Transport Layer Security (TLS) IETF-85

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.

TLS Agenda

IETF-85 TLS Meeting
TUESDAY, November 6, 2012 - 1700-1830
---

1. Note Well, Agenda, Note Takers, Blue sheets (5 Min)
2. Cached Info (10 Min) - Tschofenig
   http://tools.ietf.org/html/draft-ietf-tls-cached-info-13
3. Certificate Status Extension (5 Min) - Pettersen/Chairs
   http://tools.ietf.org/html/draft-ietf-tls-multiple-cert-status-extension-02
4. Out-of-band public key validation (15 Min) - Wouters
   http://tools.ietf.org/html/draft-ietf-tls-oob-pubkey-06
5. HTTP 2.0 Upgrade - Nottingham (10 min)
6. Origin Bound Certificates update (10 min) - Langley
7. DTLS Multicast Security (15 Min) - Sye Loong
   http://tools.ietf.org/html/draft-keoh-tls-multicast-security-00
8. TLS Tack (15 Min) - Perrin
   http://tools.ietf.org/html/draft-perrin-tls-tack-01

Cached Info

http://tools.ietf.org/html/draft-ietf-tls-cached-info-13

- Last call completed
- Open issues
  - ability to indicate intermediate CA certs are cached
  - length of ID field

Multiple OCSP

http://tools.ietf.org/html/draft-ietf-tls-multiple-cert-status-extension-02

- Removed SCVP
- Ready for WGLC

Out-of-band public key verification

http://tools.ietf.org/html/draft-ietf-tls-oob-pubkey-06

- New revision uses cert type approach, however we do not have consensus on how it is incorporated related to PGP spec

Request for TLS from HTTPbis

This is a request from the HTTPbis Working Group for you to commence work upon a mechanism that allows clients and servers to negotiate the particular application protocol to use once the session is established.

Our use case is for HTTP/2.0 in conjunction with HTTPS URIs; rather than defining a new port, which incurs both performance and deployment penalties, a negotiation mechanism would allow for better deployment of HTTP/2.0 for HTTPS URIs.

We would expect such a mechanism to allow the client and server to negotiate the use of one of potentially many such protocols (in our case, HTTP/1.x and HTTP/2.x), identified by tokens, and falling back to a default for the port in use (in our case, HTTP/1.x) when either side doesn't support negotiation, or an agreement can't be found.

We also note existing work in this area:

http://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

http://www.ietf.org/id/draft-friedl-tls-applayerprotoneg-00

The HTTPbis Working Group will be happy to coordinate schedules, review drafts and provide further input as required.