IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Creation of a PMKSA with FILS Authentication | | | | |
| Date: 2013-01-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA | +1 408 227 4500 | dharkins at arubanetworks dot com |
|  |  |  |  |  |

Abstract

At the IEEE 802.11 Plenary November 2012 there was considerable interest in creating a PMKSA as a byproduct of FILS Authentication. This submission proposes such a thing.

***Instruct the editor to modify section 11.5.1.1.1 as indicated:***

**11.5.1.1.1 General**

A security association is a set of policy(ies) and key(s) used to protect information. The information in the

security association is stored by each party of the security association, needs to be consistent among all

parties, and needs to have an identity. The identity is a compact name of the key and other bits of security

association information to fit into a table index or an MPDU. The following types of security associations

are supported by an RSN STA:

— PMKSA: A result of a successful IEEE 802.lX exchange, SAE authentication, FILS Authentication,

preshared PMK information, or PMK cached via some other mechanism.

***Instruct the editor to modify section 11.5.1.1.2 as indicated:***

**11.5.1.1.2 PMKSA**

When the PMKSA is the result of a successful IEEE 802.1X authentication, it is derived from the EAP authentication and authorization parameters provided by the AS. When the PMKSA is the result of a successful SAE authentication or FILS Authentication, it is generated as a result of the successful completion of the SAE exchange or FILS Authentication exchange, respectively. This security association is bidirectional. In other words, both parties use the information in the security association for both sending and receiving. The PMKSA is created by the Supplicant’s SME when the EAP authentication completes successfully, FILS Authentication completes successfully, or the PSK is configured. The PMKSA is created by the Authenticator’s SME when the PMK is created from the keying information transferred from the AS, when IEEE 802.1X authentication is utilized, when the SAE exchange successfully completes, when the FILS Authentication exchange successfully completes, or when the PSK is configured. The PMKSA is used to create the PTKSA. PMKSAs are cached for up to their lifetimes. The PMKSA consists of the following elements:

***Instruct the editor to modify section 11.11.2.3 as indicated:***

**11.11.2.3 Key Derivation with FILS Authentication**

Key derivation with FILS Authentication uses the KDF from 11.6.1.7.2 to produce sixkeys, two key encryption keys (KEK and KEK2), two confirmation keys (KCKand KCK2), a Pairwise Master Key (PMK), and a traffic key (TK). The inputs to the KDF are the two 16 octet nonces produced by the STA and AP, a constant label, the ERP secret result if a TTP is being used, and, the Diffie-Hellman shared secret, ss, if PFS is being used. The length of the KEK and KEK2 shall be 128 bits, and the length of the KCK, KCK2, and PMK shall be 256 bits, and therefore the output from the KDF shall be 1024+TK\_bits, where TK\_bits is determined from table 11-4.

KCK2 | KEK2 | KCK | KEK | PMK | TK = KDF-X(NSTA | NAP, "FILS KECK PTK Derivation", [rMSK][ | ss])

Where X is 1024+TK\_bits from table 11-4, rMSK is the output of the ERP exchange if a trusted third party was used, and ss is the shared secret resulting from the Diffie-Hellman exchange if PFS was used. Upon completion of the key derivation computation, the shared secret shall be irretrievably destroyed.

***Instruct the editor to modify section 11.11.2.4 as indicated:***

**11.11.2.4 Key Confirmation with FILS Authentication**

If authentication is a failure, the KCK2, KEK2, KCK, KEK, PMK, and TK shall be irretrievably destroyed. Otherwise authentication succeeds. In that case, STA and AP shall irretrievablly destry the temporary keys KCK2 and KEK2 and both shall use the TK with the cipher indicated by the negotiated ciphersuite. The KCK, KEK and PMK shall be used for subsequent key management as specified in section 11.5. The STA and AP shall set the lifetime of the PMKSA to the value dot11RSNAConfigPMKLifetime.

**References:**