UniKey Operational Compliance Checklist

Status: Normative

Purpose: Provide acquirers, auditors, and partners with a clear checklist to evaluate UniKey compliance.

1. Trust Packet Compliance

- Canonicalization matches RFC-001
- Signatures verified deterministically
- Replay protection enforced
- Fail-closed behavior confirmed

2. Key Discovery & DKIM Profile

- DNS key discovery follows DKIM/DNS Profile
- Only allowed DKIM tags accepted
- Minimum key strength enforced
- Key rotation supported
- Revocation honored

3. DNS Hardening

- Multi-resolver validation implemented
- TTL and change detection active
- DNSSEC treated as additive
- Anomalies trigger rejection or revalidation

4. Delegation Enforcement

- Delegation packets validated
- Scope monotonicity enforced
- Chain revocation honored
- Delegation depth limits applied

5. Operational Controls

- Incident response for key compromise

- Logging of verification decisions
- Monitoring for DNS anomalies

6. Audit Readiness

- Deterministic verification reproducible
- Historical verification explainable
- Spec references documented

7. Attestation

Implementations MAY attest:

"This system conforms to UniKey Trust Packet, DKIM/DNS, DNS Hardening, and Delegation specifications."

8. Non-Compliance

Any unchecked item represents a trust violation.