COSE - Interim 2021-02-17

2021-02-17 @ 16:00 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

- Administrivia
- Update on drafts status and charter (Chairs)
- x509
- AOB

Administrivia

- Note well
- Minutes - https://codimd.ietf.org/notes-ietf-interim-2021-cose-02-cose
  - Note taker(s): ?? + Matthew as a backup
- Jabber -
  - Jabber Scribe: ?? + Matthew as a backup
- Meeting and attendees are recorded
- Agenda bartering

Document status

- Draft-ietf-cose-hash-algs - in RFC-Editor Queue
- Draft-ietf-cose-rfc8152bis-algs - in RFC-Editor Queue
- Draft-ietf-cose-rfc8152bis-struct - in RFC-Editor Queue
- Draft-ietf-cose-countersign - in Working Group
  - Editor, Russ Housley
  - Call for shepherds
- Rechartering

Draft-ietf-cose-x509

Open issues:

1. JWS differences
   a. Increased attack surface if x5u not in protected headers - providing different certificates to different entities (Ben)
   b. Generating extra requests?
2. Parts of the end-entity certificate need to be integrity protected. This would make the current specification of x5bag and x5chain insecure (Jon)
   a. Putting everything in protected would be problematic for Michael's use case with middleboxes removing intermediary certs.
   b. Putting the cert in external_aad like EDHOC would change the COSE processing
3. Other SDOs

Draft-ietf-cose-x509 and other drafts

Open issues:

1. Optimizations for EDHOC
2. Optimizations for CBOR Certificates

AOB?

Sbohem a přeji hezký den

(Goodbye and have a nice day)