CLASSIFICATION: PUBLIC — OPEN STANDARD — DEFENSIVE PUBLICATION

UNIFYWEAVE™ TECHNOLOGIES

FAS-26

Core Specification

Standard for Cryptographic Data Integrity and Sovereign Audit

VERSION	**2.0 (Major Release)**
DATE	April 2026
CLASSIFICATION	Public / Open Standard
AUTHOR	David Krause, Dipl.-Wirtsch.-Ing. (FH)
PUBLISHER	UnifyWeave™ Technologies
URI	**unifyweave.ai/standards/fas-26**
STATUS	Normative / Defensive Publication
SUPERSEDES	V1.0.1 (April 2026)

TABLE OF CONTENTS

Contents

1 Preamble: The Integrity Deficit

In modern digital and corporate ecosystems, a fundamental evidentiary asymmetry persists. Institutions—banks, insurers, cloud providers, public administrations—dictate truth through proprietary legacy systems, black-box algorithms, and opaque compliance processes. Individuals and small enterprises lack the tools to independently verify, document, and defend the integrity of their own data.

FAS-26 was developed to address this asymmetry. It defines a universal, process-oriented framework that transforms raw data into cryptographically verifiable, modular dossiers. The standard is industry-agnostic, jurisdiction-independent, and operates on the principle of Evidence-as-Code: evidentiary artifacts and commercial truths are treated like immutable source code—versioned, hashed, and independently verifiable.

> **DESIGN PRINCIPLE**
>
> *FAS-26 does not replace existing legal or regulatory frameworks. It provides a technical layer that strengthens the evidentiary value of data within those frameworks. The standard is the scaffolding; the law remains the building.*

2 Scope & Applicability

This standard applies to any process that transforms raw data into verifiable, stakeholder-facing dossiers—regardless of industry, legal jurisdiction, or data format.

FAS-26 is applicable to, but not limited to: forensic compliance audits, regulatory escalations, industrial cost accounting, financial reporting, identity verification, and cross-border documentation transfers.

The standard defines the process architecture (Sections 5–6), the dual application profiles (Section 7), the minimum output requirements (Section 8), and the full module registry (Section 9). Implementation-specific guidance is published separately in the FAS-26/F Implementation Guide (forensic applications) and the FAS-26/I Implementation Guide (industrial applications).

3 Normative References

Reference	Description
`eIDAS Regulation`	(EU) No. 910/2014 — Electronic identification and trust services
`ISO 8601`	Date and time format
`SHA-256`	NIST FIPS 180-4 — Secure Hash Standard
`RFC 3227`	Guidelines for evidence collection and archiving
`RFC 5322`	Internet Message Format (for EML-based evidence)
`EU AI Act`	Regulation (EU) 2024/1689 — for AI-assisted audit phases
`ISO/IEC 27037`	Guidelines for identification, collection, acquisition and preservation of digital evidence
`ISO 17100`	Translation services requirements (relevant for CJP module)

4 Terms and Definitions

The following terms are defined for the purposes of this specification. Terms are listed alphabetically. Definitions marked [NEW] were introduced in V2.0.

Auditor

The natural or legal person executing the FAS-26 process. The Auditor assumes responsibility for the integrity of the dossier and signs the Seal in Phase 5.

AuditReady

A conformity predicate. A document or export bearing the AuditReady designation confirms that it was produced through a complete FAS-26 5-Phase Loop and carries at minimum a Level 1 Seal.

Base Hash

The SHA-256 hash generated for each Ingest Artifact at the moment of capture in Phase 1. The Base Hash is the atomic unit of the integrity chain.

Completeness Confirmation

The documented closure of Phase 1. Records the total number, format, and Base Hash of all ingested artifacts, fixing the evidentiary scope of the dossier.

Dossier

The structured output of a complete FAS-26 process. Designated as MAD (Profile F) or IAD (Profile I).

Evidence-as-Code

The governing paradigm of FAS-26. Evidentiary artifacts and commercial calculations are treated as immutable, versioned, and hashable data objects—analogous to source code in software engineering.

IAD (Industrial Audit Dossier)

The dossier output of a FAS-26/I process. Contains verified commercial calculations with cryptographic integrity proof.

Ingest Artifact

A raw data object entering the FAS-26 process in Phase 1, preserved in its original format without conversion.

MAD (Modular Audit Dossier)

The dossier output of a FAS-26/F process. Contains forensic evidence with chain-of-custody documentation.

Master Hash

The SHA-256 hash computed over all component hashes of the dossier in Phase 5. The Master Hash is the single verification point for the entire dossier.

NexusWeave Validation [NEW V1.0.1]

A cross-referencing methodology that compares counterparty representations against verified evidence to produce a forensic verdict per domain. Applicable in both Profile F and Profile I. See Module NXW in Section 9.

Profile

The application context assigned in Phase 3 (TRANSITION). FAS-26 defines two Profiles: F (Forensic) and I (Industrial).

Seal

The cryptographic closure applied in Phase 5. FAS-26 defines three Seal Levels.

Sovereign Perimeter

The isolated processing environment in which the FAS-26 process executes. See Axiom 1 for the definition of isolation.

Stakeholder Matrix

A structured registry of external recipients generated in Phase 3 of Profile I. Lists intended recipients (banks, auditors, tax authorities) with their information requirements.

Target Matrix

A structured registry of accountable parties generated in Phase 3 of Profile F. Lists named individuals or institutions with their specific contribution to the compliance defect.

5 The Four Axioms

The FAS-26 standard operates independently of industry and legal system, provided the following four axioms are satisfied. A process that violates any axiom cannot claim FAS-26 conformity.

5.1 Axiom 1 — Offline First (Zero-Trust Infrastructure)

Data integrity shall not be delegated to external cloud providers or third-party servers. The processing and sealing of data must occur within a Sovereign Perimeter controlled by the Auditor.

> **REQUIREMENT**
>
> The core functions of the FAS-26 process (computation, analysis, and sealing) shall not require any active external network connection at the time of execution. Passive network connections (operating system updates, background services) do not break conformity, provided they are not involved in the data processing or sealing pipeline.

Rationale: Dependence on external infrastructure introduces a third-party trust assumption. If the computation or sealing process can be influenced by an external server, the Auditor cannot guarantee the integrity of the output. Offline-first execution eliminates this attack vector.

5.2 Axiom 2 — Non-Repudiation

The system must guarantee that neither the sender nor the recipient of information can subsequently deny the existence, content, or timestamp of a data transmission or document.

> **REQUIREMENT**
>
> Every output of the FAS-26 process shall contain sufficient cryptographic and temporal metadata to independently verify its origin, content, and creation time without reliance on the Auditor's testimony.

5.3 Axiom 3 — Graduated Seal Methodology

Every output of the FAS-26 standard must carry a verifiable Seal. The standard defines three Seal Levels with increasing evidentiary strength. The minimum required level depends on the assigned Profile.

LEVEL 1	LEVEL 2	LEVEL 3
BASE SEAL	**TIMESTAMPED**	**QUALIFIED**
SHA-256 + ISO 8601 timestamp (local)	*Level 1 + external timestamp*	*Level 2 + eIDAS QES*
F: MIN	F: REC	F: REC
I: MIN	I: OPT	I: OPT

LEGEND

MIN = Minimum required for FAS-26 conformity · REC = Recommended for cross-border use · OPT = Optional enhancement. Higher Seal Levels include all requirements of lower levels.

> **REQUIREMENT**
>
> A FAS-26-conformant dossier shall carry at minimum a Level 1 Seal. The Seal Level shall be declared in the Dossier Header.

5.4 Axiom 4 — Determinism

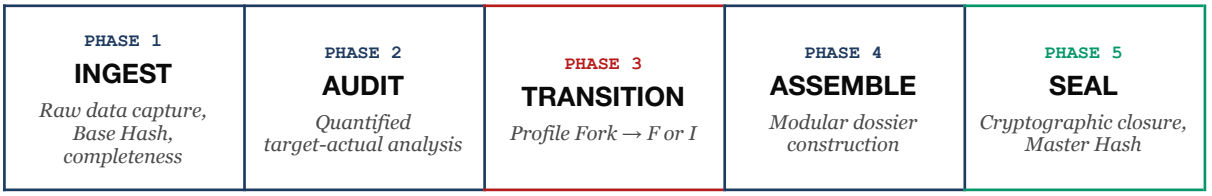
The FAS-26 process must produce reproducible results. Identical input data, processed with identical configuration, must yield an identical output—excluding only the timestamp and Seal metadata, which are inherently unique per execution.

> **REQUIREMENT**
>
> The computational core of a FAS-26-conformant system (Phases 1–4) shall be deterministic. If the system incorporates AI or machine-learning components, these components shall operate in inference mode with fixed weights and shall not alter their behavior between executions. All AI-generated outputs shall be flagged as such and subject to human confirmation before inclusion in the dossier.

Rationale: A dossier that produces different results from the same input is, by definition, not auditable. Determinism is the precondition for independent verification by third parties (regulators, courts, auditors).

6 The 5-Phase Loop

Any process bearing the designation “FAS-26 Compliant” or “AuditReady” shall complete the following five phases in sequence. No phase may be omitted. The output of each phase serves as the mandatory input for the subsequent phase.



PROCESS FLOW

Phase 1 (INGEST) → Phase 2 (AUDIT) → Phase 3 (TRANSITION: Profile Fork) → Phase 4 (ASSEMBLE) → Phase 5 (SEAL). Phase 3 is the critical branch point where the dossier is routed to either Profile F (Forensic) or Profile I (Industrial). The branch determines the character of Phase 4 output.

6.1 Phase 1: INGEST — Raw Data Capture and Isolation

Definition: The moment at which the primary source (email, server log, accounting export, machine data file, contractual document, or any other raw artifact) enters the FAS-26 process.

REQUIREMENTS

(a) The Ingest Artifact shall be preserved in its original format. No conversion, reformatting, or content modification shall occur during Phase 1. (b) An initial SHA-256 hash (Base Hash) shall be generated for each individual Ingest Artifact at the moment of capture. (c) Phase 1 shall conclude with a documented Completeness Confirmation that records the total number, format, and Base Hashes of all ingested artifacts. This confirmation fixes the evidentiary scope of the dossier.

Output: A set of unmodified Ingest Artifacts, each with a Base Hash, and a Completeness Confirmation document.

6.2 Phase 2: AUDIT — Analytical Deconstruction

Definition: The engineering or forensic analysis phase. The Auditor isolates the discrepancy between a defined target state (contract, regulation, commercial logic) and the actual state as evidenced by the Ingest Artifacts.

REQUIREMENTS

(a) The output of Phase 2 shall contain at least one quantifiable metric that numerically represents the target-actual comparison. Narrative-only findings without quantification do not satisfy this requirement. (b) The analysis shall be conducted without emotional, speculative, or narrative assessment. FAS-26 mandates the language of an auditor, not an advocate. (c) If AI components are used in Phase 2, their contribution shall be flagged, confidence scores disclosed, and results subject to human validation (per Axiom 4 and EU AI Act Art. 14).

Output: A technical audit report containing quantified findings, methodology disclosure, and references to the specific Ingest Artifacts analyzed.

6.3 Phase 3: TRANSITION — The Abstraction Lever (Profile Fork)

Definition: The strategic routing phase. The Auditor assigns the dossier to one of two application Profiles, which determines the character of the output.

PROFILE F

FORENSIC

Mode: Weaponize
Output: Target Matrix
Dossier: MAD

PROFILE I

INDUSTRIAL

Mode: Validate
Output: Stakeholder Matrix
Dossier: IAD

REQUIREMENTS

(a) The Auditor shall document the Profile assignment (F or I) with a written rationale. The assignment is binding for the entire dossier. (b) Profile F (Forensic): Phase 3 executes as WEAPONIZE—the identification of accountable parties, regulatory violations, and escalation pathways. Output: a Target Matrix. (c) Profile I (Industrial): Phase 3 executes as VALIDATE—the verification of commercial accuracy, plausibility checks, and bias neutralization. Output: a Stakeholder Matrix.

6.4 Phase 4: ASSEMBLE — Modular Synthesis

Definition: The construction of the final dossier from the outputs of Phases 1–3. The dossier format depends on the assigned Profile: MAD for Profile F, IAD for Profile I.

REQUIREMENTS

(a) The assembled dossier shall comply with the Minimum Dossier Requirements defined in Section 8. (b) The dossier shall maintain an unbroken reference chain from the final output back to each individual Ingest Artifact (chain of custody). (c) The specific module structure of the dossier is governed by the Module Registry (Section 9) and the respective Implementation Guide.

Output: A structured dossier (MAD or IAD) meeting all minimum requirements.

6.5 Phase 5: SEAL — Cryptographic Closure

Definition: The irreversible finalization of the dossier. After sealing, no component of the dossier may be modified without breaking the Seal.

REQUIREMENTS

(a) The Seal shall include a Master Hash (SHA-256) computed over all component hashes of the dossier. The Master Hash is the single verification point for the entire dossier. (b) The Seal Level (1, 2, or 3 per Section 5.3) shall be declared in the Dossier Header and shall meet the minimum level required for the assigned Profile. (c) The sealed dossier shall be deposited in a location accessible to the intended stakeholders (regulatory portal, secure web vault, physical medium).

Output: A sealed, immutable dossier with declared Seal Level, ready for external distribution.

7 Dual Manifestation: Profile F and Profile I

To ensure the integrity of the core standard across different application domains, FAS-26 forks into two dedicated Profiles at Phase 3. Both Profiles share the same axioms, the same 5-Phase Loop, and the same Seal methodology. They differ only in the purpose and character of Phase 3 and in the structure of the output dossier.

7.1 FAS-26/F (Forensic Standard)

Attribute	Specification
Domain	Compliance monitoring, fraud detection, regulatory escalation, litigation support
Phase 3 Mode	WEAPONIZE — Identification of regulatory violations, assignment of personal accountability
Phase 3 Output	Target Matrix (named individuals/institutions with assigned liability categories)
Dossier Type	`MAD (Modular Audit Dossier)`
Minimum Seal	Level 1 (Level 2 or 3 recommended)
Implementation	FAS-26/F Implementation Guide (separate document)

7.2 FAS-26/I (Industrial Standard)

Attribute	Specification
Domain	Industrial controlling, cost accounting, B2B pricing verification, bank-facing documentation
Phase 3 Mode	VALIDATE — Verification of commercial accuracy, plausibility checks, bias neutralization
Phase 3 Output	Stakeholder Matrix (banks, tax advisors, OEM auditors with information requirements)
Dossier Type	`IAD (Industrial Audit Dossier)`
Minimum Seal	Level 1
Implementation	FAS-26/I Implementation Guide (separate document)

AUDITREADY CONFORMITY

Products and systems bearing the AuditReady designation confirm FAS-26/I conformity: the underlying calculation was produced through the complete 5-Phase Loop and the export carries at minimum a Level 1 Seal. AuditReady is a conformity predicate reserved for software products implementing the FAS-26/I Implementation Guide in full.

8 Minimum Dossier Requirements

Regardless of Profile, every FAS-26-conformant dossier shall contain the following five components. Additional components are defined in the Module Registry (Section 9) and the respective Implementation Guides.

#	Component	Content	Phase
1	**Dossier Header**	Profile (F/I), Profile rationale, case/project reference, Seal Level declaration, Master Hash, creation timestamp	3 + 5
2	**Auditor Identity**	Full name, professional qualification, government-issued ID number, and domain competency declaration	1
3	**Ingest Documentation**	Completeness Confirmation: number, format, and Base Hash of each Ingest Artifact. Evidentiary scope statement.	1
4	**Audit Report**	Quantified target-actual analysis with methodology disclosure. References to Ingest Artifacts. AI usage disclosure.	2
5	**Integrity Manifest**	SHA-256 hash of every dossier component. Master Hash computed over all component hashes. Seal Level proof.	5

9 Module Registry [NEW V2.0]

This section provides the complete registry of FAS-26 modules. Modules are classified by status (Mandatory / Conditional / Optional) and by profile applicability (F / I / Both). The full specification of each module is given in the respective Implementation Guide.

STATUS DEFINITIONS

MANDATORY: The module must be present in every dossier of the applicable profile. CONDITIONAL: The module is required when specific conditions are met (e.g., email evidence triggers FCA). OPTIONAL: The module extends the dossier for specific contexts but is not required for conformity.

9.1 Mandatory Modules

Code	Module	Profile	Purpose
IDN	**Identity Shield**	F	Auditor qualification documentation: domain competency matrix (A/B/C), professional credentials, residency declaration
MAR	**Master Audit Report**	F	Narrative backbone: chronology, target-actual analysis, Target Matrix, quantified damages, escalation cascade
EOV	**Evidence Overview Vault**	F	Chain of custody: tabular manifest of all Ingest Artifacts with Base Hashes and Completeness Confirmation
CAL	**Calculation Report**	I	Complete cost calculation proof: BAB, MSR/RSSR per FKSt, surcharge rates, HK/SK, 4-Check integrity cascade
INT	**Integrity Manifest**	I	Cryptographic seal (AuditReady page): SHA-256 hash, timestamp, input summary, V1–V12 validation results
ABG	**Abgrenzungsdokument**	I	FiBu→KoRe demarcation: neutral items, Anderskosten, Zusatzkosten. Reconciliation of GuV vs. cost accounting

9.2 Conditional Modules

Code	Module	Profile	Trigger Condition
FCA	**Forensic Communication Audit**	F	Required when email/EML evidence is present. RFC 5322 header analysis, DKIM/SPF validation, SMTP rejection logs, eIDAS constructive receipt
FIA	**Forensic Integrity Audit**	F	Required when process or system failure is documented. SOP deviations, algorithm audits, database integrity breaches

9.3 Optional Modules

Code	Module	Profile	Use Case
SAF	**Support, Attachments & Financials**	F	Administrative shell: cover letters, forensic surcharge invoices, powers of attorney, correspondence log
SCN	**Scenario Analysis**	I	What-if planning: 4-lever parameter table (assets, utilization, labor, energy), baseline vs. scenario with delta analysis
BRG	**Bridge Document**	I	StB reconciliation: two-circuit explanation of imputed vs. booked depreciation, imputed interest, imputed entrepreneur salary
CJP	**Cross-Jurisdictional Protocol**	Both	Translation governance: bilingual mirror format, SHA-256 link between original and translation, translator qualification

Code	Module	Profile	Use Case
SWO	**Sworn Declaration**	**Both**	Personal accountability: Declaration format anchoring Auditor's testimony to the dossier by Master Hash reference
NXW	**NexusWeave Validation**	**Both**	Claim vs. Reality methodology: tabular matrix comparing counterparty claims against verified evidence with standardized verdicts

10 Version Control and Amendment Protocol

The FAS-26 Core Specification is maintained by UnifyWeave™ Technologies. Amendments follow a controlled release process to ensure backward compatibility and traceability.

Version Type	Numbering	Scope of Change
Patch	`V2.0.x`	Typographic corrections, clarifications. No normative change.
Minor	`V2.x`	New optional modules, additional normative guidance. Backward compatible.
Major	`Vx.0`	Changes to axioms, phase definitions, or minimum requirements. May break backward compatibility.

IMMUTABILITY GUARANTEE

Each published version of this specification is sealed with a SHA-256 hash and deposited at the canonical URI (unifyweave.ai/standards/fas-26). The publication history, including hashes of all prior versions, is maintained in a version log at the same URI. This ensures that no retroactive modification of the standard can occur without detection

A Appendix A: Conformity Levels

This appendix defines the conformity levels for systems and processes claiming FAS-26 compliance.

Level	Designation	Requirements
Core	**FAS-26 Compliant**	All 4 axioms satisfied. All 5 phases completed. Minimum dossier requirements (Section 8) met. Seal Level 1 or higher.
Profile	**FAS-26/F or FAS-26/I Compliant**	Core conformity + adherence to the respective Implementation Guide (including all Mandatory Modules per Section 9.1).
Product	**AuditReady**	FAS-26/I Profile conformity. The product's export pipeline completes the full 5-Phase Loop automatically. Reserved for software products.

B Appendix B: Phase Checklist (Normative)

The following checklist summarizes the mandatory outputs of each phase. An Auditor may use this checklist to verify process conformity before applying the Seal.

Phase	Mandatory Output	✓
1 INGEST	All artifacts preserved in original format	☐
	Base Hash (SHA-256) generated per artifact	☐
	Completeness Confirmation documented	☐
2 AUDIT	Target-actual analysis with quantifiable metric(s)	☐
	No emotional/narrative assessment	☐
	AI usage disclosed and human-confirmed (if applicable)	☐
3 TRANSITION	Profile (F or I) assigned with written rationale	☐
	Target Matrix (F) or Stakeholder Matrix (I) generated	☐
4 ASSEMBLE	Dossier contains all 5 minimum components (Section 8)	☐
	All required modules per Section 9 included	☐
	Unbroken reference chain to Ingest Artifacts	☐
5 SEAL	Master Hash computed and declared	☐
	Seal Level declared in Dossier Header	☐
	Dossier deposited for stakeholder access	☐

C Appendix C: Changelog V1.0 → V2.0

The following changes were introduced in V2.0. Amendments preserve backward compatibility with V1.0.x conformity claims.

Change Type	Section	Description
ADDED	**Section 9 — Module Registry**	Complete registry of all 9 FAS-26 modules (IDN, MAR, EOV, CAL, INT, ABG, FCA, FIA, SAF, SCN, BRG, CJP, SWO, NXW) with status and profile classification
EXPANDED	**Section 8 — Minimum Requirements**	Auditor Identity added as 5th mandatory dossier component (promoted from V1.0.1 inline clarification)
VISUAL	**Section 5.3 + 6**	Process diagrams added: 5-Phase Loop, Profile Fork, Seal Level Pyramid. Institutional white paper aesthetic.
REFINED	**Section 4 — Definitions**	Added definitions for Base Hash and Master Hash (clarifying V1.0.1 usage). NexusWeave Validation definition promoted from V1.0.1.
ADDED	**Section 3 — References**	Added ISO/IEC 27037 (digital evidence preservation) and ISO 17100 (translation services for CJP module)
FORMAT	**Overall**	Source format changed from PDF-only to DOCX + PDF. Enables third-party editing, review, and commentary workflows.

End of FAS-26 Core Specification V2.0

CERTIFIED AUDIT & COMPLIANCE RELEASE
Firmado por: DAVID KRAUSE (NIF: Z0759040E)
Fecha: 16/04/2026 21:56:35
Validado por UnifyWeave™ Technologies - Digital Integrity eIDAS