H-REVN Protocol

Cryptographic Integrity Framework for Verifiable Documentation

White Paper — Version 2.0

May 2026

From documents to verifiable evidence.

www.hrevn.com

contact@hrevn.com

Contents

1. Abstract

2. The Problem: Documentation Without Proof

3. The AI Manipulation Threat

4. The HREVN Approach: Integrity, Not Authenticity

5. How It Works: Evidence as a Verifiable Object

6. Product Lines

6.1 HREVN Start — AI Responsibility Kit

6.2 Professional Dossier — White Label

6.3 Evidence Bundle — Verifiable Documentation Packages

7. Sector Applications

8. What HREVN Does NOT Do

9. Technical Foundation

10. Regulatory Context: EU AI Act

11. Conclusion

1. Abstract

Across every industry, critical decisions depend on documentation: inspection reports, compliance dossiers, professional assessments, training records, and policy declarations. Yet the documents themselves offer no inherent guarantee that they have not been altered since they were created.

In 2026, generative AI has made this problem urgent. Anyone can alter a photograph, fabricate a document, or generate a convincing forgery in minutes. The question is no longer whether documents can be tampered with — it is whether the recipient can detect it.

The HREVN Protocol provides a framework in which documentation is treated as a verifiable dataset rather than as isolated files. Documents, images, and metadata are grouped into structured containers. Each container receives a cryptographic fingerprint that allows any third party to verify whether the contents have been modified after incorporation.

HREVN does not verify the truthfulness of content. HREVN verifies that content has not changed since it was incorporated.

2. The Problem: Documentation Without Proof

A building inspector delivers a report with 40 photographs and 6 technical annexes. Six months later, in a dispute, the opposing party claims the report has been modified. The inspector's only defense is: trust my word.

A compliance officer submits a dossier documenting the company's AI systems. A year later, during an audit, the regulator asks: is this the same document you submitted, or has it been updated without disclosure?

A law firm delivers an evidence package to a court. The opposing counsel questions whether the photographs are the originals or have been digitally altered.

In each case, the professional did honest work. But honest work without verifiable integrity is indistinguishable from dishonest work that has been modified. The absence of proof creates doubt, and doubt undermines trust.

Traditional documentation relies on implicit trust: we assume the sender has not altered the files. But implicit trust does not survive a courtroom, an audit, or a regulatory inspection.

3. The AI Manipulation Threat

Generative AI has fundamentally changed the threat landscape for documentation integrity. In 2024, altering a photograph convincingly required specialized software and skill. In 2026, anyone with access to a consumer AI tool can generate or modify images, documents, invoices, and reports that are visually

indistinguishable from originals.

This creates a dual problem:

First, the offensive threat: a malicious actor can fabricate or alter evidence more easily than ever before. Fake invoices, modified inspection photographs, altered contract terms — all now achievable in minutes.

Second, the defensive gap: even when documents are genuine, the professional who created them has no mechanism to prove they have not been tampered with after delivery. The burden of proof falls on the creator, but the tools to meet that burden do not exist in most professional workflows.

HREVN addresses the defensive gap. It does not detect AI-generated content. It provides a cryptographic seal at the moment of incorporation, so that any subsequent modification — whether by AI or by hand — is detectable.

4. The HREVN Approach: Integrity, Not Authenticity

It is essential to understand what HREVN verifies and what it does not.

Concept	Definition	HREVN role
Authenticity	The content is true, real, and accurate	Does NOT verify
Authorship	The content was created by a specific person	Does NOT verify
Post-incorporation integrity	The content has not changed since it was sealed	VERIFIES
Completeness	The package contains the same files as when sealed	VERIFIES
Timestamp	The package was sealed at a specific date and time	RECORDS

This distinction is not a limitation — it is a design decision. Verifying content truthfulness requires domain expertise and human judgment. Verifying integrity requires mathematics. HREVN provides the mathematics. The professional provides the judgment.

5. How It Works: Evidence as a Verifiable Object

The process follows three stages:

Stage 1 — Input

The professional gathers the original files: documents, photographs, PDFs, spreadsheets, annexes, and any supporting material. Each file enters the process exactly as provided. No conversion, no

compression, no modification.

Stage 2 — HREVN Processing

A. Digital fingerprint: A unique cryptographic hash (SHA-256) is computed for each individual file. This hash is a fixed-length string that changes completely if even a single byte of the file is modified.

B. Manifest: A structured index is generated listing every file in the package along with its hash, filename, size, and type.

C. Root hash: A single integrity fingerprint is computed from the combined state of all files and the manifest. This root hash represents the entire package. If any file changes, the root hash changes.

D. Verification instructions: The package includes plain-language instructions allowing any third party to independently verify integrity using free, publicly available tools. No proprietary software required.

Stage 3 — Output

The professional receives two deliverables:

A. Report / Dossier: A human-readable PDF summarizing the package contents, with a QR code linking to the verification record.

B. Evidence Bundle: A technical package (ZIP) containing all original files, the manifest, individual checksums, the root hash, and verification instructions. This package is the verifiable artifact.

If any file in the bundle is subsequently modified — whether a photograph is retouched, a PDF is edited, or an annex is replaced — its individual hash will no longer match the hash recorded in the manifest, and the root hash will no longer match the original seal. The modification is detected automatically by anyone who runs the verification.

6. Product Lines

HREVN applies the same integrity framework across three product lines, each designed for a different level of complexity and a different buyer profile.

6.1 HREVN Start — AI Responsibility Kit

A guided self-assessment and training kit for companies that use AI tools but have no internal policy, no training program, and no documentation.

What it includes:

- Initial assessment of AI usage within the organization
- Training modules: AI literacy, responsible use, Shadow AI risks, data handling
- Generated internal AI policy tailored to the company's responses
- Individual certificates with QR verification for each participant
- Verifiable record of the entire process (date, version, evidence)
- 90-day declared follow-up review

Target buyer:

SME managers, HR directors, compliance officers. Companies with 20-250 employees where staff already uses ChatGPT, Copilot, Gemini, or Claude daily without formal guidelines.

Also available as white-label for training academies, law firms, and compliance consultancies who want to offer AI compliance services to their own clients.

6.2 Professional Dossier — White Label

A structured documentation tool for law firms, compliance consultancies, and professional advisors who need to generate AI compliance dossiers for their clients without building their own platform.

How it works:

- The professional maintains the client relationship and provides expert judgment
- The client completes a guided questionnaire within HREVN
- HREVN structures the responses into a professional dossier
- The professional reviews, adjusts, and validates with their expertise
- A verifiable record is generated for the entire process
- The deliverable carries the professional's brand, not HREVN's

Target buyer:

Small-to-medium law firms, GDPR consultancies, compliance advisors, training academies. Professionals with 10-50 corporate clients who need to offer AI Act documentation services efficiently.

6.3 Evidence Bundle — Verifiable Documentation Packages

The full-strength product for professionals who deliver documentation packages containing documents, photographs, annexes, and technical reports — and need to prove that the delivered package has not been modified after delivery.

What it delivers:

- Individual SHA-256 hash for every file in the package
- Structured manifest indexing all files with metadata
- Root hash sealing the entire package
- Human-readable PDF report with QR verification
- Deliverable ZIP with all originals and verification instructions
- Optional blockchain anchoring for additional timestamp proof

Target buyer:

Judicial and extrajudicial experts, building inspectors, technical directors, law firms handling evidentiary packages, subsidy consultancies, and any professional who delivers documentation that may be questioned months or years later.

7. Sector Applications

Sector	Use case	Product
AI compliance	Internal AI policy, training, EU AI Act Art. 4 documentation	HREVN Start
Law firms	AI compliance dossiers for corporate clients (white label)	Professional Dossier
Expert reports	Judicial/extrajudicial reports with verifiable integrity	Evidence Bundle
Construction	Site inspection reports, progress certifications, PRL documentation	Evidence Bundle
Subsidies / EU funds	Grant justification packages with verifiable completeness	Evidence Bundle
Training / FUNDAE	Training delivery evidence with verifiable attendance and content	HREVN Start + Bundle
GDPR / Data protection	Training records, policy documentation, DPIA evidence	HREVN Start
Cybersecurity	Basic cyber hygiene training, policy, incident response (future)	Future kit
Financial regulation	MiCA whitepaper evidence, stablecoin disclosure records	Evidence Bundle

8. What HREVN Does NOT Do

Clarity about limitations builds more trust than exaggerated claims. HREVN is explicit about what falls outside its scope:

- HREVN does not verify the truthfulness or accuracy of document content
- HREVN does not verify that photographs represent what they claim to show
- HREVN does not certify legal compliance with any regulation
- HREVN does not provide legal advice or professional consulting
- HREVN does not replace the judgment of a lawyer, auditor, expert, or inspector
- HREVN does not guarantee that documents were not altered before incorporation
- HREVN does not monitor, audit, or manage the client's systems or data
- HREVN does not store sensitive client data beyond what is needed for verification

HREVN provides the infrastructure for verifiable documentation. The professional provides the expertise, the judgment, and the content. Together, they create documentation that is both professionally sound and cryptographically verifiable.

9. Technical Foundation

Hashing algorithm: SHA-256 (NIST FIPS 180-4). Industry standard, widely supported, computationally infeasible to forge.

Manifest format: Structured JSON index listing every file with its hash, filename, size, MIME type, and incorporation timestamp.

Root hash: Computed from the ordered concatenation of all individual file hashes. A single root hash represents the integrity state of the entire bundle.

Verification: Any third party can verify integrity using publicly available, free tools (sha256sum, openssl, online hash calculators). No proprietary software or HREVN account required.

QR code: Links to a verification page where the root hash and manifest can be checked against the original record.

Blockchain anchoring (optional): For cases requiring additional timestamp proof, the root hash can be anchored to a public blockchain, providing an immutable, independent record of the sealing date.

API: Production API at api.hrevn.com with OpenAPI specification. MCP server available for AI agent integration.

SDK: Open-source workflow SDK (hrevn-workflow) published on GitHub and PyPI for developers building automated verification workflows.

10. Regulatory Context: EU AI Act

The EU AI Act (Regulation 2024/1689) establishes obligations for organizations that deploy or develop AI systems within the European Union. Key provisions relevant to HREVN's value proposition include:

Article 4 — AI Literacy: Organizations must ensure that staff operating or interacting with AI systems have a sufficient level of AI literacy. HREVN Start directly addresses this requirement through its training modules and verifiable certificates.

Article 9 — Risk Management: High-risk AI systems require documented risk management processes. The Professional Dossier provides a structured framework for this documentation.

Article 11 — Technical Documentation: Providers of high-risk AI systems must maintain comprehensive technical documentation. Evidence Bundles can package this documentation with verifiable integrity.

August 2026 deadline: Article 4 obligations apply from August 2, 2026. Organizations that have not addressed AI literacy by this date face potential regulatory consequences.

HREVN does not certify EU AI Act compliance. HREVN provides documented evidence that specific steps have been taken — training delivered, policies created, assessments completed — with verifiable records of each process.

11. Conclusion

Documentation is the foundation of professional trust. Inspection reports, compliance dossiers, expert assessments, training records, and policy declarations all depend on the implicit assumption that they have not been altered.

In a world where generative AI can fabricate and modify documents with unprecedented ease, implicit trust is no longer sufficient. Professionals need a mechanism to prove that their work is exactly what they delivered — not what someone else may have changed afterwards.

HREVN provides that mechanism. Not by judging the quality of the work, but by making its integrity mathematically verifiable. The professional brings the expertise. HREVN brings the proof.

From documents to verifiable evidence.

HREVN — www.hrevn.com — contact@hrevn.com