Conceptual Message Wrappers

draft-ietf-rats-msg-wrap

IETF 120, Vancouver - RATS WG
Quick Recap

• Wrapper format for transporting *any* attestation message in *any* "hosting" protocol

• JSON and CBOR serialisations

• Typing based on Media Types [RFC6838]

For more details see:

• **Presentation @ CCC Attestation SIG**
Updates since IETF 119

Changes since -04 (diff)

• Feature-complete
• Editorial changes
• Early IANA allocations
Editorial changes

• Addressed early IoTDir review by Mohit

• X.509 extension criticality tweak: s/MUST NOT/SHOULD NOT/ - MAY if used in access control decisions.

• CMW CBOR Tag (cbor-tag<tn, $fmt>) defined as an extensible macro

• Clarification about usage of CMW collections to model composite attesters (Dionna, Carl)

• CoAP Content-Format registration requests for application/cmw+ {cbor, json}
Early IANA allocations

Ned requested some early allocations:

- `id-pe-cmw OID (35)` assigned in the SMI Security for PKIX Certificate Extension (1.3.6.1.5.5.7.1) - Thanks, Russ
- `application/cmw+cbor` registered in the Provisional Standard Media Type Registry
- `application/cmw+json` still TODO
- The `cmw` JWT/CWT claim request triggered some back and forth with IANA DEs
  - Lead to clarification around the syntax of the "cmw" claim used in JWT and CWT
  - Provisional Registration procedure for cm-ind values via a GitHub PRs - (Experiment)
Next Steps

• Assign shepherd (Ionuț Mihalcea)

• Solicited feedback from Mike B who raised the only remaining open issue #81 "Trust contexts to consider" (on WCHAN.)

• The editors think the document is ready for a 2nd WGLC
Questions?