

**DigiFinland**Sosiaali- ja
terveysministeriöTerveystiedon ja
hyvinvoinnin laitos

Kvanttiturvallinen sote 2035: Terveystiedon suojaaminen kvanttilaskennan aikakaudella

VISA VALLIVAARA (VTT), ANDREI LAURÉN (STM), MIKA PIHLAJAMÄKI (THL), LAURA VÄLKKILÄ
(DIGIFINLAND OY)

Sisällysluettelo

1. Johdanto	2
1.1 Julkaisun keskeinen viesti	2
2. Kvanttilaskennan näkymät 2035	2
2.1 Miksi tarkasteluhorisontti on vuosi 2035.....	3
2.2 Moscan sääntö riskienhallinnan kehyksenä	3
2.3 Kvanttilaskenta osana hybridiarkkitehtuuria	3
3. Mikä murtuu, mikä kestää - kryptografinen riskikuva	3
3.1 Julkisen avaimen menetelmät	3
3.2 Symmetrinen salaus ja tiivisteet	4
3.3 Kvanttiturvalliset standardit ja hybridiratkaisut	4
3.4 QKD:n rajattu rooli	4
4. Terveystiedon erityisriski - kerää nyt, pura myöhemmin	4
4.1 Kerää nyt, pura myöhemmin -toimintamalli	4
4.2 Genomitiedon erityinen asema	5
4.3 EHDS ja tutkimustiedon liikkuvuus	5
4.4 Keskeiset riskikohteet	5
5. Siirtymä kvanttiturvalliseen kryptografiaan	6
5.1 Omistajuus ja johtaminen	6
5.2 Kryptoinventaario ja CBOM.....	6
5.3 Krypto-ketteryys	6
5.4 Toimittajat ja hankinnat	6
5.5 Vaiheittainen etenemismalli	6
6. Ohjaus, vastuut ja seuraavat askeleet	7
6.1 Velvoittava kehikko	7
6.2 Vastuut.....	8
6.3 Osaaminen ja tutkimus	8
6.4 Kvanttilaskennan mahdolliset hyödyt.....	8
6.5 Konkreettiset suositukset	9
6.6 Jos valmistautumista ei tehdä.....	9
7. Kvanttilaskenta vuonna 2035: kolme skenaariota	10
7.1 Välivaiheet 2026–2035	10
Liitteet	12
Liite 1. Keskeiset käsitteet.....	12
Liite 2. Lähteitä ja jatkolukemista	12

1. Johdanto

Sosiaali- ja terveydenhuollon toiminta perustuu laajoihin ja pitkäikäisiin tietovarantoihin. Potilas- ja asiakastietoja, rekisteritietoja, tutkimusaineistoja ja genomitietoja säilytetään ja käytetään tilanteissa, joissa tietojen luottamuksellisuuden, eheyden ja saatavuuden on säilyttävä vuosikymmeniä. Kvanttilaskennan kehitys muuttaa tämän pitkän aikavälin riskikuvaa, koska riittävän tehokas kvanttietokone voisi murtaa useita nykyisin käytettyjä julkisen avaimen salaus- ja allekirjoitusmenetelmiä.

Kvanttiuhka ei tarkoita, että kaikki salaus lakkaisi toimimasta yhdellä kertaa. Se tarkoittaa kuitenkin sitä, että pitkäikäisiin tietoihin, järjestelmien välisiin yhteyksiin, sähköisiin allekirjoituksiin ja laite- sekä ohjelmistoriippuvuuksiin liittyvät kryptografiset riskit tulee tunnistaa ja hallita ennakoivasti. Erityisen merkittävä on niin sanottu kerää nyt, pura myöhemmin -uhka: salattua tietoliikennettä tai aineistoja voidaan kerätä talteen jo nykyisin ja pyrkiä avaamaan myöhemmin, kun tarvittava laskentakyky on käytettävissä.

Tämä julkaisu tarkastelee kvanttilaskennan vaikutuksia sosiaali- ja terveydenhuollon tietoturvaan vuoden 2035 aikajänteellä. Tavoitteena on kuvata ymmärrettävästi, mikä nykyisessä kryptografiassa eli tietojen suojaamisessa on haavoittuvaa, mitä siirtyminen kvanttiturvallisiin ratkaisuihin edellyttää sekä miten vastuut, hankinnat, osaaminen ja tekninen toimeenpano voidaan järjestää hallitusti.

Julkaisu on laadittu osana sosiaali- ja terveystieteiden ministeriön käynnistämää SOTE-tekoälyn ekosysteemin Riskienhallintatyöryhmän toimintaa. Ekosysteemin riskienhallintatyöryhmä tukee tekoälyn turvallisen käytön kansallista kehittämistä, vahvistaa hyvinvointialueiden riskienhallintaa ja kokoaa konkreettisia kehittämistoimenpiteitä. Kvanttiturvallisuus liittyy tähän kokonaisuuteen, koska tekoälyratkaisujen hyödyntäminen lisää tietovirtoja, laskentapalvelujen käyttöä ja riippuvuutta digitaalisista infrastruktuureista.

1.1 Julkaisun keskeinen viesti

Kvanttiturvallisuuteen siirtymistä ei tule käsitellä yksittäisenä salausalgoritmin vaihtona. Kyse on useita vuosia kestävästä muutosohjelmasta, joka edellyttää kryptografisten riippuvuuksien tunnistamista, riskiperusteista priorisointia, sopimus- ja hankintavaatimuksia, järjestelmätoimittajien yhteistyötä sekä selkeää johtamisvastuuta. Valmistautuminen tulee aloittaa ennen kuin kryptografisesti merkityksellinen kvanttietokone on käytettävissä, sillä tietojen suojausaika ja järjestelmien siirtymäaika voivat yhdessä olla pidempiä kuin arvioitu aika kvanttiuhan toteutumiseen.

2. Kvanttilaskennan näkymät 2035

Kvanttilaskenta hyödyntää kvanttimekaniikan ilmiöitä laskennassa. Kvanttietokoneen perusyksikkö on kubitti. Nykyiset laitteet perustuvat fyysisiin kubitteihin, jotka ovat herkkiä virheille ja ympäristön häiriöille. Luotettava laskenta edellyttää virheidenkorjausta, jossa useita fyysisiä kubitteja käytetään yhden loogisen kubitin muodostamiseen. Tämän vuoksi laitteen ilmoitettu fyysisten kubitien määrä ei yksin kuvaa sitä, mihin laite käytännössä kykenee.

Kryptografisesti merkityksellinen kvanttietokone edellyttää suurta määrää riittävän laadukkaita kubitteja, toimivaa virheidenkorjausta ja kykyä suorittaa pitkiä laskentaketjuja hallitusti. Arviot tällaisen kapasiteetin saavuttamisesta vaihtelevat, eikä tarkkaa Q-Day-ajankohtaa voida määrittää. Epävarmuus ei poista riskiä,

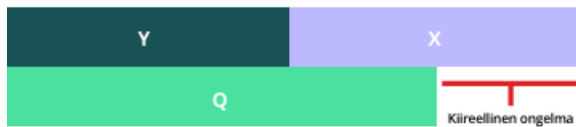
vaan on itsessään riskienhallinnan lähtökohta: vaikutukset olisivat suuria, vaikka toteutumisajankohtaan ja todennäköisyyteen liittyy epävarmuutta.

2.1 Miksi tarkasteluhorisontti on vuosi 2035

Vuosi 2035 muodostaa tarkoituksenmukaisen tarkasteluhorisontin, koska sosiaali- ja terveydenhuollon tietojen suojausajat ovat pitkiä ja järjestelmäkannan uudistaminen on hidasta. Eurooppalaisissa ja kansainvälisissä tiekartoissa siirtymä kvanttiturvalliseen kryptografiaan jaksotetaan useille vuosille. Vuoteen 2035 ulottuva näkymä mahdollistaa sen, että korkean riskin kohteet voidaan tunnistaa ja käsitellä ennen laajempaa teknologista murrosta.

2.2 Moscan sääntö riskienhallinnan kehyksenä

Moscan sääntö havainnollistaa ajoituksen merkitystä (Kuva 1). Kvanttilaskennan riski on merkittävä, jos tiedon vaadittu suojaus aika X ja järjestelmän päivittämiseen tarvittava aika Y ovat yhteensä suurempia kuin Q -Dayn arvioitu saapumisaika Q . Eli jos $X + Y > Q$, valmistautuminen on aloitettava välittömästi.



Kuva 1. Moscan sääntö. Lähde: Huoltovarmuuskeskus, Kvanttilaskennan tietoturva-vaikutukset - suositus varautua (2024).

2.3 Kvanttilaskenta osana hybridiarkkitehtuuria

Kvanttitietokoneet eivät todennäköisesti korvaa nykyisiä tietojärjestelmiä, vaan täydentävät niitä. Käytännön ratkaisut muodostuvat hybridiarkkitehtuureista, joissa perinteinen laskenta, suurteholaskenta, pilvipalvelut, tekoäly ja kvanttilaskenta toimivat rinnakkain. Kvanttilaskentaa käytetään niihin rajattuihin tehtäviin, joissa siitä voidaan saada hyötyä, kun taas tiedon esikäsittely, tulosten tulkinta, käyttöliittymät ja suurin osa sovelluslogiikasta säilyvät perinteisissä ympäristöissä.

Sosiaali- ja terveydenhuollossa todennäköinen käyttömalli on keskitetty laskentapalvelu.

Hyvinvointialueiden tai yksittäisten sairaaloiden ei tarvitse omistaa kvanttitietokonetta, vaan kapasiteettia voidaan käyttää palveluna kansallisen tai kansainvälisen laskentainfrastruktuurin kautta. Malli edellyttää erityistä huolellisuutta siinä, mitä tietoa laskentapalveluun siirretään, missä muodossa tieto käsitellään ja miten salausavaimet, käyttöoikeudet, lokit ja palautuvat tulokset suojataan.

3. Mikä murtuu, mikä kestää - kryptografinen riskikuva

Kvanttilaskennan vaikutukset kohdistuvat eri tavoin eri kryptografiin menetelmiin. Riskiviestinnässä on tärkeää välttää väitettä, jonka mukaan kaikki nykyinen salaus murtuisi samalla tavalla. Julkisen avaimen kryptografia, symmetrinen salaus, tiivistefunktiot ja allekirjoitukset muodostavat erilaisia riskiluokkia ja edellyttävät erilaisia hallintatoimia.

3.1 Julkisen avaimen menetelmät

Shorin algoritmi muodostaa keskeisen uhan laajasti käytetyille julkisen avaimen menetelmille. Riittävän tehokkaalla virheenkorjatulla kvanttitietokoneella RSA:han, elliptisiin käyriin ja Diffie-Hellman-avaimenvaihtoon perustuvien ratkaisujen turvallisuus voidaan murtaa. Näitä menetelmiä käytetään muun muassa palvelinten ja käyttäjien tunnistamiseen, salausavainten vaihtoon, varmenteisiin ja sähköisiin

allekirjoituksiin. Siksi vaikutus ulottuu yksittäisiä sovelluksia laajemmalle koko digitaaliseen luottamusketjuun.

3.2 Symmetrinen salaus ja tiivistet

Groverin algoritmi heikentää symmetristen menetelmien turvallisuusmarginaalia, mutta ei tee niitä käyttökeltvottomiksi samalla tavoin kuin Shorin algoritmi julkisen avaimen menetelmille. Riittävän pitkät avaimet ja vahvat tiivistefunktiot muodostavat edelleen keskeisen osan kvanttiturvallista kokonaisuutta. Käytännön siirtymässä on tarkasteltava sekä algoritmia että avainpituutta, käyttötapaa, toteutusta ja avainten hallintaa.

3.3 Kvanttiturvalliset standardit ja hybridiratkaisut

Post-quantum cryptography eli PQC tarkoittaa tavallisilla tietokoneilla toteutettavia kryptografisia menetelmiä, joiden on tarkoitus kestää myös kvanttietokoneella tehtäviä hyökkäyksiä. NIST on standardoinut avainten kapselointiin ML-KEM-menetelmän sekä digitaalisiin allekirjoituksiin ML-DSA- ja SLH-DSA-menetelmät. Standardointi mahdollistaa toteutusten, tuotteiden ja yhteentoimivuuden kehittämisen, mutta ei poista tarvetta seurata menetelmien turvallisuutta ja toteutusten laatua.

Siirtymävaiheessa voidaan käyttää hybridiratkaisuja, joissa nykyinen ja kvanttiturvallinen menetelmä toimivat rinnakkain. Tavoitteena on säilyttää suojaus myös tilanteessa, jossa jommastakummasta menetelmästä löytyy haavoittuvuus. Hybridiratkaisut lisäävät kuitenkin toteutusten monimutkaisuutta ja edellyttävät huolellista suunnittelua, testausta ja elinkaaren hallintaa.

3.4 QKD:n rajattu rooli

Kvanttiavainten jakelu eli QKD on erillinen teknologia, jolla voidaan havaita avainten jakeluun kohdistuvaa salakuuntelua tietyissä viestintäympäristöissä. Se ei korvaa yleiskäyttöistä kvanttiturvallista kryptografiaa, ratkaise päätelaitteiden tai sovellusten haavoittuvuuksia eikä sovellu sellaisenaan koko hajautettuun sosiaali- ja terveydenhuollon järjestelmäkenttään. Tämän julkaisun pääasiallinen ratkaisutarkastelu kohdistuu PQC-siirtymään ja kryptografiseen ketteryyteen.

4. Terveystiedon erityisriski - kerää nyt, pura myöhemmin

Kvanttiuhka on erityisen merkityksellinen tiedoille, joiden luottamuksellisuusvaatimus ulottuu pitkälle tulevaisuuteen. Sosiaali- ja terveydenhuollossa tällaisia ovat potilas- ja asiakastiedot, kansalliset rekisteriaineistot, tutkimusaineistot, diagnostiset tiedot, genomitiedot sekä viranomaisten salassa pidettävät tiedot. Tietojen arvo hyökkääjälle voi säilyä pitkään, vaikka tietojen käyttötilanne tai alkuperäinen palvelutapahtuma olisi jo päättynyt.

4.1 Kerää nyt, pura myöhemmin -toimintamalli

Hyökkääjä voi tallentaa salattua tietoliikennettä tai kopioida salattuja aineistoja jo ennen kuin niiden avaamiseen tarvittava teknologia on käytettävissä. Tiedot voidaan pyrkiä purkamaan myöhemmin. Riskin kannalta ratkaisevaa ei siten ole vain se, onko nykyinen salaus tänään murrettavissa, vaan se, kuinka pitkään tiedon tulee säilyä luottamuksellisena ja kuinka nopeasti suojaus voidaan uusaa koko tiedon elinkaaren kattavasti.

4.2 Genomitiedon erityinen asema

Genomitieto muodostaa poikkeuksellisen pitkäikäisen ja vaikeasti korvattavan tietovarannon. Salasanoja, varmenteita ja tunnisteita voidaan vaihtaa, mutta yksilön perimää ei voida vaihtaa. Genomitiedosta voidaan lisäksi tehdä päätelmiä henkilön biologisista ominaisuuksista ja sukulaisuussuhteista. Tietoturvaloukkauksen vaikutukset eivät siksi rajoitu vain siihen henkilöön, jolta näyte tai tieto on alun perin kerätty.

Genomitietojen käsittelyssä on arvioitava erityisesti aineistojen siirrot, pitkäaikaissäilytys, varmuuskopiot, tutkimuskumppaneiden käyttöympäristöt, pilvipalveluriippuvuudet ja avainten hallinta. Pseudonymisointi vähentää suoraa tunnistettavuutta, mutta ei yksin ratkaise riskiä, jos aineisto voidaan yhdistää muihin tietolähteisiin tai jos genomitieto itsessään mahdollistaa tunnistamisen.

4.3 EHDS ja tutkimustiedon liikkuvuus

Euroopan terveystietoalue lisää terveystiedon käyttöä ja liikkuvuutta rajat ylittävissä palveluissa sekä tutkimuksen, innovoinnin ja päätöksenteon tarpeisiin. Laajempi tiedonvaihto kasvattaa niiden järjestelmien, rajapintojen, käyttöympäristöjen ja toimijoiden määrää, joiden muodostaman kokonaisuuden on säilyttävä turvallisena.

Kvanttiturvallisuus tulee huomioida osana turvallisten käyttöympäristöjen teknisiä vaatimuksia, tiedonsiirtoa, identiteetin- ja pääsynhallintaa, lokitusta, avainten hallintaa sekä pitkäaikaissäilytystä. Pelkkä tiedonsiirtoyhteyden suojaaminen ei riitä, jos tieto on käyttöympäristössä saatavilla salaamattomana liian laajasti tai jos salausavaimet voidaan saada haltuun. Kvanttiturvallinen kryptografia täydentää siten muuta tietoturvaa, mutta ei korvaa sitä.

4.4 Keskeiset riskikohteet

Riskikohde	Miksi priorisoitava	Ensimmäinen tehtävä
Pitkäikäiset potilas- ja asiakastiedot	Luottamuksellisuus vuosikymmeniä	Tunnista tietovarannot
Kanta ja integraatiot	Tieto liikkuu useiden toimijoiden välillä	Selvitä kriittiset tietovirrat
Varmuuskopiot	Salaus voi vanhentua	Arvioi salaus ja palautus
Identiteetti- ja varmennepalvelut	Luottamusketjun perusta	Selvitä riippuvuudet
Lääkinnälliset laitteet	Pitkä elinkaari	Pyydä päivityspolut

1. Rekisteri- ja tutkimusaineistojen siirrot organisaatioiden, käyttöympäristöjen ja valtioiden välillä.
2. Kanta-palveluihin, arkistoihin ja pitkäaikaissäilytykseen liittyvät kryptografiset riippuvuudet.
3. Toisiokäytön turvalliset käyttöympäristöt ja niiden rajapinnat, etäyhteydet sekä avainten hallinta.
4. Varmuuskopiot ja muut aineistot, joiden salaus on suunniteltu pitkäksi ajaksi mutta joiden salausmenetelmää ei voida helposti vaihtaa jälkikäteen.
5. Sähköiset allekirjoitukset, aikaleimat ja varmenteet, joiden eheyden ja kiistämättömyyden on säilyttävä vuosikymmeniä.
6. Lääkinnälliset laitteet, verkkokomponentit ja sulautetut järjestelmät, joiden elinkaari on pitkä ja päivitettävyyden rajallinen.

5. Siirtymä kvanttiturvalliseen kryptografiaan

Siirtymä kvanttiturvalliseen kryptografiaan on vaiheittainen kokonaisuus. Kaikkia järjestelmiä ei voida päivittää samanaikaisesti, eikä täydellisen tilannekuvan valmistumista ole tarkoituksenmukaista odottaa ennen ensimmäisiä toimia. Työ tulee käynnistää korkean riskin tietovarannoista ja palveluista, joiden suojausaika on pitkä, joiden korvaaminen on hidasta tai joiden vaarantumisella olisi vakavat vaikutukset.

5.1 Omistajuus ja johtaminen

Valmistautumisen ensimmäinen edellytys on omistajuuden nimeäminen. Organisaation tulee määrittää, kuka koordinoi kvanttiturvallisuuteen liittyvää tilannekuvaa, riskien arviointia, priorisointia ja toimeenpanoa. Vastuu ei voi jäädä yksittäisen asiantuntijan kiinnostuksen varaan, vaan sen tulee kytkeytyä tietoturvan, kokonaisarkkitehtuurin, jatkuvuudenhallinnan ja hankintojen johtamisrakenteisiin.

5.2 Kryptoinventaario ja CBOM

Kryptoinventaarion tavoitteena on tunnistaa, missä järjestelmissä, laitteissa, ohjelmistoissa, rajapinnoissa, varmenteissa ja tietovirroissa käytetään kryptografiaa. Cryptographic Bill of Materials eli CBOM kokoaa tiedot käytetyistä algoritmeista, avainpituuksista, kirjastoista, varmenteista, riippuvuuksista ja omistajista. Inventaario muodostaa perustan vaikutusarvioinnille ja siirtymän seurannalle.

Inventaario kannattaa rakentaa riskiperusteisesti. Ensimmäisessä vaiheessa tunnistetaan pitkäikäiset ja arkaluonteiset tietovarannot, internetiin tai laajoihin verkkoihin kytkeytyvät palvelut, laajat integraatiot, identiteetti- ja varmennuspalvelut sekä järjestelmät, joiden toimittaja- tai laiteriippuvuus vaikeuttaa päivityksiä. Inventaarion kattavuutta parannetaan vaiheittain samalla, kun kiireellisimmät suojaustoimet etenevät.

5.3 Krypto-ketteryys

Krypto-ketteryys tarkoittaa kykyä vaihtaa algoritmeja, avaimia, varmenteita ja kryptografisia kirjastoja ilman koko järjestelmän uudelleenrakentamista. Periaate tulee sisällyttää arkkitehtuuriin, ohjelmistokehitykseen, integraatioihin ja hankintoihin. Käytännössä se edellyttää kryptografian erottamista sovelluslogiikasta, konfiguroitavia menetelmiä, automatisoitavaa varmenteiden ja avainten hallintaa sekä testattuja päivitys- ja palautusmenettelyjä.

5.4 Toimittajat ja hankinnat

Sosiaali- ja terveydenhuollon organisaatiot ovat laajasti riippuvaisia valmisohjelmistoista, lääkinnällisistä laitteista, pilvipalveluista, verkkolaitteista ja ulkoisista palveluntarjoajista. Organisaatio ei voi toteuttaa siirtymää yksin, jos keskeiset tuotteet eivät tue uusia standardeja tai jos toimittaja ei tarjoa päivityspolkua.

Uusissa hankinnoissa tulee edellyttää kuvausta käytetyistä kryptografisista menetelmistä, tukea standardoiduille PQC-ratkaisuille, krypto-ketteryyttä, hallittavaa avain- ja varmenne-elinkaarta, päivitysten saatavuutta sekä läpinäkyvää haavoittuvuuksien hallintaa. Sopimuksissa tulee määrittää vastuut, aikataulut ja kustannukset tilanteessa, jossa kryptografinen menetelmä tai toteutus on vaihdettava.

5.5 Vaiheittainen etenemismalli

Kuvassa 2 kuvattuna siirtymän vaiheet.

1. Käynnistä johtaminen: nimeä omistaja, aseta tavoitteet ja liitä työ organisaation riskienhallintaan.
2. Tunnista kriittiset tiedot ja palvelut: arvioi suojausaika, vaikutukset ja siirtymän vaikeus.
3. Laadi kryptoinventaario: kokoa algoritmit, varmenteet, rajapinnat, laitteet, ohjelmistot ja omistajat.

4. Priorisoi ja pilotoi: aloita korkean riskin yhteyksistä, identiteettipalveluista ja pitkäikäisistä tiedoista.
5. Sisällytä vaatimukset hankintoihin: varmista tuotteiden päivitettävyyden ja toimittajien siirtymäsuunnitelmat.
6. Toteuta hallittu siirtymä: käytä tarvittaessa hybridiratkaisuja ja testaa suorituskky, yhteentoimivuus sekä palautuminen.
7. Seuraa ja ylläpidä: päivitä inventaariota, riskiarvioita ja tiekarttaa standardien sekä uhkakuvan muuttuessa.



Kuva 2. Kvanttiturvallisen siirtymän suunnittelun keskeisiä vaiheita.

6. Ohjaus, vastuut ja seuraavat askeleet

Kvanttiturvallisuus edellyttää kansallista ohjausta ja organisaatiokohtaista toimeenpanoa. Sääntely, viranomaisohjeet ja tekniset standardit määrittävät vähimmäistason, mutta käytännön siirtymä toteutuu tietovarantojen omistajien, palvelunjärjestäjien, kansallisten tietojärjestelmäpalvelujen, tutkimustoimijoiden ja järjestelmätoimittajien yhteistyönä.

6.1 Velvoittava kehikko

Kvanttiturvallisuutta tulee tarkastella osana olemassa olevia tietoturva- ja tietosuojavelvoitteita. Keskeisiä kokonaisuuksia ovat NIS2-sääntely, kyberkestävyysäädös, yleisen tietosuoja-asetuksen 32 artiklan mukainen käsittelyn turvallisuus, tiedonhallintalaki, kansalliset kryptografiset vahvuusvaatimukset sekä toimialakohtaiset vaatimukset. Velvoitteet korostavat riskiperusteisuutta, tekniikan tason huomioimista, toimitusketjujen hallintaa ja suojatoimien jatkuvaa ylläpitoa.

6.2 Vastuut

Toimija	Keskeinen vastuu
Organisaation johto	Päättää tavoitteista, riskin hyväksynnästä, resursseista ja seurannasta.
Tietohallinto ja kokonaisarkkitehtuuri	Ylläpitää järjestelmä- ja riippuvuustilannekuvaa sekä suunnittelee teknisen siirtymän.
Tietoturva ja tietosuojaja	Arvioi riskit, määrittää suojausvaatimukset ja seuraa toimeenpanoa.
Tietovarantojen ja palvelujen omistajat	Määrittävät tietojen suojausajat, vaikutukset ja toiminnalliset prioriteetit.
Hankinta ja sopimushallinta	Sisällyttää kvanttiturvallisuuden, päivitettävyyden ja toimittajavastuut vaatimuksiin.
Järjestelmä- ja palvelutoimittajat	Toteuttavat standardien tuen, päivityspolut, testauksen ja haavoittuvuuksien hallinnan.
Kansalliset palvelutoimijat	Koordinoivat yhteisten palvelujen, rajapintojen ja luottamuspalvelujen siirtymää.
Tutkimusorganisaatiot ja yliopistosairaalat	Seuraavat kehitystä, rakentavat osaamista ja arvioivat turvallisia hyödyntämiskohteita.

6.3 Osaaminen ja tutkimus

Kvanttiturvallisuuden osaamista tarvitaan sekä tietoturvan että tutkimuksen näkökulmasta. ICT- ja tietoturva-asiantuntijoiden ei tarvitse hallita kvanttifysiikkaa, mutta heidän tulee ymmärtää riskin aikajänne, kryptografiset riippuvuudet ja siirtymän periaatteet. Tutkimustoiminnassa tarvitaan lisäksi valmiutta arvioida, millaisiin laskentatehtäviin kvanttilaskenta voi tuoda hyötyä ja millä ehdoilla arkaluonteista tietoa voidaan käyttää turvallisesti.

Yliopistosairaaloiden ja muiden tutkimusintensiivisten organisaatioiden kannattaa nimetä vastuuhenkilö tai asiantuntijaryhmä seuraamaan kvanttilaskennan kehitystä. Tavoitteena ei ole hankkia omaa kvanttietokoneita, vaan rakentaa kykyä tunnistaa tarkoituksenmukaiset käyttökohteet, tehdä yhteistyötä laskentapalvelujen tarjoajien kanssa ja varmistaa, että tutkimuskäyttö täyttää tietoturvan sekä tietosuojaan vaatimukset.

6.4 Kvanttilaskennan mahdolliset hyödyt

Kvanttilaskenta voi pitkällä aikavälillä tarjota uusia menetelmiä molekyylien ja biologisten prosessien simulointiin, optimointiin sekä vaativiin tutkimusongelmiin. Mahdolliset sovellukset liittyvät esimerkiksi lääkekehitykseen, tutkimuksen laskentamenetelmiin, resurssien optimointiin ja monimutkaisten mallien ratkaisemiseen. Hyötyjen toteutuminen riippuu laitteiden, algoritmien, datan saatavuuden ja perinteisten laskentamenetelmien yhteisestä kehityksestä.

Hyötynäkökulma ei vähennä tarvetta varautua kryptografisiin riskeihin. Ensimmäiset laajasti merkittävät vaikutukset voivat kohdistua nimenomaan nykyisten salaus- ja allekirjoitusmenetelmien turvallisuuteen. Siksi sote-toimialan tulee edistää samanaikaisesti kahta tavoitetta: suojata pitkäikäinen tieto ja rakentaa hallittu valmius hyödyntää kvanttilaskentaa tutkimuksessa.

6.5 Konkreettiset suositukset

1. Nimetään jokaisessa keskeisessä sote-organisaatiossa kvanttiturvallisuuden omistaja ja liitetään aihe osaksi johdon riskiraportointia.
2. Tunnistetaan pitkäikäiset terveys-, tutkimus- ja genomitiedot sekä arvioidaan niiden suojausaika Moscan säännön avulla.
3. Käynnistetään riskiperusteinen kryptoinventaario ja ylläpidetään tietoa kryptografisista riippuvuuksista koko järjestelmäkannan elinkaaren ajan. Tehdään riskiarvio tiedon suojausajasta ja kriittisyydestä.
4. Sisällytetään krypto-ketteryys, PQC-valmius, päivityspolut ja toimittajavastuut uusiin hankintoihin ja sopimusmuutoksiin.
5. Pilotoidaan standardoituja PQC- ja hybridiratkaisuja rajatuissa korkean riskin palveluissa ennen laajaa käyttöönottoa.
6. Varmistetaan kansallinen koordinaatio Kanta-palvelujen, toisiokäytön ympäristöjen, luottamuspalvelujen, tutkimusinfrastruktuurien ja hyvinvointialueiden välillä.
7. Rakennetaan osaamista tietohallintoon, tietoturvaan, hankintoihin ja tutkimukseen sekä seurataan standardien ja uhkakuvan kehitystä säännöllisesti.

6.6 Jos valmistautumista ei tehdä

Valmistautumisen lykkääminen kasvattaa sekä tietoturvariskiä että muutoksen kustannuksia. Organisaatio voi joutua uusimaan useita kriittisiä järjestelmiä samanaikaisesti, jos siirtymä käynnistyy vasta ulkoisen määräajan tai konkreettisen uhan pakottamana. Tällöin testaukselle, kilpailutuksille, yhteentoimivuuden varmistamiselle ja henkilöstön koulutukselle jää liian vähän aikaa.

Vakavimmassa skenaariossa nykyisin tallennettu pitkäikäinen tieto voidaan tulevaisuudessa avata, sähköisten allekirjoitusten luotettavuus heikkenee tai keskeisiä palveluja ei voida päivittää hallitusti. Seurauksina voivat olla luottamuksellisten tietojen paljastuminen, palvelukatkot, oikeudelliset vastuut, kustannusten kasvu ja luottamuksen heikkeneminen. Ennakoiva, vaiheittainen siirtymä pienentää näitä riskejä ja mahdollistaa kustannusten jakamisen usealle vuodelle.

7. Kvanttilaskenta vuonna 2035: kolme skenaariota

Seuraavat skenaariot eivät ole ennusteita, vaan vaihtoehtoisia kehityskulkuja riskienhallinnan, varautumisen ja päätöksenteon tueksi. Todennäköinen kehitys voi sisältää piirteitä useammasta skenaariosta, ja tilannetta tulee arvioida säännöllisesti teknologian, standardien ja uhkakuvan muuttuessa.

Skenaario 2035	Teknologinen tilanne	Tekoäly ja kvanttilaskenta	Riskienhallinta ja kyberturvallisuus
1. Hidas kehitys	Kvanttikoneet ovat edelleen pääasiassa tutkimuksen ja rajattujen erityisongelmien välineitä. Virheenkorjaus ja skaalautuminen rajoittavat laajaa käyttöä.	Tekoäly toimii pääosin klassisilla CPU- ja GPU-alustoilla. Kvanttilaskentaa kokeillaan rajatusti esimerkiksi optimoinnissa ja simuloinnissa.	Välitön kvanttiuhka nykyiselle kryptografialle pysyy rajallisena, mutta PQC-siirtymä etenee. Keskeisiä riskejä ovat investointien ajoitus, osaamisvajae ja riippuvuus harvoista teknologiatoimittajista.
2. Hybridimaailma	Kvanttilaskenta muodostuu osaksi pilvi- ja HPC-infrastruktuuria. QPU toimii erikoistuneena kiihdyttimenä CPU:n ja GPU:n rinnalla.	Tekoäly, HPC ja kvanttilaskenta muodostavat yhteisen laskentakokonaisuuden. Tekoäly voi tunnistaa tehtävän ja ohjata sen tarkoituksenmukaisimmalle laskentaresurssille.	Hybridiympäristö kasvattaa toimitusketju-, pilvi-, rajapinta- ja riippuvuusriskejä. Korostuvat kryptografinen ketteryys, jatkuvuudenhallinta, toimittajariippuvuudet, datan suojaaminen ja teknologinen suvereniteetti.
3. Kvanttiläpimurto	Riittävän suuret virheenkorjatut kvanttikoneet tuottavat merkittävää hyötyä useilla sovellusalueilla.	Tekoälyn ja kvanttilaskennan yhdistelmä mahdollistaa uudenlaisia optimointi-, simulointi- ja mahdollisesti koneoppimiskäytöksiä.	Kyberympäristö muuttuu olennaisesti, jos kryptografisesti merkityksellinen kvanttilaskenta toteutuu. Organisaatioiden on tällöin oltava siirtyneet kvanttiturvalliseen kryptografiaan. Samalla syntyy uusia strategisia riippuvuuksia laskentakapasiteetista, osaamisesta ja infrastruktuurista.

7.1 Välivaiheet 2026–2035

Kehitystä voidaan jäsentää neljän toisiaan täydentävän vaiheen kautta. Vaiheet ovat suuntaa antavia, ja niiden ajoitus voi muuttua teknologian kehityksen myötä.

2026–2028 – varautumisen vaihe. Kvanttilaitteet kehittyvät, mutta organisaatioille keskeisin kysymys on kvanttivalmius. Tähän kuuluvat kryptografisten riippuvuuksien kartoittaminen, PQC-siirtymän suunnittelu, kerää nyt, pura myöhemmin -riskin arviointi sekä kvanttiosaamisen rakentaminen.

2028–2031 – kokeilujen ja ensimmäisten käyttötapausten vaihe. Kvanttilaskentaa kokeillaan tekoälyn ja HPC:n rinnalla esimerkiksi optimoinnissa, materiaalitutkimuksessa ja lääketutkimuksessa. Riskienhallinnassa on arvioitava, missä kvanttilaskentaa kannattaa käyttää ja missä ei. Teknologiariski, kustannukset, toimittajalukkiutuminen ja datan sijainti korostuvat.

2031–2033 – integraatiovaihe. Kvanttilaskenta voi muuttua erillisestä teknologiasta osaksi laajempaa laskentainfrastruktuuria. Riskienhallinta laajenee yksittäisen teknologian arvioinnista tekoälyn, HPC:n ja QPU-resurssien muodostaman kokonaisuuden hallintaan. Kyberturvallisuuden lisäksi korostuvat jatkuvuus, toimitusketjut, vastuut ja digitaalinen suvereniteetti.

2033–2035 – orkestroitu hybridimalli. Käyttäjän ei välttämättä tarvitse tietää, missä laskenta suoritetaan. Tekoälypohjainen orkestrointi voi jakaa tehtävän CPU:n, GPU:n ja QPU:n kesken ja yhdistää tulokset päätöksenteon tueksi.

Data → tekoäly → tehtävän luokittelu → CPU / GPU / QPU → tulosten yhdistäminen → päätöksenteko

Riskienhallinnan näkökulmasta keskeinen muutos on, että kvanttiriski ei enää tarkoita vain salauksen murtumisen riskiä. Se laajenee koko teknologisen ekosysteemin hallintaan: kuka hallitsee laskentakapasiteettia, missä data käsitellään, mihin toimittajiin toiminta on sidoksissa, miten tekoäly ohjaa laskentaresurssien käyttöä ja miten toiminta jatkuu kriittisen komponentin häiriötilanteessa.

Liitteet

Liite 1. Keskeiset käsitteet

CBOM: Cryptographic Bill of Materials, kuvaus järjestelmän kryptografisista komponenteista ja riippuvuuksista.

CRQC: Cryptographically Relevant Quantum Computer, kvanttietokone, joka kykenee käytännössä murtamaan merkityksellisiä nykyisiä julkisen avaimen menetelmiä.

Krypto:

Yleisnimitys kryptografialle eli menetelmille, joilla suojataan tietoja ja varmistetaan niiden luotettava käsittely, siirto ja säilytys.

Krypto-ketteryys: Kyky vaihtaa kryptografisia menetelmiä, avaimia ja varmenteita hallitusti ilman koko järjestelmän uudelleenrakentamista.

PQC: Post-quantum cryptography, tavallisilla tietokoneilla toteutettava kryptografia, jonka on tarkoitus kestää myös kvanttihyökkäyksiä.

Q-Day: Ajankohta, jolloin käytettävissä on nykyisiä laajasti käytettyjä julkisen avaimen menetelmiä käytännössä murtava kvanttietokone.

QKD: Quantum Key Distribution, kvantti-ilmiöihin perustuva avainten jakeluteknologia.

Fyysinen kubitti: Kvanttilaitteen fyysinen informaation perusyksikkö, joka on altis virheille.

Looginen kubitti: Virheenkorjauksen avulla useista fyysisistä kubiteista muodostettu luotettavampi laskennallinen kubitti.

Liite 2. Lähteitä ja jatkolukemista

8. Huoltovarmuuskeskus (2024). Kvanttilaskennan tietoturva-vaikutukset - suositus varautua. <https://www.huoltovarmuuskeskus.fi/julkaisu/kvanttilaskennan-tietoturva-vaikutukset-suositus-varautua>
9. Liikenne- ja viestintävirasto Traficom / Kyberturvallisuuskeskus. Kvanttiturvallinen salaus ja PQC-siirtymä. <https://kyberturvallisuuskeskus.fi/fi/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille/kvanttiturvallinen-salaus-ja-pqc-siirtyma>
10. National Institute of Standards and Technology (NIST). FIPS 203, FIPS 204 ja FIPS 205.
FIPS 203: <https://csrc.nist.gov/pubs/fips/203/final>
FIPS 204: <https://csrc.nist.gov/pubs/fips/204/final>
FIPS 205: <https://csrc.nist.gov/pubs/fips/205/final>
11. European Union Agency for Cybersecurity (ENISA). Post-quantum cryptography -ohjeistus ja siirtymää tukevat julkaisut. ENISA Cryptography: <https://www.enisa.europa.eu/topics/digital-identity-and-data-protection/cryptography>
ENISA Post-Quantum Cryptography: Current State and Quantum Mitigation: <https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation>
12. Beyond Limits of PQC -tutkimushanke: www.pqc.fi.