JSON Object Signing and Encryption (JOSE) Working Group

August 1, 900-1130

IETF 84 --- Vancouver, BC, CA

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.
•

JOSE WG

- Web page: charter, current documents
  - http://datatracker.ietf.org/wg/jose/charter
- Mailing List: jose@ietf.org
  - To Subscribe: jose-request@ietf.org
  - Archive: http://www.ietf.org/mail-archive/web/jose
- Chairs
  - Jim Schaad ietf@augustcellars.com
  - Tony Hansen (out going) tony@att.com
  - Karen O'Donoghue (in coming)
- Security Area Director
  - Sean Turner turners@ieca.com

Milestones

- June 2012 WGLC on object integrity document
- June 2012 WGLC on object encryption document
- June 2012 WGLC on key format document
- June 2012 WGLC on algorithm document
- July 2012 Submit JWS to IESG
- July 2012 Submit JWE to IESG
- July 2012 Submit JWA to IESG
- July 2012 Submit JWK to IESG

Agenda

- Administrivia
- Documents
  - Use Cases – Richard Barnes
  - JSON WEB * - Mike Jones
  - JavaScript Message Security Format – Richard Barnes
  - AEAD w/ AES-CBC and HMAC-SHA – David McGrew
  - Serialization Documents – Mike Jones
- Open Issue Discussion
- Other Presentations
  - Jose In Action: XMPP E2E – Matt Miller
  - JWA Algorithm Deployment – Mike Jones
- Open Mic