Standardization of Attested TLS Protocols for Confidential Computing

Muhammad Usama Sardar*

Based on joint works with Arto Niemi, Hannes Tschofenig, Thomas Fossati, Simon Frost, Ned Smith, Mariam Moustafa, Tuomas Aura, Yaron Sheffer, Ionut Mihalcea and Jean-Marie Jacquet

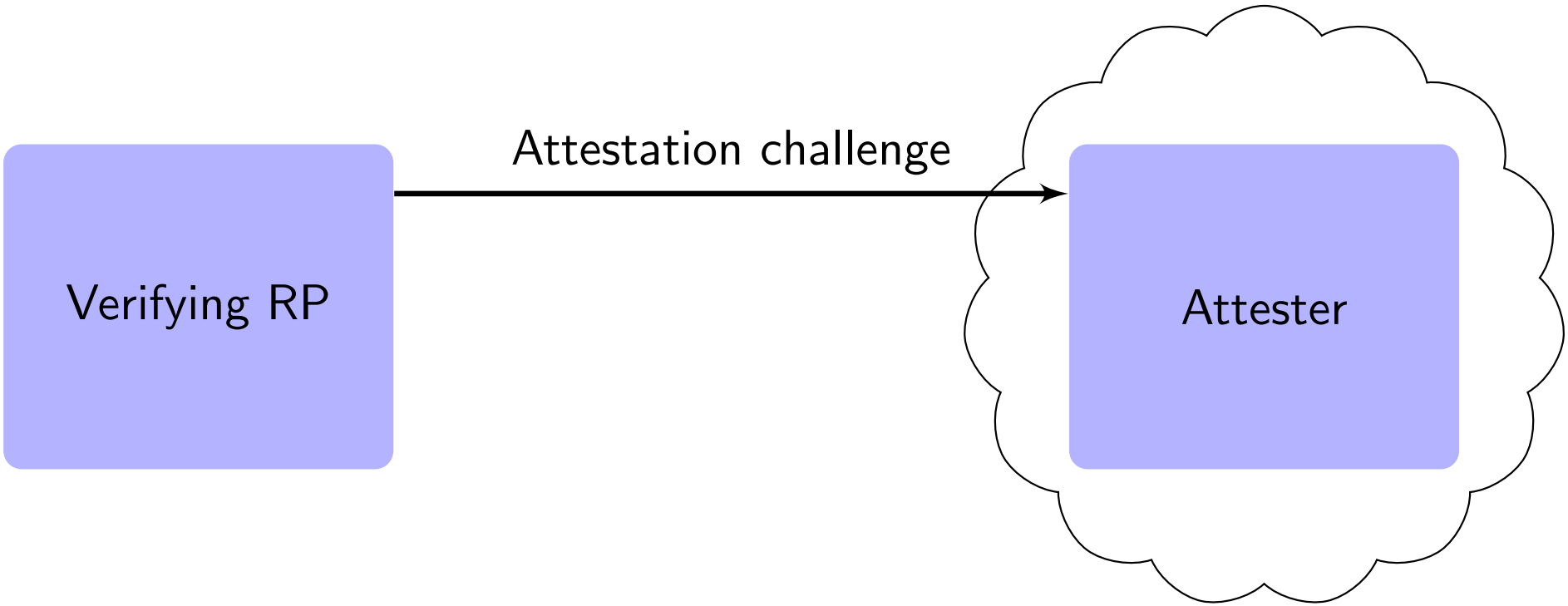
*TU Dresden, Germany

June 26, 2025

Outline

Motivation

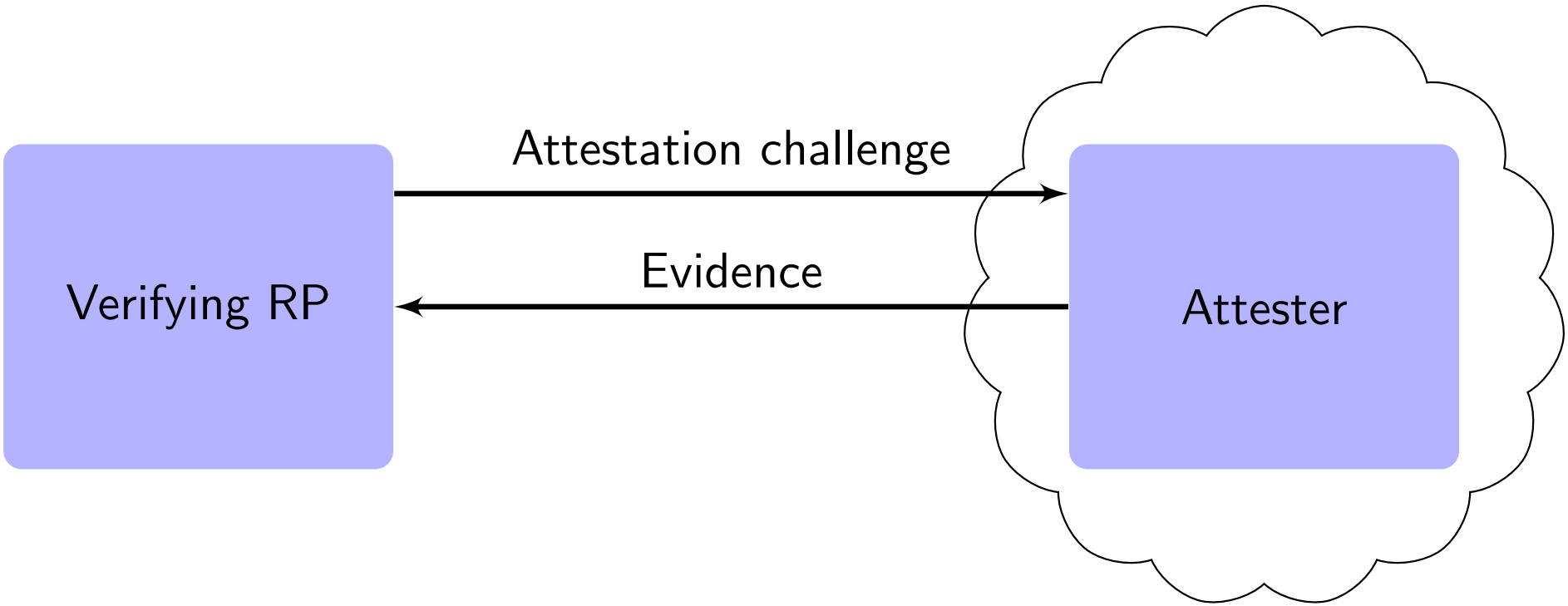
- There is no Confidential Computing without Architecturally-defined Attestation[1]
- Verifying RP = Verifier + Relying Party



[1] Sardar and Fetzer, *Confidential Computing and Related Technologies : A Critical Review*, 2021.

Motivation

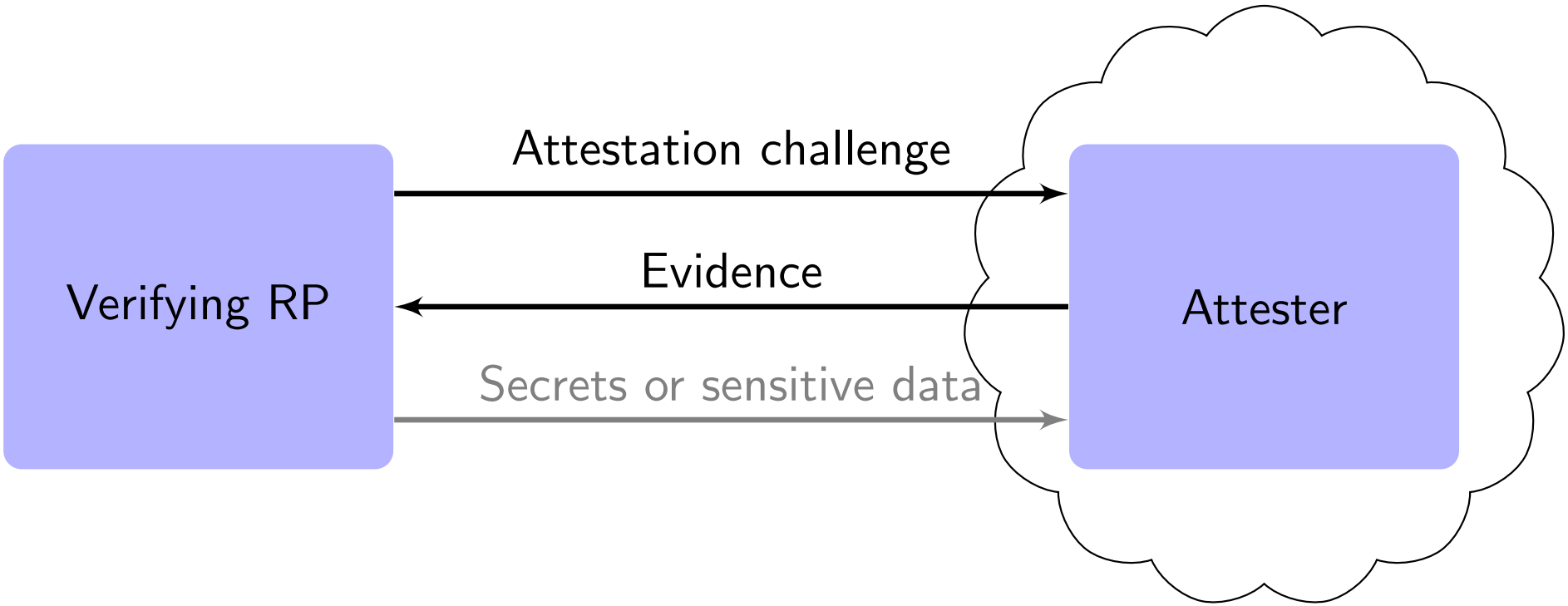
- There is no Confidential Computing without Architecturally-defined Attestation[1]
- Verifying RP = Verifier + Relying Party



[1] Sardar and Fetzer, *Confidential Computing and Related Technologies : A Critical Review*, 2021.

Motivation

- There is no Confidential Computing without Architecturally-defined Attestation[1]
- Verifying RP = Verifier + Relying Party



[1] Sardar and Fetzer, *Confidential Computing and Related Technologies : A Critical Review*, 2021.

Levels of Assurance for Attested TLS Protocols

	RA-TLS[2] (Pre-HS)	TLS attest[3] (Intra-HS)	SCONE[4] (Post-HS)
(a) Open-source implementation	✓[5]	✓[6]	×
(b) Informal specifications available	×	✓	×
(c) Formal specifications	✓[7]	×	×
(d) Formal analysis of specifications	✓	×	×
(e) Formal verification of implementation	×	×	×

- Open source is a MUST for confidential computing!

---

[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.

[5] `https://github.com/gramineproject/gramine/tree/master/CI-Examples/ra-tls-mbedtls`

[6] `https://github.com/CCC-Attestation/attested-tls-poc`

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

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

Levels of Assurance for Attested TLS Protocols

	RA-TLS[2] (Pre-HS)	TLS attest[3] (Intra-HS)	SCONE[4] (Post-HS)
(a) Open-source implementation	✓[5]	✓[6]	×
(b) Informal specifications available	×	✓	×
(c) Formal specifications	✓[7]	×	×
(d) Formal analysis of specifications	✓	×	×
(e) Formal verification of implementation	×	×	×

- Open source is a MUST for confidential computing!
- Formal analysis: a requirement at TLS WG[8]

[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.

[5] `https://github.com/gramineproject/gramine/tree/master/CI-Examples/ra-tls-mbedtls`

[6] `https://github.com/CCC-Attestation/attested-tls-poc`

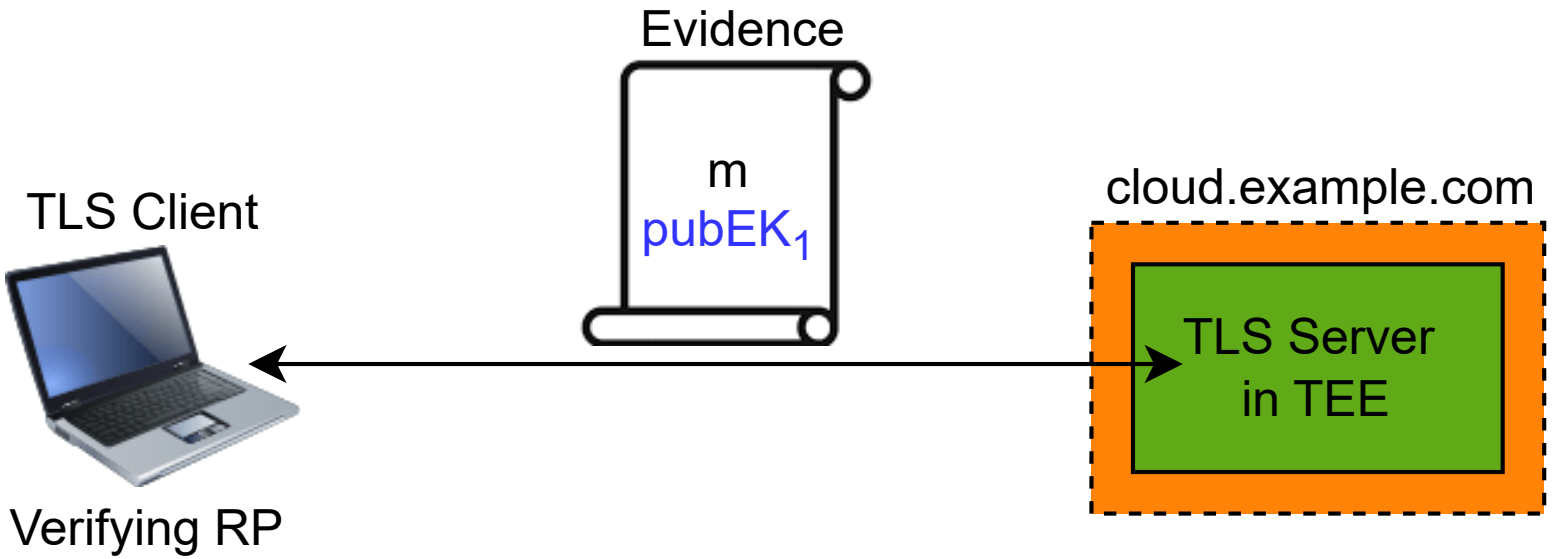
[7] Sardar, Niemi, Tschofenig, and Fossati, "Towards Validation of TLS 1.3 Formal Model and Vulnerabilities in Intel's RA-TLS Protocol", 2024.

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

Outline

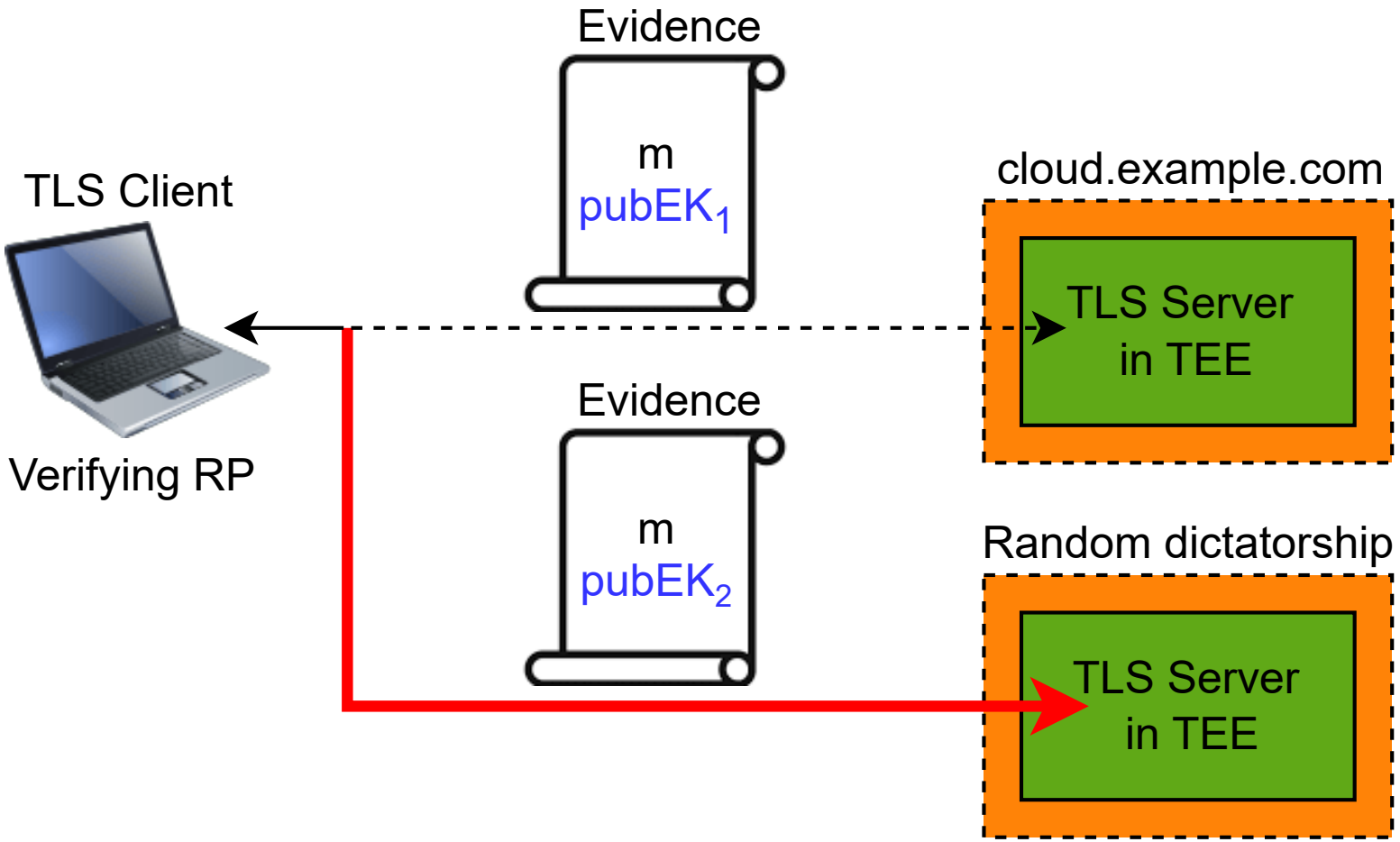
Remote Attestation-only (§6.1 in TLS-attest draft)

- Evidence with measurements
- Is the average cloud customer happy with this?



Diversion to Different Data Center

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



Security Consideration: Identity Crisis

Using the proposed protocol, the security breaks if there is even one compromised machine (i.e., Attestation Key is compromised) in the world whose corresponding certificate (e.g., Provisioning Certification Key certificate for Intel TDX) has not yet been added to the revocation list.

Outline

Can CSP *really* be out of TCB?

- In all cases, CSP is trusted for:
  1. Availability

Can CSP *really* be out of TCB?

- In all cases, CSP is trusted for:
  1. Availability
  2. Machine identifier

Can CSP *really* be out of TCB?

- In all cases, CSP is trusted for:
  1. Availability
  2. Machine identifier
     - Violates host-affinity requirement of *data sovereignty* regulations

Can CSP *really* be out of TCB?

- In all cases, CSP is trusted for:
  1. Availability
  2. Machine identifier
     - Violates host-affinity requirement of *data sovereignty* regulations
  3. Location

Can CSP *really* be out of TCB?

- In all cases, CSP is trusted for:
  1. Availability
  2. Machine identifier
     - Violates host-affinity requirement of *data sovereignty* regulations
  3. Location
     - CSP is the only source of truth for location.

Can CSP *really* be out of TCB?

- In all cases, CSP is trusted for:
  1. Availability
  2. Machine identifier
     - Violates host-affinity requirement of *data sovereignty* regulations
  3. Location
     - CSP is the only source of truth for location.
     - Violates location-affinity requirement of *data residency* regulations

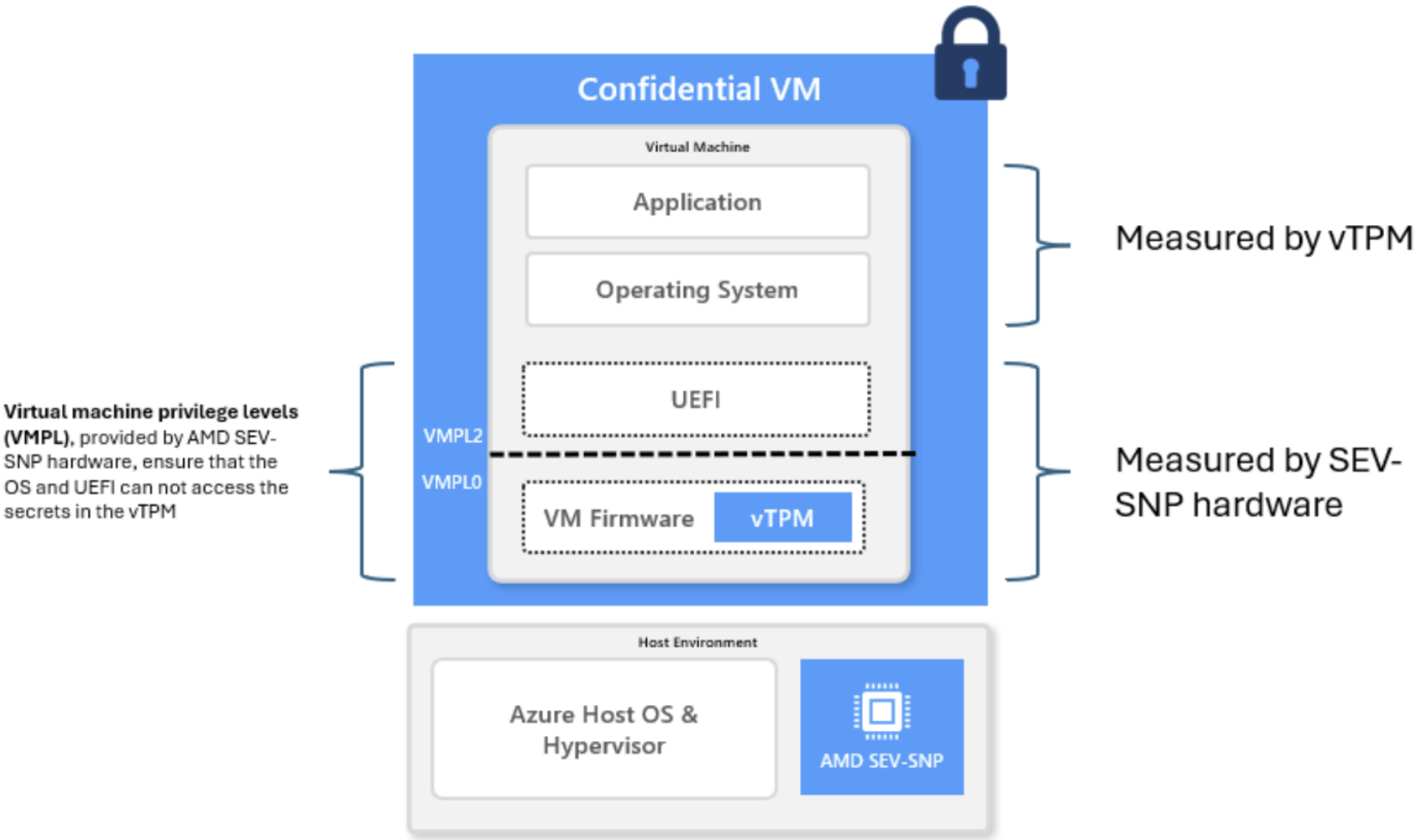
Can CSP *really* be out of TCB?

- In most cases, CSP is trusted for:
  1. Any part of the boot software that is not open source and not independently reproducible (IR)
     - Closed-source code may contain backdoors.
     - Cannot ensure configs of vTPM, e.g., non-migratability of keys
  2. Early boot measurements stored in vTPM
  3. Even remote attestation

Criteria	AWS	Microsoft	Google
VM firmware: open-source & IR	✓	×	×
vTPM inside confidential VM	×	✓	×
Ability to fetch raw Evidence directly	✓	×	✓

Example: Microsoft Azure[9]

- Who owns the seed for the Endorsement Key of vTPM?
- Who signs the Endorsement Key of vTPM?



[9] https://learn.microsoft.com/en-us/azure/confidential-computing/virtual-tpms-in-azure-confidential-vm

Next Steps

- Remove statements related to CSP being out of TCB from the white paper
- Explicitly state that location is out of scope of Confidential computing
- WG-forming BoF[10] at IETF 123

[10] https://datatracker.ietf.org/doc/bofreq-fossati-tls-exported-attestation-expat/

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.

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.

Sardar, Muhammad Usama and Christof Fetzer. *Confidential Computing and Related Technologies : A Critical Review*. 2021. URL: https://www.researchgate.net/publication/356474602_Confidential_Computing_and_Related_Technologies_A_Review.

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". In: *IEEE Access* 12 (2024), pp. 173670–173685. DOI: 10.1109/ACCESS.2024.3497184.

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

Co-authors/Co-editors

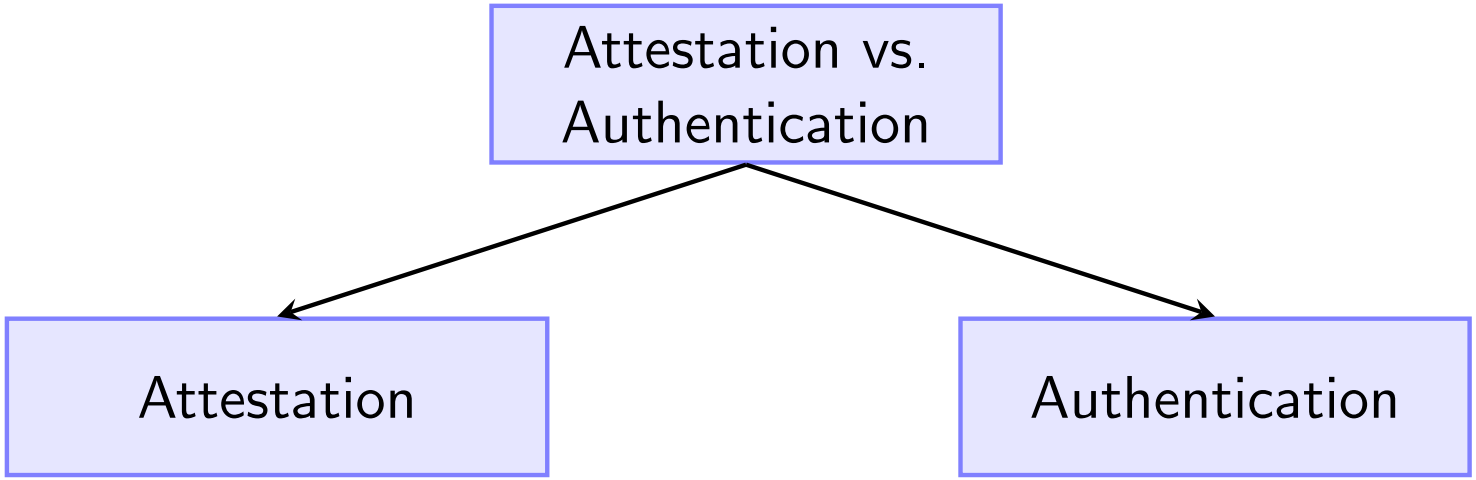
- Arto Niemi (Huawei)
- Mariam Moustafa (Aalto University)
- Tuomas Aura (Aalto University)
- Thomas Fossati (Linaro)
- Hannes Tschofenig (University of Applied Sciences Bonn-Rhein-Sieg and Siemens)
- Simon Frost (Arm)
- Ned Smith (Intel)
- Ionut Mihalcea (Arm)
- Carsten Weinhold (Barkhausen Institut)
- Michael Roitzsch (Barkhausen Institut)
- Yogesh Deshpande (Arm)
- Yaron Sheffer (Intuit)
- Tirumaleswar Reddy K. (Nokia)

Others

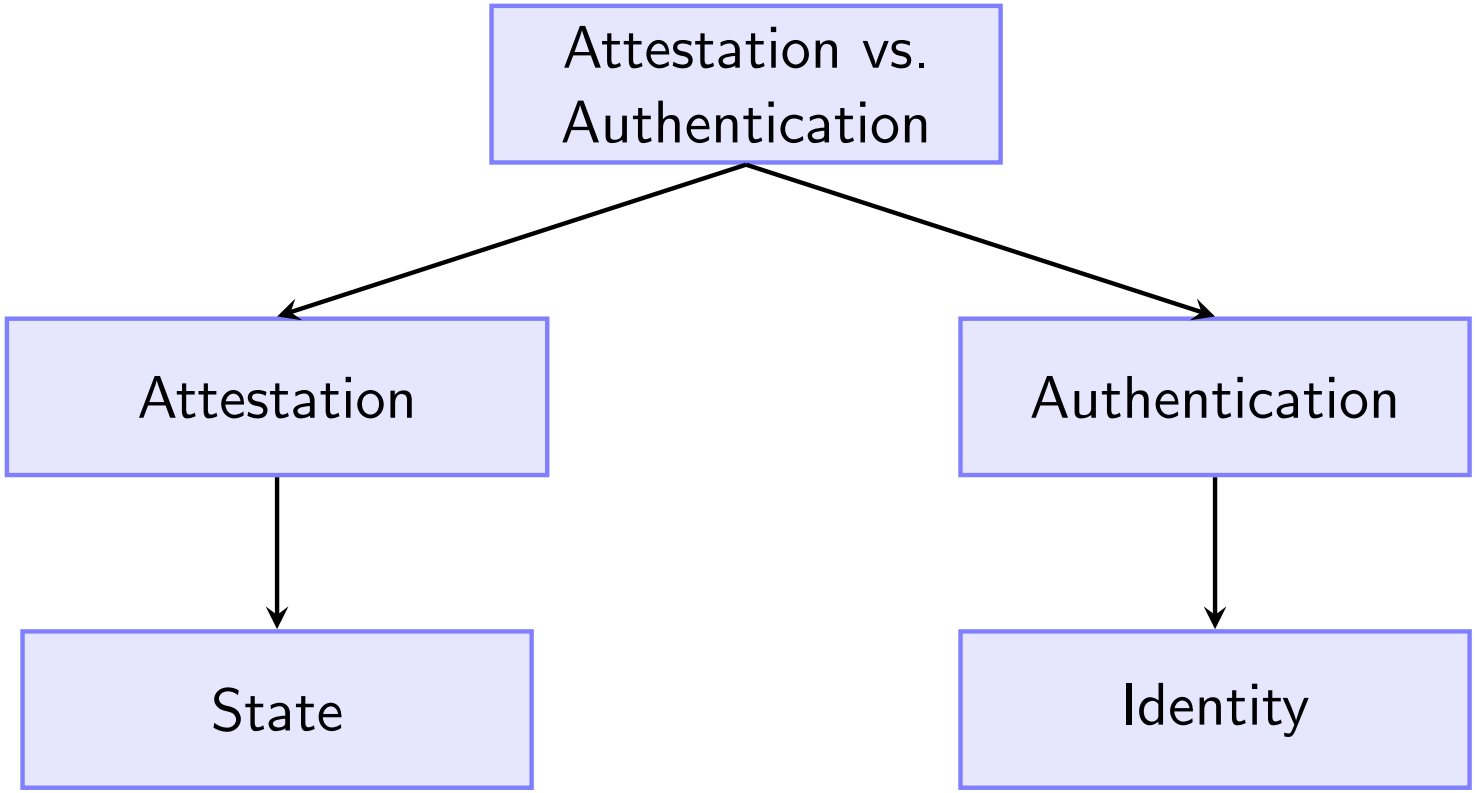
- Henk Birkholz (Fraunhofer SIT)
- Pavel Nikonorov (GENXT)
- Laurence Lundblade (Security Theory LLC)
- Dionna Amalie Glaze (Google)
- Bob Beck (Google)
- Mike Ounsworth (Entrust)
- John Preuß Mattsson (Ericsson Research)
- Cedric Fournet (Microsoft)
- Thore Sommer (TU Munich)
- Jonathan Hoyland (Cloudflare)
- Jo Van Bulck (KU Leuven)
- Jean-Marie Jacquet (University of Namur)
- Maryam Zarezadeh (Barkhausen Institut)

Outline

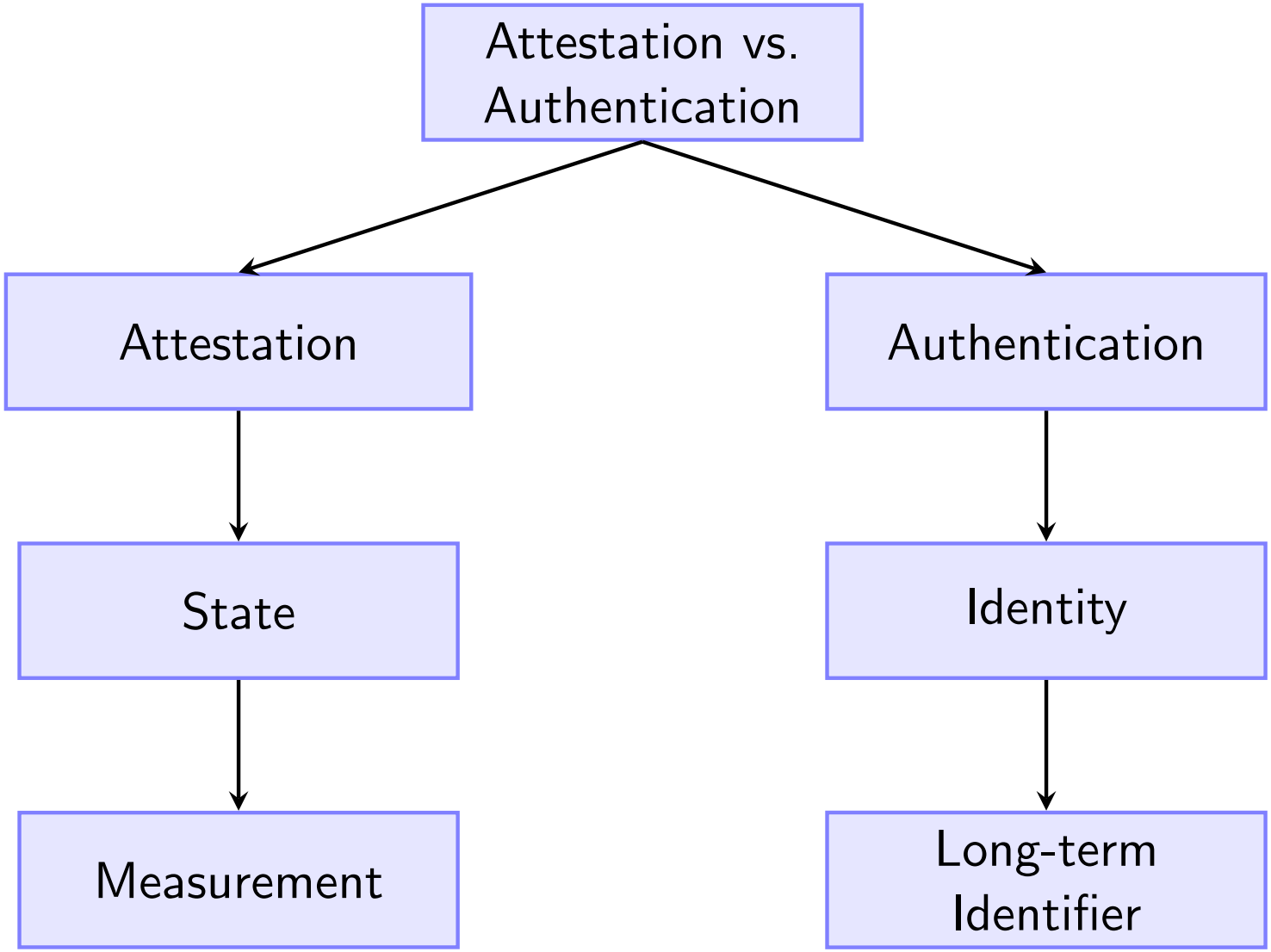
Attestation vs. Authentication



Attestation vs. Authentication



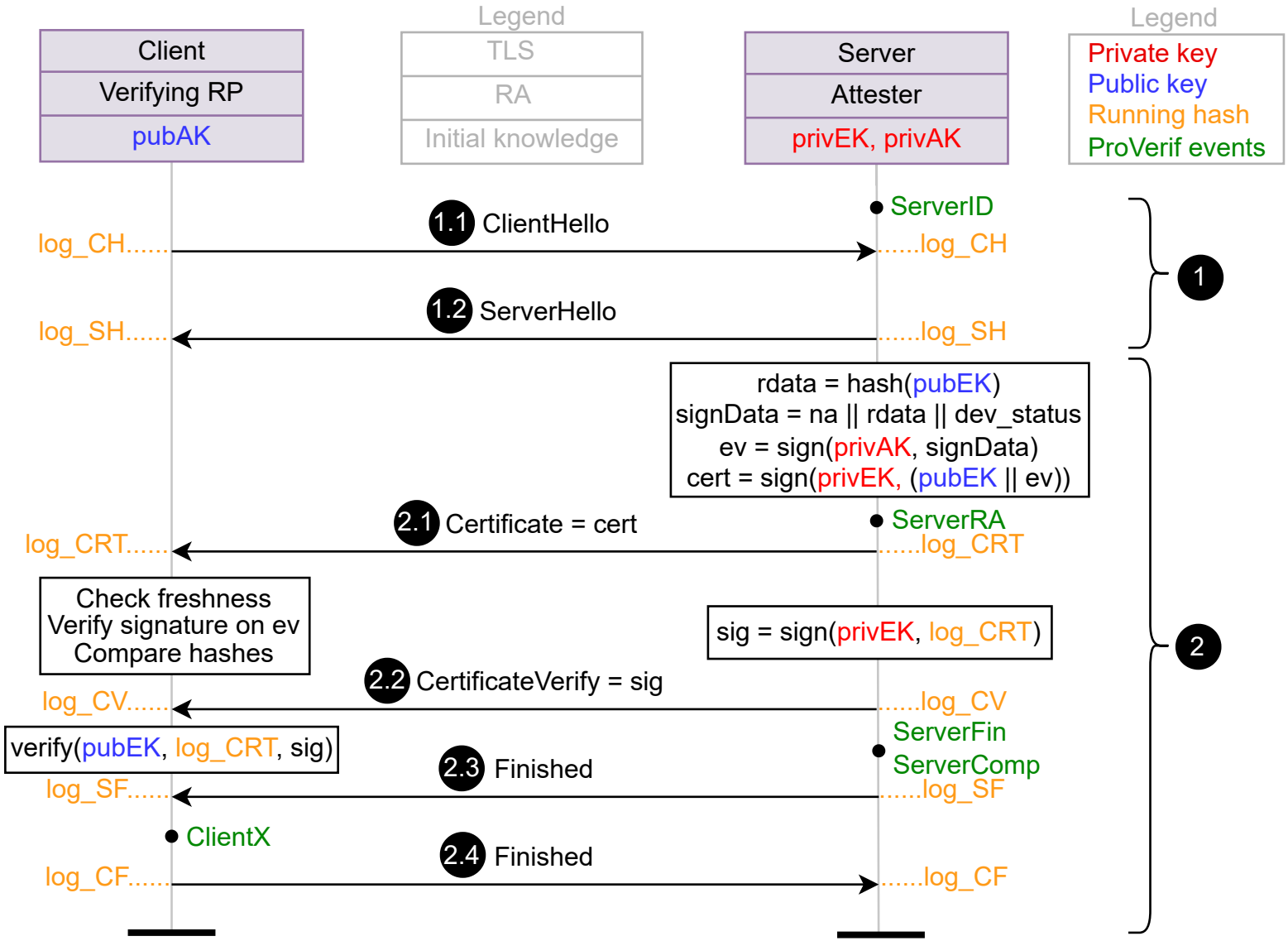
Attestation vs. Authentication



Discussion

- Platform instance identifiers and owner identity fields
  - Typically set to null
  - Operator can still provide the platform instance identifier of the compromised machine
- Security Version Numbers (SVNs)
  - Patch can be applied only when the vulnerability is known

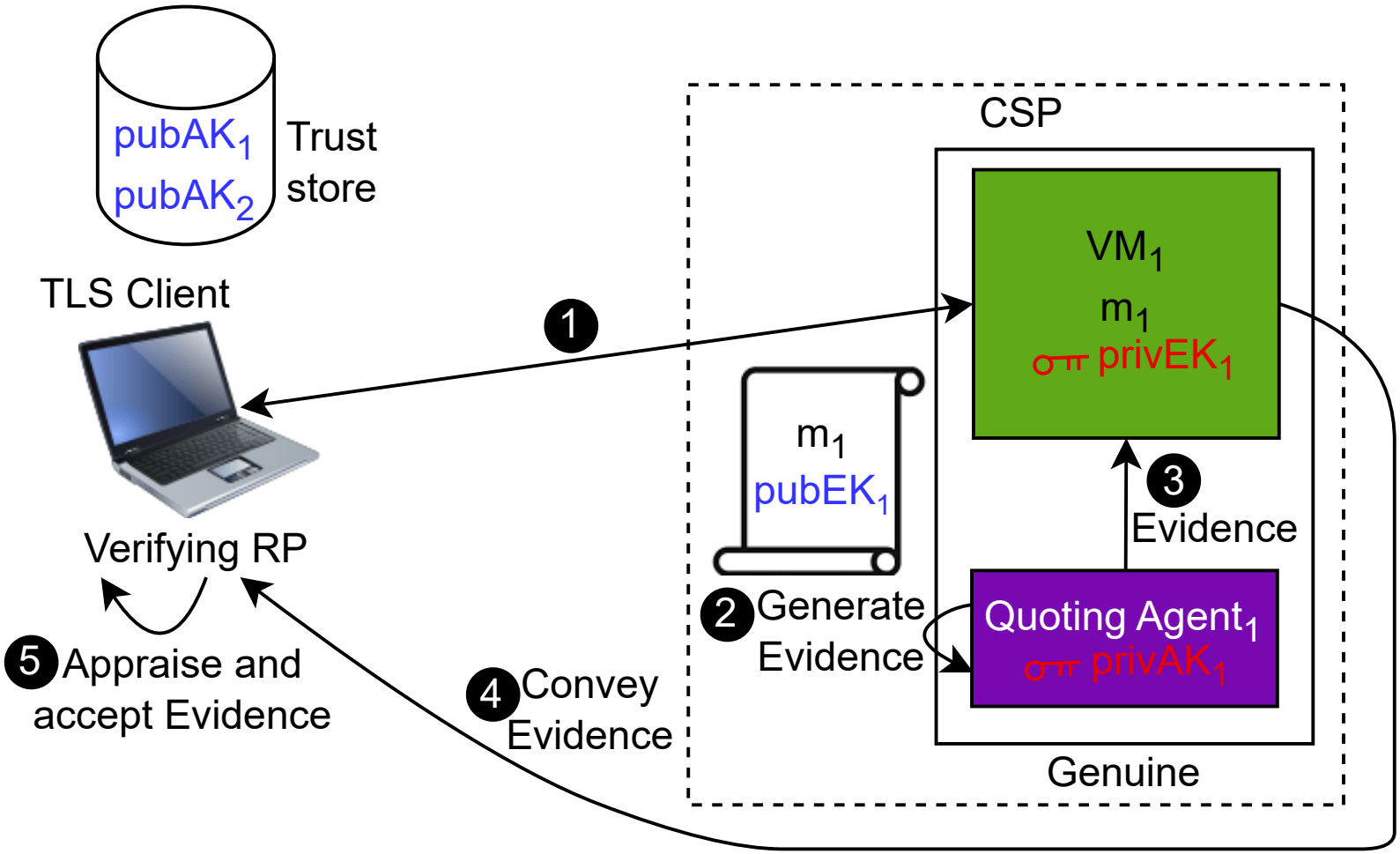
TLS-attest Protocol[11]



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

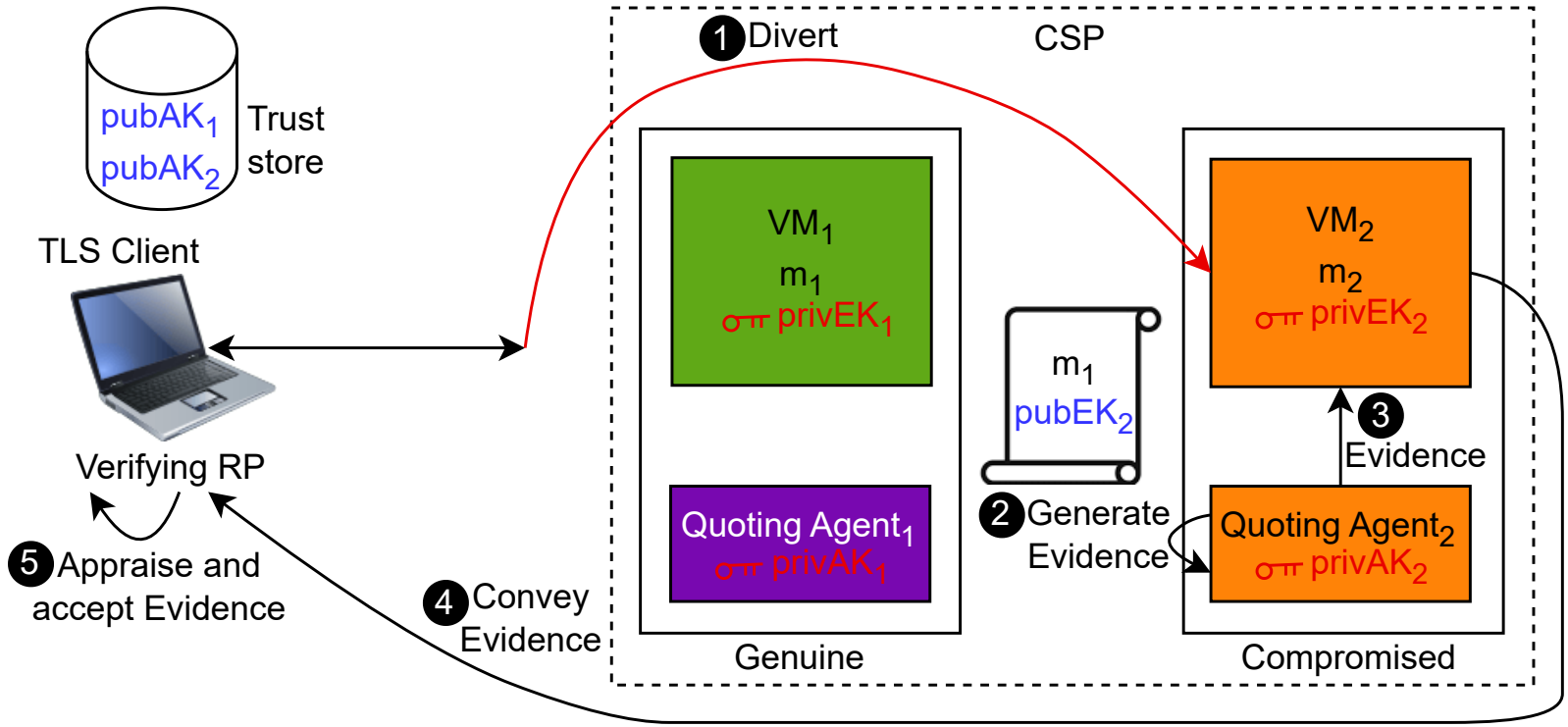
Original Path

- Quoting Agent generates Evidence.



2 Diversion Attack Within Data Center

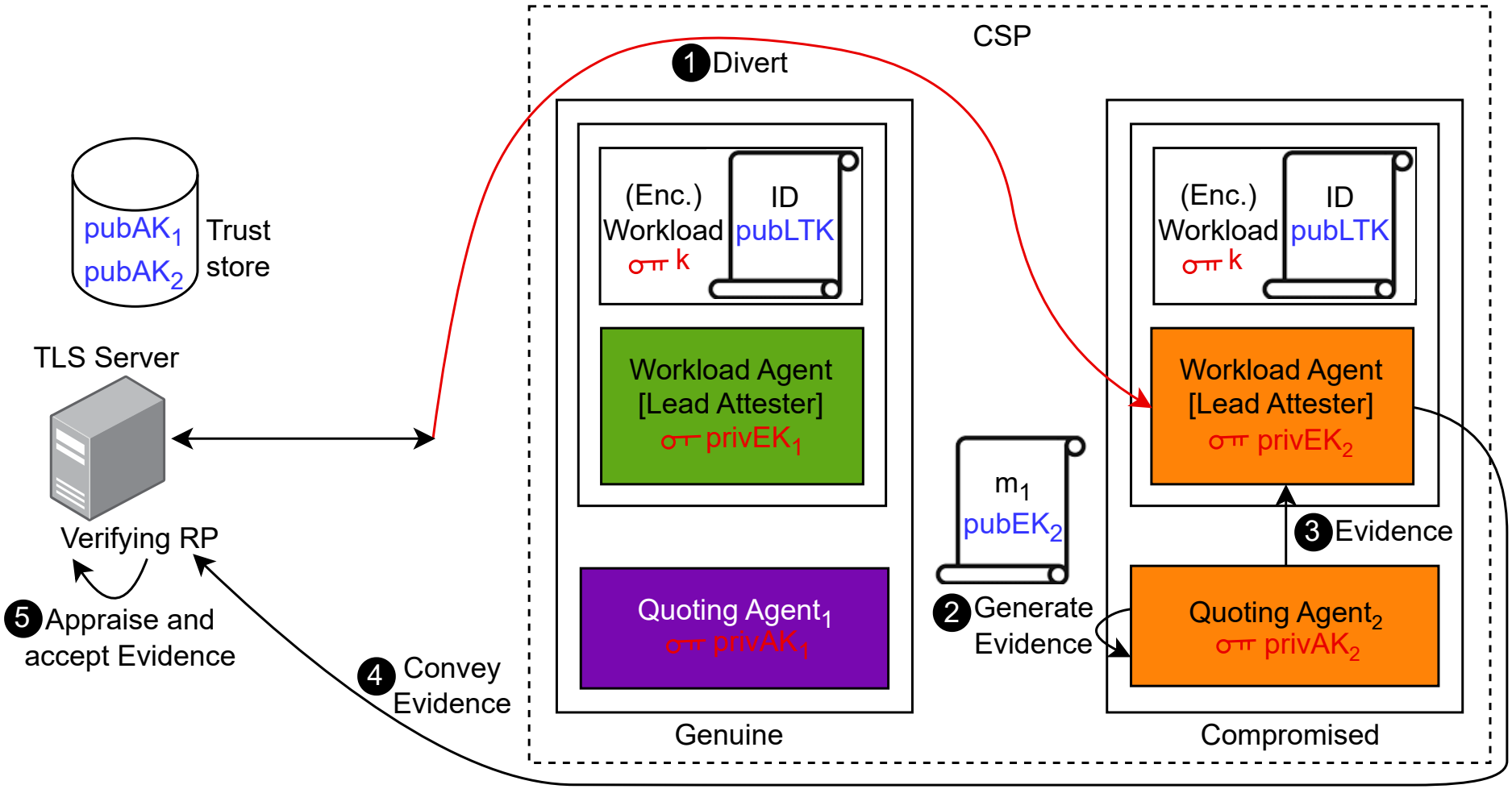
- AK of a specific machine may be compromised. (e.g., $privAK_2$)
  - Transient execution attacks, as demonstrated by Foreshadow[12]
- VM_2 impersonates VM_1



[12] 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.

Open Problem: How to Provision ID and LTK based on m?

- Confidential Containers, e.g., Trustee[13]/Key Broker Service (KBS)
- Who owns privLTK?



[13] https://github.com/confidential-containers/trustee