IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Text for Identifiable Random MAC, IRM  |
| 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

Original Proposed text for the Identifiable Random MAC scheme as presented in 22/0753

This proposal eliminates the use of robust Action frames

Rev 1 – corrected reference, corrected octets in IRMK KDE

Rev 2 – added ANQP element and pre-association text.

*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).

**identifiable random medium access control (MAC) key (IRMK):** a (72-bit) key used to resolve an identifiable random medium access control (MAC) address (IRMA)

*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. |

*Insert new row in Table 9-72 – Element IDs*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Element** | **Element ID** | **Element ID Extension** | **Extensible** | **Fragmentable** |
| IRM (see 9.4.2.xxx IRM element) | 255 | <ANA> | No | No |

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

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | IRM  | The IRM element is present if IRM Capability subfield is set to 1. |

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

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | IRM  | The IRM element is present if IRM Capability subfield is set to 1. |

*Insert new clause 9.4.2.xxx*

**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  | IRM Indicator | IRM OKM(Present only if IRM Indication is “Known”) | IRMK Check(Optional) |

Octets: 1 1 1 1 (9) (2)

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

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

The IRM Indicator field indicates IRM related information as defined in Table 9 – zzz.

 **Table 9–zzz – IRM Indicator**

|  |  |  |
| --- | --- | --- |
| **IRM Indicator bit**  | **Field name** | **Notes** |
| 0 | Private | A non-AP STA sets the IRM Indicator field bit 0 to 1 to indicate that the non-AP STA is using a private random MAC address, i.e., is not using an IRMA. Otherwise bit 0 is set to 0 |
| 1 | Unknown | A non-AP STA sets the IRM Indicator field bit 1 to 1 to indicate that the non-AP STA has not previously provided an IRMK to the AP. Otherwise bit 1 is set to 0 |
| 2 | Known | A non-AP STA sets the IRM Indicator field sets bit 3 to 1 to indicate that the non-AP STA has previously provided an IRMK to the AP. Otherwise bit 3 is set to 0. |
| 3-7 | Reserved |  |

The IRM OKM field is not present if the IRM Indicator field is set to “Private” or “Unknown". The IRM OKM field is a (72-bit) hash that is derived from the IRMA and the IRMK as defined in 12.2.xx.2.

The IRM Check field is defined in 9.2.4.xxx.1.

**9.2.4.xxx.1 IRMK Check field**

The IRMK Check field is optionally present in the IRM element if the IRM Indicator field is set to Known.

The format of the IRM Check field is shown in Figure 9-jjj

|  |  |
| --- | --- |
| IRMK Offset | Check |

 Octets: 1 1

**Figure – 9-jjj – IRMK Check field format**

The IRMK Offset field has a value N between 0 and 56.

The Check field contains 8 bits representing the EX-OR of the 8 bits of the IRMK, bN to bN+7 with the following 8 bits (bN+8 to bN+15).

i.e. For n = 0 to 7 the 8 bits in Check field are:

 bn = EX-OR (bN+n, bN+n+8) where bN is Nth bit in IRMK

Note: As an example, if the IRMK Offset field has a value of 42, then the Check field b0 is EX\_OR of b42 and b50 of the IRMK, and Check field b7 is EX-OR of b49 and b57 of the IRMK.

*Insert new row to Table 9-404 - ANQP-element definitions*

|  |  |  |
| --- | --- | --- |
| **ANQP-element name** | **InfoID** | **ANQP-element (subclause)** |
| Identifiable Random MAC (IRM)  | <ANA> | 9.4.5.aaa |

*Insert new Clauses to 9.4.5.*

**9.4.5.aaa Identifiable Random MAC (IRM) ANQP-element**

The IRM ANQP-element is used by a non-AP STA that is using an IRMA and has previously provided an IRMK to that AP. The format of the IRM ANQP-element is defined in Figure 9 – xyz.

|  |  |  |  |
| --- | --- | --- | --- |
| Info ID | Length | IRM OKM | IRM Check (optional) |

 Octets: 1 1 9 2

**Figure – 9-xyz – IRM ANQP-element format**

The Info ID and Length fields are defined in 9.4.5.1 (General)

The IRM OKM field is a (72-bit) hash that is derived from the IRMA and the IRMK as defined in 11.xx.2.

The IRM Check field is optionally present and is defined in 9.4.xx.1.

The Info ID and Length fields are defined in 9.4.5.1 (General)

**9.4.5.bbb IRMK element**

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

|  |  |  |  |
| --- | --- | --- | --- |
| Element ID | Length | Element ID Extension  | IRMK  |

Octets: 1 1 1 9

**Figure – 9-xxy – IRMK element format**

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

**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> | IRMK |

*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).

|  |  |
| --- | --- |
|  | IRMK |
| Octets: | 9 |

Figure 12-48aaa—IRMK KDE format

**12.7.4 EAPOL-Key frame notation**

*Add to 12.7.4 a new line*

 IRMK KDE is a KDE containing an IRMK

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 {IRMK KDE}

*Modify 12.7.6.5 as follows*

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

 Key Data =

— May include IRMK 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.

To indicate that the non-AP STA intends to be identifiable, the non-AP STA sets the IRM Indicator field to “Unknown”, or “Known”. If the non-AP STA intends that it not be identifiable, the IRM element does not include an IRM OKM field and the IRM Indicator field is set to “Private”.

Each time the non-AP STA associates to an AP, the non-AP STA sends the IRMK KDE during the initial 4-way handshake EAPOL-Key msg 4/4. When using FILS authentication, the IRMK 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 IRMK as an identifier for that non-AP STA.

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

When a non-AP STA associates with an IRMA as the TA, and indicates “Unknown”, the IRM element does not include the IRM OKM field.

When a non-AP STA associates with an IRMA as the TA, and indicates “Known”, the IRM element includes an IRM OKM field and may include the IRMK Check field. The IRM OKM field value is derived from the IRMA and the IRMK that was provided by the non-AP STA at the last association with that AP. The AP shall calculate an IRM OKM value using each of its stored IRMKs until it finds the IRMK that produces the same IRM OKM value as that included in the IRM element. If the non-AP STA included an IRMK Check field in the IRM element, then the AP can use the information in the IRM Check field to reduce the number of IRMKs that need to be checked. .

A list of IRMKs 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 IRMK exchanged with a particular AP such that the next time the non-AP STA associates to that AP, the AP can identify the non-AP STA.

**11.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). To indicate that the non-AP STA intends to be identifiable, the IRM OKM field is included in the IRM element.

**11.xx.2 Identifiable random MAC (IRM) OKM**

The IRM OKM field value is the HKDF-Expand function of the IRMK and the IRMA.

 IRM OKM = HKDF-Expand (IRMK, IRMA, 9)

The 72-bit IRM OKM field is included in the IRM element when the non-STA intends to be identifiable.

**11.xx.3 Identifiable random MAC (IRM) association**

A non-AP STA that supports IRM shall include the IRM element in Association and Reassociation Request frames.

If the non-AP STA has not previously provided an IRMK to the AP, then the IRM Indicator field value in the IRM element in the Association Request frame, shall be set to “Unknown”. If the non-AP STA has previously provided an IRMK to the AP, the IRM Indicator field shall be set to “Known”. If the IRM Indicator is set to “Known”, the IRMK Check field may be included in the IRM element.

Note: Including the IRM Check field in the IRM element enables an AP to reduce by a factor of 256 the number of possible IRMKs to be checked.

If the non-AP STA is not associating with an IRMA but with a private randomized MAC address, then the IRM Indicator field value in the IRM element in the Association or Reassociation Request frame, shall be set to “Private” and neither the IRM OKM field nor the IRMK Check field shall be present in the IRM element.

If a non-AP STA associates to an AP for the first time, using an IRMA, the IRM Indicator field is set to “Unknown”. The non-AP STA shall omit the IRM OKM field and the IRMK Check field in the IRM element.

If, in an (Re)Association Request frame, the IRM Indicator field value in the IRM element is set to “Known”, the non-AP STA shall include the IRM OKM field in the IRM element and may include an IRMK Check field. The IRMK Check field may be used by an AP to down-select stored IRMKs and reduce the number of calculations required in order to find the correct IRMK. The AP may, prior to association, check through its stored IRMKs to determine the IRMK that, together with the IRMA, produces the IRM OKM value that the non-AP STA included in the IRM element in the Association Request frame. Alternatively, the AP shall, after association, check its stored IRMKs in order to determine the IRMK that, together with the IRMA, produces the IRM OKM value that the non-AP STA included in the IRM element. The AP shall then store the new IRMK, provided by the non-AP STA during association, as the identifier for that non-AP STA.

The IRMA, IRM OKM and IRMK change for every association.

Note: Because the IRMA, IRM OKM and the IRMK change for every it is impossible for a third party to identify the non-AP STA.

**12.2.xx.4 Identifiable random MAC (IRM) pre-association**

A non-AP STA, using an IRMA as the TA, that has previously provided an IRMK to an AP, may send an IRM ANQP-element to that AP that contains the IRM OKM field and may contain an IRM Check field, such that the AP can identify the non-AP STA pre association using the stored IRMKs.

A non-AP STA, using an IRMA as the TA, that has previously exchanged an IRMK with an AP, may include the IRM element in a directed probe to the AP with the IRM indicator field set to “Known”. A non-AP STA should use a different IRMA as the TA together with a different IRM OKM in every directed probe.

Note 1: By sending a directed probe a non-AP STA might advertise its presence to an AP before or without the need to associate.

Note 2: When using a series of directed probes, the non-AP STA may change the IRMA and IRM OKM values for each probe, the IRM OKM being calculated each time using the same IRMK.

**12.2.xx.5 Stored IRMKs**

An AP maintains a list of stored IRMKs and non-AP STAs. The AP shall use this list to identify a specific non-AP STA to an IRMK. 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 IRMKs from its stored list for various reasons e.g., time, capacity. If a non-AP STA sets the IRM Indicator field in the IRM element to “Known”, and the AP does not find a corresponding IRMK, 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 IRMKs and non-AP STAs with the new IRMK received from the non-AP STA during association.