February 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 (January 18, 2023)
- PKCS#11 v3.1
    - Statements of Use
    - 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, Tony C seconded. No objections, abstentions or comments. Agenda approved.

Motion to approve Minutes (January 18, 2023)

- Minutes posted for January 18, 2023
- Greg S moved, Hamish C seconded. No objections, abstentions or comments. Minutes approved.

PKCS#11 V3.1

Motion for Statements of Use

- That the TC members approve and accept the Statements of Use received and posted to the TC document register and mailing list on behalf of Utimaco dated 20-January-2023 https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/70709/PKCS11v3.1-SOU-Utimaco-Jan2023.pdf, Information Security Corporation on 20-January-2023 https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/70708/ISC PKCS 11 v3.1 Statement of Use v103.pdf and Cryptsoft on 31-January-2023 https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/70712/PKCS11v3.1-SOU-Cryptsoft-31-Jan-2023.pdf as acceptable Statements of Use with respect to the PKCS #11 Profiles Version 3.1, Committee Specification 01, approved 14 July 2022 and PKCS #11 Specification Version 3.1, Committee Specification 01, approved 11 August 2022.
- Greg S moved, Tony C seconded. No objections, abstentions or comments. Motion passed.

Motion for Special Majority Vote for Profiles

- That the OASIS PKCS11 TC submit PKCS #11 Profiles V3.1 CS01 at https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/70194/pkcs11-profiles-v3.1-cs01.html as a Candidate OASIS Standard and direct the Chairs to take any necessary steps to carry out that submission pursuant to the OASIS TC Process 3.4.1, with a public review not exceeding the process requirements (presently 60 days).
- Greg S moved, Tony C seconded. No objections, abstentions or comments. Motion passed.

Motion for Special Majority Vote for Specification

- That the OASIS PKCS11 TC submit PKCS #11 Specification V3.1 CS01 at https://www.oasis-open.org/apps/org/workgroup/pkcs11/download.php/70262/pkcs11-spec-v3.1-cs01.html as a Candidate OASIS Standard and direct the Chairs to take any necessary steps to carry out that submission pursuant to the OASIS TC Process 3.4.1, with a public review not exceeding the process requirements (presently 60 days).
- Greg S moved, Tony C seconded. No objections, abstentions or comments. Motion passed.

PKCS#11 V3.2

3.2 Work Items

- Item #1 - Completed.
- Item #2 - Completed.
- Item #3 - No update.
- Item #4 - Completed.
- Item #5 - Bob R released updated version of proposal Pub from Priv Draft 2 - Hamish C to take up names with Bob R goal to vote on this for next meeting.
- Item #6 - Added 2 proposals documents to repo - 1 updated existing spec and then second for new algorithms. Kem Algorithms and Add KEM APIs to PKCS #11 For review and discussion at next meeting.
- Item #7 - Completed.
- Item #8 - Bob R has updated proposal in repo Trust Objects draft 2 - goal to vote on that proposal next meeting.
- Item #9 - 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 - Waiting for Dieter
- Action #9 - Jonathan suggested there was no current work being done on this, confirmed by Bob R - Close Item

Work Items Deferred Items from 3.1

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

Public Comments Items

- PC Item #1 No Update.
- PC Item #2 Closed.
- PC Item #3 No update.

v3.0 Errata

- No update pending V3.1 being completed.

New Business

- Jonathan S - Sent a question about TLS 1.2 Extended Master Secret to the mail list - New mechanism to 3.2 - Proposal required - Action Item on Bob to show how NSS did this. Greg S to add as a Work Item

Next Meeting

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

Call for Late Arrivals

- Tim H, Jerry S

Motion to Adjourn

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

Meeting Adjourned at 1:38 PM PDT