EAT for WGLC

IETF 115, London

Laurence Lundblade

Changes Since IETF 114
Drafts 15, 16 and 17

Semantic Changes Affecting Implementations

- Nonce made optional — Allows for timestamp-based freshness (address comments from Hannes and others)
- Submodule Digest Input Bytes
  - Added missing definition for JSON
  - Remove bstr wrapping requirement for CBOR
- Detached Submodle Digest Identification — Changed the way detached-submodule-digests are indicated in JSON tokens. This simplifies both the text and a JSON implementation by avoiding overloading some of the JSON
- Remove Security Level Claim (moving on because consensus couldn’t be etablished)

Major Changes to Wording

- EAT described as a framework — Addresses confusion Eliot experienced
- Redirect to RATS Security model — Address questions Hilarie had
- Rewrite submodules section for clarity and brevity — Long planned, Michael had commented on the need for this
- Remove section on including public keys in claims — It was only advice. Addresses comments from Hannes and others
- Remove all mention of the CTI and JTI claims — It was only advice. Addresses comments by Hannes, Michael and others
- Clarify that submods can be used for both evidence and results — Addresses comment from Thomas and others
- Non-normative reference to UCCS — Adds clarity to definition and integration of future token formats

Changes to Security & Privacy Considerations

- Add section on freshness in security considerations
- Add section on claim trustworthiness
- Remove discussion on JTI/CTI privacy and use for freshness

Issues for Review

EAT authors believe no changes are needed to resolve the following issues

RATS Chairs Spreadsheet issue #8: SW Name claim

- Eliot is concerned about SW name being free-form.
- SW Name claim wording improved in draft-14; SW Name is however still free form
- SPDX and CycloneDX were added as an non-free form alternative
- CoSWID is also available
- No objections on mailing list since July 2022; Eliot never got back

RATS Chairs Spreadsheet #9: security level claim

- Security level claim removed

RATS Chairs Spreadsheet #10: clarifications for DLOAs claim

- Eliot requested improved wording on DLOAs claim
- DLOAs claim wording improved in draft-14
- No comments since July 2022

RATS Chairs Spreadsheet #11: SPDX and CycloneDX requested

- Eliot requested SPDX and CycloneDX claims
- SPDX and CycloneDX claims added in draft-14
- No comments since July 2022 (3 months)

RATS Chairs Spreadsheet #12: Section 9.2 not useful for IANA

- Eliot commented that IANA will not know what to do with section 9.2.
- It was moved to an appendix in draft-14.

Spreadsheet #13: Minor issues and nits (with the introduction)

- Eliot commented on the introduction
- Major work on introduction in drafts 14, 15 and 17

Spreadsheet #14: Comment block from Hannes

Spreadsheet #15: Comment block from Michael

- Dozens of changes made, mostly clarifications and wording
- Remaining issues from Hannes and Michael are now in GitHub and will be presented later

Spreadsheet #16: Extensibility of message type and CDDL sockets

- Issue was with openness to new EAT message types from use of CDDL sockets
- Draft-14 changed to indicate new EAT messages types must be standard
- Discussion on the mailing list closed this out

Spreadsheet #17: Security level

- The security level claim was removed in draft-15, 4 weeks ago.

Spreadsheet #18: Endorsements

- Unclear what the issue actually is other than something to do with endorsements
- Clarification sought but no response in 5 months

Comments on Freshness Requested (GitHub Issue #297)

- Issues requests improved text for nonce and freshness
- Nonce and freshness changes were made since draft 14
- Easiest way to review is search for “fresness” and “nonce”. Not a lot of text to review
- Would like comments in the next week or so

Secure Boot Definition (GitHub PR #287)

- Current text requires booted SW to be under control of the OEM
- Proposed text would anyone to control secure boot
- Authors prefer current text
- Secure boot claim definition has been stable since draft-05 (December 2020) and was approved for pre allocation

Expert Review for EAT Claims (GitHub PR #296)

- Suggestion is for new separate expert review criteria for EAT claims
- EAT authors see existing expert review for the JWT and CWT claims registries as sufficient
  - Applying separate review criteria for EAT claims would increase complexity and require distinguishing EAT claims from non-EAT claims
- History
  - Comment was against draft-13 raised on mailing list May 31 (5 months ago)
  - No supporting comments
  - Was against section 9.2 which is called “Claims Characteristics” which was moved to appendix in draft-14 (Claims Characteristics Appendix is useful non-normative advice for creating claims that was the outcome of some productive early EAT discussions)

Endorsement / Verification Keys (GitHub PR #295)

- Requests specification of methods for verification key/endorsement ID
- Response:
  - Appendix F provides good examples of UEID-based, certificate-based and various forms of COSE kid
  - Verification key/endorsement IDs will vary widely and wildly from use case to use case
  - Verification key/endorsement IDs should be specified in separate documents

- History
  - Comment was against draft-13 raised on mailing list May 31 (5 months ago)
  - No supporting comments

Measurement results claim too general (GitHub PR #293)

- Requests that measurement results claim be removed because it is too general for RP to interpret
- Response:
  - Measurement results claim has a simple pass/fail option
  - RP must always understand Verifier policy to understand any claim
  - Measurement results claims carefully explicitly explains why it is general

- History
  - Comment was against draft-13 raised on mailing list May 31 (5 months ago)
  - No supporting comments

UEIDs labels & UEID being the same as SUEID (GitHub PR #291)

- Issue asks how SUEID labels are assigned
- Response: Text in draft-13 (against which issues was filed) explains that their assignment is itentionally left open
- History
  - Comment was against draft-13 raised on mailing list May 31 (5 months ago)
  - No supporting comments

- Issue asks if UEID and SUEID can be the same
- Response: Rules for UEID and SUEID implicitly allow them to be the same; rules are clear as they are and don’t need improving
- History
  - Comment was against draft-13 raised on mailing list May 31 (5 months ago)
  - No supporting comments

Reordering of Sections (GitHub PR #144)

- Suggests re ordering with claim definition happening later in the document
- Response: Ordering matches that of JWT and CWT RFC; Other section & structure improvements since issue was filed
- History
  - Issues was raised in October 2021
  - No supporting comments

Registration of YANG objects (GitHub PR #10)

- The issue requests guidance on how to create YANG objects for claims
- Response: Overreach for the EAT document which focuses on CBOR and JSON
- History
  - Issues was raised in 2019
  - No supporting comments for a few years