Network Working Group
Internet-Draft
Intended status: Experimental
Expires: July 21, 2026

Peavey Koding
Independent Researcher

January 21, 2026

Kaspa Kinesis Transport Protocol (KKTP) Threat Model
draft-koding-kktp-threat-model-00

Status of This Memo

Abstract

This document defines the adversary model, security assumptions, security goals, and explicit non-goals for the Kaspa Kinesis Transport Protocol (KKTP). It describes the capabilities of potential attackers, the trust assumptions required for correct operation, and the limits of the protocol’s security guarantees. This document is intended to complement the main KKTP specification.

1. KKTP Threat Model

This document defines the adversary model, security goals, non-goals, and trust assumptions for the Kaspa Key Transport Protocol (KKTP). It is intended to be referenced from the main specification.

2. Adversary Capabilities

KKTP is designed under the assumption of a powerful adversary with the following capabilities:

- Global Observation
  The adversary MAY observe all Kaspa transactions, including anchors, mailbox messages, public keys, SIDs, mailbox identifiers, timestamps, and transaction ordering.

- Active Network Participation
  The adversary MAY submit arbitrary Kaspa transactions, including malformed or malicious KKTP payloads, and MAY attempt to flood mailboxes subject to transaction fee costs.

- Message Reordering and Delay

Due to the BlockDAG structure, the adversary MAY influence message arrival order and MAY delay message inclusion, but CANNOT selectively suppress transactions once accepted by the network without incurring economic cost.

- Replay Attempts
  The adversary MAY replay previously observed valid KKTP messages.

- Key Compromise (Limited)
  The adversary MAY compromise long-term signing keys or ephemeral session keys after a session has completed, but is assumed NOT to compromise both parties' ephemeral DH private keys during an active session.

- No Cryptographic Breaks
  The adversary is assumed NOT to break standard cryptographic primitives (X25519, Ed25519, XChaCha20-Poly1305, BLAKE2b, HKDF).

3. Security Goals (In Scope)

KKTP provides the following guarantees against the adversary described above:

- Confidentiality
  Message contents are confidential to session participants. Observers cannot recover plaintext without access to the session key.

- Integrity and Authenticity
  Message tampering, forgery, or bit-flipping is detected via AEAD authentication tags.

- Replay Protection
  Replayed messages are detected and rejected via strict per-direction sequence enforcement.

- Session Binding
  Messages are cryptographically bound to a specific session via mailbox identifiers, session identifiers (SID), and key agreement material.

- Public Verifiability
  Any observer can verify that a session was established between specific public keys and that observed messages are attributable to that session.

- Forward Secrecy
  Compromise of long-term signing keys does not compromise past session contents, provided ephemeral DH keys were securely erased.

4. Explicit Non-Goals (Out of Scope)

KKTP explicitly does not attempt to provide the following properties:

- Cryptographic Deniability
  Session establishment is signed and publicly anchored. Participants cannot plausibly deny session participation after the fact.

- Metadata Privacy
  Traffic patterns, message timing, mailbox identifiers, and session existence are visible on-chain.

- Anonymity
  KKTP does not hide the relationship between public keys and sessions.
  Anonymity requires external measures such as ephemeral identities or network-level privacy systems.

- Guaranteed Delivery
  KKTP provides ordered, authenticated messaging if messages are
  observed, but does not guarantee delivery in the presence of sustained censorship, reor
ganization, or fee exhaustion.

- Endpoint Compromise Resistance
  KKTP does not protect against malware, key exfiltration, or malicious
  behavior on compromised endpoints.

5. Man-in-the-Middle (MITM) Considerations

- KKTP prevents passive MITM attacks through authenticated key agreement
and AEAD encryption.
- Active MITM attacks are detectable through signature verification and
session binding.
- Full resistance to active MITM attacks requires trusted public keys or out-of-band veri
fication.
- Optional VRF binding strengthens detection of key substitution,
replay, and backdating attacks but does not replace identity
authentication.

6. Denial-of-Service (DoS) Considerations

- KKTP is subject to DoS attempts via mailbox flooding.
- Kaspa transaction fees impose an economic cost on large-scale
flooding attacks.
- Implementations MUST perform AEAD authentication checks before
allocating significant memory or performing expensive processing.
- Implementations MUST enforce strict bounds on out-of-order message
buffering.

7. Key Compromise Scenarios

- Compromise of Long-Term Signing Keys
  Enables impersonation in future sessions but does not compromise confidentiality of pas
t sessions.

- Compromise of Ephemeral DH Keys During an Active Session
  Compromises confidentiality for that session only.

- Compromise After Session Termination
  Does not compromise past session confidentiality if ephemeral keys
  were securely erased.

8. Trust Assumptions

KKTP assumes:

- Correct implementation of cryptographic primitives.
- Secure random number generation.
- Proper key erasure by implementations.
- Correct enforcement of Kaspa consensus rules.

Violation of these assumptions may weaken or invalidate the stated
security guarantees.

9. IANA Considerations

This document has no IANA actions.

10. References

10.1. Normative References

None.

10.2. Informative References

[KKTP] Peavey2787, "Kaspa Kinesis Transport Protocol (KKTP)", draft-peavey-kktp-00, January 2026.

Author’s Address

Peavey Koding
Independent Researcher
Email: peavey2787@yahoo.com
GitHub: https://github.com/peavey2787