Specifications of Attested TLS

Muhammad Usama Sardar[1], Thomas Fossati[2], Hannes Tschofenig[3], Simon Frost[4] and Ned Smith[5]

[1]TU Dresden, Germany

[2]Linaro, Lausanne, Switzerland

[3]University of Applied Sciences Bonn-Rhein-Sieg and Siemens, Germany

[4]Arm, Cambridge, UK

[5]Intel Corporation, USA

November 5, 2024

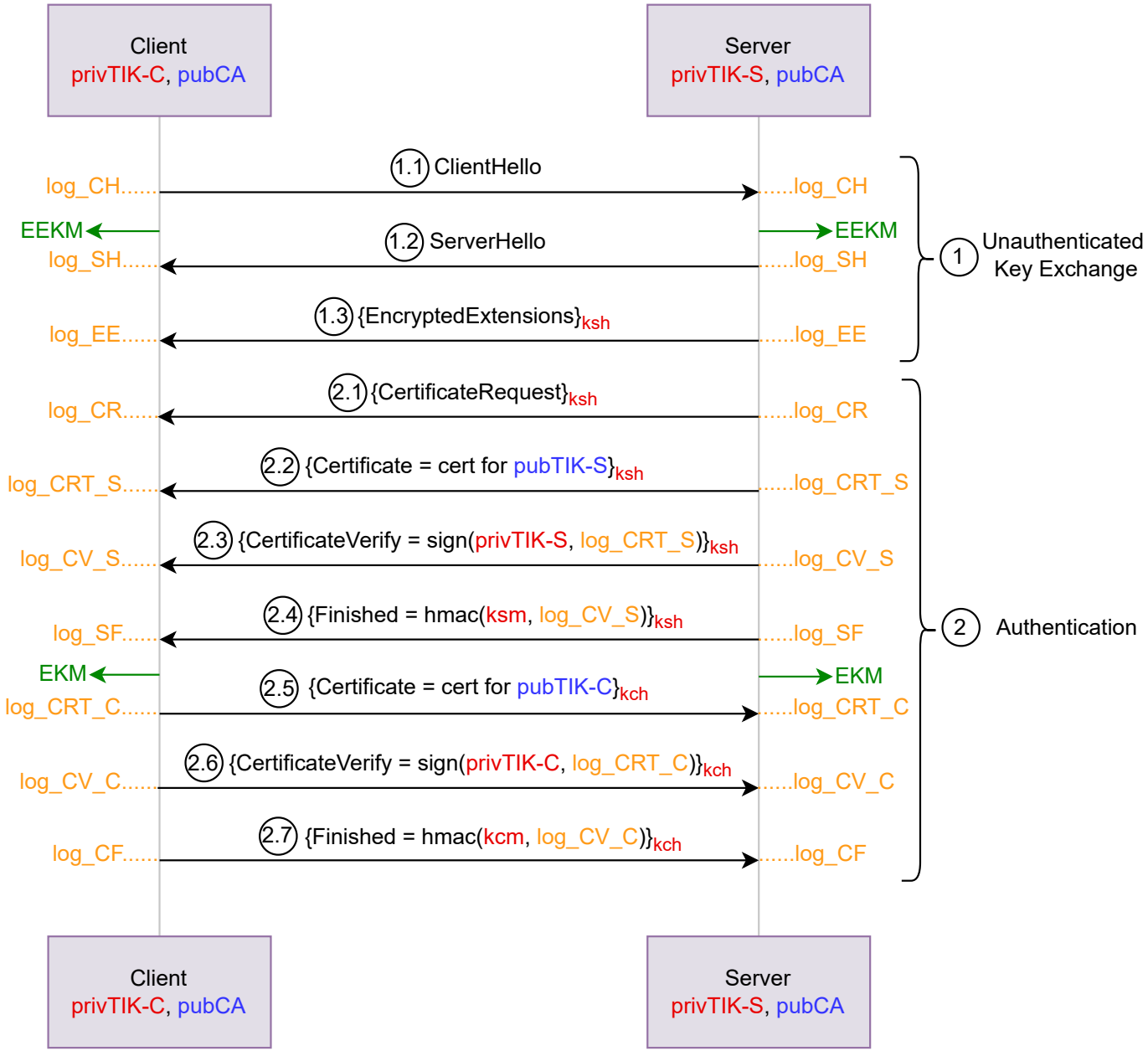
Outline

Relevance to IETF

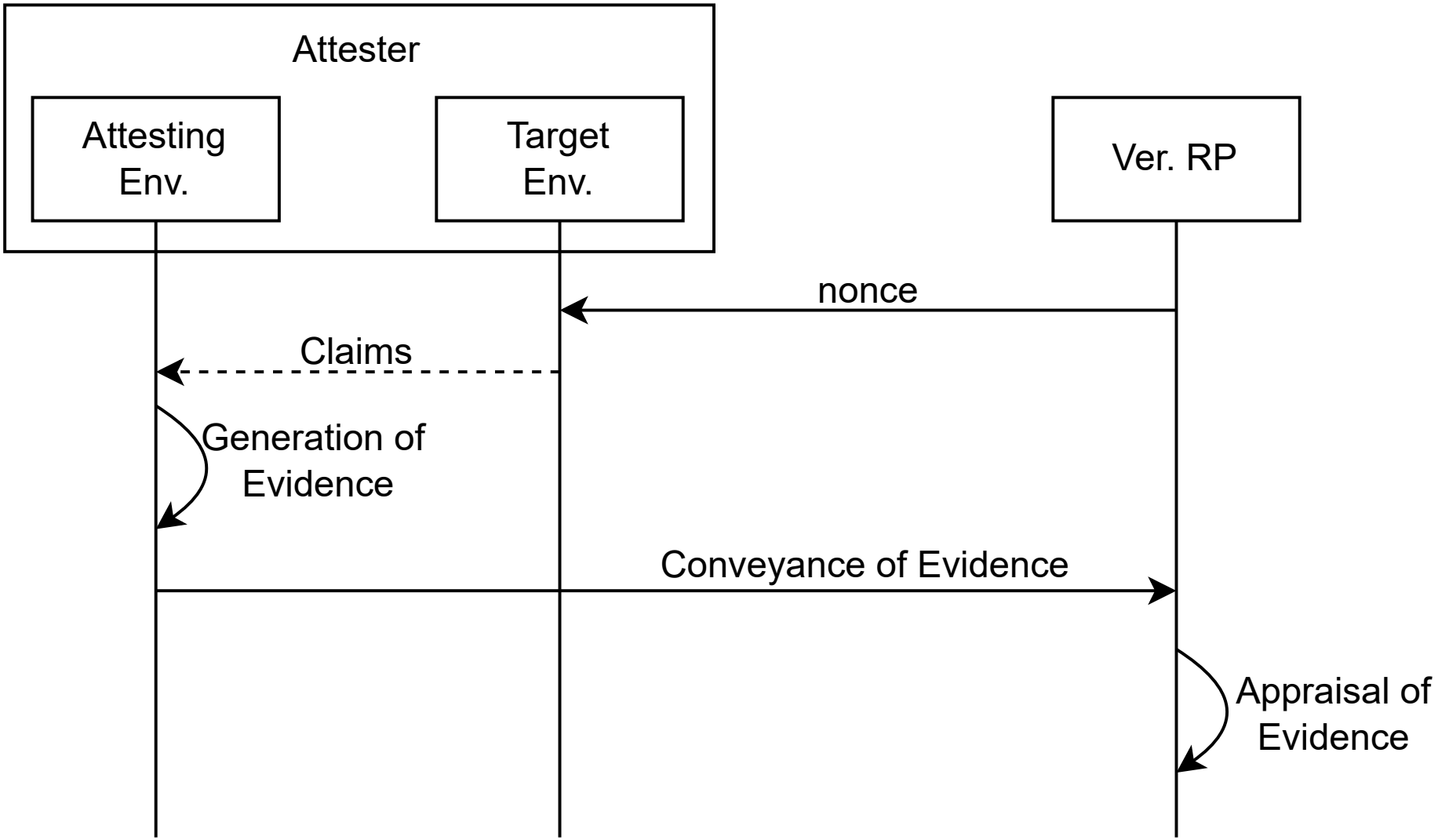
In support of I-D draft-fossati-tls-attestation[1]

[1] Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Network Security (TLS HS with Client AuthN)



Endpoint Security (Remote Attestation)



Attested TLS = Composition of RA and TLS

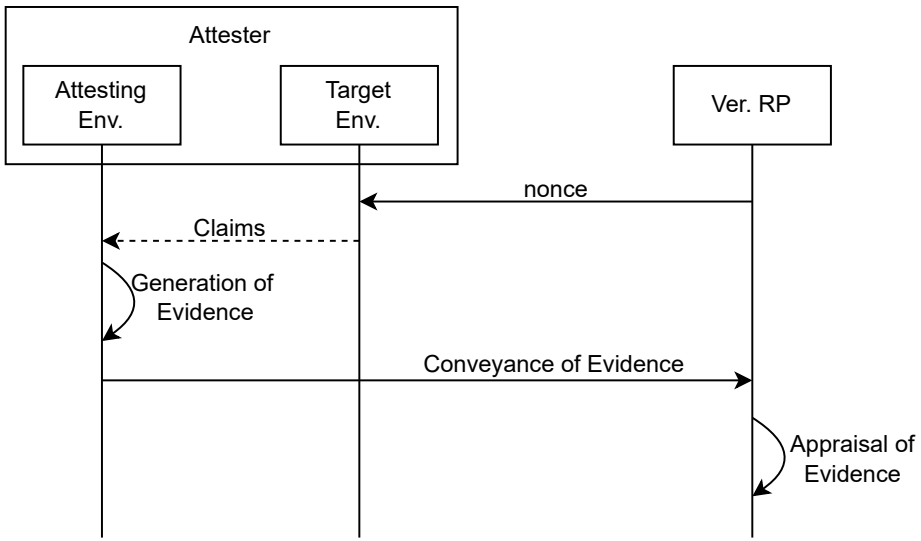


Figure: Remote Attestation

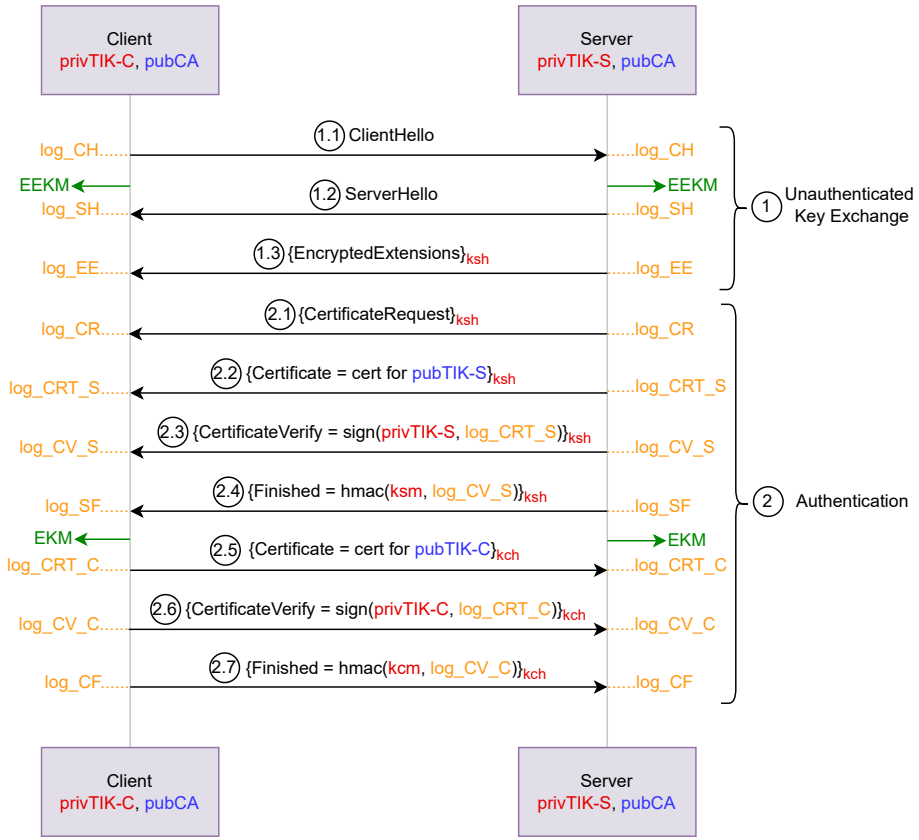
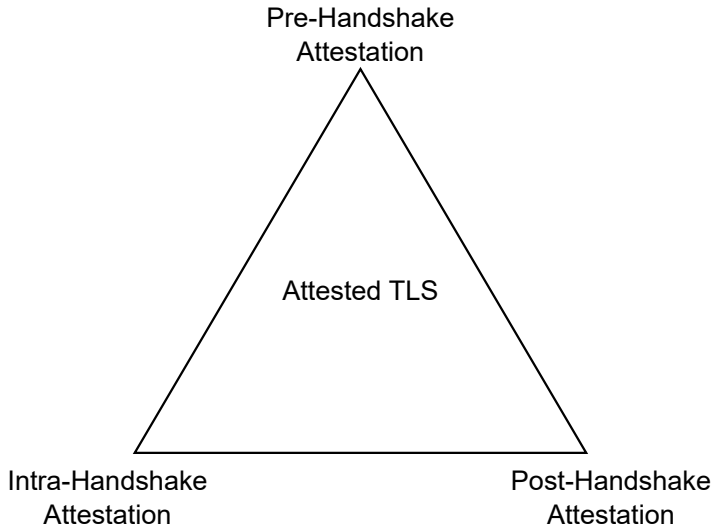


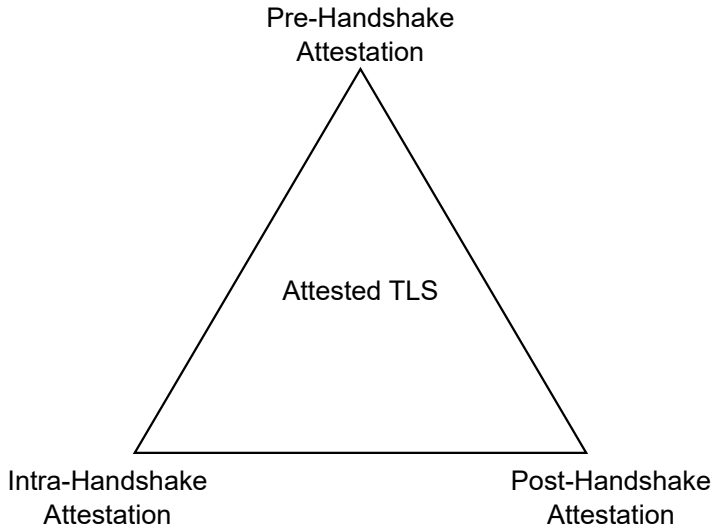
Figure: TLS with Client AuthN

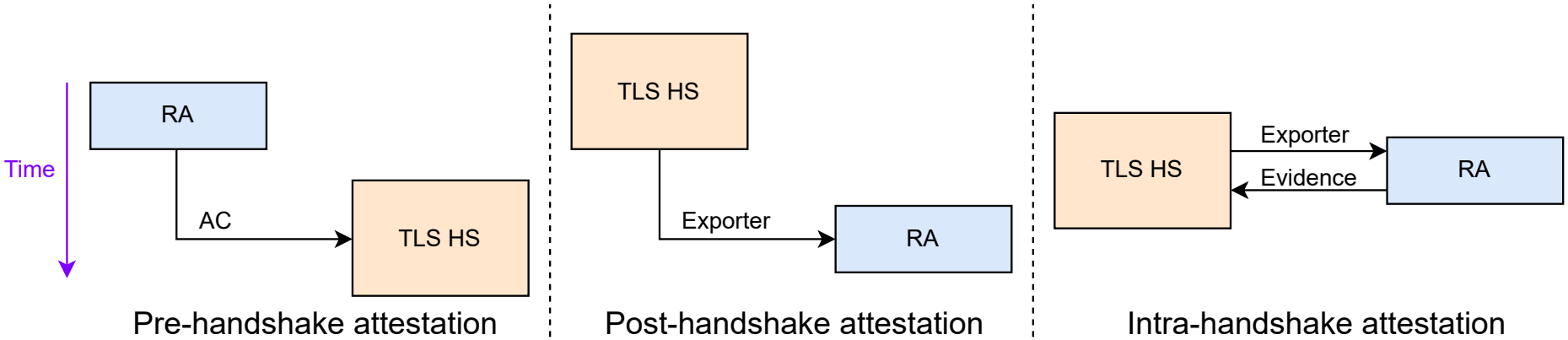
Outline

Design Options

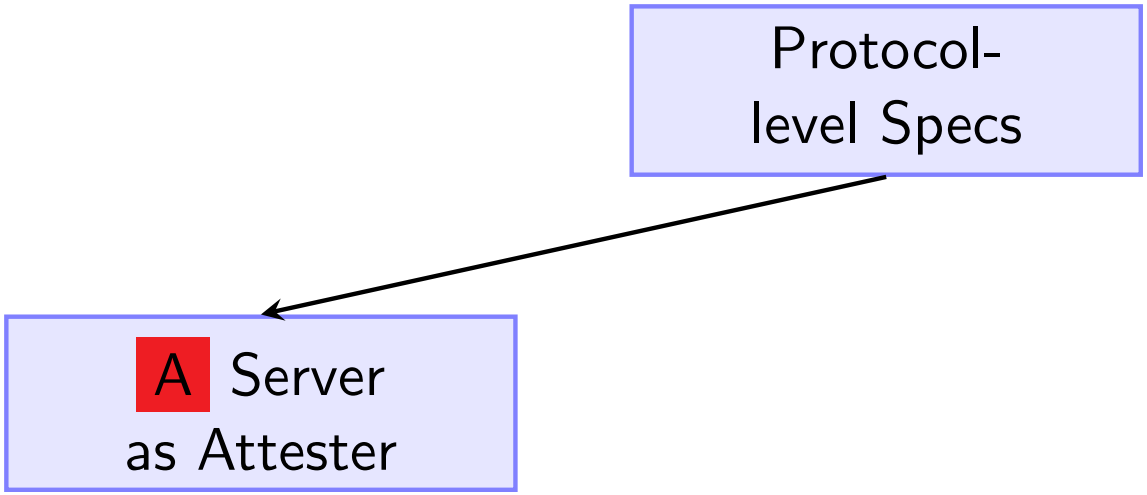


Design Options

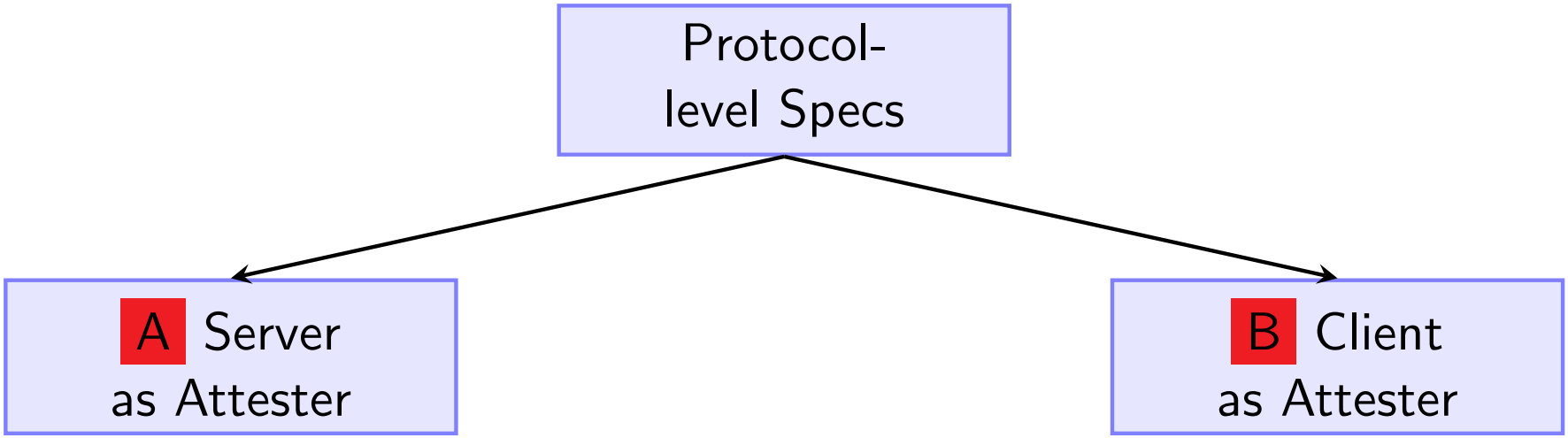




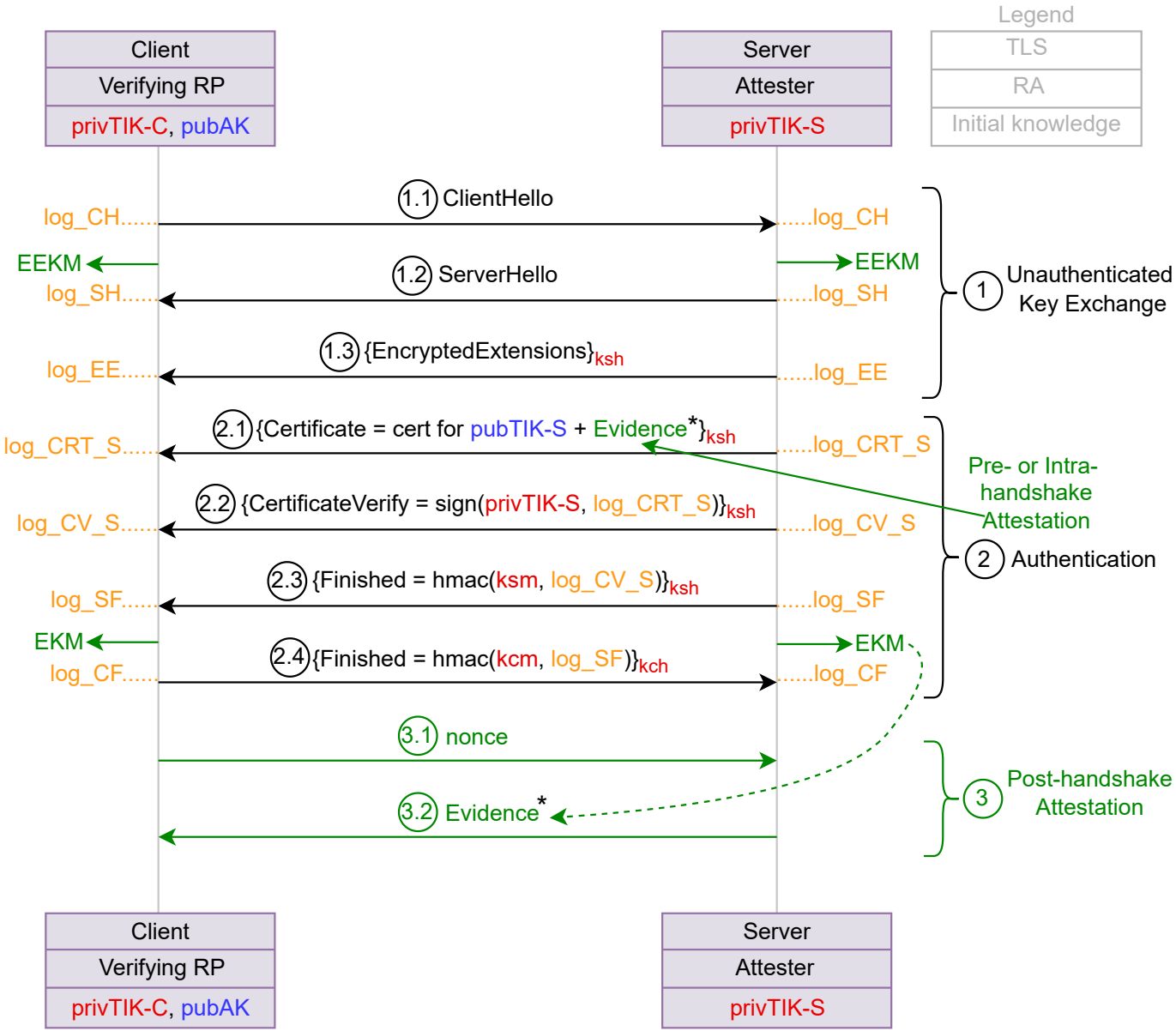
Protocol-level Specs



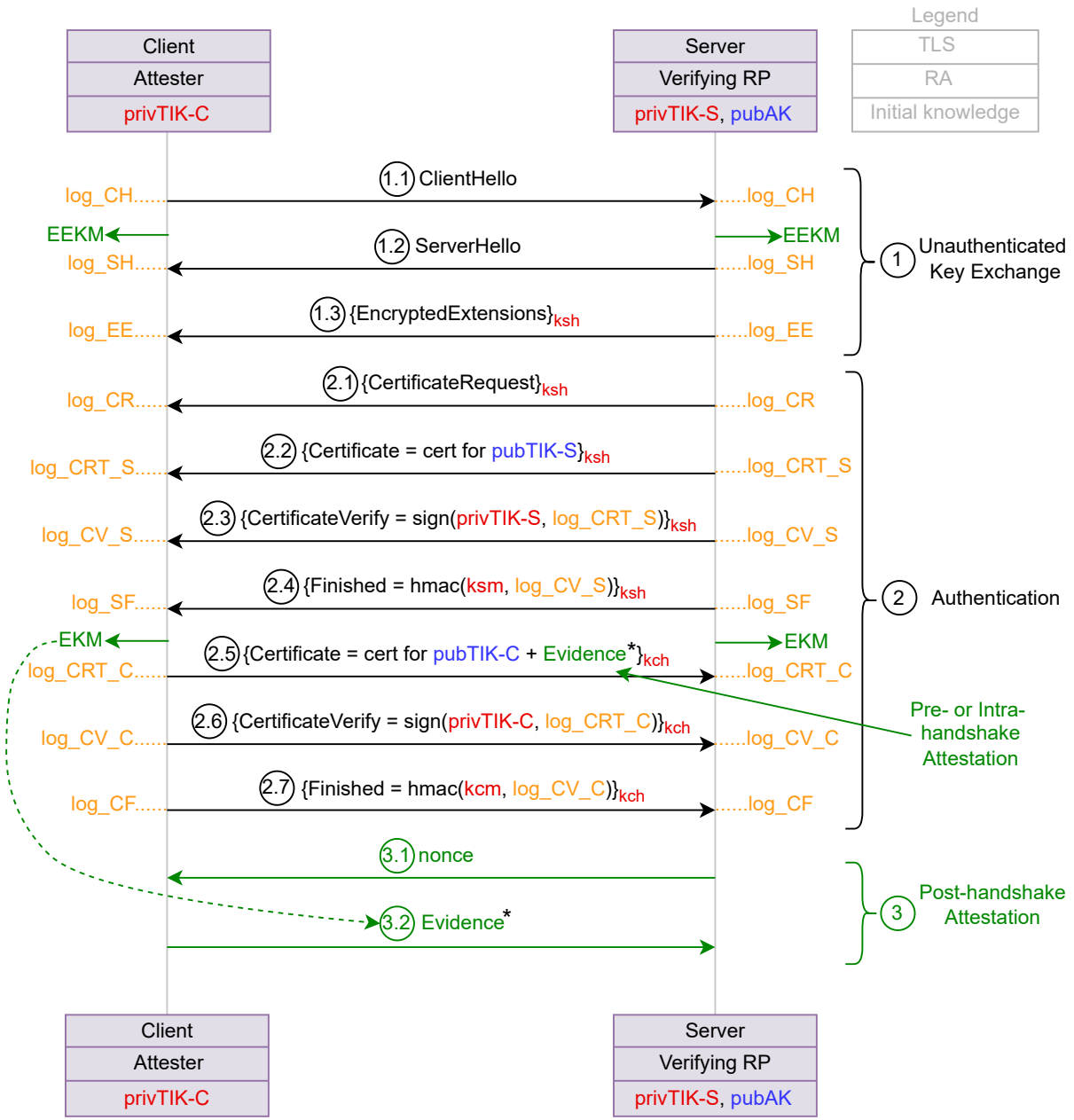
Protocol-level Specs



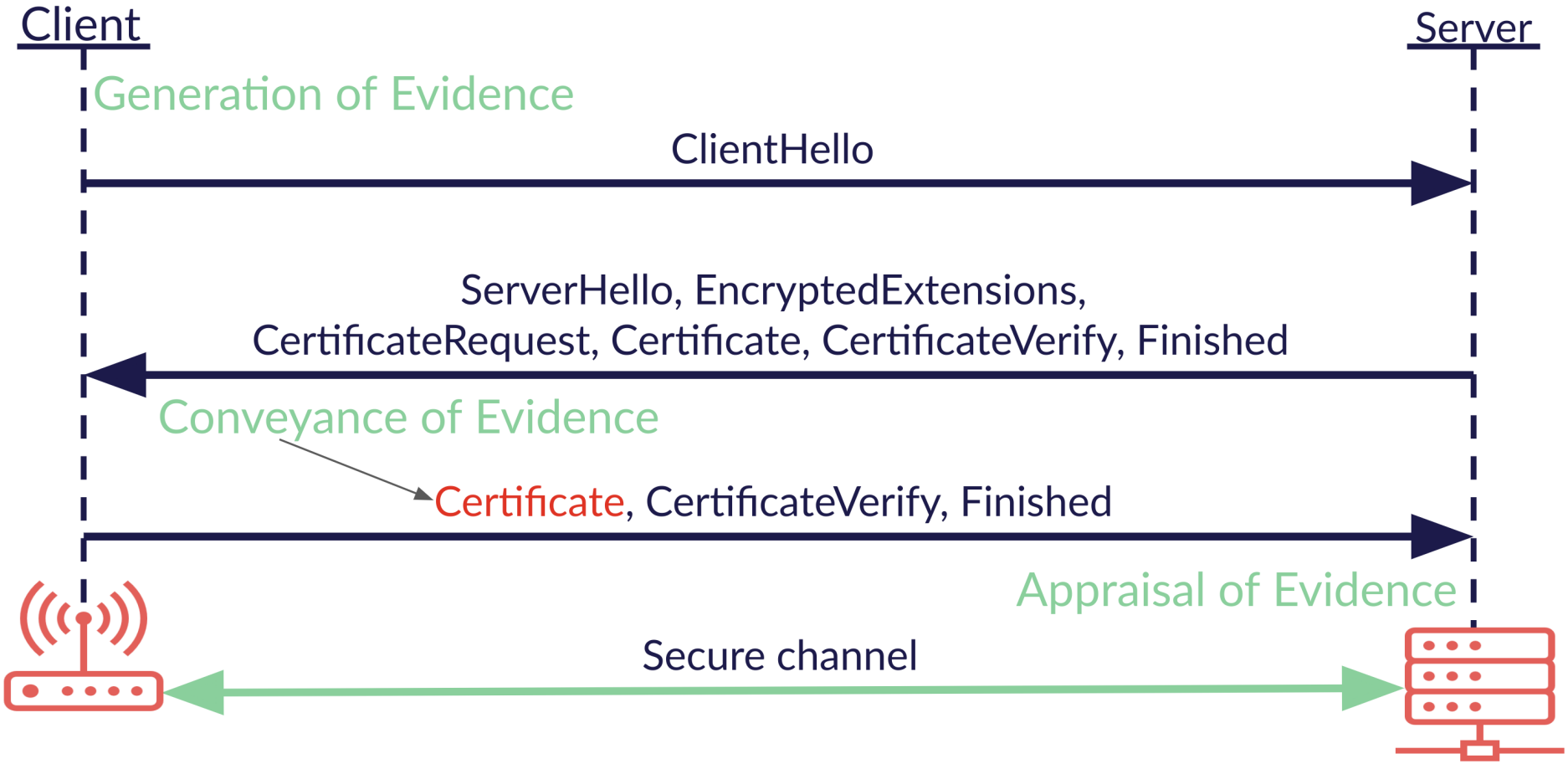
A Generic Protocol (Server as Attester)



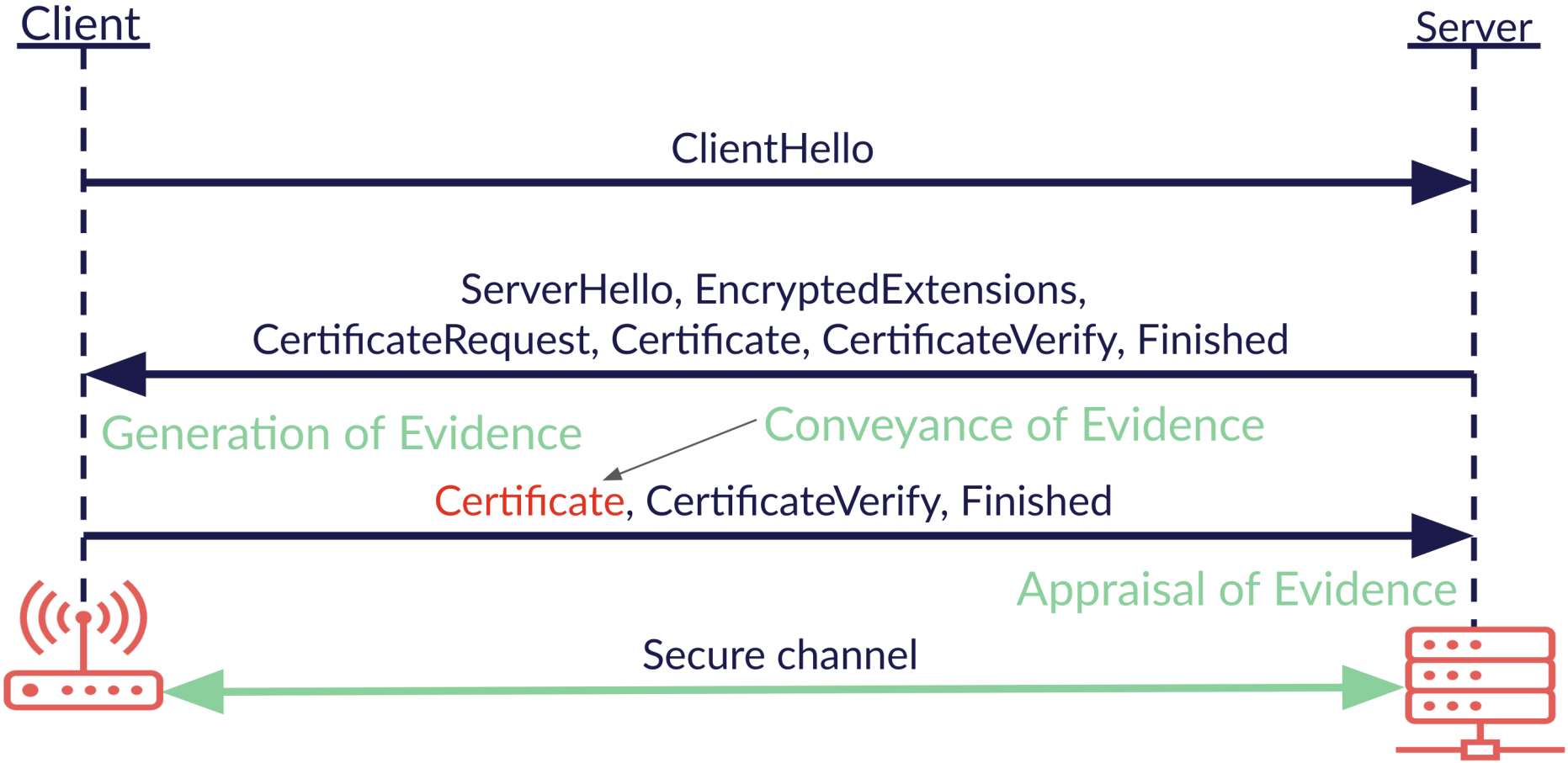
B Generic Protocol (Client as Attester)



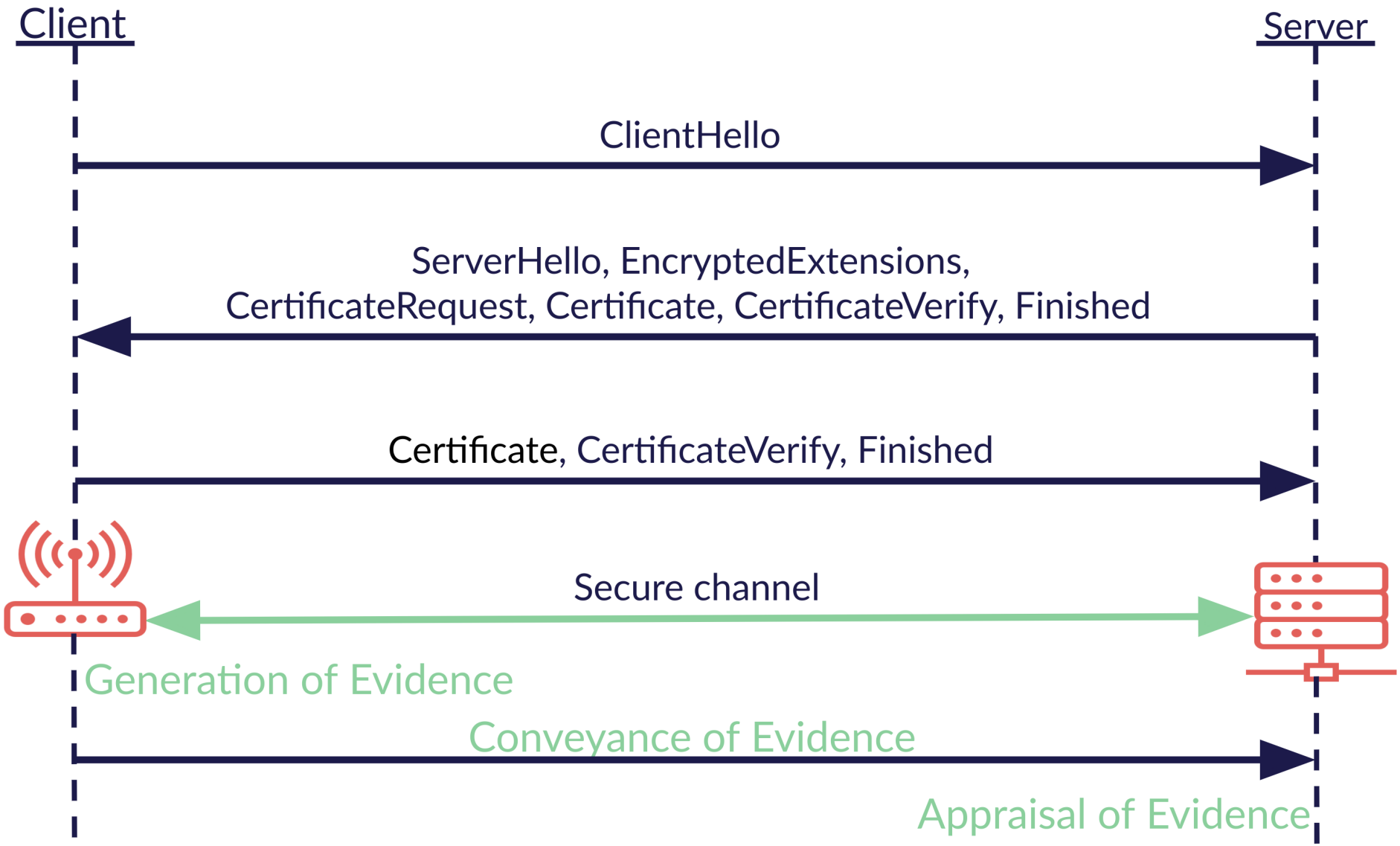
B.1 Pre-HS Attestation (Client as Attester)



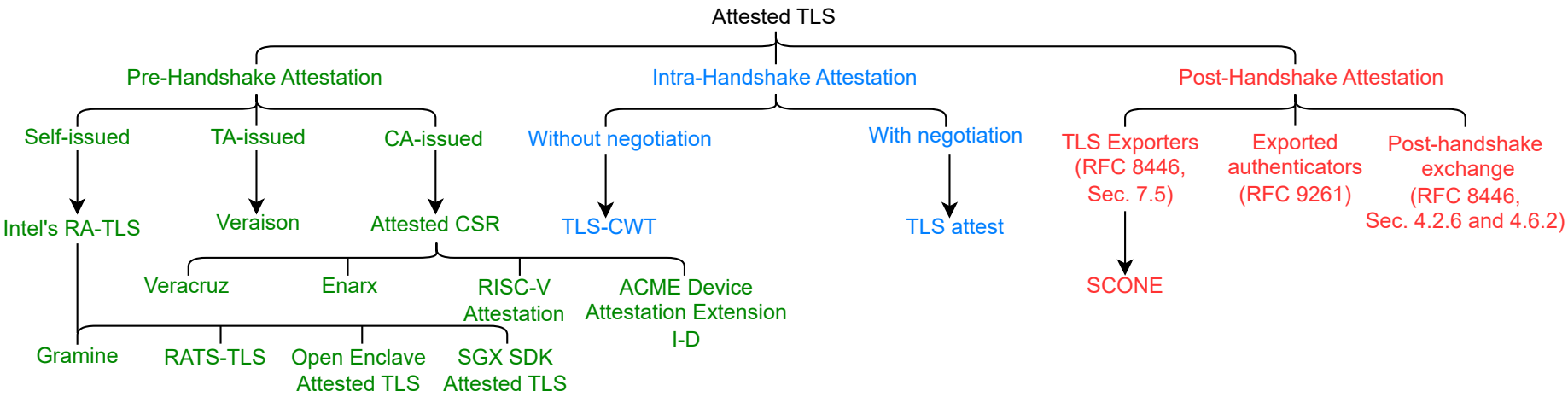
B.2 Intra-HS Attestation (Client as Attester)



B.3 Post-HS Attestation (Client as Attester)



Design Space for Attested TLS



- Discussion: any other fundamental design option?

Specifications in Key Exchange Part (CH, SH)

	RA-TLS[2]	**TLS attest**[3]	**SCONE**[4]
A. Extensions	×	✓	×
B. Attestation nonce	×	✓	×

- Discussion: any other fundamental design option?

[2] T. Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

[3] Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

[4] Arnautov, Trach, Gregor, Thomas Knauth, Martin, Priebe, Lind, Muthukumaran, O'keeffe, Stillwell, et al., "SCONE: Secure Linux Containers with Intel SGX", 2016.

Specifications in Authentication Part

		RA-TLS[5]	**TLS attest**[6]	**SCONE**[7]
A.	Lifetime of key	Short-term	Short-/Long-term	Short-term
B1.	Info in Certificate	Evidence	Evidence	Public key
B2.	Signer	Self-signed	Self-/CA-signed	Self-signed
B3.	Format	X.509	Negotiated	X.509
C.	Extensions	×	✓	×
D.	Exporters	×	✓	✓

- Note: B1 = Certificate msg of TLS (vs. cert)
- Exporter: label, context and key length should be specified. (SCONE uses empty context!)
- Discussion: any other fundamental design option?

[5] T. Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

[6] Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

[7] Arnautov, Trach, Gregor, Thomas Knauth, Martin, Priebe, Lind, Muthukumaran, O'keeffe, Stillwell, et al., "SCONE: Secure Linux Containers with Intel SGX", 2016.

Threat Model

- Scope: TLS mode = non-PSK handshake
- For TLS, similar to Bhargavan et al.[8]
  - Weak hash, e.g., SLOTH (represented by `WeakHash`)
  - Weak DH groups, e.g., Logjam (represented by `WeakDH`)
  - Bad elements within strong DH groups (rep. by `SentBadElement`)
- With and without weak (or compromised) ephemeral key `privTIK`
  - Side-channel attacks
  - Vulnerabilities within TEE
- Without weak (or compromised) attestation key `privAK`

[8] Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

Properties for Attested TLS

- Base security properties of subprotocols

[9] Birkholz, Thaler, Richardson, Smith, and Pan, *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS has well-defined properties, e.g., server authentication

[9] Birkholz, Thaler, Richardson, Smith, and Pan, *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS has well-defined properties, e.g., server authentication
  - RA: RFC9334[9] is super vague about security considerations

[9] Birkholz, Thaler, Richardson, Smith, and Pan, *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS has well-defined properties, e.g., server authentication
  - RA: RFC9334[9] is super vague about security considerations
    - RA: Per-session evidence freshness

[9] Birkholz, Thaler, Richardson, Smith, and Pan, *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS has well-defined properties, e.g., server authentication
  - RA: RFC9334[9] is super vague about security considerations
    - RA: Per-session evidence freshness
    - RA: Integrity of evidence

[9] Birkholz, Thaler, Richardson, Smith, and Pan, *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS has well-defined properties, e.g., server authentication
  - RA: RFC9334[9] is super vague about security considerations
    - RA: Per-session evidence freshness
    - RA: Integrity of evidence
- WiP: Relay attacks

[9] Birkholz, Thaler, Richardson, Smith, and Pan, *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS has well-defined properties, e.g., server authentication
  - RA: RFC9334[9] is super vague about security considerations
    - RA: Per-session evidence freshness
    - RA: Integrity of evidence
- WiP: Relay attacks
- WiP: Channel binding properties (Credits: Cedric Fournet)

[9] Birkholz, Thaler, Richardson, Smith, and Pan, *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS has well-defined properties, e.g., server authentication
  - RA: RFC9334[9] is super vague about security considerations
    - RA: Per-session evidence freshness
    - RA: Integrity of evidence
- WiP: Relay attacks
- WiP: Channel binding properties (Credits: Cedric Fournet)
  - If connection is established, client and server agree on attestation (evidence).

[9] Birkholz, Thaler, Richardson, Smith, and Pan, *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS has well-defined properties, e.g., server authentication
  - RA: RFC9334[9] is super vague about security considerations
    - RA: Per-session evidence freshness
    - RA: Integrity of evidence
- WiP: Relay attacks
- WiP: Channel binding properties (Credits: Cedric Fournet)
  - If connection is established, client and server agree on attestation (evidence).
  - If RA appraisal succeeds, client and server agree on all connection parameters (TLS transcript).

[9] Birkholz, Thaler, Richardson, Smith, and Pan, *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS has well-defined properties, e.g., server authentication
  - RA: RFC9334[9] is super vague about security considerations
    - RA: Per-session evidence freshness
    - RA: Integrity of evidence
- WiP: Relay attacks
- WiP: Channel binding properties (Credits: Cedric Fournet)
  - If connection is established, client and server agree on attestation (evidence).
  - If RA appraisal succeeds, client and server agree on all connection parameters (TLS transcript).
- Discussion: any other property?

[9] Birkholz, Thaler, Richardson, Smith, and Pan, *Remote ATtestation procedureS (RATS) Architecture*, 2023.

(Typical) Comparison/Tradeoffs

Property	Pre-handshake	Intra-handshake	Post-handshake
Modification	TA/CA	TLS	Application
Replay protection	×	✓	Possible
Impact on connection establishment latency	Medium ($t_{hs} + t_a$)	High ($t_{hs} + t_g + t_a$)	Low (t_{hs})
Effective connection establishment latency	Low	Low	High ($\geqslant$0.5RTT)

- t_{hs} = Time for TLS handshake (without attestation)
- t_g = Time for generation of evidence
- t_a = Time for appraisal of evidence
- WiP
  - Usability/Ease of use
  - Complexity of implementation/formal verification
- Discussion: any other property?

Outline

Summary

Underspecified = NOT trustworthy!

Key References

Arnautov, Sergei, Bohdan Trach, Franz Gregor, Thomas Knauth, Andre Martin, Christian Priebe, Joshua Lind, Divya Muthukumaran, Dan O'keeffe, Mark L Stillwell, et al. "SCONE: Secure Linux Containers with Intel SGX". In: *USENIX Symposium on Operating Systems Design and Implementation*. 2016, pp. 689–703. URL: https://www.usenix.org/conference/osdi16/technical-sessions/presentation/arnautov.

Bhargavan, Karthikeyan, Bruno Blanchet, and Nadim Kobeissi. "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate". In: *2017 IEEE Symposium on Security and Privacy (SP)*. 2017, pp. 483–502. DOI: 10.1109/SP.2017.26.

Birkholz, Henk, Dave Thaler, Michael Richardson, Ned Smith, and Wei Pan. *Remote ATtestation procedureS (RATS) Architecture*. RFC 9334. Jan. 2023. DOI: 10.17487/RFC9334. URL: https://www.rfc-editor.org/info/rfc9334.

Knauth, T., M. Steiner, S. Chakrabarti, L. Lei, C. Xing, and M. Vij. *Integrating Remote Attestation with Transport Layer Security*. Tech. rep. Intel Labs, 2018. URL: https://arxiv.org/abs/1801.05863.

Tschofenig, Hannes, Yaron Sheffer, Paul Howard, Ionuț Mihalcea, Yogesh Deshpande, Arto Niemi, and Thomas Fossati. *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*. Internet-Draft draft-fossati-tls-attestation-08. Work in Progress. Internet Engineering Task Force, Oct. 2024. 34 pp. URL: https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/08/.

ACK

- Cedric Fournet (Microsoft)
- Ionut Mihalcea (Arm)
- Yaron Sheffer (Intuit)
- Thore Sommer (Kiel University)