IEEE P802.11  
Wireless LANs

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Comments related to Section 11.11.2 | | | | | |
| Date: 2013-11-05 | | | | | |
| 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

* Authentication for Fast Initial Link set-upsetup

STAs, both AP STAs and non-AP STAs, who share a means of authentication-either mutual trust of a TTP (such as authentication server), or using a certificate authority when a TTP is not present -may use that shared trust to mutually authenticate and derive a shared key in a more efficient manner than using IEEE 802.1X [CID2803]

The FILS Authentication protocol authenticates STAs to each other, optionally using a TTP. When a TTP is used the authentication exchange can optionally be performed with PFS. When a TTP is not used, PFS shall be used. When the FILS authentication protocol is performed with PFS, the STA and AP derive ephemeral public and private keys with respect to a particular set of domain parameters that define a finite cyclic group and then exchange public keys. The result of the FILS Authentication protocol is a PTKSA. FILS Authentication is an RSNA authentication protocol.

* Assumptions on FILS authentication

The security of FILS authentication depends on the following assumptions:

* Communication between the STAs and the trusted third party, when applicable, is protected with a secure deterministic authenticated encryption function.
* When using a TTP, each STA shares a valid rRK as defined in IETF RFC 5295 & IETF RFC 6696[13/0860r0] with the trusted third party that is capable of being used with EAP-RP[CID #1154]; when not using a TTP, each STA shall have a means to trust the public key of the other STA.
* When PFS is used, a finite cyclic group is negotiated for which solving the discrete logarithm problem is computationally infeasible.
* When PFS is used, both the STA and AP have at least one finite cyclic group from the dot11RSNAConfigDLCGroupTable in common.

All FILS Association frames shall be encrypted and authenticated (see 11.11.2.5 and 11.11.2.6).

* FILS authentication protocol

[CID2551, CID2099]The STA and AP perform key establishment using Authentication frames and perform key confirmation using Association Request, Association Response, Reassociation Request and Reassociation Response frames.

After exchanging Authentication frames, the STA and AP derive a shared and secret key which will be used to derive a set of secret keys that are authenticated after exchanging Association Request, Association Response, Reassociation Request and Reassociation Response frames.

When a trusted third party is used for FILS authentication, [CID2804] and if the STA shares a valid rRK with the TTP, then EAP-RP as defined in [IETF RFC 5295/6696] shall be used.

* Discovery with FILS authentication

An AP indicates that it is capable of performing FILS Authentication by constructing a FILS-capable Beacon or Probe response. FILS-capable 802.11 Beacons or Probe responses shall contain an AKM indicating support for FILS Authentication. [13/0860r0]

When trusted third party is used, AP may advertise up to seven realms using a 2 octet hashed domain name of the domain information of FILS Indication IE in Beacon, Probe Response and FILS Discovery frames. If the STA discovers a FILS-capable AP that advertised a hashed domain name that matches the hashed value of the realm of the third party authentication server with which the STA shares a valid rRK as defined in [IETF RFC 6696], the STA may begin the FILS authentication protocol with the AP. The domain name hashing is specified in 10.43.1. [13/0860r0]

[13/0860r0] A STA that discovers a FILS-capable AP that advertises an identity for which the STA has a trusted public key may begin the FILS Authentication protocol to the AP and perform mutual authentication using trusted public keys.

* Key establishment with FILS authentication

A FILS-capable STA and AP establish a shared key by exchanging Authentication frames. The specific contents of the Authentication frame depend on the particular authentication technique-whether a TTP is being used or whether digital signatures are being used-and whether PFS is obtained in the exchange or not.