IETF 91: TLS WG Session

20141113 – 9 – 11:30 – Coral 5

Joe Salowey

Sean Turner

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.

Aloha!

- Note Well
- Administrivia
  - Jabber Scribe
  - Minute Taker
- Bashing of Agenda
  - Status of WG drafts
    - FFDHE
    - TLS 1.3 review
  - TLS 1.3: OPTLS
  - WG adoption(s)
    - 4492bis
    - SSL3.0 + die*1M
    - False Start

WG drafts

- RC4 DIE*1M
  - http://datatracker.ietf.org/doc/draft-ietf-tls-prohibiting-rc4/
  - WGLC ~100 messages
  - Summary: There are different views on when to deprecate RC4 with the majority view seeming to fall within the next few years.
  - Submitted to IESG for publication.
- Session Hash
  - http://datatracker.ietf.org/doc/draft-ietf-tls-session-hash/
  - Latest version has no known issues – WGLC will start PDQ.

WG drafts

- Downgrade SCSV
  - http://datatracker.ietf.org/doc/draft-ietf-tls-downgrade-scsv/
  - WGLC issue ~200 messages
  - Joe provided a summary and these were incorporated in -01
    - Be explicit about it being a hack
    - Applies to DTLS
    - IANA instructions
    - Better describe the conditions of when the client SHOULD include the SCSV and what the client SHOULD do if it receives an inappropriate_fallback alert.
  - New comment from Florian: indicate version in inappropriate_fallback alert message.
  - After -02 published headed to IESG.

WG drafts

- Cached Info
  - http://www.ietf.org/archive/id/draft-ietf-tls-cached-info-16.txt
  - WGLC comments received – Awaiting revised draft.
- Finite Field DHE negotiation
  - http://datatracker.ietf.org/doc/draft-ietf-tls-negotiated-ff-dhe/
  - cue dkg
- TLS 1.3 Topics continued/Recap
  - http://datatracker.ietf.org/doc/draft-ietf-tls-tls13/
  - Cue status

WG Adoptions

- 4492bis
  - http://datatracker.ietf.org/doc/draft-nir-tls-rfc4492bis/
- SSL3.0*1M*DIE
  - http://datatracker.ietf.org/doc/draft-thomson-sslv3-diediedie/
- False Start
  - http://datatracker.ietf.org/doc/draft-bmoeller-tls-falsestart/