2024

Post Quantum Cryptography, hardened secure solution for the next 20 years

winbond
We Deliver

A Global Supplier of
Advanced Memory Solutions

Topics

- Quantum computing – an overview
- CNSA 2.0 and market trends
- Merits of implementing PQC in nonvolatile memories

Quantum computer

- IBM, Google developing early examples
- Startups showing promise
- Still in early stages

- Solves some problem uniquely
  - Chemistry, material simulation
  - Blockchain
  - Breaking cryptography

The 2030 challenge: Post Quantum Cryptography

PQC: Post-Quantum Cryptography

- Cryptography after Quantum computing become available

Decryption performance, *more or less*

1x

1000x

(today 50 qubit)

23,652,000,000,000x

(~2030 1M qubit)

473,040,000,000,000,000x

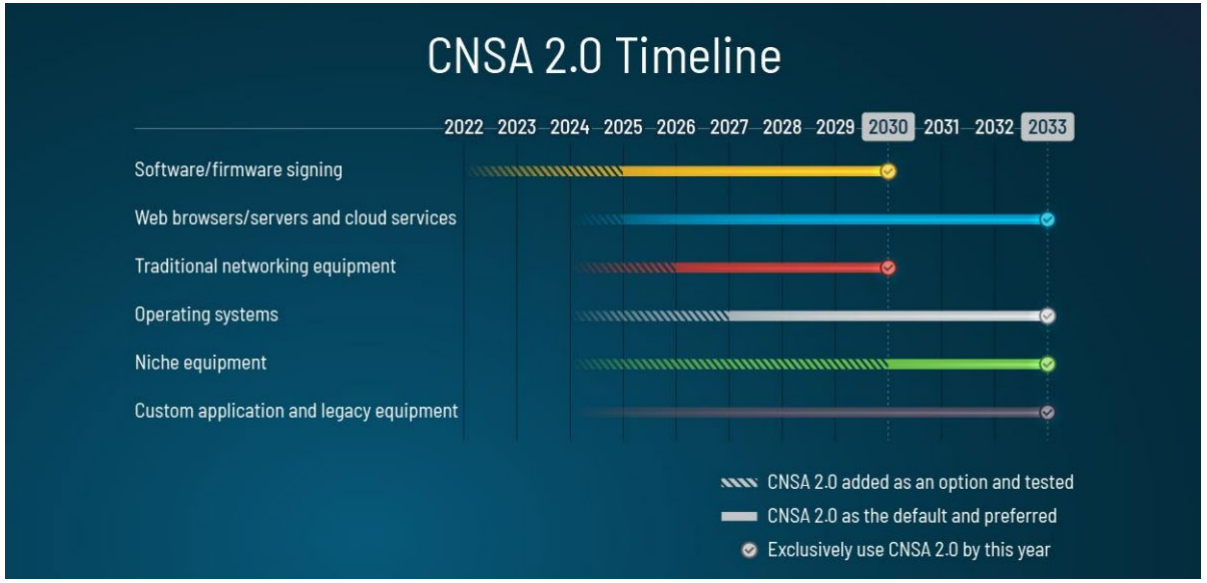
Current security can be made vulnerable by 2030; RSA, ECC

Why do high-security systems need to be prepared?

- Adversaries are harvesting encrypted data now, for processing later with quantum computer
- Products launched today may remain in service by 2030

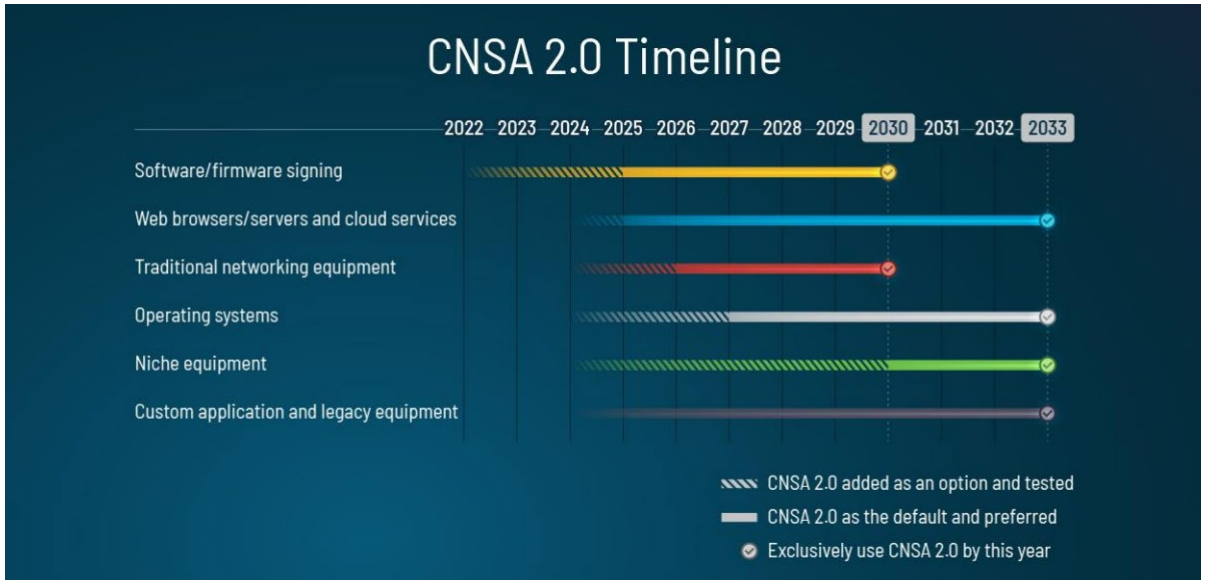
Why Post-Quantum Cryptography become important?

- 2030 is the year when traditional cryptography may become inefficient
- For instance, platforms with more than 7y life cycles introduced in 2024 will become vulnerable after 2030
- US NSA and UK NCSC selected PQC algorithms for digitally signing firmware and software updates
- Software and firmware OTA signing: **begin transitioning immediately**, support and prefer CNSA 2.0 **by 2025**, and exclusively use CNSA 2.0 **by 2030**.



CNSA 2.0 compliant systems markets

- US Gov't agency 'National Security System'
- Infrastructure installations – may follow
- Financial markets – may follow



Security implementation on NVM vs host or Secure Element

- Secure Element can be BOM cost adder
- Software solutions: performance and certification / approval processes
- Secure NVM may leave no footprint change - no PCB change
- Certification can be lengthy and expensive
  - For pre-certified secure NVM, vendors can apply for composite certification – incremental certs
  - Revision of SE code may trigger recerts
  - For host-based system, product update to new processor triggers recerts

Challenges in promoting security

- How much does it cost?
  - Depends, from ‘checkbox’ solution to full implementation
- What is the value?
  - How do you value insurance?
- Will market pay for it?
  - No; until they need it
- Am I forced to adopt?
  - When enough incidents take place