

QUANTUM CORE INSTITUTE

QCI-PN-01

Quantum Key Distribution: A Position Note

Why QKD is not a substitute for post-quantum cryptography governance

Document ID	QCI-PN-01
Version	1.1
Status	Published — Free to download and cite
Publisher	Quantum Core Institute (QCI)
Normative ref	QCI-QS1 Version 2.3 (September 23, 2026). This note explains a scope boundary of the standard. It does not modify it. Clause references are QCI requirement identifiers.
Effective date	September 23, 2026
Review cycle	Annual, or upon material NSA, NCSC, or EU agency QKD guidance change, or a new edition of QCI-QS1

QCI's position is short. Quantum Key Distribution is not a substitute for post-quantum cryptography, and it is not a quantum-readiness action under QCI-QS1. It is a narrow, hardware-based link-protection technology with a real but small set of uses, none on the critical path of a migration program. This note states why, so the question does not have to be relitigated in every engagement.

What changed in version 1.1

Version 1.1 aligns this note to QCI-QS1 version 2.3. The crypto-agility reference in section 3 pointed to a clause number the standard does not use; it now points to gate G80 and the test requirements of QCI-4.7. Section 3 also states where QKD sits relative to the approved cryptographic profile of QCI-4.5-01, and section 6 restates the rule in the terms of the exposure-flag and treatment records of QCI-5.3. The agency positions in section 4 are now tied to the references in QCI-QS1 Annex E. The position itself is unchanged.

1. The position

Where a client already runs QKD, QCI-QS1 treats it as a compensating control on the specific links it protects, documented and owned, never as evidence of readiness and never as a reason to move a score. QKD protects one hop of one link. A quantum-readiness program is about signatures, credentials, and trust chains across the whole institution, and QKD does nothing for any of those. The migration is still the work.

2. What QKD is, and what it is not

QKD uses the physics of quantum states to distribute symmetric keys between two endpoints, with tampering detectable in principle because measuring a quantum state disturbs it. That is the whole of it. It exchanges keys. It does not encrypt data, it does not sign anything, and it does not prove who is on the other end of the fiber.

The consequences of that narrow function are easy to miss under the marketing. QKD has no native authentication, so it must be bootstrapped with classical or post-quantum authentication anyway, which means it inherits the very cryptography it is sometimes sold as replacing. It runs over dedicated fiber or free-space optics. It is distance-limited without trusted relays or quantum repeaters, and repeaters do not yet exist at scale. It needs special-purpose hardware at both ends. It is a point-to-point key pipe, not a network security architecture, and it cannot be routed across the internet the way public-key cryptography can.

3. Why QKD sits outside QCI-QS1 scope

QCI-QS1 governs cryptographic risk across an institution, and the standard's central finding is that the expensive exposure is authentication, not confidentiality. Signatures forged. Credentials minted. Nonrepudiation lost. QKD does nothing about any of that. It touches key exchange, which is the recoverable, bounded third of the problem.

A migration program that adopted QKD would still hold every quantum-vulnerable signature, certificate, and credential chain it started with. Scoring a readiness program upward because a QKD link exists would be measuring the wrong thing. That is why QKD does not appear in the QASI record set as a mitigation for signing exposure, does not satisfy any Q-Risk Score pillar, and does not pass gate G80. G80 lifts only on a representative end-to-end test of an algorithm change over a critical trust pathway under QCI-4.7, completed within the last 12 months, and a QKD deployment is not that.

The approved cryptographic profile makes the boundary explicit. QCI-4.5-01 requires each organization to hold a profile listing the algorithms and constructions it permits for key establishment, signatures, and hashing, and QCI-4.5-03 governs how hybrid key establishment is constructed and what it falls back to. QKD is not an algorithm and does not belong in that list. Where a link uses QKD-derived keys, the profile records it as a restricted mechanism on named

links, alongside the classical or post-quantum authentication that bootstraps it, and the profile's key-establishment method for everything else is unchanged. A profile that named QKD as its key-establishment method would fail the requirement, because it would have no method for any link QKD does not reach.

4. What the security agencies actually say

This is the mainstream read, not a contrarian one, and a standards body that cites these agencies as authority elsewhere does not get to ignore them here. QCI-QS1 Annex E carries the references.

- The U.S. National Security Agency does not support QKD for National Security Systems and does not anticipate certifying QKD products unless the current limitations are overcome. It points to post-quantum cryptography as the more practical and maintainable path, and the CNSA 2.0 guidance the standard cites (Annex E, S14) sets out that path without QKD.
- The U.K. National Cyber Security Centre recommends post-quantum cryptography as the primary mitigation and considers QKD unsuitable for government and military use, citing implementation vulnerabilities and the difficulty of securing complex integrated systems (Annex E, S16 and S18).
- France's ANSSI, Germany's BSI, and the Dutch and Swedish national authorities put the clear priority on migration to post-quantum cryptography and place QKD in a small set of niche uses for now, while encouraging continued research to overcome its limitations. The EU Coordinated PQC Roadmap (Annex E, S17) sets the migration calendar those authorities apply.

5. Where QKD does fit

There is a real place for it, and honesty about the limits makes the real case stronger. QKD earns its keep on a small number of high-value, fixed, fiber-connected links where both endpoints are known and controlled: sovereign network backbone, links between an organization's own data centers, and the national infrastructure the EU is building under the European Quantum Communication Infrastructure (EuroQCI) and the IRIS2 secure-connectivity programme.

The emerging consensus is a blend, not a contest. QKD at the link where it is available, post-quantum cryptography at the session and the application everywhere else. QKD protects one hop. PQC protects the transaction end to end, on the same regulator-driven clock that runs to the 2030 and 2035 migration deadlines. Quantum random number generation, a cousin often bundled into QKD pitches, is treated more favorably by the same agencies as a source of entropy, but it too is a component, not a governance action.

6. The rule for a QCI-QS1 program

The rule is clean. QKD is an enabler, never a readiness action, and it never appears on the critical path. A client that has deployed it records it in the QASI as a compensating control on the specific links it protects, with a named owner and a review date, exactly as the standard treats network segmentation where cryptography cannot yet change. In the standard's terms: the exposure flag on the link (QCI-5.3-01) stays raised, the QKD deployment is recorded as treatment (QCI-5.3-02) once its operation and its authentication bootstrap have been verified, and the flag clears only when the link's key establishment moves to an approved post-quantum

method. It does not substitute for migrating the signatures, the certificates, or the credentials, and it does not move the Q-Risk Score.

How to use this note

Hand it to anyone who asks whether QKD changes the plan. It does not. The danger is not the technology, it is the marketing around it, which invites institutions to believe they can buy their way out of a migration with a photon box. They cannot. The plan is post-quantum cryptography, governed, inventoried, and scored. QKD is at most a specialized layer on a handful of links after that work is underway.

Revision history

Version	Date	Changes
1.1	September 23, 2026	Aligned to QCI-QS1 v2.3: crypto-agility reference corrected to gate G80 and QCI-4.7; position relative to the approved cryptographic profile (QCI-4.5-01, 4.5-03) added; rule restated in exposure-flag and treatment terms (QCI-5.3); agency positions tied to Annex E references. Position unchanged.
1.0	June 10, 2026	First edition, aligned to QCI-QS1 v2.2.

Independent assessment against QCI-QS1 is performed by the Quantum Core Institute. Scope one at quantumcoreinstitute.com/independent-assessment. An independent assessment is not QCI certification (QCI-1.2-03).