Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 3 November 2026

S. AG (Sovereign)
SVTP Protocol
3 May 2026

Sovereign Verification & Trust Protocol (SVTP) v1.0
draft-sovereign-svtp-00

Abstract

This document specifies the Sovereign Verification & Trust Protocol (SVTP), a foundational framework for establishing verifiable identity, attribution, and governance for autonomous machines. SVTP provides a non-repudiable "Root of Trust" for both digital AI agents and physical autonomous systems (e.g., industrial robotics, autonomous vehicles). By defining the SVTP-DID (did:svtp) and the Protocol Seal mechanism, this standard enables secure machine-to-machine (M2M) interaction, automated compliance with NIST-800-218, and institutional-grade liability containment in the machine economy.

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 3 November 2026.

Additional Information and Repository Access

Official Repository: https://github.com/Sovereign-AG/sovereign-core
Official SDK: https://pypi.org/project/svtp-sdk/
Project Website: https://svtp-protocol.org
API Root Authority: https://api.sovereign.ag
Governance Body: Sovereign AG
Technical Compliance: NIST SP 800-218 (April 2026 Revision)

Table of Contents

1. Introduction

The proliferation of autonomous systems---ranging from large-scale language model agents to physical industrial automation---has created a "Trust Gap." Existing identity protocols (e.g., OAuth, SAML) assume a human-in-the-loop, which is insufficient for the high-velocity machine economy.

SVTP addresses this by establishing a decentralized, cryptographically anchored identity standard. It moves away from "permission-based" trust toward "certainty-based" trust.

2. Terminology

Sovereign Verification & Trust Protocol (SVTP): The core protocol defining the issuance and verification of machine trust.

Root of Trust (RoT): The foundational cryptographic anchor that certifies the identity and behavioral bounds of a machine.

Autonomous Machine (AM): Any software or hardware entity capable of independent decision-making and tool-execution.

did:svtp: The decentralized identifier format specific to the SVTP standard.

Controller Entity: The legal organization or institutional body responsible for the governance, liability, and cryptographic oversight of an Autonomous Machine.

3. The Three Pillars of Trust

The SVTP framework is constructed upon three immutable pillars that ensure the integrity of the Universal Root of Trust.

3.1. Pillar I: Decentralized Machine Identity (DID)

Every autonomous unit is issued a permanent did:svtp identifier. This identifier is cryptographically anchored to a verified institutional controller, ensuring that every machine has a verifiable "legal persona" in the machine economy.

3.2. Pillar II: Just-In-Time (JIT) Authorization

SVTP enforces a "Zero-Trust" model for machine agency. Trust is not granted globally; it is issued JIT for specific tool-calls or mechanical operations. This minimizes the attack surface and prevents lateral movement in autonomous clusters.

3.3. Pillar III: Immutable Audit Chain (Usage Ledger)

Every SVTP-certified action is recorded to an NDJSON-based Usage Ledger. Each entry is hashed and chained to the previous block, creating a tamper-proof record of autonomous decisions that satisfies international audit requirements.

4. Technical Architecture

4.1. Cryptographic Primitives

SVTP utilizes Ed25519 for signature generation and SHA-384 for ledger integrity. These choices prioritize high-performance M2M throughput while maintaining quantum-resistant safety bounds.

4.2. The Protocol Seal

For every high-fidelity action, the SVTP Root generates a "Protocol Seal." This seal acts as a cryptographic proof-of-intent, linking the machine’s DID to a specific timestamp and action payload.

4.3. High-Velocity Anchoring (6.42us Performance)

SVTP is optimized for mass-scale industrial deployment. The core protocol achieves a mean Anchoring and Handshake speed of 6.42 microseconds. This allows for the near-instantaneous formation of secure identity anchors and M2M trust pathways, ensuring that dynamic fleets can be provisioned and secured without computational bottlenecking.

4.4. Autonomous Self-Healing (Recovery and Continuity)

SVTP provides a unique "Self-Healing" mechanism for compromised nodes. In the event of a cryptographic breach or unauthorized behavioral drift, the protocol initiates an autonomous recovery sequence. Instead of a complete system cessation, the SVTP Root enforces a Rollback to the last verified anchor, re-issues a clean protocol seal, and restores the machine to a trusted state without service interruption. This ensures mission-critical continuity in hostile execution environments.

4.5. Global Revocation (The Kill-Switch)

In the event of an anomalous variance, the SVTP Root Controller retains the ability to issue a global signature revocation. This operation propagates in <100ms, effectively "air-gapping" the rogue unit from the trusted ecosystem.

5. Compliance Mapping (NIST-800-218 and ISO-42001)

SVTP is designed to satisfy the non-repudiation and identity provenance requirements of NIST SP 800-218. Furthermore, it aligns with ISO/IEC 42001 governance standards for trustworthy artificial intelligence systems.

6. Implementation Accessibility (Transparent Integration)

A core design requirement of SVTP is "Low-Friction Adoption." The protocol is implemented via a high-performance Transparent Proxy Architecture. This allows institutions to wrap existing autonomous models and industrial control systems in the SVTP Root without modifying the underlying logic or model weights.

By utilizing a single-line cryptographic wrapper, developers activate the Three Pillars of Trust (Identity, Auth, and Audit) instantaneously, ensuring rapid global standardization across legacy and genesis autonomous fleets.

7. Protocol Economics

To ensure the sustainability of the Root of Trust, SVTP incorporates a three-tiered settlement mechanism:
- MINT: Initial identity anchor formation ($1.00)
- ACTION: High-fidelity tool-call verification ($0.01)
- PULSE: Continuous system heartbeat monitoring ($0.0001)

8. Security Considerations

SVTP assumes a "Hostile Execution" environment. By separating the identity layer from the model logic, it prevents prompt injection or mechanical variance from compromising the institutional root.

9. Conclusion

SVTP (Sovereign Verification & Trust Protocol) is the definitive standard for the machine economy. By providing a universal Root of Trust, it enables the safe and verifiable deployment of autonomous intelligence at a multi-trillion dollar scale.

Appendix A. Reference Implementation (Quickstart)

To demonstrate the feasibility and low-friction adoption of the SVTP standard, a reference SDK is provided for rapid integration.

A.1. Installation

```
$ pip install svtp-sdk
```

A.2. One-Line Standard Implementation

The following snippet demonstrates the transparent wrapping of an autonomous function to activate SVTP Three-Pillar governance:

```
from svtp_sdk import ProtocolAnchor

@ProtocolAnchor.secure()
def autonomous_action(payload):
    # SVTP Root of Trust Active
    # Non-repudiable Audit and DID Attestation Enabled
    pass
```

A.3. Verification

Institutional controllers can verify the SVTP integrity of any machine action via the global trust endpoint:

```
$ svtp-verify --did did:svtp:72a1 --seal <PROTOCOL_SEAL>
```

Author’s Address

Sovereign AG
Email: office.sovereign.ag@gmail.com