IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PQC SG 27 March 2025 Teleconference Meeting Minutes | | | | |
| Date: 2025-04-01 | | | | |
| 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 27th of March 2025.

# 

1. The Chair, Stephen Orr (Cisco), calls the meeting to order at 12:02 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. Other guidelines for IEEE WG meetings, Patent-related information.
   2. IEEE SA Copyright Policy. Chair requests the secretary to ensure the presentation of the **Copyright Policy** is minuted.
   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 <http://mentor.ieee.org> shall be used, the repository “PQC SG” was created for submissions.
3. Agenda for the meeting, which in this instance only will be limited to 1 hour and thus shorter than usual, can be found at [11-25-0510r02](https://mentor.ieee.org/802.11/dcn/25/11-25-0510r02-0PQC-pqc-sg-agenda-03-27-2025.pptx).
   1. Agenda approved with unanimous consent.
4. Vice Chair appointment: Mark Hamilton (Ruckus/ CommScope), Secretary appointment: Alex Lungu (Samsung)
   1. Question on the need for an editor.
      1. There is no need for an editor at this point.
   2. First author of [11-25-0462r02](https://mentor.ieee.org/802.11/dcn/25/11-25-0462-02-0000-post-quantum-crypto-project.pptx) notes that there is not much process on appointing the VC and Secretary of a SG, but he is disappointed that he initiated the work to form a SG and he was not considered or contacted to be in a leadership position of this group.
   3. Question on the need to be an 802.11 voting member to be a Secretary
      1. Chair noted he will check the need to have voting rights. Unless there are any updates, Secretary will proceed.
5. PQC SG Background and Kickoff
   1. There were 2 presentations delivered during the 11th of March Plenary WNG session – authors stated nothing material changed, hence there is no reason to re-deliver. Members can review the existing material.
   2. Three presentation were delivered during the mid-week plenary
   3. This work lead to the motion to form the SG.
   4. Scope of the SG: Post-Quantum Cryptography (PQC) Study Group: Enhance 802.11 WLAN security with post-quantum cryptography
   5. Output of the SG: Complete a PAR and CSD at or before the May 2025 Interim session
   6. Timeline allows for March – April to review contributions, PAR and CSD. In May the aim is to approve the PAR & CSD, and, if possible, have technical discussions and preparation for TG formation.
6. Teleconference plan: Chair put in a fair amount of effort to set up a meeting that would allow wide participation. Mondays look the best at the moment.
   1. There was a question regarding a golden timeslot, as the currently proposed 1PM ET slot is not friendly for Asia. Asking for 9AM ET.
      1. Chair will look into finding a friendlier slot for 21st of April. The meeting on the 7th of April will stay scheduled 1PM – 3PM.
7. Project Authorization Request - PAR
   1. Scope of the project – section 5.2.b was rephrased before the meeting as a list comprised out of 4 bullet points.
   2. Question on the last bullet point of section 5.2.b – modifications to symmetric key handshaking: are these modifications absolutely required?
      1. The text was amended to add “as needed” to avoid later misunderstandings.
   3. Question on the PAR’s scope being wide enough to allow modifications of the digests’ size for secure hashing algorithms.
      1. The conclusion was that the scope is wide enough.
   4. Question on the last bullet point of section 5.2.b: who requires this update?
      1. There is no clear answer to this question, hence why the text was amended to say “as needed”.
   5. Question on existing protocols using digital signatures in the SG’s scope.
      1. FILS uses digital signatures.
   6. Question on symmetric key cryptography being public key cryptography or not.
      1. Public key cryptography is handled by subpoint b) of section 5.2.b of the PAR. Subpoint d) of the same section handles symmetric key cryptography.
   7. Question on leaving the PAR open for addition of new data confidentiality or integrity protocols.
      1. We would like to limit the scope as much as possible.
   8. Question on “this amendment adds support” phrasing.
      1. There was a previous feedback item that led to this phrasing, more work may follow off-line.
   9. Question for assurance that actions will be taken in all 4 areas listed in section 5.2.b and in no other area.
      1. At least the last bullet is still open.
   10. Question on subpoint a) of section 5.2.b, “authenticated key management” – should this be “authentication key management”.
       1. Yes, to be aligned with .11.
   11. Question on subpoint a) of section 5.2.b, should the “AKM” abbreviation be added?
       1. Yes, there is a high degree of familiarity with the abbreviation.
   12. Question on section 5.5, regarding the “disallow” wording for NIST.
       1. NIST’s IR 8547 does state “disallow” in section 4.1.2.
       2. However, NIST’s scope is not global and the wording should reflect that.
   13. Question on section 5.2.b: Should a “may” be added to avoid discussions on meeting all 4 points?
       1. As there was an earlier comment in the same spirit this should be further looked into.
   14. Question on adding HQC in section 8.1
       1. HQC was just approved and not yet standardized, so adding it would be premature.
8. Criteria for Standards Development – CSD
   1. The CSD now has more content, so can be read as a brand new document. Focus is put on controversial areas.
   2. Question on the need for a CSD – is there a need for a CSD?
      1. Chair intends to clarify, but for the moment we should proceed assuming it is needed.
   3. Question on adding non-US timelines.
      1. Yes, additions should be made wherever possible.
   4. Question on the need to review the CSD, if it may not be required.
      1. Earlier contributor clarified that the CSD is indeed required, only the coex componenet is not.
      2. The CA document is already marked “No” in the CSD.
   5. Question on fragmenting frames being a factor for Known Cost Factors.
      1. The text was added to reflect the burden on devices, rather than the financial cost – probably too much detail.
   6. Question on what the minor increase in operational costs will be.
      1. Probably there will not be one, document was updated.
9. Chair issues a re-reminder to fill in attendance. Next meeting will be on the 7th of April at 1PM ET, via teleconference.
10. Adjourned at 13:01 ET.

**Appendix A - Attendance:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Breakout** | **Timestamp** | **Name** | **Affiliation** |
| PQC SG | 03/27/2025 | baron, stephane | Canon Research Centre France |
| PQC SG | 03/27/2025 | Baykas, Tuncer | Self |
| PQC SG | 03/27/2025 | Bhandaru, Nehru | Broadcom Corporation |
| PQC SG | 03/27/2025 | Campiglio, Ugo | Cisco Systems, Inc. |
| PQC SG | 03/27/2025 | Carty, Clark | Juniper Networks, Inc. |
| PQC SG | 03/27/2025 | Chappell, Matthew | Cox Communications Inc. |
| PQC SG | 03/27/2025 | Li, Weiyi | Spreadtrum Communication USA, Inc |
| PQC SG | 03/27/2025 | Lungu, Alexandru | SAMSUNG ELECTRONICS |
| PQC SG | 03/27/2025 | Manoharan, Jegan | Cisco Systems, Inc. |
| PQC SG | 03/27/2025 | McCann, Stephen | Huawei Technologies Co., Ltd |
| PQC SG | 03/27/2025 | Montemurro, Michael | Huawei Technologies Co., Ltd |
| PQC SG | 03/27/2025 | Nezou, Patrice | Canon Research Centre France |
| PQC SG | 03/27/2025 | Orr, Stephen | Cisco Systems, Inc. |
| PQC SG | 03/27/2025 | Pettersson, Charlie | Ericsson AB |
| PQC SG | 03/27/2025 | Kurapov, Anton | Wireless Networks Lab |
| PQC SG | 03/27/2025 | RISON, Mark | Samsung Cambridge Solution Centre |
| PQC SG | 03/27/2025 | Sand, Stephan | German Aerospace Center (DLR) |
| PQC SG | 03/27/2025 | Schelstraete, Sigurd | MaxLinear |
| PQC SG | 03/27/2025 | Sevin, Julien | Canon Research Centre France |
| PQC SG | 03/27/2025 | Sun, Bo | Sanechips |
| PQC SG | 03/27/2025 | Swartz, Matt | Cisco |
| PQC SG | 03/27/2025 | Thakore, Darshak | Cable Television Laboratories Inc. (CableLabs) |
| PQC SG | 03/27/2025 | Wang, Zisheng | ZTE Corporation |
| PQC SG | 03/27/2025 | Yang, Jay | ZTE Corporation |
| PQC SG | 03/27/2025 | Rodriguez, Stephen | Cisco Systems, Inc. |
| PQC SG | 03/27/2025 | Kumar, Manish | NXP Semiconductors |
| PQC SG | 03/27/2025 | Kim, Sang Gook | LG ELECTRONICS |
| PQC SG | 03/27/2025 | Kandala, Srinivas | SAMSUNG |
| PQC SG | 03/27/2025 | Choi, Jinsoo | LG ELECTRONICS |
| PQC SG | 03/27/2025 | Contreras Albesa, Javier | Cisco Systems, Inc. |
| PQC SG | 03/27/2025 | Cui, Yaoshen | TP-Link Systems Inc. |
| PQC SG | 03/27/2025 | DeLaOlivaDelgado, Antonio | InterDigital, Inc. |
| PQC SG | 03/27/2025 | Dumdei, Alan | Cisco Systems |
| PQC SG | 03/27/2025 | Eastlake 3rd, Donald | INDEPENDENT |
| PQC SG | 03/27/2025 | Fan, Shuang | Sanechips Technology Co., Ltd. |
| PQC SG | 03/27/2025 | Ficara, Domenico | Cisco Systems, Inc. |
| PQC SG | 03/27/2025 | Fujimori, Yuki | Canon Research Centre France |
| PQC SG | 03/27/2025 | Georgiev, Zahari | Cisco Systems, Inc. |
| PQC SG | 03/27/2025 | GUIGNARD, Romain | Canon Research Centre France |
| PQC SG | 03/27/2025 | Gupta, Binita | Cisco Systems, Inc. |
| PQC SG | 03/27/2025 | Halasz, David | Morse Micro |
| PQC SG | 03/27/2025 | Hamilton, Mark | Ruckus/CommScope |
| PQC SG | 03/27/2025 | Harkins, Daniel | Aruba Networks, Inc. |
| PQC SG | 03/27/2025 | Hart, Brian | Cisco Systems, Inc. |
| PQC SG | 03/27/2025 | Huang, Po-Kai | Intel |
| PQC SG | 03/27/2025 | Hussein, Abdalla | Huawei Technologies Co., Ltd |
| PQC SG | 03/27/2025 | Jang, Insun | LG ELECTRONICS |
| PQC SG | 03/27/2025 | Yee, James | MediaTek Inc. |
| PQC SG | 03/27/2025 | Zuniga, Juan Carlos | Cisco Systems, Inc. |