Tamper-Evident Seal Monitoring

by Nick Clark | Published April 25, 2026

What It Specifies

Physical units carry tamper-evident seals: cryptographic, mechanical, or hybrid. Health monitoring verifies seal integrity; compromised seals enter as credentialed events with declared tamper analysis.

Seal events carry: unit identity, seal class, integrity status, tamper analysis, monitoring authority signature. Downstream operations admit the events against admissibility.

Why It Matters Structurally

Physical-integrity monitoring without seal verification faces structural blindness. Physical compromise (extraction of cryptographic material, replacement of internal components, supply-chain interception) leaves no architectural trace.

Seal monitoring produces structural detection. Physical compromise surfaces as seal events; affected units can be flagged or quarantined structurally.

How It Composes With Mesh Operation

The architecture defines the seal-class taxonomy, the integrity-verification primitives, and the event recording. Implementations apply the architecture; monitoring operations proceed within the framework.

Seals compose with other features. Cross-jurisdictional seal monitoring, byzantine-robust evaluation under adversarial seal reports, and dispute mechanism for seal disputes all build on the seal primitive.

What This Enables

Defense physical-integrity monitoring gains structurally-supported seal verification. Civilian critical-infrastructure physical integrity gains the same.

The architecture also supports seal evolution. As tamper-evident-seal technologies mature, monitoring protocols update through governance procedures.