RATS
Internet-Draft
Intended status: Standards Track
Expires: 8 January 2026

H. Labiod
A. Lamouchi
J. Zhang
Huawei Technologies France S.A.S.U.
A. Duda
Grenoble INP - Ensimag, LIG Lab
H. Birkholz
Fraunhofer SIT

7 July 2025

Attester Groups for Remote Attestation
draft-labiod-rats-attester-groups-03

Abstract

This document proposes an extension to the Remote Attestation Procedures architecture by introducing the concept of Attester Groups. This extension aims to reduce computational and communication overhead by enabling collective Evidence appraisal of high number of homogeneous devices with similar characteristics, thereby improving the scalability of attestation processes.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 January 2026.

Table of Contents

1. Introduction

[RFC9334] defines Attesters as entities comprising at least one Attesting Environment and one Target Environment co-located in one entity. It also presents different ways to compose the Attesting and Target Environments, such as Composite Devices and Layered Attesters. Layered Attester reflects a cascade of staged Environments. It is more related to one device with different layers and there is a relationship between them. However, mechanisms for efficiently managing multiple, independent Attesters are missing. Assessing the trustworthiness of large numbers of independent devices individually can result in high conveyance and processing overhead. This comes into effect particularly when these devices share identical hardware or firmware components, which can lead to redundancy between all individual remote attestation procedures. One example would be a smart factory scenario where numerous sensors of the same model monitor different parts of the manufacturing process. These sensors share identical hardware and firmware configurations. This document proposes a model by which these separate sensors devices can be grouped into a single Attester Group and a shared remote attestation procedure can appraise their authenticity collectively rather than individually. Direct Anonymous Attestation (DAA) [I-D.ietf-rats-daa] has a similar concept of using one unique ID for one group of Attesters, but its goal is to mitigate the issue of uniquely (re-)identifiable Attesting Environments, while scalability is the major concern in this document.

2. Terminology

The following terms are imported from [RFC9334]: Attester, Composite Device, Evidence, Layered Attester, Verifier.

Newly defined terms for this document:

Attester Group: A role performed by a group of Attesters whose Evidence must be appraised in order to infer the extent to which the individual Attesters comprising the group are considered trustworthy.

group-id: A new Attester Identity type (see Section 2.2.1. of [I-D.ietf-rats-ar4si]). It is a unique identifier assigned to each Attester Group, allowing the group to dynamically adjust its membership without redefining its fundamental identity.

2.1. Requirements Notation

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.

3. Attester Group and Comparison to Composite Devices

We should be able to leverage the similarities between Attesters to avoid redundant attestations. An Attester Group is by definition a dynamic entity. Attesters can join or leave the group, in contrast to Composite Devices that have a static composition with a pre-defined set of Attesting Environments and fixed parameters. The dynamic nature of an Attester Group allows for the flexibility to tailor group parameters. This kind of flexibility facilitates the implementation of various group attestation schemes that can optimize the resources required to conduct remote attestation procedures for large device groups. A composite device is an entity composed of multiple sub entities. Each sub entity is an Attester. In a composite device we can have multiple Attesters with a Lead Attester. The Attesters are appraised via the main Lead Attester’s help. The lead Attester generates Evidence about the layout of the whole composite device, while sub-Attesters generate Evidence about their respective (sub-)modules. Composite device model is not enough flexible to represent our definition of Attester Group where we do need a leader Attester nor a composition of evidences of the Attesters.

The table below summarizes the key differences between the Group Attester concept and the Composite Device concept.

Composite Device	Attester Group
Lead Attester	No Lead Attester
The Composite Device is identifiable by the Lead Attester	The Attester Group is identifiable by a group-id a unique identifier
Composition of Evidence of sub-modules (Attesters)	No composition

Table 1

4. Attester Group Extension

In Section 3 (Architectural Overview) of [RFC9334]: we could add a subsection 3.4 titled "Attester Groups". In addition, in Section 2.2 of [I-D.ietf-rats-ar4si] about Non-repudiable Identity, we could add an Identity Type "group-id" (i.e add another row in the Table 1 in [I-D.ietf-rats-ar4si]).

5. Use Case Scenarios with a large scale network

In this section, we provide three examples of applications where all devices are homogeneous with similar characteristics.

Use Case 1: Remote maintenance in the aerospace domain

Context: EU ASSURED H2020 Project. Once an aircraft lands, there is the need for the physical presence of an engineer to go and connect to the "head unit" (in the cockpit) for extracting log data so as to check whether something needs to be checked/maintained. We need attestation of all core PLCs and embedded systems responsible for the core functionalities of the aircraft. All attestation reports are remotely sent (in a secure manner) to the control station once landed. We can group the attested elements into different Attester Groups.

Approach: We can consider an Attester Group of 1000 aircrafts (same manufacturing brand)

Use Case 2: Automotive domain, a Vehicle with embedded Electronic Control Units (ECUs)

Context: CONNECT EU H2020 project. The automotive industry is moving to a more hierarchical in-vehicle architecture where ECUs are monitored by Zonal Controllers and these in turn communicate with the Vehicle Computer. This is, for instance, how kinematic data are extracted from the sensors all the way up to the vehicle computer to be encoded into a V2X message. This data need to be associated with Evidence on the integrity of the sensor as a data source and this is where group attestation is an interesting capability. The Attester Group can be formed for hierarchical-based attestation, like Attester Group of all in-vehicle ECUs or attested group of vehicles within an intersection.

Approach: we can consider an Attester Group of a fleet of 70000 vehicles (same brand). We can also consider an Attester Group of similar ECUs.

Use Case 3: AI computing cluster

Context: An AI computing cluster is a composite computing environment composed of a group of computing nodes/chips on which one ore more computing tasks are executed. A user or an application/large model provider needs to verify the integrity of the collected measurement/ evidence information from the composite computing environment.

Challenge: The cluster may contain heterogeneous trusted roots, and the composition may be dynamically updated. Repeated attestation is not efficient if done without context and can be very expensive.

Approach: We can consider a large group of Attesters or a set of group Attesters. An Attester group that maps to the nodes of a cluster that executes a specific task may be dynamically created or dissolved according to the requirements of the computing task. One ore more remote attestation server/Verifier appraise collected evidence/measurements for the entire composite computing environment. The intend of remote group attestation is to hide the complexity of that back-end computing node interaction from customers (the Relying Parties), while still being able to assess its trustworthiness. Generally, a master node in the group is responsible for communicating with the Verifiers (or indirectly with the customer if they triggered remote attestation as a Relying Party), responding to the remote attestation challenge request of the client, collecting evidence claims of all group nodes as a whole, and sending the evidence to the Verifier for appraisal.

When all computing nodes/chips in a computing Attester group are provided by the same vendor or deployed by the same cloud vendor, using a unified and centralized dedicated hardware root of trust can be considered (e.g., hardware security chip, centralized hardware

DIE, or BMC) to offload important security functions (secure storage, security monitoring, etc.) to this independent root of trust module. The trusted boot and other related evidence claims of the group are securely stored on that unified root of trust. During the remote attestation procedure, the master node of the group collects claims aggregated and signed already as evidence by the centralized module. If a single root of trust manages multiple chips, a single point of failure (such as malicious intrusion and system breakdown) of the root of trust affects the security of the entire Attester group managed by the root of trust. The unified trusted root should support distributed and pooled design. Multiple roots of trust may work together to enhance overall security and reliability.

In heterogeneous interconnection scenarios where all computing nodes and chips in a computing cluster are provided by different vendors, it might not be possible to deploy a unified root of trust. During the group remote attestation procedure, the master node needs to communicate with each group node to collect its individual evidence claims. The node evidence is signed by the private attestation key of each node. The master node collects the information, packs the information, and sends it to the remote Verifier for appraisal. The dynamicity of the computing attested group is reflected through the following aspects: * Creation and dissolving of groups is dynamically triggered by the life cycle management of computing tasks the groups execute. The member scale, type, and quantity of evidence claims to be collected are dynamically generated and dynamically change. Before performing remote attestation, customers are required to dynamically obtain all related information through a management system interface. Based on this management information, a template-based remote attestation request message is defined and sent to the master node. * According to the dynamic requirements of computing task functions, performance, and to the trustworthy state changes of member nodes, the overall state of the group (including the state change of each existing node, the exit of the existing node from the group, the addition of a new node to the group, the replacement of the existing node by the new node, etc.) is dynamic. These dynamic changes lead to the need for real-time dynamic update of group remote attestation. Incremental update should also be supported to reduce communication and computing load in large groups. In the process of Attester group, the client can not only integrate the communication key negotiation with the master node, but also support the communication key negotiation with other nodes in the group. Therefore, the key negotiation material is required to be generated by the client and different nodes separately. In addition, each group node that need to communicate can calculate the session key for mutual communication, so as to implement the subsequent establishment of the security channel.

6. Security Considerations

[TBD]

7. IANA Considerations

This document has no IANA actions

8. References

8.1. Normative References

[I-D.ietf-rats-ar4si]
Voit, E., Birkholz, H., Hardjono, T., Fossati, T., and V. Scarlata, "Attestation Results for Secure Interactions", Work in Progress, Internet-Draft, draft-ietf-rats-ar4si-08, 6 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-ar4si-08>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://doi.org/10.17487/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://doi.org/10.17487/RFC8174>.

8.2. Informative References

[I-D.ietf-rats-daa]
Birkholz, H., Newton, C., Chen, L., and D. Thaler, "Direct Anonymous Attestation for the Remote Attestation Procedures Architecture", Work in Progress, Internet-Draft, draft-ietf-rats-daa-07, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-daa-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://doi.org/10.17487/RFC9334>.

Appendix A. Implementation Considerations

Details on creating and maintaining Attester Groups, choosing the number of Lead Attesters, and methods for evidence collection and signing are left to the implementer’s discretion, allowing for tailored security measures.

Authors’ Addresses

Houda Labiod
Huawei Technologies France S.A.S.U.
18, Quai du Point du Jour
92100 Boulogne-Billancourt
France
Email: houda.labiod@huawei.com

Amine Lamouchi
Huawei Technologies France S.A.S.U.
France
Email: aminelamouchi@huawei-partners.com

Jun Zhang
Huawei Technologies France S.A.S.U.
18, Quai du Point du Jour
92100 Boulogne-Billancourt
France
Email: junzhang1@huawei.com

Andrzej Duda
Grenoble INP - Ensimag, LIG Lab
France
Email: Andrzej.Duda@imag.fr

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt
Germany
Email: henk.birkholz@sit.fraunhofer.de