COSE - IETF 107

2020-04-02 @ 17:00 UTC

NOTE WELL

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

AGENDA

1. Administrivia (Chairs) - 5 Minutes
    - Note Well
    - blue sheets (etherpad)
    - Minutes: https://etherpad.ietf.org:9009/p/notes-ietf-107-cose?useMonospaceFont=true
    - Jabber: cose@jabber.ietf.org
2. Document Statuses (Chairs) - 15 Minutes
3. CBOR Compressed Certificates (John Mattsson) - 10 Minutes
4. Rechartering (Chairs) - 30 Minutes

DRAFTS STATUS (RFC Editors Queue)

- draft-ietf-cose-hash-sigs
  - In RFC EDIT

DRAFTS STATUS (PUBREQ)

- draft-ietf-cose-webauth-algorithms
  - Datatracker snafu, fixed now
  - Waiting on AD review and go-ahead
- draft-ietf-cose-rfc8152bis-struct
  - Waiting on AD review and go-ahead
- draft-ietf-cose-rfc8152bis-algs
  - Needs metadata edit (Internet Standard → Informational)
  - Waiting on AD review and go-ahead

DRAFTS STATUS (WG CONSENSUS)

- draft-ietf-cose-hash-algs
  - Consnesus declared, needs shepherd writeup
- draft-ietf-cose-x509
  - Consensus to be declared, needs shepherd writeup

CBOR Compressed Certs

Rechartering - Intro

COSE has been picked up and is being used both by a number of groups
within the IETF (i.e. ACE, CORE, ANIMA, 6TiSCH and SUIT) as well as
outside of the IETF (i.e. W3C and FIDO). There are a number of
implementations, both open source and private, now in existence. The
specification is now sufficiently mature that it makes sense to try
and advance it to STD status.

. . . .

There are a small number of COSE related documents that will also be
addressed by the working group dealing with additional attributes and
algorithms that need to be reviewed and published. The first set
are listed below in the deliverables. A re-charter will be required
to expand this list.

The WG will have five deliverables:

1. Republishing a version of RFC 8152 suitable for advancement to Internet Standard.

2. Use of Hash-based Signature algorithms in COSE using draft-housley-suit-cose-hash-sig as a starting point (Informational).

3. Placement of X.509 certificates in COSE messages and keys using draft-schaad-cose-x509 as a starting point (Informational).

4. Define the algorithms needed for W3C Web Authentication for COSE using draft-jones-webauthn-cose-algorithms and draft-jones-webauthn-secp256k1 as a starting point (Informational).

5. Define a small number of hash functions for X.509 certificate thumbprints and for indirect signing (for SUIT) (Informational).

Rechartering - Suggested Work

- draft-schaad-cose-more-algs
  - So far just AES-KW-Padding
- draft-mattsson-cose-cbor-cert-compress
  - Presented today

… Anything else?

Rechartering - DISCUSS

Any Other Business?

Thank you!