IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Communication from Wi-Fi Alliance re: P802.11az D3.1 | | | | |
| Date: 2021-09-15 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dorothy Stanley | Hewlett Packard Enterprise | 3333 Scott Blvd. Santa Clara, CA 95054 | +1 630-363-1389 | [dstanley@ieee.org](mailto:dstanley@ieee.org) |
|  |  |  |  |  |

Abstract

This document contains a communication received from Wi-Fi Alliance (WFA) related to P802.11az D3.1. The received communication is embedded below, and copied on the following pages.



Stanley, Dorothy

From: Susan Silveira <ssilveira@wi-fi.org>

Sent: Tuesday, September 14, 2021 11:26 AM

To: Stanley, Dorothy; 'Segev, Jonathan'

Cc: Consuelo Ortiz; Chuck Hoover

Subject: Wi-Fi Alliance Location Task Group Communication to IEEE 802.11 WG

Hello Dorothy & Jonathan –

As part of ongoing Wi-Fi Alliance development of enhancements to the Wi-Fi CERTIFIED Location interoperability certification program, Wi-Fi Alliance engaged a 3rd party to conduct a security review of P802.11az D3.1. While no major issues were identified, several minor items were raised, which are included below.

Wi-Fi Alliance requests the IEEE802.11 Working Group to review the following items and consider their potential for improving the P802.11az draft specification.

NOTE: The bold references indicate the page number, period, and line number or range of line numbers of P802.11az D3.1.

* General: Are all the authentication options required? The concern is implementation errors in infrequently used options.
* 68.12: In Figure 9-664, simply crossing out “variable” doesn’t give the reader any idea about the sizing of the field. The following text merely says that 12.11 and 12.12 use it. Given that any element includes the first three fields in Figure 9-664, we recommend saying something about the length or deleting the figure altogether.
* 68.21: For bit 9, it might be worth mentioning what should be done if a STA does not support Secure RTT Measurement exchange.
* 87.20-21: This sentence would seem to indicate that an ephemeral public key and finite cyclic group ID might not be present. This does not align with 12.12.3.2 and other portions of 12.12, which expects an ephemeral key to be present.
* 114.24: It says, “In an infrastructure BSS, association is required.” But this isn’t necessarily true when an infrastructure BSS is only used for location services.
* 125.5: Clauses 12.6.19 and 12.6.20 make no mention of PTKSA establishment.
* 125.8: We suggest moving the note above the previous paragraph and dropping “NOTE—“.
* 125.8: s/the PTKSA/a PTKSA/
* 174.2: The figure needs some fixing near “Error”. The arrowhead is located between the two lines in the ladder diagram, which is confusing.  199.3: s/signals/is set to 1 to signal/
* 211.3: This clause could be much clearer in initially describing the options it offers for the different ways that PASN may be employed. Instead, the reader is left to intuit that there are different options from the salient points list on page 211, lines 9-17. For example, lines 9-10 leaves the reader assuming a PMKSA is implied, but lines 15-17 contradict that. We recommend starting with an enumeration of the PASN “modes” and then providing salient points for each of the modes.
* 211.4: Use of “AKM” here might be better served by “AKM selector value” or “AKM suite type”. See usage in REVmd D5.0, page 1109 or page 2613, respectively. We recognize that the base standard is also inconsistent in its usage.
* 211.12: A PMKSA is not itself an RSNA protocol. A PMKSA might be established with an AKMP that has a key management type listed as an RSNA type in Table 9-151.
* 213.21: Would it make sense to provide a minimum value for a PTKSA lifetime? At some point, a PTKSA must have a lifetime so short that the STA will not have sufficient time to perform location determination with the AP for which the PMK lifetime is close to expiry.
* 214.22: This is the first PASN authentication frame. What validation has been performed that could have failed? Is it the original validation of the second PASN authentication frame that contained the Comeback Info field? If so, please make that clear.
* 216.5: The statement “The Cookie field is optionally set.” can be implied from the previous sentence, but could be more logically tied to the Cookie Length.
* 216.11: Prior to deriving the PTKSA, the AP should derive the Diffie-Hellman shared secret (DHss) needed in the derivation of the PTKSA. The PTKSA derivation clause (12.12.7) does not actually spell out how this is done, but REVmd D5.0 on page 2702 shows an example of suitable text.
* 216.18: The text says “PMKID count of 1”, and this seems correct, but Figure 12-55a (212.17) shows “PMKID[0..n]”. The figure should show “PMKID[0..1]” for authentication step 2.
* 217.6: An active attacker could set the Status Code field to FAIL and cause early termination of the protocol. This would be similar to mangling the MIC except that the MIC is not checked until 217.32.
* 217.27: The STA should compute the Diffie-Hellman shared secret (DHss) prior to deriving the PTKSA, as discussed above (see 216.11).
* 218.21: The second half of this sentence (key installation) should only occur if the status code being sent was success.
* 218.23: The STA inserts a status code into the third PASN frame indicating success or failure. Upon receipt of the third PASN frame, the AP, however, does not check the status code.
* 220.29-31: Since these are called as out as little endian are the others big endian?
* 222.6: If computational costs are a concern, in the case that the AKM suite selector value is other than

PASN, which employs a fixed PMK, it might be worth considering sacrificing the PFS. In place of the DHss, S-Ephemeral Pub || A-Ephemeral Pub would serve a similar purpose to the nonces in other versions of PTK generation within the base specification.

* 222.6, 222.20-27: The meaning of KDF-HASH-NNN would be more approachable if it were simply written as is done on page 2650 of REVmd D5.0. Another similar approach is shown in IEEE 802.11az D3.1 on pages 207, lines 6-22.
* 222.18: clarify the meaning of “higher layer security”.
* 222.27: If a KCK is 32 octets and a TK is 16 or 32 octets, then with a KDK of either 256 bits or 0 bits, totals of 640 and 768 are not always guaranteed.
* 222.28-29: It might make more sense to move this sentence to 222.19 if this is what is meant by higher layer security, otherwise there’s a contradiction between the two statements.

Thank you,

Wi-Fi Alliance

Susan Silveira

Director, Business Development

Wi-Fi Alliance

M 760.420.7654

O 512.498.9439

**References:**