Authority Taxonomy: Hierarchical Credentialing Structure

by Nick Clark | Published April 25, 2026

What the Authority Taxonomy Specifies

The taxonomy classifies all credentialed observation sources into structurally-distinct authority levels: regulatory (departments of transportation, federal aviation authorities, port authorities, defense command authorities), commercial (fleet operators, infrastructure providers, certified service operators), advisory (registered participants contributing observations without command authority), peer (other operating units in the immediate operational context), and adversarial (sources known or suspected to be adversarial, included so the architecture has structural answers to their observations).

Each level has different default admissibility properties. Regulatory observations carry the highest admissibility weight; commercial observations are admitted under the consuming unit's policy regarding the commercial authority's scope; advisory observations contribute at lower weight; peer observations are evaluated against the receiving unit's own peer policy; adversarial observations trigger expanded admissibility evaluation including hostility-classification logic.

Why Flat Authority Models Don't Match Operating Reality

Many current authentication models treat all authenticated sources as equivalent. A signed message is admitted; an unsigned message is rejected; the architecture has no concept of differential authority weight. The pattern works for closed-system communication; it fails for the heterogeneous-authority operating reality of governed-mesh deployment.

Operating reality involves continuous interaction across authority levels. A vehicle operating in a state's roadway consumes regulatory observations from the state DOT, commercial observations from the vehicle's own operator, advisory observations from registered fleet participants, peer observations from neighboring vehicles, and potentially adversarial observations from compromised or hostile sources. The authority taxonomy provides the structural framework for handling all five simultaneously.

How the Taxonomy Composes With Composite Admissibility

The composite admissibility evaluator consumes the observation's authority class as one of its inputs. The consuming unit's policy specifies how each authority class contributes to the overall admissibility decision: regulatory observations may be admissible at higher confidence, commercial at moderate confidence, advisory at lower weight, peer subject to peer-specific policy, adversarial subject to expanded-envelope hostility evaluation.

The taxonomy is itself extensible through credentialed updates. New authority classes can be defined for new operating contexts (coalition authorities for joint defense operations, regulatory cross-recognition authorities for international shipping, etc.). The architecture handles taxonomy evolution as a credentialed governance update rather than as a re-architecture event.

What This Enables for Cross-Authority Operation

Cross-jurisdictional operation handles transitions structurally. A vehicle entering a new jurisdiction consumes the local authority's policy through the same taxonomy framework. International operation handles cross-recognition between national authorities. Coalition operation handles allied-force coordination through the taxonomy's structural support.

The taxonomy is the architectural element that makes governance-credentialed mesh operation tractable across the heterogeneous authority structures the operating reality presents.