CoRIM

https://datatracker.ietf.org/doc/draft-ietf-rats-corim/03
I-D Health: Key Progress (from IETF 117)

• Miscellaneous editorial enhancements
• Alignment with draft-dthaler-rats-endorsements-03
• Clarified scope on cardinality of CoBOM
• Handling Extensions
• More details on Verifier algorithm
• github health: 9 issues resolved 26 new issues created
Enhancements

• CryptoKey Enhancements
  a. Introduced cryptokeys that are protected by Target Environment
  b. Rules specified for how the keys need to be compared

• Optional `Authorized-by` added to `measurement-map` to state the `authority` of the supply chain issuing measurements

• Clarification on some key terms that are used to explain appraisal procedure
Alignment with RATS Endorsements
(draft-dthaler-rats-endorsements-03)

Striving for full alignment

Work in progress on two fronts:

1. Terminology
   a. actual state / accepted claims set (ACS)
   b. reference state / reference values
   c. conditionally endorsed values
   d. identity endorsement

2. Simplified appraisal procedure
**Concise Bill Of Material (CoBOM)**

- A means to activate a list of related CoMID and CoSWID tag identifiers for a given appraisal procedure

- CoBOM has:
  a. A unique BoM Identifier AND
  b. A `concise-bom-tag` structure that contains the list of CoMID and/or CoSWID tag identifiers

- A CoBOM is packaged in a CoRIM

- CoMID and CoSWID tags need not be part of the same CoRIM that contains a CoBOM

- Verifier policy determines which authorities are expected to create CoBOMs

- Appraisal Policy for Evidence specifies the CoBOM requirements
  a. 0,1.. N CoBOMs may be required
  b. When no CoBOMs are required, a CoMID/CoSWID tag is activated as soon as it is processed
  c. When 1 CoBOM is required, a designated authority activates the tags.
  d. Still under discussion: When multiple CoBOMs are required?
Extensions

• The base CoRIM data definition is described using CDDL[RFC 8610]
• Only where sockets are introduced, base CoRIM data definition can be extended
• It is a framework to introduce controlled flexibility in the specification

Why are extensions needed?
  a. To meet certain vendor specific requirements
  b. To meet any proprietary requirements
  c. It is not possible to predict future use cases, hence they allow long term specification relevance
Extensions

• Two Types of CDDL sockets (extension points)
  ▫ Group Choice Sockets (for maps), using the naming convention $$NAME-EXTENSION
  ▫ Type Choice Sockets, using the naming convention $NAME-type-choice

• Sockets must be documented to enable interoperability

• CoRIM profiles explain how extensions are exercised

• Progress from IETF 117
  • Clarified extension points in the draft and tidied up specific semantics wherever applicable

• Practical examples
  • https://datatracker.ietf.org/doc/draft-fdb-rats-psa-endorsements/
  • https://datatracker.ietf.org/doc/draft-cds-rats-intel-corim-profile/
Improvements to Evidence Collection Phase

• Clarified the concept of Accepted Claim Set (ACS), represents the format required for Evidence Appraisal
• ACS also depicts the state of Verification at a given time
• ACS contains Evidence claims from Attester, once the integrity of Evidence is Verified
• ACS may also contain Endorsements, once the Reference Values match the Evidence Claims
A common activity in appraisal of actual state is adding Conditional Endorsements to the Accepted Claims Set (ACS)
  i. These Endorsements are only added when the ACS is in a particular state
  ii. For example, if a Target Environment digest is A then endorse with version B

Conditional Endorsements are a class of triple that has conditional matching semantics

The scope of the conditional statement of a conditional endorsements is currently under discussion
  a. Scoped context uses the place holder name “group”
  b. The design team is discussing what comprises a group and how appraisal functions manage grouping contexts correctly