This provides responses to comments JTC1 ballot of IEEE Std 802.1X-2020 (ISO/IEC/IEEE FDIS 8802-1X (Ed 2))

The voting results on IEEE Std 802.1X-2020 (ISO/IEC/IEEE FDIS 8802-1X (Ed 2)) in SC6N17643:

- Support need for ISO standard? Passed 9/1/9
- 2 comments 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 Std 802.1X-2020:

ISO/IEC/IEEE FDIS 8802-1X (Ed 2) is a revision of IEEE Std 802.1X-2010 incorporating IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck-2018. China has voted against IEEE 802.1X and its amendments because of the following technical reasons.

ISO/IEC/IEEE FDIS 8802-1X (Ed 2) is still based on the concept that the link between the Authenticator and AS belongs to the internal network, or is easy to be setup by the controllable and trusted network channel. It was pointed out for many times that the structural concept is unable to apply and guide the network construction based on the current public network environment. Using IEEE 802.1X in the public network directly will be faced with many security threats, such as man-in-the-middle attacks, session hijacking attacks, denial of service attacks, MAC address forging. This technology is not able to match a variety of other network security protocols or assumptions.

ISO/IEC/IEEE FDIS 8802-1X (Ed 2) cannot achieve the real mutual authentication between the Supplicant and Authenticator and there is no Authenticator identity in the authentication process. The equipment that has no identity and cannot be identified in the network will lose the basic functionality of identity legitimacy, hence it cannot meet the requirements of the management control of network access and the requirements of the networking construction development with the current sensor network (SN), Internet of Things (IOT) etc..

IEEE once replied that "the China NB has alleged that man-in-the-middle (and other) attacks are possible without the technical details of such an attack being supplied or the attack being demonstrated." However, this is not true. Documents 6N15613, 6N15662, 6N15523 have illustrated those problems in detail.

<u>Proposed Change:</u>

It is suggested to improve the structural concept of ISO/IEC/IEEE FDIS 8802-1X (Ed 2).

IEEE 802 response to CN.1 on IEEE Std 802.1X-2020:

The China NB comment is substantially based on a statement, "*Documents 6N15613, 6N15662, 6N15523 have illustrated those problems in detail"*; that is inaccurate. IEEE 802 responded to the referenced documents in a timely manner more than eight years ago (i.e., shortly after the documents were made available, in 2013). The IEEE 802 responses at the time explained why the Switzerland NB contributions

6N15613 and 6N15662 were based on misunderstandings of the technology and a variety of invalid assumptions and described how the attacks described in the China NB contribution 6N15523 will fail. Despite numerous requests from IEEE 802, there have been no further technical descriptions or clarifications sent to IEEE 802 in relation to the China NB's concerns since that time. In the absence of any technical details of a man-in-the-middle (or other) attack being provided, or a demonstration of the efficacy of any such attack, IEEE 802 cannot justify making corresponding changes to IEEE Std 802.1X-2020 (revision to ISO/IEC/IEEE 8802-1X:2013).

The China NB comment also suggests that secure connectivity between an Authenticator and an Authentication Server (AS) cannot be provided in the current public network environment. IEEE 802 points out that that communication between any management server for a network (not just an AS) and any system providing access to that network must be secured. Furthermore, IEEE 802 notes that there are numerous methods to secure connectivity between two communicating parties that are well established and capable of providing secure connectivity when part or all of the intervening communication path traverses any public network (e.g., an IPsec-based VPN).

The China NB comment also raises a concern about MAC address forgery. IEEE 802 notes that the Authenticator-to-AS link is not relevant for MAC address and privacy protection. When an external AS is deployed, the communication is performed and secured at a higher layer.

In addition, IEEE 802 observes that an external AS may not be required if certificates are used to provide authentication (or verifiable identity), as described previously in 6N15845 (*Explanation of Certificate Use in 802.1X EAP-TLS*). An external AS is an optimization to allow for deployment of certain types of client credentials (e.g., passwords) to scale. If all entities require certificates for authentication, then the AS and Authenticator are one-and-the-same.

The China NB's ballot response continues to assert their opinion that IEEE Std 802.1X is defective. However, the China NB has failed to substantiate these claims. IEEE 802 has requested clarification and demonstration multiple times since at least 2012. The general assertions raised in the China NB's comments 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 responded to all comments 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 explained why none of the attacks described in 6N15613 (*NB of China's contribution on Effective Attack on IEEE 802.1X-the further analysis of 6N15523*) are effective and how the attacks described in the China NB contribution 6N15613 will fail.

- In June 2013 in 6N15646 (*IEEE 802 Response to 6N15523*), IEEE 802 explained 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 the technology, invalid assumptions, and an 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 observed in response 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 shared a contribution that described the use of certificates in IEEE 802.1 security standards.

- In July 2015 in 6N16255 (*IEEE 802 response to China NB comments on IEEE Std 802.1Q and IEEE Std 802.1Xbx*), IEEE 802 responded to concerns raised in relation to IEEE Std 802.1Q and IEEE Std 802.1X. Specifically, IEEE 802 pointed out that IEEE Std 802.1Q does not depend on the use of IEEE Std 802.1X. In response to the unsubstantiated claim that there are alleged "security problems" in IEEE Std 802.1X, the IEEE 802 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 operational experience from deployments of IEEE Std 802.1X-2004.

- 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 or subsequently. Moreover, there has been no technical discussion in SC6 meetings since that time.

IEEE 802 has requested clarification and corroboration for every instance that the China NB submitted comments that perpetuate these alleged claims about security in IEEE 802 standards under consideration per the PSDO agreement. However, the China NB has failed to provide any such clarification and corroboration.

IEEE 802 welcomes the opportunity to hear and discuss further any concerns about IEEE Std 802.1X-2020 (revision to ISO/IEC/IEEE 8802-1X:2013) from China NB representatives. The invitation for a representative of the China NB (as well as representatives from other interested SC6 NBs) to attend an IEEE 802 Plenary meeting remains open. These meetings are currently being conducted remotely due to the COVID situation and so attendance should not be difficult.

China NB comment 2 on IEEE Std 802.1X-2020:

This proposal uses MACSec (defined by IEEE 802.1AE) to protect the security of the network. However, China NB has pointed out the security problems of MACSec for several times during the previous ballots, e.g. 6N15556 and 6N15770.

China also submitted the comments on IEEE 802.1AE-2018, which has technical issues including inconsistence between content and title, using high cost Hop-by-Hop Encryption, only permitting to use specific cryptographic algorithms like AES (not including other compliant options that are compliant with ISO/IEC international standards) and so on (see detailed comments in 6N17207).

The security issues about IEEE 802.1AE have not been properly resolved until now, hence the use to MACsec will lead to security risks in engineering implementation and network operation.

The reply in SC6N17493 was noted. This reply did not take any actions to resolve the technical problem mentioned above. Therefore, China cannot approve this project.

<u>Proposed Change</u>:

Security mechanism should be improved or changed.

IEEE 802 response to CN.2 on IEEE Std 802.1X-2020:

This comment from the China NB on IEEE Std 802.1X-2020 (revision to ISO/IEC/IEEE 8802-1X:2013) provides no additional technical description or clarification of any concerns alluded to by the China NB, despite numerous requests from IEEE 802 in the past. Additionally, IEEE 802 observes that while IEEE Std 802.1X-2020 (revision to ISO/IEC/IEEE 8802-1X:2013) references the use of IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE (Ed 2)) MACsec, it does not require it. Furthermore, IEEE 802 notes the current comment does not explain in any detail what updates to IEEE Std 802.1X-2020 (revision to ISO/IEC/IEEE 8802-1X:2013) are suggested by the China NB.

IEEE 802 notes that the China NB submitted comments on the previous ballots of IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE (Ed 2)) in documents 6N15556 and 6N15770 and IEEE 802 responded to these comments in a timely manner (see documents 6N15608 and 6N15859). Specifically, for the comments in 6N15770, a summary of IEEE 802 responses in 6N15859 follows:

- In the first comment, there were no technical suggestions, therefore no action could be taken in the absence of any proposed changes.
- For the second comment, IEEE 802 concurred that as part of the normal maintenance process, the IEEE 802.1 WG reviews the references to ensure that only required references are included, RFC references are up to date, and normative RFC references have an appropriate status.

Likewise, for comments on IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE (Ed 2)) submitted in 6N17207, complete IEEE 802 responses are available for review in 6N17266.

IEEE 802 believes that none of the alleged security defects asserted by the China NB have been shown to be valid, and in the absence of further technical details to substantiate any concerns, IEEE 802 cannot make corresponding changes IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE (Ed 2)) or IEEE Std 802.1X-2020 (revision to ISO/IEC/IEEE 8802-1X:2013).