

SATP Core Protocol

Updates to core-02

draft-ietf-satp-core-02

IETF117 San Francisco

Martin Hargreaves, Thomas Hardjono and Rafael Belchior

Summary of Updates

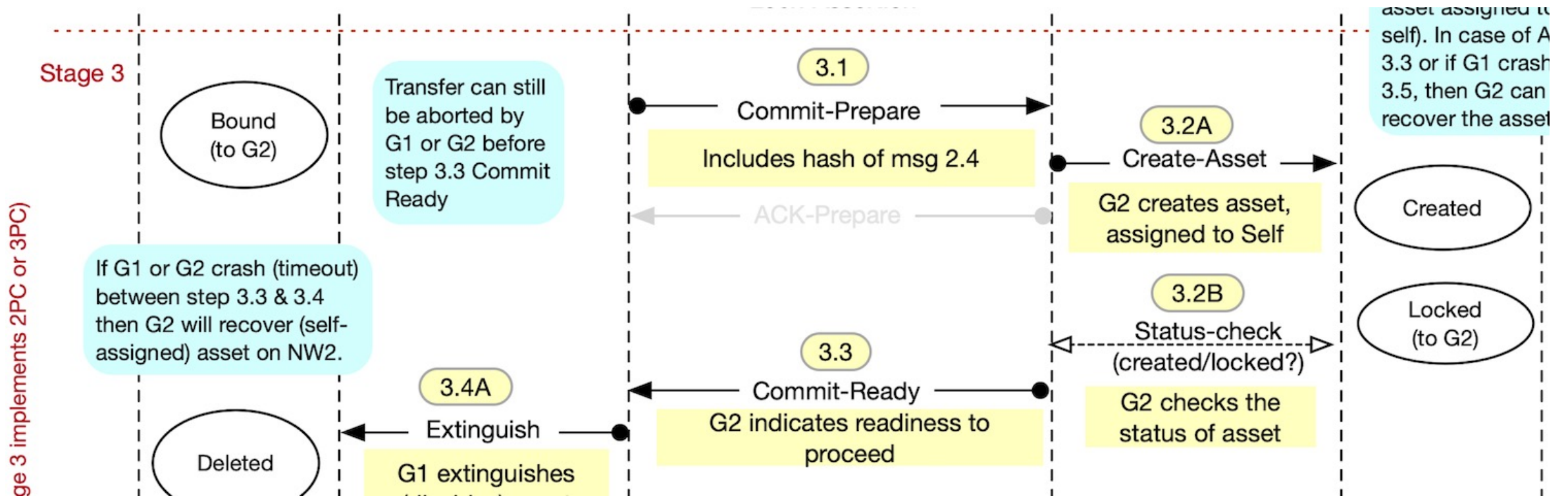
- Removal of redundant ACK-Prepare
- Transfer Commence flows now in Stage-1
- Transfer Initiation Claims
- Session Resumption
- Updated to Architecture draft

Message Flow Diagram (v19) in Github repo: <https://shorturl.at/diAFU>

Redundant ACK-Prepare

- The ACK-Prepare is part of the classic 3PC design
 - One Coordinator & multiple Subordinates
 - In 3PC an explicit ACK-Prepare is required from the Subordinates (all or majority)
- SATP Core is currently defined for 1 sender gateway and 1 receiver gateway exactly
 - ACK-Prepare can be reintroduced for future use-cases, without affecting remainder of flow.

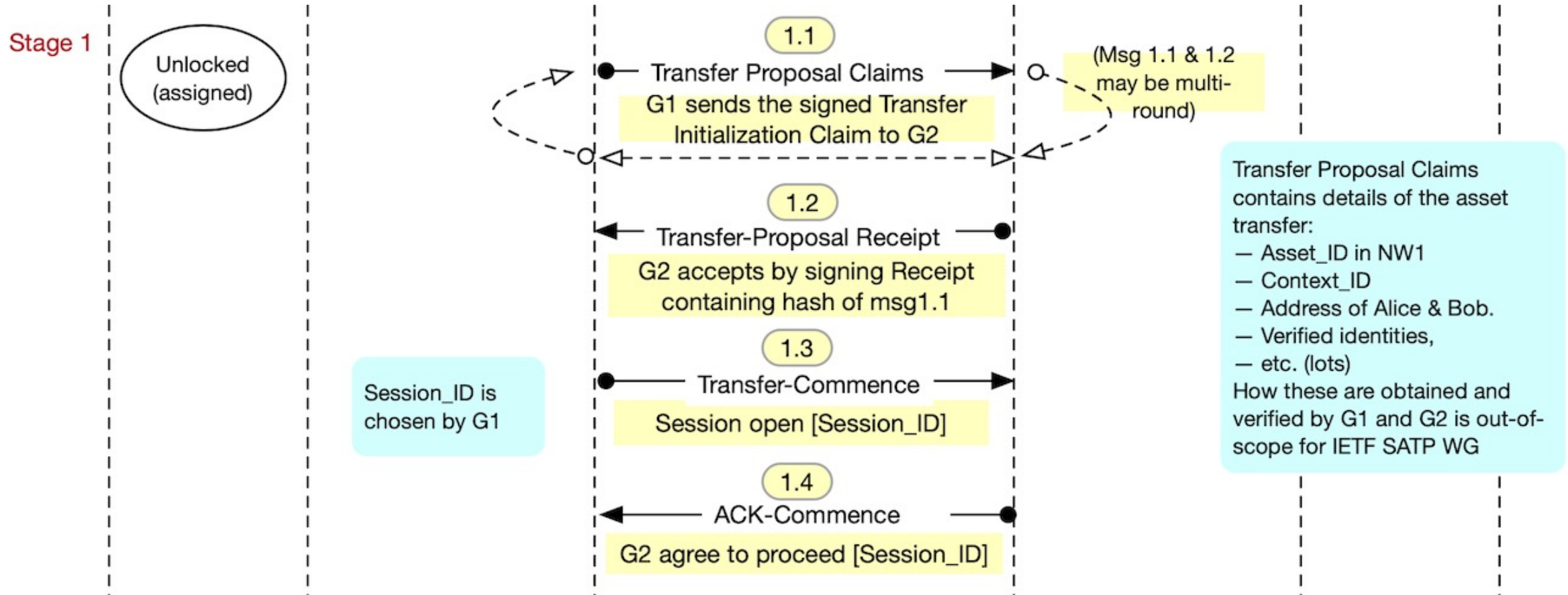
Redundant ACK-Prepare (grey)



Transfer Commence Flows (Stage 1)

- Transfer Commence & ACK were previously located in Stage-2
 - Now moved-up to Stage-1
- Multiple rounds of Transfer Proposal Claims
 - Gateway G1 proposes an initial set of parameters (claims)
 - If G2 is satisfied, it must sign an explicit Receipt
 - Else G2 can counter-propose
 - If G2 quits, it sends a counter-proposal with empty claims

Transfer Commence Flows (Stage 1)



Transfer Initialization Claims (Section 7.1)

- Group together Claims pertaining to:
 - Asset and actors
 - Gateway service and network characteristics
- Relevant claims:
 - Asset-profile identifier; asset identifier in NW1
 - Verified identities (of Alice & Bob)
 - Gateway Service Provider (Owner) identifier
 - Gateway identifier; network identifier

Some example Claims (see Section 7.1)

`digital_asset_id`

`asset_profile_id`

`client_identity_pubkey`

`server_identity_pubkey`

`verified_originator_entity_id`

`verified_beneficiary_entity_id`

`originator_pubkey`

`beneficiary_pubkey`

`sender_gateway_owner_id`

`receiver_gateway_owner_id`

`sender_gateway_network_id`

`recipient_gateway_network_id`

Claims about Gateway/Network Characteristics

- List of capabilities of G1 and NW1
- Examples of capabilities claims:
 - signature_algorithm (chosen by client this session)
 - supported_signature_algorithms (available at client)
 - lock_type
 - lock_expiration_time
- (More needed)

Session Resumption

- Primary-Backup model
 - Backup has access to local system logs
- Session Resumption messages-types:
 - Recovering gateway sends message-type “Recover”
 - If agree, counterparty sends “Recover-Update”
 - Recovering gateway syncs its logs and sends “Recover-Success”
- Else, proceed to Roll-Back (see crash recovery draft)

Architecture draft (now draft-01)

- Updated to sync with SATP Core draft-02
 - Stages and flow descriptions
- Added text regarding ISO 20022
 - This was a recommendation from IETF116
- References also updated.

Next Steps & General Questions

- Continue work on Error types and messages
- Continue work Transfer Initialization Claims
 - Separate claims draft (?)
 - Dependence on Asset Profile work
- Others?

Thank You and Q&A

Contact: hardjono@mit.edu