Runtime-Signed Adaptation Artifacts

by Nick Clark | Published April 25, 2026

What It Specifies

Each artifact carries: adaptation authority signature, artifact content hash, declared admissibility profile, runtime-signing context (operating environment, applicable platforms, applicable operating profiles). Consumers verify the signature before activating.

Runtime signing is governance-credentialed. The signing authority, signing primitives, and resulting signed artifacts all enter lineage; downstream operations admit against the chain.

Why It Matters Structurally

Adaptation without runtime signing produces structural integrity risk. Compromised artifacts, replaced artifacts, or unauthorized artifacts can enter operational deployment without architectural detection.

Runtime-signed artifacts produce structural integrity. The signature binds artifact to authority; consumers verify before activation; unauthorized artifacts fail verification structurally.

How It Composes With Mesh Operation

The architecture defines the signing protocol, the verification primitives, and the artifact-deployment integration. Implementations apply the architecture; adaptation operations proceed within the framework.

Signing composes with other features. Cross-jurisdictional signing, byzantine-robust verification under disputed signatures, and dispute mechanism for verification disputes all build on the signing primitive.

What This Enables

Defense adaptation operations gain structurally-supported integrity. Civilian critical-infrastructure adaptation gains the same.

The architecture also supports signing evolution. As signing standards mature, signing protocols update through governance procedures.