

CoRIM

IETF 125

Snapshot of progress

- Multiple Reviews Received
 - ARTART Review
 - OPSDIR Review
 - Shepherd Review
- Incorporated Review Comments – Work In Progress
- Enabled better inter-operability with other standards
- Many existing features clarified
- General Tidy up/Minor Improvements

Review Comments

- Major re-factor of Verifier Algorithm (Section 9) for better readability
- Removed Optional Phases of Verifier Claims, Policy Claims and Internal Attestation Results processing (Phase 5,6 & 7)
- Updated CoRIM Implementation Status:
 1. Project Veraison – Rust library for CoRIM – github.com/veraison/corim-rs
 2. Project Veraison CoRIM based Verifier (cover) – github.com/veraison/cover
- Tidy up triggered as part of Review feedback
 - Clarified non-emptiness requirements for flags-map

Enabling Inter-Operability

- Support for COSE Detached Payloads [RFC 9052 Section 2](#)
- Support for COSE Hash Envelopes [IETF Draft COSE Hash Envelope](#)
- Enables Interoperability with existing SCITT Standard
- Summary of Changes
 1. Define clearly the protected header map for hash envelope
 2. COSE-Sign-1 payload can be *unsigned CoRIM* or a *bstr carrying hash or nil*

Feature Clarifications

- Domain Dependency Triples
- Refactored Conditional Endorsement Series Triples
- Key Verification section re-worded for clarity
- Further clarification on Domain Membership Triples

Domain Dependency Triple – Slide 1

Domain Dependency Triple – Slide 2

Other feature Clarifications

Refactored Conditional Endorsement Series (CES) Triples

- Modified CDDL for CES Triples
- The subject has been modified
- Stateful Environment modified to Environment with Optional Claims
- Fully backward compatible

In addition, Section 9 **Domain Membership Triples (DMT)** Comparison Algorithm has been clarified to state that DMT Environment Claims Tuple(ECTs) needs to be compared against Corroborated Evidence ECTs in addition to Evidence ECTs

Key Verification Triples

- Problem: How to verify dynamically generated keys post deployment?
- Solution: Added additional steps for Key Triple Verification
- Treat Key Triples as Endorsements during Appraisal

General Tidy up

- Removed duplication of digest-type, now referred from EAT Measured Component
- Refined CoRIM Processor diagram
- Security Considerations have been refactored
- Reuse CDDL for IP Address from RFC9164

BACKUP SLIDES

General Improvements/Tidy Up

- Clarification around flags map
- Security Considerations re-factoring
- Re-use Digest from EAT-MC
- Remove Optional Phases
- Tidied up CoRIM processor diagram

Key Highlights

- Review Comments Incorporated
- Few Features clarified
- Enabled further interoperability with other standards
- Minor Improvements