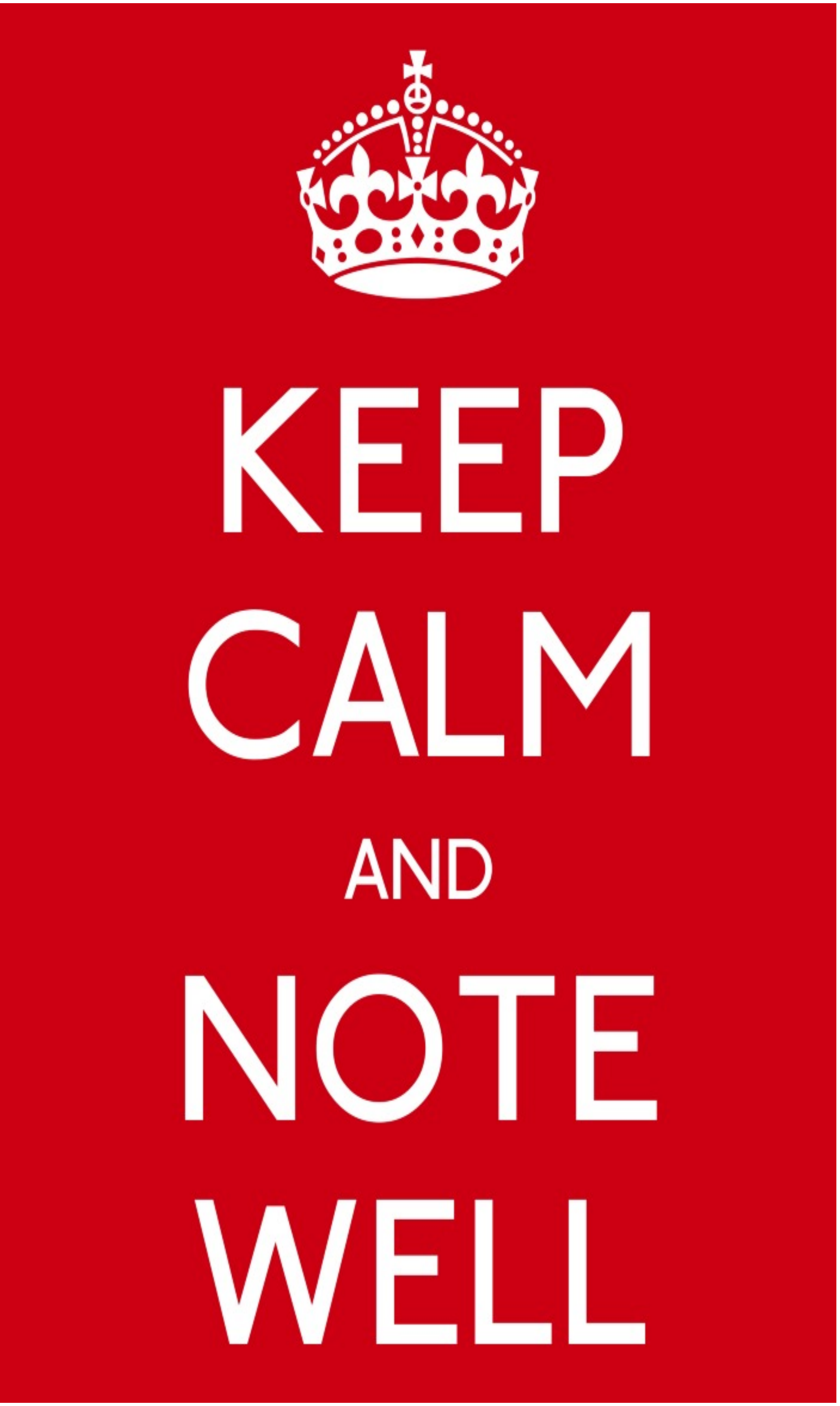
TLS WG @ IETF 93

Chairs: Joe Salowey & Sean Turner

Mailing List: tls@ietf.org

© Jorge Royan / http://www.royan.com.ar



- 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

agenda

Day 1

10 min – Bash! & Status Update (chairs)

30 min – TLS 1.3 Overview (ekr)

20 min – Known Config Mechanism (ekr)

20 min – 0-RTT (ekr)

20 min – PSK and Resumption (ekr)

20 min – Client Authentication (popov)

Day 2

05 min – Bash!

45 min – Day 1 TLS 1.3 Recap (ekr)

30 min – Ciphersuites (ekr)

15 min – 4492bis (nir)

15 min – Cached Info

05 min – DANE or DNSSEC Validation Chain (shore)

05 min – IEEE 1609 Certificates (kaiser)

05 min – Session Key Interface (mattsson)

05 min – ECDHE-PSK (mattsson)

05 min – Hybrid Quantum Safe Ciphersuites in TLS (whyte)

Published RFCs

RFC 7645

TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks

RFC 7568

Deprecating Secure Sockets Layer Version 3.0

Image courtesy of Joris Toonders on LinkedIn

Drafts with RFC Editor

draft-ietf-tls-session-hash

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

draft-ietf-tls-negotiated-ff-dhe

Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for TLS

Image source http://tinyurl.com/ov7wfjy

Newly Adopted

draft-ietf-tls-falsestart

Transport Layer Security (TLS) False Start

draft-ietf-tls-curve25519

Curve25519 and Curve448 for Transport Layer Security (TLS)

draft-ietf-tls-chacha20-poly1305

The ChaCha20-Poly1305 AEAD Cipher for Transport Layer Security

Image source http://tinyurl.com/oy6qoe2

Active Drafts

draft-ietf-tls-cached-info

Transport Layer Security (TLS) Cached Information Extension

draft-ietf-tls-padding

A TLS ClientHello padding extension

draft-ietf-tls-rfc4492bis

Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier

draft-ietf-tls-tls13

The Transport Layer Security (TLS) Protocol Version 1.3

Image source http://tinyurl.com/pbtnygo