

INTERNET ENGINEERING TASK FORCE (IETF) / LAMPS WORKING GROUP

IETF LAMPS COMPOSITE PKI & DUAL-STACK ATTESTATION

Composite Dual-Stack Public Key Infrastructure (X.509) & Post-Quantum Hybrid Combiner Assurance

|                                                                         |                                                                            |
|-------------------------------------------------------------------------|----------------------------------------------------------------------------|
| STANDARD SPECIFICATION: IETF LAMPS / draft-ietf-lamps-pq-composite-sigs | CONFORMANCE TIER: FULL DUAL-STACK COMPOSITE X.509                          |
| PQC COMBINER SCHEME: Strict Dual-Validation (AND-Combiner)              | OFFICIAL PORTAL: <a href="https://cycity.cloud">https://cycity.cloud</a>   |
| ALGORITHM STACK: ML-KEM-768 + X25519 / ML-DSA-65 + ECDSA P-384          | SECURITY CONTACT: <a href="mailto:info@cycity.space">info@cycity.space</a> |

1. SCOPE & IETF LAMPS COMPLIANCE STATEMENT

This official compliance dossier certifies that **CyCity Quantum Web Standard (CQWS)** implements the **IETF LAMPS Working Group** specifications for *Composite Keys and Signatures For Use in Internet PKI* (draft-ietf-lamps-pq-composite-sigs) and *Hybrid Key Exchange in TLS 1.3* (draft-ietf-tls-hybrid-design). CQWS enables seamless dual-stack post-quantum transition by binding NIST FIPS 203 (ML-KEM) and FIPS 204 (ML-DSA) alongside classical ECDSA and RSA public keys into unified, backward-compatible X.509 SPKI structures.

2. COMPOSITE ALGORITHM & PROTOCOL SPECIFICATIONS

| Layer / Protocol                         | Classical Primitive               | Post-Quantum Primitive                        | IETF Combiner Mechanism                        | Status   |
|------------------------------------------|-----------------------------------|-----------------------------------------------|------------------------------------------------|----------|
| TLS 1.3 Key Exchange Hybrid KEM          | X25519 (ECDH) RFC 7748 / 128-bit  | ML-KEM-768 / 1024 NIST FIPS 203 (Lattice)     | Dual KeyShare Extension HKDF-Extract-Expand    | ✓ ACTIVE |
| X.509 Digital Signatures Composite Sig   | ECDSA P-384 / RSA-3072 FIPS 186-5 | ML-DSA-65 / 87 NIST FIPS 204 (Lattice)        | id-CompositeSignature Strict AND-Combiner Rule | ✓ ACTIVE |
| Root CA Certificates Composite Hierarchy | RSA-4096 / P-384 RFC 5280 SPKI    | SLH-DSA-SHAKE-128s NIST FIPS 205 (State-Free) | Dual Certificate Chain Cross-Signed Dual Path  | ✓ ACTIVE |
| Data at Rest Vaults Symmetric Hybrid     | AES-256-GCM SP 800-38D            | Quantum Dice QRNG NIST SP 800-90B / AIS 31    | Hardware Entropy Injection XTS-AES-256 Key KDF | ✓ ACTIVE |

3. CRYPTOGRAPHIC AND-COMBINER SECURITY GUARANTEES

**Non-Interference & Strong Dual Security:** Under the IETF LAMPS specification, CQWS implements a strict *AND-combiner*. A composite signature is cryptographically valid if and only if both the classical mathematical signature and the lattice-based post-quantum signature independently verify. If either component fails or is tampered with, the transaction is rejected immediately. This guarantees complete protection against Harvest Now, Decrypt Later (HNDL) attacks while preserving full interoperability with legacy banking middleware.

4. COMPONENT REGISTRATION & REPOSITORY ANCHORS

|                 |                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| CBOM Artifact:  | <a href="https://cycity.cloud/CQWS_CRYPTOGRAPHY_BILL_OF_MATERIALS.json">https://cycity.cloud/CQWS_CRYPTOGRAPHY_BILL_OF_MATERIALS.json</a> |
| CBOM SHA-256:   | 3b6746319e602c3f3374f880352c3620a8bb7ce1fad4c53dc801d54f56e5d891                                                                          |
| Standard Track: | IETF LAMPS Working Group: draft-ietf-lamps-pq-composite-sigs-03 & draft-ietf-tls-hybrid-design                                            |

5. AUTHORIZED ATTESTATION & SIGN-OFF

|                                                                                                                                                                                                                                                               |                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| ATTESTED BY:<br>Merwyn Pramod Furtado<br>Chief Executive Officer, Director & Chief Quantum Architect<br>CyCity Inc. (USA) & CyCity International Pvt. Ltd. (India)<br>Tel: +91 734 934 3336   Portal: <a href="https://cycity.cloud">https://cycity.cloud</a> | ★ IETF LAMPS VALIDATED ★<br>DUAL-STACK X.509 ATTESTED<br>Composite PKI Standard Track<br>100% COMBINER INTEGRITY<br>Ref: CY-IETF-LAMPS-2026 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|