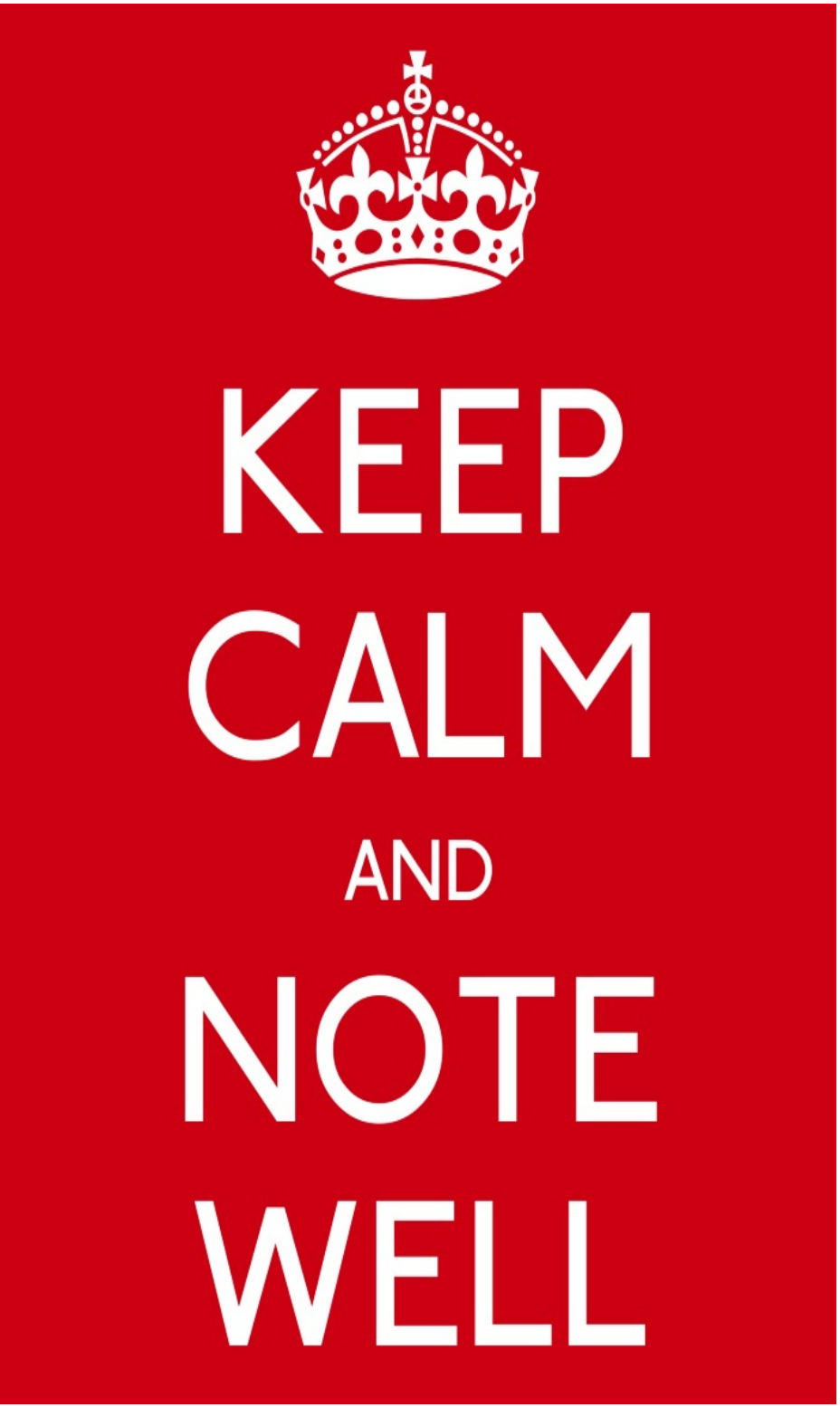

TLS Interim WG Meeting Fall ‘15
Chairs: Joe Salowey & Sean Turner
Mailing List: tls@ietf.org
© Patrick Rodriguez



- 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).

Requests

Jabber Scribe

Minute Taker

Sign the Blue Sheets

Client Authentication:
https://github.com/tlswg/tls13-spec/pull/209

Encrypted Content Type and Padding:
https://github.com/tlswg/tls13-spec/pull/147
https://github.com/tlswg/tls13-spec/pull/51
https://github.com/tlswg/tls13-spec/pull/249
https://github.com/tlswg/tls13-spec/pull/250

Replace DH_anon with Ray Public Keys:
https://github.com/tlswg/tls13-spec/issues/233

https://github.com/tlswg/tls13-spec/labels/discuss-seattle

Quantum Safe Crypto Draft

Published RFCs

RFC 7627

Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension

Image courtesy of Joris Toonders on LinkedIn

Image source http://tinyurl.com/ov7wfjy

Drafts with RFC Editor

draft-ietf-tls-negotiated-ff-dhe

Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for TLS

draft-ietf-tls-padding

A TLS ClientHello padding extension

Active Drafts

draft-ietf-tls-cached-info

Cached Information Extension

draft-ietf-tls-chacha20-poly1305

The ChaCha20-Poly1305 AEAD Cipher

draft-ietf-tls-rfc4492bis

Elliptic Curve Cryptography (ECC) Cipher Suites for TLS 1.2 and Earlier

draft-ietf-tls-curve25519

Curve25519 and Curve448 for TLS

draft-ietf-tls-falsestart

TLS False Start

draft-ietf-tls-tls13

TLS Protocol Version 1.3

Image source http://tinyurl.com/pbtnygo