SECURE EVIDENCE & ATTESTATION TRANSPORT WG

SEAT  Architecture

IETF 126 • Vienna

Nathanael Ritz · Thomas Fossati · Tiru Reddy.K · Ionut Mihalcea · Yuxuan Song

Why a SEAT Architecture Document?

draft-many-seat-architecture-00 — a design input for the chartered protocol work, not a new deliverable

Why a SEAT Architecture Document?

1 One security argument

(D)TLS 1.3. Session-specific binding value, directional binders, credential or transcript committed to the binder.

draft-many-seat-architecture-00 — a design input for the chartered protocol work, not a new deliverable

Why a SEAT Architecture Document?

1 One security argument

(D)TLS 1.3. Session-specific binding value, directional binders, credential or transcript committed to the binder.

2 Cross-cutting properties have no other home

Downgrade prevention, relay attack, and re-attestation freshness.

draft-many-seat-architecture-00 — a design input for the chartered protocol work, not a new deliverable

Why a SEAT Architecture Document?

1 One security argument

(D)TLS 1.3. Session-specific binding value, directional binders, credential or transcript committed to the binder.

2 Cross-cutting properties have no other home

Downgrade prevention, relay attack, and re-attestation freshness.

3 One coherent answer to the IAB statement

The open-Internet attestation scope boundary should be argued once at architecture level, not restated inconsistently in every draft.

draft-many-seat-architecture-00 — a design input for the chartered protocol work, not a new deliverable

Why a SEAT Architecture Document?

1 One security argument

(D)TLS 1.3. Session-specific binding value, directional binders, credential or transcript committed to the binder.

2 Cross-cutting properties have no other home

Downgrade prevention, relay attack, and re-attestation freshness.

3 One coherent answer to the IAB statement

The open-Internet attestation scope boundary should be argued once at architecture level, not restated inconsistently in every draft.

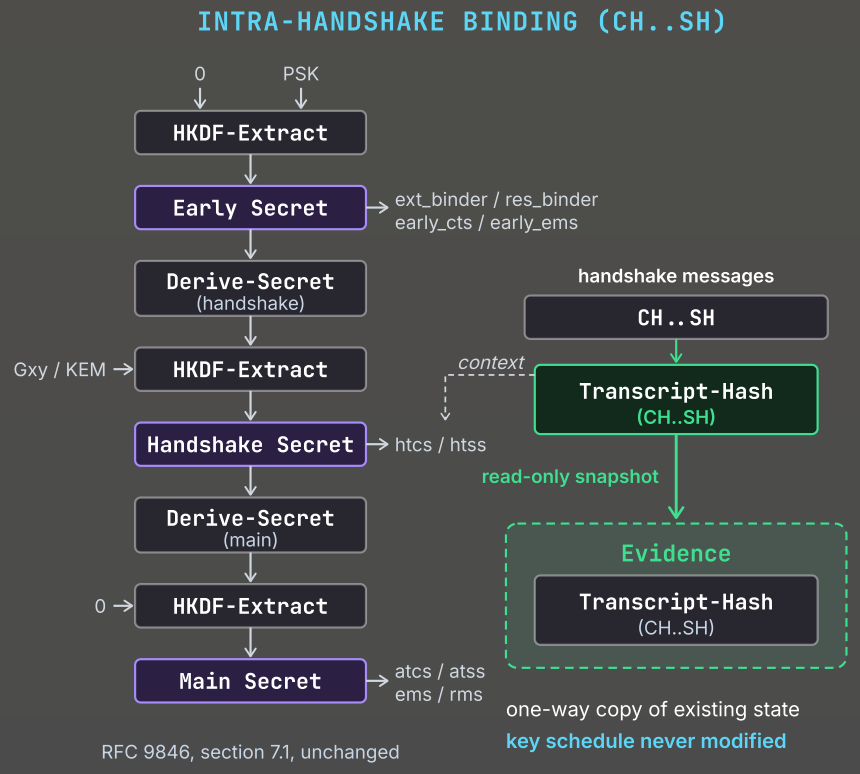
4 Solution drafts need shared vocabulary

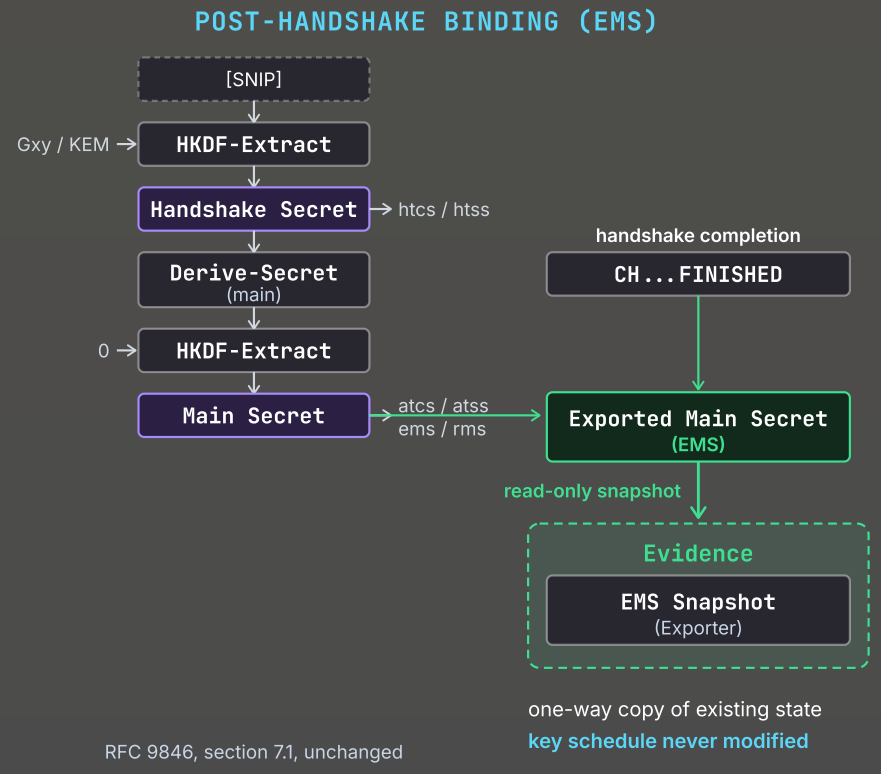
Attestation Binder, Session Binding Value, Transmission / Verification Anchor, tbK / hbK / aeK / arK — define once, or every protocol draft invents its own.

draft-many-seat-architecture-00 — a design input for the chartered protocol work, not a new deliverable

One security argument

The primary objective is for both attestation timing models to act purely as observers of an immutable key schedule.





Cross-cutting properties have no other home

- Binding attested state to connection
- Per-connection freshness, Evidence + AR
- Applying charter requirements across conveyance models
- Linking hardware evidence to the TLS public key to prevent platform spoofing

CROSS-PROTOCOL BASELINE

| Solution drafts define message formats, not the universal cryptographic rules linking hardware trust to transport identities.

| The architecture document provides that unified home.

One coherent answer to the IAB statement

- **Object-Level Encryption:**
  - ▶ *Channel Independence:* Decoupled from TLS layer.
- **Selective Disclosure:**
  - ▶ *Redacted disclosures:* excluding *hwQuote* from Attestation Results.

IAB TRACKING RISK

> In line with the privacy risks highlighted by the IAB, the draft puts emphasis on minimizing the exposure of detailed client identifiers and vendor-specific claims to help mitigate long-term tracking and linkability concerns.

Privacy properties are fundamentally inherited from the underlying RATS framework.

Solution drafts need shared vocabulary

- **tbK (TEE-Bound):** Ephemeral TEE key generated inside the Target Environment to sign handshake actions.
- **hbK (Hardware-Bound):** Long-lived platform identity key validation (e.g., WebPKI) that can authorize the tbK.
- **aeK & arK:** Keys used exclusively to sign Evidence hardware claims (aeK) and downstream Verifier Results (arK).

TRANSPORT TERMINOLOGY

| Specializes foundational RATS concepts for secure channel environments.

| Unique transport-specific primitives—such as protocol anchors and timing models—normalize attestation properties across protocol layers.

Next steps

1. Ongoing key discussions
2. Passport AR binding
3. Privacy: Evidence to an unauthenticated RP, selective disclosure (SPICE collab?)
4. Other suggestions?

THANK YOU!

`github.com/tls-attestation/seat-architecture`

Issues and PRs welcome