jamk

Turvallisuusluokan IV tietojenkäsittely vaatimukset langattoman lähiverkon tiedonsiirrolle

Aleksi Korkalainen

Opinnäytetyö
Helmikuu 2023
Insinööri (AMK), Tieto- ja viestintätekniikan tutkinto-ohjelma

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Korkalainen Aleksi

Turvallisuusluokan IV tietojenkäsittely vaatimukset langattoman lähiverkon tiedonsiirrolle

Jyväskylä: Jyväskylän ammattikorkeakoulu. Helmikuu 2023, 33 sivua.

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

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Toimeksiantajan on tarkoitus parantaa tiedonhallintalain voimaan tulon myötä turvallisuusluokitellun tiedon käsittely-ympäristöjen tietoturvaa ja tähän kuuluu saada turvallisuusluokan IV vaatimukset täyttävä ratkaisu langattomissa lähiverkoissa tapahtuvaa tiedonsiirtoa varten.

Tavoitteena oli saada toimeksiantajalle tietoa siitä, kuinka Katakrin vaatimuksia täyttävä ratkaisu langattomalle tiedonsiirrolle saadaan täytettyä, jotta voidaan käsitellä turvallisuusluokan IV tietoa langattomassa lähiverkossa niin, että käyttökokemus ei kärsi. Tämä toteutettiin tutustumalla Katakri 2020 vaatimuksiin ja tutkimalla esimerkiksi kuinka turvallisuusluokittelu toimii, mitkä ovat salausratkaisun vaatimukset ja kuinka sen arviointi- ja hyväksyntäprosessi toimii.

Tutkimuksen tuloksena saatiin tieto siitä mitkä ovat Katakrin vaatimukset langattomalle tiedonsiirrolle ja kuinka salausratkaisun arviointi- ja hyväksyntäprosessi toimii.

Avainsanat (asiasanat)

Turvallisuusluokka IV, Katakri 2020, Langaton verkko, Tietoliikenne, Turvaluokiteltu tieto

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Korkalainen Aleksi

Classified information class IV data processing requirements for wireless LAN data communication

Jyväskylä: JAMK University of Applied Sciences, February 2023, 33 pages.

Engineer, Information and Communication Technology Degree

Permission for web publication: Yes

Language of publication: Finnish

Abstract

With the entry of the Information Management Act, the client intends to improve the information security of classified information processing environments, and this includes getting a solution for wireless local area networks that meets the requirements of classified information class IV for data transfer in wireless LANs.

The goal was to provide the client with information on how a solution for wireless data communication meets Katakri's requirements, so that classified information class IV data can be processed in the wireless local area network so that the user experience does not suffer. This was done by getting to know the Katakri 2020 requirements and studying how security classification works, what the encryption solution's requirements are and how its evaluation and approval process works.

As a result of the research, information about Katakri's requirements for wireless data communication was obtained and how the encryption solution evaluation and approval process works.

Keywords/tags (subjects)

Katakri 2020, Wireless Network, network, Classified information

Miscellaneous (Confidential information)

Sisältö

Kuviot

Lyhenteet ja termit

802.1x	IEEE 802.1X-stantardi
AD CS	Active Directory Certificate Services
AES	Advanced Encryption Standard
CA	Certificate Authority
CAA	Crypto Approval Authority
EAP	Extensible Authentication Protocol
EU	European Union
IANA	Internet Assigned Numbers Authority
IPsec	Internet Protocol Security
Katakri	Kansallinen turvallisuusauditointikriteeristö
MAC	Media Access Control
NCSA	National Communications Security Authority
NIST	National Institute of Standards and Technology
PSK	Pre Shared Key
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1 Johdanto

1.1 Taustaa työstä

Opinnäytetyössä oli tavoitteena tutkia, kuinka saadaan toteutettua työn toimeksiantajalle Katakrin turvallisuusluokan IV vaatimukset täyttävä ratkaisu turvallisuusluokan IV tietojen käsittelyyn langattomissa lähiverkoissa. Katakri on viranomaisten käyttämä turvallisuusauditointikriteeristö, mitä käytetään arvioidessa organisaation kykyä suojata kansallista tai kansainvälistä turvallisuusluokiteltua tietoa, eli tietoa mikä on salassa pidettävää mahdollisen paljastumisen tai käytön tuomien haittojen takia. Katakri on käytössä erityisesti valtionhallinnossa ja se on käytössä myös työn toimeksiantajalla, joka on virasto. Tietohallintalain voimaan tulon myötä toimeksiantajan on tarkoitus parantaa turvallisuusluokitellun tiedon käsittely-ympäristöjen tietoturvaa ja tähän kuuluu saada turvallisuusluokka IV:n vaatimukset täyttävä ratkaisu langattomien lähiverkojen tiedonsiirtoa varten. Nykypäivänä langattoman tiedonsiirron käyttö kasvaa koko ajan, sekä päätelaitteet että työt ovat yhä enemmän liikkuvia. Työn toimeksiantajalla on paljon työntekijöitä, joiden työ vaatii langatonta tiedonsiirtoa myös organisaation toimipisteillä. Tämä tekee tutkimuksen hyvin ajankohtaiseksi, jotta tiedetään, kuinka on yhä mahdollista toteuttaa langaton tiedonsiirto tietohallintalain siirtymäajan päättymisen myötä.

1.2 Työn tavoitteet

Opinnäytetyön tavoitteena oli saada toimeksiantajalle tieto siitä, kuinka Katakrin vaatimukset täyttävä ratkaisu saadaan toteutettua, jotta voidaan käsitellä turvallisuusluokan IV tietoa langattomassa verkossa, niin että käyttökokemus ei kärsi. Tutkimuksella pyrittiin selvittämään mahdolliset sudenkuopat sekä pohjatiedot toteutusta varten ja lisätä tietoisuutta Katakrin vaatimuksista. Työn tutkimusmenetelmänä käytettiin konstruktiivista tutkimusta, koska opinnäytetyössä tutkittiin tiedonhallintalain ja Katakrin turvallisuusauditointikriteeristön vaatimuksia, jotta saatiin selville parhaat vaihtoehdot lopulliseen toteutukseen.

1.3 Opinnäytetyön rakenne

Opinnäytetyön rakenne etenee seuraavasti. Luvussa 2 käydään läpi opinnäytetyön tutkimuskysymykset, -menetelmät, -etiikka ja -eettisiä asioita. Luvussa 3 käydään läpi opinnäytetyöhön liittyvää

teoriaa, jossa esitellään esimerkiksi lainsäädäntöä, Katakria ja sen rakennetta, sekä langatonta tiedonsiirtoa vaatimuksiin liittyen. Luvussa 4 käydään läpi tarkemmin Katakrin vaatimuksia koskien turvallisuusluokan IV tietojen käsittelyä langattomassa tiedonsiirrossa. Luvussa 5 kerrotaan, kuinka salausratkaisun arviointi- ja hyväksyntäprosessi toimii ja lopuksi 6 luvussa käydään läpi muutokset langattomassa tiedonsiirrossa turvallisuusluokan IV tietojen käsittelylle ja VPN (Virtual Private Network) -salausratkaisun käyttökokemusta.

2 Tutkimusasetelma

2.1 Tutkimuskysymykset

Tämän opinnäytetyön tutkimuskysymys on seuraava:

- Kuinka saadaan toteutettua Katakri 2020 vaatimukset täyttävä ratkaisu turvallisuusluokan IV tiedon käsittelyyn langattomassa tiedonsiirrossa?

Tämä pääkysymys on jaettu seuraaviin täsmentäviin alikysymyksiin:

- Kuinka Katakri 2020 vaatimuksia vastaava ratkaisu turvallisuusluokalle IV saadaan toteutettua parhaiten, jotta käyttökokemus ei kärsi?
- Kuinka VPN-salausratkaisu toteuttaa Katakri 2020 vaatimukset?

2.2 Tutkimusmenetelmä

Opinnäytetyön tavoitteiden ratkaisemiseksi, käytetään työssä tutkimusmenetelmänä konstruktiivista tutkimustapaa. Konstruktiivisella tutkimuksella tarkoitetaan tutkimustapaa, missä yritetään ratkaista reaalimaailman ongelmia ja näin samalla tuottaa lisää tieteenalalle, joten tämä tutkimustapa sopii hyvin tämän työn ongelman ratkaisemistapaan (Lukka 2001.). Opinnäytetyössä tutkitaan Katakrin vähimmäisvaatimuksia sekä, julkisuus- ja tiedonhallintalain vaatimuksia, jotta löydettäisiin paras vaihtoehto mikä ei tee käyttökokemuksesta hankalampaa.

2.3 Tutkimusetiikka

Opinnäytetyö on tehty noudattaen Jyväskylän ammattikorkeakoulun eettisiä ohjeita. Työssä ei rikota tekijänoikeuksia ja eikä käsitellä henkilökohtaisia tietoja. Työssä on käytetty lisensoituja tuotteita ja viitataan alkuperäisiin teoksiin Jyväskylän ammattikorkeakoulun raportointiohjeen mukaisesti. Opinnäytetyön tekemisestä sovittiin toimeksiantajan kanssa niin, että työ on tehtävissä ilman salassapitosopimusta. Tämä toteutuu niin, että työntoimeksiantajasta kerrotaan vain yleisellä tasolla yksilöimättä kohteena olevaa virastoa. Tämä tehtiin siksi, että otettiin huomioon tutkimusetiikka mahdollisen rikollisen toiminnan välttämiseksi.

3 Teoria

3.1 Lainsäädäntö

Tiedonhallintalaki toimii julkisen hallinnon eli viranomaisten tiedonhallinnan lakina, joka sisältää tiedonhallintaan, tietojärjestelmiin, katseluyhteyksiin ja tietoturvallisuuteen liittyviä säädöksiä. Tiedonhallintalain säädöksiin liittyy asetuksia mitkä on tarkennettu koskemaan turvallisuusluokiteltuja tietoja. (L 906/2019 ja L 1101/2019) Julkisuuslaki toimii viranomaisten toiminnan julkisuuden säätelyä varten, siinä säädellään viranomaisten tietoaineistojen julkisuutta ja salassapitoa. Lakiin kuuluu myös viranomaisten toiminnan vaitiolovelvollisuudet. (L 621/1999)

Tiedon turvallisuusluokittelu

Organisaatiossa on käytössä tietojen turvallisuusluokittelu-määrittely. Tietojärjestelmien, työasemien, älylaitteiden, toimitilojen ja tietoverkkojen on vastattava turvallisuudeltaan niissä käsiteltävän tiedon luokittelun vaatimuksia. Turvallisuusluokittelu määräytyy tiedonhallintalain mukaisesti luokkiin I-IV (L 906/2019). Julkisuuslain mukaan viranomaisen toiminnan julkisuudesta määrittää, että kaikki viranomaisten asiakirjat ovat julkisia, paitsi jos ne ovat erikseen turvallisuusluokiteltuja tai salassa pidettäviä julkisuuslain kohtien tai jonkin muun lain mukaan (L 621/1999, 24 §).

Turvallisuusluokittelu toimii neliportaisena turvallisuusluokka I-IV. Turvallisuusluokitellut asiakirjat ovat aina salassa pidettäviä, mutta asiakirjat mitkä ovat salassa pidettäviä eivät kuitenkaan ole aina turvallisuusluokiteltuja (L 1101/2019.). Turvallisuusluokittelua osoittava merkintä tehdään, jos

asiakirja tai sen sisältämä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain momentin 1, 2, 5 tai 7-11 kohdan perusteella (L 621/1999, 24 §). Turvallisuusluokat I, II, III ja IV merkataan asiakirjoihin edellä mainitun järjestyksen mukaan leimoin “ERITTÄIN SALAINEN”, “SALAINEN”, “LUOTTAMUKSELLINEN” ja “KÄYTTÖ RAJOITETTU”. Asiakirja voidaan myös merkitä ”SALASSA PIDETTÄVÄ” leimalla, jos se ei ole saanut turvallisuusluokittelua. Silloin se on salassa pidettävä toisen tai yleisen edun vuoksi. (L 1101/2019.)

Tiedon käsittely-ympäristöjen tulee täyttää niissä käsiteltävän tiedon luokittelun mukaiset turvallisuusvaatimukset. Tietojenkäsittely-ympäristön vaatimusten mukaisuus voidaan todentaa Katakrin avulla, ottaen huomioon Katakrin sisältämät vähimmäisvaatimukset koskien kansainvälisiä velvoitteita sekä kansallisia säädöksiä, mitkä pitävät täyttyä, jotta turvallisuusluokiteltua tietoa voidaan käsitellä tietyssä tiedonkäsittely-ympäristössä. (Katakri 2020.)

Kun turvallisuusluokiteltua tietoa kasaantuu suureksi määräksi esimerkiksi tietojärjestelmiin, tätä kutsutaan kasautumisvaikutukseksi. Tästä syystä kyseiset käsittely-ympäristöt voidaan joutua rakentamaan vastaamaan korkeampaa turvallisuusluokkaa. Määrä ei välttämättä ole ainoa tekijä asiaan, vaan myös käsittely-ympäristöjen yhdistäminen voi vaatia turvallisuustason noston. (Katakri 2020.)

Turvallisuusluokka IV

Jos tieto on salassa pidettävää julkisuuslain tai muun lain perusteella, sekä täyttää jonkun julkisuuslain momentin 1, 2, 5 tai 7-11 kohdan, se saa turvallisuusluokan IV merkinnän (L 621/1999, 24 §). Luokittelun perusteena on tiedon oikeudettoman paljastumisen tai käytön aiheuttama vahinko Suomen turvallisuudelle tietohallintalaissa määritetyllä tavalla. Tätä samaa kaavaa noudatetaan myös muihin turvallisuusluokkiin I, II ja III. Mahdollisen vahingon suuruus vaikuttaa kuinka korkea turvallisuusluokka asetetaan. (L 906/2019, 18 §)

3.2 Katakri ja sen rakenne

Katakri on viranomaisten tietoturvallisuuden auditointityökalu, mitä käytetään muun muassa arvioidessa organisaation kansainvälisen tai kansallisen turvallisuusluokitellun tiedon suojauskykyä. Katakri 2020 on auditointityökalun uusin versio. Katakri sisältää vähimmäisvaatimukset koskien

kansainvälisiä velvoitteita ja kansallisia säädöksiä. Kansallisen lainsäädännön vaatimuslähteet koskevat lakia julkisen hallinnon tiedonhallinnasta sekä asetusta, jonka valtionneuvosto on asettanut asiakirjoille niiden turvallisuusluokittelusta. Ohjetta noudatetaan Suomen valtionhallinnossa kansainvälisen ja kansallisen turvallisuusluokitellun tiedon suojaamisessa. Vaatimukset perustuvat tällä hetkellä voimassa olevaan Suomen lainsäädäntöön ja kansainvälisiin tietoturvallisuusvelvoitteisiin mihin Suomi sitoutuu. Tämän takia Katakri ei itsessään aseta tietoturvallisuudelle vaatimuksia. (Katakri 2020.) Katakrissa on käytetty Euroopan Unionin (EU) turvallisuussääntöjä kansainvälisenä lähteenä, mitkä sisältävät suojaamista koskevat perusperiaatteet ja vähimmäisvaatimukset EU:n turvallisuusluokittelun tiedon käsittelyä varten (2013/488/EU). Katakriin kuuluu kolme eri osa-aluetta, jotka koskevat turvallisuusjohtamista, fyysistä turvallisuutta sekä teknistä tietoturvallisuutta (Katakri 2020.).

3.2.1 Turvallisuusjohtamisen osa-alue

Turvallisuusjohtamista koskevaan osa-alueeseen kuuluu organisaation henkilöstöturvallisuuden menettelyt turvallisuusluokiteltujen tietojen suojaamista varten sekä toimiva turvallisuuden hallintajärjestelmä. Turvallisuusjohtamisen osa-alueen vaatimuksia ovat muun muassa, että organisaation johto vastaa, turvallisuusperiaatteiden olevan kattavat turvallisuusluokiteltujen tietojen suojaamista varten ja että organisaatiossa valvotaan riittävästi ohjeiden noudattamista.
Organisaatiossa on hyvin tärkeää arvioida turvallisuusluokiteltuihin tietoihin kohdistuvia riskejä ja toteuttaa riskiarviointiin perustuvat tietoturvallisuustoimenpiteet. Viranomaisten tietojenhallintaa koskeva lakisääteinen vaatimus on, että salassa pidettävää tietosisältöä sisältävät aineistot ja asiakirjat pitää varustaa turvallisuusluokkaa vastaavalla merkillä. Jos henkilön tarvitsee työtehtävissä käsitellä turvallisuusluokiteltua materiaalia, hänen luotettavuutensa selvitetään tekemällä hänelle asianmukainen turvallisuusselvitys, sekä henkilön on annettava vakuutus tietojen suojaamista koskevasta vastuustaan. (Katakri 2020.)

3.2.2 Fyysisen turvallisuuden osa-alue

Fyysinen turvallisuus tarkoittaa turvatoimien toteuttamista teknisten ja fyysisten toimien osalta niin, että pystytään estämään muun muassa turvallisuusluokiteltuihin tietoihin luvaton pääsy. Fyysisen turvallisuuden toimenpiteillä voidaan arvioida turvallisuusluokitellun tiedon suojaamisen

vahvuutta. Fyysisen turvallisuuden osa-alueen vaatimuksiin kuuluu muun muassa se, että tietoaineistoa säilytetään ja käsitellään sellaisissa toimitiloissa missä sen eheyteen, saatavuuteen ja luottamuksellisuuteen liittyvät vaatimukset voidaan toteuttaa riittävän turvallisesti. Toimitilojen osalta fyysisten turvallisuusvaatimusten määrittely on oltava osana toimitilojen rakenteita ja suunnittelua. Turvallisuusluokiteltujen tietojen suojaamista varten on fyysisesti suojattuja turvallisuusalueita kuten turva-alueita ja hallinnollisia-alueita. Hallinnollinen alue on normaalissa työskentelyssä käytettävät tilat, kuten toimistotilan. Turva-alue on hallinnollisen alueen sisällä olevat tarkemmin suojatut alueet ja tilat, näissä tiloissa kuuluu säilyttää ja käsitellä turvallisuusluokiteltua tietoa. Fyysisen turvallisuuden riskien arviointi pitää toteuttaa säännöllisin väliajoin. Tällaisessa riskiarvioinnissa pitää käydä läpi turva-alueiden turvatoimet sekä suojauksen tehokkuus. Turvallisuusluokiteltuja tietoja on tärkeä käsitellä niin, että pääsy turvallisuusluokiteltuihin tietoihin on estetty sivullisilta, joilla ei ole tarvetta saada kyseistä tietoa tai laiton tiedustelu on estetty. Turvallisuusluokiteltujen tietojen säilytys ja käsittely tehdään pääsääntöisesti turvallisuusalueilla. Satunnaisesti tietoja voidaan käsitellä myös turva-alueiden ulkopuolella sekä jossain määrin etätöissä. Kansallisten ja kansainvälisten turvallisuusluokiteltujen tietojen käsittely on turva-alueiden sisällä sekä niiden ulkopuolella toteutettava niin, että pääsy kyseisiin tietoihin on suojattu sivullisilta. (Katakri 2020.)

3.2.3 Teknisen tietoturvallisuuden osa-alue

Teknisen tietoturvallisuuden osa-alueen vaatimukset kuvaavat turvallisuusjärjestelyiden riittävyyden viranomaisten turvallisuusluokiteltujen tietojen käsittelyä varten sähköisessä käyttöympäristössä. Vaatimuksiin kuuluu tietojärjestelmä- tietoliikenne- ja käyttöturvallisuuden osiot. Asiakokonaisuuksiin kuten langattomat verkot, etäkäyttö, hallintayhteydet ja varmuuskopiointi on määritetty niiden vaatimukset. Jotta organisaatio saa toimivaltaiselta viranomaiselta myöntävän hyväksynnän tietojärjestelmälle, on organisaation suojausten oltava riittäviä organisaation ja toimivaltaisen viranomaisen riskiarviointiin nähden. Kun uusia rajapintoja tai palveluja lisätään vanhaan tietojenkäsittely-ympäristöön, se voi tuoda mahdollisesti riskejä tietoturvaan. Riskien pienentämiseksi on hyvä tehdä muutoksia turvallisuuden ylläpitämisen toimiin sekä vanhaan tietojenkäsittely-ympäristöön. (Katakri 2020.)

3.2.4 Yritysturvallisuusselvitys

Yhtenä Katakrin osana on myös yritysturvallisuusselvitykset, jotka määräytyvät turvallisuusselvityslaista (L 726/2014). Tähän selvitykseen kuuluu muun muassa se, että toimivaltainen viranomainen tarkistaa vastuuhenkilöt henkilöturvallisuusselvityksellä. Tällä prosessilla saadaan vältettyä asiattomien pääsyä tiloihin sekä turvallisuusluokiteltuihin tietoihin. Yritysturvallisuusselvityksessä voidaan käyttää Katakria apuna, kun arvioidaan mitä tiloihin ja tietojärjestelmiin kohdistuvia järjestelyjä tarvitaan. Esimerkiksi turvallisuusluokitellun tiedon suojaamiseksi on syytä ottaa turvallisuusjohtamisen, fyysisen turvallisuuden ja teknisen tietoturvallisuuden osa-alueet huomioon Katakrista. (Katakri 2020.)

3.2.5 Tietojärjestelmien ja turvallisuuden arviointi

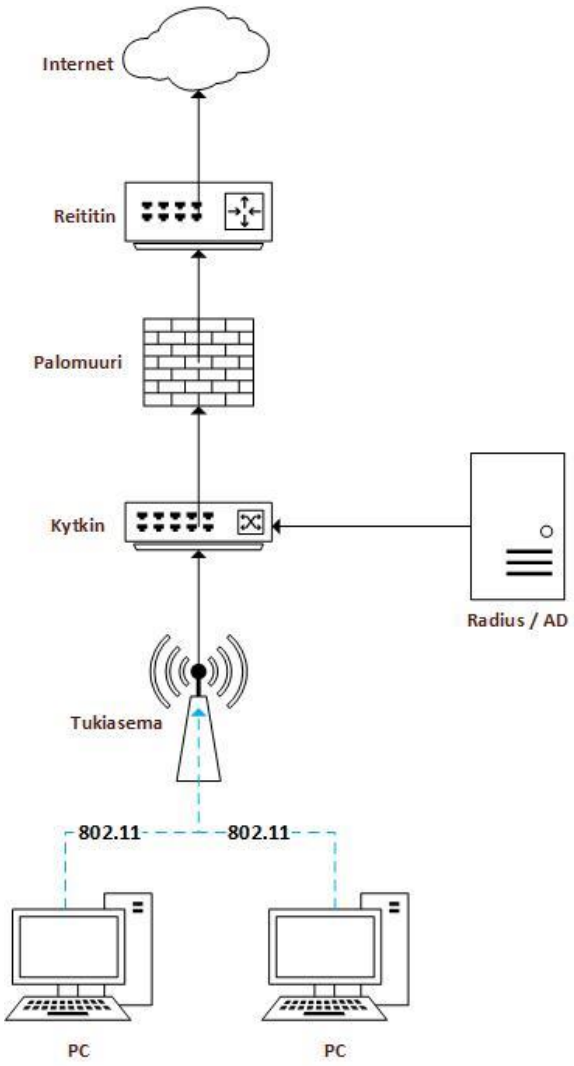
Tietoturvallisuuden arvioinnissa otetaan huomioon tietojärjestelmät ja tietoliikennejärjestelyt. Katakria käytetään tässä arvioidessa tietoturvallisuuden suojausvaatimuksien täyttymistä tietojärjestelmissä ja tietoliikenteen järjestelyissä. Katakrin turvallisuusmalli koostuu vähimmäissuojauksista, jotka auttavat pienentämään riskejä mitkä kohdistuvat turvallisuusluokiteltuihin tietoihin. Riskiperusteet tulevat yleisistä turvallisuusluokiteltuun kohdistuvista riskeistä ja käyttöympäristön riskeistä. (Katakri 2020.)

3.3 Langaton tiedonsiirto

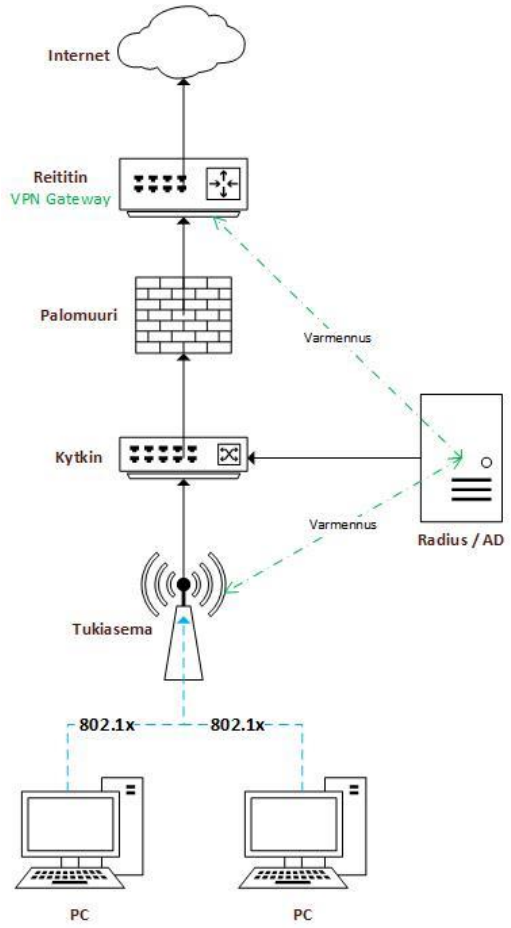
Langattomalla tiedonsiirrolla tarkoitetaan kaikkea tiedonsiirtoa mikä tapahtuu langattomasti kuten matkapuhelinverkot ja langattomat lähiverkot. WLAN (Wireless Local Area Network) verkolla tarkoitetaan paikallista langatonta lähiverkkoa, jossa esimerkiksi laite ottaa yhteyden WLAN-tukiasemaan. (Korowajczuk 2011.) Tässä opinnäytetyössä keskitytään WLAN-verkon ratkaisuun ja siihen liittyviin Katakrin Turvallisuusluokan IV vaatimuksiin. Tässä luvussa esitellään langattomaan tiedonsiirtoon liittyviä oleellisia teknisiä ratkaisuja mitkä liittymät Katakrin tuomiin vaatimuksiin, kuten millaiset ovat laitteiden tunnistusvaatimukset langattomassa verkossa. (Katakri 2020.)

3.3.1 Langattomat verkot

Langattomassa lähiverkossa laitteet pystyvät toteuttamaan tiedonsiirron keskenään käyttäen radioaaltoja siirtovälineenä. Langattoman lähiverkon käyttäjät pystyvät yhdistämään laitteita toimipaikan WLAN-tukiasemia käyttäen lähiverkkoon. (Harte 2004.) RADIUS-palvelimen (Remote Authentication Dial In User Service) ja AD-palvelimen (Active Directory), avulla mahdollistetaan käyttäjien ja laitteiden tunnistautuminen langattomaan verkkoon (Wrightson 2012.). WLAN-verkon topologia yrityksissä on kuvattu yleisellä tasolla ilman salausratkaisua (ks. kuvio 1) ja salausratkaisulla (ks. kuvio 2).



Kuvio 1 Yleinen yrityksen WLAN-verkko



Kuvio 2 Yleinen yrityksen WLAN-verkko VPN-salausratkaisulla

3.3.2 Laitteiden tunnistaminen lähiverkossa

Pääsyoikeuksien hallintaan kuuluu myös laitetunnistus, joka toteutetaan 802.1x avulla. 802.1x avulla voidaan antaa tietylle laitteelle pääsy yrityksen verkkoon tai vierailijaverkkoon, kun laite yhdistetään verkkoon. 802.1x port-based authentication, eli porttikohtainen todentaminen toimii niin että käyttäjän ja laitteen antamilla tunnistustiedoilla tarkastetaan, onko käyttäjällä oikeutta verkon käyttämiseen. Langattoman verkon laitteen todennuksessa EAP (Extensible Authentication Protocol) todennusmenetelmä on erinomainen laitteen yhdistäessä verkkoon. Kun 802.1X-todennustekniikkaa käytetään langattomassa tai langallisessa verkossa, tietoturvamekanismina täytyy päättää mitä EAP-menetelmää käytetään. (Geier 2008.) EAP-menetelmiä on listattu IANA (Internet Assigned Numbers Authority) omalle listalle (IANA 2022.). EAP varmistaa laitteen heti, kun laite kytketään verkkoon, jotta voidaan varmistua, että verkkoon pääsee vain sinne halutut laitteet esimerkiksi tulostusverkkoon tulostimet ja työasemat työasemaverkkoon. Todentamisessa voidaan käyttää muun muassa käyttäjätunnusta ja salasanaa, salausavainta, sertifikaattia tai laitteen MAC

(Media Access Control) osoitetta. (Geier 2008.) Laitetunnistuksessa myös voidaan tehdä niin, että laite ei pääse ollenkaan toimipisteen lähiverkkoon vaan pelkästään internettiin. 802.1x käytetään toimipisteen lähiverkon pääsyn hallinnassa, jos siellä on esimerkiksi asiakkaita tai vierailijoita käymässä erilaisissa tilaisuuksissa, jossa heidän pitää päästä internettiin käsiksi langallisesti tai langattomasti. (Geier 2008.)

3.3.3 Sertifikaatit

Pääsyoikeuksien hallintaan kuuluu käyttäjän tai laitteen tunnistaminen. Se tapahtuu yleensä sertifikaattia käyttäen. Sertifikaatin myöntää sertifikaattien hallinnoija eli CA (Certificate Authority). CA voi olla luotettu ulkoinen palveluntarjoaja tai voidaan käyttää omaa sisäistä CA palvelua. Oikein rakennettu sisäinen CA on luotettava ja käyttökelpoinen ratkaisu, kun sertifikaatti tarve on suuri. Tällöin tulee huolehtia siitä, että sertifikaatin alkuperä voidaan varmistaa riittävän luotettavasti myös oman verkon ulkopuolelle tarjottavissa palveluissa tai käyttää niissä ulkoisen palveluntarjoajan sertifikaatteja. On myös olemassa palvelun itse itselleen määrittelemä tunnistus sertifikaatti eli self-signed certificate, joka ei noudata tunnistettavuudeltaan jäljitettävyys periaatetta, koska se ei perustu luotettavaan juurisertifikaattiin. Sertifikaatin yleisesti suositeltu minimi koko on 2048-bittiä, jota tukevat yleisimmät selaimet ja sovellukset. Turvallisuussertifikaatti voi olla myös 4096-bittinen, mutta sitä eivät kaikki sovellukset tue ja se saattaa hidastaa palvelua. Sertifikaattien päivittäminen on tärkeää, jotta pääsy oikeus palveluun ei lakkaa. (Katakri 2020.)

3.3.4 AD CS

AD CS (Active Directory Certificate Services) toimii digitaalisten sertifikaattien myöntämisen ja hallinnan palveluna. AD CS:n tarjoamia digitaalisia sertifikaatteja voidaan käyttää käyttäjä-, tietokone- ja laitetilien todentamiseen verkossa, tai asiakirjojen ja viestien salaamiseen. Todennettaville tileille voidaan myös asentaa yksilölliset avaimet parantamaan turvallisuutta. Sovellukset mitkä tukevat AD CS ovat esimerkiksi VPN, suojatut langattomat verkot, SSL (Secure Sockets Layer) / TLS (Transport Layer Security) ja IPsec (Internet Protocol Security). (AD CS 2022.)

3.3.5 SSL/TLS

SSL/TLS on protokolla, jonka avulla voidaan tehdä turvallinen verkon liikenne salaamalla verkon viestintää kahden laitteen välillä. Salatulle verkkoliikenteelle oleellista on luottamuksellisuus,

eheys ja todennus. SSL/TLS protokollassa luottamuksellisuus toteutetaan salausalgoritmin avulla, mitä käytettään palvelimen ja käyttäjän välisessä sovellustietojen salauksessa käyttäen kirjoitusavainta, jonka avulla vastaanottaja voi purkaa salauksen. Eheys varmennetaan palvelimen ja käyttäjän MAC avaimia vertaillen. Todennus tehdään käyttäen sertifikaatteja, jotta voidaan varmistua käyttäjien ja laitteiden tunnistamisesta. (Aditya & Prasoon 2015.) Salauksen toteutuksessa oleellinen asia on miten palvelimen tietoliikennesalaus saadaan hyödyntämään turvallisia salainalgoritmeja ja mahdollisesti poistetaan heikot salaimet käytöstä. TLS 1.2 tuntee noin 40 salainta, joista kaikki eivät kuitenkaan ole enää luokiteltu turvalliseksi. TLS 1.3:ssa salaimia on vain viisi ja TLS 1.3 salaimet ovat toistaiseksi kaikki turvallisia. Kaikki TLS 1.3 salaimet ja TLS 1.2 salaimista useimmat täyttävät Traficomin kryptografiset vaatimukset. (Kryptografiset vaatimukset 2021.)

3.4 Langattoman verkon salausratkaisut

Verkkoliikenteen salauksessa voidaan käyttää esimerkiksi VPN-salausratkaisua salaamaan tiedonsiirtoa kahden laitteen välillä jaetun tai julkisen verkon kautta. Tiedonsiirron yhteydessä varmistetaan tiedon muuttumattomuus tarkastussummin ja salauksella estetään sivullisen pääsy tiedonsiirto tunneliin. Tiedonsiirrossa tieto salataan salausavaimia käyttäen ja kyseiseen tietoon pääsee käsiksi ainoastaan niitä salausavaimia käyttäen. Salausavainten kryptografinen vahvuus tuo tiedolle mitä salataan luottamuksellisuutta siitä, että kyseinen tieto turvataan riittävän hyvin. Kryptografisella vahvuudella tarkoitetaan vahvuutta vastustaa kryptoanalyysiä. Tietoliikenne- ja tietoturvaprotokollia käyttäessä on tärkeää käyttää uusinta, vakaata versiota, jotta tiedon turvallisuus on ajan tasalla, sekä kyseiset vakaat versiot ovat viestintäviraston suosittelemia ja tämä otetaan huomioon salaustuotteenarvioinnissa. (Tiller 2000.) Salausratkaisu on ainoa vaihtoehto suojata turvallisuusluokiteltua tietoa käyttäessä julkista tai muuta matalamman turvallisuusluokan verkkoa. Tämän takia on hyvin tärkeä kiinnittää erityistä huomiota turvalliseen käyttötapaan sekä salausratkaisun valintaan. Salausratkaisun valinnassa on tärkeää huomioida erilaiset riskit esimerkiksi käsiteltäessä viranomaisten turvallisuusluokiteltua tietoa mikä on suojattava yleensä valtion turvallisuuden näkökulmasta. Salausratkaisua valittaessa on erityisen tärkeää turvallisuusluokitellun tiedon suojaamisen kannalta, nähdä riittävä määrä luotettavaa näyttöä turvallisuudesta. On myös syytä huomioida salausvahvuus ja käyttöympäristön uhkataso. Uhkatasot eroavat hyvin paljon tilannekohtaisesti, esimerkiksi jos liikennöidään Internetin yli, verrattuna jos liikennöidään hallitun fyysisesti suojatun alueen sisällä. Myös salausratkaisun lähdekoodin tarkastus voi olla hyvin oleellinen tarkistaa, jotta saadaan mahdollinen peukalointi estettyä. (Katakri 2020.)

VPN-salausratkaisussa käytettäviä tunnelointiprotokollia ovat SSL- ja IPsec-protokolla. SSL- ja IPsecVPN eroavaisuuksia on esimerkiksi, että SSLVPN on ainoastaan etäyhteys, kun taas IPsecVPN tukee etäyhteyttä ja Site-to-Site yhteyttä. IPsecVPN:n avulla saadaan tunnistettua ja salattua kommunikaation paketit esimerkiksi kahden tietokoneen välillä ja yhdistettyä joko hosteja tai jopa kokonaisia verkkoja toisiinsa. SSLVPN:n avulla saadaan salattua linkki palvelimen ja verkkosivun, selaimen tai sähköpostipalvelimen välillä, eli yhdistetään vain käyttäjiä ohjelmiin tai palveluihin. (Tiller 2000.)

3.4.1 WEP ja WPA salausmenetelmät

WEP (Wired Equivalent Privacy) salauksessa käytetään jaettua avainta, tarkistamaan käyttäjien pääsyä langattomaan verkkoon. Tämä todennus tapahtuu tukiaseman ja käyttäjän välillä, jossa tukiasema vertaa täsmääkö WEP-avaimella salatut arvot keskenään. WEP-todennus ei ole turvallinen nykypäivänä, koska jaetun avaimen todennuksella on tietoturvahaavoittuvuus. Tämä koskee salauksen toiminnan yksinkertaisuutta ja verkko haistelulla helposti selville saatavia arvojen takia. (Wrightson 2012.)

WPA2 (Wi-Fi Protected Access) on salausmenetelmä, jossa käytetään AES (Advanced Encryption Standard) salausstandardia, jonka NIST (National Institute of Standards and Technology) on hyväksynyt. AES on lohkosalausmenetelmä, jossa lohkojen koko on 128 bittiä, mutta sillä voi olla kolme eri avaimenpituutta 128-, 192- ja 256-bittiä (FIPS PUBS 2001.). WPA salauksessa käytetään RADIUS-palvelinta, jonka avulla mahdollistetaan käyttäjien tunnistautuminen langattomaan verkkoon. WPA2 salauksessa voidaan käyttää WPA-PSK (Pre Shared Key) avaintenhallinta tekniikkaa, jossa tukiasemille annetaan salasana, mitä käytetään salattujen pakettien purkamisessa. (Wrightson 2012.) WPA2 menetelmä täyttää Katakrin asettamat kryptografiset vahvuusvaatimukset, jotka täyttyvät AES-128 lohkosalausmenetelmän käytöstä (Kryptografiset vaatimukset 2021.).

4 Katakrin vaatimukset turvallisuusluokan IV tietojen käsittelylle langattoman verkon tiedonsiirrossa

Tässä kappaleessa käydään läpi Katakrin vaatimuksia turvallisuusluokan IV tiedon käsittelylle. Langaton tiedonsiirto luokitellaan julkisen verkon kautta liikennöinniksi. Tästä syystä Katakrin vaatimuksiin kuuluu, että langattomassa tiedonsiirrossa käytetään toimivaltaisen viranomaisen hyväksymää salausratkaisua.

4.1 Verkon rakenteellisen turvallisuuden vaatimukset

Turvallisuusluokalle IV on Katakrissa asetettu vaatimukseksi verkon rakenteelliselle turvallisuudelle, että tietojenkäsittely-ympäristöt missä käsitellään turvallisuusluokan IV tietoa, on syytä erottaa muista verkkoympäristöistä, sekä niiden yhteys muihin turvallisuusluokkiin on syytä suojata palomuuriratkaisulla (L 1101/2019, 11 §). Nämä vaatimukset saadaan toteutettua esimerkiksi käyttämällä verkkoympäristöjen erittelemiseen sisä- ja ulkopalomuureja, sekä segmentoimalla verkot erillisiin VLAN (Virtual Local Area Network) verkkoihin. Turvallisuusluokan IV vaatimuksiin kuuluu myös se että, jos liikenne menee hallitun fyysisen turva-alueen ulkopuolelle, yhteys on salattava salausratkaisulla minkä toimivaltainen viranomainen hyväksyt. (L 1101/2019, 12 § ja 11 § ja L 906/2019, 14 §)

Tietojenkäsittely-ympäristöjen erottelu on hyvin tärkeä osa turvallisuusluokiteltujen tietojen suojaamisessa. Erottelu mahdollistaa tiedonkäsittelyn riittävän turvallisissa ympäristöissä ja käsittely-ympäristön hallinta helpottuu. Korkeamman turvallisuusluokan ympäristöissä on sallittua käsitellä matalamman turvaluokituksen materiaalia. Organisaation toimipisteiden tietojenkäsittely-ympäristöt, jotka on luokiteltu samalle turvallisuusluokalle, voidaan yhdistää toimivaltaisen viranomaisen hyväksymällä salausratkaisulla. Kun turvallisuusluokan IV tietojenkäsittely-ympäristö yhdistetään Internettiin tai ei luotettuihin verkkoihin, on käsittely-ympäristöä suojattava esimerkiksi vähentämällä riskejä verkossa ottamalla huomioon erilaiset asiat, kuten poikkeuksien havainnointi ja korjaaminen, käyttämällä vähimpien oikeuksien periaatetta käyttöoikeushallinnassa, järjestelmänkovennukset ja ohjelmistopäivitykset. (Katakri 2020.)

4.2 Tietoliikenne-verkon vyöhykkeistäminen ja suodatussäännöstöt

Tietoliikenneverkolle Katakrin asettamiin vaatimuksiin kuuluu turvallisuusluokan sisällä verkon vyöhykkeistäminen erillisiin verkkoalueisiin tietojen suojaamista varten. Näihin pienempiin turvallisuusluokkien verkkoalueisiin on syytä käyttää vähimpien oikeuksien periaatetta mikä tarkoittaa sitä, että sallitaan vain tarpeelliset yhteydet lähde ja kohde kohtaisesti. Myös palomuurin tietokantaa on syytä käydä säännöllisesti läpi ja poistaa turhia ja käytöstä poistuneiden yhteyksien avauksia, sekä avauksien ylimääräisiä protokollia. (L 1101/2019, 7 § ja 11 §) Verkkohyökkäyksiin varautuminen on hyvin tärkeää, joten hyvän tietoturvan saamiseksi on syytä käsitellä kaikkia tietotekniikanjärjestelmiä epäluotettavina, jotta saadaan suojattua tietoverkkoa mahdollisilta hyökkäyksiltä mahdollisimman hyvin.

4.3 Verkkojen hallinnointi ja hallintayhteyksien vaatimukset

Katakri asettaa myös vaatimuksia verkon hallintayhteyksien turvallisuuteen liittyviin asioihin. Kun hallinnoidaan turvallisuusluokan IV verkkoa, pitää hallintayhteyksien täyttää Katakrin turvallisuusluokan IV salausvaatimukset. Hallintayhteydet on syytä olla rajattuja pääsyiltään ja oikeuksiltaan vain tarvittaviin asioihin, myös käyttäjät on oltava tunnistettuja ja yhteyksien istunnot on syytä olla aikarajoitettuja. Hallintayhteys oikeuksia antaessa, on syytä ottaa huomioon myös, kuinka monella on syytä päästä tietoihin käsiksi. (L 1101/2019, 12 § ja 11 § ja L 906/2019, 14 §) Verkon ja sen valvota- ja suodatusjärjestelmien tarkastusta ja dokumentaatiota ylläpidetään säännöllisin väliajoin esimerkiksi vuosineljänneksittäin tai puolivuosittain. Kyseiset dokumentaatiot tulee olla riittävän tarkkoja, että niiden pohjalta voidaan verkkoalueiden rakenteellinen auditointi tehdä asetettuja vaatimuksia vasten. (L 1101/2019, 11 § ja L 906/2019, 13 §)

4.4 Langattoman verkon tietojenkäsittely-ympäristön pääsyoikeusvaatimukset

Katakrin vaatimukset pääsyoikeuksien hallinnalle on, että pääsyoikeudet annetaan vain henkilöille, joiden käsittelyoikeudet on todennettavissa esimerkiksi jonkin sopimuksen avulla. Tarpeettomat käyttäjätunnukset on syytä poistaa heti, kun esimerkiksi käyttäjä lopettaa työt organisaatiossa. Myös käyttäjien pääsyoikeuksia pitää katselmoida säännöllisesti kuten 6 kuukauden välein. Käyttäjien oikeuksia on syytä hallita niin, että käyttäjällä ei ole tarpeettoman laajoja oikeuksia erilaisiin järjestelmiin ja käyttöoikeusien hallintaan on nimetty vastuuhenkilö(t). (L 1101/2019, 8 § ja 11 §, L 906/2019, 16 §)

Tietojenkäsittely-ympäristön laitteille, henkilöille ja tietojärjestelmiin on oltava käytössä luotettava tunnistautuminen ja todentaminen. Käyttäjän tunnistaminen ja todennus on toteutettava yksilöllisillä henkilökohtaisilla käyttäjätunnisteilla, sekä turvallisella tekniikalla, kuten hyödyntäen 802.1x standardin mukaista todennus- ja avaintenhallintamekanismia. Tunnistuksessa on syytä käyttää myös suojaavia menetelmiä, kuten jos tunnistus epäonnistuu liian monta kertaa, tunnus on syytä lukita väliaikaisesti. Todennuksen minimivaatimus on, että käytetään salasanaa. Tunnuksien salasanan vahvuusvaatimukseksi on määritetty Katakrissa 15 merkkiä, salasanan vaihto on myös syytä tehdä säännöllisin väliajoin. Tietojärjestelmien välisen tiedonsiirron tunnistautuminen on tehtävä salattuja yhteyksiä pitkin ja käyttäen salasana- tai avaintekniikkaa. Tunnistuksessa on syytä suojautua erilaisilta hyökkäyksiä kuten välimieshyökkäyksiä, uudelleenlähetyshyökkäyksiä ja väsytyshyökkäystä vastaan. Langattoman lähiverkon verkkotunnuksen SSID (Service Set Identifier) lähetys on pidettävä pois päältä, jolla saadaan vähän parempaa tietoturvaa jakamalla ne verkkoasetuksina vain tarpeellisille laitteille. (L 1101/2019, 11 §)

4.5 Langattoman verkon salausratkaisun vaatimukset

Katakrin asettama vaatimus langattoman verkon tiedonsiirtoon on se, että tiedonsiirtoyhteys pitää salata viranomaisen hyväksymällä salausratkaisulla, koska langaton tiedonsiirto luokitellaan julkisen verkon kautta liikennöinniksi (L 1101/2019, 12 § ja L 906/2019, 14 §). Katakrin vaatimuksiin kuuluu, että käytettävä salausratkaisu on viranomaisen hyväksymä tietylle salaustasolle, jotta saadaan salassa pidettävät tiedot turvattua luvattoman paljastumisen tai muuntelun estämiseksi. Salaustuotteenarviointi- ja hyväksyntäprosessi kuuluu vaatimuksiin, jotta saadaan vaatimuksia täyttävä salausratkaisutoteutettua. Salaiset avaimet on oltava vain käyttäjien ja prosessin käytössä, jotka on valtuutettu. Avainten on oltava kryptografisesti vahvoja, myös avaintenjakelu ja säilytys on toteutettava turvallisesti. Avaimia tulee myös vaihtaa säännöllisin väliajoin. (L 1101/2019, 11 §) Langattoman verkon tiedonsiirrossa on tärkeää toteuttaa vastaanottajan tunnistus tai varmistus tietoturvallisesti vahvalla tavalla ennen kuin turvallisuusluokiteltuihin tietoihin pääsee käsiksi (L 1101/2019, 12 § ja 11 §, ja L 906/2019, 14 §).

Vähimmäissuositus salausalgoritmiksi on että salauksen toteutuksessa sallitaan vain TLS 1.2 turvallisten salausalgoritmien ja kaikkien TLS 1.3 salainten käyttö yhteyksissä. SSL kaikki versiot on syytä poistaa sekä TLS 1.0 ja 1.1 ottaa pois käytöstä, koska nämä ovat turvattomia. TLS 1.3 on syytä asettaa suositusprotokollaksi ja TLS 1.2 varalle toiseksi vaihtoehdoksi poistaen turvattomat salaimet

käytöstä. Jos yhteys on toimeksiantajan toimistoverkosta turvallisuusluokan IV alueelle, pitää käyttää 2048-bitin sertifikaattia samoin palvelussa, joka on turvallisuusluokan IV alueen sisäistä. Ulkoisista lähteistä turvallisuusluokan IV alueelle kohdistuvassa liikenteessä voidaan harkinnan perusteella käyttää 4096-bitin sertifikaatteja. Turvallisuusluokan IV alueelta turvallisuusluokan III alueelle kohdistuvassa liikenteessä käytetään 4096-bittistä sertifikaatteja ja mahdollisuuksien mukaan TLS 1.3 tiedonsiirtoprotokollaa. Miniminä kaikkiin palveluihin käytetään TLS 1.2 protokollaa turvallisiksi tunnustettuja salaimia käyttäen. Heikoimman turvatason salaimet, on syytä poistaa käytöstä. Turvallisuusluokka IV tuo verkolle avaimen kokoon vaatimukseksi vähintään 2048-bittiä ja kun taas turvallisuusluokalle III 4069-bittiä. (Katakri 2020.)

4.6 Järjestelmäkovennus ja monitasoisen suojaamisen vaatimukset

Käytössä olevien laitteiden ja palveluiden asetuksia on syytä muuttaa niin, että järjestelmien haavoittuvuutta saadaan pienennettyä. Muutettavia asioita on esimerkiksi vaihtaa laitteiden ja palveluiden oletussalasanat, poistaa tarpeettomat ohjelmistot ja käyttäjätilit. Riskien pienentämisen kannalta on syytä ottaa käyttöön vain olennaiset laitteet, palvelut ja toiminnot. (L 1101/2019, 11 § ja L 906/2019, 13 §) Järjestelmäkovennukset, turvallisuuspäivitykset, käyttöoikeusrajaukset ja tietoturvapoikkeamien havainnointi on tärkeä osa järjestelmien suojaamista. Järjestelmissä on syytä aina käyttää vähimpien oikeuksien periaatetta. Myös järjestelmissä on syytä pitää turvallisuuspäivitykset aina ajan tasalla, sekä haittaohjelman torjuntaohjelmat on otettu käyttöön kaikkiin järjestelmiin missä se tuo lisäsuojaa. Järjestelmiä käyttävien henkilöiden tietoturvallisuuden osaamisesta on varmistuttava erilaisten ohjeistuksien avulla. (L 1101/2019, 11 §) Tietojärjestelmien käytöstä ja tietojenluovutuksesta pitää olla lokitietojen keräys päällä, järjestelmien tietojen käytön, luovutuksen seurantaan ja virheidenselvitystä varten. Tietojen on oltava riittävän kattavia tietomurtojen tai niiden yritysten todentamista varten, myös lokitietojen poistamisesta ja muuttamisesta on syytä saada havainto lokitietoihin. (L 906/2019, 17 § ja 15 § ja L 1101/2019, 7 §) Verkkoliikenteen poikkeamien havainnointikyky on tärkeää verkon suojaamisessa. Vaatimuksiin kuuluu, että verkon liikenteen normaalista tilasta eroavat tapahtumat havaitaan esimerkiksi yhteyksien, protokollien ja liikennemäärien osalta. Poikkeamatilanteissa on pyrittävä rajoittamaan esimerkiksi hyökkäyksien vaikutukset niin pieneen osaan tietoja kuin mahdollista ja estämään vahingot. Tietojenkäsittely-ympäristöt on syytä olla mahdollista palauttaa suojattuun tilanteeseen mahdollisimman nopeasti. (L 906/2019, 13 § ja 17 § ja L 1101/2019, 7 §)

5 Salausratkaisun arviointi- ja hyväksyntäprosessi

Salausratkaisua valittaessa langattomalle verkolle on salausratkaisun läpäistävä salausratkaisun arviointi- ja hyväksyntäprosessi. Salaustuotteet arvioi ja hyväksyy EU:n jäsenmaiden oma kansallinen salaustuotteiden hyväksyntäviranomainen CAA (Crypto Approval Authority). Salaustuotteiden hyväksyntäviranomaisena Suomessa toimii liikenne- ja viestintävirasto Traficom. Arviointi- ja hyväksyntäprosessin tilaaja organisaatio laittaa prosessin aluilleen ja Traficom suorittaa salaustuotteen arviointi- ja hyväksyntäprosessin yhdessä tilaaja organisaation kanssa, prosessi sisältää tilaajaorganisaatiolta vaadittavia ehtoja salausratkaisuun liittyen. Tietoturvallisuusarvioinnit ja -hyväksynnät mitä Traficom suorittaa edellyttää prosessin tilaajaorganisaatiolta perusteltua tarvetta käsitellä kyseisessä salaustuotteessa turvallisuusluokiteltua tietoa. (Salaustuotearvioinnit ja -hyväksynnät 2020.) Arviointi- ja hyväksyntäprosessista peritään tilaajaorganisaatiolta maksu, maksun suuruus perustuu käytettyyn työmäärään (L 588/2004).

5.1 Arviointi- ja hyväksyntäpyyntö

Arviointi- ja hyväksyntäpyyntö suositellaan lähetettäväksi Traficomin käsiteltäväksi vasta kun uskotaan että salaustuote vastaa Katakrin vaatimuksia (Salaustuotearvioinnit ja -hyväksynnät 2020.). Traficom on tehnyt pyyntöön esitäytetyn lomakkeen, mikä on saatavilla Traficomin sivuilta (NCSA-tarkastelupyyntölomake 2020.).

Traficomin arviointi- ja hyväksyntäprosessipyynnöstä pitää saada seuraavat asiat selville. Arvioitavan- ja hyväksyttävän salaustuotteen nimi, käyttöönottopäivä, omistaja, rakentaja ja ylläpitäjä, yhteyshenkilön tiedot, lyhyt selitys salaustuotteesta ja sen laajuudesta, tieto siitä käsitteleekö salattavassa järjestelmässä salassa pidettävää tietoa ja jos käsitellään niin kuinka korkeaa turvallisuusluokkaa, salaustuotteen tämänhetkinen tila onko se tällä hetkellä suunnitteilla tai rakenteilla, salaustuotteen sisäiset tai ulkoiset vaatimukset, laskutustiedot ja mahdolliset aikaisemmat arvioinnit koskien kyseistä salaustuotetta. (Arviointi- ja hyväksyntäprosessit 2021.)

Kun pyyntö on saapunut Traficomin käsiteltäväksi, tilaajaorganisaatio saa vastauksen pyyntöön neljän viikon sisällä. Traficomin vastauksesta selviää seuraavat vaiheet arviointi- ja hyväksyntäprosessille, esimerkiksi ehdotus esipalaverin ajankohdalle ja siihen vaadittavat dokumentit. Mikäli

pyynnössä selviää, että arviointi- ja hyväksyntäprosessin aloituksen edellytykset ei vielä täyty, niin pyyntö palautetaan uudelleen täytettäväksi. (Salaustuotearvioinnit ja -hyväksynnät 2020.)

5.1.1 Arviointi- ja hyväksyntäprosessin esipalaveri

Arviointi- ja hyväksyntäprosessin esipalaverissa käydään läpi tilaajaorganisaation ja Traficomin kanssa yleiskuva tarkastettavasta salaustuotteesta ja prosessien käytännön toimien läpikäynti. Traficomille luovutetaan myös arviointi- ja hyväksyntäprosessissa vaativia dokumentteja kuten kuvaus salaustuotteen rakenteesta, mahdolliset aikaisemmat tarkastukset raportteineen ja salaustuotekohtaiset erityisvaatimukset. (Salaustuotearvioinnit ja -hyväksynnät 2020.) Traficomin on mahdollista antaa hyväksyntä vanhojen tarkastuksien perusteella kansallista salassa pidettävää tietoa käsittelevälle salaustuotteelle, mikäli arviointiraporttien tiedot ovat riittävät ja tarvittaessa tekee lisäselvityksiä tietoturvallisuusvaatimuksien osalta (L 1406/2011).

5.1.2 Tarkastuksen valmistelutoimet

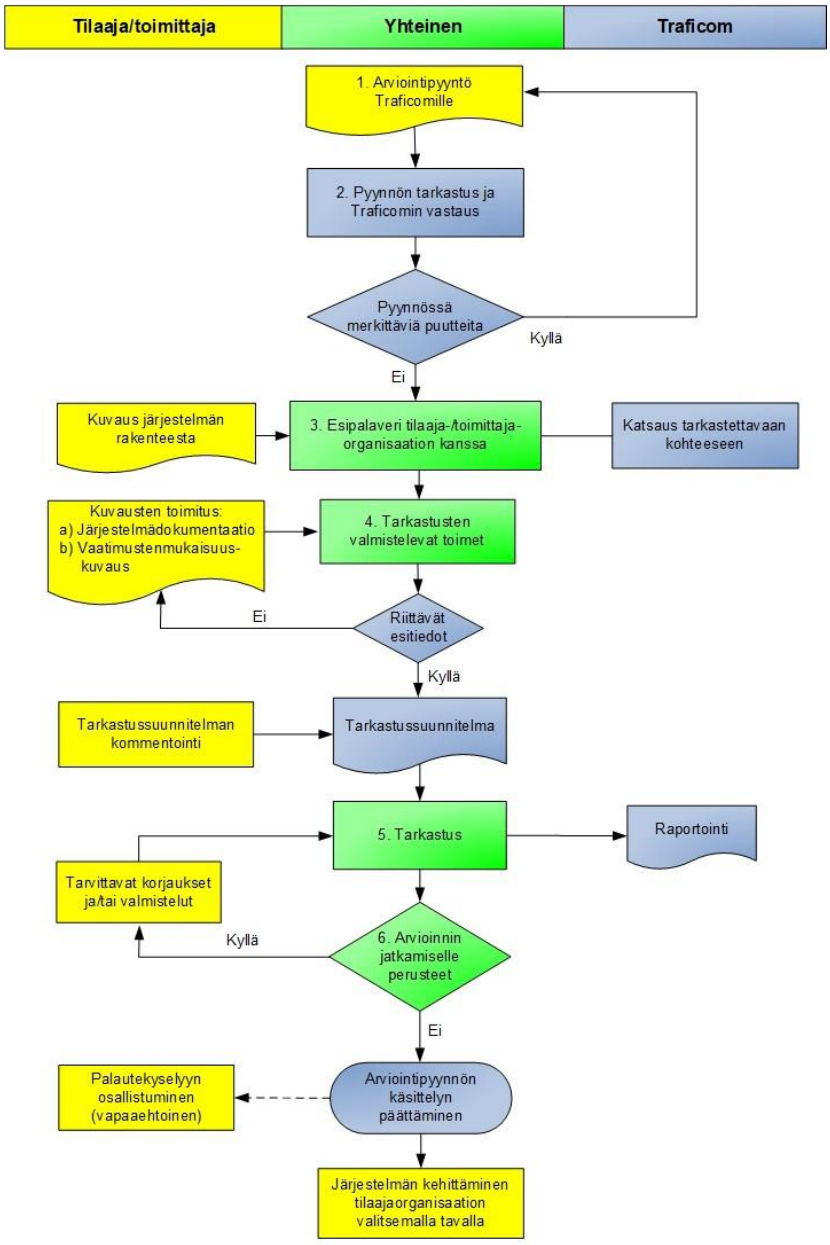
Traficom tekee tarkastusta varten tarkastussuunnitelmaluonnoksen, tähän luonnokseen kuvataan yleisellä tasolla prosessissa läpikäytävän salaustuotteen tarkastamisen asiakokonaisuudet ja aikataulutus tarkastamiselle. Tarkastussuunnitelmaluonnosta varten tarvitaan tilaajaorganisaatiolta salaustuotedokumentaatiosta tarkat tiedot salaustuotteen rakenteesta, suojaamiskäytännöistä ja toimintaperiaatteista, sekä itsearviointi salaustuotteen tämänhetkisestä vaatimustenmukaisuudesta. (Salaustuotearvioinnit ja -hyväksynnät 2020.) Traficom on tehnyt kuvaukseen vaatimustenmukaisuuden nykytilasta esitäytetyn lomakkeen, mikä on saatavilla Traficomin sivuilta (Kuvaus vaatimuksenmukaisuuden nykytilasta 2020.).

5.1.3 Tarkastus

Tarkastusvaiheessa käydään salaustuotteen tietoturvallisuutta läpi ja selvitetään vastaako salaustuotteen tietoturvallisuusvaatimuksia. Tarkastukseen kuuluu hallinnollinen, tekninen ja fyysisen turvallisuuden osuus. Tarkastuksen jälkeen käydään havainnot läpi Traficomin ja tilaajaorganisaation välisessä palaverissa. (Salaustuotearvioinnit ja -hyväksynnät 2020.)

5.2 Salaustuotteen arviointiprosessi

Salaustuotteen arviointiprosessilla tarkoitetaan prosessia, jossa saadaan selville, että salaustuote täyttää siihen kohdistuvat vaatimukset ja sen valmistuttua hyväksyntäviranomainen on antanut virallisen lausunnon siitä, että ne täyttyvät salaustuotteessa. Arviointiprosessi (ks. kuvio 3) kuuluu osaksi hyväksyntäprosessia. (Salaustuotearvioinnit ja -hyväksynnät 2020.) Arviointimenettelyyn kuuluvia asioita on muun muassa viranomaisen järjestelmät, joista on pyydetty Traficomilta arviointipyyntö, myös valtiovarainministeriön pyytämät selvitykset tietoturvallisuudesta viranomaisten tietojärjestelmistä tai tietoliikennejärjestelyistä (L 1406/2011 ja L 10/2015).

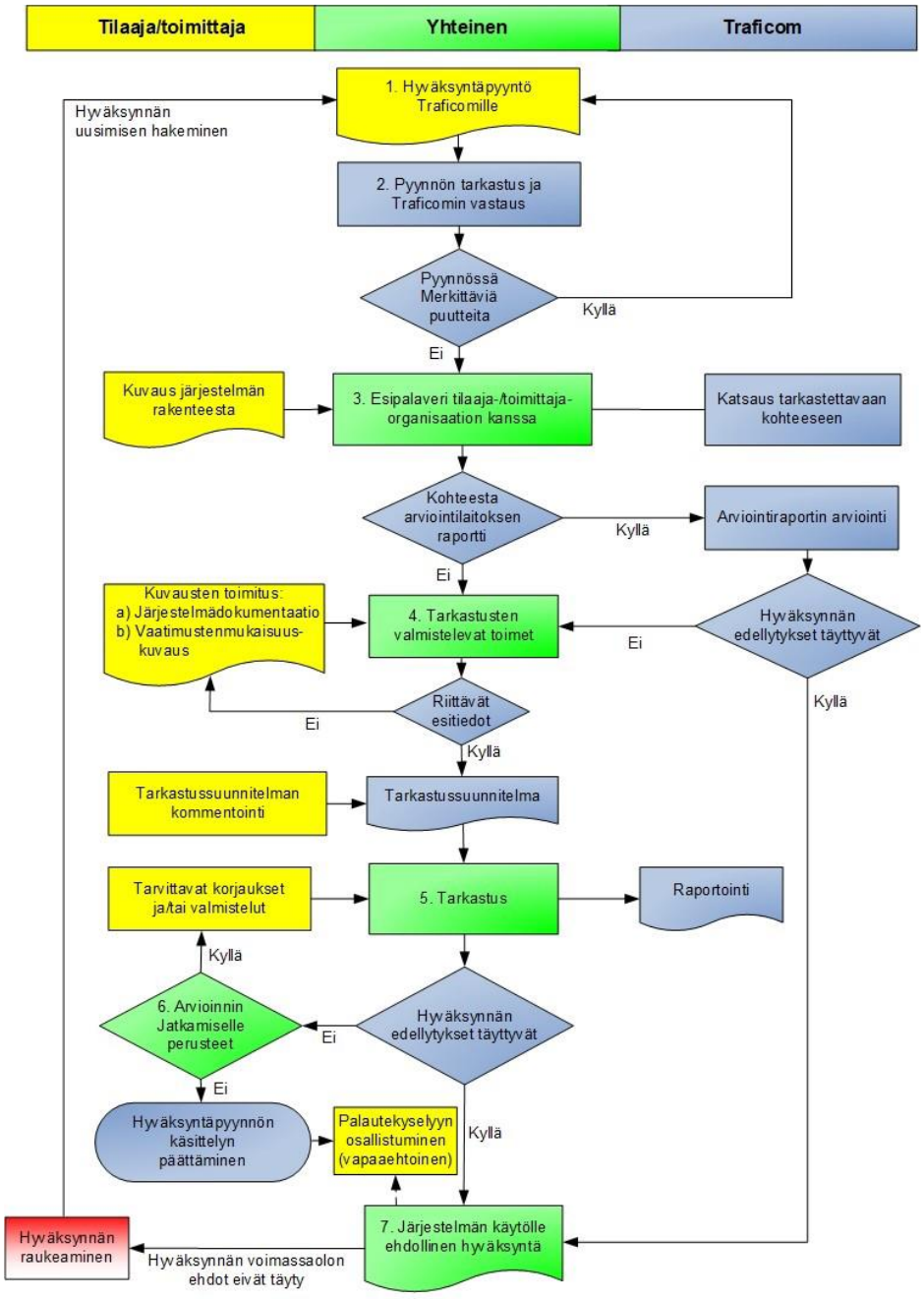


Kuvio 3 Arviointiprosessi (Salaustuotearvioinnit ja -hyväksynnät 2020.)

5.3 Salaustuotteen hyväksyntäprosessi

Salaustuotteen hyväksyntäprosessilla (ks kuvio 4) tarkoitetaan prosessia, jonka valmistuttua hyväksyntäviranomainen antaa virallisen lausunnon, että salaustuote on hyväksytty tietylle turvallisuusluokalle. Hyväksynnän saaminen edellyttää sitä, että hyväksytyt turvatoimet on toteutettu salaustuotetta varten. (Käsittely ohje 2020.) Ohjelmistopohjaiset salausratkaisut turvallisuusluokille, kuten luokalle IV ja myös luokalle III erityisehdoilla, on yleensä hyväksyntäprosessin mukaan hyväksyttävissä. Turvallisuusluokalle II on hyväksyntäprosessissa enemmän vaatimuksia. (Katakri

2020.) Kun salaustuotteita käytetään käsitellessä EU:n turvallisuusluokiteltuja tietoja, tulee salaustuotteen olla hyväksytty EU:n turvallisuussääntöjen 10 artiklan 6 kohdan mukaisesti (2013/488/EU). Hyväksyntämenettelyyn kuuluvia asioita on muun muassa viranomaisten tietojärjestelmät, mistä haetaan todistusta vaatimuksien täyttymisestä. Hyväksyntämenettelyyn kuuluu myös valtionhallinnon toimijoiden tietojärjestelmät, jos kyseisiin tietojärjestelmiin kuuluu kansainvälisiä tietoturvavelvoitteita (L 1406/2011 ja L 588/2004). Hyväksyntäprosessia jatketaan, kunnes hyväksyttävän salaustuotteen vaatimukset on todettu täyttyvän ja kykenee turvallisuuden tason säilyttämiseen. Traficomilta saatu hyväksyntä on voimassa 3 vuotta myöntämisestä, mutta madolliset suureet muutokset järjestelmän turvallisuudelle voi aiheuttaa hyväksynnät raukeamisen. Muutoksia suunnitellessa on huomioitava, että niistä on saatava Traficomin hyväksyntä. (Salaustuotearvioinnit ja -hyväksynnät 2020.)



Kuvio 4 Hyväksyntäprosessi (Salaustuotearvioinnit ja -hyväksynnät 2020.)

5.4 NCSA toiminnon hyväksytyt salausratkaisut

Liikenne- ja viestintävirasto Traficom ylläpitää listaa EU:n neuvoston ja NCSA (National Communications Security Authority) -toiminnon hyväksymistä salaustuotteista, mitkä sopivat turvallisuusluokiteltujen tietojen suojaamiseen EU tasolla ja kansallisella tasolla (Salaustuotearvioinnit ja -hyväksynnät 2020.). Näistä hyväksytyistä salausratkaisuista on olemassa lista Traficomin verkkosivuilla (NCSA salausratkaisut 2022.).

6 Turvallisuusluokka IV langattoman tiedonkäsittelyverkon tutkinta

Turvallisuusluokan IV tietojen käsittelyvaatimuksia langattomalle verkolle läpi käydessä saatiin selville, että langaton tiedonsiirto vaatii salausratkaisun käyttöä, kun tiedonsiirrossa käsitellään turvallisuusluokan IV tietoa. Lisäksi käytiin läpi, kuinka on varmistettava salausratkaisun olevan hyväksytetty Traficomin arviointi- ja hyväksyntäprosessin avulla. NCSA-toiminnon jo hyväksytyt salausratkaisut löytyvät Traficomin sivulta ja ne on hyvä käydä läpi ennen arviointi- ja hyväksyntäprosessin aloitusta. Nämä salaustuotteen vaatimukset ja prosessi tiedot saatiin selville Katakrin vähimmäisvaatimuksista. (Katakri 2020.)

6.1 Muutokset langattoman verkon käyttöön

Katakrin vaatimuksia läpi käydessä saatiin kuva siitä, kuinka toimipisteiden langattomia lähiverkkoja käyttäessä tulee jatkossa käyttää Katakrin vaatimuksia täyttävää salausratkaisua, jotta turvallisuusluokan IV tason tietoa voidaan käsitellä langattomasti ja salausvaatimukset täyttyvät. Traficomin salaustuotteen arviointi- ja hyväksyntäprosessin läpäisemällä salaustuotteella voidaan toteuttaa tämä. Esimerkiksi VPN-salausratkaisu, joka on läpäissyt arviointi- ja hyväksyntäprosessin, mahdollistaa tietoliikenteen salauksen myös langattomalta osuudelta sekä lisää verkon yleistä tietoturvallisuutta. Kun toimipisteen langattomaan verkkoon yhdistetään laite, pitää käyttää VPN-salausratkaisua sekä pyytää käyttäjiä käynnistämään ja kirjautumaan VPN-ohjelmistolla organisaation AD-tunnistuksella, jotta pääsynhallinta ja salaus saadaan toteutettua. Pääsynhallinnalla mahdollistetaan yksilöidyillä käyttäjätunnuksilla oikeuksien rajaus ja pääsy vain tarvittaviin järjestelmiin. Käyttäjien ja laitteiden todennus voidaan tehdä käyttäen 802.1x standardin mukaista todennus- ja avaintenhallintamekanismia verkkoon liittyessä. Muutoksen myötä toimipisteen langattomasta verkosta pääsisi ilman VPN-yhteyttä ainoastaan internettiin eikä organisaation järjestelmiin.

6.2 VPN-salausratkaisun käyttökokemus

Toimipisteiden langattomia lähiverkkoja käyttäessä on asetettava VPN-salausratkaisu pakolliseksi, jotta verkon salaaminen saataisiin toteutettua turvallisuusluokan IV-tasolle. Pakotettu VPN-salausratkaisu langatonta verkkoa käyttäessä tuo mahdollisesti loppukäyttäjälle haasteita eritilanteissa kuten telakkalaitetta käyttäessä. Kun laite kiinnitetään telakkaan, niin tulee laite vaihtaa

käyttämään langallista yhteyttä erikseen. Tässä tilanteessa käyttäjän on syytä katkaista yhteys langattomasta verkosta. Myös kun laite irrotetaan telakasta, laite yhdistää langattomaan verkkoon automaattisesti, mutta täytyy manuaalisesti kirjautua VPN-salausratkaisun avulla.

Mahdollisia haasteita tuo myös VPN-ratkaisun käyttö etätöissä verrattuna toimipisteellä, jossa mahdollinen turva-alue mahdollistaa pääsyn järjestelmiin, joiden käyttö etätyössä ei ole sallittua. Langattoman lähiverkon käyttäjää on opastettava VPN salausratkaisun käytössä ohjeella, jossa kerrotaan muun muassa seuraavat asiat:

- Mitä tehdään, kun käytetään telakkaa ja/tai Ethernet-kaapelia lähiverkossa.
- Kuinka VPN yhteys laitetaan päälle.
- Kuinka VPN sovelluksen käyttäjätunnistus tehdään.
- Kerrotaan mihin käyttäjä ei pääse, jos VPN salausratkaisu ei ole käytössä.
- Mitä tehdä erilaisissa ongelmatilanteissa.

7 Tulokset

Opinnäytetyön lopputuloksena saatiin vastaus siihen, mitkä ovat Katakrin tuomat vähimmäisvaatimukset turvallisuusluokan IV tiedon käsittelylle langattomassa tiedonsiirrossa. Luvuissa 6.1 ja 6.2 käydään läpi, kuinka muutoksen jälkeen esimerkiksi VPN-salausratkaisu yleisellä tasolla toteutuksena toimii ja millainen on käyttökokemus loppukäyttäjille organisaatiossa. Tarkemmin VPN-salausratkaisun vaatimuksia käydään esimerkiksi kappaleessa 4.5. Työn päätutkimuskysymykseen, kuinka saadaan toteutettua Katakri 2020 vaatimukset täyttävä ratkaisu turvallisuusluokan IV tiedon käsittelyyn langattomassa tiedonsiirrossa, saatiin vastaus vaatimuksia läpikäydessä. Tärkein vastaus oli, että langaton tiedonsiirto luokitellaan julkisen verkon kautta liikennöimiseksi ja tästä syystä langattomassa tiedonsiirrossa on käytettävä viranomaisen hyväksymään salausratkaisua. Käytettävä salausratkaisu on hyväksytettävä Traficomin salausratkaisun arviointi- ja hyväksyntäprosessilla tai valittava salausratkaisu jo hyväksyttyjen listalta, nämä prosessit on kerrottu kappaleessa 5. Alikysymyksiinkin saatiin vastaukset, kuten käyttökokemusta koskeviin asioihin, että kuinka käyttökokemus ei kärsisi liikaan salausratkaisua käyttäessä. Hyvä käyttökokemus on ratkaistavissa pääsynhallinnalla ja siihen liittyvän käyttäjä tunnistautumisen opastamisella käyttäjä ohjeiden avulla. Yksi selkeä muutos toimipisteiden langattoman verkon käytössä mikä haittaa pienesti käyttökokemusta on, että VPN-salausratkaisun tunnistautuminen pitää tehdä, kun siirrytään langallisesta lähiverkosta käyttämään langatonta lähiverkkoa. Tutkimuskysymykseen kuinka VPN-

salausratkaisu toteuttaa Katakrin 2020 vaatimukset löytyvät tarkemmat selitykset kappaleista 3.4 ja 4.5. VPN-salausratkaisulla saadaan salattua verkkoliikenteen tiedonsiirto kahden laitteen välillä jaetun tai julkisen verkon kautta, jotta Katakrin vaatimukset täyttyvät.

8 Yhteenveto

Tässä opinnäytetyössä tutkittiin Katakrin tuomat vähimmäisvaatimukset turvallisuusluokan IV tietojen käsittelylle langattomassa tiedonsiirrossa. Opinnäytetyössä saatiin selville mitkä ovat kyseiset Katakrin tuomat vaatimukset ja mitä salausratkaisuvaatimuksiin kuuluu ja kuinka se on hyväksyttävä viranomaisen hyväksyntäprosessilla. Opinnäytetyön tutkimuskysymyksenä oli, kuinka saadaan toteutettua Katakri 2020 vaatimukset täyttävä ratkaisu turvallisuusluokan IV tiedon käsittelyyn langattomassa tiedonsiirrossa. Tähän saatiin vastaus käymällä Katakrin vaatimuksia läpi turvallisuusluokan IV vaatimuksien osalta. Tämä pääkysymys oli jaettu seuraaviin täsmentäviin alikysymyksiin. Kuinka Katakri 2020 vaatimuksia vastaava ratkaisu turvallisuusluokalle IV saadaan toteutettua parhaiten, jotta käyttökokemus ei kärsi? Kuinka VPN-salausratkaisu toteuttaa Katakri 2020 vaatimukset? Näihin saatiin vastauksen käymällä pääsynhallintaan liittyviä asioita läpi, sekä tutkimalla Katakrin salausratkaisu vaatimuksia.

Opinnäytetyön aihe oli hyvin mielenkiintoinen mutta myös hyvin haastava monen lakiin liittyvien asioiden takia, nämä toivat hyvin aikaa vievää tutkimusta ja tarkastelua. Opinnäytetyö oli melko vaikea myös pitää aiheen kannalta kasassa, jotta ei lähde käsittelemään asiaa liian laajalti, jonka takia aiheen selkeyskin kärsisi. Tästä syystä opinnäytetyön tekovaiheessa tuli muutamia muutoksia aiheen käsittelyjärjestykseen ja laajuuteen. Katakrin vaatimuksia läpikäydessä opin paljon turvallisuusluokiteltuun tietoon liittyvistä asioista, sekä monista muista lakiin liittyvistä asioista. Toimeksiantaja hyötyi työstä saamalla tietoa Katakri 2020 vaatimuksiin liittyvistä asioista ja kuinka salausratkaisun hyväksyntäprosessi toimii.

Lähteet

2013/488/EU. 2013. EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä. Viitattu 27.3.2022. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32013D0488&from=EN.

AD CS. 2016. Active Directory Certificate Services Overview. Microsoft. Viitattu 30.10.2022. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831740(v=ws.11).

Aditya, L. & Prasoon D. 2015. SSL/TLS Security and Troubleshooting. EMC. Viitattu 21.11.2022.

Arviointi- ja hyväksyntäprosessit. 2021. Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit. Traficom. Viitattu 23.11.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf.

FIPS PUBS. 2001. Announcing the Advanced Encryption Standard (AES). NITS. Viitattu 9.1.2023. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

Geier, J. 2008. Implementing 802.1X Security Solutions for Wired and Wireless Networks. John Wiley & Sons. Viitattu 19.11.2022.

IANA. 2022. Extensible Authentication Protocol (EAP) Registry. IANA. Viitattu 30.10.2022. https://www.iana.org/assignments/eap-numbers/eap-numbers.xhtml#eap-numbers-4.

Harte, L. 2004. Introduction to Wireless Local Area Network (WLAN)—Technology, Market, Operation, Profiles and Services. ALTHOS. Viitattu 7.1.2023.

Katakri 2020. 2020. Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille. Traficom. Viitattu 11.2.2022. https://um.fi/documents/35732/0/Katakri-2020_201218.pdf.

Korowajczuk, L. 2011. LTE, WiMAX and WLAN Network Design, Optimization and Performance Analysis. John Wiley & Sons. Viitattu 22.11.2022.

Kryptografiset vaatimukset. 2021. Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat. Traficom. Viitattu 25.2.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf.

Kuvaus vaatimuksenmukaisuuden nykytilasta. 2020. Kuvaus järjestelmän vaatimustenmukaisuuden nykytilasta. Traficom. Viitattu 30.10.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/kuvaus-jarjestelman-vaatimuksenmukaisuuden-nykytilasta-2020.docx.

Käsittelyohje. 2020. Kansainvälisen turvallisuusluokitellun tiedon käsittelyohje. Traficom. Viitattu 30.10.2022. https://um.fi/turvallisuusluokitellun-tiedon-kasittelyohje.

L 10/2015. Laki julkisen hallinnon turvallisuusverkkotoiminnasta. Viitattu 22.11.2022. https://www.finlex.fi/fi/laki/alkup/2015/20150010?search%5Btype%5D=pika&search%5Bpika%5D=10%2F2015.

L 1101/2019. Valtionneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa. Viitattu 24.2.2022. https://www.finlex.fi/fi/laki/alkup/2019/20191101.

L 1406/2011. Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista. Viitattu 25.10.2022. https://www.finlex.fi/fi/laki/ajantasa/2011/20111406.

L 588/2004. Laki kansainvälisistä tietoturvallisuusvelvoitteista. Viitattu 25.10.2022. https://www.finlex.fi/fi/laki/ajantasa/2004/20040588.

L 621/1999. Laki viranomaisten toiminnan julkisuudesta. Viitattu 24.2.2022. https://www.finlex.fi/fi/laki/ajantasa/1999/19990621.

L 726/2014. Turvallisuusselvityslaki. Viitattu 18.11.2022. https://www.finlex.fi/fi/laki/alkup/2014/20140726.

L 906/2019. Laki julkisen hallinnon tiedonhallinnasta. Viitattu 24.2.2022. https://www.finlex.fi/fi/laki/alkup/2019/20190906.

Lukka, K. 2001. Konstruktiivinen tutkimusote. Viitattu 4.3.2022. https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/.

NCSA salausratkaisut. 2022. Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut. Traficom. Viitattu 30.10.2022. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat-salausratkaisut.

NCSA-tarkastelupyyntölomake. 2020. Pyyntö tietojärjestelmän tietoturvallisuushyväksynnälle/-arvioinnille. Traficom. Viitattu 30.10.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA-tarkastuspyyntolomake.docx.

Salaustuotearvioinnit ja -hyväksynnät. 2020. Liikenne- ja viestintävirasto Traficomin suorittamat salaustuotearvioinnit ja -hyväksynnät. Traficom. Viitattu 11.8.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-salaustuotearvioinnit-ja-hyvaksynnat.pdf.

Tiller, S. 2000. A Technical Guide to IPSec Virtual Private Networks. Auerbach Publishers. Viitattu 21.11.2022.

Wrightson, T. 2012. Wireless Network Security: A Beginner's Guide. McGraw-Hill/Osborne. Viitattu 9.1.2023.