IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Text for Identifiable Random MAC, IRM - 3 |
| Date: 2022-06 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Instructions:

Abstract

Initial draft text for the Identifiable Random MAC scheme as presented in 22/0894

R1 – corrected document number

*Add following definitions to 3.2.*

**identifiable random medium access control (MAC) (IRM)**: a scheme where a non-AP STA uses identifiable random medium access control (MAC) addresses (IRMA) to prevent third parties from tracking the non-AP STA while still allowing trusted parties to identify the non-AP STA.

**identifiable random medium access control (MAC) address (IRMA):** a randomized medium access control (MAC) address used by a non-AP STA using identifiable random medium access control (MAC) (IRM).

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

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | IRM | The IRM 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> | IRM | The IRM 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> | IRM | The IRM 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> | IRM | The IRM 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 |
| IRM (see 9.4.2.x IRM element) | 255 | <ANA> | No | No |

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

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

**9.4.2.xxx Identifiable Random MAC (IRM) element**

The IRM element is used by a non-AP STA that is using an IRMA. The format of the IRM element is defined in Figure 9–yyy.

|  |  |  |  |
| --- | --- | --- | --- |
| Element ID | Length | Element ID Extension  | IRMA  |

Octets: 1 1 1 1

**Figure – 9-yyy – IRM element format**

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

The IRMA field is a 48-bit MAC address

**12.7.2 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 | <ANA> | IRMA |

*Add the following description of the new KDE at the end of 12.7.2 (P3212 L55) as shown below:*

The format of the IRMK KDE is shown in Figure 12-48aaa (Device ID KDE format).

|  |  |
| --- | --- |
|  | IRMA |
| Octets: | 6 |

Figure 12-48aaa—IRMA KDE format

**12.7.4 EAPOL-Key frame notation**

*Add to 12.7.4 a new line*

 IRMA KDE is a KDE containing an IRMA

12.7.6 4-way handshake

*Modify 12.7.6.1 as follows:*

Message 4: Supplicant  Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,{} or {IRMA KDE}

*Modify 12.7.6.5 as follows*

 Encrypted Key Data = 1 when using an AEAD cipher or if the IRMA KDE is included, or 0 otherwise

 Key Data =

— May include IRMA KDE

*Add new subclause at end of 12.2.*

**12.2.xx Identifiable random MAC (IRM) operation**

**12.2.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. IRM operation enables a non-AP STA to use an identifiable random MAC address for every (re)association. An AP can then store a list of identified non-AP STAs and a non-AP STA can store a list of identities and APs.

A non-AP STA advertises support for IRM by setting the IRM Capability subfield to 1 in the Extended Capabilities element in Probe Request, Association Request and Reassociation Request frames. A non-AP STA includes an IRM element in its Association Request and Reassociation Request frames. An AP advertises support for IRM by setting the IRM Capability subfield to 1 in the Extended Capabilities element in its Beacon and Probe Response frames.

Each time the non-AP STA associates to an AP, the non-AP STA sends the IRMA KDE during the initial 4-way handshake EAPOL-Key msg 4/4. When using FILS authentication, the IRMA is sent in the (Re)Association Request frame. When using FT, the IRMK is sent during the initial mobility domain association EAPOL-Key msg 4/4, but not during the FT protocol reassociations within the same ESS. The AP shall store that IRMA as an identifier for that non-AP STA.

Note: The IRMA is changed on every association to prevent any tracking of the non-AP STA.

Each time the non-AP STA associates to an AP, the non-AP STA uses the IRMA provided at the last association to that AP as the TA.

A list of IRMAs and non-AP STAs shall be stored by the AP and used as an identifier for each non-AP STA that has previously associated. A non-AP STA shall store the last IRMA provided to a particular AP such that the next time the non-AP STA associates to that AP, the AP can identify the non-AP STA.

**12.2.xx.2 Identifiable random MAC (IRM) Address**

A non-AP STA that supports IRM and that intends to be identified, (re)associates to an AP that also supports IRM, using an identifiable random MAC address (IRMA) as its TA. An IRMA is a randomized MAC address constructed from the locally administered address space (see 12.2.10).

**12.2.xx.3 Identifiable random MAC (IRM) pre-association**

A non-AP STA that has previously provided an IRMA to the AP, may use that IRMA as the TA in a directed probe to that AP such that the AP may identify the non-AP STA preassocation.

Note: By sending a directed probe a non-AP STA might advertise its presence to an AP before or without the need to associate.

**12.2.xx.4 Stored IRMAs**

An AP maintains a list of stored IRMAs and non-AP STAs. The AP shall use this list to identify a specific non-AP STA associated to an IRMA. 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 such IDs may be out of scope.

An AP might delete IRMAs from its stored list for various reasons e.g., time, capacity. If, preassocaition, or after association, the AP does not find a corresponding IRMA, then the AP may determine further information or IDs about the associated non-AP STA so as to identify it, and then update the list of stored IRMAs and non-AP STAs with the new IRMA received from the non-AP STA during association.