IETF 112 RATS WG
Concise Reference Integrity Manifests

12 November 2021, Session II, notinmadrid

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

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

Internet Engineering Task Force

Production by Meetecho

IETF®

Quick Recap on CoRIM

- Mission Statement: a "sea of triples" to describe Attesters to Verifiers
- Initial cut includes:
  - Reference values
  - Verification key material
  - Endorsed values (e.g., certification status of a module)
- Also, eventually:
  - Representation of allowed/expected hierarchical composition of modules in an Attester
  - A module's firmware life-cycle (i.e., update/patch)
  - Anything else! – bring your own triple to the group and we'll do design team sessions

Extensibility and widely available codepoints!

(see RATS Architecture Figure 9: Multiple Attesters and Relying Parties with Different Formats)

CoRIM Applicability

- TCG DICE (by definition, especially to Layered Attestation)
- ARM PSA Token, an EAT profile (see draft-fdb-rats-psa-endorsements)
- Concise TPM-based Evidence in enterprise setting

Flexibility and Interoperability!

Specs Status

- Information model described in TCG's "DICE Endorsements Architecture" (under ballot, not yet public, a matter of weeks)
- Data Model specified in https://www.ietf.org/archive/id/draft-birkholz-rats-corim-01.html
  - Bleeding edge CDDL @ github.com/ietf-rats/ietf-corim-cddl

Implementation Status

Go packages (Apache 2.0 license, closely tracking upstream spec):

- https://github.com/veraison/corim/corim
  - Low-level CoRIM manipulation – CBOR, JSON (bespoke) codecs
- https://github.com/veraison/corim/comid
  - Low-level CoMID manipulation – CBOR, JSON (bespoke) codecs
- https://github.com/veraison/swid
  - CBOR (CoSWID, draft-ietf-sacm-coswid) and JSON (bespoke)
  - XML (SWID, ISO/IEC 19770-2:2015, NISTIR-8060),
- github.com/veraison/corim/cocli
  - Command Line Interface to deal CoRIMs, CoMIDs and CoSWIDs, for the (supply chain) end user

CoRIM & the RATS Charter Scope – Charter Goals

- Current charter's **goals addressed by CoRIM**
  - CoRIM **standardizes formats for describing assertions about system components** in the form of reference values, endorsed values, and environment endorsements based on their environment identity. These **assertions are directly associated with Evidence** as they are used in the appraisal procedures conducted by Verifiers in order to generate Attestation Results
  - CoRIM **content is protected using COSE signing capabilities**
  - CoRIMs are **intended to be consumed by Verifiers** (and not Relying Parties) and they suppliy the data inputs that enable a Verifier's appraisal procedures. The inputs originate from supply chain entities. CoRIMs **do not supply Appraisal Policies for Verifiers** in support of their appraisal procedures.
  - CoRIMs are specified **in collaboration with several supply chain stakeholders** that provide solutions for Attesting Environments designs and **in cooperation with the TCG**

CoRIM & the RATS Charter Scope – Charter Deliverables

- Current charter's **program of work defined deliverables addressed by CoRIM**
  - CoRIM involves the "system component providers" (e.g., OEM or ODM) by enabling them to provide conceptual message content, such as reference values about the Attester, endorsed values about the Attester and requirements (i.e., identity identifiers) on signing key material of the Attester, which is content of **deliverable two**.
  - CoRIM specifies a manufacturer's, OEM's, and others supply chain entities' requirements on providing information about system components characteristics of an Attester (described in, e.g., use case 2.1, 2.3, or 2.4), which is content of **deliverable three.**
  - CoRIM also standardizes a corresponding to data model the implement and secure the defined information model using a COSE like manifest similar to SUIT, which is content of **deliverable four**.

Next Step: Call of for WG Adoption (WGAC)

- Editor's version work items are documented in:
  - https://github.com/ietf-rats/draft-birkholz-rats-corim/issues
    - 8 open, 34 closed
  - https://github.com/ietf-rats/ietf-corim-cddl/
    - 26 open, 63 closed
- The editor's version is now in a fairly stable state
- It's the output of eleven months of thrice-weekly design meetings involving multiple Attesting Environments manufactures and various cross-SDO inputs and corresponding consensus
- The authors think this document is ready for adoption and in alignment with the current RATS charter