IETF RATS Timestamps in EAT

Remote ATtestation ProcedureS (rats) WG Virtual Meeting: 2020-03-31
Laurence Lundblade
Value Generation

- Examples: GPS fix acquired; SW measurement taken
- May happen long before attester is involved in turning data into a claim. For example the GPS subsystem may intrinsically cache locations and report them with time stamps
- Handle this in EAT with claim-specific timestamps. Only a minority of claims will work this way.
- No need for general means to associate an acquisition time with any arbitrary claim
- Thus, Individual claims must be modified
- The proposal for location:
  ```
  location-type = {
    latitude => number,
    longitude => number,
    ? altitude => number,
    ? accuracy => number,
    ? altitude-accuracy => number,
    ? heading => number,
    ? speed => number,
    ? timestamp => time-int,
    ? age => uint
  }
  ```
  Discussion on age versus timestamp on next slide
Timestamp / age for Acquisition Time

**Timestamp**
- Absolute time based on UTC/UNIX Epoch time; CBOR tag 1
- Preferred to age
- Disallow floating-point values

**Age**
- Alternate for devices that don’t have a clock or whose clock is unset
- Device must have a ticker to measure elapsed time; an uptime ticker will work
- Is elapsed time between acquisition and token assembly; between time(vg) and time(eg)
- Verifier can compute the range of the absolute time of acquisition from time(ns), nonce generation and time(er), evidence receipt. If window is small, this can be quite accurate
Nonce

- No need to record time(ns) in a token
This the time that all claims are formatted and the signature is applied.

The IssuedAt or “iat” claims from CWT / JWT can be used for this

It is always an absolute time, never an “age”

If the device has no clock or the clock is unset, then this claim is omitted and the Verifier has to go by time(ns) and time(er) to establish range.
Assumption is that the Attestation Results is in EAT format

The CWT/JWT Expiration claim is used to record time(rx)

The CWT/JWT IssuedAt time, “iat” claim is used to record time(rg)

Open Issue: how to carry both time(eg) and time(rg) in the Attestation Result?

- Relying party will want to know
- Can’t both be “iat” claim

Some Options

a) Include the full Attestation Evidence as a sub-part of the Attestation Result
b) Define a “results issued at” (“riat”) claim so they can coexist

Other....