Identity Crisis in Attested TLS for Confidential Computing

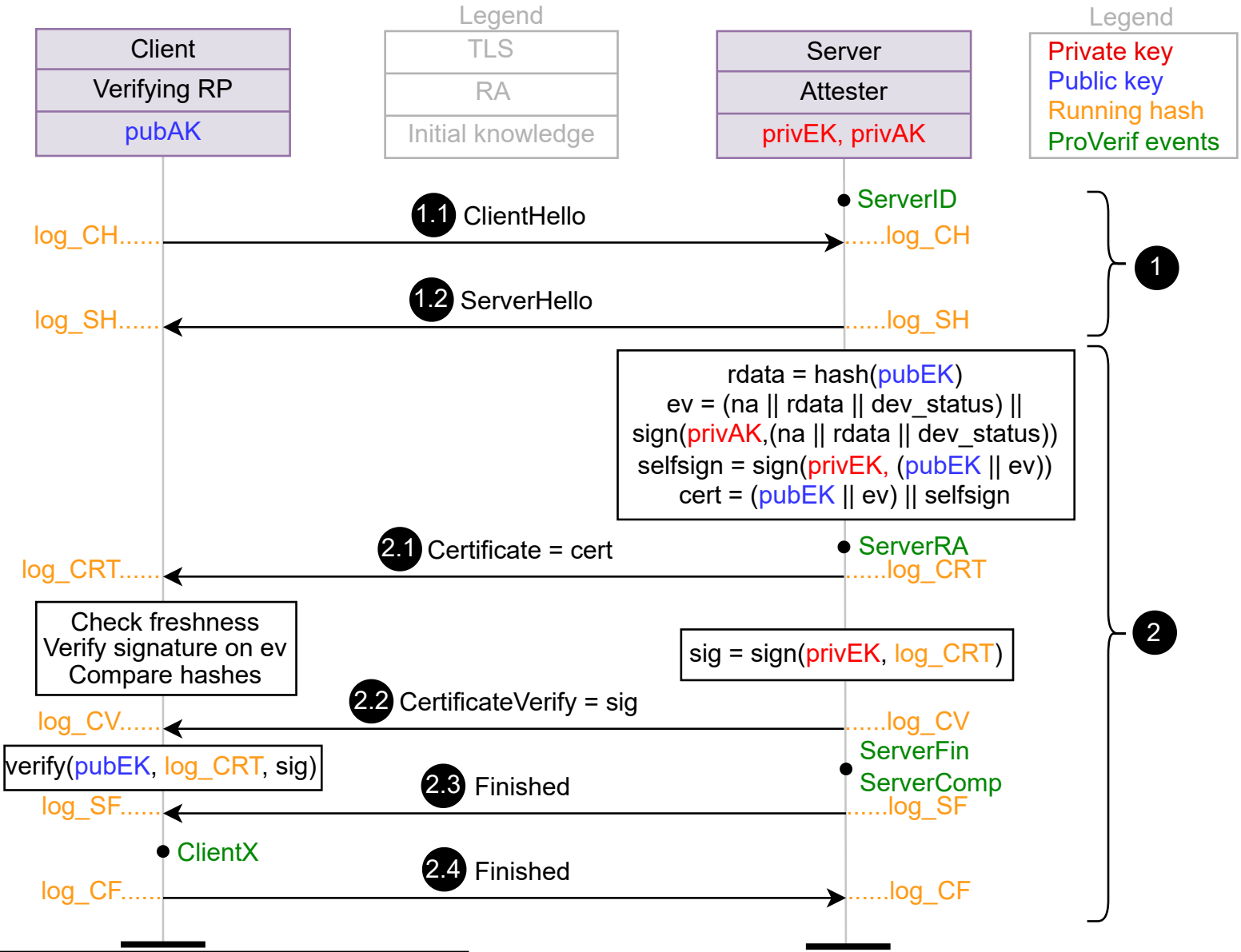
Muhammad Usama Sardar[1], Mariam Moustafa[2] and Tuomas Aura[2]

[1]TU Dresden, Germany

[2]Aalto University, Espoo, Finland

March 11, 2025

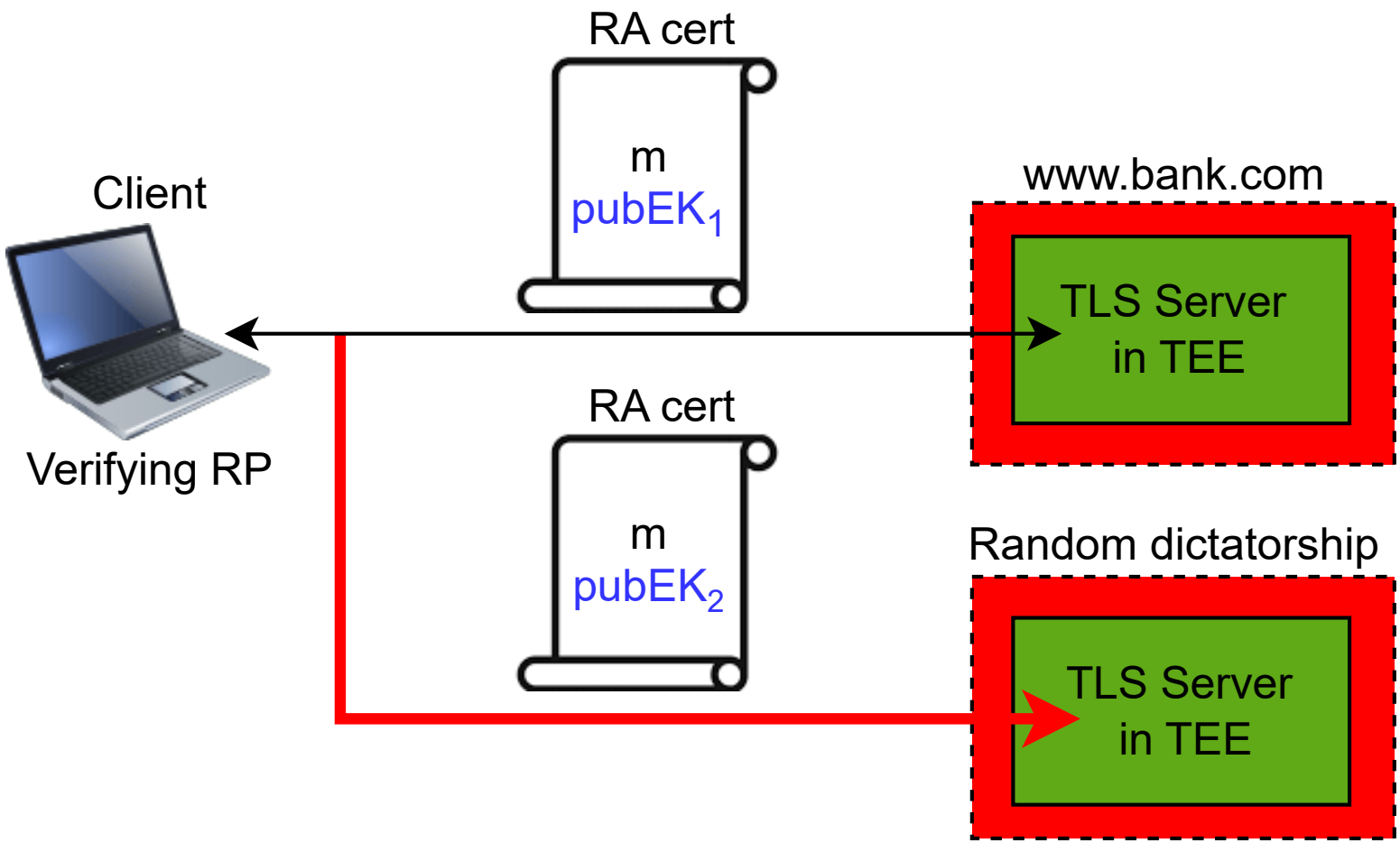
TLS-attest[1]



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

Problem with Remote Attestation-only

- PKI cert not presented $\Longrightarrow$ No identity auth
- Is the average cloud customer happy with this?



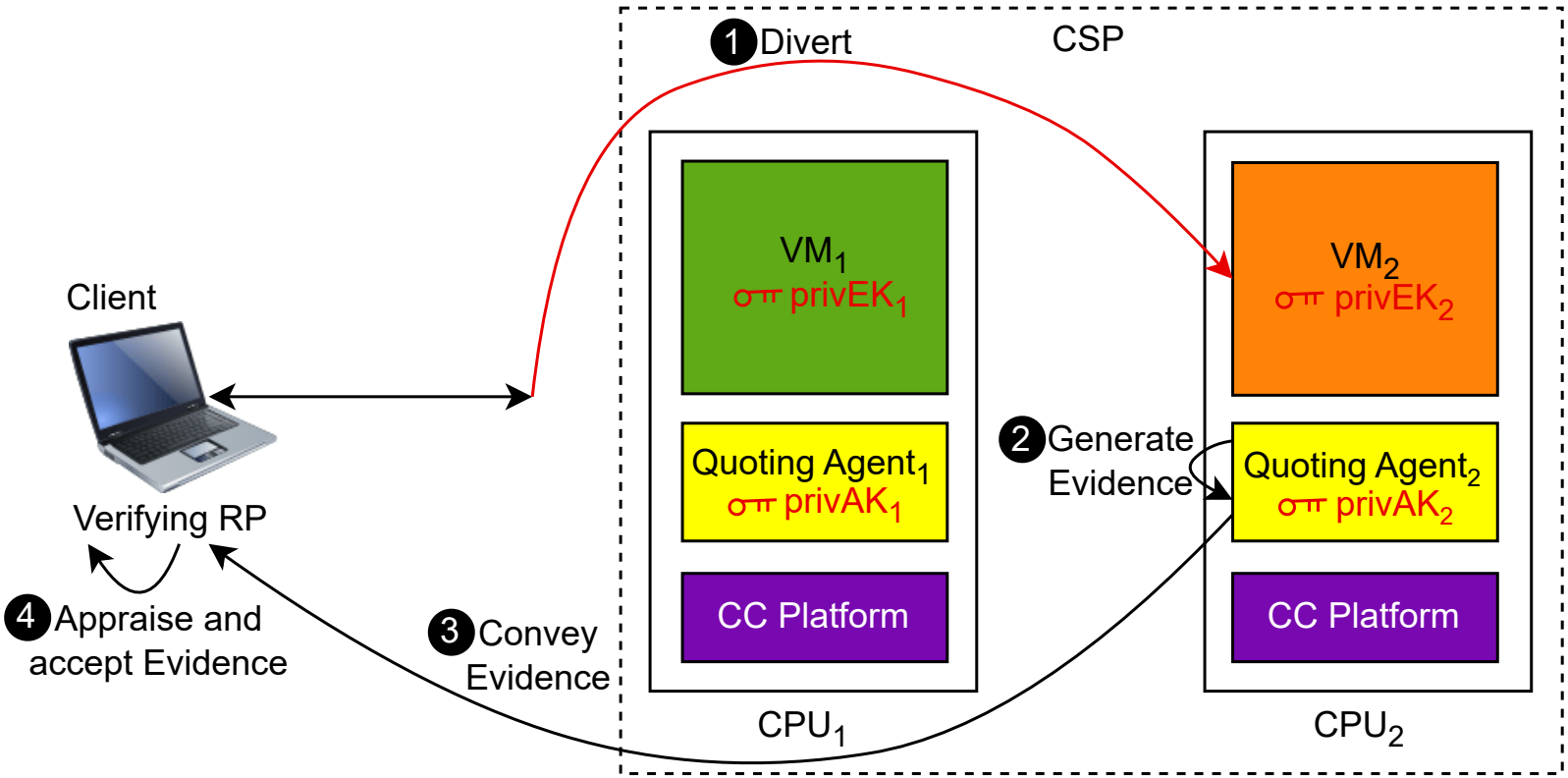
Solutions

- Augment rather than replace Server Authentication
  - Web PKI cert for ID, e.g., hostname
  - RA cert to prove integrity of its computing environment
- Challenge: CertificateVerify message is not extensible!
- Possible solutions
  1. Make CertificateVerify extensible
  2. Allow multiple CertificateVerify messages
     - 2a. As part of handshake
     - 2b. Post-handshake[2]
  3. New signature algorithm that is a concatenation of two cryptographic signatures. (Fully threshold signatures?)
  4. Identity key (LTK) signs CertificateVerify. EK only signs self-signed certificate, which contains the channel binder as part of the evidence.

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

Diversion Attack

- $privAK_2$ compromised via e.g., Foreshadow[3]
- VM_2 impersonates VM_1



[3] 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.

How to assign ID and LTK?

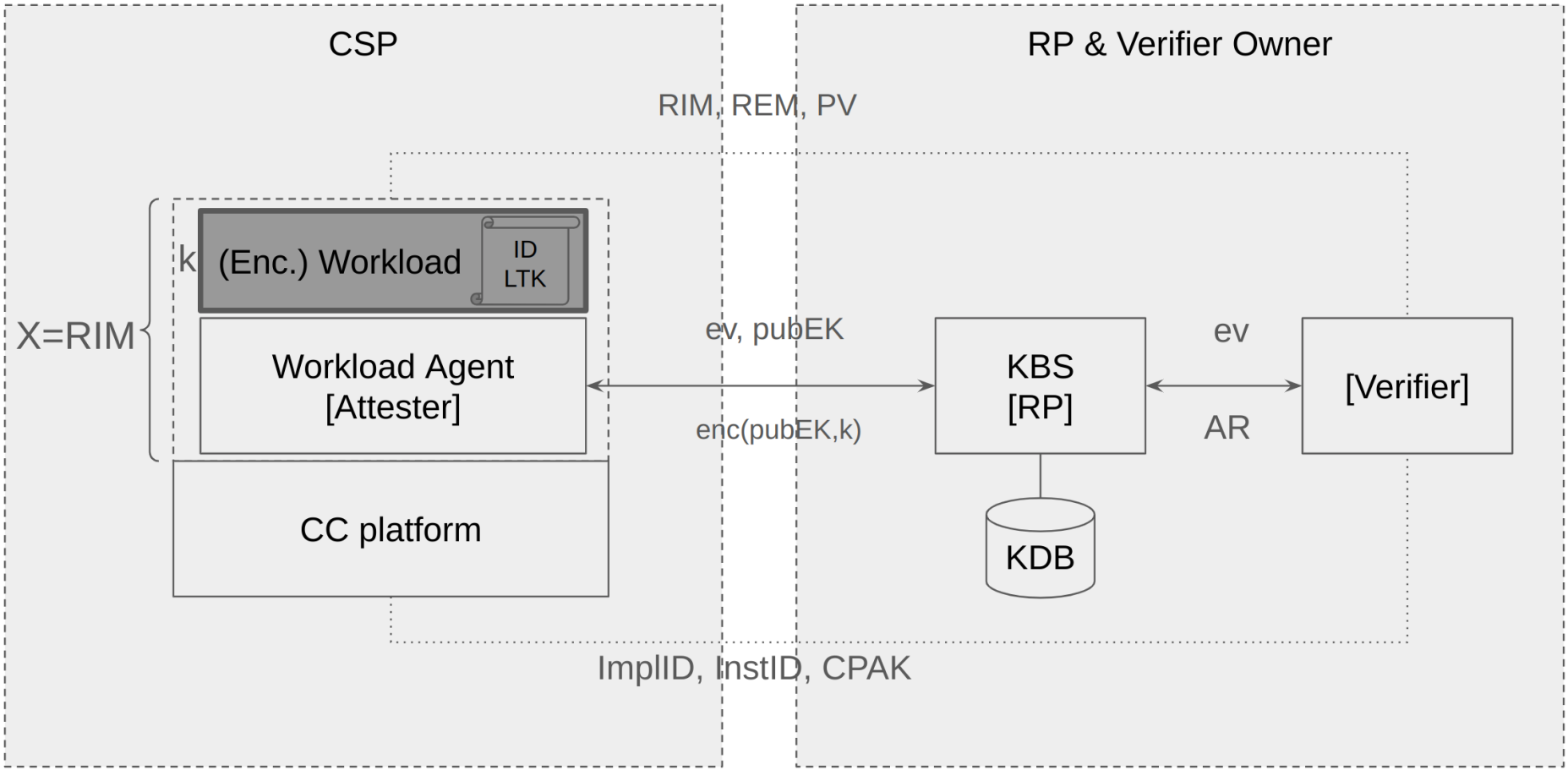


Image credits: Thomas Fossati

Key References

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/.

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)