Secure Evidence and Attestation Transport
Internet-Draft
Intended status: Informational
Expires: 17 July 2026

M. U. Sardar
TU Dresden

13 January 2026

Early Attestation is Broken
draft-usama-seat-early-attestation-is-broken-00

Abstract

Sheffer et al. published [I-D.fossati-seat-early-attestation] on 9th January, 2025 and despite being wildly out of scope of SEAT charter, the draft made its place -- getting two-thirds of meeting time -- in the agenda for upcoming SEAT interim meeting within hours of publishing. In comparison, our request to present [I-D.fossati-seat-expat] fully within the charter was refused. In this document, we disprove the claim made in [I-D.fossati-seat-early-attestation] for backward compatibility with standard TLS [I-D.ietf-tls-rfc8446bis]. We argue that [I-D.fossati-seat-expat] is a much more reaonsable way of achieving the goal within the scope of SEAT charter.

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/seat-early-attestation-broken/draft-usama-seat-early-attestation-is-broken.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-usama-seat-early-attestation-is-broken/.

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

Source for this draft and an issue tracker can be found at https://github.com/muhammad-usama-sardar/seat-early-attestation-broken.

Status of This Memo

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

This Internet-Draft will expire on 17 July 2026.

Copyright Notice

Table of Contents

1. Introduction

We argue that:

* [I-D.fossati-seat-early-attestation] is out of scope of SEAT WG charter.

* Several claims in [I-D.fossati-seat-early-attestation] are broken. Specifically, we prove that proposed key schedule is inconsistent with [I-D.ietf-tls-rfc8446bis].

* [I-D.fossati-seat-early-attestation] breaks most -- if not all -- proofs done to date for TLS 1.3.

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.

3. Out of Scope

[SEAT-Charter] has:

> The attested (D)TLS protocol extension will not modify the (D)TLS protocol itself. It may define (D)TLS extensions to support its goals but will not modify, add, or remove any existing protocol messages or modify the key schedule.

Contrary to the crystal clear statement of scope:

* Section 4.1 of [I-D.fossati-seat-early-attestation] adds a new protocol message named "Attestation".

* Section 5.6 of [I-D.fossati-seat-early-attestation] modifies the key schedule.

Both are subtle and error-prone. Such intesive changes should not bypass FATT process at TLS WG by any means. SEAT has just a mention of formal analysis in its charter and no real process. SEAT also does not have the blessing of many TLS experts. It makes pursuing such a work in SEAT almost surely to lead to failure. We recommend the authors of [I-D.fossati-seat-early-attestation] to submit the draft to TLS WG, where such changes are in scope.

3.1. Comparison with our draft

In comparison, [I-D.fossati-seat-expat] makes no changes to TLS and is fully in scope of SEAT charter.

4. Broken Claims

Too many claims in [I-D.fossati-seat-early-attestation] are broken. We present one example which invalidates most of other claims. The key schedule proposed in Section 5.6 of [I-D.fossati-seat-early-attestation] is not consistent with [I-D.ietf-tls-rfc8446bis].

Using notations from [Key-Schedule]:

hs = HKDF-Extract(salt1,gxy)

whereas this draft proposes:

hs’ = HKDF-Extract(0,gxy)

4.1. Proof

Using definition of salt1 [Key-Schedule]:

salt1 != 0

Therefore, it comes that:

hs != hs’

Hence, the key schedule in [I-D.fossati-seat-early-attestation] is inconsistent with [I-D.ietf-tls-rfc8446bis].

4.2. Comparison with our draft

In comparison, [I-D.fossati-seat-expat] uses standard TLS key schedule without any changes.

5. Breaking Formal Proofs

Because of above key schedule change, the draft breaks most -- if not all -- proofs done to date for TLS 1.3.

5.1. Comparison with our draft

In comparison, we are making a careful effort to preserve security properties for our draft [I-D.fossati-seat-expat].

6. Security Considerations

This draft helps make this world more secure by refuting the security claims in [I-D.fossati-seat-early-attestation] and by pushing against disruption of FATT process of TLS WG. Security is dependent on weakest link and we believe [I-D.fossati-seat-early-attestation] is the weakest link in the security of TLS. Hence, we view post-handshake attestation as the most appropriate option.

7. IANA Considerations

This document has no IANA actions.

8. References

8.1. Normative References

[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>.

[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

[I-D.fossati-seat-early-attestation]
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-seat-expat]
Fossati, T., Sardar, M. U., Reddy.K, T., Sheffer, Y., Tschofenig, H., and I. Mihalcea, "Remote Attestation with Exported Authenticators", Work in Progress, Internet-

Draft, draft-fossati-seat-expat-00, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-fossati-seat-expat-00>.

[Key-Schedule]
Sardar, M. U., "Perspicuity of Attestation Mechanisms in Confidential Computing: Validation of TLS 1.3 Key Schedule", October 2025, <https://www.researchgate.net/publication/396245726_Perspicuity_of_Attestation_Mechanisms_in_Confidential_Computing_Validation_of_TLS_13_Key_Schedule>.

[SEAT-Charter]
IETF, "Secure Evidence and Attestation Transport (SEAT): Charter for Working Group", <https://datatracker.ietf.org/wg/seat/about/>.

Acknowledgments

We thank the authors of [I-D.fossati-seat-early-attestation] for putting together something, which is already long overdue.

Since the proof in Section 4.1 is based on the working done in [Key-Schedule], we thank all those acknowledged there: namely Arto Niemi, Hannes Tschofenig, Thomas Fossati, Eric Rescorla, and Ionut Mihalcea

Author’s Address

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