IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution for CID 246 | | | | |
| Date: 2017-12-15 | | | | |
| Author: | | | | |
| Name | Affiliation | Address | Phone | Email |
| Edward Au | Huawei Technologies | 303 Terry Fox Drive, Suite 400, Ottawa, Ontario K2K 3J1 |  | [edward.ks.au@huawei.com](mailto:edward.ks.au@huawei.com) |

##### This submission present a resolution for CID 246.

##### Revision history:

##### R0 – initial version

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 246 | 12.7.9.2 |  |  | The wording for the "where" stuff is inconsistent with other cases (see 16/0447) | Make it consistent (see 16/0447) |

***Discussion:***

|  |
| --- |
| Hello Edward,  I'm happy for you to present re CID 246, assuming you are OK with the resolution I'm proposing (below).  Thanks,  Mark |

As referred to lines 12~25 in page 2195 below, we have a definition of Hash and KDF-Hash-Length.



However, Mark points out that the way the definitions are presented is not consistent with those in other subclauses, e.g., 12.4.4.2.2 (c.f., lines 46-48 in page 2074) and 12.4.4.3.2 (c.f., lines 7-9 in page 2077), as follows:



Mark’s proposal is to replace the two definitions from line 22 to line 25 in page 2195 with the following one definition:

KDF-Hash-*Length* is the key derivation function defined in 12.7.1.7.2 (Key derivation function (KDF)) using the hash algorithm identified by the AKM suite selector (see Table 9-133 (AKM suite selectors)

***Proposed resolution:***

**Revised**

|  |
| --- |
| At lines 22-25 of page 2195 in D0.2,  change  Hash is the hash algorithm identified by the negotiated AKM suite selector specified in Table 9- 133 (AKM suite selectors)  KDF-Hash-*Length* is the key derivation function defined in 12.7.1.7.2 (Key derivation function (KDF)) that uses Hash to generate a key whose length is TK\_bits + 128  to  KDF-Hash-*Length* is the key derivation function defined in 12.7.1.7.2 (Key derivation function (KDF)) using the hash algorithm identified by the AKM suite selector (see Table 9-133 (AKM suite selectors)) |

|  |
| --- |
| At line 62 of page 2155 in D0.2, change “is the KDF as defined in 12.7.1.7.2” to “is the key derivation function defined in 12.7.1.7.2”. |

|  |
| --- |
| At line 47 of page 2156 in D0.2, change “is the KDF as defined in 12.7.1.7.2” to “is the key derivation function defined in 12.7.1.7.2”. |

|  |
| --- |
| At line 22 of page 2157 in D0.2, change “is the KDF as defined in 12.7.1.7.2” to “is the key derivation function defined in 12.7.1.7.2”. |

|  |
| --- |
| At line 57 of page 2078 in D0.2, change “KDF-Hash-512 is the key derivation function defined in 12.7.1.7.2 (Key derivation function (KDF)) using the hash algorithm defined by the negotiated AKM in Table 9-133 (AKM suite selectors).” to “KDF-Hash-512 is the key derivation function defined in 12.7.1.7.2 (Key derivation function (KDF)) using the hash algorithm defined by AKM suite selector (see Table 9-133 (AKM suite selectors))”. |