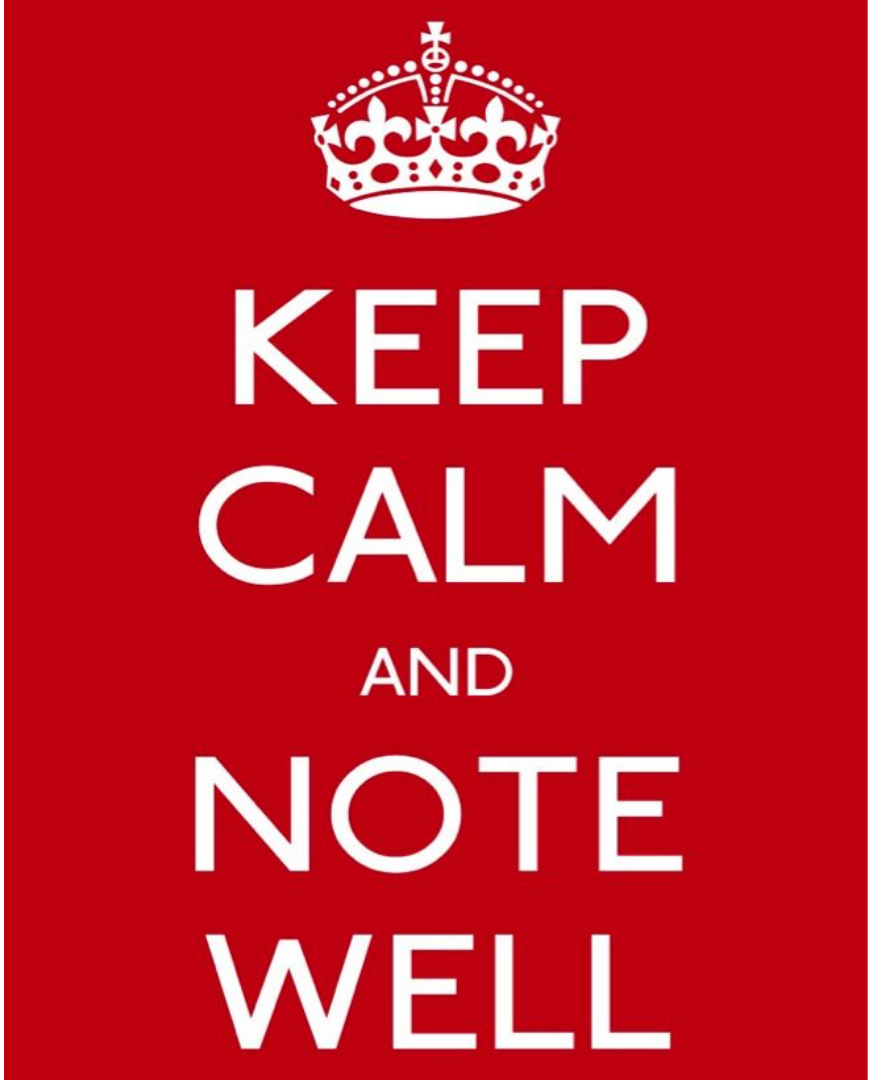
IETF 95
TLS WG

Chairs: Joe Salowey
Sean Turner

Gaucho on Horseback, Argentina
Photograph by Luis Marden
http://photography.nationalgeographic.com/wallpaper/photography/photos/odysseys-photographs-gallery/gaucho-horseback/



- 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 (original)

Tuesday - 1000-1230 - Alantico B

1000-1005 - Administrivia - Joe and Sean

1005-1015 - Documents' Status - Joe and Sean

1015-1030 - RFC 4492bis - Yoav Nir

1030-1230 - TLS 1.3 Status - ekr

Thursday - 1000-1230 - Atlantico C

1000-1005 - Administrivia - Joe and Sean

1005-1105 - 0-RTT Considerations - ekr

1105-1220 - TLS 1.3 Update - ekr

If time:

10 mins - D. Zhang:
A TLS Extension for Service Indication

Agenda (bashed)

Tuesday - 1000-1230 - Alantico B

1000-1005 - Administrivia - Joe and Sean

1005-1015 - Documents' Status - Joe and Sean

1015-1030 - RFC 4492bis - Yoav Nir

1030-1230 - TLS 1.3 Status - ekr

Thursday - 1000-1230 - Atlantico C

1000-1005 - Administrivia - Joe and Sean

1005-1105 - 0-RTT Considerations - ekr

1105-1220 - TLS 1.3 Update - ekr

1220-1230 - From the Hackathon:
TLS 1.3 Demo - R.Barnes+N.Sullivan

See UTA slides: D. Zhang:
A TLS Extension for Service Indication

Status

draft-ietf-tls-negotiated-ff-dhe

With RFC editor, but pinned waiting on draft-ietf-tls-falsestart.

draft-ietf-tls-cached-info

Made it through IETF LC and IESG review and then ...

Karthik uncovered problem with the truncated hash.

Solution: Don’t truncate, publish new version, done.

Status (continued)

draft-ietf-tls-falsestart

- Made it through WGLC.
- AD review:
  - Explain why some ciphersuites are good/bad to use with this extension.
  - Hold it and publish it as Historic when TLS 1.3 goes out the door?

draft-ietf-tls-chacha20-poly1305

- Completed IETF LC (Tuesday).
- Note: code points already assigned.

Status (continued)

draft-ietf-tls-pwd

This is wrapped up in the suggested IANA registry rule changes.

draft-ietf-tls-rfc4492

See Yoav's slides.

draft-ietf-tls-tls13

It's the main show.

Note: when CFRG is done with draft-irtf-cfrg-eddsa goes to IRSG the chairs will issue an early IANA code point assignment call.