February 15, 2023 Meeting Minutes

Meeting commenced 1:05 PM PST

- 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 1, 2023)
- PKCS#11 v3.1
  - Special Majority Vote
- 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

- Greg S moved, Hamish C seconded. No objections, abstentions or comments. Agenda approved.

Motion to approve Minutes (February 1, 2023)

- Minutes posted for February 1, 2023
- Greg S moved, Michael M seconded. No objections, abstentions or comments. Minutes approved.

PKCS#11 V3.1

- Minutes from last meeting are now approved and Greg S will now lodge tickets for the Special Majority Vote with 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 - Private Mechanism deriving Public Key.
  - Motion: That the version entitled Pub from Priv draft 2 be approved for Version 3.2.
  - Bob R moved, Jerry S seconded. No objections, abstentions or comments. Proposal approved.
- Item #6 - Bob R has now released an additional document Post Quantum Signatures at this point 3 proposals have been sent out to the mailing list recently and some discussions in email are occurring however we are not yet ready for a vote while discussions continue. For reference the previous documents are Add KEM APIs to PKCS#11 and Kem Algorithms.
- Item #7 - Completed.
- Item #8 - Updated draft 3 posted by Michael M. - Discussion on Trust Objects and usage - Michael M indicated he would be sending an updated draft to clarify this discussion.
- Item #9 - No update.
- Item #10 - Bob R to send NSS details to mailing list.

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 just prior to the meeting - Review for next meeting
- Action #9 - Closed.

Work Items Deferred Items from 3.1

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

Public Comments Items

- PC Item #1 Hamish has been working on this and plans to upload an update before next meeting.
- PC Item #2 Closed.
- PC Item #3 No update.

v3.0 Errata

- No update pending V3.1 being completed.

New Business

- V3.2 Darren J mentioned that he has been catching up after an absence from the TC and has sent a number of emails asking questions about some already approved proposals, expecting that there will be some discussions necessary as a result of these emails
- Bob R indicated that he had noted Darren's message that there was a previous proposal on XMSS that seemed to have been dropped, to be added as a work item.

Next Meeting

- Motion: Next meeting will be March 1, 2023
- Greg S moved, Dieter B & Hamish C seconded. No objections, abstentions or comments. Motion passed.

Call for Late Arrivals

- None

Motion to Adjourn

- Dieter B moved, Greg S seconded. No objections, abstentions or comments. Meeting adjourned.

Meeting Adjourned at 1:50 PM PST