



Post-Quantum Cybersecurity

Autumn - 2025



Tomorrow's Cyber Security, Today

IRONCAP

Quantum Threat

What is the Quantum Threat (Q-Day)?

- Quantum computers will crack current encryption methods
- Everything is vulnerable: email, financials, crypto, AI, etc.
- Everything needs to be protected - \$trillion market size

What separate 01 Quantum with its competitors?

- 4 US patents (2 granted + 2 pending)
- IronCAP cryptographies are endorsed by NIST
- 3 years of end-user SaaS product lead (commercially available)

Why Today?

- Quantum-driven cybersecurity threat urgently need solutions today
- Harvest-Now-Decrypt-Later attack = Q-Day is today's problem



Q-Day Attention **Heated UP!**



IBM 2025-2029 Deliveries

Loon (2025) → Kookaburra (2026) → Full fault-tolerant (2029)

Quantinuum (Honeywell)

New version within 2025 will be 1 billion times faster

Microsoft

“Majorana 1” topological core in Feb 2025

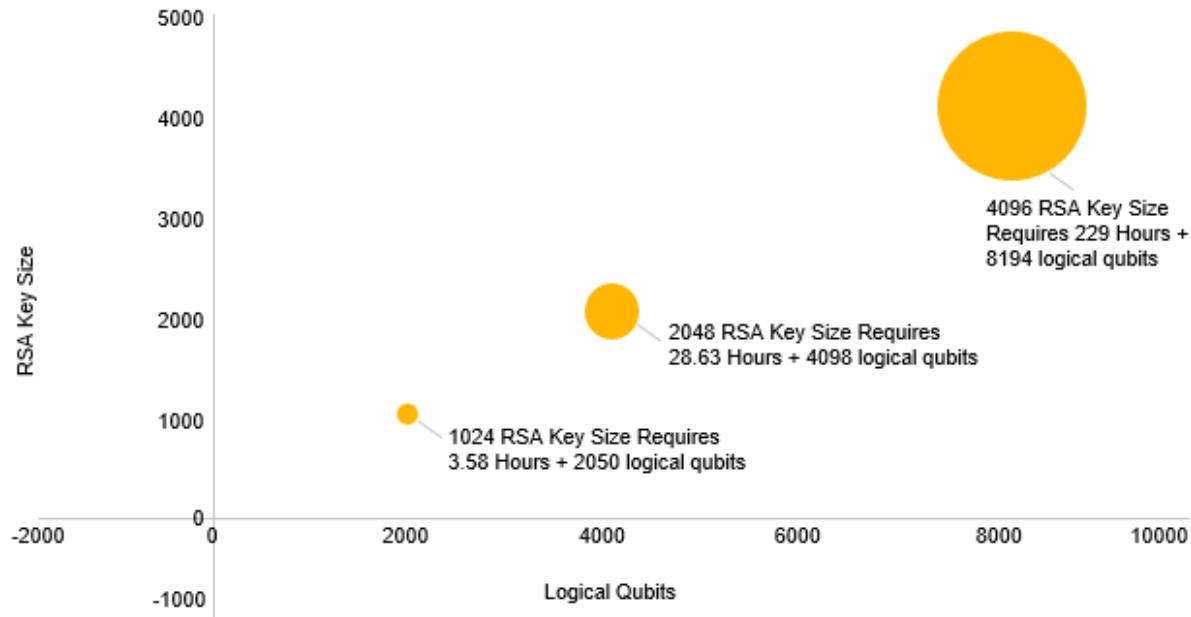
Google

Willow achieved a major breakthrough in Dec 2024



Q-Day has Arrived!

Figure 2 – RSA Key Size vs Qubits requirement in breaking



Source: Quantum Computing: Progress & Prospects (2019) Emily Grumbling and Mark Horowitz



Q-Day is today's problem

Executive Office of the US President

- Reminded agencies to be mindful that encrypted data can be recorded now and decrypted at a later date by operators of a future Quantum Computer.

US Secretary of Commerce (Howard Lutnick)

- The worldwide cybersecurity will be totally broken by quantum computers if we don't act immediately.

Canadian Government

- The Carney government has named quantum technologies as a priority topic in the G7 meeting.

Starmer and Trump to sign Quantum Computing Pact

- Designed to counter China's aggressive attempts



THE DIRECTOR

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young 
Director

SUBJECT: Migrating to Post-Quantum Cryptography

This memorandum provides direction for agencies to comply with National Security Memorandum 10 (NSM-10), on *Promoting United States Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems* (May 4, 2022).¹

I. OVERVIEW

Federal agencies² (“agencies”) are moving to a zero trust architecture, as directed by Executive Order 14028, *Improving the Nation’s Cybersecurity* (May 12, 2021)³ and Office of Management and Budget (OMB) Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022).⁴ This paradigm shift relies in part on the ubiquitous use of strong encryption throughout agencies.

As outlined in NSM-10, the threat posed by the prospect of a cryptanalytically relevant quantum computer (CRQC)⁵ requires that agencies prepare now to implement post-quantum cryptography (PQC). Once operational, a CRQC is expected to be able to compromise certain widely used cryptographic algorithms used to secure Federal data and information systems.

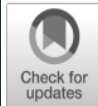
¹ Available at: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>

² The term “agency” has the meaning given in 44 U.S.C. § 3502.

³ Available at: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

⁴ Available at: <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>

⁵ Defined as quantum computers that are capable of actually attacking real world cryptographic systems that would be infeasible to attack with a classical computer.



Q-Day Preparation - NIST

NIST 4th Round PQC – March 2025

☐ HQC selected

* Already offered by IronCAP engine since 2022 (expected to be part of ISO)

** To be included into next version of IronCAP

Algorithm	Algorithm Class
Classic McEliece*	Code-based
HQC (selected)**	Code-based
BIKE (out)	Code-based



Source: <https://csrc.nist.gov/News/2023/three-draft-fips-for-post-quantum-cryptography>

1 FIPS 203 (Draft)

2 Federal Information Processing Standards Publication

3

4 Module-Lattice-based 5 Key Encapsulation 6 Standard

7 FIPS 204 (Draft)

8 Federal Information Processing Standards Publication

9 Module-Lattice-Based Digital 10 Signature Standard

Category: Computer Security

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.FIPS.204.pdf>
Published August 24, 2023



U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce

14

15 U.S. Department of Commerce

16 Gina M. Raimondo, Secretary

17 National Institute of Standards and Technology

18 Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

FIPS 205 (Draft)

Federal Information Processing Standards Publication

Stateless Hash-Based Digital Signature Standard

Category: Computer Security

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.FIPS.205.pdf>
Published: August 24, 2023



U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

category: Cryptography

IronCAP Patents

Patent Portfolio

US#11,271,715: cryptographic system incorporating advanced post-quantum cryptographic technology

US#11,669,833:
Quantum-Safe blockchain endpoints and crypto Wallets

Patent-pending

- Secure AI platform
- Quantum-Safe blockchain



Global Partnerships



THALES
Building a future we can all trust

KEYFACTOR

pwc

CGI

@Hitachi Solutions Create

ISA mirata Ltd

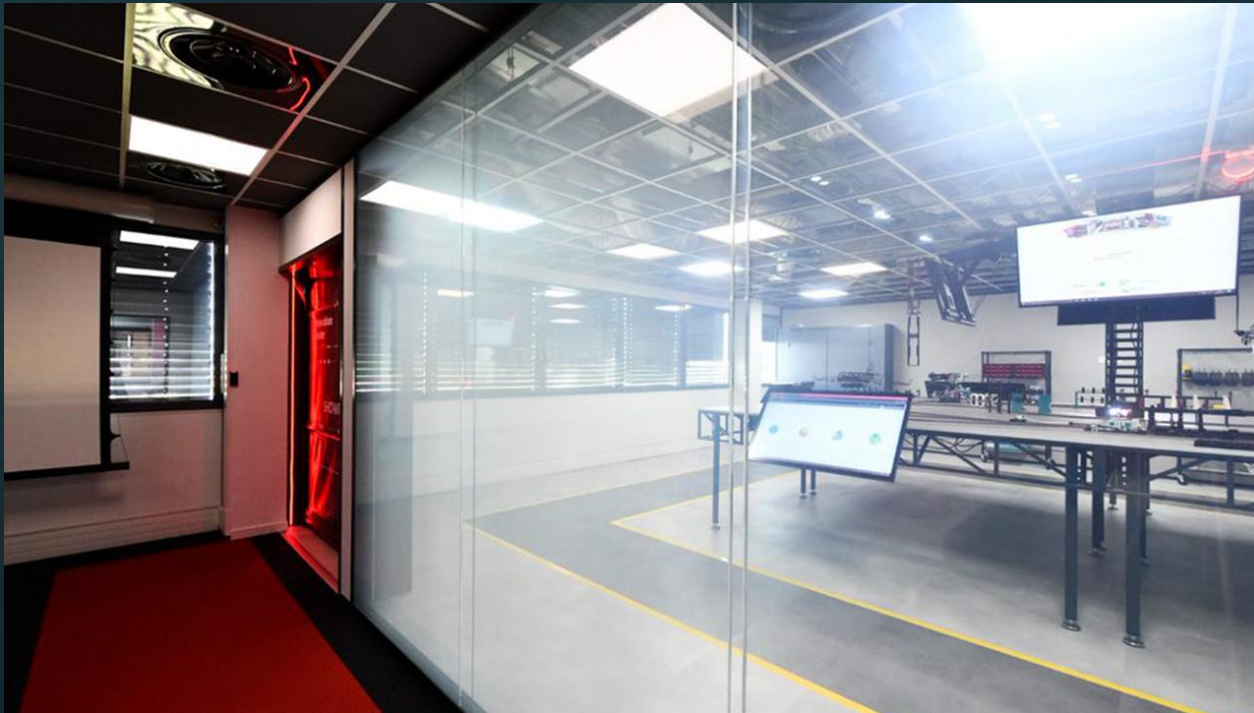
REAL MATTER



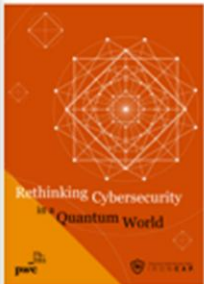
CGI - Innovation Center

IronCAP Demo

<https://ironcap.ca/demo/cgi/>



PwC - Thought Leadership Papers



Rethinking Cybersecurity
in a Quantum World

<https://www.pwccn.com/en/issues/cybersecurity-and-privacy/rethinking-cybersecurity-in-a-quantum-world-jul2021.html>



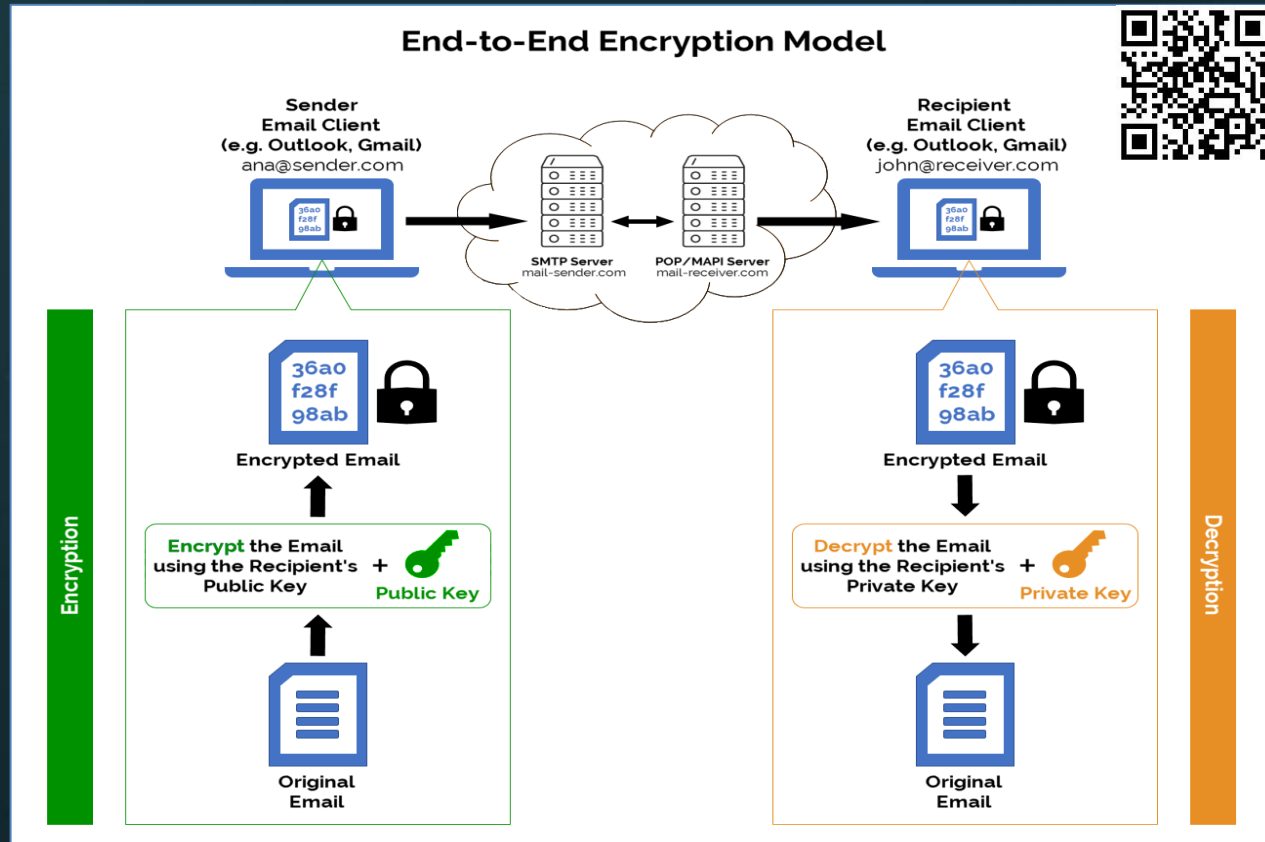
Email Phishing Culprit
behind Ransomware

<https://www.pwccn.com/en/issues/cybersecurity-and-privacy/email-phishing-culprit-behind-ransomware-apr2022.html>

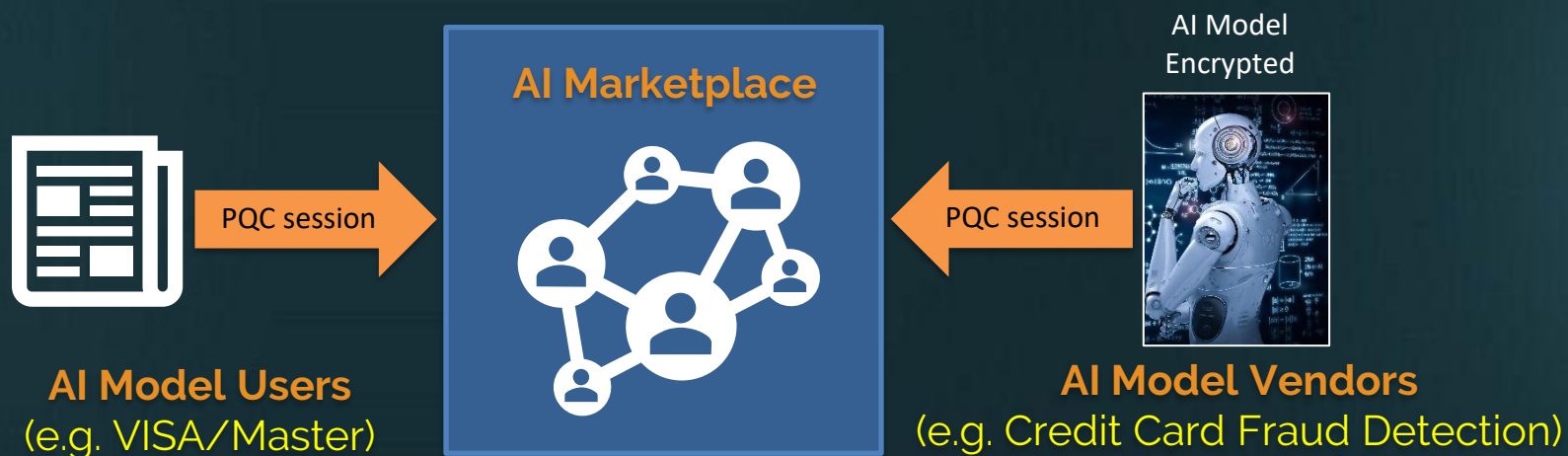


Use Case #1 – Email Security

<https://ironcap.ca/ironcap-x/>

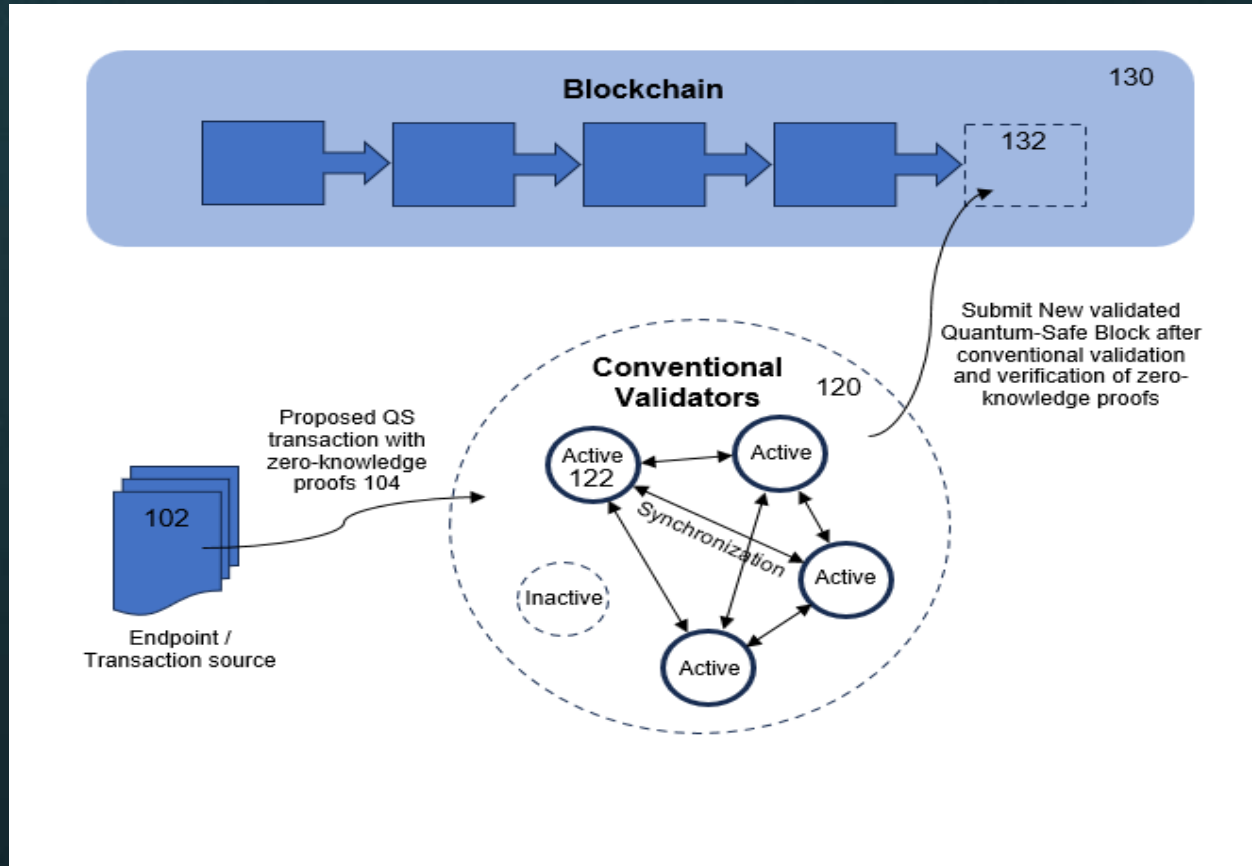


Use Case #2: Quantum-Safe AI



- All AI operations are 100% quantum-vulnerable
- The world's first Amazon-like **Quantum-Safe** marketplace for AI models
- Encrypting confidential user input and AI model (**Zero-Trust**)
- Commercially ready by mid-2026

Use Case #3 - Cryptocurrency



Use Case #4 - DAEM

Digital Asset Exchange Machine

We helped a customer in Hong Kong to launch the world's first quantum-safe DAEM at Cyberport in Hong Kong. DAEM

DAEM adopts 2 layers of authentication to ensure end-to-end security between:

1. User's device and DAEM.
2. DAEM and the host application.



Use Case #5 – Multi-Signature

Partnership with Real Matter

Quantum-Safe Multi-Signature

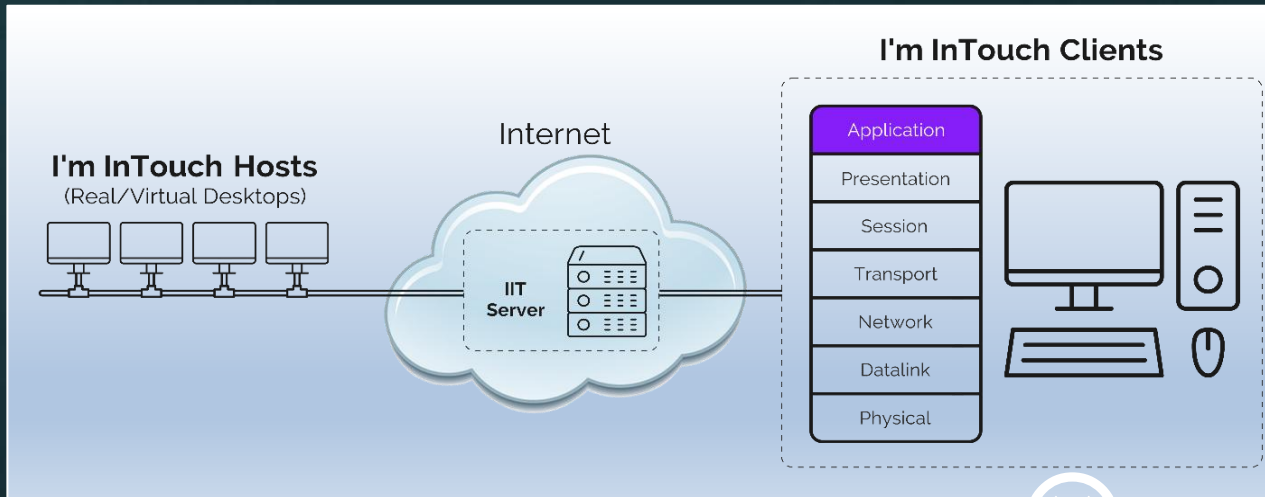
QSMS is an innovative technology built on top of the existing digital signature framework (RSA). It introduces an optional QSMS Blockchain Ledger layer that enhances security with quantum-safe additional signatures while preserving the independence of the existing RSA framework. Both systems can operate separately without interference.

Demo:
<https://quantumsafe-multisig-pin4321.web.app/>



Use Case #6 - Remote Access

Quantum-Safe + Zero Trust



No access to corporate LAN



Use Case #7 – Thales Luna HSM



Use Case #8 – Keyfactor EJBCA

Keyfactor's Customers
(e.g. Banks, Enterprises, etc.)



Issue, Revoke, Renew, Manage
Post-Quantum keys

KEYFACTOR



EJBCA



By combining both NIST-approved PQC algorithms as well as our own patent-protected quantum-safe technologies, 01 Quantum has extensive hands-on experience in Post-Quantum Cybersecurity to help you transform your systems to become quantum-safe.

For more information:

www.01quantuminc.com | www.01com.com
+1 905-795-2888 (tel)
+1 800-668-2185 (toll-free)
Sales@01com.com

Global Partners:



KEYFACTOR

THALES
Building a future we can all trust

 **Hitachi Solutions Create**

REAL MATTER



Take Away:

- Quantum Threat is here
- Everything is vulnerable
- Need to act now
- IronCAP is the Solution