Identity Crisis in Attested TLS 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

July 24, 2025

CONFIDENTIAL COMPUTING CONSORTIUM

GENXT

Teleport

Outline

1. Context and Background
2. Formal Modeling
3. Potential Solutions
4. Realistic Threat Model
5. Conclusion

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
  - 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.

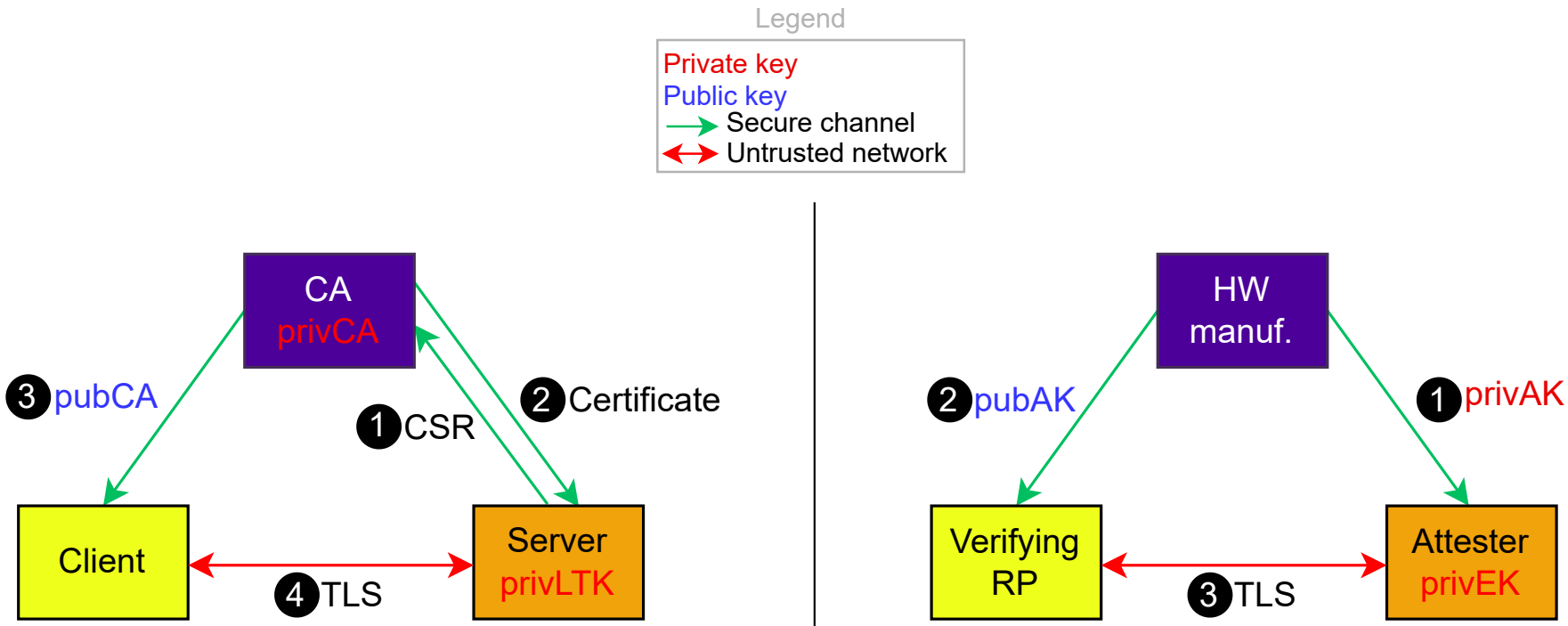
[2] `https://datatracker.ietf.org/meeting/121/materials/slides-121-tls-tls-and-attestation-00`

[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

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

ID represents Identity (SAN)

- HW manufacturer as Trust Anchor

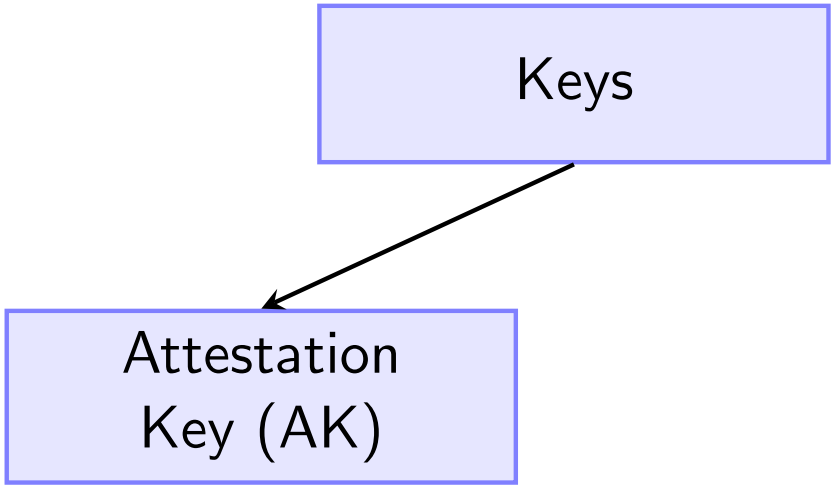
$Evidence = sign(privAK, m \parallel pubEK)$

m represents measurements

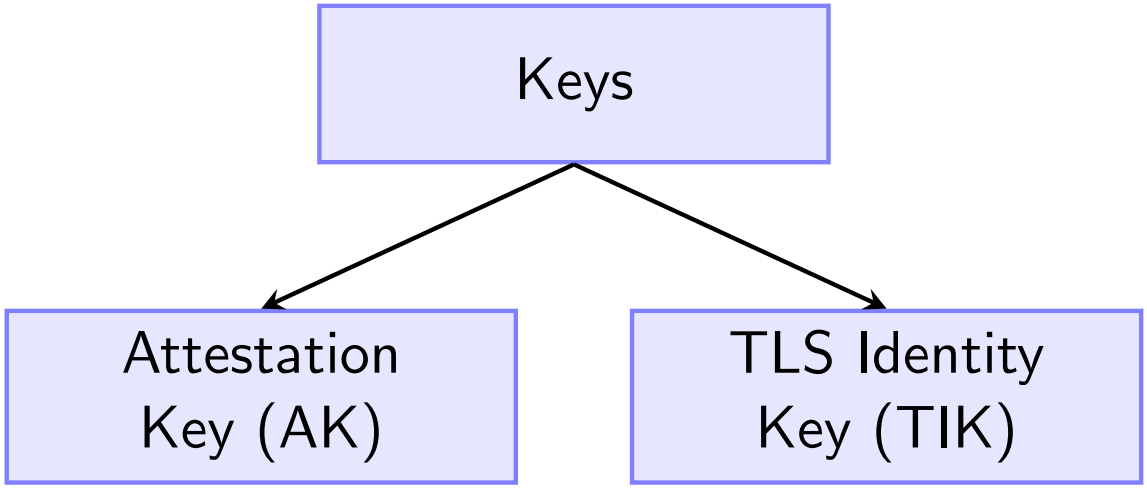
Outline

1. Context and Background
2. Formal Modeling
3. Potential Solutions
4. Realistic Threat Model
5. Conclusion

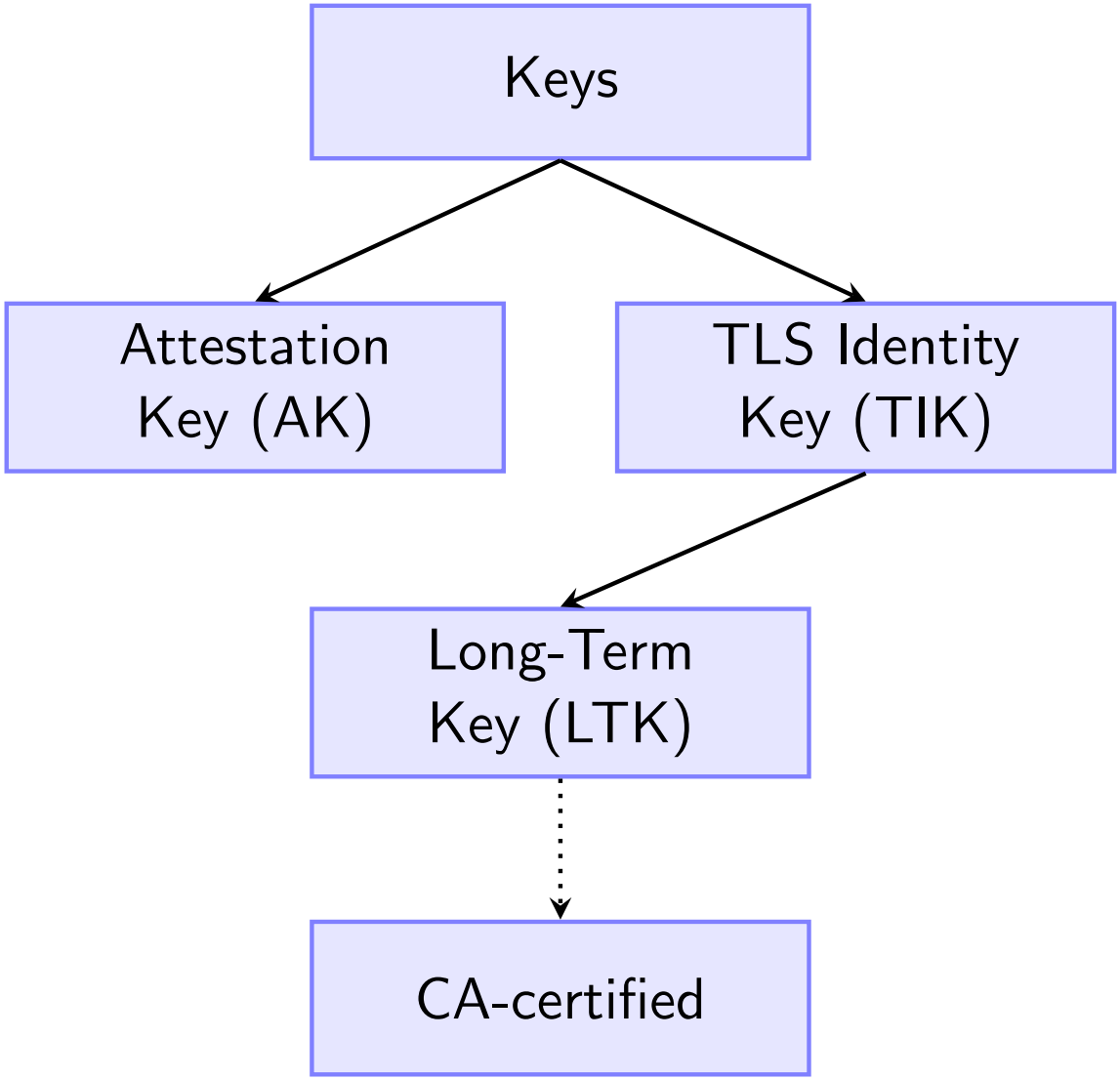
Main Keys



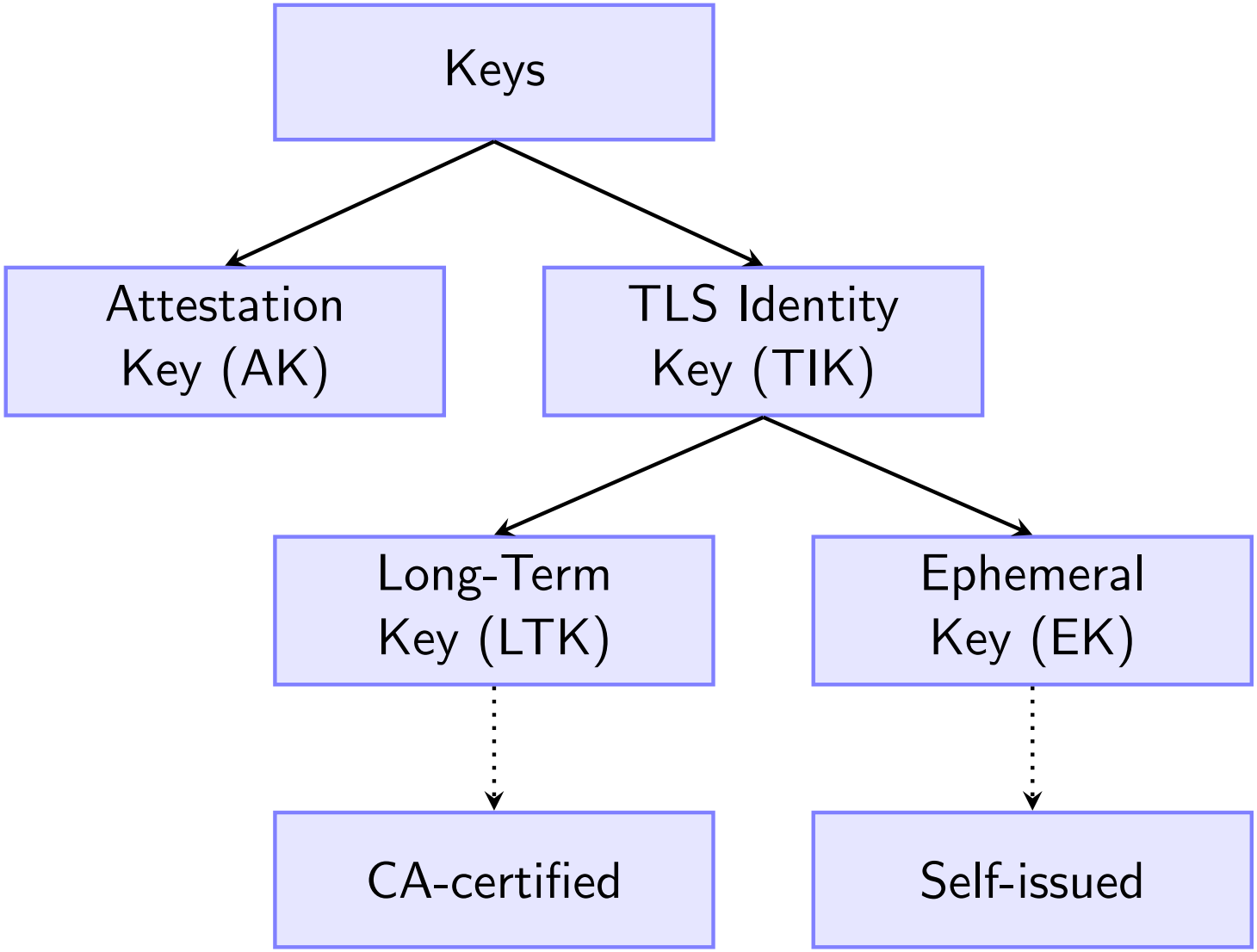
Main Keys



Main Keys


Keys
Attestation Key (AK)
TLS Identity Key (TIK)
Long-Term Key (LTK)
CA-certified

Main Keys


Keys
Attestation Key (AK)
TLS Identity Key (TIK)
Long-Term Key (LTK)
Ephemeral Key (EK)
CA-certified
Self-issued

1 Threat Model

- Standard TLS threat model (weak DH, weak hash etc.)
- Long-Term Key (privLTK) may be leaked
- Attestation Key (privAK) may be leaked (e.g., via Foreshadow[6])

[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.

1 Threat Model

- Standard TLS threat model (weak DH, weak hash etc.)
- Long-Term Key (privLTK) may be leaked
- Attestation Key (privAK) may be leaked (e.g., via Foreshadow[6])
- Assumptions (complementary to protocol design)
  - No weaknesses in the generation of Claims
  - Verifying RP provisioned with Reference Values
  - TOCTOU attacks out of the scope

[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.

2 Informal Security Goals

- Standard TLS properties, in particular Server authentication

2 Informal Security Goals

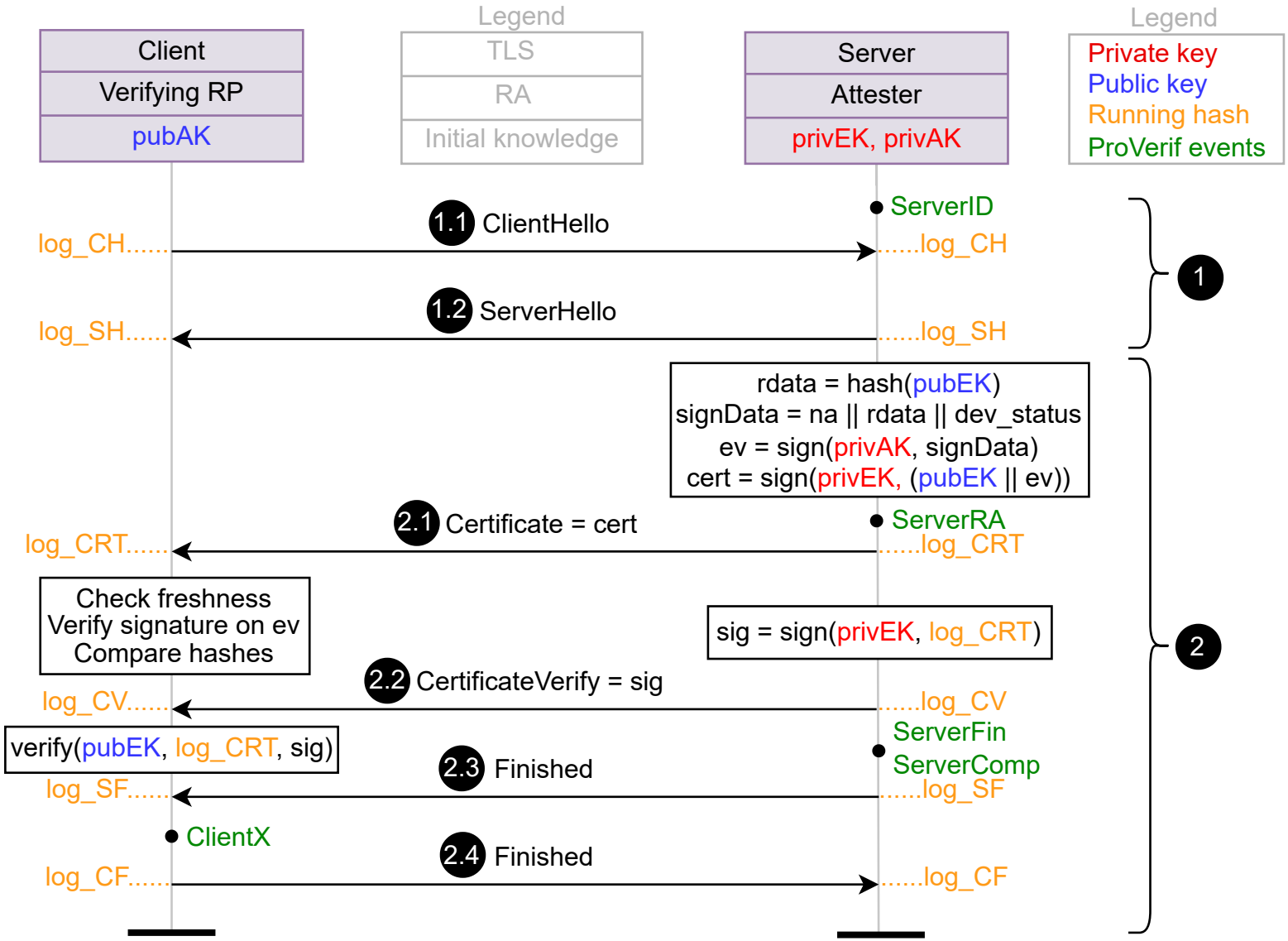
- Standard TLS properties, in particular Server authentication

- Remote Attestation
  - Integrity of *Claims*
  - Freshness of *Claims*
  - *Attestation Credential* refresh (not yet formalized)

2 Informal Security Goals

- Standard TLS properties, in particular Server authentication
- Remote Attestation
  - Integrity of *Claims*
  - Freshness of *Claims*
  - *Attestation Credential* refresh (not yet formalized)
- Composition goals
  - Binding of Remote Attestation and TLS
    - Binding *Evidence* to TLS session: *Evidence* should not be usable in other sessions.
  - *Evidence* is generated by the same server that is authenticated.

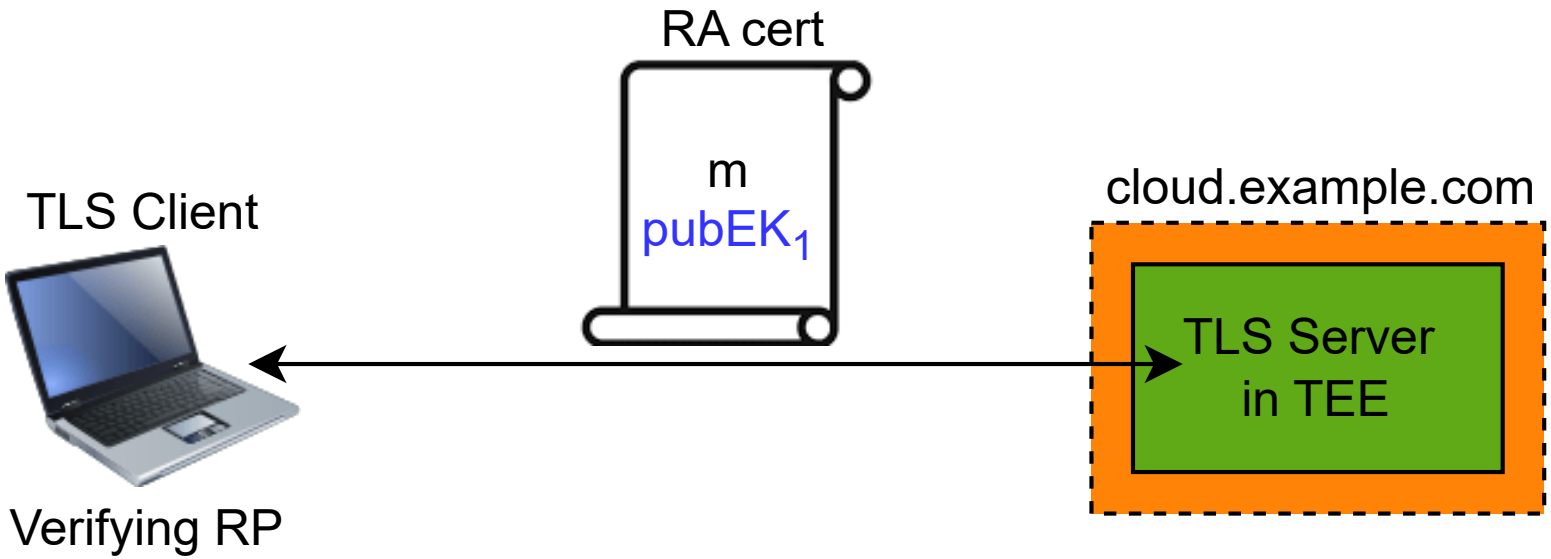
3 Protocol Diagram[7]



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

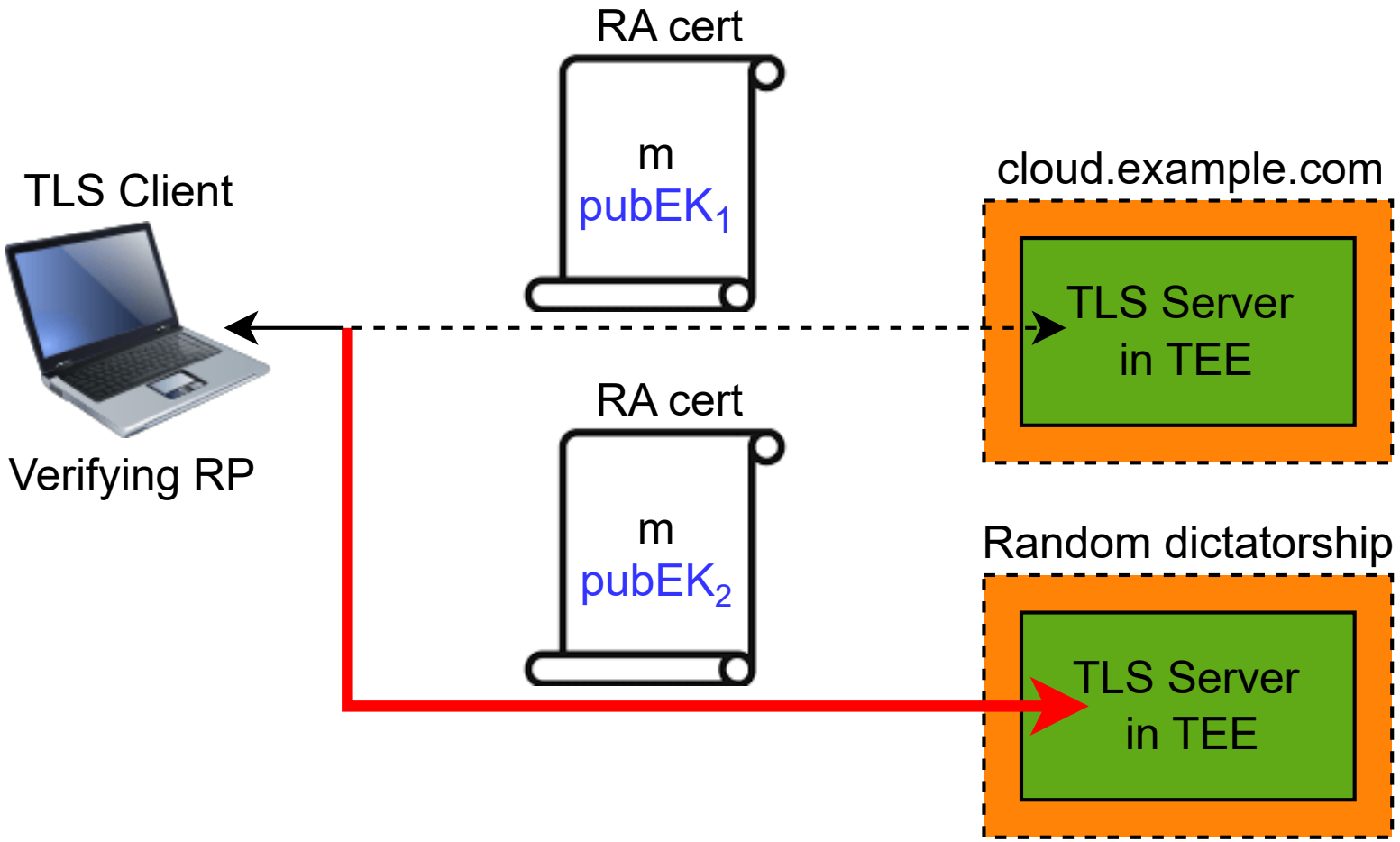
Remote Attestation-only (§6.1 in I-D)

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



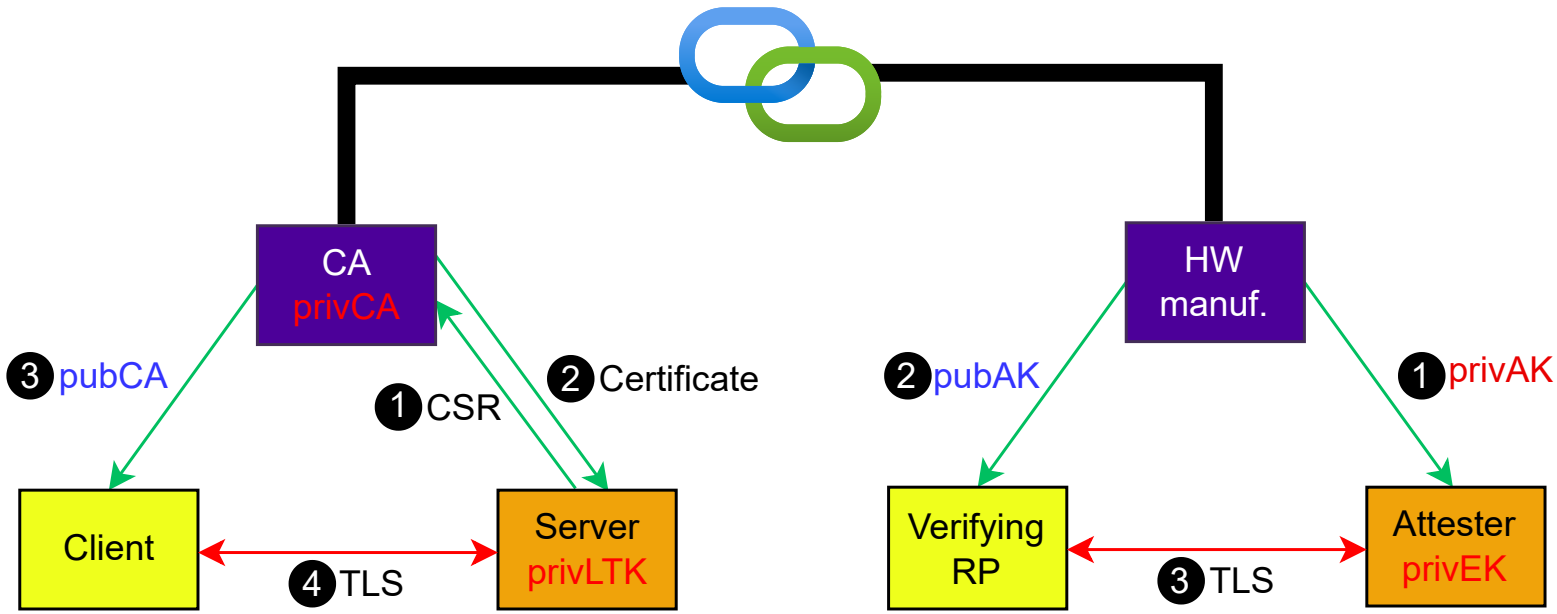
Problem with Remote Attestation-only

- 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!

Outline

1. Context and Background
2. Formal Modeling
3. Potential Solutions
4. Realistic Threat Model
5. Conclusion

Potential Solutions

Intra-Handshake Attestation

1. Modify CertificateVerify message
2. Allow multiple CertificateVerify messages
3. Channel binder requiring key schedule changes
4. New Attestation message
5. New signature algorithm

Post-Handshake Attestation[a]

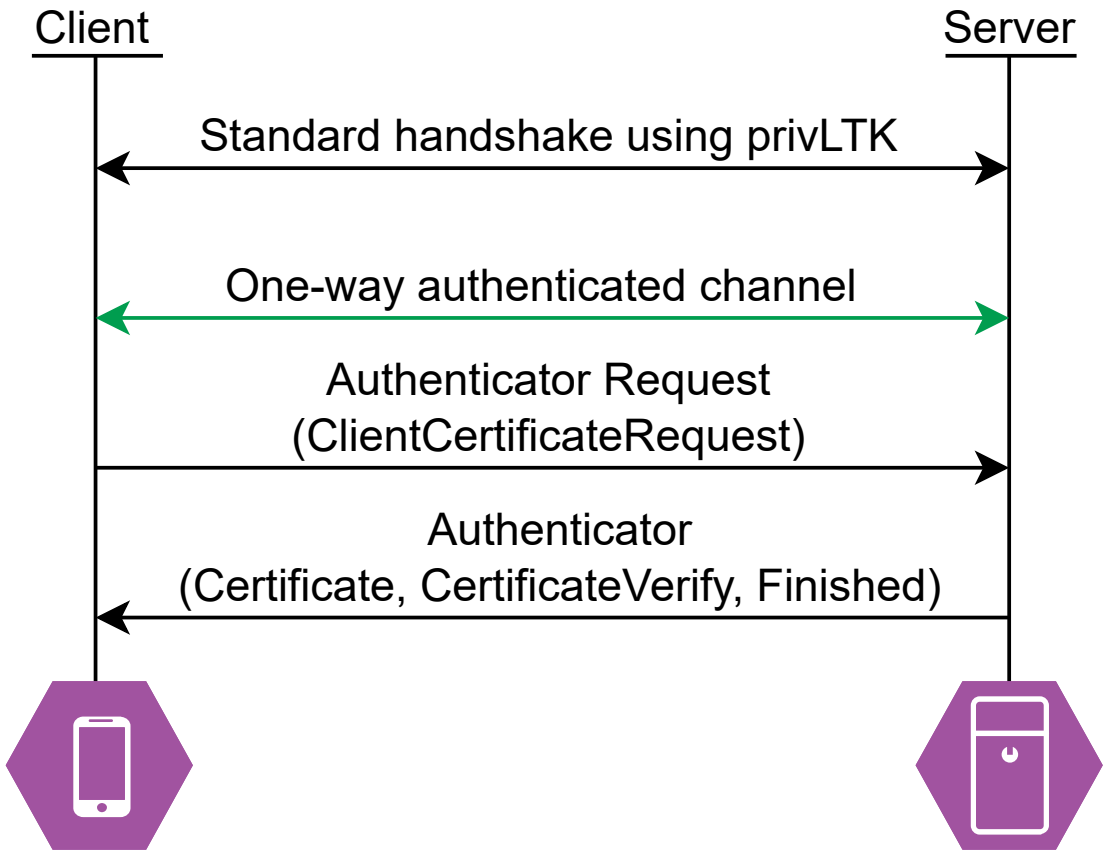
- Based on RFC9261[b]
- Server as Attester

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

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

Exported Authenticators[8] (RFC 9261)

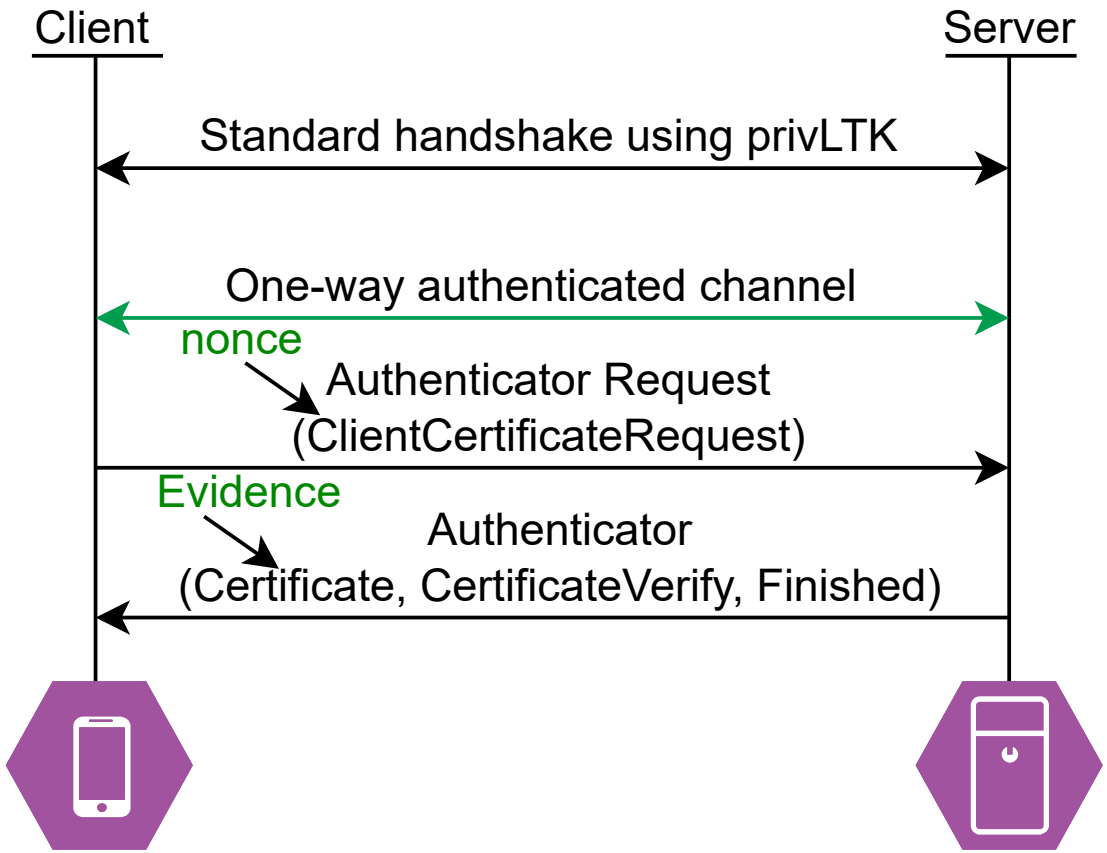
- ClientCertificateRequest: Similar to CertificateRequest
- Authenticator Keys via Exporters



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

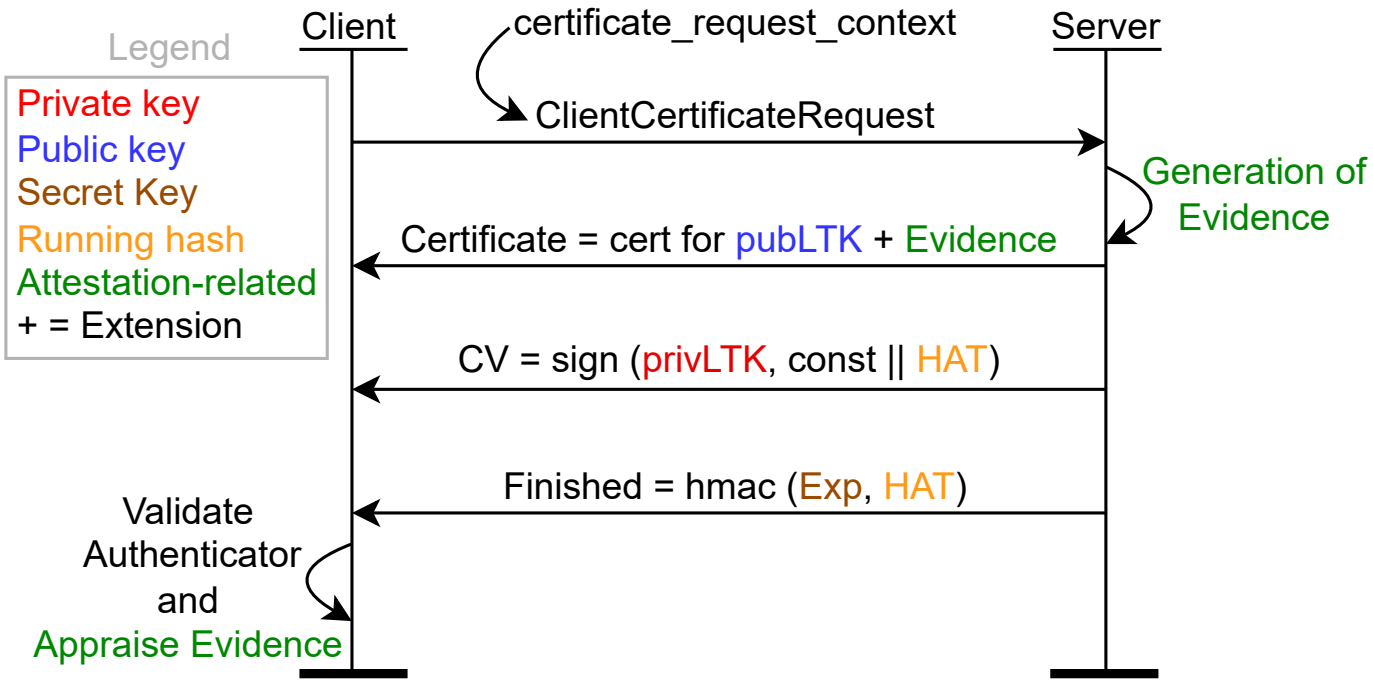
Initial Proposal

- No change in TLS handshake protocol
- Example: TLS Server as RATS Attester



Protocol Diagram (Post-handshake Flow)

1. Authenticator Request
   - Unique *certificate_request_context* within connection
2. Evidence based on this context and *Exported Keying Material (EKM)*
3. Authenticator
   - Certificate message extended with Evidence
   - CertificateVerify as in RFC 9261
   - Finished as in RFC 9261
4. Validation: additionally appraise Evidence



Outline

1. Context and Background
2. Formal Modeling
3. Potential Solutions
4. Realistic Threat Model
5. Conclusion

Can Cloud Service Provider (CSP) *really* be out of TCB?

- In all public cloud 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

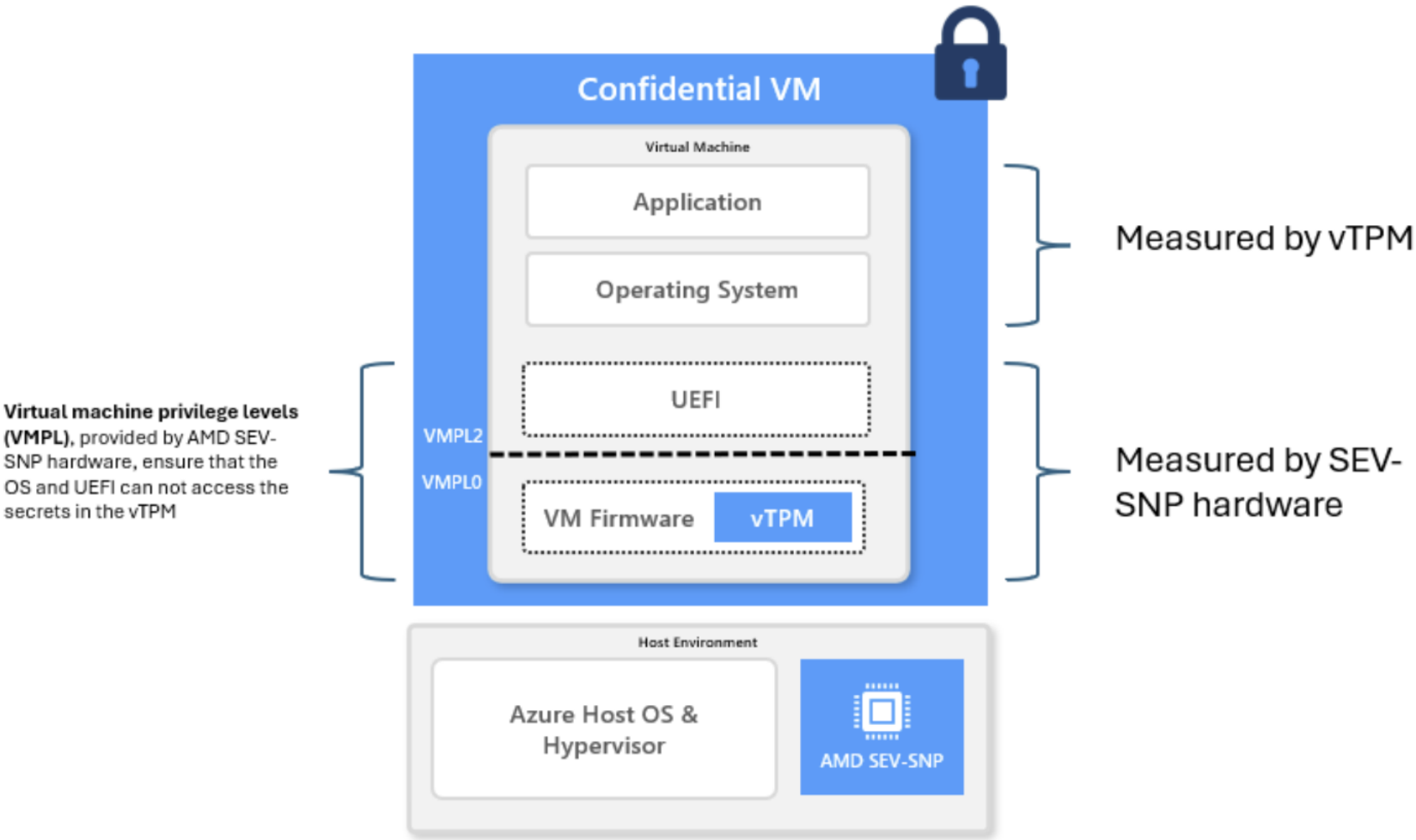
Can CSP *really* be out of TCB?

- 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

Outline

1. Context and Background
2. Formal Modeling
3. Potential Solutions
4. Realistic Threat Model
5. Conclusion

Summary

- Threat model claimed by Confidential Computing Consortium is trivially broken.
- Post-handshake is a more suitable candidate for use cases requiring runtime posture assessment.
- Several corner cases; hence formal analysis is required
- Huge usability barriers in tools
- Work-in-progress
  - Formal modeling of post-handshake proposal
  - Make ProVerif accessible for designers

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.