November 05, 2014 Meeting Minutes

Role Call

- Bob performed roll call, we have quorum. This will be an official meeting.

Proposed Agenda

1 Opening remarks (co-chairs)

2 Roll call

3 Review / approval of the agenda

4 Review of previous meeting minutes

5 Old Business

- Status of V2.40
  - Vote on request for ballot for V2.40 committee specs / note (cs02, cn02)
  - SHA-512 issue raised by Dina
  - Test vector issue raised by Oscar
  - CKM_TLS_MAC issues raised by Oscar
- Face to face planning
- 2.40 Errata
- Implementation page
- V2.x topics
  - Update on outstanding v2.x items (Wan-Teh proposal)
  - Tim H./Sven's list for 2.41 features update
- v3.0 topics
  - Graham's proposal on Secure Key Import
- Topics for next call

6 New Business

7 Review Action Items

8 Adjourn

Opening Remarks

Agenda Additions

Motion to accept agenda

- Tim moved, Gershon seconded. No objections or abstentions or discussions.

Approve Previous Meeting Minutes

- September 24, 2014 - had to revert, no reapproval required
- October 8, 2014 - Deferred until next meeting

Status on 2.40

Vote on request for ballot for V2.40 committee specs / note (cs02, cn02)

Motion #1

- Do you approve the following documents as Committee Specification Draft or Committee Note Draft, as indicated, and designate the Word version of each document as authoritative?

PKCS #11 Base Specification Version 2.40 working draft 11 contained in https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/54456/pkcs11-base-v2.40-wd11.doc as Committee Specification Draft

csd04 (authoritative source)

PKCS #11 Current Mechanisms Specification Version 2.40 working draft 12 contained in https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/54453/pkcs11-curr-v2.40-wd12.doc as Committee

Specification Draft csd04 (authoritative source)

PKCS #11 Historical Mechanisms Specification Version 2.40 working draft 07 contained in https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/54450/pkcs11-hist-v2.40-wd07.doc as Committee

Specification Draft csd03 (authoritative source)

PKCS #11 Usage Guide Version 2.40 working draft 08 contained in [[[[https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/54447/pkcs11-ug-v2%2040-wd08.doc|https://www.oasis-|https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/54447/pkcs11-ug-v2%2040-wd08.doc|https://www.oasis-]]

open.org/apps/org/workgroup/pkcs11/download.php/54447/pkcs11-ug-v2%2040-

wd08.doc]] as Committee Note Draft cnd03 (authoritative source)

- Tim moves, Bob R seconded. No objections or abstentions or discussions. Unanimous motion passed as stated above.

Motion #2

- Do the members of the PKCS 11 TC authorize the Co-Chairs to submit requests to TC Administration to hold a Special Majority Ballot to approve the following documents as Committee Specification or

Committee Note, as indicated?

PKCS #11 Base Specification Version 2.40 csd04 contained in https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/54456/pkcs11-base-v2.40-wd11.doc as Committee Specification (authoritative

source)

PKCS #11 Current Mechanisms Specification Version 2.40 csd04 contained in https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/54453/pkcs11-curr-v2.40-wd12.doc as Committee Specification

(authoritative source)

PKCS #11 Historical Mechanisms Specification Version 2.40 csd03 contained in https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/54450/pkcs11-hist-v2.40-wd07.doc as Committee

Specification (authoritative source)

PKCS #11 Usage Guide Version 2.40 cnd03 contained in [[[[https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/54447/pkcs11-ug-v2%2040-wd08.doc|https://www.oasis-|https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/54447/pkcs11-ug-v2%2040-wd08.doc|https://www.oasis-]]

open.org/apps/org/workgroup/pkcs11/download.php/54447/pkcs11-ug-v2%2040-wd08.doc]] as Committee Note (authoritative source)

The TC affirms that only non-material changes have been made to these documents since the last public review. The changes made are documented in https://www.oasis-

open.org/apps/org/workgroup/pkcs11/download.php/xxxxx. The TC judges these changes to be Non-Material in accordance with the definition in the OASIS TC Process (http://www.oasis-open.org/policies-

guidelines/tc-process#dNonmaterialChange).

In addition, do the members also approve requesting TC Administration to update the following Designated Cross-References during publication of the Committee Specification:

- Current references to be updated:

[PKCS #11-Base] PKCS #11 Cryptographic Token Interface Base Specification Version 2.40. Latest version. http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-v2.40.html.

[PKCS #11-Curr] PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40. Latest version. http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/pkcs11-curr-v2.40.html.

[PKCS11-Hist] PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification Version <<VERSION>>. <<DATE>>, OASIS Working Draft, http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/pkcs11-

hist-v2.40.html

[PKCS #11-Prof] PKCS #11 Cryptographic Token Interface Profiles Version 2.40. Latest version. http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/pkcs11-profiles-v2.40.html.

[PKCS #11-UG] PKCS #11 Cryptographic Token Interface Usage Guide Version 2.40. Latest version. http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/pkcs11-ug-v2.40.html.

- Tim moves, Bob R seconded. No objections or abstentions or discussions. Unanimous motion passed as stated in two parts above.

SHA-512 issue raised by Dina

- Dina: When SHA-512 was proposed - there was an issue with the HMAC_General as we just copied that in. On investigation, it doesn't really make sense to have SHA-512_HMAC_General, as you would just use SHA-512_HMAC. So it appears that HMAC-General was a mistake to add and should be removed. A second question is why is HMAC_general there for SHA-1 etc?
- Bob R: HMAC general simply allowed you to get the bits you need and cut it down.
- Dina: So in the context of SHA-512, does it still make sense to keep HMAC_General?
- Bob R: If you just wanted truncated version of the HMAC, then it makes sense to keep it.
- Dina: Bob R are you saying we need to keep SHA-512_HMAC_general?
- Bob R: I don't know if it's in use but it is not exactly superfluous as some folks

may use it.
- Tim: I think consistency is important here - I can't see the use for a truncated HMAC but other folks may use it.
- Bob G: I would propose to leave SHA-512_HMAC_general should remain for the next release and we'll reconsider if someone proposes a reason
- No further concerned raised - leave HMAC_general in.

Test vector issue raised by Oscar

- Oscar: How do we get test against the new test vectors proposed by Encipher folks on the IETF site
- Bob R: Tim, do you have any isight into the test vectors?
- Tim: The published test vectors including the IETF work is well out of date
- Bob G: Valerie - does it make sense so canvas the various companies and publish some known test vectors?
- Valerie: Unsure how we would go about using or certifying it but it makes sense to collate them
- Bob R: We don't have any vectors for later versions - they're either older tests or NSS-specific tests.
- Tim: I'm not aware of anything like what Oscar is chasing but I think collating the known tests into the wiki would be good.
- Tim: I'm happy to set up a wiki page to that effect.

CKM_TLS_MAC issues raised by Oscar

- Oscar: The latest PKCS11 - there are two designs (CKM_TLS_1.2_MAC and CKM_TLS_MAC) - do we include both in the header files?
- Bob R: TLS_MAC refers to TLS 1.0 and TLS 1.1 and TLS_MAC 1.2 refers to TLS 1.2 so we should keep both.
- Oscar: OK so we'll keep both.

Face to Face

- Bob G: I've looked at the various dates and locations and commenced construction of the straw poll and wondered if folks had further suggestions. I'm also including the NIST crypto workshop in Gaithersburg in April.
- Sven: I believe there's an IBM event in Las Vegas a few weeks after the Barcelona event
- Bob G: Thanks Sven, can you please send details and I'll include that in the poll

2.40 Errata

- Bob G: After talking to OASIS - we can't do an errata unless it's a candidate spec so we'll need to make the changes as part of the next point release, so no change there.

Implementation page

- PKCS11 known implementations: https://wiki.oasis-open.org/pkcs11/KnownPKCS11Implementations
- Tim: Folks are adding items in there which is good to see.
- Valerie: Just a reminder to folks to review it and add items as you can.

V2.x topics

- Update on outstanding v2.x items (Wan-Teh proposal) - no update at this point from Bob R

V2.41 feature list

- Sven: I'd propose a call with a smaller group to work on this.
- Bob G: I feel you should bring forward a proposal
- Sven: I'm at a conference this week at a smartcard event with token management people (Interceded, Bell ID, Opentrust, entrust, etc) and they have a pile of requirements that depend on the commands I've also proposed for personalization and initialization. But that's a level of detail that I think might not be appropriate for this forum. I would suggest a 1-2 hour meeting to get into the details and refine the proposal.
- Bob G: Valerie could we do a call at the this time next week as a sub-group
- Valerie: Yes I believe that makes sense as long as that's OK under OASIS
- BoB R: I'll send out an invitation for a meeting next week.

v3.0 topics

- Graham's proposal on Secure Key Import - no update

Topics for Next Call

- Bob R: I'd like to discuss and agree the scope and content of the pointr release before we break for the holiday season. I'll pull together a list as a first cut for that meeting.

New Business

- Sven: A quick feedback on my presentation of the US Smartcard Government conference - NIST, NSA, DOD, etc were all represented. Discusses the 6M issued smartcards for the US-PIV (SP-800-73). There was a panel discussion that agreed that "we have the opportunity to make PKCS11 the standard for the different mobile platforms" so it appears that we have the support of the US

government to push this through in SP-800-73-v4 to allow use and deployment on tokens and mobile platforms.mobile devices.

- Bob G: I'll touch base with you to see if there's something that needs to be included in the next release, so we can discuss it on our next call.

Action Items

- Valerie: create 3.0 suggestion document, move 2.40 suggestions over into new 3.0 suggestion document. (not started, yet) (09042014.01)
  - Bob: will make a first pass by going through meeting minutes. I will send to Valerie, who can clean it up and post to the wiki.(09042014.02) (Complete Aug 3, 2014)
- Valerie (et al): add new suggestions to the 3.0 wiki, so we can track if they have owners and are moving forward. (09042014.03)
- Bob G: how about I take time to write up a couple of paragraphs on how to get out a new mechanism to take to the team by the next meeting? (04062014.01)
- Tim H: send suggestions on how to handle minor updates prior to v3.0 to the list (16072014.01)
- Valerie: Check with her team to see if anyone will be picking up Darren's proposal from a few weeks back (10092014.01)
- Bob G: Check with Chet to see if we have to do anything special for the header files (10092014.02)
- Valerie: Follow up on timeline for new AES-XTS proposal (10092014.03)
- Bob G: Start with Stef's document and make an amendment doc. Stef's broken definitions write-up (24092014.01)
- Bob G: I believe we can do errata's against committee spec, so we won't have to wait 90 days, but I will check with Chet (24092014.02)
-

Motion to Adjourn

- Chris moved, Bob R seconded. No objections or abstentions or discussions. Adjourned 1:49PM US-PST.

MeetingMinutes/Minutes05112014 (last edited 2014-11-06 19:16:08 by bubbva)