E^NAT IP

Governance Continuity

An Architectural Property for Accountability in Distributed and Agentic Infrastructure

Donald W. Jacobs

July 2026

PUBLIC RELEASE

This paper is offered as an industry research contribution. Governance Continuity is maintained in documented alignment with relevant standards work; it is not submitted for standardization or adoption by any standards body.

Contents

Abstract

Distributed infrastructure has solved how systems communicate, adapt, recover, and scale across independently governed environments. It has not solved how accountability travels with them. As communications, workloads, and — increasingly — autonomous AI agents traverse clouds, telecommunications networks, satellites, edge sites, and third-party services, the governance-relevant context that answers who authorized an action, under whose authority, under which policy, over which custody path, and with what evidence is progressively stripped, fragmented, or left unverifiable. The result is that nearly every record of consequence is authored by the party being held to account.

This paper defines Governance Continuity as an architectural property: the degree to which governance-relevant context remains sufficiently preserved across distributed infrastructure to support attribution, explainability, verification, and accountability despite continual operational, organizational, and administrative change. It introduces a structured model of that context, a single organizing principle that determines which parts of it can be made unforgeable and which cannot, and a set of concrete governance problems the property addresses. It also states, without softening, the boundary of what any such property can promise. The paper draws on a working reference realization to ground its claims, but defines the property independently of any particular implementation.

1 The Problem: Accountability Does Not Travel

Established engineering disciplines — networking, telecommunications, cloud computing, cybersecurity, identity federation, observability — each solve a real continuity problem within their scope. Communication survives link failure. Workloads survive migration. Sessions survive handover. Identity assertions cross organizational boundaries. Collectively they deliver operational continuity: the preservation of successful execution through disruption.

A distinct concern emerges precisely where these disciplines succeed. Successful operation does not preserve the context required to determine how a distributed activity occurred, under whose authority, under which policy, or on what evidence. Communication continues, but who authorized it and under what constraint is no longer reconstructable. A workload migrates, but which organization was responsible at each stage, and under which jurisdiction, is not carried with it. Controls are enforced at each boundary, but the evidence of enforcement sits in isolated systems with no governance-coherent relationship to one another. This is not a failure of any single discipline. It is a structural gap at the intersection of operational continuity and governance — a gap that widens as infrastructure becomes more distributed, more autonomous, and more independently governed.

Agentic AI turns the gap from chronic to acute. An AI agent is, in the words of the 3GPP Release 20 study on 6G service requirements (TR 22.870, adopted March 2026), an automated intelligent entity that interacts with its environment, acquires

context, reasons, and executes tasks — autonomously or in collaboration with other AI agents — to achieve a specific goal. Three properties of such agents sharpen the problem. An agent is an intermediary principal: it receives authority, applies policy, and generates evidence on behalf of a human or organization, yet that authority is typically granted informally through configuration rather than through auditable mechanisms. Agents chain across vendor and service boundaries, each hop under different authority in a different administrative domain. And the industry's default record of what an agent did is the agent's own log — testimony from the defendant.

The recurring pattern in current systems is that governance is asserted where it is not architected: a platform states that activity is subject to its governance while the identity-delegation and evidentiary machinery that would substantiate the statement is absent, or present in one deployment configuration and not another. Asserting governance is not architecting it. Governance Continuity is the property that closes — and, where it cannot close, measures — the distance between the two.

2 Definition

> *Governance Continuity is the architectural property whereby governance-relevant context remains sufficiently preserved across distributed infrastructure to support attribution, explainability, verification, and accountability despite continual operational, organizational, and administrative change.*

Three terms carry weight. It is an architectural property, not a product, protocol, or implementation — like scalability or resilience, it admits of degrees and is evaluated against objectives rather than as a binary. It concerns governance-relevant context, defined precisely in §3, not data or traffic as such. And it requires only sufficient preservation: adequacy is judged against the governance requirements of the specific environment and activity, not against a standard of perfect and total recall.

The property is defined by four governance outcomes it must support. Attribution: determining which identities participated in an activity and under whose authority. Explainability: reconstructing how an activity occurred — the sequence of decisions, the policy constraints, and their causal relations. Verification: confirming, with evidential confidence, that an activity occurred in accordance with applicable authority, policy, and intent. Accountability: assigning and enforcing organizational responsibility. An architecture exhibits Governance Continuity to the degree that these four outcomes remain achievable as activities cross governance boundaries.

3 The Model of Governance-Relevant Context

Governance-relevant context is not monolithic. It decomposes into eight typed attributes, each answering a distinct governance question. The value of the model derives from the coherence among these attributes, not from any one in isolation: identity alone cannot establish accountability, evidence alone cannot establish attribution, policy alone cannot support verification. An architecture that preserves each attribute in a separate, unrelated system provides substantially weaker assurance than one that preserves the relationships among them across the full lifecycle of an activity.

Attribute	Governance question	Preserved value
Identity (I)	Which principal or component acted?	The authenticated actor, bound to its organizational authority
Authority (A)	Under whose right was the action taken?	The delegation of authority, including on-behalf-of relationships
Policy (P)	Under which rule, at which version?	The governing policy, identified by version and jurisdiction
Evidence (E)	What record shows it occurred?	A verifiable, tamper-evident record of the action
Provenance (V)	What is the object's custody history?	Origin, custody chain, and declared transformation of information
Temporal (T)	When, in what verifiable order?	Time-ordering resistant to replay and backdating
Organizational (O)	Which institution bore responsibility?	The accountable entity at each point in the lifecycle
Administrative (D)	In which governance domain?	The administrative domain within which authority and policy apply

A boundary crossing — the transition of an activity from one independently governed domain to another — is the moment at which this context is most vulnerable. It is where relationships fragment, where attributes are stripped, and where verifiability is most often lost. The crossing is therefore treated as a first-class object in its own right, with its own record, rather than as an incidental transition between states.

4 The Organizing Principle: Fabric-Assertability

The central question of Governance Continuity is which attributes can be made unforgeable by the party being held to account, and which cannot. The answer follows from a single test applied to each attribute:

> *An attribute can be architected — made unforgeable by the principal — exactly when some party other than that principal has both the*

> *knowledge of the attribute's true value and an incentive to state it truthfully.*

Where such a party exists, it signs the attribute, and the fabric binds the signature to the crossing. The attribute becomes fabric-asserted: the principal can neither forge it, omit it, nor misreport it. Where no such party exists, the attribute remains the principal's own testimony, and the most the fabric can do is ensure that a false statement collides with a record the principal did not write.

This test partitions the eight attributes cleanly, and it does so without special pleading. It also explains, as a structural consequence rather than an engineering shortfall, why one thing can never be attested: the conduct of the principal itself. No party other than the acting principal knows what the principal actually did, and the principal has every incentive to misreport it. The limit is not a gap to be closed in a later revision; it is the shadow cast by the principle that makes everything else work.

Attribute	Party with knowledge and incentive	Basis of the attestation
Identity	The actor's own key; the issuing identity provider	An issued, non-bearer credential, stable across domain changes
Authority	The granting domain; the delegating principal	Signed delegation, and signed on-behalf-of chains
Policy	The domain that publishes the policy	A signed, versioned, effective-dated policy; the in-force version bound at the crossing
Evidence	The gateway and an independent co-signer	Signed, hash-chained, countersigned crossing records
Provenance	The releasing and receiving domains	Release and receipt attestations, grounded in the crossing record
Temporal	An independent timestamp authority	External time tokens bounding each record on two sides
Organizational	The counterparty's own gateway credential	Derived from the authenticated tunnel, never from the payload
Administrative	The counterparty's own gateway credential	Derived from the crossing itself
Conduct	— none —	Remains the principal's testimony (see §8)

5 How the Property Is Achieved

Governance Continuity does not prescribe a single implementation. The following describes the architectural capabilities from which a compliant realization draws; a working reference realization exists and is summarized in §6. Two structural ideas recur.

5.1 Relocating the recorder

The defining move is to author the record outside the party being held to account. The organization of origin is not what the actor claims; it is derived from the credential the counterparty's own gateway authenticated when the tunnel was established. Every boundary crossing emits a record naming both endpoint organizations, hash-chained to its predecessor, signed by the gateway and countersigned by a second, independently operated party — so that neither signer can unilaterally rewrite history. The record is self-contained: it verifies offline, from public keys alone, with no live system, for as long as it survives — which, for regulated and critical-infrastructure activity, must exceed the operational life of the systems that produced it.

5.2 Grounding every claim in the crossing

Because the crossing record is authored by the fabric, it becomes the ground truth to which every other attribute is anchored. Policy is resolved at the moment of the crossing: the domain's signed, effective-dated policy determines which version was in force at an externally bounded time, and that version's identity is bound into the record — the actor supplies nothing. Provenance is established by the releasing and receiving domains signing what left and what arrived, each referencing a crossing the fabric recorded, so that custody cannot be claimed across a boundary the fabric never witnessed. Authority is delegated by the domain in a signed artifact and, for agents acting on behalf of others, carried in a signed chain the fabric binds at the crossing rather than a token the agent could rewrite. In every case the same discipline holds: the attribute is asserted by the party that knows it and signed against that party's own key, and the fabric records the binding without being asked to vouch for content it cannot see.

5.3 Coherence and finding

An offline evaluator reconstructs, from the records alone, which organizations an activity touched and in what order, and checks the coherence between what the fabric recorded and what the principal claims. Incoherence is reported as typed findings — an account that omits an organization the record proves was reached; an object received with no release; a policy version cited that was not in force; a delegation absent for a domain a crossing entered. The evaluator does not certify that an activity was proper. It identifies, precisely, where the principal's account and the fabric's record diverge.

6 Evidence That the Property Is Realizable

Governance Continuity is realizable, not merely definable. A working reference realization has been built on a multi-tenant overlay-gateway substrate — a workload holding simultaneous authenticated tunnels to multiple organizations whose private address spaces overlap, with a translator projecting every node into a single coherent address realm. The realization runs on real network namespaces with genuinely colliding address space, real datagrams, and genuine external

timestamp tokens from an independent authority. It realizes all eight attributes of the context model; it is exercised by 107 property tests and nine end-to-end scenarios, including disconnected satellite and edge operation under signed leases, bandwidth scaling through parallel connections without loss of attribution, and a documented adversary evaluation. The realization is described in detail in a companion engineering record; this paper cites it only as evidence that the property defined here can be built and that its stated limits are the true limits, confirmed by attempting to violate them.

7 Governance Problems Addressed

The property, so realized, addresses a set of problems that are open in standards bodies, binding in regulation, or unresolved in practice. Each is paired with the mechanism that addresses it and an honest statement of scope. The problems fall into three groups.

7.1 Open questions in agent governance

The U.S. NIST National Cybersecurity Center of Excellence, in its 2026 concept work on software and AI-agent identity and authorization, poses questions this property answers directly:

- **Non-repudiation and tamper-proof logging for agents.** Addressed by relocating the recorder outside the audited actor: the record is authored under the counterparty's credential, countersigned, and externally time-bounded. Scope: the placement problem is settled; conduct within a crossing remains the principal's testimony.
- **Multi-hop delegation.** OAuth On-Behalf-Of handles a single hop; chains degrade into assertions about assertions. Addressed on the domain axis by making delegation a matter of connectivity and issued addressing rather than token chains, and on the principal axis — the two-principal model of 3GPP TR 22.870, where an agent acts on behalf of an entity and may sub-delegate to other agents — by binding a signed, depth-bounded on-behalf-of chain into the crossing. Scope: unforgeable attribution of whom an agent acted for, at any depth; not authorization semantics.
- **Prompt-injection as a control problem.** Addressed structurally: a target the fabric has not made reachable has no address the agent can use, so an injected instruction to reach it fails below the layer at which the agent reasons; a reachable target produces a record naming both organizations. Scope: contains network-effectuated actions, not corruption of content within an authorized crossing.

7.2 Regulatory obligations made satisfiable

The EU AI Act imposes duties this property does not answer but makes satisfiable, by supplying evidence a liable party cannot manufacture:

- **Record-keeping and log integrity (Arts. 12, 19, 26).** A record whose integrity does not depend on the good faith of the provider or deployer, verifiable offline past the lifetime of the systems that generated it.
- **Responsibility along the value chain (Art. 25).** Organizational and administrative responsibility settled at the crossing, from each party's own credential, rather than reconstructed afterward from the logs of adverse parties.
- **Cross-border transfer and residency.** A transfer to a jurisdiction the source domain's own signed policy forbids is a finding at the crossing, not a matter of after-the-fact policy interpretation. A domain cannot retroactively republish a permissive policy to legalize a past transfer, because the policy in force was bound into the record when the crossing occurred.

7.3 A long-standing architectural problem, inverted

The preservation of attribution across overlapping private address space is a documented problem: address-sharing translation, as commonly deployed, destroys attribution because the mapping is ephemeral and unlogged. The property inverts this. The same translation, made with issued and non-reusable identifiers and retained as signed evidence, converts the mechanism that destroyed attribution into the one that establishes it — the translation table becomes the source of record.

Timeline. The obligations above are being phased in: under the 2026 amendments to the EU AI Act, high-risk obligations for standalone systems apply from 2 December 2027 and for embedded systems from 2 August 2028, with transparency obligations taking effect from August 2026. The final text sets these as fixed dates; the earlier proposal's mechanism linking application to standards readiness was dropped in negotiation. Procurement for evidentiary architecture precedes such deadlines by six to twelve months.

8 The Boundary of the Property

A definition of Governance Continuity that did not state its own limits would be an assertion of the kind this property exists to expose. The boundary is precise and follows from the principle of §4.

The fabric records that a crossing occurred; it does not observe what was done within it. An actor that accurately reports which organizations it reached and misrepresents what it did there — reporting a read where it performed a write, or declaring one transformation and performing another — produces a coherent record. Operation-scope authority, the correctness of a declared transformation, and the content of evidence remain the principal's testimony. What changes is that testimony about where, when, on whose behalf, under which policy, and over which custody path now collides with records the principal did not author.

Two further limits are structural. Time is bounded, not fixed: an actor lying within its own externally-anchored interval is not caught, and only a narrower interval narrows the achievable lie. And the property's guarantees hold against any single dishonest party but not against collusion between the two independent signers of a record, nor between a gateway and a domain that agree to fabricate a crossing, nor between an agent and a principal who genuinely conspire. Mitigations — independent operation of the signing roles, third-party notarization, contractual independence of domains, scope-limited and revocable delegation — raise the number of parties who must collude; none reduces it to one. The honest statement of the property is therefore not that it makes governance provable, but that it makes single-party dishonesty falsifiable:

> *You cannot prove the actor told the truth. You can prove precisely when it did not.*

For the audiences that matter most — regulators, auditors, and counterparties, whose work runs on contradiction rather than on proof — falsification of single-party dishonesty is the operative capability, and it is the half that self-attestation cannot provide.

9 Conclusion

Governance Continuity is the architectural property that governance-relevant context — identity, authority, policy, evidence, provenance, time, organization, and administrative domain — survives the crossings between independently governed environments well enough to support attribution, explainability, verification, and accountability. Its realizability turns on a single principle: an attribute can be made unforgeable by the party under scrutiny exactly when another party with knowledge and incentive will sign it. Applied systematically, that principle relocates the record of a distributed activity out of the hands of the party it holds to account, and grounds every governance claim in a crossing that party did not author.

The property does not attest conduct, and it does not survive collusion among the parties that jointly hold the record. Within those stated bounds it converts a class of governance claims that are today merely asserted into claims that are architected — and, where they cannot be architected, into claims that are at least falsifiable. As autonomous agents increasingly act across organizational and jurisdictional boundaries on behalf of others, the distance between asserted and architected governance is where accountability will be won or lost. Governance Continuity is the property that measures that distance, and closes as much of it as the structure of the problem allows.

Correspondence: Don@ENATIP.com · enatip.com