Identity Crisis in Attested TLS for Confidential Computing

Muhammad Usama Sardar[1], Mariam Moustafa[2] and Tuomas Aura[2]

[1]TU Dresden, Germany

[2]Aalto University, Espoo, Finland

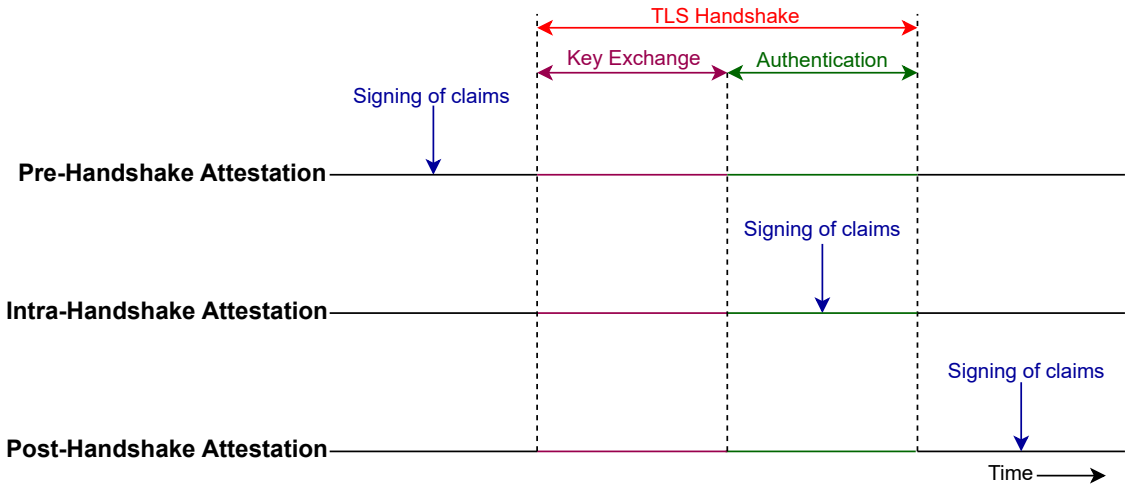
March 18, 2025

Thanks to my travel sponsor!

Outline

WIMSE Context

- WIMSE w2w[1] has TLS
- WIMSE arch[2] has attestation
- How do both fit together?
  - Intra-handshake attestation[3]
  - Post-handshake attestation[4]



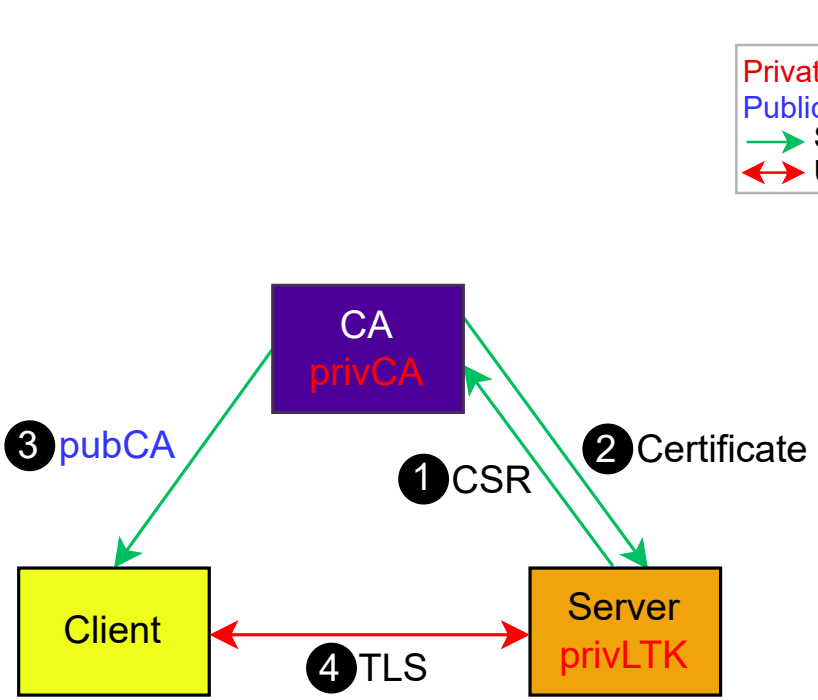
[1] Campbell, J. Salowey, Schwenkschuster, and Sheffer, *WIMSE Workload to Workload Authentication*, 2025.

[2] J. A. Salowey, Rosomakho, and Tschofenig, *Workload Identity in a Multi System Environment (WIMSE) Architecture*, 2025.

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

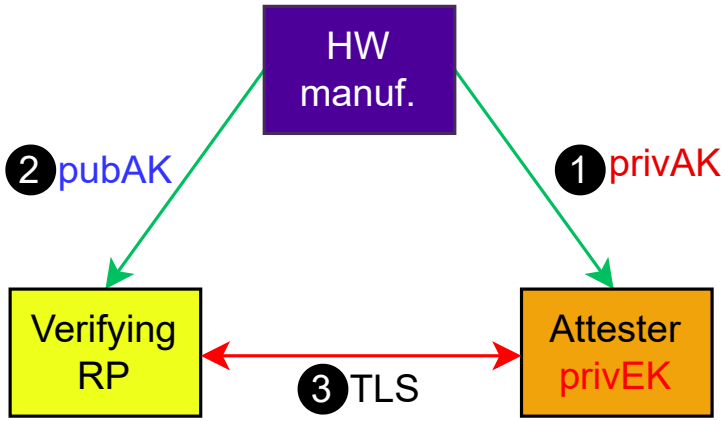
[4] Fossati, Sardar, Sheffer, Tschofenig, and Mihalcea, *Remote Attestation with Exported Authenticators*, 2025.

Standard TLS vs. Remote Attestation



- CA as Trust Anchor

$Cert = sign(privCA, ID \parallel pubLTK)$



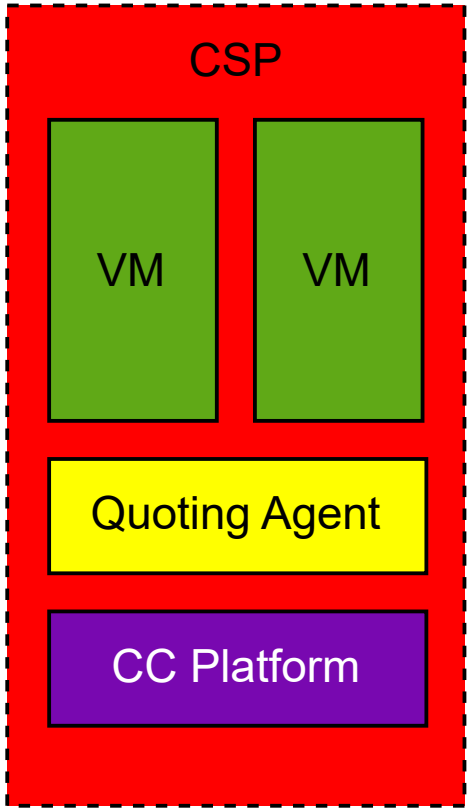
- HW manufacturer as Trust Anchor

$Evidence = sign(privAK, m \parallel pubEK)$

m represents measurements

Threat Model of Confidential Computing

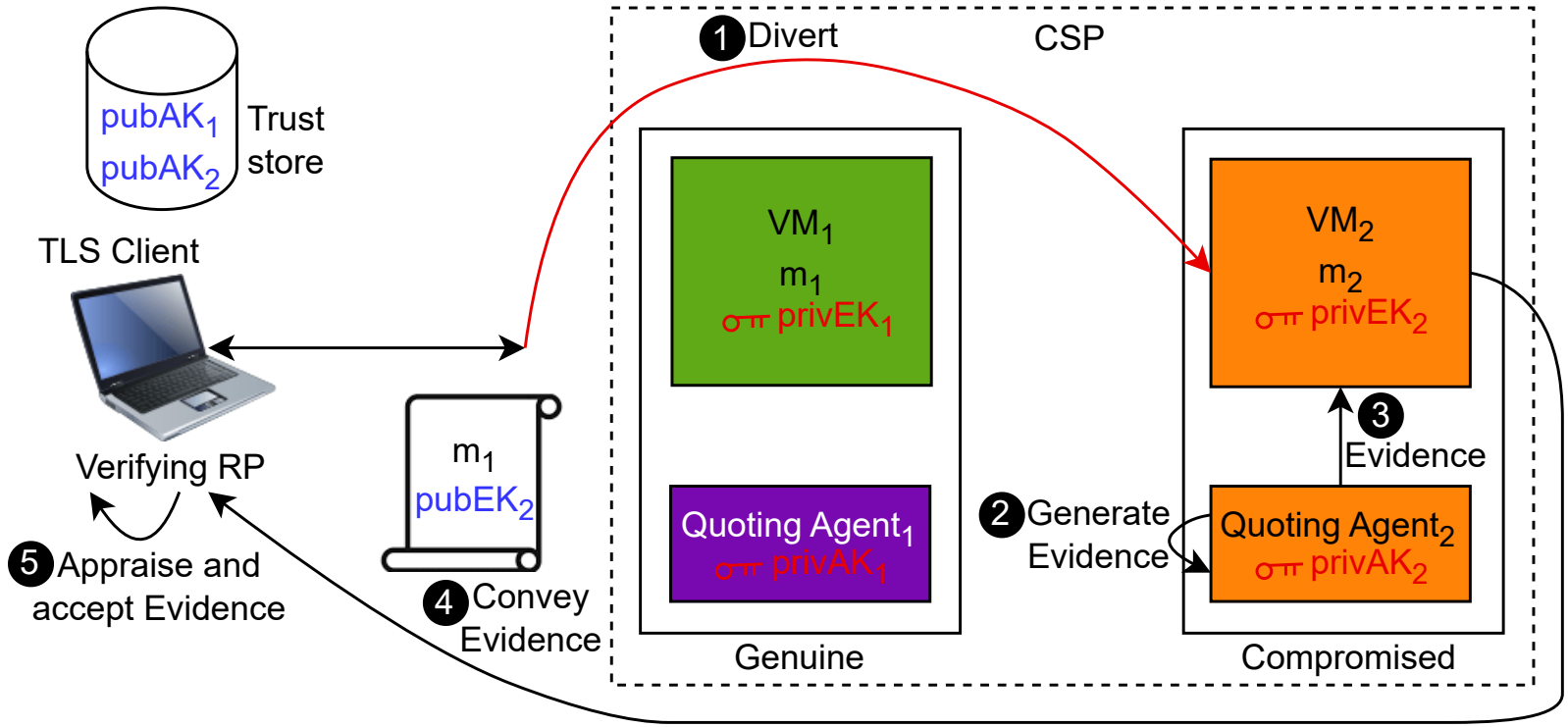
- Untrusted
  - Cloud Provider (CSP)
- Trusted
  - VM (assuming VM-based TEE)
  - Quoting Agent
  - CC Platform (HW,FW,SW)



Outline

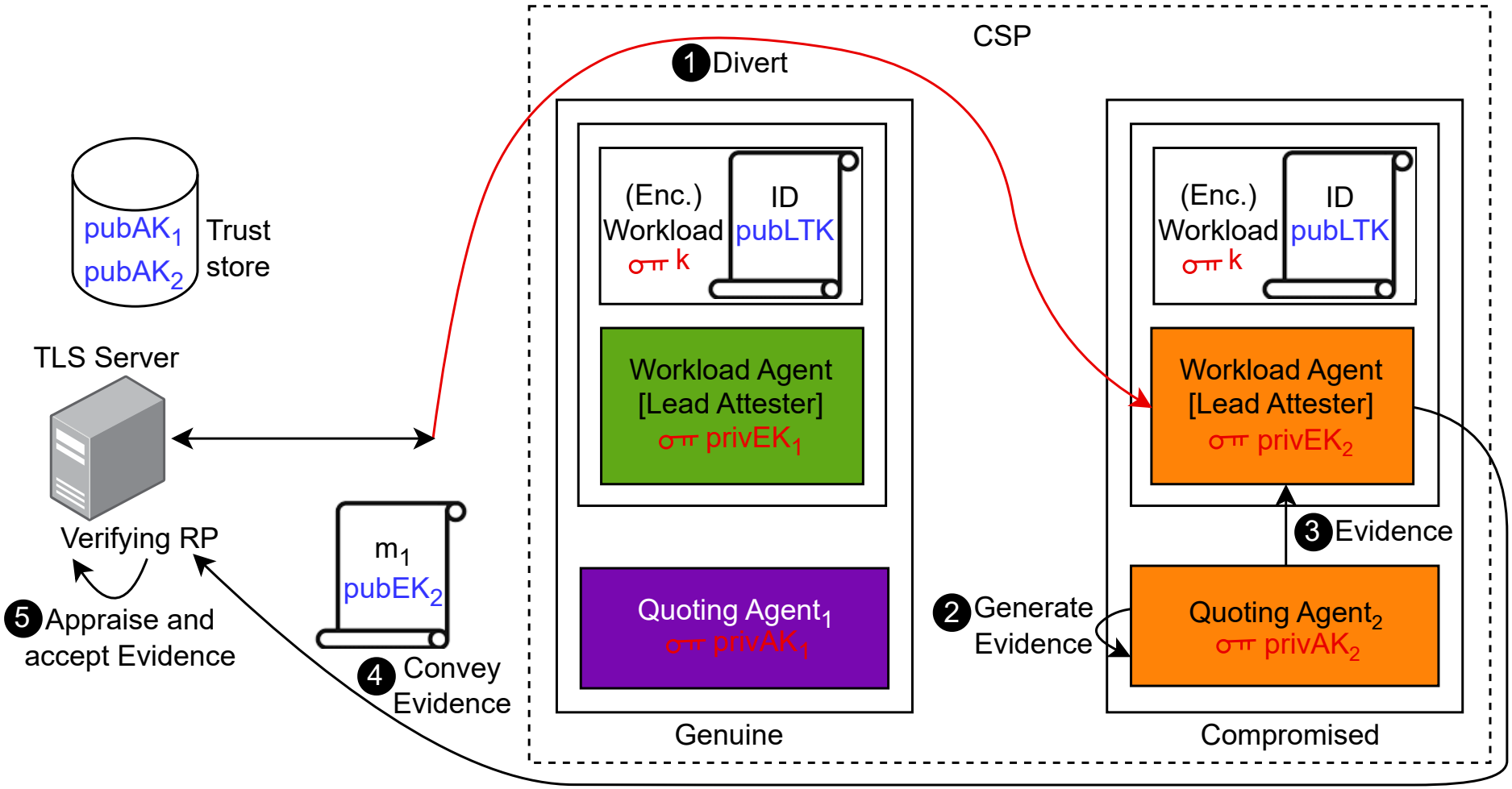
A Diversion Attack

- AK of a specific machine may be compromised. (e.g., $privAK_2$)
  - Transient execution attacks, as demonstrated by Foreshadow[5]
- VM_2 impersonates VM_1



[5] Van Bulck, Minkin, Weisse, Genkin, Kasikci, Piessens, Silberstein, Wenisch, Yarom, and Strackx, "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution", 2018.

B How to Provision ID and LTK?



Key References

Campbell, Brian, Joe Salowey, Arndt Schwenkschuster, and Yaron Sheffer. *WIMSE Workload to Workload Authentication*. Internet-Draft draft-ietf-wimse-s2s-protocol-03. Work in Progress. Internet Engineering Task Force, Mar. 2025. 27 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-wimse-s2s-protocol/03/.

Fossati, Thomas, Muhammad Usama Sardar, Yaron Sheffer, Hannes Tschofenig, and Ionuț Mihalcea. *Remote Attestation with Exported Authenticators*. Internet-Draft draft-fossati-tls-exported-attestation-00. Work in Progress. Internet Engineering Task Force, Mar. 2025. 9 pp. URL: https://datatracker.ietf.org/doc/draft-fossati-tls-exported-attestation/00/.

Salowey, Joseph A., Yaroslav Rosomakho, and Hannes Tschofenig. *Workload Identity in a Multi System Environment (WIMSE) Architecture*. Internet-Draft draft-ietf-wimse-arch-04. Work in Progress. Internet Engineering Task Force, Mar. 2025. 22 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-wimse-arch/04/.

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. Work in Progress. Internet Engineering Task Force, Oct. 2024. 34 pp. URL: https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/08/.

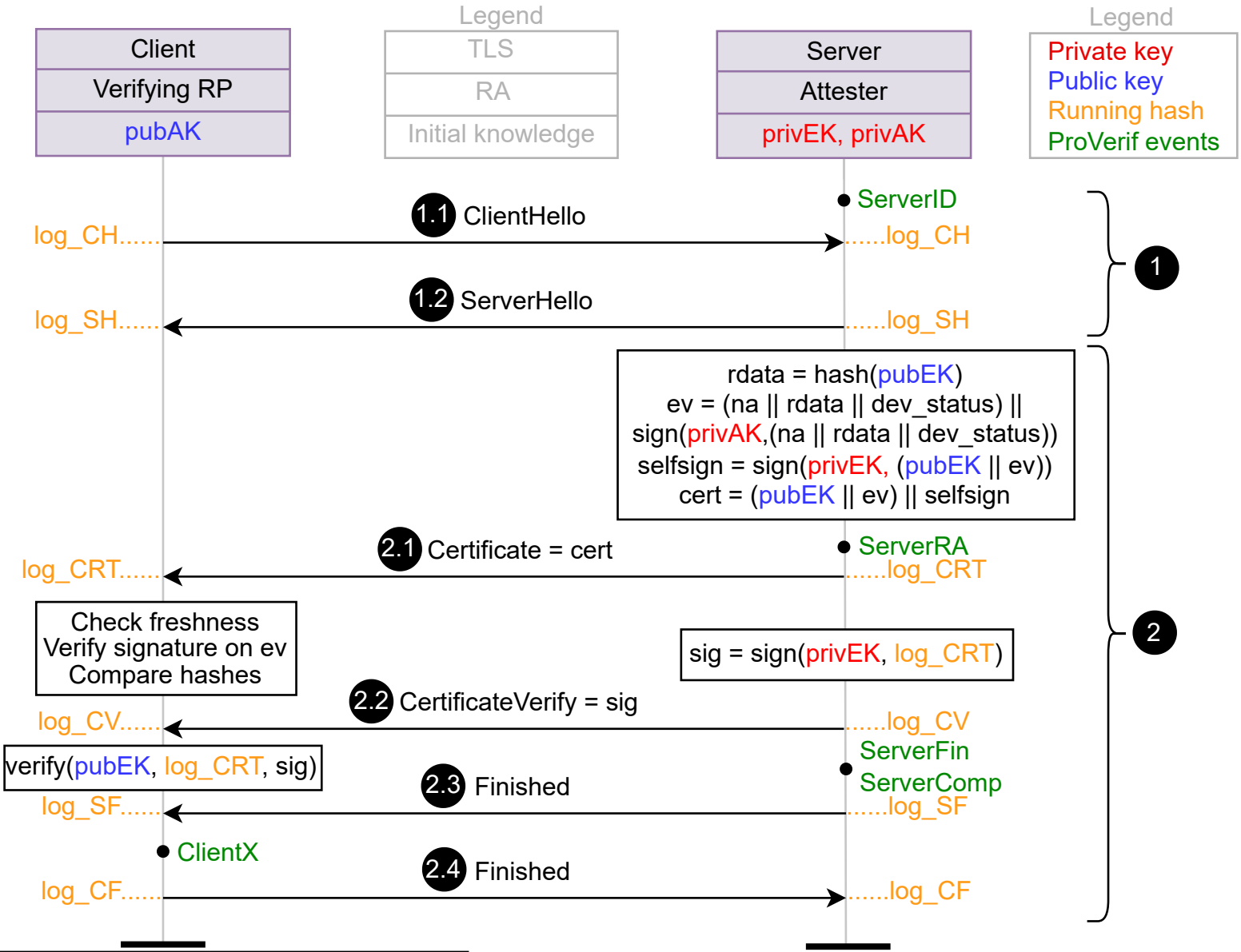
Van Bulck, Jo, Marina Minkin, Ofir Weisse, Daniel Genkin, Baris Kasikci, Frank Piessens, Mark Silberstein, Thomas F. Wenisch, Yuval Yarom, and Raoul Strackx. "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution". In: *Proceedings of the 27th USENIX Security Symposium*. USENIX Association, Aug. 2018.

ACK

- Laurence Lundblade (Security Theory LLC)
- Thomas Fossati (Linaro)
- Hannes Tschofenig (University of Applied Sciences Bonn-Rhein-Sieg and Siemens)
- Ionut Mihalcea (Arm)
- Yaron Sheffer (Intuit)
- Cedric Fournet (Microsoft)
- Thore Sommer (Kiel University)
- Jonathan Hoyland (Cloudflare)
- Jo Van Bulck (KU Leuven)
- Dionna Amalie Glaze (Google)
- Jean-Marie Jacquet (University of Namur)
- Maryam Zarezadeh (Barkhausen Institut)
- Henk Birkholz (Fraunhofer SIT)

Outline

TLS-attest Protocol[6]



[6] https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/