CoRIM

IETF 122

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	https://github.com/veraison/corim
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

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

Ideally:

- **WGLC** is really needed
- Plus: **directorate reviews** (Sec, ART and OPS)

Changes since -06

See draft-ietf-rats-corim-07 release notes

Key Highlights

- A lot of work done:
  - 67 issues closed
  - 35 Pull Request merged
  - Number of new issues decreases as the draft matures

Changes since -06

Main Enhancements:

1. Split Triples in two buckets: MTI and OTI
2. Support for usage of Unsigned CoRIM, with authority
3. Simplified syntax for raw-value and matching rules
4. Internal representation of cryptographic keys with examples
5. Added IANA registries for all the extension points

MTI vs. OTI

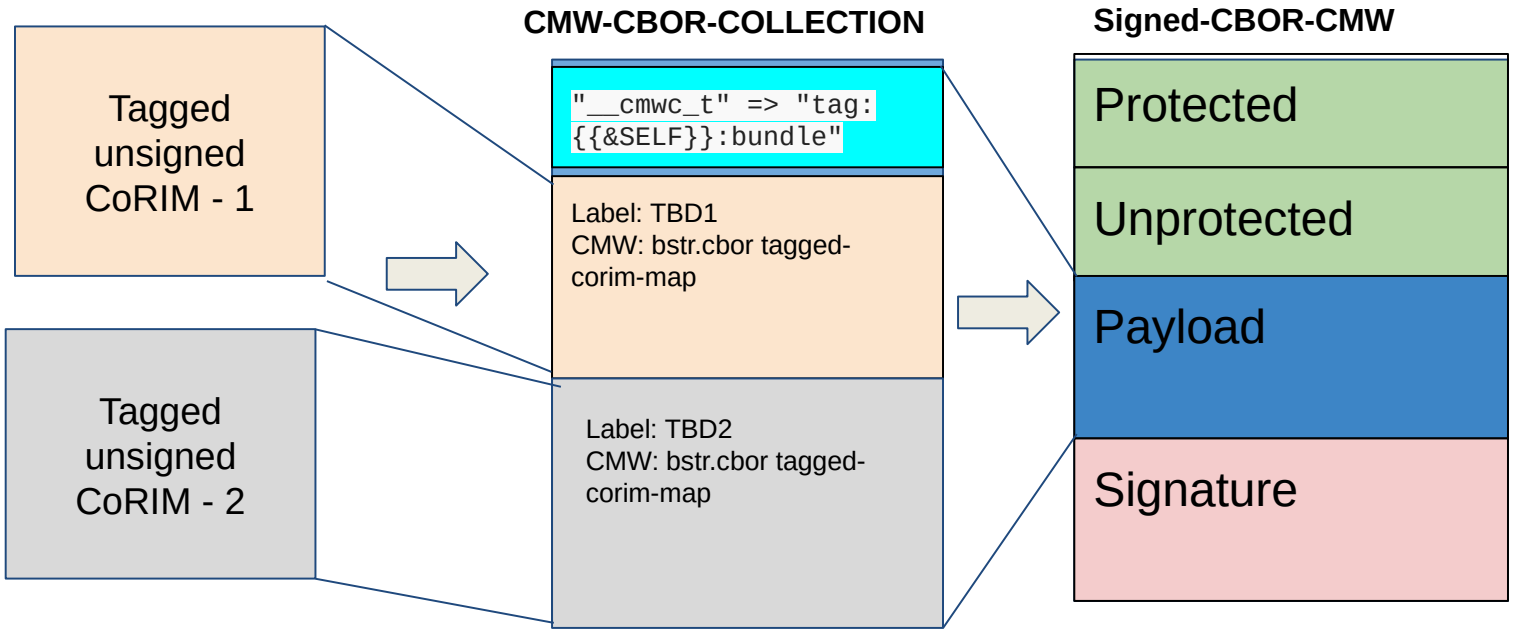
Mandatory **T**o **I**mplement (MTI)

1. Reference Value Triples
2. Endorsed Value Triples
3. Conditional Endorsement Triples

Optional **T**o **I**mplement (OTI)

1. Device Identity Triples
2. Attest Key Triples
3. Domain Membership Triples
4. Domain Dependency Triples
5. Conditional Endorsement Series Triples
6. CoMID-CoSWID Linking Triples

Usage of Unsigned CoRIMs (embedding)



I E T F

Changes since -06

Major Improvements:

1. Glossary - for clear & unambiguous definition of terms
2. Proper Triples explanation
3. Review comments from previous IETF
    a. Rename CoBOM to CoTL, and added example
    b. Improve Introduction
    c. Clarify meaning of the term “tag”

4. Removed extensibility on CoTL Map

5. Security & Privacy Consideration - Protecting Identity of Attesting Environments

IETF