# TLS Exported Attestation (EXPAT) BOF

Chairs:

Nancy Cam-Winget

Wes Hardaker

Mailing List:

https://www.ietf.org/mailman/listinfo/expat

# Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

# Note Well, page 2

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

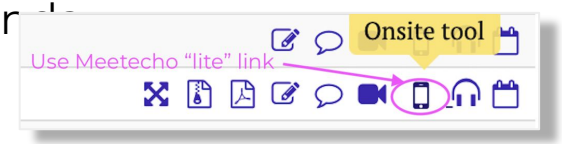
# IETF Code Of Conduct Guidelines RFC7154

1. Treat colleagues with respect
2. Speak slowly and limit the use of slang
3. Dispute ideas by using reasoned argument
4. Use best engineering judgment
5. Find the best solution for the whole Internet
6. Contribute to the ongoing work of the group and the IETF

# This session is being recorded

**In-person participants**

- Make sure to sign into the session using the Meetecho (usually the “onsite tool” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- *Keep audio and video off if not using the onsite version*




**Remote participants**

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

# EXPAT Information

**Purpose:** Standardize a TLS extension enabling attestation of one or both endpoints.

**Datatracker:** https://datatracker.ietf.org/doc/bofreq-fossati-tls-exported-attestation-expat/

**Mailing list information:**

List: expat@ietf.org

Subscribe: https://www.ietf.org/mailman/listinfo/expat

**Drafts under consideration:**

draft-fossati-tls-exported-attestation

# Agenda

| | | |
|---|---|---|
| WG Introduction | Chairs | 5m |
| Problem Statement | Chairs | 5m |
| Why not RATS / TLS? | Area Director | 5m |
| Problem to be solved | Yaron Sheffer | 10m |
| Use cases | Thomas Fossati | 10m |
| Design Space of Attested TLS | Muhammad Usama Sardar | 10m |
| Open MIC comments | Audience | 30m |
| BOF Questions | Chairs | 5m |
| Charter and scope discussion | Chairs | Remaining |

# Why are we here? Chair’s Problem Statement

- Current and evolving deployments require the need to verify the peer’s:
  - Cryptographic (private) keys are stored securely
  - Device’s software/firmware is untampered
  - Secure boot is enabled
  - Boot- and run-time integrity of a peer.

- Verification can be achieved using the Architecture defined in RATs (RFC 9334) but conveyed in a post a successful TLS handshake

# BoF Questions

1. Is the problem well understood?
2. Is this problem tractable?
3. Is the IETF the right place to address the problem?
4. Is there sufficient community interest to work on the problem?

# Proposed Charter

# Background and Motivation (1/2)

In many scenarios, particularly with the rise of Trusted Execution Environments (TEEs) and the increasing security demands for IoT devices and confidential workloads, it's crucial also to ensure that the peer’s state is as expected, in addition to conventional authentication (verification of identity)..

Remote attestation (RFC9334) addresses this by allowing an entity to produce verifiable Evidence about its current state - such as proving that its software and firmware haven't been tampered with, that secure boot is enabled, or that cryptographic keys are securely stored within a hardware-protected environment.

This provides a stronger assurance of trustworthiness, helping to prevent attacks that might compromise a system even if its traditional credentials remain valid, and enables authorization policies based on richer security signals.

# Background and Motivation (2/2)

To address this need for enhanced, verifiable trustworthiness, this WG will deliver a Standards Track solution based on a post-handshake exchange for TLS that enables the attestation of one or both TLS endpoints.

Such a mechanism would allow an entity to produce (fresh) Evidence or an Attestation Result about itself for another party to evaluate.

This effort will focus on leveraging the (D)TLS handshake protocol as-is. It will also leverage the existing RATS toolbox to ensure interoperability with existing and future attestation technologies.

# Scope (1/2)

This working group has a narrow focus: to produce a single document specifying a post-handshake exchange for TLS that provides attestation of one or both TLS endpoints.

More specifically:

- The protocol should be agnostic to remote attestation technologies.
- TLS 1.3 handshake protocol should be used as-is, leveraging its existing deployment and security guarantees, including formal validation.
- The protocol may specify negotiation mechanisms within the initial TLS handshake.
- The protocol must allow per-session freshness.

# Scope (2/2)

The working group will not extend TLS or create new remote attestation technologies or cryptographic protocol mechanisms.

The working group will engage with the research community on the formal analysis of the protocol atefacts in parallel with the specification work.

The WG will consider using Exported Authenticators [RFC9261] as the post-handshake mechanism and Conceptual Message Wrapper (CMW) as the format for the attestation credential.

# Dependencies and Liaisons

- The working group will keep the TLS and RATS working groups informed of its activities by presenting updates at their meetings and requesting reviews.

- The working group will engage with the UFM research group regarding formal analysis of the resulting work.

# Forming WG Charter Question

1. Is there support to form a WG with the proposed charter?