IEEE P802.11
Wireless LANs

|  |
| --- |
| Two AEAD Comments |
| Date: 2016-05-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 1322 Crossman avenue, Sunnyvale, California, United States of America | +1 415 555 1212 |  |
|  |  |  |  |  |

Abstract

This submission addresses CIDs 20124 and 20167.

|  |  |  |  |
| --- | --- | --- | --- |
| 20124 | "AES-SIV" is not used consistently in Table 9-132: the FT AKMs leave out "AES-" while the non-FT ones include it. | On page 55 line 51, replace "and SIV-256" with "and AES-SIV-256".On page 55 line 57, replace "and SIV-512" with "and AES-SIV-512". | Accepted |

Discussion:

The proper reference should be “AES-SIV-256” and “AES-SIV-512” in both places, so accept.

|  |  |  |  |
| --- | --- | --- | --- |
| 20167 | The AAD used with the AEAD algorithm is defined as a concatenation of number of data items. The only AEAD algorithm that is used in the P802.11ai is AES-SIV which supports multiple variable-length octet strings ("a vector of strings") as the authenticated data. As such, the concatenation to construct a single AAD seems unnecessary for SIV. Is this in support of some other AEAD algorithms or should these be define as a vector of strings instead? | Clarify how AES-SIV vector of strings is used (a single AAD vs. separate string for each of the data items). Same for (Re)Association Response frame in 12.11.2.6.3. | Revised: change the AAD to a vector per the changes specified in <this document>. |

Discussion:

One of the unique features of SIV is that it can take multiple, distinct pieces of AAD. The comment identifies the fact that our AAD is concatenated into one single component and passed, as one thing, to SIV while it would be equally possible to break it up and pass all components as separate components of the “vector” of AAD. It might be easier to pass pointers to the separate components than to engage in a gather-scatter form of AAD marshalling.

***Instruct the editor to modify section 12.11.2.6.2 as indicated:***

**12.11.2.6.2 (Re)Association Request for FILS key confirmation**

The (Re)Association Request frame shall be encrypted using the AEAD algorithm as defined in 12.11.2.7 (AEAD cipher mode for FILS) with the KEK as the key. The AAD used with the AEAD algorithm for the Association Request frame consists of the following data passed as separate components in the following order:

— The STA’s MAC address,

— The AP’s BSSID,

— The STA’s nonce,

— The AP’s nonce,

— The contents of the (Re)Association Request frame from the Capability Information field (inclusive) to

 the FILS Session element (inclusive).

***Instruct the editor to modify section 12.11.2.6.3 as indicated:***

**12.11.2.6.3 (Re)Association Response for FILS key confirmation**

The (Re)Association Response frame shall be encrypted using the AEAD algorithm as defined in 12.11.2.7 (AEAD cipher mode for FILS) with the KEK as the key. The AAD used with the AEAD algorithm for the (Re)Association Response frame consists of the the following datapassed as separate components in the following order:

— The AP’s BSSID,

— The STA’s MAC address,

— The AP’s nonce,

— The STA’s nonce,

— The contents of the (Re)Association Response frame from the Capability Information field (inclusive)

 to the FILS Session element (inclusive).

**References:**