IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Text for MAAD 2 |
| Date: 2022-03 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

Proposed text for the MAAD MAC 2 scheme as per 22/0424r0

Note: This proposed text uses text from “Network generated Device ID” 22/0187r1

In particular, the text concerning the Device ID that is provided to the non-AP STA in msg 3.

QUESTIONS:

1 In “Opaque Device ID” 22/0154r0, the ID BLOB is padded, tweaked and encrypted. I don’t see this in the text 22/0187r1. I have assumed the ID is a 6 octet MAC Address, is this OK?

2 How do we cover the ESS? Do we assume that the MAAD MAC address is allocated at a central controller in the ESS? Do we need to add words or MIBs?

3 Reassociation. The STA will use the new MAAD MAC address as the ESS expects this. Think this is fine assuming ESS knows it.

4 Although saving a single Action Frame exchange, are we convinced this is a ‘better’ scheme than MAAD MAC 1? Requires 6 octet additions to Association and Reassociation requests and responses for FILS. What is the chance that implementation issues might occur?

Introduction:

The MAAD scheme uses an ID allocated by an AP during a previous RSN association as the TA for a new association. The TA is changing every association.

The following provides the instructions for inserting the new text into the Standard.

Instructions:

802.11 me Draft 1.1 is base

*Add following Acronym to 3.4.*

MAAD MAC Address Designation

*Insert new row in Table 9-62 Association Request frame body P1027*

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | MAAD | The MAAD element is optionally present when using FILS authentication; otherwise it is not present |

*Insert new row in Table 9-63 Association Response frame body P1031*

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | MAAD | The MAAD element is optionally present when using FILS authentication; otherwise it is not present |

*Insert new row in Table 9-64 Reassociation Request frame body P1035*

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | MAAD | The MAAD element is optionally present when using FILS authentication; otherwise it is not present |

*Insert new row in Table 9-65 Reassociation Response frame body P1040*

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | MAAD | The MAAD element is optionally present when using FILS authentication; otherwise it is not present |

*Insert new row in Table 9-128 Element IDs P1178*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element | Element ID | Element ID Extension | Extensible | Fragmentable |
| MAAD (see 9.4.2.x MAAD element) | 255 | <ANA> | No | No |

*Insert new row in Table 9-190 Extended Capabilities field, Clause 9.4.2.26 P1310*

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| <ANA> | MAAD Capability | A STA sets MAAD Capability subfield to 1 to indicate support for MAAD and sets to 0 if MAAD is not supported. |

*Add a new subclause at the end of 9.4.2*

9.4.2.x MAAD element

The MAAD element contains a MAAD MAC address. The format of the MAAD element is shown in Figure 9-y.

|  |  |  |  |
| --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | MAAD MAC |

 Octets 1 1 1 6

**Figure 9-y MAAD element**

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The MAAD MAC field is a 48-bit MAC address.

*Add a new subclause at the end of 12.2 subclauses*

**12.2.z MAAD MAC**

An AP may provide a MAAD MAC address to a non-AP STA and the non-AP STA may use this MAAD MAC address as its TA when it returns to the ESS so as to allow the network to recognize the same non-AP STA.

The provision of this MAAD MAC address is protected from third parties to limit the tracking capability to the APs in an ESS. The non-AP STA uses the MMAD MAC address as the TA when it next associates or addresses the ESS. Each time the non-AP STA associates to the ESS, it receives a new MAAD MAC address. A non-AP STA uses a different TA for every association to an ESS and hence cannot be identified by a third party by the TA it is using.

When using FILS authentication, the AP sends a new MAAD MAC address in the Association Response frame. When using FT, the AP sends a new MAAD MAC address in the EAPOL-Key message 3; the new MAAD MAC address is sent during the FT protocol reassociations within the same ESS. For other cases the AP sends a new MAAD MAC address in the EAPOL-Key message 3.

* EAPOL-Key frames

*Add a new row into Table 12-10 (KDE selectors) P3211 as shown below:*

|  |
| --- |
| * KDE selectors
 |
| OUI | Data type | Meaning |
| 00-0F-AC | 0 | Reserved |
| ... | ... | ... |
| 00-0F-AC | 15 | WIGTK KDE |
| 00-0F-AC | 16 | MAAD KDE |
| 00-0F-AC | 17–255 | Reserved |
| Other OUI or CID | Any | Vendor specific |

*Make following additions for the new KDE at the end of 12.7.2 P3214 as shown below:*

The format of the MAAD KDE is shown in Figure 12-48a (MAAD KDE format).

|  |
| --- |
| MAAD MAC |

 Octets 6

Figure 12-48a—MAAD KDE format

The MAAD MAC field contains MAAD MAC address from an AP in the ESS.

* EAPOL-Key frame notation

*Inser “MAAD MAC KDE” in 12.7.4 (P3217 L25) as shown below:*

 OCI KDE is a KDE containing operating channel information

 MAAD KDE is a KDE containing a MAAD MAC

 RSNXE is described in 9.4.2.241 (RSN Extension element (RSNXE))

 PMKID identifies the PMKSA selected by the Authenticator

 “{a} or {b}” means that exactly one of either {a} or {b} is present as the {Key Data}

* 4-way handshake
* General

*Modify 12.7.6.1 P3218.2 as shown below:*

RSNA defines a protocol using EAPOL-Key frames called the *4-way handshake*. The handshake completes the IEEE 802.1X authentication process. The information flow of the 4-way handshake is as follows:

Message 1: Authenticator  Supplicant: EAPOL-Key(0,0,1,0,P,0,0,ANonce,0,{} or {PMKID})

Message 2: Supplicant  Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,{RSNE} or {RSNE, OCI KDE} or {RSNE, RSNXE} or {RSNE, OCI KDE, RSNXE}

Message 3: AuthenticatorSupplicant:
EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,{RSNE,GTK[N]} or
{RSNE, GTK[N], OCI KDE} or {RSNE, GTK[N], RSNXE} or
{RSNE, GTK[N], OCI KDE, RSNXE} or {RSNE, GTK[N], MAAD KDE} or
{RSNE, GTK[N], OCI KDE, MAAD KDE} or {RSNE, GTK[N], RSNXE, MAAD KDE} or
{RSNE, GTK[N], OCI KDE, RSNXE, MAAD KDE})

Message 4: Supplicant  Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,{}).

* 4-way handshake message 3

*At P 3222.55 Modify 12.7.6.4 as shown below:*

* Additionally, contains an OCI KDE when dot11RSNAOperatingChannelValidationActivated is true on the Authenticator.
* Additionally, may include a MAAD KDE.
* The RSNXE that the Authenticator sent in its Beacon or Probe Response frame, if this element is present in the Beacon or Probe Response frame that the Authenticator sent.

*Add a new subclause at the end of clause 11 (MLME)*

**11.xx MAC Address Designation (MAAD) operation**

**11.xx.1 General**

To mitigate tracking and traffic analysis, a non-AP STA may randomly change its MAC address (see 4.5.4.10). For some services, however, it may be desirable to the user that the non-AP STA is identified by the AP and network services. MAAD operation enables a non-AP STA to use a random MAC address that is designated by the AP/ESS, and therefore the non-AP STA is identifiable by the AP/ESS whilst being unidentifiable to a third party.

A STA advertises support for MAAD by setting the MAAD Capability subfield to 1 in the Extended Capabilites element in Probe Response, Association Response and Reassociation Response frames.

Each time the non-AP STA associates to the AP/ESS, it receives a new MAAD MAC address during the RSN association. The non-AP STA may then use that MAAD MAC address as its TA the next time it probes or requests association to that same AP/ESS.

When the associating non-AP STA advertises support for MAAD, the AP shall allocate a new MAAD MAC address to the non-AP STA by including a MAAD KDE in message 3 of the 4-way handshake or, when using FILS authentication, including the MAAD element in the Association Response frame.

The non-AP STA should store that newly allocated MAAD MAC as an identifier for that AP/ESS. The non-AP STA then may use that allocated MAAD MAC address as its TA when it again associates or reassociates to that same AP or ESS. In so doing, the AP/ESS will identify the non-AP STA.

Note 1: Allocating a new MAAD MAC during each association ensures that the non-AP STA will use a different TA for each association and hence that non-AP STA is unidentifiable to a third party.

**11.xx.2 MAAD MAC address**

The MAAD MAC addressis a 48-bit address that is constructed from the locally administered address space (see 12.2.10). The non-AP STA may then store this address and use it as the TA in the next association request to that same AP.

An AP should generate the MAAD MAC addresses on a random basis such that a returning non-AP STA cannot be identified by a third party from the TA it is using. Allocating random 48 bit addresses should suffice but an AP may embed bits into the addresses in order to categorize or aid recognition. The generation of the MAAD MAC address is out-of–scope.

**11.xx.3 Stored MAAD MAC addresses**

A list of MAAD MACs and respective non-AP STAs shall be stored by the AP and used as an identifier for each non-AP STA. A non-AP STA may store the latest MAAD MAC received from a particular AP such that the next time the non-AP STA associates to that AP, the AP can identify the non-AP STA.

The AP may determine further information or IDs about an associated non-AP STA such as membership number, guest information, family member, subscription, etc. The gathering and determination of such IDs is out-of-scope.

**11.xx.3 Pre-Association with MAAD MAC address**

A non-AP STA that has been allocated a MAAD MAC address, may use that address when directly probing the AP or ESS that allocated that address such that the AP may identify the non-AP STA and note that the particular non-AP STA is within range of the WM.

When a non-AP STA sends an Association Request using an allocated MAAD MAC address as the TA, to the AP that allocated that address, then that AP may identify the non-AP STA before association is started or completed.