ETSI/IQC Quantum Safe Cryptography Conference 2026

Quantum Computing & The Pursuit of Trust: Threats to Modern Authentication Protocols, Privacy & Institutional Credibility

Presented by:

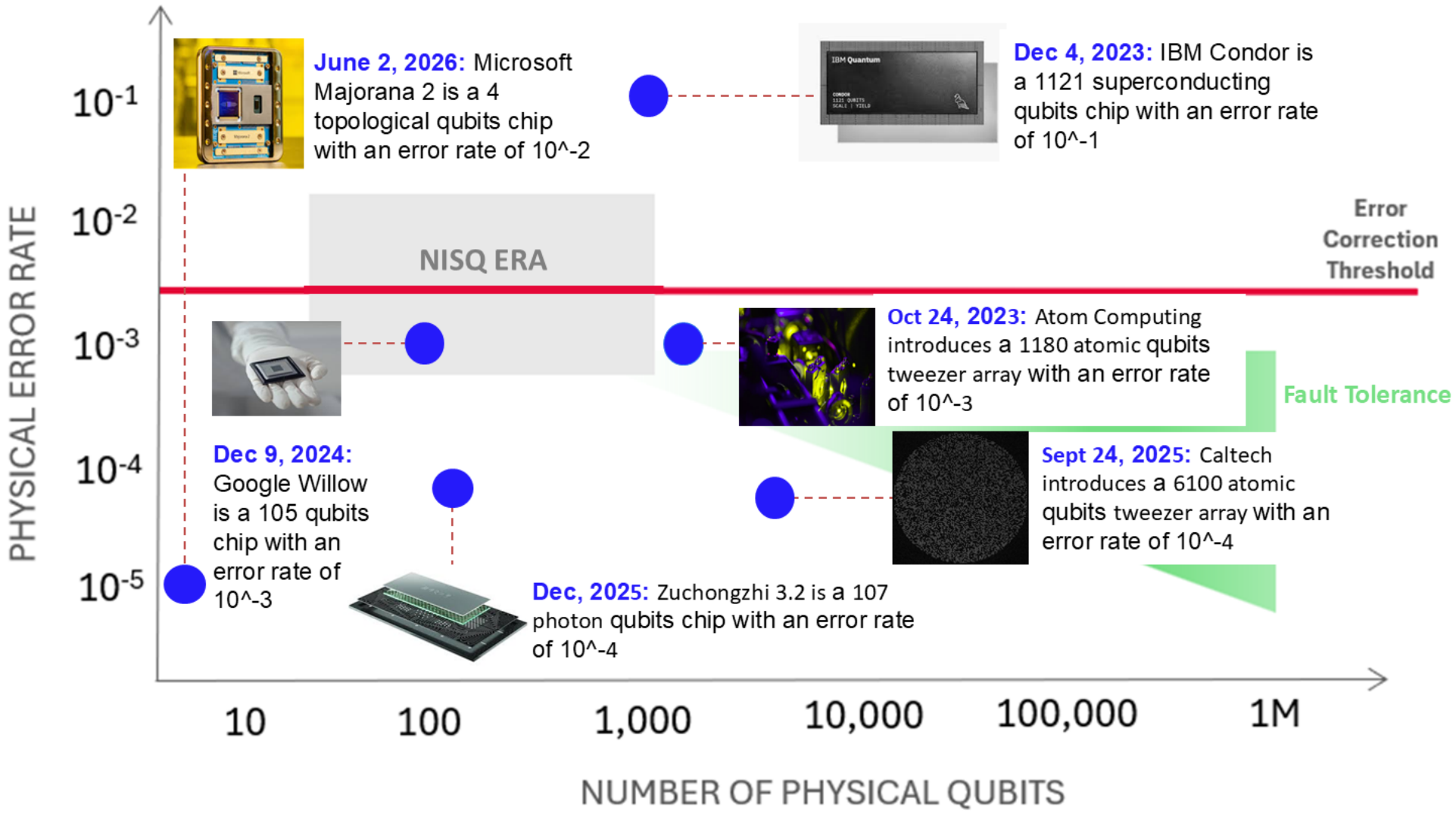
Nour Mousa, PhD Candidate | Toronto Metropolitan University

Nasreen Latheef | Osgoode Hall Law School

06/18/2026

Current State – Quantum and Modern Authentication

CURRENT STATE OF QUANTUM COMPUTING, BEYOND THE NISQ ERA



Key Takeaways

- Physical Qubit counts are rising
- Error rates continue to decline
- Multiple architectures show progress
- Fault tolerance remains the key milestone

Note: This graph is not exhaustive and intends to capture some key milestones in the advancement of quantum computing. Error correction rates have been self-reported and not all claims have provided evidence.

Current State Modern Authentication

NIST Authentication Assurance Levels (AALs) serve as a trusted industry benchmark for evaluating the strength and reliability of modern authentication mechanisms.

Zero Trust "Never Trust, Always Verify"

Verify Explicitly + Use Least Privilege + Assume Breach = Continuous enforcement of least privilege per-request access decisions in information systems

Legacy components make implementation, creates dependencies

Assured by

Non-Phishable MFA

NIST AAL 2 Capable

Phishing-Resistant + Verifier Attestation + Cryptographically-binded = Assurance of phishing-resistance for secondary factor of authentication, prevents replay attacks and credential theft.

Achieved with

Challenges removing passwords

Passwordless Authentication

NIST AAL 2, 3 Capable

fido CERTIFIED FIDO2 (WebAuthn + CTAP) = FIDO2/WebAuthn Standards for phishing-resistant authentication.

Implemented as

Lack of regulatory-driven mandates

Device-Bound Passkeys

NIST AAL 3 Capable (Highest Assurance)

Hardware-security based multi factor credential
Eg. FIDO2 Key

Synced-Passkeys

NIST AAL 2 Capable (Moderate Assurance)

Single factor credential stored & synced across user's trusted devices. Eg. Biometric for Password Manager

Note: To achieve NIST AAL 3, you must have hardware-based MFA with verifier attestation.

User Stories: PQC Authentication Analysis

User Profile:

Sarah is a citizen of the EU

User Activity:

Sarah uses her European Digital Identity Wallet to verify her identity when traveling.

Authentication Protocols:

- *OpenID4VP*, OpenID for Verifiable Presentations (ECDSA, EdDSA, RSA)
- *OID4VCI*, OpenID for Verifiable Credential Issuance (ECDSA, RSA)
- *ISO/IEC 18013-5*, mDL Proximity Authentication, (ECDH, ECDSA)

Impact:

- *Trust Now Forge Later:* Digital Cloning of Identity
- *Harvest Now, Decrypt Later:* Sensitive PII data may be compromised
- Fraudulent activities under compromised individual's name
- Account recovery may be difficult

User Profile:

John is a diabetes patient

User Activity:

John is checking his bloodwork results on his phone.

Authentication Protocols:

- *JSON Web Token* (ECDSA, EdDSA, RSA)
- *Blockchain, Smart Contract signatures* (ECDSA, EdDSA)
- SAML (RSA, ECDSA)
- WebAuthn / FIDO2 (RSA, ECDSA)

Impact:

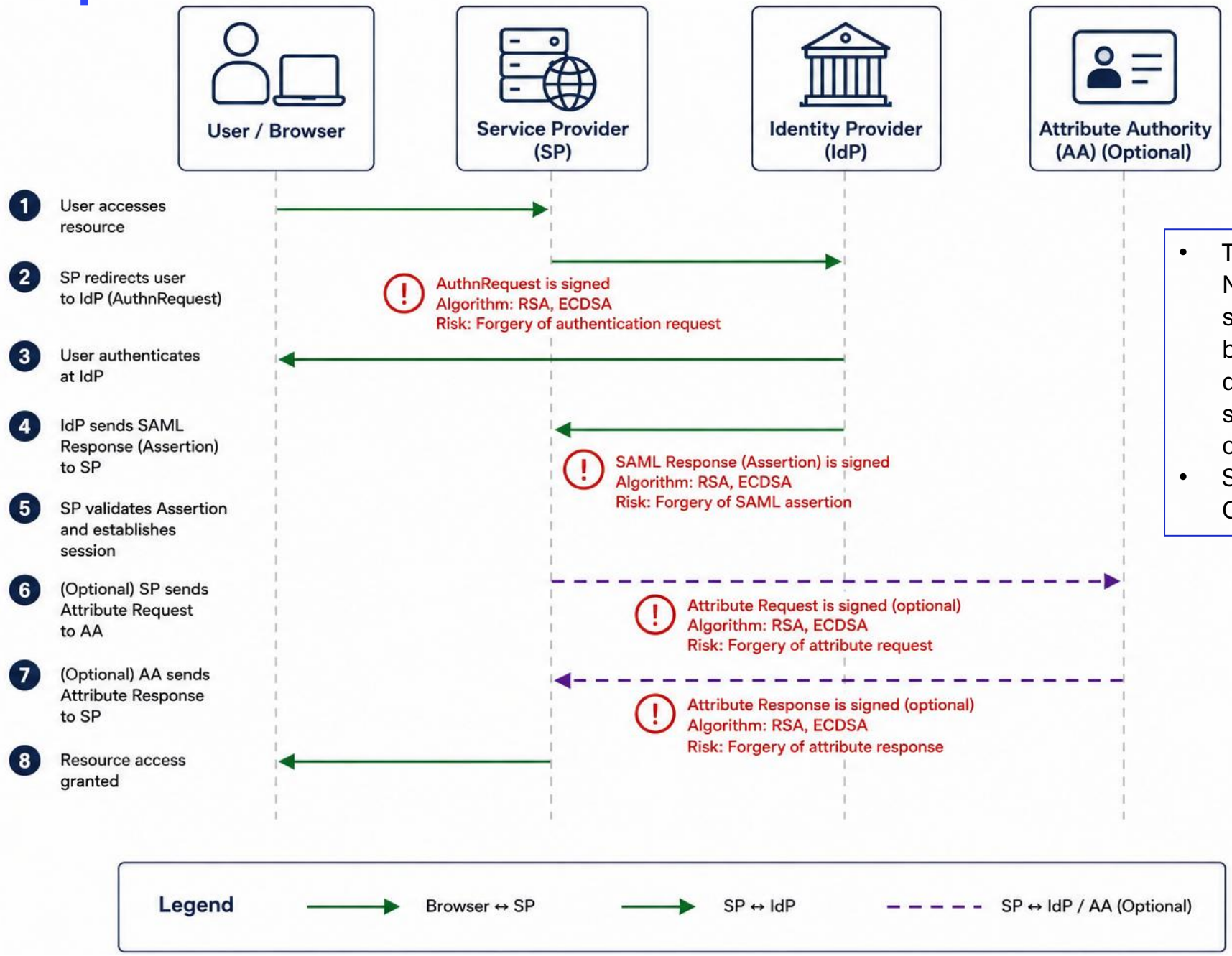
- *Trust Now Forge Later:* Altering of Health Records
- *Harvest Now, Decrypt Later:* Sensitive PII data may be compromised
- Unauthorized dispensing of medical prescriptions
- Account recovery may be difficult

If we can no longer provide authentication assurance through existing mechanisms, how can we uphold digital trust?

Reference: European Digital Identity Wallet Architecture and reference framework", (2021), online: Architecture and reference framework - EUDI Wallet <https://eudi.dev/1.4.0/arf/>.

Authentication – NIST and SAML

SAML Deep Dive



- The Security Assertion Markup Language (SAML) standard defines an XML-based framework for describing and exchanging security information between on-line business partners
- SAML Enables: Single Sign-On, Federated Identities

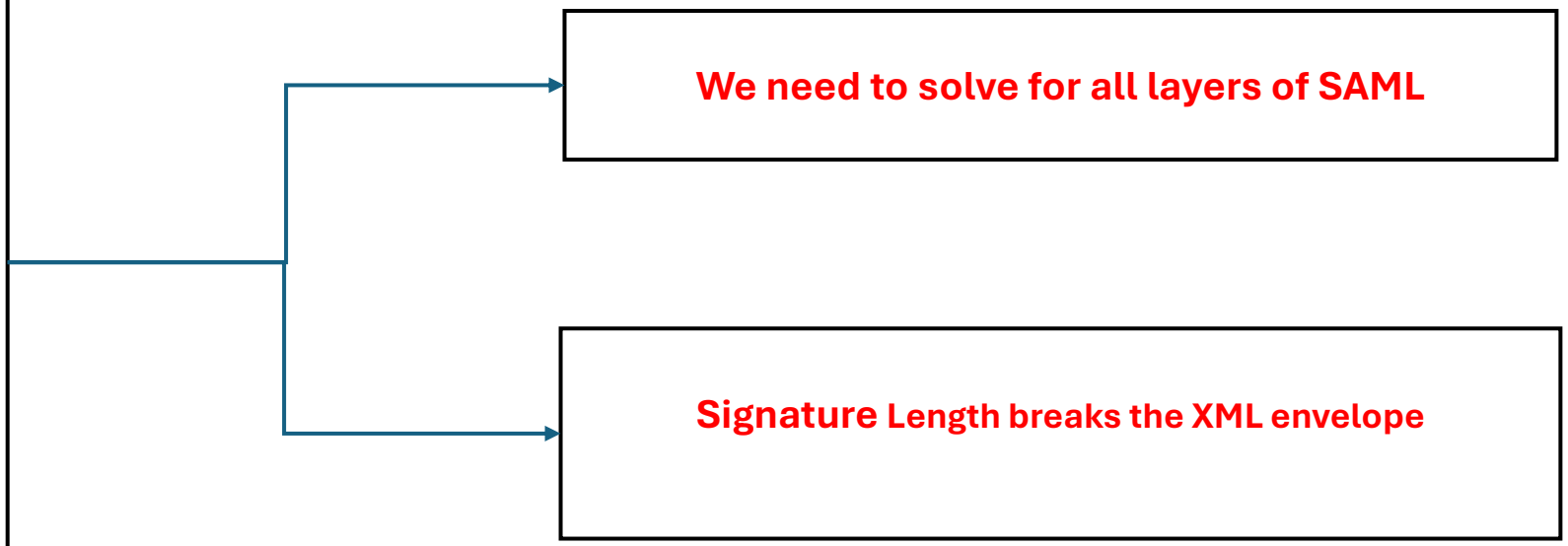
SAML 2.0 and Mapping to NIST Standards

SAML 2.0 is an authentication and federation protocol. It depends on cryptography for security, including:

- Digital signatures on SAML assertions
- TLS/HTTPS connections between parties
- Certificate-based trust relationships

Many deployments currently use:

- RSA signatures
- Elliptic Curve Cryptography (ECC) signatures
- TLS certificates based on RSA or ECC



Cryptographic Integrity and Semiconductor Governance

Canada - Existing Legislature

Semiconductor governance is critical to support manufacturing, supply chains and export regulations.

- Silicon-based qubits are built using processes similar to conventional chips.
- Quantum systems depend on specialized chips, sensors, and cryogenic electronics.

Canada currently does not have a standalone Chips Act. Canada participates in the Wassenaar Arrangement and controls exports of specific cryptographic technology and semiconductor equipment (however, this is very fragmented).

Bills C-2 and C-8 would expand Canada's regulatory authority over critical digital infrastructure and AI systems. However, neither directly addresses semiconductor manufacturing sovereignty or cryptographic hardware certification compared EU Chips Act or the Cyber Resilience Act.

New AI & Quantum Initiatives (June 2026)

Canada, Australia, and India are formalizing a trilateral technology and innovation partnership covering AI, quantum, trade missions, and more

Partnership : Australia's AI Safety Institute, Canada-Japan Joint Economic Committee.

Global Cryptographic Integrity and Standards

							
Cryptographic Standards Body	Australian Signals Directorate (ASD). Australian Cyber Security Centre (ACSC). ISM (Information Security Manual).	Communications Security Establishment (CSE) ITSG-33 (IT Security Risk Management) ITSG-31 (Cryptographic Algorithms).	ENISA. ETSI TC CYBER. CEN/CENELEC JTC 13. ISO/IEC 19790 (cryptographic modules). eIDAS Regulation (trust services).	Federal Office for Information Security (BSI). Technical Guidelines (TR series). Common Criteria certification for crypto hardware.	CERT-In. No standalone crypto standards body. IT Act 2000, s 84A (encryption rules). STQC (testing/certification).	Federal IT Steering Unit / Digital Transformation Office. Aligned with ISO/IEC standards. No standalone crypto regulator.	National Cyber Security Centre (NCSC). CESG (now part of NCSC). Independent standards aligned with but distinct from NIST/EU.
PQC Transition	Five Eyes alignment. Adopting NIST FIPS 203–205 (Kyber, Dilithium, Falcon). ASD guidance published 2024.	Five Eyes alignment. CSE guidance on PQC transition. ITSP.40.111 (draft). Aligned with NIST FIPS 203–205.	Commission Recommendation C(2024) 2393 (April 2024): Coordinated PQC Implementation Roadmap. CEN/CLC JTC 22 WG4 on PQC.	BSI TR-02102 updated for PQC. BSI actively evaluating hybrid PQC & classical schemes. Leading EU PQC standardisation work.	Early stage. No formal PQC transition plan published. Academic research (IITs, C-DAC). CERT-In monitoring.	Aligned with ETSI/ISO standards. Academic research (ETH Zürich, IBM Research Zürich). No national PQC mandate yet.	NCSC PQC guidance published 2024. Recommending migration planning by 2025, hybrid implementations by 2028. Five Eyes aligned.
Trusted Hardware/Chip Certification	Common Criteria recognition. ASD Evaluated Products List. No domestic Trusted Foundry program.	CSE Canadian Centre for Cyber Security: evaluated products. Common Criteria recognition. No Trusted Foundry equivalent.	EU Cybersecurity Certification Framework (CSA). Cyber Resilience Act (2024): mandatory security for digital products. Common Criteria.	BSI certification for crypto hardware. Common Criteria national scheme (one of the strongest globally). BSI TR-03153 (TPM requirements).	STQC Common Criteria scheme. Limited domestic certification capacity. Relies on international mutual recognition.	Common Criteria recognition. No national certification body for crypto hardware. Relies on EU/international schemes.	UK IT Security Evaluation & Certification Scheme (CLEF/NCSC). Common Criteria. Post-Brexit independent scheme.
Encryption Export Controls	Wassenaar Cat 5 Part 2. DSGL (Defence and Strategic Goods List). Permits required for strong encryption exports.	Wassenaar Cat 5 Part 2. Export Control List, Group 1. CSE role in assessment. Exemptions for mass-market encryption.	EU Dual-Use Regulation, Annex I Cat 5 Part 2. Intra-EU transfer exempt. 2025 update adds quantum crypto controls.	EU framework via BAFA. Germany historically among strictest EU enforcers of crypto export controls.	SCOMET List Cat 5. DGFT licensing. Restrictions align with Wassenaar but enforcement capacity limited.	SECO (State Secretariat for Economic Affairs). Goods Control Act. Aligned with Wassenaar. Independent enforcement.	Export Control Act 2002. Strategic Export Licensing (ECJU). Broadly aligned with Wassenaar Cat 5 Part 2.
Cybersecurity Legislation Covering Hardware	Critical Infrastructure Security Act 2018. Security of Critical Infrastructure Act 2018 (SOCI). IoT voluntary code.	Bill C-2 (proposed). Bill C-26 (Critical Cyber Systems). PIPEDA. No mandatory IoT hardware security yet.	Cyber Resilience Act (Reg (EU) 2024/2847, in force Dec 2024). NIS2 Directive (2022/2555). Mandatory for all digital products.	EU CRA + NIS2 apply. BSI Act (BSIG). IT Security Act 2.0 (2021). Mandatory incident reporting for critical infrastructure	IT Act 2000 (amended 2008). CERT-In Directions (April 2022): 6-hour incident reporting. DPDP Act 2023.	Federal Information Security Act (ISG, revised 2024). NCSC (operational since 2024). NIS alignment for critical infrastructure	Product Security and Telecommunications Infrastructure Act 2022 (PSTI). UK Cyber Security Strategy. IoT mandatory baseline.

Note - Effective April 2026 ; References available on slides 16-18

What next? Regulatory Alignment

Proposed Legislature

Recommendation 1 - Addition of Quantum Technology in Bill C-2 and Bill C-8:

Bill C-2 and C-8 must include an explicit mandate for PQC safe authentication related to all infrastructure and systems across public and private sectors. The explicit requirements must include that each organization have a cryptographic inventory of assets, require a quantum risk assessment, and build appropriate PQC migration plans according to the risk levels identified (based on sector). The PQC Migration plans must be enforced and available within 36 months (for future auditability and compliance).

Recommendation 2 – Regulatory Alignment Globally

Canadian regulators must improve existing legislative and quantum-specific legislations. This must be periodically reviewed and aligned with NIST, UK NCSC, EU PQC Roadmap, and Wassenaar agreement to ensure currency with technological innovations and corresponding threats. This includes, but not limited to, hardware requirements across all sections (aligned with the EU Cyber Resilience Act or the Common Criteria mutual recognition arrangement).

Recommendation 3 – Shift NIST AAL to Quantum Safe IAL Levels

Canada must complement NIST AAL Levels and framework to Standards that incorporate for Quantum Safe Computing. This can include accounting for quantum threats to authentication and mandate (hybrid authentication) required within 36 months and (fully quantum-safe) within 60 months.

Compliance Concerns

Implementation Challenges

1. Organizations can't deploy PQC in certified hardware until the certification bodies validate them
2. Quantum security legislation across all sectors and organizations may impose operational costs that are not sustainable. Governments must provide adequate funding to organizations that require the support in building these programs
3. Policy changes may require upskilling and training for government and judicial resources. This will require changes to education system to increase pipeline of quantum computing research, training and development.

Christine Parker & Vibeke Lehmann Nielsen, "Compliance: 14 Questions" in Peter Drahos, ed, **Regulatory Theory: Foundations and Applications** (Canberra: ANU Press, 2017) 217 at 221–232 [Parker & Nielsen].

Conclusion

Digital Trust is rooted in IAM controls that provide mechanisms to uphold the confidentiality and integrity of data within a Zero Trust Framework. Institutional credibility is only possible if organizations are able maintain digital trust in the quantum era. They must be able to provide a level of Quantum-Safe assurance (QAALs) for Authentication in order to create a cyber-resilient ecosystems. In a post-quantum world, every authentication mechanism built on classical public-key cryptography becomes vulnerable. Modern authentication must therefore evolve beyond NIST AALs to incorporate Quantum-Safe assurance levels

The international consensus is clear - the transition to post-quantum cryptography is not a question of whether, but of when and how fast. However, Canada's proposed critical infrastructure legislation — Bills C-2 and C-8 — does not currently reflect this consensus.

The quantum era will not arrive with a single moment of disruption. It will arrive incrementally — through the steady improvement of quantum hardware, the quiet accumulation of harvested data, and the gradual erosion of the classical cryptographic assumptions. This is the basis on which every digital identity, every financial transaction, every medical record, and every legal privilege currently depends. Canada's critical infrastructure will face this threat – and Canadian legislative framework must be ready when it does.


Thank you

Contact Us

Nour Mousa, CISSP | LinkedIn
n1mousa@torontomu.ca

Nasreen Latheef | LinkedIn
nlatheef@protonmail.com

Acronyms

- ACSC (Australian Cyber Security Centre)
- ASD (Australian Signals Directorate)
- BAFA (Bundesamt für Wirtschaft und Ausfuhrkontrolle)
- BSI (Bundesamt für Sicherheit in der Informationstechnik)
- CERT-In (Indian Computer Emergency Response Team)
- CRA (Cyber Resilience Act)
- CSE (Communications Security Establishment)
- DGFT (Directorate General of Foreign Trade)
- DORA (Digital Operational Resilience Act)
- ECJU (Export Control Joint Unit)
- ENISA (EU Agency for Cybersecurity)
- ETSI (European Telecommunications Standards Institute)
- FIPS (Federal Information Processing Standards)
- ISM (India Semiconductor Mission / Information Security Manual [Australia])
- NCSC (National Cyber Security Centre)
- NIST (National Institute of Standards and Technology)
- NIS2 (Network and Information Security Directive 2)
- SCOMET (Special Chemicals, Organisms, Materials, Equipment and Technologies)
- SECO (State Secretariat for Economic Affairs)
- SME (Semiconductor Manufacturing Equipment)
- QAAL (Quantum Safe Authentication Assurance Level)
- QIAL (Quantum Safe Identity Assurance Level)

References – Part 1

I. Legislation

A. Canadian Statutes

Anti-terrorism Act, 2015, SC 2015, c 20 [Bill C-51].

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

Protecting Canadians from Online Crime Act, SC 2014, c 31.

B. Canadian Bills

Bill C-2, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 45th Parl, 2025.

Bill C-8, *An Act to enact the Artificial Intelligence and Data Act and to make related and consequential amendments to other Acts*, 3rd Sess, 45th Parl, 2026.

C. European Union Legislation

EC, *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector*, [2022] OJ, L 333/1 [DORA].

EC, *Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem*, [2023] OJ, L 229/1 [European Chips Act].

EC, *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence*, [2024] OJ, L 2024/1689 [EU AI Act].

EC, *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements*, [2024] OJ, L 2024/2847 [Cyber Resilience Act].

D. United States Legislation

False Claims Act, 31 USC § 3729.

E. International and Administrative Materials

New York State Department of Financial Services, *Cybersecurity Requirements for Financial Services Companies*, 23 NYCRR 500, as amended 1 November 2023.

OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (22 May 2019, amended 3 May 2024).

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (est 1996, as amended).

III. Secondary Sources

A. Government and Institutional Reports

Communications Security Establishment Canada. *National Cyber Threat Assessment 2025–2026* (Ottawa: CSE, 2024).

Communications Security Establishment Canada. "Preparing Your Organization for the Quantum Threat to Cryptography", ITSAP.00.017 (2024), online: Canadian Centre for Cyber Security <https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017>.

Government of Canada. *Canada's National Quantum Strategy* (Ottawa: Innovation, Science and Economic Development Canada, 2023).

Government of Canada. *National Quantum Strategy Consultations: What We Heard Report* (Ottawa: ISED, 2022).

References – Part 2

Online Sources and Institutional Web Pages

Alberta Machine Intelligence Institute (Amii), online: <https://www.amii.ca>.

Arms Control Association. “The Wassenaar Arrangement at a Glance”, online: <https://www.armscontrol.org/factsheets/wassenaar>.

Australian Signals Directorate. “For Business and Government”, online: Cyber.gov.au <https://www.cyber.gov.au>.

Australian Signals Directorate. “Domestic and International Partners”, online: <https://www.asd.gov.au/about/domestic-and-international-partners>.

Australian Signals Directorate. “Modern Defensible Architecture”, online: Cyber.gov.au <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines>.

Canada & United Kingdom. “Memorandum of Understanding on AI, Quantum, and Digital Partnerships” (2024).

CMC Microsystems, FABrIC Network, online: <https://www.cmc.ca>.

ESMC. “ESMC Breaks Ground on Dresden Fab” (2024), online: ESMC.

European Commission. "European Chips Act: Shaping Europe's Digital Future", online: European Commission https://digital-strategy.ec.europa.eu/en/policies/european-chips-act.

European Commission. “Quantum: Shaping Europe’s Digital Future”, online: <https://digital-strategy.ec.europa.eu/en/policies/quantum>.

European Commission. “Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography”, C(2024) 2393 (11 April 2024), online: <https://digital-strategy.ec.europa.eu>.

European Commission. “Simpler EU Digital Rules and New Digital Wallets to Save Billions for Businesses” (2025), online: <https://ec.europa.eu>.

European Commission. “European Chips Act: Shaping Europe’s Digital Future”, online: <https://digital-strategy.ec.europa.eu/en/policies/european-chips-act>.

Europol. *The Second Quantum Revolution: The Impact of Quantum Computing and Quantum Technologies on Law Enforcement* (The Hague: Europol, 2023).

Fasken. “Privacy Commissioner Decisions Impose Sweeping Notification Requirements for Ransomware and Email Account Compromise Incidents”, online: Fasken Knowledge.

FIDO Alliance. *FIDO: Fast Identity Online* (December 2014), online: <https://fidoalliance.org/wp-content/uploads/2014/12/fido.pdf>.

Germany, Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security], "Minimum Standards for the Security of Federal Administration Information Technology" (Bonn: BSI), issued pursuant to § 8(1) *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* [BSI Act] (BSIG), online: BSI https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mindeststandards_node.html [BSI, "Minimum Standards"].

"Goods Control Act", online: *Wikipedia, The Free Encyclopedia* https://en.wikipedia.org/wiki/Goods_Control_Act (April 8, 2026).

Government of India, Ministry of Electronics and Information Technology. "India Semiconductor Mission" (December 2021), online: ISM https://ism.gov.in/.

IBM, “What is quantum computing?” (last visited 8 April 2026), online: IBM https://www.ibm.com/think/topics/quantum-computing

Microsoft. “Resource Estimator: Quantum Safe Planning”, online: Microsoft Learn <https://learn.microsoft.com/en-us/azure/quantum/resource-estimator-quantum-safe-planning>.

National Institute of Standards and Technology (NIST). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (Gaithersburg: NIST, January 2023).

National Institute of Standards and Technology (NIST). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Special Publication 800-171 Rev 2 (Gaithersburg: NIST, February 2020).

National Institute of Standards and Technology (NIST). “Post-Quantum Cryptography”, online: CSRC <https://csrc.nist.gov/projects/post-quantum-cryptography>.

National Institute of Standards and Technology (NIST). “Frequently Asked Questions about Post-Quantum Cryptography”, online: Migration to Post-Quantum Cryptography Project <https://csrc.nist.gov/projects/pqc-migration>.

National Institute of Standards and Technology (NIST). “NIST PQC Security Strength Categories (1–5) Explained”, online: CSRC.

National Institute of Standards and Technology (NIST). *SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management* (Gaithersburg: NIST, 2024).

National Institute of Standards and Technology (NIST). “Roadmap: NIST Special Publication 800-63-4 Digital Identity Guidelines”, online: NIST <https://www.nist.gov/digital-identity-guidelines>.

National Cyber Security Centre (UK). “Timelines for Migration to Post-Quantum Cryptography” (2024), online: NCSC <https://www.ncsc.gov.uk/whitepaper/pqc-timelines>.

OECD. *OECD Artificial Intelligence Policy Observatory*, online: OECD.AI <https://oecd.ai>.

Open Quantum Safe Project. “liboqs”, online: <https://openquantumsafe.org/liboqs/>.

openparliament.ca. “Bill C-8”, online: <https://openparliament.ca/bills/45-1/C-8/>.

Quantum Canary. “Cryptography Regulations Across the World in 2025” (24 June 2025), online: <https://www.quantumcanary.org/insights/cryptography-regulations-across-the-world-in-2025>.

Applied Quantum. “Quantum Computing, Quantum Security, Comms, Sensing, AI”, online: <https://www.appliedquantum.com>.

LinkedIn. “Transparency Blog” (Community Report), online: LinkedIn.

Vector Institute for Artificial Intelligence, online: <https://vectorinstitute.ai>.

World Economic Forum. *Quantum Security for the Financial Sector: Informing Global Regulatory Approaches* (Geneva: WEF, 2024), online: <https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/>.