud Catalyst 9800, Aironet 4800, 3802, 2802, 1562	IOS-XE 16.12
WLAN-järjestelmä	Kampus WLAN	Cisco	Controllers 8540, 5520, 3504 and Aironet Acces Points 4800, 3802, 2802, 1562	AireOS Release 8.10

WLAN-järjestelmä	Kampus WLAN	CommScope	SZ-144, SZ-300, vSZ-E, vSZ-H, vSZ-D, R610, R650, R750, T610, T710, R850	R5.2.1.3
WLAN-järjestelmä	Kampus WLAN	Ruckus Wireless	SZ-104, SZ-124, SZ-300, vSZ-E, vSZ-H, vSZ-D R610, R710, R720, T610, T610S, T710, T710S	R5.1.1.3