IETF 97: TLS WG

Chairs: Joe Salowey & Sean Turner

Info: https://datatracker.ietf.org/wg/tls/charter/

Image: http://wikitravel.org/en/Seoul

NOTE THEE WELL

- 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

Reminders:

- State your name @ mic for the scribes/minutes
- Keep it professional @ the mic

Agenda

Tuesday (2 hours):

Administrivia (5 min):
Note Well | Blue Sheets | Scribes: Jabber/Minutes

Document Status (5 min)

OpenSSL Status (5 min)

TLS 1.3 (95 min)

TLS Visibility Inside the Data Center: Seve/Jason - 20min

Exported Authenticators in TLS (aka Post-handshake Auth): Nick - 20 min

Agenda

Friday (2 hours):

TLS 1.3 (60 min):

- Revisit any issues from Tuesday and anything we didn't get to.
- Rebranding (aka PR#612): Sean 7min

DTLS (10 min): ekr

DNS validation chain extension:
Melinda - 10min

Delegated Credentials: Nick - 20min

Example Handshake Traces for TLS 1.3: MT - 5min

Other Document(s): Chairs - Time Permitting

Time Permitting:

TLS Server Identity Pinning with Tickets:
Yaron - 10min

TLS/DTLS Optimizations for Internet of Things:
Hannes - 10 minutes

Document Status

Published:

- RFC 7918: TLS False Start
- RFC 7919: Negotiated FF-DHE Parameters for TLS
- RFC 7924: TLS Cached Info

WGLC:

- TLS 1.3

In-Progress:

- ECC CSs for TLS v1.2 & earlier
- ECDHE_PSK w/ AES-GCM & AES-CCM CSs for TLS
- A DANE Record and DNSSEC Authentication Chain Extension for TLS

Uplifting: (Informational to Proposed Std):

- TLS EC CSs with SHA-256/384 & AES-GCM

Adopted:

- D/TLS IANA Registry Updates

TBD:

- DTLS 1.3
- TLS 1.2 Update for Long-term Support
- Exported Authenticators in TLS
- Example Handshake Traces for TLS 1.3
- TLS Server Identity Pinning with Tickets
- Applying GREASE to TLS Extensibility
- Delegated Credentials

Document Status - Updated

Published:

- RFC 7918: TLS False Start
- RFC 7919: Negotiated FF-DHE Parameters for TLS
- RFC 7924: TLS Cached Info

WGLC:

- TLS 1.3
- ECC CSs for TLS v1.2 & earlier
- ECDHE_PSK w/ AES-GCM & AES-CCM CSs for TLS

In-Progress:

- A DANE Record and DNSSEC Authentication Chain Extension for TLS

Uplifting: (Informational to Proposed Std):

- TLS EC CSs with SHA-256/384 & AES-GCM

Adopted:

- D/TLS IANA Registry Updates

TBD:

- DTLS 1.3
- TLS 1.2 Update for Long-term Support
- Exported Authenticators in TLS
- Example Handshake Traces for TLS 1.3
- TLS Server Identity Pinning with Tickets
- Applying GREASE to TLS Extensibility
- Delegated Credentials