IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Suite B AKM Update | | | | |
| Date: 2016-04-21 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 1322 Crossman avenue, Sunnyvale, California,  United States of America | +1 408 555 1212 | dharkins at aruba networks as one word dot com |
| Russ Housley | Vigil Security | 918 Spring Knoll Drive, Herndon, Virginia,  United States of America | +1 703 435 1775 | housley at vigilsec dot com |

Abstract

This submission fixes an ambiguity regarding the Suite B AKM in light of recent guidance on the use of Suite B.

Discussion:

The National Security Agency (NSA) of the United States of America recently release guidance on the use of Suite B cryptography. Part of this guidance allowed for RSA digital signatures (of a suitable key length) to be used in a Suite B-compliant cipher suite in addition to ECDSA digital signatures. Subsequent guidance will allow for the RSA key exchange in addition to ECDH.

The current definition of the Suite B AKMs states that the EAP method used in 802.1X authentication shall support an elliptic curve of the appropriate strength which is somewhat ambiguous as whether that requirement is on the digital signatures as well as on the Diffie-Hellman calculation, it is also problematic because it might be possible to have a Suite B-compliant EAP method that does not do EC at all. Since the particulars of how the Suite B options get instantiated is entirely an EAP issue and 802.11 (and 802.1X) is agnostic regarding such matters, the only thing 802.11 needs is AKMs specifying whether it’s the Suite B suite that uses SHA-256 or the Suite B suite that uses SHA-384.

Proposed resolution:

While the digital signature and key exchange may be subject to further guidance, the hash algorithm will not. State that the Suite B compliant EAP method shall support the appropriate hash algorithm and be silent on the digital signature and key exchange used.

***Instruct the editor to modify table 9-132 in section 9.4.2.25.3 as indicated:***

**9.4.2.25.3 AKM suites**

**Table 9-132—AKM suite selectors (continued)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| OUI | Suite Type | Authentication Type | Key management type | Key derivation type |
| 00-0F-AC | 11 | Authentication negotiated over IEEE Std 802.1X or using PMKSA caching as defined in 12.6.10.3 (Cached PMKSAs and RSNA key management) using a Suite B compliant EAP method supporting SHA-256 | RSNA key management as defined in 12.7 (Keys and key distribution) or using PMKSA caching as defined in 12.6.10.3 (Cached PMKSAs and RSNA key management) | Defined in 12.7.1.7.2 (Key derivation function (KDF)) using SHA-256 |
| 00-0F-AC | 12 | Authentication negotiated over IEEE Std 802.1X or using PMKSA caching as defined in 12.6.10.3 (Cached PMKSAs and RSNA key management) using a Suite B compliant EAP method supporting SHA-384 | RSNA key management as defined in 12.7 (Keys and key distribution) or using PMKSA caching as defined in 12.6.10.3 (Cached PMKSAs and RSNA key management) | Defined in 12.7.1.7.2 (Key derivation function (KDF)) using SHA-384 |

**References:**