DigiEmu Core Determinism & Hash Integrity – Formal Definition v1.0

Status: Normative Supporting Framework – Enterprise Edition
Scope: Formal Determinism & Snapshot Hash Guarantees
Date: 2026-02-17

1. Purpose

This document formally defines determinism and hash integrity requirements for DigiEmu Core implementations. It establishes the mathematical and procedural conditions under which snapshot reproducibility and SHA-256 integrity guarantees are considered valid within enterprise and regulated environments.

2. Deterministic State Definition

A system is deterministic if identical inputs produce identical outputs under equivalent specification-compliant conditions. For DigiEmu Core, identical ContentVersions, Claims, and Tenant context MUST produce an identical canonical snapshot payload and identical SHA-256 hash.

3. Canonical Serialization Requirements

Snapshot payloads SHALL be generated using canonical serialization rules. Serialization MUST enforce deterministic field ordering, stable data typing, and environment-independent encoding. No runtime-dependent or non-deterministic metadata MAY influence the payload.

4. Hash Computation Requirements

The snapshot hash SHALL be computed using SHA-256 over the exact canonical payload. The hash MUST be byte-identical across compliant systems. Any deviation in payload structure or ordering invalidates determinism.

5. Environment Independence

Determinism MUST hold across different operating systems, runtime environments, and infrastructure deployments. Implementation-specific optimizations MUST NOT alter canonical ordering or serialization logic.

6. Snapshot Reproducibility Test

A compliant system MUST be capable of reconstructing any historical snapshot from immutable stored entities and MUST reproduce the identical canonical payload and identical SHA-256 hash. This property is mandatory for certification.

7. Mutation Detection

Any unauthorized mutation of a committed ContentVersion, Claim, or Snapshot MUST result in hash mismatch upon recomputation. Hash mismatch SHALL be treated as integrity violation.

8. Formal Integrity Guarantee

Given immutable inputs I and canonical serialization function C, Snapshot S = C(I). Hash H = SHA256(S). For all compliant systems, identical I SHALL yield identical H.

9. Compliance & Certification Impact

Determinism verification is a prerequisite for Level 1 Conformance. Audit-aligned verification requires reproducibility testing under controlled validation conditions. Enterprise Certification requires documented proof of determinism testing procedures.

10. Governance & Version Control

Any modification to canonical serialization logic or hashing algorithm constitutes a breaking change and SHALL require a MAJOR version increment under the DigiEmu Versioning & Stability Policy.