March 01, 2023 Meeting Minutes

Meeting commenced 1:00 PM PDT

- Roll call (Bob) - quorum achieved.
- Greg S taking minutes.

Attendance

- Attendance noted in KAVI

Proposed agenda

- Roll call
- Review / approval of the agenda
- Approve Minutes (February 15, 2023)
- PKCS#11 v3.1
- PKCS#11 v3.2
    - Work Items
    - Action Items
    - Work Items Deferred from 3.1
    - Public Comments Items
- v3.0 Errata
- New Business
- Next Meeting
- Call for late arrivals
- Adjourn

Motion to approve Agenda

- Tim H moved, Jonathan S seconded. No objections, abstentions or comments. Agenda approved.

Motion to approve Minutes (February 15, 2023)

- Minutes posted for February 15, 2023
- Jonathan S moved, Hamish C seconded. No objections, abstentions or comments. Minutes approved.

PKCS#11 V3.1

- Logging tickets has commenced for TC Admin.

PKCS#11 V3.2

3.2 Work Items

- Item #1 - Completed.
- Item #2 - Completed.
- Item #3 - No update.
- Item #4 - Completed.
- Item #5 - Completed.
- Item #6 - Discussion on Post-Quantum KEM and RSA mechanism, 3 options for mapping RSA. Rob R asked Michael M to post a definition of the mechanism to list - Use of the RSA-KEM Algorithm in the Cryptographic Message Syntax (CMS) - Bob R will push a proposed update for signatures and an minor update to discuss next meeting.
- Item #7 - Completed.
- Item #8 - Trust Objects Draft 4 was posted by Michael M after last meeting, to be reviewed prior to vote.
- Item #9 - No update.
- Item #10 - Bob R to send NSS details to mailing list.
- Item #11 - No update.

3.2 Action Items

- Action #1 - Closed.
- Action #2 - Closed.
- Action #3 - Closed.
- Action #4 - Closed.
- Action #5 - Closed.
- Action #6 - No Update.
- Action #7 - No Update.
- Action #8 - Dieter - Circulated proposal on C_UnwrapKey before last meeting and this discussed changes to error code, after some discussion Dieter agreed to update the proposal.
- Action #9 - Closed.

Work Items Deferred Items from 3.1

- Item #1 - Closed.
- Item #2 - Closed.

Public Comments Items

- PC Item #1 Hamish has uploaded proposal GCM and CCM iv/nonce token generated for wrapping looking for feedback. Dieter indicated that he has some feedback to send.
- PC Item #2 Closed.
- PC Item #3 No update.

v3.0 Errata

- No update pending V3.1 being completed.

New Business

- Welcome Valerie Fenwick

Next Meeting

- Motion: Next meeting will be March 15, 2023
- Greg S moved, Hamish C seconded. No objections, abstentions or comments. Motion passed.

Call for Late Arrivals

- None

Motion to Adjourn

- Tim H moved, Greg S seconded. No objections, abstentions or comments. Meeting adjourned.

Meeting Adjourned at 1:48 PM PDT