Secure Asset Transfer Protocol: Messages and Flows

IETF114 – SAT BOF

26 July 2022
Martin Hargreaves, Alex Chiriac (Quant Network)
Resource Descriptors
Resource Descriptors

• Identified by URL
• New Media Type: application/satres
• Access Protocol: SAT

satres://quant/api.gateway1.com/tradelens/xxxxxADDRESSxxxxx

- Organization identifier (LEI or other)
- Gateway Endpoint ID (FQDN)
- Network or System Identifier
- Resource (a resource held on the underlying network)
Message Format
SATP Message Format

The messages exchanged are in JSON format. The mandatory fields are:

- Version
- Session ID
- Sequence Number
- SAT Phase
- Resource URL
- Developer URN
- Action/Response

- Credential Profile
- Credential Block
- Payload Profile
- Application Profile
- Payload
- Payload Hash
- Message Signature
Flows
SATP Defines 3 Core Flows

• Transfer Initiation Flow – after the identity and asset verification flow (out of scope), a sender gateway proposes a session to a receiver gateway

• Lock-Evidence Verification Flow – conveyance of claims regarding the lock status of a digital asset by one gateway and the verification of the evidence by the other gateway

• Commitment Establishment Flow – asset transfer and commitment establishment between two gateways on behalf of their networks
Transfer Initiation Flow

• Initialization Request Message
• Initialization Request Message Response
Lock-Evidence Verification Flow

• Transfer Commence Message
• Transfer Commence Response Message
• Lock Evidence Message
• Lock Evidence Response Message
Commitment Establishment Flow

- Commit Preparation Message
- Commit Preparation Response
- Commit Final Message
- Commit Final Response Message
- Transfer Complete Message
Thank you!