TLS@IETF102

WG Info: https://datatracker.ietf.org/wg/tls/about/
Chairs: Chris Wood, Joe Salowey, and Sean Turner

NOTE WELL

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

As a reminder:

- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process),
- BCP 25 (Working Group processes),
- BCP 25 (Anti-Harassment Procedures),
- BCP 54 (Code of Conduct),
- BCP 78 (Copyright),
- BCP 79 (Patents, Participation),
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

Requests

Minute Taker(s)

Jabber Scribe(s)

Sign Blue Sheets

State your name @ the mic

Keep it professional @ the mic

Agenda

Monday - 1330-1550

10min	Administrivia
05min	TLS1.3 Adoption
10min	Deprecate TLS 1.* < 1.2?
10min	Exported Authenticators
30min	DTLS 1.3 & Connection ID
20min	DNSSEC Chain Extension
15min	Delegated Credentials
10min	Layered Authenticators

Agenda

Thursday - 1810-1910

05min	Administrivia
10min	Certificate-based Authentication with External PSK
15min	Ticket Requests
30min	ESNI

Document Status

AUTH48:

- TLS 1.3
- ECC CSs for TLS v1.2 & earlier

Approved by IESG:

- ECDHE_PSK w/ AES-GCM & AES-CCM CSs
- IANA Registry Updates for TLS and DTLS
- Record Size Limit Extension for TLS

Cycling back to the WG:

- A DANE Record and DNSSEC Authentication Chain Extension for TLS

In IETF LC:

- Example Handshake Traces for TLS 1.3

Addressing WGLC comments:

- Exported Authenticators for TLS

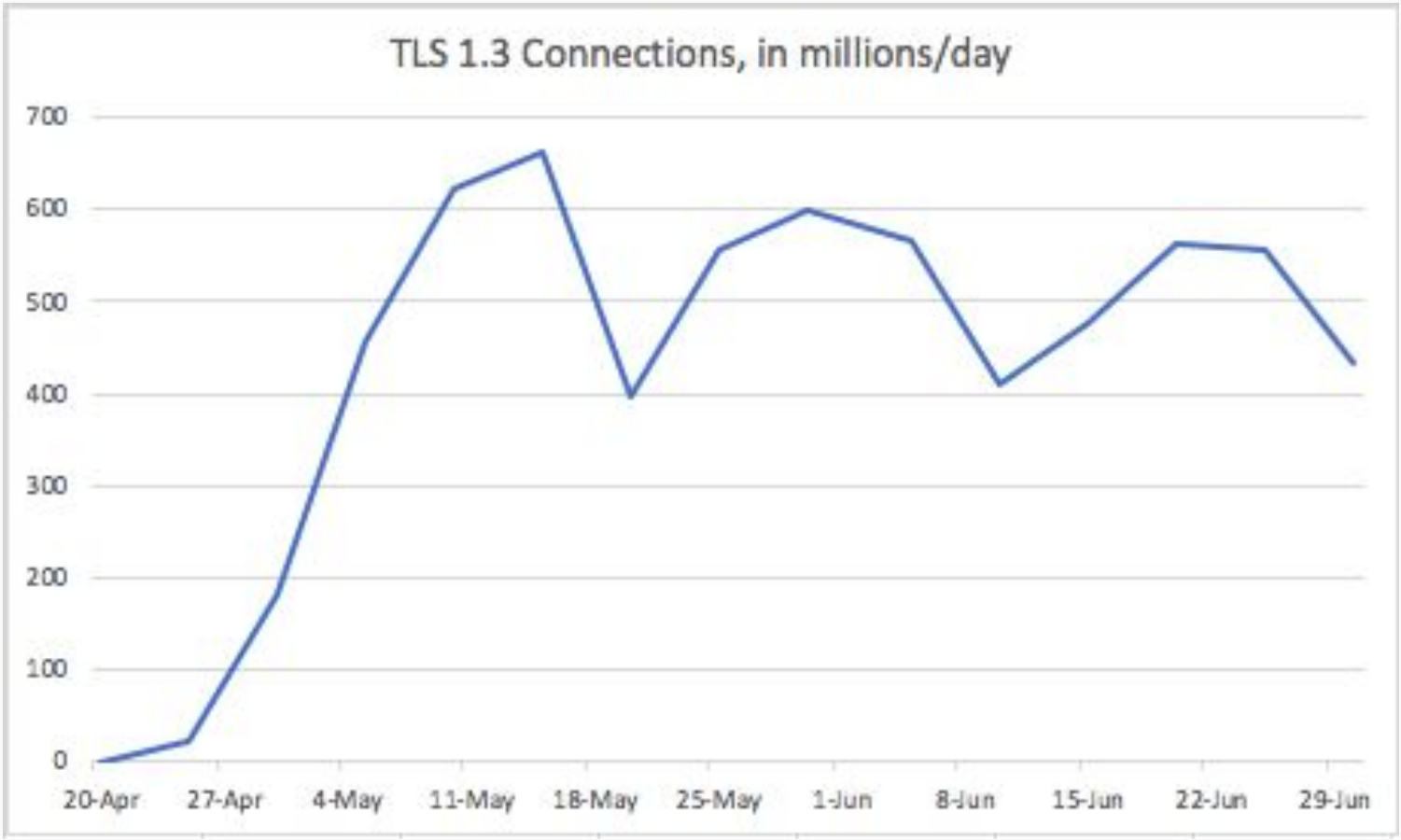
Ready for WGLC:

- Issues and Requirements for SNI Encryption in TLS

In Progress:

- DTLS 1.3
- DTLS Connection ID
- TLS Certificate Compression
- Applying GREASE to TLS Extensibility
- Delegated Credentials

TLS 1.3 Adoption Metrics


TLS 1.3 Connections, in millions/day
700
600
500
400
300
200
100
0
20-Apr
27-Apr
4-May
11-May
18-May
25-May
1-Jun
8-Jun
15-Jun
22-Jun
29-Jun

Protocol	Fraction
TLS 1.1	0.000474
TLS 1.0	0.00884
TLS 1.3	0.0257
TLS 1.2	0.964

Don't miss EMU!

Several TLS related agenda items:

- Using EAP-TLS with TLS 1.3
  draft-ietf-emu-eap-tls13
- Handling Large Certificates in EAP-TLS
  draft-ms-emu-eaptlscert

Friday 9:30 – 11:30, Notre Dame

emu by Jon Bunting https://www.flickr.com/photos/84744710@N06/14766013011