# 0REI Appendix A Technical Spec

Genesis v1.1

FIDUS AI – AN ASKEYCAPITAL COMPANY

## 0REI Technical Specification Appendix A

**Protocol Version:** 1.1 Genesis **Domain Separator:** 0REI_IMMUTABLE_LEDGER **Date:** 2026-01-28

### 1. Canonicalization and Data Hash

Payloads are canonicalized using RFC 8785 JSON Canonicalization Scheme (JCS). data_hash = SHA256( CanonicalJSON(payload) )

### 2. Binding Root Derivation

To prevent concatenation ambiguity, variable length fields are length prefixed using little endian unsigned 64 bit integers.

binding_root = SHA256( DomainSeparator || LE_u64(len(entity_id)) || entity_id || LE_u64(len(entity_type)) || entity_type || LE_u64(version) || LE_u64(len(data_hash)) || data_hash )

### 3. Version Semantics

version is u64 and must be strictly increasing per pair (entity_id, entity_type).

### 4. Encodings

• Public keys are hex lowercase, 64 characters (32 bytes)

• Signatures are hex lowercase, 128 characters (64 bytes)

• Hashes are hex lowercase, 64 characters (32 bytes)

• Timestamps use ISO 8601 in UTC

### 5. Evidence Packet Contents

An Evidence Packet is a self contained bundle that enables offline verification.

core payload.json canonical_payload.json seal_record.json manifest.json

proof verify.sh verification_output.txt

docs APPENDIX_A_Protocol_Spec.pdf