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 presented in 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 3/4.

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 can simply use the new MAAD MAC address as the ESS knows it. 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 Assocaition and Reassocaition 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:

*Add following Acronym to 3.4.*

MAAD MAC Address Designation

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

|  |  |  |
| --- | --- | --- |
| **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*

|  |  |  |
| --- | --- | --- |
| **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*

|  |  |  |
| --- | --- | --- |
| **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*

|  |  |  |
| --- | --- | --- |
| **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*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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*

|  |  |  |
| --- | --- | --- |
| **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) 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 as shown below:*

|  |
| --- |
| * WIGTK KDE |

The WIPN corresponds to the WIPN value that was used for computing the MIC in the last protected broadcast or group addressed WUR Wake-up frame and it is used by the receiver as the initial value for the BIP replay counter for the WIGTK.

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

|  |
| --- |
| MAAD MAC |

Octets 6

Figure 12-48a—MAAAD KDE format

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

* EAPOL-Key frame notation

*Modify 12.7.4 (P3215 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 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

*Modify 12.7.6.4 as shown below:*

Message 3 uses the following values for each of the EAPOL-Key frame fields:

Descriptor Type **=** N – see 12.7.2 (EAPOL-Key frames)

Key Information:

Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other cases 0 – same as message 1

Key Type = 1 (Pairwise) – same as message 1

Reserved = 0

Install = 0/1 – For PTK generation, 0 only if the AP does not support key mapping keys, or if the STA has the No Pairwise bit (in the RSN Capabilities field) equal to 1and only the group key is used.

Key Ack = 1

Key MIC = 0 when using an AEAD cipher or 1 otherwise

Secure = 1 (keys installed)

Error = 0 – same as message 1

Request = 0 – same as message 1

Encrypted Key Data = 1

Reserved = 0 – unused by this protocol version

Key Length = Cipher-suite dependent; see Table 12-8 (Cipher suite key lengths)

Key Replay Counter = *n+1*

Key Nonce = ANonce – same as message 1

EAPOL-Key IV = 0 (Version 2) or random (Version 1)

Key RSC = For PTK generation, starting TSC or PN that the Authenticator’s STA uses in MPDUs protected by GTK.

Key MIC = Not present when using an AEAD cipher; or otherwise, MIC(KCK, EAPOL) or MIC(SKCK, EAPOL) – MIC computed over the body of this EAPOL-Key frame with the Key MIC field first initialized to 0

Key Data Length = length of Key Data field in octets

Key Data =

* For PTK generation for the current operating band, the AP’s Beacon/Probe Response frame’s RSNE for the current operating band, and, optionally, a second RSNE that is the Authenticator’s pairwise cipher suite assignment for the current operating band, and, if a group cipher has been negotiated, the GTK and the GTK’s key identifier (see 12.7.2 (EAPOL-Key frames)) for the current operating band, and if management frame protection is negotiated, the IGTK KDE, and if beacon protection is enabled, the BIGTK KDE(11ba), and if WUR frame protection is negotiated, the WIGTK KDE, and when this message 3 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the PMKR1Name calculated according to the procedures of 12.7.1.6.4 (PMK-R1) in the PMKID List field of the RSNE and the FTE with the same contents as in the (Re)Association Response frame, the MDE with the same contents as in the (Re)Association Response frame, the reassociation deadline timeout set to the minimum  of dot11FTReassociationDeadline and the key lifetime in the TIE[ReassociationDeadline], and the PTK lifetime in the TIE[KeyLifetime]; or
* For PTK generation for a supported band other than the current operating band, the Authenticator’s Beacon/DMG Beacon/Announce/Probe Response/Information Response frame’s Multi-band element associated with the supported band, and optionally a second Multi-band element that indicates the Authenticator’s pairwise cipher suite assignment for the supported band, and, if group cipher for the supported band is negotiated, the Multi-band GTK KDE for the supported band if dot11MultibandImplemented is true, or
* For generating a single PTK for all involved bands, the Authenticator’s Beacon/DMG Beacon/Announce/Probe Response/Information Response frame’s RSNE and Multi-band element(s), and optionally, additional RSNE and Multi-band element(s) that indicate the Authenticator’s assignment of one pairwise cipher suite for all involved bands; if a group cipher for all involved bands is negotiated, the GTK and the GTK’s key identifier for all involved bands, if dot11MultibandImplemented is true and both the Authenticator and the Supplicant use the same MAC address in the current operating band and the other supported band(s), or
* For generating different PTKs for the current operating band and other supported band(s), the Authenticator’s Beacon/DMG Beacon/Announce/Probe Response/Information Response frame’s RSNE and Multi-band element(s), and optionally, additional RSNE and Multi-band elements that are the Authenticator’s pairwise cipher suite assignments for one or more involved bands; if group ciphers for the involved bands are negotiated, the Multi-band GTK KDEs for the involved bands, if dot11MultibandImplemented is true and the Joint Multi-band RSNA subfield is 1 for both the Authenticator and Supplicant, and either the Authenticator or the Supplicant uses different MAC addresses for different bands.
* 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.