December 09, 2015 Meeting Minutes

Meeting commenced 8:00PM GMT

- Roll call (Tony C)
- Quorum achieved

Opening Notes

- Valerie thanked BobR for running the meetings in her absence

Proposed agenda

- V2.40
  - Errata process update
  - "Black box warning" misplaced?
  - TLS 1.0/1.1 mechs
- V2.41
  - Next Steps
  - Dina: TLS 1.X text improvements
- V3.0
  - any discussion
- Face to face
- Interop update
- Topics for next call
- New Business
  - Non
- Review Action Items
- Adjourn

Motion to approve Agenda

- Tim Moves, Jeff Seconds, no objections, no abstentions. Agenda approved

Motion to approve meeting minutes

- November 11th, 2015

- Tim Moves, Jeff Seconds, no objections, no abstentions. Minutes approved

v2.40

Errata process update

- Bob G noted that he has uploaded the various documents for review such we can vote on them, including the header files that Tim posted.
- Tim suggested that getting a ballot done ASAP would be beneficial rather than wait until the new year given the next meeting is likely cancelled.
- Discussion about voting/ballotting process
- Agreement that we will go to a 7 day ballot for all three items - see ballot wording.
- Motion in accordance with section 3.5 of the TC process to adopt as a Committee Specification Draft the v2.40 errata and related documents (as posted by Bob Griffin and Tim Hudson - see below) and that the proposed corrections do not constitute a Substantive Change and if the motion passes for the co-chairs to submit the proposed corrections for a 15-day public review with the normal designed cross-reference changes by TC admin.
  - pkcs11-base-v2 40-errata01-wd01
  - pkcs11-curr-v2.40-errata01-wd01
  - pkcs11-hist-v2.40-errata01-wd01
  - pkcs11-base-v2.40-os-rev01-wd0
  - pkcs11-curr-v2.40-os-rev01-wd01
  - pkcs11-hist-v2.40-os-rev01-wd01
  - pkcs11-v240-errata-headers
- Tim Moves, BobG Seconds, no objections, no abstentions. Motion passes.

"Black box warning" misplaced?

- Valerie not on call - deferred

TLS 1.0/1.1 mechs

- BobG noted the item that Valerie and Dina had raised.
- BobR noted that Tim and BobR discussed this with respect to NSS.
- Tim suggested tabling this for the next meeting where Dina is present or handle it at the face to face.
- Tim noted that Bob had included the requested warning in the errata (informative only) about the TLSv1.2 mechanisms.

v2.41

Next Steps

- Chris had some items - deferred

Dina: TLS 1.X text improvements

- Dina not on call - deferred

V3.0

- Need to focus on IV generation to keep up with the NIST "recommendations"
- Valerie encouraged team members to respond to emails

Face to Face

- Straw poll has indicated that Friday 26th Feb the preferred date.

Motion to hold face to face on 26th February 2016

- BobR Moves, Jeff Seconds, no objections, no abstentions. Motion passes.

Interop update

- Tony provided an update. Participant email list is now active and Tony will send out preliminary emails to participants this week.

Next meeting date

- 13th January 2016

Next meeting proposed agenda

- F2F organisation around RSA2016

Action Items

- Moved to Jira - https://issues.oasis-open.org/browse /PKCS/?selectedTab=com.atlassian.jira.jira-projects-plugin:issues-panel
- All members with open action items to provide an update at next meeting.
- Tim to upload draft v2.40 header files to the repository (11Nov2015)
- Tim and Dina to draft a note to go into the wiki relating to issues with TLS implementation (11Nov2015)

Call for late arrivals

- 2 late arrivals noted

Motion to Adjourn

- Tim Moves, BobG seconds, no abstentions, no objections. Motion approved

Meeting Adjourned at 8:27PM GMT

Meetingminutes/Minutes09122015 (last edited 2015-12-28 03:32:46 by Tony.Cox)