JOSE Working Group

10 November 2014, 1730-1830 HDT
IETF 91 Honolulu

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.

Agenda

- Administrivia and Agenda Bashing
- Open issue resolution
- Cookbook document
- Thumbprint document
- Any other business

JWS - Barnes

- Section 6 – protection of jwu parameter
  - Needs to have Richard and Jim get together and talk.
- Section 7.2 – Flattening of signature
  - This is currently in the document
  - There has been some push-back on the list about it.
  - List discussion was minimal

JWS - Resnick

- Section 3.1 , Section 3.1 JWE – unprotected headers in compact representation – Pete will declare self in the rough
- Section 5.2 – Pete has requested “reject signature” rather than “reject JWS” or “reject”
- Section 5.1, 5.2 – Pete will look at a potential re-write of the algorithm

JWE - Resnick

- Section 4.1.2 – Use of the word reject. Pete still needs to scan the document to see what needs to change
- Section 5.1, 5.2 – Pete is going to review the algorithm to see if he believes he can write a clear and acceptable algorithm

JWK

- No open issues

JWA - Resnick

- Section 3.1 – Pete will declare self in the rough
- Section 4.6.2, 4.8.1.1 – Pete will provide a message on how cut and paste can cause re-normalization to occur. This can lead to issues.
- Section 4.8 – Pete has issues with the fact that normalization is not a part of this. He is going to find the status of the PRECIS work would is a better path, but perhaps not easily usable.

JWA - Ferrell

- Removal of “oth” parameter
  - Implementation is provided by two WebCrypto versions. I expect this is sufficient to get Steve to remove the discuss