CoRIM

IETF 123

Early Adopters

Organization	Reference
NVIDIA	NVIDIA Device Attestation and CoRIM-based Reference Measurement Sharing v2.0
Intel	https://www.intel.com/content/www/us/en/content-details/783079/device-attestation-model-in-confidential-computing-environment.html
Altera	https://github.com/altera-opensource/verifier
Arm/Linaro/AMD	https://github.com/veraison/corim AND https://github.com/veraison/corim-rs
Oracle	https://fosdem.org/2025/schedule/event/fosdem-2025-5259-remote-attestation-in-the-cloud/
Google	https://www.ietf.org/id/draft-deeglaze-amd-sev-snp-corim-profile-02.html
AMD	https://www.ietf.org/id/draft-deeglaze-amd-sev-snp-corim-profile-02.html,
SOLIDIGM	https://www.solidigm.com/support-page/drivers-downloads/ka-01851.html

Note: Open Compute Project (OCP) has embraced CoRIM

Reviewers Needed

The document is ***big***

We need feedback to understand if we are on the right track

Goal:

- Authors view: Document is ready for **WGLC**
- Plus: **directorate reviews** (Sec, ART and OPS)

Changes since -07

See draft-ietf-rats-corim-08 release notes

Key Highlights

- Work receding as the document is maturing:
  - 14 issues closed
  - 16 Pull Request merged
  - Feature set is frozen

Changes since -07

Main Enhancements:

1. Support for Integer Ranges
2. Domain Membership Triples-
    I. Definition
    II. Internal Representation
    III. Processing Algorithm Added
3. Mandated single Signer requirement in CoRIM Entity Map

Int - Range

- A new code point in measurement values map
- Describes an integer value used to compare against a linear order in a target environment

```
measurement-values-map = non-empty<{
? &(int-range: 15) => int-range-type-choice   }
```

```
int-range-type-choice = int / tagged-int-range
tagged-int-range = #6.564(int-range)
int-range = [min: int / negative-inf, max: int / positive-inf]
positive-inf = null; negative-inf = null
```

Int – Range - Comparison

CONDITION	ENTRY	Outcome = TRUE
int	int	When both are equal
int-range	int	Range Inclusion: TRUE if Entry >= Condition.Min AND Entry <= Condition.Max
int	int-range	ONLY if Entry.Min == Entry.Max == Condition
int-range	int-range	Range subsumption All values of Condition range MUST be included in Entry Range

Domain Membership Triple (DMT)

What is a Domain ?

Hierarchical description of a Composite Attester in terms of its constituent environments & their compositional relationships

What is the purpose of a DMT ?

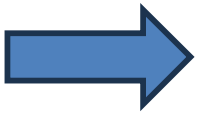
- A DMT links a domain-identifier to its member Environments, which in themselves can be domain-identifiers
- Allows Endorsers to issue an authoritative statement about the composition of an Attester (as a collection of Environment)
- Used by a Verifier to match a Reference composition to actual composition (reported in an Evidence)

DMT Internal Representation

DMT

domain-type = environment-map

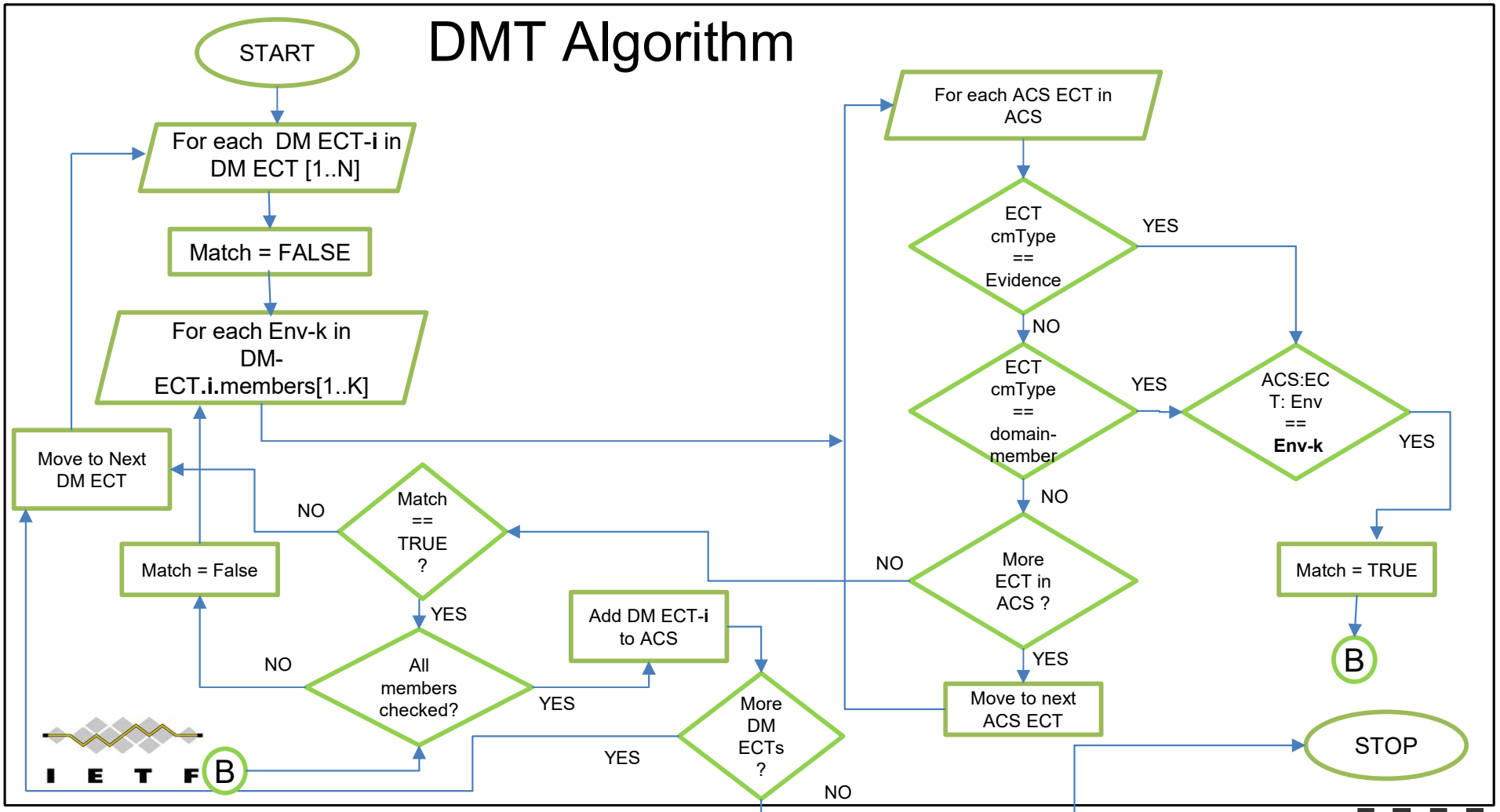
dmt-record = [
  domain-id: domain-type
  members: [+ domain-type]
  ]



Domain ECT Structure

ECT = {
  ? environment: environment-map ➔ **domain-id**
  ? element-list: [+ element-map]
  ? authority: [+ $crypto-key-type-choice]
  ? **members: [+ environment-map]**
  cmtype: **domain-member**
  ? profile: $profile-type-choice
}

I E T F


DMT Algorithm
START
For each DM ECT-i in DM ECT [1..N]
Match = FALSE
For each Env-k in DM-ECT.i.members[1..K]
Move to Next DM ECT
Match = False
Match == TRUE ?
NO
YES
All members checked?
NO
YES
Add DM ECT-i to ACS
More DM ECTs ?
YES
NO
For each ACS ECT in ACS
ECT cmType == Evidence
YES
NO
ECT cmType == domain-member
YES
NO
ACS:ECT: Env == Env-k
YES
Match = TRUE
B
More ECT in ACS ?
NO
YES
Move to next ACS ECT
STOP
I E T F
B

Tidy Up/Bug Fixes

1. Clarified Reference Values processing
2. Fixed Normative Language
3. Corrected ambiguous Instance ID semantics
4. Corrected EAT UEID definition

IETF