

uta @ IETF-90

Prague 2015

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

The IETF plenary session

The IESG, or any member thereof on behalf of the IESG

Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices

Any IETF working group or portion thereof

Any Birds of a Feather (BOF) session

The IAB or any member thereof on behalf of the IAB

The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

- Agenda Bashing & Note Well
- Document Status
 - RFCs and Errata
 - draft-ietf-uta-email-tls-certs (WGLC take 2)
- Deployable Enhanced Email Privacy (30 min)
 - draft-ietf-uta-email-deep
- TLS and DTLS Security Modules (10 min)
 - draft-urien-uta-tls-dtls-security-module-00
- Open Mic (10 min)

RFCs and Errata

RFCs

 RFC 7457 <i>(was draft-ietf-uta-tls-attacks)</i> Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS) 	2015-02 13 pages	Informational RFC
 RFC 7525 <i>(was draft-ietf-uta-tls-bcp)</i> Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) 	2015-05 27 pages	Best Current Practice RFC
 RFC 7590 <i>(was draft-ietf-uta-xmpp)</i> Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP)	2015-06 9 pages	Proposed Standard RFC

draft-ietf-uta-email-tls-certs

- Finished WGLC
- Some last-minute comments
- Need second WGLC?