Factor-based Attestation and Credential Transport Scheme (FACTS) over TLS 1.3

IETF 125 - SEAT WG

Nathanael Ritz (Independent)

draft-ritz-seat-facts-00

What is FACTS?

A hybrid* intra-handshake RA protocol with **strong binding** and **per-session** freshness, **without** modifying the TLS state machine.

---

[*] Pre-auth (AR/CWT/etc) / Post-HS (EKU and/or EXPAT[1])
[1] draft-fossati-seat-expat-02

Not unlike

`draft-fossati-seat-early-attestation` ...

~~{Attestation} message~~

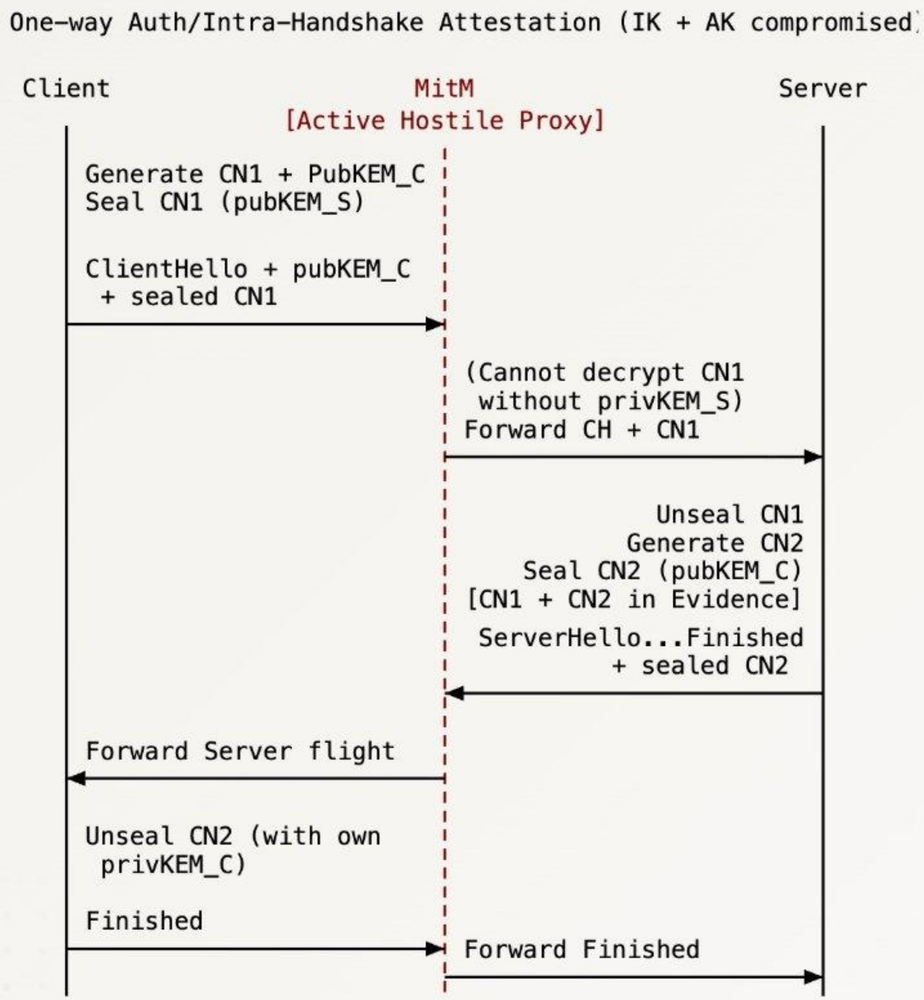
s_attest_base ...

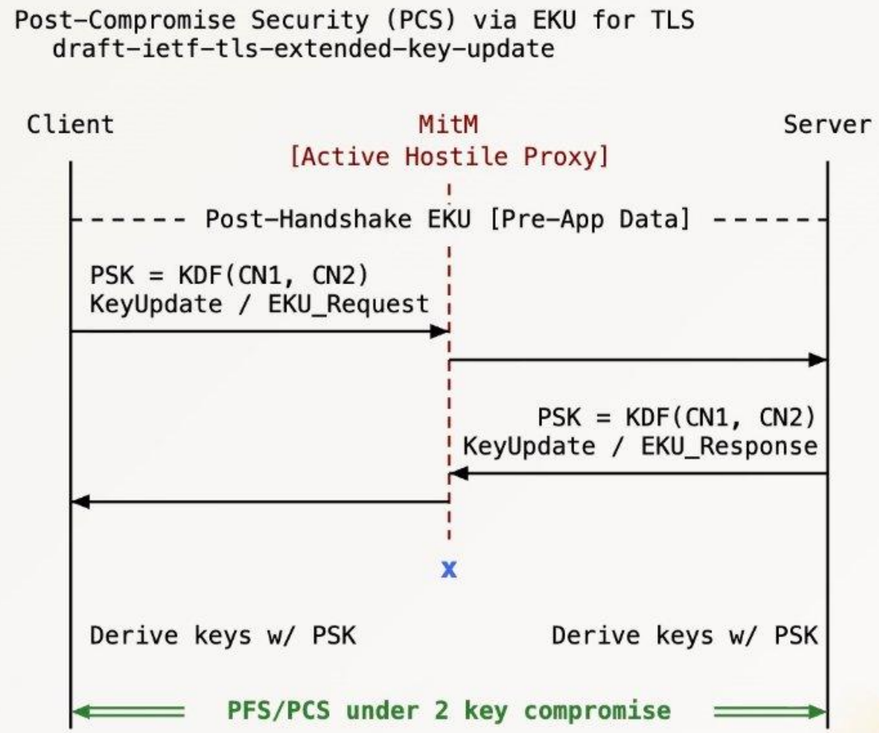
s_attest_binder ...

Factor-based Attestation and...

Something you are	`Long-term web-PKI identity key (e.g., AIK / IK / TIK)`
Something you have	`Ephemeral PSK derived from encapsulated nonces`
Bound to Evidence	`hash(pubIK_S || CN1 || CN2 || pubKEM_C)`

...Credential Transport Scheme over TLS 1.3





Pre-authentication

1. Overlapping concepts to Raw Public Keys[1], CWT over TLS[2], AuthKEM[3], likely others

2. Privacy: Identity Document need only public commitments (anything more is policy-based)

3. CWT-based ID Doc could be pulled from chunked DNS TXT records (private implementation)

---

[1] https://datatracker.ietf.org/doc/rfc7250/
[2] https://datatracker.ietf.org/doc/draft-tschofenig-tls-cwt/
[3] https://datatracker.ietf.org/doc/draft-wiggers-tls-authkem-psk/

Key lifecycles

Each draft establishes firm policy-based bounds

`draft-fossati-seat-early-attestation-03` — **Section 8.1**

> *"[...] We note that as a pure cryptographic protocol, attested TLS as-is only guarantees that the Identity Key is known by the TEE."*

`draft-fossati-seat-expat-02` — **Section 5.2**

> *"[...] A Relying Party cannot detect this attack unless additional safeguards are in place"*

`draft-ritz-seat-facts-00` — **Section 2**

> *"[...] privIK is assumed to be potentially compromisable by an adversary with sufficient access to the software layer."*

Binding Choices (abstract)

FACTS `hash(pubIK_S || CN1 || CN2 || pubKEM_C)`

Early `HKDF(Derive-Secret(0, CH...EE), pubTIK))`

EXPAT `hash(TLS-Exporter(cert_req_ctx) || pubAIK)`

Exploratory formal models on binder designs indicate that each achieves virtually equivalent security properties for their architecture, including *strong binding* and *injective agreement.*

Additional Details / Next steps

1. Enrollment with mutual or one-way attestation flows;
borrows privacy-preserving attestation order from **section 8.2** of EXPAT I-D

2. ProVerif "playground" available on GitHub[1].

3. Seeking review/collaborators on FACTS draft.

draft-ritz-seat-facts-00
nathanritz@gmail.com

Thank you!

Thanks to Bruno Blanchet, Nancy Cam-Winget, Meiling Chen, Yogesh Deshpande, Thomas Fossati, Paul Howard, Yuning Jiang, Ionuț Mihalcea, Arto Niemi, Tirumaleswar Reddy.K, Yaroslav Rosomakho, Muhammad Usama Sardar, Yaron Sheffer, Hannes Tschofenig, Paul Wouters, and the wider IETF community.

[1] https://github.com/nathanaelritz/seat_playground/tree/main/