P802.1AEef
Media Access Control (MAC) Security—Amendment: Ascon Cipher Suite

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 is at:

https://www.ieee802.org/1/files/public/docs2025/ef-ascon-macsec-cipher-suite-PAR-1125-v00.pdf

with a version tracking the changes at:

https://www.ieee802.org/1/files/public/docs2025/ef-ascon-macsec-cipher-suite-PAR-1125-v00-trk.pdf

The updated CSD is at:

https://www.ieee802.org/1/files/public/docs2025/ef-ascon-macsec-cipher-suite-CSD-1125-v00.pdf

802.3 comment on the PAR

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

- Comment:
  In 8.1: the first note indicates that Ascon is “in the NIST… publication….” Which publication is it or is Ascon in all of them? Suggest to reference a specification publication such as the one in the last note of this section.
- Response:
  “SP 800-232” has been added before the instance of “publication” referenced in the comment. The further instance of “the NIST publication” in the explanatory note for 5.2.b has been replaced by “NIST SP 800-232”.

802.3 comment on the CSD

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

- Comment:
  In 1.2.4 item (b), please send the sentence with a full stop “period”.
- Response:
  The requested change has been made.

802.11 comment on the PAR (1)

[From doc.: IEEE 802-11-25/1818r1 Slide 18]

- Comment:
  5.2.b Typically the Expansion of Acronyms occurs first and then the acronym… i.e. Media Access Control security (MACsec) Cipher Suite.
- Response:
  The suggested change has been made, with the initial letter of ”security” capitalised to agree with the title of the base standard.

802.11 comment on the PAR (2)

[From doc.: IEEE 802-11-25/1818r1 Slide 18]

- Comment:
  5.2.b Expand Acronym prior to first use “National Institute of Standards and Technology (NIST)”
- Response:
  The requested change has been made.

802.11 comment on the PAR (3)

[From doc.: IEEE 802-11-25/1818r1 Slide 18]

- Comment:
  5.5 replace the following sentence: “There is a growing awareness for the need for data integrity, confidentiality, and origin authenticity for all network communication.” to “Network security requires data integrity, confidentiality, and origin authenticity for all communication.” This field is not “growing”.
- Response:
  The requested change has been made.

802.11 comment on the PAR (4)

[From doc.: IEEE 802-11-25/1818r1 Slide 18]

- Comment:
  5.5 “Tag” is mentioned twice – only use one “Tag”. Suggest delete first “Tag”.
- Response:
  The suggested change has been made.

802.11 comment on the PAR (5)

[From doc.: IEEE 802-11-25/1818r1 Slide 18]

- Comment:
  6.1.2 – Proposed replacement sentence: “Registration Authority Committee (RAC) review is appropriate to assure terminology and descriptions of usage are correct and up to date.”
- Response:
  The proposed change has been made.

802.11 comment on the CSD (1)

[From doc.: IEEE 802-11-25/1818r1 Slide 19]

- Comment:
  CSD - 1.2.1 – A - missing ending period.
- Response:
  A period has been added, and an explicit hyperlink created to avoid a potential issue with a copy of the link including the period.
- Comment:
  CSD - 1.2.1 – B - missing ending period.
- Response:
  A period has been added.

802.11 comment on the CSD (2)

[From doc.: IEEE 802-11-25/1818r1 Slide 19]

- Comment:
  CSD – 1.2.3 – format of response paragraph needs attention.
- Response:
  The paragraph width has been adjusted.

802.15 comments on the PAR and CSD

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

802.1 PARs and CSDs

P802.1AEef - Amendment - Ascon Cipher Suite, PAR and CSD

- No comments