

Remote Attestation with Multiple Verifiers

[draft-deshpande-rats-multi-verifier-04 - Remote Attestation with Multiple Verifiers](#)

IETF 125

March 18, 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 Birkholz (henk.birkholz@ietf.contact), Fraunhofer SIT

Contributors from linaro, Ubitech, Nvidia, and Orange

Internet Engineering Task Force

© 2026 IETF Trust

Production by Meetecho



Update since version 03 (after IETF124)

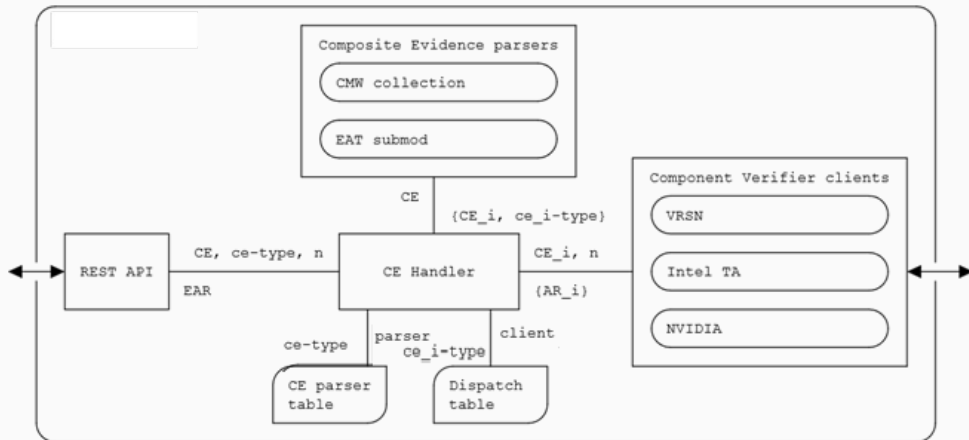
- Add definition of **Partial Evidence (PE)**
- Consistent use of identical terminology throughout the document
- Tidied up the diagrams for various topological patterns
- **Security considerations:**
 - Reframed the importance of Verifier Security, in the overall RATS Architecture
 - *The Verifier is not part of the Attester's Trusted Computing Base (TCB) but acts as a critical component in the Relying Party's trust decision chain.*
- **Privacy considerations:**
 - Improved text to highlight how multi-verifier architecture when carefully designed can improve privacy
- **Progress on Implementation – Project Veraison**

Implementation Status

- Lead Verifier Implementation – **Project Veraison**
 - Currently Work in Progress



Lead Verifier Architecture



For latest progress – please refer to
Lead Verifier Veraison Project Board at:

<https://github.com/orgs/veraison/projects/17>

Call for Adoption Request

- Consensus reached in IETF 124

BACK UP SLIDES

Notations

Composite Attester:

A Composite Attester is either a Composite Device or a Layered Attester or any composition involving a combination of one or more Composite Devices or Layered Attesters.

Component Attester:

A Component Attester is a single Attester of a Composite Attester. For this document, a Component Attester is an entity which produces a single Evidence which can be appraised by a Component Verifier.

Composite Evidence (CE):

Evidence produced by a Composite Attester.

Partial Evidence (PE):

It is an extract from a Composite Evidence. It consists of at least one or more Component Evidence.

Lead Verifier (LV):

A Verifier which acts as a main Verifier to receive Composite Evidence from a Composite Attester in a Hierarchical pattern.

Component Verifier (CV):

A Verifier which is responsible for the Verification of one single component or a layer.

Partial Attestation Results (PAR):

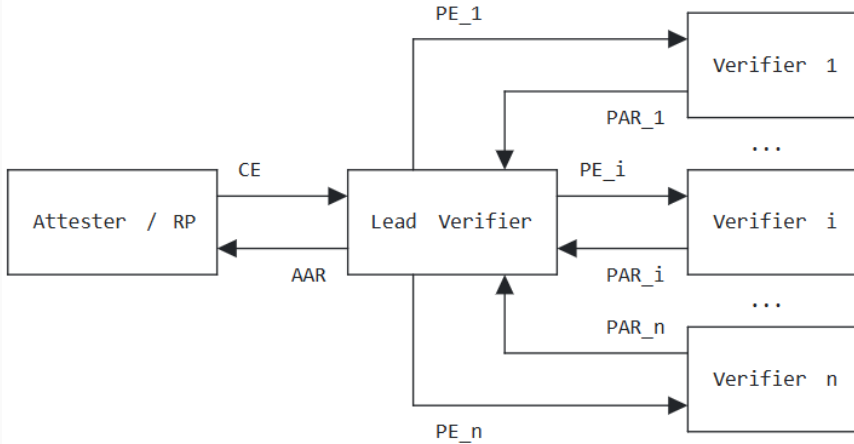
Attestation Results produced by a Component Verifier, which contains partial results from at least one or more Component Attesters.

Aggregated Attestation Results (AAR):

An Aggregated Attestation Results refers to a collection of Attestation Results produced upon completion of appraisal of a Composite Attester.



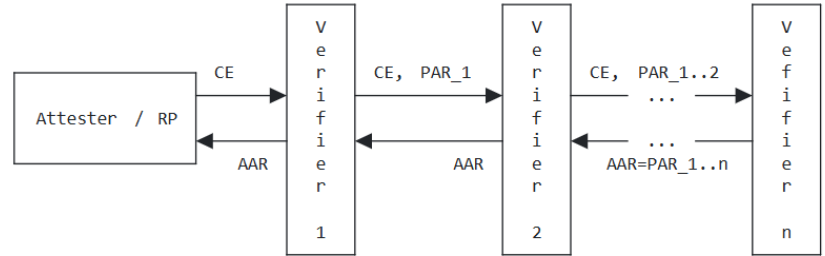
Hierarchical Pattern & Cascade Pattern



Legend:

- CE: Composite Evidence
- AAR: Aggregated Attestation Results
- PE_i: Partial Evidence of i-th Component Attester
- PAR: Partial Attestation Results

Figure 1: Hierarchical Pattern



Legend:

- CE: Composite Evidence
- AAR: Aggregated Attestation Results
- PAR: Partial Attestation Results

Figure 2: Cascaded Pattern

Use Case 1: Verification of Heterogenous Attester – Hierarchical Pattern

- A device may contain a CPU, as well as heterogeneous acceleration components (GPUs, NPUs, and TPUs). Combined this Evidence is considered Composite Evidence (CE).
- Due to organizational policies (e.g., scalability, complexity, or cost of infrastructure), a Verifier for each type of component may have to be deployed separately for each component vendor.
- While separate Verifiers return Partial Attestation Results (PAR), the Lead Verifier (LV) combines those into Aggregated Attestation Results (AAR)

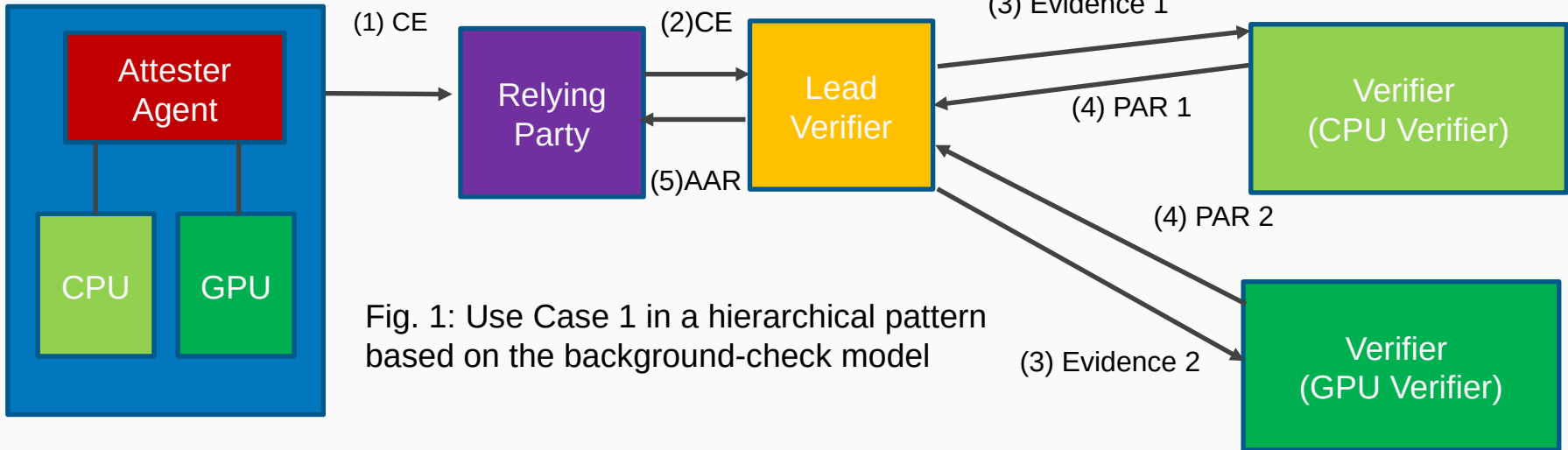


Fig. 1: Use Case 1 in a hierarchical pattern based on the background-check model

Use Case 1: Verification of Heterogenous Attester – Cascade Pattern

- Verifiers take turn to verify the Component Evidence (from CPU or GPU) and output the Partial Attestation Result (PAR)
- The last Verifier Aggregates all PARs and generates Aggregated Attestation Results (AAR) and it is sent back to the first Verifier in the reverse order to the propagation of CE.

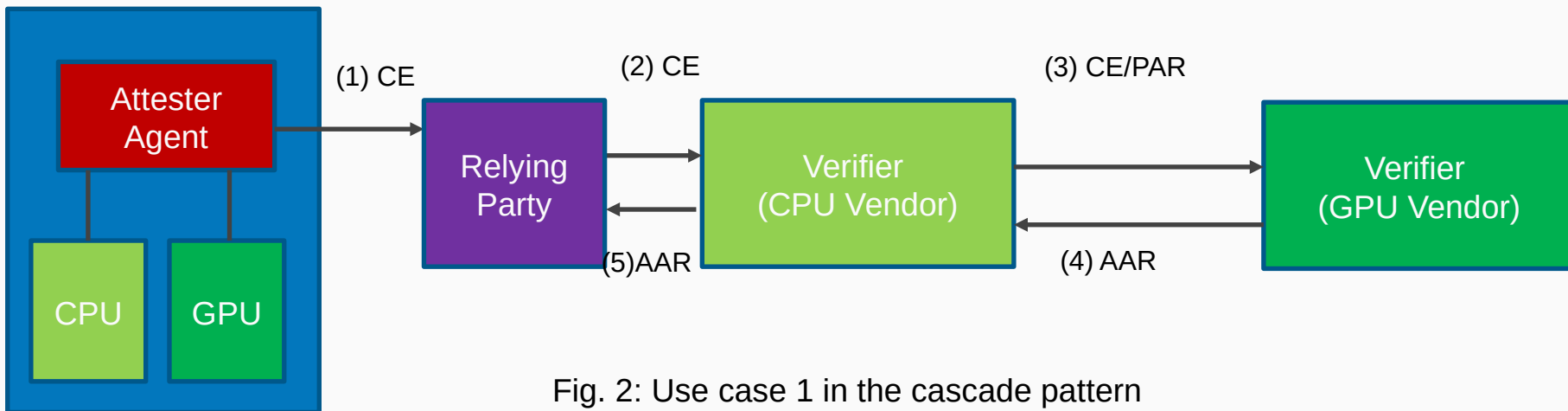


Fig. 2: Use case 1 in the cascade pattern (also based on the background-check model)

Use Case 2: Verification of Workloads operating in Confidential Computing environment

- A layered Attester containing a Platform and a confidential Workload running in a CC environment
- Workload Owner and Platform Owner deploy their Verifiers separately.
- KMS (RP) releases the key to the Attester once it is attested (both for workload and platform)
- Evidence from workload and Platform Should be encrypted when privacy is a concern.

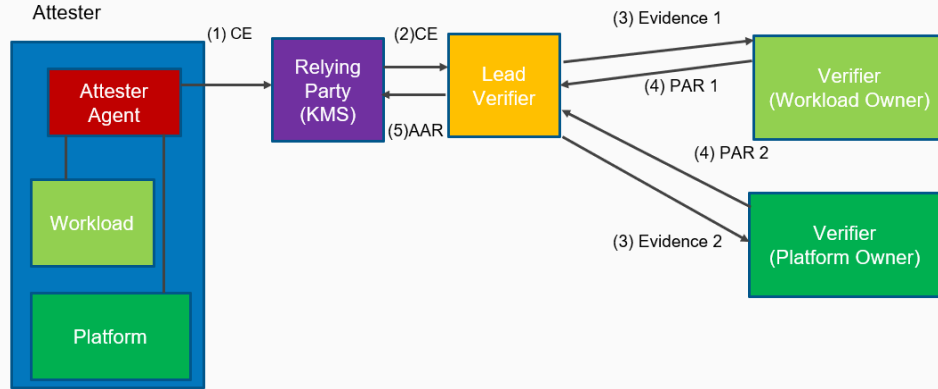


Fig. 3: Use Case 2 in a hierarchical pattern based on the background-check model

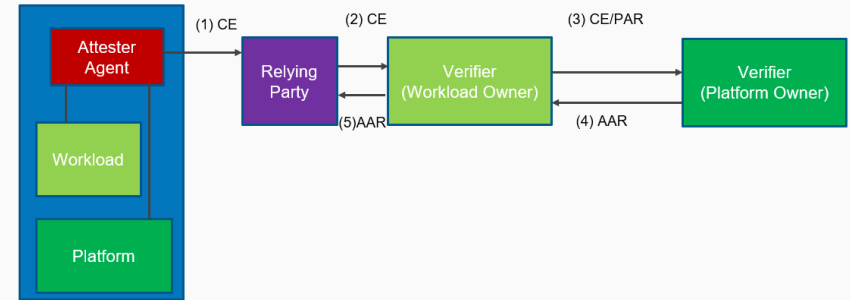


Fig. 4: Use Case 2 in a cascade pattern based on the background-check model