SA ballot comments on P802.1AEef/D2.0

The installed base of MACsec implementations supports 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 (or three) different conformance levels for MACsec: e.g., Ascon and default or IOT and classic. This would allow a device to be conformant to one of these levels and would also set the stage for future levels 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 could also support a more restrictive IOT implementation (that only supports the Ascon CS and other lightweight CS) as per the apparent intent of 5.4 (j) [that should be 5.4 (k)]

In the current draft, the text and PICS proforma specify the OR on the CS. I propose to change this to OR (one or the other) on an implementation (or profile). This allows the implementation to be explicit with a (or dual) 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). Further, this allows the explicit description of the three devices: classic, intermediate and IOT. This gives the installed base a clear recognition.

This proposal does not include any additional prohibit statements that could be used to restrict the CS for IOT devices.

Option A

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

- *Default CS – Classic: M and Intermediate:M*
- *Ascon CS – IOT:M and Intermediate: M*

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

A.1

Item	Feature	Status	References	Support
CSI	*Does the implementation support Integrity Protection using the Default Cipher Suite as specified in Clause 14?*	Classic: M [1] Intermediate: M [2]	*5.3(k), 5.4(e),* *Clause 14,* *14.5*	Yes [ ] No[ ]
ACSI	*Does the implementation support Integrity Protection using the Ascon-XPN-128 Cipher Suite?*	Intermediate: M IOT: M [3]	*5.3(k),* *Clause 14,* *14.9*	Yes [ ] No[ ]
CSA	*Does the implementation include additional Cipher Suites specified in Clause 14*	O	*5.4(h), 5.4(i)* *A.16*	Yes [ ] No[ ]
CSV	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?	O	*5.4(k),* *A.17*	Yes [ ] No[ ]

[1] *Classic – this represents traditional implementations with the default CS and has similar conformance to IEEE Std 802.1AE-2018*

[2] *Intermediate – this represents an intermediate implementation with both the default CS and an IOT CS*

[3] *IOT – this represents low capability devices with an initial lightweight CS*

In the current draft 5.3(k)

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

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-XPN-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 three conformance classes:*
>
> *a) Classic implementations (representing similar conformance to IEEE Std 802.1AE-2018) shall support the GCM-AES-128 Cipher Suite as specified in 5.3, may implement one or more of the Optional Cipher Suites in table 14-1, and may support alternate Cipher Suites that meet the requirements of 14.2 and 14.3, and guidelines of 14.4.1, and shall not implement any other Cipher Suite or other combination of cryptographic algorithms and parameters.,*
> *b) Intermediate IOT implementations shall support the GCM-AES-128 and Ascon-XPN-128 Cipher Suites as specified in 5.3, may implement one or more of the Optional Cipher Suites in table 14-1, and may support alternate Cipher Suites that meet the requirements of 14.2 and 14.3, and guidelines of 14.4.1, and shall not implement any other Cipher Suite or other combination of cryptographic algorithms and parameters.,*
> *c) IOT implementations shall support the Ascon-XPN-128 Cipher Suite as specified in 5.3, may implement one or more of the Optional Cipher Suites in table 14-1, and may support alternate Cipher Suites that meet the requirements of 14.2 and 14.3, and guidelines of 14.4.1, and shall not implement any other Cipher Suite or other combination of cryptographic algorithms and parameters.*
>
> *Every conformant implementation shall include at least one Cipher Suite that does not encrypt User Data.*

In the current draft the first paragraph of14.4.1 is changed 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-XPN-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 avoid repeating most of 14.4, this is rephrased as an addition to 14.4 (which makes sense since it's a subclause):

An implementation of MACsec that claims conformance to this standard with Cipher Suite variance, in addition to the conformance classes of 14.4, may also 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.

- Classic
  Default CS – M
  Other CS -O
- Intermediate
  Default CS – M
  Ascom CS – M
  Other CS - O
- IOT
  Ascon CS – M
  Other CS - O

A.1

Item	Feature	Status	References	Support
CLC	Is this a classic implementation ?	O.1	*5.4, 14.4*	Yes [ ] No[ ]
INT	Is this an IOT intermediate implementation ?	O.1	*5.4, 14.4*	Yes [ ] No[ ]
IOT	Is this an IOT implementation ?	O.1	*5.4, 14.4*	Yes [ ] No[ ]
CSI	*Does the implementation support Integrity Protection using the Default Cipher Suite as specified in Clause 14?*	CLC: M INT: M	*5.3(k), 5.4(e),* *Clause 14,* *14.5*	Yes [ ] No[ ]
ACSI	*Does the implementation support Integrity Protection using the Ascon-XPN-128 Cipher Suite?*	CLC: O INT: M IOT: M	*5.3(k),* *Clause 14,* *14.9*	Yes [ ] No[ ]
CSA	*Does the implementation include additional Cipher Suites specified in Clause 14*	O	*5.4(h), 5.4(i)* *A.16*	Yes [ ] No[ ]
CSV	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?	O	*5.4(k),* *A.17*	Yes [ ] No[ ]