

Updates on SATP Architecture and Core drafts

draft-ietf-satp-architecture-09
draft-ietf-satp-core-13

SATP Working Group – IETF125 Shenzhen
18 March 2026

Thomas Hardjono

Updates on SATP Architecture (draft-09)

- Consistent use of “TLS1.3” throughout
- Improved text about Stage-0 as being necessary for setting-up a transfer
- Reading order: readers need to read Arch first before reading Core
- Cleaning-up Terminology section and alignment with Use-Cases draft

Updates on SATP Architecture (draft-09) - cont

- Text clarification on 2PC commitment subprotocol
 - Removing mention of 3PC to avoid confusion
- Clarification on: SHOULD, MUST, MUST-NOT
- Several typos and unclear sentences have been fixed

Updates on SATP Core (draft-13)

- Consistency of terminology and wording
 - 2-Phase-Commit (no mention of 3PC)
 - Consistent use of “TLS1.3” throughout
 - Consistent Pubkey vs. PublicKey (e.g., originatorPublicKey)
 - Broken citations/references have been corrected
 - Add citations to systems that utilize hash-lock & hash-time-lock/HTLC (Sect. 5.3.15. Asset Lock Mechanisms)
 - Lots of typos have been corrected

Updates on SATP Core (draft-13) – cont.

- All SATP implementations **MUST** implement at minimal the ECDSA signature algorithm with the P-256 curve and the SHA-256 hash function.
- Other signature algorithms used by gateways for SATP messages SHOULD be selected from those defined in the JSON Web Algorithms (JWA) specification [RFC7518], with key types defined in JSON Web Key (JWK) specification [RFC7517].
- The digital asset identifier is a JSON object, which may be encoded as a string in base64
- The default hash algorithm that all SATP implementations **MUST** support is the SHA-256 algorithm [RFC7515]

Updates on SATP Core (draft-13) – cont.

- Errors codes (table): *how this code would arise in a run of the protocol?* (e.g. “err_1.1.11”)
- New text to clarify (Section 13.1):

Many of the errors arising from invalid identifiers (e.g., invalid transferContextId, invalid digitalAssetId) may arise within the execution of the SATP protocol because these identifiers depart from those agreed-upon in Transfer Initialization Claim in the transfer proposal message.

The validity of these identifiers must be verified by the gateways during Stage-0, which is beyond the scope of the current specification.

Huge thank you to
Orie Steele (Security AD)
for extensive review of the SATP drafts.

Q&A