How to prepare for Post-Quantum transition?

27-05-2025

Antti Leskinen, Pre-Sales Consultant

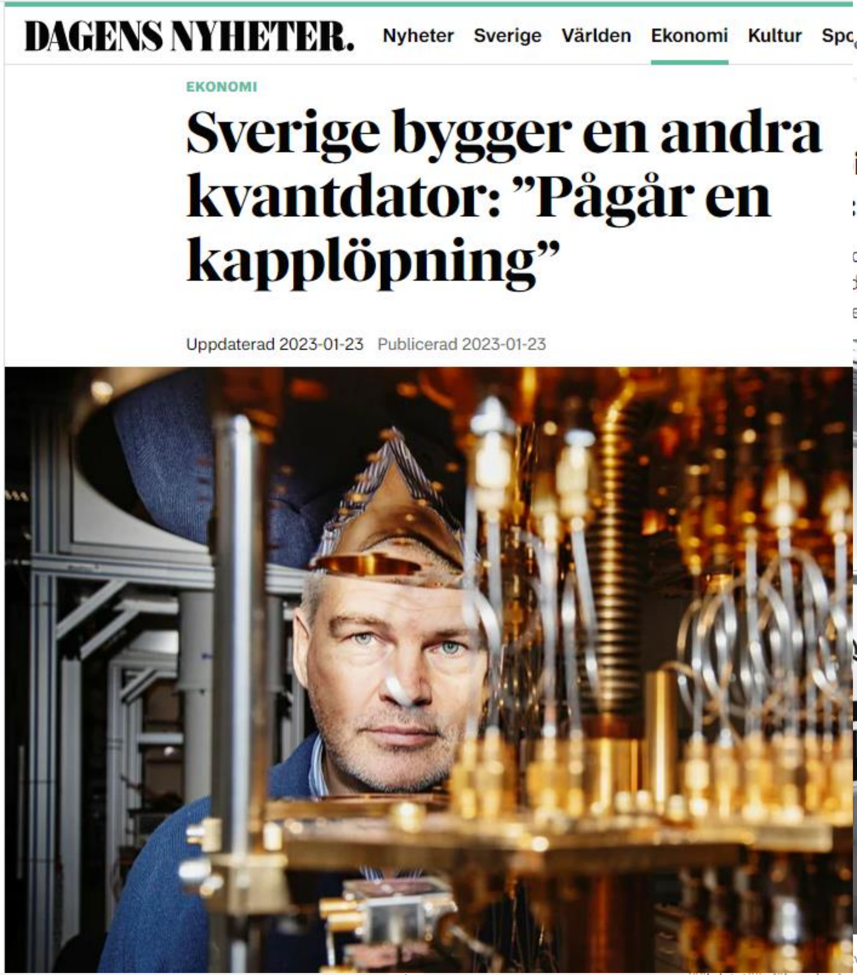
www.thalesgroup.com

What is a quantum computer?

A **proposed** new type of computer that seeks to exploit the properties of **quantum mechanics** such as entanglement and superposition to exponentially speedup computing performance for **some** hard problems.

Quantum comp

Google Sycamor

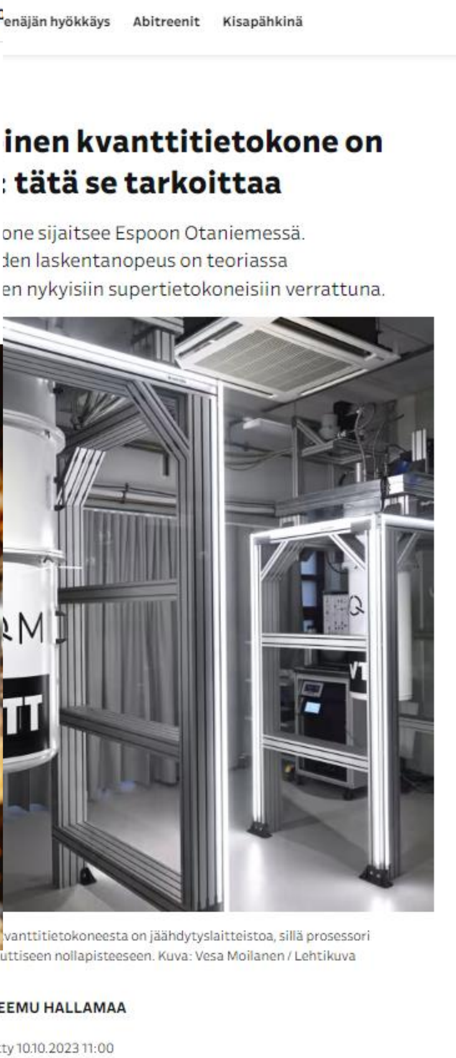


DAGENS NYHETER. Nyheter Sverige Världen Ekonomi Kultur Spo

EKONOMI

Sverige bygger en andra kvantdator: ”Pågår en kapplöpning”

Uppdaterad 2023-01-23 Publicerad 2023-01-23



enäjän hyökkäys Abitreenit Kisapähkinä

inen kvanttitietokone on : tätä se tarkoittaa

one sijaitsee Espoon Otaniemessä.
den laskentanopeus on teoriassa
en nykyisiin supertietokoneisiin verrattuna.

vanttitietokoneesta on jäähdytyslaitteistoa, sillä prosessori jäähdytetään lähes absoluuttiseen nollapisteeseen. Kuva: Vesa Moilanen / Lehtikuva

SIMO KYMÄLÄINEN, TEEMU HALLAMAA

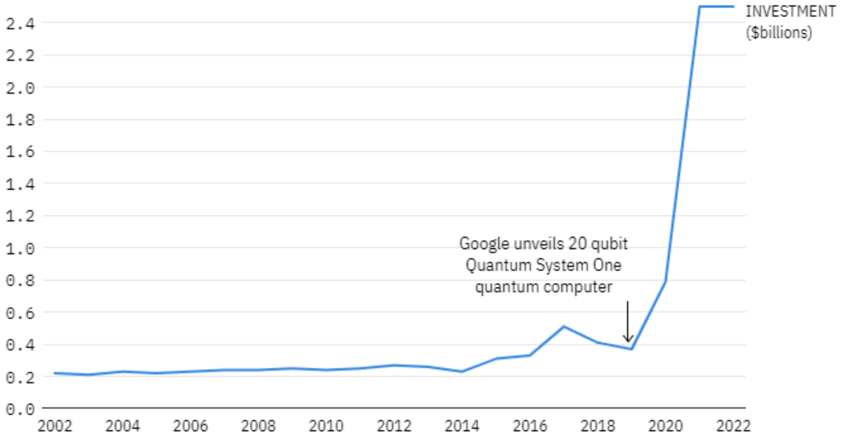
10.10.2023 9:00 · Päivitetty 10.10.2023 11:00

With record funding and investment in Quantum Tech

Private and Public Investments in Quantum Technologies continues to rise dramatically

Quantum investment hit record high in 2021

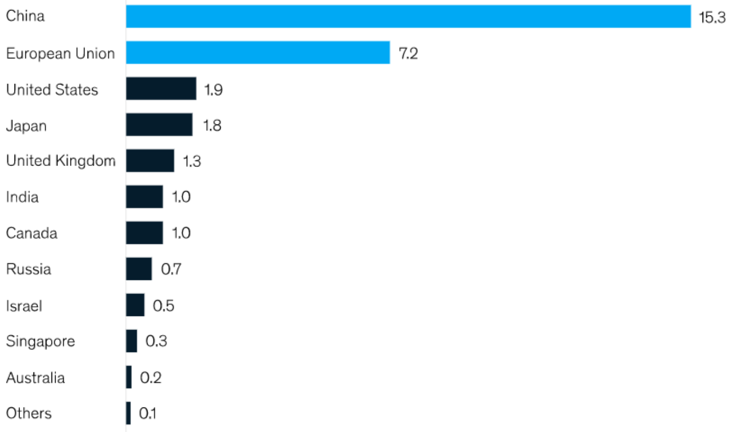
Investors started to pour billions into quantum technologies from 2021 after years of relatively stable investment levels.



TECHMONITOR

China and the European Union have announced the most public funding planned for quantum computing efforts.

Announced planned governmental funding,[1] $ billion



[1] Total historic announced funding; timelines for investment of funding vary by country.
Source: Johnny Kung and Muriam Fancy, *A quantum revolution: Report on global policies for quantum technology*, CIFAR, April 2021; McKinsey analysis

McKinsey & Company

THALES

What is so important about this topic?

World Depends on Public Key Infrastructure (PKI) to Establish Trust

- TLS, IPsec, SSH, S/MIME for the Internet
- Code signing technology that maintains software integrity
- Document signing to prove authenticity
- Information rights management solutions

PKI Depends on Asymmetric Key Protocols

RSA, ECC and others are vulnerable to Quantum attacks

Quantum computers and research will efficiently crack PKI and Code Signing

Tech industry is working hard and fast to make a quantum computer. Waiting until one is made is too late to act.

Post-Quantum Cryptography (PQC) will maintain our "way of life"

Crypto agile products allow us to use PQC algorithms and keys today

Simply said

Without quantum-resistant encryption, **everything** that has been transmitted, or will ever be transmitted over a network, **will be vulnerable** to eavesdropping and public disclosure.

—ETSI White Paper No. 8 Quantum Safe Cryptography and Security

Area of high risk: Authenticated Software

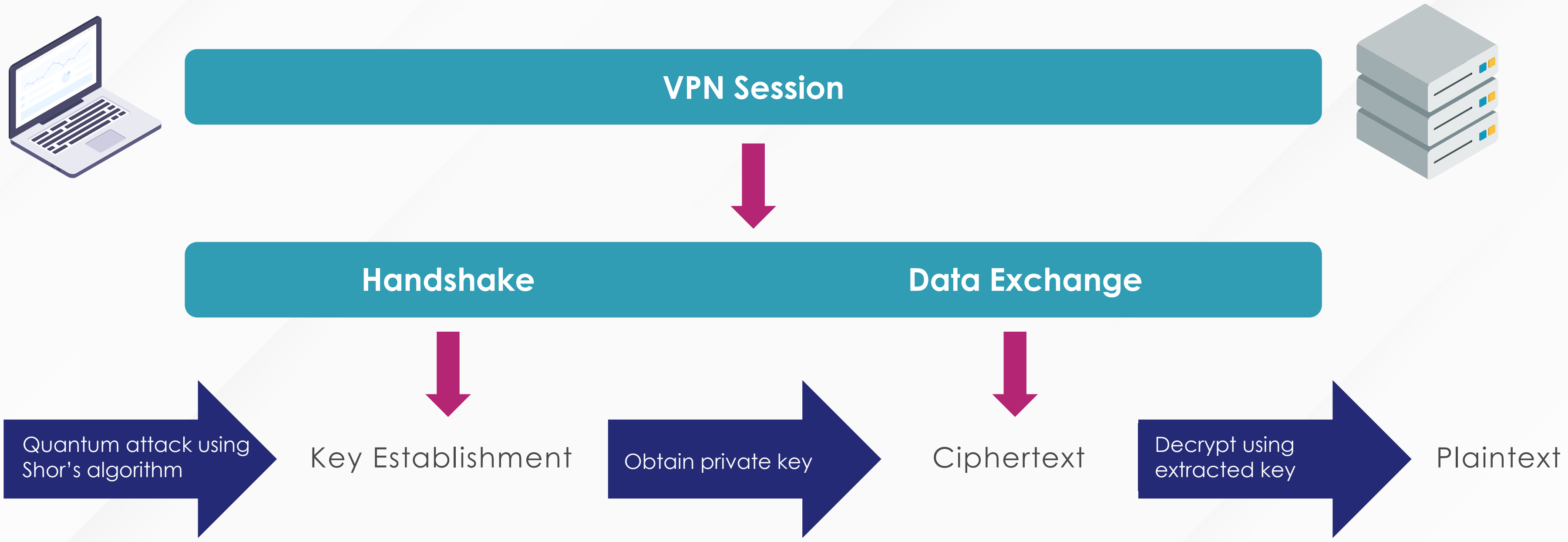
What's at risk?

Durable connected devices (IoT) with **long in-field lives**

What's the attack?

Forged software updates by quantum-enabled adversaries

Area of high risk: Confidential Communications



VPN Session

Handshake

Data Exchange

Quantum attack using Shor's algorithm

Key Establishment

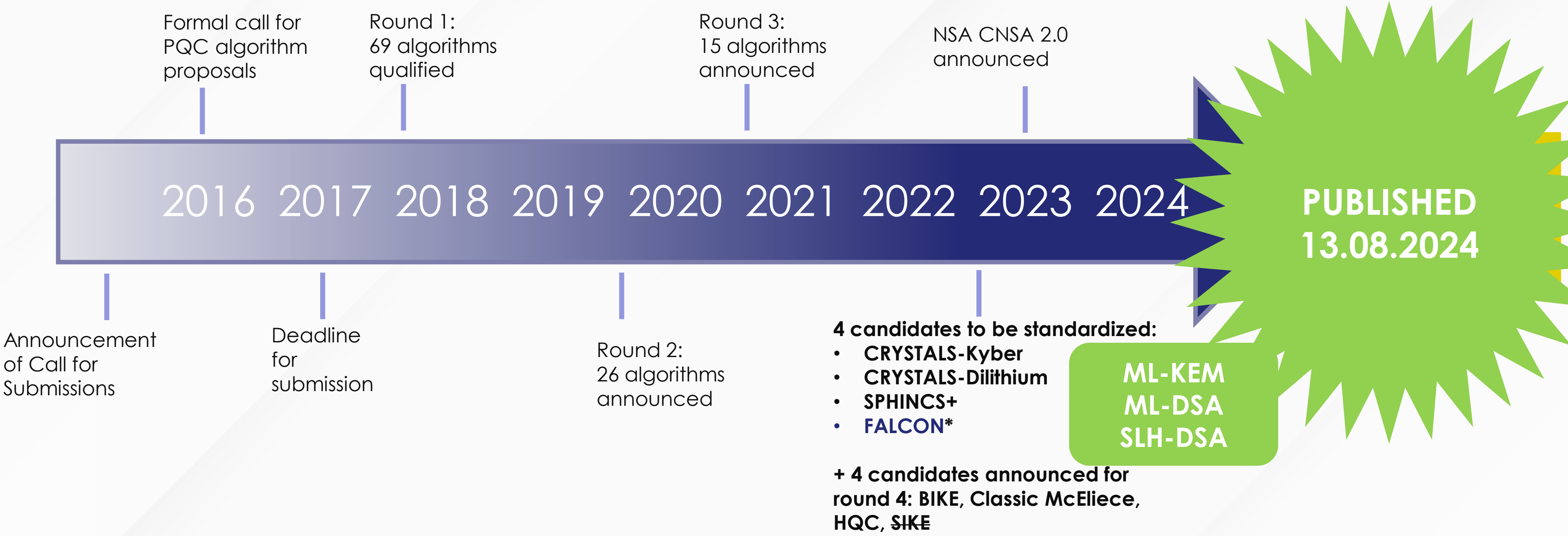
Obtain private key

Ciphertext

Decrypt using extracted key

Plaintext

The NIST Standardization Process



2016 2017 2018 2019 2020 2021 2022 2023 2024

Announcement of Call for Submissions

Formal call for PQC algorithm proposals

Deadline for submission

Round 1: 69 algorithms qualified

Round 2: 26 algorithms announced

Round 3: 15 algorithms announced

4 candidates to be standardized:

- **CRYSTALS-Kyber**
- **CRYSTALS-Dilithium**
- **SPHINCS+**
- **FALCON***

ML-KEM
ML-DSA
SLH-DSA

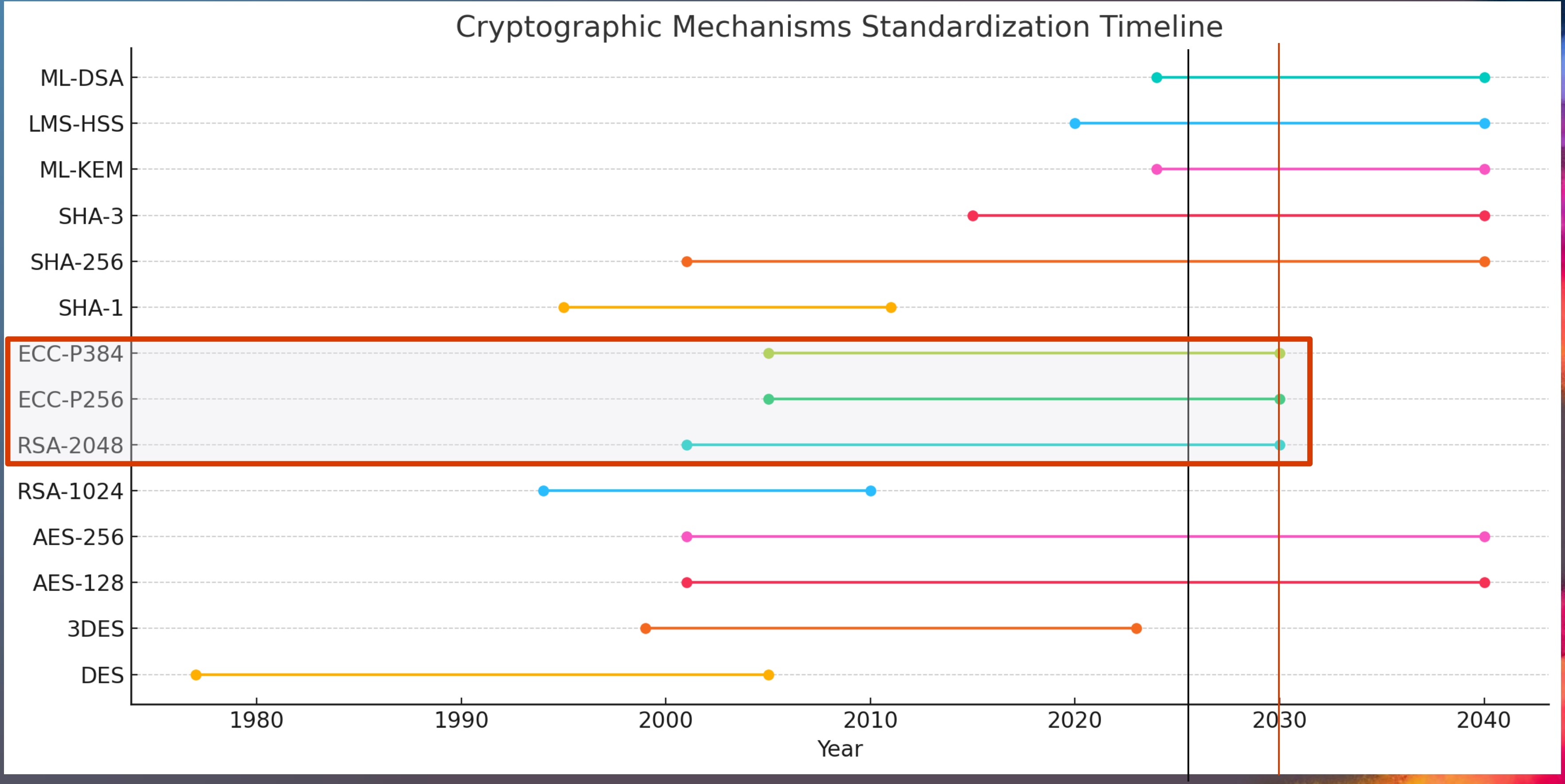
+ 4 candidates announced for round 4: BIKE, Classic McEliece, HQC, ~~SIKE~~

NSA CNSA 2.0 announced

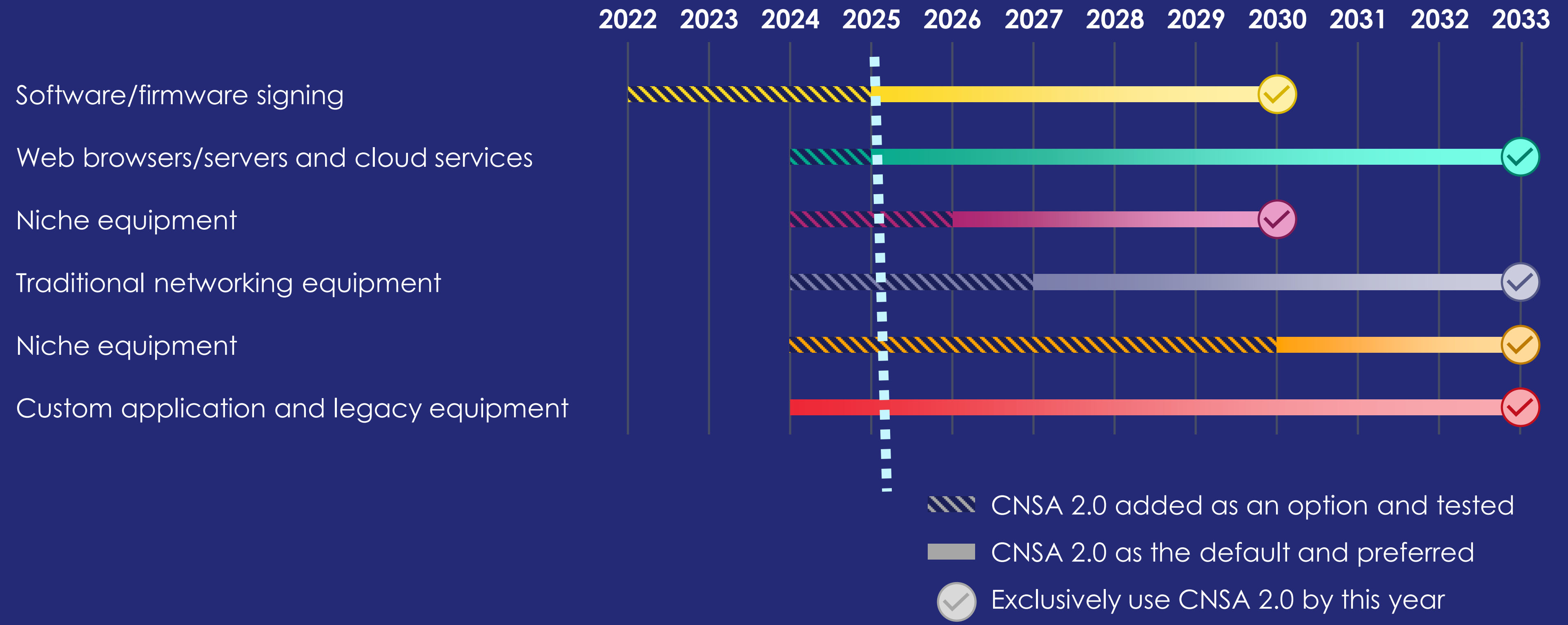
PUBLISHED 13.08.2024

*FALCON was sponsored and co-developed by Thales along with academic and industrial partners from France (University of Rennes 1, PQShield SAS), Switzerland (IBM), Canada (NCC Group), and the US (Brown U, Qualcomm).

Crypto agility



Understanding implementation timelines by industry type



Software/firmware signing

Web browsers/servers and cloud services

Niche equipment

Traditional networking equipment

Niche equipment

Custom application and legacy equipment

▨ CNSA 2.0 added as an option and tested

▬ CNSA 2.0 as the default and preferred

✓ Exclusively use CNSA 2.0 by this year

2024 – PQC Implementation Becomes Reality

NIST

PKI Consortium

CAB CA/BROWSER FORUM

I E T F

Accredited Standards Committee X9 Inc. Financial Industry Standards

ANSI

ETSI World Class Standards

cloud security alliance® CSA

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Hybrid of classical cryptography and PQC

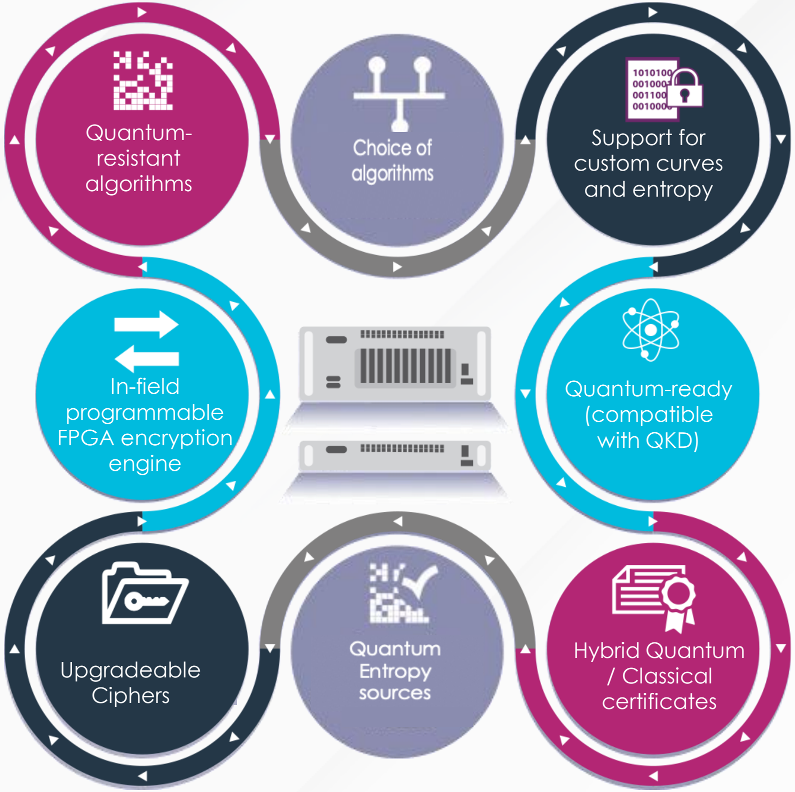
Crypto agile solutions

In 2024, NIST published the first PQC Standards – with other global standard bodies set to quickly adopt those as their own. Each of these bodies recommend beginning implementation immediately using solutions that are hybrid to start and crypto agile.

Best defence is Crypto Agility

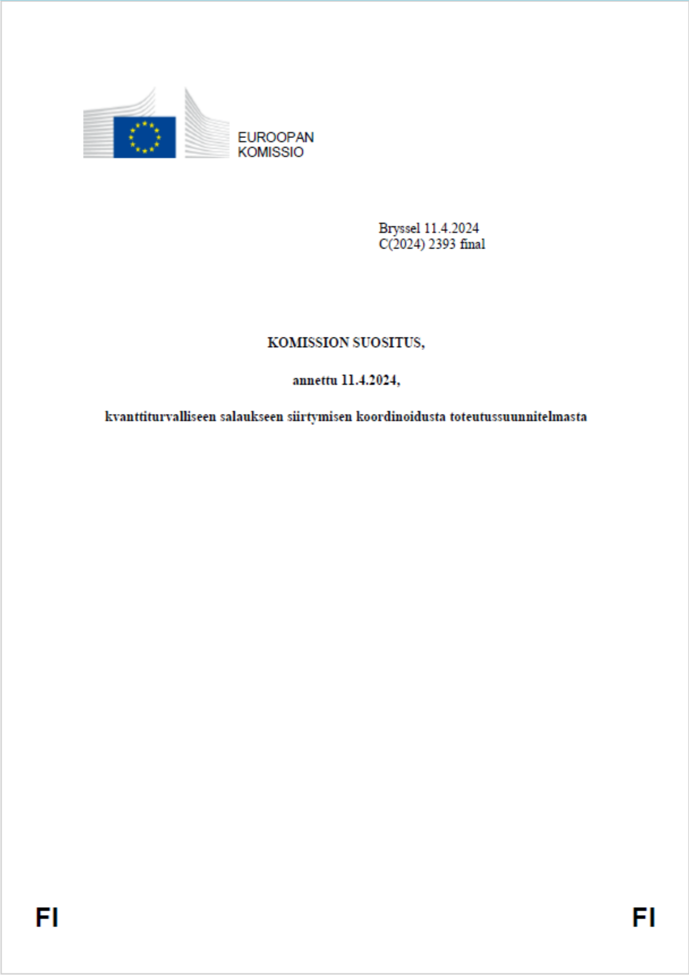
Crypto agility means:

- The ability to quickly modify underlying crypto primitives
- Flexible upgradeable technology
- No built-in obsolescence


Quantum-resistant algorithms
Choice of algorithms
Support for custom curves and entropy
In-field programmable FPGA encryption engine
Quantum-ready (compatible with QKD)
Upgradeable Ciphers
Quantum Entropy sources
Hybrid Quantum / Classical certificates

Recommendation on a Coordinated Implementation Roadmap - 11.4.2024

- Public administration and critical infrastructure
- ”as soon as possible”
- via hybrid schemes
- Coordinated



EUROOPAN
KOMISSIO

Bryssel 11.4.2024
C(2024) 2393 final

KOMISSION SUOSITUS,

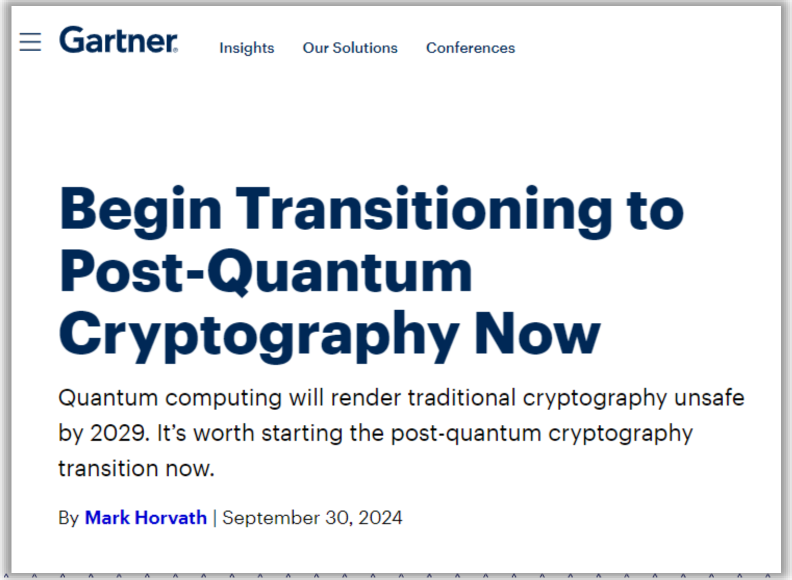
annettu 11.4.2024,

kvanttiturvalliseen salaukseen siirtymisen koordinoidusta toteutussuunnitelmasta

FI FI

Breaking news! (in Sept. 2024)

Gartner brings forward Q-DAY

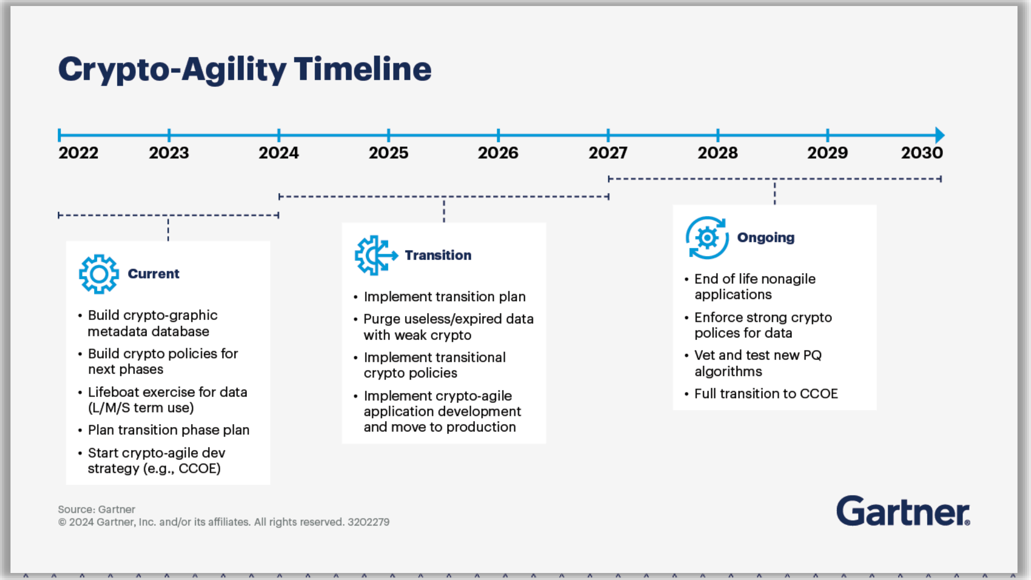


Begin Transitioning to Post-Quantum Cryptography Now

Quantum computing will render traditional cryptography unsafe by 2029. It's worth starting the post-quantum cryptography transition now.

By Mark Horvath | September 30, 2024

Start transition to PQC now



Crypto-Agility Timeline

Current

- Build crypto-graphic metadata database
- Build crypto policies for next phases
- Lifeboat exercise for data (L/M/S term use)
- Plan transition phase plan
- Start crypto-agile dev strategy (e.g., CCOE)

Transition

- Implement transition plan
- Purge useless/expired data with weak crypto
- Implement transitional crypto policies
- Implement crypto-agile application development and move to production

Ongoing

- End of life nonagile applications
- Enforce strong crypto polices for data
- Vet and test new PQ algorithms
- Full transition to CCOE

Source: Gartner
© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. 3202279

Preparation to the transition/ Thales products

PRACTICE

Crypto Agility & Crypto Discovery

Thales High Speed Encryptors (HSE)

APPLY

Quantum Key Generation

Thales Luna Hardware Security Modules (HSM)

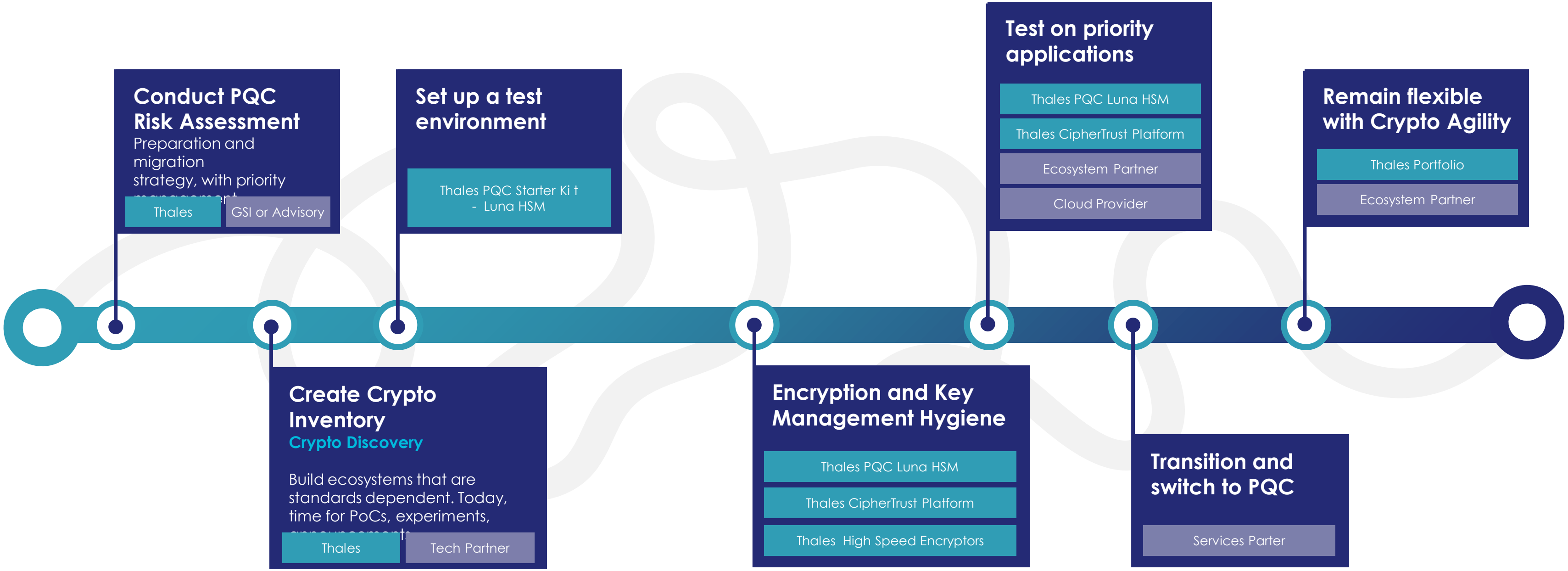
IMPLEMENT

Quantum Resistant Algorithms

LEVERAGE

Quantum Key Distribution

PQC: Simplifying a complex journey



Conduct PQC Risk Assessment
Preparation and migration strategy, with priority management
Thales | GSI or Advisory

Create Crypto Inventory
Crypto Discovery
Build ecosystems that are standards dependent. Today, time for PoCs, experiments, announcements
Thales | Tech Partner

Set up a test environment
Thales PQC Starter Ki t - Luna HSM

Encryption and Key Management Hygiene
Thales PQC Luna HSM
Thales CipherTrust Platform
Thales High Speed Encryptors

Test on priority applications
Thales PQC Luna HSM
Thales CipherTrust Platform
Ecosystem Partner
Cloud Provider

Transition and switch to PQC
Services Parter

Remain flexible with Crypto Agility
Thales Portfolio
Ecosystem Partner

Go Hybrid
Classic & Quantum crypto
Support classic and Qsafe Algorithm modes

Build ecosystem
Changing algorithms, protocols, key can be costly, complex, time-consuming & needs multiple players

Evolve with the standards
NIST-certified Random Number Generators
As Standards are approved, implement and re-certify

Thales has solutions and partnerships in place today to support your quantum safe journey

THALES

Thank you!