Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 17, 2026

K. Singh
Apex Intelligence Empire

May 16, 2026

Proof of Stateful Integrity (PSI) for Vulnerable Populations
draft-singh-apex-psi-04-00

Abstract

This document specifies the PSI-04 Protocol, a cryptographic framework for establishing the Proof of Stateful Integrity (PSI) for data involving vulnerable subjects (e.g., Clinical Trial participants, NDIS recipients, and Aged Care residents). The protocol mandates a verifiable "Chain of State" that prevents post-hoc data manipulation by ensuring the final submission is mathematically anchored to the point of inception. PSI-04 utilizes Ed25519 signatures canonicalized via RFC 8785 and verified through a 3-node Multi-Party Computation (MPC) consensus mechanism.

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 November 17, 2026.

Copyright Notice

1. Introduction

In critical human-centric sectors like Pharmaceuticals and Disability Support (NDIS), current "stateless" auditing relies on trust and retrospective reviews. PSI-04 introduces a technical mandate for Stateful Integrity, where every state-transition of a data asset--from laboratory capture to regulatory filing--is cryptographically locked. This ensures that corporate entities cannot "scrub" or alter data without breaking the mathematical integrity proof.

2. Terminology

PSI (Proof of Stateful Integrity): A mathematical proof that a data asset has maintained an authorized state-chain.

Vulnerable Population: Subjects protected under the PSI-04 mandate (NDIS, Clinical Trials).

Apex Lattice: The cross-node mesh used for multi-party authentication and consensus.

Inception-Lock: The immediate ($t < 10ms$) cryptographic anchoring of a raw signal to the lattice.

3. Protocol Architecture

3.1. Canonicalization and Signing

To ensure deterministic verification, all data payloads MUST be canonicalized using RFC 8785 (JSON Canonicalization Scheme) before signing. Verification is performed using Ed25519 digital signatures to ensure non-repudiation across the Apex Lattice.

3.2. The Integrity Equation

A data asset is considered integer if and only if:

$$State(n) == Hash(Origin + Sum\ of\ Authorized\ Transitions)$$

3.3. Multi-Party Computation (MPC) Consensus

Integrity verification is distributed across three independent nodes (Alpha, Beta, and Gamma). A 2/3 threshold consensus is required to issue a "Verified" attestation, preventing a single point of failure or corruption from compromising the proof.

4. Domain Application: NDIS and Pharma

NDIS Shield: Participant data is anonymized using hash-based identifiers while maintaining a stateful record of service delivery and compliance.

Pharma Provenance: Clinical trial data is "Inception-Locked" at the site of capture, providing regulators with a tamper-proof audit trail that satisfies EU AI Act Article 12 and 15 requirements.

5. Security Considerations

PSI-04 provides "Zero-Knowledge" accountability. Entities can prove compliance with regulatory standards without disclosing the underlying proprietary data or protected identities of vulnerable subjects.

6. IANA Considerations

This document requests the registration of the psi://vulnerable URI scheme for the global resolution of stateful integrity proofs.

7. References

[RFC8785] Rundgren, A., Jordan, B., and S. Erdtman, "JSON Canonicalization Scheme (JCS)", RFC 8785, DOI 10.17487/RFC8785, June 2020.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017.

Authors' Addresses

Kawaljeet Singh
Apex Intelligence Empire
Balaclava, Victoria, Australia
Email: kawaljeet.singh3008@gmail.com
URI: https://apex-infrastructure.com