Extensions to TLS FATT Process (draft-usama-tls-fatt-extension)

Muhammad Usama Sardar[1,2]

[1]TU Dresden, Germany

[2]Co-chair, Trusted Research Environment (TRE) Open Suite,
Global Alliance for Genomics and Health (GA4GH)

March 20, 2026

Motivation and Main Idea

- Motivation
  - Genomics and health data require high assurances. Formal analysis is a natural fit.
  - Early integration may avoid major protocol changes late in the process.
- Scope: Only for those documents that need formal analysis
- Main idea: Open-source, reproducible, extendable proofs
- Agenda
  1. Best practices template for authors
  2. Proposed FATT process tracking
  3. Some modest and not-so-modest proposals of Verifier
     - Verifier == shorthand for 'team doing the formal analysis'
     - Neither a gatekeeper nor a role in WG process
     - Recall that I supported 8773bis with a small change[1]

[1] https://mailarchive.ietf.org/arch/msg/tls/6Wk82oBGd61rTK23DgfYb7BmRKM/

1a How authors can help the Verifier to help them?

Ask to the Authors

- Motivation is critical: It helps us make a stronger case for you in adoption/WGLC. It should preferably contain:
  - compelling arguments
  - authentic references
- Realistic threat model
- Informal desired security goals
  - As draft matures, Verifier helps authors transform these goals to the achieved security goals.
- Diagrams
  - Protocol diagram (similar to the *Protocol Model* in RFC4101)
  - Key schedule diagram for changes compared to 8446bis (RFC9846)

1b Best practices template (Partial)

Ask to the Authors

- Non-binding, non-normative
- Variations possible: *Motivation* may be part of *Introduction*
- Easy for everyone (readers, reviewers, formal analysis, ...)
- Protocol and key schedule diagrams go in "Proposed solution"

2 Proposed FATT process tracking[2] (PR# 16)

Ask to the Chairs

- The process should be transparently followed.
- I volunteer to help Chairs maintain repo in the future.

Current drafts

Document	FATT Point Person	Decision email	Initial report
Key update	Thom Wiggers	TBA	TBA
PAKE	TBA	TBA	TBA
RFC9147bis	TBA	TBA	TBA

Completed documents

Document	FATT Point Person	Final report
RFC8773bis	Britta Hale	Report

Documents not reviewed by FATT

- MLKEM
- ECDHE-MLKEM
- Hybrid key exchange in TLS 1.3

[2] https://github.com/tlswg/tls-fatt/pull/16

3a Some modest proposals

- The process should be as transparent to the WG as possible.
- WG consultation and information in decisions
- FATT review may help guide/resolve some of the contention in controversial drafts.
- Active engagement from authors is requested. If authors do not respond to Verifier's questions within a reasonable time frame (e.g., a few weeks), Verifier may not pursue formal analysis of their draft.

3b Some not-so-modest proposals

- Encourage early consultation with TLS WG for TLS-related WGs (e.g., SEAT WG) if their rechartering includes making changes to the TLS protocol and key schedule beyond what is explicitly allowed in their charter.
  - More details in draft[3]
- Verifier should be allowed to contact FATT directly. CC Chairs is fine.
  - Small formal methods community; limited folks with knowledge of TLS
  - Feedback on list is limited

[3] https://www.ietf.org/archive/id/draft-usama-tls-fatt-extension-02.html#section-3.1

Discussion

- Explicitly clarify scope of FATT
  - Is computational security analysis in scope?
- Which drafts (do not) need formal analysis and why?