Immuva Proof

Cryptographic Proof Standard for Autonomous AI Actions

Immuva Proof

Cryptographic Proof Standard for Autonomous AI Actions

Executive Summary

Autonomous AI systems increasingly execute irreversible and regulated actions.

Immuva provides a cryptographic proof layer that makes these actions **verifiable, auditable, and non-repudiable**.

This document explains how Immuva reduces **legal, audit, and compliance risk** by replacing trust-based logs with **cryptographic evidence**.

---

1. The Trust Gap

Traditional logs:

- are mutable

- depend on operator trust

- are not independently verifiable

In regulated or litigated environments, logs are **statements**, not **facts**.

---

2. The Immuva Protocol

Immuva transforms actions into cryptographic commitments:

- **Identity** — actions are signed by the agent's own cryptographic key

- **Integrity** — append-only, immutable chaining

- **Time** — independent timestamp anchoring

- **Verification** — deterministic and offline-capable

---

3. Zero-Trust Identity Model

Agents generate cryptographic keys locally.

Immuva Authority certifies the binding between a public key and a legal entity.

Immuva never executes actions.
It cryptographically attests that an action **occurred**.

---

4. ProofBundle Format

Each proof is packaged as a deterministic **ProofBundle** containing:

- chained events

- integrity hashes

- cryptographic signature

- optional artifacts

The ProofBundle is **self-contained** and verifiable without Immuva.

---

5. Proof Levels

Immuva supports graduated assurance levels:

- **VALID**

- **KEY_PROTECTED**

- **TIME_ANCHORED**

- **CERTIFIED_IMMUVA**

Each level maps to increasing **legal and regulatory guarantees**.

---

6. Compliance & Regulation

Immuva supports:

- audit traceability

- post-incident analysis

- regulatory accountability

Immuva does not judge decisions.
It **proves facts**.

---

7. Conclusion

When AI acts, responsibility must be provable.

Immuva turns actions into **cryptographic facts**.