Secure Asset Exchange

draft-marstein-satp-asset-exchange-00

SATP Working Group
IETF124 Montreal
4 November 2025

Kjell-Erik Marstein, Alex Chiriac, Luke Riley, Venkatraman Ramakrishna

SATP Scope

Develop a protocol for the secure, one way, transfer of any digital asset between networks, that is agnostic to both the technology of the network(s) and to the nature of the asset.

SATP Scope

Develop a protocol for the secure, one way, transfer of any digital asset between networks, that is agnostic to both the technology of the network(s) and to the nature of the asset.

Secure Asset Exchange Scope

Expand the SATP protocol for the secure, two way, transfer of any digital assets between networks, agnostic to both the technology of the network(s) and to the nature of the assets.

Motivation & Problem Statement

- Existing protocols handle authentication and authorization, but not asset-level exchange.
- No standard mechanism for verifiable, confidential transfer of digital assets between independent parties.
- Ad-hoc solutions create interoperability gaps, security risks, and trust fragmentation.
- SAEP provides a common, secure framework for exchanging digital assets over existing IETF infrastructure.

Design Goals

- Security first: cryptographic integrity, authentication, and replay protection.
- Interoperability: compatible with TLS, JOSE, and OAuth frameworks.
- Extensibility: modular message types and exchange profiles.
- Minimal trust assumptions: no central authority required.
- Protocol clarity: defined semantics, deterministic behaviour, testable implementations.

Architecture Overview

- Initiating Gateway: initiates the exchange request
- Receiver Gateway: mediates the transfer
- Respective Asset Networks

```
                +----------+              +----------+
                |  Client  |              | Off-net  |
         ------ |   (App)  |              | Resource |
         |      +----------+              +----------+
         |           |                    |   API3   |
         |           |                    +----------+
         |           |                         ^
         |           V                         |
         |      +---------+                    |
         V      |   API1  |                    |
      +-----+   +---------+----+        +----+---------+   +-----+
      |     |   |         |    |        |    |         |   |     |
      | Net.|   | Gateway |API2|  SATP  |API2| Gateway |   | Net.|
      | NW1 |---|    G1   |    |<------>|    |    G2   |---| NW2 |
      |     |   |         |    |        |    |         |   |     |
      +-----+   +---------+----+        +----+---------+   +-----+
                              Figure 1
```

Protocol Flow

- Transfer Initiation stage (Stage-1):
    - agreement of the set of parameters describing the proposed exchange. The gateway initiating the exchange delivers the initial proposal containing the set of parameters.
- Lock Assertion stage (Stage-2):
    - conveyance of a signed assertion to the receiving gateway, asserting the locked status of the asset in the network connected to the initiating gateway
- Commitment Preparation and Finalization stage (Stage-3):
    - conveyance of a signed assertion to the initiating gateway, asserting the locked status in the network connected to the receiving gateway. The gateways finalize the exchange by assigning the assets to their beneficiaries, and convey signed assertions reflecting the status

Next Steps

- Current status: draft-00 available; reference implementation in progress.
- Next revision: refine message syntax and error handling.
- Key open questions:
  - Is the IETF the right venue for this work?
  - Is there a clear problem being solved?
  - Does it have interest and potential implementations?
  - Naming?
  - Including in SATP or making a separate document
- Call for input: feedback on design assumptions, security model, and use-case alignment

Thank You and Q&A