Secure Asset Transfer Protocol: Charter Discussion

IETF114 – SAT BOF

26 July, 2022

SATP Charter (Proposed)

- Charter text has been posted to the SAT mail-list
- Also available in the following public repo:
  - github.com/CxSci/IETF-SAT

SATP Charter: Objective

There is currently a growing interest in several industry sectors of using the Internet as the foundation for the exchange of digital assets.

The goal of Secure Asset Transfer (SAT) is to develop a standard protocol which operates between two peer gateways for the purpose of transferring digital assets between networks or systems.

SATP problem space and architecture (1/3)

Each gateway represents one network or system, and the SAT protocol performs a unidirectional transfer of a digital asset from the origin network to a destination network, with third-party verifiability.

A key goal for the SAT protocol is to ensure that the properties of atomicity, consistency, isolation and durability (ACID) are satisfied in an asset transfer, and that rollbacks are supported in the case of a failure in satisfying all these properties.

SATP problem space and architecture (2/3)

The requirement of consistency implies that asset transfer protocol always leaves both networks in a consistent state (that at any moment the asset must be valid in one network only). Atomicity means that the protocol must guarantee that either the transfer commits entirely (completes) or entirely fails, where failure is taken to mean there is no change to the state of the asset in the origin network.

SATP problem space and architecture (3/3)

The property of isolation means that while a transfer is occurring to a digital asset from an origin network, no other state changes can occur to the asset. The property of durability means that once the transfer has been committed by both gateways on behalf of the respective networks, the commitment must hold regardless of subsequent unavailability (e.g. crash) of the gateways implementing the transfer protocol.

SATP Scope (1/2)

SAT will use existing IETF standards for various aspects of the protocol, including secure channel establishment (TLS), payload formats (e.g. JSON, JOSE, JWT, CBOR, COSE), digital signatures and encryption (JOSE, JWE), digital certificates (PKIX) and others.

Although the immediate focus is on a unidirectional asset transfer protocol, the resulting building blocks should be usable to support future designs of bidirectional transfers.

SATP scope of work

- API-endpoint definitions (e.g. RESTful APIs)
- Resource identifiers
- Message flows and payloads
- Some terminology (extending NISTIR-8202 or ISO-22739)

SATP Milestones (Proposed)

- SAT Use-Cases document – 6 months
- SAT Architecture document – 12 months
- SAT Protocol document – 12 months

Thank You & Questions

Contact: hardjono@mit.edu