RATS Message Wrappers

draft-ftbs-rats-msg-wrap-02

RATS WG, IETF 116, Yokohama

Why and What

One may want to tunnel RATS "conceptual" messages (CM) through another protocol (X.509, TLS, a ReST API)

And do so in such a way that the intermediate nodes (e.g., a RP) only need to understand the high-level bits, ignoring any details. (Typically, to assist negotiation and correct forwarding without requiring tight coupling)

→ CMW provides a *uniform* encapsulation format for RATS CM based on media types (and CBOR tags)

Example Use Cases

Stashing evidence, endorsements/ref-vals and attestation results in certs, CSRs and CRLs extensions [DICE]

Embedding attestation results or evidence as first class authentication credentials in TLS handshake messages [TLS-A]

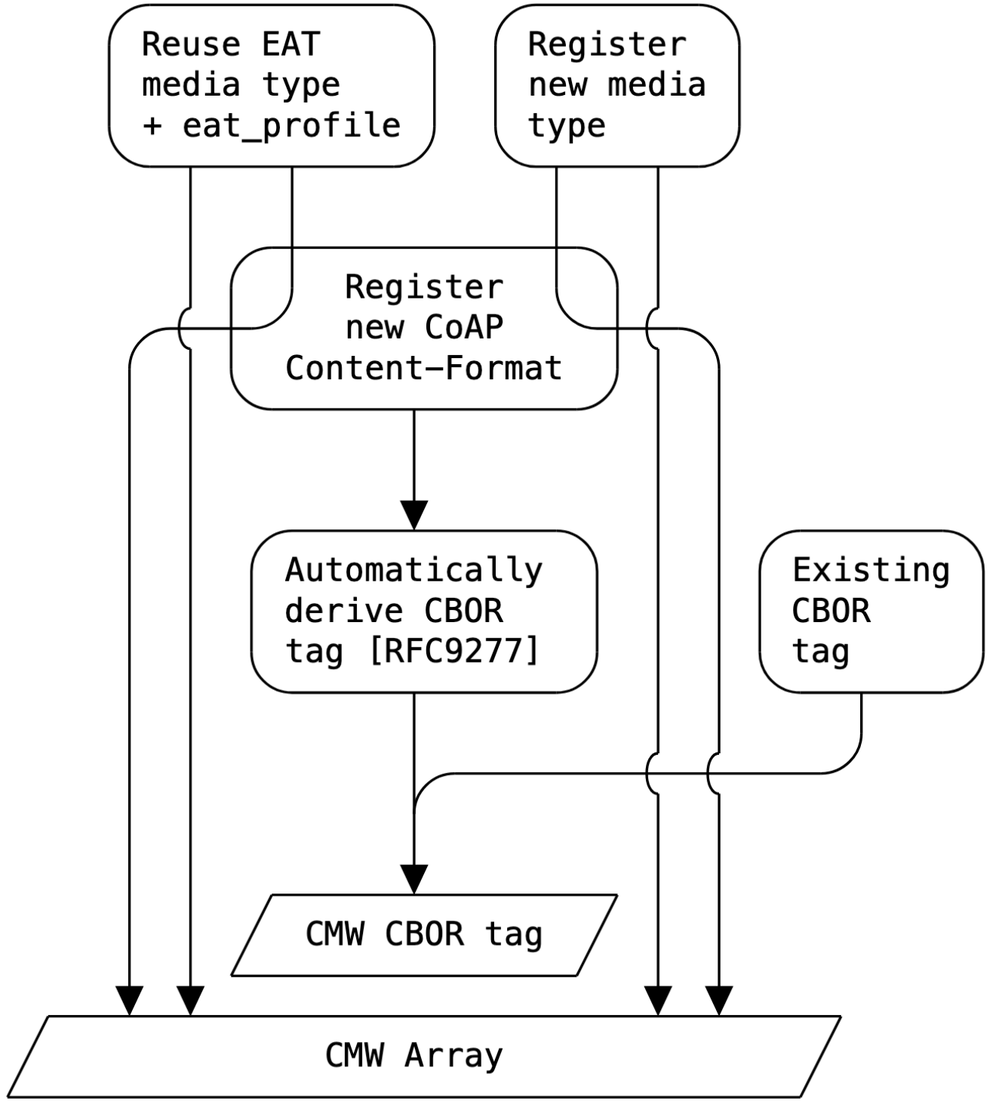
Transporting attestation-related messages in RESTful APIs payloads [Veraison's EvidenceBlobs]

Archival of attestation results as file system objects

Advantages

Converging on a common format

- Allows multiple different protocols to tunnel attestation data in a homogeneous way eases
  - consumption by RPs and Verifiers
  - composition across different protocols boundaries (no need to encap-decap-encap)
- (by-product) interfaces / API to Attesting Environments can become more uniform


Reuse EAT media type + eat_profile
Register new media type
Register new CoAP Content-Format
Automatically derive CBOR tag [RFC9277]
Existing CBOR tag
CMW CBOR tag
CMW Array

Since London

Editorial

-02 published

- Address comments and incorporate suggestion and fixes from Carl and Carsten, including:
  - add examples in CBOR "pretty" format (annotated hex)
  - re-use RFC9193 terminology (e.g., *"Content-Type"*, *"Media-Type-Name"*)
  - ditto for the `Content-Type` ABNF
  - using a shiny new CDDL feature (non-literal tag numbers) to express CBOR tag ranges

Editorial (cont.)

Work in progress

- Some review comments from Carl are still pending (issue#15)
- Discussion about whether to add an optional CM "indicator", e.g.:

```
cm-type = &(
  reference-values: 0
  endorsements: 1
  evidence: 2
  attestation-result: 3
)
```

```
cmw = [
  type: coap-cf / media-type
  value: bytes
  ? ind: bytes .bits cm-type
]
```

Cross-{WG,SDO} Activities

- Work in TCG (DICE WG) to add an X.509 extension for CMW
  - Targeting version 1.1 of *"DICE Attestation Architecture"*
  - Publication (and allocation of the associated OID) not very far away
  - The CMW I-D is referenced and the relevant CDDL/ABNF are copied in
- Discussion with Carl and Russ about using CMW is CSRs (see this thread on the LAMPS ML)
  - Decision: use the CMW extension in draft-ietf-lamps-key-attestation-ext by referencing the TCG doc, once published

Summary

- Simple encap format
- Useful in a number of different scenarios
- Used by another SDO (TCG)
- Transitively used in another WG (LAMPS)

Adopt ?