COSE - Virtual Interim 6

2021-10-12 @ 15:00 UTC

© Brian Campbell

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)
2. Document Status (Chairs)
3. x509
4. Slides from Göran
5. AOB

Administrivia

- Note well
- Minutes - https://codimd.ietf.org/notes-ietf-interim-2021-cose-06-cose?both
  - Note taker(s):
- Jabber - chairs
  - Jabber Scribe:
- Meeting and attendees (in the minutes) are recorded
- Agenda bartering

Document status

- Draft-ietf-cose-hash-algs - in RFC-Editor wait reply
- Draft-ietf-cose-rfc8152bis-algs (RFC 9053 to be) - AUTH48, almost all questions/discussions are completed
- Draft-ietf-cose-rfc8152bis-struct (RFC 9052 to be) - AUTH48, waits confirmation of latest version and publication
- Draft-ietf-cose-x509 - past IESG evaluation, some open discussion on next slide
- Draft-ietf-cose-countersign - have shepherd writeup, press the button?

x509

- How much should we force people not to make mistakes as opposed to providing them good guidance in the security considerations section
    - A required proof-of-possession of the subject's private key to issue an end-entity certificate?
        - Suggested on github

          Protecting the integrity of the x5bag, x5chain and x5t contents by placing them in the protected header bucket MAY mitigate some risks of a misbehaving certificate authority (c.f. Section 5.1 of [RFC2634]).

- media-types #37

Slides from Göran

AOB?

Goodbye and have a nice day!