Abstract

This document defines a standardized information model (IM) for assertions that can be used in remote attestation procedures (RATS). The information elements defined include attestation assertions which provide information about system components characteristics, as well as commonly used attributes and attribute structures that are required by protocols facilitating remote attestation.

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 January 9, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction ............................................. 2
   1.1. Document Structure ............................ 3
2. RATS Information Elements .......................... 4
3. Security Considerations ............................. 8
4. Acknowledgments ...................................... 8
5. Change Log ............................................. 8
6. Contributors .......................................... 8
7. References ............................................. 8
   7.1. Normative References ......................... 8
   7.2. Informative References ....................... 9
Authors’ Addresses ................................. 9

1. Introduction

Remote attestation procedures (RATS) are used to increase the trust
in the trustworthiness of an attester. This is typically
accomplished by conveying attestation evidence from an attester to a
verifier that is able to appraise the evidence. The exact
definitions of RATS roles, such as an attester or a verifier, are
specified in the RATS architecture [I-D.birkholz-rats-architecture].
This document defines the common information elements (IE) that are
able to express the characteristics of an attester. Ultimately,
these IE can be used to compose attestation evidence (attestation
assertions that are accompanied by a proof of their validity).

In general, RATS convey information elements that:

- enable the functionality of remote attestation protocols,
- are able to express assertions about an attester’s composition,
  configuration, or operational state,
- represent the provenance of assertions, including entities that
  provide assertions on behalf of the attester,
- compose a type of proof of validity with respect to other
  assertions, and that
- are either verifiable (via comparison with trusted reference
  values) or non-verifiable.
1.1. Document Structure

Every information element listed is annotated with one or more of these attributes:

Protocol (P): This IE is used on a remote attestation protocol layer, typically on the control plane or as protocol-specific data plane content.

Hardware (H): This IE expresses characteristics about an attester’s hardware components or the composition of its hardware components.

Software (S): This IE expresses characteristics about an attester’s software components or their semantic relationship. The term software component - in the scope of this document - subsumes firmware, bootloader, BIOS/(U)EFI, and microcode.

Operational State (O): This IE is used to convey information about the combination of applied configuration and system state as defined in [RFC8342].

Verifiable (V): This IE requires reference integrity measurements (RIM), compliance-policy, certification-path, or another type of trust-chain in order to be appraised appropriately by a verifier.

Additionally, every IE definition includes a reference to the source of its definition, if it is not specified in this document for the first time (which is the most likely case). If a source of a definition is not a specification or (proposed) standard, but a draft, a web resource, or source that cannot be attribute with a DOI or ISSN, the following attribute is associated.

Unstable (U): The source of the definition of this IE may change in the future and is not considered to be stable at the time of publication of this document.

Information elements might reference other information elements or have to be associated in a set (with or without a specific order) in order to convey the intended meaning to a verifier. Reference to other IE inside this documents simply use their name as reference. In consequence, an IE can be a superstructure composed of other IE with its own name (and potentially additional definition text that defines its purpose and or usage).

The RATS Information Model allows for expressing a hierarchical taxonomy. If an IE is a specialisation of another IE, the last sentence in the definition includes a "This IE is a specialization of _IE NAME_."
The ordering of IE is in descending alphabetical order; independent of source or semantic relationship to other IE, or other types of hierarchy.

2. RATS Information Elements

Age: The latency between the creation of an assertion value (e.g. by asserters such as a hardware sensors or the Linux Integrity Measurement Architecture) including its composition into attestation evidence and its following conveyance to another RATS Actor/Role in RATS. The Age IE does not require a threshold at which point another information element is considered "old" and an age information element has to be included.

Reference: [I-D.ietf-rats-eat]

Assertion Selection: [P]

A filter expression that enables the conveyance of a subset of all attestation assertions available to the attester, if requested by a verifier.

Attestation Evidence: [H, S, O, V]

A composite IE that must include at least an Authentication-Secret Identifier, an Attester Identity, and at least one Attestation Assertion. Attestation Evidence is always signed via the Authentication Secret and thereby binds the listed information elements cryptographically. Attestation Evidence can only be trusted by a verifier if it is associated with a trust anchor the verifier also trusts.

Attester Identifier: [P, O, V]

A value associated or bound to a distinguishable attester that is intended to uniquely identify it, but is not directly associated with a trust anchor. Additional Endorsement Documents can increase the level of confidence in an Attester Identifier.

Attester Identity: [P, S, V]

A document about a distinguishable attester issued and signed by a third party. If not cryptographically associated with a trust anchor directly or indirectly, this IE is a specialization of Attester Identifier.

Attestation Result: [P]
A set of one or more values that are created by an appraisal action of a verifier. Attestation Result is the most generic definition of the output of RATS and are typically consumed by relying parties.

Authentication-Secret Identifier: \([O, V]\)

An identifier that is associated with an authentication secret used to sign attestation evidence.

Authorization Challenge: \([P]\)

The input to an challenge-response protocol hand-shake. This IE can be Nonce, but also the output of a local attestation procedure.

Reference [I-D.tschofenig-rats-psa-token]


A document about the capabilities and functionality of one or more sub-components of a distinguishable attester issued and signed by a third party. Endorsement Documents are intended to render Attestation Evidence trustworthy. If not cryptographically associated with a trust anchor directly or indirectly, this IE is a specialization of System Component Identifier.

Location: A global standardized set of coordinates and related attributes representing the geographic position of a device based on a geodetic system, such as Navstar GPS. The coordinate values can have different meaning with respect to the geographic position of a device depending on the geodetic system used. The default is WGS-84.

The basic location attributes include: latitude, longitude, altitude, accuracy, altitude accuracy, heading, and velocity.

Reference [I-D.ietf-rats-eat]

Measured Boot Characteristics: \([H, S, V]\)

If every piece of software is measured by a root-of-trust for measuring during boot time and across staged computing contexts (e.g. UEFI, Bootloader, Kernel, Rich OS), associated information about how and in which operational states these measurements are conducted is vital to RATS. This IE represents several states of a (composite) device with respect to measured boot (previously often called secure boot) including: "Secure Boot Enabled", "Debug
Disabled", "Debug Disabled Since Boot", "Debug Permanent Disable", "Debug Full Permanent Disable".

Nonce: [P]

An information element with two major uses: the prevention of replay-attacks and as an IE that can be used in a challenge-response interaction model. It is created by the requester to provide evidence about the freshness of the corresponding response. It is important to highlight that a nonce by itself does not protect from relay-attacks.

OEM Identifier: [H, S, V]

A organizationally unique identifier (OUI) assigned by the IEEE Registration Authority (IEEE RA). This IE is associated with a device or a distinguishable sub-component of a composite device with its own computing context. It intended to identify a device(component) during its life-cycle. This is a specialization of System Component Identifier.

Reference [I-D.ietf-rats-eat]

Origination: [P, S, V]

An IE representing attestation provenance. Attestation Assertions or Attestation Evidence are produced by a specific source of information that is intended to be uniquely identifiable. The source of information is a distinguishable computing context (see [I-D.birkholz-rats-architecture]) of a device or the sub-components of a composite device.

Reference [I-D.ietf-rats-eat]

Universal Entity ID: [P, H, V]

A unique identifier permanently associated with an individual manufactured entity / device, such as a mobile phone, a water meter, a Bluetooth speaker or a networked security camera. This IE is intended to either identify an device or a submodule or subsystem of a device. It does not identify types, models or classes of devices. It is akin to a serial number, though it does not have to be sequential. This IE is a specialization of System Component Identifier.

Reference [I-D.ietf-rats-eat]

Uptime: [H, S]
An IE representing the number of seconds since the first computing context of a (composite) device is able to measure it.

Reference [I-D.ietf-rats-eat]

Security Level: [H, S, V]

A level of confidence with respect to the resilience against attacks intended to compromise attestation evidence. A Security Level can be associated with an Origination. This IE is context specific and requires a scope-specific definition of values as part of a security framework. The [I-D.ietf-rats-eat] document, for example, provides an enumeration of security levels that is similar to the Metadata Service defined by the Fast Identity Online (FIDO) Alliance.

Reference [I-D.ietf-rats-eat]

Software Component Identifier: [S, V]

An IE representing one or more distinguishable Software Components [I-D.ietf-sacm-terminology] that were loaded and measured by an appropriate root-of-trust. The use of this IE typically requires the use of Measured Boot.

Reference [I-D.tschofenig-rats- PSA-token]

System Component Identifier: [H, S, V]

An identifier intended to uniquely identify a distinguishable system component. System components can be hardware components or software components (e.g. a virtual machine). The system component can be an "atomic" device (i.e. a composite device with only one hardware component) or a part of a composite device.

Timestamp: [P, S]

A generic information element that represents a certain point of time in the past. The level of confidence in the value of a timestamp is based on the trustworthiness of the source of time, which can be local or remote, a composite of multiple time sources to represent the state synchronization, as well as the precision and the accuracy of the source of time itself.

Timestamps can be time-zone specific and therefore change their meaning if the definition of time zones changes.

Verification Service Indicator: [P, S, V]
This IE provides a hint (typically consumed by a Relying Party) that enables the discovery of an appropriate Verification Service or Remote Attestation Service, e.g. a URL.

Reference [I-D.tschofenig-rats-psa-token]

3. Security Considerations

Probably none

4. Acknowledgments

TBD

5. Change Log

Initial version -00

6. Contributors

TBD

7. References

7.1. Normative References

[I-D.birkholz-rats-architecture]

[I-D.birkholz-rats-basic-yang-module]

[I-D.birkholz-rats-tuda]
Fuchs, A., Birkholz, H., McDonald, I., and C. Bormann, "Time-Based Uni-Directional Attestation", draft-birkholz-rats-tuda-00 (work in progress), March 2019.

[I-D.ietf-rats-eat]
7.2. Informative References

[I-D.birkholz-rats-reference-interaction-model]

[I-D.ietsacm-terminology]

[I-D.richardson-rats-usecases]

Authors' Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
Darmstadt 64295
Germany

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

Email: michael.eckel@sit.fraunhofer.de