TLS@IETF106

WG Info: https://tlswg.org
Chairs: Joe Salowey, Sean Turner, Chris Wood
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
<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 min</td>
<td>Administrivia</td>
</tr>
<tr>
<td>15 min</td>
<td>Importing External PSKs for TLS</td>
</tr>
<tr>
<td>05 min</td>
<td>Exported Authenticators</td>
</tr>
<tr>
<td>05 min</td>
<td>Delegated Credentials</td>
</tr>
<tr>
<td>25 min</td>
<td>Compact TLS 1.3</td>
</tr>
<tr>
<td>15 min</td>
<td>Semi-Static Diffie Hellman</td>
</tr>
<tr>
<td>15 min</td>
<td>Batch Signing in TLS</td>
</tr>
<tr>
<td>15 min</td>
<td>TLS 1.3 Extended Key Schedule</td>
</tr>
<tr>
<td></td>
<td>Re-charter discussion</td>
</tr>
</tbody>
</table>
## Agenda

**Thursday Afternoon Session III**

<table>
<thead>
<tr>
<th>Duration</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 min</td>
<td>Administrivia</td>
</tr>
<tr>
<td>05 min</td>
<td>Well-known URIs for ESNI</td>
</tr>
<tr>
<td>10 min</td>
<td>Deprecating MD5+SHA1</td>
</tr>
<tr>
<td>40 min</td>
<td>Encrypted SNI</td>
</tr>
</tbody>
</table>
Document Status

RFC Editor Queue

- GREASE
- Issues and Requirements for SNI Encryption in TLS

IETF LC

- Cert+PSK for TLS 1.3

Publication Requested (waiting on AD):

- DTLS 1.3
- TLS Certificate Compression

AD Evaluation (waiting on AD):

- Deprecating TLS 1.0 and 1.1

Waiting for Write-Up (chairs):

- Exported Authenticators for TLS

WGLC: (just completed)

- Ticket Requests

In WGLC Soon:

- Delegated Credentials
- DTLS Connection ID

In Progress:

- ESNI for TLS
- External PSK Importers
- Deprecating MD5+SHA1
- TLS Flags Extension
Discussion Needed

Hybrid key exchange

RSASSA-PKCS1-v1_5 codepoints for TLS 1.3