Transport Layer Security (TLS)

Chairs:

Eric Rescorla

Joe Salowey

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**
- **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

1. Administrivia (Blue Sheets, note takes, agenda bashing) (5min)
2. DTLS 1.2 issues (15 min) (Eric Rescorla)

   draft-ietf-tls-rfc4347-bis-05
3. Charter (10min) (Joe Salowey / Sean Turner)
4. Next Protocol Negotiation (15 min) (Adam Langly / Mike Belshe) draft-agl-tls-nextprotoneg-00
5. AES-CCM Ciphers (5 min) (Matt Campagna) draft-mcgrew-tls-aes-ccm-ecc-01draft-mcgrew-tls-aes-ccm-01
6. EAP and TLS (5 min) (Yoav Nir) draft-nir-tls-eap-10
7. Renegotiation Patch status (5 min) (Yngve N. Pettersen)

   http://my.opera.com/securitygroup/blog/2010/11/04/a-few-results-from-the-tls-prober
8. Multiple OCSP enhancements (time permitting) (Yngve N. Pettersen) draft-pettersen-tls-ext-multiple-ocsp-02

Open DTLS Issues

Charter Revision

- TLS Charter is many years old and needs to be revised
- Primary goals of the WG are to maintain
  - The TLS protocol, RFC 5346
  - The TLS extension definitions, RFC 6066;-
  - The DTLS protocol, RFC 4347bis.
  - avoid gratuitous changes to these protocols
- The secondary goals of the WG are to publish
  - Recommendations for use of TLS
  - Extensions to TLS and DTLS
  - Cipher suites

Next Protocol Negotiation

- Mike Belshe

AES-CCM Ciphers

- Matt Campagna

Renegotiation Patch Status

- Yngve N. Pettersen

Multiple OCSP Extension

- Yngve N. Pettersen