

# Attester Groups for Remote Attestation

draft-labiod-rats-attester-groups

Houda Labiod, Amine Lamouchi, Jun Zhang, Andrezj Duda, Henk Birkholz

RATS Interim meeting

27<sup>th</sup> September, 2024

# Motivation

**Objective:** Reduce computational and communication overhead by enabling collective Evidence appraisal attestation of high number of homogeneous devices with similar characteristics, thereby improving the scalability of remote attestation processes.

Redundant individual appraisal procedures for a large number of identical devices

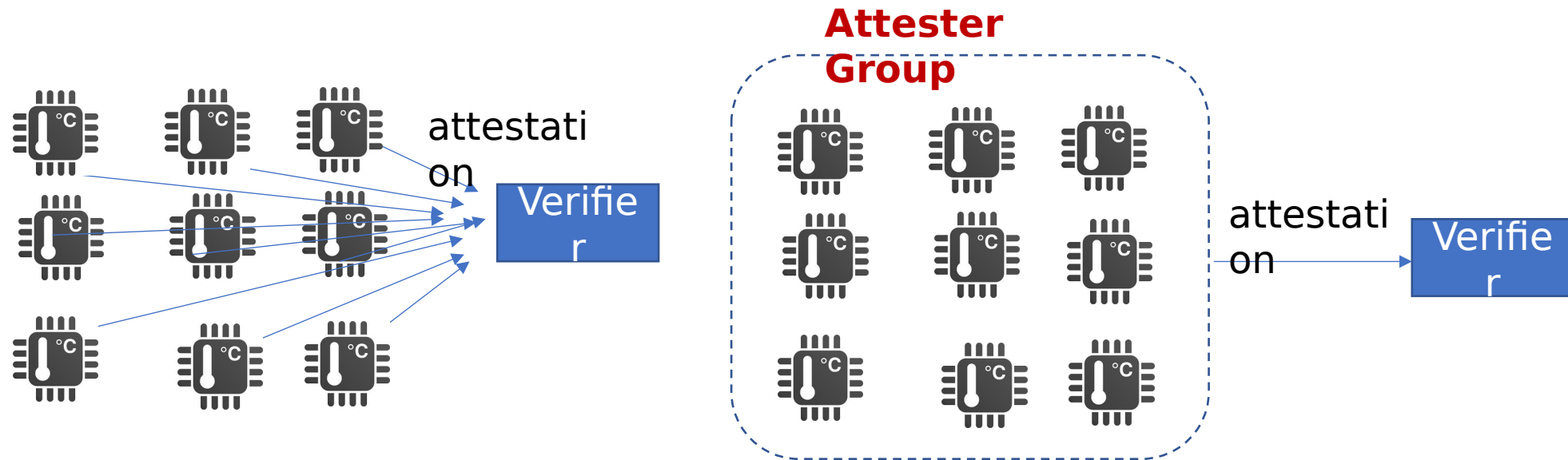


Fig. 1: Attester Group vs. Device attester

## Goal

Propose an extension to the Remote Attestation Procedures architecture as defined in [RFC9334] by introducing the concept of Attester Groups.

# Use Case Scenarios with a large-scale network

All devices are homogeneous with similar characteristics

**Application:** 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 consider an attester group of 1000 aircrafts (same manufacturing brand)**

**Application:** 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. Hierarchical-based attestation - attester group of all in-vehicle ECUs; attested group of vehicles within an intersection (for instance)

**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.**

# Attester Group vs RFC9334 attester definitions

## Background:

In RATS, one peer (the "Attester") produces believable information about itself ("Evidence") to enable a remote peer (the "Relying Party") to decide whether or not to consider that Attester a trustworthy peer. RA procedures are facilitated by an additional vital party (the "Verifier"). The Verifier appraises Evidence via appraisal policies and creates the Attestation Results to support Relying Parties in their decision process.

RFC9334 presents an architectural overview of the entities involved in Remote Attestation Procedures. In particular, it defines an Attester (fig. 1) as « *at least one Attesting Environment and at least one Target Environment co-located in one entity* ». It also presents different ways to compose the Attesting and Target environments such as *Layered Attesters* (fig. 2) and *Composite Devices* (fig. 3).

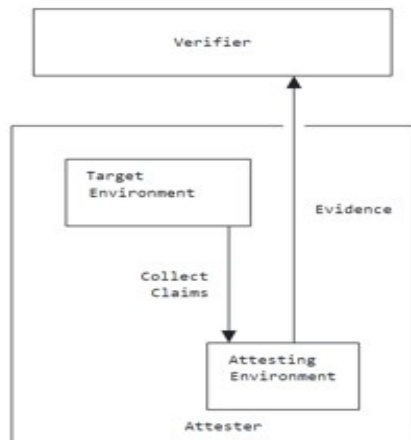


Figure 1: Attester Architecture

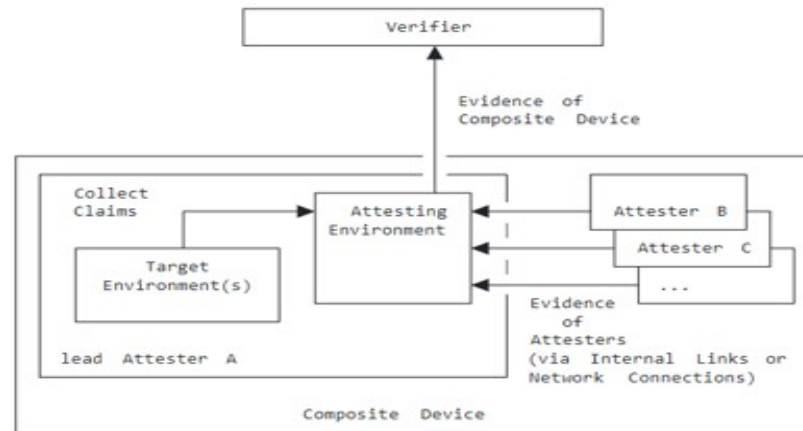


Figure 2: Composite Device

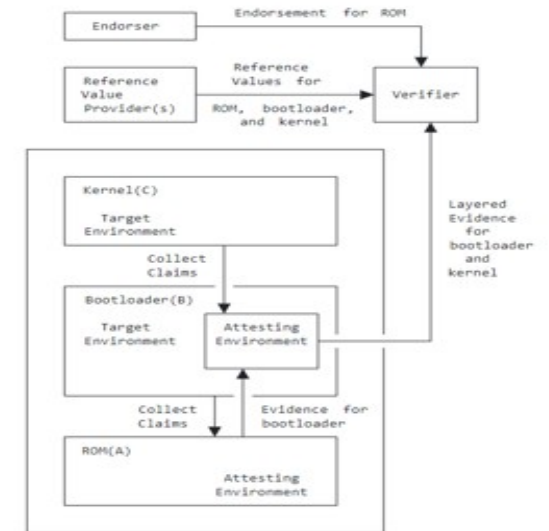


Figure 3: Layered Attester

# Attester Group vs. Composite Device

A composite device is an entity composed of multiple sub-entities. The appraisal of all these sub-entities is needed. Each sub-entity is an attester. In a composite device, we can have multiple attesters with a lead attester. They are managed and appraised via the main lead attester 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.

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: Comparison between a composite device and attester group

# Where will the Attester Group extension be added ?

- In [RFC9334 - Section 3 - Architectural Overview](#): we will add a subsection 3.4 titled « Attester Groups »

## [3. Architectural Overview](#)

### [3.1. Two Types of Environments of an Attester](#)

### [3.2. Layered Attestation Environments](#)

### [3.3. Composite Device](#)

- In the draft [Attestation Results for Secure Interactions - Section 2.2 - Non-repudiable Identity](#): we will add an Identity Type « group-id » (i.e add another row in the table below)

Attester Identity type	Process-based	VM-based	HSM-based
chip-vendor	Mandatory	Mandatory	Mandatory
chip-hardware	Mandatory	Mandatory	Mandatory
target-environment	Mandatory	Mandatory	Optional
target-developer	Mandatory	Optional	Optional
instance	Optional	Optional	Optional

# What next ?

- We should be able to leverage the similarities between attesters to avoid redundant attestations. The Attester Group is by definition a dynamic entity. Attesters can join or leave the group.
  - Define a **new mechanism** ( not based on a composition of evidences)

**Thank you**