Secure Asset Transfer Protocol
Internet-Draft
Intended status: Informational
Expires: 7 May 2026

K. Marstein
Cathmere
A. Chiriac
L. Riley
Quant Network
V. Ramakrishna
IBM Research
3 November 2025

Secure Asset Exchange Protocol
draft-marstein-satp-asset-exchange-00

Abstract

This document describes the Secure Asset Exchange (SAE) Protocol. SAE is an extension of the Secure Asset Transfer (SAT) Protocol that enables the asset exchange interoperability mode. It specifies the required modifications necessary to the SAT message flows to facilitate asset exchange between asset networks. Gateways that support the SAT protocol can be extended to also support SAE, enabling support for both asset transfer and asset exchange in a single set of gateways.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://ietf-satp.github.io/draft-marstein-satp-asset-exchange/draft-marstein-satp-asset-exchange.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-marstein-satp-asset-exchange/.

Discussion of this document takes place on the Secure Asset Transfer Protocol Working Group mailing list (mailto:sat@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/sat/. Subscribe at https://www.ietf.org/mailman/listinfo/sat/.

Source for this draft and an issue tracker can be found at https://github.com/ietf-satp/draft-marstein-satp-asset-exchange.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft will expire on 7 May 2026.

Copyright Notice

Table of Contents

1. Introduction

This document presents the Secure Asset Exchange Protocol (SAEP), an extension of the Secure Asset Transfer (SAT) Protocol [SATP] that facilitates asset exchange between asset networks. The asset exchange protocol is a mediated cross-authentication protocol for cross-network digital asset exchange. SATP gateways can be extended to support the asset exchange mode, enabling support for both the asset transfer and asset exchange interoperability modes through a single set of gateways. The reader is directed to [SATA] for further discussion of the interoperability modes recognized in SATP.

The SAE protocol uses a lock-and-assign pattern to facilitate the asset exchange, where all assets included in the exchange are locked or otherwise disabled within their respective networks before being assigned to the designated beneficiaries. This process is coordinated by peer gateways, where each gateway is connected to one of the digital asset networks involved in the exchange. The lock-and-assign pattern is used to facilitate atomicity, consistency, isolation, and durability (ACID) in the cross-network exchange process.

The goal of this draft is to define an asset exchange protocol that builds upon the architectural and procedural foundations established in earlier SATP drafts ([SATA], [SATP]). Asset exchange as a core interoperability requirement is recognized in the SATP architecture [SATA], and is, thus, a natural progression of the protocol. The reader is directed to [SATU] for further discussion of the use cases enabled by the asset exchange version of SATP.

2. Terminology

The following are some terminology used in the current document. We borrow terminology from [NIST] and [ISO] where possible, introducing new terms only when needed:

* Digital asset: A digital representation of a value or of a right that can be transferred and stored electronically using distributed ledger technology or similar technology [MICA].

* Asset network (system): The network or system where a digital asset is utilized.

* Secure Asset Transfer Protocol (SATP): The protocol used to transfer (move) a digital asset from one network to another using gateways.

* Secure Asset Exchange Protocol (SAEP): The protocol used to exchange a digital asset in one network for a digital asset in another network using gateways.

* Asset transfer: A fail-safe process of moving an asset from one network to another, with the destruction of the asset in the origin network and its recreation in the destination network occurring as a single atomic action.

* Asset exchange: A fail-safe process of exchanging (or swapping) assets held by a pair of owners, each asset being maintained in a different network, with the two in-network transfers occurring as a single atomic action.

3. The Secure Asset Exchange Protocol

3.1. Overview

The Secure Asset Exchange Protocol (SAEP) is a gateway-to-gateway protocol enabling cross-network digital asset exchange, first introduced in [SAEP]. The protocol intends to have a low barrier of adoption in systems that already implement SATP by potentially being enabled through the same set of gateways.

This document presents the modifications necessary to the SATP message flows and to the asset network actions to support the asset exchange mode. The asset exchange protocol inherits the SATP model and behavior where not otherwise stated. The reader is directed to [SATP] for further discussion of SATP and non-modified behavior.

While several variations of the message flows can be used to support a gateway-to-gateway asset exchange protcol, a conscious design choice is to diverge as little as possible from the asset transfer version of SATP by reusing established definitions, semantics, and security guarantees where possible. This allows the protocol to leverage the progress of SATP and simplifies integration with existing SATP compliant systems.

The gateway referred to as the "sender gateway" in SATP takes on the role as "initiating" gateway of the asset exchange, and the gateway referred to as the "recipient gateway" takes on the role as "receiving" gateway, referring to each gateway's role in initiating the exchange. The protocol defines API endpoints, resources and identifier definitions, and message flows used in orchestrating the asset exchange between the two gateways.

3.2. Stages of the Protocol

The SAE protocol follows the same three message stages as SATP:

* Transfer Initiation stage (Stage-1): The gateways come to an 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): The initiating gateway conveys 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): The receiving gateway conveys 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 pertaining to the status of the assets in their respective networks to the counterparty gateway.

The interactions between the peer gateways prior to the initiation stage is referred to as the setup stage (Stage-0), which is outside the scope of the current specification of SATP.

3.3. Message Types

This refers to the type of request or response to be conveyed in the message. The values are defined in [SATP].

The possible values for an asset exchange session facilitated by SAEP are:

* transfer-proposal-msg: The exchange proposal message sent by the gateway initiating the exchange. The message contains the set of parameters proposed for the exchange.

* proposal-receipt-msg: The signed receipt message indicating acceptance of the exchange proposal by the receiving gateway.

* reject-msg: The reject message sent from a gateway to another. The message contains an indication of the reason for the rejection.

* transfer-commence-msg: The exchange commence message sent by the gateway initiating the exchange, requesting to begin the commencement of the asset exchange.

* ack-commence-msg: Response to accept the commencement of the asset exchange.

* lock-assert-msg: The gateway has performed the locking of the asset in its network.

* assertion-receipt-msg: The receiving gateway acknowledges receiving the signed lock-assert-msg.

* commit-prepare-msg: The initiating gateway requests the start of the commitment stage.

* ack-prepare-msg: The receiving gateway acknowledges receiving the previous commit-prepare-msg and agrees to start the commitment stage.

* ack-commit-final-msg: The gateway has performed the asset assignment in its network.

* commit-transfer-complete-msg: The initiating gateway indicates closure of the current transfer session.

* error-msg: This message is used to indicate that an error has occured at the SATP layer. It can be transmitted by either gateway.

* session-abort-msg: This message is used by a gateway to abort the current session.

The reader is directed to [SATP] for further discussion of the message types.

4. Modified Message Flows

The SAE protocol follows the same Stage-1 and Stage-2 message flows as [SATP].

Stage-1 flows pertain to the initialization of the transfer session between the two gateways.

Stage-2 flows cover the conveyance of the signed assertion pertaining to the asset's locked status in network N1 connected to the initiating gateway G1.

If the signed assertion conveyed by gateway G1 in Stage-2 is accepted by gateway G2, it must in return initiate Stage-3 and transmit a signed receipt to gateway G1 that it has correctly locked the asset in network NW2 connected to gateway G2.

The remaining Stage-3 flows commit gateways G1 and G2 to assigning the locked assets to their respective benficiaries. The initiating gateway G1 must assign (unlock) the asset in network NW1 to the correct benficiary in network NW1 and gateway G2 must assign (unlock) the asset in network NW2 to the correct beneficiary in network NW2.

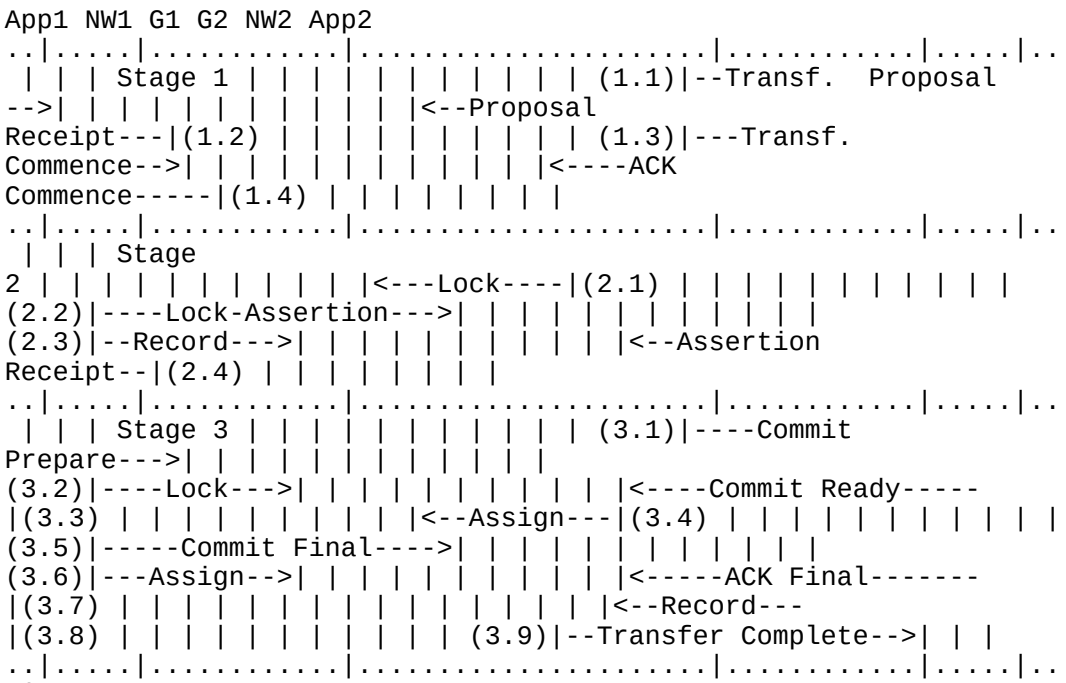

Figure 2

4.1. Transfer Initiation Stage (Stage 1)

This section describes the transfer initiation stage, where the initiating gateway and the receiving gateway prepare for the start of the asset exchange.

The initiating gateway proposes the set of transfer parameters and asset-related artifacts for the exchange to the receiving gateway. The parameters are contained in the Transfer Initiation Claim.

The SAE protocol requires two Transfer Initiation Claims, one for each asset involved in the exchange. The inclusion of two Transfer Initiation Claims in the proposal signals to the receiving gateway that the session should be conducted using SAEP as opposed to SATP.

The reader is directed to [SATP] for further discussion of Stage-1.

4.2. Lock Assertion Stage (Stage 2)

The messages in this stage pertain to the initiating gateway providing the receiving gateway with a signed assertion that the asset in network NW1 has been locked or disabled, and under the control of the initiating gateway.

The reader is directed to [SATP] for further discussion of Stage-2.

4.3. Commitment Preparation and Finalization (Stage 3)

This section describes the exchange commitment agreement between the client (initiating gateway) and the server (receiving gateway).

This stage must be completed within the time specified in the lockAssertionExpiration value in the lock-assertion or commit ready message, whichever is shortest.

The reader is directed to [SATP] for further discussion of required HTTP endpoints, methods, request parameter serialization, and digital signatures for this message.

4.3.1. Commit Preparation Message (Commit-Prepare)

The purpose of this message is for the client to indicate its readiness to begin the commitment of the exchange. In response to this message, the receiving gateway must lock or otherwise disable the asset in network NW2.

The reader is directed to [SATP] for further discussion of the Commit Preparation Message.

4.3.2. Commit Ready Message (Commit-Ready)

The purpose of this message is for the server to indicate to the client that the server has locked or otherwise disabled the asset in network NW2 and that the server is ready to proceed to the next step. In response to this message, the initiating gateway can perform the assignment of the asset in network NW1 to its designated benficiary.

This message is sent from the server to the Commit Ready Endpoint at the client.

The message must be signed by the server.

The SAE protocol requires the message transmitted in this step to be formatted as a lock-assert-msg instead of following the commit-ready-msg format specified for this step in SATP.

The parameters of this message consist of the following:

* messageType REQUIRED. It MUST be the value urn:ietf:satp:msgtype:lock-assert-msg.

* sessionId REQUIRED: A unique identifier chosen earlier by client in the Initialization Request Message.

* transferContextId REQUIRED: A unique identifier used to identify the current exchange session at the application layer.

* hashPrevMessage REQUIRED. The hash of the previous message.

* lockAssertionClaim REQUIRED. The lock assertion claim or statement by the server.

* lockAssertionClaimFormat REQUIRED. The format of the claim.

* lockAssertionExpiration REQUIRED. The duration of time of the lock or escrow upon the asset.

Example:

{\ "messageType": "urn:ietf:satp:msgtype:lock-assert-msg",\
"sessionId": "d66a567c-11f2-4729-a0e9-17ce1faf47c1",\
"transferContextId": "89e04e71-bba2-4363-933c-262f42ec07a0",\
"hashPrevMessage":
"8dcc8dc4e6c2c979474b42d24d3747ce4607a92637d1a7b294857ff7288b8e46",\
"lockAssertionClaim": {},\ "lockAssertionClaimFormat":
"LOCK_ASSERTION_CLAIM_FORMAT_1",\ "lockAssertionExpiration":
"2024-12-23T23:59:59.999Z",\ }\

4.3.3. Commit Final Assertion Message (Commit-Final)

The purpose of this message is for the client to indicate to the server that the client (initiating gateway) has completed the assignment of the asset in network NW1.

The message must contain a standalone claim related to the assignment of the asset by the client. The standalone claim must be signed by the client.

This message is sent from the client to the Commit Final Assertion Endpoint at the server.

The message must be signed by the client.

The SAE protocol requires the message transmitted in this step to be formatted as an ack-commit-final-msg instead of following the commit-final-msg format specified for this step in SATP.

The parameters of this message consist of the following:

* messageType REQUIRED. It MUST be the value urn:ietf:satp:msgtype:ack-commit-final-msg.

* sessionId REQUIRED: A unique identifier chosen earlier by the client in the Initialization Request Message.

* transferContextId REQUIRED: A unique identifier used to identify the current exchange session at the application layer.

* hashPrevMessage REQUIRED. The hash of the previous message.

* assignmentAssertionClaim REQUIRED. The claim or statement by the client that the asset has been assigned by the client to the intended beneficiary.

* assignmentAssertionClaimFormat REQUIRED. The format of the claim.

Example:

```
{\ "messageType": "urn:ietf:satp:msgtype:ack-commit-final-msg",\
"sessionId": "d66a567c-11f2-4729-a0e9-17ce1faf47c1",\
"transferContextId": "89e04e71-bba2-4363-933c-262f42ec07a0",\
"hashPrevMessage":
"b92f13007216c58f2b51a8621599c3aef6527b02c8284e90c6a54a181d898e02",\
"assignmentAssertionClaim": {},\ "assignmentAssertionClaimFormat":
"ASSIGNMENT_ASSERTION_CLAIM_FORMAT_1",\ }\
```

4.3.4. Commit-Final Acknowledgement Receipt Message (ACK-Final-Receipt)

The purpose of this message is to indicate to the client that the server has completed the assignment of the asset to the intended beneficiary in network NW2.

The reader is directed to [SATP] for further discussion of the Commit-Final Acknowledgement Receipt Message.

4.3.5. Transfer Complete Message

The purpose of this message is for the client to indicate to the server that the asset exchange session (identified by sessionId) has been completed and no further messages are to be expected from the client in regards to this transfer instance.

The reader is directed to [SATP] for further discussion of the Transfer Complete Message.

4.4. Error Messages

The reader is directed to [SATP] for further discussion of error messages.

5. Security Considerations

The reader is directed to [SATP] for further discussion of security considerations.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[ISO] ISO, "Blockchain and distributed ledger technologies- Vocabulary (ISO:22739:2020)", July 2020, <https://www.iso.org/standard/82208.html>.

[MICA] European Commission, "EU Directive on Markets in Crypto-Assets Regulation (MiCA)", June 2023, <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>.

[NIST] Yaga, D., Mell, P., Roby, N., and K. Scarfone, "NIST Blockchain Technology Overview (NISTR-8202)", October 2018, <https://doi.org/10.6028/NIST.IR.8202>.

[SAEP] Marstein, K., Davita, P., and L. Riley, "Adapting the Secure Asset Transfer Protocol for Secure Cross-Network Asset Exchange, IEEE ICBC Cross-Chain Workshop (ICBC-CCW)", June 2025, <https://doi.org/10.1109/ICBC64466.2025.11185062>.

[SATA] Hardjono, T., Hargreaves, M., Smith, N., and V. Ramakrishna, "Secure Asset Transfer (SAT) Interoperability Architecture, IETF, draft-ietf-satp-architecture-08", July 2025, <https://datatracker.ietf.org/doc/draft-ietf-satp-architecture/>.

[SATP] Hargreaves, M., Hardjono, T., Belchior, R., Ramakrishna, V., and A. Chiriac, "Secure Asset Transfer Protocol (SATP) Core, IETF, draft-ietf-satp-core-11", August 2025, <https://datatracker.ietf.org/doc/draft-ietf-satp-core/>.

[SATU] Ramakrishna, V., Hardjono, T., and C. Liu, "Secure Asset Transfer (SAT) Use Cases, IETF, draft-ietf-satp-usecases-06", July 2025, <https://datatracker.ietf.org/doc/draft-ietf-satp-usecases/>.

7.2. Informative References

[Abebe19] Abebe, E., Behl, D., Govindarajan, C., Hu, Y., Karunamoorthy, D., Novotny, P., Pandit, V., Ramakrishna, V., and C. Vecchiola, "Enabling Enterprise Blockchain Interoperability with Trusted Data Transfer (Middleware 2019 - Industry Track)", December 2019, <https://arxiv.org/abs/1911.01064>.

[BVGC20] Belchior, R., Vasconcelos, A., Guerreiro, S., and M. Correia, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends", May 2020, <https://arxiv.org/abs/2005.14282v2>.

[Clar88] Clark, D., "The Design Philosophy of the DARPA Internet Protocols, ACM Computer Communication Review, Proc SIGCOMM 88, vol. 18, no. 4, pp. 106-114", August 1988.

[HLP19] Hardjono, T., Lipton, A., and A. Pentland, "Towards an Interoperability Architecture for Blockchain Autonomous Systems, IEEE Transactions on Engineering Management", June 2019, <https://doi:10.1109/TEM.2019.2920154>.

[HS2019] Hardjono, T. and N. Smith, "Decentralized Trusted Computing Base for Blockchain Infrastructure Security, Frontiers Journal, Special Issue on Blockchain Technology, Vol. 2, No. 24", December 2019, <https://doi.org/10.3389/fbloc.2019.00024>.

[HTLC21] "Hash Time Locked Contracts, Bitcoin Wiki", n.d., <https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts>.

[SRC84] Saltzer, J., Reed, D., and D. Clark, "End-to-End Arguments in System Design, ACM Transactions on Computer Systems, vol. 2, no. 4, pp. 277-288", November 1984.

Authors' Addresses

Kjell-Erik Marstein
Cathmere
Email: kjell-erik@cathmere.com

Alex Chiriac
Quant Network
Email: alexandru.chiriac@quant.network

Luke Riley
Quant Network
Email: luke.riley@quant.network

Venkatraman Ramakrishna
IBM Research
Email: vramakr2@in.ibm.com