QRCS: A Summary of Patent Potential, Licensing, and Value Projection

A brief study of the intellectual property profile, investment costs and potential value returns for the QRCS suite of protocols and libraries.

(QSC Library · HKDS · MPDC-I · QSMP · QSTP · PQS · SKDP)

Revision 1a, April 12, 2025

John G. Underhill – contact@qrcscorp.ca

Index

1. Patent Eligibility Assessment for Core Protocols

All six protocol constructions (HKDS, MPDC-I, QSMP, QSTP, PQS, and SKDP) implement post-quantum-secure cryptographic workflows at system or protocol level rather than at the level of primitive algorithms. In most jurisdictions (notably the USPTO, CIPO, JPO, KIPO and the Australian IPO) computer-implemented architectures that provide a *technical effect* beyond mere calculation remain patent-eligible. The EU/EPO is stricter, but software that "solves a technical problem in a novel, non-obvious way" is still patentable.

1.1 Patent Premise and Supported Conclusions

Across the set we see multiple patent-supportable themes:

Theme	**Appears in**	**Why it is patent-supportable**

Two-key forward-secure symmetric derivation	HKDS, SKDP	Combines an immutable embedded key with an ephemeral token key to generate per-transaction caches, removing DUKPT scalability limits and providing post-quantum security. This *architectural coupling* is absent from prior art.
Distributed entropy injection by authenticated agents	MPDC-I	Multi-party domain agents each contribute encrypted key fragments that are recombined into session keys, thwarting man-in-the-middle even by quantum adversaries. No centralized MPC scheme today uses *symmetrically encrypted fragments keyed by pre-exchanged master fragment keys (mfk)*.
Root-signed certificate hierarchy for quantum-safe tunnelling	QSTP	Classical SSH/TLS rely on two-party exchanges; this protocol adds a *domain controller / root-server third party* to bind lattice-based keys into lightweight tunnels with <4 kB state, providing scalability that existing PQC VPNs lack.
Secure messaging (Simplex & Duplex) Peer-to-peer communications streams	QSMP	• *Simplex*: client→server one-way trust, 256-bit tunnel, 2 RTT setup • *Duplex*: mutual auth, combines two secrets into 512-bit channel • Built-in keep-alive & error model • Explicit forward secrecy & replay protection
One-way trust simplex exchange with Kyber/Dilithium	PQS	A *server-only* authenticity model lowers client complexity and allows massive fan-out. This is distinct from SSH or Signal double-ratchet.

1.2. Individual Construction Analysis

Construct	Patent-relevant novelty	Prior-art risk	Suggested claim focus	US obviousness mitigation
HKDS	Two-key token system; hierarchical device/branch/master identifiers; PRF-generated “transaction-key cache” with forward & predictive resistance; KMAC-	DUKPT (VISA), ANSI X9.24-3; EMV key-management specs.	*Method* of deriving per-transaction symmetric keys using [a] static embedded key + [b] server-generated	Highlight 4×–8× throughput vs DUKPT and post-quantum security as unexpected

	authenticated remote token exchange.		encrypted token + [c] cSHAKE/Keccak PRF constraints; *System* of POS terminal + server.	technical benefit.
SKDP	Pure-symmetric two-party duplex tunnel with separate TX/RX shared secrets each generated by own endpoint; keeps pre-shared device keys secret yet provides forward secrecy; AEAD packet-header authentication using UTC “packet-valid-time”.	Double-ratchet, Noise-Symmetric.	Dual-direction independent secret derivation; time-bound packet authentication scheme.	Compare to TLS 1.3 requiring asym. ops; show lower computational load on embedded endpoints.
MPDC-I	Multi-agent fragment system (encrypted with per-pair *efk* derived from long-term *mfk*); agents add entropy without seeing final key; supports arbitrarily large agent sets with symmetric crypto only.	Threshold-ECDH MPC, MLS group key, Kerberos pre-auth.	Steps of requesting, encrypting, combining authenticated fragments; topology & certificate workflow.	Stress quantum-resilience + linear scalability as non-obvious over heavy MPC protocols.
QSTP	Three-party root-signed certificate + client-server tunnel; path-independent 256-bit quantum security; per-packet UTC anti-replay, dynamic proxy chaining governed by root.	TOR, WireGuard, OpenVPN-PQ patches.	Certificate workflow & proxy-mesh creation with Kyber/McEliece & RCS/AES-GCM tunnels having fixed-length packets.	Emphasize reduced latency versus layered TLS-style encryption.
PQS (Post-Quantum Shell)	One-way trust (client trusts server) simplex key-exchange; 4 kB per-client state.	SSH-2 “simplex” modes;	Lightweight registration + Kyber encapsulation framed inside	Argue improved load ability (hundreds k clients) as

		Google CECPQ1/2.	authenticated RCS/AES-GCM tunnel.	teaching away from prior art.
QSMP	Peer-to-peer quantum-safe messaging with authenticated receipt sequencing.	Signal protocol, MLS.	Unique integration of RCS wide-block cipher, Keccak ratchet.	Document concrete resource gains and quantum resistance.

1.3. Protecting the Portfolio – Procedural Guidance

1.3.1 Prior-art & freedom-to-operate search

- Run keyword and classification searches (USPTO CPC subclasses H04L 9/32; G06F 21/57—21/79).
- Compare against NIST PQC candidate implementation patents and well-known open-source licenses.

1.3.2 Filing sequence

- File **US provisional** for each construction capturing full protocol flow diagrams, state tables and performance metrics.
- Within 12 months, consolidate into a **PCT (WO)** with claims book split by construction. Use PCT multiple-dependent claims to keep examination cost low.
- Enter national phase: US, CA, EP, KR, JP, AU, SG; consider CN if export licenses allow.

1.3.3 Claim drafting strategy

- **Independent claim set A (method):** steps of key generation, authentication, tunnel operation.
- **Set B (system):** client, server/agent, root controller hardware configured to execute steps.
- **Set C (computer-readable medium):** executable instructions causing processors to perform method.
- For EU, add *further technical effect* language: “improves resistance to quantum cryptanalysis while halving memory bandwidth”.

1.3.4 Obviousness / inventive-step prosecution

- Prepare comparative throughput & resource charts (from C reference benchmarks) to supply as *secondary evidence of non-obvious technical effect*.
- Point out that combining *post-quantum primitives* with legacy scalability constraints yields unexpected synergies (e.g., HKDS token system overcomes DUKPT key-tree exhaustion).
- In OA response, rely on *Helmsley*/*DDR Holdings* line of cases in US and *T 641/00 (COMVIK)* at the EPO.

1.3.5 Open-source coexistence

- All specs cite closed educational-purposes-only proprietary license C code. Release code under adjusted license (commercial) *after* priority date to avoid self-collision.
- Keep patent scope on *system workflow*, allowing community to implement primitives freely.

1.4 Interim Conclusion

Each construction introduces at least one architecturally novel mechanism that is absent from existing cryptographic key-management or tunnelling standards. The strongest, most defensible claim sets lie in:

- **HKDS & SKDP** – token-based dual-key caches for high-volume payment and IoT devices.
- **MPDC-I** – scalable agent-assisted entropy injection without heavy MPC math.
- **QSTP & PQS** – quantum-safe VPN/SSH replacements delivering enterprise-grade certificate logistics.

Properly drafted, these innovations support a cohesive patent family that can be leveraged offensively (licensing) or defensively (cross-license shielding) as the post-quantum transition accelerates.

2. QSC Library Certification Path (standardized components only)

2.1 Certification Roadmap

The QSC C library implements approved primitives (AES, SHA-2/3, SHAKE, KMAC) and soon-to-be-approved PQC algorithms (ML-KEM, ML-DSA). A pragmatic certification roadmap is:

1. **Scope & gap analysis**
   Define cryptographic boundary, roles/services, RNG/entropy sources.
   2 weeks, ~US $5 k consulting.
2. **Algorithm validation (CAVP)**
   Submit each enabled primitive in QSC to an NVLAP lab using ACVTS.
   – SHA-3/SHAKE/KMAC AVCs.
   – AES modes AVCs.
   – Add ML-KEM & ML-DSA once ACVTS test vectors are published (target 2025).
   Cost: **US $10 k–25 k** per primitive set; NIST fee $0.
3. **Entropy Source Validation (ESV)** *(QSC embeds DRBG / RNG)*
   Adds ~US $7 k–15 k lab cost.
4. **FIPS 140-3 module testing**
   Level 1 software-only module covering libqsc.
   - Documentation (Security Policy, finite-state machine, roles & services).
   - Lab evidence & penetration testing.
   - Submission to CMVP.
     NIST CR/ECR: **US $8 k–10 k + 3 k–4 k**. [1]
     Lab: **US $60 k–120 k**; timeline 9–14 months including CMVP review queue.
5. **Maintenance strategy**
   Use CMVP Scenario 1A for minor code updates (US $2 k CR, $1 k ECR; minimal retest). [4]
6. **Global re-use**
   After US/CA validation, pursue **CSEC (Sweden) and BSI (Germany) recognition** via the Cryptographic Module Validation Program reciprocity list to avoid duplicate testing.

Outcome: A single **FIPS 140-3 Level 1 certificate** covering the QSC core plus individual AVL certificates for each algorithm gives OEMs an “out-of-the-box” compliant crypto library, dramatically lowering integration overhead for HKDS, MPDC-I, QSMP, QSTP, PQS and SKDP deployments in regulated markets.

2.2 Patent cost–value outlook for the six constructions

Protocol family	**Expected patent families †**	**Draft-to-grant cost ‡**	**Comparable deal / benchmark**	**Distinctiveness & overlap leverage**	**10-year value outlook §**
HKDS	3–4 (token hierarchy, dual-key cache, predictive-resistant derivation, remote entropy renewal)	US $70 k – 110 k (PCT + US/CA/EP)	VISA DUKPT vs Certicom ECC: Certicom sold for **US $106 M** (≈ US $300 k per patent) [5]	Replaces DUKPT in payments, overlaps with PCI PTS, FIDO, post-quantum POS.	**High** – royalties on every POS/HSM with PQ tokenization; blocking position against "PQ-DUKPT" clones.
MPDC-I	4–5 (agent fragment scheme; mfk/efk envelope; symmetric MPC session fusion; topology-aware revocation)	US $90 k – 140 k	MPC start-ups typically command 5-10× revenue multiples; no public sale comps yet.	Only scheme offering PQ multi-party key exchange **without** lattices; reusable for IoT mesh, 6G edge, AI federated learning.	**Very high** – platform-level standard candidate; likely to attract cross-license offers from cloud & telco vendors.
QSMP	2–3 (RCS wide-block ratchet; authenticated receipt sequencing)	US $50 k – 80 k	Signal patent-free but trademark-restricted; few blocking patents on secure-messaging transports.	Clear delta from double-ratchet; may cover "post-quantum Signal" evolutions.	**Moderate** – enforcement depends on adoption volume; good defensive asset.
QSTP	2–3 (root-signed proxy mesh; fixed-size PQ VPN packets;	US $60 k – 90 k	WireGuard's negligible patent shield leaves space;	Distinct packet structure & root-control layer could read	**High-moderate** – licensing to security

	UTC anti-replay)		quantum-VPN patent families emerging since 2023 [6]	on future SASE/Zero-Trust VPNs.	gateways, 5G/6G slices, automotive OTAs.
PQS	2 (one-way trust simplex KEM+signature; 4 kB client state swap)	US $40 k – 70 k	SSH patents expired 2006; no blocking art on PQ simplex shells.	Ideal to cover lightweight IoT/SCADA remote shells; incremental to OpenSSH PQ extensions.	**Moderate** – niche but strategic; bundling with HKDS or MPDC increases leverage.
SKDP	2 (dual-direction symmetric KDF; packet-valid-time AAD)	US $35 k – 60 k	Few pure-symmetric tunnel patents exist; Certicom licence to General Dynamics underscores military appetite [7]	Low-cost embedded VPN, zero-asym-crypto edge devices; complements HKDS in constrained nodes.	**Medium** – valuable for MCU/RTOS vendors; cross-license bargaining chip.

† Independent claim sets with 20 claims each, assuming one provisional + PCT consolidation.
‡ Includes attorney, USPTO/EPO/CA fees and first-phase national filings (US / CA / EP). Sources: industry cost surveys [8].
§ Indicative potential: *High ≥ US $25 M*, *Moderate US $5–25 M*, *Medium < US $5 M* net present value from licensing, defensive settlements or acquisition uplift.

2.3 FIPS algorithm-level standardization & validation costs (SHA-3, AES, Dilithium/ML-DSA & Kyber/ML-KEM)

Algorithm	Current FIPS status	Validation pathway	Typical direct costs*	Typical elapsed time

SHA-3 family (SHA-3-224/256/384/512, SHAKE128/256, KMAC)	Approved in FIPS 202 (2015).	CAVP ACVTS testing – submit implementation to an NVLAP lab. Algorithm Validation Certificate (AVC) issued. Feed AVC into FIPS 140-3 module submission.	• Lab ACVTS fee ≈ US $10 k–25 k • NIST algorithm fee = $0 (CAVP) [1]	1–3 months for algorithm cert, excludes module queue
AES-128/192/256 (ECB, CBC, GCM, CCM, XTS)	Approved in FIPS 197; modes in SP 800-38A/B/D/E/F.	Same CAVP→AVC process as SHA-3.	• Lab ACVTS fee ≈ US $8 k–20 k • NIST fee = $0	1–3 months
Kyber → ML-KEM	Final FIPS 203 issued Aug 2024. [2]	NIST to add ML-KEM KAS-KEM test suites to ACVTS (expected Q4 2025). NVLAP labs begin validations. AVC feeds FIPS 140-3.	• First-wave lab pilot fees typically higher: US $20 k–40 k • NIST fee = $0 (algorithm)	6–9 months once ACVTS live
Dilithium → ML-DSA	Final FIPS 204 issued Aug 2024. [3]	ACVTS adds ML-DSA digital-signature tests (parallel to FIPS 186-5 ECDSA tests). Lab validation → AVC.	• Lab fee ≈ US $20 k–35 k • NIST fee = $0	6–9 months

*Costs are for algorithm certificates only; they exclude full FIPS 140-3 module fees. When the validated algorithm is rolled into a module, NIST cost-recovery fees apply (CR = certificate review, ECR = engineering review): **US $8 k–10 k CR + US $3 k–4 k ECR** for most Level 1–3 scenarios. Lab effort for a Level 1 software crypto module typically ranges **US $50 k–150 k** depending on boundary complexity [1].

2.4 Future value drivers

- **Standardization tail-winds** – FIPS and NIST PQ transition will force vendors to redesign key-management and tunnelling stacks; families that read on those redesigns (HKDS, MPDC-I, QSTP) gain blocking power.

- **Adjacency expansion** – MPDC-I’s agent-fragment concept generalizes to cloud MPC wallets, federated-AI weight encryption and zero-trust credentials; HKDS dual-key cache maps to automotive firmware chains.
- **Portfolio synergy** – Bundling SKDP (symmetric tunnel) with HKDS (token derivation) or PQS (shell) creates platform licenses attractive to OEMs who prefer a one-stop PQ stack, raising royalty rates.
- **Litigation posture** – Cryptographic portfolios historically command strong settlements (e.g., RSA’s 900-licensee program; ECC royalties to US DoD via Certicom). Such precedents underpin valuation multiples. [5]
- **Market growth** – The quantum-secure market is projected to rise from ≈ US $0.1 B (2022) to > US $3 B by 2030 [6], lifting royalty pools.

2.5 Risk & mitigation

Risk	Impacted families	Mitigation
Prior-art assertions from open-source PQC codebases	PQS, QSTP	Claim workflows, not primitives; keep code dual-licensed post-priority.
Rapid standards convergence reducing design freedom	SKDP	File broadly on packet-valid-time + dual secret directions now; maintain continuations.
Cost overruns in multi-jurisdiction prosecution	All	Stage filings: US-only first, expand when commercial traction proven; use Patent Prosecution Highway for EP/JP/KR.

2.6 Bottom-line

The **HKDS and MPDC-I** families exhibit the highest distinctiveness and cross-industry reach, justifying a **strategic-value focus** and broad jurisdiction coverage. **QSTP** offers strong mid-term licensing potential in VPN/Zero-Trust markets, while **PQS, QSMP and SKDP** deliver tactical value and defensive depth at lower cost. A staggered filing strategy, prioritizing HKDS → MPDC-I → QSTP, maximizes return on IP investment while maintaining optionality for the remaining constructions.

3. Value Proposition of a FIPS-approved, third-party-certified QSC Library

3.1 Why FIPS validation matters

A FIPS 140-3 certificate is mandatory for all U.S.-federal procurements that "use cryptography" and is rapidly becoming a de-facto requirement in defense, finance, healthcare and critical-infrastructure supply chains ("FIPS Inside" model). Vendors that cannot ship a validated module must either license one or invest 9-18 months and > US $100 k in fees to certify their own. [9] *QSC* offers a ready-made, boundary-defined software module that already includes classic (AES, SHA-2/3, KMAC) **and** the new NIST-standardized post-quantum algorithms ML-KEM (Kyber) and ML-DSA (Dilithium). That first-mover position removes an adoption road-block for any OEM facing the 2027–2030 federal PQC migration deadline.

3.2 Primary use-cases

Sector	How QSC is consumed	Example value delivered
Cloud & SaaS	Drop-in *FIPS provider* shared by all micro-services (OpenSSL-style).	Avoid separate validations per service; FedRAMP/FedRAMP-High compliance. [10]
IoT / embedded / automotive	Static-linked Level 1 module in firmware images.	Meets DoD supplier rules; enables firmware OTA signing with ML-DSA.
Mobile & desktop OS	System crypto API (similar to Red Hat OpenSSL provider).	Lets OEM ship a single validated base while updating the OS weekly.
Payment & fintech stacks	Underpins HKDS tokenization and SKDP tunnels.	PCI PTS acceptance without duplicating DUKPT hardware keys.
Industrial & SCADA	Supplies PQ-safe VPN (QSTP) and shell (PQS) channels.	NERC-CIP alignment; quantum-resilient remote maintenance.

3.3 Revenue mechanisms

1. **Per-SKU perpetual license** – market standard is **US $7 k–10 k per product** (wolfSSL charges $7.5 k).
2. **Annual support & maintenance** – 15-25 % of license value, covering algorithm updates and certificate upkeep.

3. **Validation-as-a-Service (VaaS)** – QSC team extends its certificate to a customer's OS/CPU in ~60 days, billed at **US $30 k–50 k** plus NIST/OE fees (mirrors SafeLogic model).
4. **Bundled protocol royalties** – discounted packages when QSC is used with HKDS, MPDC-I, QSTP, etc., raising overall ASP and stickiness.

A conservative model of **50 OEM licenses at US $9 k** each in the first three years produces **≈ US $0.45 M upfront** plus **US $90 k recurring/year**, scaling as PQC mandates bite.

3.4 Benchmarks & comparable transactions

Library / company	**Deal / metric**	**Implied valuation insight**
Certicom Toolkit	Acquired by BlackBerry for **US $106 M** (2009)	~US $300 k per patent + 6× revenue multiple for FIPS-validated ECC stack.
PrimeKey EJBCA	Merged with Keyfactor in 2021; **US $125 M growth round** to fund combined crypto/PKI platform	Shows investor appetite for "crypto-as-a-service" suppliers.
wolfCrypt	Commercial FIPS SDK at **US $7.5 k per SKU** with > 80 validated OEs	Proof that volume OEM licensing is sustainable for a lean library vendor.
Dell BSAFE	Continues as a FIPS-validated SDK inside Dell & VMware stacks	Demonstrates staying power and cross-portfolio integration value.

These comparables indicate that a lean library company with 10–15 engineers and a strong certificate pipeline can trade at **4–8× recurring revenue** or **> US $300 k per core patent** once adoption is visible.

3.5 Projected enterprise value for QSC

- **Short term (2025-27)** – Early FIPS-PQ module, 100 OEM SKUs, est. **US $1.2 M annual license + support** → EV **US $6–10 M** at 5–8× ARR.
- **Mid term (2028-30)** – PQC deadlines hit; library embedded in HKDS, MPDC-I reference designs; 500 SKUs; **US $6–8 M ARR** → EV **US $50–80 M**.

- **Exit paths** – Acquisition by an OS vendor (Red Hat, Canonical), silicon provider (NXP, Renesas) or a “crypto-ops” platform (Keyfactor, Venafi) seeking a validated PQC core.

3.6 Strategic advantages over competing tool-sets

- **First wave PQ–FIPS** – No commercial library today ships a FIPS-validated ML-KEM + ML-DSA module; QSC can capture “default” status.
- **Protocol lock-in** – Deep integration with the six patented constructions means OEMs who adopt QSC face minimal migration pain and higher switching cost.
- **Certificate agility** – By maintaining variant OE certificates (Linux, RTOS, bare-metal), QSC emulates wolfSSL’s broad coverage yet adds PQ primitives, widening addressable market to automotive and 5G edge that lack such options today.
- **Defensive IP umbrella** – QSC code plus the HKDS / MPDC-I / QSTP patents form a mutually reinforcing portfolio, discouraging competitors from clean-room re-implementation.

Bottom-line: a FIPS-approved, third-party-certified **QSC library** is a high-margin, rapidly scalable product whose market value is amplified by looming PQC compliance deadlines and by the library’s tight coupling to the broader QRCS protocol suite. When mapped against past library acquisitions and current licensing economics, QSC’s prospective enterprise value comfortably sits in the **US $50 M–US $100 M** range within the next five years—making it both a lucrative stand-alone revenue stream and a strategic acquisition target.

4. International Post-Quantum Migration Timeline

Post-quantum cryptography (PQC) is moving from research topic to regulatory mandate. Governments now recognize that adversaries may harvest encrypted traffic today and decrypt it once practical quantum computers arrive (“harvest-now-decrypt-later”). In response, the United States, Australia, Canada and the European Union have each published binding policies that require public-sector systems, and, by extension, suppliers in defense, finance, healthcare and critical infrastructure, to migrate to NIST-standardized PQC algorithms within the next decade. The following timeline graph summarizes these mandates, showing when hybrid deployments must begin and when classical public-key algorithms will be formally retired. Organizations that understand this schedule can better plan inventories, hybrid roll-outs and full cut-overs, and can gauge the value of ready-made, FIPS-validated tool-sets such as the **QSC** library.

4.1 PQ migration Timelines by Jurisdiction

Jurisdiction	Binding mandates & guidance	Partial-migration phase (hybrid / crypto-agile)	Full-migration target
United States	National Security Memorandum-10 [11] OMB M-23-02 [12], Quantum Computing Cybersecurity Preparedness Act [13], NIST IR 8547 draft [14]	**2024-2029** — crypto inventory, dual-cert composites (RSA/ECC + ML-DSA), KEM-TLS pilots across FedRAMP clouds	**2030** deprecation of RSA-2048/ECC-256, **2035** disallowance; all federal systems PQC-only [14]
Australia	ASD *Planning for PQC* [15], Information Security Manual update [16]	**2024-2027** — agency inventories, hybrid VPN & PKI pilots, annual ASD algorithm list	**2030** Commonwealth entities PQC-by-default; critical infrastructure by **2032** [15][16]
Canada	CSE bulletin *Preparing for the quantum threat* [17], ISED National Quantum Strategy roadmap [18], GC Enterprise Cyber-Security Strategy [19]	**2025-2032** — Treasury Board crypto inventory, hybrid cert roll-out in GC PKI, Kyber VPN pilots	**2032-2035** PQC mandatory for Secret-level traffic; provinces follow within 2-3 years [17][19]
European Union	Commission Recommendation on a Coordinated PQC Roadmap [20], ENISA PQC mitigation report [21], NIS2 Directive transposition deadline [22]	**2025-2029** — hybrid TLS & S/MIME in NIS2-sector operators, EU-funded composite-cert pilots	**2029** PQC default for “crypto-critical” sectors; draft Digital Resilience Act proposes **2035** union-wide ban on vulnerable algorithms [20][21]

4.2 Migration strategies

Partial (2024-2029)

- Inventory & risk-tiering of all crypto systems.

- Deploy hybrid certificates and KEM-TLS sessions.
- Build crypto-agility layers using libraries such as QSC.
- Run limited-scope PQC tunnels and signing pilots.

Full (2030-2035)

- Deprecate and disable RSA/ECC in roots of trust and firmware.
- Re-encrypt archives with ML-KEM-wrapped keys; reissue PKI anchors with ML-DSA.
- Integrate PQC monitoring into FIPS/CC recertification cycles and maintain algorithm agility.

Key takeaway: Formal policies in the U.S., Australia, Canada and the EU converge on PQC-in-production by the early 2030s and complete elimination of quantum-vulnerable public-key algorithms by 2035. Early hybrid roll-outs and crypto-agile tooling are essential to avoid last-minute compliance cliffs.

Conclusion

QRCS's portfolio positions the company at the confluence of three accelerating curves: **(i)** the statutory drive to eliminate quantum-vulnerable public-key algorithms by 2030-2035, **(ii)** the near-term shortage of FIPS-validated post-quantum tool-sets, and **(iii)** the market's demonstrated willingness to pay strategic premiums for cryptographic patents and certified libraries.

- **Patent strength and breadth.** HKDS and MPDC-I supply heavyweight, system-level claims that read directly on high-volume verticals; payments, IoT, cloud key-management, while QSTP, PQS, QSMP and SKDP populate the defensive perimeter with focused, low-cost filings. Together they form a **balanced patent stack** capable of both blocking imitators and attracting cross-licence negotiations with incumbents.
- **Certification catalyst.** The forthcoming **FIPS 140-3 certificate for QSC** is more than a compliance checkbox; it is a commercial accelerant. By bundling validated primitives with protocol licences, QRCS can deliver an end-to-end "PQC inside" offering that OEMs can integrate in weeks rather than quarters—exactly when migration timelines (§4) begin to bite.
- **Revenue realism.** Conservative OEM-licence scenarios already support a **US $50–100 million enterprise valuation** for QSC alone within five years. Layering protocol royalties, validation-as-a-service fees and defensive-settlement upside lifts the blended IRR well beyond comparable security-software exits.
- **Execution roadmap.** Immediate priorities are clear:

1. **Lock priority dates**—file the staged provisional set for HKDS → MPDC-I → QSTP this quarter.
2. **Complete QSC validation**—target CMVP submission within nine months to retain first-mover status.
3. **Pilot deployments**—seed three reference integrations (payments terminal, IoT gateway, SaaS micro-service) to generate field metrics that reinforce non-obviousness arguments and de-risk customer adoption.

- **Strategic optionality.** Whether QRCS pursues organic growth, a platform partnership or a full acquisition, the IP and certification artifacts outlined in this paper are structured to compound in value: every new hardware port, every licence, every additional jurisdictional filing increases both royalty flow and defensive leverage.

In short, **QRCS controls a uniquely synergistic mix of patents, certified software and protocol designs that map directly onto mandatory government timetables**. Executed with disciplined prosecution and targeted go-to-market pilots, this portfolio can secure durable revenue streams today and command outsized strategic premiums tomorrow.

References

1. NIST Cryptographic Algorithm Validation Program CAVP. NIST Computer Security Resource Center
2. NIST Announcing Issuance of Federal Information Processing Standards (FIPS) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard NIST Publications
3. NIST FIPS 204 Module-Lattice-Based Digital Signature Standard NIST Publications
4. Recent and Upcoming Changes in the CMVP 2020-09 atsec.com
5. BlackBerry Maker Acquires Certicom For $106 Million InformationWeek
6. Quantum Cryptography Growth: The Latest Data on Post-Quantum Security PatentPC
7. Certicom licenses Intellectual Property to General Dynamics certicom.com
8. How Much Does a Software Patent Cost? Pricing Breakdown From Top Patent Lawyers Gearhart Law, LLC
9. FIPS Inside: Is It Right For Me? corsec.com
10. FIPS - Federal Information Processing Standards access.redhat.com

11. National Security Memorandum-10, *Promoting U.S. Leadership in Quantum Computing while Mitigating Risks to Vulnerable Cryptographic Systems*, May 4 2022. The White House

12. OMB Memorandum M-23-02, *Migrating to Post-Quantum Cryptography*, Nov 18 2022. The White House

13. **Public Law 117-260**, *Quantum Computing Cybersecurity Preparedness Act*, Dec 21 2022. Congress.gov

14. NIST Interagency Report 8547 (initial public draft), *Transition to Post-Quantum Cryptography Standards*, Oct 2024. NIST Computer Security Resource Center

15. Australian Signals Directorate, *Planning for Post-Quantum Cryptography*, May 2023. Cyber.gov.au

16. Australian Cyber Security Centre, *Information Security Manual* (Dec 2024) — post-quantum update. Cyber.gov.au

17. Communications Security Establishment, *Preparing Your Organization for the Quantum Threat to Cryptography*, Mar 2024. Canadian Centre for Cyber Security

18. Innovation, Science and Economic Development Canada, *National Quantum Strategy Roadmap: Quantum Communication & PQC*, Feb 2025. ISED

19. Government of Canada, *Enterprise Cyber Security Strategy* (web update), Oct 2024. Canada.ca

20. European Commission, *Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, Apr 3 2024. Digital Strategy

21. ENISA, *Post-Quantum Cryptography: Current State and Quantum Mitigation*, Mar 2024. ENISA

22. European Commission, *NIS2 Directive information page* — Member-State transposition deadline Oct 17 2024. Digital Strategy