TLS Working Group
IETF-90

Chairs
Eric Recorla
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.

Agenda

Monday July 21, 2014 (IETF 90 TLS Meeting - Session 1)

Fairmont Royal York - Ontario C

Toronto, ON, Canada

15:20 - 15:35 Blue sheets/scribes/etc. (chairs)

15:35 - 15:45 WG Document Status (chairs)

15:45 - 16:00 ECC to Standards Track/MTI (all)

16:15 - 16:35 ChaCha/Poly1305 (AGL)

16:35 - 16:50 SCSV/Downgrade (AGL)

Agenda

Thursday July 24, 2014 (IETF 90 TLS Meting - Session 2)

Fairmont Royal York - Ontario C

17:30 - 17:35 Blue sheets/scribes/etc. (chairs)

17:35 - 18:00 New curves:

Report from CFRG (CFRG Chairs)

Discussion

18:00 - 18:15 Named DH Groups (DKG)

18:15 - 18:30 Hardware Crypto Considerations (MSJ)

wg status (1/2)

- Dead (waiting for time-out):
  - draft-ietf-tls-rfc5246-bis-00
- Parked:
  - draft-ietf-tls-pwd-04
- Submitted to IESG (incorporating directorate reviews then to IETF LC)
  - draft-ietf-tls-encrypt-then-mac-02.txt
- Up for adoption:
  - draft-bhargavan-tls-session-hash

wg status (2/2)

- Recently Adopted (discussed today):
  - draft-ietf-tls-negotiated-dl-dhe-00
  - draft-ietf-tls-downgrade-scsv-00
  - draft-ietf-tls-prohibiting-rc4-02 (was draft-popov-tls-prohibiting-rc4-02)
- Active wg drafts:
  - draft-ietf-tls-cached-info-16
  - draft-ietf-tls-tls13-02

wg list issues

- Issues sent to the list:
  - Extended master secret (without SCSV)
- TLS 1.3:
  - Remove renegotiation with some for of rekeying as well as client initiated authentication
  - Encrypted SNI
  - AEAD length changes
  - Removing unnamed DH groups
  - Encrypted content-type (and maybe remove version too)