IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11be D2.0 CR for 11056 | | | | |
| Date: 2022-12-13 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

11056

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Editorial 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 TGbe D2.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe D2.0 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 11056 | Po-Kai Huang | 4.3.16a | 55.62 | The intention of having Mandatory support for GCMP-256 is to enable increased security strength. However, to enable incerased security strength, we need to also mandate the AKM that are used to support higher secuirty strength, i.e. SHA-384 for key derivaiton. | Suggest to add the following in 12.6.3 RSNA policy selection in an infrastructure BSS. "If an EHT AP includes the AKM suite selector value 00-0F-AC:8 in the RSNE, then the EHT AP shall include the AKM suite selector value 00-0F-AC:24 in the RSNE."  "If an EHT AP includes the AKM suite selector value 00-0F-AC:1 or 00-0F-AC:5 in the RSNE, then the EHT AP shall include the AKM suite selector value 00-0F-AC:23 in the RSNE." | Revised –  Agree in principle with the commenter. AKM 24 allows PMK length to be negotaied under SAE rather than limited by AKM 8 under SAE. This is needed to accommodate the requirement of mandatory support of GCMP-256.  TGbe editor to make the changes shown in 11-22/2158r1 under all headings that include CID 11056 |

**Discussion: None**

***TGbe editor:******Change 12.12.3 Security constraints for EHT as follows (track change on).***

**12.5.4 GCM protocol (GCMP)  
12.5.4.1 GCMP overview**

***Change the first paragraph as follows:***Subclause 12.5.4 (GCM protocol (GCMP)) specifies the GCMP, which provides data confidentiality,  
authentication, integrity, and replay protection. A DMG RSNA STA shall support GCMP-128. (#11056)

**12.12.3 Security constraints for EHT(#11039)**

An EHT RSNA STA shall support GCMP-256. (#11056)

If an EHT AP includes the AKM suite selector value 00-0F-AC:8 in the RSNE, then the EHT AP shall include the AKM suite selector value 00-0F-AC:24 in the RSNE.(#11056)

(#13533)(#11039)An EHT AP shall have dot11BeaconProtectionEnabled set to 1 when using RSN.

(#11038)NOTE—An EHT AP has dot11RSNAProtectedManagementFramesActivated set to 1 when using RSN due to  
the requirement that if dot11RSNAProtectedManagementFramesActivated is false, dot11BeaconProtectionEnabled  
needs to be set to false (see 11.52 (Beacon frame protection procedures)).