Transport Layer Security (TLS)

IETF 73
Thursday, November 20 2008 0900-1130
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,
•-any IETF working group or portion thereof,
•-the IESG or any member thereof on behalf of the IESG,
•-the IAB or any member thereof on behalf of the IAB,
•-any IETF mailing list, including the IETF list itself,
•any working group or design team list, or any other list
•functioning under IETF auspices,
•-the RFC Editor or the Internet-Drafts function
•

All IETF Contributions are subject to the rules of RFC 3978 (updated by RFC 4748) 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 3978 (and RFC 4748) 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.

Agenda

- Agenda bashing (5 minutes) - chairs
  Bluesheets, Agenda changes, Scribe for minutes, Jabber scribe
- Document status (5 minutes) - chairs
  Progress since last IETF
- DTLS 1.2 (30 minutes) - Eric Rescorla
  draft-ietf-tls-rfc4347-bis-01.txt
  Known issues
  Next steps
- PSK Ciphersuite Drafts (10 min) - chairs
  draft-ietf-tls-ecdhe-psk-05.txt
  draft-ietf-tls-psk-new-mac-aes-gcm-05.txt
- TLS Extensions: Extension Definitions (10 minutes) – Don Eastlake
  draft-ietf-tls-rfc4366-bis-03.txt
  Open issues
  Next steps

Document Status

- draft-ietf-tls-des-idea-02
  - Completed IETF Last Call
- PSK Cipher suites
  - draft-ietf-tls-ecdhe-psk-05 and draft-ietf-tls-psk-new-mac-aes-gcm-05
  - Handed off to IESG, one issue to discuss today
- draft-ietf-tls-extractor-03
  - In WG last call
- draft-ietf-tls-rfc4366-bis-03
  - Open Issues
- draft-ietf-tls-rfc4347-bis-01
  - Open Issues

Cipher Suites Question

- When we define new cipher suites that do not require TLS 1.2 features (like AEAD), should we

  (1) specify that they are for TLS 1.2 only

  (MUST NOT be negotiated with TLS 1.0/1.1)

  (2) allow them to be used with TLS 1.0/1.1

  (e.g. say that TLS 1.0/1.1 PRF is used when 1.0/1.1 is negotiated)

Extension Draft
Open Issues

- Cert URL Hash
  - Close call between “just deprecate” and “make hash mandatory”
  - If mandatory do we need crypto-agility
- Hash Agility for Certificate URLs
  - Is it needed?