IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PQC SG 07 April 2025 Teleconference Meeting Minutes | | | | |
| Date: 2025-04-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Alex Lungu | SAMSUNG | OCS, CB4 0AE, U.K. | +44 1223 434600 | da.lungu@samsung.com |

Abstract

This document containes the minutes for the PQC SG teleconference that took place on the 7th of April 2025.

# 

1. The Chair, Stephen Orr (Cisco), calls the meeting to order at 13:02 ET.
2. Chair provides reminders:
   1. Please record your attendance during the session by using the IMAT system.
   2. No recordings are allowed.
   3. Please use the mute function unless addressing the group.
   4. Please announce your affiliation when you first address the group during a meeting slot.
3. Policy and procedures

Chair informs that participants have a duty to inform the IEEE of each holder of any potential Essential Patent Claims of which they are personally aware if the claims are owned or controlled by the participant or the entity the participant is from, employed by, or otherwise represents.

Participants should also inform the IEEE (or cause the IEEE to be informed) of the identity of any other holders of potential Essential Patent Claims.

**Nobody speaks up.**

1. Chair presents:
   1. Patent-related information.
   2. IEEE SA Copyright Policy. Chair requests the secretary to ensure the presentation of the **Copyright Policy** is minuted.
   3. Other guidelines for IEEE WG meetings.
   4. Participant behavior in IEEE-SA activities is guided by the IEEE Codes of Ethics & Conduct
   5. Participants in the IEEE-SA “individual process” shall act independently of others, including employers.
   6. IEEE-SA standards activities shall allow the fair & equitable consideration of all viewpoints.
2. For documentation the “PQC SG” repository in <http://mentor.ieee.org> shall be used for submissions.
3. Meeting minutes for the previous meeting can be found at [11-25/0572r0](https://mentor.ieee.org/802.11/dcn/25/11-25-0572-00-0PQC-pqc-sg-27-march-2025-teleconference-meeting-minutes.docx).
   1. Meeting minutes approved with unanimous consent.
4. Agenda for the meeting can be found at [11-25/0596r1](https://mentor.ieee.org/802.11/dcn/25/11-25-0596-01-0PQC-pqc-sg-agenda-04-07-2025.pptx).
   1. Agenda approved with unanimous consent.
5. Meeting plan
   1. Question on finding a timeslot which is better suited for Asia contributors.
      1. Chair has attempted to find an ET morning slot amongst other standards meeting, and has also reached out to at least one contributor in an attempt to accommodate all stakeholders.
   2. Question on changing the timeslot for the 21st of April meeting to 09:30AM ET.
      1. No objections.
6. PQC Draft proposed PAR - [11-25/0597r0](https://mentor.ieee.org/802.11/dcn/25/11-25-0597-00-0PQC-pqc-draft-proposed-par.docx)
   1. Document was moved to the PQC SG repository.
   2. Changes done to incorporate feedback provided before the meeting were presented.
   3. Question on maintaining consistency in section 5.2.b: PQC-enabled vs just PQC.
      1. Consistency was lost after feedback was incorporated. Wording can be updated to maintain consistency.
   4. Question on discussing more than the US requirements in section 5.5, such as various market verticals (e.g. financial applications).
      1. Another contributor asked to for UK’s NCSC requirements to be added to the CSD, somewhat contradictory to the question at hand.
      2. The US example is deemed to be relevant, and adds color.
   5. Suggestion to remove “PQC-enabled” wording from section 5.2.b, as it is undefined.
      1. Author will review the suggestion after the meeting.
      2. Suggestion was relayed on chat as well:
         1. provides authentication and key management (AKM) suites for PQC\*\*\*delete -enabled protocols\*\*\*,
         2. specifies \*\*\*delete the use of PQC\*\*\* digital signature and key establishment algorithms \*\*\*add that use PQC\*\*\*,
         3. defines a \*\*\*delete PQC-enabled\*\*\* password authenticated key exchange \*\*\*add that uses PQC\*\*\*, and
         4. considers modifications to symmetric key handshake protocols \*\*\*delete to support\*\*\*\*\*\*add for\*\*\* PQC.
   6. Comment on section 5.5, emphasis should be put on the global reach. Specific examples could be moved to section 8.1.
      1. Author to consider the suggestion off-line.
   7. Question on section 5.2.b: the “provides / specifies / defines” verbs should be aligned and put above of the list.
      1. Author agrees.
   8. Question on section 5.2.b point d), why is “considers” used? If the group decides to no less than discussed in the PAR, that is not a problem. The PAR would still be met, as the group has not over-extended. Suggestion is to remove “considers”.
      1. There are no objections.
      2. If there are no issues with doing less then the PAR, then that should not be a problem.
   9. Comment on section 5.2.b point c), PQ PAKE have a name and it should probably be used: post-quantum password-authenticated key exchange.
   10. Comment on section 5.2.b, point “e) considers addition of quantum resistant cipher suites and integrity protocols” should be added, especially in light of the fact that there is no penalty if all points in the PAR are met.
   11. Comment on section 8.1, the NIST document which lists the 2035 target should probably be included.
       1. Author requested the 3 comments above to be sent in an e-mail.
   12. Comment on not having the PAR too narrow, or too US-centric. ETSI has published also its own standards: <https://www.etsi.org/deliver/etsi_ts/104000_104099/104015/01.01.01_60/ts_104015v010101p.pdf>.
       1. Chair asked for specific reference documents to be sent directly, so they can be added to the agenda slides.
   13. Comment on being able to not meet all the PAR’s scope – given the new information the suggestions minuted in points f), g), i) above should be progressed.
   14. Questions on removing the uncertanty from section 5.2.b point d), is there a possibility that the groups would <have> to perform the change listed in this point?
       1. The group would like to ensure the uncertainty regarding point “d) modifications to symmetric key handshake protocolsing to support PQC-enabled protocols.” is noted. It is unclear if changes for symmetric key exchanges are required. Similar for the new point e), the addition of quantum resistant cipher suites and integrity protocols.
       2. There is also no expectation that an entity would ensure the entire PAR was met.
   15. Comment on the PAR being owned by the group and the goal is to make visible what points are considered.
   16. Comment on the CSD being possibly the place to store the uncertainty regarding the points in section 5.2.b point d).
   17. Comment on possibly modifying the PAR, section 8.1, to note the uncertainty noted above.
   18. Question on feasibility of SA ballot in November 2026.
       1. Dates have largely been derived from the CNSA 2.0 timeline.
       2. An answer will be provided after off-line consideration.
   19. Comment on having the 2027 deadline from NSA in CNSA 2.0 in the PAR as a reminder for the aggressive schedule.
7. PQC Draft Proposed CSD - [11-25/0598r0](https://mentor.ieee.org/802.11/dcn/25/11-25-0598-00-0PQC-pqc-draft-proposed-csd.docx)
   1. Document was moved to the PQC SG repository.
   2. Changes done to incorporate feedback provided before the meeting were presented.
   3. Question on “Cryptographically relevant post quantum computers” – is this intentional?
      1. Document was modified to note “Cryptographically-relevant quantum computers”.
   4. Comment on superfluous “with some probability” and missing “cryptography”.
      1. Document was updated.
8. Next meeting will be on the 21st of April at 09:30AM ET, via teleconference. Scheduled for 2 hours.
9. Chair issues a re-reminder to fill in attendance.
10. Adjourned at 14:09 ET.