H-REVN Protocol

Cryptographic Integrity Framework for Physical Evidence

White Paper - Conceptual Specification

Version 1.0 - March 2026

Abstract

The H-REVN Protocol proposes a conceptual framework designed to improve trust in documentation describing physical events. Across many industries, decisions depend on documentation that attempts to represent real world activities. Photographs, inspection reports, spreadsheets, and PDF files are widely used to record evidence of work performed or assets installed. However, these documents do not inherently provide guarantees of authenticity or provenance.

The H-REVN Protocol introduces a structured model in which physical evidence is treated as a verifiable dataset rather than as an isolated document. Evidence captured in the field is associated with contextual metadata and grouped into structured containers called Evidence Bundles. Each bundle can be associated with a cryptographic integrity fingerprint allowing third parties to verify that the dataset has not been altered.

The Physical Truth Gap

Digital systems have achieved high reliability when verifying purely digital information. However, reliability decreases when digital systems attempt to represent events occurring in the physical world. This discrepancy creates what can be described as the Physical Truth Gap.

A photograph may represent a real installation but it may also be taken in a different location or at a different time. A written inspection report may describe a condition but the document itself does not guarantee that the observation occurred as described. As a result many verification processes still depend on manual auditing.

Evidence as a Verifiable Object

Traditional documentation systems treat evidence artifacts separately. Images, written observations, and contextual information are often stored in different places. This fragmentation makes verification difficult and time consuming.

The H-REVN Protocol introduces the concept of the Evidence Bundle. An Evidence Bundle is a structured digital container representing the documentation of a physical event or asset state. Instead of isolated files the protocol groups images, metadata, and observations into a single coherent dataset.

Physical Veracity Mechanism

The Physical Veracity Mechanism or PVM describes the conceptual workflow through which evidence datasets are created and secured. Field operators capture evidence artifacts such as photographs or measurements during inspections or technical interventions.

Contextual metadata such as timestamps, location references, and asset identifiers are then associated with the captured evidence. The resulting dataset is structured as an Evidence Bundle and a cryptographic

fingerprint can be generated from the bundle state. Any modification of the dataset produces a different fingerprint enabling independent verification.

Institutional Applications

Structured evidence verification can improve documentation reliability across many sectors. Infrastructure operators rely on inspection reports describing the condition of assets such as buildings, energy installations, or industrial equipment. Evidence bundles can make these reports easier to verify.

Public administrations responsible for subsidies or infrastructure programs must confirm that installations or works have been completed correctly. Structured evidence datasets can simplify auditing processes and reduce the need for repeated physical inspections.

Conclusion

As digital systems increasingly depend on accurate representations of physical events the limitations of traditional documentation methods become more visible. Static documents provide useful records but they do not guarantee authenticity or integrity.

The H-REVN Protocol proposes a framework in which evidence is treated as a structured and verifiable dataset. By associating evidence artifacts with contextual metadata and cryptographic fingerprints the protocol creates a foundation for trustworthy documentation of real world events.