Transport Layer Security
Internet-Draft
Intended status: Informational
Expires: 3 September 2026

M. U. Sardar
TU Dresden

2 March 2026

Extensions to TLS FATT Process
draft-usama-tls-fatt-extension-02

Abstract

This document applies only to non-trivial extensions of TLS, which require formal analysis. It proposes the authors provide a threat model and informal security goals in the Security Considerations section, as well as motivation and a protocol diagram in the draft. We also briefly present a few pain points of the team doing the formal analysis which -- we believe -- require refining the process:

* Contacting FATT
* Understanding the opposing goals
* No response from some authors
* Slots at meeting
* Provide protection against FATT-bypass by other TLS-related WGs
* Process not being followed

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://muhammad-usama-sardar.github.io/tls-fatt-extension/draft-usama-tls-fatt-extension.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-usama-tls-fatt-extension/.

Discussion of this document takes place on the Transport Layer Security Working Group mailing list (mailto:tls@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/tls/. Subscribe at https://www.ietf.org/mailman/listinfo/tls/.

Source for this draft and an issue tracker can be found at https://github.com/muhammad-usama-sardar/tls-fatt-extension.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

While the TLS FATT process [TLS-FATT] marks a historic change in achieving high cryptographic assurances by tightly integrating formal methods in the working group (WG) process, the current FATT process has some practical limitations. Given a relatively smaller formal methods community, and a steep learning curve as well as very low consideration of usability in the existing formal analysis tools, this document proposes some solutions to make the FATT process sustainable.

Specifically, the TLS FATT process does not outline the division of responsibility between the authors and the team doing the formal analysis (the latter is hereafter referred to as the "Verifier"). This document aims to propose some solutions without putting an extensive burden on either party.

An argument is often presented by the authors that an Internet-Draft is written for the implementers. We make several counter-arguments here:

* Researchers and protocol designers are also stakeholders of such specifications [I-D.irtf-cfrg-cryptography-specification].

* Even implementers may like to understand the security implications before blindly starting to implement it.

* With the FATT process, this argument is clearly invalid. The Verifier may not be the same as the implementer.

This document outlines the corresponding changes in the way Internet-Drafts are typically written. For the Internet-Draft to be useful for the formal analysis, this document proposes that the draft should contain four main items, namely:

* motivation,

* a threat model,

* informal security goals, and

* a protocol diagram (Section 2.1).

Each one of these is summarized in Section 4. Future versions of this draft will include concrete examples.

Responsibilities of the Verifier are summarized in Section 6.

1.1. Motivation

A clear separation of responsibilities would help IRTF UFMRG to train the authors and verifiers separately to fulfill their own responsibilities.

Moreover, we believe that the experiences can help improve the FATT process.

1.2. Scope

The scope of this document is only non-trivial extensions of TLS, which require formal analysis.

2. Conventions and Definitions

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.

2.1. Protocol Diagram

In the context of this document, a Protocol Diagram specifies the proposed cryptographically-relevant changes compared to the standard TLS protocol [I-D.ietf-tls-rfc8446bis]. This is conceptually similar to the Protocol Model in [RFC4101]. However, while [RFC4101] only recommends diagrams, we consider diagrams to be essential.

2.2. Verifier

In this document, the Verifier refers to the person (team) doing the formal analysis.

2.3. Definition of Attack

Any ambiguity originating from the threat model, informal security goals, and a Protocol Diagram is to be considered as an attack. The authors are, therefore, encouraged to be as precise as possible. The Verifier may propose text for consideration by authors/WG to disambiguate or propose a fix to the attack.

3. Pain Points of Verifier

From the two extremes -- [I-D.ietf-tls-8773bis] where Russ kindly provided all requested inputs and we were able to get it through (with a small change (https://mailarchive.ietf.org/arch/msg/tls/6Wk82oBGd61rTK23DgfYb7BmRKM/)) without any formal analysis to [I-D.fossati-tls-attestation-08] where formal analysis revealed vulnerabilities [ID-Crisis] and resulted in a separate WG to tackle this problem -- we summarize the pain points of the Verifier with the hope that we can refine the process.

Note that we are not at all asserting that the authors have no pain points. They very likely have their own -- that is another indication that the process needs a refinement.

3.1. Provide Protection Against FATT-bypass by Other TLS-related WGs

TLS-related WGs in particular those where the representation of TLS WG is a minority -- including the one (SEAT WG) that the author has defended himself as one of the six proponents -- MUST NOT be allowed to make changes to the TLS protocol beyond what is explicitly allowed in their charter.

If rechartering of such WGs is _absolutely unavoidable_ and includes non-trivial changes to the TLS protocol, it MUST only be done after agreement with the TLS WG. This will prevent the short-circuit path for FATT. If the WG does not have proper FATT-like process, TLS WG may request FATT review before WGLC.

In short, our concern is:

What’s the point of such a TLS FATT process when other WGs can simply bypass this process to make key schedule level changes?

For example, [I-D.fossati-seat-early-attestation-00] makes key schedule level changes, breaks the SEAT WG charter and SEAT WG has no formal FATT-like process.

3.2. Process not being followed

The process [TLS-FATT] states:

> When a document is adopted by the working group the chairs will make a determination whether the change proposed by the document requires review by the FATT to determine if formal protocol analysis is necessary for the change. For example a proposal that modifies the TLS key schedule or the authentication process or any other part of the cryptographic protocol that has been formally modeled and analyzed in the past would likely result in asking the FATT, whereas a change such as modifying the SSLKEYLOG format would not. The working group chairs will inform the working group of this decision.

However, such information has not been provided to the WG for at least the following 2 documents:

3.2.1. ML-KEM

For the draft [I-D.ietf-tls-mlkem], the chairs acknowledge (https://mailarchive.ietf.org/arch/msg/tls/L2bWqpT3q8HVmACwD1Ta3NFimw0/) that the process was not followed:

> Unfortunately, the chairs did not announce this decision on the list (this is something that should be corrected in the process).

However:

It remains unclear what exactly "corrected in the process" entails.

The chairs further say (https://mailarchive.ietf.org/arch/msg/tls/L2bWqpT3q8HVmACwD1Ta3NFimw0/) :

> | The chairs made this decision because the mechanism in this draft
> | fits into a well defined place in the TLS protocol and does not
> | change the protocol itself.

We believe this argument does not stand, given the single data point that has gone through the FATT process -- [RFC8773bis]. Both of the mentioned conditions apply equally to [RFC8773bis] which indeed went through FATT process. The mechanism defined in [RFC8773bis] "fits into a well defined place in the TLS protocol" and "did not change the protocol itself". So we request clarification of the matter in comparison to [RFC8773bis].

We believe the security considerations of {{I-D.ietf-tls-mlkem}} are insufficient. We also believe FATT review could have significantly improved it, including but not limited to the key reuse ambiguity. We have provided significant feedback during the two WGLCs. However, almost none of that is actually reflected in the updated editor’s version.

3.2.2. Key Update

The process [TLS-FATT] states:

> | The output of the FATT is posted to the working group by the FATT
> | point person.

Based on authors’ email (https://mailarchive.ietf.org/arch/msg/tls/KFUD3FPcrUlJmnXSyb3s25UFbdo/), while it is great that FATT could find some threat, in our observation, the FATT process does not seem to be followed in spirit.

3.3. Contacting FATT

The FATT process restricts the Verifier from contacting the FATT directly. We argue that the Verifier should be allowed to contact the FATT (at least the FATT person for a specific draft) because of the following reasons:

* Formal methods community is small and within this small community, those with deep knowledge of TLS are quite limited.

Such a restriction would not have been there if the Verifier were not a member of the TLS WG and analyzing the same draft and free to contact the same FATT for advice. Being a member of the TLS WG actually puts the Verifier at unnecessary disadvantage.

* The feedback we receive on the list is really limited.

* Communication via chairs is a source of misunderstandings, as it has already happened with the chairs summarizing the intent of "Tamarin-like" to just "Tamarin".

3.4. Understanding the Opposing Goals

The authors need to understand that the task of the Verifier is to find the subtle corner cases where the protocol may fail. This is naturally opposed to the goal of the authors -- that is, to convince the WG that the protocol is good enough to be adopted/published.

Unless the Verifier remains really focused on checking subtleties, there is little value of formal analysis.

In particular, some topics like remote attestation need more precise specifications because small changes or ambiguites may make a big difference.

3.5. No Response from Some Authors

Some authors of adopted drafts do not respond for several months, despite repeated reminders [FormalAnalysisPAKE].

If any authors would like us not to do the analysis, it’s absolutely fine to clearly say so.

3.6. Slots at Meeting

Formal analysis -- just like any other code development -- is an iterative process and needs to be progressively discussed with the WG (and not just authors!) to be able to propose secure solutions.

So at least some time should be allocated in the meetings for discussion of formal analysis.

* We requested a slot for 10 minutes (and 5 minutes if tight on schedule) for discussion of our questions about [I-D.ietf-tls-extended-key-update] at IETF 124. It seemed that the slots were spread over the meeting time to show that there is no time left for our topic. In the end, the meeting ended one hour earlier where 10 minutes from that could have been utilized for discussion on formal analysis of [I-D.ietf-tls-extended-key-update]. Given that the authors were informed [FormalAnalysisKeyUpdate] about the issues, what the authors presented was not very helpful in terms of progressing the formal analysis work and proposing some solutions. Key schedule is a subtle topic and not something we can talk effectively on the mic without a proper diagram on display. It is unclear why formal analysis is such a low priority to the chairs.

* If the authors are doing the formal analysis themselves, they should also present the current state of formal analysis for discussion. This will help the Verifier give any feedback and avoid any repititive effort.

4. Responsibilities of Authors

This document proposes that the authors provide the following four items:

4.1. Motivation

The motivation of the work (i.e., the proposed extension of TLS) needs to primarily come from the authors. The Verifier can ask questions to improve it, but he cannot just cook it up.

4.2. Threat Model

A threat model outlines the assumptions and known weaknesses of the proposed protocol. The threat model could be the classical Dolev-Yao adversary. In addition, it could specify any keys (e.g., long-term keys or session keys) which may be compromised (i.e., available to the adversary).

4.3. Informal Security Goals

Knowing what you want is the first step toward achieving it. Hence, informal security goals such as integrity, authentication, freshness, etc. should be outlined in the Internet-Draft. If the informal security goals are not spelled out in the Internet-Draft, it is safe to assume that the goals are still unclear to the authors.

4.4. Protocol Diagram

A Protocol Diagram should clearly mention the initial knowledge of the protocol participants, e.g., which authentic public keys are known to the protocol participants at the start of the protocol. An example of a Protocol Diagram for [I-D.fossati-tls-attestation-08] is provided in Figure 5 in [ID-Crisis].

5. Document Structure

While the needs may differ for some drafts, we propose the following baseline template, with an example of [I-D.wang-tls-service-affinity]:

TODO: Currently it is almost a copy of the guidance email (https://mailarchive.ietf.org/arch/msg/tls/LfIHs1OVwDKWmDuCEx0p8wP-KPs/) to the authors. We will add details in next version.

5.1. Introduction

* Problem statement: Say in general what the problem is.

* For [I-D.wang-tls-service-affinity], we believe this should _not_ include CATS. Anyone unfamiliar with CATS should be able to understand your problem.

5.2. Terminology

* Define any terms not defined in RFC8446bis or point to other drafts from where the definition is used.

5.3. Motivation and design rationale

* We really like how Russ motivates the problem statement in [I-D.ietf-tls-8773bis]. Use it as a sample.

* Here authors should address all the concerns from WG, including justification with compelling arguments and authentic references why authors think it should be done within TLS WG (and within handshake).

* For [I-D.wang-tls-service-affinity], authors could put CATS here as a motivational use case.

5.4. Proposed solution (one or more sections)

* Protocol design with Protocol Diagram: we work on the formal analysis of TLS 1.3 exclusively. Please contact someone else if your draft relates to older versions.

5.5. Security considerations

5.5.1. Threat model

5.5.2. Desired security goals

As draft proceeds these desired security goals will become what the draft actually achieves.

5.5.3. Other security implications/considerations

6. Responsibilities of Verifier

When the authors declare the version as ready for formal analysis, the Verifier takes the above inputs, performs the formal analysis, and brings the results back to the authors and the WG. Based on the analysis, the verifier may propose updates to the Security Considerations section or other sections of the Internet-Draft.

7. Security Considerations

The whole document is about improving security considerations.

8. IANA Considerations

This document has no IANA actions.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[TLS-FATT] IETF TLS WG, "TLS FATT Process", June 2025, <https://github.com/tlswg/tls-fatt>.

9.2. Informative References

[FormalAnalysisKeyUpdate]
Sardar, M. U., "Comments on draft-ietf-tls-extended-key-update", October 2025, <https://mailarchive.ietf.org/arch/msg/tls/P_VdWSi20TZG0rJEaz7VCPKDIOg/>.

[FormalAnalysisPAKE]
Sardar, M. U., "Formal analysis of draft-ietf-tls-pake", January 2026, <https://mailarchive.ietf.org/arch/msg/tls/igQGFE1INA6eR_Fdz8eTp74ffVc/>.

[I-D.fossati-seat-early-attestation-00]
Sheffer, Y., Mihalcea, I., Deshpande, Y., Fossati, T., and T. Reddy.K, "Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", Work in Progress, Internet-Draft, draft-fossati-seat-early-attestation-00, 9 January 2026, <https://datatracker.ietf.org/doc/html/draft-fossati-seat-early-attestation-00>.

[I-D.fossati-tls-attestation-08]
Tschofenig, H., Sheffer, Y., Howard, P., Mihalcea, I., Deshpande, Y., Niemi, A., and T. Fossati, "Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", Work in Progress, Internet-Draft, draft-fossati-tls-attestation-08, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-fossati-tls-attestation-08>.

[I-D.ietf-tls-8773bis]
Housley, R., "TLS 1.3 Extension for Using Certificates with an External Pre-Shared Key", Work in Progress, Internet-Draft, draft-ietf-tls-8773bis-13, 5 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-8773bis-13>.

[I-D.ietf-tls-extended-key-update]
Tschofenig, H., T端xen, M., Reddy.K, T., Fries, S., and Y. Rosomakho, "Extended Key Update for Transport Layer Security (TLS) 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-extended-key-update-10, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-extended-key-update-10>.

[I-D.ietf-tls-mlkem]
Connolly, D., "ML-KEM Post-Quantum Key Agreement for TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-mlkem-07, 12 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-mlkem-07>.

[I-D.ietf-tls-rfc8446bis]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8446bis-14, 13 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8446bis-14>.

[I-D.irtf-cfrg-cryptography-specification]
Sullivan, N. and C. A. Wood, "Guidelines for Writing Cryptography Specifications", Work in Progress, Internet-Draft, draft-irtf-cfrg-cryptography-specification-02, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-cryptography-specification-02>.

[I-D.wang-tls-service-affinity]
Wang, W., Wang, A., Sahni, M., and K. Sheth, "Service Affinity Solution based on Transport Layer Security (TLS)", Work in Progress, Internet-Draft, draft-wang-tls-service-affinity-00, 17 October 2025, <https://datatracker.ietf.org/doc/html/draft-wang-tls-service-affinity-00>.

[ID-Crisis]
Sardar, M. U., Moustafa, M., and T. Aura, "Identity Crisis in Confidential Computing: Formal Analysis of Attested TLS", November 2025, <https://www.researchgate.net/publication/398839141_Identity_Crisis_in_Confidential_Computing_Formal_Analysis_of_Attested_TLS>.

[RFC4101] Rescorla, E. and IAB, "Writing Protocol Models", RFC 4101, DOI 10.17487/RFC4101, June 2005, <https://www.rfc-editor.org/rfc/rfc4101>.

[RFC8773bis]
Housley, R., "TLS 1.3 Extension for Certificate-Based Authentication with an External Pre-Shared Key", RFC 8773, DOI 10.17487/RFC8773, March 2020, <https://www.rfc-editor.org/rfc/rfc8773>.

Appendix

Document History

-02

* Added document structure
* FATT-bypass by Other TLS-related WGs
* FATT process not being followed

-01

* Pain points of Verifier Section 2.1
* Small adjustment of phrasing

Author’s Address

Muhammad Usama Sardar
TU Dresden
Email: muhammad_usama.sardar@tu-dresden.de