

May 2nd 2025

Remote Attestation MultiVerifier

IETF Interim meeting

Authors:

Yogesh [Deshpande\(yogesh.deshpande@arm.com\)](mailto: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\(henk.birkholz@sit.fraunhofer.de\)](mailto:henk.birkholz@sit.fraunhofer.de), Fraunhofer SIT

Contributors:

Thomas Fossati

Linaro

Email: Thomas.Fossati@linaro.org

Thanassis Giannetsos

UBITECH Ltd.

Email: agiannetsos@ubitech.eu

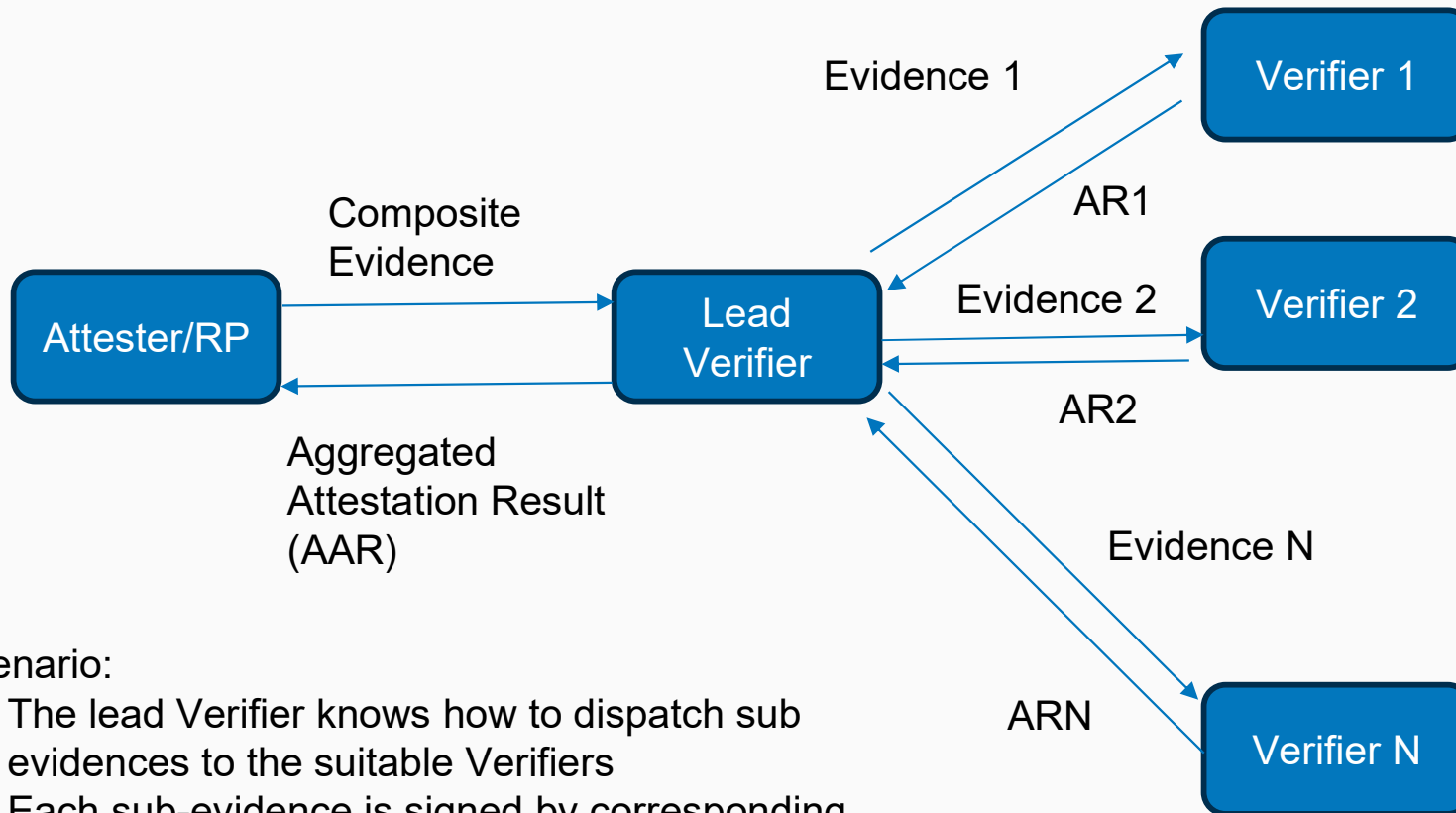
Internet Engineering Task Force
© 2025 IETF Trust
Production by Meetecho



WHY – Multi Verifier RATS ?

- Attesters are getting complex
 - Effectively a combination of multiple component Attesters
 - For example, an Attester may comprise of a CPU and a GPU
- One Verifier may not possess the diverse set of Reference Values and Endorsements required for complete appraisal of such an Attester
- How does one perform Appraisal of complex Attesters ?
- Multiple Verifiers need to work together
- Proposed RATS MultiVerifier (<https://www.ietf.org/archive/id/draft-deshpande-rats-multi-verifier-01.html>)

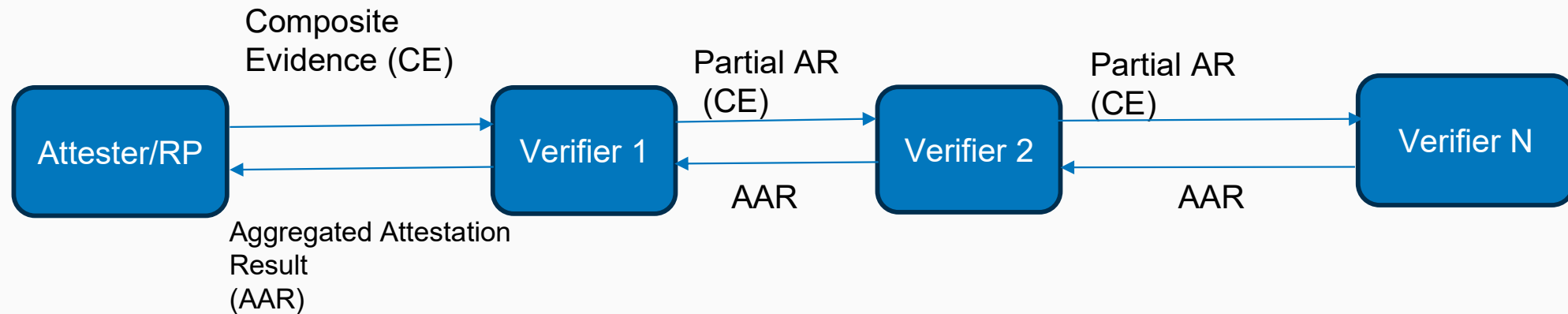
Hierarchical model



Scenario:

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

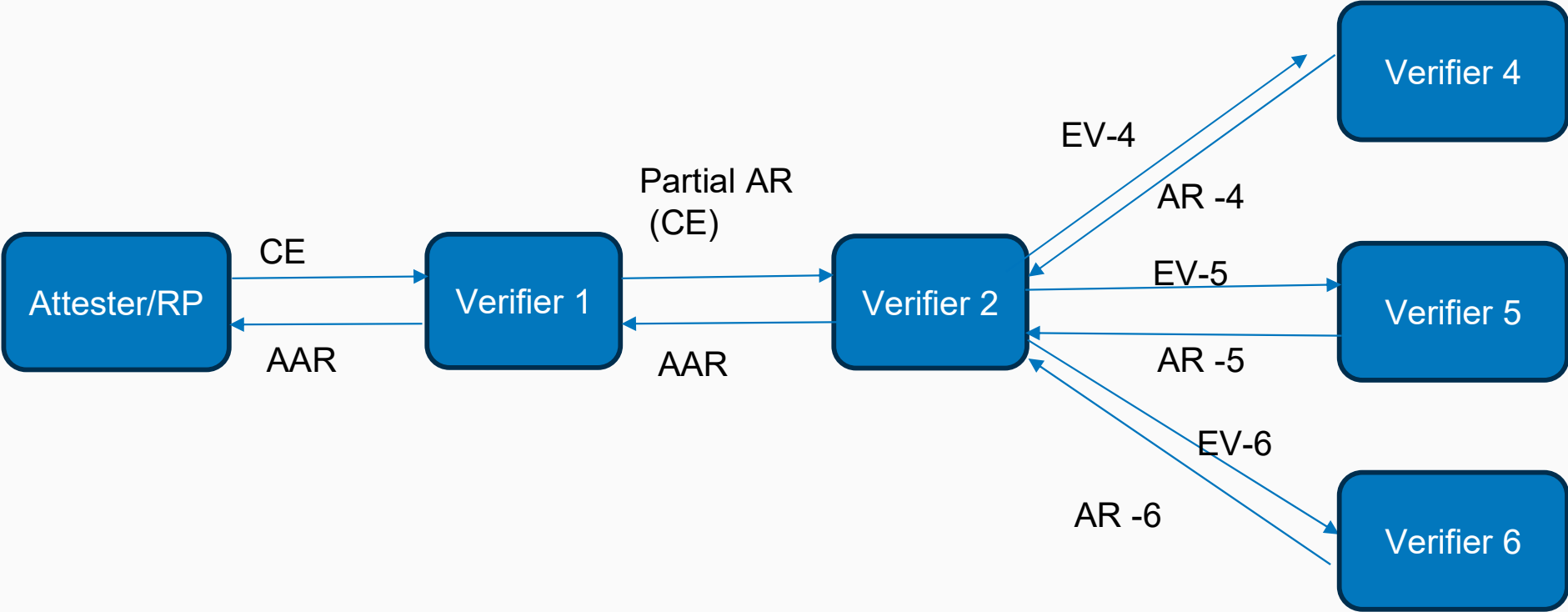
Cascade model



Scenario:

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

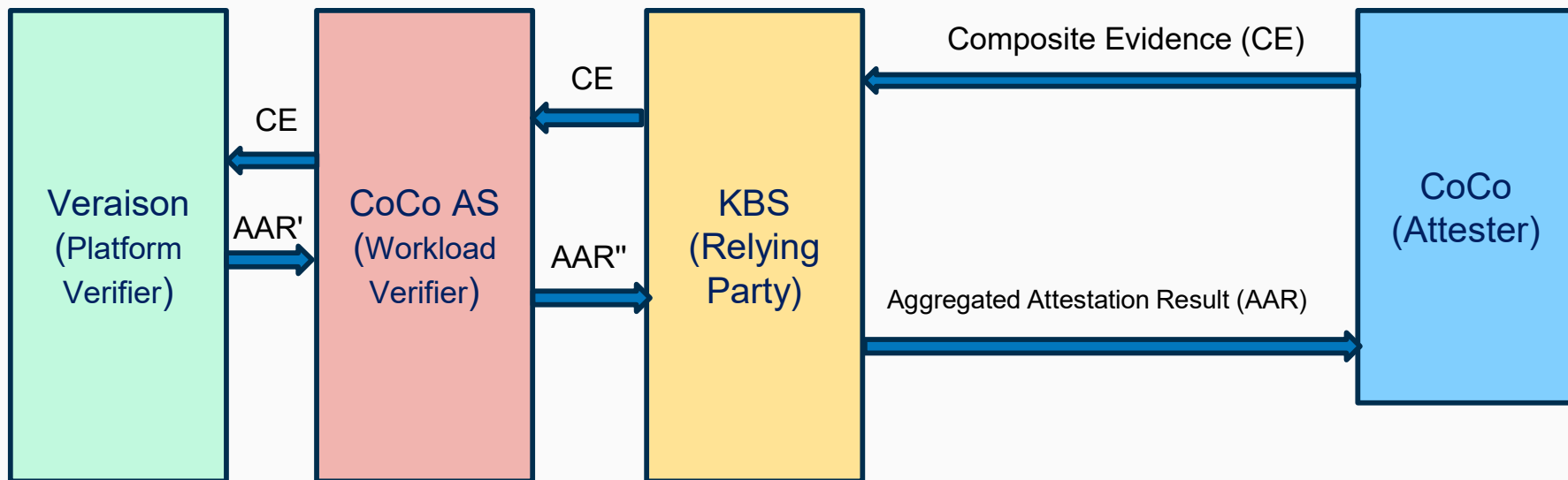
Hybrid model



Multi Verifier Use Cases

Enable cloud native confidential computing using containers

<https://github.com/confidential-containers/trustee>



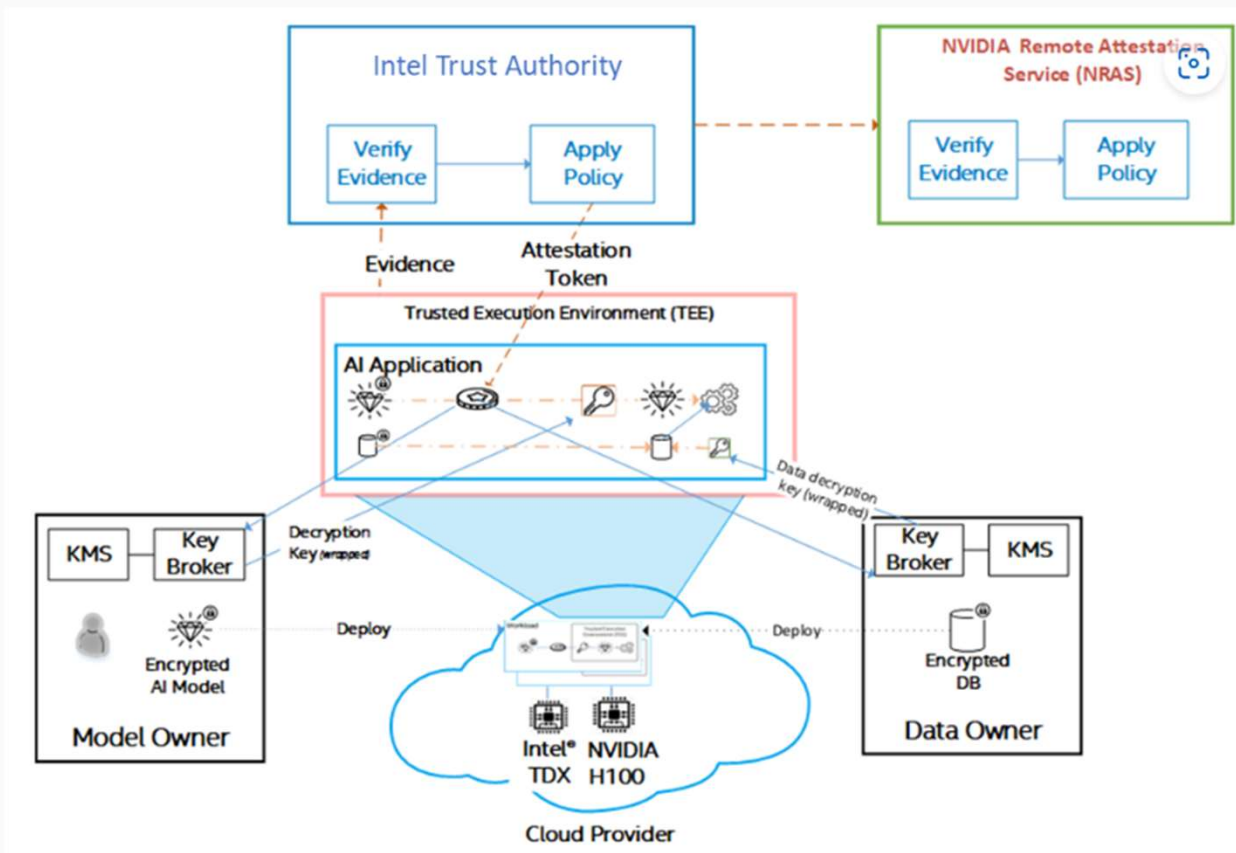
Same deployment for Veraison Key Broker Demo

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

Multi Verifier Use Cases

Confidential training use case

A Composite Device (CPU and a GPU)



[Source: Seamless attestation of IntelTDX and NVIDIA H100 TEEs with Intel Trust Authority](#)

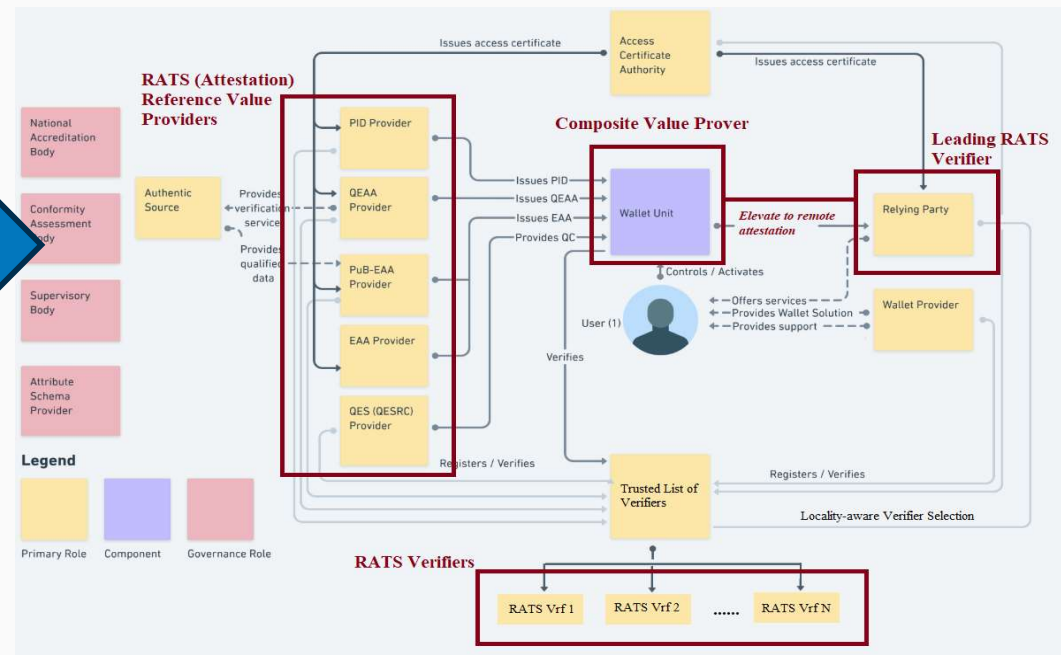
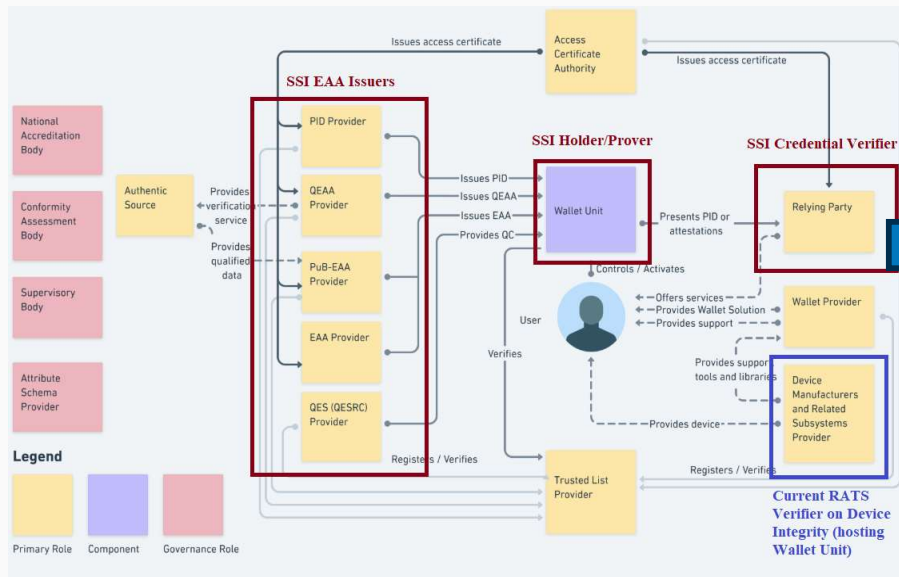
[Source: Confidential mesh computing \(MarbleRun\)](#)

Multi Verifier Use Cases

EU Digital Identity Wallet Qualified Attestation of Attributes

RATS Mapping

Hierarchical Model



Verification of attributes against authentic sources

- Zero Trust Principle for Issuers, Provers (Holder), Verifiers
- Mapping to multiple RATS Prover/Verifier modalities
 - eIDAS Electronic Attestation of Attribute (EAA) Prover vs. RATS Prover
 - RATS Verifier vs. EUDI Credential Verifier

Source: [Verification of attributes against authentic sources \(eIDAS Implementing Act Article 45e\)](#)

Source: [EUDI ARF v1.7.0 \(Stable Version\)](#)



Thank you

Comments? Questions?

All welcome.