IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution of China National Body CIBs |
| Date: 2021-07-01 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Abstract

The Chinese National Body made several comments during the PSDO process in ISO to advance the 11md draft to an international standard. This submission proposes resolutions to those comments.

**CN1**

Comment: “China 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:

Discussion: The CNB does not propose any change, which makes comment resolution difficult to achieve. It is noted that the previous detailed comments they mention are repeated here—6N15494 is repeated by CN4, CN5, CN8, CN9, CN10, CN11, and CN12; 6N16794 is repeated by CN4, CN5, CN7, CN8, CN11, CN12, CN13, CN14, and CN18; CN16982 is repeated by CN15 and CN16; 6N17204 is repeated by CN17; 6N17205 is repeated by CN14; and, 6N17208 is repeated by CN14. Therefore, this comment will be marked as a duplicate of the other comments submitted in this ballot.

Proposed Resolution: duplicate of CN4, CN5, CN6, CN7, CN8, CN9, CN10, CN11, CN12, CN13, CN14, CN15, CN16, CN17, and CN18.

**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 flaws have 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 attacks mentioned in the paper are “implementation flaws”. These include not checking consecutive packet numbers, mixing plaintext and encrypted fragments, processing broadcast fragments, forwarding EAPoL frames, treating fragments as full frames, and failure to verify the integrity of a fully reconstructed frame (when using the obsoleted protocol TKIP). While there is always room for improvement of a standard to further clarify some behavior to ensure implementations are robust, the comment does not recommend anything other than postponing standardization of the draft and that is not an appropriate response to this paper.

The paper also addressed the unauthenticated A-MSDU flag in a QoS header. IEEE Std 802.11-2020 already provides for a way to authenticate the A-MSDU flag in a QoS header, the problem is that few implementations implemented it. Again, the appropriate response to this paper is for implementations to follow the standard, not to delay adopting of the standard.

The current maintenance task group, TGme, is currently discussing proposed changes to the standard to explicitly define proper behavior vis-à-vis fragmentation to help ensure implementations do the right thing. That is the proper procedure.

Proposed Resolution: Reject. The proposed change would not address any problem. The issues in the paper have been studied and determined to be implementation issues and not design flaws in the standard. There is a parallel effort in TGme to provide implementation guidance concerning fragmenting A-MSDUs, not forwarding EAPoL frames, not combining encrypted and unencrypted fragments or fragments encrypted with different keys, requiring consecutive packet numbers, etc. This effort will ensure that the fragmentation issues associated with implementations discussed in the referenced paper are completely addressed.

**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: The standard is developed by IEEE and it therefore refers to IEEE standards.

Proposed Resolution: As IEEE 802.11-2020 is an IEEE standard, it is appropriate to reference IEEE standards.  In addition, the standards referenced were developed and published by IEEE and many were adopted by ISO under the ISO/IEEE PSDO Agreement.

**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: The PMK is not required to be transported from an external authentication server to an access point. The use of a separate authentication server is an optimization for certain deployments and the authentication server is a logical entity which can be coincident with the access point. The PMK can be generated on the access point without the use of an authentication server if EAP-TLS is used and both the client and access point use certificates (in the same sort of use case that WAPI addresses).

As stated in 6N16812, techniques in the standard to derive a PMK on both the STA and AP/Authenticator include:

1. The SAE protocol (section 12.4) which describes a way to derive a PMK between STA and AP using a zero knowledge proof authenticated with a simple password.
2. The Fast Initial Link Setup (FILS) protocol, which amends ISO/IEC/IEEE 8802-2016 and has been adopted under the ISO/IEEE PSDO agreement, includes the ability to establish a PMK as the result of a Diffie-Hellman key exchange between STA and AP that is 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. To use the example from comment CN3 [per 6N16812], EAP-TLS using certificates could easily be terminated on the Authenticator without requiring an external Authentication Server.

So the statement that a PMK “has to be transported from the authentication server to the access point” is incorrect.

Proposed Resolution: Reject. The PMK can already be created by the AP and STA directly and no transmission of the PMK is required. There are no security problems in that case. Transmission of a PMK by an authentication server is an optional optimization for certain use cases which is supported by, but not required by, IEEE Std 802.11-2020.

**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: IEEE 802.11 does not assume the use of an external authentication server. That is an optimization for certain use cases. The AS is a logical entity which can be coincident with the AP. Real mutual authentication with separate identities is supported when both parties use certificates and authenticate with EAP-TLS (the same use case that WAPI addresses) or when they use SAE with password identifiers. A AAA protocol is not necessary.

As stated in 6N16812, since ISO/IEC/IEEE 8802-11 is restricted to 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 8802-11 clearly describes the requirements placed on the Authenticator-to-AS protocol if a deployment requires 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.

Proposed Resolution: Reject. Real mutual authentication is supported. There is no requirement to use a AAA protocol.

**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.”

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: There is an existance 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 are billions of devices deployed 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. 6N16812 did not “solve the authentication issue” because there is no issue to solve. This is not a problem.

As stated in 6N16812, ISO/IEC/IEEE 8802-11 places security requirements on implementations, it does not require that any particular EAP method be supported, especially not EAP methods that are susceptible to attack.

The standard clearly states that if IEEE 802.1X-2010 is used, the EAP method shall support 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.

In fact, the freedom afforded deployments by this minimal requirement has resulted in plain unitary EAP methods, tunnelled EAP methods, and chained EAP methods that address unique and complex requirements seen in the real world dealing with machine authentication in addition to user authentication using every credential possible—certificates, smart cards, SIM cards, token cards, username/password, etc. The wide deployment of 802.11 with 802.1X/EAP authentication indicates a great success in this approach, not the problem alleged in the comment.

Proposed Resolution: Reject, this is not a problem and the world-wide deployment of this technology is evidence that no problem exists.

**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.”

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: The specific EAP method used when doing 802.1X authentication with IEEE 802.11 is outside the scope of the standard. The security of IETF standards are described in the relevant RFC, there is no need for IEEE 802.11 to note the security provided by each possible EAP method. Any EAP method susceptible to a MITM attack would not be suitable for use in IEEE 802.11. 6N16812 “did not solve the authentication issue” because there is no issue to solve. But 6N16812 did say that while ISO/IEC/IEEE 8802-11 places security requirements on implementations, it does not require that any particular EAP method be supported, especially not EAP methods that are susceptible to attack.

The standard clearly states that if IEEE 802.1X-2010 is used, the EAP method shall support 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.

In fact, the freedom afforded deployments by this minimal requirement has resulted in plain unitary EAP methods, tunnelled EAP methods, and chained EAP methods that address unique and complex requirements seen in the real world dealing with machine authentication in addition to user authentication using every credential possible—certificates, smart cards, SIM cards, token cards, username/password, etc. The wide deployment of 802.11 with 802.1X/EAP authentication indicates a great success in this approach, not the problem alleged in the comment.

Proposed Resolution: Reject, the authentication protocol does not need to be re-designed because there is no interoperability issue as evidenced by the world-wide deployment of this technology.

**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 SC6N16812 said “*This issue has been acknowledged and will be addressed by the IEEE 802.11 Working Group through the normal maintenance process of JTC1/SC6/IEEE FDIS 8802-11.*”, but 6N17495 doesn’t show any improvement conforming to the above statement.”

Discussion: This needs resolution.

Proposed Resolution: 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.

**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: An external authentication server is an optional optimization for certain use cases which can be deployed at scale when authentication is centralized. Not all use cases compel such a deployment. For example, the use case of WAPI where the client and AP each have certificates is supported in IEEE 802.11 without the need for an external authentication server. For use cases that compel the use of an external authentication server, not only does that not “limit the expansibility and flexibility of users”, it enables extensibility and flexibility. It enables these particular credentials to be deployed at scale. Requirements on the security of the channel, when used, are listed in IEEE 802.11.

Proposed Resolution: Reject, IEEE 802.11 defines the requirements for securing the channel when such a channel is used. What particular protocol is used to effect that security does not need to be specified, this allows for various protocols—e.g. IPsec or TLS—to be used as the deployment requires. There are no complications in network configuration when using a secure channel.

**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: There is nothing to resolve. The comment mentions a 20 message exchange but as 6N16812 notes, the total number of messages could be less if a different EAP method is used. For instance, the EAP method defined in RFC 5931 satisfies the requirements ISO/IEC/IEEE 8802-11 places on EAP methods and uses 6 messages.

Proposed Resolution: Reject, it is not known where the 20 message exchange comes from but there are exchanges that are considerably less than 20. Any potential issue has already been resolved.

**CN11**

Comment: “It’s glad to see statements in 12.2.1*’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.”

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.”

Discussion: The security defects of WEP would not go away if it was completely removed from the IEEE 802.11 standard. As 6N16812 mentions, WEP is deprecated and included for historical reasons. That does clearly explain why it is still in the standard. It’s for historical reasons. This allows those who maintain older implementations to see that WEP has been deprecated. WEP is not suitable for use in IEEE 802.11 and conformant products will not use it.

Proposed Resolution: Reject, WEP is obsolete. It is unsuitable for use in IEEE 802.11. It does not need to be removed from the standard and remains for historical reasons.

**CN12**

Comment: “It’s glad to see statements in 12.2.1 *‘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 220 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.”

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: The security defects of TKIP would not go away if it was completely removed from the IEEE 802.11 standard. As 6N16812 mentions, TKIP is deprecated and included for historical reasons. That does clearly explain why it is still in the standard. It’s for historical reasons. This allows those who maintain older implementations to see that TKIP has been deprecated. TKIP is not suitable for use in IEEE 802.11 and conformant products will not use it.

Proposed Resolution: Reject, TKIP is deprecated. It is unsuitable for use in IEEE 802.11. It does not need to be removed from the standard and remains for historical reasons.

**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.

**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 ciphersuite according to requirements in different countries and regions.’”

Discussion: We agree with the China National Body (CNB) that security protocols and cryptographic algorithms can indeed have a degree of independence. That is one of the reasons that IEEE Std 802.11 allows for the addition of new cryptographic algorithms and authentication and key management suites, either as part of the standards process or as vendor-specified algorithms or cryptographic suites. 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. The IEEE 802.11 Working Group would gladly welcome participation from others who propose expanding the algorithms available for use within the IEEE Std. 802.11 and by extension ISO/IEC/IEEE 8802-11. That said, IEEE Std 802.11 is a contribution-driven specification. The content found in the standard is a direct reflection of the contributions from the participants in the standardization process. To date, we have not had active participation from any entity or contributor to expand the number of encryption algorithms.

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 ciphersuites and if the CNB wishes to follow that process then new ciphersuites can be assigned for their ciphers. IEEE 802.11 again repeats its offer to have representatives of the CNB come to 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: There is no interoperability issue. Each side could use a different technique, provided it satisfies the requirements placed on it by IEEE Std 802.11, and it would have no impact on the protocol. In fact, the STA has no way of knowing what technique the AP is using to secure its communications with the AS.

A secure channel is provided because the standard describes the requirements it places on that channel to ensure it is secure. Provided an implementation complies with the standard, the channel will be secure and no security risks will arise.

Proposed Resolution: Reject, there is no interoperability issue because this backend communication has no bearing on the FILS shared key authentication protocol.

**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 standard uses credentials and places requirements on them for their use. Specification of how to achieve those requirements are out-of-scope. There are plenty of valid ways to achieve trust in a public key. Using a certificate signed by a trusted third party is a prime example. Describing the behavior and function of certification authorities is out of scope for IEEE Std 802.11-2020.

Proposed Resolution: Reject, trust establishment is outside the scope of this standard.

**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: RSN specifies the security of the IEEE 802.11 wireless network. A CMMG BSS is an IEEE 802.11 BSS and therefore it shall use the same RSN operations in a DMG BSS. If the CNB wants other cryptographic algorithms to be used in IEEE 802.11 (and therefore in ISO/IEC 8802-11), it is requested to engage with IEEE 802.11 for consideration of any proposals.

Proposed Resolution: Reject, relaxation of the security to permit undefined security methods would dangerously impact the security of the IEEE 802.11-2020 standard.

**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 recognised.”

Discussion: This is a duplicate from the previous round of balloting (6N16794) and has already been rejected.

Proposed Resolution: Reject. Many of the mentioned identifiers are specific to ISO/IEC/IEEE 8802-11 and managed by the IEEE 802.11 ANA. 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:** 11-18/0691r2, aka 6N16812