March 15, 2023 Meeting Minutes

Meeting commenced 1:00PM PDT

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

Attendance

- Attendance noted in KAVI

Proposed agenda

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

Motion to approve Agenda

- Hamish C moved, Dieter B seconded. No objections, abstentions or comments. Agenda approved.

Motion to approve Minutes (March 1, 2023)

- Minutes posted for March 1, 2023
- Jonathan S moved, Hamish C seconded. No objections, abstentions or comments. Minutes approved.

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 - No update. Bob R. noted that there were comments.
- Item #7 - Completed.
- Item #8 - [Trust Objects Draft 4](#) is available. Please review prior to next meeting.
- Item #9 - No update.
- Item #10 – No update.
- 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 B moved to have the v2 of the proposal [C_Unwrap-CKA_VALUE_LEN-V2.docx](#) be adopted. Jonathan S seconded. No objections, abstentions, or comments noted. Proposal approved.
- Action #9 - Closed.

Work Items Deferred Items from 3.1

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

Public Comments Items

- PC Item #1 Dieter's feedback on the mailing list was discussed. New function names: C_WrapKeyAuthenticated and C_UnwrapKeyAuthenticated were well received. Hamish will update the proposal.
- PC Item #2 Closed.
- PC Item #3 Much discussion on C_SetPinUser and C_InitPinUser. Tim H. will update the proposal to:
  - ☐ Change the function names (C_SetPinUsername, C_InitPinUsername);
  - ☐ Add a new function (C_InitTokenUsername);
  - ☐ Add a new function (C_LoginUsername) that duplicates the exiting function (C_LoginUser) so function names are consistent;
  - ☐ Add the user type as a parameter to the functions;
  - ☐ Add a flag indicating that the token supports usernames; and

☐ Add a new return code for the case where the username is unknown to the token.

New Business

- Bob R. states that we can't use Bluejeans after April 1, 2023 and offered either Zoom or Google Meet. Next meeting will use Bluejeans. In the meantime, Bob R will create a test meeting in Zoom and a test meeting in Google Meet so that members can determine which service works for them. A decision on which to use will be made at the next meeting.

Next Meeting

- Motion: Next meeting will be March 29.
- Tim H moved, Mike M seconded. No objections, abstentions, or comments. Motion passed.

Call for Late Arrivals

- Valerie F, Mike M added.

Motion to Adjourn

- Tim H moved. Hamish C seconded. No objections, abstentions, or comments. Meeting adjourned.
- Meeting Adjourned at 1:45 PM PDT