IEEE P802.11
Wireless LANs

|  |
| --- |
|  Resolution of Comments Received from IEEE 802.11ai ballot in ISO |
| Date: 2017-04-21 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 333 Scott blvdSanta Clara, California, United States of America | +1 408 555 1212 |  |
|  |  |  |  |  |

Abstract

IEEE 802.11ai-2016 was submitted as 6N16545 to ISO/IEC JTC1/SC6 by IEEE 802 for fast-track adoption under the ISO/IEEE PSDO Agreement. The results of the ballot and comments received were presented in document 6N16608.

This submission proposes resolutions to the comments in that document.

The 60-day ballot on IEEE 802.11ai, which was conducted to satisfy the processes of the PSDO agreement between ISO and IEEE-SA, ran from 2017-02-17 to 2017-04-17 and asked the following questions:

1. “Do you support the need for an ISO International Standard on the subject?” and,
2. “Do you support the submission of this proposal for FDIS ballot?”

The results of the ballot were: Q1—9 yes, 1 no, 10 abtain; Q2—9 yes, 1 no, 10 abstain.

The following comments, each marked to be both technical and general, were received and IEEE 802’s proposed resolutions follow.

Comment CN1 001:

*IEEE 802.11ai is the amendment of its base standard IEEE 802.11-2016. China NB has voted against IEEE 802.11-2016 for fast-track adoption as an international standard with detailed comments due to its security problems.*

Proposed resolution:

Reject

IEEE 802.11ai is a stand-alone amendment to the IEEE 802.11-2016 base standard. The China NB’s comment does not address anything in the IEEE 802.11ai amendment that was under ballot and does not propose any change, and is therefore not actionable.

Comment CN2 002:

*IEEE 802.11ai itself has the following security problems:*

*1) In FILS shared key authentication, the shared key is generated between STA and AS and stored in these two devices, the key needs to be delivered by AS to AP through network when Link setup, so, a secure channel should be provided, but the security channel is not specified in the standard, which causes a security risk.*

*2) In FILS public key authentication, Subclause 12.12.1 mentioned that "when FILS Public Key*

*authentication is used, each STA has a means to trust the public key of the other STA", but the*

*standard does not provide specific means on how STA trust public key of other STAs. Furthermore, such means may be difficult to implement in real scenarios, thus will bring a very serious security issues.*

*Based on the above concerns, China votes against IEEE 802.11ai to become an international*

*standard. Such opposition stands until our comments towards the base standard and the standard itself are completely and satisfactorily resolved.*

Proposed IEEE 802 resolution:

Reject

The scope of the IEEE 802.11-2016 base standard, and the IEEE 802.11ai amendment, are the PHY and MAC layers of the OSI network model. As such, the protocols defined in these documents are limited to the PHY and MAC layers. The China NB’s comments refer to definition of protocols defined at higher layers that are outside the scope of the document being balloted.

Specifically:

1. The protocol defining the link between the AP and AS in FILS shared key authentication will involve connections at the network and application layers (and possibly above). FILS is an RSNA protocol and is therefore bound to the existing requirements of RSNA as defined in IEEE 802.11-2016. Section 12.2.6 sub d) explicitly states *“The AP and AS have a trustworthy channel between them that can be used to exchange cryptographic keys without exposure to any intermediate parties.”* Provided the secure channel, established by means outside the scope of the document under ballot, satisfies the requirements in 12.2.6 there is no security issue. Although outside the scope of IEEE 802.11ai, IEEE 802 note that examples of such channels are widely deployed and are considered to satisfy these requirements, such as DIAMETER [RFC 6733] secured by TLS [RFC 5246] or IPsec [RFC 4303] using IKE [RFC 7296]. Also, ISO/IEC 19772:2009 defines an internationally standardized mechanism for key wrapping, and the scope of ISO/DIS 20038 is “*This Standard defines a method for packaging cryptographic keys for storage and transport*.” Given the existence of ISO standards in this area, the notion that transporting a cryptographic key through a trustworthy channel between two mutually authenticated devices is a “*security risk*” is without technical foundation.
2. The establishment of trust in a public key is out of scope of the document under ballot. The public key used in FILS Public key authentication is conveyed using the element described in 9.4.2.181 of IEEE 802.11ai, which refers to documents which can be used to help establish necessary trust. Although outside the scope of IEEE 802.11ai, IEEE 802 note the existence of deployed technology for the establishment of such trust based on a public key infrastructure (PKI) as defined by ISO/IEC 9594-8:2014, with enrollment into a PKI using a technique such as EST (RFC 7030).

The suggestion that opposition to IEEE 802.11ai becoming an ISO/IEC/IEEE standard “*stands until [the China NB’s] comments towards the base standard and the standard itself are completely and satisfactorily resolved*” indicates that the comments are not directed at the document being balloted. Therefore, there are no changes that can be made to IEEE 802.11ai to satisfactorily resolve China NB’s comments.

**References:**