Design Space, Tradeoffs and Formal Analysis of Attested TLS Protocols for Confidential Computing

Muhammad Usama Sardar*

Based on joint works with Arto Niemi, Hannes Tschofenig, Thomas Fossati, Simon Frost, Ned Smith, Ionut Mihalcea, Yaron Sheffer, Tirumaleswar Reddy, Carsten Weinhold and Michael Roitzsch

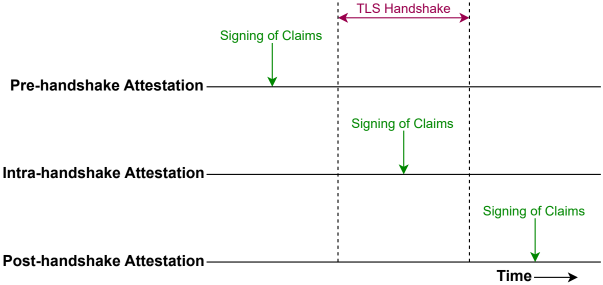
*TU Dresden, Germany

July 21, 2025

Teleport

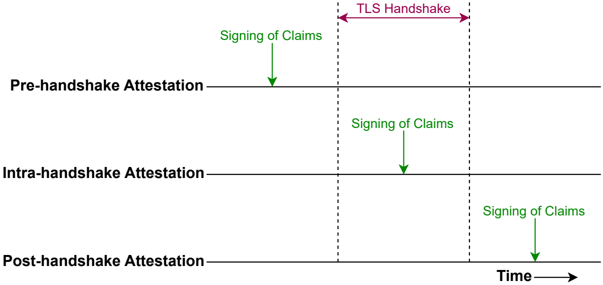
Categories of Attested TLS Protocols

- Temporal ordering of Remote Attestation and TLS at Attester side



Categories of Attested TLS Protocols

- Temporal ordering of Remote Attestation and TLS at Attester side

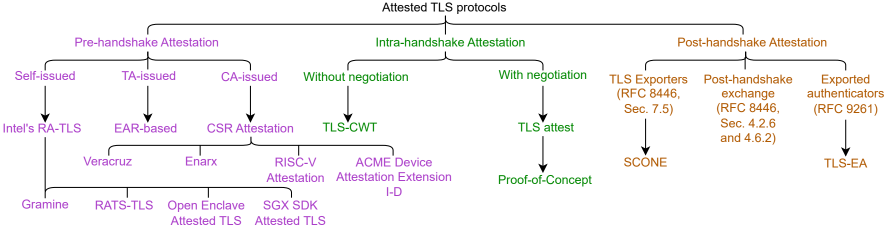


- Typical changes in each category
  - CA/RA/TA = Certification/Registration/Trusted Authority

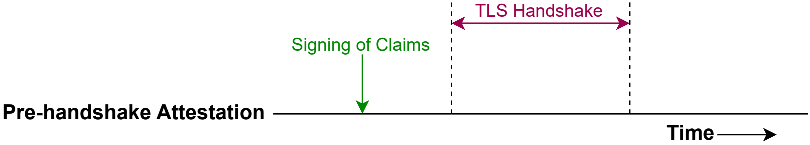
	Protocol	Deployment	Application layer
Pre-handshake attestation	✓	✓ (CA/RA/TA)	×
Intra-handshake attestation	✓ (Invasive)	×	×
Post-handshake attestation	✓ (Negotiation extension)	×	✓

Design Space

- Fragmentation in industry



Pre-handshake Attestation

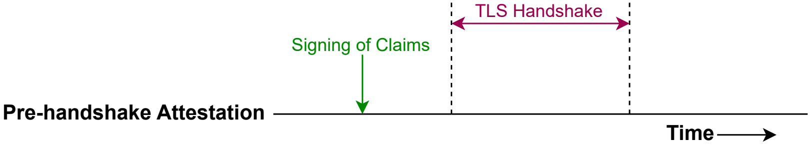


- General limitation
  - Per-session Evidence freshness[1] is not provided.

[1]Sardar, Niemi, Tschofenig, and Fossati, "Towards Validation of TLS 1.3 Formal Model and Vulnerabilities in Intel's RA-TLS Protocol", 2024.

[2]Ounsworth, Tschofenig, Birkholz, Wiseman, and Smith, *Use of Remote Attestation with Certification Signing Requests*, 2025.

Pre-handshake Attestation

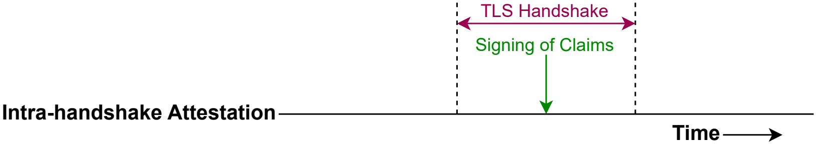


- General limitation
  - Per-session Evidence freshness[1] is not provided.
- Example: CSR attestation[2]

[1] Sardar, Niemi, Tschofenig, and Fossati, "Towards Validation of TLS 1.3 Formal Model and Vulnerabilities in Intel's RA-TLS Protocol", 2024.

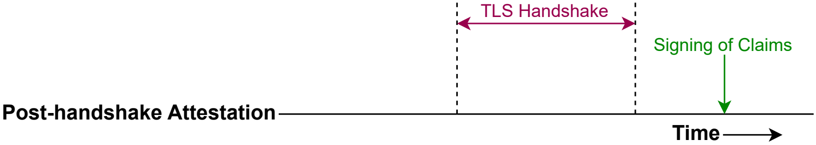
[2] Ounsworth, Tschofenig, Birkholz, Wiseman, and Smith, *Use of Remote Attestation with Certification Signing Requests*, 2025.

Intra-handshake Attestation



- General limitations
  - Invasive changes in TLS protocol (potentially as deep as key schedule)
  - Challenges in attestation credential refresh

Post-handshake Attestation



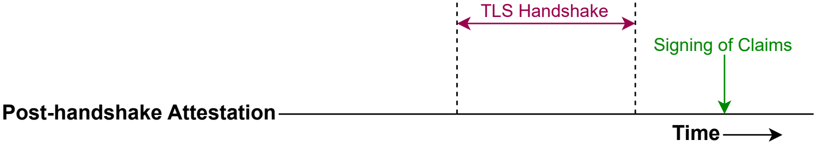
- General limitations
  - Requires application-layer changes
  - Small latency impact (only for first authentication request)

[3] Fossati, Sardar, Reddy.K, Sheffer, Tschofenig, and Mihalcea, *Remote Attestation with Exported Authenticators*, 2025.

[4] Sullivan, *Exported Authenticators in TLS*, 2022.

[5] Birkholz, Smith, Fossati, Tschofenig, and Glaze, *RATS Conceptual Messages Wrapper (CMW)*, 2025.

Post-handshake Attestation



- General limitations
  - Requires application-layer changes
  - Small latency impact (only for first authentication request)
- Proposal[3]
  - Mechanism: Exported Authenticators[4]: RFC 9261
  - Format: Conceptual Message Wrapper[5] (CMW)
  - Formal analysis in ProVerif (work in progress)

[3] Fossati, Sardar, Reddy.K, Sheffer, Tschofenig, and Mihalcea, *Remote Attestation with Exported Authenticators*, 2025.

[4] Sullivan, *Exported Authenticators in TLS*, 2022.

[5] Birkholz, Smith, Fossati, Tschofenig, and Glaze, *RATS Conceptual Messages Wrapper (CMW)*, 2025.

Key References

Birkholz, Henk, Ned Smith, Thomas Fossati, Hannes Tschofenig, and Dionna Glaze. *RATS Conceptual Messages Wrapper (CMW)*. Internet-Draft draft-ietf-rats-msg-wrap-16. Work in Progress. Internet Engineering Task Force, July 2025. 39 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-rats-msg-wrap/16/.

Fossati, Thomas, Muhammad Usama Sardar, Tirumaleswar Reddy.K, Yaron Sheffer, Hannes Tschofenig, and Ionuț Mihalcea. *Remote Attestation with Exported Authenticators*. Internet-Draft draft-fossati-tls-exported-attestation-01. Work in Progress. Internet Engineering Task Force, May 2025. 15 pp. URL: https://datatracker.ietf.org/doc/draft-fossati-tls-exported-attestation/01/.

Ounsworth, Mike, Hannes Tschofenig, Henk Birkholz, Monty Wiseman, and Ned Smith. *Use of Remote Attestation with Certification Signing Requests*. Internet-Draft draft-ietf-lamps-csr-attestation-19. Work in Progress. Internet Engineering Task Force, May 2025. 51 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-lamps-csr-attestation/19/.

Sardar, Muhammad Usama, Arto Niemi, Hannes Tschofenig, and Thomas Fossati. "Towards Validation of TLS 1.3 Formal Model and Vulnerabilities in Intel's RA-TLS Protocol". In: *IEEE Access* 12 (2024), pp. 173670–173685. DOI: 10.1109/ACCESS.2024.3497184.

Sullivan, Nick. *Exported Authenticators in TLS*. RFC 9261. July 2022. DOI: 10.17487/RFC9261. URL: https://www.rfc-editor.org/info/rfc9261.

ACK

Co-authors

- Arto Niemi (Huawei)
- Thomas Fossati (Linaro)
- Hannes Tschofenig (University of Applied Sciences Bonn-Rhein-Sieg and Siemens)
- Simon Frost (Arm)
- Ned Smith (Intel)
- Ionut Mihalcea (Arm)
- Carsten Weinhold (Barkhausen Institut)
- Michael Roitzsch (Barkhausen Institut)
- Yogesh Deshpande (Arm)
- Yaron Sheffer (Intuit)
- Tirumaleswar Reddy K. (Nokia)
- Henk Birkholz (Fraunhofer SIT)
- Mariam Moustafa (Aalto University)
- Tuomas Aura (Aalto University)

Contributors

- Christopher Patton (Cloudflare)
- Jean-Marie Jacquet (University of Namur)
- Pavel Nikonorov (GENXT)
- Laurence Lundblade (Security Theory LLC)
- Dionna Amalie Glaze (Google)
- Bob Beck (Google)
- Mike Ounsworth (Entrust)
- John Preuß Mattsson (Ericsson Research)
- Cedric Fournet (Microsoft)
- Thore Sommer (TU Munich)
- Nikolaus Thümmel (Scontain)
- Giridhar Mandyam (Mediatek)
- Jonathan Hoyland (Cloudflare)
- Jo Van Bulck (KU Leuven)

CONFIDENTIAL COMPUTING CONSORTIUM

GENXT