Secure Asset Transfer Protocol (SATP)

BOF Chair:

Wes Hardaker

Mailing List:

https://www.ietf.org/mailman/listinfo/sat

Agenda

1. BOF Introduction	Chair	10m
○ Note-takers: Denis – Thank you!		
2. Problem and Proposed Starting Solutions	(w/ clarifying questions)	
○ SATP problem space and goals	Thomas Hardjono	10m
○ Use case: Supply Chain Trade	Venkatraman Ramakrishna	10m
○ Use case: Regulated CBDC/Finance	Martin Hargreaves	10m
○ Status Report on SATP activity	Thomas Hardjono	10m
3. Open discussion		50m
4. BOF Questions and AD comments/questions		10m

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Note Well, page 2

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

IETF Code Of Conduct Guidelines RFC7154

1. Treat colleagues with respect
2. Speak slowly and limit the use of slang
3. Dispute ideas by using reasoned argument
4. Use best engineering judgment
5. Find the best solution for the whole Internet
6. Contribute to the ongoing work of the group and the IETF

Please keep these in mind both at the mic and on Jabber/Meetecho IM

This session is being recorded

In-person participants

- Make sure to sign into the session using the Meetecho (usually the “onsite tool” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- *Keep audio and video off if not using the onsite version*

Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

General BOF goals (RFC5434)

- Does the problem need solving?
- Is the IETF the right place to solve it?
- Are there enough participants to help?
- Is the scope well defined?
- Are the deliverables right?
- Is the WG likely to succeed?

Agenda

1. BOF Introduction	Chair	10m
○ Note-takers: Denis – Thank you!		
2. Problem and Proposed Starting Solutions	(w/ clarifying questions)	
○ SATP problem space and goals	Thomas Hardjono	10m
○ Use case: Supply Chain Trade	Venkatraman Ramakrishna	10m
○ Use case: Regulated CBDC/Finance	Martin Hargreaves	10m
○ Status Report on SATP activity	Thomas Hardjono	10m
3. Open discussion		50m
4. BOF Questions and AD comments/questions		10m

Charter: Objective

There is currently an interoperability problem in many digital asset networks, where assets in one network cannot be moved easily to another network. The problem is more acute in the case of private asset networks, where external entities have no visibility into the state of an asset in the private network.

One example is the private shipping logistics networks where the digital Bill of Lading as the value-bearing data-object is not accessible to external entities, such as trade finance networks, seeking to issue Letters of Credit based on the Bill of Lading. A second example is regulated digital representations of real-world private assets, such as property ownership certificates, and regulated government-issued digital currencies.

The goal of the Secure Asset Transfer Protocol (SATP) working group will be to develop a standard protocol which operates between two peer gateways for the purpose of transferring digital assets and asset-related data between an originator in the origin asset network to a beneficiary in destination asset network.

Charter: Problem space and architecture (1/2)

To begin addressing these challenges, SATP will employ the gateway paradigm as a means for digital assets to be moved from one asset network to another through a standardized asset transfer message flow implemented between peer gateways. The same gateway paradigm will be utilized for sharing of asset-related data between two asset networks, when one or both are private networks. Thirdly, the gateway model will be used to address the case of coordinated asset swaps occurring simultaneously in two distinct asset networks. A swap here means that both users require identities on both networks, and that they agree to perform two local exchanges in a coordinated fashion.

Each gateway represents one network or system, and the SAT protocol performs a voluntary transfer of a digital asset from the origin network to a destination network, in such a way that evidence of the transfer can be obtained from both networks by a trusted third-party audit entity in the case of disputes. Both the origin and destination networks are assumed to share a common understanding of the digital asset.

Charter: Problem space and architecture (2/2)

There might be several gateways representing the same asset network or system. It is assumed that the same peer gateways representing the respective networks are participating in the entire asset transfer sequence from the beginning to the end.

The SAT protocol commences with the assumption that the Originator and Beneficiary, or Exchanging, entities have agreed out-of-band to proceed on the transfer or exchange of assets or asset-related data, and that both the origin and destination asset-networks can support the type of asset or data being transferred. The service providers who own and operate the respective gateways are assumed to have regulatory compliance when needed with regards to the digital asset or assets, and have agreed to facilitate the transfer or exchange between these networks.

In the case of asset transfers, a key requirement of SATP is to ensure that the digital asset is valid in one network only at any given time. This means that SATP must ensure that the properties of atomicity, consistency, isolation, and durability (ACID) of the underlying networks are satisfied in an asset transfer, and that commitments or rollbacks are supported in the case of a success or failure of the asset transfer operations among the participating networks. The starting point for the discussion regarding ACID properties can be found in draft-hardjono-sat-architecture-00.

Charter: Scope (1/2)

The deliverables of the SATP Working Group will be as follows:

(1) SATP Architecture: The immediate scope of work for SATP will be a base architecture that utilizes the gateway paradigm that ensures a common semantic understanding to be shared among the message flows pertaining to asset transfers, the sharing of asset-related data and the coordinated asset exchanges.

(2) Asset Transfer Message Flow: The asset transfer message flow implements the transfer of a digital asset from one gateway to another, satisfying the ACID properties.

(3) Asset-Related Data Sharing Message Flow: This message flow will securely reveal views of asset-related data from an asset network to an authorized external entity using its gateway, in such a way that the correctness and authenticity of the views can be validated by the entity.

Charter: Scope (2/2)

(4) Asset Exchange Message Flow: This message flow will perform a coordinated exchange of two assets in two respective asset networks, with the two corresponding gateways implementing the coordination. Work on this message flow in the SATP working group will commence only after the work on other two flows have reached their final stages.

(5) SATP Use-Cases: Various real-world use-cases will be collected and described succinctly, with the goal of providing the background to the SATP work.

SATP will define common identifiers, message flows and payloads among the above three protocol modes. A common terminology will be defined in the architecture document.

SATP will reuse existing IETF standards for various aspects of the protocol modes, including but not limited to secure channel establishment (TLS), payload formats (e.g., JSON, CBOR, ProtoBuf, etc.), digital signature and encryption (e.g., JOSE, COSE, etc.), digital certificates and tokens (e.g., PKIX, JWT, etc.), and others. SATP may also reuse existing standards from other organizations (e.g., W3C with DIDs).

Legal frameworks are outside of the scope of the SATP work.

Charter: Milestones

SATP Architecture document: Adoption - 3 months; Delivery to IESG – 18 months. The likely starting point for the working group will be draft-hardjono-sat-architecture

Asset Transfer Message Flow document: Adoption - 3 months; Delivery to IESG – 18 months. The likely starting point for the working group will be draft-hargreaves-sat-core

Asset-Related Data Sharing Message Flow document. Adoption - 3 months; Delivery to IESG – 18 months. The likely starting point for the working group will be draft-ramakrishna-sat-views

SATP Use-Cases document: Adoption - 3 months; Delivery to IESG – 12 months. The likely starting point for the working group will be draft-ramakrishna-sat-use-cases