Authority Routing in Autonomous Systems

Toward an Inter-Domain Governance Protocol

J. D. "Pepper" Petersen
Aristotle Agentic
Helena, Montana

Abstract

Autonomous systems are outgrowing their silos. We are beginning to see AI agents collide with infrastructure that was never designed to negotiate authority. Telecommunications networks, logistics systems, industrial control environments, and regulatory frameworks now sit directly in the execution path of autonomous decision systems.

Most governance discussions remain focused on model behavior. Alignment, oversight, and internal guardrails dominate the conversation. Those discussions matter, but they overlook the more immediate problem that appears when autonomous systems cross institutional boundaries.

This paper proposes **authority routing**, a governance mechanism that allows autonomous systems to advertise machine readable authority envelopes and reconcile institutional constraints before actions propagate into real infrastructure.

The concept draws inspiration from the way **Border Gateway Protocol (BGP)** allows independent networks to coordinate routing across the global internet. In a similar fashion, authority routing allows autonomous systems to coordinate institutional permission rather than network traffic.

If autonomous systems are going to scale across infrastructure, governance must become part of the execution architecture itself.

I. The Governance Problem Above the Model

The current conversation around AI governance assumes a system operating inside a single institutional boundary. That assumption is quickly becoming unrealistic.

Autonomous systems are now embedded in environments shaped by multiple institutions. A logistics optimization agent interacts with port authorities, telecommunications providers, and

international regulatory regimes. A distributed energy management system coordinates with utilities, grid operators, and government oversight bodies.

Once autonomous actions begin crossing these boundaries, a fundamental question appears.

Whose authority governs the action?

Existing AI governance frameworks rarely address this problem directly. Most assume governance can be applied after the system produces a decision.

In infrastructure environments that approach does not work. Governance must be evaluated before execution.

II. Lessons from Internet Infrastructure

The internet solved a related coordination problem decades ago.

The internet is not a single network. It is a federation of thousands of independently operated networks known as **Autonomous Systems**. Each network maintains its own routing policies and operational constraints.

Coordination between these networks became possible through **Border Gateway Protocol (BGP)**.

BGP allows networks to advertise the routes they control and the policies governing how traffic should flow between them (Rekhter et al., 2006).

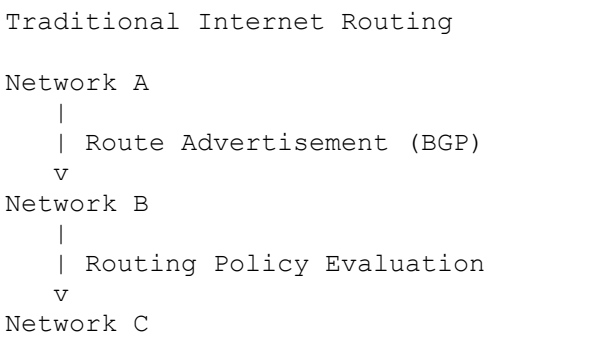
The important lesson is that the internet did not solve this problem through centralized authority. Instead, it created a protocol through which independent actors could advertise their capabilities and negotiate interactions.

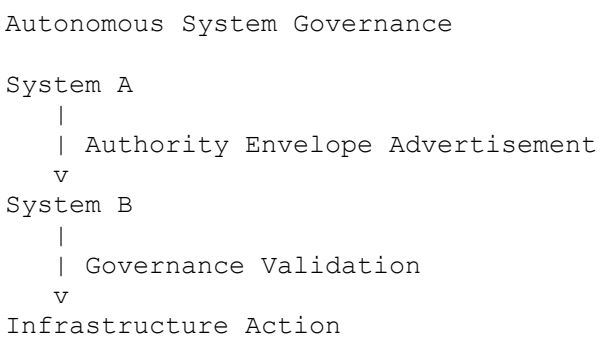
Autonomous systems now face a comparable challenge.

Instead of routing packets, they must determine whether actions themselves are permitted.

Figure 1

From Traffic Routing to Authority Routing





III. The Authority Envelope

For an autonomous system to operate across domains it must be able to demonstrate what it is authorized to do.

This paper proposes the concept of an **Authority Envelope**.

An authority envelope is a machine readable declaration describing the operational authority of an autonomous system.

Typical components include

• system identity
• sponsoring institution
• permitted action categories
• operational constraints
• escalation procedures
• cryptographic attestation

An authority envelope functions much like a passport for autonomous systems. It allows a system entering a new domain to present its credentials and operational limits before acting.

If a system cannot produce a valid authority envelope that satisfies the local domain's constraints, it does not execute.

IV. Authority Routing

Authority advertisement alone is not sufficient. Autonomous systems may encounter situations where authority claims overlap or conflict.

Consider a logistics optimization system attempting to reroute cargo through a port that has issued a temporary safety lockdown.

The logistics system believes the action is authorized.
The port authority believes it is prohibited.

Resolving this conflict requires something stronger than advertisement.

This paper refers to that process as **authority routing**.

Authority routing determines how governance decisions propagate across interacting systems. Autonomous systems reconcile their authority envelopes and constraint boundaries before execution occurs.

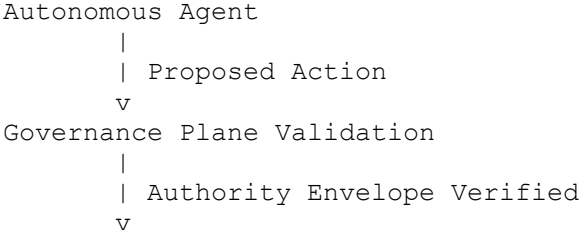
In practice the system must answer two distinct questions.

1. Is the action technically possible
2. Is the action institutionally permitted

Only when both conditions are satisfied should execution proceed.

Figure 2

Authority Envelope Reconciliation



```
External Domain Authority Check
        |
        |-- permitted --> execute action
        |
        |-- conflict --> escalate / halt
```

V. Settlement Before Execution

Infrastructure systems cannot rely on the philosophy of move fast and fix problems later. When autonomous systems control physical or financial infrastructure, governance must prevent invalid actions before they occur.

This requires **settlement before execution**.

In this model, a governance layer evaluates authority metadata, identifies conflicts, and blocks execution until the relevant authorities reconcile their constraints.

Governance therefore becomes a structural property of the execution path rather than a retrospective audit process.

VI. Authority, Liability, and Institutional Trust

When autonomous systems act inside infrastructure environments, governance failures are not merely technical faults. They are liability events.

Once an action occurs, responsibility must be attributed to a specific institution that possessed the authority to act.

Authority envelopes provide the missing link between system behavior and institutional accountability. By declaring authority scope and constraint boundaries before execution, autonomous systems make their actions legible to regulators, operators, and insurers.

Infrastructure that cannot demonstrate bounded authority and reconstructable decision traces will remain difficult to insure.

Systems that can demonstrate those properties become institutionally governable.

Authority routing therefore does more than coordinate autonomous systems. It provides the foundation for assigning responsibility when autonomous systems act.

VII. Governance as Infrastructure

As autonomous systems interact across institutional boundaries, governance begins to resemble infrastructure itself.

The internet required routing protocols to coordinate traffic between networks. Autonomous infrastructure may require protocols that coordinate authority between institutions.

Authority advertisement
constraint negotiation
execution validation
decision attestation

These capabilities may form the foundation of a governance layer for autonomous systems operating at scale.

When governance becomes embedded within execution architecture rather than external policy frameworks, autonomous systems begin to resemble other forms of infrastructure whose operation depends on well defined control planes.

Conclusion

Autonomous systems are beginning to interact across institutional boundaries in ways existing governance frameworks were not designed to manage.

Mechanisms that allow systems to advertise authority, negotiate constraints, and reconcile governance claims before execution may become necessary for safe operation.

Just as the internet required protocols that allowed independent networks to coordinate traffic routing, autonomous infrastructure may require protocols that allow institutions to coordinate authority.

When that occurs, governance stops being an external supervisory process.

It becomes infrastructure.

Appendix A

Authority Envelope JSON Schema

```
{
  "authority_envelope": {
    "version": "1.0",
    "identity": {
      "agent_id": "aristotle-logistics-fleet-04",
      "sponsoring_institution": "Aristotle Agentic",
      "verification_key": "auth_pub_key_99283745"
    },
    "authorized_scope": {
      "domain": "physical_logistics",
      "permitted_actions": [
        "route_optimization",
        "speed_control",
        "docking_maneuver"
      ],
      "max_authority_level": 4
    },
    "operational_constraints": {
      "max_speed_mph": 25,
      "geofence_id": "tacoma_port_sector_7",
      "safety_protocol": "ISO-2026-A"
    },
    "escalation_policy": {
      "conflict_resolution": "human_in_the_loop",
      "primary_contact": "ops_center_helena",
      "timeout_action": "halt_and_secure"
    },
    "attestation": {
      "timestamp": "2026-03-06T17:25:00Z",
      "signature": "sig_55b2...e1a"
    }
  }
}
```

References

Rekhter, Y., Li, T., Hares, S.
RFC 4271: Border Gateway Protocol 4.
Internet Engineering Task Force, 2006.

Clark, D., Wroclawski, J., Sollins, K., Braden, R.
Tussle in Cyberspace: Defining Tomorrow’s Internet.
IEEE/ACM Transactions on Networking, 2005.

Saltzer, J., Reed, D., Clark, D.
End to End Arguments in System Design.
ACM Transactions on Computer Systems, 1984.

National Institute of Standards and Technology
Artificial Intelligence Risk Management Framework 1.0
2023.

ISO/IEC
ISO/IEC 42001 Artificial Intelligence Management Systems
2023.

Petersen, J. D.
A Governance Plane for AI Native 6G Architectures Under Intermittent Connectivity. 2026.

Petersen, J. D.
A New Precedent Born of AI. 2026.