Post-Quantum Cryptography in Canada: Requirements, Standards and Vendor Readiness

10 November 2026

Junior Williams

trustcyber.ca

Summary: what is current as of 10 November 2026

This guide collects the published post-quantum cryptography (PQC) requirements, standards and vendor capabilities that matter to Canadian organizations, and the author's reading of how to test and report them. Sources were checked November 7 to 10, 2026. PQC is public-key cryptography designed to resist classical and quantum attacks, and it runs on ordinary computers. [1]

Area	What is current
Federal government of Canada	The Treasury Board notice, effective October 9, 2025, binds covered federal organizations. Initial migration plans were due April 1, 2026. High-priority systems are to be migrated by December 31, 2031 and the rest by December 31, 2035. [2]
Canadian algorithm guidance	The Cyber Centre's ITSP.40.111 version 5 (guidance) took effect May 29, 2026. It phases out today's quantum-vulnerable public-key algorithms by December 31, 2035 where they are used without a post-quantum scheme. [3]
Canadian private sector	The Personal Information Protection and Electronic Documents Act (PIPEDA) requires safeguards appropriate to sensitivity and prescribes no algorithm or migration date. [4] The March 2026 bulletin from the Office of the Superintendent of Financial Institutions (OSFI) describes readiness phases as discretionary practices. [5][6]
United States standards	The National Institute of Standards and Technology (NIST) published its transition report, IR 8547 (guidance), in final form on October 27, 2026. Quantum-vulnerable public-key algorithms are deprecated after December 31, 2030 and disallowed after December 31, 2035. [7]
United States federal buyers	Executive Order 14412 of June 22, 2026 sets December 31, 2030 for key establishment and December 31, 2031 for signatures on high-value and high-impact civilian systems. The order also directs an acquisition rule, due to be proposed about December 19, 2026, that would require covered contractors to comply with Federal Information Processing Standards (FIPS), including PQC, by December 31, 2030. [8][9]
Module validation	Since September 22, 2026, only FIPS 140-3 validations remain on the active list of the Cryptographic Module Validation Program (CMVP). [10]
Cloud services	The AWS Key Management Service has offered post-quantum signing keys since June 13, 2025 and key-encapsulation keys since October 26, 2026, in most Regions. [11] Google Cloud's equivalent has offered post-quantum signing since July 16, 2026, with key encapsulation in preview. [12][13] Microsoft's Managed HSM (hardware security module) documentation lists no post-quantum key types; AES key wrap in Key Vault Premium is in public preview. [14][15][16]

Contents

1. What the quantum threat changes 3
2. What post-quantum cryptography replaces and what it leaves alone 4
3. Dates and who they apply to 5
4. Where the migration work lands, by type of system 7
5. What breaks in deployment 9
6. Supported, enabled, observed, retired 10
7. What vendors offer today 11
8. What migration cost depends on 13
Standards status 14
What will date this edition 15
Glossary 15
Sources 16

1. What the quantum threat changes

Quantum cryptanalysis threatens the public-key mechanisms in use today, including Rivest-Shamir-Adleman (RSA) and elliptic-curve key establishment and signatures. The capability is conditional. Two things make the threat current anyway: data that can be recorded today, and equipment deployed today that will still be verifying signatures years from now.

In a harvest-now, decrypt-later attack, an adversary records encrypted traffic today and keeps it until an attack becomes practical. Changing cryptography later cannot retrieve copies already collected. [7]

Confidentiality path	Authenticity path
1. Capture today. Encrypted traffic and vulnerable key-exchange material are recorded.	1. Trust deployed today. Certificates, updates or firmware rely on quantum-vulnerable signatures.
2. Future key recovery. An attack on the public-key mechanism exposes session keys.	2. Future signature forgery. A vulnerable scheme no longer proves authentic origin.
3. Sensitive data exposed. Recorded information may still need protection.	3. False trust. A forged identity or update is accepted while its trust path stays vulnerable.

Two paths of quantum exposure, each read from 1 to 3. Key establishment and signatures migrate separately. [7][17]

What can be collected today depends on the key exchange in use. Ephemeral elliptic-curve key exchange provides classical forward secrecy but remains vulnerable to a sufficiently capable quantum attack on a recorded exchange. Static RSA key transport widens the exposure: one recovered private key opens every recorded session that used it.

The lifetime test

Whether a data flow meets the lifetime threshold comes down to three numbers: confidentiality lifetime L, migration lead time M and time to a chosen threat scenario T. M and T are counted in years from today; L is how long the data must stay confidential from when it is created.

> Recorded traffic and stored copies: $L \geq T$. Information collected today is still sensitive when the threat scenario arrives.
>
> Services that keep generating sensitive data: $L + M \geq T$. Data created just before migration completes must stay confidential for L more years after that.

The test adapts the one in *Canadian National Quantum-Readiness: Best Practices and Guidelines*, published by the Quantum-Readiness Working Group of the Canadian Forum for Digital Infrastructure Resilience (migration time plus shelf-life time greater than the threat timeline), and treats equality as meeting the threshold. [18] Running it at more than one horizon shows how much the result depends on the scenario.

Flow	Rule	T = 5 years	T = 10 years	T = 15 years
Records needing 12 years of confidentiality, already recorded in transit	12 ≥ T	**Threshold met**	**Threshold met**	Below threshold
Same records, from a service needing 3 years to migrate	12 + 3 = 15 ≥ T	**Threshold met**	**Threshold met**	**Threshold met**
Two-year data lifetime, one-year migration	2 + 1 = 3 ≥ T	Below threshold	Below threshold	Below threshold

"Threshold met" means the flow warrants a treatment decision under that threat scenario, and is a reason to examine the flow first. "Below threshold" means only that this lifetime test is not met; it does not establish absence of exposure or override business impact, signing dependencies or contractual dates.

The author's planning assumptions are the threat horizons of 5, 10 and 15 years, which are stress tests rather than probabilities, and a simpler first screen: assess now any information that must stay confidential past 2035. That year is anchored to NIST's disallowance of quantum-vulnerable public-key algorithms after December 31, 2035 [7] and the Treasury Board's December 31, 2035 target. [2] Where the 2035 screen and the lifetime test disagree, the 2035 screen is the wider net; shorter-lived information can still meet the lifetime test.

Signatures and long-lived verifiers

Signatures do not share the passive-collection problem. The exposure is the installed lifetime of the verifier: a device that will operate for fifteen years and cannot replace its verification key needs an engineering decision now, even if it holds no long-lived confidential data. What decides the timing is the update path, the trust anchors and the last feasible replacement date.

2. What post-quantum cryptography replaces and what it leaves alone

PQC replaces the public-key mechanisms threatened by quantum cryptanalysis. The Canadian algorithm guidance names them: RSA, finite-field and elliptic-curve Diffie-Hellman and Menezes-Qu-Vanstone (MQV) key agreement, the Digital Signature Algorithm (DSA), its elliptic-curve form (ECDSA) and the Edwards-curve form (EdDSA). [3] Larger RSA keys can address some classical-security requirements, but they do not remove RSA's quantum vulnerability. [3] [7]

Job	Current PQC building block	What has to be settled
Establish shared key material	Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), FIPS 203 [19]	A supported protocol and parameter set. ML-KEM establishes a shared key but does not authenticate the parties; that typically comes from digital signatures and certificates. [20]

Job	Current PQC building block	What has to be settled
Sign and verify	Module-Lattice-Based Digital Signature Algorithm (ML-DSA), FIPS 204 [21]; Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), FIPS 205 [22]; the stateful hash-based Leighton-Micali Signature (LMS) and eXtended Merkle Signature Scheme (XMSS), NIST Special Publication (SP) 800-208 [23]	Signer, verifier, certificate format and key lifecycle support
Encrypt bulk data	Symmetric encryption such as the Advanced Encryption Standard (AES), unchanged	How each key is generated, wrapped, transported, recovered and accessed

The public-key parts change and the symmetric parts stay. Quantum computers do not directly break AES-encrypted files; the exposure runs through the public-key mechanism that established or protects the key. [3][7] "We use AES-256" therefore answers the bulk-encryption question only: the key may still be wrapped with RSA or carried over a classical exchange. For stored data the same question reaches backups, archives, key wrapping, recovery systems and external key-management services.

Symmetric and hash settings need a review, not a wholesale replacement. NIST does not call for general replacement of approved symmetric algorithms as part of the transition. It does say that its symmetric standards at the 112-bit security level "will be disallowed in 2030", and ITSP.40.111 phases out the 224-bit Secure Hash Algorithm variants SHA-224 and SHA3-224 by December 31, 2030. Canadian guidance continues to recommend AES key lengths of 128, 192 and 256 bits. [3][7]

Quantum key distribution is a different technology that uses specialized quantum communications infrastructure; the Cyber Centre recommends standardized PQC for addressing the quantum threat. [1]

3. Dates and who they apply to

Each row is marked Binding, Guidance or Proposed for the organizations named in its first column. End-of-year dates are written as Dec. 31; where a source gives only a year, the table says so. The table covers the Canadian, United Kingdom, European Union, United States and NIST sources cited; sector rules and contracts can also apply.

Authority and who it applies to	Status	Date	What it sets
Canada: federal organizations covered by the Treasury Board notice [2]	**Binding**	Apr. 1, 2026 (date already past)	Initial migration plan; annual reporting thereafter; aligned PQC clauses in digital-component contracts entered after this date
		Apr. 1, 2027	Plans updated for the identification phase
		Apr. 1, 2028	Inventories, priorities and transition plans updated; systems begin transitioning
		Dec. 31, 2031	High-priority systems migrated

Authority and who it applies to	Status	Date	What it sets
		Dec. 31, 2035	Remaining systems migrated
Canada: systems using the Cyber Centre algorithm guidance, ITSP.40.111 version 5 [3]	**Guidance**	Dec. 31, 2030	Phase-outs including DSA, SHA-224 and SHA3-224
		Dec. 31, 2035	RSA, finite-field and elliptic-curve Diffie-Hellman and MQV, ECDSA and EdDSA phased out where used without a post-quantum scheme
Canada: financial institutions regulated by OSFI [5][6]	**Guidance**	Phased readiness; no deadline	The bulletin's practices are discretionary, not regulatory expectations; it notes that external guidance generally points to 2035
Canada: organizations subject to PIPEDA [4]	**Binding**	No date	Safeguards appropriate to sensitivity, kept current; no algorithm or migration date prescribed
United Kingdom: National Cyber Security Centre guidance, aimed especially at larger organizations and complex or critical infrastructure [24]	**Guidance**	By 2028 By 2031 By 2035 (years only)	Discovery and plan Highest-priority migrations Completion
European Union: coordinated roadmap for Member States and their national implementation [25][26]	**Guidance**	Dec. 31, 2026 Dec. 31, 2030 2035 (year only)	Start of transition High-risk use cases As many systems as feasible
United States: civilian federal agencies, for high-value assets and high-impact and agency-prioritized systems; National Security Systems are excluded [8][9]	**Binding**	Dec. 31, 2030 Dec. 31, 2031 Through 2035 (year only)	Key establishment (Executive Order 14412) Signatures (Executive Order 14412) Remaining transition (Office of Management and Budget memorandum M-26-15)
United States: federal contractors, if the rule is adopted [8]	**Proposed**	Rule to be proposed about Dec. 19, 2026	Would require covered contractors to comply with FIPS, including PQC, by Dec. 31, 2030
United States: National Security Systems, under their own policy framework [27][28]	**Binding**	2027 and 2030 (years only)	From 2027, new commercial National Security Systems must be capable of supporting quantum-resistant algorithms; by 2030, legacy systems that cannot are phased out
NIST: users of NIST standards and guidelines [7]	**Guidance**	After Dec. 31, 2030 After Dec. 31, 2035	Vulnerable public-key algorithms deprecated The same algorithms disallowed

Federal departmental dates bind covered government organizations; their suppliers deliver against their contracts. The U.S. contractor row reaches Canadian suppliers to U.S. federal agencies if the rule is adopted; the National Security Systems row reaches suppliers to U.S. national-security programmes.

The Canadian requirements in more detail

For federal departments and agencies, the Treasury Board notice applies to the organizations covered by section 6 of the *Policy on Government Security*. Its migration-plan scope runs through Protected B; departments handling Protected C or classified information must contact the Cyber Centre. [2]

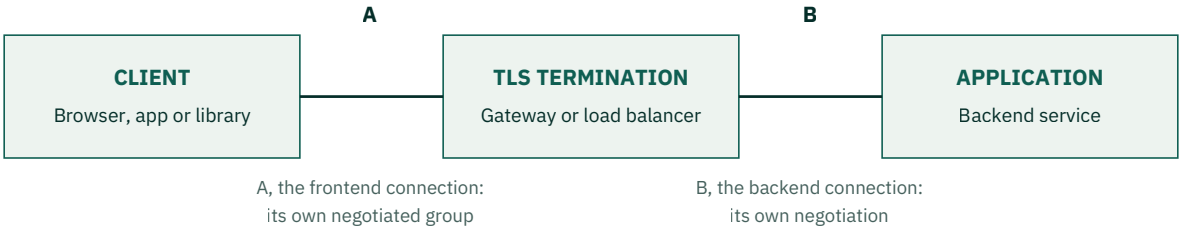
For government suppliers, covered departments must include aligned PQC procurement clauses in digital-component contracts entered into after April 1, 2026. The clauses support PQC recommended by the Cyber Centre, modules certified under the CMVP and cryptographic agility. [2] The Cyber Centre's ITSM.00.501 provides example clauses, including sample support dates at the end of 2026 that become supplier commitments only through the terms a contract actually adopts. [29]

For financial institutions, the discretionary status of OSFI's bulletin leaves an institution's technology, cyber-risk, privacy and contractual obligations in place. [5] [6]

For privacy, the Privacy Commissioner's guidance says PIPEDA does not prescribe particular safeguards and stresses keeping protection current. PQC can contribute to safeguards appropriate to sensitivity; adopting it is not by itself a compliance determination. [4]

4. Where the migration work lands, by type of system

Migration arrives as separate changes in systems that different teams own. The figure shows why Transport Layer Security (TLS) has to be read one connection at a time. The table then gives, for each type of system, what changes, what tends to break and one fact that is easy to miss. Firmware signing and certificates need more room and follow the table.



Every termination point negotiates its own key exchange. A hybrid key exchange on connection A is evidence for A only; B can still run a classical exchange, and the certificates on each need their own check. [30] [31]

System type	What changes	What breaks	Easy to miss
Network and application transport	Key exchange moves to a hybrid group at every point that terminates TLS. Request for Comments (RFC) 10024 specifies three for TLS 1.3: X25519MLKEM768, SecP256r1MLKEM768 and SecP384r1MLKEM1024. [30]	Clients that cannot negotiate the hybrid groups; those clients determine how long servers keep offering classical groups. Intermediaries on the route: content delivery network, web application firewall, inspection proxy, load balancer, service mesh.	A hybrid group combines a classical and a post-quantum key exchange and is designed to stay secure if at least one of them does, given the specified construction and a correct implementation. [30] It leaves certificate signatures unchanged.

System type	What changes	What breaks	Easy to miss
Certificates and public key infrastructure (PKI)	Certificate signatures, through roots, intermediates, issuing authorities, templates, enrolment and revocation	Every relying party must parse and verify the new algorithm, including mutual-TLS clients, device identities and pinned certificates. A new chain is worthless to a verifier that rejects its algorithm or encoding.	Two ML-DSA-44 certificates carry 7,464 bytes in key and signature alone. [32]
Firmware and code signing	The verification key and signature format in each product, with its update agent, recovery image and anti-rollback counter	A verification key fixed in boot read-only memory cannot be changed by a software update	The NSA's suite for U.S. National Security Systems excludes the multi-tree variants of LMS and XMSS, which ITSP.40.111 version 5 lists with conditions. [3][28]
Cloud and key management	Interface transport, application transport, data encryption, key wrapping, signing and recovery are separate boundaries, each with a provider capability and a customer configuration	Differences by region, endpoint and software development kit version; features still in preview	A provider's transport protection and its post-quantum key types are different capabilities: AWS's hybrid post-quantum TLS protects the connection to the Key Management Service endpoint, not data encrypted under its keys. [33]
Legacy and embedded systems	A component with no supported upgrade gets one of four treatments in the Cyber Centre roadmap: upgrade, replace, isolate or tunnel. [17]	Physical work, outages, supplier support and replacement windows	A protective tunnel covers traffic crossing the segment and does nothing for a signature verifier inside the device.
Algorithm choice and fallback	A contingency means a second standardized family. ML-KEM and ML-DSA are lattice-based; SLH-DSA, LMS and XMSS are hash-based. Hamming Quasi-Cyclic (HQC), the code-based mechanism NIST selected, and FN-DSA, the signature scheme derived from Falcon, are still being standardized. [7][34]	A fallback whose verifier, key lifecycle and operating cost were never tested	An SLH-DSA-128s signature is 7,856 bytes, more than three times the 2,420 bytes of ML-DSA-44. [22][32] For key establishment there is no second standardized mechanism until HQC is finished. The classical component hedges against weaknesses in the post-quantum component against classical attackers; it is not a second quantum-resistant alternative. [30]
Validation and cryptographic agility	Algorithm and parameter choices move into configuration covered by inventory updates and release-pipeline regression tests	Module validation evidence (section 7)	Changing one cryptographic setting in a controlled release and rolling it back is one demonstration of agility. The rollback keeps the service available and restores the exposure the change removed.

Firmware signing

A product whose verification key is fixed in boot read-only memory needs a field-provisioning path for a new key, or replacement. The transition build is the hard part: the old verifier must accept the update that installs the new one, and an interrupted update must recover.

The Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) of the U.S. National Security Agency (NSA) approves LMS and XMSS, specified in NIST SP 800-208, and ML-DSA-87 for firmware and software signing in National Security Systems. It excludes SLH-DSA and the multi-tree variants of LMS and XMSS, known as the Hierarchical Signature System (HSS) and XMSS-MT. [23][28] Outside that regime, SLH-DSA is the stateless hash-based option.

SP 800-208 forbids exporting an LMS or XMSS private key, even encrypted, because a copied key can reuse a one-time key. SP 800-208 describes both independent signing keys on separate modules and distributed multi-tree arrangements; the applicable policy and verifier capabilities determine which approach is usable. [23] CNSA 2.0's exclusion of the multi-tree variants binds U.S. National Security Systems. [28] ITSP.40.111 version 5 lists HSS and XMSS-MT, subject to conditions on hash function and private-key state management. [3]

Certificates

The ML-DSA-44 public key in FIPS 204 is 1,312 bytes and its signature 2,420 bytes. [32] Two certificates each carrying an ML-DSA-44 key and signature hold 7,464 bytes in those two fields alone: 2 × (1,312 + 2,420). A real chain also carries names, validity, extensions and encoding, so the chain a deployment sends is larger again. Issuance, renewal and revocation change along with verification.

5. What breaks in deployment

Larger keys and signatures change message sizes, buffering, fragmentation and device memory requirements. The table lists where that surfaces, and what a pilot on the complete traffic and trust path measures.

Surface	What fails	What a pilot measures
TLS inspection and middleboxes	Rejected group identifiers, split ClientHello handling, silent classical fallback	Negotiation result through every production intermediary; fallback observations
Certificates and mutual TLS	Chain or field-size limits, unsupported signature identifiers, enrolment and renewal failures	Measured chain bytes; successful issuance, verification, renewal and revocation tests
Datagram TLS (DTLS) and constrained devices	Lost fragments, retransmissions, pressure on the maximum transmission unit (MTU) and on memory	Handshake success under representative loss and MTU; memory and latency results
Domain Name System Security Extensions (DNSSEC)	Larger signed responses, truncation and failed fallback to the Transmission Control Protocol	Resolver and authoritative interoperability and response-size tests with supported implementations

Surface	What fails	What a pilot measures
Secure/Multipurpose Internet Mail Extensions (S/MIME)	Sender and recipient algorithm support, message processing, archive and gateway handling	Send, receive, verify, decrypt and archive recovery across the actual mail estate
Signing tokens and hardware security modules (HSMs)	Unsupported key types, object storage, interface limits, signing throughput and recovery	Vendor capability evidence plus generation, signing, backup, restore and verifier tests

Sizes are easy to misquote. The X25519MLKEM768 client key share in RFC 10024 is 1,216 bytes; that is the size of the key share, not of the whole handshake. [30] The Domain Name System has no universal 1,232-byte limit either. That figure is a common User Datagram Protocol payload choice derived from the Internet Protocol version 6 (IPv6) minimum MTU; RFC 9715 recommends 1,400 bytes, with smaller values allowed. [35]

An algorithm standard is not yet DNSSEC or S/MIME support; each needs a supported protocol profile. AWS flags proxy and firewall compatibility as a deployment concern [33], and the application guidance from the Internet Engineering Task Force is still an Internet-Draft. [36]

Pilot tests

Eight tests cover the failure surfaces above:

1	Intended negotiation or signature verification	**5**	Loss, MTU, fragmentation and constrained memory
2	Intermediary and relying-party compatibility	**6**	Renewal, rotation, backup and recovery
3	Certificate, handshake and message sizes against limits	**7**	Classical fallback detection and policy
4	95th- and 99th-percentile latency, error rate and capacity	**8**	Rollback and restoration of intended protection

6. Supported, enabled, observed, retired: telling a claim from a deployment

Supported means the supplier has implemented the capability in an identified release. **Enabled** means the deployed configuration selects it. **Observed in use** means a representative transaction or verification actually uses it. **Retired** means the vulnerable path has been removed from the named scope. Keep mitigated paths and accepted exceptions separate.

State	Evidence	What it shows
Supported	Supplier release evidence	Exact product, version, protocol and algorithm
Enabled	Deployment evidence	Configuration on the named service and endpoints

State	Evidence	What it shows
Observed in use	Transaction evidence	Negotiated group or successful signature verification
Retired	Closure evidence	Vulnerable path removed from the named scope

The Cyber Centre roadmap treats migration as complete when quantum-vulnerable algorithms are disabled, isolated or tunnelled, not when PQC is merely supported. [17] In this guide's terms a disabled path is retired; isolated and tunnelled paths are mitigated and reported separately.

The four states are counted against one named scope, service by service. For example, an illustrative report in these terms could read: "Of ten priority services, nine are supported, eight enabled, six observed in use and four retired. The customer virtual private network (VPN) is waiting on a supplier release." Each state is counted within the one before it. A single readiness score or an enterprise-wide percentage hides what that sentence shows. A count of upgraded assets can conceal the one dependency that still exposes a sensitive service, and a percentage of an incomplete inventory overstates coverage.

The same reading applies to marketing terms. "Quantum-safe", "quantum-proof", "government approved", "fully compliant" and "post-quantum encryption" are claims with a scope: which key-establishment, encryption or signing function the product supplies, approved by whom, for what use, against which version, under which configuration and with what exclusions.

7. What vendors offer today

Cloud providers

The table lists what AWS, Google Cloud and Microsoft Azure documented. An existing subscription may already include a capability; the third column is what remains on the customer's side of the boundary.

Provider capability	What it protects or supplies	What the customer still verifies
AWS Key Management Service (KMS)	Hybrid post-quantum TLS protects the connection between a supported client and the KMS endpoint, not data encrypted under KMS keys. [33] ML-DSA signing keys generally available since June 13, 2025; ML-KEM-512, ML-KEM-768 and ML-KEM-1024 keys available since October 26, 2026, except in the United Arab Emirates, Bahrain and China Regions. [11]	A compatible client, the actual proxy and firewall path and the negotiated group; for signing, the consuming verifier
Azure Key Vault and Managed HSM	Managed HSM documents RSA, elliptic-curve and AES keys, with AES key wrap; no post-quantum key types as of November 10, 2026. [14][15] AES keys and AES key wrap in Key Vault Premium are in public preview. [16]	The application's wrapping and transport paths; each required operation against the service tier and its preview status

Provider capability	What it protects or supplies	What the customer still verifies
Google Cloud Load Balancing	X25519MLKEM768 on frontend TLS connections. Google's page, last updated November 9, 2026, says default enablement begins in October 2026 and lists the current state as disabled by default. A DEFERRED setting postpones enablement until October 2027, after which it is always enabled. [31]	The policy attached to each load balancer, client compatibility and the negotiation actually observed
Google Cloud KMS	ML-DSA and SLH-DSA signing generally available since July 16, 2026. [12] ML-KEM-768, ML-KEM-1024 and X-Wing (a hybrid of ML-KEM-768 and X25519) key encapsulation in preview since September 23, 2025. [13]	Algorithm, launch stage, protection level and location; that the consuming application can verify or use the result

A rollout announcement does not report an endpoint's state; the attached policy and the observed negotiation do. The fields that pin a provider claim down are the exact service, endpoint, region, software development kit version, algorithm, availability state and validation scope.

TELUS announced a commercial VPN service, marketed as Quantum-Safe VPN, on November 14, 2025, using Palo Alto Networks technology and integrated with its Managed Next Generation Firewall service. [37]

Discovery tooling

A **cryptographic bill of materials (CBOM)** represents cryptographic assets and dependencies in machine-readable form. CycloneDX, which added the capability in version 1.6, supports algorithms, keys, certificates and their relationships to software components. [38] The Cyber Centre roadmap says discovery should use multiple methodologies [17]; each category of tool below sees a different part of the estate.

Tool category	What it can show	What it cannot see
Network and certificate discovery	Protocols, endpoints, chains and observed negotiation on the selected routes	Unused paths, offline devices, internal key wrapping and application code
Source and dependency analysis	Cryptographic interfaces and libraries in representative languages and builds	Dynamic configuration, proprietary components and runtime behaviour
Host and runtime discovery	Actual libraries and configuration linked to running services	Unmanaged hosts and inaccessible supplier systems
Cloud inventory and configuration interfaces	Keys, service configuration and identities mapped to an account or project	Provider-internal implementations and connections outside the collected scope
CBOM aggregation	Import, export, deduplication, provenance and version tracking	Accuracy and completeness of the contributing observations

The preliminary draft of SP 1800-38B from NIST's National Cybersecurity Center of Excellence provides a discovery architecture and test approach. [39]

Validation records

Algorithm validation under the Cryptographic Algorithm Validation Program (CAVP) and module validation under the CMVP are different evidence. [29] A CMVP certificate covers a named module, version and operating environment. It does not cover a product built on that module; the supplier's product-to-module mapping is separate evidence. [10] The official record gives the certificate number, FIPS 140 version, security policy, module version, operating environment, status, sunset date and caveats.

On the CMVP list, historical and revoked are different statuses: a revoked validation cannot demonstrate FIPS 140 compliance. Whether a FIPS 140-2 deployment can stay in use, and whether it remains eligible for procurement, depends on the applicable policy and contract. [10]

Questions for a supplier

Thirteen questions separate a capability available now from a roadmap. A supplier can answer each with a product, a version and evidence (available now) or with a dated delivery commitment (roadmap); the two are recorded separately.

1	Protected connection, key or signature; included components	**8**	Product-to-module mapping and PQC service coverage
2	Product, version, region or endpoint, and operating environment	**9**	Negotiation or use evidence; permitted fallback and monitoring
3	Algorithms, parameters, protocol and group identifiers	**10**	Agreed workload, latency and error limits, compatibility matrix
4	Available now, preview, or committed release with date	**11**	Key generation, storage, rotation, recovery and retirement
5	Required client, gateway and verifier versions	**12**	Upgrade, rollback, support, errata and exit arrangements
6	Hybrid construction and authentication	**13**	Delivery price and stated dependencies
7	CAVP or CMVP certificate, module and security policy		

As an illustration of an observable acceptance test for a TLS service: "The named client and gateway versions negotiate the agreed hybrid group through the listed inspection path, meet the agreed 95th- and 99th-percentile latency and error thresholds under the agreed workload, and produce evidence that detects classical fallback." Contract wording of this kind needs legal and procurement review, which is also how ITSM.00.501 presents its own example clauses. [29]

8. What migration cost depends on

The Cyber Centre roadmap requires a departmental migration plan to have a cost estimate that includes resource allocation. [17] It gives no figures. What follows is the author's view of what moves an estimate and what a first one can leave out.

Server count describes the estate; application dependencies and change complexity drive the cost. An estimate rises with shared gateways and intermediaries, application changes, supplier coordination, poorly documented legacy components and repeated compatibility testing. A blocked vendor release extends elapsed time whatever the effort.

A first estimate can leave out the items specific to post-quantum work, namely replacement of hardware security modules, bespoke firmware redesign and broad PKI replacement, as well as replacement of other major appliances, training, cloud consumption, taxes, business downtime and supplier delays. It can also leave out the recurring work after migration: inventory changes, exception review, supplier and standards tracking, and regression checks.

Standards status

Item	Status	What it governs
ITSP.40.111 [3]	Version 5, effective May 29, 2026; phase-out dates in section 3	Recommended algorithms, parameters and phase-out dates for Canadian systems
NIST IR 8547 [7]	Final, October 27, 2026	Transition rules for current public-key use
FIPS 203, ML-KEM [19]	Final August 13, 2024; a planning note of November 17, 2025 identifies a correction for a future update	Key establishment
FIPS 204, ML-DSA [21]	Final August 13, 2024; a planning note of July 31, 2026 points to minor issues for a future revision	Signatures
FIPS 205, SLH-DSA [22]	Final August 13, 2024	Stateless hash-based signatures: parameter choice, signature size and verifier support
SP 800-208, LMS and XMSS [23]	Final, October 2020	Stateful signatures for firmware and code signing, including private-key state management
SP 800-227 [20]	Final September 18, 2025	Requirements for integrating key-encapsulation mechanisms such as ML-KEM
RFC 10024 [30]	Published August 2026; Standards Track, Proposed Standard	The hybrid groups for TLS 1.3
HQC and FN-DSA [7] [34]	Standards under development in NIST's October 2026 transition report	Alternatives, once final standards and supported products exist
CMVP active list [10]	Since September 22, 2026, only FIPS 140-3 validations remain on the active list	A module's current certificate, security policy and service coverage

What will date this edition

This edition is fixed at November 10, 2026 and is not updated on a schedule. Any of these events would put part of it out of date:

- The Cyber Centre revises ITSP.40.111, or Treasury Board or another relevant jurisdiction changes migration direction
- NIST revises FIPS 203 or 204, or publishes the HQC or FN-DSA standard
- The U.S. acquisition rule is proposed or finalized, or the U.S. Cybersecurity and Infrastructure Security Agency publishes its CBOM guidance, directed for about March 2027 [8]
- A provider changes the availability or scope of a cited service, such as Google Cloud KMS moving ML-KEM to general availability or Azure adding post-quantum key types

Glossary

CAVP / CMVP. Cryptographic Algorithm Validation Program / Cryptographic Module Validation Program

CBOM. Cryptographic bill of materials: cryptographic assets and dependencies in machine-readable form

CNSA 2.0. The NSA's Commercial National Security Algorithm Suite 2.0, governing algorithms for U.S. National Security Systems

Cryptographic agility. The ability to change algorithms, parameters and implementations while preserving secure operation

FIPS. Federal Information Processing Standard, published by NIST

FN-DSA. The signature standard NIST is developing from Falcon

Harvest now, decrypt later. Recording encrypted traffic for a future attack

HQC. Hamming Quasi-Cyclic, a code-based KEM selected by NIST for standardization

HSM. Hardware security module

HSS / XMSS-MT. Multi-tree variants of LMS and XMSS in NIST SP 800-208

Hybrid key agreement. A specified combination of a classical and a post-quantum key-establishment mechanism

KEM. Key-encapsulation mechanism, used to establish shared key material

LMS / XMSS. Leighton-Micali Signature and eXtended Merkle Signature Scheme: stateful hash-based signatures, NIST SP 800-208

ML-DSA. Module-Lattice-Based Digital Signature Algorithm, FIPS 204

ML-KEM. Module-Lattice-Based Key-Encapsulation Mechanism, FIPS 203

National Security Systems. A distinct U.S. policy scope with its own algorithm requirements

OSFI. Office of the Superintendent of Financial Institutions

PIPEDA. Personal Information Protection and Electronic Documents Act

PKI. Public key infrastructure, including certificate issuance and relying-party trust

PQC. Post-quantum cryptography: public-key cryptography designed to resist classical and quantum attacks, run on ordinary computers

RFC. Request for Comments, the publication series of the Internet Engineering Task Force; not every RFC is an Internet Standard

SLH-DSA. Stateless Hash-Based Digital Signature Algorithm, FIPS 205

TLS / DTLS. Transport Layer Security / Datagram Transport Layer Security

X-Wing. Hybrid KEM combining ML-KEM-768 and X25519

Sources

Sources checked November 7 to 10, 2026.

[1] Canadian Centre for Cyber Security. *Preparing your organization for the quantum threat to cryptography*. ITSAP.00.017. February 2025.
https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017

[2] Treasury Board of Canada Secretariat. *Security Policy Implementation Notice: Migrating the Government of Canada to post-quantum cryptography*. Effective October 9, 2025.
https://www.canada.ca/en/government/system/digital-government/policies-standards/spin/migrating-government-canada-post-quantum-cryptography.html

[3] Canadian Centre for Cyber Security. *Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information*. ITSP.40.111 version 5. Effective May 29, 2026.
https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111

[4] Office of the Privacy Commissioner of Canada. *PIPEDA fair information principle 7: Safeguards*.
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_safeguards/

[5] OSFI. *Quantum Readiness Phases and Timelines*. Technology risk bulletin. Dated March 2026.
https://www.osfi-bsif.gc.ca/en/risks/technology-cyber-risk-management/technology-risk-bulletin/quantum-readiness-phases-timelines

[6] OSFI. *Technology Risk Bulletin*. Index page describing the discretionary status of the bulletins.
https://www.osfi-bsif.gc.ca/en/risks/technology-cyber-risk-management/technology-risk-bulletin

[7] NIST. *Transition to Post-Quantum Cryptography Standards*. IR 8547. Final, October 27, 2026.
https://csrc.nist.gov/pubs/ir/8547/final

[8] The White House. *Securing the Nation Against Advanced Cryptographic Attacks*. Executive Order 14412. June 22, 2026.
https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/

[9] Office of Management and Budget. *Execution of the Migration to Post-Quantum Cryptography*. M-26-15. June 24, 2026.
https://www.whitehouse.gov/wp-content/uploads/2026/06/M-26-15-Execution-of-the-Migration-to-Post-Quantum-Cryptography.pdf

[10] NIST. *Cryptographic Module Validation Program frequently asked questions*. Includes the active-list transition (items CL-4, CL-8, CL-10, CL-12).
https://csrc.nist.gov/projects/cryptographic-module-validation-program/faqs

[11] AWS. *AWS KMS developer guide: Post-quantum keys in AWS KMS*. What's New, ML-DSA, June 13, 2025; What's New, ML-KEM, October 26, 2026.
https://docs.aws.amazon.com/kms/latest/developerguide/mldsa.html
https://aws.amazon.com/about-aws/whats-new/2026/10/kms-ml-kem-post-quantum/

[12] Google Cloud. *Cloud KMS digital signatures*. Release notes entry for general availability, July 16, 2026.
https://docs.cloud.google.com/kms/docs/digital-signatures

[13] Google Cloud. *Cloud KMS key encapsulation mechanisms*. Last updated October 27, 2026; release notes entry for preview, September 23, 2025.
https://docs.cloud.google.com/kms/docs/key-encapsulation-mechanisms

[14] Microsoft Learn. *About keys, Azure Key Vault Managed HSM*. May 21, 2026.
https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/about-keys

[15] Microsoft Learn. *Managed HSM key types, algorithms and operations*. Includes AES key wrap. May 21, 2026.
https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/about-keys-details

[16] Microsoft Tech Community. *Azure Key Vault Premium and AES-KW post-quantum resistant key wrapping in public preview*. Page last updated August 5, 2026.
https://techcommunity.microsoft.com/blog/post-quantum-crypto-tech-blog/azure-key-vault-premium-and-aes-kw-post-quantum-resistant-key-wrapping-in-public/4544358

[17] Canadian Centre for Cyber Security. *Roadmap for the migration to post-quantum cryptography for the Government of Canada*. ITSM.40.001. June 23, 2025.
https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001

[18] Quantum-Readiness Working Group, Canadian Forum for Digital Infrastructure Resilience. *Canadian National Quantum-Readiness: Best Practices and Guidelines*. Version 04. July 10, 2024.
https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/documents/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf

[19] NIST. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. FIPS 203. Final August 13, 2024; planning note November 17, 2025.
https://csrc.nist.gov/pubs/fips/203/final

[20] NIST. *Recommendations for Key-Encapsulation Mechanisms*. SP 800-227, section 4.1. Final September 18, 2025.
https://csrc.nist.gov/pubs/sp/800/227/final

[21] NIST. *Module-Lattice-Based Digital Signature Standard*. FIPS 204. Final August 13, 2024; planning note July 31, 2026.
https://csrc.nist.gov/pubs/fips/204/final

[22] NIST. *Stateless Hash-Based Digital Signature Standard*. FIPS 205. Final August 13, 2024.
https://csrc.nist.gov/pubs/fips/205/final

[23] NIST. *Recommendation for Stateful Hash-Based Signature Schemes*. SP 800-208. October 2020.
https://csrc.nist.gov/pubs/sp/800/208/final

[24] UK National Cyber Security Centre. *Timelines for migration to post-quantum cryptography*. March 20, 2025.
https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[25] European Commission. *Post-quantum cryptography*. Policy page. Updated October 20, 2026.
https://digital-strategy.ec.europa.eu/en/policies/post-quantum-cryptography

[26] EU NIS Cooperation Group, PQC workstream. *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*. Part 1, version 1.1. Published June 23, 2025.
https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[27] National Security Agency. *NSA announces post-quantum cryptography measures to safeguard national security*. Press release, October 1, 2026.
https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4615285/nsa-announces-post-quantum-cryptography-measures-to-safeguard-national-security/

[28] National Security Agency. *Commercial National Security Algorithm Suite 2.0 and Quantum Computing Frequently Asked Questions*. Version 2.2. October 2026.
https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

[29] Canadian Centre for Cyber Security. *Recommended contract clauses for cryptography*. ITSM.00.501. September 2025.
https://www.cyber.gc.ca/en/guidance/recommended-contract-clauses-cryptography-itsm00501

[30] RFC Editor. *Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3*. RFC 10024. August 2026, Proposed Standard.
https://www.rfc-editor.org/rfc/rfc10024.html

[31] Google Cloud. *Post-quantum TLS for Cloud Load Balancing*. Last updated November 9, 2026.
https://docs.cloud.google.com/load-balancing/docs/post-quantum-tls

[32] NIST. *Module-Lattice-Based Digital Signature Standard*. FIPS 204 full text, key and signature size table.
https://nvlpubs.nist.gov/nistpubs/fips/NIST.FIPS.204.pdf

[33] AWS. *AWS KMS developer guide: hybrid post-quantum TLS*.
https://docs.aws.amazon.com/kms/latest/developerguide/pqtls.html

[34] NIST. *NIST selects HQC as fifth algorithm for post-quantum encryption*. March 2025.
https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

[35] RFC Editor. *IP Fragmentation Avoidance in DNS over UDP*. RFC 9715. January 2025, Informational.
https://www.rfc-editor.org/rfc/rfc9715.html

[36] Internet Engineering Task Force. *Post-Quantum Cryptography Recommendations for TLS-based Applications*. draft-ietf-uta-pqc-app-03. July 4, 2026, Internet-Draft.
https://datatracker.ietf.org/doc/draft-ietf-uta-pqc-app/

[37] TELUS. *TELUS launches Quantum-Safe VPN service*. Media release, November 14, 2025.
https://www.telus.com/en/about/news-and-events/media-releases/telus-launches-quantum-safe-vpn-service

[38] CycloneDX. *Cryptography Bill of Materials*. Capability page; version and date from the release announcement, CycloneDX v1.6 Released, April 9, 2024.
https://cyclonedx.org/capabilities/cbom/
https://cyclonedx.org/news/cyclonedx-v1.6-released/

[39] NIST National Cybersecurity Center of Excellence. *Migration to Post-Quantum Cryptography*. SP 1800-38B, preliminary draft. December 2023.
https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf

Post-Quantum Cryptography in Canada: Requirements, Standards and Vendor Readiness. Version 1.0, 10 November 2026.
Sources checked 7 to 10 November 2026.
General information.
© 2026 Junior Williams. All rights reserved. trustcyber.ca