Remote Attestation with Multiple Verifiers

draft-deshpande-rats-multi-verifier-02 - Remote Attestation with Multiple Verifiers

IETF 123
July 25, 2025

Authors:
Yogesh Deshpande(yogesh.deshpande@arm.com), Arm Ltd

Jun Zhang (junzhang1@huawei.com), Huawei Technologies France

Houda Labiod (houda.labiod@huawei.com), Huawei Technologies France

Henk Birkholtz (henk.birkholz@sit.fraunhofer.de), Fraunhofer SIT

Contributors:

Thomas Fossati
Linaro
Email: Thomas.Fossati@linaro.org
Thanassis Giannetsos
UBITECH Ltd.
Email: agiannetsos@ubitech.eu

Recap of Hackathon

- Brainstorm on the challenges of remote attestation of a Composite Attester with one Single Verifiers and the need for multiple Verifiers

- Multiple Verifiers needed, when Attester is composite:
    - Composite Attester: each sub-Attester has its **own** Verifier
    - **Trust and capability requirements:** Verifiers have to meet the trust and capability requirements of all sub-Attesters
    - **Regulation requirements**: Verifiers in different physical locations or domains
    - Different **Appraisal Policy** of Evidence for each Verifier

Remote Attestation Challenges in Complex Scenarios Side Meeting

Two side meetings
- Side meeting 1 (Tuesday 16-17pm): 13 onsite+ 4 online
- Side meeting 2 (Wednesday 17-18pm) 10 onsite + 2 online

Device attestation becomes composite attestation story.
- Composite attester **Evidence**
- Supply chain **Endorsement** for composite Attester
- Attestation **Verification** of Composite Attester
- **Attestation Result** for Composite Attester

Fig. 1: Composite Device:
(with CPU, NIC, GPU)

Discussions during side meeting 1 & meeting 2
- There is a need for multiple Verifiers when device is composite (with CPU, GPU, etc)
- Need for guidance on Verifier-Verifier topology, standard interfaces and message exchange, to avoid fragmentation

IETF

Update since version 01 (after Interim meeting)

- Update title (Remote Attestation MultiVerifier→ Remote Attestation with Multiple Verifiers)
- Add motivation (section 2: **Need for Multiple Verifiers**)
- Add Security and Privacy consideration (**6. Security and Privacy Considerations**)
- Update list of authors and contributors
- And some minor corrections

Adopt me?

- ✓ It is within scope of WG charter
- ✓ It shall define topological patterns, standard interfaces and message exchange between Multiple Verifiers

BACK UP SLIDES

Need for Multiple Verifiers

- 1: An Attester's composition can **change over time**. It may not be economically viable to build and maintain such a degree of complexity in a single Verifier.

- 2. A Verifier Owner may have an Appraisal Policy for Evidence of a Component Attester that is internal to them and which they **may choose not to reveal to** a “monolithic" Verifier.

- 3. A Reference Values Provider **may not wish to reveal its Reference Values** or their lifecycle to a monolithic Verifier.

- 4. There may not be a single actor in the ecosystem that can stand up and take ownership of verifying every Component Attester due to **a lack of knowledge, complexity, regulations or associated cost**.

- 5. The mix today is a **combination of Verifier** services provided by component manufacturers, Verifiers provided by integrators, and Verifiers under local authority (i.e., close to the attester).

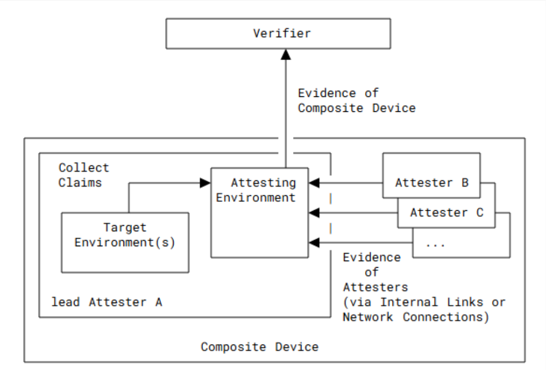


Fig. 1: Composite attester

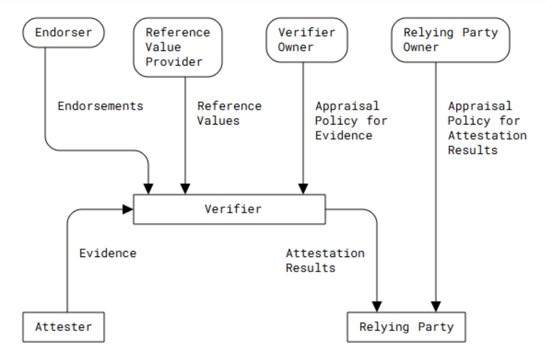
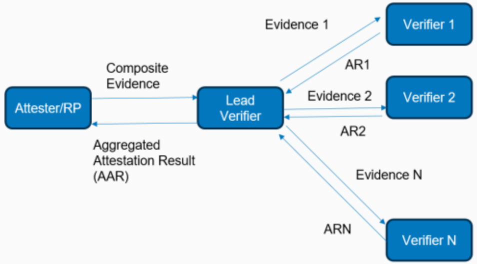


Fig. 2: RATS architecture

Security and Privacy considerations

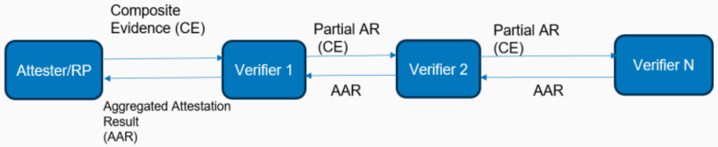
- In general, Verifiers should follow security and privacy guidance in Section 11 of [I-D.draft-ietf-rats-corim].

- In hierarchical model,
  - Secure channel between Lead Verifier and sub-Verifier
  - Partial Attestation Result is signed by key known by Lead Verifier.
  - Lead Verifier signs sub-Evidence if it is not signed (by attester).
  - Lead Verifier may encrypt sub-Evidence if confidentiality is required.



Hierarchical model

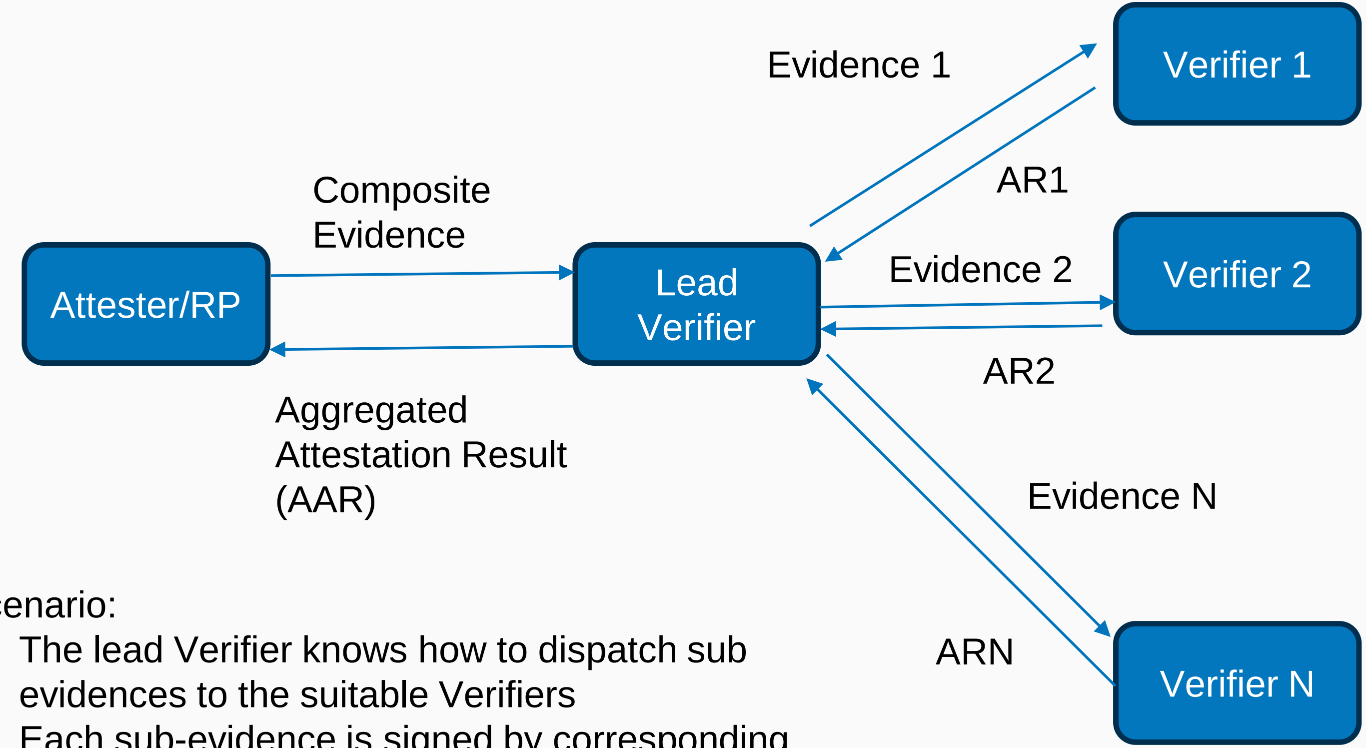
- In cascade model,
  - TBD, but few options currently
    - Verifiers in the Eco-System share a common Trust Anchor Store.
    - The Verifier always communicates with a known Verifier in the chain.



Cascade model

IETF

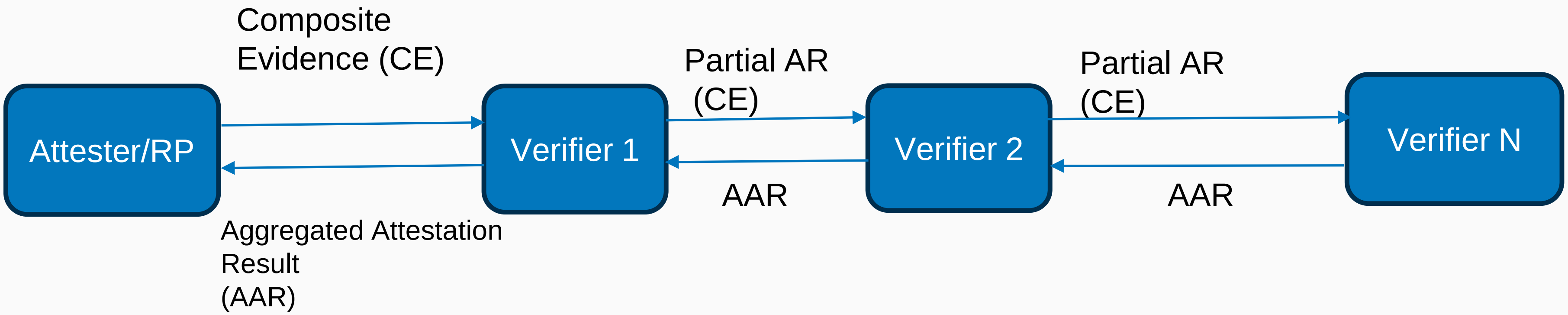
Hierarchical model



Scenario:

- The lead Verifier knows how to dispatch sub evidences to the suitable Verifiers
- Each sub-evidence is signed by corresponding attesting environment

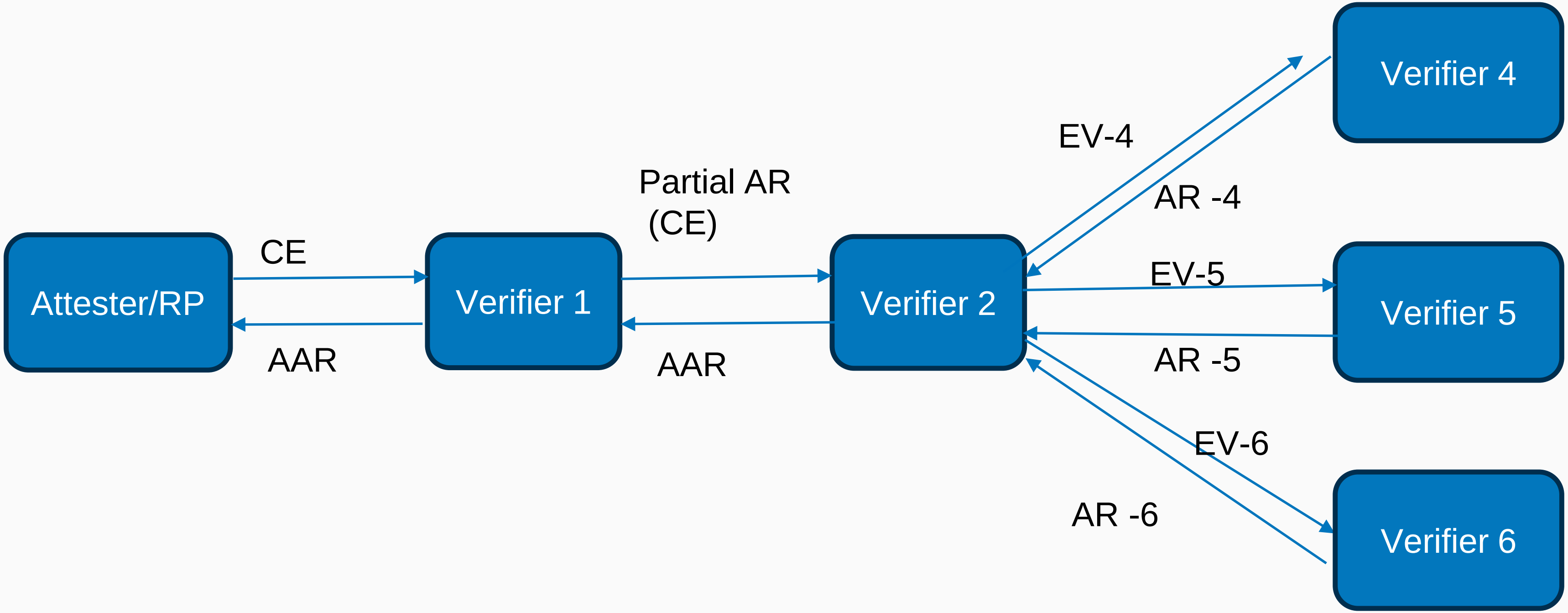
Cascade model



Scenario:

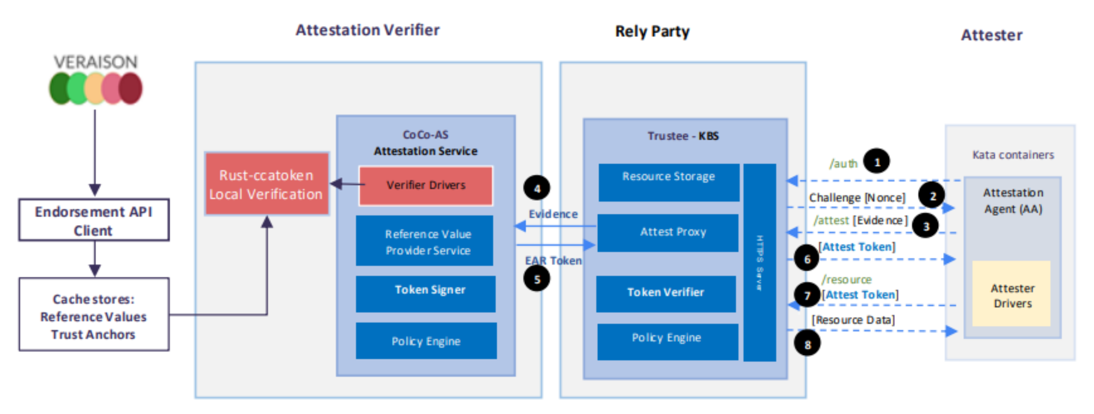
- Certain processing order is required between Verifiers
- Certain Verifier receives Partial AR (with CE) as the input for verification

Hybrid model



Multi Verifier Use Cases

Enable cloud native confidential computing using containers
https://github.com/confidential-containers/trustee

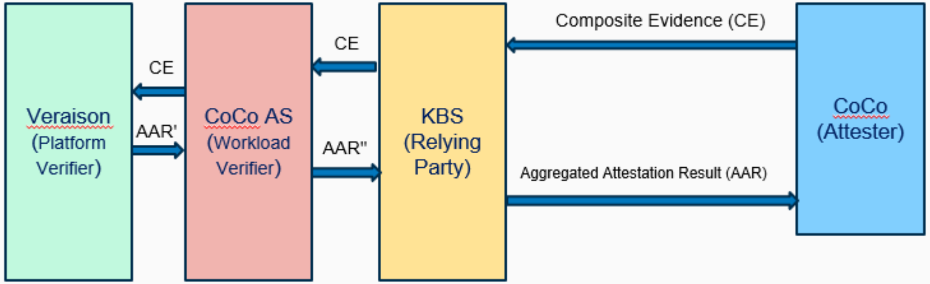


From: Attestation Everywhere (Arm, Linario)

Planned topology

Same deployment for Veraison Key Broker Demo

https://github.com/veraison/keybroker-demo

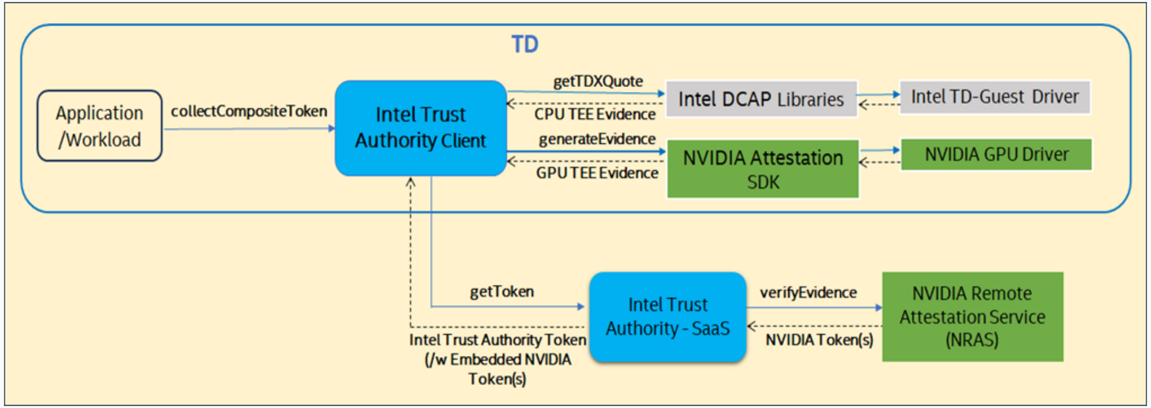


Abstracted topology

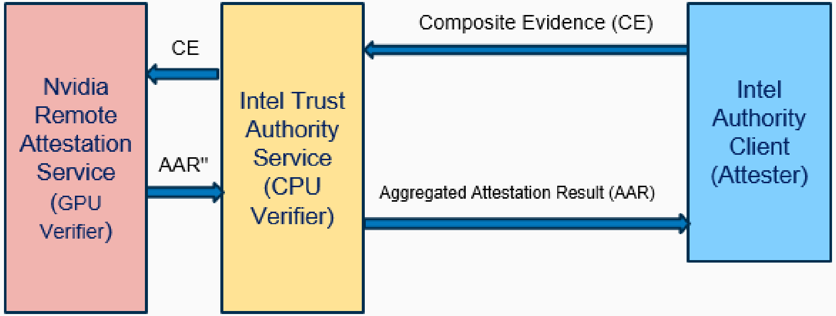
Multi Verifier Use Cases

Confidential training use case

[Seamless attestation of IntelTDX and NVIDIA H100 TEEs with Intel Trust Authority]



Real topology



Abstracted topology