QUEY

True Random Entropy as a Service

NIST Validation Certificate

Cryptographic validation of the Quey hardware entropy pipeline against the U.S. National Institute of Standards and Technology test suites SP 800-22 Rev 1a and SP 800-90B.

VERDICT: VALIDATED

Identification

Pipeline tested	Quey v2 (capture → LSB extraction → Von Neumann debiasing → SHA3-256 conditioning)
Hardware source	Sony IMX708 NoIR CMOS sensor on Raspberry Pi 5, in light-isolated enclosure
Physical phenomenon	Photonic shot noise and dark current in total darkness
Date of validation	8 May 2026
Validation operator	Aaron Loeb, founder & technical lead
Certificate issued	19 May 2026

Test 1 — NIST SP 800-22 Rev 1a (Statistical Test Suite)

The 15-category statistical test suite was executed on 100 MB of conditioned pipeline output, partitioned into 838 bitstreams of 1 million bits each.

Total test lines executed	188
Test lines passed	188 / 188
Minimum pass-rate observed	98.0 % (NIST threshold: 96.89 %)
Categories with 100 % pass	All 15
Result	**PASS**

Test 2 — NIST SP 800-90B (Entropy Source Validation)

Min-entropy estimation was performed on 1 million raw LSB samples extracted directly from the IMX708 sensor, prior to debiasing and conditioning. NIST convention takes the minimum across all non-IID estimators as the official value.

Min-entropy estimate (Most Common Value)	0.8804 bits/bit
Min-entropy estimate (Markov)	0.8811 bits/bit
Min-entropy estimate (T-Tuple)	0.7754 bits/bit
Min-entropy estimate (LZ78Y)	0.8804 bits/bit
Min-entropy estimate (Compression — bottleneck)	0.6236 bits/bit
OFFICIAL VALUE (minimum across estimators)	**0.6236 bits/bit**

Security Margin

The pipeline applies SHA3-256 conditioning on 1024-byte input blocks, producing 32-byte output blocks. Combined with the measured source min-entropy:

Source min-entropy	0.6236 bits/bit
Bits per conditioner input block	1024 × 8 = 8192 bits
Total entropy per input block	8192 × 0.6236 ≈ 5108 bits
Bits per conditioner output block	32 × 8 = 256 bits
Effective conditioning ratio	5108 / 256 ≈ 19.95×
NIST minimum recommended ratio	2×
Security margin over NIST minimum	**≈ 10×**

Methodology

Three independent binary samples were generated from three distinct stages of the pipeline, allowing each stage to be validated separately:

Sample	Stage	Size	Tests applied
raw_lsb	Before Von Neumann debiasing	128 MB	SP 800-90B
debiased	After Von Neumann, before SHA-3	32 MB	SP 800-90B
conditioned	Final pipeline output	100 MB	SP 800-22

Each binary sample is fingerprinted with SHA-256 and archived together with the raw test outputs, the tool versions (commit hashes), and the capture metadata. The validation is fully reproducible from these artifacts.

Tools used

NIST SP 800-90B EntropyAssessment	Official C++ binaries from github.com/usnistgov/SP800-90B_EntropyAssessment
NIST SP 800-22 STS	Statistical Test Suite version 2.1.2, official NIST distribution
Conditioning function	SHA3-256 (NIST FIPS 202), Python hashlib

Acknowledged limitations

In the interest of full disclosure, the following limitations of the present validation are documented:

• The validation was performed on the output of a single hardware unit. No cross-validation against a second identical device has yet been conducted.

• The IID hypothesis was rejected on the raw LSB sample, which is expected for a CMOS sensor (spatially neighboring pixels share readout electronics). NIST non-IID estimators were used as the official value, in line with NIST convention.

• Environmental robustness (temperature, vibration, power supply fluctuations) has not been quantified.

• Restart-test entropy correlation (ea_restart) has not been measured. Recommended for future certification work.

• This certificate attests to validation under SP 800-22 and SP 800-90B. It is not a FIPS 140-2/3 certification, nor a Common Criteria certification, nor an eIDAS qualification.

Issued by Aaron Loeb, on behalf of Quey

Founder & technical lead — queyquantum.io

The complete internal validation report (with raw test outputs, sample fingerprints, and methodology details) is available on request to qualifying parties.