May 02, 2018 Meeting Minutes - Approved

Meeting commenced 1:00 PM PST

- Roll call (Tony) - quorum achieved.

Proposed agenda

- Roll call
- Review / approval of the agenda
- Review of previous meeting minutes (April 11, 2018)
- RSA2018 Interop Showcase
- V3.0 Items (Other business to be covered in the following meetings)
  - Review Spec V3 from Chris Z
  - Review Mechanisms V3 form Chris Z
  - Planning for review/complete
  - Get function list and functions in header files (Bob)
  - Revisit Function list
  - Stef's Proposals
- Comment on comments list (Girish Kumar, CKA_TRUSTED). (Tony C) (https://lists.oasis-open.org/archives/pkcs11-comment/201709/msg00000.html)
- Comments list query (Timo Teras, ETSI TS 103 097 certificates)
- Letter to NIST regarding AES GCM IV generation (Tony)
- New business
- Next meeting
- Call for late arrivals
- Adjourn

Motion to approve Agenda

- Greg moved, Gerry seconded. No objections, comments or abstentions. Agenda approved.

Motion to approve meeting minutes

- April 11, 2018
- Gerry moved. Greg seconded. No objections, comments or abstentions. Minutes approved.

RSA2018 Interop Showcase

- 4 vendors participated, had some generic PKCS#11 presentations (Bob & Tony), lots of visitors and questions. Vendors covered what they were doing for PKCS#11 in their slides as well.
- Passed on message to Dee and Jane that the TC will not be requesting booth space at RSA 2019, but would rather focus on ICMC 2019.

v3.0 Items

Review Spec V3 from Chris Z, Review Mechanisms V3 form Chris Z

- Tony had action item to ask Chris to provide context diffs, he has passed on this request. Chris, when ready, will upload to repository.
- Tony/Chris: 3.0 is 'locked' so Chris can finish.
- Bob: There were a few approved things that hadn't made the document and the work items page, that was updated, plus Stef's.
- Chris: No more after that?
- Tony: Unless something uncovered during the review, of course.
- Valerie: Will the comments already been provided be incorporated?
- Chris: I haven't seen them, but if I can find them, they will be incorporated. I need to work in batches. will go back and read the reflector.
- Valerie noted they won't necessarily have obvious subjects, they may refer to 3.0 or to a specific section or mechanism

Profiles document

- Tim: Haven't had time, but will get these updates shortly.

Planning for review/complete

- Tony: Let's keep pushing these forward, check in next week.

Stef's proposals

- All ballots approved, Tony will make sure they are on the 3.0 Work Items wiki

Get function list and functions in header files

- Bob will make the changes to get the new functionlist in there.
- Hamish: brought up git review comment on missing montgomery related items - will that be addressed?
- Bob: Documented several changes to reflector that were approved in F2F, please check when the review comes out to make sure they are done.
- Hamish: Looking at the working version in github, is that the right place?
- Bob: The OASIS github? Hamish: yes.
- Valerie: You will be sending out contextual diffs? Bob: Yes, when ready to review.
- Bob: Using the identifier allocator had found a few missing items, appreciates feedback.

Revisit function list naming

- (last discussed in detail 7 March 2018, first came up on 7 February 2018)
- Tony, Tim believe the discussion was complete. Valerie noted we deferred on April 4 and deferred on April 11.
- Tim we had a deliberate ballot with the names as it was, that was on purpose. No views have changed. Tim thought it came up in a meeting he missed, but it came up from review comments. Bob noted that there was follow-on discussion Bob & Tim had missed,
- Daniel - it was my review comment. I was puzzled. Nobody could explain why. If it was deliberate, someone should be able to explain.
- Bob: we did this so we would not have functions with the same name but a new meeting.
- Daniel: Understood, but I had a counter proposals where we switch only the suffix.
- Bob: When we wrote sample code, it was confusing in the two loops w/out the names being more different. Now you can see what's inner/outer.
- Daniel: It sounds like it's just you're used to it?
- Bob: Don't want to get into bike shedding
- Tim: We did have a few versions of this proposal and TC chose this option.
- Tim moves to stick with the function names in the already balloted proposal from before. Bob seconds. Any objections, abstentions or comments? 1 objection (Daniel),
    - Comments:
    - Chris: thought there would be more discussion and hash out. Seemed brushed under rug. Valerie concurs. Valerie is not saying she did not participate in the discussion, but not happy with how the discussion has happened (or not happened).
    - Bob: Naming can always be contentious, bringing up stuff late in the game makes it hard to address. There are valid reasons to like it and not like it. As much as Daniel doesn't like this, Bob does not like the other way. There are good reasons to do both, but does not revisit. We made the decision once, we should not continue to revisit, unless it was a mistake.
    - Daniel: He got replies personally from other TC members that his point was valid, so probably not alone. What are we doing in this review process right now? Shouldn't we get new people's opinions? What if something is not fine?
    - Valerie: review purpose is 2 fold: Making sure proposals are accurately captured and make sure they are technically correct (no non-functioning mechanisms, mismatched identifiers, etc, like found in 2.40 that led to an errata)
    - Bob: Could've dialed back the rhetoric to make it clear it was done on purpose, not a mistake
    - Daniel: The only time to change it is now, not after header files are out.
    - no additional objections, abstentions or comments. Motion approved.

Comment on comments list (Girish Kumar, CKA_TRUSTED). (Tony) (https://lists.oasis-open.org/archives/pkcs11-comment/201709/msg00000.html)

- Tony to reply.

Comments list query (Timo Teras, ETSI TS 103 097 certificates) - Tony to reply

- Tony to reply

Letter to NIST regarding AES GCM IV generation (Tony)

- No response to our letter, do we wish to reiterate? Or let it lie?
- Tim suggested co-chairs and secretary try to touch base with NIST at ICMC.
- Valerie - do we need to check with OASIS Admin?
- Tony does not believe this is necessary, since it is conversation vs written letter. We could just have a casual conversation.
- Tim - we could move to appoint an official liaison to NIST?
- no disagreements with doing this casually at ICMC.

New business

-

Next meeting

- 16 May 2018, week after ICMC

Call for late arrivals

- Bruce, Indra

Motion to Adjourn

- Tim moved. Gerry seconded. No objections, comments or abstentions. Adjourned.

Meeting Adjourned at 1:53 PM PST

Meetingminutes/Minutes02052018 (last edited 2018-05-02 20:58:56 by bubbva3)