CoRIM

https://datatracker.ietf.org/doc/draft-ietf-rats-corim/02/

Yogesh Deshpande

Agenda

- Content Topics
  - I-D **progress** "health"
  - Readability of **Introduction**, better addressing fresh readers
  - Section 5 **Verifier behavior**
  - **Pre-allocation** of CBOR tags? **Earmark concept**
- Current Issue: Changes of state in multiple CoRIM
- Every document has a life-cycle
  - But CoRIMs always compose a set of active CoRIM tags from multiple authorities (governed by a CoBOM tag) that are relevant to appraise of a product
    - Life-cycle of **CoBOM** tags
  - How to create a set of CoRIMs from multiple authors/authorities?
    - How to produce update CoBOMs

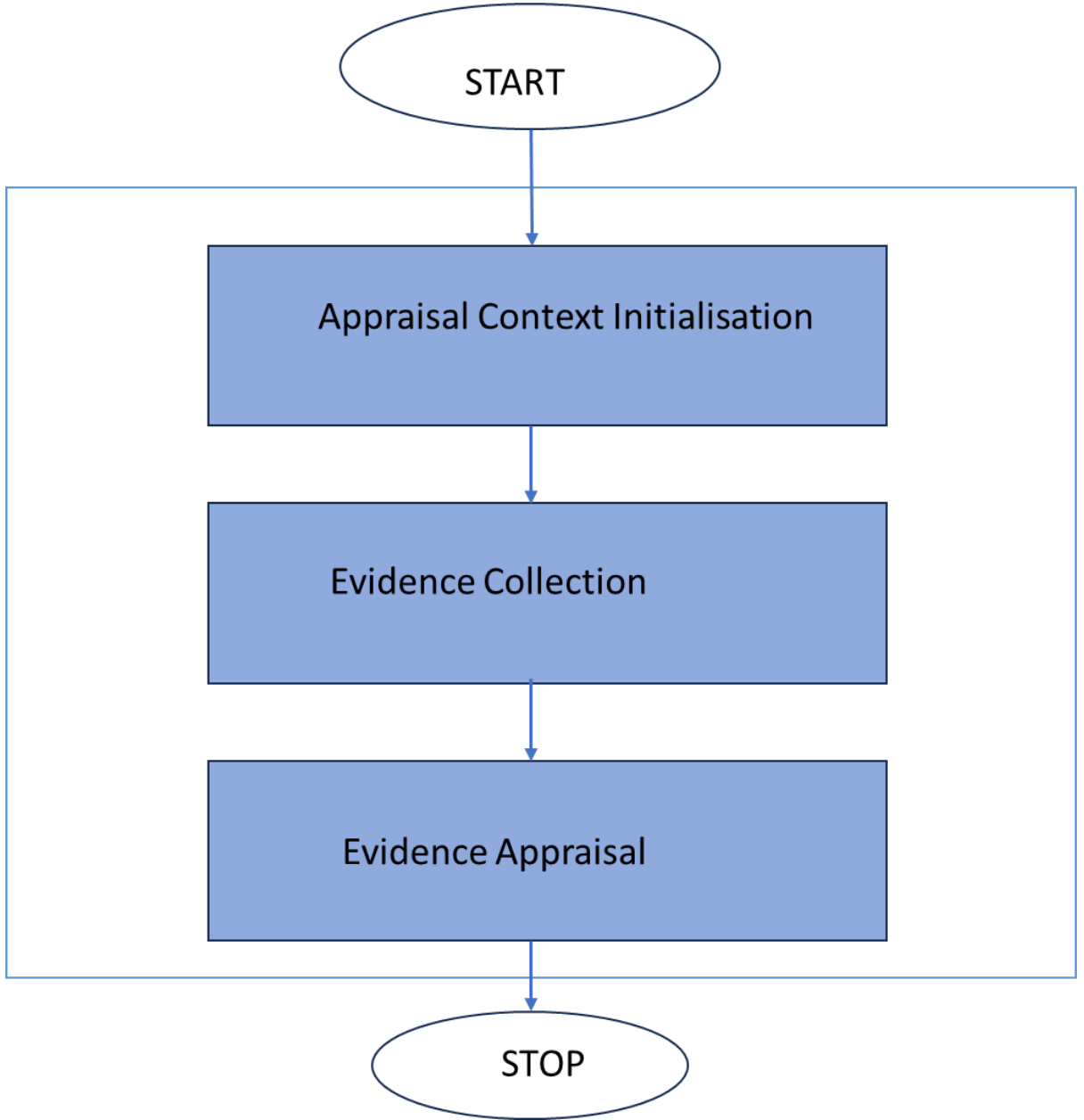
I-D Health: Key Progress (from IETF 116)

- Updated placeholder Introduction text, highlighting the requirements for CoRIM standardization
- Increased level of detail of CoRIM and CoMID description & enhanced readability, significantly
- Added high-level **appraisal workflows** (note: might need better term)
- Clarified the need and usage of CoRIM profiling
- Augmented `tagged-cose-key-type` to have COSE_Key and COSE_KeySet
- Pre-allocation of `cbor-tags`?
  - 15 defined tags ready for **early allocation** today!
  - tag-range 500-599 is "**earmarked**" for future allocations (experimental!)
- Github Health: 10 issues resolved, and 15 new issues created

CoRIM Based Appraisal of Evidence

- New Section 5 added description of how Verifiers use CoRIM documents
- Required for multiple usage scenarios:
  - Verifier is associated with a Relying Party
  - Multiple CoRIMs are produced by the supply chain
  - Each CoRIM can be produced by a different (supply chain) entity
  - CoRIMs are updated over time (e.g., after firmware or device composition change): updates do not necessarily "outdate" all current CoRIMs; the CoBOM will tell you
- Providing a standard reference implementation for Appraisal Procedures
- Comparison has three steps

Abstract Evidence Appraisal Flow



Step 1: Appraisal Context Initialization

- In this step, the Verifer acquires and processes CoRIM files
- Signatures of CoRIM documents are checked
  - CoRIMs without acceptable signatures are silently ignored
- Verifier semantically composes all triples from all acceptable CoRIMs
  - Information from aggregated CoRIMs can be used for multiple appraisal procedures

Step 2: Evidence Collection

- Verifier runs Evidence collection protocols
  - These protocols acquire Evidence from Attesting Environments
  - Multiple Evidence Collection protocols can be supported
- Verifier runs cryptographic authenticity checks of Evidence
  - Required checks are specified by collection protocols
- Verifier transforms Evidence acquired by collection protocols into a standard representation
  - No constraint on data structures within the Verifier
  - Current I-D provides transformation procedures how to convert DICE and SPDM Evidence
  - Additional Evidence transformation procedures for different types of Evidence formats can be part of a CoRIM profile I-Ds or separate specifications

Step 3: Evidence Appraisal

- In this step the Verifier compares Reference Values in CoMID triples against Evidence

- Still working on the details of this step
  - There is a proposal for how to compare a single Reference Value against Evidence
  - Discussions on Attester Composition and how to handle Evidence appraisal

Current Topics in Weekly Meetings

Topics:

1. How to model composite Attester Endorsements using CoRIM
2. How to model life-cycle events (e.g., production, replacement, X-ing) related to Reference Values, Endorsed Values and Conditional Endorsed Values