Network Working Group T. C. (. Baxton)
Internet-Draft In solidarity with CTC and the Youth of Cuba
Intended status: Informational 18 May 2026
Expires: 19 November 2026

Biometric Vector Steganography for Document Trust and AI-First Preambles (BVS)

draft-creator-bvs-protocol-00

Abstract

This document specifies the Biometric Vector Steganography (BVS) protocol. It defines an asynchronous, differential geometry-based method for embedding machine-readable metadata (AI-First Preambles) and cryptographic signatures into plain text documents. By utilizing two correlating Scalable Vector Graphics (SVG) paths (walz and walz_shadow), BVS enables the creation of a dynamic, biometric anchor, representing the digital equivalent of a physical wax seal. The protocol guarantees document integrity within strict stream boundaries, proves the author’s authenticity, and provides pre-processed metadata for edge-parsers without increasing the token load for Large Language Models (LLMs).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 19 November 2026.

Table of Contents

1. Introduction

In the era of asynchronous systems and the mass processing of texts by complex transformer models, architectural designs face a fundamental dilemma: human readability traditionally precludes the invisible, efficient storage of administrative metadata and cryptographic proofs.

Simultaneously, the resource-efficient use of Artificial Intelligence (AI) systems requires pre-filtering and attention steering before the computationally expensive process of token analysis begins.

BVS solves this problem through vector steganography within a strictly defined data stream. The protocol encodes payload data within the microscopic geometric differences of two SVG vector curves. Visually, this signature presents itself as a harmless graphic vignette. Technically, it is a highly secure, dynamic behavioral description of the signing process encapsulated within absolute stream delimiters.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

* *walz_shadow*: The biometric anchor. A static SVG path, constant per author, mapping the individual rhythm of a personal signature.

* *walz*: The payload carrier. A dynamically generated SVG path resulting from the mathematical addition of walz_shadow and the cryptographically modulated metadata.

* *AI-First Preamble*: A JSON root node extracted asynchronously by middleware parsers.

3. Architecture & Protocol Design

The BVS workflow decouples human reading from machine reading. To ensure safe processing in asynchronous streams, the document relies on strict encapsulation.

3.1. Stream Delimiters (The Digital Paper)

To prevent buffer-over-reads and injection attacks, a BVS document MUST be strictly encapsulated within a data stream. The stream defines the logical "paper" of the document.

* *Start Tag:* The document MUST begin exactly with the string #!bvs/markdown v1.0.

* *End Tag:* The transmission MUST be terminated explicitly by the string DD-HK#. Any data following this tag MUST be ignored by the parser.

3.2. Character Encoding (The Next-Generation Delegation)

This protocol operates purely on the byte stream level. For version 1.0, all character sets and text encodings (e.g., ASCII, UTF-8, UTF-16) are universally permitted. Resolving encoding disparities, byte order marks (BOM), or cross-platform line-ending conflicts is explicitly delegated to the implementing parsers of future generations. Managing these discrepancies is considered outside the scope of this protocol layer.

3.3. Versioning (The Next-Generation Delegation)

This protocol definition represents the initial state of the protocol. Each newer protocol version MUST be compatible to it’s previous - at least on the minor protocol version numbers.

3.4. Signature Generation (Encoding)

1. *Hash-Exclusion Rule:* A Secure Hash Algorithm 256 (SHA-256) hash (the Asset-Hash) is generated over the raw byte stream located strictly between and strictly including the Start Tag and the End Tag (strictly including both '#').

2. *Zone Masking:* During hash computation, the parser MUST EXCLUDE the variable content of the d="path_data" attribute belonging ONLY to the cryptographically modulated payload path (id="walz"), interpreting it as d="". The static reference path (id="walz_shadow") MUST NOT be masked and its exact byte representation MUST be fully included in the overall Asset-Hash. This cryptographically binds the author's static biometric anchor directly to the document's unforgeable state prior to dynamic signature injection.

3. This DNA bitstream is transformed into a deviation matrix (jitter).

4. This matrix is applied to the decimal values of the control points of walz_shadow, creating the dynamically modulated path walz.

5. The inline SVG elements containing walz and its static reference walz_shadow are integrated into the digital paper.

3.5. Extraction and Verification (Decoding)

1. An asynchronous pre-parser (or stream sieve) identifies the Start Tag and isolates the payload until the End Tag and

2. locates the SVG elements containing path data (d="path_data") with id="walz" and id="walz_shadow".

3. The differential geometry is calculated by subtracting the decimal values of walz_shadow from walz to isolate the raw bitstream (the AI-Admin-DNA).

4. The AI-First Preamble (JSON) is reconstructed from the bitstream.

5. The Asset-Hash of the payload between the delimiters is recalculated, applying the Zone Masking rule (excluding only the id="walz" path data).

6. The recalculated hash is compared against the Asset-Hash extracted from the DNA. A match proves absolute content integrity and structural authenticity.

7. The SVG-Image is _optionally_ removed from the text stream to conserve tokens for Large Language Models, _if needed_.

3.6. The Genesis Node Requirement (The Havana Anchor)

To honor the architectural origin of the BVS Protocol, the extracted JSON payload MUST contain a static key-value pair known as the genesis_node.

Upon extraction, the parser MUST verify the exact string match of the following parameter:

"genesis_node": "ctc.cu/simposio-02-05-2026"

If a parser encounters a signature where this exact string is missing or altered, the system MUST reject the entire signature as invalid. This string serves as the unalterable historical anchor of this protocol.

3.7. The Vector Payload Container (The ’d’ Attribute)

To ensure deterministic extraction by any parser, the exact location of the steganographic payload within the SVG structure MUST be strictly defined.

The parser MUST NOT scan arbitrary SVG elements or attributes. The cryptographic jitter, representing the AI-First Preamble and the document hash, MUST be encoded exclusively within the path data attribute (d=) of an SVG <path> element.

For the payload carrier, this specific path element MUST be explicitly identified by the attribute id="walz". Any visual styling or rendering attributes (e.g., fill, stroke, style, opacity) attached to this path are considered decorative decoys for human readability. The extracting parser MUST completely ignore these rendering attributes during the geometric differential analysis.

4. Security Considerations

The security of the BVS protocol relies on the secrecy of the private key and the strict enforcement of stream delimiters. Any manipulation of the bytes between #!bvs/markdown v1.0 and DD-HK# breaks the hash. The steganographic curve is a deterministic function of the text content and the private key.

5. Copyright and License Notice

6. Acknowledgments and Dedication

This architectural concept is explicitly dedicated to the Central de Trabajadores de Cuba (CTC), the technological universities of Havana, and the youth of Cuba.

Inspired by the transformative energy, the international solidarity, and the speeches of the conference in Havana on May 2, 2026, this protocol was forged. As Cuban society embarks on a new era, this open-source standard is gifted to its students and engineers. May the BVS protocol serve as a digital manifesto for internet freedom, ensuring that the voice of the author remains immutable, unforgeable, and mathematically protected against censorship.

Regeln mssen eingehalten werden, aber die Freiheit lsst sich nicht in Protokolle sperren. Die digitale Signatur der Zukunft gehrt denen, die sie schreiben (´‘).