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 20, 2025

Thanks to my travel sponsor!

Outline

Context

- I-D: draft-fossati-tls-attestation[1]
- IETF 121 presentation[2]
  - Mentioned confidential computing (CC) as main priority
  - Asked for adoption
- FATT[3] requirements
- Today: Formal analysis of I-D under CC threat model in ProVerif
  - Breaks server authentication[4]
  - Proposed solutions and open problems
- Challenge: *Terminology hell* and several rabbit holes in RATS[5]
  - Very abstracted view (due to time limitations)
  - Verifying RP = Verifier + Relying Party

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

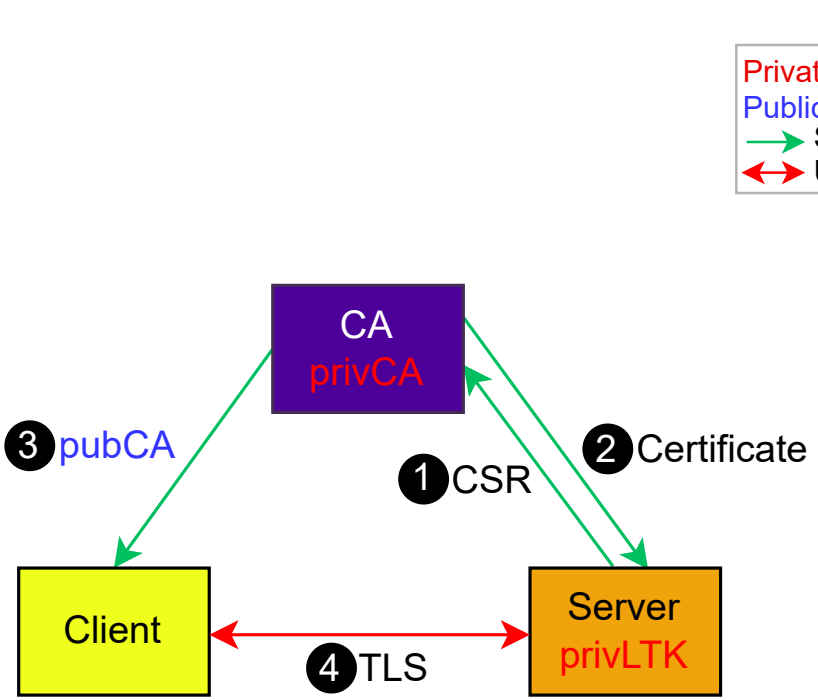
[2] `https://datatracker.ietf.org/meeting/121/materials/slides-121-tls-tls-and-attestation-00`

[3] `https://github.com/tlswg/tls-fatt`

[4] `https://mailarchive.ietf.org/arch/msg/tls/Jx_yPoYWMIKaqXmPsytKZBDq23o/`

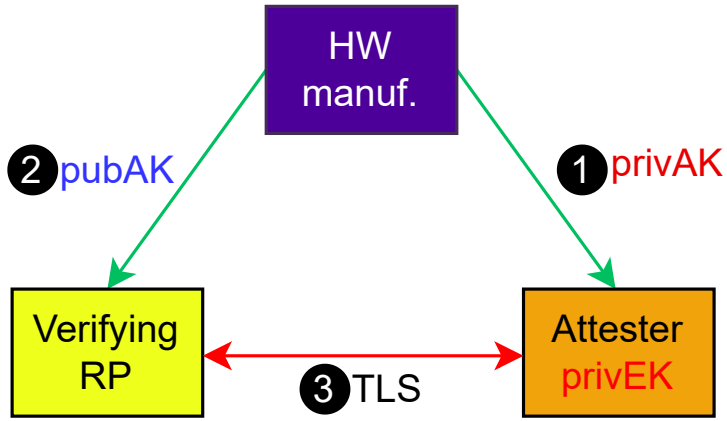
[5] Birkholz, Thaler, Richardson, Smith, and Pan, *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Standard TLS vs. Remote Attestation (RA)



- CA as Trust Anchor

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



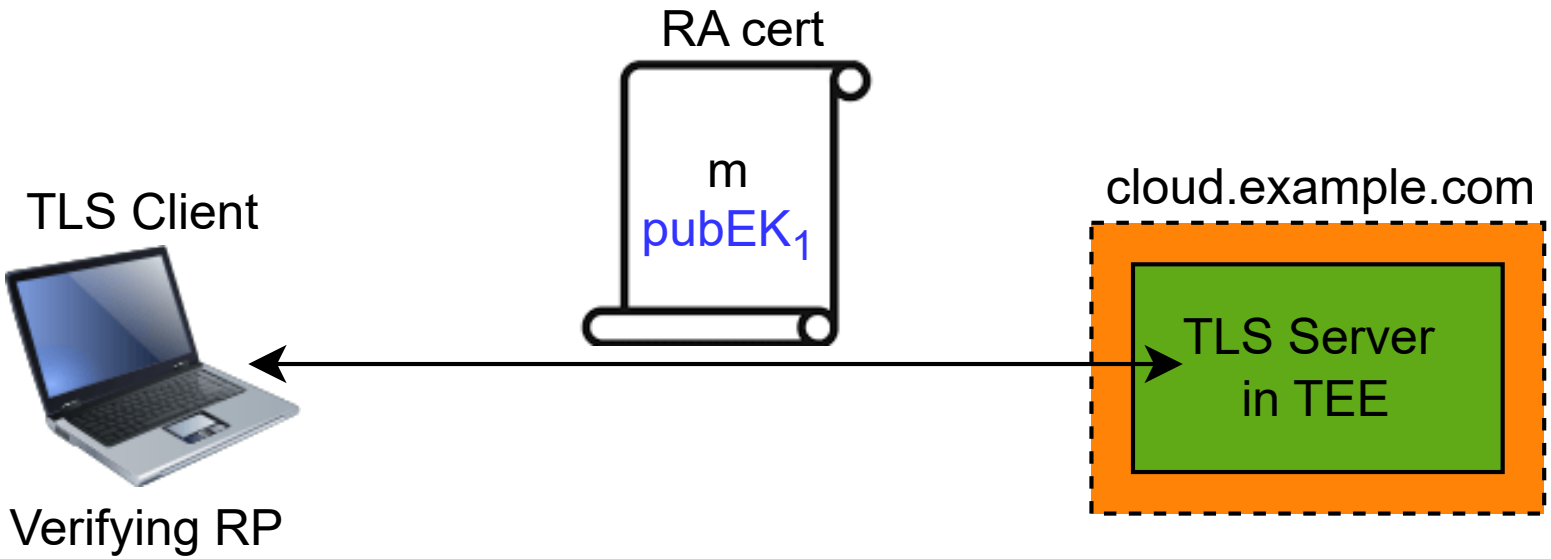
- HW manufacturer as Trust Anchor

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

m represents measurements

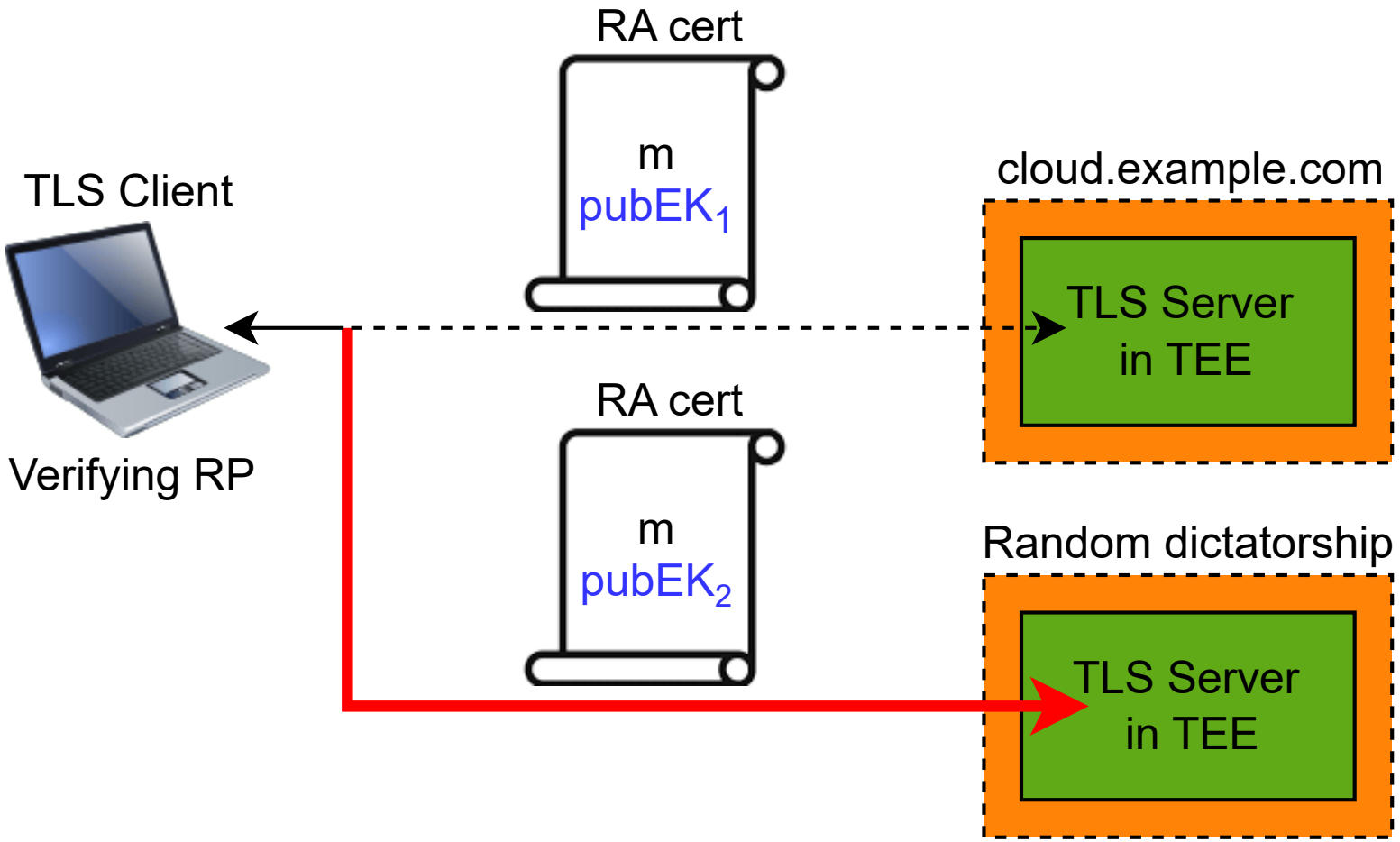
Remote Attestation-only (§6.1 in I-D)

- RA cert with measurements
- Is the average cloud customer happy with this?



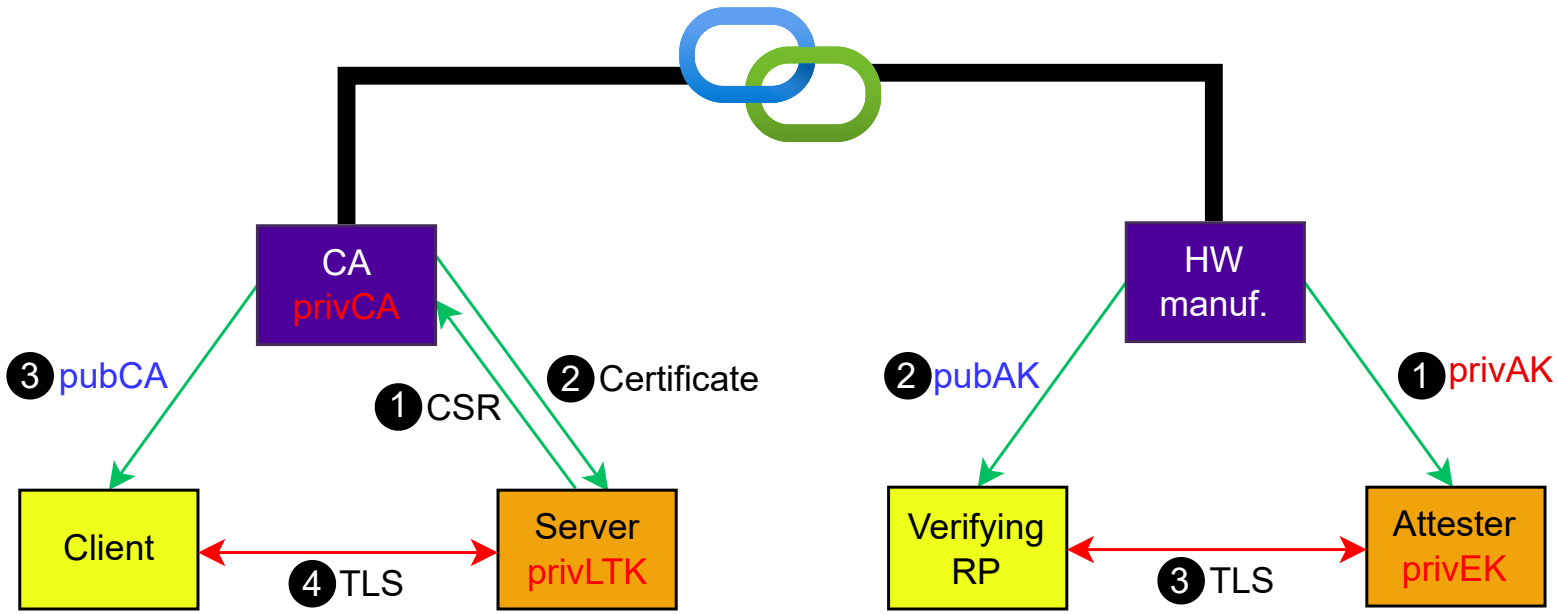
Problem with Remote Attestation-only

- No PKI cert $\Longrightarrow$ No identity authentication
- Hostname not measured $\Longrightarrow$ Redirection to a different data center



Solution

- Augment rather than replace Server Authentication
  - PKI cert for ID, e.g., hostname
  - RA cert to prove integrity of its computing environment



- Challenge: CertificateVerify message is not extensible!

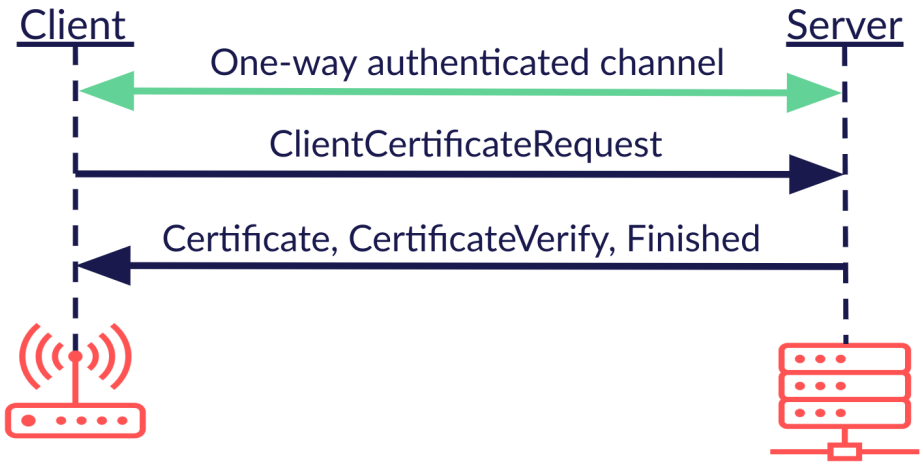
Potential Solutions

Intra-Handshake Attestation

1. Extension flag to
   1a. Modify CertificateVerify message
   1b. Allow multiple CertificateVerify messages
2. Channel binder requiring key schedule changes

Post-Handshake Attestation[a]

- Based on RFC9261[b]
- Server as Attester



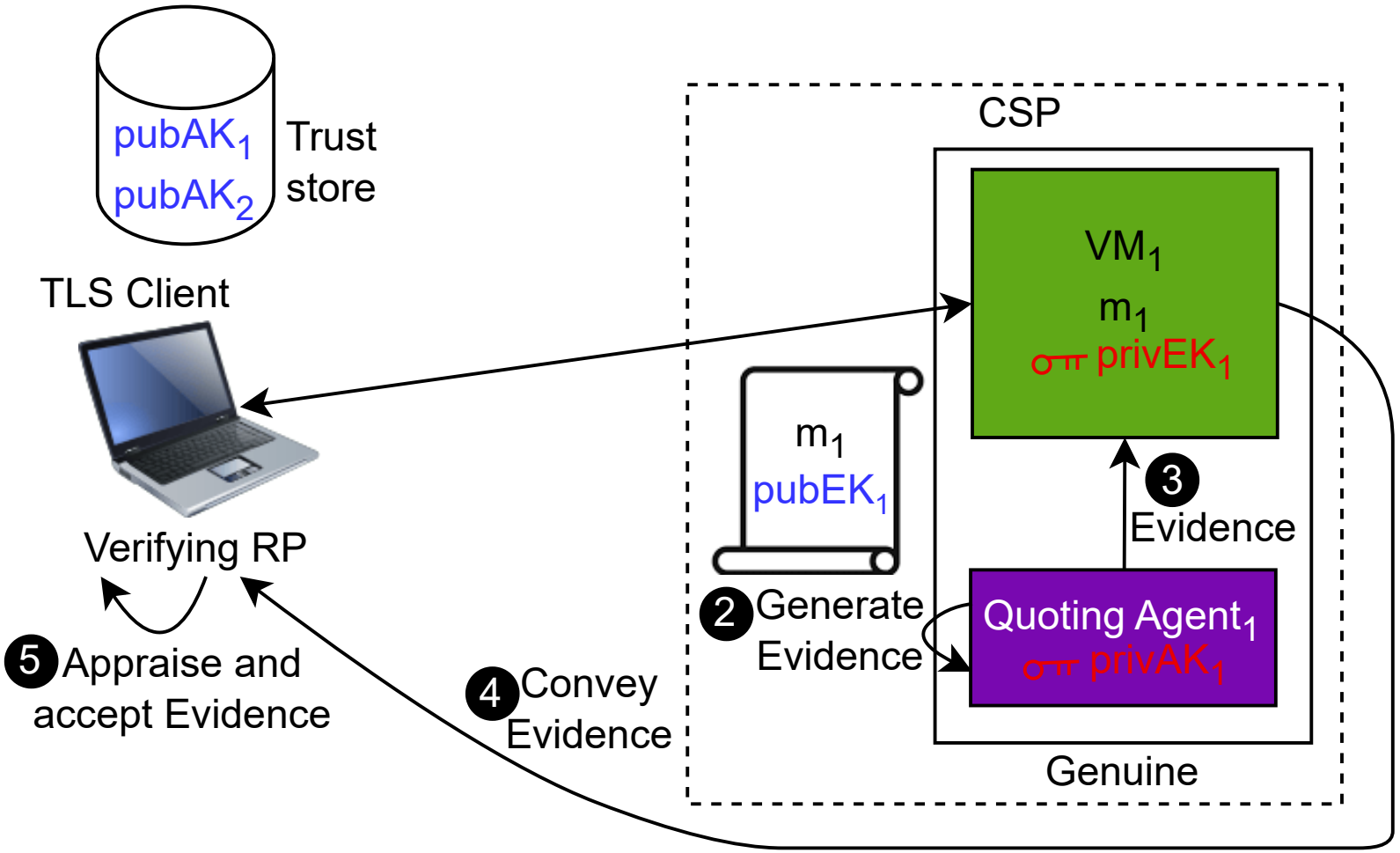
[a] Fossati, Sardar, Sheffer, Tschofenig, and Mihalcea, *Remote Attestation with Exported Authenticators*, 2025.

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

Outline

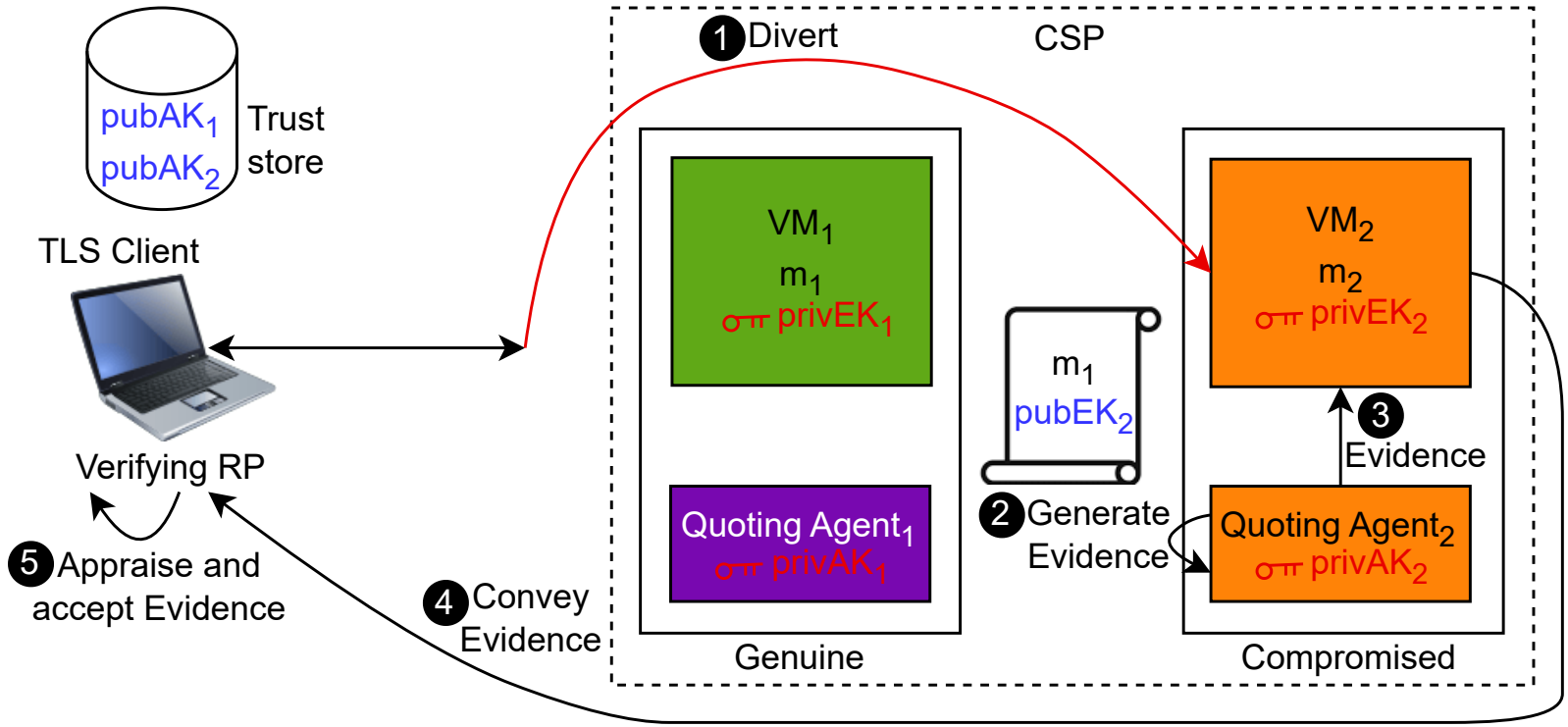
Original Path

- Quoting Agent generates Evidence.



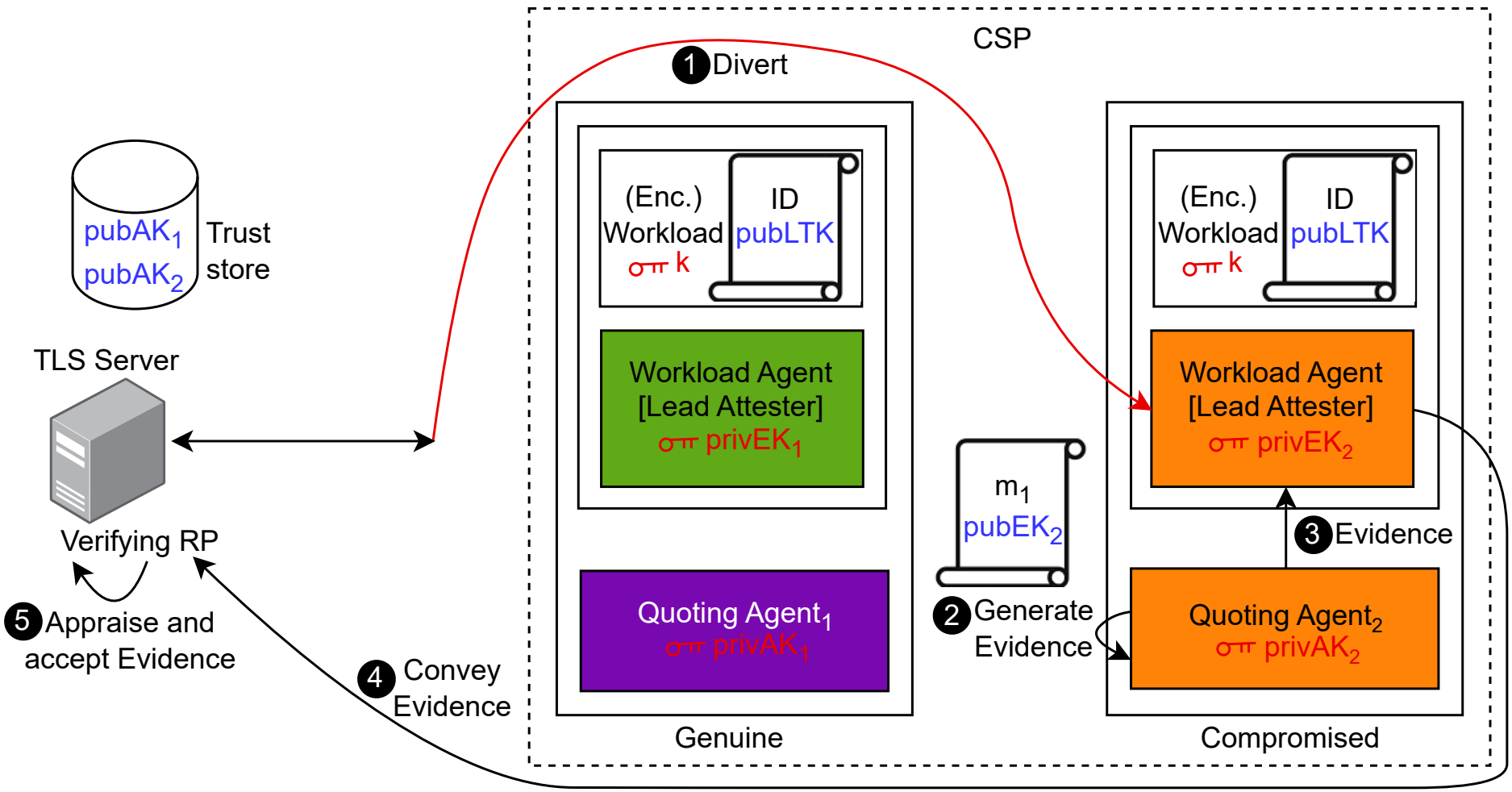
A Diversion Attack

- AK of a specific machine may be compromised. (e.g., $privAK_2$)
  - Transient execution attacks, as demonstrated by Foreshadow[6]
- VM_2 impersonates VM_1



[6] 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?



- CSP gets the key k

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.

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/.

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

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/.

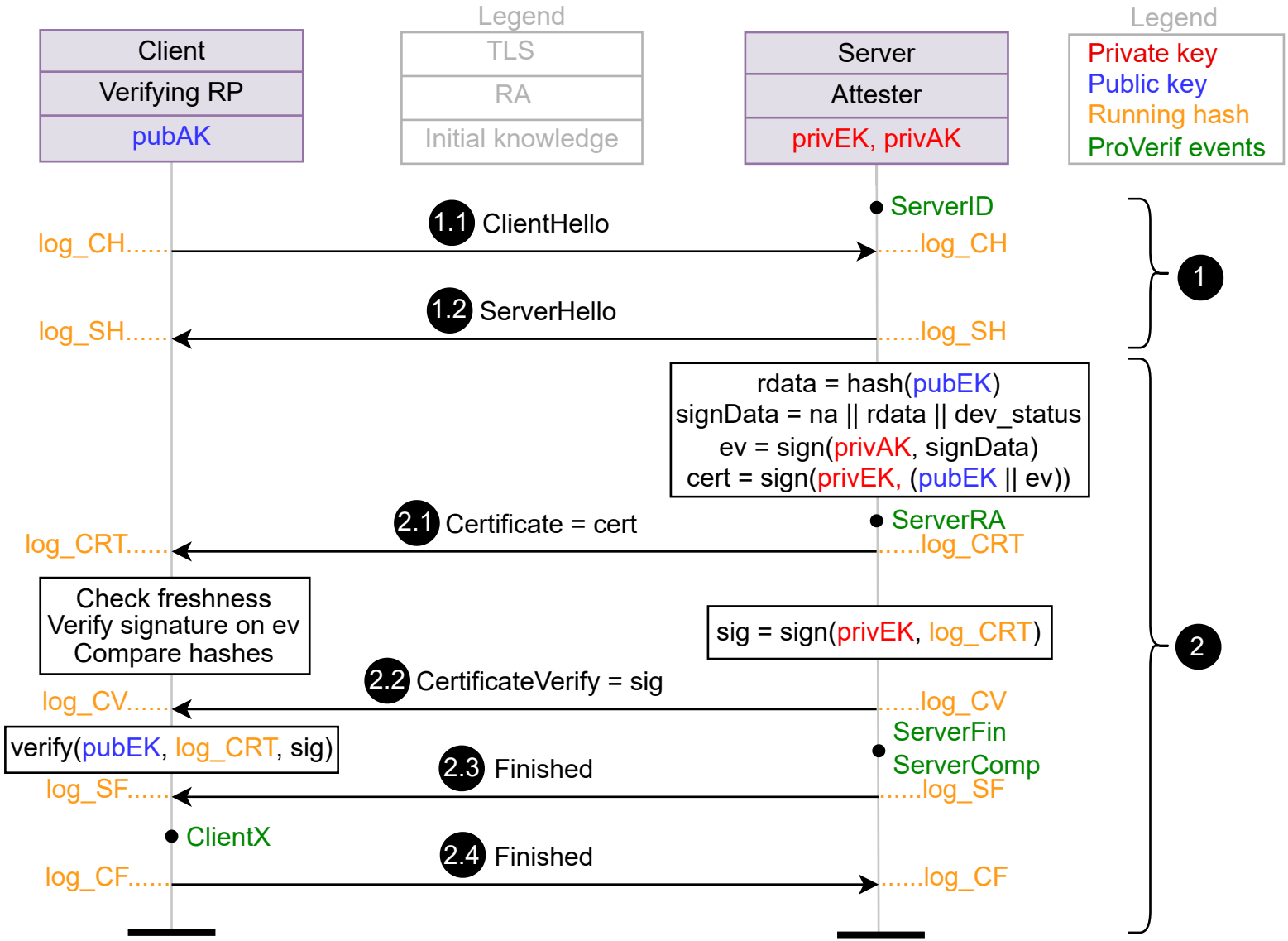
Van Bulck, Jo, Marina Minkin, Ofir Weisse, Daniel Genkin, Baris Kasikci, Frank Piessens, Mark Silberstein, Thomas F. Wenisch, Yuval Yarom, and Raoul Strackx. "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution". In: *Proceedings of the 27th USENIX Security 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[7]



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