

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

FINAL VERDICT
PASS

Wycheproof Ed25519 Conformance

Signature checker vs Google's public adversarial vectors

SYSTEM

dcs-rseries-core

TEST SUITE

test/test_wycheproof_ed25519.mjs

FROZEN TAG

audit-tob-v1.1.0 · 697f339

REPRODUCED

27 Jul 2026

Closing metrics

150

VECTORS PASSED

0

FAILURES

150/150

EXACT MATCH

0

PROD DEPENDENCIES

What this run demonstrates

We tested our signature checker against Google's public library of 150 deliberately tricky test cases — the ones the security industry uses to catch bugs in this kind of software. It got all 150 right: it accepts valid signatures and rejects invalid or malformed ones.

What this does not prove: Anything about the post-quantum leg — this report covers classical Ed25519 only.

Technical verification record

Test file	test/test_wycheproof_ed25519.mjs
Vectors passed	150 of 150
Failures	0
Vector source	Google Project Wycheproof (public)
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	960c1c82a23c16cd5106a9d4c94688d192b2870dd32ae620094b0e06b40c9e11
Final verdict	PASS — reproduced, no failures
Raw machine record	DCS_RSeries_Wycheproof_Ed25519_Record.json

Complete test summary

- The verifier's accept/reject behaviour matches Google's Wycheproof Ed25519 vectors on all 150 edge cases.
- Coverage includes malformed encodings, small-order points, boundary values and known attack shapes.
- Valid signatures are accepted; invalid or malformed ones are rejected.

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.