

# OREI Appendix A Technical Spec

Genesis v1.1

FIDUS AI – AN ASKEYCAPITAL COMPANY

## OREI Technical Specification Appendix A

**Protocol Version:** 1.1 **Genesis Domain Separator:** OREI\_IMMUTABLE\_LEDGER **Date:** 2026-01-28

### 1. Canonicalization and Data Hash

Payloads are canonicalized using RFC 8785 JSON Canonicalization Scheme (JCS).  $\text{data\_hash} = \text{SHA256}(\text{CanonicalJSON}(\text{payload}))$

### 2. Binding Root Derivation

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

$\text{binding\_root} = \text{SHA256}(\text{DomainSeparator} \parallel \text{LE\_u64}(\text{len}(\text{entity\_id})) \parallel \text{entity\_id} \parallel \text{LE\_u64}(\text{len}(\text{entity\_type})) \parallel \text{entity\_type} \parallel \text{LE\_u64}(\text{version}) \parallel \text{LE\_u64}(\text{len}(\text{data\_hash})) \parallel \text{data\_hash})$

### 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