

Cryptographic Fuel Intelligence (CFI)

Technical White Paper — Public Cut

How physical ground measurements become cryptographically sealed, auditable records — interface architecture and provenance (without proprietary internals)

Field	Value
Document ID	HPS-09-WPO-01-PUB
Version ID	1.0
Effective Date	2026-09-24
Supersedes	none (public cut)
Classification	Technical Public
Author	High Plains Shield, LLC
Format	F3 — Technical white paper (per HPS-PUB-STD-001 v1.1)
Audience	Operations & engineering · Asset management · Risk & compliance · Audit / GIS
Based on	HPS-09-WPO-01 TM Final Cut (internal master retained; not overwritten)

Executive Abstract (short)

Wildfire fuel layers used for WMP dockets, insurance renewals, and litigation discovery often cannot be independently audited. Satellite composites, aerial estimates, and analog field notes may be operationally useful, yet they typically lack collection-time integrity proof and attributable observer custody.

Cryptographic Fuel Intelligence (CFI) is an enterprise technology **category** — not a product SKU and not “the open standard.” CFI defines the properties fuel data must satisfy to be independently auditable: physical ground measurement, cryptographic sealing at capture, and verifiable observer custody. **GFMS-1.0** is the open **interface standard**. **PlotSeal** names the **registry / system of record** concept that holds sealed measurements for verification and docket use. **RiskWise** is a **commercial vehicle** that may deliver CFI-conformant field programs; it is not the category and not the standard.

This Technical Public white paper goes deeper than the executive cut on **interfaces and provenance** — dual-digest structure, RFC 8785 canonicalization at category level, sealed payload *classes*, offline verification workflow, and GFMS interchange expectations. It does **not** disclose proprietary collection engines, named scoring/exposure engines, registry implementation architecture, calibration recipes, trade-secret thresholds, pricing, or go-to-market programs. Soft next step only: read GFMS-1.0 (Public) and evaluate current fuel layers against CFI properties.

1. Problem — The Auditability Gap in Current Fuel Data

The wildfire fuel mapping industry commonly relies on three data sources: satellite-derived vegetation-index composites (e.g., Landsat-resolution NDVI stacks), airborne LiDAR-derived canopy/fuel estimates, and analog field-note surveys digitized into GIS. Each can be useful for planning. None of them, by itself, typically satisfies independent cryptographic auditability.

Auditability (technical sense) requires three properties that many legacy sources do not co-provide:

Property	What it demands	Typical legacy gap (illustration)
Temporal proof	Traceability to the moment of collection	Multi-date satellite stacks; flight-level (not plot-level) LiDAR time; optional analog timestamps
Observer attribution	Traceability to who measured, with which instrument/method class	No observer identity on remote products; analog signatures without cryptographic binding
Tamper evidence	Detectable mismatch if any sealed field changes after capture	Absent from most standard fuel-mapping products

Claim (problem thesis): This is primarily a **provenance** gap, not merely a resolution or model-accuracy gap. Measurements may be careful; processes may be rigorous; people may act in good faith — none of that is proven from the data itself unless the record carries collection-time integrity and custody.

***Softened comparative note (teach, don't sell):** Many satellite, aerial, and analog programs remain valuable for situational awareness and planning context. They typically do **not**, by themselves, satisfy all CFI properties at once. That is a category boundary — not a claim that every non-CFI product is unfit for every use.*

Consequence: When fuel data appears in a WMP docket, rate case, underwriting file, or discovery package, authentication challenges often reduce to: *Can you prove when it was measured, by whom, and that it has not been altered?* An unverifiable composite invites post-hoc alteration arguments even when no alteration occurred.

2. Category Requirements — CFI Interface Properties

Cryptographic Fuel Intelligence (CFI) defines a class of wildfire fuel data systems. A system claiming CFI-class properties must satisfy the following requirements at the **interface / evidence** level:

C1 — Physical ground measurement

CFI-class data originates from plot-level physical measurement by a human observer with a calibrated instrument class. Remote sensing, aerial imagery, and modelled estimates may provide context; they are not substitutes for the sealed physical anchor. Measurement occurs against an open grid/cell scheme consistent with GFMS-1.0 spatial support (e.g., fine cells on the order of ~30×30 m) and records physical fuel attributes with explicit **basis** tags (Measured / Modelled / Grounded) as published in GFMS-1.0.

C2 — Sealed at capture

The measurement payload is cryptographically sealed on the field device at the moment of capture — before network transmission where connectivity is absent — using NIST-approved digest functions over a canonical payload. Post-transmission-only sealing introduces a custody gap between field collection and ledger entry that is unacceptable under CFI. CFI-conformant systems disclose the digest algorithm(s) used at the interface.

C3 — Tamper evidence

Any post-seal modification to a sealed field (including location, timestamp, or measured values) produces a detectable digest mismatch under independent verification. Verification must be executable by a third party with standard SHA-256 (and, where dual-digest is claimed, SHA3-256) implementations — **without** requiring proprietary sealing-library source code.

C4 — Observer chain of custody

Every sealed record includes attributable observer identity (or authorized role) and instrument/method context in the sealed payload. Custody cannot be added, removed, or changed without breaking the seal. Gaps in sealed coverage (cells without a sealed measurement) are flagged in GFMS-1.0-conformant output.

Naming lock: CFI is a **category**. It is **not** “the emerging standard” and not a product. The open standard in this stack is **GFMS-1.0**. RiskWise is a commercial vehicle that may implement CFI-conformant workflows; PlotSeal names the registry / SoR concept.

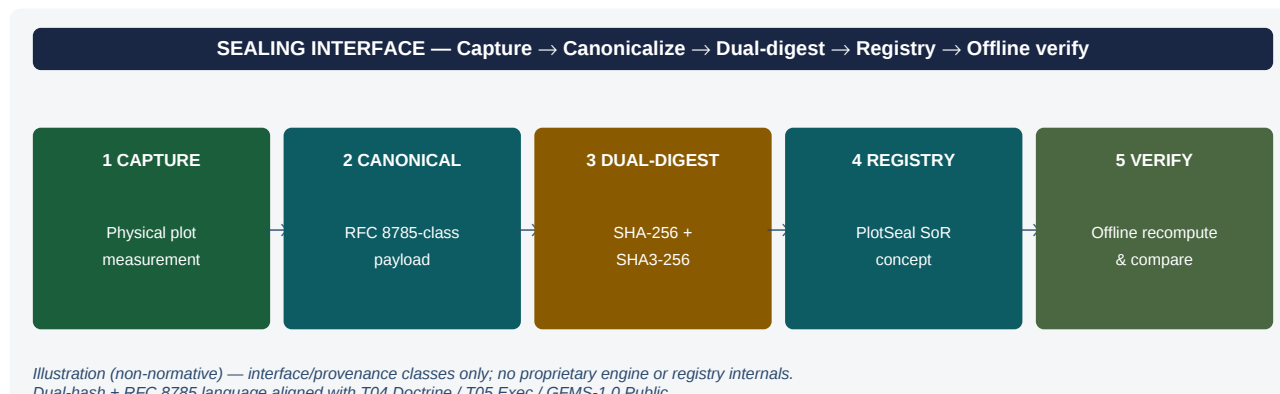


Figure 1 — Sealing interface flow (capture → canonicalize → dual-digest → registry → offline verify). Illustration (non-normative).

3. Architecture at Interface Level — Provenance Without Trade Secrets

This section describes **what interfaces and evidence classes** CFI-class systems expose. It does **not** disclose proprietary field-collection engines, registry internals, device-binding or key-management architecture, commercial scoring/exposure engines, calibration recipes, or trade-secret thresholds.

3.1 Dual-digest sealing (public-safe)

CFI-class sealing applies two independent NIST-approved digests to every sealed record:

Digest	Informative role
SHA-256 (FIPS 180-4)	Primary, widely deployed digest; verifiable in standard libraries and CLI tools
SHA3-256 (FIPS 202)	Secondary, architecturally independent (Keccak sponge); dual-algorithm posture reduces single-algorithm risk

Claim (integrity property): Both digests are stored with the sealed record (and in the registry / SoR extract). Independent verification recomputes both from the canonical payload and confirms both match. A match on one digest alone is not treated as full dual-digest success where dual-digest is claimed.

3.2 Canonicalization (RFC 8785 class)

Before hashing, the measurement payload is serialized under an **RFC 8785 JSON Canonicalization Scheme (JCS)**-class representation so that: object keys order deterministically; optional whitespace outside strings is eliminated; string Unicode form is normalized; and numeric serialization is deterministic for the declared precision rules of the interface. **Implication:** Any party with the raw sealed export and a compliant RFC 8785 implementation can reconstruct the canonical bytes and verify digests — no proprietary viewer required.

3.3 Sealed payload — category field classes (not an implementation schema)

Public-safe sealed payloads bind the following **classes** of fields (illustrative; normative field lists live in GFMS-1.0 where published):

Class	Public meaning
Location	Geospatial coordinates and accuracy context at measurement time
Time	Collection timestamp (UTC) bound into the seal
Custody	Observer identifier (or authorized role) and instrument/method identifier
Spatial key	Open grid/cell identifier consistent with GFMS-1.0 spatial support
Measured attributes	Physical fuel observations (e.g., depth, load, moisture, canopy cover, surface type) with basis tags
Seal metadata	Digest algorithm identity / seal version for future algorithm agility

Out of scope here: Exact proprietary field schemas, instrument product names, decision-tree classification codes, risk/exposure engine outputs, and internal calibration blocking logic. Those belong in Format **F5** Operational Specifications (internal / NDA / Partner) per HPS-PUB-STD-001 §3–§4.

3.4 Offline verification workflow (interface)

A third-party auditor can verify integrity **without** High Plains Shield system access:

- Receive the sealed JSON export for the site and date range
- Receive the registry / SoR hash-ledger extract for the same scope
- For each record: canonicalize → compute SHA-256 and SHA3-256 → compare to ledger entries
- Any mismatch is a tamper flag on that record

Python standard libraries or OpenSSL-class CLI tools are sufficient for steps 3–4. **Illustration:** this is documentary-evidence posture, not a guarantee of acceptance in every jurisdiction.

3.5 Open vs. proprietary boundary

Open (interface)	Not disclosed in this Public cut
Representation rules, basis taxonomy, spatial support, uncertainty fields as in GFMS-1.0	Proprietary field-collection execution engines
RFC 8785 canonicalization + dual-digest structure	Registry implementation architecture; key-management; device attestation internals
Conformance checklist for claiming GFMS-1.0 compliance	Commercial scoring / exposure / classification engine internals
Offline verification procedure (above)	Calibration recipes, weights, thresholds, pricing, GTM playbooks

Allowed public phrase: Proprietary field-collection protocols may produce GFMS-1.0-conformant payloads; they are not required for external conformance.

4. GFMS-1.0 — Open Interoperability Interface

The **Grounded Fuel Mapping Standard (GFMS) version 1.0** is the open **interface standard** published by High Plains Shield, LLC (see Document ID **HPS-09-MAP-01**, Technical Public). It defines interchange format, spatial support, basis tags, uncertainty representation, and cryptographic seal structure that CFI-conformant systems use for auditable spatial fuel records.

Informative use cases: (1) regulatory / WMP-style documentary packages; (2) third-party audit by underwriters, consultants, or discovery teams; (3) multi-vendor interchange so an operator can change commercial vehicles without losing sealed history.

4.1 Spatial support (public summary)

- Fine cell scheme consistent with common remote-sensing native resolutions and fuel-mapping conventions (e.g., ~30×30 m cells)
- Projected coordinates with cell IDs encoding zone and grid precision as published in GFMS-1.0
- Coverage completeness: outputs **should** distinguish sealed ground measurements from interpolated or unmeasured cells; interpolated cells are not treated as CFI-sealed anchors for audit purposes

4.2 Interchange

GFMS-1.0 JSON-class output is designed for ingestion by GIS platforms that accept JSON with spatial fields (e.g., ArcGIS, QGIS, FME-class tools) without a proprietary viewer. Licensing and normative clauses are those of the GFMS-1.0 Public cut — not restated here.

Naming lock: GFMS-1.0 describes **what** must be representable for interchange and conformance. It does **not** require any one vendor's collection engine. Registry / SoR implementation (PlotSeal concept) is separately bounded: public documents may describe dual-hash / RFC 8785 / category-level provenance; implementation depth remains internal.

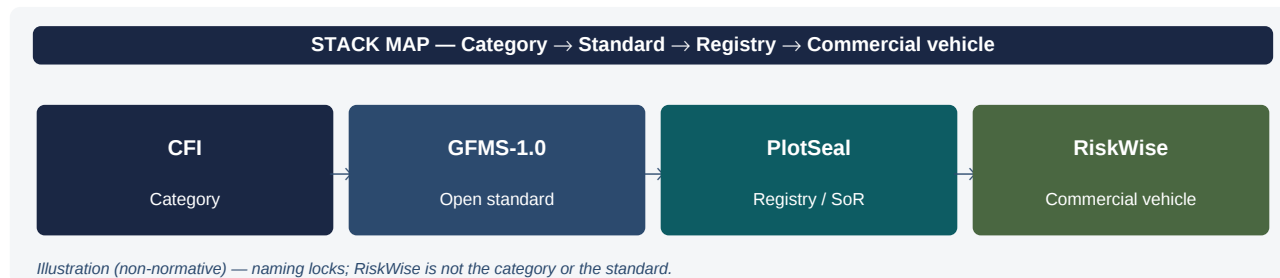


Figure 2 — Stack map: CFI → GFMS-1.0 → PlotSeal → RiskWise. Illustration (non-normative).

5. Mapping — CFI, GFMS-1.0, PlotSeal, RiskWise

Name	Role	Public classification
CFI	Category / discipline boundary	This technical WP + Doctrine (HPS-09-CFI-01-PUB) + Exec WP (HPS-09-WPE-01-PUB)
GFMS-1.0	Open interface standard	Technical Public open standard (HPS-09-MAP-01)
PlotSeal	Registry / SoR concept for sealed measurements	Named SoR concept; not "Wildfire Data Center"; implementation internals not public
RiskWise	Commercial vehicle for CFI-conformant field programs	Commercial packaging (not the category; not the standard)

5.1 Capability classes for a CFI-conformant commercial program (illustration)

At technical altitude — capability classes, **not** internal module codes or named proprietary engines:

- **Field program** — GIS pre-plot against an open grid/cell scheme; calibrated instrument class; registered observer identity and instrument state before collection; on-device sealing at observation time (including offline capture with later sync).
- **Sealed ground record** — physical measurements as the foundation; optional derived classification and risk/exposure overlays that remain **traceable to sealed measurements** rather than asserted solely from imagery; export in GFMS-1.0 interchange format.
- **Registry / SoR extract** — hash ledger / seal extract enabling independent offline verification of integrity and custody for the engagement's date range.

RiskWise (commercial vehicle — context only): RiskWise, developed by High Plains Shield, LLC, is one commercial vehicle that may operationalize CFI-conformant workflows and deliver a sealed **Ground Record** package suitable for WMP documentation, insurance files, and discovery readiness. Mention here is **implementation context**, not the thesis of this paper. Category membership does not require exclusive use of any one vendor.

6. Validation, Uncertainty, and Out-of-Scope Notes

Topic	Public posture
Validation campaigns / field accuracy studies	Out of scope for this Public cut; belong in scoped technical annexes or F5 materials under appropriate classification
Uncertainty representation	Interface rules for declaring uncertainty live in GFMS-1.0; quantitative performance claims for any engagement are out of scope here
Modelled / interpolated cells	Must be basis-tagged and must not be presented as sealed physical anchors
Derived overlays (classification, risk, exposure)	May exist in commercial vehicles; public docs require only that derived values remain traceable to sealed measurements where CFI-class claims are made — engine internals stay internal
Calibration routines & weights	Trade-secret / F5 territory; not published here

Claim labeling rule: Any quantitative accuracy, timeline, or cost assertion for a commercial engagement must be labeled **claim**, **requirement**, or **illustration** in its own scoped proposal — not implied by this white paper.

7. Compliance Alignment (Informative — Not Certification)

CFI-class sealed records and GFMS-1.0 interchange are designed to **support documentation postures** common in infrastructure wildfire-risk frameworks. The following table is **informative alignment**, not a legal opinion and not a certification claim.

Framework (illustration)	Relevant documentation need	CFI / GFMS posture (public)
NERC FAC-003-class vegetation records	Time- and location-documented inspection evidence	Sealed records with location, timestamp, observer custody; machine-readable GFMS export
NFPA 850-class plant / substation fire docs	Documented fuel / exposure context near critical assets	Sealed ground records within defined clearances; derived exposure overlays only if traceable
CPUC / state WMP-style dockets	Ground-truthed, defensible spatial fuel data	GFMS-1.0 interchange; sealed custody supporting documentary challenge defense
IEEE C2 / NESC-class clearance docs	Per-span / corridor vegetation documentation	Cell coverage enabling per-span fuel-load documentation
BESS fire-hazard docs (NFPA 855 / IFC-class)	Hazard documentation near energy storage	Sealed measurements in standoff context; exposure modelling internals not public
Pipeline ROW vegetation (PHMSA-class)	Location-dated vegetation management evidence	Sealed measurements with location and date aligned to ROW documentation needs

Operators should confirm applicability with qualified regulatory counsel. High Plains Shield, LLC does **not** assert that any commercial vehicle is "certified" under the frameworks above — language is limited to **aligned with / supports documentation for**.

8. Limitations — What This Document Is Not

- **Is not** an open standard (see GFMS-1.0, HPS-09-MAP-01).
- **Is not** a product datasheet, SKU list, pricing sheet, or sales proposal.

- **Is not** a disclosure of proprietary field-collection protocols, PlotSeal **implementation** architecture, key-management, device attestation, named commercial scoring/exposure/classification engines, calibration recipes, weights, or trade-secret thresholds.
- **Is not** a go-to-market program plan or competitive win/loss playbook.
- **Does not** claim that every remote-sensing or aerial product is unfit for all uses; it claims those approaches alone typically do not satisfy all CFI properties where physical, sealed, custody-bound fuel mass is decision-critical.
- **Does not** guarantee regulatory, insurer, or court acceptance in any specific matter.
- **Does not** overwrite or replace the internal Final Cut master (HPS-09-WPO-01 TM Final Cut).
- **Does not** reopen locked sibling Public cuts (HPS-09-CFI-01-PUB; HPS-09-WPE-01-PUB; HPS-09-MAP-01).
- **Does not** publish Format F5 Operational Specification content.

Quantitative performance, timeline, or cost claims for any commercial engagement are **out of scope** here.

9. Glossary

Term	Public meaning
CFI	Enterprise technology category for physical, cryptographically proven fuel intelligence. Not “the standard.”
GFMS-1.0	Open interface standard for representation, spatial support, uncertainty, and cryptographic provenance of physical fuel data.
Basis	Mandatory tag: Measured / Modelled / Grounded.
Dual-hash / dual-digest	Concurrent SHA-256 and SHA3-256 digests over a canonical payload.
RFC 8785 / JCS	JSON Canonicalization Scheme — deterministic serialization class used before hashing.
Observer custody	Attributable chain binding observer (or role), place, time, method class, and evidence to the sealed record.
PlotSeal	Registry / SoR concept. Not “Wildfire Data Center.” Implementation internals not public.
RiskWise	Commercial vehicle . Not the category; not the open standard.
Ground Record	Sealed, custody-bound package of field measurements and interchange exports.
Offline verification	Ability to check digests without proprietary API authentication or vendor intervention.
Technical Public	Classification for technical documents approved for external distribution under HPS-PUB-STD-001 (deeper interface depth than general Public primers; still no Level 3–4 secrets).

10. Soft Next Step (Teach, Don't Sell)

- Inventory current fuel layers against C1–C4 (physical ground measurement · sealed at capture · tamper evidence · observer custody).
- Read **GFMS-1.0** (Public cut) — Document ID HPS-09-MAP-01 — for normative interface requirements.
- Read **CFI Doctrine** (Public) — HPS-09-CFI-01-PUB — and the **Executive White Paper** (Public) — HPS-09-WPE-01-PUB — for category and executive framing.
- Contact High Plains Shield, LLC at info@highplainshield.com for standards clarification or conformant-implementation questions — not a product hard sell.

High Plains Shield, LLC · Defending Property. Protecting Infrastructure.
info@highplainshield.com · highplainshield.com

Document Control

Field	Value
Document ID	HPS-09-WPO-01-PUB
Title	CFI Technical White Paper — Public Cut
Version	1.0
Effective	2026-09-24
Supersedes	none (public cut)
Classification	Technical Public
Author	High Plains Shield, LLC
Governing house standard	HPS-PUB-STD-001 v1.1
Internal master (retained)	HPS-09-WPO-01 TM Final Cut
Contact	info@highplainshield.com

Revision History

Version	Effective	Summary / Gates
TM Final Cut	prior	Internal technical white paper (master retained; not overwritten). Prior packaging included Business Confidential face, PlotSeal implementation depth, named field/scoring engines, field-protocol recipes, and absolute industry-failure claims — not public.

Version	Effective	Summary / Gates
Public v1.0	2026-09-24	Parallel Technical Public cut: High Plains Shield, LLC sole authorship; face block; Classification Technical Public; F3 Technical spine; naming locks; absolute claims softened; Field Gauge/TrueFuel/WROS/VALOR internals, PlotSeal implementation depth, calibration/weights/trade secrets, GTM/pricing scrubbed; dual-hash / RFC 8785 / category-level provenance retained public-safe; Figures 1–2; Limitations + Glossary; soft CTA; clean Markdown → PDF. Author → Technical Review → Publication Review → Release recorded under High Plains Shield, LLC process.

Pre-Publish Checklist (Hard Gate) — Recorded Pass

- Format F3 Technical; short exec abstract · problem · interface architecture/provenance · GFMS/PlotSeal/RiskWise mapping · validation/uncertainty OOS · limitations · glossary · soft CTA
- Author = High Plains Shield, LLC everywhere (incl. metadata)
- Face block complete (Document ID · Version · Effective · Supersedes · Classification · Author)
- Naming locks: CFI=category · GFMS-1.0=standard · RiskWise=commercial · PlotSeal=registry/SoR · restricted method codes absent · not “Wildfire Data Center”
- Claims vs illustrations labeled; Limitations + Glossary present
- IP gate cleared: FMES/HPFS/Method 1.1/Structural MVE/PlotSeal implementation/Field Gauge/TrueFuel/WROS/VALOR engines/trade secrets/calibration/weights/GTM-pricing absent; dual-hash/RFC 8785 retained public-safe as T04/T05
- Visual proof: Figure 1 (sealing interface flow) + Figure 2 (stack map)
- Production clean from Markdown (no DOCX artifacts); Final Cut master not overwritten
- Technical Review + Publication Review recorded (HPS process); No Netlify (held to T19)
- Teach-don't-sell tone verified; deeper than Exec WP on interfaces without Level 3–4 leakage; T04/T05 not reopened

© 2026 High Plains Shield, LLC. All rights reserved.