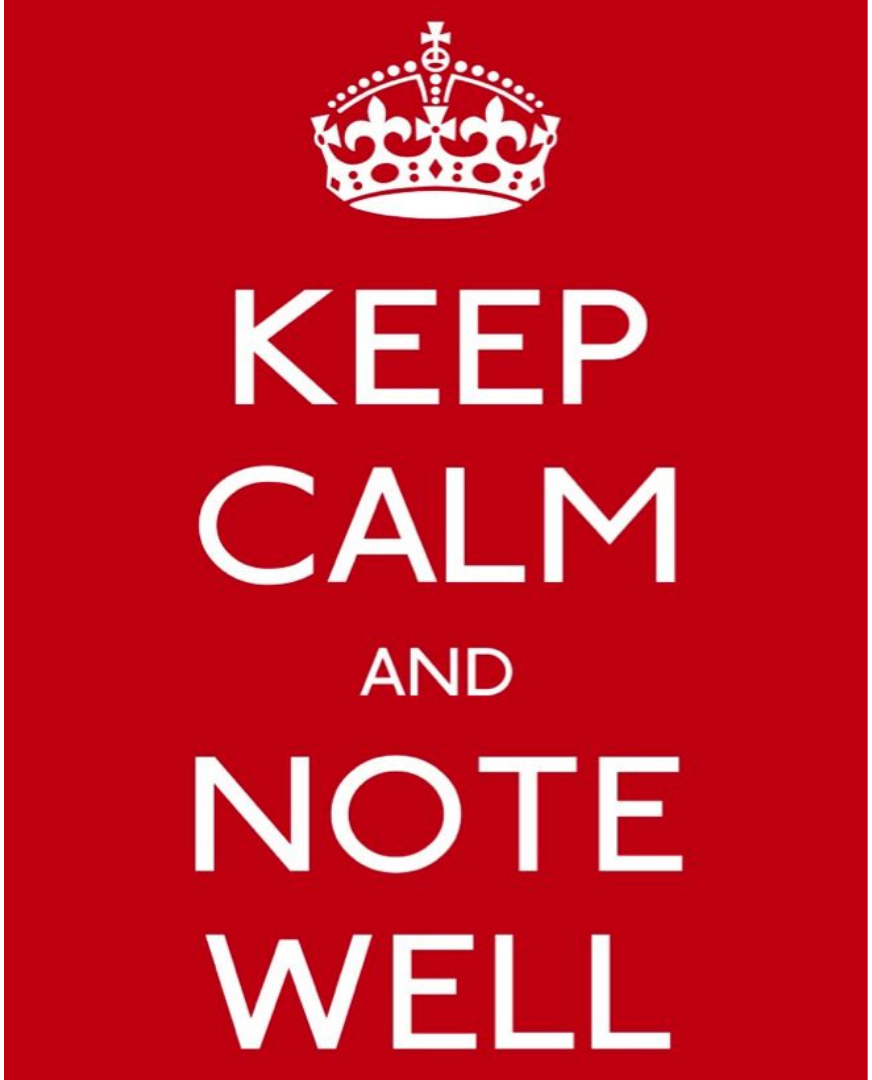
IETF 96
TLS WG

Chairs:
Joe Salowey
Sean Turner



- The brief summary:
  - This summary is only meant to point you in the right direction, and doesn't have all the nuances; see below for the details.
  - By participating with the IETF, you agree to the follow IETF processes.
  - If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.
- You understand that meetings might be recorded and broadcast.
- The details:
  - For further information, talk to a chair, ask an Area Director, or review BCP 9 (on the Internet Standards Process), BCP 25 (on the Working Group processes), BCP 78 (on the IETF Trust), and BCP 79 (on Intellectual Property Rights in the IETF).

Jabber Scribe(s)

Minute Taker(s)

Sign the Blue Sheets

Agenda

Administrivia (5 min):

Note Well | Blue Sheets | Scribes

Document Status (10 min)

TLS 1.3 (120 min):

- Recent Changes (30 min)
- Post handshake msgs key (20 min)
- Other open issues (45 min)
- Key update ack - PR426 (10 min)
- Separating signature types (10 min)

Time Permitting:

- Secondary Certificates in HTTP
- AES-OCB - https://datatracker.ietf.org/doc/draft-zauner-tls-aes-ocb/
- TLS Client Puzzles - https://datatracker.ietf.org/doc/draft-nygren-tls-client-puzzles/
- TLS Blocking Alert - https://tools.ietf.org/html/draft-lemon-tls-blocking-alert-00
- TLS Server Identity Pinning with Tickets - https://datatracker.ietf.org/doc/draft-sheffer-tls-pinning-ticket/

CS = Cipher Suite

Document Status

Published:

RFC 7905: ChaCha20-Poly1305 CSs for TLS

AUTH48:

1. TLS Cached Info Extension
   (all approvals received)
2. TLS False Start
   (pinned on FF-DHE)
3. Negotiated FF-DHE Parameters for TLS
   (..cough.. DKG)

Adopted:

- ECDHE_PSK w/ AES-GCM & AES-CCM CSs for TLS
- A DANE Record and DNSSEC Authentication Chain Extension for TLS

The Show:

- TLS 1.3
- ECC CSs for TLS v1.2 & earlier

Set Free:

Secure Password CSs for TLS

TBD:

TLS 1.2 Update for Long-term Support