P802.1AReg
Security Device Identity— Amendment: Support for the Module-Lattic-Based Signature Algorithm

Responses to comments received from other 802 Working Groups on the Project Authorization Request(PAR) and Criteria for Standards Development (CSD)

2025-11-12

Comments received from 802.3, 802.11, and 802.15.

A copy of the updated PAR showing changes made is at:

https://www.ieee802.org/1/files/public/docs2025/eg-ml-dsa-PAR-1125-v00.pdf

The updated CSD is at:

https://www.ieee802.org/1/files/public/docs2025/eg-ml-dsa-CSD-1125-v00.pdf

802.3 comment on the PAR (1)

[Email from the Chair, IEEE 802.3 PAR adhoc, November 9, 11.10 PM]

- Comment:
  In section 5.5, the first sentence suggests that quantum may provide the computer power then the second sentence says that it will protect against quantum attacks. And the “expected computing capability of quantum computer attacks”.
- Response:
  5.5 Need for the Project: Change second sentence to: “This amendment provides cryptographic algorithms which are expected to secure devices against attacks from both classical and quantum computers.”

802.3 comment on the PAR (2)

[Email from the Chair, IEEE 802.3 PAR adhoc, November 9, 11.10 PM]

- Comment:
  In the third sentence,it is unlikely that all governments in the world will require the proposed requirement. Consider changing to “some government procurements” or “many government”.
- Response: Change the third sentence to:
  “Post Quantum Cryptography supported DevIDs are expected to become a requirement for many governmental procurements (in January 2027 in the United States of America, with a full transition by 2031, as prescribed in US Quantum Computing Cybersecurity Preparedness Act (US 117-260)).”

802.3 comment on the PAR (3)

[Email from the Chair, IEEE 802.3 PAR adhoc, November 9, 11.10 PM]

- Comment:
  In section 6.1.1 Explanation, Change “will” to “expected to” unless the solution is already adopted by the group. If already adopted, then please add more detail to explain its adopting. Regarding the copyright permission and the prior statement, consider adding “if needed” to the end of the sentence. .
- Response: Change the explanation as follows:
  Explanation: “The amendment is expected to include a fragment of Abstract Syntax Notation 1 (ASN.1) quoted from IETF RFC 9881. Copyright permission will be sought from the IETF Trust if needed.”

802.3 comment on the PAR (4)

[Email from the Chair, IEEE 802.3 PAR adhoc, November 9, 11.10 PM]

- Comment:
  Lastly in 6.1.1, is the referenced IETF RFC the same one as stated in 5.3 If not, please clarify or provide specific reference.
- Response: In 5.3 we are changing the response to No and removing the explanation. The RFC previously referenced RFC has now been published as RFC 9881.

802.3 comment on the PAR (5)

[Email from the Chair, IEEE 802.3 PAR adhoc, November 9, 11.10 PM]

- Comment:
  In 8.1, please denote that NIST is a part of the US Department of Commerce, which may not be clear to individuals outside the USA. Such as “NIST is the National Institute of Standards and Technology (U.S. Department of Commerce)”.
- Response: Change first sentence to:
  “#5.2.b: ML-DSA parameter sets are specified in National Institute of Standards and Technology (NIST—U.S. Department of Commerce) Federal Information Processing Standards (FIPS) 204 and in other national and international standards.”

802.3 comment on the CSD

[Email from the Chair, IEEE 802.3 PAR adhoc, November 9, 11.10 PM]

- Comment:
  Section 1.2.1: restructure the last sentence to remove “We”. The issue of saying “We have” is ambiguous to as to “We” are. In IEEE 802, “we” cannot be vendors as IEEE 802 is an individual process. Consider revising to be “Multiple vendors are known to be preparing…”
- Response: Change 1.2.1 last sentence to:
  “Multiple vendors are known to be preparing device identification solutions to meet the market demand.”

802.11 comment on the PAR (1)

[From doc.: IEEE 802-11-25/1818r1 Slide 20]

- Comment (split into the two components of the original comment):
  5.5 ~~This amendment provides~~ There is a need for identifiers of cryptographic algorithms which ~~can~~ are believed to secure devices against both classical and quantum computer attacks.
- Response: Change sentence to:
  “The need is for the inclusion of cryptographic algorithms as part of IEEE Std 802.1AR-2018 Secure Device Identify, including identifiers for the algorithms, that are believed to secure devices against attacks from both classical and quantum computers.”

802.11 comment on the PAR (2)

[From doc.: IEEE 802-11-25/1818r1 Slide 20]

- Comment (split into the two components of the original comment):
  Post Quantum Cryptography supported DevIDs are expected to become a requirement for government procurements in January 2027 with a full transition required by 2031, as prescribed in "…. ". The reference would need to be specified and added to 8.1
  The concern is if the "government" is just US or other governments. Does this need to expand to include a reference to justify the timing noted ("January 2027" and "2031").
- Response:

The text is updated as a result of 802.3 comments, and a specific reference included as per this comment.

802.15 comments on the PAR (1)

[From doc#:IEEE 802 15-25-0627-00-0mag]

- Comment:
  In 5.3, IETF document is already published as RFC 9881, please correct the Explanation

- Response:

We changed 5.3 to “no” and removed the explanation.

802.15 comments on the PAR (2)

[From doc#:IEEE 802 15-25-0627-00-0mag]

Comment:

In 5.5, NIST standards are used by many nations; if describing government procurements, please specify which government, and the source of the dates

- Response

We changed this based on 802.3 comment.