
COSE - IETF 112
2021-11-10 @ 14:30 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)

Living the IETF Code of Conduct

Reminder of key points of the Code of Conduct [RFC 7154]:

1. IETF participants extend respect and courtesy to their colleagues at all times.
2. IETF participants have impersonal discussions.
3. IETF participants devise solutions for the global Internet that meet the needs of diverse technical and operational environments.
4. Individuals are prepared to contribute to the ongoing work of the group

Agenda

1. Administrivia (Chairs) - 5 min
2. Document Status (Chairs) - 5 min
3. x509 (Chairs) - 10 min
4. draft-ieft-cbor-encoded-cert (Göran Selander) - 10 min
5. HPKE for COSE (Russ) - 10 min
6. Fast-verification friendly ECDSA (Rene Struik) - 10 min
7. AOB - 10 min

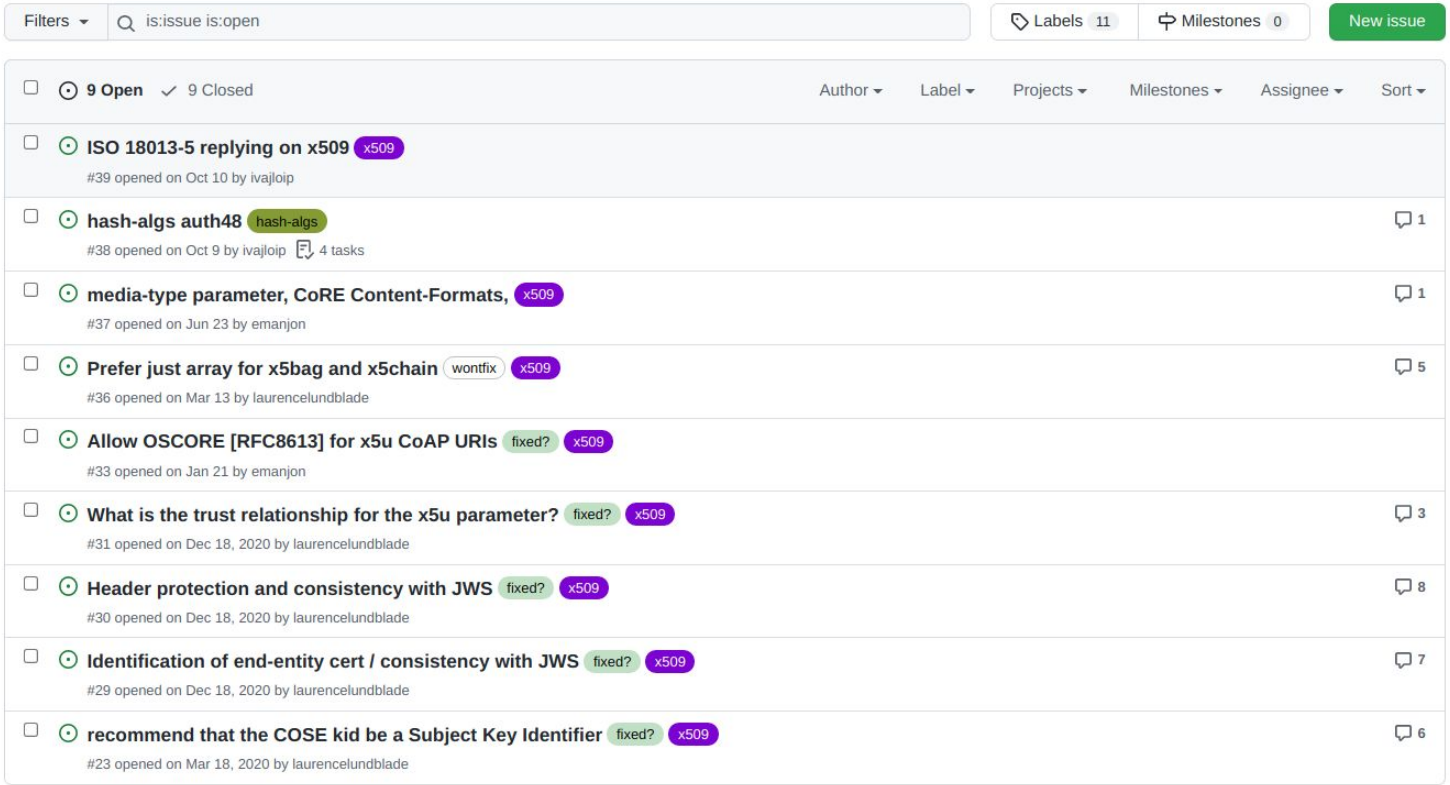
Administrivia

- Note well
- Minutes - https://codimd.ietf.org/notes-ietf-112-cose
  - 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
  - My suggestion for the reply: https://github.com/cose-wg/X509/issues/38
- 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

x509


Filters
is:issue is:open
Labels 11
Milestones 0
New issue
9 Open
9 Closed
Author
Label
Projects
Milestones
Assignee
Sort
ISO 18013-5 replying on x509 x509
#39 opened on Oct 10 by ivajloip
hash-algs auth48 hash-algs
#38 opened on Oct 9 by ivajloip 4 tasks
1
media-type parameter, CoRE Content-Formats, x509
#37 opened on Jun 23 by emanjon
1
Prefer just array for x5bag and x5chain wontfix x509
#36 opened on Mar 13 by laurencelundblade
5
Allow OSCORE [RFC8613] for x5u CoAP URIs fixed? x509
#33 opened on Jan 21 by emanjon
What is the trust relationship for the x5u parameter? fixed? x509
#31 opened on Dec 18, 2020 by laurencelundblade
3
Header protection and consistency with JWS fixed? x509
#30 opened on Dec 18, 2020 by laurencelundblade
8
Identification of end-entity cert / consistency with JWS fixed? x509
#29 opened on Dec 18, 2020 by laurencelundblade
7
recommend that the COSE kid be a Subject Key Identifier fixed? x509
#23 opened on Mar 18, 2020 by laurencelundblade
6

x509

- Figure out the concrete phrasing of the mandate to *integrity protecting 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

draft-ieft-cbor-encoded-cert - Göran

HPKE for COSE - Russ

Fast-verification friendly ECDSA - Rene Struik

AOB?

Goodbye and have a nice day!