IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PQC SG May 2025 Interim Meeting Minutes | | | | |
| Date: 2025-05-23 | | | | |
| 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 contains the minutes for the PQC SG hybrid meeting that took place during the 2025 May Interim in Warsaw.

# 

1. The Chair, Stephen Orr (Cisco), calls the meeting to order on 2025-05-13 at 10:31 CEST.
2. Chair presents registration requirements for the interim session.
3. Chair provides reminders:
   1. Please record your attendance during the session by using the IMAT system.
   2. No recordings are allowed.
   3. Webex etiquette for hybrid meetings.
   4. Please announce your affiliation when you first address the group during a meeting slot.
4. 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. Patent-related information, including a link to patent policy is also presented.

**Nobody speaks up.**

1. Chair presents:
   1. Other guidelines for IEEE WG meetings.
   2. Participants in the IEEE-SA “individual process” shall act independently of others, including employers.
   3. IEEE-SA standards activities shall allow the fair & equitable consideration of all viewpoints.
   4. IEEE SA Policy and Rules Documents
   5. IEEE SA Copyright Policy. Chair requests the secretary to ensure the presentation of the **Copyright Policy** is minuted.
2. For documentation the “PQC SG” repository in <http://mentor.ieee.org> shall be used for submissions.
3. Agenda for the meeting can be found at [11-25/0861r3](https://mentor.ieee.org/802.11/dcn/25/11-25-0861-03-0PQC-pqcsg-may-2025-meeting-agenda.pptx).
   1. Question on presenting a technical contribution, <https://mentor.ieee.org/802.11/dcn/25/11-25-0722-00-0PQC-ml-kem-in-802-11.pptx>, before running the PAR motion.
      1. The group agreed to discuss the SP in the proposal before running the motion.
   2. Question on having technical contributions listed after motions, and not Thursday.
      1. The group agrees.
   3. Agenda approved by unanimous consent.
4. Meeting minutes for the previous meeting can be found at [11-25/0719r0](https://mentor.ieee.org/802.11/dcn/25/11-25-0719-00-0PQC-pqc-sg-21-april-2025-teleconference-meeting-minutes.docx).
   1. Meeting minutes approved with unanimous consent.
5. PQC draft proposed PAR - [11-25/0597r5](https://mentor.ieee.org/802.11/dcn/25/11-25-0597-05-0PQC-pqc-draft-proposed-par.docx)
   1. The content was presented. Minor editorial updates were brought since the last meeting.
   2. Question on the timeline of the PAR’s progression.
      1. Best line of action is to have the PAR posted a month before the plenary on the LMSC reflector. Afterwards during the plenary starting on the 27th of July, most likely Tuesday evening, we will have some feedback, and we can aim for approval on Friday. This chain of actions should allow to have the TG formed in September.
   3. Question on section 5.2.b, point e). Why is this used? Does not GCMP-256 suffice? There is a concern that this has HW impact.
   4. Question on section 5.2.b, point e), how about removing the “cipher suite” part?
   5. Question on adding “no hardware changes” to section 5.2.b, point e).
   6. Group has reached consensus to remove point e) from section 5.2.b. The point was removed.
   7. Proposal from the SP in 11-25/0722r0 to add “This amendment shall be backward compatible with legacy IEEE 802.11 devices (e.g. the encryption key of ML-KEM shall not be added into Beacon frame).” to the PAR.
      1. Comment on how PQC cannot break 802.11 compatibility. Maybe a hash of said key should be added, not an entire key.
      2. Comment to possibly add "The extensions shall not prevent deployed IEEE 802.11 STAs to connect to the same BSS." although unnecessary as the only way to add this is to only allow backwards compatible solutions.
      3. Consensus to not add any text was reached.
6. PQC draft proposed CSD - [11-25/0598r3](https://mentor.ieee.org/802.11/dcn/25/11-25-0598-03-0PQC-pqc-draft-proposed-csd.docx)
   1. The content was presented.
7. **Motion** - Believing that the PAR contained in the document referenced below meets IEEE-SA guidelines, Request that the PAR contained in 11-25-0597r5 be posted to the IEEE 802 LMSC agenda for LMSC approval to submit to NesCom, granting the WG chair editorial license.
   1. Yes: 54
   2. No: 0
   3. Abstain: 1
8. **Motion** - Believing that the CSD contained in the document referenced below meets IEEE-SA guidelines, Request that the PAR contained in 11-25-0598r3 be posted to the IEEE 802 LMSC agenda for LMSC approval, granting the WG chair editorial license.
   1. Yes: 44
   2. No: 0
   3. Abstain: 2
9. ML-KEM in 802.11 - [11-25/0722r0](https://mentor.ieee.org/802.11/dcn/25/11-25-0722-00-0PQC-ml-kem-in-802-11.pptx)
   1. Question on OWE not requiring a 4-way handshake to derive the PMK.
   2. Question on ML-KEM requiring a 2-way handshake, not a 3-way handshake.
      1. A key confirmation step was seen as essential and included in the count.
   3. Question on the need to use Probe Request/ Response frames to perform authentication.
   4. Question on surveying other KEMs, not only ML-KEM?
      1. Other KEMs have not been surveyed.
   5. Question on a potential misunderstanding of the quoted intention to include all encapsulation keys/ hash of key.
   6. Question on potential risks brought by adding keys to Probe Response frames.
   7. Question on looking at EAP cases at well. Reuse 11bi solution for authentication?
10. a-pqc-pake - [11-25/0770r1](https://mentor.ieee.org/802.11/dcn/25/11-25-0770-01-0PQC-a-pqc-pake.pptx)
    1. Question on NoIC having a quantum security proof, as the referenced paper has in section 2: “Although the constructions in these works are less efficient than the ones discussed in this paper, they come with a proof that considers quantum adversaries: the former in the standard model and the latter in the QROM”.
    2. Question on crypto-agility brought by generic PAKE-over-KEM mechanisms.
    3. Question: Are all frames involved in the exchange authentication frames?
       1. Yes.
    4. Question: Is there an out of band step in the proposed exchange?
       1. Yes, there is one.
    5. Comment: we can fragment MMPDUs, and still use authentication frames.
    6. Comment on the need to notify other groups if we go down the route of MMPDU fragmentation, as this may have an impact on them.
    7. Question on wether the intent is replace SAE, not extend it?
       1. Yes, the intent is to replace SAE.
    8. Comment on the need to work with 11bi to avoid duplication of effort.
11. Further presentations/ discussions?
    1. Nobody speaks up.
12. Recessed at 11:21.
13. Midweek plenary
    1. PAR and CSD are likely to suffer minor editorial changes, mostly going from “802.11” to “IEEE Std. 802.11”.
    2. During the mid-week plenary, the PAR & CSD were approved by the WG.
       1. PAR votes Yes: 150, No: 0, Abstain: 7
       2. CSD votes Yes: 140, No: 0, Abstain: 8
    3. Adjourned during the mid-week plenary, on 2025-05-14 at 13:52.
14. Next meeting will be a teleconference to be scheduled in June.
15. For the July plenary three slots are expected to respond to PAR comments.