

January 04, 2023 Meeting Minutes

Meeting commenced 1:01 PM PDT

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

Attendance

- Attendance noted in KAVI

Proposed agenda

- Roll call
- Approve Minutes (December 07, 2022)
- PKCS#11 v3.1
 - Statement of Use
- 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, Dieter B seconded. No objections, abstentions or comments. Agenda approved.

Motion to approve Minutes (December 07, 2022)

- Minutes posted for 🌐 December 07, 2022
- Greg S moved, Hamish C seconded. No objections, abstentions or comments. Minutes approved.

PKCS#11 V3.1

- Statements of Use (minimum of 3 required)
- Utimaco, ISC and Cryptsoft ones are prepared
- Motion to accept last meeting (December 07, 2022), Need today's minutes approved

for next step.

PKCS#11 V3.2

3.2 Work Items

- Item #1 - Completed
- Item #2 - Completed.
- Item #3 - No update.
- Item #4 - Completed.
- Item #5 - No update.
- Item #6 - No update.
- Item #7 - Completed.
- Item #8 - No update.
- Item #9 - No Update.

3.2 Action Items

- Action #1 - Closed.
- Action #2 - Closed.
- Action #3 - Closed.
- Action #4 - Closed.
- Action #5 - Closed.

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.
- PC Item #4 No update.

v3.0 Errata

- No update pending V3.1 being completed.

New Business

- Message from Jonathan S -  email message December 15, 2022 interoperability issue using OAEP (optimal Asymmetric Encryption Padding for RSA)
 - Discussion around Source type should be one of the specifiers even if the parameter is empty.
 - Greg S to add item to Wiki referencing email and minutes so that editors can check back to see if this can be made clearer.

Next Meeting

- Motion: Next meeting will be January 18, 2023
- Greg S moved, Tony 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 1:18 PM PDT