Conceptual Message Wrappers

draft-ietf-rats-msg-wrap-10

IETF 121, Dublin - RATS WG

Quick Recap

- Wrapper format for transporting *any* remote attestation message in *any* "hosting" protocol
- JSON and CBOR serialisations
- Typing based on Media Types [RFC6838]

For more details see:

- Presentation @ CCC Attestation SIG

Hackathon Report (Ionuț)

- Work towards updating the Veraison CMW implementation, which was based on an early version of the draft
  - Most time spent on figuring out how to create an ergonomic abstraction for the recursive nature of CMWs in -09
  - Work will continue on the `draft-09` branch
  - Progress made so far validates the work done on harmonizing the encodings and formats
- Identified options for minor improvements in the draft (PR #128)

Updates since IETF 120

2nd WGLC (Changes since -06)

- Editorial clarifications (Ionuț and Mike B. Jones)
- More security considerations (Laurence)
- Remove "double wrapping" for non-native CBOR tags (Carl)
- Slight restructuring (Editors)
- Better registration requests (IANA)

Editorial clarifications

- Changes to abstract and intro to clarify document scope (PR #112)
- `s/base64/base64url/g` (PR #109)

More Security Considerations

Extend security considerations especially around collections.

- Clarify that CMW is *just* an encapsulation: the attester is responsible for creating the security harness
- Discuss *requirements* for both CMW monads and collections (especially in the context of composite attesters)

More Security Considerations (cont.)

Re-work Section 9:

- Add considerations specific to Collections
- Separate treatment of monads (9.1) and collections (9.2)

Rework Section 3.3:

- Point out the need for collection-wise security when a CMW collection represents a single composite/layered attester

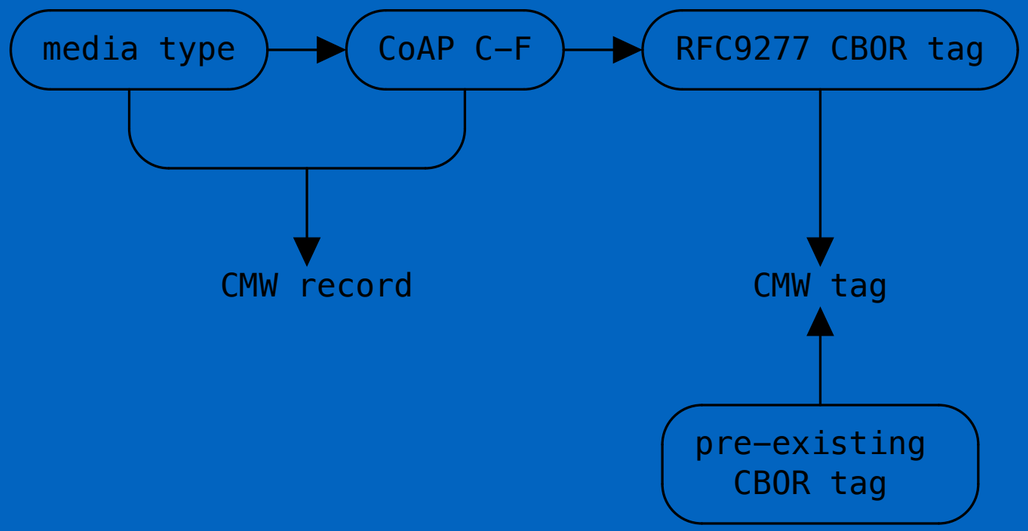
(PR #113, PR #117)

Open Point

- Tighter type system

Tighter Type System

Current



Pros

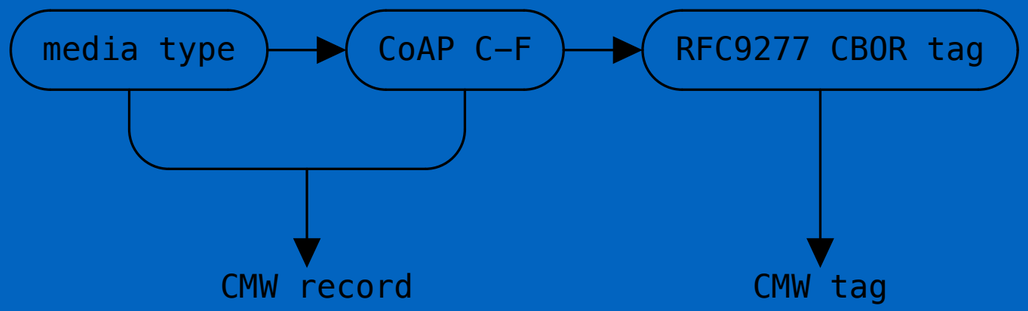
- If you only want CMW in tag form, you don't need to register a media type / CoAP C-F

Cons

- There are two potential sources of truth

Tighter Type System (cont.)

Alternative



Pros

- Type system coherency
- Homogeneous decoding/hand-off path (no special cases)

Cons

- Breaks legacy implementations

Next Steps

- Assign shepherd (Ionuț Mihalcea) ✔
- Decide on the "tighter type system" topic
- Publish new version
-  it!

FIN