IEEE P802.11
Wireless LANs

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
| CR for KEK size |
| Date: 2024-05-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel  |  |  | po-kai.huang@intel.com |
| Ilan Peer |  |  |  |
| Emily Qi |  |  |  |
| Ido Ouzieli |  |  |  |

 |

Abstract

This submission proposes CR for the following comments on P802.11-bh D4.0:

21

**Revision History:**

R0: Initial version.

R1: Further revision.

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbh D4.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbh D4.0 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbh Editor: Editing instructions preceded by “TGbh Editor” are instructions to the TGbh editor to modify existing material in the TGbh draft. As a result of adopting the changes, the TGbh editor will execute the instructions rather than copy them to the TGbh Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 21 | Po-Kai Huang | 12.7.3 | 41.12 | For AKM 21 row, When Base AKMP is 21, i.e., PASN, 128 KEK\_bits may not align with the security strength when pairwise cipher uses GCMP-256. Similar consideration for AKM 26 row. Suggest to align the KEK\_bits based on pairwise cipher. | For AKM 21 row, change "128 if Base AKMP is 00-0F-AC:21" to "128 if Base AKMP is 00-0F-AC:21 and pairwise cipher is not 00-0F-AC:9 or 00-0F-AC:10. 256 if Base AKMP is 00-0F-AC:21 and pairwise cipher is 00-0F-AC:9 or 00-0F-AC:10." For AKM 26 row, change "256" to "256 if pairwise cipher is not 00-0F-AC:9 or 00-0F-AC:10. 512 if pairwise cipher is 00-0F-AC:9 or 00-0F-AC:10" | Revised – Agree in principle with the commenter. TGbh editor to make the changes shown in 11-24/0891r1 under all headings that include CID 21 |

## Discussion:

Reference for cipher suite selector is shown below.







|  |
| --- |
|  |

*TGbh editor: Change Clause 12.7.3 as follows (track change on):*

**12.7.3 EAPOL-Key PDU construction and processing**

***Modify the following row in Table 12-11 (Integrity and key wrap algorithms) as shown below.***

**Table 12-11—Integrity and key wrap algorithms**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **AKM**  | **Integrity algorithm** | **KCK\_bits**  | **Size of MIC (octets)** | **Key wrap algorithm** | **KEK\_bits**  | **KCK2\_bits**  | **KEK2\_bits** |
| 00-0F-AC:21 | See NOTE | N/A  | N/A  | As defined by Base AKMP in Table 12-11 if Base AKMP is not 00-0F-AC:21. NIST AES Key Wrap if Base AKMP is 00-0FAC:21. | As defined by Base AKMP in Table 12-11 if Base AKMP is not 00-0F-AC:21. 128 if Base AKMP is 00-0FAC:21 and pairwise cipher is not 00-0F-AC:09 or is not 00-0F-AC:10. 256 if Base AKMP is 00-0FAC:21 and pairwise cipher is 00-0F-AC:09 or 00-0F-AC:10.(#21) | N/A  | N/A |
| 00-0F-AC:26 | See NOTE | N/A  | N/A  | AES-SIV-256 if pairwise cipher is not 00-0F-AC:09 or is not 00-0F-AC:10. AES-SIV-512 if pairwise cipher is 00-0F-AC:09 or 00-0F-AC:10.(#21) | 256 if pairwise cipher is not 00-0F-AC:09 or is not 00-0F-AC:10. 512 if pairwise cipher is 00-0F-AC:09 or 00-0F-AC:10.(#21) | N/A  | N/A  |