

CBOR Object Signing and Encryption (COSE)

WG Chairs:

Justin Richer, jricher@mit.edu

Kepeng Li, kepeng.lkp@alibaba-inc.com

Security AD:

Kathleen Moriarty, Kathleen.Moriarty.ietf@gmail.com

Mailing List: cose@ietf.org

To Subscribe: <https://www.ietf.org/mailman/listinfo/cose>

Note Well

- Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:
 - The IETF plenary session
 - The IESG, or any member thereof on behalf of the IESG
 - Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
 - Any IETF working group or portion thereof
 - Any Birds of a Feather (BOF) session
 - The IAB or any member thereof on behalf of the IAB
 - The RFC Editor or the Internet-Drafts function
- All IETF Contributions are subject to the rules of [RFC 5378 and RFC 3979 \(updated by RFC 4879\)](#).
- Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult [RFC 5378 and RFC 3979 for details](#).
- A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.
- A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Requests

- Jabber Scribe
- Minute Taker
- Blue Sheets

Milestone Check

Date	Milestone
Jan 2016	Submit COSE constrained-appropriate algorithms to the IESG, for publication as a Proposed Standard
Jan 2016	Submit COSE specification to the IESG, for publication as a Proposed Standard
Jun 2015	Submit COSE constrained-appropriate algorithms as a WG item
Done	Submit COSE specification as a WG item

Agenda

- Opening & Welcome - 5 min (Justin/Kepeng)
- COSE message status and update - 15 min (Jim)
 - <https://datatracker.ietf.org/doc/draft-ietf-cose-msg/>
- CBOR Encoded Message Syntax: Additional Algorithms - 15 min (Jim)
 - <https://datatracker.ietf.org/doc/draft-schaad-cose-alg/>
- Using RSA Algorithms with COSE Messages - 15 min (Mike)
 - <https://datatracker.ietf.org/doc/draft-jones-cose-rsa/>
- Issues and open discussion - 10 min