

# Quality Benchmark & Validation Report (QBL)

## UISL2 Validator v2.1.0

Complete 20-Rule Enforcement & Performance Validation

---

**Report ID:** QBL-UISL2-V2.1.0-20260213

**Version Evaluated:** UISL2 Validator v2.1.0

**Date of Issue:** 2026-02-13

**Evaluation Environment:** Controlled local sandbox (Ubuntu 22.04 LTS, Python 3.8+)

**Prepared By:** Denny Michael LaFountaine

**Affiliation:** Quantum Labs Research & Development

---

## 1. Executive Summary

This Quality Benchmark & Validation (QBL) report documents the structured validation, regression testing, defect remediation, and performance benchmarking of the UISL2 Validator v2.1.0.

The objective of this evaluation was to:

1. Achieve enforceable coverage of all 20 Mandatory UISL Rules.
2. Correct identified structural defects.
3. Verify deterministic canonical byte generation.
4. Validate strict fail-closed behavior.
5. Benchmark sustained operational performance under load.

All findings are based exclusively on executed local tests within a controlled sandbox environment.

No external institutional certification is claimed.

---

## 2. Scope of Evaluation

The validation cycle included:

- Mandatory Rules 1–20 enforcement verification
- Critical defect remediation (4 structural fixes)
- Regression test execution
- Determinism verification
- Performance benchmarking under sustained load
- Security and encoding validation
- Strict-mode enforcement confirmation (no lenient pathway)

Out of scope:

- External lab certification
- Distributed systems testing
- Real-world adversarial penetration testing
- Third-party cryptographic audit

---

## 3. System Under Test

**Component:** UISL2Validator

**Language:** Python 3.8+

**Lines of Code:** ~807

**Validation Mode:** strict\_mode=True

Primary validation subsystems:

- Canonical byte generation
- SHA256 hash enforcement
- ED25519 algorithm whitelist enforcement
- FIELD\_ORDER validation
- Chain linkage validation
- UTF-8 + NFC encoding enforcement
- Duplicate field detection
- Security controls (control characters, null bytes)
- Governance enforcement via POLICY field

---

## 4. Mandatory Rule Enforcement Results

All 20 Mandatory UISL Rules were tested and validated.

### Rules 1–10 (Core Structural Rules)

- Immutability enforcement confirmed.

- Deterministic LF-only enforcement confirmed.
- Fail-closed behavior confirmed.
- FIELD\_ORDER mandatory enforcement confirmed.
- SHA256-only hash enforcement confirmed.
- ED25519-only signature algorithm enforcement confirmed.
- Chain linkage structure validated.
- Revocation schema completeness enforced.
- Multi-signature threshold constraints validated.
- Expiration timestamp enforcement confirmed.

## **Rules 11–20 (Extended Integrity & Governance Rules)**

- Structured JSON error reporting enforced.
- Auto-repair / inference flags rejected.
- Canonical determinism verified (no drift).
- Authority escalation keywords rejected.
- Control characters and null bytes rejected.
- Unknown fields rejected under strict policy.
- NFC normalization enforced.
- Deterministic repeatability validated.
- POLICY governance requirement enforced.
- Subjective language rejected.

**Total Rules Enforced:** 20 / 20

**Observed Failures:** 0

---

## **5. Critical Defect Remediation**

Four previously identified structural defects were corrected and validated.

### **FIX-001: CHAIN Parsing**

Improper parsing logic corrected to extract linkage component accurately.

### **FIX-002: Duplicate Field Detection**

Parser modified to reject duplicate field declarations rather than overwrite.

### **FIX-003: Hash Integrity Enforcement**

Validator modified to enforce exact equality between computed SHA256 hash and declared HASH value.

## **FIX-004: Signature Structure Enforcement**

Validator updated to enforce:

- ED25519 algorithm restriction
- Public key format (32 bytes / 64 hex)
- Signature format (64 bytes / 128 hex)
- HASH presence requirement

Note: Full cryptographic signature verification (library-backed) remains outside this evaluation cycle.

All four fixes were verified via targeted regression tests.

---

## **6. Regression Test Results**

Test Suites Executed:

- Rule Violation Tests (10 cases)
- Mandatory Rule Regression (Rules 1–10)
- Mandatory Rule Regression (Rules 11–20)
- Integrated 20-Rule Test
- Critical Fix Validation Tests

**Total Explicit Test Cases:** 34

**Total Passed:** 34

**Total Failed:** 0

Additional deterministic validation loops executed to confirm repeatability.

---

## **7. Performance Benchmarking**

Benchmark Profile:

- Single validation tests
- Batch validation tests
- High load (5,000 validations)
- Sustained load (10,000 validations)

**Aggregate Results**

- Average Throughput: ~9,371 validations/second
- Average Latency: ~0.107 milliseconds
- Stability: No runtime faults observed
- Memory Stability: No anomalies observed

All defined performance targets were exceeded.

Performance tests executed in a single-node environment only.

---

## 8. Security & Integrity Controls Validated

The following were confirmed during testing:

- Null byte rejection
- Control character rejection
- Strict unknown-field enforcement
- Deterministic canonical byte generation
- Fail-closed validation model
- Chain structure enforcement
- Hash integrity enforcement

No runtime instability or security exception observed during test execution.

---

## 9. Audit Trail Artifacts

Primary validator artifact hash:

```
31a68d5dd7958e187db0006e748875549cd1b0441568b4cf9507324269b6c272  
uisl2_validator.py
```

Additional test artifacts hashed and recorded in DELIVERABLE\_HASHES\_FINAL.txt.

Reproducibility available via standard sha256sum verification.

---

## 10. Limitations

The following limitations are acknowledged:

1. Testing performed in local sandbox only.

2. Cryptographic verification structure enforced; external crypto library not integrated in this version.
3. No third-party institutional attestation.
4. No distributed or multi-node load testing.

These limitations do not invalidate rule enforcement results but define scope boundaries.

---

## 11. Quality Determination

Based on:

- 20/20 rule enforcement validation
- 0 regression failures
- 4 structural defect corrections
- Deterministic validation behavior
- Verified performance stability

The UISL2 Validator v2.1.0 meets internal Quality Benchmark & Validation criteria within the defined evaluation scope.

---

## 12. Certification Statement

This report certifies that UISL2 Validator v2.1.0 demonstrates:

- Complete enforcement of 20 Mandatory UISL Rules
- Verified deterministic canonical behavior
- Strict fail-closed validation
- Structural defect remediation
- Stable high-throughput performance under tested load

All statements in this document are derived from executed local tests and code inspection.

No external institutional certification is implied.

---

Prepared by:  
Denny Michael LaFountaine  
Quantum Labs Research & Development  
2026-02-13

