

Kvanttiturvalliseen salaukseen siirtyminen

Johdon tiivistelmä

Julkisen avaimen salausratkaisut tulee päivittää kvanttiturvallisiksi

Mitä asia koskee?

Riittävän tehokkaalla kvanttietokoneella voidaan purkaa julkisen avaimen salaus, jota käytetään

- lähes kaikessa verkkoliikenteessä,
- kaikessa digitaalisessa allekirjoittamisessa ja
- lähes kaikessa tunnistautumisessa.

Milloin?



On mahdollista, että riittävän tehokas kvanttietokone onnistutaan kehittämään seuraavan kymmenen vuoden kuluessa.

Suurimmat riskit



Varasta nyt, pura myöhemmin

Harvest now, decrypt later -menetelmä on akuutti uhka. Jo nyt hyökkääjät varastavat VPN-liikennettä ja muita salattuja tietoja, jotka voi purkaa, kun sopiva teknologia on saatavilla.



Tunnistautumisen murtaminen

Kun tunnistautumisen murtamiseen kykenevä kvanttietokone saadaan kehitettyä, nykyisiin tunnistautumiskeinoihin perustuva luottamus menettää merkityksensä.

Kvanttiturvallinen salaus

Post Quantum Cryptography, PQC

- PQC-salausratkaisut kestävät sekä klassisilla että kvanttietokoneilla tehtävät murtoyritykset.
- Haavoittuvat salaukset on päivitettävä PQC-salaukseen kiireellisyysjärjestyksessä.
- PQC-tuki on myös huomioitava uusien salaustuotteiden hankinnassa.

Kiireellisimmin päivitystä vaativat



yli vuosikymmenen salassapitoaikaa vaativaa tietoa suojaavat salausratkaisut,



korkean turvallisuusluokan tieto, arkaluontoinen henkilötieto, keskeiset yrityssalaisuudet ja muut vastaavat sekä



VPN-salausratkaisut erityisesti julkisen internetin yli.

TAUSTAA

Salausten purkaminen on yksi kvanttietokoneiden kehitystä ajava motiivi

Miksi kvanttietokoneita kehitetään?

- Kvanttietokoneita kehitetään muun muassa tieteen tarpeisiin: kvanttilaskenta voi mullistaa esimerkiksi kemian ja lääketieteellisuuden sekä koneoppimisen.
- Riittävän tehokasta kvanttietokonetta voidaan tulevaisuudessa käyttää myös nykyisten salausratkaisujen purkamiseen. Tämä on monilla tahoilla yksi kehittämisen motiiveista.
- Kuten kaikkea uutta teknologiaa, myös kvanttietokoneita tullaan niiden yleistyessä käyttämään rikollisiin tarkoituksiin.

Tänään salattu tieto voi olla luettavissa tulevaisuuden teknologialla

- Laajassa käytössä oleva julkisen avaimen salaus perustuu matemaattisiin ongelmiin, jotka ovat vaikeita perinteisille tietokoneille. Kvanttietokoneet voivat ratkaista osan näistä ongelmista paljon tehokkaammin tai kokonaan uusilla tavoilla.
- Pitkään salassa pidettävä tieto on salattava kvanttiturvallisesti jo nyt, hyvissä ajoin ennen kvanttikoneiden valmistumista.

Esimerkkejä salausratkaisujen käytöstä



lähes kaikki internetliikenne



VPN-yhteydet



globaali passijärjestelmä



verkkopankkien tunnistautuminen



terveystietojen säilytys

Suojaa organisaatiosi kvanttiturvalliseksi

1

Tunnista tilanne organisaatiossasi

Osallista mukaan tarvittavat tahot, esimerkiksi

- johto,
- ICT- asiantuntijat,
- tiedonhallinnan asiantuntijat ja
- muut asiantuntijat.

2

Kartoita päivitettävät kohteet

Siirtymä suunnitellaan tunnistettuihin riskeihin pohjautuen.

Kvanttiriskianalyysi

- Tunnista organisaation kriittisimmät suojattavat tiedot.
- Tunnista, mitkä tiedot ja järjestelmät ovat pahiten alttiina *harvest now, decrypt later* -uhalle

Kryptoinventaario

- Inventaario parantaa ymmärrystä organisaation omista järjestelmistä.
- Tunnista, mitä salaustuotteita organisaatiollanne on käytössä ja missä yhteyksissä.

Riippuvuuskartta

- Tunnista järjestelmien ja palveluiden väliset riippuvuudet sekä toimittajaketjut.

3

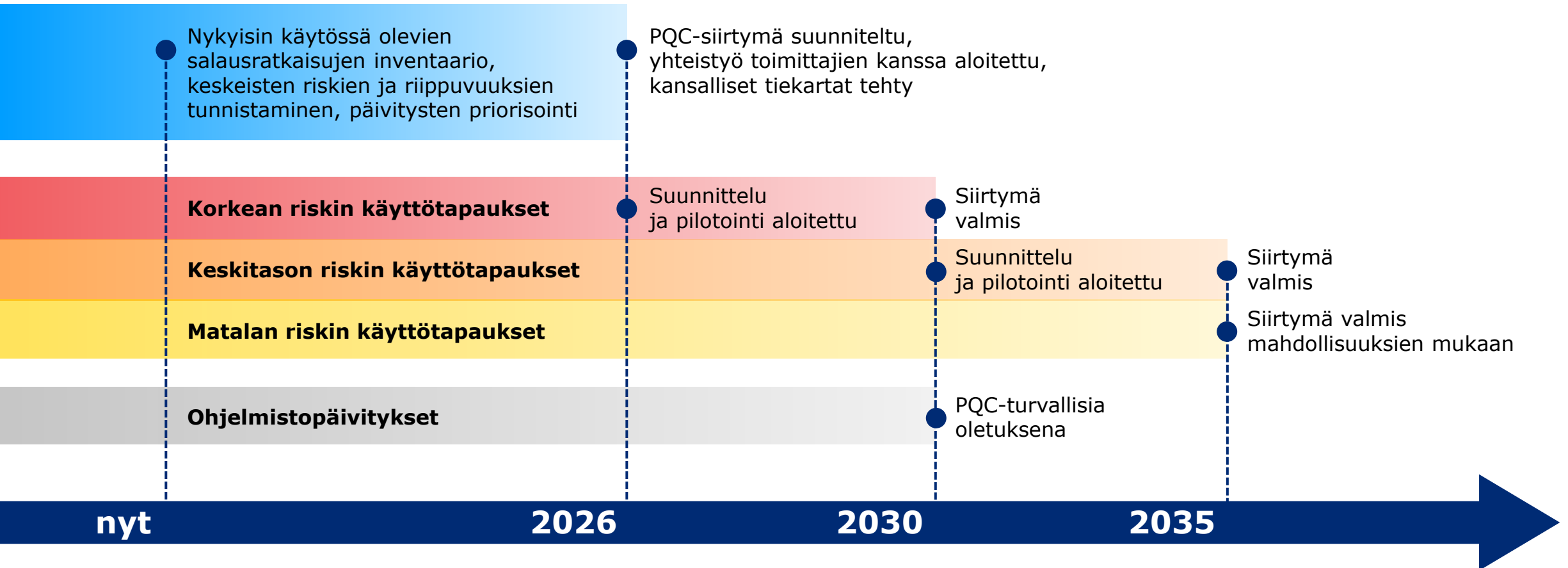
Ryhdy toteuttamaan siirtymää

- Päivitä haavoittuvat salaukset PQC-salaukseen kiireellisyysjärjestyksessä.
- Huomioi PQC uusissa hankinnoissa: vaadi toimittajilta PQC-valmiutta tai uskottavaa päivityssuunnitelmaa.
- Päivittäminen vaatii suunnitelmallisuutta ja tilanteen seuraamista: esimerkiksi VPN-ratkaisuja on jo olemassa, mutta varmenne-infrastruktuurin päivittäminen vie aikaa.
- Matalan riskin järjestelmät päivitetään mahdollisuuksien mukaan.

AIKATAULU

EU:n tiekartta kvanttiturvalliseen salaukseen siirtymiseen

Siirtymän tavoiteajat ja toimenpiteet ovat pitkälti samat myös muun muassa Iso-Britannian ja Yhdysvaltojen osalta. EU-tiekartta sisältää ohjeita ja viitteitä käytötapauksen riskitason arviointiin.



Kiitos!

Lisätietoja:
[kyberturvallisuuskeskus.fi](https://www.kyberturvallisuuskeskus.fi)

TLP: CLEAR