IEEE P802.11  
Wireless LANs

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IP address Setup Proposal Text | | | | | |
| Date: 2013-07-15 | | | | | |
| Author(s): | | | | | |
| Name | Affiliation | Address | | Phone | email |
| George Cherian  Jouni Malinen  Santosh Abraham | Qualcomm | 5775 Morehouse Dr, San Diego, CA, USA | +1 858 651 6645 | | [gcherian@qti.qualcomm.com](mailto:gcherian@qti.qualcomm.com)  [jouni@qca.qualcomm.com](mailto:jouni@qca.qualcomm.com)  sabraham@qti.qualcomm.com |

Abstract

This document addresses CID 1382 (from Rene) + additional clean-ups

Comment from Rene: Clause 11.5.9.1, p. 79, l. 30-31: What happens if a STA and AP have different TTPs and the AP flags one that the STA does not know? Does this mean that the AP keeps advertising different TTPs it may have relationships with in the hope that one of these would suit the STA? Suggested remedy: Behavior in the event of a mismatch (or seeming mismatch) in terms of mutual trusted third parties needs to be adequately described (esp. since this is a pre-condition for starting the FILS protocol.)

***Modify the clause 8.4.2.179 as follows:***

**8.4.2.179 FILS Identity element**

The FILS Identity element is used for conveying an identity to use with the FILS authentication protocol

(see 11.11.2). The FILS Identity element is included in Authentication frames sent by STAs to initiate the FILS

authentication protocol. The format of the FILS Identity element is shown in Figure 8-401cz.

The ID type values are as follows:

0: Reserved

1: Trusted Third Party identity

2: STA identity

3 to 255: Reserved

When using a trusted third party for authentication, the semantics of the FILS Identity depend on the ID type

as well as the namespace used by the Trusted Third Party to identify itself and entities with which it has a

trusted relationship; they are therefore out of scope of this specification. When authenticating without a

trusted third party, the ID type subfield shall be 2 (STA identity) for both the STA and AP, and the contents

of the FILS Identity field shall be an X.500 distinguished name (DN) that identifies either a certified or a

raw public key.

***Modify the clause 8.4.2.179 as follows:***

**8.4.2.179 FILS Identity element**

The FILS Identity element is used for conveying an identity to use with the FILS authentication protocol

(see 11.11.2). The FILS Identity element is included in Authentication frames sent by STAs to initiate the FILS

authentication protocol. The format of the FILS Identity element is shown in Figure 8-401cz

***Modify the clause 8.4.2.185 as follows:***

**8.4.2.185 FILS Indication**

[…]

AP sets the Number of Domains field in the FILS indication to 7 to indicate that more than 7 domains are available. Seven of the domains are included in the element. STA can obtain the information about the other domains by querying for FILS Domain Information ANQP element.

[…]

***Insert the new row in Table 8-184 – ANQP element definitions with values :***

FILS Domain Information, <ANA>, 8.4.4.22

***Insert the new clause 8.4.4.22:***

**8.4.4.22 FILS Domain Information ANQP-element**

The FILS Domain Information ANQP-element provides a list of information about the Domains and the corresponding IP address types.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Info ID | Length | Domain Information #1 | … | Domain Information #n  (optional) |
| **Octets:** | 2 | 2 | 4 |  | 4 |

The Info ID field is equal to the value in Table 8-184 corresponding to the FILS Domain Information ANQP-element.

The Length field is a 2-octet field whose value is set to the total length of the Domain Information field.

The Domain Information field is defined in Figure 8-401dg

***Modify the clause 10.43.1 as follows:***

**10.43.1 FILS Indication element**

In Beacon and Probe Response frames, a FILS indication element is included by an AP with

dot11FILSActivated set to true. FILS indication element indicates properties of the FILS authentication protocol

used and also indicates if concurrent IP address assignment is performed by the AP. The IP address

type is also indicated.

When trusted third party is used, an AP can indicate up to 7 realms that the AP is connected to using the hashed domain name field of the Domain Information field of the FILS Indication element. The domain name is set to the realm as defined in [IETF RFC 6696]. For each of the indicated

domain names, the FILS element carries a 2 octet hash of the network domain name and the IP address type

of the corresponding domain. The hash of the domain name (that is RFC 1035 “Preferred Name Syntax”

compliant) is computed as follows:

Hashed Domain Name = L(CRC-32(Domain Name (all set to lower case)), 0, 16), where L is defined in 11.6.1

The CRC-32 shall be computed using the method given in clause 8.2.4.8.

For each domain, the type of IP address available is also indicated (Table 8-183af).

***Modify the clause 11.11.1 as follows:***

**11.11.1 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 with the trusted third party that is

capable of being used with ERP; 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).

**11.11.2.1 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.

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

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.

[…]

**11.11.2.2.1 FILS key establishment with trusted third party**

STA may initiate FILS authentication with a FILS capable AP that is connected to a trusted third party authentication server that shares a valid rRK as defined in [IETF RFC 6696] with the STA. If there is no valid rRK, a full EAP exchange may be performed via IEEE Std 802.1X authentication to establish rRK as defined in [IETF RFC 6696].

If the STA chooses to initiate FILS authentication using a trusted third party, the STA first chooses a random 16 octet nonce, and constructs an EAP-Initiate/

Re-auth packet as specified in [IETF RFC6696], with the following additional clarification:

— Regarding ERP Flags

o The 'B' flag shall be set to 0, indicating that this is not an ERP bootstrap message.

o The 'L' flag shall be set to 1, indicating that the trusted third party is to provide the lifetimes of

rRK and rMSK in the EAP-Finish/Re-auth Packet.

— The "Cryptosuite" field shall not be set to 1.

If PFS is desired, the STA selects a finite cyclic group from the dot11RSNAConfigDLGGroupTable, generates

an ephemeral secret private key, and performs the group's scalar-op (see 11.3.4.1) with its random

ephemeral private key and the generator from the selected finite cyclic group to compute an ephemeral public

key.

[…]