

SA ballot comments on [P802.1AEeg/D2.0](#)

The installed base of MACsec implementations support the default cipher suite (GCM-AES-128). While the addition of a more lightweight Ascon cipher suite is relevant for low capability devices, this should not come at the cost of confusing the installed base by removing the default cipher suite as the default.

Instead consider using two different conformance levels for MACsec: e.g., Ascon and default or light and traditional. This would allow a device to be conformant to one of these profiles and would also set the stage for future profiles to be defined. This separation of conformance levels is already implied by the grouping of conformance items in 5.4 for implementations supporting the Default CS and those supporting the Ascon CS.

This would also support a more restrictive Ascon profile (that only supports the Ascon CS) as per the apparent intent of 5.4 (j) [currently labeled as the second 5.4(i)]

In the current draft, the text and PICS proforma specify inclusive OR (one or the other or both) on the CS. I propose to change this to exclusive OR (one or the other) but on a profile. This allows the profile to be explicit with a single conditional mandatory CS simply based on a predicate concept similar to what has been proposed in the latest revision of P802.1Q-2020rev ([see A.19](#)).

Option A

The predicate is conceptually a profile. In this case that would be:

- *Default CS – Default: M*
- *Ascon CS – Ascon:M and Default:O*

In addition, some items are indicated as Ascon:X to align with the grouping in 5.4

I propose to amend the PICS Table A.1 as follows:

A.1

Item	Feature	Status	References	Support
CSI	<i>Does the implementation support Integrity Protection using the Default Cipher Suite as specified in Clause 14?</i>	Default: M ¹	5.3(k), 5.4(e), Clause 14, 14.5	Yes [] No []
ACSI	<i>Does the implementation support Integrity Protection using the Ascon-XPB-128 Cipher Suite?</i>	Default: O Ascon: M ²	5.3(k), Clause 14, 14.9	Yes [] No []
CSA	<i>Does the implementation include additional Cipher Suites specified in Clause 14</i>	Default: O Ascon: X	5.4(h), 5.4(i) A.16	Yes [] No []
CSV	<i>Does the implementation include Cipher Suites other than those specified in Clause 14, but meeting the criteria specified</i>	Default: O Ascon: X	5.4(k), A.17	Yes [] No []

¹ Default – this profile represents traditional implementations with a default CS and has similar conformance to IEEE Std 802.1AE-2018

² Ascon – this profile represents low capability devices limited to supporting a single CS

	in 14.2, 14.3, 14.4.1?			
--	---------------------------	--	--	--

In the current draft 5.3(k)

Support Integrity Protection using either or both of the GCM-AES-128 and Ascon-XPB-128 Cipher Suites specified in Clause 14.

I suggest changing 5.3(k) to:

Support Integrity Protection using at least one of the GCM-AES-128 and Ascon-XPB-128 Cipher Suites specified in Clause 14.

In 5.4 the groupings are “may” to fit into the previous inclusive OR scheme. With separate implementation profiles, these need to both be “shall”:

An implementation of a MAC Security Entity that supports Integrity Protection using the Default Cipher Suite (GCM-AES-128) shall:

An implementation of a MAC Security Entity that supports Integrity Protection using the Ascon-XPB-128 Cipher suite shall:

In the current draft 14.4 is changed to:

An implementation of MACsec that claims full conformance to this standard supports either or both of the GCM-AES-128 and Ascon-XPB-128 Cipher Suites as specified in 5.3 and 5.4, can support the additional Cipher Suites specified in this clause (Clause 14) as specified in 5.4, and does not implement any other Cipher Suite. Every conformant implementation shall include at least one Cipher Suite that does not encrypt User Data.

I suggest changing 14.4 to:

An implementation of MACsec that claims full conformance to this standard shall support one of two profiles:

- a) The default profile (representing similar conformance to IEEE Std 802.1AE-2018) shall support the GCM-AES-128 Cipher Suites as specified in 5.3, can support the additional Cipher Suites specified in this clause (Clause 14) as specified in 5.4, and does not implement any other Cipher Suite.*
- b) The ascon profile shall support the Ascon-XPB-128 Cipher Suites as specified in 5.4, and does not implement any other Cipher Suite. Every conformant implementation shall include at least one Cipher Suite that does not encrypt User Data.*

In the current draft 14.4.1 is change to

An implementation of MACsec that claims conformance to this standard with Cipher Suite variance, supports either or both of the GCM-AES-128 and Ascon-XPB-128 Cipher Suites as specified in 5.3 and 5.4, can support the additional Cipher Suites specified in this clause (Clause 14) as specified in 5.4, and may implement alternate Cipher Suites that meet the requirements of 14.2 and 14.3, and the following guidelines, and shall not implement any other Cipher Suite, or other combination of cryptographic algorithms and parameters.

In order to align with the single CS intent of the Ascon profile, which would not support a variance, I propose to change 14.4.1 to simply:

An implementation of MACsec that claims conformance to this standard with Cipher Suite variance, shall implement the Default Cipher Suite of 14.5, may implement one or more of the optional Cipher Suites in Table 14-1, and may implement alternate Cipher Suites that meet the requirements of 14.2 and 14.3, and the following guidelines, and shall not implement any other Cipher Suite, or other combination of cryptographic algorithms and parameters.

Option B

Alternatively, we could be more explicit about there being two profiles with separate PICS rows for each. The text changes from option A would be the same.

- Default Profile
Default CS – M
Other CS -O
- Ascon Profile
Ascon CS – M
Other CS - X

A.1

Item	Feature	Status	References	Support
DP	Does the implementation support the default profile?	O.1	5.4, 14.4	Yes [] No []
AP	Does the implementation support the ascon profile?	O.1	5.4, 14.4	Yes [] No []
CSI	Does the implementation support Integrity	DP: M DA: X	5.3(k), 5.4(e), Clause 14,	Yes [] No []

	<i>Protection using the Default Cipher Suite as specified in Clause 14?</i>		14.5	
ACSI	<i>Does the implementation support Integrity Protection using the Ascon-XPB-128 Cipher Suite?</i>	DP: O DA: M	5.3(k), Clause 14, 14.9	Yes [] No []
CSA	<i>Does the implementation include additional Cipher Suites specified in Clause 14</i>	DP: O DA: X	5.4(h), 5.4(i) A.16	Yes [] No []
CSV	<i>Does the implementation include Cipher Suites other than those specified in Clause 14, but meeting the criteria specified in 14.2, 14.3, 14.4.1?</i>	DP: O DA: X	5.4(k), A.17	Yes [] No []