IEEE P802.11
Wireless LANs

|  |
| --- |
| Clarity |
| Date: 2016-03-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 1322 Crossman avenue, Sunnyvale, California, United States of America | +1 408 555 1212 | An ASCII string consisting of the initial of the first name concatenated with entire last name, all lower-case, followed by the “at sign” (a single octet whose value is 0x40) and aruba networks as one word followed by the dot character (a single octet whose value is 0x2E) and the three letter abbreviation for commercial. |
|  |  |  |  |  |

Abstract

This submission proposes resolution to CIDs 7533, 7536, and 7537.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  CID |  Page.Line |  Section |  Comment |  Proposed Resoluiton |
|  7533 | 1002.07 | 9.4.2.118 | "the  bit  string  of  {GTK  ||  Key  RSC || GTKExpirationTime}" -- what is the format of the GTK as an octet string? | Revised: GTK is the GTK, and make it all one sentence. |

***Instruct the editor to modify section 9.4.2.118 as indicated:***

**9.4.2.118 Authenticated Mesh Peering Exchange element**

The GTKdata field is optional. When present, it contains the bit string of {GTK || Key RSC || GTKExpirationTime} as the GTK data material. When present, the GTKdata field is protected by the exchange in which it is contained (see 14.5 (Authenticated mesh peering exchange (AMPE))). GTK is the GTK, Key RSC denotes the last frame sequence number sent using the GTK asspecified in Table 12-5 (Key RSC field) of 12.7.2 (EAPOL-Key frames), and GTKExpirationTime denotes the key lifetime of the GTK in seconds usingthe format is specified in Figure 12-40 (Lifetime KDE format) of 12.7.2 (EAPOL-Key frames).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  CID |  Page.Line |  Section |  Comment |  Proposed Resoluiton |
|  7536 |  2138.01 | 14.5.7 | Selected AKM Suite || min(localMAC, peerMAC) || max(localMAC, peerMAC)). -- what's the format of the Selected AKM Suite as an octet string? | Revised: add text to indicate that it’s a 4 octet string: OUI plus Suite type |
|  7537 |  2138.15 |  14.5.7 |  Ditto |  Ditto |

***Instruct the editor to modify section 14.5.7 as indicated:***

**14.5.7 Keys and key derivation algorithm for the authentication mesh peering exchange (AMPE)**

The AEK is mutually derived by the local STA and the peer STA once a new PMK has been selected. The

AEK shall be derived from the PMK by

AEK 🡨 KDF-Hash-256(PMK, “AEK Derivation”, Selected AKM Suite ||

min(localMAC, peerMAC) || max(localMAC, peerMAC))

where KDF-Hash-256 is the key derivation function defined in 12.7.1.7.2 (Key derivation function (KDF))

using the hash algorithm defined by the AKM in Table 9-132 (AKM suite selectors) to generate an AEK of

length 256 bits, and Selected AKM Suite is a four octet string formed by concatenating the OUI and suite type.

The temporal key (MTK) shall be derived from the PMK by

MTK 🡨 KDF-Hash-Length(PMK, “Temporal Key Derivation”, min(localNonce,

peerNonce) || max(localNonce, peerNonce) || min(localLinkID,

peerLinkID) || max(localLinkID, peerLinkID) || Selected AKM Suite ||

min(localMAC, peerMAC) || max(localMAC, peerMAC))

where KDF-Hash-Length is the key derivation function defined in 12.7.1.7.2 (Key derivation function (KDF)) using the hash algorithm defined by the AKM in Table 9-132 (AKM suite selectors) to generate an MTK of a specified length. Both CCMP and GCMP use Length = 128. Selected AKM Suite is a four octet string formed by concatenating the OUI and suite type. The “min” and “max” operations for IEEE 802 addresses are with the address converted to a positive integer, treating the first transmitted octet as the most significant octet of the integer as specified in 12.7.1.3 (Pairwise key hierarchy). The “min” and “max” operations for nonces are encoded as specified in 9.2.2 (Conventions). The “min” and “max” operations for LinkIDs select the minimum and maximum, respectively, of the two unsigned integers.

**References:**