Mandate

Discuss a shared data model that can be used for attestation evidence in:

- Interoperable Attested TLS
- TLS+CWT (now draft-fossati-tls-attestation)

Converging on a common format

- Allows multiple different protocols (not only TLS) to tunnel attestation data in a homogeneous way => easier consumption by RPs and Verifiers, as well as composition across different protocols (no need to encap-decap-encap).
- (by-product) interfaces / API to Attesting Environments can become more uniform

Where we left

- CBOR-tag based

  vs

- WebAuthn based

Where we are

We had another round of email discussion and think we have found a common ground:

- Agreed on the use of media-types as type discriminators

Where we are (cont.)

This allows us to can build a variety of generic "RATS conceptual message" wrapping formats, including using CBOR tagging based on the RFC9277's `TN()` transform.

For example a type-value wrapper build using a CDDL array:

```
    rats-conceptual-message-wrapper = [ type, value ]
```

(Note it can be given its own tag.)

Type

"type" is either a CoAP C-F code-point or a media type string:

```
type = coap-content-format / media-type

coap-content-format = uint .size 2
media-type = text .abnf ("media-type" .det RFC6838)
```

Value

”value” is a CBOR byte string for the CBOR encoding (or a base64 equivalent for JSON serialisations):

```
value = cbor-bytes /   ; CBOR
        base64-string ; JSON

cbor-bytes = bytes
base64-string = text .regexp "[A-Za-z0-9_=-]+"
```

Example

Suppose you go ahead and register `"application/vnd.intel.sgx"` and then you also register the compressed CoAP C-F equivalent - let's say `30001`.

IANA considerations

The first registration is an email to the IANA expert (Alexey or Murray); the second (since >10000 == FCFS) would be another email to IANA, this time bypassing expert review altogether.

Encoding

- CBOR type-val array

```
[
    30001,
    h'abcdabcd' /  CBOR bytes containing the SGX evidence blob /
]
```

- JSON type-val array

```
[
    "application/vnd.intel.sgx",
    "q82rzQ=="
]
```

Grab a CBOR tag automatically using RFC9277's `TN()`

Since `TN(30001)=1668576818`

- CBOR tag

```
1668576818(h'abcdabcd')
```

IANA considerations (cont.)

- FCFS allocation
- The bureaucracy is three emails in total: the first one with a possibly longer RTT due to human expert processing

Overhead considerations

The overhead of the two (CBOR) wrappers is essentially the same:

- CBOR tag:

```
da 63747632     # tag(1668576818)
   44           # bytes(4)
      abcdabcd # "\xAB\xCD"
```

- CBOR type-value array (one byte less):

```
82              # array(2)
   19 7531      # unsigned(30001)
   44           # bytes(4)
      abcdabcd # "\xAB\xCD"
```

Summary

- Using media types and associated registration machinery
- Refine the format and make a concrete proposal to the RATS working group for a "RATS conceptual message" wrapper
- Next step: Spec to CCC projects with Attested TLS code to get their ACKs/Feedback. [Shanwei]