Post-Quantum

Cryptography Conference

ASEAN's Post-Quantum Future: Securing Communications in an Era of Disruptive Change

Jonathan Jackson

Senior Director, Strategic Solutions at BlackBerry Malaysia

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

BlackBerry Secure Communications

PKI Consortium

The path to Quantum Resistant Secure Comms

Post-Quantum Cryptography Conference

October 28-30, Kuala Lumpur, Malaysia

Jonathan Jackson

Senior Director, PQC Solutions, BlackBerry Malaysia

Why Act Now on Quantum-Safe Security?

What's the fuss all about?

- Today's encryption (RSA/ECC/DH) is **not future proof** for the long term
- Though large-scale quantum computers capable of executing these algorithms are still in development, **the risk is not theoretical**. Experts predict that such machines could be viable in the next **5-10 years** (by the 2030s).
- Adversaries are intercepting and storing encrypted data (which cannot be read today) in hopes of decrypting it in the future — the so-called **"harvest now, decrypt later" HNDL** strategy.
- This especially threatens information that needs long-term confidentiality: **national security intel, personal healthcare records, intellectual property,** etc.

PQC Timeline Requirements

"Every organization managing information technology (IT) systems must migrate cyber security components to become quantum-safe" - Canadian Centre for Cyber Security

Canadian Centre for Cyber Security

Communications Security Establishment Canada

Milestones and deliverables for federal departments and agencies are as follows:

- April 2026: Develop an initial departmental PQC migration plan
- Beginning April 2026 and annually after: Report on PQC migration progress
- End of 2031: Completion of PQC migration of high priority systems
- End of 2035: Completion of PQC migration of remaining systems

NIST

Transition to Post-Quantum Cryptography Standards - migration phases and deadlines:

- **Now to 2030**: Begin phasing out quantum-vulnerable encryption like RSA and ECC, and start piloting post-quantum cryptography in parallel with existing systems.
- **By 2030**: All 112-bit security algorithms (e.g., RSA-2048, ECC-256, DH) should no longer be used in new systems.
- **By 2035**: Fully complete migration to PQC and have quantum-vulnerable algorithms retired from all production systems, in step with public mandates (such as NSM-10).

European Commission

By 2026: Initial national PQC transition roadmaps have been established by all Member States.
By 2030: The PQC transition for high-risk use cases has been completed.
By 2035: The PQC transition for medium-risk use cases has been completed.

National Cyber Security Centre

The key milestones are:

By 2028

- Define your migration goals
- Carry out a full discovery exercise (assessing your estate to understand which services and infrastructure that depend on cryptography need to be upgraded to PQC)
- Build an initial plan for migration

By 2031

- Carry out your early, highest-priority PQC migration activities
- Refine your plan so that you have a thorough roadmap for completing migration

By 2035

- Complete migration to PQC of all your systems, services and products

How many logical QuBits will be needed to break RSA-2048 encryption?

Between 4096, to around 1000, depending on who you believe.

The path projection to 1600 Logical QuBits – June 2025

IonQ Roadmap for Large-Scale, Fault-Tolerant Quantum Computers

Built on pioneering trapped ion research, IonQ's roadmap is enabled by the nearly 1,000 patented hardware and software breakthroughs that were developed at IonQ integrated from strategic acquisitions.

Original IonQ #AQ Roadmap

2024	2025	2026	2027	2028
36 Algorithmic Qubits	**64** Algorithmic Qubits	**256** Algorithmic Qubits	**384** Algorithmic Qubits	**1,024** Algorithmic Qubits

Updated Technology Development Roadmap

2024	2025	2026	2027	2028	2029	2030
					Commercial Quantum Computers	Commercial Quantum Computers
36+ Physical Qubits	**64-100+** Physical Qubits	**100-256+** Physical Qubits	**10,000** Physical Qubits	**20,000** Physical Qubits	**200,000** Physical Qubits	**2,000,000** Physical Qubits
99.96% Physical Qubit Fidelity	**99.99%** Physical Qubit Fidelity	**99.99%** Physical Qubit Fidelity	**99.99%** Physical Qubit Fidelity	**99.99%** Physical Qubit Fidelity	**99.99%** Physical Qubit Fidelity	**99.99%** Physical Qubit Fidelity
		12 Logical Qubits	**800** Logical Qubits	**1,600** Logical Qubits	**8,000** Logical Qubits	**80,000** Logical Qubits
		<1.00E-7 Logical Error Rate	**<1.00E-7** Logical Error Rate	**<1.00E-7** Logical Error Rate	**<1.00^-12** Logical Error Rate	**<1.00^-12** Logical Error Rate
All-to-All Connectivity	All-to-All Connectivity	All-to-All Connectivity	All-to-All Connectivity	All-to-All Connectivity	All-to-All Connectivity	All-to-All Connectivity
Optical Gate Operations	Microwave Gate Operations	Microwave Gate Operations	Microwave Gate Operations	Microwave Gate Operations	Microwave Gate Operations	Microwave Gate Operations
1D Qubit Array	2D Qubit Array	2D Qubit Array	2D Qubit Array	2D Qubit Array	2D Qubit Array	2D Qubit Array
	Mid-Circuit Measurement	Mid-Circuit Measurement	Mid-Circuit Measurement	Mid-Circuit Measurement	Mid-Circuit Measurement	Mid-Circuit Measurement
	Parallel Operations	Parallel Operations	Parallel Operations	Photonic Interconnect	Photonic Interconnect	Photonic Interconnect
				Parallel Operations	Parallel Operations	Parallel Operations

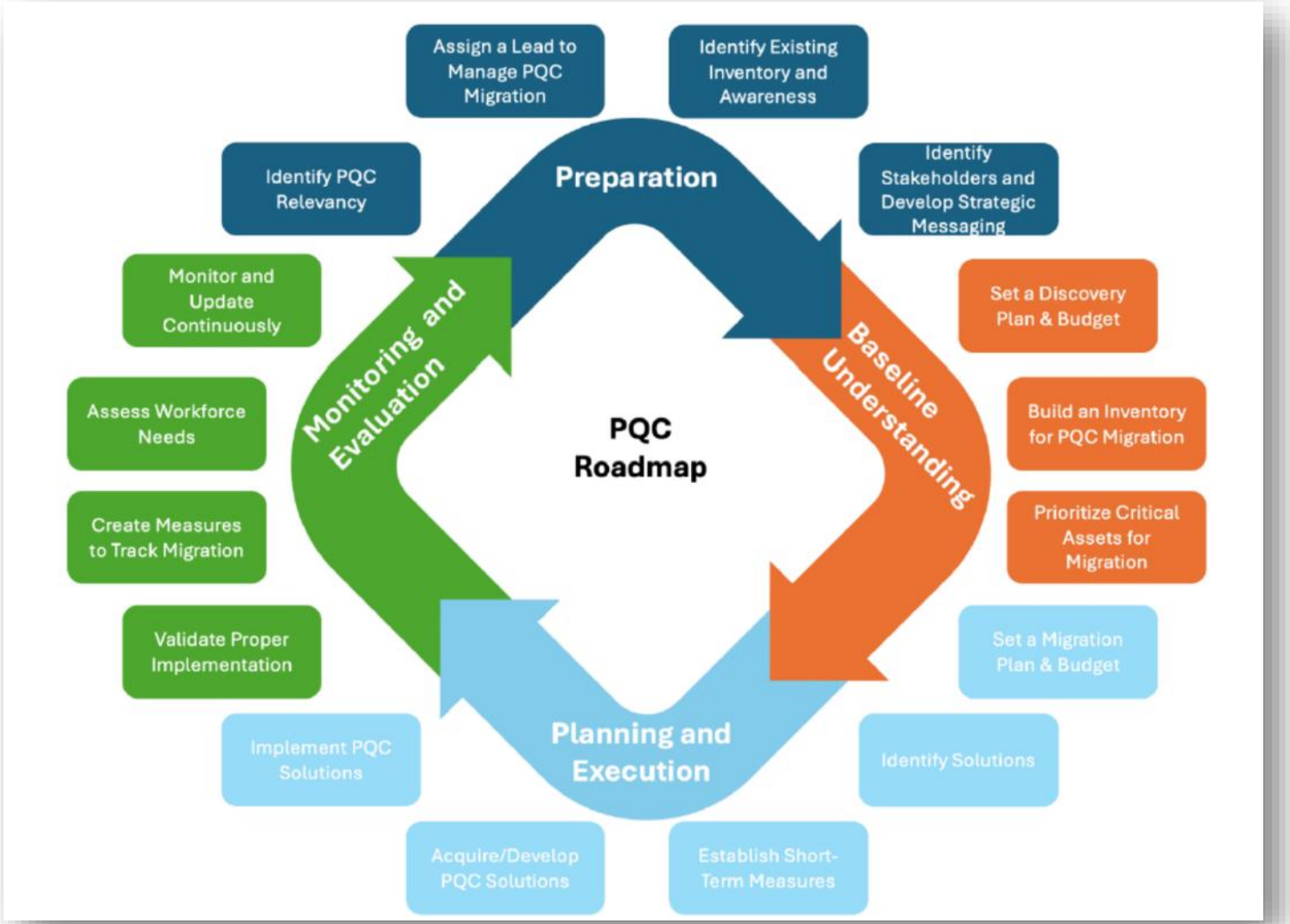
The 80/20 Rule

The path to PQC is 80% about **Process and People**, and only 20% about **Technology**

PQC Migration Planning - 5 Domains

Risk Assessments	Identify and prioritise your key assets
Governance	Establish a coordinated and sustainable plan across the organisation
Technology	Guide the implementation steps and considerations to execute migration
Training & Capability	Develop the knowledge and competencies needed for migration
External Engagements	Work with vendors and ecosystem partners to drive migration

PQC Roadmap - Post-Quantum Cryptography Coalition (PQCC)



Crypto Agility

What does it actually mean? (or Hybrid Crypto)

BlackBerry Secure Communications Focus Areas 2025/26

Protect Conversations & Identities

- Prevent Eavesdropping Attacks & Conceal Patterns of Life
- Secure Mobile Device Use
- Verify Identities Cryptographically

Why it Matters:

Surveillance and cyber threats are evolving, and securing every layer is critical.

User Experience

- Needs to be lightning fast
- Should show PQC Compliance
- Requires Collaboration Globally

Why it Matters:

In a PQC world, the end user experience should not be impacted. Security and cryptographic controls need to be seamless and invisible

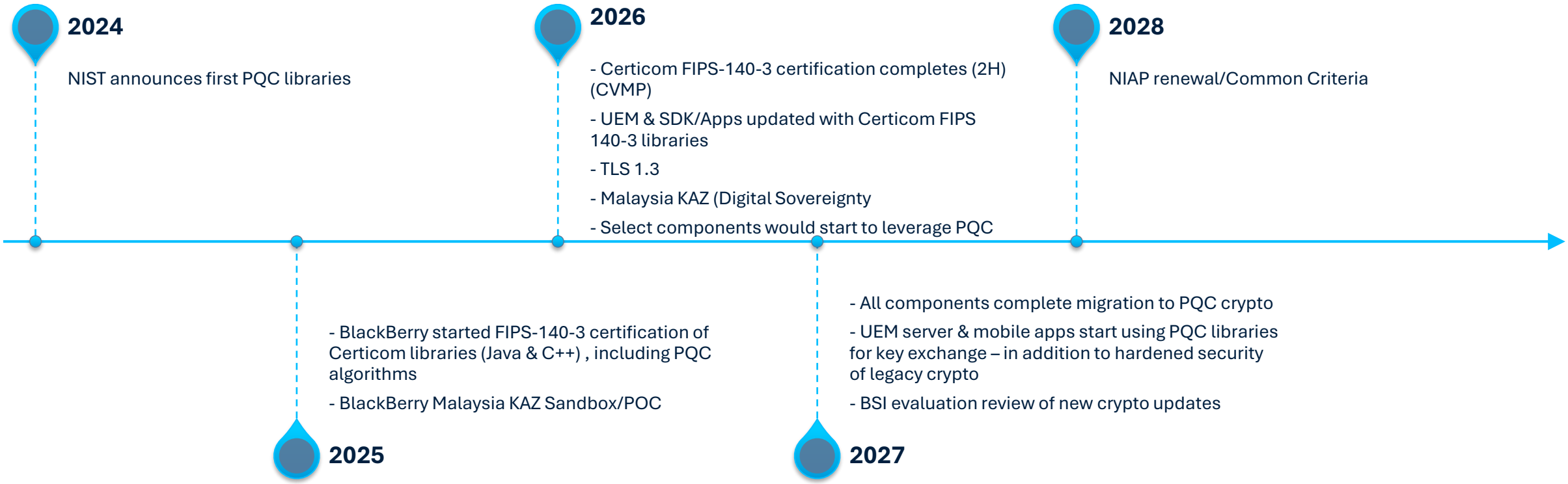
Sovereign Control & Compliance

- Sovereign On-Prem Control in Malaysia
- Centralized Management
- Government-Validated Certifications

Why it Matters:

If you don’t control your infrastructure, you don’t control your security.

BlackBerry Roadmap to PQC



PCQ Planning – some useful references

Be informed – Educate!! ☺

- Quantum-Safe Migration Handbook – CSA Singapore 2025
- PQC Migration Roadmap, PQCC (2025)
- SP 1800-38B (Prelim.) - Migration to PQC: Cryptographic Discovery, NIST NCCoE (2023)
- TR 103 619 v1.1.1 - Migration Strategies & Recommendations to Quantum-Safe Cryptography, ETSI (2020)
- Preparing for a Post-Quantum World by Managing Cryptographic Risk, FS-ISAC (2023)
- The PQC Migration Handbook (2nd ed.), TNO/CWI/AIVD (2024)
- IBM Quantum Safe

PKI Consortium

https://www.linkedin.com/in/jonathanjackson1

Thank you

https://www.blackberry.com/us/en/contact-us

BlackBerry | Secure Communications