

Transport Layer Security
Internet-Draft
Intended status: Informational
Expires: 11 July 2026

M. U. Sardar
TU Dresden
7 January 2026

Extensions to TLS FATT Process
draft-usama-tls-fatt-extension-01

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, and a protocol diagram in the draft. We also briefly present a few pain points of the one doing the formal analysis which require refining the process:

- * Contacting FATT
- * Understanding the opposing goals
- * No response from some authors
- * Slots at meeting

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

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 11 July 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	3
1.1. Motivation	4
2. Conventions and Definitions	4
2.1. Protocol Diagram	4
2.2. Definition of Attack	4
2.3. Verifier	4
3. Pain Points of Verifier	4
3.1. Contacting FATT	5
3.2. Understanding the Opposing Goals	5
3.3. No Response from Some Authors	5
3.4. Slots at Meeting	5
4. Responsibilities of Authors	6
4.1. Threat Model	6
4.2. Informal Security Goals	6
4.3. Protocol Diagram	6
5. Responsibilities of Verifier	6
6. Security Considerations	6
7. IANA Considerations	6
8. References	6
8.1. Normative References	6

8.2. Informative References	7
Appendix	8
Document History	8
Author's Address	8

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 one 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 three main items, namely:

- * 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 5.

1.1. Motivation

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

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. 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.

2.3. Verifier

In this document, verifier refers to the person doing the formal analysis.

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 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.

3.1. Contacting FATT

The verifier should be allowed to contact the FATT at least once some draft is out from the TLS WG. Formal methods community is small and those with deep knowledge of TLS are quite limited. Not being able to contact them puts the verifier at great disadvantage.

3.2. 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. But unless the verifier remains really focused on doing that, there is little value of formal analysis. In particular, some topics like remote attestation need more precise specifications because small changes may make a big difference.

3.3. No Response from Some Authors

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

3.4. Slots at Meeting

Formal analysis -- just like any other code development -- is an iterative process and needs to be progressively discussed with the WG 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 repetitive effort for the verifier.

4. Responsibilities of Authors

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

4.1. 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).

4.2. 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.

4.3. 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. 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.

6. Security Considerations

The whole document is about improving security considerations.

7. IANA Considerations

This document has no IANA actions.

8. References

8.1. 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>>.

8.2. 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-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-07, 1 November 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-tls-extended-key-update-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>>.

[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>>.

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

Appendix

Document History

-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