



TLS@IETF104

WG Info: <https://tswg.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
<hr/>	
05 min	New Website
10 min	Cert+PSKs
<hr/>	
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
<hr/>	
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
<hr/>	
10 min	OPAQUE + TLS 1.3
10 min	Hybrid Key Exchange
10 min	TLS with CWTs
10 min	Fake SNI Extension



Document Status

WGLeCed:

- [Issues and Requirements for SNI Encryption in TLS](#)
- [Applying GREASE to TLS Extensibility](#)
- [Exported Authenticators for TLS](#)

Soon in WGLeC:

- [DTLS 1.3](#)
- [TLS Certificate Compression](#)
- [DTLS Connection ID](#)

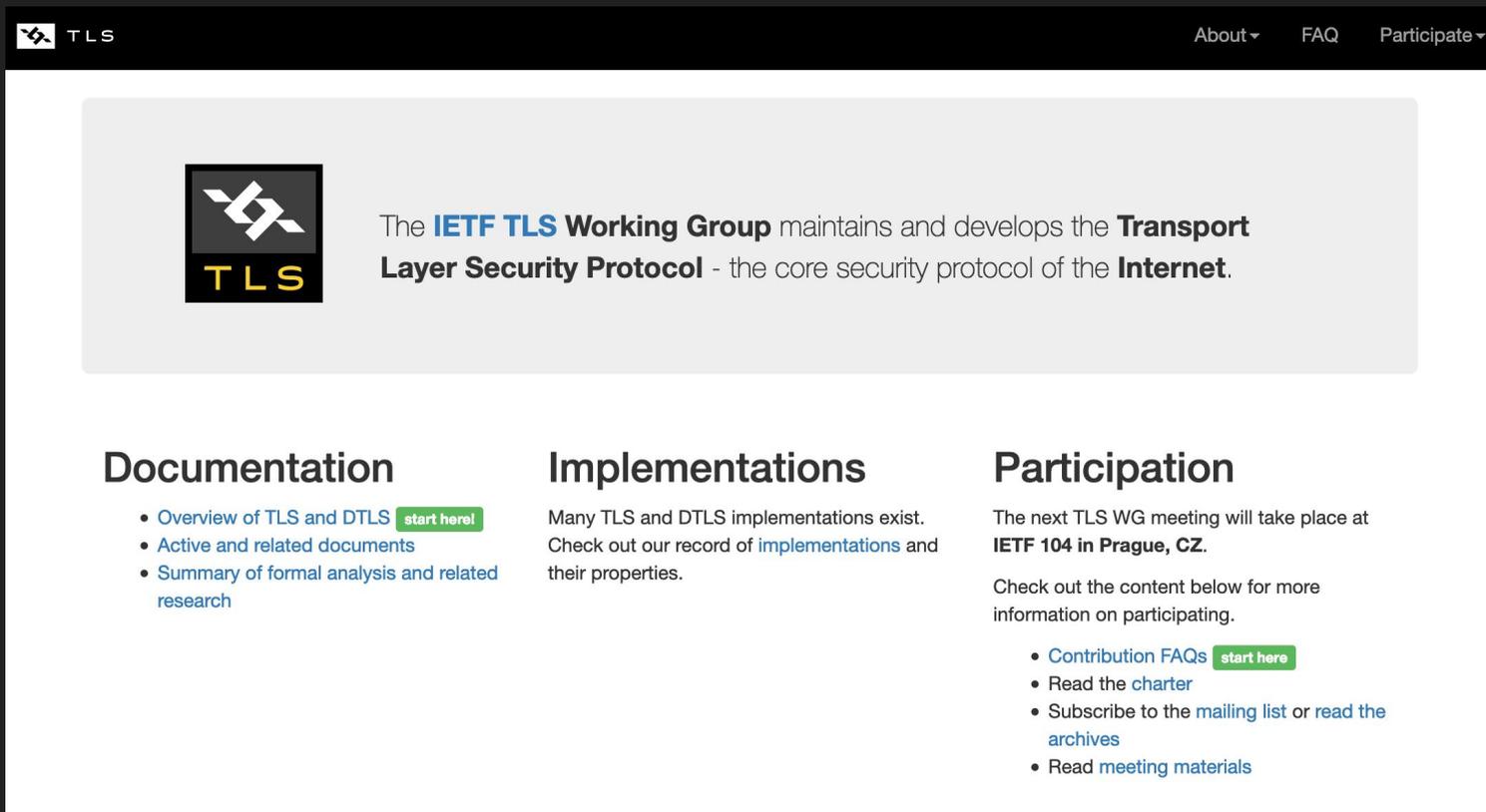
In Progress:

- [Delegated Credentials](#)
- [ESNI for TLS](#)

Adopted:

- [Deprecating TLS 1.0 and 1.1](#)
- [Ticket Requests](#)
- [Cert+PSK for TLS 1.3](#)

New Website



The screenshot shows the homepage of the IETF TLS Working Group website. At the top, there is a dark navigation bar with the TLS logo on the left and links for 'About', 'FAQ', and 'Participate' on the right. Below the navigation bar is a large light gray banner containing the TLS logo and a descriptive paragraph. Underneath the banner, the page is divided into three columns: 'Documentation', 'Implementations', and 'Participation'. Each column contains a list of links and a brief description. The 'Documentation' column lists links for an overview, active documents, and formal analysis. The 'Implementations' column states that many implementations exist and provides a link to a record of implementations. The 'Participation' column announces the next meeting in Prague, CZ, and provides links for FAQs, the charter, mailing list, archives, and meeting materials.

 [About](#) [FAQ](#) [Participate](#)

 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

The screenshot shows the IETF TLS Working Group website. At the top left is the TLS logo. At the top right are navigation links: "About", "FAQ", and "Participate". The main content area features the TLS logo on the left and a text block on the right stating: "The IETF TLS Working Group maintains and develops the Transport Layer Security Protocol - the core security protocol of the Internet." Below this are three columns: "Documentation", "Implementations", and "Participation". The "Documentation" column lists links for an overview, active documents, and formal analysis research, with a "start here" button next to the overview link. The "Implementations" column states that many implementations exist and provides a link to a record of implementations. The "Participation" column announces the next meeting in Prague, CZ, and lists links for contribution FAQs, charter, mailing list, archives, and meeting materials, with a "start here" button next to the contribution FAQs link. Three yellow callout boxes with the text "Help wanted!" are overlaid on the page: one pointing to the "start here" button in the Documentation section, one pointing to the "start here" button in the Participation section, and one pointing to the "Implementations" section header. An orange callout box with the text "Experiment" is also overlaid on the Documentation section.

TLS

About ▾ FAQ Participate ▾

 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](#)

Experiment

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](#)

Help wanted!

Help wanted!

Help wanted!