IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Text for Identifiable Random MAC, IRM  |
| Date: 2021-10 |
| 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 Identifiable Random MAC scheme as presented in 21/1585

Rev 1

* Added “No IRMK found” reason code to New IRMK request to cover case where AP has deleted “old” IRMKs. AP might delete IRMKs for time or capacity.
* Added “Private” to IRM element such that an IRM STA can still use private MAC address when indicating support for IRM. This eliminates the I/G bit set to 1.

Rev 2

* Correction to Element format figure.
* Edits to frame names
* Added IRMK Check field
	+ provides a hint to AP such that AP can quickly find the IRMK
	+ AP can confirm IRMK and STA can check without declaring the IRMK.

Rev 3

* Use Change to prevent any brute-force attack
* Typos and minor edits

Rev 4

* Removed “Provide IRMK” (No good use case)

Rev 5

* Edits

Note: The following instructions relate to 802.11me D0.3

*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 (128-bit) key used to resolve an identifiable random medium access control (MAC) address (IRMA)

*Insert new row in Table 9-79 Action field Clause 9.4.1.11*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Code** | **Meaning** | **See subclause** | **Robust** | **Group addressed Privacy** |
| <ANA> | IRM  | 9.6.aa | Yes | No |
| <ANA> -125 | Reserved |  |  |  |

*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 9-128 – 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 Hash(Not present if IRM Indicator set to 0) | IRMK Check(Optional) |

Octets: 1 1 1 1 (16) (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 field value** | **Field name** | **Notes** |
| 0 | Private | A non-AP STA sets the IRM Indicator field value to 0 to indicate that the non-AP STA is using a private random MAC address, i.e., is not using an IRMA  |
| 1 | Unknown | A non-AP STA sets the IRM Indicator field value to 1 to indicate that the non-AP STA has not previously provided an IRMK to the AP |
| 2 | Known | A non-AP STA sets the IRM Indicator field value to 2 to indicate that the non-AP STA has previously provided an IRMK to the AP |
| 3 | Change | A non-AP STA sets the the IRM Indicator field value to 3 to indicate that the non-AP STA has previously provided an IRMK to the AP but will change the IRMK once associated |
| 3-255 | Reserved |  |

The IRM Hash field is not present if the IRM Indicator field is set to 0. The IRM Hash field is a (128-bit) hash that is derived from the IRMA and the IRMK as defined in 11.xx.2.

**9.2.4.xxx.1 IRM Check field**

The IRM Check field is optionally present in the IRM element if the IRM Indicator field is set to Known or Change and is preset in the IRM Confirm Action field.

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 112.

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 72, then the Check field b0 is EX\_OR of b72 and b80 of the IRMK, and Check field b7 is EX-OR of b79 and b87 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 Clause 9.4.5.aaa*

**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 Hash | IRM Check (optional) |

 Octets: 1 1 16

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

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

The IRM Hash field is a (128-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.

*Insert new clause at end of 9.6 Action frame format details*

**9.6.aa IRM Action frame details**

**9.6.aa.1 General**

Several Action frame formats are defined for IRM purposes. These frames are identified by the single octet IRM Action field, which follows immediately after the Category field. The values of the IRM Action field are defined in Table 9-bbb (IRM Action field).

**Table 9-bbb – IRM Action field**

|  |  |
| --- | --- |
| **Action field value** | **Meaning** |
| 0 | IRMK Request |
| 1 | IRMK Response |
| 2 | IRMK Confirm |
| 3 | New IRMK Request  |
| 4-255 | Reserved |

**9.6.aa.2 IRMK Request**

The IRMK Request Action frame is transmitted by an AP to a non-AP STA that associated to the AP with the IRM Capability bit set to 1 in the Extended Capabilities field, the IRM element includes an IRM Hash field, and the IRM Indicator field in the IRM element is set to “Unknown”. The format of the IRMK Request Action field is shown in Figure 9-ccc.

|  |  |
| --- | --- |
| Category | IRM Action |

 Octets: 1 1

**Figure – 9-ccc – IRMK Request Action field format**

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined in Table 9-bbb in 9.6.aa.1 (General).

**9.6.aa.3 IRMK Response**

The IRMK Response Action frame is transmitted from a non-AP STA to an AP in response to an IRMK Request frame. The format of the IRMK Request Action field is shown in Figure 9-ddd.

|  |  |  |
| --- | --- | --- |
| Category | IRM Action | IRMK |

 Octets: 1 1 16

**Figure – 9-ddd – IRMK Response Action field format**

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined in Table 9-bbb in 9.6.aa.1 (General).

The IRMK field is a (128-bit) key that is used together with the IRMA to derive the value of the IRM Hash field that is sent in the IRM element.

**9.6.aa.4 IRMK Confirm**

The IRMK Confirm Action frame is transmitted from an AP to a non-AP STA to confirm that an IRMK has been recognized. The format of the IRMK Confirm Action field is shown in Figure 9-eee.

|  |  |  |
| --- | --- | --- |
| Category | IRM Action | IRMK Check |

 Octets: 1 1 2

**Figure – 9-eee – IRMK Confirm Action field format**

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined in Table 9-bbb in 9.6.aa.1 (General).

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

**9.6.aa.5 New IRMK Request**

The New IRMK Request Action frame is transmitted by an AP to a non-AP STA when an AP requests the non-AP STA to provide a new IRMK. The format of the new IRMK Request Action field is shown in Figure 9-iii.

|  |  |  |
| --- | --- | --- |
| Category | IRM Action | IRMK Reason |

 Octets: 1 1 1

**Figure – 9-iii – New IRMK Request Action field format**

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined in Table 9-bbb in 9.6.aa.1 (General).

The values of the IRMK Reason field are defined in Table 9-ddd

**Table 9-ddd – IRMK Reason field values**

|  |  |
| --- | --- |
| **IRMK Reason field value** | **Meaning** |
| 0 | No reason provided |
| 1 | Non-AP STA requested change |
| 2 | No IRMK found |
| 3 | Duplicate Key exists |
| 4 | Key not random |
| 5-255 | Reserved |

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

**11.xx Identifiable random MAC (IRM) 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. IRM operation enables a non-AP STA to use a random MAC address for every (re)association, or pre association.

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

To indicate that the non-AP STA intends to be identifiable, an IRM Hash field is included in the IRM element. If the non-AP STA intends to not be identifiable, then in the IRM element, the IRM Indicator field is set to “Private” and the IRM Hash field is not present.

A non-AP STA generates a 128-bit IRMK which may be constant or may vary for each SSID or AP or ESS. A non-AP STA may request an IRMK from an AP. The non-AP STA uses a randomized MAC address, as its TA, and sends an IRM element to the AP. If the non-AP STA intends that it be identifiable, the IRM element includes an IRM Hash field and the randomized MAC address is an IRM Address (IRMA). If the non-AP STA intends that it not be identifiable, the IRM element does not include an IRM Hash field and the IRM Indicator field is set to “Private”. The IRM Hash value is derived from the IRMA and an IRM Key (IRMK). An IRMK may be stored by the AP and used as an identifier for that non-AP STA. A non-AP STA may store the IRMK exchanged with a particular AP such that each 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, 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, an IRM Hash field is included in the IRM element.

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

The IRM Hash field value is the SHA-256/128 function of the IRMK and the IRMA. SHA-256/128 is the truncated SHA-256 where the leftmost 128 bits of the 256-bit hash generated by SHA-256 are selected as the truncated 128 bit IRM Hash

 IRM Hash = SHA-256/128 (IRMK, IRMA)

The 128-bit IRM Hash field is included in the IRM element and the IRM-ANQP element.

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

The non-AP STA includes the IRM element in the Association Request frame. The AP includes the IRM element in its beacons.

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, is set to “Unknown”. If the non-AP STA has previously provided an IRMK to the AP, then the IRM Indicator field value is set to “Known”. If the non-AP STA has previously provided an IRMK to the AP, but intends to change the IRMK once associated, then the IRM Indicator field value is set to “Change”.

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 Request frame, is set to “Private” and neither the IRM Hash field nor the IRMK Check field is present in the IRM element.

If a non-AP STA associates to an AP using an IRMA and the IRM Indicator field is set to “Unknown”, the non-AP STA constructs an IRMK and calculates the IRM Hash value (see 11.xx.2). Once associated, the AP transmits an IRMK Request frame to the non-AP STA and the non-AP STA sends an IRMK Response frame to the AP that includes the IRMK that the non-AP STA has used to calculate the IRM Hash value that was sent in the IRM element. The AP may calculate an IRM Hash value using the IRMA and the IRMK provided by the non-AP STA, and confirm that it is identical to the IRM Hash provided by the non-AP STA in the IRM element.

If, in the Association Request frame, the IRM Indicator field value in the IRM elelent is set to “Known”, or “Change”, the non-AP STA shall also include in the IRM element the IRM Hash field and may include the IRMK Check field.

Note: An AP might use the IRMK Check field to down select stored IRMKs and reduce the number of hash calculations in order to find the correct IRMK.

The AP may, prior to association, check the stored IRMK(s) in order to determine the IRMK that, together with the IRMA, produces the IRM Hash value that the non-AP STA included in the IRM element. Alternatively, the AP shall, after association, check the stored IRMK(s) in order to determine the IRMK that, together with the IRMA, produces the IRM Hash value that the non-AP STA included in the IRM element. After the non-AP STA has associated, the AP shall transmit an IRMK Confirm frame, including the IRMK Check field, to the non-AP STA to inform the non-AP STA that its IRMK has been confirmed and the non-AP STA has been recognized.

If, in the Association Request frame, the IRM Indicator field value is set to “Change”, once the non-AP STA is associated and the AP has determined the IRMK for the non-AP STA, the AP shall transmit a New IRMK Request frame with the IRMK Reason field value set to 1 (“non-AP STA requested change”). The non-AP STA may then transmit an IRMK Response frame with the new IRMK. The AP shall then use this IRMK as the new identifier for the non-AP STA.

When associated, a non-AP STA may send an IRMK Response Action frame to the AP at any time in order to change its IRMK.

An AP may request an associated non-AP STA to provide a new IRMK by sending a New IRMK Request Action frame to the non-AP STA. The AP shall include a reason for the request in the IRMK Reason field, see Table 9-ccc. The non-AP STA may either respond with an IRMK Response Action frame that includes a new IRMK to be used as its identifier, or may ignore the request, or may take other action such as disassociate. 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 request the associated non-AP STA to provide an IRMK by sending a New IRMK Request Action frame to the non-AP STA with the IRM Reason field set to 2 (“No IRMK found”). The non-AP STA may then respond with an IRMK Response Action frame that includes a new IRMK or may provide the orginal IRMK.

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

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

*Make following edits to 12.2.10*

*P3034.54*

~~However,~~ Unless the non-AP STA is using identifiable random MAC (IRM) (see 11.xx), the non-AP STA shall not change its MAC address during a transactional exchange,

P3035.21

Unless the non-AP STA is using identifiable random MAC (IRM) (see 11.xx), ~~The~~ the non-AP STA connecting to an infrastructure BSS shall retain a single MAC address for the duration of its connection across an ESS