Identity Crisis in Attested TLS for Confidential Computing

Muhammad Usama Sardar[1] and Tuomas Aura[2]

[1]TU Dresden, Germany

[2]Aalto University, Espoo, Finland

February 25, 2025

Outline

Main Motivation

3 Adopted SIG projects

Main Motivation

3 Adopted SIG projects

Standardization

Main Motivation

3 Adopted SIG projects

Standardization

- FV as part of TLS WG adoption process[1]

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

Goal

Secure channel should terminate inside the TEE

Attested TLS (Server as Attester)

- Client as Verifying Relying Party

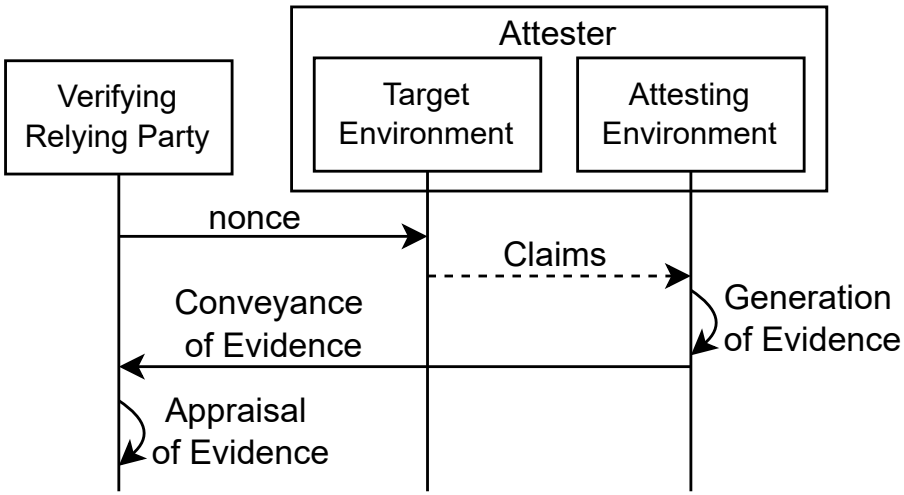


Figure: Remote Attestation

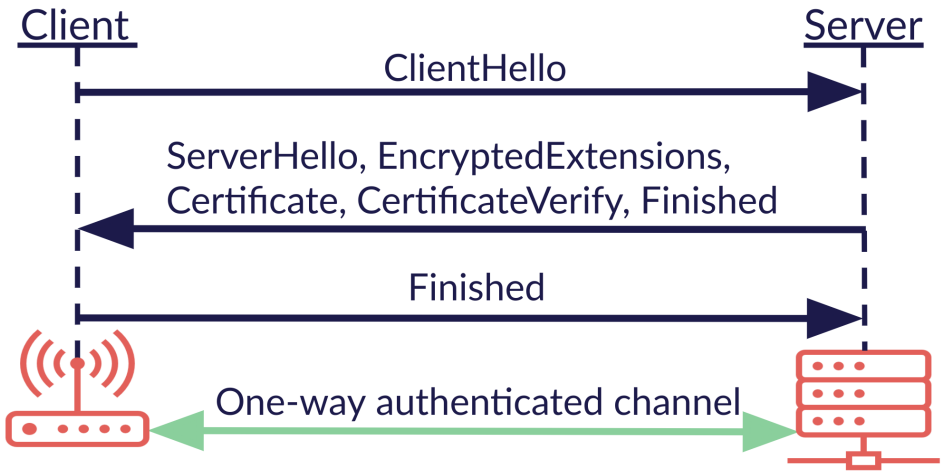
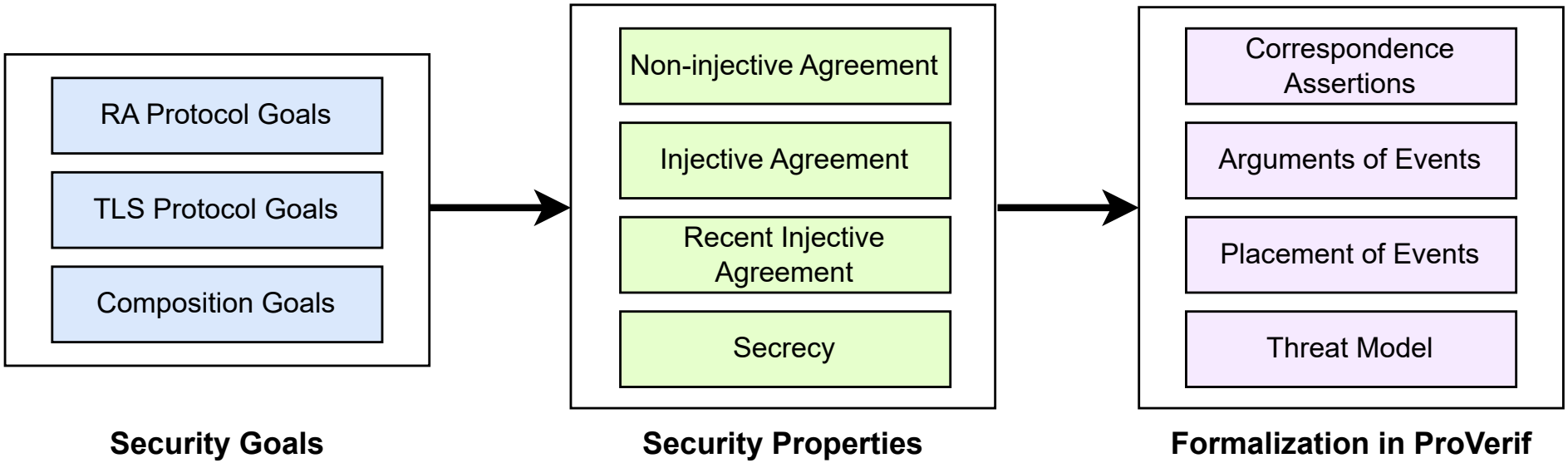


Figure: TLS 1.3

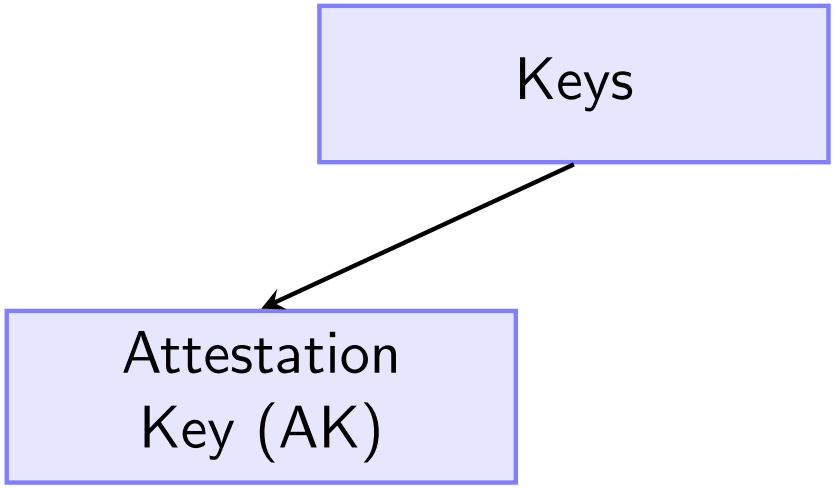
Approach



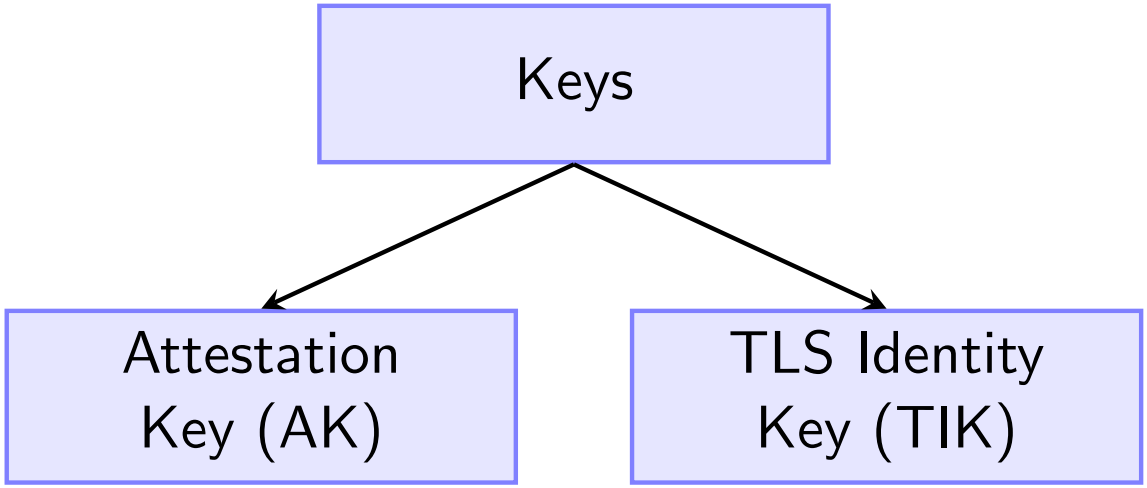
Future Goal: Modularity: TLS replaceable by Noise, EDHOC etc.

Outline

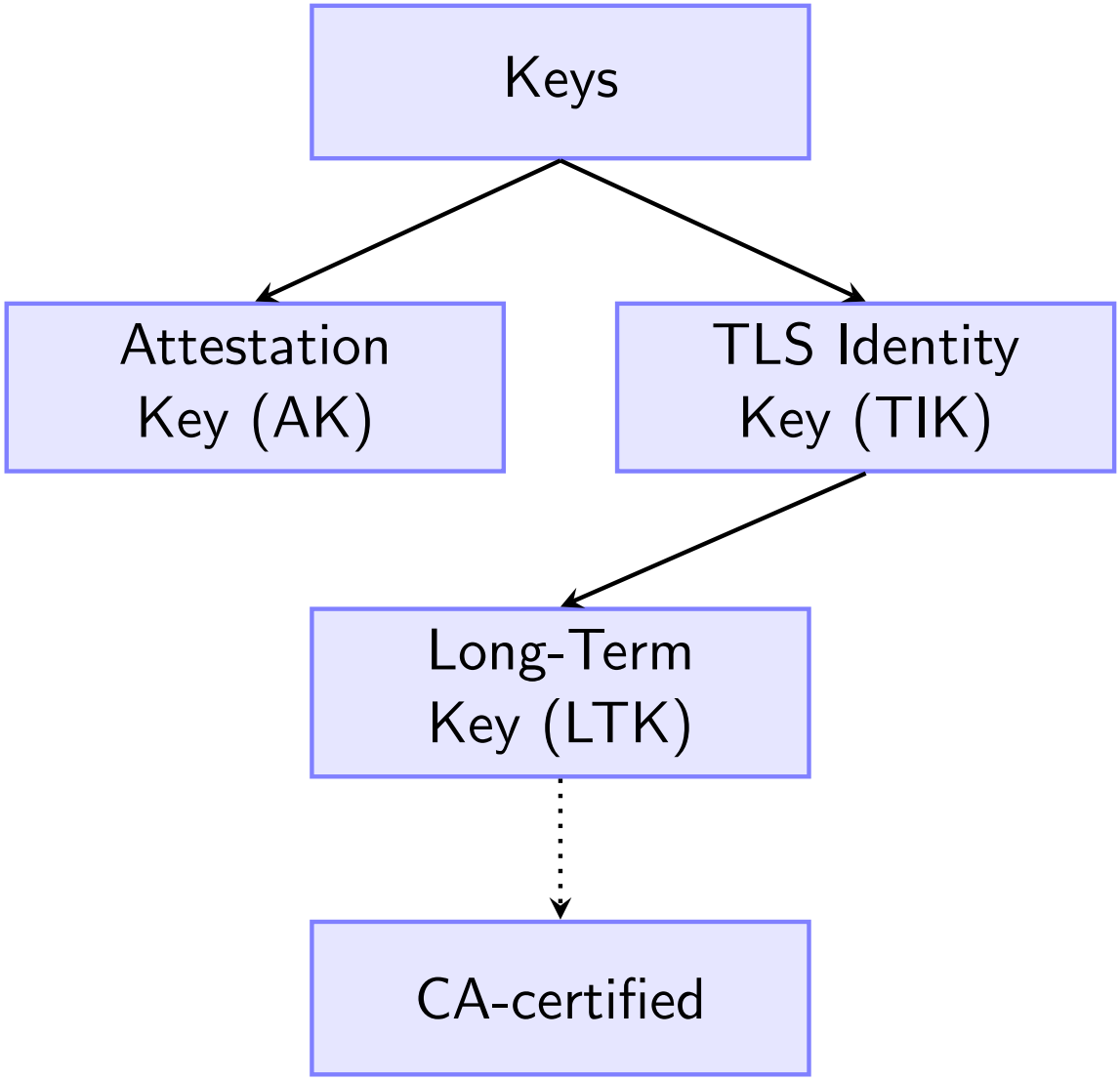
Main Keys



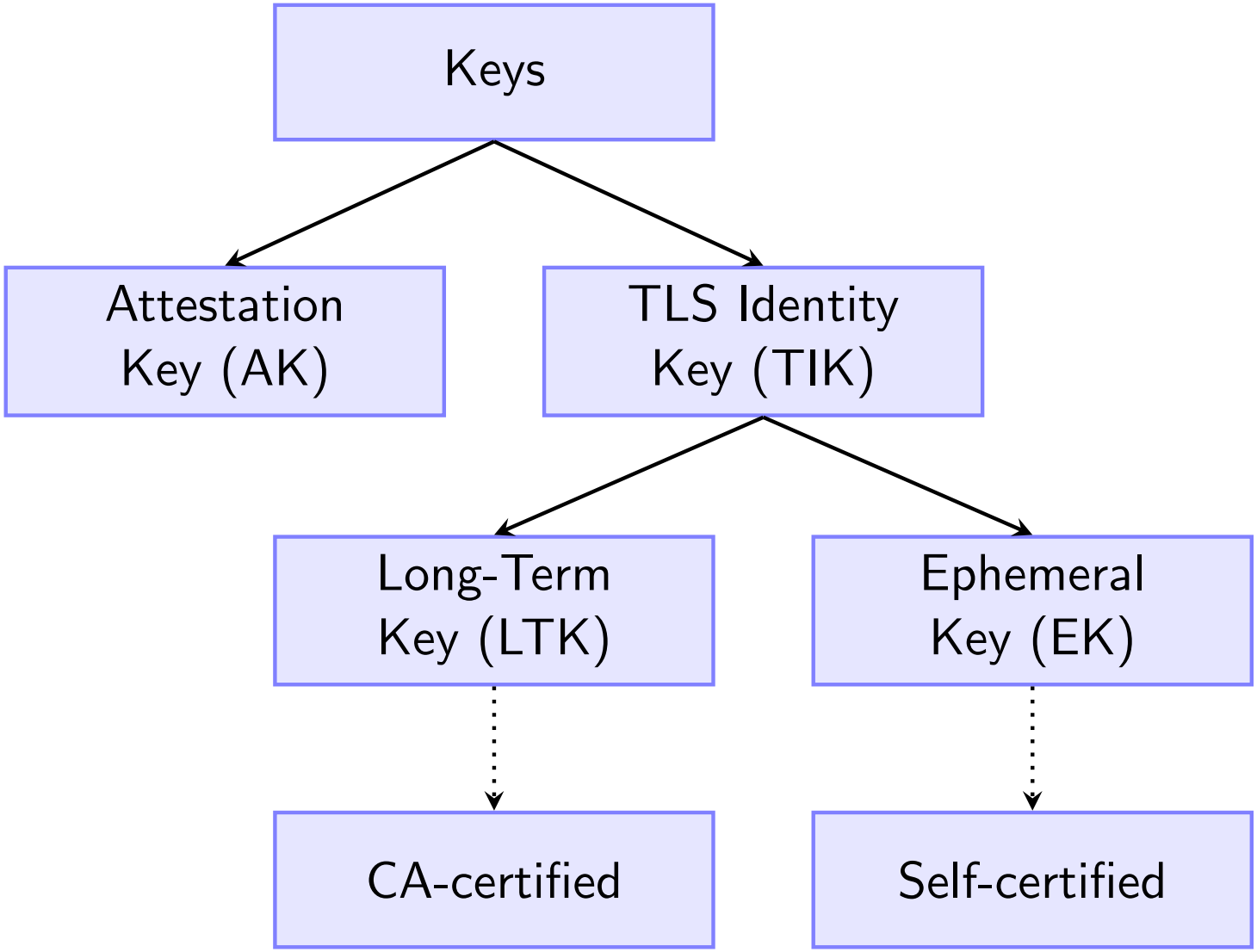
Main Keys



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-certified

Threat Model for AK

- Fine-grained threat model

Threat Model for AK

- Fine-grained threat model
  - Previous[2]: No AK is compromised.

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

Threat Model for AK

- Fine-grained threat model
  - Previous[2]: No AK is compromised.
  - Now: AK of some specific machines may be compromised.

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

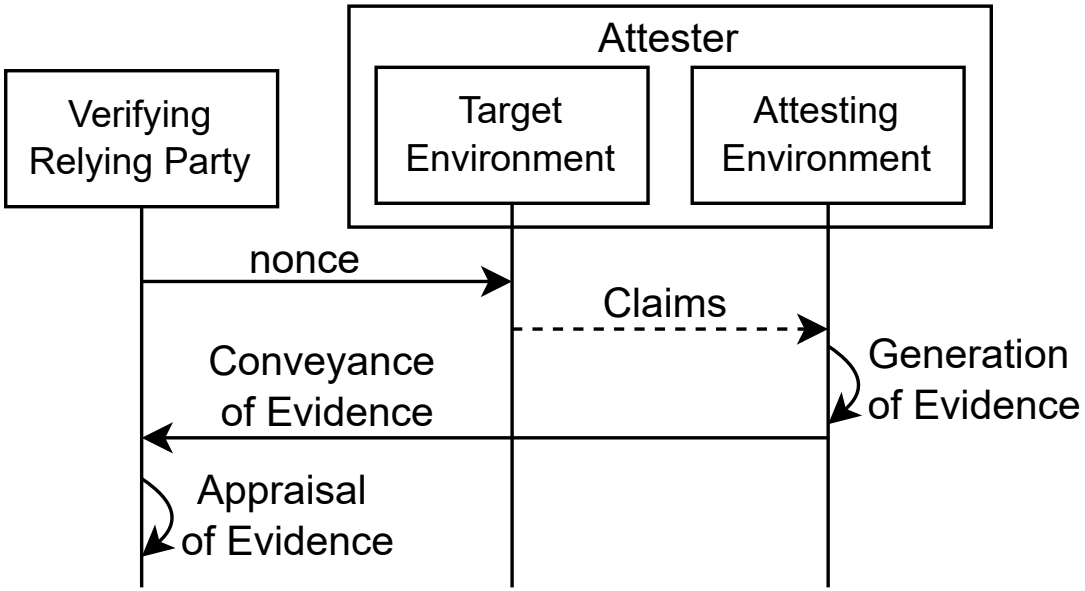
Threat Model for AK

- Fine-grained threat model
  - Previous[2]: No AK is compromised.
  - Now: AK of some specific machines may be compromised.
    - Transient execution attacks, as demonstrated by Foreshadow[3]

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

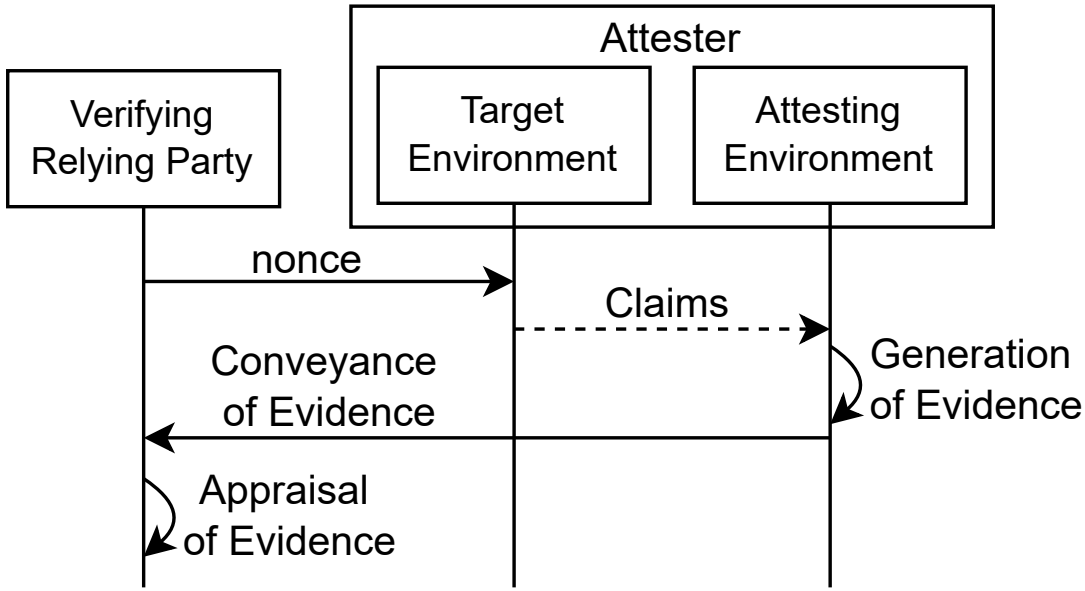
[3] Van Bulck, Minkin, Weisse, Genkin, Kasikci, Piessens, Silberstein, Wenisch, Yarom, and Strackx, "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution", 2018.

Assumptions



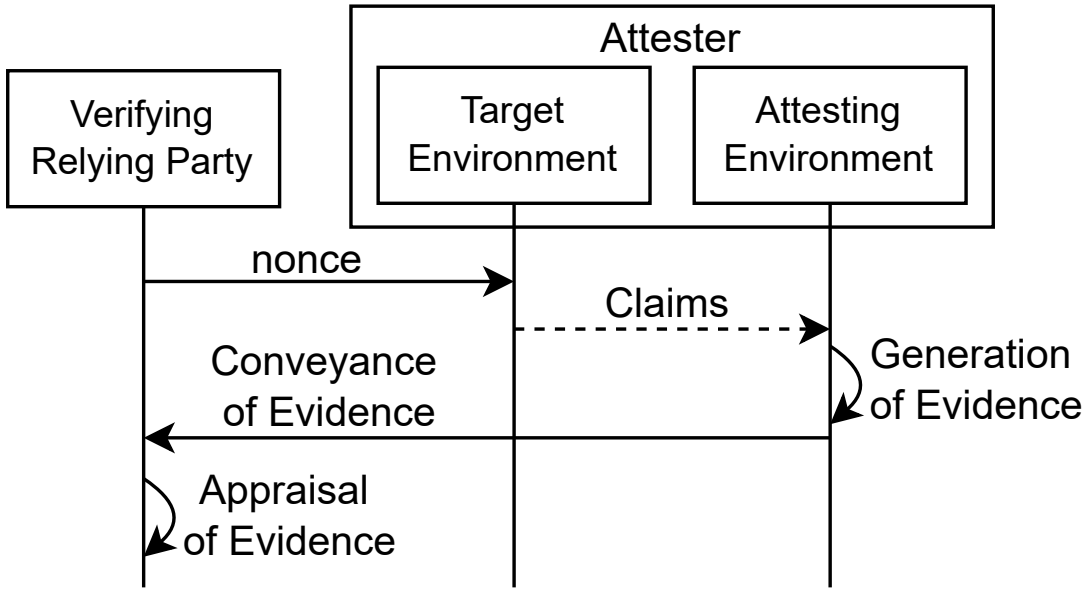
- Secure channel between AE and TE already exists.

Assumptions



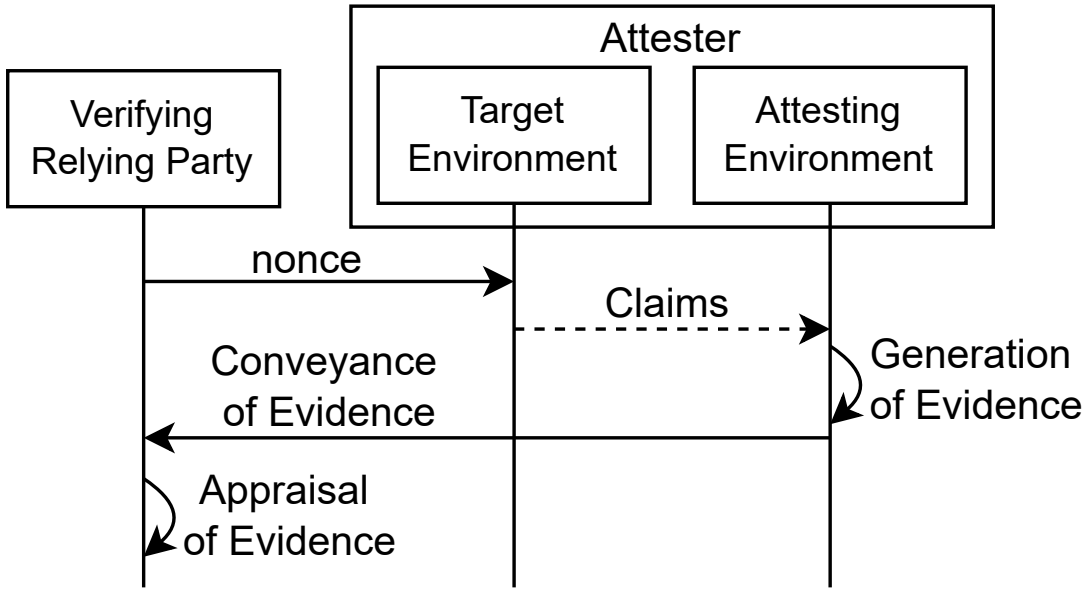
- Secure channel between AE and TE already exists.
- Sampling and collection of claims for TE is perfectly done.

Assumptions



- Secure channel between AE and TE already exists.
- Sampling and collection of claims for TE is perfectly done.
- Everything in TCB from HW to Workload is measured.

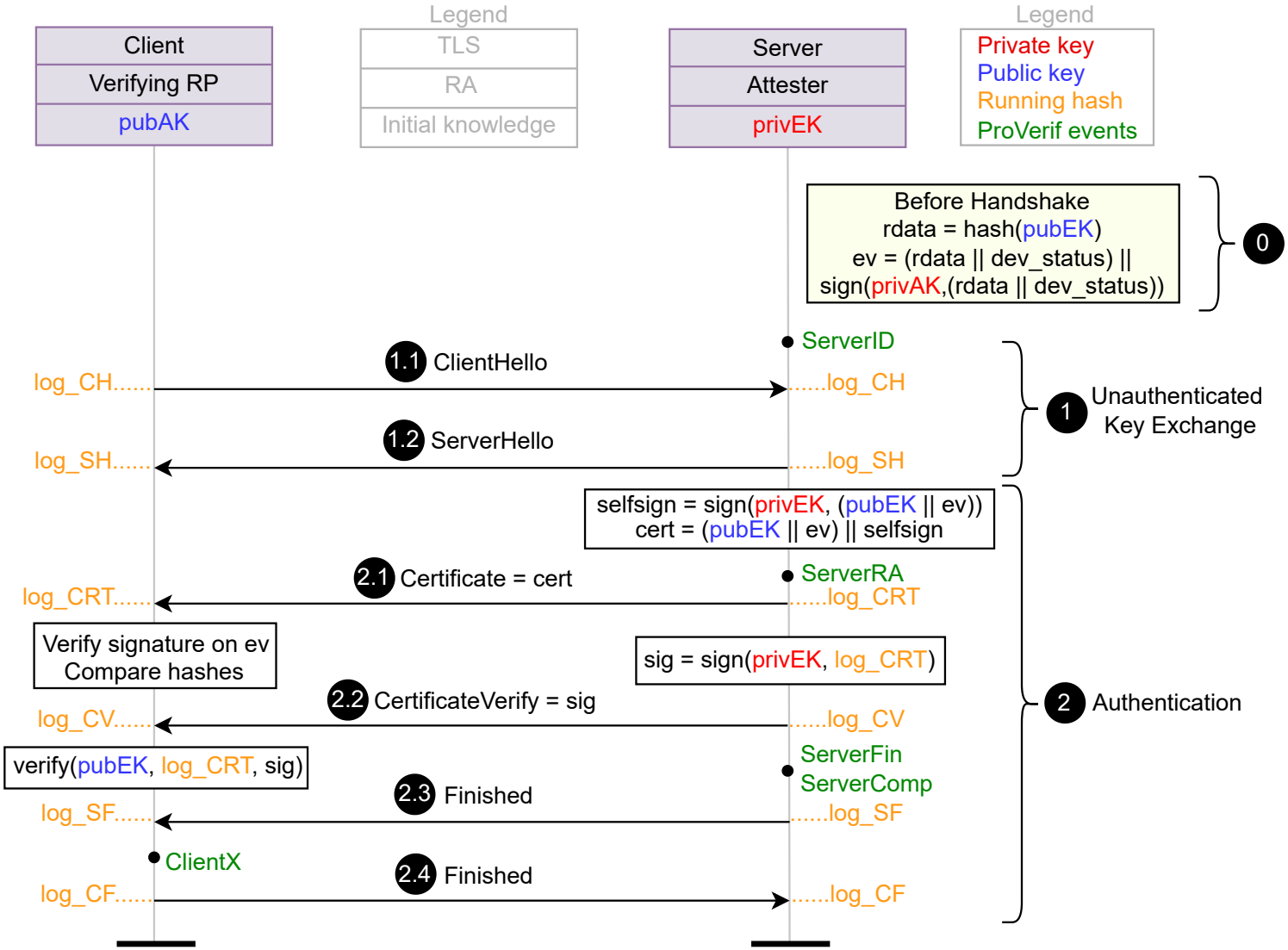
Assumptions



- Secure channel between AE and TE already exists.
- Sampling and collection of claims for TE is perfectly done.
- Everything in TCB from HW to Workload is measured.
- Time-Of-Check-to-Time-Of-Use (TOCTOU) attacks out of scope

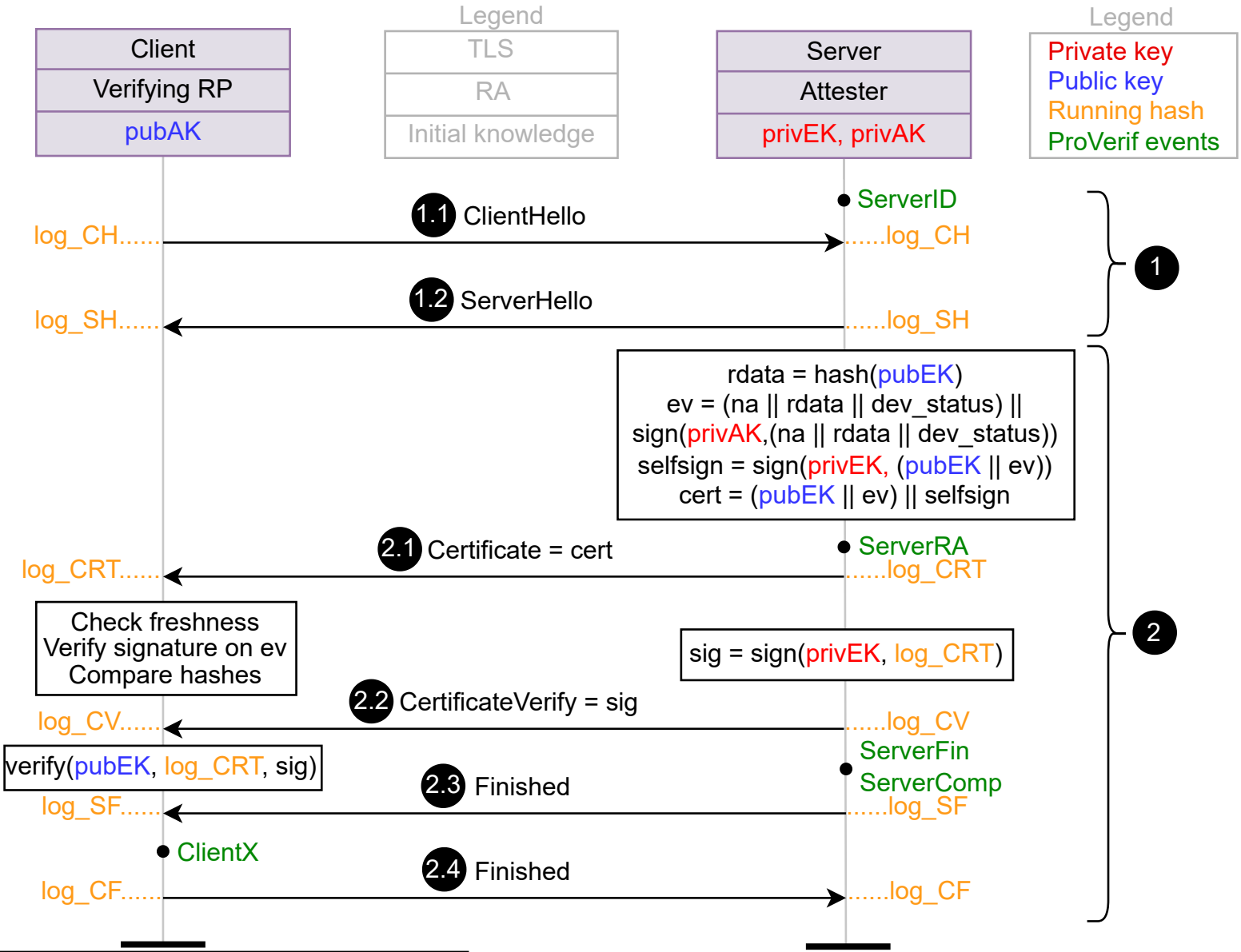
Outline

SIG Project 1: IRA-TLS[4]



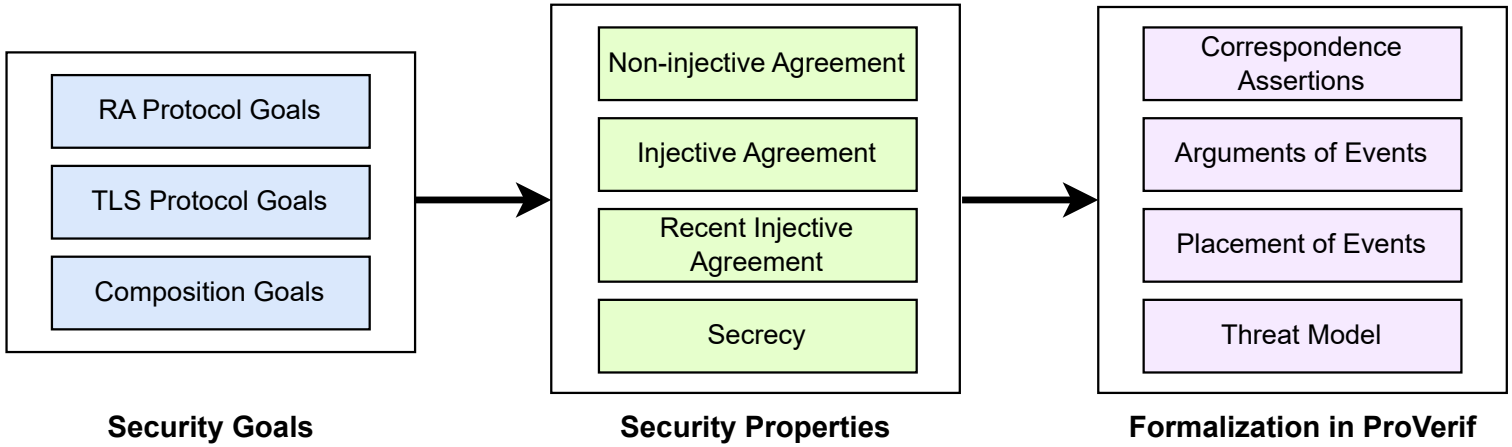
[4] https://github.com/ccc-attestation/interoperable-ra-tls

SIG Project 2: TLS-a[5]



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

Results

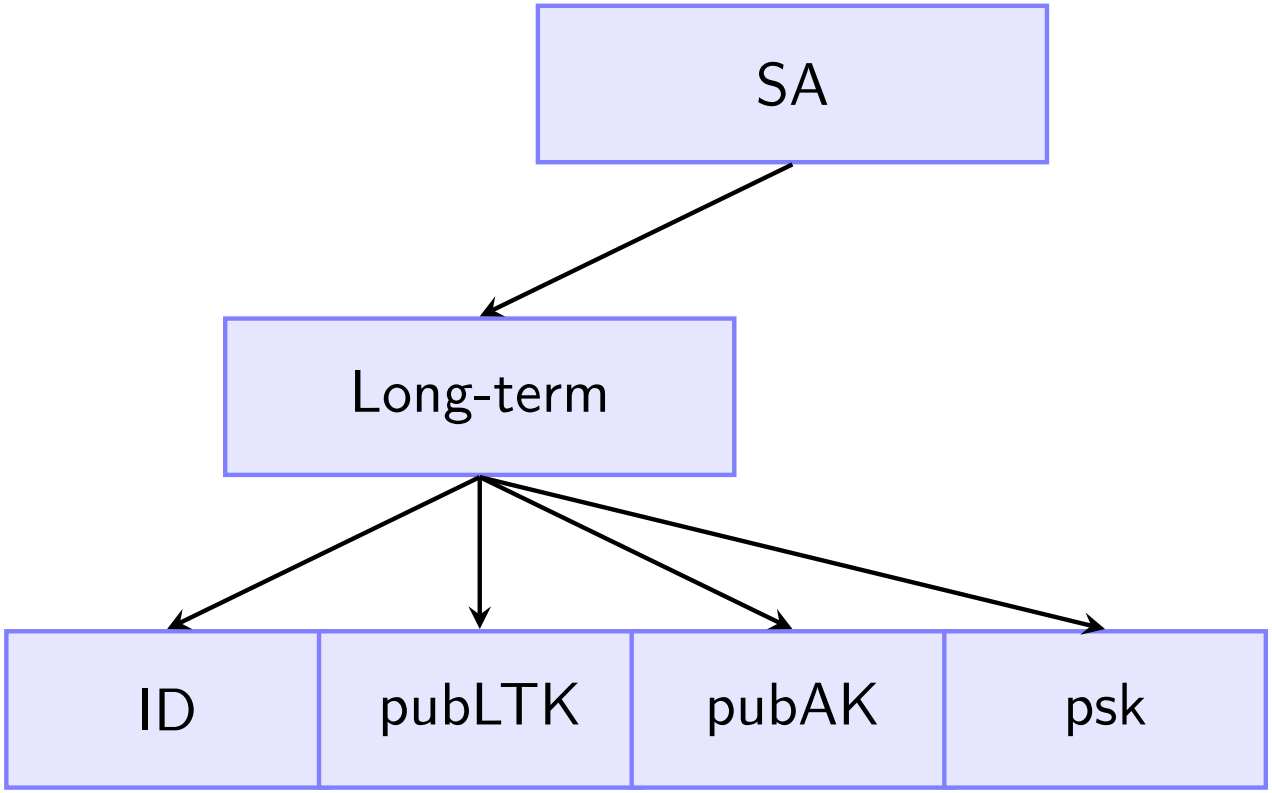


S. No.	Security goal	ProVerif property	IRA-TLS[6]	TLS-a[7]
1	**G-RA1**: Integrity of Evidence	IE	✓	✓
2	**G-RA2**: Freshness of Evidence	FE	×	✓
3	**G-RA3**: Secrecy of Attestation Keys	SK	✓	✓
4	**G-TLS1**: Server Identity	SI	×	×
5	**G-TLS2**: Server Authentication	SA	×	×
6	**G-C1**: Compound Authentication	CA	×	×
7	**G-C2**: Agreement of All Parameters	CP	×	×

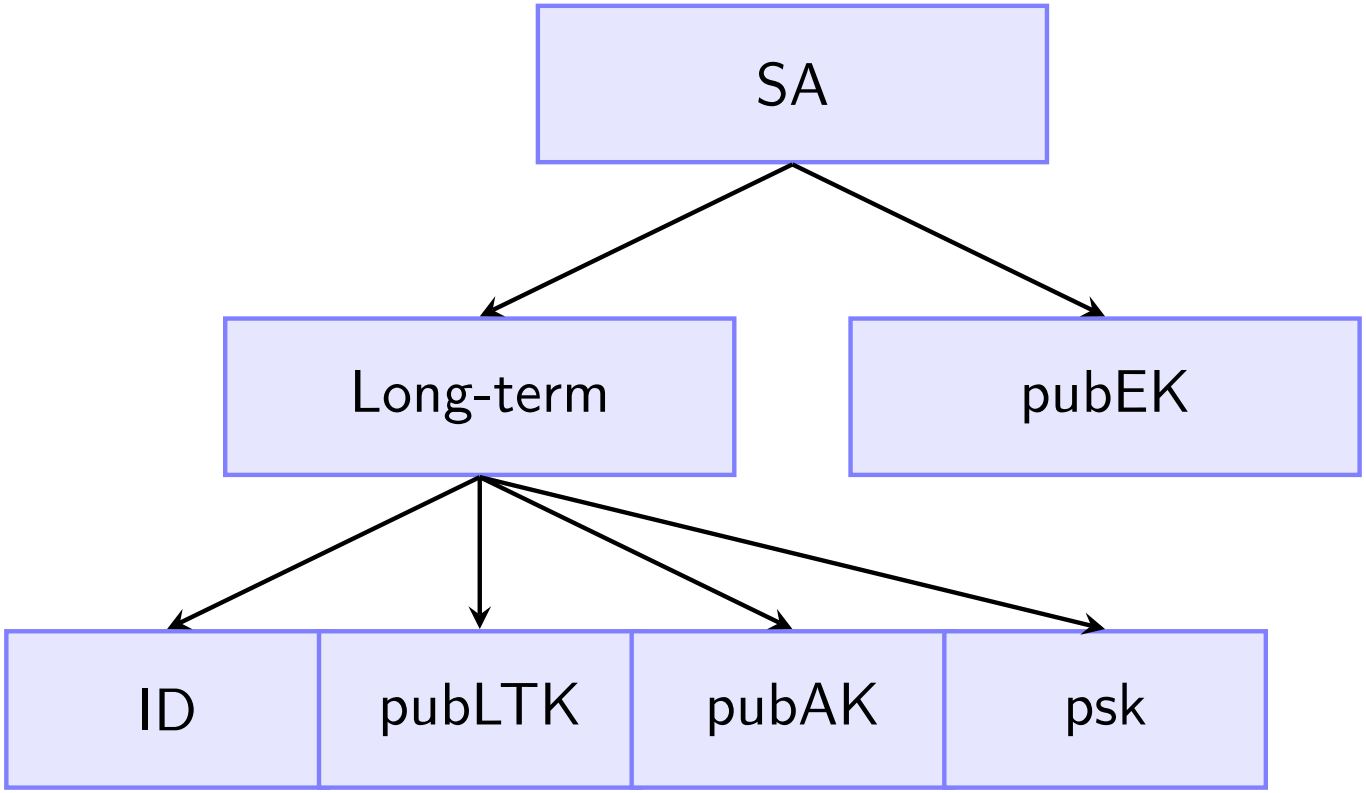
[6] `https://github.com/ccc-attestation/interoperable-ra-tls`

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

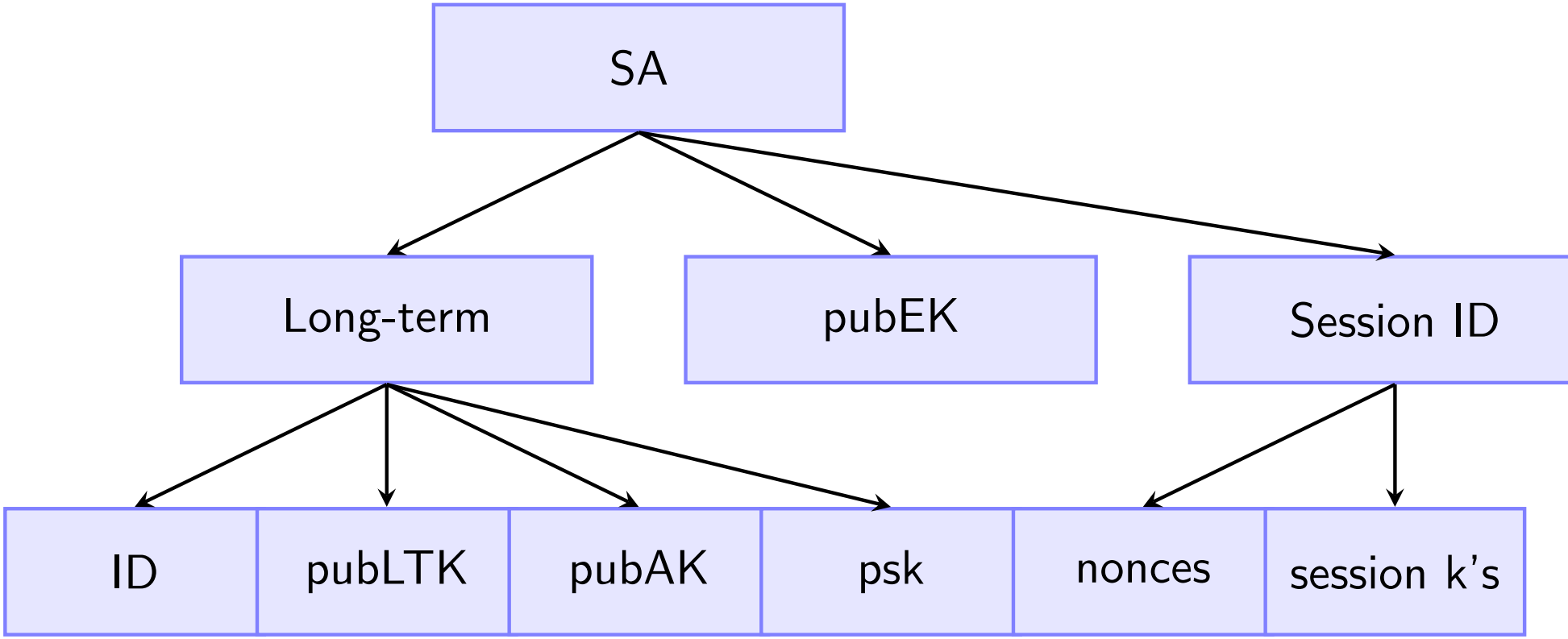
Arguments for SA Property



Arguments for SA Property

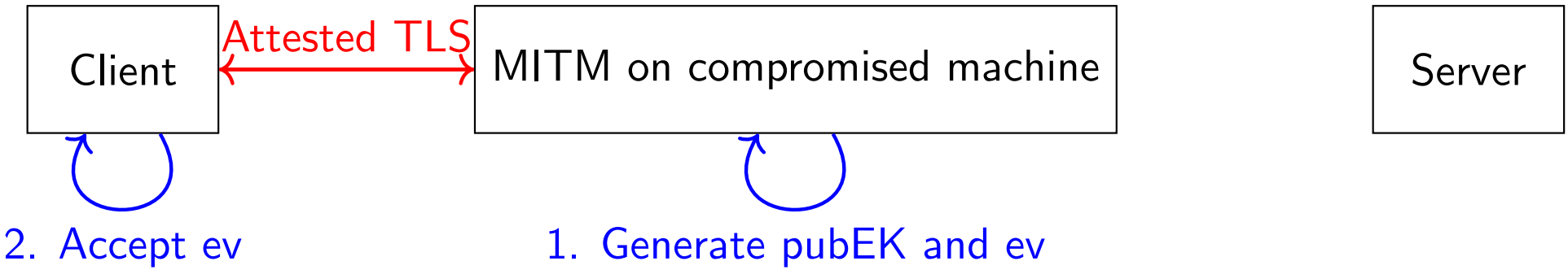


Arguments for SA Property



Impersonation of Server (SA Property)

- Server as Attester
- Client as Verifying Relying Party



Vulnerability

- Server authentication in both protocols may fail if there is even one compromised CC machine (i.e., AK is compromised) in the world whose corresponding certificate (e.g., PCK certificate for Intel TDX) has not yet been added to the revocation list.
- Security is based on the assumption that no machine is ever compromised.

Proposal

- Augment rather than replace Server Authentication
  - Web PKI certificate for hostname
  - Perform RA to prove integrity of its computing environment

Outline

Quick Preview of SIG Project 3: KBS[8]

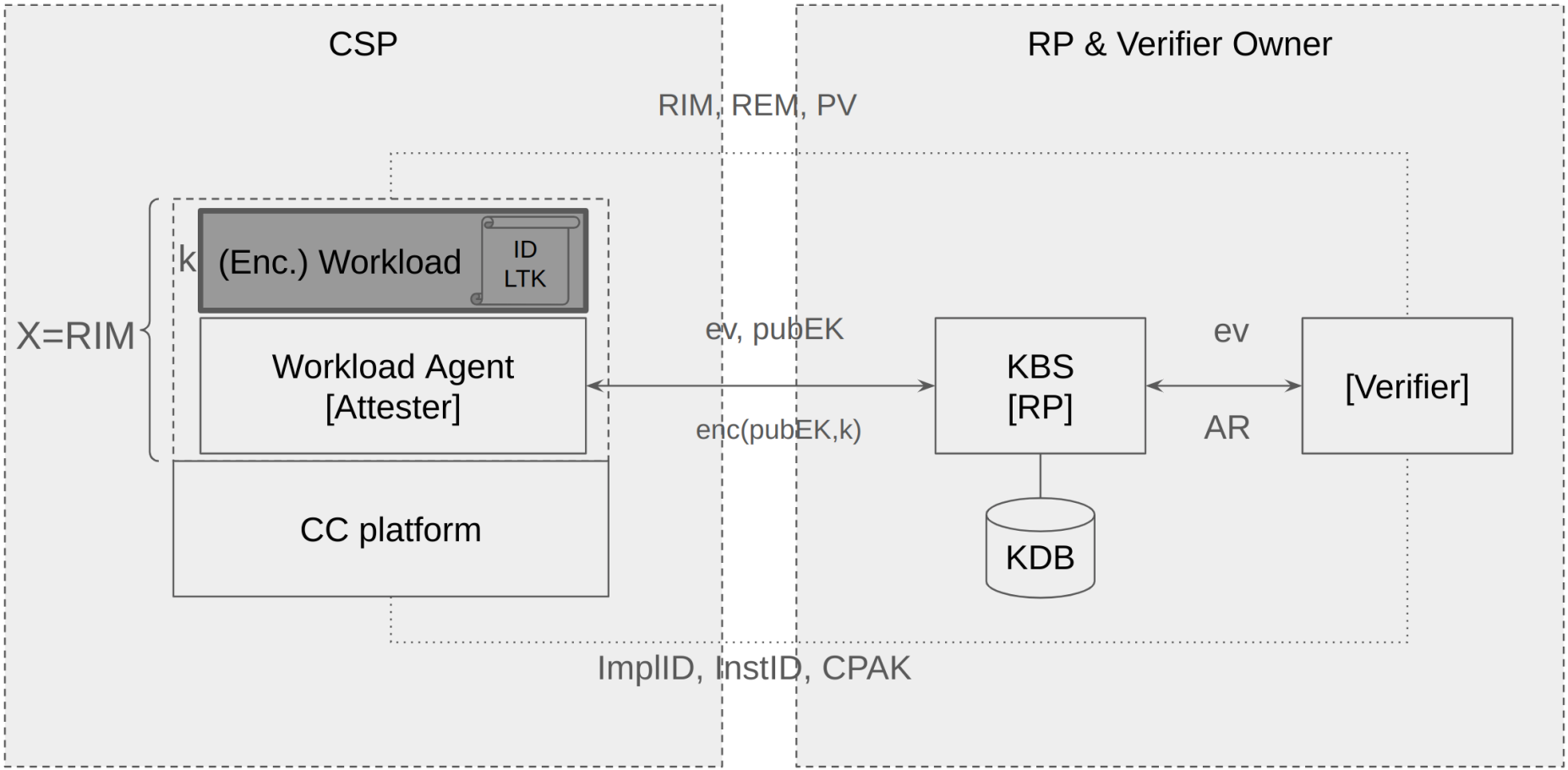


Image credits: Thomas Fossati

[8] https://github.com/CCC-Attestation/formal-spec-KBS

Quick Preview of Standardization[9]

Workgroup:	Network Working Group
Internet-Draft:	draft-fossati-rats-exported-attestation-latest
Published:	17 February 2025
Intended Status:	Standards Track
Expires:	21 August 2025

Authors:	T. Fossati	M. U. Sardar	H. Tschofenig
	Linaro	*TU Dresden*	*H-BRS*

Remote Attestation with Exported Authenticators

Abstract

This specification defines a method for two parties in a communication interaction to exchange attestation evidence and attestation results using exported authenticators, as defined in RFC 9261. This approach falls into the category of post-handshake attestation by exchanging payloads in the application layer protocol while binding the remote attestation to the underlying communication channel. This document supports both the passport and background check models from the RATS architecture.

[9] `https://hannestschofenig.github.io/exported-attestation/draft-fossati-tls-exported-attestation.html`

Key References

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.

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)