Comments on IEEE P802.11bt PAR & CSD

From IEEE 802.1

Contact:

Mark Hantel

802.1 Maintenance TG Chair

Glenn Parsons

802.1 Working Group Chair

- These comments are on the PAR and CSD found in:
  - https://mentor.ieee.org/802.11/dcn/25/11-25-0958-00-0PQC-draft-p802-11bt-par.pdf
  - https://mentor.ieee.org/802.11/dcn/25/11-25-0598-03-0PQC-pqc-draft-proposed-csd.docx

PAR

- Suggest Aligning the PAR title to “Support for Post Quantum Cryptography”
- 5.5 - Sentence 2
  - Sentence 2: Suggest rewording "There is a strong market need to define post-quantum protocols" to: "There is a strong market need to specify post-quantum resistant protocols".
  - Sentence 3: starting with "As an example", suggest rephrasing "digital signatures based classic cryptography" to "digital signatures based on classic cryptography".
  - Last sentence: Suggest removing last sentence "It is believed that these requirements will also appear in other market verticals".
- 8.1
  - What section(s) do the FIPS references apply to?

CSD

- Overall: Suggest using the latest template document for the CSD

https://mentor.ieee.org/802-ec/dcn/18/ec-18-0064-02-0PNP-csd-template-in-doc-format.doc

- CSD - The title of the CSD is not consistent with the PAR, suggest rewording to "Support for Post Quantum Cryptography"
- 1.2.1 Page 2 Line 41:
  - Suggest rewording "CRQC will void the security mechanisms" to "CRQC is expected to void or weaken the security mechanisms".
- 1.2.5 Page 4:
  - Lines 16, 24 and 29 talk about both firmware and software. Suggest unifying terms to software.