Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: 19 November 2026

J. van de Meent
Humotica

18 May 2026

TIBET TAT: Touch-and-Transfer Protocol
draft-vandemeent-tibet-tat-00

Abstract

This document specifies TIBET TAT, a Touch-and-Transfer protocol for moving sealed continuity-bearing objects across proximity, relay, and local-network handoff lanes.

TAT defines a consent-bound handoff model, a seed exchange for tunnel establishment, encrypted chunk streaming, and mutual transfer anchoring between sender and receiver.

TAT does not define identity truth, semantic class, or sealed object class by itself. Instead, it defines the wire and handoff layer that carries such objects once sender and receiver have agreed to transfer. TAT is intended to sit between the Continuity Envelope Protocol (CEP) and higher-level application profiles such as IDDrop.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 19 November 2026.

Copyright Notice

Table of Contents

1. Introduction

Many systems can transport bytes, but fewer specify the exact handoff semantics of a consensual sealed transfer.

TIBET TAT addresses this gap. TAT is the wire and handoff protocol for touch-and-transfer and related relay delivery paths.

The key design principle is simple: transfer MUST be consent-bound, anchored, and sealed.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

TAT The Touch-and-Transfer protocol specified in this document.

Seed A compact signed handshake object exchanged before tunnel opening.

Consent The explicit receiver-side decision to accept, reject, or request more information before transfer continues.

Transfer Pair The sender-side transfer_out anchor and receiver-side transfer_in anchor that together record a single handoff event.

TAT Tunnel The encrypted transport channel established after seed validation and consent.

Tombstone An optional finality record written after successful transfer to indicate deactivation or succession.

3. Protocol Overview

TAT sits between general continuity messaging and higher-level application protocols. TIBET decides causal truth, TAT decides transfer flow, ICC or TZA/TBZ sealed carriers decide object structure, and SSM decides visible dispatch surface.

TAT is intended as the generic transfer profile that a specialized application profile MAY build upon.

TAT MAY be used across multiple transport modes including proximity touch, local relay, local network handoff, and HTTP-assisted handoff. The transport substrate MAY vary, but the TAT consent, tunnel, and transfer-pair semantics MUST remain invariant.

4. TAT Objects

Seed Object Advertises transfer intent and carries minimum material for validation and tunnel setup.

Consent Object The receiver-side signed response that echoes the transfer identifier and states accept, reject, or request_more.

Transfer-Out Anchor The sender-side record of initiated transfer. It MUST be written before protected content flows.

Transfer-In Anchor The receiver-side record of received and verified transfer. It MUST only be written after integrity verification succeeds.

Optional Tombstone An optional finality object recording deactivation or succession after transfer.

5. Touch-and-Transfer Flow

1. sender generates an ephemeral X25519 keypair and a new transfer_pair_id

2. sender emits a Seed Object

3. receiver validates the seed and performs consent

4. receiver emits a signed Consent Object

5. sender verifies consent

6. sender writes transfer_out

7. both sides derive the tunnel key

8. encrypted chunks are streamed

9. receiver verifies final integrity and writes transfer_in

10. sender MAY write a tombstone

A relay or HTTP flow follows the same logical sequence. Implementations MUST NOT weaken bilateral consent, transfer-pair integrity, or receiver binding merely because the transport is not NFC-based.

6. Tunnel Establishment

TAT seeds are RECOMMENDED to be encoded compactly, for example using CBOR, when the seed must traverse a narrow proximity channel.

TAT RECOMMENDS X25519 for ephemeral ECDH [RFC7748] and HKDF-SHA256 [RFC5869] for deriving a per-transfer tunnel key and nonce prefix.

The transfer itself SHOULD use an authenticated encryption scheme such as AES-256-GCM [RFC5116]. Chunks MUST be sequenced and integrity checked, and the receiver MUST compare the final result to the sender’s summary before writing transfer_in.

7. Validation Rules

1. *Bilateral Consent*: a sender MUST NOT begin protected content transfer before an explicit receiver-side consent has been verified.

2. *Seed Authenticity*: the receiver MUST verify the seed signature, fingerprint, and transfer identifier before producing consent.

3. *Transfer-Pair Consistency*: the same transfer_pair_id MUST appear in the initiating seed, the receiver consent, the sender transfer_out anchor, and the receiver transfer_in anchor.

4. *Stream Integrity*: the receiver MUST verify the stream integrity and final content summary before writing transfer_in.

5. *Mutual Anchoring*: the sender MUST write transfer_out before content flow, and the receiver MUST write transfer_in only after successful verification.

6. *Post-Transfer Finality*: if a sender claims deactivation or succession, this MUST be represented by an explicit tombstone or equivalent finality object rather than by silent deletion alone.

8. Relationship to CEP, TIBET, SSM, ICC, and IDDrop

TAT is lower than IDDrop, complementary to SSM, orthogonal to ICC or TZA/TBZ sealed object semantics, and anchored by but not identical to TIBET causal truth.

CEP is the umbrella continuity model, TAT is the generic handoff and transfer profile, and IDDrop is an identity-transfer application profile over TAT.

* TIBET decides causal truth

* TAT carries the handoff

* ICC or TZA seals the object

* SSM makes the outer surface routable

* IDDrop decides identity-transfer semantics above TAT

9. Security Considerations

TAT is designed to reduce ambiguity in sealed handoff, but several security properties depend on correct composition. Physical proximity alone is insufficient without explicit consent. Transport confidentiality is insufficient without mutual anchoring. Transfer success is insufficient without final integrity checks. Silent deletion is insufficient as proof of retirement.

Implementations SHOULD surface fingerprint, sender identity, or equivalent trust hints before consent. Implementations MUST treat transfer_pair_id reuse as suspicious. Replayed or stale consent responses MUST be rejected.

10. IANA Considerations

This document has no IANA actions.

11. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008, <https://www.rfc-editor.org/info/rfc5116>.

[RFC5869] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, May 2010, <https://www.rfc-editor.org/info/rfc5869>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, December 2020, <https://www.rfc-editor.org/info/rfc8949>.

12. Informative References

[CAUSAL] van de Meent, J., "TIBET Causal Time", Work in Progress, Internet-Draft, draft-vandemeent-tibet-causal-time-02, May 2026, <https://datatracker.ietf.org/doc/html/draft-vandemeent-tibet-causal-time-02>.

[SSM] van de Meent, J., "TIBET Semantic Surface Manifest", Work in Progress, Internet-Draft, draft-vandemeent-tibet-semantic-surface-manifest-02, May 2026, <https://datatracker.ietf.org/doc/html/draft-vandemeent-tibet-semantic-surface-manifest-02>.

[CEP] van de Meent, J., "Continuity Envelope", Work in Progress, Internet-Draft, draft-vandemeent-continuity-envelope-00, May 2026, <https://datatracker.ietf.org/doc/html/draft-vandemeent-continuity-envelope-00>.

[IDDROP] van de Meent, J., "IDDrop", Work in Progress, Internet-Draft, draft-vandemeent-iddrop-00, May 2026, <https://datatracker.ietf.org/doc/html/draft-vandemeent-iddrop-00>.

Author’s Address

Jasper van de Meent
Humotica
Netherlands
Email: info@humotica.com
URI: https://humotica.com/