RATS
Internet-Draft
Intended status: Informational
Expires: 8 January 2026

Y. Deshpande
Arm Ltd
J. Zhang
H. Labiod
Huawei Technologies France S.A.S.U.
H. Birkholtz
Fraunhofer SIT

7 July 2025

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

Abstract

IETF RATS Architecture, defines the key role of a Verifier. In a complex system, this role needs to be performed by multiple Verfiers coordinating together to assess the full trustworthiness of an Attester. This document focuses on various topological patterns for a multiple Verifier system.

Discussion Venues

This note is to be removed before publishing as an RFC.

Source for this draft and an issue tracker can be found at https://github.com/ietf-rats/draft-deshpande-multi-verifier.

Status of This Memo

Table of Contents

1. Introduction

A Verifier plays a central role in any Remote Attestation System. A Verifier appraises the Attester and produces Attestation Results, which are essentially a verdict of attestation. The results are consumed by the Relying Party to conclude the trustworthiness of the Attester, before making any critical decisions about the Attester, such as admitting it to the network or releasing confidential resources to it. Attesters can come in wide varieties of shape and form. For example Attesters can be endpoints (edge or IoT devices) or complex machines in the cloud. Composite Attester Section 3.1, generate Evidence that consists of multiple parts. For example, in data center servers, it is not uncommon for separate attesting environments (AE) to serve a subsection of the entire machine. One AE might measure and attest to what was booted on the main CPU, while another AE might measure and attest to what was booted machine's GPU. Throughout this document we use the term Component Attester Section 3.1 to address the sub-entity or an individual layer which produces its own Evidence in a Composite Attester system.

In a Composite Attester system, it may not be possible for a single Verifier to possess all the capabilities or information required to conduct a complete appraisal of the Attester. Please refer to Section 2 for motivation of this document. Multiple Verifiers need to collaborate to reach a conclusion on the appraisal and produce the Attestation Results.

This document describes various topological patterns of multiple Verifiers that work in a coordinated manner to conduct appraisal of a Composite Attester to produce an Attestation Results.

2. Need for Multiple Verifiers

To conduct the task of Evidence appraisal, a Verifier requires:

1. Reference Values from trusted supply chain actors producing, aggregating, or administering Attesters (Reference Value Providers)

2. Endorsements from trusted supply chain actors producing, certifying, or compliance checking Attesters (Endorsers)

3. Appraisal Policy for Evidence, which is under the control of the Verifier Owner

The Verifier inputs listed above are linked to the shape of the Attesters. Typically, Composite Attesters come with a varying degree of heterogeneity of Evidence formats, depending on the type of

Attesting Environments that come with each Component Attester, for example, CPU variants or GPU/FPGA variants. When conducting Evidence appraisal for a Composite Attester, the following challenges remain:

1. An Attester’s composition can change over time based on market requirements and availability (e.g., a set of racks in a data center gets thousands of new FPGAs). It is highly unlikely that there is always one appropriate Verifier that satisfies all the requirements that a complex and changing Composite Attesters imposes. 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). Rarely is it just one of these.

3. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document uses terms and concepts defined by the RATS architecture. For a complete glossary, see Section 4 of [RFC9334].

Specifically this document heavily uses the terms Layered Attester Section 3.2 of [RFC9334] and Composite Device Section 3.3 of [RFC9334]

3.1. Glossary

This document uses the following terms:

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 Verifier.

Composite Evidence: Evidence produced by a Composite Attester.

Lead Verifier: A Verifier which acts as a Main Verifier to receive Composite Evidence from a Composite Attester.

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

4. Multi Verifier topological patterns

A Composite Attester has multiple Component Attesters. Each Attester requires a different set of Verifiers. Hence multiple Verifiers collaborate to appraise a Composite Attester.

4.1. Hierarchical Pattern

Figure below shows the block diagram of a Hierarchical Pattern.

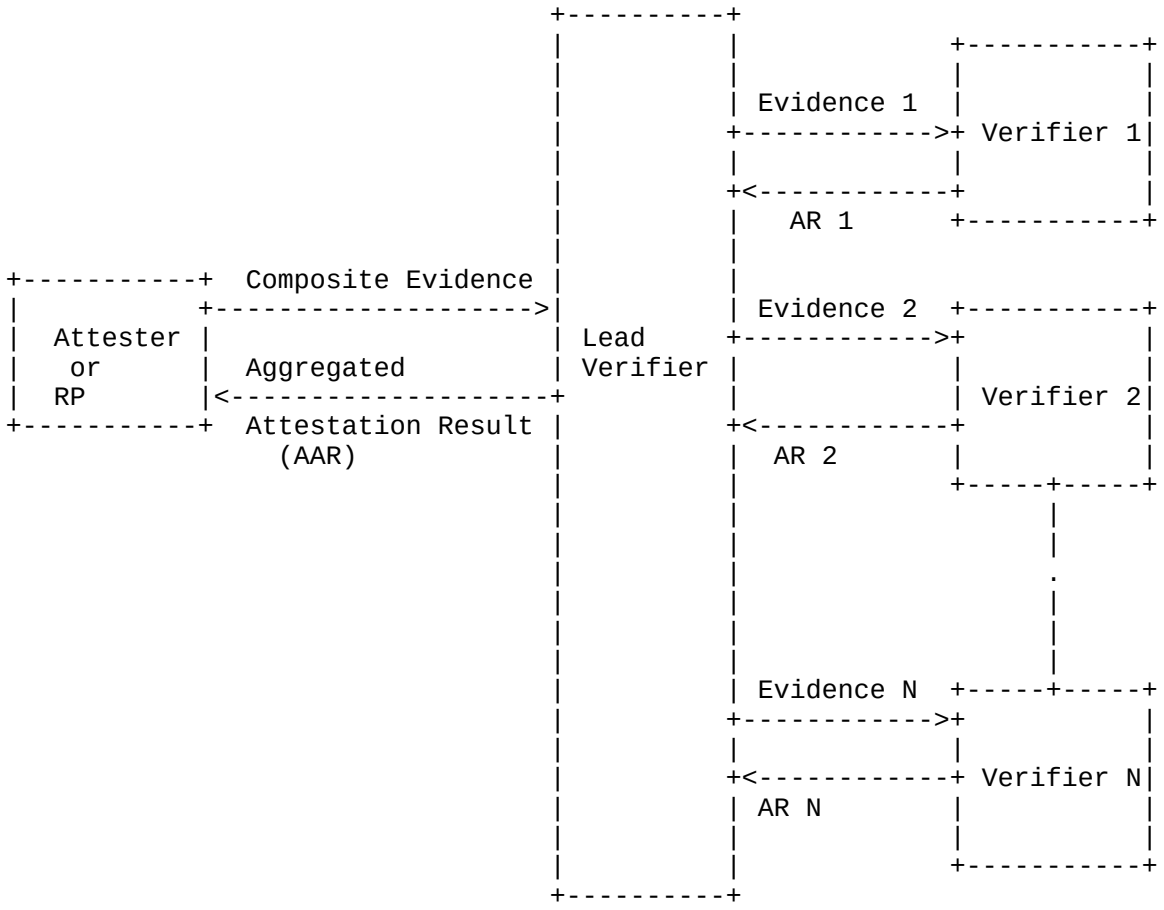

Figure 1: Hierarchical Pattern

The following sub-sections describe the various roles that exist in this pattern.

4.1.1. Lead Verifier

In this topological pattern, there is an Entity known as Lead Verifier.

Lead Verifier is the central entity in communication with the Attester (directly in passport model or indirectly via the Relying Party in background-check model). It receives Attestation Evidence from a Composite Attester. If the Composite Attestation Evidence is signed, then it validates the integrity of the Evidence by validating the signature. If signature verification fails, the Verification is terminated. Otherwise it performs the following steps.

* Lead Verifier has the knowledge about the overall structure of the Composite Evidence. It decodes the Composite Evidence to extract the Component Attester Evidence. This may lead to "N" Evidence, one for each Component Attester.

* Lead Verifier delegates each Component Attester Evidence to their own Verifier and receives Component Attester Attestation Results after successful Appraisal of Evidence.

* Once the Lead Verifier receives Attestation Results from all the Verifiers, it combines the results from each Verifier to construct a Aggregated Attestation Results (AAR). The Lead verifier may apply its own policies and also add extra claims as part of its appraisal.

* Lead Verifier conveys the AAR to the Attester (in Passport model) or to the Relying Party (in background check model).

The overall verdict may be dependent on the Appraisal Policy of the Lead Verifier.

In certain topologies, it is possible that only the Composite Evidence is signed to provide the overall integrity, while the individual Component Attester Evidence (example Evidence 1) is not protected. In such cases, the Lead Verifer upon processing of Composite Evidence may wrap the Component Attester Evidence (example Evidence 1) in a signed Conceptual Message Wrapper (CMW), and send it to each Verifier (example Verifier 1).

4.1.2. Verifier for Component Attester

The role of a Component Attester Verifier is to receive Component Attester Evidence from the lead Verifier and produce Attestation Results to the Lead Verifier.

4.1.3. Trust Relationships

In this topology the Lead Verifier is fully trusted by Component Attester Verifiers (example Verifier 1).

Also, each of the Component Attester Verifier is fully trusted by the Lead Verifier. Lead Verifier is provisioned with the Trust Anchors for Verifier 1..N.

4.2. Cascaded Pattern {: #sec-verifier-cascade }

Figure below shows the block diagram of a Cascaded Pattern.

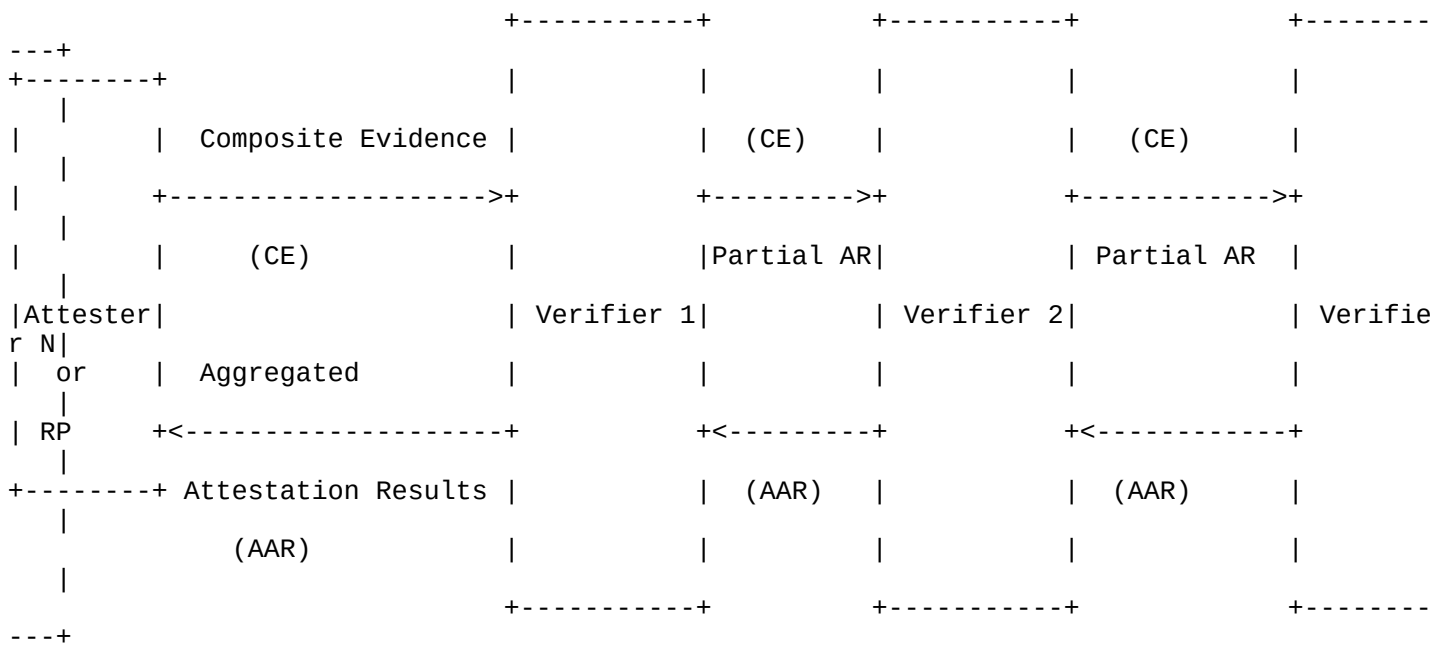

Figure 2: Cascaded Pattern

In this topological pattern, the Attestation Verification happens in sequence. Verifiers are cascaded to perform the Attestation Appraisal. Each Verifier in the chain possess the knowledge of the entire Composite Attester topology.

Attester may send the Composite Evidence(CE) to any of the Verifier (directly in the passport model, or indirectly via the Relying Party in the background-check model). The Verifier which processes the Composite Evidence, Verifies the signature on the Evidence, if present. It decodes the Composite Evidence performs Appraisal of the Component Attester whose Reference Values and Endorsements are in its database. Once the appraisal is complete, it forwards the Composite Evidence and partial Attestation Results to the subsequent Verifier.

The process is repeated, until the entire appraisal is complete. The last Verifier, i.e. Verifier-N, completes its Appraisal of the Component Attester Evidence and returns the complete Attestation Results to the N-1 Verifier, which passed Evidence to it. The N-1 Verifier then simply passes the Aggregated Attestation Results(AAR) from where it received its Combined Evidence. Alternatively, it may also modify the AAR based on the inspection of received AAR. For example, it may add its own Verifier Added Claims (policy claims) and produce a new AAR. The process is repeated, until the Verifier, which recieved the initial Evidence is reached. At this point in time the Aggregated Attestation Results are signed and the Aggregated Attestation Results are sent to the Attester (in Passport Model) or Relying Party (in background check model).

As shown in the picture, the partial results and Combined Evidence is transmitted to a chain of Verifier, till the Appraisal is complete. The Verifier combines the incoming partial results, combines the results from it own Evidence Appraisal and passes the Aggregated Attestation Results to the Verifier from which it receives Combined Evidence.

4.2.1. Trust Relationships

4.2.2. Verifiers

In the cascaded pattern, the communicating Verifiers fully trust each other. Each Verifier has the trust anchor for the Verifier it is communicating to (i.e. either sending information or receiving information). This prevents man in the middle attack for the partial Attestation Results received by a Verifier or a Aggregated Attestation Results (AAR) which it receives in the return path.

4.2.3. Relying Party and Verifiers

In the cascaded pattern, the RP may communicate with any Verifier and thus receive its Attestation Results. Hence RP fully trusts all the Verifiers.

4.3. Hybrid Pattern

In a particular deployment, there is a possibility that the two models presented above can be combined to produce a hybrid pattern. For example Verifier 2 in the Cascaded Pattern becomes the Lead Verifier for the remaining Verifers from 3, to N.

5. Freshness

The Verifier needs to ensure that the claims included in the Evidence reflect the latest state of the Attester. As per RATS Architecture, the recommended freshness is ascertained using either Synchronised Clocks, Epoch IDs, or nonce, embedded in the Evidence. In the case of Hierarchical Pattern, the Verification of Freshness should be checked by the Lead Verifier.

In the Cascaded Pattern, the freshness is always checked by the first Verifier in communication with either the Attester (Passport Model) or Relying Party (Background Check Model).

6. Security and Privacy Considerations

The Verifier is effectively part of the Attesters' and Relying Parties' trusted computing base (TCB). Any mistake in the appraisal procedure conducted by the Verifier could have security implications. For Security and Privacy considerations while conducting appraisal procedure the Verifiers described in this document MUST follow the guidance detailed in Security and Privacy considerations of a RATS Verifier as detailed in Section 11 of [I-D.draft-ietf-rats-corim].

6.1. Conceptual Message Protection

6.1.1. Hierarchical Pattern

In this topology the Lead Verifier communicates with the Attester/RP and with other Verifiers.

The Security and Privacy consideration for the messages between the Lead Verifier and the Attester/RP follows the guidance provided in RATS Architecture Section 11 and Section 12 of [RFC9334].

The Lead Verifier conveys Component Attester Evidence to each of the sub-Verifiers and receives partial Attestation Results from them.

1. The communication among the Verifiers should use secure channels, such as TLS. This ensures confidentiality, integrity and authenticity of the message exchanged between the Verifiers.

2. For integrity protection at the application layer, each partial Attestation Result Message is signed by a key known to the Lead Verfier.

3. The Composite Attester Evidence contains Component Attester Evidence, each having signature from the Attesting Environments that generated it. This ascertains the authenticity and

integrity protection of individual Evidence exchanged between the Verifier. However there may be cases (for example UCCS), where the individual Evidence is not signed. In such scenarios, the Lead Verifier may add its own signature using a private key whose public key is known to the sub Verifiers.

4. Evidence might contain sensitive or confidential information, there might be a need for confidentiality protection of the individual Evidence from Lead Verifier to sub Verifiers. The Lead Verifier may choose to Encrypt the individual Evidence using the public Key of the Verifier it communicates.

If there isn’t confidentiality protection of conceptual messages themselves, the underlying conveyance protocol should provide these protections.

6.1.2. Cascaded Pattern

In this pattern, the Composite Evidence is received by each Verifier in the chain. As a result, the Security and Privacy consideration of Evidence between the Attester/RP and each of the Verifier follows the guidance provided in RATS Architecture Section 11 and Section 12 of [RFC9334].

Partial and Aggregated Attestation Results are exchanged among the Verifiers. It is TBD how the Security and Privacy of these messages can be ascertained. Few possible options are listed below.

1. All the Verifiers in the Eco-System share a common Trust Anchor Store. The Sender Ensures the Confidentiality and Integrity of the Partial/Aggregated AAR. The receiver Verifies the Confidentiality of these messages using the Private Keys in its database. It Verifies the authenticity and integrity of these messages using the Trust Anchor Store Public Keys.

2. The Verfier always communicates with a known Verifier in the chain. Hence it only maintains the trust roots for its communicating Verifier.

If there isn’t confidentiality protection of conceptual messages themselves, the underlying conveyance protocol should provide these protections

These and new options will be discussed further in the RATS Working Group.

7. IANA Considerations

8. Acknowledgements

// TODO

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

9.2. Informative References

[I-D.draft-ietf-rats-corim] Birkholz, H., Fossati, T., Deshpande, Y., Smith, N., and W. Pan, "Concise Reference Integrity Manifest", Work in Progress, Internet-Draft, draft-ietf-rats-corim-07, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-corim-07>.

[RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334, January 2023, <https://www.rfc-editor.org/rfc/rfc9334>.

Contributors

Thomas Fossati
Linaro
Email: Thomas.Fossati@linaro.org

Thanassis Giannetsos
UBITECH Ltd.
Email: agiannetsos@ubitech.eu

Authors' Addresses

Yogesh Deshpande
Arm Ltd

Email: yogesh.deshpande@arm.com

Jun Zhang
Huawei Technologies France S.A.S.U.
Email: junzhang1@huawei.com

Houda Labiod
Huawei Technologies France S.A.S.U.
Email: houda.labiod@huawei.com

Henk Birkholtz
Fraunhofer SIT
Email: henk.birkholz@sit.fraunhofer.de