Tampereen ammattikorkeakoulu

Julkisen avaimen infrastruktuurin hyödyntäminen OpenVPN-yhteyksien varmentamiseen yksityisen verkon IoT-laitteissa

Axel Sjöholm

OPINNÄYTETYÖ
Maaliskuu 2024
Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

SJÖHOLM, AXEL:

Julkisen avaimen infrastruktuurin hyödyntäminen OpenVPN-yhteyksien varmentamiseen yksityisen verkon IoT-laitteissa

Opinnäytetyö 33 sivua, joista liitteitä 4 sivua
Maaliskuu 2024

Opinnäytetyön tarkoituksena oli tuottaa nykyaikaista tietoa X.509-standardin mukaisen julkisen avaimen infrastruktuurin käytöstä OpenVPN-yhteyksien varmentamiseen IoT-laitteissa yksityisessä verkkoympäristössä sekä X.509-standardin julkisen avaimen infrastruktuurin varmenteiden hallinnasta. Opinnäytetyössä esitellään X.509-standardin, OpenVPN:n, VPN-, IoT-, ja M2M-yhteyksien yleisiä periaatteita, käsitteitä sekä ominaisuuksia.

Opinnäytetyössä käytettiin lähteinä alan artikkeleita, julkaisuja, kirjoja, seminaareja sekä verkkosivuja. Tutkitun tiedon perusteella esitellään suositus X.509-standardin julkisen verkon infrastruktuurin hyödyntämisestä OpenVPN-yhteyksien varmentamiseen yksityisessä verkossa.

IoT-laitteiden yleistyessä tulevaisuudessa voidaan olettaa myös yksityisten verkkojen käytön IoT-yhteyksissä lisääntyvän etenkin kriittisen infrastruktuurin, kuten sähköverkkojen, uusiutuvan energiatuotannon ja lämmönjakelun yhteydessä. Tietoliikenteen suojaaminen ja salaaminen yksityisessä verkossa on myös tärkeää. OpenVPN soveltuu hyvin luotettavuudeltaan, hallittavuudeltaan ja turvallisuudeltaan yhdessä X.509-standardin julkisen avaimen infrastruktuurin kanssa yksityisessä verkossa olevien IoT-yhteyksien suojaamiseen.

Asiasanat: pki, x.509, openvpn, iot, yksityinen verkko

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunications and Networks

SJÖHOLM, AXEL:

Utilization of Public Key Infrastructure in Authentication of OpenVPN Connections in Private Network IoT Devices

Bachelor's thesis 33 pages, appendices 4 pages
March 2024

The purpose of this thesis was to produce up-to-date information of the X.509 standard regarding public key infrastructure when authorizing OpenVPN connections in IoT devices in a private network and the management of certificates based on the X.509 standard in public key infrastructure. In addition, the thesis covered the principles of the X.509 standard, OpenVPN, IoT and M2M connections.

The information in this thesis was compiled from several different articles, publications, books, seminars, and websites. From the information compiled, a suggestion using the public key infrastructure based on the X.509 standard was made to authenticate OpenVPN connections in a private network.

In the future, with the amount of IoT devices continuously increasing, it may be assumed that the use of private networks in IoT connections will also increase, especially in critical infrastructure, such as in electric grids, the production of renewable energy and in heat distribution. It is also important to note that it is necessary to secure the network connections in a private network. OpenVPN, due to its reliability, controllability, and security along with the X.509 standard public key infrastructure is more than suitable to secure IoT connections in a private network.

Key words: pki, x.509, openvpn, iot, private network

SISÄLLYS

LYHENTEET JA TERMIT

2G	Toisen sukupolven mobiiliverkko
3G	Kolmannen sukupolven mobiiliverkko
4G	Neljännen sukupolven mobiiliverkko
5G	Viidennen sukupolven mobiiliverkko
APN	Access Point Name
CA	Certificate Authority, Varmentaja
CIA	Confidentiality, Integrity, Availability
ESP	Encapsulating Security Payload
FDD	Frequency Division Duplex
GMaaS	Grid Management as a Service
GPRS	General Packet Radio Service, 2.5G
IoT	Internet of Things
IPSec	Internet Protocol Security
LTE	Long Term Evolution, 4G
M2M	Machine-to-Machine
OSI	Open Systems Interconnection model
P2P	Peer-to-Peer
PKI	Public key infrastructure
SSL	Secure Socket Layer
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunications System, 3G
UDP	User Datagram Protocol
VPN	Virtual Private Network
W-CDMA	Wideband Code-Division multiple access
X.509	Kansainvälisen televiestintäliiton (ITU) standardi julkisen avaimen salauksessa käytettäville varmenteille

1 JOHDANTO

Opinnäytetyössä tutkitaan X.509-standardin mukaista julkisen avaimen infrastruktuurin (Public key interface, PKI) toimintaa sähköverkkojen tietoliikenneympäristössä peer-to-peer yhteyksissä. Opinnäytetyössä keskitytään esineiden internet (Internet of Things, IoT) ympäristössä olevien laitteiden varmenteiden (Certificate) ja varmentajan (Certificate Authority) elinkaareen hallintaan sekä niiden käyttöön OpenVPN-palvelun kanssa. Opinnäytetyön tavoitteena on tuottaa tietoa nykyaikaisesta, tietoturvallisesta ja käytettävyydeltään järkevästä ratkaisusta hallinnoida OpenVPN:n käyttämiä varmenteita koko varmenteiden elinkaaren ajalta, yksityistä varmentajaa käyttäen.

Opinnäytetyön teettäjä on Emtele, joka on suomalainen kriittisen infrastruktuurin, kuten sähköverkkojen tietoliikennepalveluiden-, ja GMaaS- (Grid Management as a Serivce) palveluntarjoaja. GMaaS:lla tarkoitetaan sähköverkkojen hallinnan ja tietoliikenneympäristön toteuttamista palveluna. Palvelua hyödynnetään sekä sähkönjakeluverkoissa että uusiutuvan energian voimalaitosverkoissa.

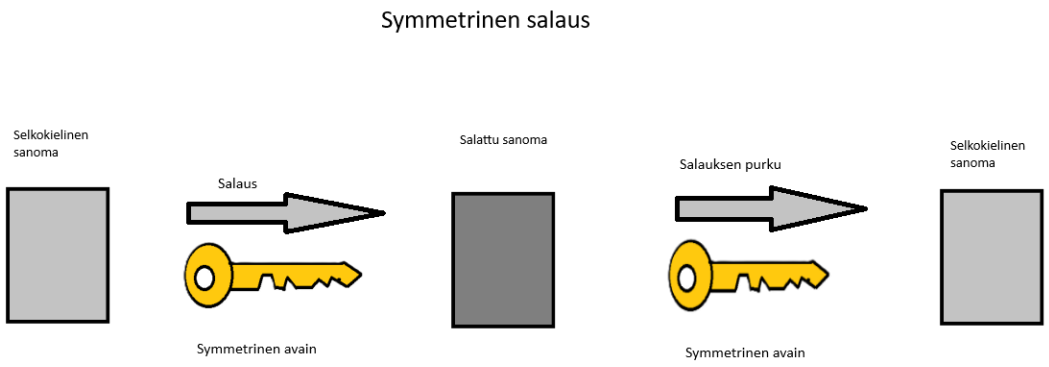
Työssä käsitellään eri aihealueita, jolla pyritään luomaan lukijalle selkeä käsitys aihesisällöstä. Opinnäytetyön alussa käsitellään julkisen avaimen infrastruktuuria, sen toimintaa, rakennetta ja olennaisia konsepteja peer-to-peer -ympäristössä sekä laitteelta-laitteelle kommunikaation periaatteita osana PKI:ta. Seuraavaksi käsitellään VPN:n periaatteita sekä OpenVPN:n toimintaa, varmentajan ja varmenteiden toimintaa OpenVPN-ympäristössä. Lopuksi esitetään suositus PKI:n toteuttamiseksi yksityisessä verkossa hyödyntäen OpenVPN:ää.

2 PKI

Julkisen avaimen infrastruktuuri eli PKI on laaja kokonaisuus, joka käsittää eri käytäntöjä, menetelmiä, laitteita ja ohjelmistoja, joilla hallitaan varmenteiden elinkaarta. Osiossa tutkitaan julkisen avaimen infrastruktuuria peer-to-peer -liikenteessä. Julkisen avaimen infrastruktuuria käytetään tietoliikenteen salaamisessa. Tietoliikenteen salaaminen on välttämätöntä, jotta voidaan olla varmoja tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta. Tämä tunnetaan myös CIA-kolmiona (Confidentiality, Integrity, Availability). CIA-kolmiossa luottamuksellisuudella tarkoitetaan tiedon salassapitoa, eheydellä tiedon säilymistä muuttumattomana ja saatavuudella tiedon saatavuutta vain niille, joilla on oikeus päästä tietoon (Fortinet n.d.).

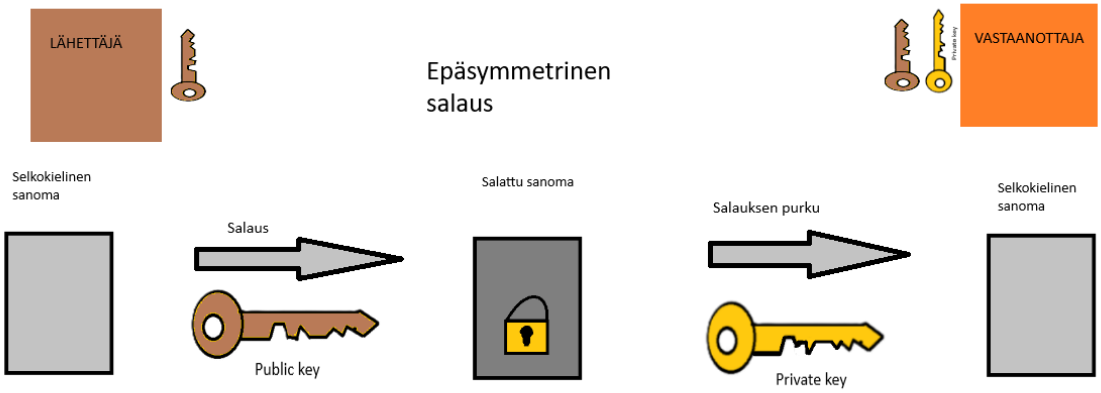
Tietoliikenteen salaaminen voidaan toteuttaa epäsymmetrisellä salauksella, jossa tieto salataan yhdellä salausavaimella ja puretaan toisella salausavaimella tai symmetrisellä salauksella, jossa sekä salaus että purkaminen tehdään samalla salausavaimella (Keyfactor n.d.). Salausavain tai yksityinen avain (Private key) on salausalgoritmilla luotu bittijono, jolla voidaan hajottaa tieto niin, että se ei ole enää luettavissa.

Kuviossa 1 on havainnollistettu symmetrisen salauksen toimintaa, jossa sama avain toimii viestin salaajana sekä salauksen purkajana. Symmetrisen salauksen ilmeisenä riskinä on se, että jokainen, jolla on symmetrinen avain hallussaan voi purkaa jokaisen sillä salatun sanoman.



KUVIO 1. Symmetrinen salaus.

Kuviossa 2 on puolestaan havainnollistettu epäsymmetrisen salauksen toimintaa, missä lähettäjällä on tiedossa julkinen avain, jolla selkokielinen sanoma salataan, kun taas vastaanottajalla on sekä yksityinen, että julkinen avain tiedossa. Epäsymmetrisen salauksen ilmeisiä etuja on, että lähtökohtaisesti vain sanoman tarkoitettu saaja voi purkaa sanoman yksityisellä avaimellaan, sillä purkamiseen vaaditaan aina avainpari. Tämä on kuitenkin myös epäsymmetrisen salauksen yksi heikkous, sillä mikäli yksityinen avain pääsee vuotamaan, ei avainparia voida enää luottamuksellisesti käyttää. (Ashbourn 2023.).



KUVIO 2. Epäsymmetrinen salaus.

Molemmissa salausmenetelmissä on selkeitä hyviä- ja huonoja puolia. Symmetrisen salauksen toiminnan luonteen takia symmetristen avainten käyttäminen useamman laitteen välillä, esimerkiksi useamman IoT-laitteen liikennöinnin salaamiseen on ilmeisen riskialtista, sillä jos avain vuotaa, vaarantuu koko liikennöintiketju. Toisaalta symmetrinen avain on kuitenkin kooltaan pienempi kuin epäsymmetrinen avain, jolloin avaimen säilyttäminen vaatii vähemmän tallennusmuistia. Epäsymmetrinen avain vaatii puolestaan enemmän tallennusmuistia ja näin ollen avaimen käsittelyprosessin aikana enemmän suoritustehoa laitteelta. (Ashbourn 2023.).

2.1 Salausalgoritmit

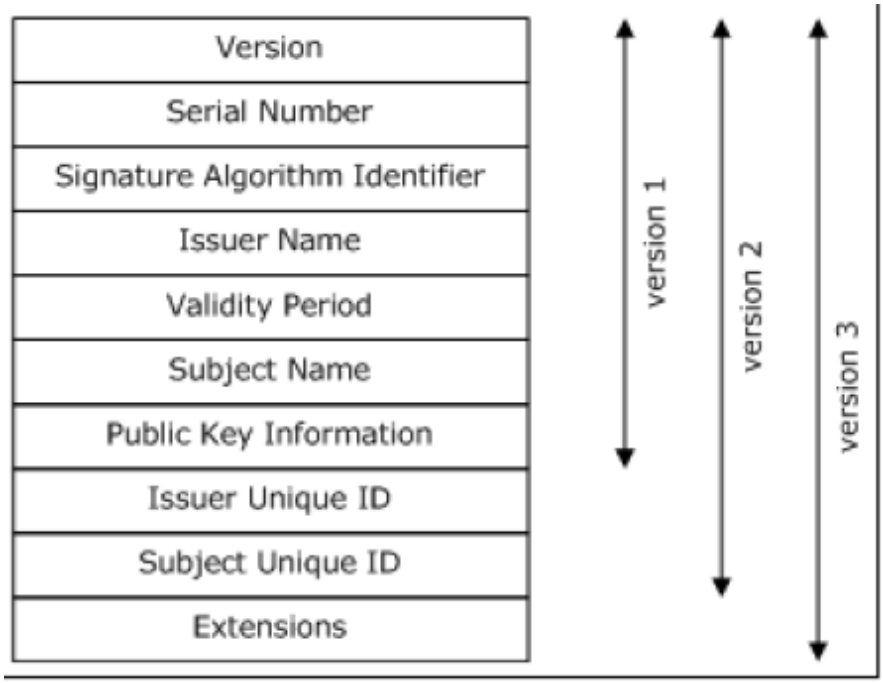
Salausalgoritmeja on useita erilaisia, mutta jokaisen päämäärä on muuntaa sanoma sellaiseksi, jota ei voi suoraan tulkita. Nykyään käytetyimpiä salausalgoritmeja ovat RSA (Rivest-Shamir-Adlema), jota käytetään epäsymmetriseen salaukseen ja AES (Advanced Encryption Standard), jota käytetään symmetriseen salaukseen. (Ashbourn 2023.).

Nykyaikaiset salausalgoritmit käyttävät salaamisen matemaattisia menetelmiä ja salaus tapahtuu binaaritason muutoksilla, missä ensin varmenteen sisältävä julkinen avain toimii salauksen “siemenenä”, jonka pohjalta salausalgoritmi luo uuden avaimen, usein hyödyntäen sekä symmetristä että epäsymmetristä algoritmia salausprosessissa (Ashbourn 2023.). Lisäksi on hyvä huomioida, että avaimen luomisen yhteydessä määritellään käytettävä bittimäärä eli avaimen pituus, joka määrittää avaimen kestävyyttä niin sanotun Brute-Force -hyökkäyksen alla, missä avainta koitetaan ratkaista raa’alla laskentavoimalla. Nykyinen suositus avaimen pituudelle on vähintään 2048-bittinen RSA julkiselle avaimelle ja 256-bittinen SHA (Secure Hash Algorithms) yksityisen avaimen salaamiseen (Barker & Dang 2015.).

2.2 Varmenteet

Varmenteet ovat osa julkisen avaimen infrastruktuuria, jossa varmenteet ovat luotetun varmentajan allekirjoittamia digitaalisia todistuksia julkisen salausavaimen voimassaolosta sekä luotettavuudesta (Cooper et al 2008.). Varmenteet sisältävät kopion julkisesta avaimesta, tietoa julkisen avaimen omistajasta, varmenteen voimassaoloajan, varmenteen myöntäjän digitaalisen allekirjoituksen, käytetyn algoritmin tunnisteen sekä muuta tietoa, kuten digitaalisia sormenjälkiä käytetyistä algoritmeista ja varmenteen käyttötarkoituksen (Schukat & Cortijo 2015.).

X.509-standardi määrittelee kolme eri varmenneversiota, kuten kuviosta 3 voidaan tulkita, mutta opinnäytetyössä käsitellään ainoastaan kolmatta versiota, sillä se on opinnäytetyön tarkoituksessa monipuolisin ja yleisimmin käytetty varmenneversio.

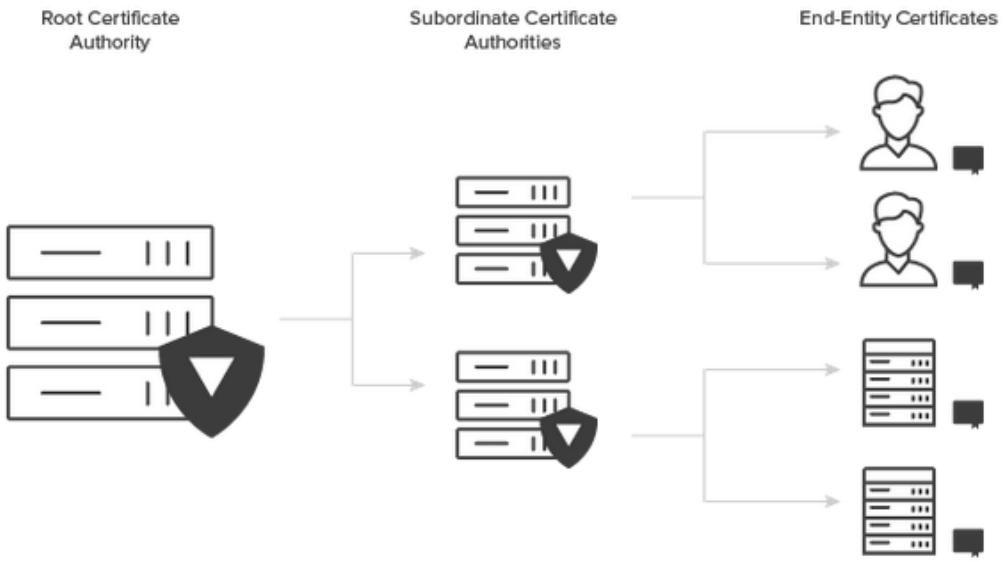


KUVIO 3. X.509-standardin mukaiset varmennekentät, versiot 1, 2 ja 3. (Schukat & Cortijo 2015.).

2.3 Varmentaja

Varmentaja eli Certificate Authority on palvelin tai palvelimella toimiva osa, jonka tehtävä on luoda sekä julkisia että yksityisiä avaimia, varmenteita, sekä varmistaa näiden eheys. Varmentajia voi olla yksi tai useampia osana julkisen avaimen infrastruktuuria (Schukat & Cortijo 2015.). Julkiset varmentajat ovat yleisesti jonkin luotetun tahon ylläpitämiä palveluita, joita asiakkaat, yleisesti yritykset voivat ostaa varmentaakseen esimerkiksi verkkosivunsa. Yksityisiä varmentajia puolestaan käytetään yleisesti yrityksen sisäisten avainten ja varmenteiden luomiseen, joka vähentää huomattavasti julkisen varmentajan käytön tuomaa tietoturvariskiä (Yamakawa et al 2021.). Lisäksi yksityisen varmentajan käyttö on välttämätöntä yksityisen verkon liikenteessä, kun halutaan estää liikennöinti julkiseen verkkoon.

Jokaisella varmentajalla on myös oma varmenne. Ylimmän tason varmentajaa kutsutaan juurivarmentajaksi (Root Certificate Authority), joka on luonut ja allekirjoittanut oman varmenteensa. Ylimmän tason varmentajalla voi olla useampia alemman tason varmentajia hierarkiassaan, jotka luovat edelleen varmenteita alemmalle tasolle, kuten kuviossa 4 havainnollistetaan. (Keyfactor n.d.). Varmentajien hierarkia lisää turvallisuutta sekä julkisen että yksityisen varmentajan käytössä, kun käytetään pienemmän oikeuden periaatetta, missä käyttö- tai pääsyoikeudet järjestelmiin tai palveluihin myönnetään vain tehtävän suorittamisen osalta välttämättömiin järjestelmiin tai palveluihin, jolloin niin sanotun juurivarmenteen (Root Certificate) vuotamisen riski voidaan minimoida.

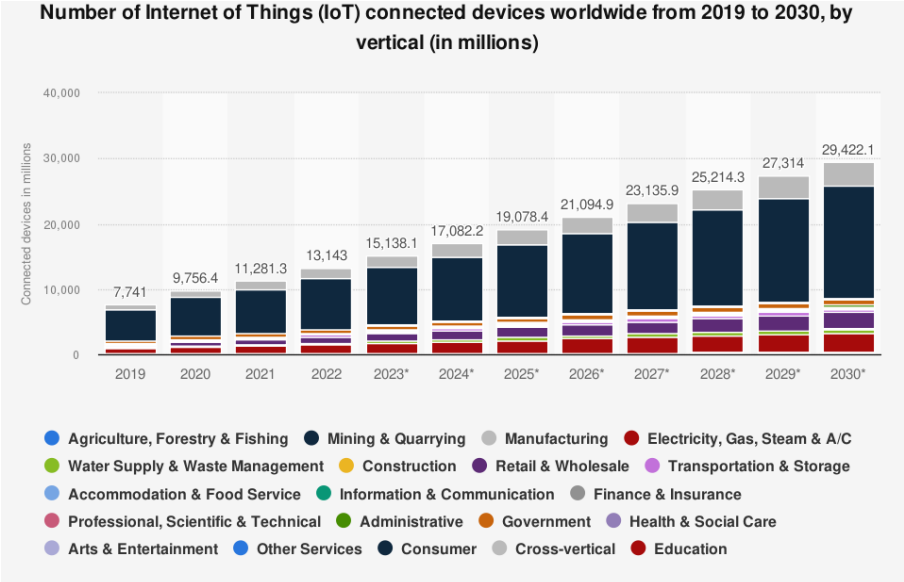


KUVIO 4. Varmentajan hierarkia. (Keyfactor n.d.).

2.4 PKI JA IoT

Julkisen avaimen infrastruktuuria voidaan hyödyntää myös laitteiden välisen liikenteen salaamiseen hyödyntäen VPN-yhteyttä. IoT eli laitteiden internetillä tarkoitetaan useammasta sensorista, anturista tai muusta laitteesta koostuvaa ryhmää, joka kommunikoi keskenään internetin välityksellä. IoT voi hyödyntää julkista tai yksityistä verkkoa. Usein laitteiden internettiin voidaan yhdistää M2M eli Machine-to-Machine -käsite, mikä tarkoittaa suoraan laitteelta laitteelle tapahtuvaa kommunikointia ilman tai hyvin vähäisellä ihmisen väliintulolla. M2M-liikennettä hyödynnetään muun muassa eri sensorien tai antureiden mittaamien tietojen keskittämiseen yhdelle etäpääteyksikölle, joka kerää ja käsittelee tiedon ja lähettää sen edelleen internetin välityksellä keskitetylle palvelimelle (Stojmenovic 2014.).

IoT-ympäristöt kehittyvät jatkuvasti ja IoT:n merkityksen maailmassa sekä teollisuuden, kaupunkien ja kotitalouksien ympäristöissä voidaan odottaa vain kasvavan, kuten kuviosta 5 voidaan päätellä. Yhä kasvavassa IoT-maailmassa on jo vuonna 2023 ollut arviolta yli 15 miljardia IoT-laitetta, joista yleisimpiä ovat olleet erilaiset anturit. Tämän luvun odotetaan kasvavan jopa yli 29 miljardiin IoT-laitteeseen vuoteen 2030 mennessä. (Vailshery 2023.).

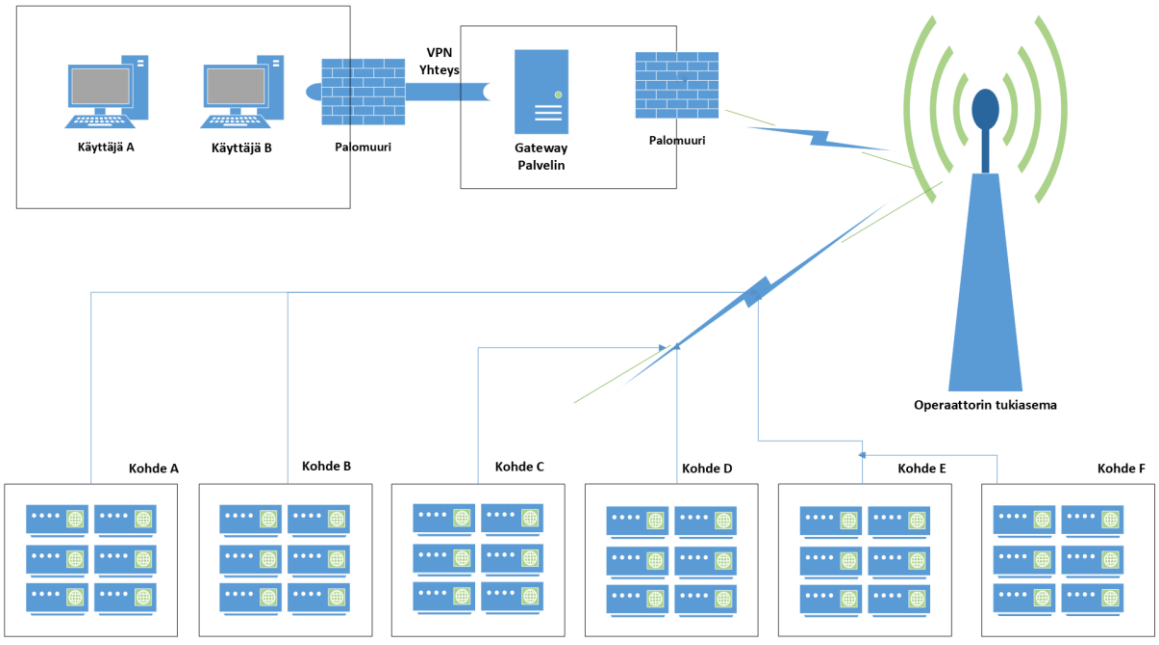


KUVIO 5. IoT-laitteiden määrä, tyyppi ja ennustettu kasvu (Statista 2023.).

3 M2M YMPÄRISTÖ

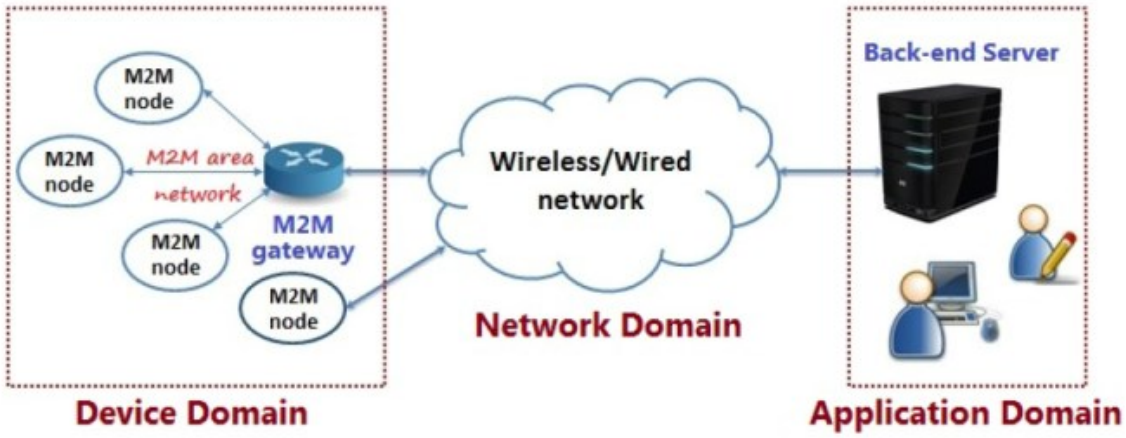
M2M-ympäristössä laitemäärä vaihtelee huomattavasti. Pelkästään teollisuudessa käytettyjen M2M-laitteiden määrä yksittäisellä toimijalla voi vaihdella muutamasta yksittäisestä laiteesta useampaan tuhanteen laitteeseen, usein kuitenkin niin, että laitteet ovat niin sanotuissa ryhmittymissä, joita puolestaan voi olla useampia. Näin ollen M2M-ympäristössä olevien laitteiden tiedon käsittelyn ja selkeyden takia voidaan hyödyntää yhteyksien keskittämistä yhteen tai useampaan M2M-yhdyskäytävään, jolloin yhteyksien seuranta voidaan hoitaa yhden tai useamman pisteen kautta (Stojmenovic 2014.).

Kuviossa 6 havainnollistetaan yksinkertaisesti M2M-liikenteen keskittämistä niin sanotun gateway- eli yhdyskäytäväpalvelimen avulla, missä kohteiden A, B, C, D, E ja F sisällä olevat laitteet ovat yhteydessä “Gateway-palvelimeen” operaattorin tukiaseman välityksellä. “Gateway-palvelin” toimii yhteyksien keskittäjänä, jolloin käyttäjät voivat helposti havainnoida ja hallita useampien laitteiden yhteyksiä samanaikaisesti.



KUVIO 6. M2M-ympäristön havainnointi.

Kuviossa 7 havainnollistetaan M2M-ympäristön verkon topologiaa supistetusti. Verkko on jaettu kolmeen osa-alueeseen, laite-, verkko- ja sovellusalueeseen, missä laitealue sisältää IoT-, laitteet ja sensorit, joista data kerätään ja välitetään edelleen verkkoalueeseen. Verkkoalueessa kerätty data välitetään eteenpäin sovellusalueelle, yleisesti langattomalla verkkoteknologialla, kuten 2G-verkon GPRS (General Packet Radio Service) tai 4G-verkon LTE FDD (Long Term Evolution Frequency-Division Duplexing) teknologiolla. Aiemmin myös IoT-ympäristöissä laajemmin käytetty 3G-verkon W-CDMA (Wideband Code Division Multiple Access), josta on jouduttu luopumaan Suomessa vuoden 2023 aikana operaattorien sulkiessa 3G-verkot vuoden loppuun mennessä. Sovellusalueella palvelin käsittelee ja säilyttää datan. Edellä mainittu prosessi tapahtuu reaaliajassa yhteyksien ollessa ylhäällä, mahdollistaen valtuutetuille henkilöille tai laitteille datan reaaliaikaisen käsittelyn sekä tarvittaessa jokaisen osa-alueen reaaliaikaisen muokkaamisen. (Barki et al 2016.).



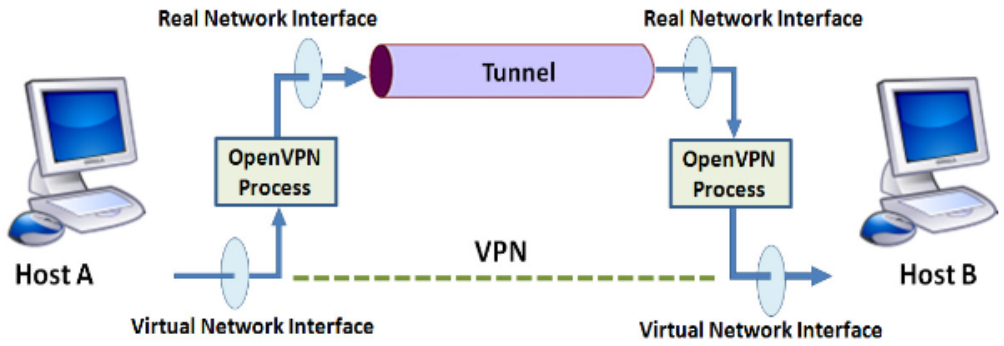
KUVIO 7. M2M-verkon yksinkertainen esimerkkitopologia esitettynä. (Barki et al 2016.).

M2M-ympäristössä on tärkeää ottaa huomioon myös yleiset tietoturvallisuuteen liittyvät kysymykset. Täysin yksityistä verkkoa käyttäessä maantieteellinen etäisyys tuo haasteita tietoliikenneratkaisuiden järjestämiseen, joten kustannustehokkuuden kannalta on järkevää käyttää jo valmiiksi rakennettua verkkoinfrastruktuuria, esimerkiksi ostamalla tietoliikennepalveluita operaattorilta. Operaattorit ovat jo pitkään tarjonneet lisääntyvään yritysverkkoinfrastruktuuriin sekä IoT-ympäristöihin omia ratkaisujaan, kuten yksityisen APN:n (Access Point Name). APN toimii joko langallisena tai langattomana yhdyskäytävänä välittäen yhteyden suoraan mobiililaitteelta yrityksen verkkoon, jolloin tietoliikenne ei välity julkisen verkon kautta (DNA n.d.).

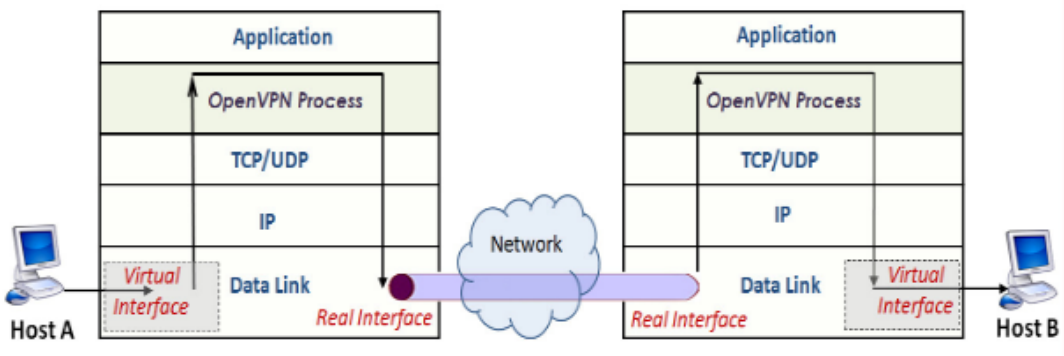
M2M-gateway voi toimia myös varmentajana sekä VPN-palvelimena IoT-kenttälaitteille, jolloin gateway luo tarvittavat varmenteet laitteille VPN-yhteyden muodostamista varten. VPN-yhteyksien käyttäminen lisää tietoturvallisuutta, sillä jokainen verkkoon yhdistävä laite vaatii tunnistautumisen. On kuitenkin hyvä mainita, että jos sama palvelin toimii sekä varmenteiden luojana että varmentajana, on näillä VPN-yhteyksien avulla saatu tietoturvahyöty kyseenalainen. M2M-liikenteessä VPN-yhteyksien tunnistautuminen toteutetaan yleisesti varmentajan luomien varmenteiden avulla.

4 OPENVPN

OpenVPN on GNU GPL (GNU General Public License) lisenssin alla oleva avoimen lähdekoodin SSL VPN-ohjelmisto, joka sisältää sekä palvelinpuolen että käyttäjäpuolen sovellukset. Ohjelmistolla voidaan luoda VPN-yhteyksiä. Kuviossa 8 on havainnollistettu OpenVPN:n toimintaperiaatetta kahden päätelaitteen välillä, missä tietoliikenne liikkuu kohteelta A ensin virtuaalisen verkkosovittimen välityksellä OpenVPN-prosessiin ja siitä edelleen oikean verkkosovittimen läpi tunneliin. Sama toistuu käänteisessä järjestyksessä kohteen B puolella. Kuviossa 9 OpenVPN:n tietoliikenteen polku on havainnollistettu tarkemmin OSI (Open Systems Interconnection) mallin kerrosten mukaisesti.



KUVIO 8. OpenVPN toimintaperiaate. (Likhar et al 2011.).



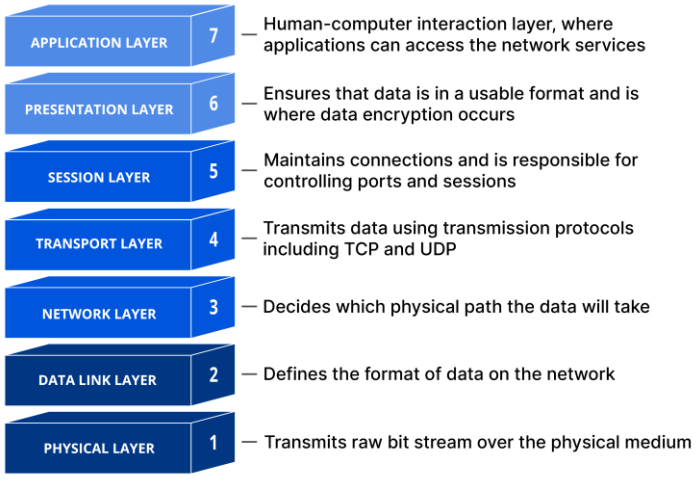
KUVIO 9. OpenVPN tietoliikenteen polku. (Likhar et al 2011.).

4.1 VPN yleisesti

VPN eli Virtual Private Network on niin sanottu yksityinen verkkotunneli, joka salaa tietoliikenteen päästä päähään OSI-mallin (Kuvio 10.) 2. tai 3. kerroksilla eli siirto- ja verkkokerroksilla käyttäen yleisesti SSL/TLS protokollaa.

VPN:llä voidaan luoda muun muassa paikasta-paikkaan -yhteys, esimerkiksi yrityksen kahdessa eri maantieteellisessä paikassa sijaitsevat toimistot, joiden tarvitsee olla yhteydessä toisiinsa ja päästä käsiksi sisäiseen verkkoon (Skendzic & Kovačić 2017.) tai etäkäyttöyhteys, jota voidaan hyödyntää esimerkiksi etätöissä tai yksityisessä verkossa olevien IoT-laitteiden hallinnassa.

Avoimen lähdekoodin VPN-, sovelluksia ja protokollia löytyy useampia OpenVPN:n lisäksi, kuten Openswan, SoftEther ja Tunnelblick. Käyttötarkoituksen ja ympäristön takia tässä opinnäytetyössä keskitytään ainoastaan OpenVPN:ään ja sen toimintaan eikä muita vaihtoehtoja esitellä tämän tarkemmin.



KUVIO 10. OSI-malli. (Cloudflare n.d.).

4.2 Salaus ja turvallisuus

OpenVPN:n kehityksessä on alusta asti painotettu salauksen ja turvallisuuden merkitystä. OpenVPN:n käyttämä suojaus on suunniteltu suojaamaan sekä aktiivisilta että passiivisilta hyökkäyksiltä. Suojaus perustuu SSL/TLS:n käyttöön istunnon varmentamisessa ja IPSec:in yhteydessä kehitetyn ESP (Encapsulating Security Payload) protokollan käyttöön UDP-tunneloinnissa. (Likhar et al 2011.). On kuitenkin hyvä huomioida, että OpenVPN ei itsessään tue tai käytä IPSec protokollaa. OpenVPN tukee myös nykyaikaisia salausmenetelmiä, kuten 256-bittistä AES:ää.

OpenVPN:n ollessa lähes täysin käyttäjän konfiguroitavissa, aiheuttaa tämä omat haasteet turvallisuuteen liittyen. Mikäli käyttäjä muuttaa perustason konfiguraatiota eikä käyttäjä ole täysin varma toiminnastaan, hän voi tietämättään luoda uusia riskejä VPN:n käyttöön. Käyttäjän lisäksi suurimmat riskit OpenVPN:n käytössä liittyvät lähinnä OpenVPN:n protokollaa käyttävien kaupallisten palvelujen ratkaisuihin.

OpenVPN:n käyttäjän tunnistamiseen voidaan hyödyntää muun muassa X.509-standardin varmenteita istunnon varmentamiseen sekä kaksivaiheista tunnistautumista, älykortteja, käyttäjätunnusta ja salasanaa tai näiden yhdistelmiä käyttäjän varmentamiseen. (OpenVPN. n.d.b).

4.3 Käyttö

OpenVPN:ää voidaan hyödyntää samoihin tarkoituksiin kuin muitakin VPN-yhteyksiä, kuten tietoliikenteen salaamiseen, verkkoyhteyksien tunneloimiseen organisaation verkkoon tai useamman verkon yhdistämiseen site-to-site eli kohteelta-kohteelle -yhteydellä. OpenVPN eroaa muista VPN-protokollista eritoten turvallisuudessa ja käytettävyydessä (Skendzic & Kovačić 2017.). OpenVPN protokollan sekä OpenVPN yhteisöversion perustuessa avoimen lähdekoodin GPL-lisenssiin voi jokainen halutessaan tarkastella OpenVPN:n lähdekoodia ja osallistua sen kehittämiseen, jonka johdosta OpenVPN on myös käyttävissä jokaisella yleisesti tunnetulla käyttöjärjestelmällä.

On kuitenkin hyvä huomioida, että OpenVPN tarjoaa myös samalla nimellä maksullisia CloudConnexa ja Access Server palveluitaan, jotka eivät ole GPL-lisenssin piirissä (OpenVPN n.d.a).

Kuten aiemmin mainittiin, VPN-yhteyksiä hyödynnetään teollisuudessa myös esimerkiksi IoT-laitteiden datan keräämiseen keskitetysti yhdelle tai useammalle välipalvelimelle sekä mahdollisesti näiden laitteiden ohjaamiseen ja hallitsemiseen. Laitteet voivat sijaita maantieteellisesti missä tahansa, ainoana vaatimuksena on toimiva internet-yhteys.

4.4 Palvelimen hallinta

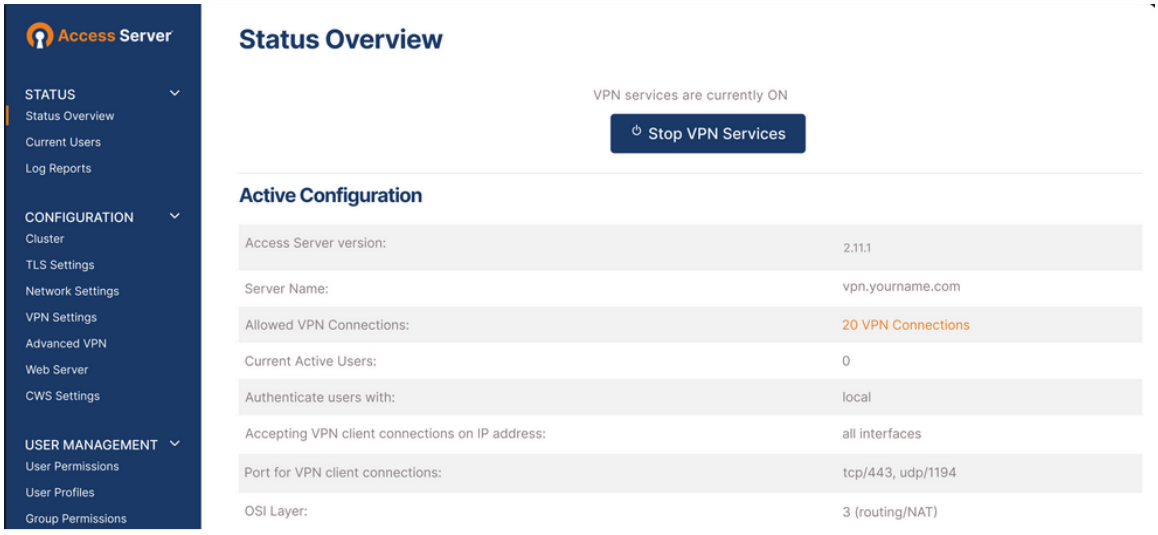
OpenVPN-palvelimia voi olla käyttötarkoituksen perusteella yksi tai useampia. Palvelimen tai palvelimien kanssa on hyvä noudattaa yleisesti tiedossa olevia ja suositeltuja periaatteita niin konfiguroinnin, käytön sekä turvallisuudenkin suhteen.

OpenVPN avoimen lähdekoodin palvelin tukee useampaa eri käyttöjärjestelmää, kuten tunnetuimpia Linux jakelupaketteja, Windows-käyttöjärjestelmän eri versioita sekä Windows Server -käyttöjärjestelmän eri versioita. (OpenVPN n.d.a). On kuitenkin hyvä huomioida, että suurin osa OpenVPN yhteisöversion ohjeista ja dokumentaatiosta on suunnattu nimenomaan eri Linux-versioille.

GNU GPU lisenssin alla julkaistun OpenVPN yhteisöversion palvelimen hallinta tapahtuu kokonaan komentorivin kautta, riippumatta käyttöjärjestelmästä. Vaihtoehtoisesti kolmannen osapuolen tarjoamia graafisen käyttöliittymän projekteja on saatavilla esimerkiksi GitHub alustalta, mutta nämä vaikuttavat olevan lähinnä suunnattuja pienelle määrälle yhteyksiä, esimerkiksi kotiverkkojen OpenVPN-yhteyksien hallintaan. Näin ollen käyttäjän tulee olla hyvin perehtynyt valitsemansa käyttöjärjestelmän toimintaan, jonka päällä haluaa OpenVPN-palvelinta ylläpitää.

Vaihtoehtoisesti OpenVPN tarjoaa maksullisia ratkaisuja palvelimen ylläpitoon. Näistä CloudConnexa® on pilviympäristössä toimiva OpenVPN palvelinverkosto

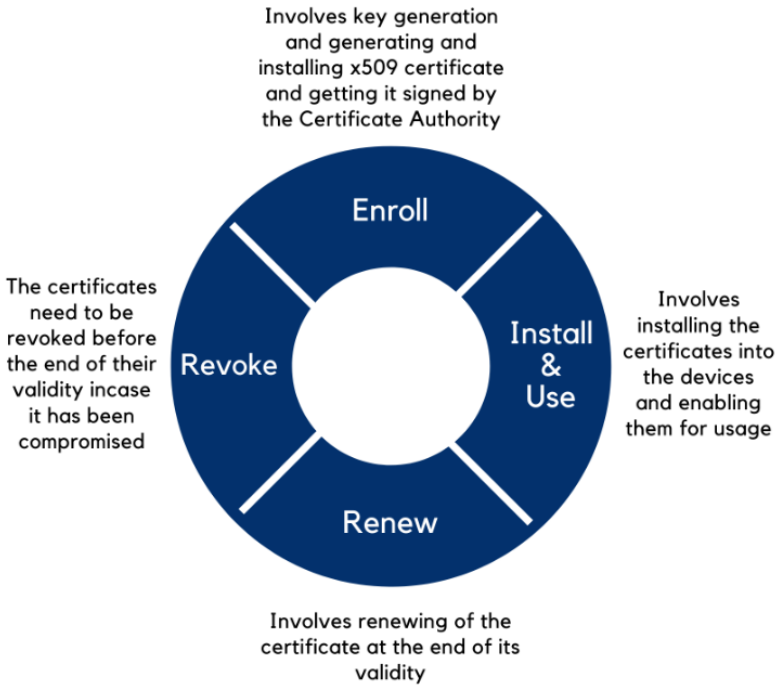
ja Access Server puolestaan paikallisesti, omassa verkossa tai pilvessä ylläpidetty palvelin, joka on rakennettu OpenVPN avoimen lähdekoodin pohjan päälle. Sekä CloudConnexa®:n että Access Serverin käyttöympäristö ovat täysin visualisoitu graafisella käyttöliittymällä. Kuviossa 11 havainnollistetaan Access Serverin graafista käyttöliittymää. Access Serveriä on mahdollista ylläpitää myös täysin internetissä erotetussa verkossa. (OpenVPN n.d.a).



KUVIO 11. OpenVPN Access Serverin graafinen käyttöliittymä. (OpenVPN n.d.a).

4.5 Elinkaarenhallinta

Jokaisen PKI-ympäristössä toimivan varmenteen, kuten OpenVPN-varmenteiden elinkaarenhallinta voidaan jakaa neljään osaan, varmenteiden luomiseen (Enroll), asennukseen ja käyttöön (Install & Use), uusimiseen (Renew) ja perumiseen (Revoke), kuten kuviossa 12. havainnollistetaan. Lisäksi elinkaaren hallintaan voidaan sisällyttää vielä analysointi sekä seuranta, missä analysoinnilla tarkoitetaan nimenomaan oikeanlaisen varmenteen luomista halutulle laitteelle riippuen käyttötarkoituksesta, -ajasta sekä sijainnista. Seurannalla tarkoitetaan varmenteen käytön, tilan sekä voimassaoloajan seurantaa.



KUVIO 12. PKI varmenteen elinkaari. (Krishnan et al 2022.).

Varmenteiden luominen sisältää sekä julkisen että yksityisen avaimen luomisen, varmenteen allekirjoittamispyynnön sekä sen allekirjoittamisen varmentajan toimesta. Varmenteen luomisen jälkeen varmenne tulee sijoittaa laiteeseen, jossa varmennetta tullaan käyttämään. Varmenne tulisi säilyttää laitteella turvallisesti, mutta opinnäytetyössä ei oteta laitepuolen säilytykseen tämän enempää kantaa. Kun varmenne on sijoitettu laitteelle, voidaan varmennetta hyödyntää aktiivisesti VPN yhteyden muodostamiseen. Varmenteita sekä varmenteita käyttäviä laitteita tulee seurata aktiivisesti niiden koko elinkaaren aikana mahdollisen vuotamisen varalta. Mikäli varmenne todetaan vuotaneeksi, voidaan se perua eli poistaa käytöstä ennen varmenteen vanhenemista. (Krishnan et al 2022.). Elinkaaren lopussa varmenne vanhenee ja näin poistuu automaattisesti käytöstä. Tilanteessa, missä laite, joka hyödyntää varmennetta poistuu ennen varmenteen elinkaaren umpeutumista käytöstä, tulisi myös varmenne poistaa käytöstä samanaikaisesti.

4.6 Varmentajan varmenteet ja toiminta OpenVPN-ympäristössä

Varmenteiden ja erityisesti CA:n varmenteiden hallintaan tulee kiinnittää erityistä huomiota. Varmenteet voidaan luokitella arkaluontoisiksi tiedoiksi ja varmenteiden käsittelyssä sekä hallinnassa tämä tulee ottaa huomioon. CA:n varmenteet ovat niin kutsuttuja juurivarmenteita, jotka ovat CA:n itsensä allekirjoittamia eli varmentamia ja mikäli CA:n varmenne vuotaa, on koko CA:n alaisuudessa ollut PKI vaarantunut.

OpenVPN palvelin tukee yksityisen PKI:n käyttöä sekä oman varmentajan käyttöä OpenVPN 2.x konfiguraatiossa, joka noudattaa X.509-standardin periaatteita. Näin ollen palvelin tarvitsee vain oman varmenteensa, jonka CA on allekirjoittanut eikä sen tarvitse erikseen tuntea OpenVPN-yhteyden muodostamista pyrkivien laitteiden varmenteita, vaan henkilöllisyyden varmistamiseksi riittää yhteyden muodostamista pyrkivän laitteen varmenteen allekirjoituksen varmistaminen. CA:n ei tarvitse olla samassa laitteessa tai verkossa OpenVPN-palvelimen kanssa ja se voi olla kokonaan irtikytkettynä verkosta. (OpenVPN n.d.c).

Kuviossa 12 esitellään CA:n avaimen luomista OpenVPN-palvelimen käyttöön easy-rsa -paketilla, joka on openssl-komentoriviin perustuva paketti. Paketti toimii skriptiluontoisesti ja järjestelee var-arvot automaattisesti ja luo varmenteen kansioon, josta skripti ajetaan.

```
ai:easy-rsa # ./build-ca
Generating a 1024 bit RSA private key
...........++++++
..........++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [KG]:
State or Province Name (full name) [NA]:
Locality Name (eg, city) [BISHKEK]:
Organization Name (eg, company) [OpenVPN-TEST]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:OpenVPN-CA
Email Address [me@myhost.mydomain]:
```

KUVIO 13. CA:n avaimen luonti. (OpenVPN n.d.c).

Kuviossa 13 esitetään eri varmenteet ja avaimet sekä niiden käyttötarkoitukset ja tarpeet. Kuten kuviosta 14 voidaan tulkita, CA:n ca.crt-tiedoston tarvitsevat OpenVPN-palvelin sekä jokainen yhteyttä muodostava laite, kun puolestaan ca.key-tiedoston tarvitsee ainoastaan avaimia allekirjoittava palvelin.

Filename	Needed By	Purpose	Secret
ca.crt	server + all clients	Root CA certificate	NO
ca.key	key signing machine only	Root CA key	YES
dh{n}.pem	server only	Diffie Hellman parameters	NO
server.crt	server only	Server Certificate	NO
server.key	server only	Server Key	YES
client1.crt	client1 only	Client1 Certificate	NO
client1.key	client1 only	Client1 Key	YES
client2.crt	client2 only	Client2 Certificate	NO
client2.key	client2 only	Client2 Key	YES
client3.crt	client3 only	Client3 Certificate	NO
client3.key	client3 only	Client3 Key	YES

KUVIO 14. Lista OpenVPN:n tarvitsemista avaimista ja varmenteista (OpenVPN n.d.c).

5 YHTEENVETO

Tietoa X.509-standardin julkisen avaimen infrastruktuurin hyödyntämistä OpenVPN-yhteyksien muodostamiseen niin sanotussa yksityisessä verkossa löytyi opinnäytetyötä tehdessä varsin suppeasti ja aihetta käsitelleet tutkimusartikkelit olivat varsin suppeita. Näin ollen opinnäytetyössä on koostettu tietoa useamman tutkimusartikkelin, verkkosivun sekä kirjan sisällöstä OpenVPN yhteisöversion palvelimen käytöstä VPN-yhteyksien muodostamiseksi hyödyntäen OpenVPN-protokollaa sekä X.509-standardin mukaista julkisen avaimen infrastruktuuria yksityisessä verkossa.

Vuonna 2021 julkaistussa tutkimusartikkelissaan “Enhancing Digital Certificate Usability in Long Lifespan IoT Devices by Utilizing Private CA” Yamakawa et al ehdotti yksityisen CA:n käyttämistä pilvipohjaisissa IoT-arkkitehtuureissa, jolloin yritykset voivat itse hallinnoida varmenteita sekä varmentajaa. Pilvipohjaisessa yksityisen PKI:n ja varmentajan käytössä voidaan julkisen CA:n käytön riskit minimoida. Schukat & Cortijon vuonna 2015 julkaistussa tutkimusartikkelissa “Public key infrastructures and digital certificates for the Internet of things.” käsitteli julkisen avaimen infrastruktuuria IoT-ympäristöissä sekä julkisen CA:n käytön riskejä IoT-ympäristössä. Artikkelissaan Schukat & Cortijo kyseenalaistavat tarpeen hyödyntää julkisia, maailmanlaajuisia varmentajia, etenkin jos IoT-laitteet ovat omassa ympäristössään. Sekä Schukat (2014) että Díaz-Sánchez et al. (2019) käsittelivät tutkimusartikkeleissaan TLS:n käyttöä PKI:n yhteydessä M2M-, ja IoT-ympäristöissä. Molemmissa artikkeleissa todetaan, että TLS on tunnettu, testattu ja vakiintunut menetelmä IoT-, ja M2M-ympäristöjen VPN-yhteyksien varmentamiseen PKI-ympäristössä. Kuitenkin sekä Schukat että Díaz-Sánchez et al. muistuttavat, että menetelmä ei ole aukoton ja suosittelevat menetelmän vahvistamista, esimerkiksi varmenteen kiinnittämisellä. Suosittelenkin lukemaan nämä edellä mainitut artikkelit IoT-, tai M2M-ympäristön PKI-ratkaisuja suunnitteleville.

Näin ollen opinnäytetyössä on käynyt selkeästi esille, että IoT-järjestelmien VPN-yhteyksien varmentamiseen tietoturvallisin ratkaisu on nimenomaan hyödyntää X.509-standardin mukaista PKI:ta OpenVPN -protokollan sekä -palvelimen kanssa. Kuten aiemmin mainitsin X.509-standardi ei itsessään ole aukoton, mutta se lienee tietoturvan, käytettävyyden ja muokattavuuden kannalta paras pohjaratkaisu VPN-yhteyden varmistamiselle. On hyvä huomioida, että opinnäytetyössä ei arvioitu muita VPN-protokollia tai vertailtu näiden tehokkuuksia. Opinnäytetyö on tehty sen olettamuksen pohjalta, että yksittäisen IoT-laitteen tietoliikenne ei vaikuta OpenVPN-palvelimen suorituskykyyn merkittävästi.

Tietoturvan tasoa OpenVPN-ympäristössä voidaan lisätä hyödyntämällä varmenteiden kiinnitystä nimetylle laitteelle, jolloin varmenteen väärinkäyttämisestä tulee huomattavasti haastavampaa. X.509-standardin mukainen PKI:n toteuttaminen IoT-ympäristössä käyttämällä useampaa CA:ta on suositeltavaa mikäli IoT-laitteiden määrä on suuri. Useamman CA:n hierarkisella ympäristöllä voidaan rajata esimerkiksi eri kohteiden tai mahdollisten asiakkuuksien laitteiden pääsy muihin OpenVPN-palvelimiin, jolloin toimintaympäristön hygienia säilyy hyvänä. Tämä on mahdollista toteuttaa myös useammalla verkkoadapterilla ja palomuureilla, mutta skaalautuvassa IoT-ympäristössä tämä ei liene järkevin toimintamalli. Mikäli ympäristössä päädytään käyttämään useamman CA:n hierarkiaa, tulisi ylimmän tason CA ideaalisessa tilanteessa olla vähintään täysin irrotettuna julkisesta verkosta, sillä lähtökohtaisesti ensimmäisten varmenteiden ja avainparien luomisen jälkeen ei kyseisellä palvelimella tarvitse muutoin asioida poikkeustilanteita lukuun ottamatta.

OpenVPN-palvelimen tai palvelimien, niin kuin kaikkien palvelimien kanssa tulisi noudattaa vähimmän oikeuden periaatetta. Mikäli OpenVPN-palvelin tai palvelimet ovat kriittisiä yrityksen toiminnalle, tulisi palvelimilla aina olla niin sanottu failover-palvelin, johon VPN-yhteydet automaattisesti ohjataan, jos niin sanottu pääpalvelin lakkaa jostain syystä toimimasta. Tämä on myös mahdollista toteuttaa ilman failover-palvelinta hyödyntämällä palomuurisääntöjä sallimalla esimerkiksi suora yhteys IoT-laitteen omaan IP-osoitteeseen, mutta tämän osalta herää kysymys tietoturvallisuudesta, sillä tällöin liikenne on lähtökohtaisesti selkokielistä

tai vähintäänkin salaamatonta. OpenVPN-palvelimien osalta useamman palvelimen käyttäminen on suositeltavaa, mikäli samanaikaisia VPN-yhteyksiä on suuri määrä.

Varmenteiden kohdalla on järkevää käyttää 256-bittistä SHA:ta, joka on varsin riittävä kestämään mahdollisia brute-force -hyökkäyksiä pitkälle tulevaisuuteen. Avainten luomiseen voi olla järkevää käyttää erillistä palvelinta, mikäli IoT-laitteiden määrä on suuri. Tällöin mahdolliseen avainpalvelimeen ja sen tietoturvaan tulisi kiinnittää tarkasti huomiota. Verkkoyhteyksien osalta operaattorin tarjoamat yksityiset APN-ratkaisut lienevät kustannustehokkaimmat ratkaisut julkisesta verkosta erotetulle verkolle. Yksityiset APN-ratkaisut luotettavilta operaattoreilta tuovat pohjalle myös IoT-ympäristön käyttöön riittävän tietoturvallisuuden tason.

Liitteissä 1 ja 2 on esitelty esimerkin muodossa yksinkertaista ja tietoturvallista verkon topologiaa fiktionaalisessa toimisto- sekä palvelinympäristössä. Liitteessä 1 esitellään toimistoverkon topologiaa, jossa on havainnollistettu toimistoympäristössä yleisesti löytyviä palvelimia sekä päätelaitteita. Palvelimet ovat värikoodattu keltaiseen sekä punaiseen alueeseen, missä keltainen alue tarkoittaa palvelimia, jotka ovat jatkuvasti yhteydessä verkkoon, toimien esimerkiksi alemman tason varmentajina. Punaisella värillä koodattu palvelin esittää puolestaan ylimmän tason varmentajaa, jonka tulisi olla verkkoon aktiivisesti yhteydessä ainoastaan uusien varmentajien luomisen yhteydessä.

Liitteessä 2 on puolestaan havainnollistettu palvelinympäristön verkon topologiaa. Palvelimet on eroteltu värikoodauksella vihreään sekä harmaaseen alueeseen, missä vihreä alue tarkoittaa aktiivisia, käytössä olevia palvelimia ja harmaa alue puolestaan niin sanottuja failover- tai backup-palvelimia. Esitetyt palvelimet voivat toimia osana julkisen verkon infrastruktuuria alemman tason varmentajina tai VPN-palvelimina. Tämä esimerkki verkon topologiasta toimii suosituksena yksinkertaisen PKI-ympäristön rakentamiseen, ottamatta sen enempää kantaa ympäristön laitteisiin tai toimintaan, kuten palomuurien konfiguraatioihin.

LÄHTEET

Ashbourn, J. 2023. *PKI Implementation and Infrastructures*. E-Kirja. First edition. Vol. 1. Milton: CRC Press. Vaatii käyttöoikeuden. https://learning.oreilly.com/library/view/pki-implementation-and/9781000844962/

Barker, E., & Dang, Q. 2015. Recommendation for key management. National Institute of Standards and Technology. Viitattu 14.12.2023. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-57pt3r1.pdf

Barki, A., Bouabdallah, A., Gharout, S. & Traoré, J. 2016. M2M Security: Challenges and Solutions. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18. NO. 2. Viitattu 28.12.2023. Vaatii käyttöoikeuden. https://ieeexplore.ieee.org/document/7373528

Cloudflare. N.d. What is the OSI Model?. Cloudflare. Viitattu 27.12.2023. https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

Cooper, D., Santesson, S., Farrell, S., Boyen, S., Housley, R. & Polk, W. 2008. X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile. Network Working Group. Viitattu 20.12.2023. https://www.ietf.org/rfc/rfc5280.txt

Díaz-Sánchez, D., Marín-Lopez, A., Medonza, F.A., Cabarcos, P.A. & Sherratt, R. S. 2019. TLS/PKI Challenges and Certificate Pinning Techniques for IoT and M2M Secure Communications. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 21, NO 4. Viitattu 21.12.2023. https://ieeexplore.ieee.org/document/8704893

DNA. N.d. Asiakaskohtainen APN. DNA. Viitattu 27.12.2023. https://www.dna.fi/yrityksille/tietoliikenneyhteydet/yrityskohtainen-apn

Fortinet. N.d. CIA Triad. Fortinet. Verkkosivu. Viitattu 20.12.2023. https://www.fortinet.com/resources/cyberglossary/cia-triad

Keyfactor. N.d. What is PKI? A Public Key Infrastructure Definitive Guide. Keyfactor. Verkkosivu. Viitattu 20.12.2023. https://www.keyfactor.com/education-center/what-is-pki/

Krishnan, A. A., Rajendran, S.K, Sunil Kumar, T.K. 2022. Improved PKI Certificate Lifecycle Management With Centralized Device Management For Indrustial IoT. IEEE International Conference on Public Key Infrastructure and its Applications (PKIA). Viitattu 22.1.2024. https://doi.org/10.1109/PKIA56009.2022.9952216

Likhar, P., Yadav, R.S. & Rao, K.M. 2011. Securing IEEE 802.11g WLAN Using Open VPN and its Impact Analysis. International Journal of Network Security & Its applications (IJNSA), VOL. 3, NO. 6. Viitattu 28.12.2023. http://dx.doi.org/10.5121/ijnsa.2011.3607

OpenVPN. N.d.a Access Server or CloudConnexa® Which secure networking solution is right for you?. OpenVPN. Viitattu 27.1.2024. https://openvpn.net/product-comparison/

OpenVPN. N.d.b Overview of OpenVPN. OpenVPN. Viitattu 27.12.2023. https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn

OpenVPN. N.d.c Setting up your own Certificate Authority (CA). OpenVPN. Viitattu 27.1.2024. https://openvpn.net/community-resources/setting-up-your-own-certificate-authority-ca/

Shuckat, M. 2014. Securing Critical Infrastructure. IEEE. Viitattu 27.1.2024. https://ieeexplore.ieee.org/document/6868731

Shuckat, M., & Cortijo, P. 2015. Public key infrastructures and digital certificates for the Internet of things. IEEE. Viitattu 21.12.2023. https://ieeexplore.ieee.org/document/7163785

Skendzic, A., & Kovačić, B. 2017. Open source system OpenVPN in a function of Virtual Private Network. IOP Conference Series Materials Science and Engineering. 200 012065. IOP Publishing. Viitattu 28.12.2023. doi:10.1088/1757-899X/200/1/012065

Statista. 2023. Number of IoT connected devices worldwide from 2019 to 2023, by vertical (in millions). Statista Inc. Viitattu 26.1.2024. https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/

Stojmenovic, I. 2014. Machine-to-Machine Communications With In-Network Data Aggregation, Processing, and Actuation for Large-Scale Cyber-Physical Systems. IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 2. Viitattu 21.12.2023. Vaatii käyttöoikeuden. https://ieeexplore.ieee.org/document/6766661

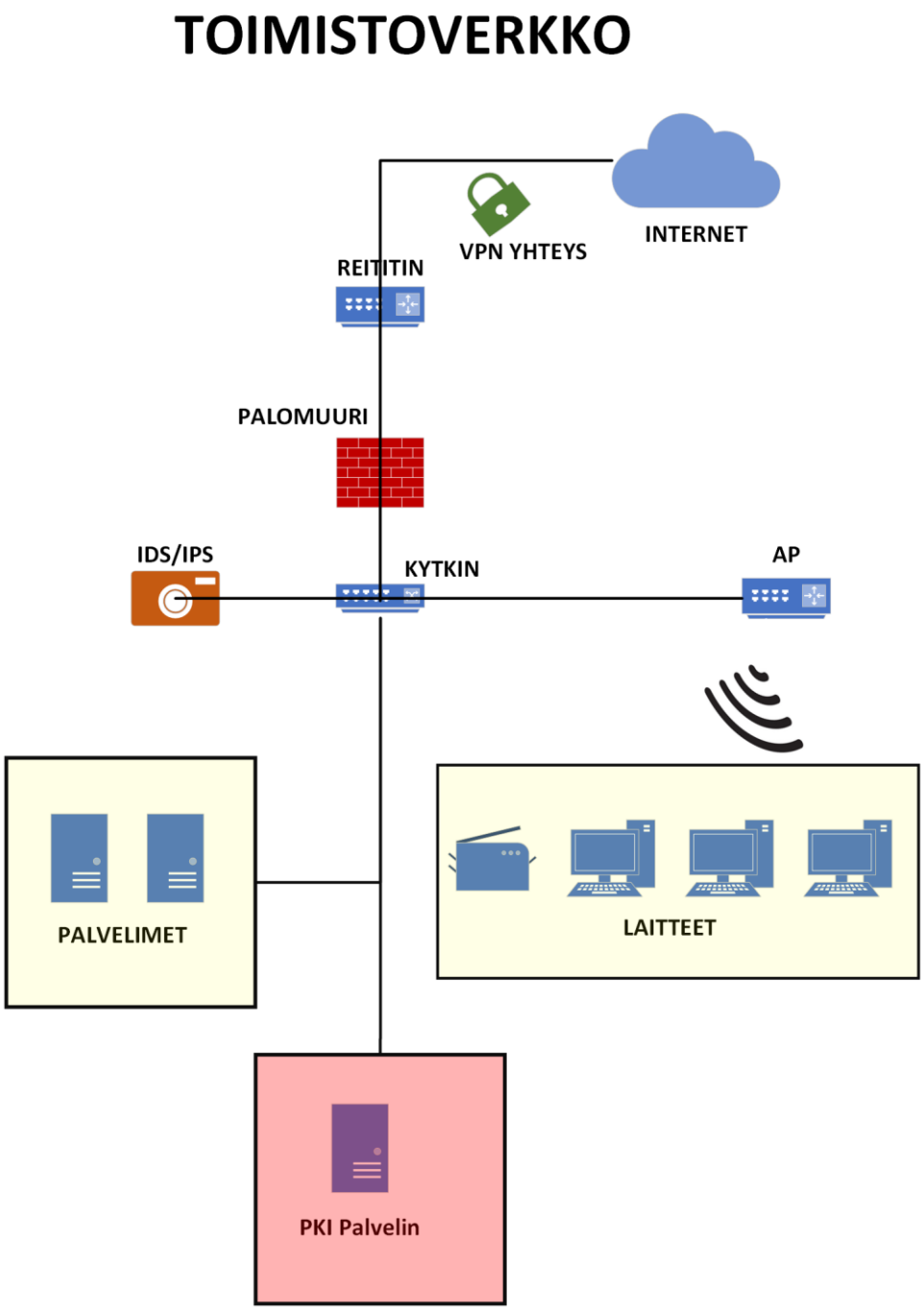
Vailshery, L.S. 2023. Number of IoT connected devices worldwide 2019-2023, with forecasts to 2030. Statista. Viitattu 14.1.2024. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Yamakawa, D., Okimoto, T., Teerakanok, S., Inomata, A. & Uehara, T. 2021. Enhancing Digital Certificate Usability in Long Lifespan IoT Devices by Utilizing Private CA. Hindawi. Viitattu 21.12.2023. https://doi.org/10.1155/2021/6610863

LIITTEET

Liite 1. Esimerkki toimistoverkon topologiasta

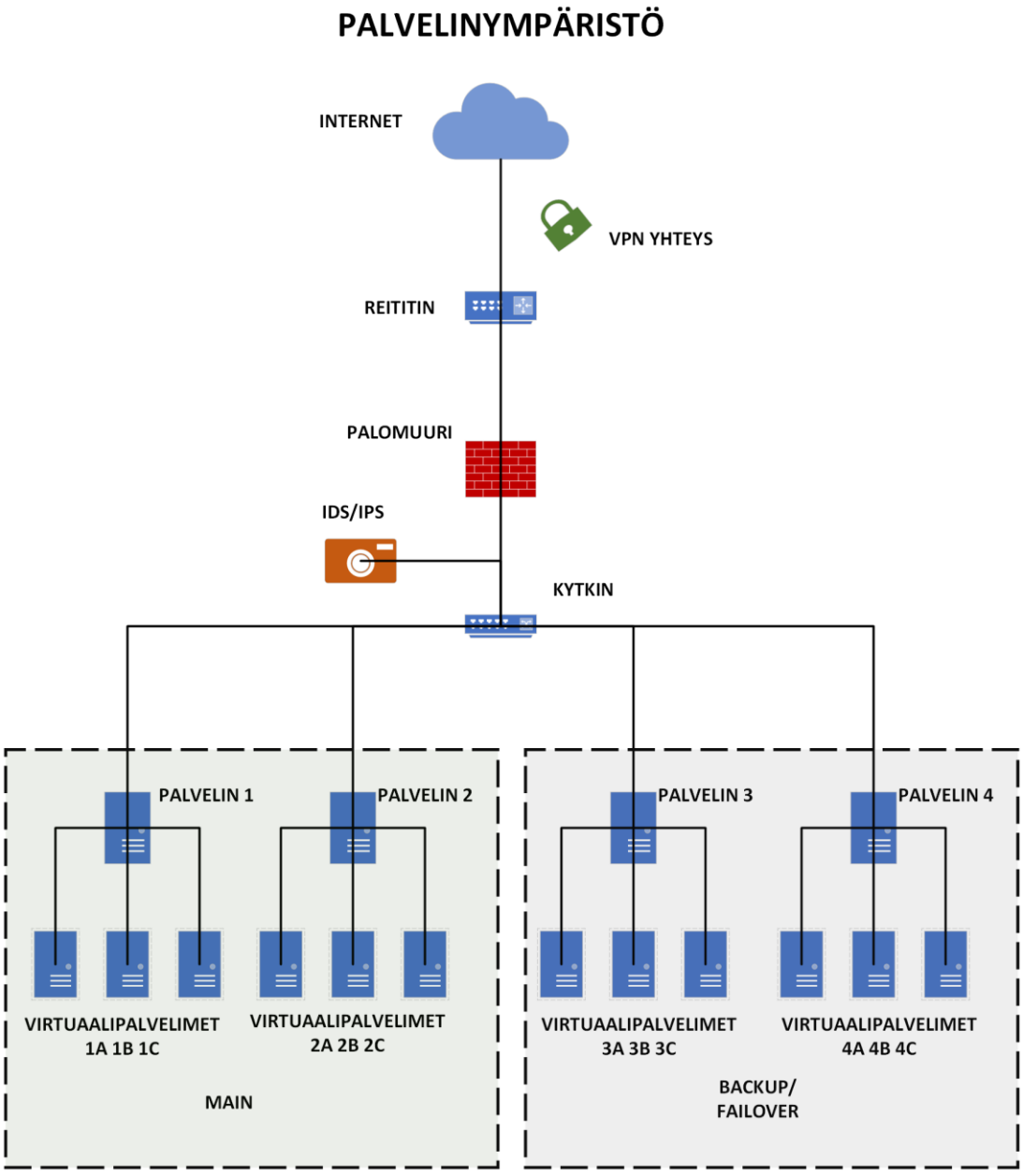
1(2)



Kuviossa on havainnollistettu fiktionaalisen toimistoverkon topologiaa, missä PKI-palvelin voi toimia ylemmän tason CA:na, palvelimet voivat olla esimerkiksi OpenVPN ja niin sanottu avainpalvelin. Värikoodit voivat havainnollistaa myös käyttöoikeuden myöntämisen kriteerejä, missä keltainen on kevyemmin perustein myönnettävissä ja punainen puolestaan tiukemmin perustein myönnettävissä.

Liite 2. Esimerkki palvelinverkon topologiasta.

1(2)



Kuviossa on havainnollistettu fiktionaalisen palvelinympäristön yksinkertaista verkon topologiaa, missä vihreällä värikoodattu alue toimii niin sanottuna pääpalvelinympäristönä ja harmaalla värikoodattu alue toimii varapalvelinympäristönä. Palvelimet voivat olla esimerkiksi alemman tason varmentajia, OpenVPN-palvelimia tai avainpalvelimia. Todellisuudessa sekä palvelimia että palvelinympäristöjä tulisi säännöllisesti yliheittää, jolloin tuoreimmat varmuuskopiot sekä päivitykset voidaan muodostaa ja ladata ilman käyttökatkoja sekä mahdolliset viat ja häiriöt havaitaan ennen niin sanottua todellista failover-tilannetta.