Remote Attestation with Exported Authenticators (draft-fossati-seat-expat)

Muhammad Usama Sardar[1,2], Thomas Fossati, Tirumaleswar Reddy K.[3], Yaron Sheffer, Hannes Tschofenig, and Ionuț Mihalcea

[1]TU Dresden, Germany

[2]Co-chair, Trusted Research Environment (TRE) Open Suite, Global Alliance for Genomics and Health (GA4GH)

[3]Nokia, India

March 17, 2026

Outline

1. Community Interest
2. Quick Recap of Protocol
3. Status of Formal Analysis
4. Discussion

Community Interest Since IETF 124

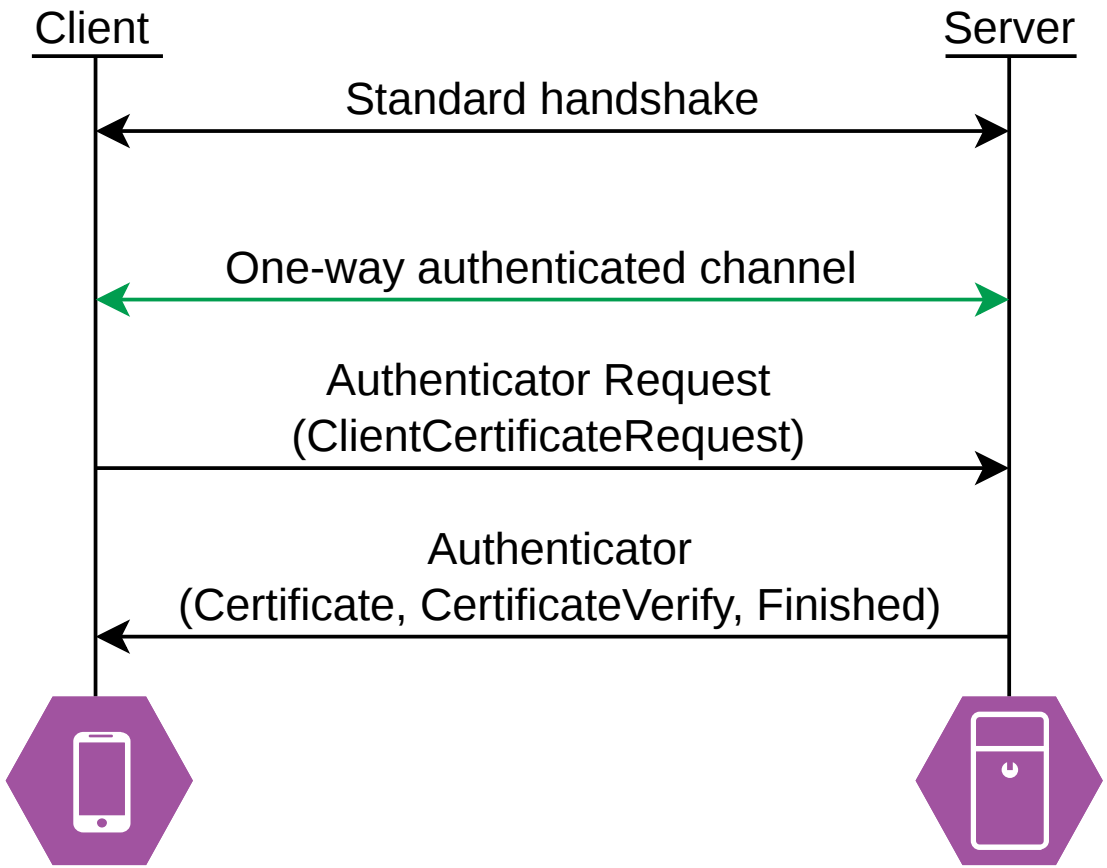
- Real implementors interest with real use cases
  - GA4GH and ELIXIR Europe (Pavel Nikonorov)
  - Edgeless Systems (Markus Rudy)
  - Zama (Ayoub Benaissa)
  - Flashbots (Peg Jones)
- Cocos AI publicly shared migration plan from intra-handshake to post-handshake attestation
- Internet-Drafts using our protocol
  - draft-aylward-aiga-2
  - draft-condrey-rats-pop-appraisal
  - draft-condrey-rats-pop-protocol
  - draft-ayerbe-trip-protocol (editor's version link)
- Internet-Draft with public commitment to use our protocol
  - draft-barney-caam (commitment link)
- Cited in CCC's response to NIST RFI (NIST-2025-0035)
- Invited talk at GlobalPlatform
- Presented in several CCC Attestation SIG meetings, FOSDEM, Linux Plumbers Conference, GA4GH etc.

Outline

1. Community Interest
2. Quick Recap of Protocol
3. Status of Formal Analysis
4. Discussion

Exported Authenticators[1] (RFC 9261)

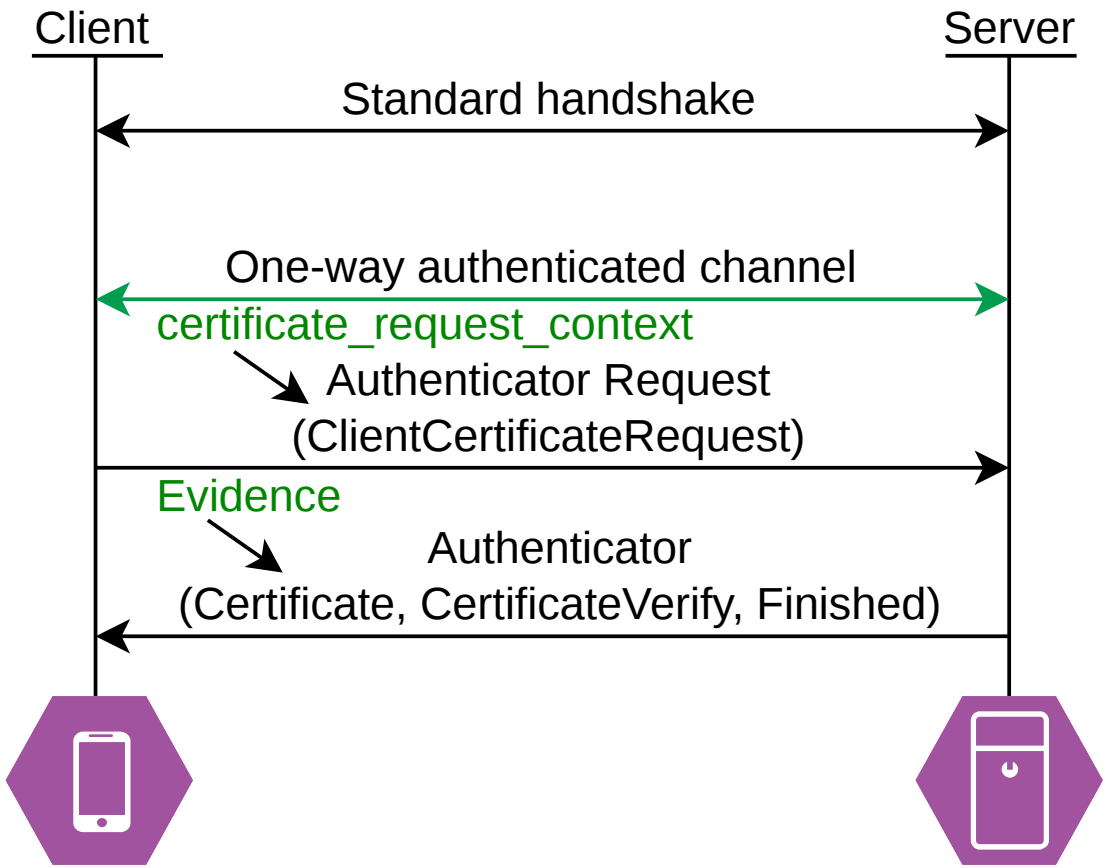
- ClientCertificateRequest: Same as CertificateRequest
- Key for HMAC of Finished using Exported Keying Material (EKM)



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

Post-handshake Attestation[2]

- No change in TLS handshake protocol
- Example: TLS Server as RATS Attester



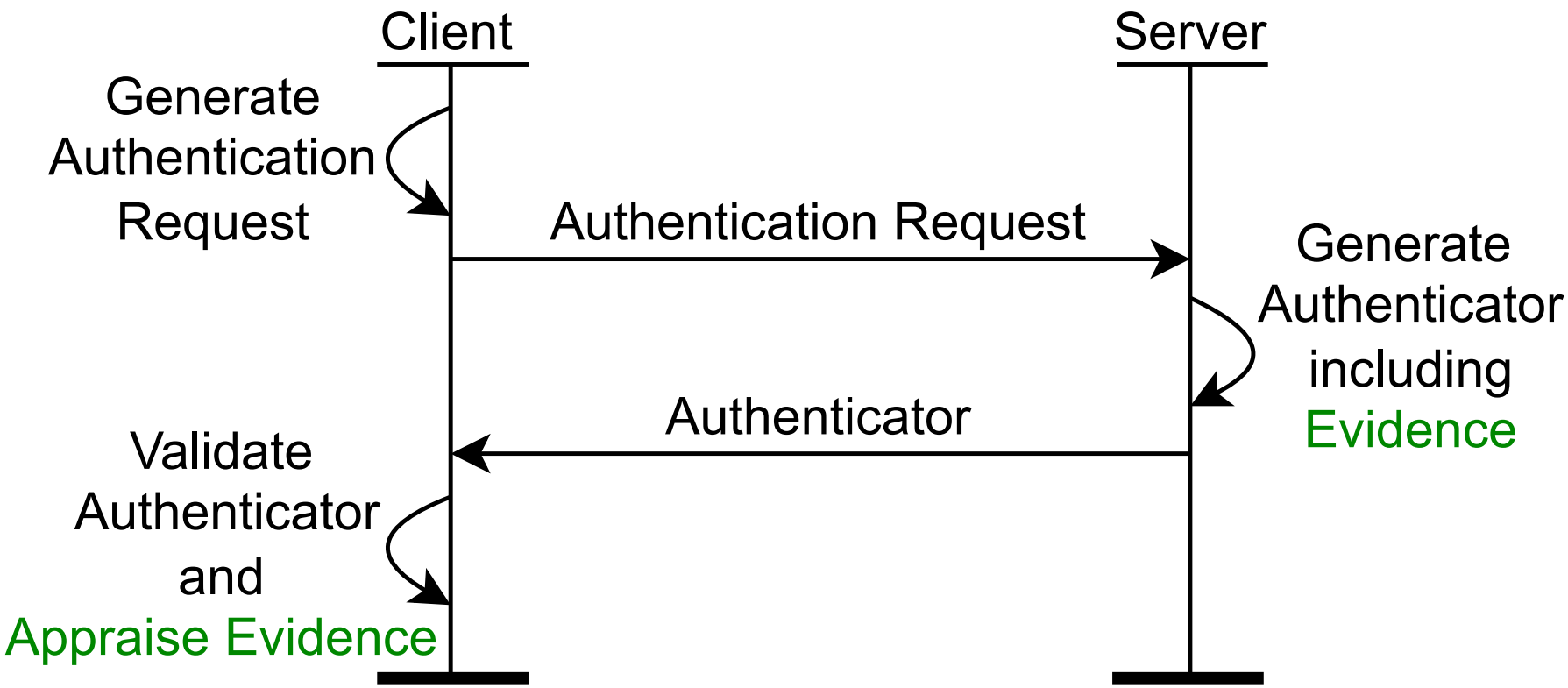
[2]Sardar, Moustafa, and Aura, "Identity Crisis in Confidential Computing: Formal Analysis of Attested TLS", 2026.

Benefits

- Simple, clean, and secure solution
- Orthogonality of TLS and RA
- Well-known and formally verified[3] mechanisms for strong channel bindings
  - What remains is the attestation part
- The draft adds (D)TLS extension and does not alter protocol messages or modify the key schedule.
- Supports background-check and passport model
- Supports re-attestation
- Avoids extra round trips for re-establishment
- Full claims availability
- Supports all use cases (inc. stringent requirements, e.g., GA4GH)

[3] Hoyland, "An Analysis of TLS 1.3 and its use in Composite Protocols", 2018.

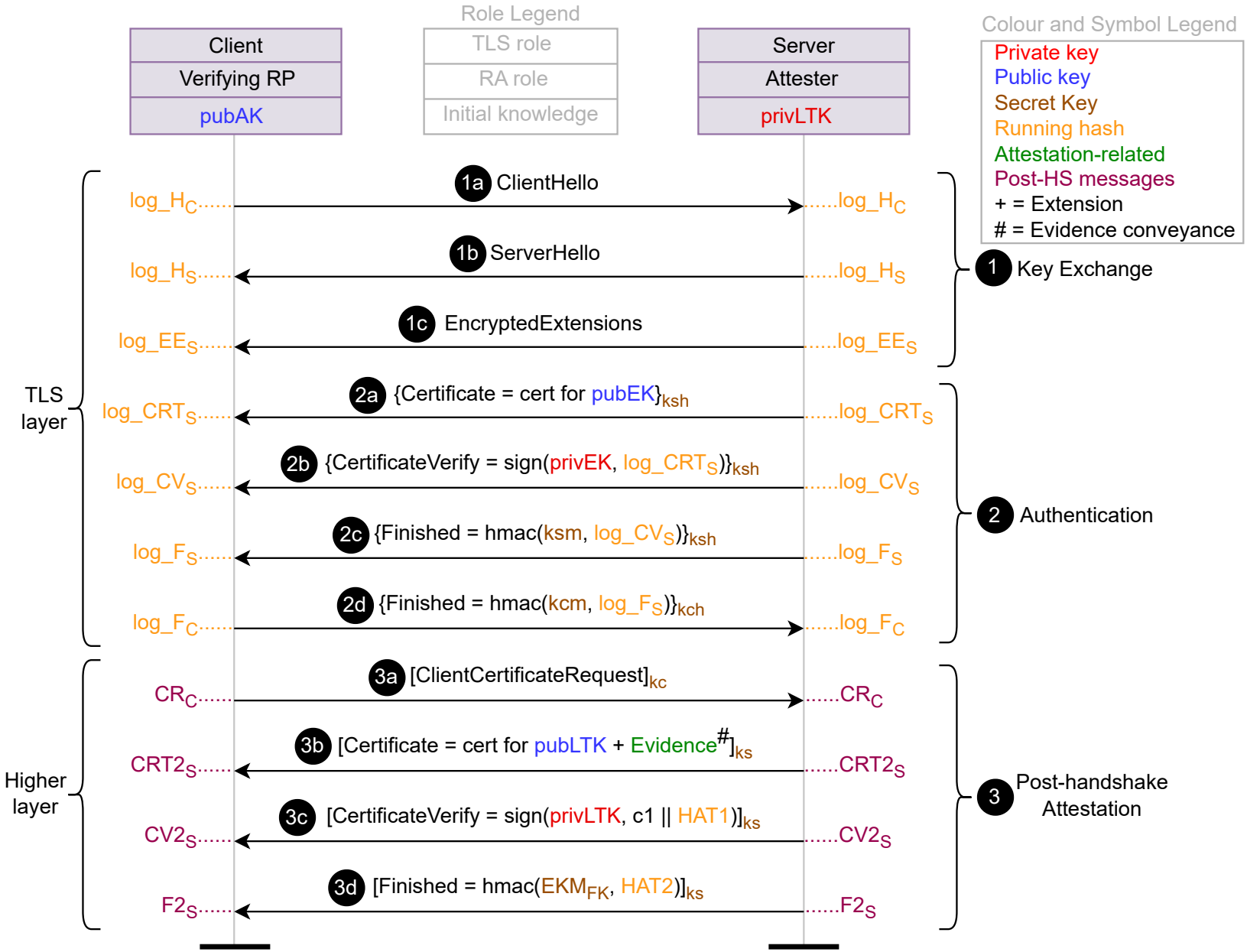
Overview of Post-handshake Flow



Outline

1. Community Interest
2. Quick Recap of Protocol
3. Status of Formal Analysis
4. Discussion

Detailed Model



Authenticator Request

- Let *na* represent the attestation nonce, then:

$$certificate\_request\_context = na \tag{1}$$

Authenticator

- Certificate message with CMW extension for Evidence

$$EKM_{RD} = TLS\text{-}Exporter(\text{"}attestationRD\text{"}, na, L) \tag{2}$$

$$\begin{aligned} rdata &= Hash(pubEK \mid\mid EKM_{RD}) \\ ev &= sign(privAK, rdata||dev\_state) \end{aligned} \tag{3}$$

- CertificateVerify message

$$EKM_{HC} = TLS\text{-}Exporter(\text{"}attestationHC\text{"}, na, L) \tag{4}$$

$$\begin{aligned} AT1 &= EKM_{HC} \mid\mid CR_C \mid\mid CRT2_S \\ HAT1 &= Hash(AT1) \end{aligned} \tag{5}$$

- Finished message

$$EKM_{FK} = TLS\text{-}Exporter(\text{"}attestationFK\text{"}, na, L) \tag{6}$$

$$HAT2 = Hash(AT1 \mid\mid CV2_S) \tag{7}$$

Core Idea for Relay Attack Protection

- Exporters for Certificate, CertificateVerify, and Finished messages bind them all to the connection
- Evidence bound to a fully authenticated endpoint
- Correlation properties in ProVerif

Outline

1. Community Interest
2. Quick Recap of Protocol
3. Status of Formal Analysis
4. Discussion

Next Steps

- Requesting WG adoption call
- Present at CFRG for crypto scrutiny
- Some readings to be done for polishing formal analysis (Thanks to Nick for the pointers).
- Work with Nick for Errata of RFC9261
- Some open issues: welcome any feedback
- Shim layer vs. per-protocol integration
  - CCC Attestation SIG discussions seemed to converge to SHIM layer
- Seek more feedback from implementers

Links to Resources

- Wiki page
  - `github.com/EuroProofNet/ProgramVerification/wiki/AttestedTLS`
- Work-in-progress Implementation
  - `https://github.com/tls-attestation/attestation-exported-authenticators`
- Formal proof of insecurity of pre- and intra-handshake attestation
  - `github.com/CCC-Attestation/formal-spec-id-crisis`
- Attestation in Arm CCA and Intel TDX
  - `github.com/CCC-Attestation/formal-spec-TEE`
- Technical Concepts
- Validation of TLS 1.3 Key Schedule
- General Approach
- Weekly meetings: `github.com/tls-attestation#meetings`

Key References


Hoyland, Jonathan. "An Analysis of TLS 1.3 and its use in Composite Protocols". PhD thesis. Royal Holloway, University of London, 2018. URL: https://pure.royalholloway.ac.uk/en/publications/an-analysis-of-tls-13-and-its-use-in-composite-protocols/.


Sardar, Muhammad Usama, Mariam Moustafa, and Tuomas Aura. "Identity Crisis in Confidential Computing: Formal Analysis of Attested TLS". In: *Proceedings of the 21st ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2026)*. New York, NY, USA: ACM, 2026. URL: https://www.researchgate.net/publication/398839141_Identity_Crisis_in_Confidential_Computing_Formal_Analysis_of_Attested_TLS.


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