

CYCITY INC. (USA) & CYCITY INTERNATIONAL PRIVATE LIMITED

NIST ACVP ALGORITHM VECTOR VALIDATION REPORT

Automated Cryptographic Validation Protocol Test Suite (4,100 / 4,100 Vectors Passed Across 13 Primitives & QRNG)

TEST SESSION ID: ACVP-CYCITY-2026-FIPS203-204-PROD-v3	ALGORITHM VECTORS TESTED: 4,100 / 4,100 PASSED (0 Failed, 0 Bit Flips)
TESTED ENGINE: CyCity Quantum Web Standard (CQWS) v4.2-PROD	VERDICT: 100.0% NIST VECTOR CONFORMANT (13 ALGORITHMS + QRNG)
TEST HARNESS: NIST Automated Cryptographic Validation Protocol (ACVP v1.0)	REPORT HASH (SHA-256): 4ff22af2113ec6fe...592a01b1bb15

1. EXECUTIVE SUMMARY & TEST METHODOLOGY

Self-tested against official NIST ACVP and CAVP vector suites, **4,100 / 4,100 algorithm test vectors passed with 0 failures and 0 bit flips**. The cryptographic algorithm implementations within **CyCity Quantum Web Standard (CQWS)** execute all official **NIST Known Answer Tests (KATs)**, seed expansions, Monte Carlo stress tests, and Fujisaki-Okamoto (FO) error-rejection vectors. Full coverage spans Post-Quantum Cryptography (**FIPS 203 ML-KEM, FIPS 204 ML-DSA, FIPS 205 SLH-DSA**), Classical Asymmetric & Hybrid (**RSA-2048/3072, ECDSA P-256, X25519**), Symmetric Authenticated Ciphers (**AES-128/256-GCM**), Cryptographic Hashes (**SHA-256, SHA3-512, SHAKE-256**), and physical entropy via Quantum Dice DISC™ under **NIST SP 800-90B / AIS 31** (NIST ESV Program). Fully conformant with ActaSeal CBOM semantic validation.

2. COMPREHENSIVE ALGORITHM VECTOR TEST RESULTS BREAKDOWN (14 SUITES)

Standard & Algorithm	Parameter Set & Security Level	Vector Types Tested	Vectors	Status
NIST FIPS 186-5 RSA-2048	2048-bit Modulus Legacy Classical (112-bit eq.)	SigGen, SigVer (PKCS#1 v1.5 / PSS), Decapsulation	300	✓ PASSED
NIST FIPS 186-5 RSA-3072	3072-bit Modulus Classical Asymmetric (128-bit eq.)	SigGen, SigVer, CRT KeyGen, Modulus Validation	250	✓ PASSED
NIST FIPS 186-5 ECDSA / secp256r1	256-bit Prime Field (P-256) NIST Level 1 (128-bit eq.)	KeyGen, KeyVer, SigGen, SigVer, Edge Cases	300	✓ PASSED
RFC 7748 X25519	Curve25519 Montgomery ECDH Key Exchange (128-bit eq.)	Scalar Multiplication, RFC 7748 KAT Vectors	200	✓ PASSED
NIST FIPS 197 AES-128-GCM	128-bit Key / 96-bit IV SP 800-38D Authenticated	Encrypt/Decrypt KATs, GMAC Auth Tag Verification	250	✓ PASSED
NIST FIPS 180-4 SHA-256	256-bit Cryptographic Hash Collision Resistance (128-bit eq.)	Short/Long Msg KATs, Monte Carlo, Byte Alignment	200	✓ PASSED
NIST FIPS 203 ML-KEM-768	k=3 (Lattice KEM) NIST Level 3 (AES-192 eq.)	KeyGen KAT, Encaps/Decaps, FO Implicit Rejection	250	✓ PASSED
NIST FIPS 203 ML-KEM-1024	k=4 (Lattice KEM) NIST Level 5 (AES-256 eq.)	KeyGen Seed Expansion, Encaps/Decaps Vectors	200	✓ PASSED
NIST FIPS 204 ML-DSA-65	(k,l)=(6,5) (Lattice Sig) NIST Level 3 (AES-192 eq.)	Pure & Hedged Sign, Verify (+), Tamper Rejection (-)	300	✓ PASSED
NIST FIPS 204 ML-DSA-87	(k,l)=(8,7) (Lattice Sig) NIST Level 5 (AES-256 eq.)	KeyGen KAT, Deterministic Sign, Verification (+/-)	250	✓ PASSED
NIST FIPS 205 SLH-DSA-SHAKE-128s	Stateless Hash Signature NIST Level 1 (AES-128 eq.)	SHAKE-256 KeyGen, Tree Hash Verification	100	✓ PASSED
NIST FIPS 197 AES-256-GCM	256-bit Key / 96-bit IV NIST Level 5 (Ring-0 L3/L4)	Line-Rate Netfilter Encap/Decap, Auth Tag Verification	250	✓ PASSED
NIST FIPS 202 SHA3-512 / SHAKE-256	Keccak-p[1600] / XOF NIST Level 5 (256-bit Collision)	Variable Output Length, XOF Matrix Sampling KATs	250	✓ PASSED
NIST SP 800-90B (ESV) Quantum Dice QRNG	Photonic Quantum Entropy NIST ESV Validated (H ≥ 7.999)	Repetition Count (RCT), Adaptive Proportion (APT), SP 800-22	1,000	✓ ESV PASS

3. CHECKSUM & PUBLIC AUDIT ANCHORS

Raw ACVP Test JSON:	https://cycity.cloud/CQWS_NIST_ACVP_VECTOR_TEST_REPORT.json
SHA-256 Checksum:	4ff22af2113ec6fe9563e7b0f632a899a6a5786c86e14b60bd97592a01b1bb15
Standard Reference:	NIST CAVP / ACVP Special Publication 800-140C & Draft ACVP RFC (ActaSeal 1.1.0 Verified)

4. AUTHORIZED ATTESTATION & EXECUTIVE SIGNATURE

ATTESTED BY: Merwyn Pramod Furtado Chief Executive Officer, Director & Chief Quantum Architect CyCity Inc. (USA) & CyCity International Pvt. Ltd. (India) Inquiries: info@cycity.space Portal: https://cycity.cloud	★ PRE-VALIDATION COMPLETE ★ FIPS 203 / 204 / 205 CONFORMANT 4,100 / 4,100 Algorithm Vectors Passed CAVP Validation In-Progress Accredited NVLAP CST Lab Engagement
---	--