IEEE 802/802.11 Working Group Response to ISO/IEC/IEEE FDIS 8802-11 Ballot comments

TO:

- Mr. Jungyup OH, Committee Manager ISO/IEC JTC1/SC6

CC:

- Dr Hyun Kook Kahng, Chair ISO/IEC JTC1/SC6, kahng@korea.ac.kr
- Dr Zhenhai Huang, Convenor ISO/IEC JTC1/SC6 WG1, zhenhai.huang@iwncomm.com
- Jodi Haasz, IEEE, j.haasz@ieee.org
- Konstantinos Karachalios, IEEE-SA Standards Board, Secretary, IEEE-SA Board of Governors sasecretary@ieee.org
- Paul Nikolich, IEEE 802 chair, p.nikolich@ieee.org
- Jon Rosdahl, Vice-chair, IEEE 802.11 WLAN Working Group jrosdahl@ieee.org
- Robert Stacey, IEEE 802.11 Vice Chair, IEEE 802.11 WLAN Working Group robert.stacey@intel.com
- Andrew Myles, Chair, IEEE 802 JTC1/SC6 Standing Committee, amyles@cisco.com

SUBJECT: IEEE 802/802.11 Working Group Response to ISO/IEC/IEEE FDIS 8802-11 Ballot comments

DATE: 2022-08-11

Dear Mr. Jungyup OH,

The attachment below contains the IEEE 802/802.11 WG approved responses to the FDIS Ballot comments on ISO/IEC/IEEE 8802-2020 from the China National Body.

Please contact me with any questions.

Yours sincerely,

/s/

Dorothy Stanley
Chair, IEEE 802.11 Working Group
dstanley@ieee.org

ATTACHMENT 1: FDIS Ballot comment responses

ATTACHMENT 1: 8802-2020 FDIS Ballot comments and responses

CN1

Comment:

IEEE 802.11-2020 is based on IEEE Std 802.11-2016, into which the following amendments have been incorporated:

— IEEE Std 802.11ai™-2016 (second printing): Fast Initial Link Setup (Amendment 1)

— IEEE Std 802.11ah™-2016: Sub 1 GHz License Exempt Operation (Amendment 2)

— IEEE Std 802.11aj™-2018: Enhancements for Very High Throughput to Support Chinese Millimeter Wave Frequency Bands (60 GHz and 45 GHz) (Amendment 3)

— IEEE Std 802.11ak™-2018: Enhancements for Transit Links Within Bridged Networks

(Amendment 4)

— IEEE Std 802.11aq™-2018: Preassociation Discovery (Amendment 5).

The China National Body voted against and made technical comments on IEEE 802.11-2016 and its amendments in the past, see detailed comments in 6N15494, 6N16794, 6N16982, 6N16983, 6N17204, 6N17205 and 6N17208.

It is good to see some comments are acknowledged and revised accordingly, but is should be noticed that security methods specified by this proposal still have many technical weaknesses to be addressed and security defects that cause serious concern. For instance, WEP and TKIP, which should not be used in WLAN because of their weak and well-known security defects, are still reserved in pre-RSNA and RSNA security (though some statements in this proposal have indicated that they are unsuitable).

Proposed Change:

None

Discussion:

WEP and TKIP must not be used. For that reason they are deprecated and, in the case of WEP, obsoleted. As noted, they are unsuitable for use by the standard. They remain *reserved* simply because the identifiers that have been allocated for them cannot go away nor can they be reused by different protocols. Keeping them as reserved, and thereby unavailable, is the way deprecated and obsolete protocols are handled.

The comment has no proposed change. It mentions “many technical weaknesses” but only lists WEP and TKIP. Since these protocols have already been deprecated and obsoleted there is no other work to be done. The comment suggests further work to be done but does not suggest what that could be.

Proposed Resolution:

Reject, the identified protocols which suffer from technical weaknesses have already been rendered unsuitable for the standard and cannot be used by a compliant implementation.

CN2

Comment:

Recently, Mathy Vanhoef published a paper “Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation” in USENIX Security Symposium. *(It’s free for downloading from the Internet.)*

This paper presents three design flaws in the 802.11standard that under pins Wi-Fi. One design flaw is in the frame aggregation functionality, and another two are in the frame fragmentation functionality. These design flaws enable an adversary to forge encrypted frames in various ways, which in turn enables exfiltration of sensitive data. They also discovered common implementation flaws related to aggregation and fragmentation, which further worsen the impact of our attacks. The author concluded that their results affect all protected Wi-Fi networks (IEEE 802.11 compliant), ranging from WEP all the way to WPA3, meaning the discovered flaw shave been part of IEEE 802.11 since its release in 1997.

Proposed Change:

It is recommended to postpone the subsequent ballot on IEEE 802.11 in ISO until the discovered design flaws are sufficiently studied and resolved.

Discussion:

The implementation flaws in the paper highlighted the fact that the 802.11 standard already included ways to protect A-MSDU flags, but the defined mechanisms were not widely implemented.

The other attacks identified in the paper have been acknowledged and resolutions incorporated into the next revision of the 802.11 standard, currently under development (see submission 11-21/0816, co-authored by Mathy Vanhoef).

Proposed Resolution:

Reject. Since the discovered design flaws have already been studied and are addressed in IEEE Std 802.11-2020 and P802.11REVme D1.0, there is no need to postpone subsequent ballots on IEEE 802.11 in ISO.

CN3

Comment:

If a standard has been published as an international standard, the normative references should use the title of the international standard.

Proposed Change:

Change all IEEE standards to ISO/IEC/IEEE standard if they have been published.

Discussion:

ISO/IEC/IEEE FDIS 8802-11 is the adoption of an IEEE standard; as such, it is appropriate that an IEEE standard reference other IEEE standards.

Proposed Resolution:

Reject. As IEEE Std 802.11-2020 is an IEEE standard, it is appropriate to reference other IEEE standards. In addition, the standards referenced were developed and published by IEEE. While many were adopted by ISO under the ISO/IEEE PSDO Agreement, the ISO/IEC version of an IEEE standard does not supercede the IEEE published version.

CN4

Comment:

Pairwise Master Key (PMK) is an important security element, but it has to be transported from the authentication server to the access point, which will result in security risk of PMK.

Proposed Change:

The PMK is suggested to be created at AP and STA to avoid security problem in transmission.

Discussion:

An authentication server is not a mandatory part of an 802.11 system. Many authentication and key management (AKM) suites, like SAE and FILS public key authentication that generate PMKs already generate them on the AP and STA. Even AKMs that support the use of an optional authentication server can generate the PMK on the AP and STA—e.g. using IEEE Std 802.1X with an EAP method of EAP-TLS wherein both the AP and STA possess certificates (which can be properly validated) and corresponding private keys.

Proposed Resolution:

Reject. There is no change necessary to the standard as it already supports generation of a PMK without the use of an authentication server.

CN5

Comment:

Devoid of real mutual authentication.

Though IEEE 802.11 assumes a mutual authentication between an authentication server and a station, the authenticated identities of the access point and the station are not known by each other. For example, in the EAP-TLS protocol, authentication by certificate happens between the client and server. So extra secure channels are needed to be negotiated between AP and server to notify AP the result of authentication and the secure parameter PMK. Also, the AAA protocol, which is necessary to this proposal, cannot guarantee the security of key delivery from the authentication server to the access point. So, the forgery attack against the access point or the station is possible.

Proposed Change:

The AP shall have an independent identity. Both a non-AP STA and AP shall authenticate each other directly.

Discussion:

The use of an authentication server is optional for an 802.11 deployment. Therefore, the IEEE 802.11 standard does not assume its presence, let alone require a mutually authenticated state with one. Similarly, a AAA protocol cannot be necessary since an authentication server is not required.

The comment references EAP-TLS as an example. With EAP-TLS, both the non-AP STA and AP can be deployed with certificates (which can be properly validated) and corresponding private keys (this is similar to the only way that WAPI can be deployed). In this case, EAP-TLS will be performed without the use of an authentication server and without the need for “extra secure channels”.

The comment states that the standard is “devoid of real mutual authentication” but does not say what is “real” authentication or what could be “fake” authentication. In any event, strong cryptographic mutual authentication between the non-AP STA and AP is possible using any of the defined AKMs in 802.11.

When an authentication server is used and a AAA protocol is used, the standard explicitly lists the requirements necessary to protect communication between the AP and authentication server. If those requirements are met, a forgery attack against the access point or station is not possible. On the other hand, if those requirements are not met then the implementation is not compliant with the standard.

Proposed Resolution:

Reject. The standard already has the ability to mutually authenticate the non-AP STA and AP directly. Every defined AKM that supports PMK generation supports this deployment.

When an authentication server is used and an AAA protocol is used, the standard explicitly lists the requirements necessary to protect communication between the AP and authentication server. If those requirements are met, a forgery attack against the access point or station is not possible. On the other hand, if those requirements are not met then the implementation is not compliant with the standard.

CN6 and CN7

CN6 Comment:

The authentication protocol is not specified. It just provides an authentication framework 802.1X EAP, but there are no detailed methods. It will result in compatibility issue.

CN6 Proposed Change:

The response in SC6N16812 is noticed, but the reply did not solve the authentication issue in this comment. The authentication protocol shall be re-designed in order to resolve the issue.

CN7 Comment:

There are many different EAP-based protocols for WLAN specified by IETF drafts, such as EAP-TLS, EAP-MD5 EAP-TTLS, EAP-PEAP, and so on. The security of each 802.1X-EAP protocol is another problem which shall be noted. Furthermore, there are many methods for breaking up 802.1X-EAP protocols in the internet like MITM attack. They have to be implemented for interoperability and then make conformance difficult and management complex.

CN7 Proposed Change:

The response in SC6N16812 is noticed, but the reply did not solve the authentication issue in this comment. The authentication protocol shall be re-designed in order to resolve the issue.

Discussion for both CN6 and CN7:

There is nothing to solve. There is an existence proof that leaving the specific protocol outside the scope of the IEEE 802.11 standard does not result in a compatibility issue, and that is that there is widespread deployment of devices around the world using IEEE 802.11 and they negotiate the specific protocol to use for network access appropriate with the credential assigned to the client.

The IEEE 802.1X standard can be used with any ***compliant*** EAP method. The 802.11 standard imposes requirements on those EAP methods to ensure they provide mutual authentication. Any EAP method that was susceptible to “breaking up” in the form of a MITM attack would not satisfy that requirement. There is no requirement to implement all EAP methods, much less EAP methods susceptible to attack. EAP already provides a way to negotiate through a series of supported methods in order for the supplicant and authenticator to agree on a method and this has proven to be useful in practice.

It is true that EAP methods must be implemented for interoperability but in practice this has not been shown to “make conformance difficult” nor has it made “management complex.” On the contrary, the IEEE 802.11 standard using the IEEE 802.1X standard has been deployed around the world in large networks and small, something we would not see if it was complex and difficult to deploy.

There is no compatibility issue and the world-wide deployment of IEEE 802.11 using IEEE 802.1X and a wide variety of EAP methods underscores this fact.

Proposed Resolution for both CN6 and CN7:

Reject. There is no compatibility issue and no change is needed to the standard.

CN8

Comment:

The 4-way handshake protocol described in IEEE 802.11 is incomplete. When Supplicant receives message 3 and sends message 4, its controlled port is open, but the controlled port of Authenticator is still closed. If message 4 isn't received by Authenticator, then the port statuses of both sides are not the same. The loss of msg.4 will result in the loss of synchrony of peers and the failure of 4-way handshake protocol, even though it doesn't include security issues. Because the retransmit of msg.3 in plaintext is not accepted by the station which has unblocked the control port and expected the cipher text.

Proposed Change:

The mechanism shall be re-designed in order to resolve the issue.

The response in SC6N17600 said "Revised, this issue has been accepted as a work item of the TGme maintenance group and is being addressed by the IEEE 802.11 Working Group through the normal maintenance process in IEEE 802.11. It is agreed that there are no security concerns associated with this issue.", but new submitted version doesn't show any improvement conforming to the above statement.

Discussion:

The problem mentioned in the comment has been acknowledged and the IEEE 802.11 Working Group is working on the matter. When the ballot resolution process for P802.11REVme has finished, resulting in the next version of the 802.11 standard, that standard will subsequently be sent to ISO/IEC JTC1/SC6 under the PSDO process, and the issue will be resolved.

Proposed Resolution:

Revised, this issue has been accepted as a work item of the IEEE 802.11 Working Group through the normal maintenance process in the IEEE 802.11 Working Group. It is agreed that there are no security concerns associated with this issue.

CN9

Comment:

Though PMK can be delivered through an additional secure channel, the details of the secure channel are not specified in this proposal. This does not guarantee security of secure channels. Besides, every AP should establish a secure channel with the authentication server before supplying services to clients. This complicates the configuration of network and limits the expansibility and flexibility of users, especially for large-scale networks.

Proposed Change:

The secure channel is an important factor in the authentication procedure in this proposal. How to establish the secure channel shall be clearly specified in this proposal to ensure the feasibility and compatibility.

Discussion:

There is no requirement in ISO/IEC/IEEE FDIS 8802-11 to transmit a PMK from an authentication server to the Authenticator. The comment is correct that a PMK “can be delivered through an additional secure channel”, but it is not required to do so. An external AS is an optional enhancement for authentication credentials that are more suited to central management, for instance using username/password credentials.

Techniques in the standard to derive a PMK on both the non-AP STA and AP/Authenticator without the use of an authentication server include:

1. The SAE protocol which describes a way to derive a PMK between non-AP STA and AP using a zero knowledge proof authenticated with a simple password.
2. The Fast Initial Link Setup (FILS) protocol, part of IEEE Std 802.11-2020, includes the ability to establish a PMK as the result of a Diffie-Hellman key exchange between non-AP STA and AP authenticated using either X.509 certificates or raw public keys.
3. Terminating the EAP exchange directly on the AP/Authenticator and deriving a PMK there.

Proposed Resolution:

Reject. Since ISO/IEC/IEEE FDIS 8802-11 is restricted to the PHY and MAC layers of the OSI model, description of communication between the Authenticator and a centrally-managed authentication server is out of the scope of the standard.

While such a protocol is out of scope, section 4.10.6 of ISO/IEC/IEEE FDIS 8802-11 clearly describes the requirements placed on the Authenticator-to-AS protocol if a deployment wishes to use one.

- The first two are “[m]utual authentication between the Authenticator and the AS” and “[a] channel for the Supplicant/AS authentication.” Suitable protocols to satisfy these requirements are listed in 4.10.6 as RFC 2865 (RADIUS) and RFC 3588 (Diameter) with further discussion in section 12.7.1.3.
- The final requirement is “[t]he ability to pass the generated key from the AS to the Authenticator in a manner that provides authentication of the key source, preserves integrity of the key transfer, and preserves data confidentiality of the key from all other parties.” A suitable technique to ensure the confidentiality and integrity of the key as well as an authenticated key transfer is using either one of the aforementioned protocols with RFC 6218 attributes and ISO 20038-2017 Key Wrapping using AES.

CN10

Comment:

Figure 4-37—Example using IEEE 802.1X authentication operates the authentication procedure depending on over 20 messages exchange. It is much too complex and time-consuming, and should be improved.

Proposed Change:

The response in SC6N16812 is noticed, but the reply did not solve the raised concerns. The authentication protocol shall be re-designed in order to resolve the issue.

Discussion:

It is not clear where “over 20 messages” came from. The EAP method defined in RFC 5931 satisfies the requirements ISO/IEC/IEEE FDIS 8802-11 places on EAP methods and uses 6 messages.

In addition, the Fast Initial Link Setup (FILS), part of the IEEE 802.11 standard that was balloted, performs a Diffie-Hellman key exchange, authenticated with digital signatures, and generates traffic encryption keys all in just 4 messages total, including the 802.11 Authentication and 802.11 Association frames.

Proposed Resolution:

Reject. There is no issue to resolve. If the total number of messages used to authenticate presents a problem, there are other EAP methods to use (e.g. RFC 5931) and other AKMs (e.g. FILS public key authentication) to use to address that problem. There is no requirement in the standard to use 20 messages to authenticate with the IEEE 802.1X standard.

CN11 and CN12

CN11 Comment:

It's glad to see statements in12.2.1*"WEP is obsolete. The WEP algorithm is unsuitable for the purposes of this standard."*

But WEP security mechanism is reserved in 12.3.2 and all known WEP security defects still exist. Products conformed to IEEE 802.11 may use WEP mechanism which will result in the loss of security. In addition, the security of the system applying higher security mechanism will be actually downgraded in the mixed environment which allows the multiple security mechanisms to coexist. So TKIP and AES-CCMP cannot protect the traffic as expected in this case. The security level of the whole system will be downgraded.

CN11 Proposed Change:

SC6N16812 explained that "IEEE 802.11 includes deprecated protocols for historical reasons". This does not clearly explain why WEP needs to be still reserved, since it has been acknowledged and agreed of "*both WEP and TKIP are vulnerable to attack*".

WEP shall be removed from this proposal.

CN12 Comment:

It's glad to see statements in12.2.1 *"The use of TKIP is deprecated. The TKIP algorithm is unsuitable for the purposes of this standard."*

However, TKIP is still reserved in this proposal and it introduces denial of service attack. TKIP uses Message Integrity Code (MIC) called Michael to detect forgery attempts. Only 2^{20} security can be provided by the MIC. So the countermeasure, which means that if two invalid messages are detected within one minute (i.e. evidence of active attack) then the network will be shut down for one minute, is adopted to fill up the security loophole. Thus, if the attacker continually transmits two invalid messages every minute, the whole network is not available and DoS attack is easily launched.

CN12 Proposed Change:

SC6N16812 explained that "IEEE 802.11 includes deprecated protocols for historical reasons". This does not clearly explain why TKIP needs to be still reserved, since it has been acknowledged and agreed of "*both WEP and TKIP are vulnerable to attack*".

TKIP shall be removed from this proposal.

Discussion for both CN11 and CN12:

It is not possible to go back in time to prevent WEP or TKIP from ever being proposed. They were proposed and they were adopted. Their code points were allocated.

The comment states that "Products conformed to IEEE 802.11 may use WEP mechanisms" and that "if the attacker continually transmits two invalid messages every minute, the whole network is not available and DoS attack is easily launched". This is incorrect since WEP has been obsoleted and TKIP has been deprecated. Any implementation of IEEE Std. 802.11-2020, the document on which the comment was made, would not implement WEP or TKIP and, therefore, no attack using those protocols is possible

IEEE 802.11 cannot prevent implementations from claiming conformance to past versions of the standard which included WEP, all it can (and did) do is disallow WEP going forward.

Since WEP and TKIP were defined, the identifiers in the standard that they used have been allocated and those allocations cannot simply vanish. The way technology is deprecated is to render its use invalid. To identify the invalid use requires retaining the identifiers of the invalid technology. That is why these identifiers cannot be removed from the proposal.

Proposed Resolution for both CN11 and CN12:

Reject. The identifiers that WEP and TKIP have consumed as part of its definition cannot merely go away. They must be reserved to prevent their use going forward. The use of WEP and TKIP is prohibited.

CN13

Comment:

Transition security network (TSN) allows the creation of pre-robust security network associations (pre-RSNAs) as well as RSNAs. Beacon frames have to specify WEP as the group cipher suite in RSNE, so that pre-RSNA STAs can coexist with RSNA STAs in a BSS. Similarly, pre-RSNA STAs ignore RSNE in beacon frames, thus RSNA STAs have to use TKIP as the pairwise cipher suite and WEP for authentication in an IBSS. Due to the weakness of the WEP technology, even the CCMP, GCMP security technologies will be attacked successfully and easily.

Proposed Change:

The reply in SC6N16812 "*it is acknowledged and agreed that both WEP and TKIP are vulnerable to attack and that using either one of them, or the TSN mechanism, would result in a compromise of network security."* was noticed. This mechanism should be removed from the text.

Discussion:

Neither WEP nor TKIP is suitable for use in IEEE 802.11 and compliant implementations shall not use them. Therefore, there is no possible attack from their use on a device that complies with IEEE Std 802.11-2020. There is certainly no "easy" attack on CCMP and GCMP and none is described in the comment.

Proposed Resolution:

Reject, protocols that shall not be used will not result in security issues. The comment concerning attack on CCMP and/or GCMP is unsupported.

CN14

Comment:

CCMP/GCMP/BIP are mandatorily based on AES encryption algorithm without other options.

Actually, a cryptographic algorithm is one module of a security protocol, and it is usually used in the security protocol. The security protocol and cryptographic algorithm is relatively independent, and the security protocol is applicable to multiple different cryptographic algorithms. Cryptographic algorithms are only adoptable modules, and which algorithm to be applied is subject to the user's requirement and national/regional laws and regulations.

But in this proposal, only AES is specified. That's to say, the compliance to the proposal is being bound by using AES. It causes the neglect of other nations' interests and makes the proposal not applicable in different nations.

In fact, In 2006, the comment disposition of ISO/IEC 8802-11/Amd6 (6N13082Rev1, 6N13082Rev2, 6N13142) once accepted the similar comment by changing the text to "*CCMP is instantiated in this standard with the Advanced Encryption Standard (AES). CCMP can be instantiated with any other 128-bit block cipher by defining a new ciphersuite.*" There is no clue why such descriptions are not reserved.

Proposed Change:

This proposal should negotiate encryption modes and encryption algorithms respectively in cipher suites.

Noting that in **TMB Resolution 70/2018** (72nd meeting of the Technical Management Board) regarding Legal statements in ISO deliverables,

•text relating to compliance with contractual obligations, legal requirements and government regulations exists in many ISO standards; and

•ISO deliverables can be used to complement such requirements and serve as useful tools for all related stakeholders (which can include government authorities and industry players);

ISO clarifies that, for all ISO deliverables:

a) Statements that include an explicit requirement or recommendation to comply with ***any specific law, regulation or contract*** *(****such as a normative reference to such requirements****), or portion thereof, are* ***not*** *permitted;*

b) ***Statements related to legal and regulatory requirements that do not violate point a) are permitted****;*

It is then suggested that the text shall make it clear that "Cryptographic algorithms to be applied to information security mechanism may be subject to national and regional regulations. In this standard, cryptographic algorithms are instantiated with AES, and they can be instantiated with any other cipher suite according to requirements in different countries and regions."

Discussion:

AES is specified as the mandatory-to-implement encryption algorithm in order to provide a minimum for universal interoperability, an important feature of a worldwide standard. If there's an interest in specifying other cryptographic algorithms in addition to AES, this can be done within the context of IEEE 802.11 revisions developed within the IEEE 802.11 Working Group. These ciphers must, naturally, offer comparable security to existing IEEE 802.11 ciphers.

We further note that AES is specified in ISO/IEC 18033-3:2010, "Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers". As a design of Belgian cryptographers, it has seen specification in many international standards from multiple Standards Development Organizations. The use of AES within IEEE Std 802.11 is not a legal requirement. All IEEE 802.11 specifications are de jure standards with their implementation and use a matter of convention and market acceptance. The cited text from TMB Resolution 70/2018 is not applicable as the use of encryption technologies within IEEE Std 802.11 is not driven by any specific law, regulation, or contract.

Proposed Resolution:

Reject, there is no actionable change that can be made. There is a process to add new cipher suites and if the China National Body wishes to follow that process then new cipher suites can be assigned for their ciphers. IEEE 802.11 again repeats its offer to have representatives of the China National Body attend an upcoming IEEE 802.11 meeting and present their proposals for new ciphers.

CN15

Comment:

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. Therefore, a secure channel should be provided, otherwise security risks will raise.

Proposed Change:

The text should specify specific specifications or give the referred protocols for use in a trustworthy channel to guarantee security and interoperability in product implementation.

Discussion:

The scope of IEEE Std 802.11-2020, the document that was balloted, is the PHY and MAC layers of the OSI network model. As such, the protocols defined in this document is limited to the PHY and MAC layers. The comment refers to the need for protocols defined at higher layers that are outside the scope of the document that was 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.

FILS is an RSNA protocol and is therefore bound to the existing requirements of RSNA as defined in IEEE Std 802.11-2020 which 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 these requirements, there is no security problem.

For instance, although outside the scope of IEEE 802.11, IEEE 802 note that examples of such channels are widely deployed and are considered to satisfy the requirements that IEEE 802.11 places on them, 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.

Proposed Resolution:

Reject. The proposed change is outside the scope of the document that was balloted. Requirements on protocols to establish a “trustworthy channel” are given and any protocol that satisfies them can be used.

CN16

Comment:

In FILS public key authentication, Subclause 12.11.1 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. The text 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 Change:

It is necessary to specify how trust can be obtained.

Discussion:

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 identified using the element described in 9.4.2.182 of IEEE Std 802.11-2020. Trust in that public key is obtained in a manner outside the scope of IEEE Std 802.11-2020. Although outside the scope, IEEE 802 notes 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). Furthermore, standard techniques like OCSP (RFC 6960) can help address the mentioned difficulty in validating public keys.

Proposed Resolution:

Reject. The balloted document must mandate that trust in the public key exist prior to initiating FILS Public Key Authentication. Specifics of how to trust a public key are outside the scope of the balloted document.

Widely deployed technology exists 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). Furthermore, standardized techniques like OCSP (RFC 6960) can help address the mentioned difficulty in validating public keys.

CN17

Comment:

Regarding to the sentence “The RSN operations in a CMMG BSS shall be the same as the RSN operations in a DMG BSS.”, in the response to 60-day ballot comments on IEEE 802.11aj, IEEE 802.11 Working Group has replied that ISO/IEC/IEEE 8802-11 defines a default security mechanism for the purposes of interoperability, but implementers are always free to define and use additional methods.

It is welcome for the statement. Accordingly, it is proposed to make this clearer in the text, because currently there is no such clue that other mechanisms can be used by implementers freely.

Proposed Change:

To solve the concerns raised by this sentence, it is proposed to change as following:

The security operations in a CMMG BSS can be the same as the security operations in a DMG BSS. Other security methods and cryptographic algorithms that are defined in ISO/IEC international standards or local regulations can be implemented in a CMMG BSS.

Or

Delete the sentence.

Discussion:

It’s not clear how deleting the sentence would address a concern over adding new security methods.

The security in IEEE Std 802.11-2020 is defined to be RSN and any additional security methods that get added to IEEE 802.11 will, likewise, be RSN. Substituting “security” for “RSN” does not open up the standard to new cryptographic algorithms as the commenters appear to believe. The standard can already be amended to include new security methods and cryptographic algorithms.

Proposed Resolution:

Reject. The sentence is not problematic and the proposed change is not appropriate. IEEE 802.11 again repeats its offer to have representatives of the China National Body come to an upcoming IEEE 802.11 meeting and present their proposals for new security methods and/or cryptographic algorithms.

CN18

Comment:

URN used in this proposal is not recommended for using in ISO standards.

Proposed Change:

Use OID to manage the resources those involved in the proposal, since OID is an international standard and it is well recognized.

Discussion:

This is a duplicate comment from the previous round of balloting (6N16794) which was rejected. No additional rationale is provided.

Proposed Resolution:

Reject. Many of the mentioned identifiers are specific to ISO/IEC/IEEE 8802-11 and are managed by the IEEE 802.11 Assigned Numbers Authority. When extensibility is desired, OUIs are already used. For example, the specification of cipher suites, authentication and key management suites, and key data encapsulations allow for external organizations to use an assigned OUI to manage resources.

References:

SC6_CN_01_175_China_NB_comments_on_ISO_IEC_IEEE_FDIS_8802-11

11-19-0062-01-0jtc-resolution-of-comments-received-from-china-nb-during-fdis-ballot-on-ieee-802-11ai

11-21-1039-03-000m-resolution-of-cnb-fdis-comments