Kvanttilaskennan tietoturvavaikutukset - suositus varautua

Huoltovarmuuskeskus

Huoltovarmuuskeskus

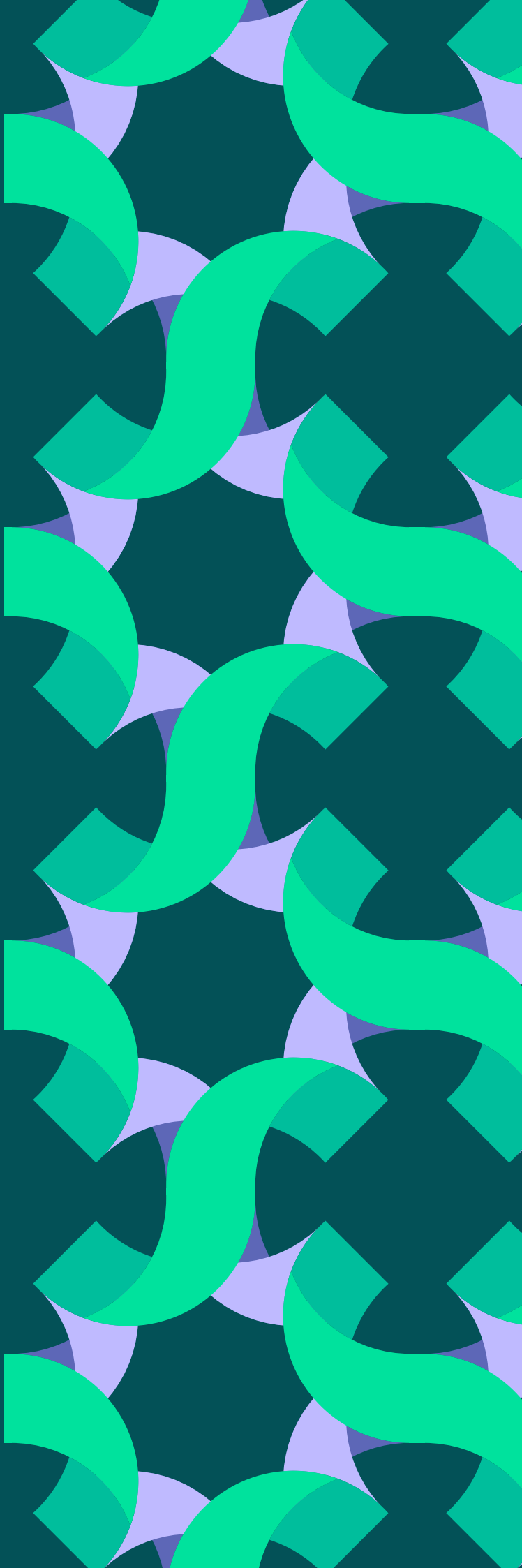
www.huoltovarmuuskeskus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.

Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Huoltovarmuusorganisaatio (HVO) on verkosto, joka työskentelee yhdessä Suomen toimintakyvyn ja sen edellyttämän huoltovarmuuden hyväksi. Siihen kuuluvat Huoltovarmuuskeskus ja sen hallitus, huoltovarmuusneuvosto sekä eri toimialojen sektorit ja poolit. Lisäksi yhteistyötä tehdään alueellisten toimijoiden, kuten aluehallintovirastojen, kuntien ja kaupunkien sekä alueellisten toimikuntien kanssa.

Julkaisija: Huoltovarmuuskeskus
Laatinut: Huoltovarmuusorganisaation Digipooli ja Vtt Oy
Kansikuva: Gettyimages
Taitto: LM Someco Oy
Julkaisuvuosi: 2024
ISBN: 978-952-7470-33-6



Sisältö

Johdanto

Tämän ohjeen tavoitteena on selventää lukijalle kvanttilaskennan hyötyjen lisäksi sen aiheuttama uhka kyberturvallisuudelle. Toisena tavoitteena on esittää toimenpiteitä, joiden avulla organisaatio voi turvata tietonsa kvanttiuhalta. Tavoitteeseen pääsemiseksi lukija perehdytetään ensin lyhyesti kvanttilaskennan vaikutuksiin kyberturvallisuuden näkökulmasta. Tämän jälkeen luodaan katsaus olemassa olevaan kirjalliseen materiaaliin keskittyen suunnitelmiin (”tiekartta”, road map), joita eri tahot ovat tehneet kvanttiuhkaan varautumiseksi. Kirjallisuuskatsauksen toisessa osassa keskitytään eri maiden kansallisiin ohjeistuksiin kvanttiuhkaan varautumisesta.

Kirjallisuuskatsauksen jälkeen esitetään tilannekatsaus suomalaisten huoltovarmuuskriittisten yritysten varautumisesta kvanttiuhkaan. Tilannekatsauksen tiedot on kerätty yrityksille suunnatulla kyselyllä, jota on täydennetty asiantuntijahaastattelulla. Katsaus osoittaa, että suomalainen elinkeinoelämä ei ole ymmärtänyt kvanttilaskennan aiheuttaman kyberuhan vaikutuksia ja on siksi myös huonosti siihen varautunut. Tämä vaarantaa yritysten kriittiset tiedot ja toiminnan häiriöttömyyden sekä edelleen suomalaisen yhteiskunnan huoltovarmuuden.

Lopuksi esitetään kirjallisuus- ja tilannekatsauksiin perustuva suunnitelma (road map) varautumisesta kvanttiuhkaan. Ohje päätetään keskeisiin johtopäätöksiin ja toimenpidesuosituksiin.

Kvanttilaskenta tuo mukanaan huiman laskentatehon mutta myös uusia uhkia kyberturvallisuudelle

Kvanttilaskennalla on keskeinen rooli käynnissä olevassa teknologisessa murroksessa. Kvanttilaskenta ei korvaa perinteistä tietojenkäsittelyä. Tietyillä sovellusalueilla kvanttilaskenta on kuitenkin täysin ylivertainen verrattuna perinteiseen tietojenkäsittelyyn. Kvanttitietokoneiden avulla voidaan ratkaista ongelmia, jotka ovat käytännössä mahdottomia tai hyvin vaikeita perinteisille supertietokoneille.

Tällaisia sovellusalueita voivat tulevaisuudessa olla esimerkiksi:

- Laajat optimointiongelmat logistiikassa ja taloudessa.
- Uusien lääkeaineiden ja materiaalien suunnittelu. Kvanttitietokoneilla voidaan simuloida molekyylien ja kemiallisten reaktioiden käyttäytymistä erittäin tarkasti ja nopeasti.
- Koneoppiminen: kvanttitietokoneet voivat parantaa huimasti koneoppimisalgoritmien suorituskykyä mahdollistaen entistä monimutkaisemmat mallit ja suuremmat tietojoukot.
- Sään ennustaminen. Kvanttilaskenta mahdollistaa sääilmiöiden tarkan ja nopean simuloinnin mahdollistaen ajallisesti ja paikallisesti tarkat sääennusteet.
- Fysiikan ilmiöiden simulointi. Kvanttilaskenta mahdollistaa esimerkiksi hiukkas- ja kvanttifysiikan ilmiöiden tarkan simuloinnin.

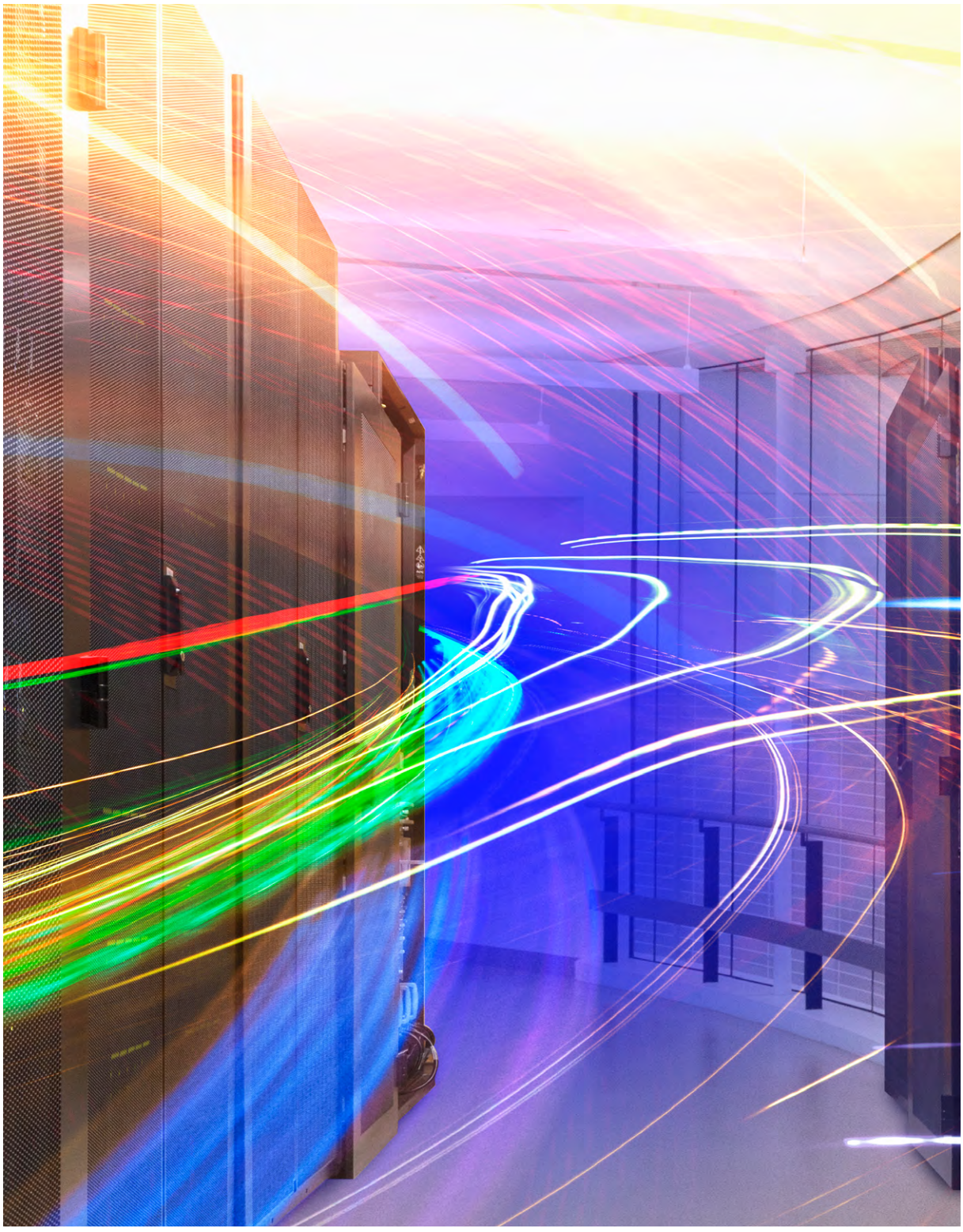
Kvanttitietokoneilla voidaan ratkaista valtavia haasteita, mutta niiden suurta laskentatehoa voidaan myös käyttää väärin. Kvanttilaskennan kehitys aiheuttaa merkittävän uhan nykyisille tiedon ja tietoliikenteen salausratkaisuille. Jo pelkästään taloudellisista syistä merkittävimmät uhat liittyvät valtiollisiin toimijoihin: vihamielisen valtion käsissä kvanttikone uhkaa muiden valtioiden kansallista turvallisuutta ja huoltovarmuutta. Tämä koskee myös Suomea. Esimerkiksi Kiina investoi kymmeniä miljardeja euroja kvanttiteknologian kehitykseen. Venäjäkin on kertonut tavoitteestaan kehittää kvanttitietokone sotilaalliseen maanpuolustukseen, joskin maan taloudellinen tilanne ja talouspakotteet heikentävät mahdollisuuksia kvanttiteknologian kehitykseen, joten heidän nykyinen kvanttilaskenta kapasiteettinsa on samalla tasolla kuin Suomessa.

Tietoja salataan tänä päivänä sekä symmetrisen eli salaisen avaimen että julkisen avaimen menetelmillä. Kvanttiuhka kohdistuu erityisesti julkisen avaimen menetelmiin, joita käytetään muun muassa sähköisissä allekirjoituksissa. Myös monet Internetissä laajalti käytetyt salausmenetelmät, esim. TLS (Transport Layer Security) ja PGP (Pretty Good Privacy), perustuvat julkisen avaimen salaukseen.

Kvanttikoneen avulla tehtäviltä hyökkäyksiltä voidaan suojautua vahvistamalla nykyisiä symmetrisiä salauksia kasvattamalla salausavaimen pituutta, kun taas julkisen avaimen menetelmissä tarvitaan kokonaan uusia algoritmeja. Uusia menetelmiä on jo olemassa, ja niiden standardointi valmistuu vuonna 2024. Näiden menetelmien käyttöönottoon pitää valmistautua nyt, jotta kriittisten tietojen ja järjestelmien turvallisuus voidaan taata myös tulevaisuudessa.

Suomi on edelläkävijä kvanttitietokoneiden kehityksessä, ja voimme olla sitä myös kvanttisuojauksessa. Osaamista meillä on, mutta tarvitsemme nyt käytännön toimia. Toisaalta kvanttiturvallinen suojauskaan ei riitä, jos nykyisten salausratkaisujen hallinnointi ja toteutus on rempallaan tai niitä ei edes tiedetä – kokonaisuus ratkaisee.

Kirjoittajat
Erikoistutkija Visa Vallivaara, Sovellettu kryptografia, VTT
Tutkija Mari Muurman, Sovellettu kryptografia, VTT
Tutkija Outi-Marja Latvala, Sovellettu kryptografia, VTT
Lead, Kyberturvallisuus, Petri Puhakainen, VTT



Kvanttilaskennan vaikutukset kyberturvallisuuteen

Kvanttilaskenta pohjautuu kvanttimekaniikan ilmiöihin. Bittien sijaan kvanttitietokoneet käyttävät kvanttibittejä eli kubitteja mahdollistaen tiettyjen ongelmien ratkaisun nopeammin kuin perinteisiä supertietokoneita käyttäen.

Kvanttitietokone on klassista tietokonetta tehokkaampi silloin, kun pitää simuloida reaalimaailman tapahtumia, joissa vaikuttaa kvantti-ilmiöitä, kuten sään ennustaminen. Kvanttilaskenta on klassista laskentaa nopeampi myös silloin, kun pitää ratkaista ongelmia, joissa on todella paljon kombinaatioita. Kvanttitietokoneen kykyä tehokkaampaan laskentaan voidaan mahdollisesti hyödyntää esimerkiksi optimointiongelmissa, jotka ovat liian monimutkaisia perinteisen tietokoneen ratkaistaviksi. Tällainen ongelma voi liittyä esimerkiksi logistiikkaan tai resursointiin. Oikein käytettynä kvanttilaskennan hyödyntämisellä voidaankin parantaa yhteiskunnan huoltovarmuutta. Vaikka kvanttilaskenta on vasta kehitysvaiheessa, se on hyötyjensä lisäksi myös uhka kyberturvallisuudelle ja huoltovarmuudelle.

Käytännöllisen kvanttikoneen avulla on mahdollista murtaa nykyiset julkisen avaimen salausmenetelmät. Ne perustuvat matemaattisiin ongelmiin, jotka ovat erittäin vaikeita ratkaista perinteisellä tietojenkäsittelyllä (ns. klassisella laskennalla), mutta jotka ovat helppoja kvanttitietokoneelle. Tällaisia ongelmia ovat esimerkiksi isojen lukujen tekijöihin jako, diskreetin logaritmin ongelmat äärellisissä kunnissa sekä diskreetin logaritmin ongelmat elliptisissä käyrissä. Edes nykyiset supertietokoneet eivät kykene ratkaisemaan kyseisiä ongelmia järjellisessä ajassa – päinvastoin kuin kvanttitietokoneet. Kvanttilaskentaa hyödyntävällä Shorin algoritmilla kyetään ratkaisemaan nykyisten julkisen avaimen salausmenetelmien perusteena olevat matemaattiset ongelmat tehokkaasti.

Kvanttiturvalliseen salaukseen, Post-Quantum Cryptography (PQC), tarvitaankin uudenlaisia matemaattisia ongelmia, joiden ratkaisemiseen ei ole tiedossa kvanttialgoritmia eli niiden ratkaiseminen on vaikeaa sekä klassisella että kvanttitietokoneella. Parhaimmat PQC-algoritmit ovat tällä hetkellä hilapohjaisia (lattice) (lisätietoa algoritmeista löytyy tämän ohjeen kappaleesta ”PQC-tukimateriaali”)

Vaikka nykyisten kvanttikoneiden kubitit ovat virhealttiita, virheenkorjaus kehittyy varsin nopeasti. Muutenkin kehitystä tapahtuu sekä kvanttikoneissa että algoritmeissa. Koska kehitystä tapahtuu näin monella alueella, on vaikeaa arvioida tarkalleen, milloin erityisesti julkisen avaimen menetelmät voidaan murtaa kvanttitietokoneella. Eri asiantuntijoiden arviot vaihtelevat alle 10 vuodesta noin 20 vuoteen[1].

Esimerkiksi terveydenhuollon ja lääketieteellisen tutkimuksen yritykselle tämä saattaisi johtaa esim. seuraavien tietojen paljastumiseen:

(1) asiakastiedot (mm. nimet, osoitteet, mahdolliset sairaushistoriat ja diagnoosit),

(2) tutkimustiedot (mm. kliinisten tutkimusten tulokset, kehitteillä olevat uudet lääkkeet ja hoitomenetelmät) ja

(3) liiketoimintatiedot (mm. talous, strategiset suunnitelmat, sopimukset). Tällä olisi merkittävät oikeudelliset ja liiketoiminnalliset seuraukset puhumattakaan pitkäaikaisesta maineen menetyksestä.

1 2023 GRI Quantum Threat Timeline Report: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

Milloin on siirryttävä kvanttiturvallisiin salausmenetelmiin ja mitä se tarkoittaa?

Vaikka kryptografisesti merkittävän kvanttitietokoneen realisoituminen on tulevaisuutta, on sen vaikutuksiin varautuminen aloitettava nyt. Siihen on ainakin kolme hyvää syytä:

(1)
Salattua verkkoliikennettä voidaan tallentaa nyt ja purkaa se kvanttitietokoneen avulla myöhemmin. Tällaisen hyökkäyksen kohteena voivat olla pitkää säilyttämistä vaativat tiedot, kuten pankki- ja terveysdata. Lisäksi on tehtävä selkeä suunnitelma tilanteeseen, jossa tällainen aiemmin varastettu tieto puretaan ja mahdollisesti julkaistaan varastajan toimesta. Tällöin varaudutaan myös siihen, että tietojen varastaja antaa ne edelleen kolmannelle osapuolelle.

(2)
Järjestelmien päivittäminen kvanttiturvallisiksi on laaja ja aikaa vievä projekti, sillä se koskettaa joka tapauksessa useita järjestelmiä ja salausratkaisuita.

(3)
Kvanttiturvallisia salausratkaisuita on jo nyt saatavilla. Lisäksi kvanttiturvallisten salausalgoritmien standardointi on valmistumassa 2024.

Ensimmäisenä organisaatioiden tulisi kartoittaa nykyisin käyttämänsä salausmenetelmät sekä tunnistaa, mitkä ovat kriittisimmät salassa pidettävät tiedot ja niiden ajallinen salassapitotarve. Kartoituksessa auttaa kryptoinventaarion laatiminen. Tämän pohjalta voidaan analysoida, mitkä järjestelmät tarvitsevat päivittämistä ja samalla tunnistaa kriittisimmät kohteet. Kaikkea ei kannata päivittää kerralla, vaan siirtymä on syytä suorittaa vaiheittain. Kartoituksen pohjalta voidaan luoda konkreettinen suunnitelma (tiekartta, road map) sisältäen aikataulun kvanttiturvallisten menetelmien testauksesta niiden viemiseen tuotantoon asti. Yleinen suositus on siirtyä kvanttiturvallisiin menetelmiin vuoteen 2030 mennessä (esim. kts. seuraava kappale: DHS).

Yksi havainnollistava työkalu kvanttiuhan arvioimiseen on ”Moscan lause” (Kuva 1). Siinä PQC-siirtymän viemää aikaa + salassapitoaikaa verrataan relevantin kvanttitietokoneen kehityksen kestoon. Sillä voi laskea sen vuoden jolloin algoritmien vaihtaminen pitää aloittaa.

Moscan lause: 2024 + Q – X –Y, missä
Q on vuodet kryptografisesti merkittävään kvanttitietokoneeseen,
Y on vuodet jotka kuluvat algoritmien vaihtamiseen toimialallasi,
X on vuodet jotka tietojen on oltava luottamuksellisia.

Joten esimerkiksi Q = 20, Y = 5 ja X = 15 niin se tarkoittaa, että valmistautuminen on aloitettava jo tänä vuonna.

Kuva 1. Moscan lause

Siirtymän keskeinen työväline: kryptoinventaario

Yksinkertaistettuna kryptoinventaario on listaus kaikista käytetyistä salausmenetelmistä organisaatiossa. Inventaariossa kuvaillaan, mitä salausmenetelmää käytetään missäkin sovelluksessa mihinkin tarkoitukseen. Se voi sisältää tietoja algoritmeista, niiden käyttötavoista, avaimista ja avaintenhallinnasta, sertifikaateista, protokollaversioista, kirjastoversioista sekä ei-teknisiä tietoja, kuten tietojen turvaluokittelu, toimitusketjut ja vastuuhenkilöt.

Kryptoinventaarion avulla organisaatio voi valvoa turvallisia salauskäytäntöjä ja reagoida nopeasti turvallisuushaasteisiin. Se auttaa suorittamaan tehokkaasti strategisia muutoksia, kuten salauspalveluiden siirtämisen pilveen tai kvanttiturvallisten salausmenetelmien käyttöönottoa. Jotkut organisaatiot ovat ylläpitäneet kryptoinventaarioita jo vuosia, mutta konseptista on vasta viime aikoina tulossa valtavirtaa standardien[2] sekä asiantuntijoiden[3] suositusten ansiosta.

Käytännössä jokaisen organisaation inventaario on hieman erilainen riippuen siitä, miten ja missä salausta käytetään suhteessa organisaation kriittiseen toimintaan. Jos tavoitteena on valvoa salaussuunnitelmaa, sitten inventaarion on oltava vähintään yhtä yksityiskohtainen kuin itse suunnitelma. Esimerkiksi jos salausstrategia sallii tietyn salausalgoritmin vain tietyn protokollan yhteydessä, niin inventaarion tulee ottaa kantaa protokolliin. Jos suunnitelma määrittää, että vain tiettyjä salauskirjastoja käytetään, niin inventaariossa on listattava käytetyt salauskirjastot ja kirjastoversiot.

2 NIST Special Publication SP 800-57 - Key management recommendations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt2r1.pdf
3 Gartner, Better Safe Than Sorry: Preparing for Crypto-Agility: https://www.gartner.com/en/documents/3645384

Kirjallisuudessa esitettyjä lähestymistapoja kvanttiuhkaan varautumiseksi

Erilaisia varautumiskeinoja kvanttiuhkaa vastaan ovat julkaisseet esimerkiksi NIST (National Institute of Standards and Technology) ja DHS (The U.S. Department of Homeland Security)[4], IBM[5], Google[6] sekä NSA[7]. Kaikissa näissä dokumenteissa esitetään samankaltaisia vaiheita, joiden tavoitteena on varmistaa turvallinen ja hallittu siirtyminen kvanttiturvallisiin ratkaisuihin.

DHS julkaisi 2021 NIST:n kanssa yhteistyössä tiekartan kvanttitietokoneiden kehitykseen liittyvien kyberriskien lieventämiseksi. Tiekartta sisältää seitsemän vaihetta:

1. Yhteistyötä standardointijärjestöjen kanssa tulisi lisätä uusien kvanttiturvallisten algoritmien kehitykseen liittyen.
2. Kriittisimpien tietoaineistojen ja niiden salassapitoaikojen kartoitus.
3. Salausratkaisujen kartoitus.
4. Organisaation sisäisten hankinta-, tietoturva- ja kyberturvastandardien tunnistaminen. Ne tulee päivittää kvanttiturvallisiksi.
5. Julkisen avaimen kryptografiaa käyttävien järjestelmien tunnistaminen ja niiden ”merkitseminen” kvanttihaavoittuviksi.
6. Järjestelmien priorisointi kvanttiturvallisiin salausmenetelmiin siirtymistä ajatellen. Tähän vaikuttavat erityisesti organisaation toimintojen ja järjestelmien kriittisyys ja niihin kohdistuva todellinen uhka ja tätä kautta riskit.
7. Suunnitelma kvanttiturvallisiin salausmenetelmiin siirtymisestä kartoitusten ja priorisointiin perustuen.

Toimenpiteiden ajoitus:
2021–2023: Järjestelmien kartoitus sekä priorisointi.
2024: Uudet kvanttiturvalliset standardit julkaistaan.
2024–2030: Järjestelmien siirtymä kvanttiturvallisiin menetelmiin.
2030: Kryptografisesti merkittävä kvanttitietokone mahdollisesti saatavilla.

IBM:n tiekartta esittelee suunnitelman kvanttiturvallisiin menetelmiin siirtymisestä. Tiekartta esittelee myös IBM:n työkaluja ja palveluita, jotka auttavat organisaatioita löytämään, tarkkailemaan ja muokkaamaan joustavasti tarvitsemiaan salausmenetelmiä. Työkaluista osa on jo saatavilla ja osa vielä kehitteillä. Esimerkiksi IBM Quantum Safe Explorer-työkalun tarkoituksena on auttaa löytämään kryptografian käyttökohteita skannaamalla lähdekoodia ja tunnistamalla yleisesti käytössä olevia kirjastoja.

IBM on myös toteuttanut joitain NIST:n standardointiin valituista kvanttiturvallisista algoritmeista (esim. CRYSTALS-Kyber ja CRYSTALS-Dilithium). IBM on mukana konsortioissa, jotka edistävät kvanttiturvallisten salausmenetelmien kehitystä ja käyttöönottoa, esimerkkinä OQS (Open Quantum Safe). OQS ylläpitää kvanttiturvallisia algoritmeja sisältäviä avoimen lähdekoodin kirjastoja. Toinen esimerkki on PQC Coalition, joka keskittyy mm. edistämään kvanttiturvallisten salausmenetelmien ymmärtämistä ja käyttöönottoa kaupallisissa ja avoimen lähdekoodin teknologioissa. Tarkempaa tietoa algoritmeista tämän ohjeen kappaleessa ”PQC-tukimateriaali”.

4 https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf
5 https://www.ibm.com/quantum/assets/quantum-safe/IBM_Quantum_Safe_Roadmap.pdf
6 https://www.nature.com/articles/s41586-022-04623-2
7 https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF

Google ja SandboxAQ julkaisivat vuonna 2021 dokumentin, joka käsittelee organisaatioiden siirtymistä kvanttiturvallisiin salausmenetelmiin. Dokumentissa esitetään suosituksia siitä, (1) miten ja milloin aloittaa siirtymä, (2) mitä standardeja seurata sekä (3) mitä resursseja hyödyntää. Dokumentissa korostetaan siirtymän kiireellisyyttä tallenna-nyt-pura-myöhemmin (Save-now-decrypt-later) -hyökkäyksen vuoksi, sillä se vaarantaa pitkäaikaisesti suojattavat arkaluontoiset tiedot.

Dokumentissa annetaan suosituksia salausten joustavuuteen, priorisointiin sekä hybridialgoritmien käyttöön seuraavasti:

(1)
Salausten joustavuus: organisaatioiden tulisi suunnitella järjestelmänsä siten, että kryptografisia algoritmeja sekä avainten pituuksia on helppo vaihtaa. Joustavuuden tärkeys korostuu erityisesti standardisoinnin ollessa vielä kesken. Puhutaan myös kryptoketteryydestä.

(2)
Priorisointi: Kaikkia järjestelmiä ei ole tarve päivittää samanaikaisesti kvanttiturvallisiksi. Kriittiset järjestelmät sekä tiedot, jotka tarvitsevat pitkäaikaista suojausta priorisoidaan.

(3)
Hybridialgoritmit: Perinteisiä sekä kvanttiturvallisia algoritmeja voidaan käyttää rinnakkain, jolloin ei tarvitse luopua jo saavutetusta turvatasosta.

NSA (National Security Agency), CISA (Cybersecurity and Infrastructure Security Agency) ja NIST (National Institute of Standards and Technology) julkaisivat syksyllä 2023 tiedotteen, joka on suunnattu kriittisten järjestelmien ylläpitäjille. Tiedotteen tarkoituksena on edistää kvanttiturvallisiin salausmenetelmiin siirtymistä. Dokumentissa korostetaan huolellisen suunnittelun ja etukäteisvalmistelun merkitystä. Näin vähennetään kryptografisesti merkittävän kvanttitietokoneen luomaa uhkaa samalla varmistaen mahdollisimman mutkaton siirtyminen kvanttiturvallisiin menetelmiin.

Dokumentti korostaa, että tavoitteeseen pääseminen edellyttää huolellista suunnittelua (ns. tiekartat) ja riskien arviointia koko tuotantoketjun osalta. Organisaatioiden pitää tunnistaa käytössään olevat salausjärjestelmät ja -menetelmät. Kartoituksen pohjalta voidaan arvioida kvanttiuhan aiheuttamat todelliset riskit ja tarve kvanttiturvallisiin salausmenetelmiin siirtymiselle. Siirtymisprosessissa pitää erityisesti tunnistaa vaiheet, joissa salausta käytetään ensisijaisena suojauskeinona toiminnan kannalta kriittisen ja mahdollisesti arkaluontoisen tiedon suojaamiseen. Tällöin pitää myös arvioida, kuinka kauan informaatiota on tarve säilyttää salattuna.

Kansallisia ohjeistuksia kvanttiuhkaan varautumiseksi

Monessa valtiossa on jo kansallisia ohjeistuksia kvanttiuhkaan varautumiseen. Ohjeistuksia löytyi Alankomaista, Australiasta, Etelä-Koreasta, Iso-Britanniasta, Ranskasta, Saksasta ja Suomesta.

Alankomaiden kansalliset viestintäturvallisuustoimijat TNO (Applied Cryptography and Quantum Algorithms), CWI (Cryptology Group) ja AIVD (Netherlands National Communications Security Agency) ovat julkaisseet vuonna 2023 käsikirjan ”The PQC Migration Handbook – Guidelines for Migrating to Post-Quantum Cryptography”. Oppaan tarkoituksena on auttaa organisaatioita (1) tekemään kvanttikoneisiin liittyvä riskianalyysi omissa systeemeissään, (2) suunnittelemaan tarvittavat toimenpiteet kvanttiturvallisiin algoritmeihin siirtymiseksi ja (3) toteuttamaan siirtymä. Ohjeistus on sekä flaamiksi että englanniksi. Käsikirjassa ohjataan organisaatioita sijoittamaan itsensä tiettyyn viiteryhmään kvanttiuhan suhteen: (1) kiireelliset omaksujat (”urgent adopters”), (2) tavalliset omaksujat ja (3) kryptoasiantuntijat. Kiireelliset omaksujat ja erityisesti näiden organisaatioiden johto ja turvallisuusarkkitehdit ovat dokumentin pääkohderyhmä. Vähemmän kiireelliset tapaukset voivat toistaiseksi jäädä odottamaan algoritmien kypsymistä. Kryptoasiantuntijat ovat yrityksiä ja muita tahoja, jotka tuottavat ratkaisuja käyttäjäorganisaatioille.

Australian hallituksen alainen ASD (Australian Signals Directorate) ohjeistaa lyhyesti kaikki yrityksiä ja julkishallintoa seuraamaan kansallista tietoturvamanuaaliaan. Se päivitetään, kun kvanttiturvallisen salausten standardointi etenee. ASD kannustaa myös laajaan tutkimus- ja kehitystyöhön kvanttilaskennan alueella. Käytännön ohjeena organisaatioita kehotetaan tekemään inventaario käyttämistään julkisen avaimen teknologioista tiedoista, jota niillä suojataan. Tämän jälkeen on tehtävä suunnitelma uusiin algoritmeihin siirtymisestä.

Etelä-Korean osalta on kielimuurin vuoksi nojauduttu uutisreferaatteihin ja konekäännöksiin. Etelä-Korean hallitus on julkaissut kuusiosaisen suunnitelman (tiekartan) kvanttiturvallisiin ratkaisuihin siirtymiseksi. Uutisoinnin perusteella suunnitelmiin kuuluu mm. teknologiakehitystä, sääntelyn päivittämistä, standardointia, koulutusta ja tukea siirtymäajalle. Etelä-Koreassa käydään myös omaa PQC-standardointikilpailua, jonka voittajat valitaan kansalliseen standardiin. Uutisoinnin perusteella kahdeksan algoritmia on siirtynyt toiselle kierrokselle.

Iso-Britannian kansallinen kyberturvakeskus (NCSC) on vuonna 2020 julkaissut whitepaperin kvanttiuhkaan varautumisesta. Myös NCSC pitää kvanttiturvallista salausta (PQC) tehokkaimpana ratkaisuna kvanttikoneiden aiheuttamaan kyberuhkaan. Suurten organisaatioiden pitäisi varautua kvanttikoneilla tehtäviin hyökkäyksiin pitkän aikavälin suunnitelmissaan. Salausjärjestelmien käyttäjiä ohjeistetaan seuraamaan ajantasaisia tietoturvaohjeita ja siirtymään kvanttiturvalliseen kryptografiaan, kunhan standardit ovat valmiita ja niitä käyttäviä tuotteita saatavilla. Ohjeistus ei varsinaisesti käytä sanaa ”hybridiratkaisu”, mutta huomauttaa, että todennäköisesti on käytettävä rinnakkain perinteisiä menetelmiä ja uusia kvanttiturvallisia menetelmiä. NCSC varoittaa, että ei pidä kiirehtiä standardoimattomien ratkaisujen käyttöönottoa mahdollisten yhteensopivuusongelmien vuoksi.

Vuonna 2023 NCSC julkaisi toisen whitepaperin, joka on suunnattu mm. kriittisen infrastruktuurin yrityksille. Julkaisussa ohjeistetaan, että suurten IT-järjestelmien tilaajien pitäisi budjetoinnissaan ottaa huomioon uusien algoritmien käyttöönoton kustannukset. Käyttöönotto kannattaa suunnitella järjestelmien tavanomaisten teknisten päivitysten yhteyteen. Dokumentissa mainitaan standardoitavaksi valitut CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+ ja FALCON sekä tilalliset hash-pohjaiset LMS ja XMSS mutta kehotetaan odottamaan lopullisia standardeja sekä algoritmeista että protokollista. Hybridiratkaisujen käytöstä mainitaan erikseen monimutkaisuus, tehottomuus ja työläs ylläpito. NCSC kuitenkin mainitsee, että PQC-aikakauteen kannattaa kutenkin joskus siirtyä vaiheittain. Tällöin huolellinen hybridiratkaisujen suunnittelu ja toteutus ovat avainasemassa.

Ranskan kyberturvavirasto ANSSI julkaisi tilannekatsauksen tammikuussa 2022 ja siihen päivityksen joulukuussa 2023. Myös ANSSI suosittelee hybridiratkaisuja ja kryptoketteryyttä kvanttiturvallisten algoritmien kypsymättömyyden vuoksi. Samalla se muistuttaa, että ei pidä kuitenkaan viivytellä uusien algoritmien käyttöönottoa kriittisissä kohteissa. Kaikkien teollisuusalojen pitäisi aloittaa uusien algoritmien käyttö vanhojen rinnalla asteittain, jotta luottamus uusia algoritmeja ja niiden toteutuksia kohtaan voisi ylipäänsä muodostua. ANSSI suosittelee hybridiratkaisuja erityisesti tiedolle ja järjestelmille, joiden oletettu käyttöikä yltää vuoteen 2030 tai sen jälkeen.

Asteittaisen siirtymän tueksi tilannekatsauksessa esitellään kolmivaiheinen tiekartta, jota myös ANSSIn myöntämät turvallisuusviisumit seuraavat: Ensimmäisessä (1) vaiheessa, eli nykytilanteessa, klassinen kryptografia on pakollinen vaatimus ja PQC-ratkaisuja voi käyttää lisäturvana. Toisessa (2) vaiheessa tilanne on muuten sama, mutta kvanttikestävyys on perusteltavissa ja se voi olla järjestelmän tai tuotteen tärkeä ominaisuus. Tässä vaiheessa ANSSI on tunnistanut kriteerit hyväksyttäville kvanttiturvallisille algoritmeille, ja ne voivat poiketa NISTin valinnoista. Toinen vaihe kestänee vuoteen 2030, ja päivitysdokumentissa sen alkua on aikaistettu vuosille 2024–2025. ANSSI listaa käyttäjien tueksi käyttökelpoisia algoritmeja (CRYSTALS-Kyber, FrodoKEM, CRYSTALS-Dilithium, Falcon, XMSS/LMS ja SPHINCS+), vaikka korostaakin, että lista ei ole täydellinen eikä se halua rajata kehitystä ja innovaatiota suosittelemalla vain tiettyjä ratkaisuja. Kolmannessa (3) vaiheessa kvanttiturvallisten algoritmien oletetaan olevan varmasti käyttökelpoisia ja voidaan toimia ilman hybridiratkaisuja.

Saksan liittovaltion tietoturvavirasto BSI julkaisi vuonna 2021 englanninkielisen version ohjeistuksestaan kvanttiturvallisiin algoritmeihin siirtymisestä: ”Migration to Post Quantum Cryptography – Recommendations for Action by the BSI”. BSI suosittelee seitsemää toimintoa kvanttiturvallisuuteen liittyen:

1. Sekä uusien että kehitettävien järjestelmien pitäisi olla kryptografisesti ketteriä, jotta ne sopeutuvat tuleviin muutoksiin.
2. Firmware-päivityksissä käytettävä tilallisia hash-pohjaisia allekirjoituksia.
3. Erityisesti pitkän aikavälin käyttökohteissa symmetristen salausalgoritmien avaimenpituus pitäisi olla jatkossa 256 bittiä.
4. Lyhyen aikavälin turvatoimena voi käyttää erillistä ennalta jaettua yhteistä avainta suojaamaan varsinaista avaintenvaihtoprotokollaa. Tosin tämän avaimen jakeluun ei ole yleispätevää ratkaisua.
5. Aina, kun se on teknisesti mahdollista, käytetään hybridiratkaisua, jossa käytetään sekä perinteisiä että kvanttiturvallisia algoritmeja. Tätä pidetään varmempana vaihtoehtona kuin pelkkää uusien algoritmien käyttöä. Korkean turvallisuustason kohteisiin vaaditaan hybridiratkaisuja.
6. On huomattava, että kryptografisiin protokolliin tulee muutoksia uusiin salausalgoritmeihin ja erityisesti hybridiratkaisuihin siirtymisen vuoksi.
7. FrodoKEM ja Classic McEliece -algoritmit ovat BSI:n konservatiivinen valinta tilanteisiin, joissa pitkän aikavälin salaisuuksia on jo suojattava kvanttikoneilta.

FrodoKEM ei päässyt standardointikilpailussa finaaliin samasta syystä, kuin BSI suosittelee sitä: se on rakenteeltaan yksinkertainen. Tehokkaampien algoritmien monimutkaisempi rakenne vähentää BSI:n luottoa niiden turvallisuuteen.

Suomessa tutkittiin kvanttiturvallisten algoritmien hyödyntämistä vuonna 2022 päättyneessä PQC Finland -projektissa. Projektissa haluttiin myös kehittää suomalaista kryptografian osaamista tulevaa kvanttikoneiden aikakautta silmällä pitäen. Projektin tuloksista julkaistiin tiedonanto (policy brief) ”Kvanttiturvalliset salausmenetelmät Suomessa”, jossa todettiin, että Suomi on tällä hetkellä eturintamassa sekä kvanttiturvallisen kryptografian että kvanttikoneiden kehityksessä mutta aseman säilyttäminen vaatii koulutettua työvoimaa sekä panostusta tutkimukseen, tuotekehitykseen ja menetelmien toteutukseen. On myös tärkeää lisätä kansallista tietoisuutta kvanttikoneiden aiheuttamasta uhasta, sillä järjestelmien päivittäminen vie paljon aikaa ja resursseja.

Kansallisista ohjeistuksista suurin ero on hybridialgoritmien käytössä. Englanninkielisissä maissa ei suositella hybridiratkaisuja vaan kehotetaan siirtymään suoraan PQC-ratkaisuihin. Euroopan unionin suurissa maissa taas selkeästi suositellaan hybridiratkaisujen käyttöä siirtymävaiheen aikana.

Kirjallisuudessa esitetyt keskeiset suositukset

Olemassa olevasta kirjallisuudesta voidaan johtaa toimenpiteitä, joita jokaisen organisaation tulee tehdä varautuessaan kvanttikoneiden aiheuttamaan kyberuhkaan:

(1) Järjestelmien luokittelu Organisaation pitää selvittää sen nykyiset salausta käyttävät järjestelmät ja dokumentoida ne selkeästi jatkotoimenpiteitä varten. Mikäli järjestelmädokumentaatio ei ole ajan tasalla, on asia joka tapauksessa laitettava tässä yhteydessä kuntoon. Ajan tasalla oleva kryptoinventaario parantaa tietoturvaa ja ketteryyttä. Tämän voi tehdä itse tai siihen voi hankkia ulkopuolista asiantuntija-apua.

Järjestelmiä on erityyppisiä – siksi kvanttiturvallisiin menetelmiin siirtyminen vaatii organisaatiolta erilaisia toimenpiteitä. **Yksi tapa jaotella järjestelmät on tehdä se palvelun tarjoajan mukaan:**

a. Ohjelmistotalojen tarjoamat varus- ja valmisohjelmistot. Tällöin kvanttiturvalliseen salaukseen siirtymisen suunnitelmasta vastaa ohjelmistotalo ja asia selviää kysymällä ohjelmistotalon edustajilta (esim. suurten ja paikallisten ohjelmistotalojen ohjelmistot: Microsoft, Oracle, SAP, Salesforce, Visma).

b. Pilvipalvelut. Kvanttiturvalliseen salaukseen siirtyminen on palveluntarjoajan vastuulla ja sen voi selvittää palveluntarjoajalta (esim. Google, Amazon, Microsoft, Oracle, IBM).

c. Ohjelmistotalojen tekemät yrityskohtaiset järjestelmät. Kvanttiturvalliseen salaukseen siirtyminen selviää ohjelmiston toimittajalta, joka myös vastaa siirtymän suunnittelusta. Jos ohjelmistoon ei sisälly PQC päivitystä, uuden hankinta täytyy suunnitella.

d. Organisaation itsensä tekemät järjestelmät. Tällaisten ohjelmistojen osalta organisaatio joutuu itse tekemään suunnitelman kvanttiturvallisiin salausmenetelmiin siirtymisestä.

e. Lisäksi on puhtaasti tietoliikenteen salaukseen käytettyjä verkkoprotokollatoteutuksia, ratkaisuja ja työkaluja kuten SSL/TSL, HTTPS, SSH, VPN, IPSec, PGPGPG, Wi-Fi Protected Access (WPA/WPA2/WPA3), DTLS ja X.509-pohjaiset varmenneratkaisut. Tällöin kulloisenkin salausratkaisun toimittaja vastaa sekä kryptoketteryydestä että kvanttiturvallisesta siirtymästä. Yksinkertaisimmillaan kyse on esim. selaimen salausominaisuuksien päivittämisestä käyttöjärjestelmäpäivityksen yhteydessä. Esimerkiksi SSH on toteuttanut tuotteisiinsa perinteisten salausratkaisujen rinnalla käytettäväksi myös kvanttiturvallisia salausratkaisuja.

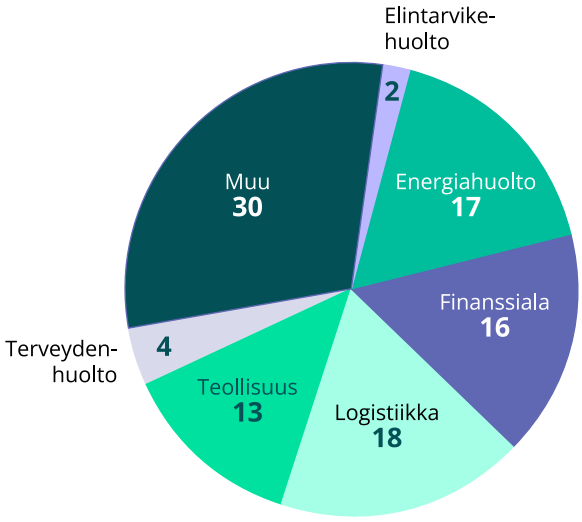
(2) Järjestelmien priorisointi Tiedot ja järjestelmät on priorisoitava kvanttisalaukseen salaukseen siirtymisen näkökulmasta. Ensin keskitytään toiminnan kannalta kriittisimpiin järjestelmiin. Organisaation on tiedettävä, mitä sen tietoja eri järjestelmissä käsitellään. Tämän voi selvittää omin avuin tai palkata ulkoista asiantuntijavoimaa. Samoin organisaation pitää ymmärtää ko. tietojen salassapitotarpeet ja -ajat. Ne määräytyvät esimerkiksi lakisääteisten tai asiakasvaatimusten mukaan. Vaatimusten lisäksi kvanttiuhan aiheuttamat todelliset riskit tiedolle ja tätä kautta yrityksen toiminnalle on analysoitava. Riskin suuruus määrittää keskeisesti kvanttiturvalliseen salaukseen siirtymisen tarpeen ja kiireellisyyden. Mikäli tietoihin ei kohdistu todellista uhkaa, ei riskiäkään ole – eikä näin ollen myöskään päivitystarvetta kvanttiturvallisiin menetelmiin. Tietoihin kohdistuvan riskin suuruuteen vaikuttavat salauksen lisäksi myös muut tiedon suojaamiseksi tehdyt toimenpiteet (l. tietoturva kontrollit). Päivitystarve ei ole kiireellinen, mikäli tiedot on riittävästi suojattu muilla toimenpiteillä.

(3) Päivitystarpeesta päättäminen Aiempien kohtien perusteella organisaatio tunnistaa, (a) mitkä järjestelmät tarvitsevat päivittämistä ja (b) kuinka kriittistä kunkin järjestelmän päivittäminen on. Kaikkea ei kannata – eikä voi - päivittää kerralla, vaan siirtymä pitää joka tapauksessa suorittaa vaiheittain.

(4) Suunnitelman luonti Vaiheiden 1–3 pohjalta luodaan organisaatiolle konkreettinen suunnitelma kunkin järjestelmän päivittämiseksi sisältäen päivittämisen kohteet, aikataulun, budjetin ja tekijät. Tähän voi hankkia ulkopuolista asiantuntija-apua. On huomattavaa, että suurta osaa päivityksistä ei tehdä itse vaan ne tehdään palveluntarjoajan tai järjestelmän toimittajan puolesta niiden yleisen aikataulun mukaisesti (kts. yllä vaihe 1)

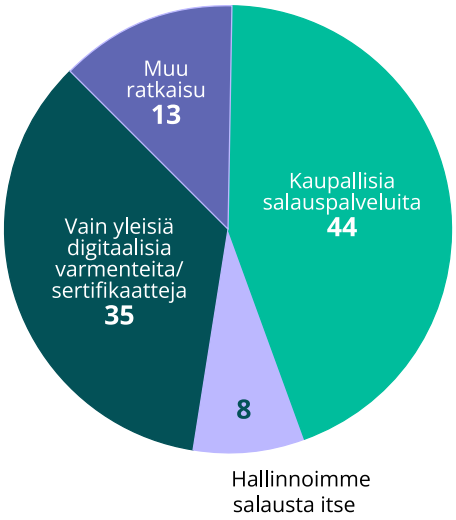
Kysely huoltovarmuustoimijoille

Hankkeen aikana tehtiin online-kysely suomalaisille huoltovarmuustoimijoille. Kysely keskittyi salausmenetelmien käyttöön ja kvanttiuhkaan varautumiseen. Kyselyä täydennettiin asiantuntijahaastattelulla. Kysymyksiä oli 20 ja vastauksia saatiin 100 laajasti eri toimialoilta (Kuva 2). Kategoriaan ”Muu” (Kuva 2) kuuluvista vastauksista merkittäviä aloja olivat media ja viestintä, vesiteollisuus, valtionhallinto sekä ympäristönhuolto. Vastanneista yrityksistä 44 % oli suuria (>250 hlö), 38 % keskikokoisia (50–249 hlö) ja 17 % pieniä.



Kuva 2. Kerätyt vastaukset toimialoittain.

Käytettävät salauspalveluntarjoajat. Kyselyn perusteella suurin osa huoltovarmuustoimijoista käyttää joko kaupallisia salauspalveluita tai ainoastaan yleisiä digitaalisia varmenteita. Näin ollen vain pieni osa vastanneista hallinnoi salaustaan täysin itse (Kuva 3). Muuhun ratkaisuun turvautuneet käyttävät pääasiassa näiden yhdistelmää tilanteen mukaan. Vastaajista 72 % voivat vaihtaa vapaasti eri kaupallisten tuotteiden välillä ja 21 %:lla on rajatut vaihtoehdot. Lopuilla vastaajista on joko yksi vaihtoehto (3 %) tai oma toteutus (4 %).



Kuva 3. Huoltovarmuustoimijoiden käyttämät salauspalvelut.

Käytössä olevat salausmenetelmät. Kirjallisuuden perusteella ensimmäinen vaihe on selvittää käytössä olevat salausmenetelmät. Suurimmalla osalla vastaajista (73 %) ei ole inventaariota käyttämistään salausmenetelmistä. Syynä tähän voi olla se, että kryptoinventaariotyökalujen markkina on vielä kehittymätön. Vastausten perusteella vaikuttaa myös ilmeiseltä, että salausmenetelmien hallinta on mielletty pitkälti ulkoistetuksi, sillä se on määrittelemättä 67 %:lla vastaajista. Salaussuunnitelmaa tai -strategiaa ei löydy 37 %:lla vastaajista (Taulukko 1).

Ei	37
Tapauskohtaisia ohjeita ja prosesseja	48
Rajoitettu suunnitelma	10
Yleinen suunnitelma	5

Taulukko 1. Salaussuunnitelmat ja -strategiat huoltovarmuustoimijoiden keskuudessa.

Noin puolella vastaajista (48 %) löytyy tapauskohtaisia ohjeita ja toimintatapoja (prosesseja), 10 %:lla on rajoitettu suunnitelma ja 5 %:lla on yleinen suunnitelma. Nämä luvut ovat globaalisti verrattuna alhaiset. Ponemon Instituten vuonna 2022 tekemässä tutkimuksessa[8] 62 %:lla vastaajista on yleinen suunnitelma, 22 %:lla rajoitettu suunnitelma ja vain 16 %:lla ei ole suunnitelmaa ollenkaan. Suomi ei ollut mukana tutkimuksessa. Yleisen suunnitelman prosenttiluvuissa on maakohtaista vaihtelua (50 %-80 %), ja esimerkiksi Ruotsissa yleinen salaussuunnitelma löytyy 50 %:lta vastaajista. Yleisen salaussuunnitelman tekeminen onkin selkeä kehityskohde suomalaisten huoltovarmuustoimijoiden keskuudessa.

Kyselyssä selvitettiin myös salausalgoritmien vaihdettavuus uusiin menetelmiin. Vastaajista 57 % kertoi, että algoritmit voi vaihtaa ulkoisen avun turvin, 18 % voi vaihtaa algoritmeja omalla työvoimalla ja 8 % vastasi, että menetelmiä on erittäin hankala vaihtaa. Loput vastaajista eivät osanneet arvioida vaihdettavuutta. Jos näin suuri osa toimijoista tarvitsee algoritmien vaihtamiseen ulkoista apua, herää kysymys, riittääkö nykyresursseilla tarvittavaa osaamista kaikille.

8 https://www.entrust.com/resources/reports/global-encryption-trends-study

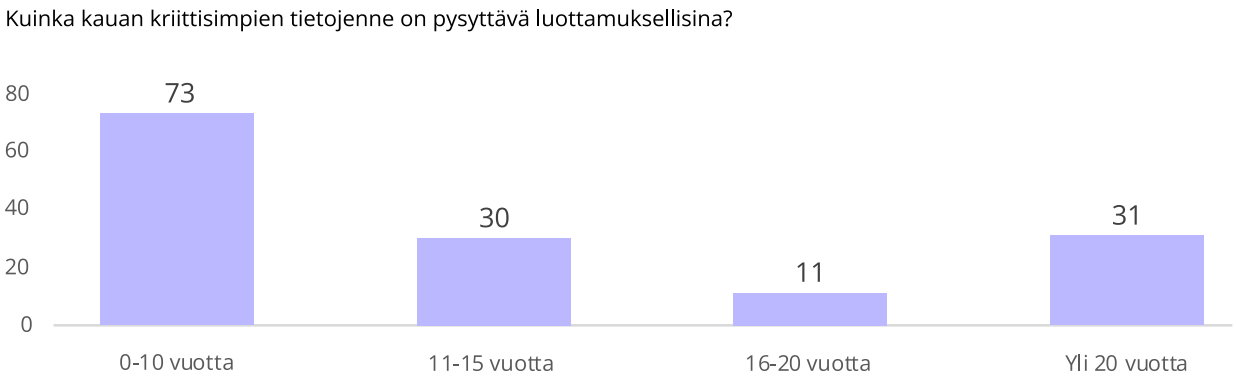
Salauskohteet. Kyselyssä tiedusteltiin salauksen käyttökohteita kolme vaihtoehtoa, joista sai valita kaikki salauksen käyttökohteet. Kommunikoinnin ja tiedonsiirron salaus sekä tietokantojen ja kovalevyjen salaus olivat suosituimmat (97 % ja 86 %). Omien tuotteiden varmenteisiin salausta käyttää 41 % vastaajista.

Salauksen kohde	kpl
Asiakas/henkilötiedot	14
Tietoliikenne	13
Salaiset ja luottamukselliset dokumentit sekä muut tiedot, tuotetiedot	12
Viestintä + sähköposti	11
Tietokannat	10
Tiedonsiirto	10
Autentikaatio/varmenteet	8
Sovellukset ja julkiset palvelut	6
Laitteet ja ohjelmistot	6
Sertifikaatit	3
VPN	3
Salasanojen hallinta	3
Tietojärjestelmät	2
Rahaliikenne	2
Kovalevyt ja massamuisti	2
TLS-protokolla	1
Käyttöliittymäyhteydet	1

Taulukko 2. Kriittisimmiksi valitut salauskohteet

Kysyttäessä salauksen kannalta kriittisimpiä kohteita avoimella vastauskentällä, kriittisimmiksi salauskohteiksi nousivat asiakas/henkilötiedot, tietoliikenne sekä erinäiset luottamukselliset dokumentit. Myös viestintä ja tiedonsiirto olivat suosittuja kohteita. Vastaajista 41 jätti kohdan tyhjäksi.

Kriittisten tietojen säilytysaika vaihteli paljon. Suurimmalla osalla vastaajista on tietoja, joiden säilytysaika on lyhyt, 0–10 vuotta, mutta noin kolmasosalta löytyy yli 20 vuotta säilytettävää luottamuksellista tietoa.



Kuva 4. Kriittisten tietojen säilytysaika. Vastaaja on voinut valita useita vaihtoehtoja

Yli kymmenen vuotta suojattavaa tietoa löytyy yhteensä 55 vastaajista. Kuvaan 4 on koottuna kaikki vastaukset. Huomattakoon, että vastaaja on voinut valita useamman vaihtoehdon.

Tietoisuus kvanttiuhasta. Kyselyllä pyrittiin selvittämään huoltovarmuustoimijoiden tietoisuutta kvanttiuhasta ja sen vaikutuksista salausmenetelmiin. Vastaajista 74 % oli tietoisia kvanttilaskennan uhasta julkisen avaimen salausmenetelmille. Kuitenkin vain 10 % kaikista vastaajista oli tutustunut kvanttiturvallisiin menetelmiin sekä NIST:n PQC-standardiin ja 34 % oli tutustunut tähän jonkin verran. Enemmistö (56 %) ei ollut tutustunut näihin ollenkaan. Useat organisaatiot ovat ainakin kuulleet kvanttiuhasta, mutta tämä ei ollut läheskään aina johtanut toimenpiteisiin.

Kvanttiuhkaan varautumattomuus tuli ilmi myös muissa kysymyksissä. Vain 21 % vastaajista oli arvioinut, mitkä heidän käyttämistään salausmenetelmistään ovat vaarassa. Kvanttiuhkaa ei ollut käsitelty johtoryhmissä: 90 % vastaajista ei ollut käsitellyt asiaa ollenkaan, 9 % oli käsitellyt, 3 % oli tehnyt toimenpiteitä ja 2 % varannut resursseja. Kysymykseen oli saanut valita useita vaihtoehtoja. Salausalgoritmien vaihtamiseksi vain 3 %:lla oli suunnitelma.

Kvanttisiirtymän toteuttamiseen tarvitaan osaavaa henkilökuntaa. Vastaajista 64 %:lla ei ole PQC-haasteisiin perehtynyttä työntekijää, 19 %:lla on osaamista omassa henkilöstössä ja 28 %:lla osaamista löytyy alihankkijalta. Kysymykseen on voinut valita useamman vaihtoehdon, joten osalla siis löytyy osaamista sekä omasta henkilöstöstä että alihankkijalta.

Huoltovarmuuden toimijat pitävät selvästi todennäköisempänä, että he tulevat hankkimaan kvanttiturvallista uutta teknologiaa (81 %) kuin että he tulevat tekemään siirtymätoimenpiteet itse (19 %). Tähän mennessä 11 % onkin jo ottanut kvanttiuhan huomioon uusissa hankinnoissa. Kvanttiuhalta puolustautumiseen siis toivotaan valmiita ratkaisuja, jotka saataisiin liitettyä omiin järjestelmiin.

Kyselyn vastauksista tutkittiin tarkemmin vielä terveydenhuollon, finanssialojen sekä vesihuollon toimialoja.

Terveydenhuolto. Terveydenhuoltoalalta saatiin neljä vastausta, joista kaksi oli keskisuurta ja kaksi isoa yritystä. Tärkeimmiksi salauskohteiksi ilmoitettiin potilastiedot, sovellukset, päätelaitteet, tietoliikenne sekä potilastietojärjestelmän ja asiakkaan välinen tietoliikenne. Kaikilta toimijoilta löytyy odotetusti yli 20 vuodeksi suojattavaa dataa. Kaikki vastaajat olivat tietoisia kvanttilaskennan kehityksen tuomasta uhasta, ja yksi toimijoista oli käsitellyt kvanttiuhkaa johtoryhmän kesken sekä ottanut uhkakuvan huomioon hankinnoissaan. Muita toimenpiteitä ei ollut tehty. PQC-siirtymään perehtyneitä työntekijöitä löytyi joko omasta tai alihankkijan henkilöstöstä kolmelta organisaatiolta neljästä.

Finanssialat. Finanssialoilta saatiin yhteensä 16 vastausta, joista 13 oli suuria ja kolme keskikokoisia yrityksiä. Kriittisimpinä salauksen kohteina olivat asiakastiedot, tietokannat, käyttäjien ja laitteiden tunnistaminen varmenteilla, tietoliikenne sekä muu liiketoimintakriittinen data. Suurin osa toimijoista voi vapaasti vaihtaa kaupallisten tuotteiden välillä, mutta merkittävällä osalla (n. 31 %) on joko rajatut vaihtoehdot tai vain yksi vaihtoehto palveluntarjoajaksi. Finanssialoilla löytyi paljon yli 20 vuotta säilytettävää salaista tietoa. Vastaajista 37,5 % oli arvioinut, mitkä salausmenetelmistä ovat vaarassa. Yksi vastaaja oli tehnyt toimenpiteitä lieventääkseen uhkaa.

Vesihuolto. Vesihuollon toimijoilta saatiin 4 vastausta, joista 3 tuli keskikokoisilta yrityksiltä ja 1 isolta. Kriittisimmiksi salauskohteiksi ilmoitettiin salasanojen hallinta, asiakasdata, luottamukselliset dokumentit sekä julkirajapinnan kautta toteutetut palvelut ja etäyhteysratkaisut. Vastanneista kaikki olivat kuulleet kvanttiuhasta mutta kukaan ei ollut vielä arvioinut tarkemmin, mitkä käytössä olevat salausmenetelmät ovat vaarassa, tai tehnyt muitakaan konkreettisia toimenpiteitä. PQC-menetelmiin perehtyneitä työntekijöitä löytyy kuitenkin kaikilta paitsi yhdeltä, joko omasta henkilöstöstä tai alihankkijalta.

Kyberalan asiantuntijahaastattelu. Kyselyn lisäksi haastattelimme FISC:n eli Kyberala ry:n johtoa. Se toi esille kvanttiturvallisiin salausmenetelmiin siirtymisen haasteita. Kyse ei välttämättä ole siitä, etteikö toimija olisi halukas ottamaan teknologiaa käyttöön. Mutta jos taustainfra ei tue kvanttiturvallisten menetelmien käyttöönottoa ilman massiivisia muutoksia, se väistämättä hidastuu kustannusten noustessa jyrkästi. Vaikka tietoisuus kvanttiuhasta on levinnyt, mielikuva asiasta saattaa olla jäsentymätön ja uhkakuva määrittämätön. Usein keskitytään enemmän kvanttilaskennan hyötyihin eikä kvanttiuhalta suojautumiseen. Haasteena on valmiiden kvanttiturvallisten ratkaisujen saatavuus ja erityisesti sertifioidut tuotteet. On aloja, joilla on hyvin tarkat vaatimukset käytetyille salausratkaisuille. Kvanttiturvallisten järjestelmien käyttöönoton nopeuttamiseksi tarvitaan valtion aktiivista ohjausta ja mahdollisesti lainsäädäntöä Yhdysvaltojen tapaan.

Huoltovarmuustoimijoilla on selkeästi tarvetta kvanttiturvallisille salausmenetelmille. Kyselyyn vastanneista 94 % käytti salausta tiedonsiirtoon ja 55 %:lla oli vastuullaan arkaluontoista, yli 10 vuotta suojattavaa tietoa. Lisäksi 31 %:lla oli vastuullaan yli 20 vuotta suojattavaa tietoa. Kvanttiturvallisiin järjestelmiin siirtyminen on haasteellista, sillä kyselyssä tuli esille huoltovarmuustoimijoiden huono ymmärrys salausmenetelmistä ja niiden käytössä. Monelta puuttui salaussuunnitelmat ja -strategiat sekä käytössä olevien salausratkaisujen inventaario. Tilanne naapurimaissa on huomattavasti parempi. On huolestuttavaa, että salausstrategioita ei velvoiteta eikä salausmenetelmien käyttöä säädellä edes huoltovarmuuskriittisten organisaatioiden osalta.

Varautumistiekartta huoltovarmuustoimijoille

Kuva 5. esittää tiekartan kvanttiuhkaan varautumiseksi. Se pohjautuu olemassa oleviin PQC-tiekarttoihin, kansallisiin suosituksiin sekä kyselyn tuloksiin ja sen perusteella jokainen organisaatio voi laatia oman suunnitelmansa l. tiekarttansa kohti kvanttiturvallisia salausratkaisuita.

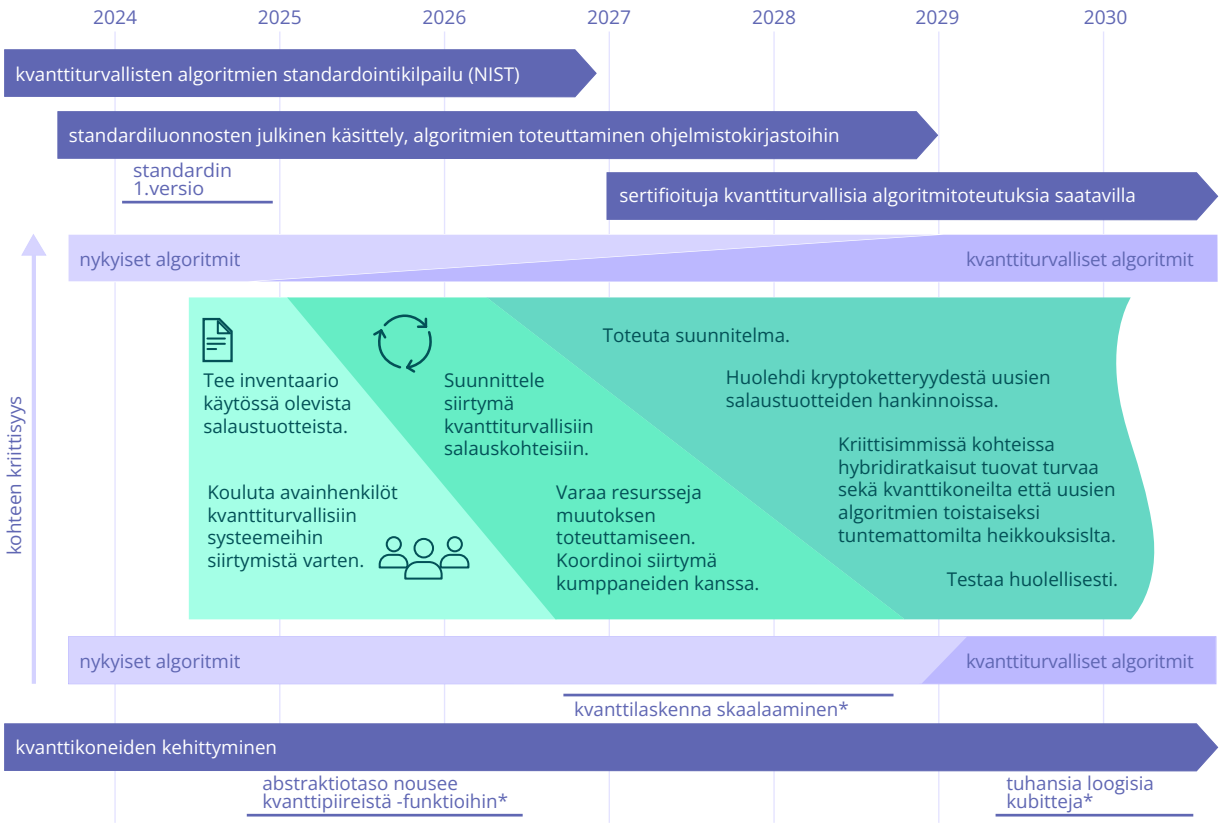
Julkisen salauksen menetelmällä toteutetut salaustuotteet ovat erityisen alttiita kvanttiuhalle. Vaikka riittävän tehokasta kvanttikonetta ei vielä ole, niiden kehitys on nopeaa. Lisäksi organisaatioilla on paljon tietoa, joka täytyy pitää turvassa kymmeniä vuosia. Siksi siirtymä kvanttiturvallisiin salaustuotteisiin pitää aloittaa hyvissä ajoin. Siirtymä sisältää karkeasti seuraavat vaiheet (Kuva 5)

1. Tee inventaario. Selvitä organisaation käytössä olevat salausratkaisut kattaen sekä ohjelmistot että laitteistot. Selvitä ainakin keskeiset salattuna talletetut tiedot ja luokittele ne salassapitotarpeen mukaan ja priorisoi tietojen uudelleensalaustarve.

2. Suunnittele siirtymä kvanttiturvallisiin ratkaisuihin. Tee huolellinen suunnitelma salausjärjestelmien päivittämisestä perustuen järjestelmien kriittisyyteen ja todellisiin riskeihin.

3. Toteuta siirtymä suunnitelman mukaisesti aloittaen riskien perusteella kriittisimmistä kohteista.

Varautumistiekartta kvanttilaskennan tietoturvavaikutuksiin



Nostoja IBM:n tiekartasta, kts. https://www.ibm.com/roadmaps/quantum/

Kuva 5. Tiekartta kvanttiuhkaan varautumisesta

1. Tee inventaario (2024–2026)

- Suurimmalla osalla huoltovarmuustoimijoista ei ollut varmaa tietoa käytössään olevista salausratkaisuista. Ensimmäinen vaihe kohti kvanttiturvallista salausta onkin tehdä kryptoinventaario: selvittää organisaation käytössä olevat salausratkaisut kattaen sekä ohjelmistot että laitteistot. Inventaarion laadinta on työlästä. Sen pitää kattaa salaustuotteissa käytetyt algoritmit, avaimenpituudet, tuotteiden käyttötavat ja elinkaari sekä niiden toimittajat. Tässä vaiheessa tunnistetaan kvanttiuhalle alttiit algoritmit jatkotoimenpiteitä varten. Tieto on dokumentoitava selkeästi jatkotoimenpiteitä varten (esim. manuaalikirjanpidon avulla kuten taulukossa 3 tai järjestelmään kuten CMDB, Configuration Management Database). Samalla selvitetään riippuvuudet salausratkaisujen toimittajiin: kuinka joustavasti organisaation käyttämiä ratkaisuja ja niiden toimittajia voidaan vaihtaa ja onko jokin kriittinen palvelu vain yhden toimittajan varassa. Salauspalveluiden tuottajien on selvitystä tehdessään syytä olla erityisen huolellisia. Seuraavaksi inventoidaan ja dokumentoidaan organisaation salattuna säilytettävät tietojoukot: millaista tietoa säilytetään salattuna ja missä ne sijaitsevat. On myös hyvä dokumentoida, mitkä tiedot ovat aktiivisessa käytössä ja mitkä taas säilytetään passiivisena. Lisäksi luokitellaan tiedot niiden salassapitovaatimusten mukaan, esim.: alle 5 vuotta, 5–15 vuotta, yli 15 vuotta. Salassapitoaika vaikuttaa kvanttiturvallisiin ratkaisuihin siirtymisen kiireellisyyteen. Taulukko 3 esittää otoksen organisaation kryptoinventaariosta. Koska tavoitteena on kattava ymmärrys organisaation käyttämistä salausmenetelmistä ja mahdollisista parannustarpeista, työ kannattaa tehdä työryhmätyönä ja osallistaa asiantuntijoita eri puolilta organisaatiota, kuten tietoturva-asiantuntijat, järjestelmäarkkitehdit, IT-ylläpitäjä ja järjestelmien omistajat (liiketoiminta).

- Arvioidaan salausjärjestelmiin ja salattuihin tietoihin kohdistuvat riskit. Viime kädessä järjestelmän ja tietojen kriittisyys organisaation toiminnalle ratkaisee kvanttiturvallisen siirtymän kriittisyyden. Mitä kriittisempää toimintoa järjestelmä ja tiedot tukevat, sitä suurempi riski ja myös kiireellisempi päivitystarve. Toisaalta on hyvä arvioida järjestelmän ja tietojen houkuttelevuus hyökkääjälle. Mitä houkuttelevampi kohde on hyökkääjän näkökulmasta sitä suurempi uhka ja myös riski.

- Järjestelmien päivitystarpeen priorisointiin vaikuttavat järjestelmän ja sen tietojen kriittisyys liiketoiminnalle, järjestelmässä käsiteltyjen tietojen kiinnostavuus hyökkääjän näkökulmasta (esim. taloudellinen arvo), muut järjestelmän suojaamiseen käytettävät suojaustoimet eli tietoturvakontrollit, järjestelmän käyttöympäristö ja tätä kautta hyökkäyksen toteutuksen helppous (pilvipalvelu, sisäverkko, julkiverkko) ja tietojen paljastumisen seuraukset yritykselle. Mikäli järjestelmä ja sen tiedot eivät ole kriittisiä ja riskit seurauksineen ovat mitättömät, järjestelmän päivittämisellä ei ole kiire. Mikäli talletettujen tietojen salassapitoaika on pitkä ja/tai niihin kohdistuu voimakkaita laki-, asiakas- tai muita sidosryhmävaatimuksia, on uudelleen salaus parasta suorittaa pian. Tällöin symmetrisen salausavaimen pituuden tuplaaminen suo jo hyvän suojan kvanttiuhkaa vastaan.

- Kvanttiturvallisiin ratkaisuihin siirtymisen suunnittelu on syytä aloittaa. Aloitetaan avainhenkilöiden kouluttaminen ja/tai ulkopuolisen avun hankinta. Samalla nimitetään organisaation vastuuhenkilöt valmistelemaan siirtymäsuunnitelmaa, jossa huomioidaan aikataulutus, budjetointi ja tekijät.

Järjestelmä	Salaus-menetelmä	Algoritmi/ protokolla	Avain	Avainten-hallinta	Salatut tiedot	Haavoittu-vuudet
CRM	Tiedonsiirto	TLS 1.3	2048 bittiä	Keskitetty	Asiakastiedot	Altis kvanttiuhalle
S-posti	Tiedonsiirto	TLS 1.3	2048 bittiä	Keskitetty	S-postit	Altis kvanttiuhalle
Backup-järj., aktiivinen	Tallennus	AES 256	256 bittiä	Paikallinen	Varmuuskopiot	Yhteensopivuus vanhojen laitteiden kanssa. Ei kriittinen kvanttiuhan näkö-kulmasta. Avain-pituuden tuplaus ei kiireellinen.

Taulukko 3. Esimerkkiotos kryptoinventaariosta

2. Suunnittele siirtymä kvanttiturvallisiin ratkaisuihin (2025–2028)

- Salausjärjestelmien päivitys suunnitellaan niiden kriittisyyteen ja niihin kohdistuviin todellisiin riskeihin perustuen. Huomioidaan kirjallisuuskatsauksessakin todetut päivitysvastuut. Vain osa päivityksistä on organisaation itsensä vastuulla. Suuresta osasta huolehtii palveluntarjoaja tai järjestelmän tekijä.
- Suunnitellaan organisaation omien salattujen tietovarantojen uudelleensalaustarve riskiperusteisesti. Mitä kauemmin tietoa pitää säilyttää salattuna ja mitä houkuttelevampi se on hyökkääjälle, sitä pikemmin se on suojattava kvanttiuhalta kasvattamalla salausavaimen pituutta uudelleensalauksessa. Siirtymäjärjestyksen lisäksi päätetään, mitä algoritmeja halutaan käyttää missäkin kohteessa. Tämä vaihe vaatii ymmärrystä sekä tietoihin ja järjestelmiin kohdistuvista riskeistä että itse salausalgoritmeista, joten useimmat organisaatiot tarvitsevat tähän oman osaamisen lisäksi ulkopuolista asiantuntija-apua.
- Kriittisimmissä kohteissa tarvitaan hybridiratkaisuja eli perinteisen ja kvanttiturvallisen salausmenetelmän yhdistelmiä. Kvanttiturvallista algoritmia käytetään suojaamaan tietoa ”tallenna nyt, pura myöhemmin” -tyyppiseltä hyökkäykseltä, ja perinteistä algoritmia käytetään siltä varalta, että uusissa algoritmeissa on vielä löytymättömiä heikkouksia.
- Vähemmän kriittisissä kohteissa odotetaan kvanttiturvallisten algoritmien kypsymistä ja siirrytään rauhassa myöhemmin suoraan kvanttiturvallisiin algoritmeihin. Suuri osa siirtymistä hoituu tosin palveluntarjoajien ja ohjelmistotalojen toimesta.
- Huolehditaan kryptoketteryydestä uusien salaustuotteiden hankinnoissa: pyritään valitsemaan ja vaatimaan palveluntarjoajilta tuotteita, joissa on helposti päivitettävät ja vaihdettavat salausmenetelmät. Tämä on erityisen tärkeää, kun hankitaan laitteistoja, joiden käyttöikä on yli kymmenen vuotta.
- Varataan suunnitellut resurssit siirtymän toteuttamiseen. Suurin osa organisaatioista toteuttanee muutoksen ulkoisen avun turvin lähempänä vuotta 2030. Haasteena voi olla tällöin asiantuntijoiden puute, joten on hyvä olla ajoissa liikkeellä.
- Siirrytään riippuvuussuhteessa olevien organisaatioiden kesken koordinoidusti kvanttiturvallisiin järjestelmiin. Lineaarisessa riippuvuussuhteessa alkupään organisaatioiden pitäisi siirtyä kvanttiturvallisiin systeemeihin ennen kuin niistä riippuvat organisaatiot toteuttavat oman siirtymänsä. Tiukasti verkottuneiden organisaatioiden pitäisi siirtyä yhtä aikaa kvanttiturvallisiin järjestelmiin.

3. Toteuta siirtymä suunnitelman mukaisesti (2026–2030)

- Siirtymä aloitetaan riskien perusteella kriittisimmistä kohteista. Kaikkia järjestelmiä ei tarvitse päivittää – riskit ratkaisevat. Kaikkein kriittisimpiä kohteita voi joutua siirtämään kvanttiturvallisiin menetelmiin jo ennen kuin koko organisaation siirtymä on suunniteltu valmiiksi ja jopa ennen kuin standardin mukaisia toteutuksia on laajasti saatavilla. Järjestelmien kryptoketteryys auttaa reagoimaan muutoksiin.

- Varataan tarpeeksi aikaa ja resursseja uusien salaustuotteiden testaamiselle. Niiden on tuotettava luvattu turvallisuustaso ja niiden on oltava yhteensopivia muiden käytössä olevien laitteistojen ja ohjelmistojen kanssa.

Yhteenveto

Huoltovarmuustoimijoilla on selkeästi tarvetta kvanttiturvallisille salausmenetelmille. Kyselyyn vastanneista 94 % käytti salausta tiedonsiirtoon ja 55 %:lla oli vastuullaan arkaluontoista, yli 10 vuotta suojattavaa tietoa ja 31 %:lla oli vastuullaan yli 20 vuotta suojattavaa tietoa. Tällä aikaskaalalla kvanttikoneet ovat todellinen uhka. Taulukko 4 summaa keskeisimmät varautumistiekartan esittämät toimenpiteet, jotka muodostettiin kirjallisuuskatsauksen ja huoltovarmuuskriittisille yrityksille suunnatun kyselyn perusteella.

Toimenpide	Vastuutaho	Huomioitavaa
Salausratkaisujen inventaario (kryptoinventaario)	Organisaatio itse, voidaan käyttää ulkopuolista asiantuntija-apua. Esim. IBM tarjoaa tähän konsultaatiota ja osin myös työkaluja	Järjestelmiä on erityyppisiä. Organisaatio itse vastaa käyttämiensä järjestelmien tunnistamisesta ja dokumentoinnista
Salattujen tietojen inventaario ja luokittelu	Organisaatio itse, voidaan käyttää ulkopuolista asiantuntija-apua	Osa tiedoista aktiivisessa käytössä ja osa passiivisia, salassapitoaika vaihtelee
Salausavainten hallinta kuntoon	Organisaatio itse, voidaan käyttää ulkopuolista asiantuntija-apua	Mikäli salausavainten hallintaa ei laiteta kuntoon, kvanttiturvallinen siirtymä on lähes turha. Osa salausavainten hallinnasta on ulkoistettu/organisaatiolta piilotettu (esim. selainliikenteen salauksessa).
Järjestelmäpäivitysten ja tiedon uudelleensalaustarpeen priorisointi riskiperusteisesti.	Organisaatio itse, voidaan käyttää ulkopuolista asiantuntija-apua	Päivitysten ja uudelleensalausten kriittisyyteen vaikuttaa mm. tietojen ja järjestelmien kriittisyys organisaation liiketoiminnalle, tietojen paljastumisen seuraukset, tietojen ja järjestelmien kiinnostavuus hyökkääjän näkökulmasta eli todelliset uhat ja riskit.
Salausratkaisujen päivitys-suunnitelma. Erityisesti julkisen avaimen menetelmiä käyttävät salausratkaisut päivitetään, mikäli riskit näin edellyttävät. Vähäriskisiä järjestelmiä ei välttämättä tarvitse päivittää.	Organisaation on hyvä tiedostaa päivitysten vastuutahot. Organisaation itse tuottamien järjestelmien ja palveluiden osalta vastuu on organisaatiolla itsellä	Usein päivittämisestä kvanttiturvallisiin salausratkaisuihin vastaa palveluntarjoaja tai järjestelmätoimittaja/ohjelmistotalo
Tietojen uudelleensalauksen päivityssuunnitelma	Organisaatio itse, voidaan käyttää ulkopuolista asiantuntija-apua	Tässäkin ollaan riippuvaisia salausratkaisujen toimittajasta. Säilössä tiedot on tyypillisesti salattu symmetrisillä menetelmillä. Salausratkaisun on tuettava avainpituuden tuplausta nykyisistä turvallisista avainpituuksista.
Kvanttiturvallisten salausratkaisujen vaatimus hankinnoissa, samoin kryptoketteryyden	Organisaatio itse	Uushankintojen on tuettava kvanttiturvallisia salausalgoritmeja ja ketterää salausmenetelmien vaihtoa
Päivitysten ja uudelleensalausten toteutus vuoteen 2030 mennessä	Organisaatio itse, voidaan käyttää ulkopuolista asiantuntija-apua. Iso osa päivityksistä tulee kuitenkin palveluntarjoajien ja järjestelmätoimittajien/ohjelmistotalojen toimesta omien suunnitelmiensa mukaisesti.	Siirtymä on laaja ja sellaisena työläs ja aikaa vievä tehtävä.
Hybridiratkaisujen tarpeen arviointi	Organisaatio itse, todennäköisesti useimmat organisaatiot tarvitsevat ulkopuolista asiantuntija-apua	

Taulukko 4. Yhteenveto varautumistiekartan toimenpiteistä

Johtopäätökset

Systemaattinen viestintä kvanttilaskennan vaikutuksista sekä tarvittavista varautumistoimenpiteistä ja ratkaisuista on tarpeen. Selvitys osoitti, että ymmärrys kvanttilaskennan aiheuttamasta kyberuhasta on vajavaista. Tämä käy ilmi esim. siitä, että vain harva yritys on tehnyt konkreettisia toimenpiteitä kvanttiuhkien huomioimiseksi. Kyselyssä havaittiin, että vaikka 74 % on tietoisia kvanttiuhasta ja 75 % on arvioinut, että algoritmit pystytään vaihtamaan, vain 27 %:lla oli listaus käytössä olevista menetelmistä ja vain 21 % oli arvioinut, mitkä salausmenetelmät ovat vaarassa.

Käytännössä tilanne on huolestuttava, sillä vain 11 % on ottanut kvanttiuhan huomioon hankinnoissaan ja vain 9 %:lla vastanneista oli johtoryhmä käsitellyt asiaa ja vain 3 % tehnyt toimenpiteitä. Tietoisuuden lisääminen on tärkeää, jotta kvanttiuhan vaatimiin toimenpiteisiin osataan varautua riittävän huolellisella suunnittelulla.

Kysely osoitti, että monilta yrityksiltä puuttui salaussuunnitelmat ja -strategiat sekä inventaario käytössä olevista salausmenetelmistä eli luvassa on suuri työmaa.

Viidesosa kyselyyn vastanneista on kiinnostunut osallistumaan tutkimushankkeeseen, jossa suunnitellaan, toteutetaan ja testataan kvanttiturvallisia salausmenetelmiä. Tähän ehdotetaan jatkohanketta yhteistyössä kvanttiturvallisia ratkaisuja tuottavien suomalaisten yritysten kanssa (esim. SSH). Hanke voisi sisältää käytännönläheisiä työpajoja, koulutusta ja kvanttiturvallisten menetelmien validointia. Jatkohankkeessa voi myös kehittää ja kokeilla kryptoinventaarion tekemiseen sopivia työkaluja ja menetelmiä.

PQC-tukimateriaali

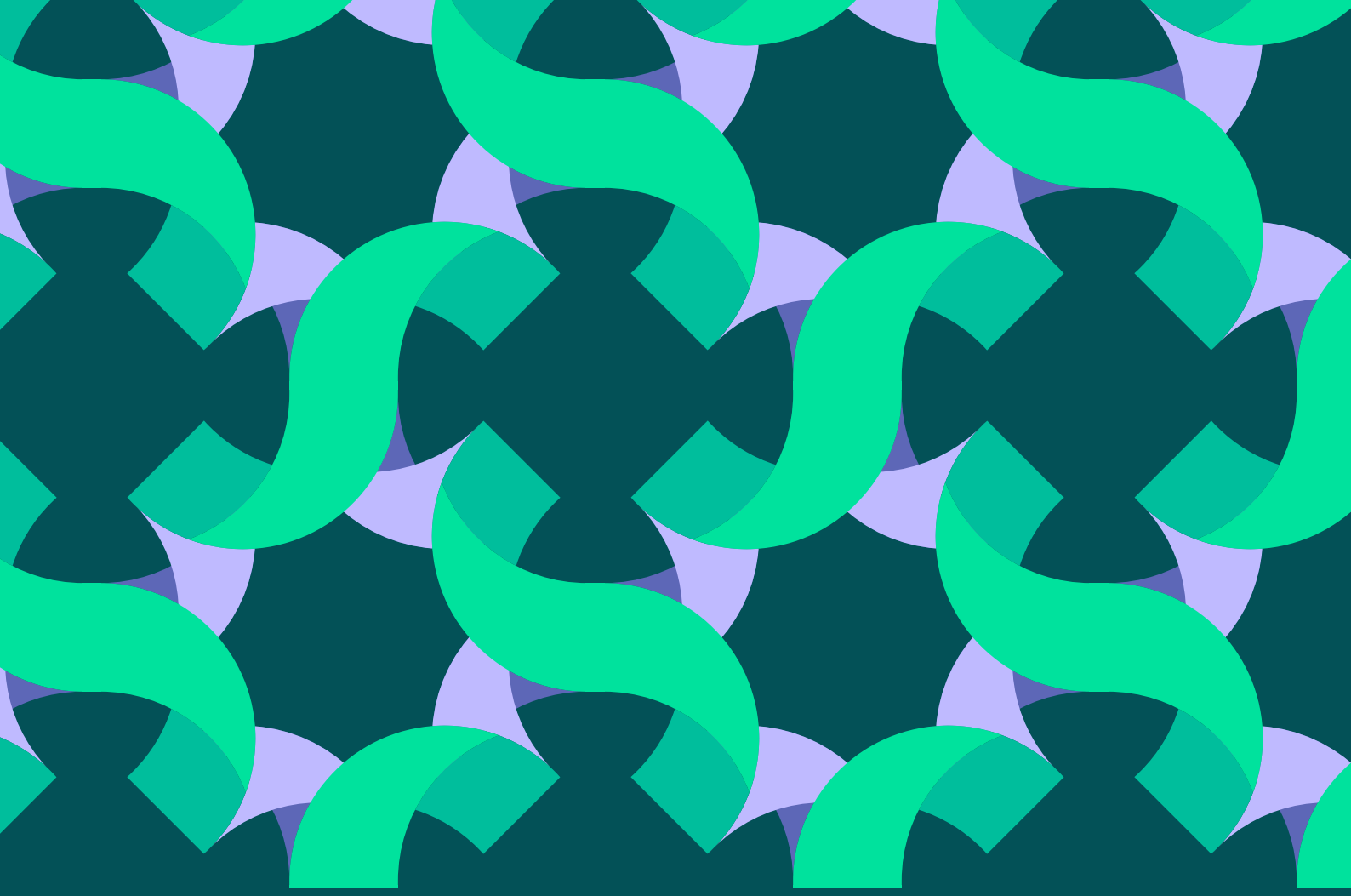
NIST standardin lisäksi Internet Engineering Task Force (IETF) on tuottanut hyvää PQC-tukimateriaalia. IETF tekee vapaaehtoisia standardeja ja ohjeistuksia, joita internetin käyttäjät, verkko-operaattorit ja laitevalmistajat usein hyödyntävät.

- NIST PQC-standardi:
  https://csrc.nist.gov/Projects/post-quantum-cryptography
- IETF PQC-opas insinööreille:
  https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/
- IETF PQC-hybridialgoritmien terminologiaopas
  https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/
- PQC ohjelmointikirjastoja:
  - PQClean (C) – Puhtaat versiot NIST-algoritmeista
  - libOQS (C) – Wrapperit C++, Python, Java, Go, .NET ja Rust kielille
  - BouncyCastle (Java), rustpq/pqcrypto (Rust), pqm4 (C, Cortex-M4)

Yhteystiedot

Projektipäällikkö
Visa Vallivaara
Tel. +358401398326
visa.vallivaara@vtt.fi
www.vttresearch

Ohjausryhmän puheenjohtaja
Antti Nyqvist
Tel. +358408619446
antti.nyqvist@teknologiateollisuus.fi
www.digipooli.fi



Huoltovarmuuskeskus