VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Kirje

26.2.2026

VN/4273/2026
VN/4273/2026-VM-2

Jakelun mukaisesti

Kvanttiturvallisiin salausratkaisuihin siirtyminen julkisessa hallinnossa: tietoperusta ja suositukset kunnille

Tausta

Suomen kyberturvallisuusstrategia 2024–2035 on hyväksytty valtioneuvoston periaatepäätöksenä 10.10.2024. Strategia on päivitetty vastaamaan muuttunutta geopoliittista ja digitaalista ympäristöä. Kyberturvallisuus ei ole enää pelkästään tekninen kysymys, vaan olennainen osa kansallista turvallisuutta ja kokonaisturvallisuuden mallia. Kyberturvallisuusstrategian toimeenpanosuunnitelma kuvaa tavoitteiden saavuttamiseksi tarvittavat toimenpiteet vastuineen ja mittareineen. Toimeenpanosuunnitelma sisältää mm. toimenpiteen 1.4: *Otetaan kansallisesti käyttöön kvanttiturvalliset salausratkaisut* sekä toimenpiteen 4.2*: Kehitetään kuntien valmiuksia ja kykyä varautua ja reagoida oikea-aikaisesti kyberhäiriöihin*.

Kvanttiturvallisiin salausratkaisuihin siirtymiselle on muun muassa Yhdysvalloissa, Iso-Britanniassa ja Euroopan Unionissa hahmoteltu pääsääntöisesti yhtenevät tavoiteaikataulut ja toimenpiteet. EU:n kvanttiturvallisiin salausratkaisuihin siirtymisen tiekartan suositusten mukaan korkean riskin kohteiden osalta siirtymä tulisi toteuttaa vuoteen 2030 mennessä ja kokonaisuudessaan vuoteen 2035 mennessä. Siirtymää edeltävinä toimenpiteinä mm. nykyisin käytössä olevien salausmenetelmien ja kriittisen tiedon tunnistaminen sekä kvanttiturvallisiin salausratkaisuihin siirtymisen suunnittelu on suositeltavaa toteuttaa vuoden 2026 kuluessa.

Työ- ja elinkeinoministeriön 24.4.2025 julkaiseman kansallisen kvanttiteknologiastrategian tavoitteiden mukaan Suomessa on samanaikaisesti kvanttiteknologisen kehityksen kanssa vahvistettava salausteknologista kyvykkyyttä myös kyberturvallisuusalan yrityksiä laajemmin eri teollisuudenaloilla, sekä muissa salausratkaisuja käyttävissä organisaatioissa. Suomen strategisena tavoitteena on olla omavarainen ja kvanttiuhkaan varautunut valtio 2030-luvun alkupuolella.

Tämän kirjeen tarkoituksena on tarjota tietoa kvanttitietokoneiden ja kvanttilaskennan muodostamasta uhkasta kyberturvallisuudelle sekä tiedon ja tietoliikenteen salausratkaisuille. Lisäksi kirjeessä suositellaan kuntatoimijoille toimenpiteitä, joiden avulla voidaan turvata kuntakentän

Postiosoite Postadress Postal Address	Käyntiosoite Besöksadress Office	Puhelin Telefon Telephone	Faksi Fax Fax	s-posti, internet e-post, internet e-mail, internet
Valtiovarainministeriö PL 28 00023 Valtioneuvosto	 Snellmaninkatu 1 A Helsinki	 0295 16001 +358 295 16001		 kirjaamo.vm@gov.fi

tietoja ja tietojärjestelmiä kvanttiuhan varalta. Lähdeluettelossa on tuotu esille teoksia sekä sivustoja, joiden kautta löytyy käsiteltäviin aiheisiin liittyvää lisätietoa ja ohjeistuksia.

Kvanttilaskennan uhat ja kvanttiturvallisen salauksen tarve

Kvanttilaskenta edustaa merkittävää harppausta laskentatehon kehityksessä, mutta sen myötä syntyy myös vakavia uhkia nykyisille salausmenetelmille. 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 ja salattujen verkkoyhteyksien muodostamisessa (SFTP-tiedonsiirto, VPN- ja SSH-yhteydet).

Perinteisten julkisen avaimen salausalgoritmien turvallisuus perustuu matemaattisiin ongelmiin (esim. alkulukujen tekijöihin jakaminen ja diskreetti logaritmi), jotka ovat nykyisillä tietokoneilla laskennallisesti vaikeita. Kvanttitietokoneet voivat kuitenkin ratkaista nämä ongelmat tehokkaasti, mikä helpottaa nykyisten salausmenetelmien murtamista huomattavasti.

Tällä hetkellä perinteisen julkisen avaimen salauksen murtamiseen kykenevää kvanttitietokonetta ei tiettävästi ole vielä käytössä. Kehitystä niin kvanttitietokoneiden kuin algoritmien osalta tapahtuu kuitenkin jatkuvasti, eikä pystytä tarkalleen arvioimaan, milloin nykyisten salausten murtaminen on mahdollista. Arviot aikataulusta vaihtelevat muutamista vuosista reiluun vuosikymmeneen.

Tällä hetkellä yksi keskeisimmistä kvanttilaskennan uhkista on kuitenkin rikollisten tahojen mahdollisuus kerätä perinteisin menetelmin suojattua dataa ja murtaa salaus sitten, kun tarpeeksi kyvykäs kvanttitietokone on käytössä (harvest now, decrypt later –uhka). Tällaisen hyökkäyksen kohteena voivat olla mm. pitkää säilyttämistä ja erityistä suojaamista vaativat tiedot sekä tietojen varmuuskopiot (esim. henkilö- ja terveysdata, valmius- ja turvallisuussuunnitelmat, tunnistetiedot ja salausavaimet, liikesalaisuuden alaiset tiedot).

Kvanttiturvalliseen salaukseen, Post-Quantum Cryptography (PQC), tarvitaan uudenlaisia matemaattisia ongelmia, joiden ratkaiseminen on vaikeaa sekä klassisella että kvanttitietokoneella. Nykyisten julkisen avaimen salausratkaisujen korvaaminen kvanttiturvallisilla salausratkaisuilla on tullut mahdolliseksi PQC-standardoinnin myötä. Yhdysvaltalainen National Institute of Standards and Technology (NIST) on julkaissut vuonna 2024 kolme epäsymmetristä salausstandardia, joiden avulla yritykset ja organisaatiot voivat päivittää salausratkaisunsa kvanttitietokoneiden aiheuttamien kyberuhkien varalta.

Kvanttiturvallisten salausratkaisujen käyttöön siirtyminen

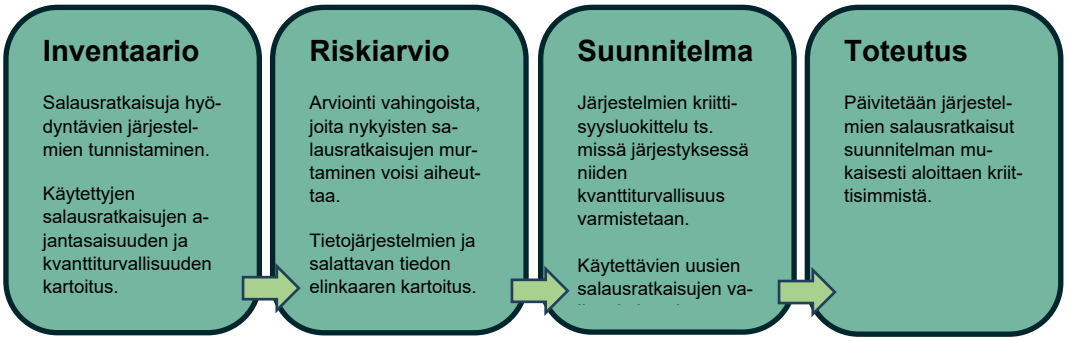
Sen lisäksi, että nykyisillä salausmenetelmillä suojattua tietoa voidaan varastoida jo tällä hetkellä myöhempää purkamista varten, tulee huomioida myös järjestelmien kvanttiturvallisiksi päivittämiseen kuluva aika. Kyseessä on useimmissa tapauksissa laaja sekä erilaisia vaiheita sisältävä kokonaisuus, jonka toteutus kestää kokonaisuudessaan useita vuosia. Tästä syystä kvanttiturvallisiin salausratkaisuihin siirtymisen toimenpiteet on syytä käynnistää mahdollisimman aikaisessa vaiheessa.

Siirtyminen kvanttiturvallisten salausalgoritmien käyttöön, eli PQC-siirtymä, tulee aloittaa kartoittamalla omissa tietojärjestelmissä ja tietoliikenneratkaisuissa nykyisin käytössä olevat salausmenetelmät. Samassa yhteydessä tulee tunnistaa organisaation kriittisimmät salassa pidettävät tiedot ja niiden ajallinen salassapito- ja säilytystarve. Tätä vaihetta kutsutaan myös kryptoinventaarioksi. Järjestelmien kriittisyysluokittelun tueksi löytyy ohjeistusta mm. Liikenne- ja

viestintävirasto Traficomin Kyberturvallisuuskeskuksen sekä Digi- ja väestötietoviraston (DVV) sivustoi-lta. Vuoden 2026 aikana julkaistaan myös aiheeseen liittyvä eOppiva-koulutus.

Seuraavaksi organisaatioiden tulee laatia suunnitelma kvanttiturvallisiin ratkaisuihin siirtymisestä mahdollisine välivaiheineen. Vaiheistus voi tarkoittaa esimerkiksi nykyisten salausratkaisujen ja PQC-ratkaisujen käyttöä rinnakkain ennen täysimääräiseen PQC-aikakauteen siirtymistä. Suunnittelun yhteydessä on hyvä laatia myös oman organisaation tiekartta, joka kuvaa PQC-siirtymän eri vaiheet ja aikataulut. Suunnitteluvaiheen jälkeen toteutetaan varsinainen siirtymä, joka aloitetaan riskiarvioinnin perusteella kriittisimmistä kohteista.

Laajasti käytössä olevien ja aktiivisesti ylläpidettyjen kaupallisten valmisohjelmistojen voidaan olettaa kehittyvän kvanttiuhkaa vastaan suojatuiksi, **kunhan ne pidetään ajantasaisina ja päivitykset otetaan käyttöön säännöllisesti** (esim. Windows-käyttöjärjestelmä, Microsoft 365 sekä yleiset toimisto- ja viestintäsovellukset). Muiden kuin kaupallisten ohjelmistotuotteiden- ja palveluiden toimittajien tietoisuus sekä kyvykkyydet kvanttiturvallisuuden ja PQC-siirtymän osalta tulee varmistaa.



Kaavio 1. Esimerkki PQC-siirtymän vaiheista, joita voi toteuttaa osin myös yhtäaikaisesti.

Kvanttiuhkaan varautumisen edellyttämät toimenpiteet kunnissa

Valtiovarainministeriö suosittelee

1) tutustumaan kvanttiuhkia ja kvanttiturvallisia salausratkaisuja koskeviin tietoaineistoihin. Lisätietoa ja ohjeistuksia löytyy kattavasti mm. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen ja Huoltovarmuuskeskuksen sivustoilta (ks. lähteet ja linkit) sekä
2) käynnistämään ja edistämään PQC-siirtymän ensimmäisten vaiheiden toimenpiteitä (mm. kryptoinventaario, suunnitelman laatiminen) vuoden 2026 aikana.

Suositukset ovat Suomen kyberturvallisuusstrategian tavoitteiden mukaisia sekä vahvistavat kansallista huoltovarmuutta ja varautumista. Suositusten ja ohjeistusten mukaisilla toimenpiteillä voidaan varmistaa kriittisten palveluiden ja tietojärjestelmien kyky kestää kvanttiteknologian aiheuttamat kyberuhkat.

Kuntia pyydetään välittämään tämä kirje myös liikelaitoksiinsa ja omistamiinsa yhtiöihin sekä muihin yhteisöihin.

Muita kyberturvallisuuden varautumistoimenpiteitä

Kyberturvallisuuskeskus tarjoaa palveluita tieto- ja kyberturvallisuuden edistämiseksi kuntasektorilla. Valtiovarainministeriö suosittelee Kyberturvallisuuskeskuksen Hyöky-palvelun ja Havaropalvelun käyttöönottoa. Hyöky-palvelu auttaa organisaatioita ennakoimaan tietoturva- ja kyberuhkia kartoittamalla niiden digitaalista hyökkäyspinta-alaa. Hyöky-palvelua tarjotaan

veloituksetta julkisen hallinnon toimijoille. Havaro-palvelu tunnistaa ja hälyttää vakavista tietoturvauh-kista. Hyöky-palvelun ja Havaro-palveluun käyttöönottoa tulisi harkita osana kokonaisvaltaista tieto- ja kyberturvallisuuden kehittämistä.

Valtiovarainministeriö suosittelee hyödyntämään tieto- ja kyberturvallisuuden kehittämisessä Digi- ja väestötietoviraston (DVV) tarjoamia palveluja. Kuntia pyydetään harkitsemaan liittymistä Digiturvan kokonaiskuvapalveluun, jonka avulla voi arvioida, seurata ja raportoida hallinnollisen kyberturvallisuuden tilannekuvaa sekä suunnitella toimenpiteitä sen edelleen kehittämiseksi. Julkri-työkalut ovat hyödynnettävissä asetettaessa tietojärjestelmän hankintavaatimuksia ja tietoturvallisuuden vaatimustenmukaisuuden arviointivaatimuksia.

Kuntakentän toimijoiden on suositeltavaa myös seurata, miltä osin mm. kvanttiturvallisuutta ja PQC-siirtymää käsitellään Kuntaliiton ylläpitämässä Kuntien tietoturvavastaavien verkostossa.

Lähteet ja linkit

Valtioneuvoston kanslia (2024). Suomen Kyberturvallisuusstrategia 2024–2035. (VNK 2024:11).

Työ- ja elinkeinoministeriö (2025). Suomen kvanttiteknologiastrategia 2025–2035: Suomen uusi kasvun moottori ja kestävän tulevaisuuden rakentaja. (TEM 2025:17).

Euroopan komissio (2025). Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. EU:n PQC-siirtymän tiekartta. Saatavilla: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. Ohjeet ja oppaat organisaatioille ja yrityksille. Saatavilla: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

Digi- ja väestötietovirasto (DVV). Kriittisten kohteiden luokittelumenetelmä ja -työkalu. Saatavilla: https://kehittajille.suomi.fi/palvelut/digiturva/jatkuvuuden-hallinta-ja-varautuminen/kriittisten-kohteiden-suojaaminen/kriittisten-kohteiden-luokittelumenetelma-ja-tyokalu

Huoltovarmuuskeskus (2024). Kvanttilaskennan tietoturvavaikutukset – suositus varautua. Saatavilla: https://www.huoltovarmuuskeskus.fi/julkaisu/kvanttilaskennan-tietoturvavaikutukset-suositus-varautua

Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. Hyöky-palvelu. Saatavilla: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/hyoky

Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. Havaro-palvelu. Saatavilla: https://havaro.fi/fi

Digi- ja väestötietovirasto (DVV). Digiturvan kokonaiskuvapalvelu. Saatavilla: https://www.suomi.fi/palvelut/digiturvan-kokonaiskuvapalvelu-digi-ja-vaestotietovirasto/1b38df61-ca48-41b4-a238-da5ab1baaf27

Kuntaliitto. Kuntien tietoturvavastaavien verkosto. Saatavilla: https://www.kuntaliitto.fi/kuntajohtaminen-ja-digitalisaatio/Digitaalinen-turvallisuus/tietoturvaverkosto

ICT-johtaja, ylijohtaja	Jarkko Levasma
Erityisasiantuntija	Kimmo Hast

Jakelu Kunnat, pl Ahvenanmaa

Tiedoksi
Valtiovarainministeriö
LVM
LVM/Valtion kyberturvallisuusjohtajan toimisto
Liikenne- ja viestintävirasto
Kuntaliitto
Digi- ja väestövirasto

VN/4273/2026-VM-2

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons:

Hast Kimmo 91360034V	Levasma Jarkko 91256614R
2026-02-26	2026-02-26