IEEE P802.22
Wireless RANs

|  |
| --- |
| IEEE 802.22b ISO FDIS Ballot Comment Resolutions |
| Date: 2017-11-09 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Apurva Mody | BAE Systems, WhiteSpace Alliance | Chelmsford, MA, USA | +1-404-819-0314 | Apurva.mody@WhiteSpaceAlliance.org  |
|  |  |  |  |  |

Abstract

This document provides the IEEE 802.22b Comment Resolutions to the 802.22b FDIS Ballot that passed, but a response is required.

**IEEE 802.22b ISO/IEC/JTC1 Comments and Resolutions**

**BACKGROUND**

* **IEEE 802.22b 60-day pre-ballot: passed on 3 April 2016. Comments were addressed and resolved**
* **FDIS ballot: passed 27 July 2017 & published with response required**
	+ Passed on 27 July 2017 by 12/1/16 (N16690)
	+ China NB voted “no” with two comments
	+ The ISO/IEC/IEEE standard was published in Oct 2017

**China NB Comment 1**

* + *ISO/IEC/IEEE 8802-22:2015/FDAM 1:2017 is based on IEEE 802.1x. Since the technical concerns China NB proposed in 6N15555 still haven’t been reasonably disposed in this text, China NB has to vote against on this ballot.*

**China NB Request 1**

* + *Recommend not referencing the defective standards or enhancing its security mechanism*

**IEEE 802 response to China NB comment & request 1**

**The China NB has requested that IEEE 802.1X-2010 related descriptions are removed from the text of IEEE 802.22b.**

**IEEE 802 declines to make this change because:**

* + IEEE 802.22b does not contain any IEEE 802.1X-2010 related descriptions
	+ There is no technical justification to remove any IEEE 802.1X-2010 related descriptions from any standard

**While the base IEEE 802.22-2011 specification does reference various IEEE 802.1 specifications including IEEE 802.1X, IEEE 802.22b includes no such references.**

**IEEE 802 recognizes that the China NB has asserted this in past that man-in-the-middle (and other) attacks are possible against IEEE 802.1X based systems. However, the technical details of such an attack (or a demonstration of an attack) have not yet been supplied by the China NB. In the absence of technical substantiation of the claims, there is no justification to remove references to IEEE 802.1X-2010 from any standard**

**China NB Comment 2**

* + *Cryptographic algorithms to be applied to information security mechanism may be subject to national and regional regulations. They should conform to national laws and regulations, and can be chosen according to specific requirements in different countries and regions. Therefore, it is not appropriate for this draft to require the same AES algorithm*

**China NB Change 2**

* + *It is suggested to clearly note that AES is optional. There is no specific implementation solution to establish security mechanism. It is recommended to provide several typical mechanisms in order to better achieve the interconnection between devices*

**IEEE 802 response to Comment 2**

* + The IEEE 802.22b Amendment and the base IEEE 802.22-2010 Standards have proposed the use of AES type of encryption for global coexistence and inter-operability of the devices
	+ Providing for additional ciphers is an excellent idea and the China NB is invited to make suggestions of particular ciphers in the context on-going revision to the IEEE 802.22 Standard.