Transport Layer Security
Internet-Draft
Intended status: Informational
Expires: 22 October 2026

M. U. Sardar
TU Dresden

20 April 2026

Extensions to TLS FATT Process
draft-usama-tls-fatt-extension-05

Abstract

This document applies only to non-trivial extensions of TLS, which require formal analysis. It proposes the authors specify 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:

* Provide protection against FATT-bypass by other TLS-related WGs

* Contacting FATT

* ML-KEM

* Understanding the opposing goals

* Response within reasonable time frame

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 an 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 5. Future versions of this draft will include concrete examples.

Responsibilities of the Verifier are summarized in Section 7.

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. The goal is to document the identified gaps with concrete examples, discuss those and mutually find the best way forward.

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 team doing the formal analysis. Note that it is NOT a new formal role in the WG process.

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. 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".

FATT is a ’design team’ as per {{RFC2418}}. We kindly request clarification under which regulation chairs can stop the Verifier from talking to a design team?

3.3. ML-KEM

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 preference of hybrids. We have provided significant feedback during the two WGLCs. However, almost none of that is actually reflected in the updated editor's version.

3.3.1. Formal analysis (Work-in-progress)

We have presented observation from our ongoing symbolic security analysis (cf. limitations in Section 8) using ProVerif on the mailing list.

We argue that in general:

1. Migration from ECDHE to hybrid is security improvement.

2. Migration from hybrid to pure ML-KEM is security regression.

3.3.1.1. Hybrid PQ/T

More formally, the property hybrid PQ/T should provide is:

Hybrid PQ/T is secure unless both ECDHE and ML-KEM are broken.

Hybrid preserves ECDHE, and adds ML-KEM as an additional factor. So as long as one of them is not broken, the system is secure. In particular, even if ML-KEM is completely broken, the system retains the security level of ECDHE.

3.3.1.2. Non-hybrid PQ

On the other hand, the formal property non-hybrid PQ provides is:

Non-hybrid PQ is secure unless ML-KEM is broken.

If ML-KEM is broken, the whole system is broken.

3.3.1.3. Comparison

Leak out the ECDHE key from hybrid PQ/T and you get a pure ML-KEM. Clearly, hybrid is in general more secure, unless ECDHE is fully broken, in which case it still falls equivalent to pure ML-KEM, or in the hypothetical scenario that there is an implementation bug in the ECDHE part which is triggered only in composition.

3.3.2. "Cost"

"Cost" has been presented on the list as the motivation for ML-KEM but no authentic reference has yet been presented. There seems to be a need for a thorough study to understand the "cost."

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. Response within reasonable time frame

If authors do not respond to the Verifier’s questions within a reasonable time frame (say a few weeks but not months), the Verifier may not pursue formal analysis of their draft.

4. Proposed solutions

In addition to those mentioned inline in the previous section, we propose the following:

4.1. Scope of FATT

* Be more explicit on:
  - what is the scope of FATT?
  - what kind of drafts need FATT review and why? Discussion on this is happening in issue 19 (https://github.com/tlswg/tls-fatt/issues/19).

4.2. Discussion 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.

If the authors are doing the formal analysis themselves, it would be helpful to also present the current state of formal analysis in meetings for discussion. This may be a single slide describing:

* Approach used: symbolic or computational

* Tool used: ProVerif, CryptoVerif etc.

* Properties established

This will help the Verifier give any feedback and avoid any repititive effort.

5. Responsibilities of Authors

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

5.1. 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.

5.2. Threat Model

A threat model identifies which threats are in scope for the protocol design. So it should answer questions like:

* What are the capabilities of the adversary? What can the adversary do?

* Whether post-quantum threats are in scope?

* What can go wrong in the system? etc.

5.2.1. Typical Dolev-Yao adversary

A typical threat model assumes the classical Dolev-Yao adversary, who has full control over the communication channel.

Any additional adversary capabilities and assumptions must be explicitly stated.

5.2.2. Potential Weaknesses of Cryptographic Primitives

In general, it also outlines the potential weaknesses of the cryptographic primitives used in the proposed protocol extension. Examples include:

* weak hash functions
* weak Diffie-Hellman (DH) groups
* weak elements within strong DH groups

5.2.3. Keys

This section should specify any keys in the system (e.g., long-term keys of the server) in addition to the standard TLS key schedule. Theoretically and arguably practically, any key may be compromised (i.e., become available to the adversary).

For readability, we propose defining each key clearly as in Section 4.1 of [ID-Crisis]. Alternatively, present as a table with the following entries for each key:

* Name (or symbol) of the key
* Purpose of the key
* (optionally but preferably -- particularly when the endpoint is not fully trusted) Which software in the system has access to the key?

If more than one servers are involved (such as migration cases), the keys for servers should be distinguished in an unambiguous way.

5.3. 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.

Examples:

* Integrity of message X holds unless some key Y is leaked.
* Freshness of message X holds unless some key Y or some key Z is leaked.

* Server Authentication holds unless some key Y or some key Z is leaked.

See Section 5.1 of [ID-Crisis] for concrete examples.

5.4. 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].

6. 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]:

The template is:

* Easy for readers

* Easy for reviewers

* Easy for formal analysis

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 versions.

6.1. 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.

6.2. Terminology

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

6.3. 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.

6.4. 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.

6.5. Security considerations

6.5.1. Threat model

6.5.2. Desired security goals

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

6.5.3. Other security implications/considerations

7. 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.

8. Security Considerations

The whole document is about improving security considerations.

Like all security proofs, formal analysis is only as strong as its assumptions and model. The scope is typically limited, and the model does not necessarily capture real-world deployment complexity, implementation details, operational constraints, or misuse scenarios. Formal methods should be used as complementary and not as subtitute of other analysis methods.

9. IANA Considerations

This document has no IANA actions.

10. References

10.1. 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>.

10.2. Informative References

[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-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-01, 8 April 2026, <https://datatracker.ietf.org/doc/html/draft-wang-tls-service-affinity-01>.

[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>.

[RFC2418] Bradner, S., "IETF Working Group Guidelines and Procedures", BCP 25, RFC 2418, DOI 10.17487/RFC2418, September 1998, <https://www.rfc-editor.org/rfc/rfc2418>.

[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

-05

* Removed process-related stuff
* Moved discussion at meeting to solutions
* Added ML-KEM

-04

* Extended threat model Section 5.2
* Helpful discussions on formal analysis in meetings in Section 4.2
* Pointer to formal analysis and costs in Section 3.3

-03

* Limitations of formal analysis in security considerations
* Proposed solutions section
* More guidance for authors: Threat Model and Informal Security Goals

-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

Acknowledgments

We thankfully acknowledge Eric Rescorla and John Mattsson for their valuable input.

The research work is funded by Deutsche Forschungsgemeinschaft.

Author’s Address

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