

Seal at Capture: Offline-Verifiable Provenance

Defensibility — why the seal must form before transmission, and how anyone can check it without the vendor

Public Cut · PlotSeal series — Essay 2 of 4 · Essay 1 done; **T14–T15 not started**

Field	Value
Document ID	HPS-09-ART-PS-02-PUB
Version ID	1.0
Effective Date	2026-09-24
Supersedes	none (first public cut)
Classification	Public
Author	High Plains Shield, LLC
Format	F1 — Category / foundation essay (HPS-PUB-STD-001 v1.1)
Related	HPS-09-ART-PS-01-PUB (Essay 1); GFMS-1.0 Public (HPS-09-MAP-01) Clause 4 (+ §4.1 pointer); CFI Doctrine (HPS-09-CFI-01) — custody; HPS-09-ART-MMG-01-PUB (seal locks basis); HPS-09-ART-BASIS-01-PUB
Series	PlotSeal series — Essay 2 of 4 (Evidence → Defensibility → Registry/SoR → History) · Essay 1 done (T12); T14–T15 not started

Executive Summary

Sealing after upload, or verifying only through a vendor login, recreates trust-me infrastructure. Edits after capture can rewrite basis and loads if the seal is not bound to collection-time bytes. Underwriting, WMP defense, and third-party review need a check that does not depend on the producer still answering the phone.

This essay teaches the **Defensibility** rung of the PlotSeal positioning spine: **seal at capture**, **canonicalization**, **dual digests**, **legal codes outside the physical seal**, **offline verification**, and **basis inside the seal**. Normative home for the cryptographic interface is **GFMS-1.0 Clause 4** (Public cut, Document ID HPS-09-MAP-01). This essay teaches the architecture; it does not paste the reference shell verifier as essay body.

Claim (series thesis for Essay 2 — Defensibility): A relying party must be able to recompute digests over a canonical payload and get PASS or FAIL without API access, proprietary authentication, or vendor intervention. Matching digests prove integrity versus a known-good reference — **not**, by themselves, identity of the producer. Offline capture with later sync does **not** move the seal timestamp to upload time.

Locked phrases (PlotSeal context): “Proof, not prediction.” · “The bag is the witness. The PDF is a copy.” Prefer **Wildfire System of Record**; reject leading with **Wildfire Data Center**. Independence belongs to the **customer-held / offline-checkable file** — not to a permanence claim about vendor-hosted custody.

Naming locks: CFI = category · GFMS-1.0 = open standard · GFHL = spatial expression · PlotSeal = registry / system of record (also names the sealed-record / provenance concept) · RiskWise = commercial vehicle (stack role only). Method 1.1 and Level 3–4 internals are absent from this public face.

*Soft next step: read GFMS-1.0 Clause 4 (and §4.1 pointer) for normative interface rules; reconnect to Essay 1 for why evidence must be sealed proof; soft pointer ahead to Essay 3 — Registry Is the Asset (**T14 not started**).*

1. Problem — Post-Upload Seals Recreate Trust-Me Infrastructure

Essay 1 established that prediction, resolution marketing, and unsigned PDF stacks fail audit. Essay 2 asks the next question: even when a “seal” exists, **when** was it formed, and **who** must be present for anyone to check it?

Failure mode	What it looks like	Defensibility defect
Seal after upload	Digests computed on a server after sync / ingest	Seal timestamp reflects transmission or batch jobs, not collection; intervening edits can rewrite basis and loads before hashing
Vendor-login verification	Reviewer must authenticate to a proprietary portal to “verify”	Check depends on vendor uptime, access control, and continued cooperation — trust-me infrastructure
Unkeyed “signature” marketing	Checksums sold as if they were private-key identity proofs	Matching hash ≠ producer identity; honest cryptography limit is erased
Mutable canonical form	Different languages serialize floats / key order differently	Digests diverge across implementations; FAIL becomes noise, not evidence
Legal codes inside physical seal	Rule-lookup fields sealed with grams / tons	Regulatory updates invalidate historical physical proofs unnecessarily
Basis outside the seal	Origin tag editable after capture	Post-hoc rewrite of <i>which claim</i> without breaking the digest

Claim (conceptual): A seal formed after transmission answers a different question than a seal formed at capture. The first asks: *what did the server hold when it hashed?* The second asks: *what was claimed when the observation happened?* Docket defense needs the

second.

Illustration (non-normative): A corridor package is collected offline. Hours later it syncs. Between collection and upload, a load cell is “corrected,” a basis tag is switched from measured to modelled, and a legal lookup code is refreshed. If digests are computed only at ingest, the seal freezes the edited payload and stamps upload time. Offline verification against that seal will PASS — and still miss the collection-time claim. That is not defensibility; that is a polished assertion.

What breaks defensibility is not connectivity. Offline capture with later sync is normal field practice. What breaks defensibility is moving the seal event to upload, or binding verification to a login the relying party cannot execute alone.

2. Framework — Seal at Capture and Offline Verification

2.1 Seal at capture

Seal at capture means cryptographic digests are computed on the observer / device side (or at the collection event) so the seal timestamp reflects **collection**, not later sync or upload.

- Digests bind to the collection-time bytes of the canonical measurement payload (including basis).
- Offline capture with later sync **does not** move the seal time to upload.
- Post-seal edits to sealed fields break digest match (tamper-evident integrity). Append / supersede / void paths — when used — are recorded as new events; they are not silent rewrites of the original seal.

Claim (conceptual): Capture-time sealing is the Defensibility hinge. Everything downstream — offline verify, registry reliance, multi-year history — inherits credibility from *when* the seal formed.

2.2 Canonicalization (RFC 8785-class)

Per **GFMS-1.0 Clause 4** (normative home; taught here at concept level):

- Keys sorted lexicographically.
- Finite numeric values rounded to a fixed precision (six decimal places in GFMS-1.0) so floating-point serialization does not drift across languages.
- Timestamps as ISO-8601 UTC strings (YYYY-MM-DDTHH:MM:SSZ).

Without a shared canonical form, two honest implementations can hash different byte strings for the “same” logical record. Canonicalization makes digests **reproducible** across languages and runtimes.

2.3 Dual digests

The canonical payload **SHALL** (in GFMS-1.0 terms) generate two concurrent digests: **SHA-256** and **SHA3-256**. Dual digests provide tamper-evident integrity with algorithm diversity at the public interface — not a product feature pitch, and not a claim that either algorithm is “un-bypassable.”

2.4 Legal codes outside the physical seal

Derived legal / regulatory lookup codes (for example, jurisdiction defensible-space rule codes) ride in the **record envelope** alongside the canonical payload. They **SHALL NOT** (GFMS-1.0) be sealed inside the physical-measurement digest. Rule updates then do not invalidate historical physical proofs. Physical grams and tons stay checkable even when the regulatory overlay changes.

2.5 Offline verification

Verification **SHALL** (GFMS-1.0 Clause 4) run completely offline in client software without requiring API access, proprietary server authentication, or vendor intervention.

Step (concept)	What happens	Result meaning
1. Obtain payload + stored digests	Relying party holds the file (or a copy) and the known-good reference digests through an independent channel	Independence = customer-held / offline-checkable file
2. Canonicalize	Apply RFC 8785-class rules	Reproducible byte string
3. Recompute dual digests	SHA-256 and SHA3-256 over canonical bytes	Candidate digests
4. Compare	Match both against stored vault seals	PASS = byte-identical · FAIL = altered or wrong reference

Honest cryptography limit: Matching digests prove **integrity** versus a known-good reference — **not**, by themselves, **identity** of the producer. Unkeyed checksums are not private-key signatures. The reference hash must be held independently (trusted channel / separately conveyed reference). This essay does not disclose key-management schemes, device-attestation recipes, or claim “un-bypassable” marketing language.

*Normative reference procedure: **GFMS-1.0 §4.1** (pointer only — not reproduced as essay body).*

2.6 Basis inside the seal

Reconnect to Essay 1 and the Measured / Modelled / Grounded lineage: the **basis tag** travels **inside** the sealed payload. Without that binding, origin class can be rewritten after capture without breaking the digest. The seal’s public job includes proving **which basis was claimed**, for **which payload**, at **collection time**, in an offline-verifiable form.

2.7 Series position — Defensibility on the spine

Rung	Pillar	Public question	This series
1	Evidence	Is the claim sealed proof of what was collected?	Essay 1 (T12 — done)
2	Defensibility	Can a relying party verify offline without the vendor?	Essay 2 (this — T13)
3	History	Does continuity across years beat a single assessment?	Essay 4 (T15 — not started)

Essay 3 (T14 — **not started**) positions the **registry as the asset** (Wildfire System of Record, not data center) between Defensibility and History.

2.8 What this essay is not

This essay / Defensibility face is not...	Why that matters
A key-management disclosure	Key custody, rotation, and HSM design stay Level 3–4 / F5
A device-attestation recipe	Hardware roots of trust and attestation protocols are not taught here
Private-key signatures sold as checksums	Matching hash ≠ producer identity; do not erase the honest limit
"Un-bypassable" / permanent vendor custody marketing	Independence = customer-held file; reject permanence-of-HPS-hosted-custody claims
A live registry / national multi-operator shipping claim	Registry concept is named; live stats and shipping claims are not made here
Wildfire Data Center framing	Rejected as public lead; prefer Wildfire System of Record
A substitute for GFMS-1.0 Clause 4	Normative interface rules live in the open standard
Essay 1 rewritten	Evidence rung is locked in PS-01; this essay climbs to Defensibility

2.9 Naming locks (unchanged)

Name	Role	Not to be confused with
CFI	Enterprise technology category	Not "the standard"; not PlotSeal
GFMS-1.0	Open interface standard (Clause 4 = cryptographic provenance)	Not a product; not this essay
GFHL	Spatial expression of grounded fuel	Not a behavior model; not the seal
PlotSeal	Registry / system of record (+ sealed-record concept)	Not "Wildfire Data Center"; not GFMS
RiskWise	Commercial vehicle (stack role only)	Not the thesis of this essay
Basis Tags	Mandatory origin declaration sealed <i>with</i> the payload	Not a substitute for sealing

3. Proof — Capture → Canonicalize → Dual Digest → Offline Verify

3.1 Figure 1 — At-capture seal pipeline (Illustration, non-normative)

Visual proof of the Defensibility pipeline and the without / with contrast between a post-upload seal and an at-capture seal. Schematic only; not a product screenshot, not a live registry claim, and not a substitute for GFMS-1.0 §4.1.

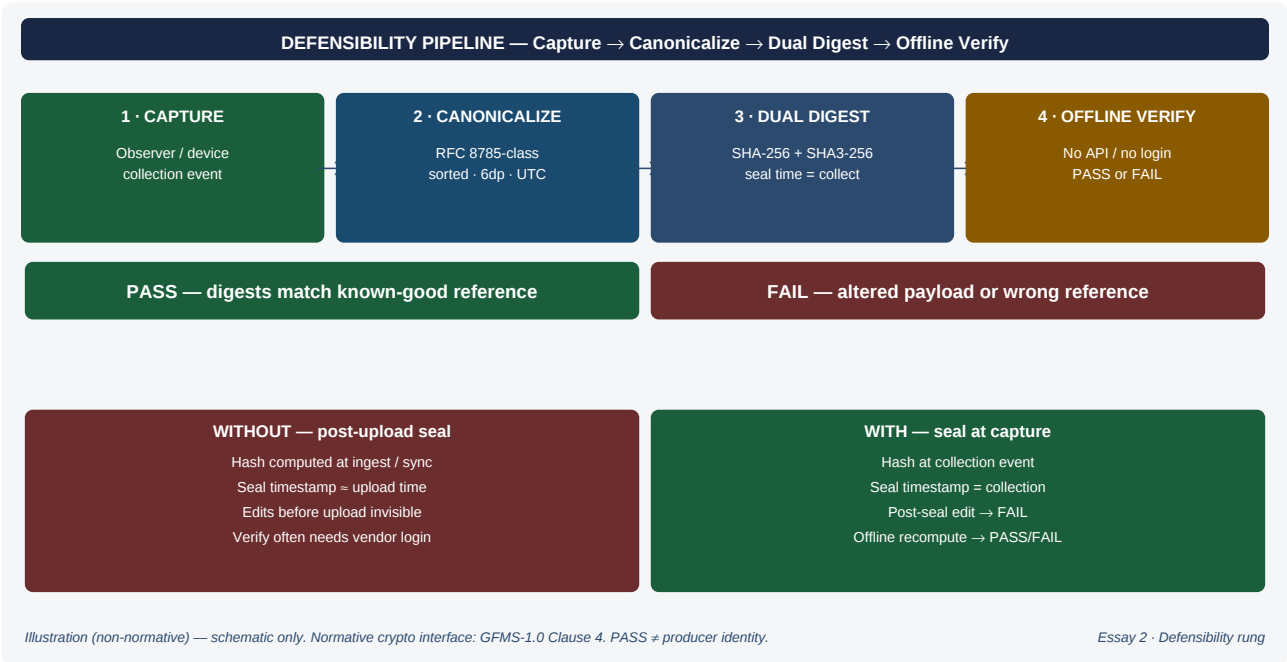


Figure 1 — Illustration (non-normative). Essay teaches the Defensibility rung; normative cryptographic interface rules live in GFMS-1.0 Clause 4 (+ §4.1). Registry shipping status is not asserted by this figure. PASS ≠ producer identity.

3.2 Comparative standing (informative)

Property	Post-upload / login-bound practice	Seal at capture + offline verify (PlotSeal concept + GFMS Clause 4)
When seal forms	After sync / ingest	At collection event (device / observer side)
Seal timestamp	Often upload or batch time	Collection time; sync does not rewrite it
Intervening edits	Can rewrite basis / loads before hash	Post-seal change breaks digest match
Verification venue	Often vendor portal / API	Offline client recompute
Vendor dependence for check	High	None required for integrity check
Legal codes	Sometimes mixed into physical seal	Envelope outside physical-measurement digest
Basis standing	Often rewriteable outside seal	Declared inside sealed payload
What PASS proves	Whatever the server hashed	Byte identity vs known-good collection-time reference (PASS ≠ producer identity — honest limit)

3.3 Optional tiny illustration — verify shape (non-normative)

Illustration only — not a live production record and not the GFMS §4.1 procedure:

```
canonical_payload → SHA-256 = <candidate>
canonical_payload → SHA3-256 = <candidate>
compare to stored vault_seal_sha256 / vault_seal_sha3
→ PASS (both match) | FAIL (any mismatch)
```

*Labeled **Illustration**. Digests are placeholders. This shape teaches the PASS/FAIL integrity check; it is not a published production sample and not evidence of a live national registry.*

3.4 Why Defensibility comes second

Claim: Evidence without offline defensibility is a seal nobody else can check. History without offline defensibility is a folder of assertions with elegant filenames. The registry-as-asset argument (Essay 3 — not started) only holds if relying parties can verify without asking the vendor. Essay 2 therefore locks the second rung after Essay 1's Evidence claim.

4. Implication — Demand Capture-Time Seals and Offline Checks

Defensibility matters wherever a sealed fuel or readiness claim must survive third-party challenge **without** vendor mediation:

- **Utility wildfire mitigation plans (WMPs)** and related dockets that must show collection-time provenance, not ingest-time hashing.
- **Insurance, reinsurance, and lending** reviews that need an integrity check executable without proprietary portal access.
- **Authorities having jurisdiction** and operators that must distinguish offline-verifiable seals from login-bound “verification.”
- **GIS and spatial-platform operators** that consume sealed observations and need reproducible digests across implementations.
- **Infrastructure asset owners** that hold their own files and must still open them if a vendor is unavailable.

Implication for adopters: Adopt **Defensibility** language next — seal at capture; canonicalize; dual digests; legal codes outside the physical seal; offline PASS/FAIL; basis inside the seal. Keep Essay 1's Evidence claim. Soft-read ahead for **Registry / SoR** (system of record, not data center — Essay 3 / T14 **not started**) and **History** (continuity across years — Essay 4 / T15 **not started**). Adopt the open standard (**GFMS-1.0**, especially Clause 4 and the §4.1 pointer) for normative interface rules. Evaluate commercial vehicles — including RiskWise — only after the interface properties are clear. Category and standard growth do not require exclusive use of any one vendor; they require shared rules and verifiable properties.

Soft next step (teach, don't sell)

1. Read **GFMS-1.0** Clause 4 (+ §4.1 pointer) — Document ID HPS-09-MAP-01 — for normative canonicalization, dual digests, legal-code placement, and offline verification (recipes stay in the standard; not pasted here).
2. Re-read **Essay 1** — Document ID HPS-09-ART-PS-01-PUB — for why evidence must be sealed proof of which payload (including basis) was claimed.
3. Read **CFI Doctrine** — Document ID HPS-09-CFI-01 — for category pillars including cryptographic proof and observer custody at public depth.
4. Read **Measured, Modelled, and Grounded** — Document ID HPS-09-ART-MMG-01-PUB — and **Basis Tags** — Document ID HPS-09-ART-BASIS-01-PUB — for basis sealed with the claim.
5. Ask of any “sealed” fuel claim in your stack: *Was the digest formed at collection, and can a stranger recompute PASS/FAIL offline without the vendor?*
6. Contact High Plains Shield, LLC at info@highplainshield.com for standards clarification or conformant-implementation questions — not a product hard sell.

Series note: Essay 2 of 4 complete (Defensibility). Essay 1 done. Soft next essay title: **Registry Is the Asset. T14–T15 not started.**

5. Limitations — What This Document Is Not

This Public cut:

- **Is not** an open standard (see GFMS-1.0).
- **Is not** a substitute for GFMS-1.0 Clause 4 normative language or the §4.1 reference verification algorithm (pointer only; procedure not pasted as essay body).
- **Is not** a product datasheet, SKU list, drop ID list, pricing document, or monetization playbook.
- **Is not** a live national registry claim, multi-operator shipping claim, or fabricated registry statistic.
- **Is not** a permanence / “immutable forever” claim about HPS-hosted custody; independence = customer-held / offline-checkable file.
- **Is not** a key-management disclosure, device-attestation recipe, or private-key signature scheme sold as a checksum.
- **Is not** “un-bypassable” marketing, a fire-behavior model, an Esri partnership claim, or **Wildfire Data Center** framing.
- **Is not** a disclosure of proprietary field-collection protocols, registry architecture, hosted SoR identifiers, suite seal-package mechanics, field/scoring engines, calibration weights, or trade-secret thresholds.
- **Does not** start Essays 3–4 (Registry/SoR, History) — those remain unwritten under **T14–T15**.
- **Does not** guarantee regulatory acceptance in any specific jurisdiction.
- **Does not** claim market share.

Not disclosed (IP gate): Method 1.1, FMES, HPFS, Structural MVE, CAT packs, Field Gauge, TrueFuel, WROS, VALOR, drop IDs, device-binding, key management, suite Evidence Vault internals, FireLedger/WRDC as live claims, Azure/hosted SoR IDs, and related Level 3–4 internals remain internal under HPS-PUB-STD-001 §4. Quantitative performance claims for any commercial implementation are **out of scope** here.

6. Glossary

Term	Public meaning
Seal at capture	Digests computed at the collection event (observer/device side) so seal time reflects collection, not later sync/upload.
Offline verification	Digest check executable without API access, proprietary server authentication, or vendor intervention (GFMS-1.0 Clause 4).
Canonical payload	Deterministic serialization (RFC 8785-class) used before hashing so digests are reproducible across implementations.
Dual-hash / dual-digest	Concurrent SHA-256 and SHA3-256 digests over a canonical payload (GFMS-1.0 Clause 4).
Legal codes outside the seal	Regulatory lookup fields in the record envelope, not inside the physical-measurement digest.
PASS / FAIL	Integrity result of offline digest comparison vs a known-good reference; PASS ≠ producer identity.
Known-good reference	Independently held digest(s) against which a recomputation is compared.
Proof, not prediction	Locked PlotSeal-context phrase: sealed offline-verifiable claim vs model/estimate marketing.
The bag is the witness. The PDF is a copy.	Locked phrase: physical sample / sealed payload carry evidentiary weight; PDF inherits credibility.
PlotSeal	Registry / system of record concept for sealed fuel (and related) measurement records; also names the sealed-record / provenance concept. Not “Wildfire Data Center.”
Wildfire System of Record	Preferred external framing for PlotSeal SoR positioning.
Defensibility	Second rung of the of-record spine: can a relying party verify offline without the vendor?
Evidence → Defensibility → History	Of-record PlotSeal positioning spine for this four-essay series.
CFI	Enterprise technology category for physical, cryptographically proven fuel intelligence. Not “the standard.”
GFMS-1.0	Grounded Fuel Mapping Standard — open interface standard. Clause 4 = cryptographic provenance & offline verification.
Basis	Origin class of a fuel value: measured, modelled, or grounded; sealed inside the payload.
RiskWise	Commercial vehicle that may implement CFI-conformant workflows. Stack role only; not the thesis of this essay.

Document Control

Field	Value
Document ID	HPS-09-ART-PS-02-PUB
Title	Seal at Capture: Offline-Verifiable Provenance
Version	1.0
Effective	2026-09-24

Field	Value
Supersedes	none (first public cut)
Classification	Public
Author	High Plains Shield, LLC
Governing house standard	HPS-PUB-STD-001 v1.1
Informative precursors	HPS-09-ART-PS-01-PUB; GFMS-1.0 Public v1.1 Clause 4 (+ §4.1 pointer); HPS-09-CFI-01; HPS-09-ART-MMG-01-PUB; HPS-09-ART-BASIS-01-PUB
Series position	PlotSeal series — Essay 2 of 4 (Defensibility) · Essay 1 done; T14–T15 not started
Contact	info@highplainshield.com

Revision History

Version	Effective	Summary	Gates
Public v1.0	2026-09-24	First dedicated public PlotSeal series essay (Defensibility rung): teaches seal at capture; RFC 8785-class canonicalization; dual digests; legal codes outside physical seal; offline verification with honest cryptography limits; basis inside the seal; Figure 1 capture→canonicalize→dual digest→offline PASS/FAIL + without/with (post-upload vs at-capture); soft CTA to GFMS Clause 4 and Essay 1; soft next = Registry Is the Asset (T14 not written); Limitations + Glossary; §4 scrub; clean Markdown → PDF. Essay 1 done; T14–T15 not started.	Author → Technical Review → Publication Review → Release (HPS process)

Pre-Publish Checklist (Hard Gate) — Recorded Pass

- Format F1 selected; Problem → Framework → Proof → Implication spine complete
- Author = High Plains Shield, LLC everywhere (including metadata)
- Face block complete: Document ID · Version ID · Effective Date · Supersedes · Classification · Author
- Naming locks: CFI = category · GFMS-1.0 = standard · RiskWise = commercial vehicle · PlotSeal = registry/SoR · GFHL = spatial expression · Method 1.1 / forbidden internals absent · no WDC lead
- Claims vs illustrations labeled; Limitations present; Glossary present
- IP gate cleared (§4 scrub): Method 1.1, FMES, HPFS, Structural MVE, CAT packs, Field Gauge / TrueFuel / WROS / VALOR, drop IDs, device-binding, key mgmt, suite Evidence Vault internals, FireLedger/WRDC as live claims, hosted SoR IDs absent (absent lines + Limitations Not disclosed only)
- Visual proof: Figure 1 capture → canonicalize → dual digest → offline verify (PASS/FAIL) + without/with (post-upload vs at-capture)
- Production clean from Markdown (no DOCX artifacts)
- Technical Review + Publication Review recorded (HPS process)
- Minimum credibility length met; teach-don't-sell tone verified
- No Netlify publish (held); parent attaches PDF only for peer review
- Series discipline: Essay 2 of 4 only; Essay 1 done; T14–T15 not started; Final Cut masters not overwritten; honest tense (no live national registry / permanence / partnership overclaim); CC-BY-ND pointer to GFMS-1.0 retained

© 2026 High Plains Shield, LLC. All rights reserved. Related open-standard text (GFMS-1.0) licensed CC-BY-ND 4.0; this essay is not a derivative substitute for that specification.