

SEAT

Secure Evidence and Attestation Transport



IETF125 - Shenzhen

Note Well

By participating in the IETF you agree to follow IETF processes and policies. This Note Well is a reminder of some of those policies. For a linked version of this text, please visit www.ietf.org/note-well or use the QR code below.

- IETF participants are expected to behave in a professional manner and extend respect and courtesy to their colleagues at all times (see *RFC 7154: IETF Guidelines for Conduct and IETF Anti-Harassment Policy*). If you have any concerns about behavior, please contact the *Ombudsteam* who have a duty of confidentiality and extensive powers to act, as set out in *RFC 7776: IETF Anti-Harassment Procedures*.
- If you are aware that any IETF contribution (as defined in *RFC 5378: Rights Contributors Provide to the IETF Trust*) is covered by patents or patent applications that are owned or controlled by you, your employer or your sponsor, you must disclose that fact, or not participate in the discussion (see *RFC 8179: Intellectual Property Rights in IETF Technology*).
- For detailed process information consult *RFC 2026: Internet Standards Process* and *RFC 2418: IETF Working Group Guidelines and Procedures* and updates to those.
- The IETF routinely makes public written, audio, video, and photographic records of IETF activities, including your personal information as set out in the *IETF Privacy Statement*.

For advice, please talk to Working Group chairs or Area Directors.



Agenda for today

- 1. Welcome, agenda bashing, interim review**
Chairs (10 minutes)
- 2. Pre-, Intra- and Post-handshake Attestation**
Usama (20 minutes)
- 3. Factor-based Attestation and Credential Transport Scheme (FACTS) over TLS 1.3**
Nathanael (20 minutes)
- 4. Remote Attestation with Exported Authenticators**
Tiru and Usama (20 minutes)
- 5. Early Attestation**
Yaron (20 minutes)



Interim topic 1/2: use cases

- **6 use cases**
- **9 integration properties**
- **Poll: is draft-mihalcea-seat-use-cases document ready for adoption?**
- **Note: once we adopt use cases, we will judge proposed attestation mechanisms against those use cases**



Interim topic 2/2: early attestation

- Initial proposal out of scope for SEAT charter
- Authors adjusted their proposal and claim that the updated specification is within the charter
 - *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.*
- **Poll: have you read draft-fossati-seat-early-attestation-03?**



Organizational notes

- Mailing list: seat@ietf.org
 - **Mailing list is the main avenue for communication in the working group!**
- GitHub: <https://github.com/ietf-wg-seat>
 - We will follow RFC8874

