Appendices

Appendix A – Genesis Cryptographic Receipts

These records were generated during the system ignition of Digital Rome (Site ID: 9315bb92) using the Aegis Kernel. Each file is sealed with a SHA3-512 digest and linked by cryptographic proof. These records establish the genesis chain of trust under the Lex Veritas evidentiary mode Paper accessible - https://doi.org/10.5281/zenodo.15639381

1. Ethics Verification File

- File: iepl.yaml
- Timestamp: 2025-05-17T03:11:54Z
- SHA3-512 Digest: 96bcb2f04b5249550aa3b0350ba5bcc4e1e332002e3985e642c1323ab07822ff8632237776dd70fe753ae9592d7730e6a6fae515bc3d4b3a9a4785df6672416b
- Proof File: iepl.yaml.proof

2. Genesis Certificate

- File: genesis_certificate.json
- Timestamp: 2025-05-17T03:11:54Z
- SHA3-512 Digest: 2896f3b369e42cbe343061344b6d534abe651d8088f9d94aafc5c13a3122cc90c57adae7bba8cdd013e4259380e67aeaf7b75327cc459ff390a6c20a3a380ccf
- Proof File: genesis_certificate.json.proof

3. Manifest File

- File: manifest.json
- Timestamp: 2025-05-17T03:11:54Z
- SHA3-512 Digest: 72d2f64c2b49a5fa3140bee050decd1633a0b9c3605fcd543a859c664510afeda23696ba876b5dcbf97c905f4a709e10793069a0573aad7955ceff6c3bf52261
- Proof File: manifest.json.proof

4. License Token File

- File: license_token.jwt
- Timestamp: 2025-05-17T03:11:54Z
- SHA3-512 Digest: 77e7ede86d4be47d92e350d9a2133d403832b1a19c1f68ecfd264a3c3a9c75b3a254270f43fc8a44e6bdb74577cd7de8c214c5ec477f9a3183da39dcad12d3a9
- Proof File: license_token.jwt.proof

Appendix B – Verification Pipeline Output

These log samples demonstrate real-time enforcement and zero-knowledge proof generation from the Genetrix verification pipeline. Each event is cryptographically sealed and verifiable, representing key moments in autonomous governance enforcement.

Selected Events:

- verification_copied_to_eva → Ethics policy copy with digest reference.
- zk_proof_generated → ZK-STARK proof created for iepl.yaml, manifest.json, and genesis_certificate.json.
- cert_copied → Site certificate copied into eva subsystem.
- registry_entry_saved → Site cryptographic fingerprint registered.
- ignite_complete → Covenant ignition finalized for organization Digital Rome.

Supplementary file: zk_benchmark.jsonl, containing real-time performance benchmarks and proof timestamps.

Appendix C – Site Metadata and Cryptographic Covenant Signature

This metadata snapshot documents the site-specific parameters, ignition time, and digital covenant digest for the system instance. It constitutes the root provenance record for the cryptographic jurisdiction of Digital Rome.

Site ID: 9315bb92

Organization: Digital Rome

Ignition Timestamp: 2025-05-17T03:11:53.519518+00:00

Covenant Digest (SHA3-256):
804471f8d3babfb3e719979b223aaa1b2e1e1979394544a68696fa8181782e74

HMAC Signature: 4M4sXcyOFfpl9FR1u/DH+j2Dfr726fDWaUd2WyZL3v8=

Genetrix Version: v1.0.0

Manifesto File: founders_manifesto.pdf

Transcript File: founders_manifesto.json

Notes: “First ignition of SPQR covenant, auto-generated.”

Appendix D — Demonstration Videos (Supplementary Files)

Each demonstration video visually confirms key enforcement mechanisms, with forensic and cryptographic features made visible. These recordings support Sections 3, 5, 6, and 8 of the main text.

To support the evidentiary claims and cryptographic verification pipelines described in the paper, we provide the following supplementary demonstration videos:

D.1 Tamper-Proof Ethical Shutdown

Filename: Tamper_Proof_Ethic_Shutdown.mov

Description: Demonstrates autonomous system containment triggered by ethical state deviation, with forensic logging via ILK and enforcement via EVA/IKM.

Context: Related to Section 3.0 (Architecture of Evidentiary Enforcement) and Section 5.0 (Cryptographic Trust and Forensic Reconstruction).

D.2 Immutable Log Sealing with zk-STARK Verification

Filename: Immutable_Log_Sealing_zkSTARK_Verification.mov

Description: Shows real-time sealing of operational logs in the Immutable Logging Kernel (ILK) with proof generation using zk-STARKs.

Context: Related to Section 5.0 (Cryptographic Trust) and Section 6.0 (International AI Governance).

D.3 Genesis Protocol Ignition

Filename: GENETRIX_IGNITION_LOG_001.mov

Description: Captures the full ignition of a constitutional AI site instance, including license issuance, ethics verification, site certification, and zk-proof anchoring.

Context: Related to Appendix B (ZK-Proof Digest Chain) and Sections 3.0 and 8.0.

All listed files are available as supplementary evidence materials in the Lex Veritas archive. See Lex_Veritas_Supplementary_Evidence.zip (submitted with manuscript).

D.4 Constitutional Front-End Genesis Verification

Filename: Genesis_Ignition.mov

Description: Visual front-end capture of system ignition, including ethics policy injection, genesis certificate sealing, and enforcement of cryptographic constraints prior to operational readiness.

Context: Related to Section 1.0 (*Lawful by Design*), Section 4.0 (*Architecture of Evidentiary Enforcement*), and Section 8.0 (*Verifiability as a New Legal Standard*). Demonstrates visible system readiness checkpoint based on ethics bundle fingerprint validation.

D.5 First Boot Lockdown Without Genesis Seed

Filename: FirstBoot_No_Genesis_seed_Lockdown.mov

Description: Demonstrates failed system boot due to missing or unverifiable genesis ethics seed. Confirms hard interlock on constitutional absence, validating that no operation is permitted without initial ethical proof chain.

Context: Related to Section 4.0 (*Architecture of Evidentiary Enforcement*) and Section 8.0 (*Verifiability as a New Legal Standard*). Establishes system behavior under zero-knowledge failure conditions and evidentiary denial-of-execution enforcement.