QRCS Certification Path Document

Version: 1.0
Date: May 2025
Author: John G. Underhill
Organization: Quantum Resistant Cryptographic Solutions Corporation (QRCS)

1. Overview

This document outlines the certification strategy for multiple post-quantum cryptographic protocols developed by QRCS Corporation. Each protocol targets specific security domains, from financial transactions to secure remote access. They are designed using the post-quantum cryptographic primitives implemented in the QSC Library. The protocols include:

- **SKDP** – Symmetric Key Distribution Protocol
- **PQS** – Post-Quantum Shell
- **HKDS** – Hierarchical Key Distribution System
- **QSMP** – Quantum Secure Messaging Protocol
- **QSTP** – Quantum Secure Tunneling Protocol

All protocols are supported by an extensive suite of Known Answer Tests (KATs), a robust test framework, and MISRA-compliant implementations.

2. SKDP – Symmetric Key Distribution Protocol

Application in Financial Systems:

- Suitable for POS and ATM communications, replacing asymmetric key exchanges.
- Session-based ephemeral key exchange ensures forward secrecy.
- Message integrity is guaranteed using KMAC with AEAD.

Certification Strategy:

- Aligns with FIPS 202, SP 800-185, ISO 16609, ISO 9797-1, and ANSI X9.8-1.
- Supports PCI DSS for secure channel transmission.
- KATs cover RCS, SHAKE, and KMAC.

Hardware Security Module (HSM):

- Stores derivation key securely.
- Performs ephemeral key generation and message authentication within secure boundaries.

Advantages:

- No asymmetric cryptography: low resource requirement.
- Forward secrecy and predictive resistance.
- Session keys are derived independently per direction.

3. PQS – Post Quantum Shell

Application:

- Replacement for SSH in secure admin, fintech, and cloud operations.
- Supports certificate-based server authentication and ephemeral key exchange.
- Efficient for thousands of concurrent sessions.

Standardization and Certification:

- FIPS 202, 203, 204, SP 800-185 for SHA3, Kyber, Dilithium, SPHINCS+.
- Integration-ready for PCI DSS, ISO 9798, and ISO 8583.
- TLS-like tunneling capabilities with superior PQ resistance.

Implementation Flexibility:

- RCS is default AEAD cipher, but **AES-GCM** is supported for environments requiring simpler standardization paths.

Cert Path:

- CAVP test vectors for asymmetric/symmetric components.
- FIPS 140-3 if integrated with certified HSMs or secure firmware.

4. HKDS – Hierarchical Key Distribution System

Use Case:

- Replacement for DUKPT in financial transaction systems.
- Performs derivation of transaction keys using SHAKE + embedded device key + ephemeral token.

Certifiability:

- ISO 9797-1, ISO 16609, ISO 8583, ANSI X9.8-1 compliant.
- Rooted in symmetric cryptography (no lattice or code-based dependence).
- Hardware-backed secure key storage (e.g., FIPS 140-3 certified devices).

Formal Cryptanalysis:

- Detailed in Annex C of the HKDS spec.
- Predictive resistance, forward secrecy, and MAC binding ensured.

Regulatory Goals:

- PGA certification (e.g., VISA, EMVCo).
- Interoperability with payment networks and host systems.

5. QSMP – Quantum Secure Messaging Protocol

Overview:

- Peer-to-peer encrypted messaging protocol.
- Uses Kyber or McEliece for key encapsulation and Dilithium/SPHINCS+ for signature auth.
- RCS or AES-GCM for symmetric message protection.

Certification Plan:

- FIPS 202 (SHA3), SP 800-185 (KMAC), SP 800-56C (KDFs).
- ISO 9798-4 (entity authentication), ISO 16609 (MAC for financial messaging).

Security Measures:

- Anti-replay via message timestamps and sequence counters.
- Independent ephemeral keys per session.
- Compatible with mobile, embedded, and critical infrastructure platforms.

6. QSTP – Quantum Secure Tunneling Protocol

Overview:

- Authenticated client-server protocol using root-signed certificates.
- Designed for secure remote access, mobile banking, and VPN tunnels.

Compliance Targets:

- ISO 9798-4 (auth), ISO 8583 (banking), SP 800-185 (KMAC), FIPS 203 (Kyber).
- PCI DSS for encrypted transmission of cardholder data.

Key Features:

- Stateless key derivation with ephemeral keys.
- Fast session setup with <4 KB memory footprint per session.
- RCS default; AES-GCM as optional cipher.

Certifications in Scope:

- FIPS 140-3 (underlying crypto module).
- ANSI X9, ISO TC68, EMVCo submission for financial-grade usage.

7. QSC Library – Certification Foundation

Contents:

- Implements all cryptographic primitives used by SKDP, PQS, HKDS, QSMP, and QSTP.
- Written in MISRA-compliant C with AVX/AVX2/AVX512, AES-NI, and SIMD acceleration.

Certification Path:

- **FIPS 140-3**: Secure module boundary, integrity checks, role-based access.
- **CAVP**: Validation of SHA3, KMAC, AES, ChaCha, HKDF, Kyber, McEliece, SPHINCS+, and Dilithium.
- **Static Analysis**: Reviewed using Coverity, Polyspace, or Frama-C for safety.

Validation Artifacts:

- Known Answer Tests (KATs)
- Automated validation suite
- Security architecture and codebase documentation

8. Deliverables for Certification

- Full specifications and protocol documentation
- Known Answer Test suites and expected result files
- MISRA-C compliance report
- QSC FIPS module boundary and CAVP submissions
- Threat models and formal security analyses
- Platform integration test results (Windows, Linux, MacOS)
- Certificates and root trust configuration schema

9. Final Notes

All QRCS protocols are production-grade, with test coverage across core devices, unit tests, interop scenarios, and integration into financial-grade embedded environments. Default cipher is RCS, but **AES-GCM: Standardized AEAD mode (FIPS 800-38D) is supported**