Post Quantum Shell (PQS)

Revision: 2.0
Date: October 2025
Author: John G. Underhill
Document Type: QRCS Executive Summary
Keywords: PQS, post-quantum SSH replacement, remote access security, Kyber, Dilithium, RCS, Keccak, PQC

1. Overview

The **Post Quantum Shell (PQS)** is a post-quantum secure remote shell protocol designed to succeed SSH in environments where long-term confidentiality, identity assurance, and cryptographic durability are paramount. PQS eliminates classical dependencies on RSA and ECDH by employing lattice, code-based, and hash-based primitives that remain secure even against quantum adversaries.

The protocol establishes a **one-way trust model**; clients authenticate servers via post-quantum certificates, removing the need for bilateral credential storage while preserving strong mutual data integrity. Each session uses **ephemeral asymmetric keys**, deriving short-lived symmetric channels through **SHAKE-based KDFs** and authenticated **RCS stream ciphers**. This architecture achieves constant-time, replay-resistant communication capable of scaling to hundreds of thousands of concurrent tunnels on a single host.

In essence, PQS is not merely an evolution of SSH, it is a re-foundation of secure remote access for the quantum era.

2. Motivation and Strategic Rationale

The rise of **quantum computing** threatens every classical cryptographic foundation upon which global digital infrastructure depends. SSH, TLS, and VPN frameworks based on elliptic-curve or RSA primitives will be rendered obsolete once large-scale quantum systems emerge.

PQS was conceived to **future-proof the global command, control, and administration layer** of networked systems. Its purpose is twofold:

1. Provide immediate defense-in-depth against hybrid classical-quantum attack vectors.

2. Ensure that future migrations toward quantum-safe infrastructures can occur **without operational disruption**.

For governments, enterprises, and fintech operators, this represents strategic insulation against a systemic cryptographic collapse, an event whose mitigation cost would otherwise exceed the value of most national data infrastructures. PQS therefore positions itself as an **asset-class technology**, defining the secure backbone for post-quantum operations across finance, defense, and cloud ecosystems.

3. Architecture and Mechanism

At its core, PQS implements the **QSMP Simplex Key Exchange**, a three-phase handshake providing authenticated key agreement, forward secrecy, and integrity-bound initialization.

- **Asymmetric Primitives:**
  - **Kyber** or **McEliece** for IND-CCA-secure encapsulation.
  - **Dilithium** and **SPHINCS+** for EUF-CMA digital signatures.
- **Symmetric Cipher: RCS (Rijndael Cryptographic Stream):** a wide-block, Keccak-expanded AEAD cipher with KMAC-based authentication.
- **Hash and KDF Layer:** SHA-3 and SHAKE derive all session keys, nonces, and MAC keys deterministically from per-session entropy.
- **Session Control:** A 21-byte packet header embeds sequence, UTC timestamp, and message size, enforcing replay and downgrade protection.
- **Performance:** Under measured conditions, PQS achieves sub-millisecond key exchanges (≈0.9 ms LAN) and multi-gigabit throughput (≈9 Gb/s @ RCS-256).

Each tunnel's cryptographic context (< 4 KB per client) supports horizontally scalable server deployments. A structured flag system governs session transitions from Connect → Exchange → Establish—and supports optional **ratchet updates** to refresh keys post-compromise, extending the model beyond SSH's static session paradigm.

4. Security Model and Post-Quantum Posture

PQS security derives from **standard hardness assumptions:**

- IND-CCA for Kyber/McEliece,

- EUF-CMA for Dilithium/SPHINCS+,
- PRF-security for SHAKE/KMAC, and
- the cryptanalytic strength of RCS as a 256-/512-bit AEAD cipher.

The protocol satisfies authenticated-key-exchange goals under the **Canetti–Krawczyk model**, guaranteeing:

- **Server Authenticity:** Acceptance implies a verified post-quantum signature under the certified key.
- **Key Secrecy & Forward Secrecy:** Ephemeral encapsulation keys ensure each session key is indistinguishable from random and unrecoverable after use.
- **Replay and Downgrade Resilience: Sequence** + UTC fields inside every MAC'd header enforce time-bounded message validity.
- **Post-Compromise Security:** Optional asymmetric and symmetric ratchets restore confidentiality after key rotation.

By combining a minimal code surface (~12 k LOC) with constant-time reference implementations, PQS significantly reduces side-channel exposure relative to OpenSSH's ≈180 k LOC footprint. The result is a system verifiable by formal methods and hardened against both classical and quantum attack models.

5. Implementation and Integration

PQS integrates directly into the **QRCS cryptographic stack**, leveraging existing **RCS**, **Keccak**, and **KMAC** primitives from the QSC library. It requires no external PKI beyond a single **root-signed certificate** for server identity, simplifying deployment in sovereign or air-gapped infrastructures.

The protocol is designed for drop-in replacement of SSH in POSIX environments, supporting socket-based communications and certificate serialization. Integration targets include:

- Secure DevOps pipelines and CI/CD automation.
- Encrypted administration channels for virtualized and bare-metal servers.
- Embedded agents within IoT or industrial systems where code size and deterministic timing are critical.

Because PQS maintains X.509 compatibility for certificate chains, organizations can migrate incrementally, retaining existing certificate management workflows while gaining post-quantum assurance.

6. Use Cases and Applications

Financial Technology (Fintech):
Quantum-secure transaction processing and encrypted exchange gateways safeguard long-term financial records and digital assets.

Government and Defense:
Protects classified channels, control networks, and cross-domain communications from future quantum decryption.

Healthcare and Bioinformatics:
Ensures HIPAA-compliant protection of patient data and secure remote access to medical instrumentation.

Critical Infrastructure:
Secures SCADA, power, and transportation networks against replay or impersonation attacks.

Cloud and Enterprise IT:
Provides high-density, quantum-safe administrative access for hyperscale data centers, replacing SSH without degrading performance.

Across all sectors, PQS enables **long-term confidentiality horizons**, measured in decades, not months, making it an indispensable component of sustainable cybersecurity strategy.

7. Economic and Operational Value

Deploying PQS yields measurable returns:

- **Operational Efficiency:** Low handshake latency and small memory footprint reduce compute cost per secure session.
- **Lifecycle Savings:** Avoids future emergency migrations triggered by quantum-era cryptanalytic breaks.

- **Compliance and Liability Reduction:** Aligns with upcoming NIST PQC standards (FIPS 203 / 204), pre-empting costly retrofits.
- **Licensing and IP Leverage:** As QRCS-owned, PQS represents an acquirable asset with intrinsic patent and code value, its defensible originality in post-quantum key-exchange architecture positions it as a cornerstone technology for acquirers seeking strategic foothold in PQC infrastructure.

For cloud providers, financial networks, or defense integrators, PQS enables secure scalability without cryptographic obsolescence, preserving both data integrity and shareholder value.

8. Long-Term Security Benefit

Beyond corporate advantage, PQS advances the public good by ensuring the **continuity of trust in digital infrastructure**. As communications, energy grids, and medical systems become quantum-vulnerable, PQS offers a verifiable and open-standards path to resilience.

Its adoption mitigates the risk of a "cryptographic black swan"; a sudden systemic failure of privacy guarantees, by embedding quantum-resistant protections at the very layer where human and machine identities interact. In doing so, PQS contributes to the ethical and societal imperative of preserving privacy, safety, and institutional continuity in the post-quantum age.

9. Conclusion

PQS represents the culmination of QRCS's commitment to quantum-resilient infrastructure: a protocol that marries engineering precision with strategic foresight. By combining Kyber, McEliece, Dilithium, SPHINCS+, Keccak, and RCS into a cohesive and efficient architecture, PQS delivers a practical, verifiable replacement for SSH that is ready for global deployment today.

Its demonstrable scalability, mathematically grounded security, and straightforward interoperability make it a prime acquisition target for organizations seeking **technological defensibility** and **market differentiation** in the coming quantum transition.

PQS is not merely a safeguard, it is the foundational instrument through which the next generation of secure communication will be conducted.

Prepared by: Quantum-Resistant Cryptographic Solutions
Contact: contact@qrcscorp.ca