# TLS@IETF104

**WG Info:** https://tlswg.org

**Chairs:** Chris Wood, Joe Salowey, 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

Be succinct @ the mic

# Agenda

Monday 11:20-12:20 CET
Morning session II

| | |
|---|---|
| 05 min | Administrivia |
| 05 min | New Website |
| 10 min | Cert+PSKs |
| 10 min | Resumption Across SNIs |
| 10 min | External PSKs |
| 10 min | Client Network Address |
| 10 min | IBC+TLS |

# Agenda

Tuesday 16:10-18:10 CET
Afternoon session II

| | |
|---|---|
| 05 min | Administrivia |
| 05 min | Deprecating TLS 1.0/1.1 |
| 10 min | DTLS 1.3 |
| 10 min | Certificate Compression |
| 10 min | Delegated Credentials |
| 15 min | ESNI |
| 15 min | ESNI A/AAAA Divergence |
| 10 min | OPAQUE + TLS 1.3 |
| 10 min | Hybrid Key Exchange |
| 10 min | TLS with CWTs |
| 10 min | Fake SNI Extension |

# Document Status

**WGLCed:**

- Issues and Requirements for SNI Encryption in TLS
- Applying GREASE to TLS Extensibility
- Exported Authenticators for TLS

**Soon in WGLC:**

- DTLS 1.3
- TLS Certificate Compression
- DTLS Connection ID

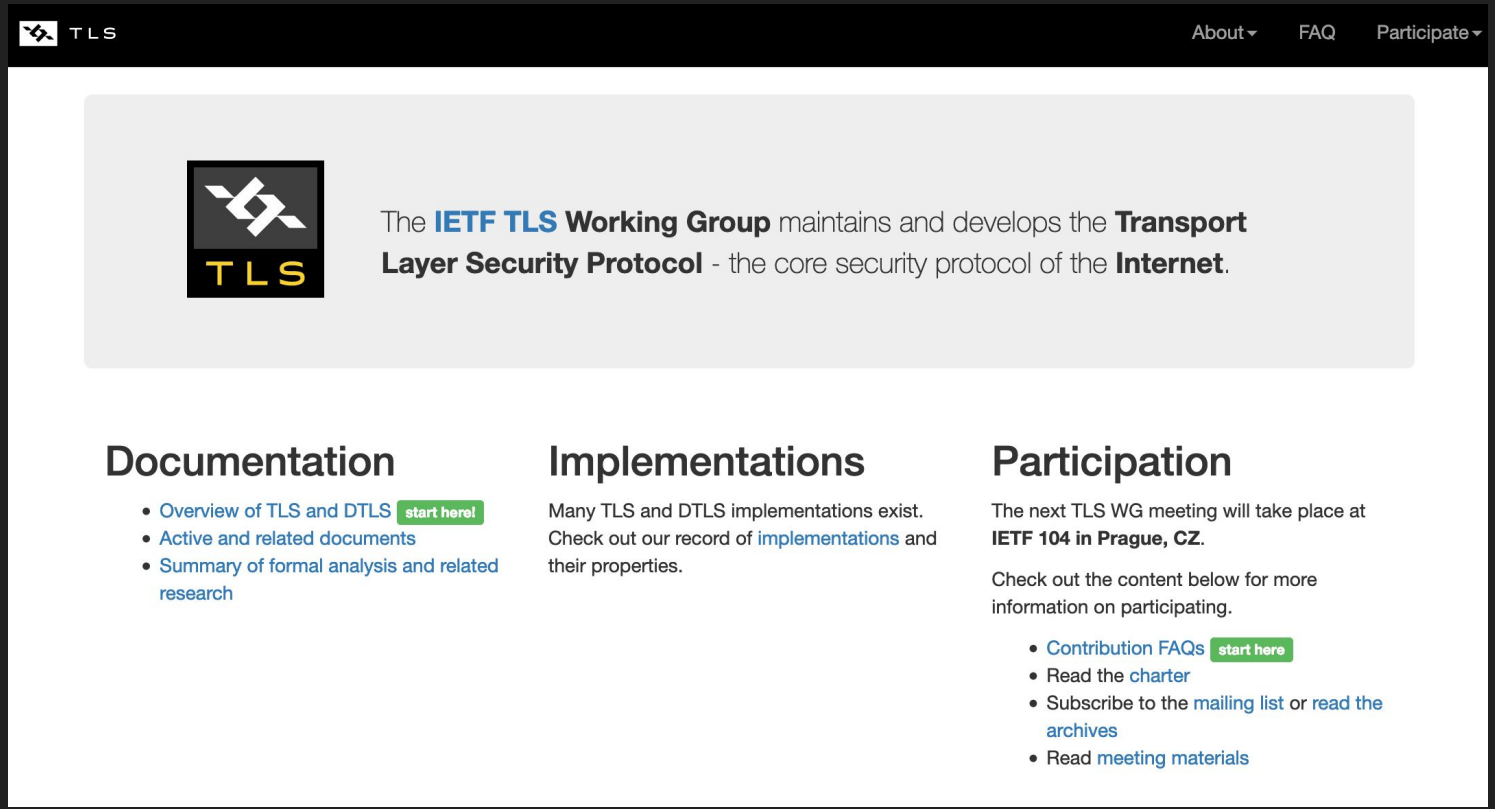
**In Progress:**

- Delegated Credentials
- ESNI for TLS

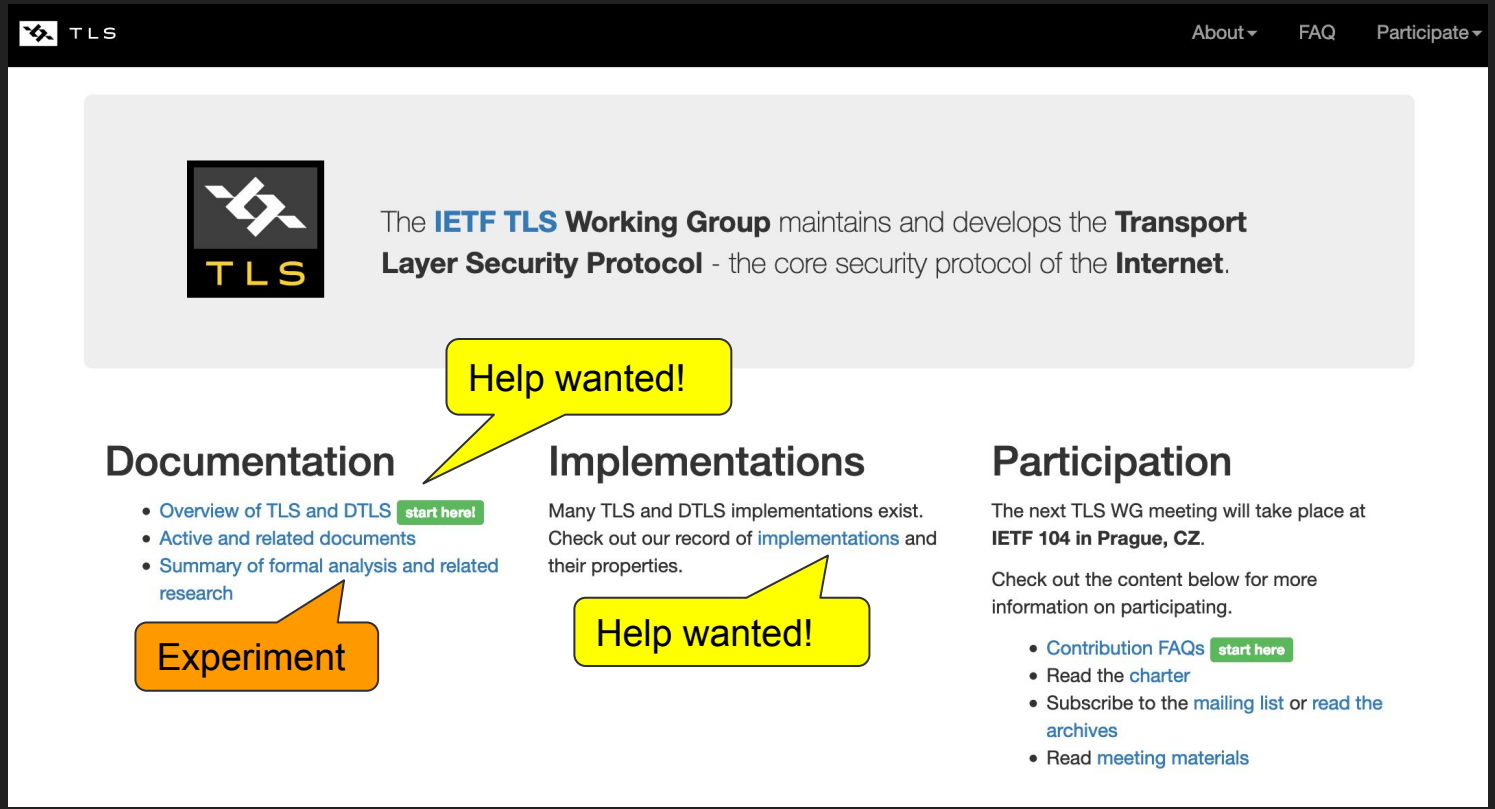
**Adopted:**

- Deprecating TLS 1.0 and 1.1
- Ticket Requests
- Cert+PSK for TLS 1.3

# New Website


TLS
About
FAQ
Participate
TLS
The IETF TLS Working Group maintains and develops the Transport Layer Security Protocol - the core security protocol of the Internet.
Documentation
Overview of TLS and DTLS start here!
Active and related documents
Summary of formal analysis and related research
Implementations
Many TLS and DTLS implementations exist. Check out our record of implementations and their properties.
Participation
The next TLS WG meeting will take place at IETF 104 in Prague, CZ.
Check out the content below for more information on participating.
Contribution FAQs start here
Read the charter
Subscribe to the mailing list or read the archives
Read meeting materials

# New Website


TLS
About
FAQ
Participate
TLS
The IETF TLS Working Group maintains and develops the Transport Layer Security Protocol - the core security protocol of the Internet.
Help wanted!
Documentation
Overview of TLS and DTLS start here!
Active and related documents
Summary of formal analysis and related research
Experiment
Implementations
Many TLS and DTLS implementations exist. Check out our record of implementations and their properties.
Help wanted!
Participation
The next TLS WG meeting will take place at IETF 104 in Prague, CZ.
Check out the content below for more information on participating.
Contribution FAQs start here
Read the charter
Subscribe to the mailing list or read the archives
Read meeting materials