IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PQC SG July 2025 Plenary Meeting Minutes | | | | |
| Date: 2025-08-21 | | | | |
| 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 July Plenary in Madrid.

# 

1. The Chair, Stephen Orr (Cisco), calls the meeting to order on 2025-07-29 at 19:33 CEST.
2. Chair presents registration requirements for the plenary session.
3. Chair provides reminders:
   1. Please record your attendance during the session by using the IMAT system.
   2. Webex etiquette for hybrid meetings.
   3. No recordings are allowed.
   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. IEEE SA Copyright Policy. Chair requests the secretary to ensure the presentation of the **Copyright Policy** is minuted.
   2. Other guidelines for IEEE WG meetings.
   3. Participant behavior in IEEE-SA activities is guided by the IEEE Codes of Ethics & Conduct.
   4. Participants in the IEEE-SA “individual process” shall act independently of others, including employers.
   5. IEEE-SA standards activities shall allow the fair & equitable consideration of all viewpoints.
2. For documentation, the “PQC SG” repository in <https://mentor.ieee.org/802.11/documents> shall be used for submissions.
   1. There is a PQC SG status page at <https://www.ieee802.org/11/Reports/pqc_update.htm>.
3. Minutes of May Interim, <https://mentor.ieee.org/802.11/dcn/25/11-25-0987-00-0PQC-pqc-sg-may-2025-interim-meeting-minutes.docx>, were approved by unanimous consent.
4. Agenda for the meeting, <https://mentor.ieee.org/802.11/dcn/25/11-25-1063-02-0PQC-pqc-sg-july-2025-plenary.pptx>, was approved by unanimous consent.
5. The SG was informed that there is a PQC session session scheduled in 802.1
   1. 802.1ar is their amendment
6. The process to progress the PAR and CSD was presented.
   1. The SG received 3 sets of comments:
      1. From 802.19 under <https://mentor.ieee.org/802.19/dcn/25/19-25-0042-00-0000-802-11bt-par-csd-comments.docx>.
      2. From 802.1 under <https://www.ieee802.org/1/files/public/docs2025/admin-PAR-CSD-comments-11bt-0725-v02.pdf>.
      3. From 802.15 under <https://mentor.ieee.org/802.15/dcn/25/15-25-0362-00-0mag-802-15-comments-on-pars-july-2025.pptx>
   2. Replies to these comments need to be agreed, and, should changes arise, the SG may need to approve a new PAR and a new CSD.
   3. Assuming all deadlines are met, TG may start in September.
7. Proposed responses to PAR and CSD comments - <https://mentor.ieee.org/802.11/dcn/25/11-25-1378-01-0PQC-proposed-responses-to-par-and-csd-comments.pptx>
   1. Discussions on comments from 802.1. The SG agreed to:
      1. Keep “Enhancement” in the PAR title.
      2. Keep post-quantum in PAR section 5.5.
      3. Update References.
      4. Update the CSD template.
      5. Align the CSD document title and abstract with the PAR.
      6. Keep the CRQC term in the CSD.
      7. Update the “firmware” reference in the CSD.
      8. Change the “Market verticals” sentence in the PAR.
   2. Discussions on comments from 802.15:
      1. The group agreed drafted PAR responses without discussions.
      2. The group discussed and agreed CSD reply wording.
   3. Discussions on comments from 802.19:
      1. Agreement on all PAR suggestions
      2. Discussions on the version of the referenced document.
   4. Discussions on formatting the answers for the respective groups.
8. **MOTION** to approve document 11-25/1378r2 as comment response to 802 WGs comments
   1. No discussions on the motion.
   2. Move: Jon Rosdahl
   3. Second: Jouni Malinen
   4. Approved by unanimous consent
      1. Y: 49
      2. N: 0
      3. A: 0
9. Recessed at 20:52 CEST.
10. The Chair, Stephen Orr (Cisco), calls the meeting to order on 2025-07-30 at 09:00 CEST.
11. Chair presents registration requirements for the plenary session.
12. Chair provides reminders:
    1. Please record your attendance during the session by using the IMAT system.
    2. Webex etiquette for hybrid meetings.
    3. No recordings are allowed.
    4. Please announce your affiliation when you first address the group during a meeting slot.
13. 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. IEEE SA Copyright Policy. Chair requests the secretary to ensure the presentation of the **Copyright Policy** is minuted.
   2. Other guidelines for IEEE WG meetings.
   3. Participant behavior in IEEE-SA activities is guided by the IEEE Codes of Ethics & Conduct.
   4. Participants in the IEEE-SA “individual process” shall act independently of others, including employers.
   5. IEEE-SA standards activities shall allow the fair & equitable consideration of all viewpoints.
2. For documentation, the “PQC SG” repository in <https://mentor.ieee.org/802.11/documents> shall be used for submissions.
   1. There is a PQC SG status page at <https://www.ieee802.org/11/Reports/pqc_update.htm>.
3. Agenda for the meeting, <https://mentor.ieee.org/802.11/dcn/25/11-25-1063-05-0PQC-pqc-sg-july-2025-plenary.pptx>, was approved by unanimous consent.
   1. The main goal is to approve changes to the PAR and CSD.
   2. No questions were raised on the path forward.
4. Proposed PAR : IEEE 802.11 Enhancements for Post-Quantum Cryptography - <https://mentor.ieee.org/802.11/dcn/25/11-25-1376-02-0PQC-draft-updates-to-pqc-par.docx>
   1. Discussion on the title. Other PARs have inconsistent titles, some include “Enhancements”, some include “IEEE 802.11”.
   2. Question on the implication of the PAR title on the amendment title.
      1. Title of the PAR document does not influence the title of the amendment, which is in section 2.1 of the PAR document.
   3. Question on the European Commision addition, as the text changed around “market verticals”, should we specify that these verticals are “beyond government use”.
      1. No disagreements, text was added.
   4. Questions on addition of a space in section 7.1.
      1. No disagreements, space was added.
   5. Question on the referenced documents: are additions needed for the EU recommendation?
      1. No disagrements, reference was added.
   6. Question do we need to add the similar NIST reference.
      1. After discussion, which included the NSA’s CNSA document, the group agrees.
   7. Proposal to remove both NIST and EC references as they are not required by the feedback received.
      1. The group agreed.
5. A CSD Proposal: IEEE 802.11 Enhancements for Post-Quantum Cryptography (PQC) - <https://mentor.ieee.org/802.11/dcn/25/11-25-1377-02-0PQC-draft-updates-to-pqc-csd.docx>
   1. Question on the relevance of mentioning “In Europe”, when a European country was already mentioned.
      1. No disagrements, text was changed.
   2. Question on modifying text which has not been commented.
      1. The group has agreed that text without comments should not be changed.
6. Discussions on how the PAR and CSD documents should be uploaded.
   1. Both the red-line and the clean version should be uploaded.
7. Group enters stand-at-ease for a few minutes until the documents get updated.
8. **MOTION -** Believing that the PAR contained in the document referenced below meets IEEE-SA guidelines, Request that the PAR contained in 11-25/1376r3 be posted to the IEEE 802 LMSC agenda for LMSC approval to submit to NesCom, granting the WG chair editorial license.
   1. Move: Alex Lungu
   2. Second: Stephen McCann
   3. Y: 37
   4. N: 0
   5. A: 0
   6. Motion passed
9. **MOTION -** Believing that the CSD contained in the document referenced below meets IEEE-SA guidelines, Request that the CSD contained in 11-25/1377r4 be posted to the IEEE 802 LMSC agenda for LMSC approval, granting the WG chair editorial license.
   1. Move: Mark Hamilton
   2. Second: Anuj Dharap
   3. Y: 35
   4. N: 0
   5. A: 0
10. Overview of PQC Exchanges - <https://mentor.ieee.org/802.11/dcn/25/11-25-1313-01-0PQC-pqc-protocol-overview.pptx>
    1. The content was presented.
    2. Comment on 11bi’s timeline being too late to change for PQC. It would be great to align 11bi to PQC, but unlikely.
    3. A couple of comments on the PFS threat in the no-signature exchange being of little concern.
    4. Discussion on TLS already being a SIGMA protocol.
    5. Comment on some regulators preferring pure PQC exchanges, while others are leaning towards hybrid exchanges. Solutions may be needed for both markets.
    6. Comment on how an alignment with 11bi to have the same transcript would be ideal.
11. PQC Protocol Definitions - <https://mentor.ieee.org/802.11/dcn/25/11-25-1108-02-0PQC-pqc-protocol-definitions.docx>
    1. Question on APs advertising supported parameter sets, or having a procedure for non-AP STAs to downgrade used parameter set if unsupported by the AP.
       1. Solutions are needed.
    2. Question on checking input parameters as required by FIPS 203.
       1. Probably redundant, but can be noted.
    3. Discussion on using Authentication frames instead of GAS.
    4. Discussion on allowing the PAKE exchange to not have PWIDs.
    5. Question on using GAS frame to perform a PQC exchange – have probe requests/ responses been considered?
       1. Could use a probe request/ response exchange, but these are usually used for discovery.
       2. GAS frames are used to get different information from the AP.
       3. GAS frames also support fragmentation, while probe frames do not.
12. Recessed at 11:00 CEST.
13. During the WG mid-week plenary the following PQC SG relevant motions were run:
    1. Believing that the PAR contained in the document referenced below meets IEEE-SA guidelines, request that the PAR contained in https://mentor.ieee.org/802.11/dcn/25/11-25-1376-03-0PQC-draft-updates-to-pqc-par.docx be posted to the IEEE 802 LMSC agenda for WG 802 preview and 802 LMSC approval to submit to NesCom.
       1. Moved by Stephen Orr on behalf of PQC SG, Second: Tuncer Baykas
       2. Result: Yes: 109, No: 1, Abstain: 13 (Motion passes)
       3. [PQC SG result: Moved: Alex Lungu, 2nd: Stephen McCann, Result: 37/0/0]
    2. Believing that the CSD contained in the document referenced below meets IEEE-SA guidelines,

request that the CSD contained in https://mentor.ieee.org/802.11/dcn/25/11-25-1377-04-0PQC-draft-updates-to-pqc-csd.docx be posted to the IEEE 802 LMSC agenda for WG 802 preview and LMSC approval.

* + 1. Moved by Stephen Orr on behalf of PQC SG, Second: Mark Hamilton
    2. Result: Yes: 104, No: 0, Abstain: 11 (Motion passes)
    3. [PQC SG result: Moved: Mark Hamilton, 2nd: Anuj Dharap, Result: 35/0/0]

1. The Chair, Stephen Orr (Cisco), calls the meeting to order on 2025-07-31 at 11:30 CEST.
2. Chair presents registration requirements for the plenary session.
3. Chair provides reminders:
   1. Please record your attendance during the session by using the IMAT system.
   2. Webex etiquette for hybrid meetings.
   3. No recordings are allowed.
   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. IEEE SA Copyright Policy. Chair requests the secretary to ensure the presentation of the **Copyright Policy** is minuted.
   2. Other guidelines for IEEE WG meetings.
   3. Participant behavior in IEEE-SA activities is guided by the IEEE Codes of Ethics & Conduct.
   4. Participants in the IEEE-SA “individual process” shall act independently of others, including employers.
   5. IEEE-SA standards activities shall allow the fair & equitable consideration of all viewpoints.
2. For documentation, the “PQC SG” repository in <https://mentor.ieee.org/802.11/documents> shall be used for submissions.
   1. There is a PQC SG status page at <https://www.ieee802.org/11/Reports/pqc_update.htm>.
3. Agenda for the meeting, <https://mentor.ieee.org/802.11/dcn/25/11-25-1063-08-0PQC-pqc-sg-july-2025-plenary.pptx>, was approved by unanimous consent.
4. Timeline was presented by the Chair:
   1. July 30th: PAR and CSD approved by 802.11 WG
   2. August 1st: LMSC review/approval
   3. Week of September 8th: NesCom/SASB review/approval
   4. PQC SG will be notified at the September Interim Session
5. Comment that Chair should already consider how many slots the SG/ TG should have during the September Interim.
   1. 2 slots were already reserved, more would be considered if needed.
   2. No other teleconferences are scheduled until Sept, no objections were raised by the SG.
6. Using proof of work techniques to protect against active attacks - <https://mentor.ieee.org/802.11/dcn/25/11-25-1296-01-0PQC-using-proof-of-work-techniques-to-protect-against-active-attacks.pptx>
   1. Author presented the contribution.
   2. Question on the balance of effort – how to balance the requirements of low-powered devices and the threat of large attackers.
      1. There is probably no perfect balance, nor a perfect solution. A dynamic amount of work will help here, but large-level malicious actors may still find the amount of work tractable.
   3. Questions on introducing new states for an AP to store proof-of-work (PoW) status.
      1. This is unlikely to be the case, but more study is needed.
   4. Question on the details of broadcasting the PoW puzzle.
      1. Hashcash scheme used for email servers was discussed.
   5. Straw poll “A proof-of-work mechanism should be considered”
      1. 67% Yes
      2. 3% No
      3. 30% Abstain
7. Post-Quantum Opportunistic Wireless Encryption specification – <https://mentor.ieee.org/802.11/dcn/25/11-25-1297-01-0PQC-post-quantum-opportunistic-wireless-encryption-specification.docx>
   1. Author presented the contribution.
   2. Discussion on tripling the number of AKM suite selectorss to convey KEM parameter sets. Considering other PQC AKMs, other than OWE, a different solution would probably be needed.
   3. Question on the KEM decaps failure rate note – is the note needed?
      1. Just for accuracy.
   4. Based on <https://eprint.iacr.org/2023/1933>, shouldn’t a KDF that binds the encapsulation key and ciphertext with the shared secred be used?
      1. Author will study the paper.
8. ML-KEM in PASN - <https://mentor.ieee.org/802.11/dcn/25/11-25-1302-01-0PQC-ml-kem-in-pasn.pptx>
   1. Author presented the contribution
9. ML-KEM in PASN PDT - <https://mentor.ieee.org/802.11/dcn/25/11-25-1303-01-0PQC-ml-kem-in-pasn-pdt.docx>
   1. Author presented the contribution
   2. Comment with similar feedback as for the OWE specification above, the KDF could have "…BSSID | pk | ct | PQCss)" to establish the proper binding properties.
   3. Question on the PASN Parameters Element – as the element is not fragmentable, can it be reused for PQC Public Key/ Ciphertext – given the size of ML-KEM encapsulation key and ciphertext?
      1. This issue needs more attention.
10. Adjourned on 2025-07-31 at 12:40 CEST.