Security Considerations of Attested TLS

Muhammad Usama Sardar[1]
Based on joint work with 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 8, 2024

Attested TLS = Composition of RA and TLS

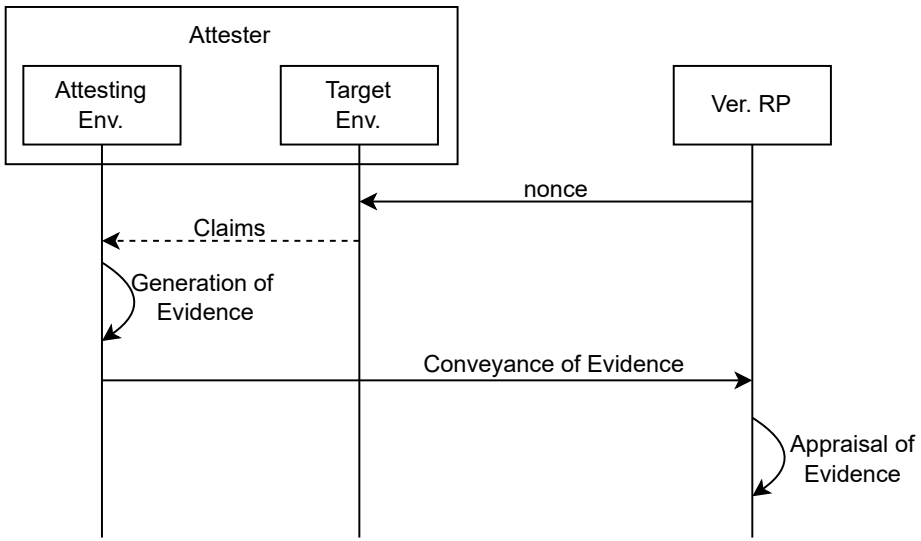


Figure: Remote Attestation

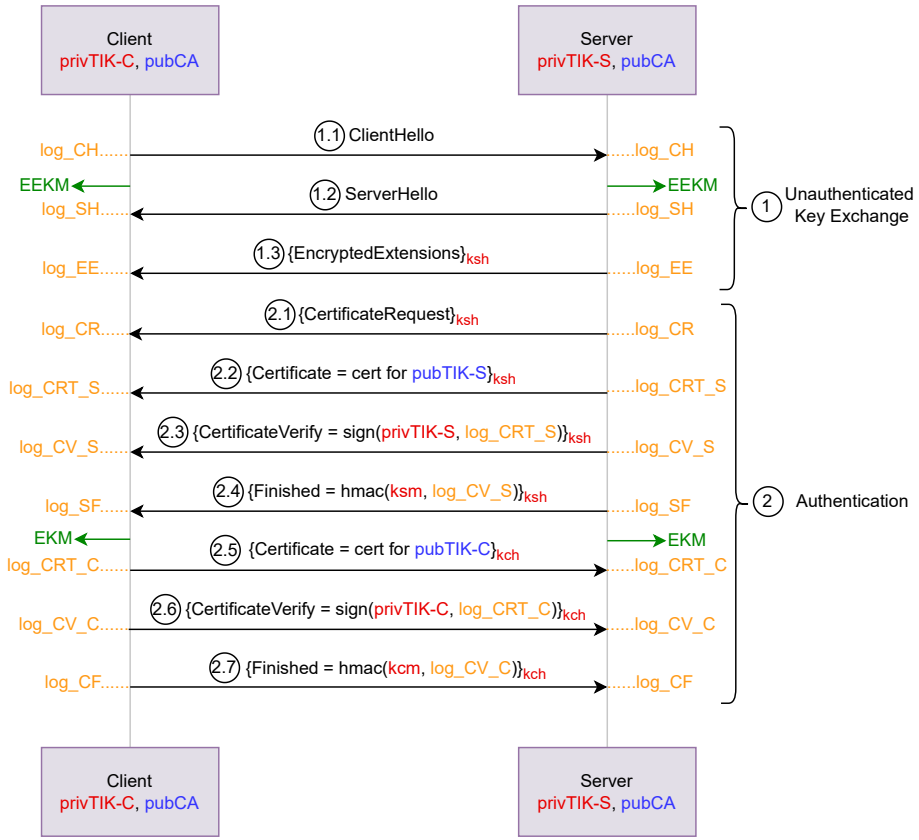
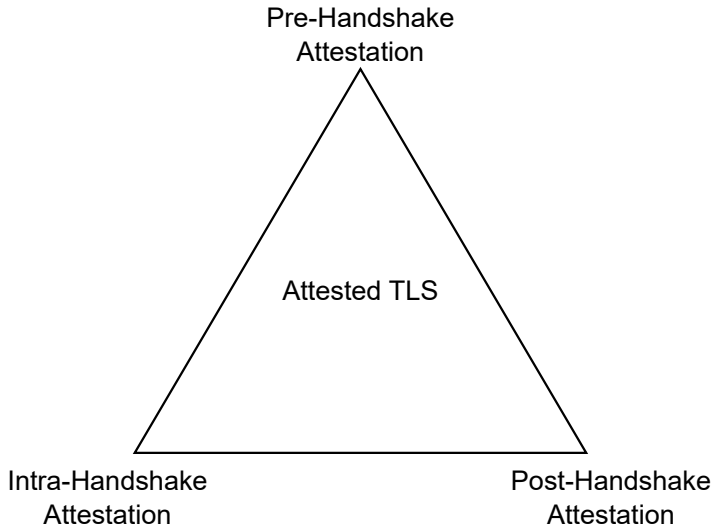
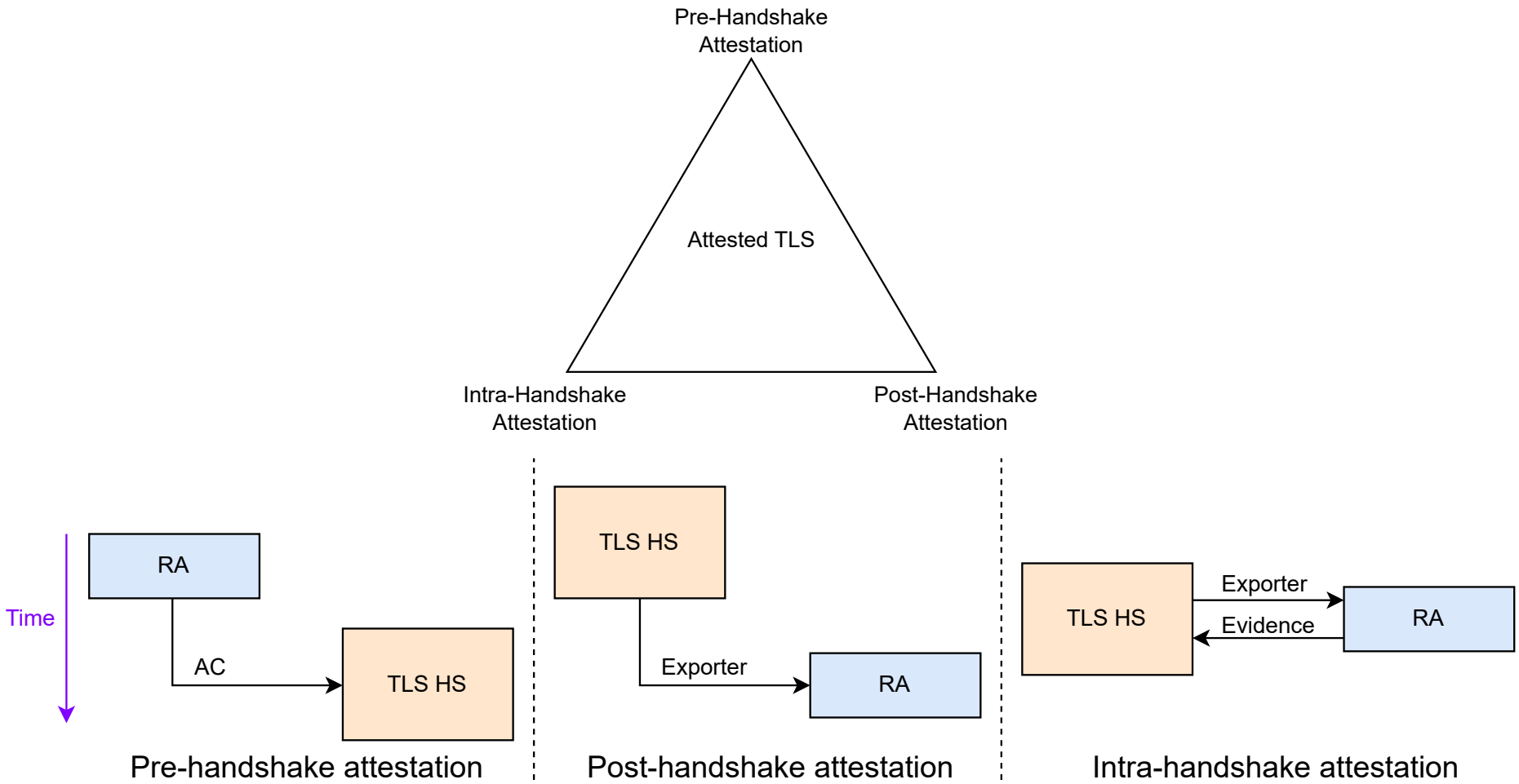


Figure: TLS with Client AuthN

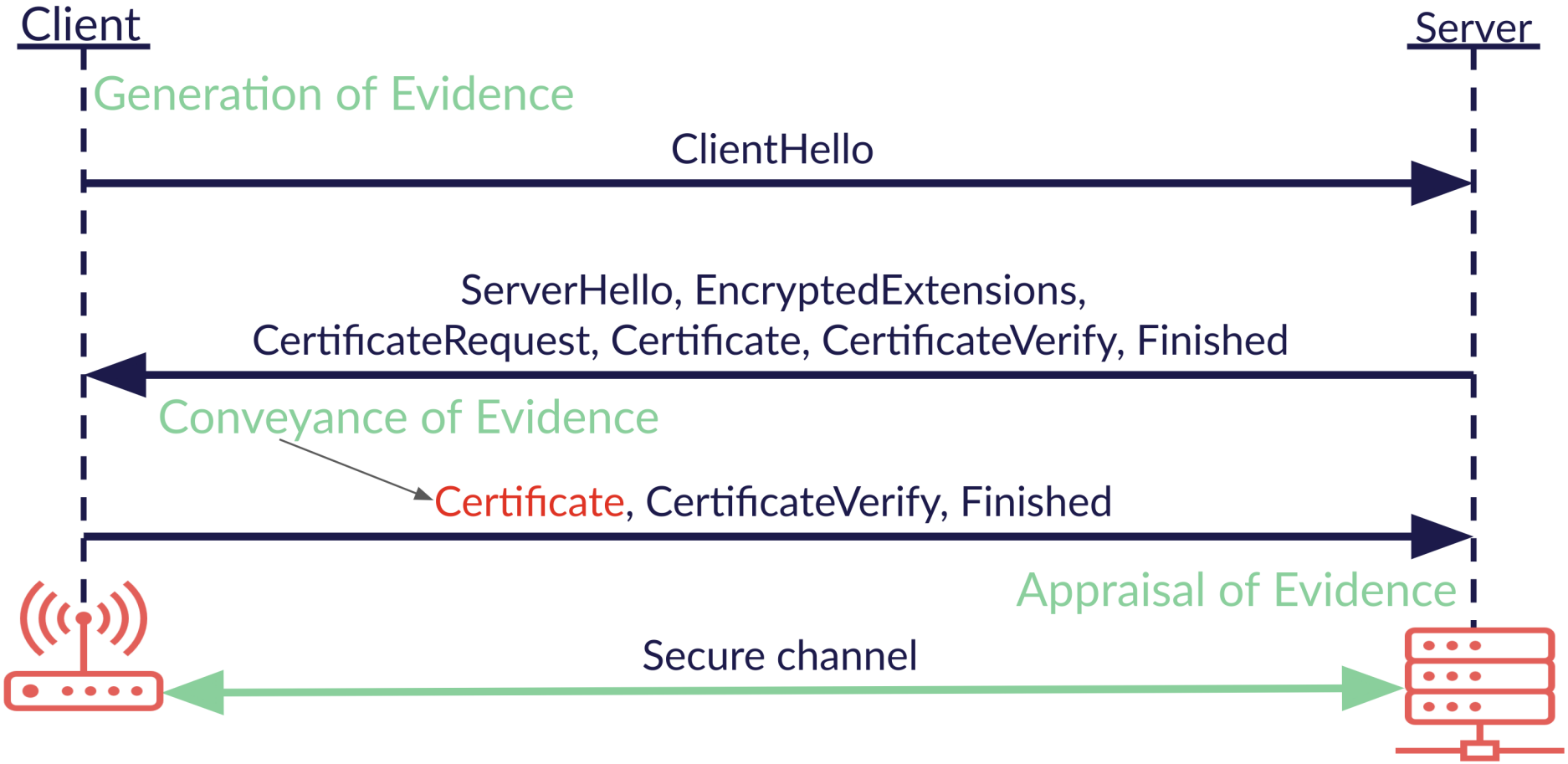
Design Options



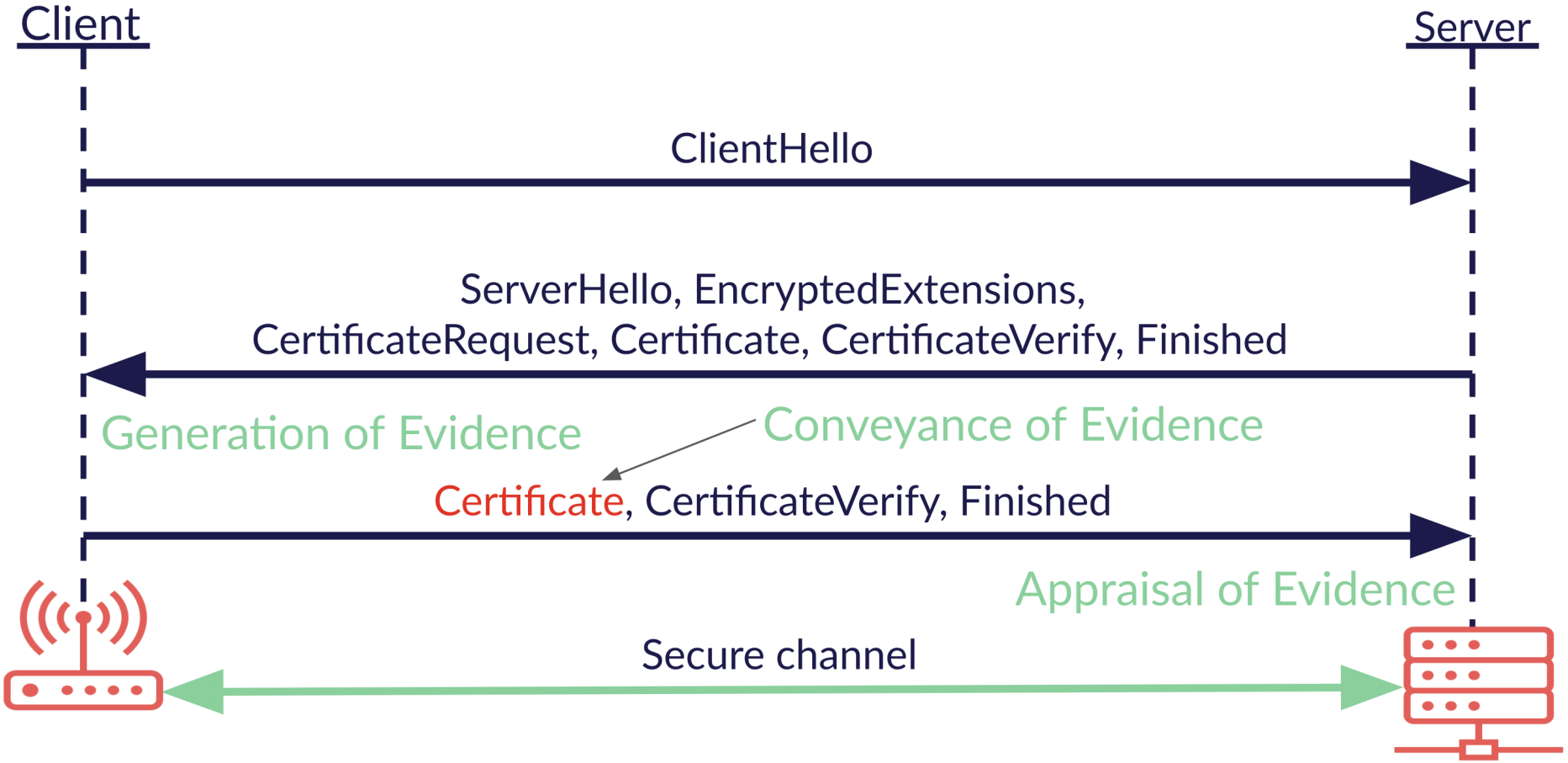
Design Options



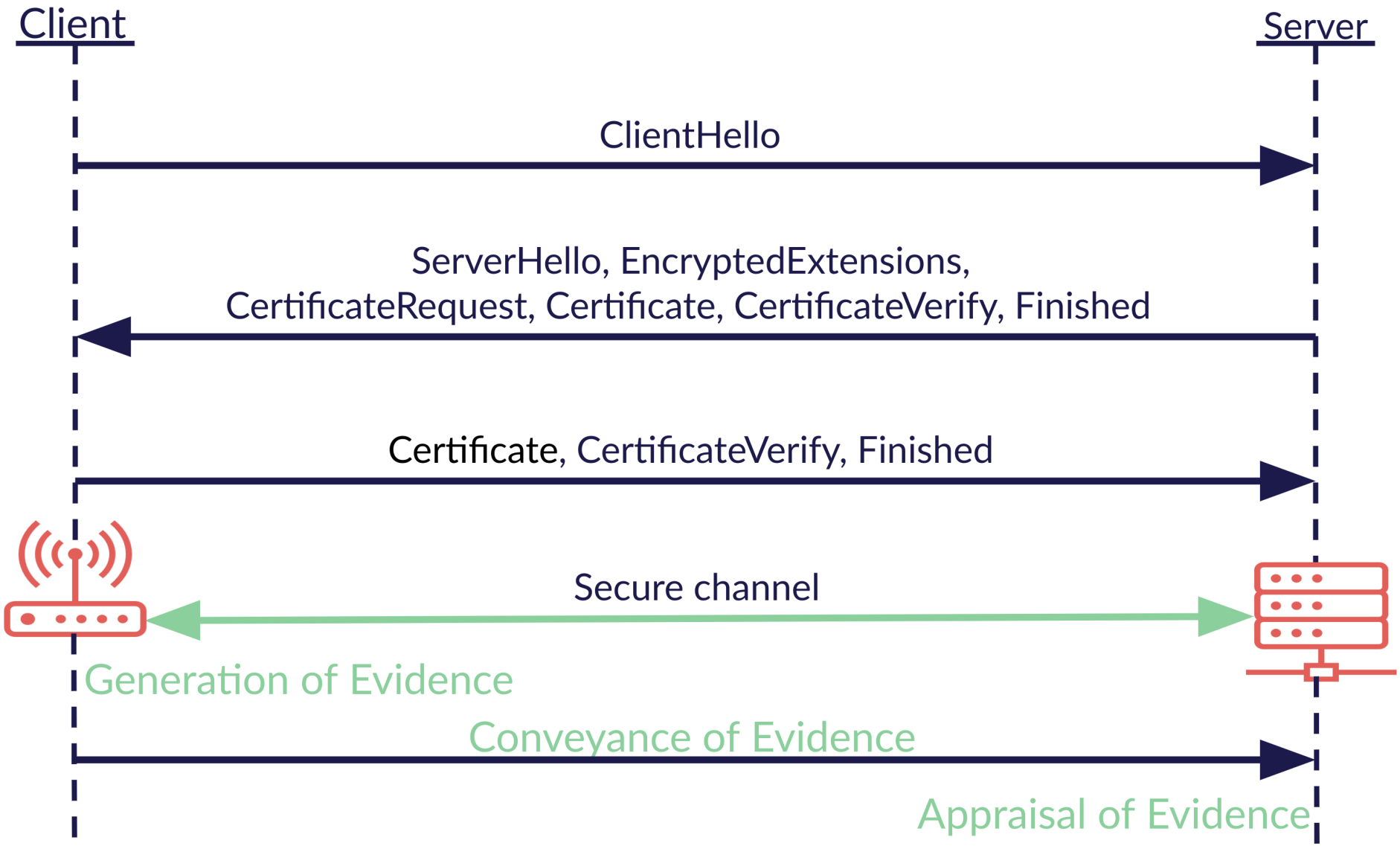
1 Pre-HS Attestation (Client as Attester)



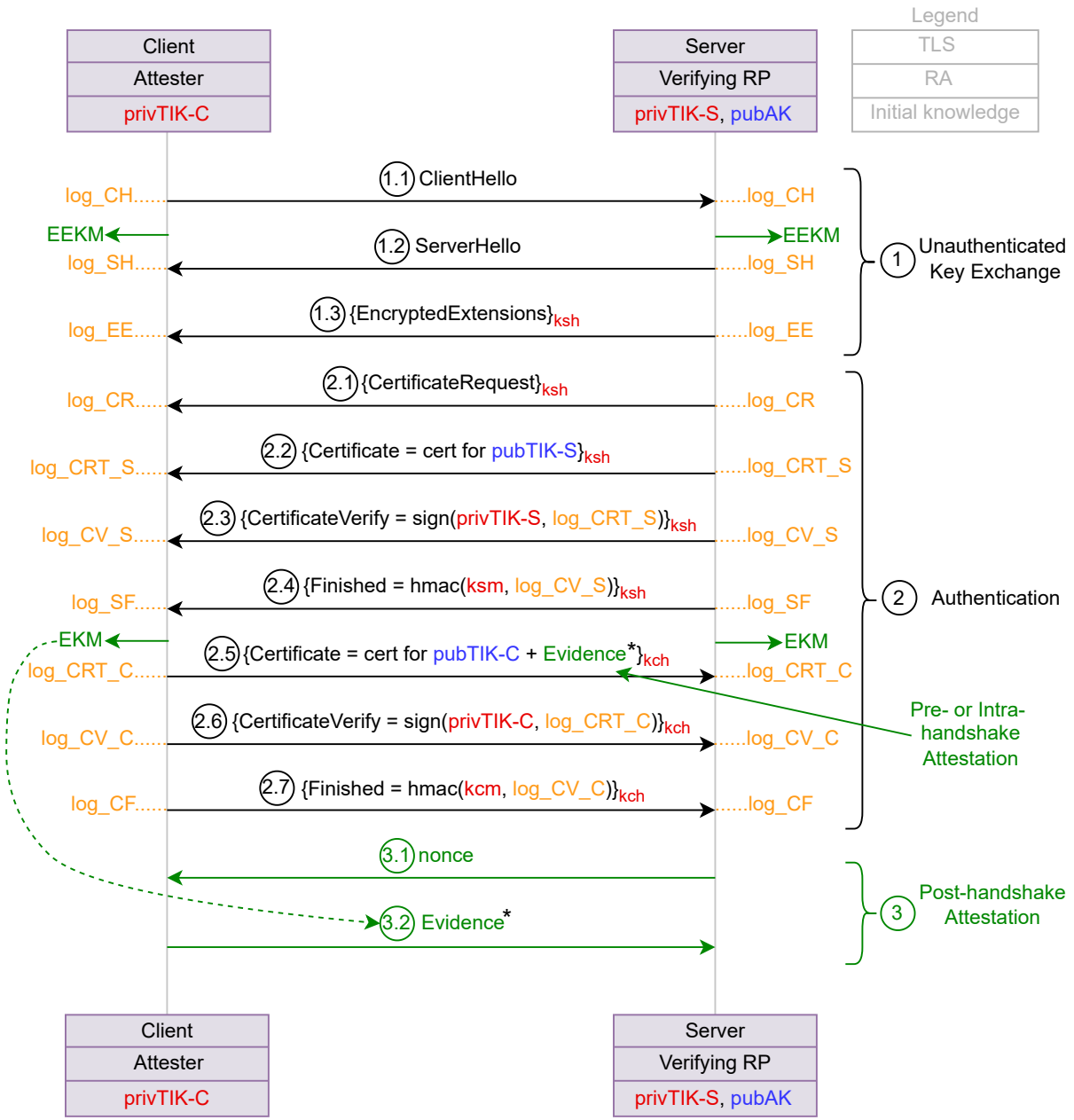
2 Intra-HS Attestation (Client as Attester)



3 Post-HS Attestation (Client as Attester)



Generic Protocol (Client as Attester)



Properties for Attested TLS

- Base security properties of subprotocols

[1] Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, 2018.

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

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

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS[1] has well-defined properties, e.g., server authentication

[1] Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, 2018.

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

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

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS[1] has well-defined properties, e.g., server authentication
  - RA: RFC9334[2] is super vague about security considerations

[1] Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, 2018.

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

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

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS[1] has well-defined properties, e.g., server authentication
  - RA: RFC9334[2] is super vague about security considerations
    - Per-session evidence freshness[3] (vs. protocol freshness)

[1] Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, 2018.

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

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

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS[1] has well-defined properties, e.g., server authentication
  - RA: RFC9334[2] is super vague about security considerations
    - Per-session evidence freshness[3] (vs. protocol freshness)
    - Integrity of evidence

[1] Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, 2018.

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

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

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS[1] has well-defined properties, e.g., server authentication
  - RA: RFC9334[2] is super vague about security considerations
    - Per-session evidence freshness[3] (vs. protocol freshness)
    - Integrity of evidence
    - Relay attacks

[1] Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, 2018.

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

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

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS[1] has well-defined properties, e.g., server authentication
  - RA: RFC9334[2] is super vague about security considerations
    - Per-session evidence freshness[3] (vs. protocol freshness)
    - Integrity of evidence
    - Relay attacks
- Channel binding properties (Credits: Cedric Fournet)

[1] Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, 2018.

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

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

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS[1] has well-defined properties, e.g., server authentication
  - RA: RFC9334[2] is super vague about security considerations
    - Per-session evidence freshness[3] (vs. protocol freshness)
    - Integrity of evidence
    - Relay attacks
- Channel binding properties (Credits: Cedric Fournet)
  - If connection is established, client and server agree on attestation state (evidence or attestation result).

[1] Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, 2018.

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

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

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS[1] has well-defined properties, e.g., server authentication
  - RA: RFC9334[2] is super vague about security considerations
    - Per-session evidence freshness[3] (vs. protocol freshness)
    - Integrity of evidence
    - Relay attacks
- Channel binding properties (Credits: Cedric Fournet)
  - If connection is established, client and server agree on attestation state (evidence or attestation result).
  - If RA appraisal succeeds, client and server agree on current transcript hash.

[1] Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, 2018.

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

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

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS[1] has well-defined properties, e.g., server authentication
  - RA: RFC9334[2] is super vague about security considerations
    - Per-session evidence freshness[3] (vs. protocol freshness)
    - Integrity of evidence
    - Relay attacks
- Channel binding properties (Credits: Cedric Fournet)
  - If connection is established, client and server agree on attestation state (evidence or attestation result).
  - If RA appraisal succeeds, client and server agree on current transcript hash.
- Binding of attestation key and platform

[1] Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, 2018.

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

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

Properties for Attested TLS

- Base security properties of subprotocols
  - TLS[1] has well-defined properties, e.g., server authentication
  - RA: RFC9334[2] is super vague about security considerations
    - Per-session evidence freshness[3] (vs. protocol freshness)
    - Integrity of evidence
    - Relay attacks
- Channel binding properties (Credits: Cedric Fournet)
  - If connection is established, client and server agree on attestation state (evidence or attestation result).
  - If RA appraisal succeeds, client and server agree on current transcript hash.
- Binding of attestation key and platform
- Discussion: any other property?

---

[1] Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, 2018.

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

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

Summary

Underspecified = NOT trustworthy!

Key References

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.

Rescorla, Eric. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. Aug. 2018. DOI: 10.17487/RFC8446. URL: https://www.rfc-editor.org/info/rfc8446.

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*. Oct. 2024. URL: https://www.researchgate.net/publication/385384309_Towards_Validation_of_TLS_13_Formal_Model_and_Vulnerabilities_in_Intel's_RA-TLS_Protocol.

ACK

- Cedric Fournet (Microsoft)
- Ionut Mihalcea (Arm)
- Yaron Sheffer (Intuit)
- Thore Sommer (Kiel University)
- Carsten Weinhold (Barkhausen Institut)
- Michael Roitzsch (Barkhausen Institut)