EAT Draft Status & Issues

Laurence Lundblade

RATS Working Group

IETF 105 Montreal

July 24, 2019

General EAT Draft Status & Plan

- -01 version published in July 2019
  - Considers an EAT to be a CWT or JWT
  - Inherits lots from those documents (claim optionality, verification process, IANA process)
  - Defines claims in text + CDDL; JSON and CBOR representations procedurally derived
- Still somewhat in early stages of document
- About a dozen issues in GitHub to be resolved
  - Have about half a dozen ready for discussion today
  - More are expected
- More claims should be added
  - Aim for a coherent set of highly useful generally applicable claims for attestation
  - Aim to not take too long adding claims
- Please use GitHub to make comments and contributions
  - File issues
  - Create Pull Requests to contribute text

Issue #23 – Claims Optionality

Current text:

* All claims are optional
* No claims are mandatory
* All claims that are not understood by implementations MUST be ignored

- Should profiles be allowed to override this?
- Should there be text that says they can?
- How does this relate to JWT/CWT optionality?

CWT & JWT text seems good:

Specific applications of CWTs will require implementations to understand and process some claims in particular ways. However, in the absence of such requirements, all claims that are not understood by implementations MUST be ignored.

Issue #21 and #12 – Random UEIDs

Current UEID text:

No two products anywhere, even in completely different industries made by two different manufacturers in two different countries should have the same UEID…

…This is a 128- to 256-bit random number generated once and stored in the device. This may be constructed by concatenating enough identifiers to be universally unique and then feeding the concatenation through a cryptographic hash function. It may also be a cryptographic quality random number generate once at the beginning of the life of the device and stored…

- Is the 128-bit minimum enough?
  - 40 bits is ~1 trillion
  - 1 trillion people each with 1 trillion devices uses 80 bits
  - Probability of a collision between two devices is 1 in 2^48 or 1 in 300 trillion
- Is the statement about crypto quality enough?
- Tom F comment:
  - Not sure how this assertion is compatible with type RAND UEIDs which – unlike the other types – are constrained only by a local choice (e.g., a "good enough" random generator) and not by any governance regime.

Issue #19 and #24 – Characteristics of Signing Keys

Existing text:

“The EAT is always signed by the attestation key material provisioned by the manufacturer.”

- Some suggest removing this to allow for ephemeral keys
- Some suggest strengthening key protection requirements
- JWT and CWT do not make any comment on the signing keys (nor does COSE)
- Perhaps this belongs in profile documents

Issue #18 – Verification Procedures

- Suggestion that verification procedures be added to the EAT document

- Note that there are two uses for “verif*”
  - CWT/JWT verification – mostly about COSE/JOSE signature verification
  - RATS end-end verification – mostly about larger RATS architecture
- EAT inherits verification procedures from JWT and CWT so no need for it in the EAT document.
- We could add some things over and above CWT and JWT, but I don't see anything obvious.
- Text could also go in the architecture document or in individual profile documents.

Issue #16 – Definition of ”entity”

- EAT draft needs to define it (at least for now).
- Definition is intended to be open and somewhat ambiguous to not artificially limit EAT use
- Includes:
  - Top-level completed devices like a phone, appliance or a car
  - Also includes subcomponents like a secure element, TEE, engine controller, entertainment subsystem, even an Android/Windows/Linux/… app
- No minimum security requirement.
- Should be some computing environment, preferably surrounded by some security boundary

- Current text needs improvement. Seeking suggestions.