CoRIM

https://datatracker.ietf.org/doc/draft-ietf-rats-corim/04/
Agenda

• Status and Progress
• General Tidy Up
• Enhancements
• Verifier Algorithm - Simplification
Status and Progress

Total GitHub Issues = 69

Pending Issues = 24

- Tags & Registry related issues = 5
- Spec Text Clarification = 8
- Verifier Algorithm Improvement = 11

Enhancements for Future Releases = 45

Progress since IETF 118
- 8 issues resolved 17 new issues created
General Tidy Up

• Tightened the usage of “profiles”

• Discussed extensibility in more detail
  ○ Extensibility using positive code points registered with IANA and documented separately
  ○ Vendor defined extensions using negative code points

• Added clarity on key terms used (example Accepted Claims Set)
Enhancements

• Added “Tagged Bytes” as a new Identifier Type, in the specification
  • Useful type to model variable length Identity in Class, Instance, or Group Identity
  • Example include, Instance Identity of Arm CCA Realm and AMD SEV-SNP Chip Identifier

• Added “Integrity Registers” as one of the Measurement Values
  • Used to model one or more named `measurement object`
  • Each measurement object has a unique identifier and one or more associated digests
  • Integrity Registers provide a mechanism to model TPM PCRs or Workload Measurements pertaining to an Environment
Enhancements

• There are cases, when Reference Value matching needs to span multiple Environments/sub-environments for a given Endorsed Value to be associated to a Target Environment

• Use case examples include

a. A security certification only granted to an Attester that runs a combination of certain software component(s) at a specific version

b. A composite Attester achieving a benchmark, only when a given combination of Target Environments (sub-Attesters) running a specific revision and configuration
Enhancements

• A new triple known as “Multi - Environment Conditional (MEC) Endorsement Triples Added”
  • Triples describing a series of Endorsements that
    • are applicable based on acceptance of a series of Stateful Environment Records

• A `mec-endorsement-triple-record` has following parameters

  ➢ Conds : all target environment, along with specified state, that need to match state-triples entries into ACS

  ➢ Endorsements : endorsements that are added to the ACS state-triples, if all conditions match
Verifier Algorithm - Simplification

• Introduced layers of Evidence Matching
• Plan to retain basic layer (relevant to all use cases) in the main parts of the specification
• More advanced stage verification will be moved to Appendix