March, 15 2017 Meeting Minutes

Meeting commenced 13:00 PST

- Roll call (Tony C) - quorum achieved

Proposed agenda

- Roll call
- Review / approval of the agenda
- Review of previous meeting minutes (March 1, 2017)
- Deadlines (Tony C.)
    - V3.0
        - Items from PR comments on 2.4 - proposals required
            - Item 12 – make the doc match the header file (Chris Z)
            - Item 20 – might be replaced by work Dina is already doing (Dina K)
            - Item 13, 21 – provide proposal for the proposed documentation content for header file items noted (Dina K)
            - Items 14, 15, 16, 18, 19 – provide proposal for the proposed documentation content for header file items noted (Bob R)
            - Item 17 – provide proposal for the proposed documentation content for header file items noted (Tim H)
    - EncryptCancel/DigestCancel/etc (Darren J)
    - Additional ECC Curves (Darren J)
    - Testing Profiles (Mark J & Anthony B.)
    - AEAD/AES GCM proposal/Extending Function Table/Forking (Bob R & Tim H)
    - Function table (Bob R)
    - CKM_AES_KEY_WRAP_PAD (Dieter B.)
    - KMIP Mappings (Tim H)
    - Associating Attributes to Wrapped Keys (Graham S)
    - DSA text improvements (Dina K, Bob R & Tony C)
    - TLS text improvements (Dina K)
    - CKM_NULL (Dina K)
    - C_LoginUser (Tim H)
    - IPSec Derive (Bob R)
    - Provisioning (Bob R)
    - SP-800-108 - KDF (Darren J)
    - Blockchain (David)
    - Additional ECC Curves (Darren J)
- Call for late arrivals
- Adjourn

Motion to approve Agenda

- Geoffrey H moves, Greg S seconds, no comments, objections or abstentions. Agenda approved.

Motion to approve meeting minutes

- March 1, 2017
- Tim H moves, Darren J seconds, no comments, objections or abstentions. Minutes approved.

Deadlines

- Reminder of May 1 deadline for ballot/motions on items to be included in v3.0

V3.0

Items from PR comments on 2.4 - proposals required

Item 12 – make the doc match the header file (Chris Z)

- No update

Item 20 – might be replaced by work Dina is already doing (Dina K)

- No update

Item 13, 21 – provide proposal for the proposed documentation content for header file items noted (Dina K)

- No update

Items 14, 15, 16, 18, 19 – provide proposal for the proposed documentation content for header file items noted (Bob R)

- No update

Item 17 – provide proposal for the proposed documentation content for header file items noted (Tim H)

- No update

EncryptCancel/DigestCancel/etc (Darren J)

- Geoffrey H - Review on this item opened a discussion on new vs changed APIs - use the init operation to clean up items in this space

- Tim H - asked how this would apply to "Find"
- Geoffrey H - confirmed that in most cases Init would be sufficient
- Tim H - Need a way to clear eveything in a session without the overhead of restarting the session. Most common usage is to kill off everything rather than specific items within a session
- Darren J - My context of usage ius a single item, unsure beyond that but a clean session does have significant value
- Bob R - Agree this would be useful
- All agreed that both approaches should be used - single item & whack eveything
- Updates to the Init functions with a NULL parameter meaning reset and Darren's existing proposal.
- Full review and motion at next meeting.

Additional ECC Curves (Darren J)

- No updates - have received feedback but have not applied it at yet

Testing Profiles (Mark J & Anthony B.)

- No updates

AEAD/AES GCM proposal/Extending Function Table/Forking (Bob R & Tim H)

- Tim completed review
- All 3 documents have been posted
- Only minor feedback received.
- Dieter provided some comments earlier today - contains both some editorial changes and some content changes regarding IVs and Nonce re NIST requirements.
- Dieter asked why the nonce needs to be generated by the token rather than an input token as NIST doesn't require it.
- BobR stated tht this is what NIST had asked for, but not specifically in the case of CCM
- Tim H indicated that we should allow for (but not prescribe) the nonce being generated by the token
- Bob R to update spec/proposal to allow two approaches (pass in nonce from application or generate in token)
- Please get any comments in so we can ballot/motion this on next call

CKM_AES_KEY_WRAP_PAD (Dieter B.)

- Will provie proposal for next meeting

KMIP Mappings (Tim H)

- No update

Associating Attributes to Wrapped Keys (Graham S)

- No update

DSA text improvements (Dina K, Bob R & Tony C)

- Dina to upload change
- BobR to allocate an ID

TLS text improvements (Dina K)

- No update

CKM_NULL (Dina K)

- No Update

C_LoginUser (Tim H)

- No update

IPSec Derive (Bob R)

- No update

Provisioning (Bob R)

- No update

SP-800-108 - KDF (Darren J)

- Initial draft for content review has been posted

Blockchain (David)

- Still working on content

New item - call numbers

- BobR has additional information form local numbers and a web dial in - Bob will send them around

Call for late arrivals

- 2 arrivals noted

Motion to Adjourn

- Tim H Moves, David seconds, No objections, no comments, no abstentions. Meeting adjourned.

Meeting Adjourned at 13:41 PST