Cryptographic Governance Evidence Ledgers (GEL): Ensuring Non-Repudiation and Insurability in Recursive Autonomous Architectures

Author: J. D. “Pepper” Petersen
Organization: Aristotle Agentic
Location: Helena, Montana, USA
Contact: jdpepper@aristotleagentic.com

Abstract

As autonomous systems assume operational control over critical infrastructure, the ability to reconstruct the chain of authority leading to a specific machine action becomes a requirement for legal and financial liability. While governance planes enforce operational constraints at runtime, they often lack a non-repudiable audit trail linking institutional intent to physical execution.

This paper introduces the **Governance Evidence Ledger (GEL)**, a forensic layer designed to complete the Petersen Governance Plane architecture. By cryptographically binding identity, model lineage, delegated authority, and execution telemetry into a tamper-resistant ledger, the GEL enables deterministic reconstruction of the governance state present at the moment of execution.

The resulting architecture provides the evidentiary guarantees required for regulatory accountability and the insurability of autonomous infrastructure.

I. Introduction

Autonomous systems are transitioning from advisory roles to operational control in telecommunications networks, robotics platforms, and cyber-physical infrastructure.

Traditional logging systems answer the question:

“What happened?”

but fail to answer:

“Why was this action authorized under the governing policy framework?”

This distinction becomes critical when autonomous systems control infrastructure where failures can have legal and financial consequences.

The **Governance Evidence Ledger (GEL)** addresses this gap by creating a cryptographic **digital warrant** for every machine action. The GEL records the intersection of:

- agent identity
- model provenance
- delegated operational authority
- runtime telemetry
- trusted timestamps

Each command executed by an autonomous system is therefore backed by a verifiable chain of governance intent.

A critical component of this chain of authority is the **Model Lineage Certificate (MLC)**, which provides cryptographic proof that the executing model has been authorized by the governing institution and has not been modified since certification [2].

II. Position in the Petersen Governance Stack

The Governance Evidence Ledger operates within the broader **Petersen Governance Architecture**, a layered system designed to ensure that autonomous infrastructure remains governable, auditable, and physically safe.

Each layer addresses a different category of system risk before a command reaches physical infrastructure.

Table 1 — Expanded Petersen Governance Stack

Layer	Component	Core Function
Institutional	Meta Authority Envelope (MAE)	Defines constitutional safety constraints governing system behavior
Recursive	Authority Envelope Validation Pipeline	Ensures operational policies remain bounded by MAE constraints
Federated	Authority Routing Layer	Resolves governance conflicts when agents traverse jurisdictions
Operational	Governance Plane	Performs runtime admissibility checks against Authority Envelopes

Layer	Component	Core Function
Communication	Event-Driven Governance Protocol	Enables distributed governance coordination under intermittent connectivity
Legitimacy	Model Lineage Certificate (MLC)	Cryptographically proves model authorization and integrity
Forensic	Governance Evidence Ledger (GEL)	Produces non-repudiable evidence linking authority to execution
Physical	Physical Invariant Gater (PIG)	Enforces deterministic hardware safety limits

---

Figure 1 — Governance Stack Architecture

```
Institutional Authority
        |
Meta Authority Envelope (MAE)
        |
Authority Envelope (AE)
        |
Governance Plane
        |
Governance Evidence Ledger (GEL)
        |
Operational Infrastructure
```

The Governance Plane determines whether an action is admissible.

The GEL records evidence that the decision occurred under the authority state that existed at the time of execution.

III. The Evidence Binding Primitive (EBP)

The central mechanism of the GEL is the **Evidence Binding Primitive (EBP)**.

The EBP generates a cryptographic digest that binds the governance context to the resulting execution.

Evidence Equation

Let:

E = Evidence Record
ID = Agent Identity

MLC = Model Lineage Certificate
AE = Active Authority Envelope
T = Execution Telemetry
TS = Secure Timestamp

The evidence record is defined as:

$$E = H(ID \parallel MLC \parallel AE \parallel T \parallel TS)$$

where

- $H()$is a cryptographic hash function
- ||denotes concatenation

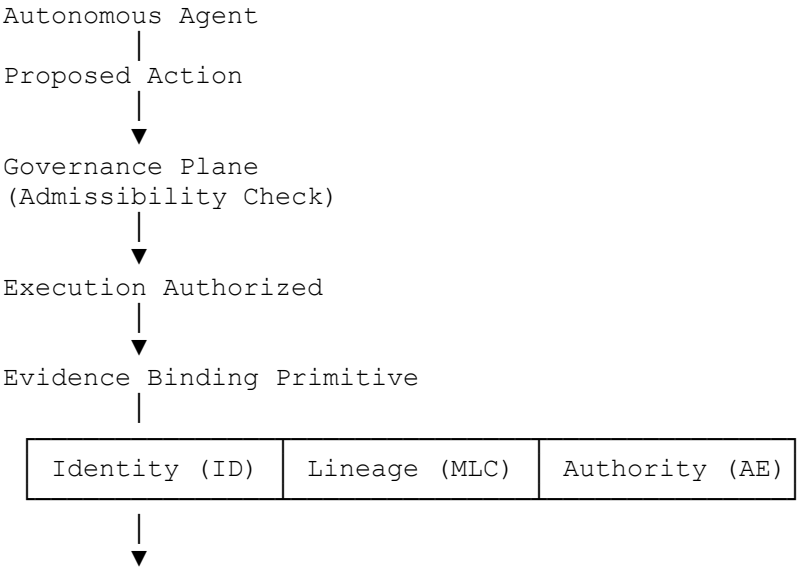
The resulting digest is signed using a hardware-protected private key.

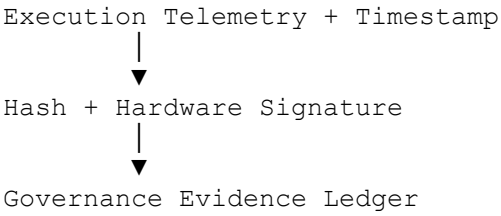
This produces an immutable representation of the execution state that cannot be altered after system compromise.

IV. Evidence Generation Flow

The Evidence Binding Primitive executes immediately after the Governance Plane authorizes an action.

Figure 2 — Evidence Generation Process





This mechanism ensures that every executed command produces a verifiable evidence record.

V. Forensic Data Structure

The Governance Evidence Ledger is implemented as a **hash-chained journal**.

Each new record includes the hash of the previous record. This structure ensures chronological integrity and prevents silent deletion of entries.

GEL Record Structure

Component	Description
Header	Ledger ID and Record Index
Authority Pointer	Hash references to MAE and AE
Execution Context	Snapshot of system state (S0–S3)
Action Payload	Command issued to infrastructure
Validation Proof	Result of Governance Plane admissibility check
Timestamp	Secure execution timestamp
Previous Hash	Hash of prior ledger entry

This structure enables complete reconstruction of the governance context present at the time of execution.

VI. Threat Model and GEL Mitigation

The GEL is designed to withstand adversarial conditions, including disconnected operation and post-incident forensic review.

Threat Surface	GEL Mitigation
Policy Repudiation	MAE and AE hashes prove governing authority at execution time

Threat Surface	GEL Mitigation
Log Tampering	Hash-chained records enforce chronological integrity
Identity Spoofing	Agent identity and model lineage bound into the evidence signature
Log Erasure	Hardware-rooted signing prevents silent deletion of records

These protections transform the GEL from a conventional logging mechanism into a **forensic governance substrate**.

VII. Insurability and Legal Non-Repudiation

Insurance carriers require deterministic evidence to underwrite autonomous infrastructure risk.

The GEL provides three essential guarantees.

Attribution

The Model Lineage Certificate links the executing agent to the responsible institutional sponsor.

Compliance

The ledger proves that the action remained within the constitutional constraints defined by the MAE.

Integrity

Hash-chained evidence records prevent alteration or deletion.

In the event of system failure, the GEL functions as a **forensic black box** capable of distinguishing between:

- institutional policy error
- operational policy misconfiguration
- enforcement system failure
- autonomous system malfunction

VIII. Conclusion

The Governance Evidence Ledger completes the forensic layer of the Petersen Governance Plane architecture.

By converting runtime governance decisions into permanent cryptographic evidence, the GEL enables deterministic reconstruction of autonomous system behavior.

This capability provides the accountability required by regulators, insurers, and infrastructure operators as autonomous systems increasingly control critical infrastructure.

The Governance Evidence Ledger therefore forms the evidentiary foundation necessary for the safe and scalable deployment of autonomous systems.

References

[1] J. D. Petersen, *Systems and Methods for Governance Enforcement of Autonomous Agents Under Intermittent Connectivity*, 2026.

[2] J. D. Petersen, *Model Lineage Certification and Legitimacy Enforcement for Autonomous Systems*, 2026.

[3] National Institute of Standards and Technology, **AI Risk Management Framework (AI RMF 1.0)**, NIST, 2023.

[4] European Union, **Artificial Intelligence Act (Regulation (EU) 2024/1689)**, European Parliament and Council, 2024.