Nick Clark · Published April 25, 2026 · PDF

How to Meet Medical-Device and Automotive Cybersecurity Fleet Rules with Verifiable Device Lineage

If you operate a fleet of connected medical devices or vehicles, regulators increasingly expect you to prove each unit's provenance, firmware integrity, and current readiness on demand, not just at manufacture time. This guide describes an architectural approach to that problem in which every device carries its own verifiable lineage and continuously attests its health, so compliance evidence is a byproduct of operation rather than a separate reporting pipeline. It describes an architecture disclosed in U.S. Provisional Application No. 64/049,409 (not a shipping library), organized around the Health and Supply-Chain Composite inventive step.

What You Are Building

You run a fleet: infusion pumps and imaging carts across a hospital system, or a mixed population of vehicles and roadside units across a region. A regulator, an auditor, or your own security team asks a deceptively simple question about any single unit: is this the device we think it is, is its firmware the firmware we approved, has it been tampered with, and is it healthy enough to be trusted right now? Medical-device and automotive cybersecurity expectations increasingly demand that you answer that question continuously and produce evidence, not that you attest it once at shipment and hope it holds.

What you are building is a fleet in which each device carries verifiable lineage and readiness state as a first-class property of every message it emits. Instead of a central inventory database you periodically reconcile against reality, provenance and health travel with the device and are checked at the point of use. This guide describes how to approach that architecture. It is a design, drawn entirely from the filed disclosure named below; you implement it yourself.

Why the Obvious Approaches Fall Short

The conventional toolkit is not wrong, it is just fragmented, and the fragmentation is where compliance gaps live.

Network management systems (SNMP, NETCONF, and vendor NMS platforms) monitor device liveness and link quality, but they authenticate with static community strings or per-vendor credentials and produce platform-internal logs with retention decided by the platform operator. There is no authority attribution that survives outside the vendor's console, and no cross-vendor record you can hand an auditor.

Public-key infrastructure gives you device identity, and it is genuinely good at that. But it establishes identity through enrollment with a certificate authority, and a stolen certificate lets an attacker impersonate a genuine device. Identity in PKI is largely a binary valid-or-invalid check at connection time; it does not, by itself, tell you whether the physical unit holding the key is the same unit that was manufactured, or whether its firmware has drifted.

Software bills of materials (SBOMs) and firmware-signing pipelines address provenance at build and release time. They answer "what did we ship," not "what is running in the field right now, and is it still sealed." The custody gap between a signed release and a device three years into deployment is exactly the gap supply-chain attacks exploit.

Each of these is a separate system with its own trust model, its own store, and its own report format. Compliance then becomes an integration exercise: stitch the NMS, the PKI, the SBOM registry, and a tamper-inspection log into a single defensible narrative per device. The structural gap is that operational health, identity, and provenance are never composed into one attributable, reconstructable record.

The Architecture

The disclosed approach treats health monitoring as a first-class architectural primitive rather than a bolt-on, and it composes device, network, governance, and supply-chain health through a single mechanism. The unit of exchange is a governed observation: a message that carries an authority credential, a device-identity attestation, a spatial and temporal reference, a payload, and a lineage field recording provenance with a cryptographic integrity attestation over those fields. Every claim a device makes about itself is a governed observation.

Identity by continuity, not just by certificate. Each device computes a dynamic device hash from device-specific entropy, sensor readings, configuration state, clock state, and the content of prior transmissions. The hash evolves gradually across successive messages, reflecting the device's real operational history. Receivers keep a windowed history of a device's hashes and evaluate each new one for consistency with genuine evolution, producing a trust-slope signal. The disclosure's stated consequence is that a discontinuity in the hash sequence is detectable even when a spoofing device holds a valid static credential, so credential theft alone is insufficient to impersonate a genuine unit. This does not require enrollment with a central certificate authority before operation and does not require long-lived secrets stored on the device.

Provenance that starts at manufacture and stays live. At manufacture, the device's public credential material plus provenance metadata (manufacturer identifier, lot identifier, hardware revision, and a hash of the firmware at manufacture time) is signed by a manufacturer authority and recorded as a manufacture-attestation

governed observation. The device leaves the line manufacturer-credentialed but deployment-uncredentialed. At installation, a deploying organization's credentialing authority verifies that manufacture attestation and issues a deployment credential binding the device to a position in a deployment-specific authority taxonomy, with a temporal scope and a revocation reference. Credentials rotate before expiry, and the renewal step evaluates the device's reputation track record and its continuous health observations before a fresh credential is issued.

Supply-chain provenance monitored continuously. The disclosure describes a supply-chain provenance integrity monitor whose components include a device authenticity attestation evaluator (reporting continuously-valid, expired, revoked, or never-attested status), a firmware integrity chain monitor tracking updates through the authorized-update-authority chain, a tamper-evident seal monitor reporting physical seal status, an authorized-service-provider history recorder, a physical-unclonable-function challenge-response monitor, a manufacturing-provenance chain evaluator, and a software-bill-of-materials attestation verifier. Firmware updates are admitted only with credentialed authority signatures validated against prior firmware-hash history. The disclosed downstream uses include firmware-integrity-gated operation, in which a device refuses to operate on detected firmware tampering, and buyer-side authenticity verification through governance-credentialed attestations.

Readiness as a governed, graded state. Rather than a device being simply up or down, a confidence governor adjusts the unit's execution readiness according to what corroborating governance-credentialed devices are available around it, and derates readiness as that support is lost. Every transition and every change in execution readiness is recorded in the lineage field, which the disclosure explicitly frames as supporting regulatory compliance reporting and incident investigation without reliance on transient telemetry.

Composition into fleet-level assessment. A fleet health aggregator consumes per-device and per-agent health observations and produces fleet-level indicators including availability rate, mean-time-between-failures, degradation trends, and cascade-risk indicators. A cross-domain composite health assessor combines device, agent, mesh, governance, and supply-chain categories. Named composite patterns in the disclosure include a device-plus-supply-chain composite (operational health combined with authenticity attestation to indicate trustworthiness) and a device-plus-governance composite (device health combined with governance-chain integrity to indicate authority-weighted operational readiness). This is the Health and Supply-Chain Composite inventive step: the point is that no single category, checked alone, answers the compliance question, and the architecture composes them.

How to Approach the Build

The steps below are an implementation order, not a checklist you can run. Interface sketches are illustrative and are faithful to the disclosure's field structure, not runnable code.

1. **Define your governed-observation record first.** Everything else is downstream of it. At minimum it carries an authority credential, a dynamic-device-hash field, spatial and temporal references, a time-to-live, a payload, and a lineage field with a cryptographic integrity attestation. Treat this as your wire format for every health and provenance claim.

```
GovernedObservation {
  authorityCredential   // taxonomy position + signature + temporal scope
  dynamicDeviceHash     // evolves per transmission
  spatialRef, temporalRef, ttl
  payload               // e.g. firmware-integrity status, seal status
  lineage {             // contributing-device id, source refs,
    ...                 // derivation-fn id, integrity attestation
  }
}
```

2. **Choose your authority taxonomy.** The disclosure gives a healthcare example with attending-physician, resident, nurse, and orderly levels, and notes the taxonomy is not limited to any fixed set. For an automotive fleet you might define fleet-operator, zone, and individual-unit levels. This taxonomy is what makes a credential mean something beyond valid-or-invalid, so design it before you issue any credentials.
3. **Implement the device-identity continuity path.** Build the dynamic-device-hash generator on the device and the windowed history store plus trust-slope validator on the receiver. Decide your tolerance windows deliberately: the disclosure notes these windows are what let legitimate device replacement, maintenance, and state transitions pass without cryptographic re-enrollment, so setting them too tight breaks servicing and too loose weakens spoofing detection.
4. **Stand up the manufacture and deployment credentialing flow.** Record the manufacture-attestation observation at production, and implement the deployment-enrollment step that verifies it and binds the device to a taxonomy position with a temporal scope and revocation reference. Then implement rotation, gating renewal on reputation and continuous health observations, and implement revocation propagation.

5. **Add the supply-chain provenance monitors incrementally.** Start with the ones your hardware supports: firmware integrity chain and SBOM attestation are software-reachable; tamper-evident seal and PUF challenge-response require hardware support. Wire firmware-integrity-gated operation so a unit that detects tampering degrades or refuses operation per your policy.
6. **Wire the confidence governor and record readiness transitions to lineage.** Make readiness a graded, corroboration-driven state, and ensure every transition is written to the lineage field. This lineage record is your compliance and incident-investigation artifact.
7. **Build the fleet aggregator last.** Once per-device observations are trustworthy and attributable, compose them into fleet indicators and the cross-domain composite assessments. Do not invert this order; a fleet dashboard built over unattributed telemetry reproduces exactly the gap you are trying to close.

What This Does Not Give You

This is an architecture, not a drop-in library. There is no package to install and nothing here "just works" out of the box; you implement each mechanism against your own hardware, credentialing authority, and regulatory context. The disclosure describes structure and mechanism, not benchmarks: it does not state throughput, latency, false-accept or false-reject rates, or key sizes, and neither should you until you measure your own build. Nothing here is a productized or production-proven system.

It also does not substitute for regulatory judgment. Meeting a specific medical-device or automotive cybersecurity rule is a determination you and your regulatory and legal advisors make against the governing framework; the architecture produces evidence and continuous attestation, but mapping that evidence to a particular requirement is your responsibility. Several monitors (tamper-evident seals, PUF challenge-response) require hardware you may not have, and the continuity-based identity mechanism

relies on tolerance windows you must tune for your servicing reality. Where devices cannot emit governed observations at all, or where you cannot control the credentialing authority, the approach does not apply.

Disclosure Scope

The architecture and mechanisms described in this guide are disclosed in U.S. Provisional Application No. 64/049,409, whose home inventive step for this material is the Health and Supply-Chain Composite inventive step covering continuous, governance-chain-preserving composition of device, network, governance, and supply-chain health with per-device verifiable lineage. This guide is educational: it explains an architectural approach a developer can build. It is not a warranty, not an offer of software or an SDK, and not a representation that any described mechanism is a shipping product, benchmarked, or certified for any regulatory purpose.

Health & Supply Chain Composite (/health-monitoring)

All 40 steps → (/inventive-steps)

Governance-chain integrity unified with supply-chain provenance. Zero-trust device health.

Provisional application

PRIMARY TECHNICAL DISCLOSURE

- Health Monitoring: Unified Governance and Supply-Chain Composite (/articles/health-monitoring-unified-governance-and-supply-chain-composite)

SECONDARY TECHNICAL

- Governance Chain Integrity Monitoring (/articles/health-monitoring/governance-chain-integrity)
- Trust Slope Anomaly Detection (/articles/health-monitoring/trust-slope-anomaly-detection)
- Revocation Propagation Evaluation (/articles/health-monitoring/revocation-propagation-evaluation)

- PUF Challenge-Response Health Verification (/articles/health-monitoring/puf-challenge-response)
- SBOM Attestation for Software Health (/articles/health-monitoring/sbom-attestation)
- Tamper-Evident Seal Monitoring (/articles/health-monitoring/tamper-evident-seal-monitoring)
- Composite Fleet Health Assessment (/articles/health-monitoring/composite-fleet-health)
- Zero-Trust Device Management (/articles/health-monitoring/zero-trust-device-management)
- Regulatory Compliance Integration (/articles/health-monitoring/regulatory-compliance-integration)

APPLICATIONS · GENERAL

- Continuous Device Authenticity and Supply-Chain Provenance for Counterfeit-Part Detection in Semiconductor and Defense Procurement (/articles/health-monitoring/device-authenticity-provenance)
- Defense Fleet Readiness Health Monitoring (/articles/health-monitoring/defense-fleet-readiness)
- Industrial IoT Fleet Health Monitoring for OT Security and Compliance (/articles/health-monitoring/industrial-iot-fleet-monitoring)
- Medical Device Fleet Health Monitoring (/articles/health-monitoring/medical-device-fleet-monitoring)
- Automotive Cybersecurity Compliance Under UN ECE R155 and R156: A Fleet Health Monitoring Substrate for CSMS Evidence (/articles/health-monitoring/automotive-cybersecurity-uneces)
- Continuous Device-Integrity Evidence for CISA-Regulated Critical Infrastructure Fleets (/articles/health-monitoring/critical-infrastructure-fleet-cisa)
- Medical Device Cybersecurity Fleet Management Under FDA 524B (/articles/health-monitoring/medical-device-cybersecurity)
- AAMI TIR57 Compliance for Connected Medical Devices: An Attested Health-Monitoring Substrate (/articles/health-monitoring/aami-tir57-medical-cyber)
- CMMC 2.0 Defense Contractor Cybersecurity Compliance: Device Integrity Evidence for C3PAO Assessment (/articles/health-monitoring/cmmc-2-defense-cyber)
- DO-326A Airworthiness Security Compliance for Aircraft Fleet Cybersecurity (/articles/health-monitoring/do-326a-aviation-cyber)
- IEC 62443 Compliance for Industrial Control Systems: Architectural Device Evidence at Fleet Scale (/articles/health-monitoring/iec-62443-industrial-cyber)
- ISO 13485 Compliance for Connected Medical Device Fleets: Continuous Attestation for Post-Market Surveillance (/articles/health-monitoring/iso-13485-medical-qms)
- Continuous Device Attestation Evidence for NIST CSF 2.0 Compliance Across Device Fleets (/articles/health-monitoring/nist-csf-2-0)

APPLICATIONS · SPECIFIC

- CrowdStrike Falcon vs Governed Fleet Health Monitoring (/articles/health-monitoring/crowdstrike-falcon-fleet)
- Medtronic CareLink Alternative: Governed Cross-OEM Medical-Device Fleet Health (/articles/health-monitoring/medtronic-carelink)
- Microsoft Defender vs Cross-Vendor Governed Fleet Health (/articles/health-monitoring/microsoft-defender-fleet)
- Armis Alternative for Attested Fleet Health: Governed Device Health Monitoring (/articles/health-monitoring/armis-iot-asset)
- Claroty xDome vs Attestable Fleet-Health Device Identity (/articles/health-monitoring/claroty-ot)
- Dragos vs Attested Fleet Health: Device-Side Integrity for OT (/articles/health-monitoring/dragos-industrial)
- Nozomi Networks vs Attestation-Grounded Fleet Health (/articles/health-monitoring/nozomi-networks)
- Tenable OT Security vs Governed Fleet-Health Attestation (/articles/health-monitoring/tenable-iot-ot)
- Governed Device-Integrity Attestation Beyond AVEVA (Schneider) Industrial Software (/articles/health-monitoring/schneider-aveva)

Health & Supply Chain Composite overview → (/health-monitoring)