• 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
Wednesday
0900-0910  Chairs  Administrivia
0910-0920  Yoav  RFC 4492bis
0920-0950  EKR  TLS 1.3 Since Prague
0950-1130  EKR  Client Authentication (PR#316)
            HelloRetryRequest (#104, #185)
            0-RTT framing mechanics (#311, #295)
            Rekey (#4, #125)
            Exporters (#282)
            AOB

Thursday
1740-1745  Chairs  Administrivia
1745-1805  Jivsov  PSS
1805-1830  DKG/EKR SNI Encryption
1840-1850  Jay    TLS/DTLS PSK Identity Extension
TRON
Workshop

Workshop Location:
San Diego, CA, USA

Workshop date (co-located with NDSS 2016):
2016-02-21

Abstracts/Expressions of interest due: 2015-12-01
Final submissions: 2015-12-15 anywhere-on-earth

https://www.internetsociety.org/events/ndss-symposium-2016
Published RFCs

RFC 7627
Transport Layer Security (TLS)
Session Hash and Extended Master Secret Extension
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
Drafts with our AD

draft-ietf-tls-cached-info
Cached Information Extension
Drafts through WGLC

draft-ietf-tls-chacha20-poly1305

The ChaCha20-Poly1305 AEAD Cipher
Active Drafts

draft-ietf-tls-curve25519
  merged into:
draft-ietf-tls-rfc4492bis
    Elliptic Curve Cryptography (ECC)
    Cipher Suites for TLS 1.2 and Earlier

draft-ietf-tls-falsestart
  TLS False Start

draft-ietf-tls-tls13
  TLS Protocol Version 1.3