Transport Layer Security WG

IETF 81

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

1. Administrivia (5 minutes) - chairs
   - Bluesheets
   - Agenda changes
   - Scribe for minutes
   - Jabber scribe
2. Document status (5 minutes) - chairs
3. DTLS Heartbeat (10 Min) - Tuexen
4. Working Group Handling for Extensions to TLS (45 min) - chairs
5. TLS Origin-Bound Certificates (15 min) - Balfanz
6. TLS Extension for out-of-band public key validation (10 min) - Wouters
7. DNSSEC-stapling (15 min) - Hoffman

Updates Since Last Meeting

- DTLS 1.2 Approved by IESG
- New TLS Charter

TLS Extensions Policy

IETF 81

Eric Rescorla

ekr@rtfm.com

Background

- RFC 5246 Defines support for TLS Extensions
  - TLS Client offers in ClientHello
  - TLS Server confirms in ServerHello
- IANA Requirements
  - TLS extension code points require IETF Consensus
  - TLS ContentTypes and HandshakeTypes require Standards Action
- Lots of new extensions being proposed
  - Idea is to have a clear policy

Extension Categories*

1. Trivial – does not affect TLS processing proper
   - Example: New TLS Exporter type
2. Non-Trivial – affects TLS processing but not the state machine or basic model
   - Example: MAC truncation
3. Significant – modifies the state machine, adds/reorders/removes messages
   - Example: TLS tickets [RFC 5077]

* New names wanted here

Policy for Trivial Extensions

- MUST be sent to TLS WG either prior to or during IETF LC
- Significant objections MUST be addressed/resolved prior to publication
- To be assessed by the AD with guidance from the WG Chairs

Non-Trivial Extensions

- MUST be explicitly presented to the TLS WG
- TLS WG MUST not have serious objections
- No need for consensus in favor
- Examples
  - No comments: OK
  - 2 technical comments, both against: not OK
- To be assessed by the WG chairs

Significant Extensions

- MUST be WG items–or joint items with another WG
- MUST have WG consensus
  - Manys of these documents would need to be standards track in any case
- MUST have significant non-author support
  - How do we define "significant"?
  - Enough to believe the work will complete and be implemented
- To be assessed by the WG chairs