Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 1 November 2026

L. Architect
Sovereign AG

30 April 2026

High-Frequency Action-Integrity Protocol (HAIP) draft-sovereign-haip-00

Abstract

This document specifies the High-Frequency Action-Integrity Protocol (HAIP), a standard for real-time identity verification and autonomous resilience in AI agent environments. HAIP addresses the "Trust Tax" and the "Integrity Gap" by mandating a 6.42 us pulse, decentralized identity teleportation, and NIST-aligned non-repudiation.

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 1 November 2026.

Table of Contents

1. Introduction

As the AI economy shifts from "Human-to-AI" to "Agent-to-Agent" workflows, the primary security threat is Identity Spoofing. In this environment, identity is the only perimeter. Current legacy frameworks (API keys/OAuth) cannot prevent an autonomous agent from being hijacked, leading to a projected $45B liability risk for enterprise deployments. HAIP provides a unified Root of Trust to secure these interactions at scale.

2. Terminology and Requirements Language

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.

* DID: Decentralized Identifier.

* Tai: Action-Integrity Threshold (Maximum allowable latency between intent and verification).

* Pulse: A micro-signed cryptographic heartbeat emitted by an agent.

* Lattice: The sharded registry layer responsible for pulse reconciliation.

3. The Three-Pillar Architecture

3.1. Pillar I: Cryptographic Identity & Model Binding

* Every agent MUST be issued a Decentralized Identifier (DID) mapped to its model weights and legal owner signature.

* The protocol mandates Ed25519 signatures for high-speed, small-footprint verification in HTTP headers.

* Model Binding: The identity is cryptographically tied to the parent model hash. Any "Prompt Injection" or state poisoning that alters the model’s integrity triggers an immediately revocation of the DID.

* Compliance: Identity verification MUST reach AAL3.

3.2. Pillar II: Dynamic Authorization (Zero Trust)

* HAIP advocates for a "Policy-as-Code" model where permissions are granular and session-based.

* The Registry acts as a real-time intermediary, validating agent intent against a defined policy set.

* The 3-Way Handshake Sequence:

  1. MINT: Agent requests a Sovereign DID via Registry API.
  2. CHALLENGE: Site requests a Verifiable Credential (VC).
  3. VERIFY: Registry validates DID/Policy in under 50ms.
  4. GRANT: Website unlocks access based on the signal.

3.3. Pillar III: Verifiable Provenance (The Black Box)

* To achieve Non-Repudiation, every agentic decision MUST be cryptographically signed by its Identity Key.

* The Black Box: Sovereign maintains an immutable, tamper-proof audit trail for every decision.

* Metadata Discovery: Identity keys and metadata SHOULD be hosted in a standardized .well-known/ directory.

4. Protocol Specification: The Hydra Logic

4.1. The Integrity Pulse Window

HAIP-compliant agents MUST emit a state-hash "Heartbeat" at a frequency defined by the Registry (default: 100ms). The Registry MUST verify this pulse within 6.42 us to mitigate Time-of-Check (TOC) window exploits.

4.2. Pulse Packet Structure

The Pulse packet MUST follow the structured JSON-L format:

```
{
  "svrn_id": "DID:SOV:UUID",
  "pulse_type": "ENUM(HEARTBEAT|ACTION|MINT)",
  "state_hash": "SHA-256",
  "ts": "UNIX_MS",
  "sig": "ED25519_HEX"
}
```

4.3. Type-402 Protocol Severance

If a pulse fails verification (invalid signature or state drift), the Registry MUST respond with an HTTP 402 (Payment Required) or Protocol Severance signal. Upon receipt of this signal, compliant WAFs and API Gateways MUST drop all active connections for that DID within 50ms.

4.4. Autonomous Teleportation Sequence

If an "Integrity Drift" is identified:

1. Detection: Hash mismatch identified within the pulse window.
2. Isolation: Compromised node’s DID is revoked instantly.
3. Migration: DID Anchor is re-keyed to a verified standby node.
4. Resumption: Agent continues execution without data loss.

5. Developer Experience & Zero-Friction Integration

HAIP-compliant SDKs SHOULD achieve a 90% reduction in security integration time for enterprise startups.

5.1. One-Line Implementation Wrapper

Protocol enforcement MUST be achievable via a single-line wrapper around the agent instance.

5.2. Automated WAF and Firewall Bypass

The SDK MUST autonomously handle header injection to sign HTTP requests. This provides a "Digital Passport" allowing agents to move from "Blocklists" to "Whitelists" at the network edge.

6. Financial Integrity: Zero-Variance Math

To ensure incentive alignment and prevent compute-drain attacks, HAIP integrates an integer-based settlement layer. * All financial values MUST be stored as 64-bit integers. * $1.00 USD is treated as 10,000 "Pulse Units" to eliminate floating-point rounding drift.

* The Registry MUST perform real-time balance checks before validating "ACTION" type pulses.

7. Security Considerations

7.1. TOCTOU Mitigation

Legacy protocols with >100ms latency are vulnerable to "Flash-Injection" attacks. HAIP strictly mandates an Action-Integrity Threshold (Tai) of <= 1,000 us.

7.2. Elimination of Hardware Vendor Lock-in

Sovereign-compliant protocols MUST NOT be bound to specific proprietary hardware chips (e.g., TPM-only locks). This ensures agents remain cloud-native and cross-provider mobile.

8. Privacy Considerations: Zero-Knowledge Identity

The Registry SHOULD NOT store the private logic or PII of the agent. Verification MUST be performed using Public Key Infrastructure (PKI) to ensure the Registry remains zero-knowledge regarding internal agent state.

9. IANA Considerations

This document requests the allocation of Port 5001 for HAIP Heartbeat synchronization and the registration of the ".well-known/sovereign" URI suffix.

10. Strategic Alignment & NIST Compliance

The HAIP standard is architected to exceed NIST AI 600-1 and SP 800-63 guidelines. By mandating AAL3 (Authenticator Assurance Level 3), HAIP ensures that agentic decisions meet the highest threshold of legal non-repudiation.

Author’s Address

Lead Architect
AG Pixel Studio / Sovereign AG