IEEE P802.11
Wireless LANs

|  |
| --- |
|  Resolution of Comment Received from CN NB on Resolution to Comment received from CN NB on IEEE 802.11ai errata ISO ballot |
| Date: 2019-01-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 3333 Scott blvdSanta Clara, California, United States of America | +1 408 555 1212 |  |
|  |  |  |  |  |

Abstract

Errata for IEEE 802.11ai-2016 was submitted to ISO/IEC JTC1/SC6 by IEEE 802 for fast-track adoption under the ISO/IEEE PSDO Agreement as 6N16663. The results of the ballot and the single comment (CN1) received were presented in document 6N16697. A response was made as 6N16725. The Chinese NB has commented (CN2) on the IEEE 802’s resolution of their single comment (CN1)

This submission proposes resolutions to the new comment as well as restates the original comment and the resolution the Chinese NB now objects to.

The 60-day ballot on the errata to IEEE 802.11ai, which was conducted to satisfy the processes of the PSDO agreement between ISO and IEEE-SA, ran from 2017-07-04 to 2017-09-01 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 second printing, which the errata has been reflected, as an IS?”

The results of the ballot were: Q1—9 yes, 1 no, 11 abtain; Q2—9 yes, 1 no, 11 abstain.

The following multi-part comment, marked both technical and general, was received and IEEE 802’s proposed resolutions follow.

Comment CN1:

*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. 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.*

Proposed IEEE 802 resolution:

Reject

The scope of the IEEE 802.11-2016 base standard, and the IEEE 802.11ai amendment including its errata, 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 need for protocols defined at higher layers that are outside the scope of the document being balloted. The need for additional higher layer protocols that are defined outside the scope of the document being balloted do not amount to “*security problems*” because numerous examples of suitable protocols exist.

Specifically:

1. The document under ballot does not need to specify the protocol used to securely transfer the shared key from the AS to the AP, it only needs to state the requirements such a protocol would have. 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 problem.

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]. Any of these can be used with FILS Shared Key Authentication to create the trustworthy channel through which cryptographic keys can be exchanged.

1. The document under ballot does not need to specify the means by which trust can be obtained in a public key, it just needs to mandate that trust in the public key exist prior to initiating FILS Public Key Authentication.

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 widely 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 techniques such as EST (RFC 7030) or CMC (RFC 5272).

That resolution was presented to ISO/IEC/JTC1/SC6 as 6N16725. Subsequently, the Chinese NB objected to the resolution of CN1 and have created a new comment, CN2.

Comment CN2:

*IEEE 802.11 WG rejected CN1 and provided reasons in 6N16725. The given reasons in 6N16725 are untenable and these topics are not out of scope, because:*

*1) The amendment does not specify specific specifications or give the referred protocols for use in a trustworthy channel, which will not guarantee security and interoperability in product implementation.*

*2) The amendment does not specify the means by which trust can be obtained, however, this is an important part in authentication and key establishment. Besides, when STA (not an AP) could not get connected to the Internet, it is difficult for PKI system to accomplish authentication and establish necessary trust. Therefore, the situation will lead to difficulty in product design and implementation.*

Proposed IEEE 802 resolution:

 Reject

The IEEE 802 restates the eminently tenable reasons that CN1 was rejected, primarily that the comments refer to protocols which are out of scope of ISO/IEC 8802-11 because they do not reside in the PHY or MAC layers. The two portions of CN2 are specifically addressed.

1. The amendment specifies requirements on protocols that can transfer a shared key from an AS to an AP. Any protocol that satisfies these requirements would be satisfactory. Contrary to the allegations made by the CN NB, interoperability of the FILS Shared Key protocol is not affected by stating these requirements because ISO/IEC 8802-11 specifies the over-the-air protocol only.

For example, assume that protocol1 and protocol2 are different and both satisfy the requirements stated in the amendment. Further assume that AP1 complies with the amendment and uses protocol1 to communicate with the AS and AP2 complies with the amendment uses protocol2 to communicate with the AS. A STA that complies with the amendment would be able to connect to AP1 and AP2 without problem. The fact that protocol1 and protocol2 are different has no impact on the protocol defined in the amendment. In fact, the STA would not even be aware that different protocols are being used by AP1 and AP2 to communicate with the AS.

1. The IEEE 802 provided the CN NB with several examples of protocols that can be used to establish trust in a public key. There is no difficulty in product design or implementation because the example protocols are well-defined and widely implemented. This is analogous to the CN NB’s old WAPI proposal which similarly used trusted public keys but did not specify how the ASUE and AE obtained these certificates nor did it specify how the ASU determined that the two certificates were trusted or not.

For example, assume that the AP uses SCEP to enroll in a Certification Authority and receive a certificate with its public key from the CA. Further assume STA1 uses EST to enroll in the same CA and to receive a certificate with its public key and that STA2 uses CMC to enroll in the same CA and to receive a certificate with its public key. Once enrolled, both STA1 and STA2 can establish secure and authenticated connections with the AP using FILS Public Key Authenticaiton. The fact that STA1 and STA2 obtained their certificates from the CA in a different manner, and furthermore that each of those manners differed from the way the AP obtained its certificate from the CA, has no impact on interoperability. The AP has no way of knowing how STA1 and STA2 obtained their certificates nor does it care because it is irrelevant.

**References:**