This provides responses to comments JTC1 ballot of IEEE 802.1AEcg-2016 (ISO/IEC/IEEE FDIS 8802-1AE:2013/FDAmd 3).

The voting results on IEEE 802.1AEcg-2016 (ISO/IEC/IEEE FDIS 8802-1AE:2013/FDAmd 3):

- Passed 10/1/11
- 1 comment was received with the China NB NO vote

China NB comment 1 on IEEE 802.1AEcg-2016 (ISO/IEC/IEEE FDIS 8802-1AE:2013/FDAmd 3)
14.5 Default Cipher Suite (GCM-AES-128) and 14.6 GCM-AES-256 further specify that the mandatory cryptographic algorithm in implementation of the standard is AES. However, policy and regulation limitations on application of cryptographic algorithm differ from countries and regions. In addition, there are many other international algorithms for choice. Therefore, it is unreasonable to specify cryptographic algorithms as mandatory implementation in this standard.

*Proposed change: Noting that in **TMB Resolution 70/2018** (72nd meeting of the Technical Management Board) regarding Legal statements in ISO deliverables,*

• text relating to compliance with contractual obligations, legal requirements and government regulations exists in many ISO standards; and

• ISO deliverables can be used to complement such requirements and serve as useful tools for all related stakeholders (which can include government authorities and industry players);

ISO clarifies that, for all ISO deliverables:

*a) Statements that include an explicit requirement or recommendation to comply with **any specific law, regulation or contract (such as a normative reference to such requirements)**, or portion thereof, are not permitted;*

*b) **Statements related to legal and regulatory requirements that do not violate point a) are permitted**;*

It is then suggested that the text shall make it clear that "Cryptographic algorithms to be applied to information security mechanism may be subject to national and regional regulations. In this International Standard, cryptographic algorithms are instantiated, and may be chosen according to specific requirements in different countries and regions."

The comments have been processed in a timely manner using the mechanisms defined and agreed in 6N15606.

This document provides the responses from IEEE 802 to the comment by China NB on this ballot.

IEEE 802 response to CN.1 on IEEE 802.1AEcg-2016 (ISO/IEC/IEEE FDIS 8802-1AE:2013/FDAmd 3):

1. The scope of the project to develop the IEEE Std 802.1AEcg-2017 amendment did not include technical changes to the Cipher Suites or their conformance requirements as specified in the already approved IEEE Std 802.1AE (ISO/IEC/IEEE FDIS 8802-1AE:2013) and accordingly no such changes are present in the amendment.

While Cipher Suite conformance changes were out of scope of the IEEE Std 802.1AEcg-2018 amendment, it should also be noted that:

(a) All standards need to have mandatory-to-implement options to ensure interoperability, which is a primary purpose of international standardization

(b) The IEEE Std 802.1AEcg Ethernet Data Encryption devices (EDEs) specification addresses a requirement to secure data carried by Provider Bridged Network (PBN) services. Two interoperating EDEs can therefore be located at a significant distance from each other and possibly in different countries or regions, thus strengthening the requirement for a universal interoperable Cipher Suite.

(c) The mandatory to implement Default Cipher Suite, GCM-AES-128, was chosen because it is well vetted, internationally designed, and recognized.

(d) IEEE Std 802. 1AE (ISO/IEC/IEEE FDIS 8802-1AE:2013) already includes Cipher Suite identification and protocol identification mechanisms to facilitate the addition of further standard Cipher Suites (by future amendment of the base standard) or the use of proprietary Cipher Suites (without amending the base standard) should an additional Cipher Suite be required for any reason. It is not necessary for the standard to speculate on, or to limit, the reasons why any specific additional Cipher Suite is desired. Technical criteria for additional Cipher Suites are already specified in IEEE Std 802.1AE (ISO/IEC/IEEE FDIS 8802-1AE:2013) clause 14.4 (Cipher Suite conformance).