This provides responses to comments received on the JTC1 ballot of IEEE 802.1AR-2018 (ISO/IEC/IEEE FDIS 8802-1AR/Ed 2).

The voting results on IEEE 802.1AR-2018 (ISO/IEC/IEEE FDIS 8802-1AR/Ed 2) in 6N17067

- Passed 11/1/0
- 2 comments received with the China NB NO vote

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 comments by China NB on this ballot.

China NB comment 1 on IEEE 802.1AR-2018 (ISO/IEC/IEEE FDIS 8802-1AR/Ed 2)

The text specifies cryptographic algorithm combinations such as RSA-2048/SHA-256, ECDSA P-256/SHA-256, ECDSA P-384/SHA-384, which are used as signature suites.
The specific algorithm(s) shall not be limited, because:
1. There are many other international algorithms for choice, which have been specified in ISO/IEC international standards.
2. The policy and regulation requirements on application of cryptographic algorithms differ from countries and regions.
Therefore, it is unreasonable to specify cryptographic algorithms such as RSA-2048, ECDSA P-256, ECDSA P-384, SHA-256 and SHA-384 as mandatory implementation in this proposal.

Proposed change: In 60-day ballot, China NB referenced TMB Resolution 70/2018 and proposed a statement that does not violate it: "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." This statement is reasonable and can solve the problem China mentioned easily. Unfortunately, IEEE 802 did not accepted this proposal in 6N16912.

However, the proposal given by IEEE 802 in 6N16912 about making amendments cannot solve the issues effectively. Besides, choosing well-vetted, internationally designed, and recognized signature suites should reasonably include other algorithms defined in International Standards.

To conclude, China would like to propose again to add a statement in the text of 802.1AR: "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 other internationally designed and recognized cryptographic algorithms may be chosen according to specific requirements in different countries and regions."

IEEE 802 response to CN.1 on IEEE 802.1AR-2018 (ISO/IEC/IEEE FDIS 8802-1AR/Ed 2):

1. ISO/IEC/IEEE 8802-1AR:2014 and the proposed revision in ISO/IEC/IEEE FDIS 8802-1AR/Ed 2 do not violate TMB Resolution 70/2018. There is no reference to a specific law, regulation or contract in this standard. It is not appropriate to reference national and/or regional regulation requirements in this Standard.

2. IEEE 802.1AR-2018 (ISO/IEC/IEEE FDIS 8802-1AR/Ed 2) has chosen well-vetted, internationally designed, and recognized signature suites. Contrary to the statement in CN.1 comment, the signature suites specified in the standard are not all mandatory to implement – any of the signature suites may be implemented, and only one must be supported to comply with the Standard. Restricting the number of conformant signature suites is highly desirable because too many options will negatively affect overall interoperability.

3. It is understood that emerging deployment scenarios for IEEE 802.1AR will likely require additional signature suites. For interoperability reasons, new signature suites may be standardized in future amendments to IEEE 802.1AR. We welcome contributions on both requirements for and the potential details of new signature suites. The contributions must reference technical rationale; it is not necessary to reference national laws or regulations for the purposes of this standard.

China NB comment 2 on IEEE 802.1AR-2018 (ISO/IEC/IEEE FDIS 8802-1AR/Ed 2)
This proposal is based on and implemented with IEEE 802.1X-2010, on which China NB has expressed sustained oppositions and submitted detailed comments on substantial issues (including 6N15555 etc.). IEEE has acknowledged the receiving of China NB's comments, but there has not been any technical improvements made on IEEE Std 802.1X and hence the defects still exist. China has noticed the reply in 6N16912, but the reply did not solve the technical problem mentioned about 802.1X.

Proposed change: NONE

IEEE 802 response to CN.2 on IEEE 802.1AR-2018 (ISO/IEC/IEEE FDIS 8802-1AR/Ed 2):
The China NB's ballot response states it will not approve IEEE 802.1AR-(ISO/IEC/IEEE FDIS 8802-1AR/Ed 2) because it references IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013), which the China NB has consistently and repeatedly asserted is defective since at least 2012. However, the China NB has failed to substantiate these assertions, despite numerous requests from IEEE 802. IEEE 802 will not make changes to approve IEEE 802.1AR-2018 (revision to ISO/IEC/IEEE 8802-1AR:2014) without substantiation of these assertions.

The general assertions raised in the China NB's ballot were discussed at length in 2013 at an IEEE 802 meeting in Geneva (with IEEE 802 and Switzerland NB representatives in attendance) and in both 2013 and 2014 at SC6 meetings in Seoul and Ottawa (with IEEE 802, China NB and Switzerland NB representatives in attendance). During those meetings, IEEE 802 fully responded to all of the claims made by both the China NB and Switzerland NB representatives and also provided additional information about the design and specification of IEEE 802 technologies. Specifically,

- In June 2013 in 6N15658 (*IEEE 802 Response to 6N15613*), IEEE 802 explains why none of the attacks described in 6N15613 (*NB of China's contribution on Effective Attack on IEEE802.1X-the further analysis of 6N15523*) are effective and reveals how the attacks described in the China NB contribution 6N15613 will fail.

- In June 2013 in 6N15646 (*IEEE 802 Response to 6N15523*), IEEE 802 explains why the analysis in 6N15523 (*NB of Switzerland's contribution on a comparative analysis of TePA/KA4 and IEEE 802.1X*

Security) is flawed, noting it produces erroneous results based on misunderstandings of technology, invalid assumptions, and analysis using an incorrect model.

- In January 2014 in 6N15870 (*IEEE 802 response to SC6N15840 – "Intentional Weaknesses in Information Security Standards and Implementations"*), IEEE 802 responded to non-specific allegations by the China NB about any security standards developed outside ISO. The China NB suggested that such standards contain intentional weaknesses. IEEE 802 responded that the best way to avoid such issues is to develop standards in an open standards process, such as that provided by IEEE 802.

- In January 2014 in 6N15845 (*Explanation of Certificate Use in 802.1X EAP-TLS*), IEEE 802 described the use of certificates in IEEE 802.1.

- In July 2015 in 6N16255 (*IEEE 802 response to China NB comments on IEEE Std. 802.1Q and 802.1Xbx*), IEEE 802 responded to the stated concerns raised on IEEE 802.1Q and IEEE 802.1X. Specifically, it was pointed out that IEEE Std 802.1Q does not depend on the use of IEEE Std 802.1X. In response to the unsubstantiated comment that there are "security problems" in IEEE Std 802.1X, the IEEE response clearly stated that IEEE Std 802.1X does not expose the public network or its user to (unspecified) security problems because it mandates the use of mutual authentication methods, reflecting current needs, best practice, and experience from IEEE 802.1X-2004.

Additionally, at the SC6 meeting in Ottawa in early 2014, the China NB and Switzerland NB representatives committed to providing additional technical details to justify their concerns. No such submissions were made to the SC6 meeting in London later that year, and no technical submissions were received subsequently. Furthermore, there has been no technical discussion since that time.

IEEE 802 is eager to hear and discuss further the details of any new concerns about IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013) from the China NB. On 21 February 2017, IEEE 802 formally invited a representative of the China NB (as well as representative from other interested SC6 NBs) to attend the IEEE 802 Plenary meeting held in Vancouver, Canada the week starting Monday, 13 March 2017. The invitation to attend a future IEEE 802 Plenary meeting remains open.

IEEE 802 believes that the attacks on IEEE 802.1X-2010 described by the China NB have all been shown to be not valid but continues to invite the China NB to submit any additional technical details for consideration. In the absence of technical substantiation of the claims, IEEE 802 cannot consider modification of the existing IEEE 802 or ISO standards.