PUF Challenge-Response Health Verification

by Nick Clark | Published April 25, 2026

What It Specifies

Each unit's hardware identity is bound to its PUF response — the unit-specific physical fingerprint. Health monitoring issues credentialed challenges; the unit responds with its PUF-derived signature; the architecture verifies the response.

PUF verification events enter as credentialed observations. The monitoring authority, the challenge, the response, and the verification result all enter lineage.

Why It Matters Structurally

Hardware-identity verification without PUF faces structural risk. Software-only identity can be cloned, replaced, or spoofed; PUF binds identity to unclonable physical structure.

PUF challenge-response produces structural verification. The architecture confirms hardware identity; compromised hardware fails verification; downstream operations admit the verification results.

How It Composes With Mesh Operation

The architecture defines the PUF challenge-response protocol, the verification primitives, and the event recording. Implementations apply the architecture; monitoring operations proceed within the framework.

PUF composes with other features. Cross-mesh PUF verification federation, byzantine-robust verification under adversarial PUF reports, and dispute mechanism for verification disputes all build on the PUF primitive.

What This Enables

Defense hardware integrity gains structurally-supported verification. Civilian critical-infrastructure hardware integrity gains the same.

The architecture also supports PUF evolution. As PUF technologies mature, verification protocols update through governance procedures.