IEEE P802.11  
Wireless LANs

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Comments related to Section 4 | | | | | |
| Date: 2013-12-01 | | | | | |
| Author(s): | | | | | |
| Name | Affiliation | Address | Phone | | email |
| George Cherian | Qualcomm | 5775 Morehouse Dr, San Diego, CA, USA | | +1 858 651 6645 | gcherian@qti.qualcomm.com |

Abstract

This document is based on 1354r2. This contribution supersedes the edits from 1354r2 for the sections that are modified in this document.

Addresses following CIDs: CID3163

* General description
* Overview of the services
* Access control and data confidentiality services
* Authentication

***Change as follows:***

***(Editor note: changes made by 802.11ad and other preceding amendments will be reflected in later drafts)***

IEEE Std 802.11 authentication operates at the link level between IEEE Std 802.11 STAs. IEEE Std 802.11 does not provide either end-to-end (message origin to message destination) or user-to-user authentication.

IEEE Std 802.11 attempts to control LAN access via the authentication service. IEEE Std 802.11 authentication is an SS. This service may be used by all STAs to establish their identity to STAs with which they communicate, in both ESS and IBSS networks. If a mutually acceptable level of authentication has not been established between two STAs, an association is not established.

IEEE Std 802.11 defines five [CID #1279, 1335, 1399 ~~four~~ 802.11 authentication methods: Open System authentication, Shared Key authentication, FT authentication, ~~and~~ simultaneous authentication of equals (SAE), and fast initial link setup **(**FILS) authentication. Open System authentication admits any STA to the DS. Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key. FT authentication relies on keys derived during the initial mobility domain association to authenticate the stations as defined in Clause 12 (Fast BSS transition). SAE authentication uses finite field cryptography to prove knowledge of a shared password. FILS authentication uses either trusted public keys or a shared key derived out-of-band. There are three FILS authentication [CID # 1032, though #1197 & 1402 the word to be “authentication” which is appropriate for this clauseuses three alternative methods usedprocedures [CID #1400]: (1) the FILS shared key authentication method performed without perfect forward security (PFS), (2) the FILS shared key authentication method performed with PFS, and (3) The FILS public key authentication andbut with PFS (refer to Table 8-53m). [CID #1033, 1091 The IEEE Std 802.11 authentication mechanism also allows definition of new authentication methods.

An RSNA might support SAE authentication and/or FILS authentication. An RSNA also supports authentication based on IEEE Std 802.1X-2010, or preshared keys (PSKs) after Open System authentication. IEEE Std 802.1X authentication utilizes the EAP to authenticate STAs and the AS with one another. This standard does not specify an EAP method that is mandatory to implement. See 11.5.5 (RSNA policy selection in an IBSS and for DLS) for a description of the IEEE Std 802.1X authentication and PSK usage within an IEEE 802.11 IBSS.

In an RSNA, IEEE Std 802.1X Supplicants and Authenticators exchange protocol information via the IEEE Std 802.1X Uncontrolled Port. The IEEE Std 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE Std 802.1X authentication procedure completes successfully over the IEEE Std 802.1X Uncontrolled Port.

Either SAE authentication, FILS authentication, or Open System 802.11 authentication is used by non-DMG STAs in an RSN for an[CID 2533, 2241] infrastructure BSS. SAE authentication, Open System 802.11 authentication or no 802.11 authentication is used in an RSN for IBSS. SAE authentication is used in an MBSS. An RSNA disallows the use of Shared Key 802.11 authentication.[CID #1180] In an RSN for DMG BSS, Open System 802.11 authentication is not used

(11.1.4)[Updated per 11ad, also referencing CIDs 2063,2615, ]

* Deauthentication

***Change as follows:***

The deauthentication service is invoked when an existing Open System, Shared Key, SAE, or FILS authentication is to be terminated. Deauthentication is an SS.

When the deauthentication service is terminating SAE authentication any PTKSA, GTKSA, mesh TKSA, or mesh GTKSA related to this SAE authentication is destroyed. If PMK caching is not enabled, deauthentication also destroys any PMKSA created as a result of this successful SAE authentication.

In an ESS, because authentication is a prerequisite for association, the act of deauthentication causes the STA to be disassociated. The deauthentication service may be invoked by either authenticated party (non-AP STA or AP). Deauthentication is not a request; it is a notification. The association at the transmitting STA is terminated when the STA sends a deauthentication notice to an associated STA. Deauthentication, and if associated, disassociation can not be refused by the receiving STA except when management frame protection is negotiated and the message integrity check fails.

In an RSN ESS, Open System 802.11 authentication is required. In an RSN ESS, deauthentication results in termination of any association for the deauthenticated STA. It also results in the IEEE Std 802.1X Controlled Port for that STA being disabled and deletes the pairwise transient key security association (PTKSA). The deauthentication notification is provided to IEEE Std 802.1X-2004 via the MAC layer.

In an RSNA, deauthentication also destroys any related pairwise transient key security association (PTKSA), group temporal key security association (GTKSA), station-to-station link (STSL) master key security association (SMKSA), STSL transient key security association (STKSA), and integrity group temporal key security association (IGTKSA) that exist in the STA and, closes the associated IEEE Std 802.1X Controlled Port, if one exists. If pairwise master key (PMK) caching is not enabled, deauthentication also destroys the pairwise master key security association (PMKSA) from which the deleted PTKSA was derived.

In an RSN IBSS, Open System authentication is optional, but a STA is required to recognize Deauthentication frames. Deauthentication results in the IEEE Std 802.1X Controlled Port for that STA being disabled and deletes the PTKSA.

* IEEE Std 802.11 and IEEE Std 802.1X-2004
* Infrastructure functional model overview

***Insert new clause 4.10.3.6 (with figure) as follows:***

**4.10.3.6 AKM operations using FILS authentication [CID3163**

FILS authentication allows faster authentication by performing authentication, association and key conformation using 4 frames.

Three FILS authentication methods are defined: (1) the FILS shared key authentication performed without perfect forward security (PFS) (2) the FILS shared key authentication method performed with PFS, and (3) The FILS public key authentication method andwith PFS (refer to Table 8-53m).

Section 4.10.3.6.1 defines FILS shared key authentication with and without PFS.

Section 4.10.3.6.2 defines FILS public key authentication exchange.

**4.10.3.6.1 AKM operations using FILS shared key authentication**

When FILS shared key authentication is used, STA and the Authentication Server validates the mutual possession of rRK as the shared key as defined in [IETF RFC 5295 & IETF RFC 6696] using EAP-RP signaling. EAP-RP signaling is encapsulated using FILS wrapped data in the IEEE 802.11 Authentication frame as shown in the Figure 4,21a. A valid rRK is derived using a prior full authentication using EAP as defined in section 4.10.3.2. The rRK that is derived using the full authentication can be used for multiple runs of EAP-RP authentications as specified in [IETF RFC 5295 & IETF RFC 6696]. [CID #1404, 1407]The following operations (see Figure 4-21a (FILS authentication)) are carried out when FILS shared key authentication:

* The STA discovers the AP’s policy through passive scanning or through active scanning[CID #1199]. If a FILS[CID #1406] STA discovers that the AP supports FILS authentication and the identity of the Authentication Server is known (and trusted) by the STA, the STA may initiate FILS authentication
* The STA initiates FILS authentication by sending an Authentication frame with the FILS information to the AP. The AP forwards the FILS Authentication information to the trusted third[CID #1168, 1303 party. Upon receiving a response from the Authentication Server, the AP responds to the STA by encapsulating EAP-RP signaling information in the FILS wrapped data of the Authentication frame. The STA and AP generate a PMK as a result of this exchange. Exchange of messages (method, procedure, format and content) between AP/Authenticator and the Authentication Server is out of scope of this specification.

1. The STA sends an Association Request frame to the AP and receives an Association Response frame from the AP. This exchange provides proof-of-possession of the PMK and enables the creation of a PTKSA.

 [figure revised, CID #1174, 1370, 1200]

* FILS Authentication using Authentication Server

4.10.3.6.2 AKM operations using FILS public key authentication

It is assumed that both STAs and APs using FILS have obtained a public key certificate from a certification authority (CA) and that they are capable of verifying each other’s certificate during execution of FILS authentication. The manner by which these certificates are obtained is outside the scope of this standard.

The following operations are carried out when performing FILS public key authentication:

1. If a STA determines that an AP supports FILS authentication (through active or passive scanning) it may initiate FILS authentication

* The STA initiates FILS authentication by sending an Authentication frame to the AP, after which the AP responds with an Authentication frame. The STA and AP generate a PMK as a result of this exchange.
* The STA sends an Association Request frame to the AP and receives an Association Response frame from the AP. This exchange provides proof-of-possession of the PMK and enables the creation of a PTKSA and further establishment of FILS state.

[CIDs #1006, 1255, 1334, and 1371 per 13/0883r1]