

DCS LABS / R-SERIES · PRE-AUDIT EVIDENCE RECORD

FINAL VERDICT
PASS

NIST ACVP ML-DSA-65 (Post-Quantum)

Verifier vs NIST FIPS 204 reference vectors

SYSTEM

dcs-rseries-core

TEST SUITE

test/test_nist_acvp_mldsa65.mjs

FROZEN TAG

audit-tob-v1.1.0 · 697f339

REPRODUCED

27 Jul 2026

Closing metrics

16

IN-SCOPE PASSED

0

FAILURES

44

OUT-OF-SCOPE SKIPPED

stand-in

NOT YET CERTIFIED

What this run demonstrates

For the post-quantum signature type we use (ML-DSA-65), our checker matched the U.S. government standards body (NIST) reference answers on all 16 relevant test cases. Honesty note, in plain terms: the version running in production today is a stand-in that is the right size and shape but is NOT a certified post-quantum implementation — see the non-claim on page 2.

What this does not prove: A FIPS-certified post-quantum implementation. The deployed signing path uses a size-conformant ground stand-in, not certified hardware.

Technical verification record

Test file	test/test_nist_acvp_mlds65.mjs
In-scope vectors passed	16 of 16
Failures	0
Out-of-scope modes	44 skipped (parameter sets not used here)
Signer status	size-conformant ground stand-in — not FIPS-certified
Environment	Node v22.22.3 · clean checkout · 0 production dependencies
Frozen root	audit-tob-v1.1.0 · 697f339 (immutable)
Reproduced	27 Jul 2026 · live reproduction from a clean checkout
Test-file sha256	f91c404d16b16a33ffb9b78a0e0bb32e48ac79dbe0fb09bec1c4410c7a1c58dc
Final verdict	PASS — reproduced, no failures
Raw machine record	DCS_RSeries_NIST_ACVP_MLDSA65_Record.json

Complete test summary

- For the ML-DSA-65 modes the receipt layer uses, the verifier matches NIST's official ACVP accept/reject vectors, 16/16.
- The 44 skipped modes are parameter sets outside receipt-layer usage — out of scope, not failures.
- ACVP conformance validates the VERIFIER logic; the deployed SIGNING path uses a size-conformant ground stand-in (see non-claim).

Evidence scope & limitations

This document reports an internal, reproduced software test — not an operational service and not an external audit. A PASS verdict means the recorded test criteria were satisfied on the frozen code (tag audit-tob-v1.1.0 · commit 697f339) under the stated conditions. It does not establish flight qualification, operational deployment, certified post-quantum hardware roots, or independent external audit completion.

Post-quantum non-claim

The Post-Quantum (PQ) leg currently utilizes size-conformant ground stand-ins (pending formal NIST FIPS 204 ML-DSA / FIPS 205 SLH-DSA hardware security module certification). Not flight-qualified. Not independently audited by external third parties.