IEEE 802.21: Media Independent Services

Liaison Communication

## Source: IEEE 802.21 Working Group

|  |  |  |
| --- | --- | --- |
| To: | Mr. KwanHoo Shin | ISO/IEC JTC 1/SC 6 Secretariat  [kyleshin7@tta.or.kr](mailto:kyleshin7@tta.or.kr) |
| CC: | Konstantinos Karachalios | Secretary, IEEE-SA Standards Board Secretary, IEEE-SA Board of Governors [sasecretary@ieee.org](mailto:sasecretary@ieee.org) |
|  | Paul Nikolich | Chair, IEEE 802 LMSC  [p.nikolich@ieee.org](mailto:p.nikolich@ieee.org) |
|  | Andrew Myles | Chair, IEEE 802 JTC1 Standing Committee [amyles@cisco.com](mailto:amyles@cisco.com) |
|  | Jodi Haasz | Stakeholder Engagement Liaison, IEEE-SA [j.haasz@ieee.org](mailto:j.haasz@ieee.org) |
| From: | Subir Das | Chair, IEEE 802.21: Media Independent Services  [sdas@vencorelabs.com](mailto:sdas@vencorelabs.com) |

Subject: Liaison reply to China NB comments on the ISO/IEC/IEEE FDIS 8802-21 ballot

Approval: Agreed to at the IEEE 802.21 WG Plenary meeting, Chicago, USA, March 06, 2018

Dear ISO/IEC JTC1 SC 6 Secretariat,

IEEE 802.21 would like to thank the China NB for their review and comments in ISO/IEC/IEEE FDIS 8802-21 ballot as part of the PSDO process. Please find below each comment and the response from the IEEE 802.21 Media Independent Services Working Group.

**China NB Comment CN1-001 on ISO/IEC/IEEE FDIS 8802-21:**

*A protocol based on EAP is designed in ISO/IEC/IEEE FDIS 8802-21 text, and this protocol clearly states to use SHA-256 and AES algorithms as default. However, policy and regulation limitations on application of cryptographic algorithm differ from countries and regions. Therefore, it is improper to specify SHA-256 and AES algorithms as the default ones.*

1 This document solely represents the views of the IEEE 802.21 Working Group, and does not necessarily represent a position of the IEEE, the IEEE Standards Association.

**China NB proposed change 1 on CN1-001**

*It is recommended to clearly state that SHA-256 and AES are examples for algorithms, so that countries and regions may replace it with a similar and regulation-compliant algorithm during implementation.*

# Response from the IEEE 802.21: Media Independent Services Working Group on CN1-001

## The China NB voted “no” in the ISO/IEC/IEEE FDIS 8802-21 due to the default use of algorithms defined in the Standard. For any standardized protocol to be interoperable, it is essential to define the parameters of the algorithms that are mandatory to implement. Towards this goal, IEEE Std 802.21-2017 defines default algorithms for encryption and digital signatures, one for each that are widely accepted by other international standards and also widely deployed in different regulatory, countries and regions. However, other cipher suites are included as options to accommodate the different security requirements. Moving all of them as examples will leave the space for user defined parameters and that will cause huge issues in interoperability. Therefore, IEEE 802.21 WG respectfully disagrees with the China NB’s comment on making SHA-256 and AES as examples instead of default algorithms defined in IEEE Std 802.21-2017.

## 

## IEEE 802.21 Working Group cordially invites the China NB to submit for consideration any

## technical details that support their concerns of improper use of default algorithms.

**China NB Comment CN1-002 on ISO/IEC/IEEE FDIS 8802-21**

*It is clearly stated in ISO/IEC/IEEE FDIS 8802-21 that this standard is implemented with IEEE 802.1X-2010 (please refer to 5.7.4), on which China NB has expressed objection and submitted detailed comments (please refer to 6N15555 etc.). IEEE has acknowledged the receiving of China NB’s comments, but there hasn’t been any technical improvements made on IEEE Std 802.1X and hence the defects still exist.*

# China NB Proposed change on CN1-002:

*It is recommended not to reference the defective standards and to enhance its security mechanism.*

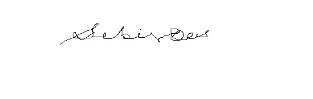
# Response from the IEEE 802.21: Media Independent Services Working Group on CN1

The China NB voted “no” on ISO/IEC/IEEE FDIS 8802-21 ballot due to the reference of IEEE Std 802.1X-2010 in the base IEEE 802.21-2017 standards. The China NB has long-standing concerns related to IEEE Std 802.1X-2010. IEEE 802 has responded to these concerns several times including a recent response to the China NB on IEEE 802.1Q-2014/Cor 1-2015, IEEE 802.1AB-2016, IEEE 802.1Qca-2015, IEEE 802.1Qbv-2015, and IEEE 802.1AC-2016.

Unfortunately, the China NB has not substantiated its concerns about IEEE 802.1X-2010, despite numerous requests from IEEE 802 over many years. IEEE 802.21 Working Group cannot make changes to IEEE 802.21-2017 without substantiation of any alleged issues.

IEEE 802.21 Working Group invites the China NB to submit for consideration any additional technical details, beyond the issues that have already been resolved, that support their concerns.

Sincerely,



Subir Das

Chair, IEEE 802.21: Media Independent Services Working Group