2015-03-26 TLS WG @ IETF 92

Chairs:

Joe Salowey

Sean Turner

AD:

Stephen Farrell

Mailing List:

tls@ietf.org

Drafts:

http://datatracker.ietf.org/wg/tls/documents/

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
- Sign the Blue Sheets

Agenda

- Welcome, note takers, blue sheets, note well (5 min) [Chairs]
- Document Status (10 Min) [Chairs]
- Backwards compatibility pull request 107 (10 Min) [All]
- OPTLS (30 Min) [EKR, KRAWCZYK]
- 0-RTT Issues (replay, PFS, etc) (30 Min) [EKR]
- Update/Rekey (10 Min) [EKR]
- Client Auth (15 Min) [EKR, POPOV]
- AOB (padding, MTI, PSS, PSK, cached info, 4492) (30 Min) [Chairs]

WG Draft Status

- With RFC Editor:
  - draft-ietf-tls-downgrade-scsv-05
- In IETF LC (until 30 April):
  - draft-ietf-tls-sslv3-diediedie-02
- With our AD:
  - draft-ietf-tls-negotiated-ff-dhe-07
  - draft-ietf-tls-sessions-hash-04
  - A TLS ClientHello padding extension: draft-ietf-tls-padding-01

WG Draft Status

- In progress:
  - draft-ietf-tls-cached-info-18
  - draft-ietf-tls-rfc4492bis-02
  - draft-ietf-tls-tls13-05
- In the wings:
  - draft-mavrogiannopoulos-chacha-tls
  - draft-josefsson-tls-curve25519-06
  - draft-bmoeller-tls-falsestart-01