RATS YANG Module for Challenge-Response-based Remote Attestation Procedures using TPMs

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Michael Eckel <michael.eckel@sit.fraunhofer.de>,
Shwetha Bhandari <shwethab@cisco.com>,
Bill Sulzen <bsulzen@cisco.com>,
Eric Voit <evoit@cisco.com>,
Liang Xia (Frank) <frank.xialiang@huawei.com>,
Tom Laffey <tom.laffey@hpe.com>,
Guy C. Fedorkow <gfedorkow@juniper.com>,

IETF 111, notinsanfrancisco, July 26th 2021, RATS WG
Document Status

• I-D depends on the RATS Architecture and RIV to clear
  • Made the reference to the RATS Interaction Models informative
• xml2rfc outdenting issue
  • Editorial issue that is probably not a blocker, tried working around that via kramdown-rfc2629 hotfixes in v1.5.5 with mixed success
• YANG Doctors comments seem to be all addressed, waiting for further feedback
• Next steps?
RATS Reference Interaction Models for Challenge-Response/Time-Based/Streamed Remote Attestation

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Michael Eckel <michael.eckel@sit.fraunhofer.de>,
Wei Pan <william.panwei@huawei.com>,
Eric Voit <evoit@cisco.com>,

IETF 111, notinsanfrancisco, July 26th 2021, RATS WG
Document Status

• Effective final issue was:
    (Authentication Secret)

• The proposal in the remaining PR #43 was vetted and is now considered to be out-of-scope. Some parts of it might move to a new document and some parts of it could move to existing I-Ds.

• Proposal for next step: request for WGLC
RATS  Direct Anonymous Attestation

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Christopher Newton <cn0016@surrey.ac.uk>,
Liqun Chen <liqun.chen@surrey.ac.uk>,

IETF 111, notinsanfrancisco, July 26th 2021, RATS WG
Document Status

• Around IETF 110, this I-D has been split out of:
• -00 received a good amount of pre-adoption reviews and comments:
  • Thanks to Hannes, Thomas, Wei, Laurence, Ned, and Guy!
• Recent feedback is primarily reflected in new Privacy & Security Considerations content:
  • https://www.ietf.org/rfcdiff?url2=draft-birkholz-rats-daa-01.txt
• Dave Thaler joins the authors team. Welcome!
• Proposal for next step: Request for WG adoption call (WGAC)
Describing Attesters to Verifiers: Concise Reference Integrity Manifests

https://datatracker.ietf.org/doc/draft-birkholz-rats-corim/

Ned Smith <ned.smith@intel.com>,
Yogesh Deshpande <yogesh.deshpande@arm.com>,
Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Wei Pan <william.panwei@huawei.com>,
Thomas Fossati <thomas.fossati@arm.com>,

IETF 111, notinsanfrancisco, July 26th 2021, RATS WG
RATS Architecture, Conceptual Data Flow in [https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-1](https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-1)
Problem Statement

One or more authorized supply chain actors (OEM, ISVs, SiPs, etc.) need to come together and "describe" an Attester to a Verifier. So, when Evidence from that Attester is passed on to the Verifier, it can use the attributes that apply to the Attester to appraise Evidence against the Appraisal Policy.

Without a standard Information Model / Data Model there is no standard tooling to reduce fragmentation or lower barriers to entry for the supply chain actors.
Problem Context & Scope

The descriptive material that flows from the supply chain to the Verifier can be, for example:
• Measurements, for example, FW – "Reference Values"
• Verification key material, certification status – "Endorsements"

It is also necessary to describe the composition of an Attester from its relevant parts (i.e., its Attesting and Target Environments):
• This is not necessary for very simple attesters (AE:TE=1:1) but can come in handy for more complex topologies where the device structure is reflected in the Evidence structure (e.g., via submodules in EAT).
• Also, it can be useful for factoring out common parts that are reused across different Attesters.

Out of scope – at least for the moment – is the delivery of Verification Policies to the Verifier by the Verifier Owner.
RATS Architecture, Conceptual Data Flow in [https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-1](https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-1)
High-Level Design

• Graph Data models (RDF-like) with its own specialized vocabulary and data types

• The "triple" is the core pattern

• Used to define an Attester "ontology" (actually a simple directed property graph)

• Tracking triples provenance via explicit cryptographic methods

• Concise representations (**CoMID, CoRIM**)
  • Concise Module Identifier are the "hardware component" complement (including firmware) to CoSWID [https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/](https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/), which are already used to represent software components.
  • Concise Reference Integrity Manifests are the trustworthy bundles of CoMID and CoSWID
What Kind of Triples Do We Need?

• Reference Values associated with a Target Environment
• Endorsements associated with an Attesting or a Target Environment
• Cryptographic identities associated with Attesting Environments
• Decomposition of a device in its constituent Attesting and Target Environments and their relational features
• Others that we haven’t yet anticipated (built-in extensibility)

• Examples (coming up in the next slides)
Reference Value Statements

Target Environment

“has reference values”

Reference Values

class-id=123abc...

m0=0xfade0000...
m1=0xfade1111...
m2=0xfade2222...
m3=0xfade3333...
m4=0xfade4444...
m5=0xfade5555...
Endorsed Value Statements

Target Environment

“has endorsed values”

Endorsed Values

Endorsed Value Statement

class-id=123abc…
cert-id=0716053550040
Cryptographic Identity Statement

Attesting Environment  "has cryptographic identity"  Key Material

instance-id=xyz789...

key=
-1:1,
-2:h'bac5b11cad8f...',
-3:h'20138bf82dc1...',
1:2,
2:'11'
Next Step: Composition Patterns

• Attester (de)composition
  • i.e., relationships between Attesting and Target Environments within an Attester
Next Step: Composition Patterns (cont.)

• Device layering
  • i.e., how different Attesters come together in a composite device
Next Step: Composition Patterns (cont.)

It turns out that both can be expressed with the same statement:

\[
\text{Attesting Environment} \{\text{class-id}\} \text{ retrieves } \{\text{"claims"|"evidence"}\} \text{ by } \{\text{"active"|"passive"}\} \text{ collection over } \{\text{"trusted"|"untrusted"}\} \text{ path from Environment } \{\text{class-id}\}
\]

where the "object" Environment could be either a Target Environment or another Attesting Environment in a sub-Attester.

Note: There is also a separate statement to describe the environments that compose a certain Attester. (This is effectively just a grouping overlay on top of a device decomposition that can be fully described by the statement above.)
- BIOS retrieves claims by active collection over trusted path from Boot Loader
- Boot Loader retrieves evidence by active collection over trusted path from BIOS
- Boot Loader retrieves claims by active collection over trusted path from Kernel

Based on RATS Architecture, Layered Attester  [https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-3](https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-3)
Next Step Example: Composition Statement

"retrieves claims by active collection over trusted path from"

Attesting Environment  | Target Environment

Composition Statement

data-type=claims
collection-type=active
path-type=trusted

class-id=123abc...
class-id=456def...
CoMID &CoSWID Usage: Grouping Statements

• Similar to CoSWID, CoMID tags are the wrapper around a bunch of statements, but pertain to hardware and firmware

• Like CoSWID tags, CoMID tags allow grouping, identification, typed linking (e.g., *supersedes*, *updates*) with other tags, plus some further encoding optimization in CoMID (e.g., if the statements subject is always the same it can be factored out)

• Grouping criteria are use-case specific. We can *suggest* a few (e.g., for handling FW updates), but we expect best practices to emerge with time and use
CoRIM Usage: Grouping Groups of Statements

• CoMIDs and CoSWIDs are grouped into CoRIMs
• CoRIMs are signed by the relevant supply chain actor
• Used as the end-to-end conveyance payload (we don’t define the transport)
• The outer signature augments the triples in the CoMID statements with provenance:
  • “Supply chain actor X says ${CoMID-statement} and/or ${CoSWID-statement}”
Pulling All Together

Navigating the sea of triples allows a Verifier to construct a comprehensive device/attester description that it can use as the backdrop against which its Appraisal Policy for Evidence is evaluated.
TL;DR

- Information Model Design Authority: TCG DICE WG
- work-in-progress
- Keep an eye on
  - https://github.com/ietf-rats/ietf-corim-cddl
  - https://github.com/ietf-rats/draft-birkholz-rats-corim
  - https://github.com/thomas-fossati/draft-psa-endorsements
This slide is intentionally left...

• ... almost blank
And a few more...

• Attester’s private key has certification path x5chain
• A and B are aliases for Attester
• Attester is a member of Group
• <insert your statement here, the format is extensible>
Key

AE

"is instance of"

AE₀

"has crypto identity"

TE

"has endorsed values"

"has reference values"

"retrieves claims ...

key=val

key=val

key=val
"has crypto identity" 

"is instance of" 

"retrieves claims ..." 

"has endorsed values" 

"has reference values"