

Using TLS in Applications WG (UTA)

IETF 111
July 28, 2021

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 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)

Meeting Details

- Chairs:
 - Leif Johansson
 - Valery Smyslov
- Responsible AD:
 - Francesca Palombini
- Meeting Slides: <https://datatracker.ietf.org/meeting/111/session/uta>
- MeetEcho: <https://meetings.conf.meetecho.com/ietf111/?group=uta&short=&item=1>
- Notes: <https://codimd.ietf.org/notes-ietf-111-uta>
- Jabber: <xmpp:uta@jabber.ietf.org?join>

Administrative Tasks

- Bluesheets (collected automatically)
- We need volunteers:
 - one Jabber Scribe
 - two Note Takers

Agenda

- 5 min **Administrivia (jabber scribes, note takers), Note Well, Agenda bashing** (chairs)
- 5 min **WG documents status update** (chairs)
- 20 min **Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)**
(Rich Salz), [draft-ietf-uta-rfc6125bis-01](#)
- 20 min **Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)**
(Peter Saint-Andre), [draft-ietf-uta-rfc7525bis-01](#)
- 5 min **Open Mic**
- 5 min **Closing** (chairs)

Document Status (WG drafts)

- [draft-ietf-uta-rfc7525bis-01](#)
Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
 - 2021-07-07, 34 pages
 - WG document
- [draft-ietf-uta-tls13-iot-profile-02](#)
TLS/DTLS 1.3 Profiles for the Internet of Things
 - 2021-07-12, 14 pages
 - WG document

Document Status (WG drafts)

- [draft-ietf-uta-rfc6125bis-01](#)
Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)
 - 2021-07-08, 35 pages
 - WG document