

Quantum Standards

Development, Maturity, and Strategic
Implications for IP and Standardization
Professionals

Table of Contents

- Executive Summary
- Introduction
- Quantum Standards: Two Distinct Tracks, Two Different Speeds
- The Standards Development Landscape
- Who Is Developing Quantum Standards
- Inside ISO/IEC JTC 3
- Maturity Stage by Domain
- Approved Standards: Post-Quantum Cryptography
- Approved Standards: Quantum Communication Networks
- Strategic Takeaways: IP and Competitive Intelligence Framing
- Conclusion
- References

Executive Summary

Quantum standardization is advancing unevenly across two distinct fronts. Post-quantum cryptography, the set of classical algorithms designed to withstand attack from future quantum computers, has reached an advanced and largely settled stage, with approved federal standards now driving enterprise migration on fixed government timelines. Quantum key distribution networking has likewise produced approved, in force international standards that establish how quantum secured connections can be built into multi node networks rather than single point to point links.

By contrast, the broader family of quantum technologies, including quantum computing, advanced quantum networking beyond key distribution, sensing, and metrology, remains at an early and largely pre-competitive stage. Working groups in these domains were formed only recently, terminology is still being settled, and very few deliverables have reached publication. This is a white space in which standard essential patent landscapes are still forming rather than consolidating.

For organizations engaged in [freedom to operate](#) analysis, [patent landscaping](#), and [standard essential patent](#) strategy, this divergence carries a clear implication. Post-quantum cryptography and quantum key distribution networking are the only binding, published quantum-adjacent standard set, with active compliance implications. At the same time, the early stage of quantum computing and quantum sensing standardization represents an opportunity to monitor and position ahead of consolidation, before working group drafts harden into adopted requirements. This white paper sets out the current state of the standards landscape, the bodies driving it, the maturity of each domain, and the intellectual property implications that follow.

1. Introduction

The phrase quantum standards is often used as though it describes a single, coherent body of work. In practice it spans two families of technology that sit at very different points of maturity, are governed by different institutions, and carry different implications for organizations tracking freedom to operate and standard essential patent exposure. Treating them as one undifferentiated category risks either overstating the certainty of the quantum computing landscape or understating the urgency of compliance obligations already in force for post-quantum cryptography.

This white paper draws a clear line between the two tracks, maps the institutions developing quantum related standards, and sets out where each domain currently sits on the path from new work item to published standard. It closes with an assessment of what this means for intellectual property strategy, including where competitive intelligence effort is best directed today and where geopolitical fragmentation is likely to shape outcomes over the coming years.

2. Quantum Standards: Two Distinct Tracks, Two Different Speeds

The phrase “quantum standards” is often used as if it described a single, unified effort. In practice it spans two families of work that sit at very different maturity levels, are driven by different organizations, and carry very different implications for patent strategy.

1. Post-Quantum Cryptography

Classical algorithms engineered to resist attack from a future quantum computer. This is the most mature corner of the field. Approved, published and in several jurisdictions mandatory-track standards already exist, enterprise migration is underway now on government set deadlines, and it is the highest-priority space for [freedom to operate](#) and [standard essential patent](#) work today.

2. Quantum Technologies Proper

Quantum computing, quantum communication and quantum key distribution, quantum sensing, and quantum metrology. This family is still in development or at the terminology stage. Very few approved and published standards exist, the industry remains fragmented, working groups have only recently formed (2024 to 2026), and it represents pre-competitive white space where the standard essential [patent landscape](#) is still forming.

The practical consequence of this divide is that a single quantum standards monitoring program cannot treat both tracks with the same cadence or the same evidentiary bar. Post-quantum cryptography requires active compliance tracking against binding deadlines. Quantum technologies proper require early-stage horizon scanning, where the value lies in identifying which working group contributions, terminology choices, and draft architectures are likely to shape the eventual standard essential patent landscape.

3. The Standards Development Landscape

Work spans a spectrum, from foundational terminology and security guidance through to interoperable quantum networks and, eventually, quantum computing.

1. Quantum Communication

- The ITU-T Y.3800 series establishes foundational terminology, architecture and functional requirements for networks supporting quantum key distribution (QKD).
- ETSI ISG QKD develops implementation-oriented specifications covering QKD components, interfaces, security requirements and network interoperability.
- IEEE activities span quantum communications, computing, terminology, performance characterization and interoperability.

2. Quantum-Safe Security

- NIST finalized major post-quantum cryptography standards for quantum-resistant key establishment and digital signatures; these complement QKD rather than replace it.
- ETSI and other standards development organizations address quantum-safe migration, hybrid security, and integration of quantum-resistant mechanisms into telecom and IT infrastructure.

3. Quantum Computing

- ISO/IEC JTC 1 and IEEE address quantum computing terminology, concepts, performance characterization, reference architecture and interoperability.
- The standards ecosystem is progressively moving from high-level frameworks toward measurable technical requirements and implementation profiles.

4. Who Is Developing Quantum Standards

A layered landscape: one international flagship committee, plus regional, national, and sector bodies.

1. ISO/IEC JTC 3

ISO/IEC JTC 3 is the flagship of the quantum standards landscape. It is a joint committee formed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), established in January 2024, with its inaugural plenary held in Seoul in May 2024^{[1][2]}. Its scope covers quantum computing, quantum communication, quantum sensing, quantum metrology, and quantum sources and detectors^[3].

2. ISO/IEC JTC 1 (SC 27)

ISO/IEC JTC 1, Subcommittee 27, is responsible for the security certification of quantum key distribution systems within the Common Criteria framework. This subcommittee predates JTC 3 and produced the ISO/IEC 23837 quantum key distribution standards^{[4][5]}.

3. NIST (USA)

The United States National Institute of Standards and Technology leads global post-quantum cryptography standardization, having finalized FIPS 203, 204, and 205^[6]. NIST also administers the United States national committee to ISO/IEC JTC 3^[2].

4. ETSI

The European Telecommunications Standards Institute runs an Industry Specification Group on quantum key distribution. ETSI ISG QKD is a major industry led forum for quantum key distribution specifications, security requirements, interfaces, and deployment guidance^[7].

5. CEN-CENELEC (FGQT) · EU

CEN-CENELEC, through its Focus Group on Quantum Technologies, sets the European regional standardization roadmap^[8]. Standardization work in this area is being funded through the EU Quantum Flagship and the EuroHPC Joint Undertaking, with an open call for proposals running through 2026 and 2027^[9].

6. ITU-T

The International Telecommunication Union develops international telecom Recommendations covering quantum key distribution network terminology, architecture, functional requirements, security, and interoperability. This work is particularly important for telecom operators and for future quantum secure network infrastructure.

7. IEEE

The Institute of Electrical and Electronics Engineers (IEEE) develops engineering standards and technical frameworks spanning quantum computing, communications, performance characterization, and interoperability. IEEE work can become particularly relevant where mandatory interfaces or measurable technical requirements are adopted.

5. Inside ISO/IEC JTC 3

As of February 2026, ISO/IEC JTC 3 comprises eight working groups, two project teams, and two advisory groups. The committee's structure reflects a deliberate progression from informal ad hoc coordination, which began in 2025, toward formal working group output. The eight working groups cover terminology and quantities, quantum computing terminology and quantities, quantum sensors, quantum computing supply chain, quantum computing benchmarking, quantum random number generators, quantum enabling technology, and quantum communication.

The two project teams are developing a technical report and a quantum photonics vocabulary, while the two advisory groups handle strategic planning and matters referred by the chair's advisory group. The committee's scope is deliberately bounded. It explicitly excludes sector specific applications, information technology security (which remains the province of JTC 1), semiconductors, fibre optics, cryogenic vessels, and nanotechnology, each of which is coordinated with the relevant existing committee.

6. Maturity Stage by Domain

Standards progress through a well-established sequence, illustrated below, running from a new work item through early development, committee draft, and draft international standard, to final publication.

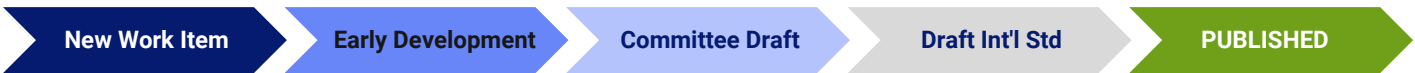


Figure 1. The standard development sequence used to assess each quantum domain.

Mapping each quantum domain against this sequence produces a clear and, for intellectual property purposes, actionable picture of where binding obligations already exist and where the landscape remains open.

DOMAIN	STAGE	STATUS
Post-quantum cryptography	MATURE / PUBLISHED	Final FIPS approved Aug 2024; migration enforced to 2030
Quantum communication – QKD networks	MATURE / PUBLISHED	ITU-T Y.3800 approved Oct. 2019; Y.3801 approved Apr. 2020; both currently In force
QKD security certification	EMERGING → PUBLISHED	ISO/IEC 23837 parts finalized under Common Criteria
Quantum terminology & vocabulary	EMERGING → PUBLISHED	ISO/IEC 4879 done; more vocabulary drafting active
Quantum computing (benchmarking, supply chain)	EARLY DEVELOPMENT	WGs active since 2025, drafting stage
Quantum sensing / metrology	NASCENT	WGs formed, very few deliverables yet
Quantum communication (beyond QKD)	NASCENT	WG formed, foundation stage

Table 1: Relative maturity of quantum standardization by domain, as of 25th August 2026.

Two domains, post-quantum cryptography and quantum key distribution networking, sit at the mature and published end of this scale, with standards already in force and, in the case of cryptography, active enforced migration. QKD security certification and quantum terminology sit in an intermediate position, moving from emerging work toward publication. The remaining domains, quantum computing benchmarking and supply chain, quantum sensing and metrology, and quantum communication beyond key distribution, remain in early development or nascent stages, with working groups formed but very few deliverables yet produced.

7. Approved Standards: Post-Quantum Cryptography

The post-quantum cryptography standards approved by the United States Secretary of Commerce, effective 24 August 2024, represent the culmination of an eight-year evaluation process that began in 2016.

Standard	Function	Algorithm
FIPS 203 (ML-KEM)	Primary encryption and key exchange standard, replacing RSA and ECDH.	CRYSTALS-Kyber
FIPS 204 (ML-DSA)	Primary digital signature standard, lattice based.	CRYSTALS-Dilithium
FIPS 205 (SLH-DSA)	Backup signature standard, based on hash functions.	SPHINCS+

Table 2. Approved FIPS post-quantum cryptography standards and their originating algorithms.

FIPS 203, based on the CRYSTALS-Kyber algorithm, is the primary general-purpose standard for encryption and key exchange, intended to replace RSA and elliptic curve Diffie-Hellman methods, and is specified across three security levels. FIPS 204, based on CRYSTALS-Dilithium, is the primary digital signature standard, offering smaller signatures and faster operations than earlier candidates. FIPS 205, based on SPHINCS+, serves as a backup signature scheme whose security rests solely on the properties of hash functions, providing resilience through a different underlying assumption than the lattice based primary standard. Two further items remain in the pipeline. FN-DSA, based on the FALCON algorithm, is a fourth signature standard drafted after the initial three. HQC was selected in March 2025 as a non lattice based key encapsulation mechanism intended to serve as a backup to ML-KEM, and is heading toward formal standardization [11]. Both are worth tracking, since a backup standard reaching publication can itself become a locus of new patenting activity distinct from the primary lattice based approaches.

8. Approved Standards: Quantum Communication Networks

Outside cryptography, the most mature, published standards address the architecture of quantum key distribution networks rather than the cryptographic algorithms themselves.

ITU-T Y.3800, approved in October 2019, provides a high-level conceptual overview of networks supporting quantum key distribution [12]. Its significance lies in how it extends the QKD network model beyond a simple point-to-point system: quantum key distribution was traditionally limited to a simple point-to-point system connecting only two devices. Y.3800 establishes a blueprint for connecting multiple devices into a full network, allowing keys to be relayed safely across long distances and shared among many users who are not directly linked by a single quantum channel.

ITU-T Y.3801, approved in April 2020, builds on this foundation by setting out the functional requirements for quantum key distribution networks [10]. Where earlier quantum security systems worked only as a direct link between two specific machines, Y.3801 provides the rules necessary to scale these connections into large, interconnected networks capable of spanning entire cities or countries while safely connecting many locations at once. Both standards remain in force today and, together with the post-quantum cryptography standards described above, represent the only binding, published quantum-adjacent standard set currently in effect.

9. Strategic Takeaways: IP and Competitive Intelligence Framing

1. Post-Quantum Cryptography and QKD Networking Are the Priority Now

Post-quantum cryptography and quantum key distribution networking are the only binding, published quantum-adjacent standard set. FIPS 203, 204, and 205 are approved and already in enforced migration under the Commercial National Security Algorithm Suite 2.0 timeline, which runs through 2030. ITU-T Y.3800, approved in October 2019, and Y.3801, approved in April 2020, are both currently in force. This is the highest-priority space for freedom to operate and standard essential patent analysis right now.

2. Quantum Computing, Sensing, and Communication Remain Pre-Competitive

Quantum computing, sensing, and communication remain pre-competitive. The field is still at a terminology stage today, and standard essential patent landscapes are still forming. The white space to watch most closely sits in the benchmarking, supply chain, and interoperability standards now being drafted in JTC 3.

3. Geopolitical Fragmentation Is a Live Risk

Geopolitical fragmentation is a live risk. Parallel efforts are underway across NIST in the United States, CEN-CENELEC in the European Union, the international ISO/IEC JTC 3 process, and national bodies in China, Japan, and Korea. This creates divergence risk, mirroring standard essential patent dynamics already seen in other technology domains.

For organizations building or refining a quantum standards monitoring program, these three points suggest a two-speed approach. Compliance-grade tracking, including deadline monitoring, essentiality mapping, and licensing exposure analysis, should be applied now to the mature cryptography and networking tracks. Horizon scanning, including working group participation tracking, draft terminology analysis, and early patent landscaping, should be applied to the computing, sensing, and broader communication tracks, with the expectation that monitoring intensity will need to increase as JTC 3's working groups move from early development toward committee drafts over the next two to three years, against a backdrop of continuing geopolitical fragmentation across the major standards jurisdictions.

10. Conclusion

Quantum standardization today is best understood as two tracks moving at two distinct speeds rather than a single unified field. Post-quantum cryptography and quantum key distribution networking have already produced binding, published standards, with active enforced migration underway on fixed timelines. This is the domain demanding immediate compliance-focused attention from any organization conducting [freedom to operate](#) or [standard essential patent analysis](#) in the quantum space.

Quantum computing, sensing, and the broader field of quantum communication beyond key distribution remain in an early, pre-competitive stage, with working groups only recently formed and very few deliverables yet published. This is not a reason to deprioritize the field. It is, instead, the clearest signal available that the standard essential patent landscape in these domains is still being written, and that organizations positioned to monitor, engage, and act early are the ones best placed to navigate the consolidation likely to follow over the coming years, against a backdrop of continuing geopolitical fragmentation across the major standards jurisdictions.

11. References:

1. ISO, IEC and ISO launch new joint technical committee on quantum technologies, January 2024. <https://www.iso.org/news/new-joint-committee-quantum-technologies>
2. NIST, New IEC/ISO Joint Technical Committee on Quantum Technologies, Inviting Participants for the U.S. National Committee Technical Advisory Group, February 2024. <https://www.nist.gov/news-events/news/2024/02/new-ieciso-joint-technical-committee-quantum-technologies-inviting>
3. ISO, ISO/IEC JTC 3, Quantum technologies, committee page. <https://www.iso.org/committee/10138914.html>
4. ISO/IEC 23837-1:2023, Information security, Security requirements, test and evaluation methods for quantum key distribution, Part 1. <https://www.iso.org/standard/77097.html>
5. ISO/IEC 23837-2:2023, Information security, Security requirements, test and evaluation methods for quantum key distribution, Part 2. <https://www.iso.org/standard/77309.html>
6. NIST, Post-Quantum Cryptography FIPS Approved, Computer Security Resource Center, August 2024. <https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved>
7. ETSI, Industry Specification Group on Quantum Key Distribution (ISG QKD). <https://www.etsi.org/technical-groups/qkd/>
8. CEN-CENELEC, Quantum Technologies topic page, Focus Group on Quantum Technologies. <https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies/>
9. EuroHPC Joint Undertaking, Standards for Quantum Technologies, call topic HORIZON-JU-EUROHPC-2026-STAND-05-01. https://www.eurohpc-ju.europa.eu/standards-quantum-technologies_en
10. ITU-T, Recommendation Y.3801, Functional requirements for quantum key distribution networks, April 2020. <https://www.itu.int/rec/T-REC-Y.3801/>
11. 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>
12. ITU-T, Recommendation Y.3800, Overview on networks supporting quantum key distribution, October 2019. <https://www.itu.int/rec/T-REC-Y.3800/>

Visit Us: www.iebrain.com

Contact Us: contact@iebrain.com

INDIA (HQ)

207-208, Welldone Tech Park
Sohna Road, Sector 48,
Gurugram, Haryana 122018
Phone No. +91 124 429 4218

USA

8 The Green, Suite B, Dover, DE
19901

Phone No. +1 302 450 1418

UK

5, Brayford Square, London, E1
0SG

Phone No. +44 770 014 9056

