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

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

*Add following definitions to 3.2.*

**identifiable random medium access control (MAC) (IRM)**: a random medium access control (MAC) scheme used by a non-AP STA 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 random medium access control (MAC) address used by a 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 and an IRMA is in use. |

*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 and an IRMA is in use. |

*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 | Element ID Extension | Length | IRM Indicator | IRM Hash |

 Octets: 1 1 1 1 16

**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 | Unknown | A non-AP STA sets the IRM Indicator field value to 0 to indicate that the non-AP STA has not previously provided an IRMK to the AP |
| 1 | Known | A non-AP STA sets the IRM Indicator field value to 1 to indicate that the non-AP STA has previously provided an IRMK to the AP |
| 2 | Change | A non-AP STA sets the the IRM Indicator field value to 2 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 a (128 bit) hash that is derived from the IRMA and the IRMK as defined in XXXXX.

*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 |

 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.

*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 ocy=tet IRM Action field, which flows immediately after the Category field. The values of the IRM Action field are defined in Table 9-bbb (IRM Action field values).

**Table 9-bbb – IRM Action field values**

|  |  |
| --- | --- |
| **Action field value** | **Meaning** |
| 0 | IRMK Request |
| 1 | IRMK Response |
| 2 | IRMK Confirm |
| 3 | Provide IRMK Request  |
| 4 | Provide IRMK Response  |
| 5 | Provide IRMK Confirm  |
| 6 | New IRMK Request  |
| 7-255 | Reserved |

**9.6.aa.2 IRMK Request frame format**

The IRMK Request 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, using an IRMA, and has set the Unknown field in the IRM element to 1. The format of the IRMK Request frame Action field is shown in Figure 9-ccc.

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

 Octets: 1 1

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

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined in 9.6.aa.1 (General).

**9.6.aa.3 IRMK Response frame format**

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

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

 Octets: 1 1 16

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

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined 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 that is sent in the IRM element.

**9.6.aa.4 IRMK Confirm frame format**

The IRMK Confirm 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 frame Action field is shown in Figure 9-eee.

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

 Octets: 1 1

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

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined in 9.6.aa.1 (General).

**9.6.aa.5 Provide IRMK Request frame format**

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

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

 Octets: 1 1

**Figure – 9-fff – Provide IRMK Request frame Action field format**

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined in 9.6.aa.1 (General).

**9.6.aa.6 Provide IRMK Response frame format**

The Provide IRMK Response frame is transmitted from an AP to a non-AP STA in response to a Provide IRMK Request frame. to confirm the value of the IRMK that the AP has determined based upon the IRM Hash, the IRMA. The format of the IRMK Confirm frame Action field is shown in Figure 9-ggg.

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

 Octets: 1 1 16

**Figure – 9-ggg – Provide IRMK Response frame Action field format**

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined in 9.6.aa.1 (General).

The IRMK field is a 128-bit key chosen by the AP.

Note: An IRMK value of 0 in the IRMK field indicates that the AP has chosen not to provide an IRMK.

**9.6.aa.7 Provide IRMK Confirm frame format**

The Provide IRMK Confirm frame is transmitted by a non-AP STA to an AP to confirm acceptance of an IRMK that has been sent in a Provide IRMK Response frame. The format of the Provide IRMK Confirm frame Action field is shown in Figure 9-hhh

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

 Octets: 1 1 1

**Figure – 9-hhh – Provide IRMK Confirm frame Action field format**

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined in 9.6.aa.1 (General).

The values of the Result field are defined in Table 9-ccc.

**Table 9-ccc – Provide IRMK Confirm Result field values**

|  |  |
| --- | --- |
| **Result field value** | **Meaning** |
| 0 | Accepted |
| 1 | Not accepted – no reason |
| 2 | Not accepted – provide another IRMK |
| 3-255 | Reserved |

**9.6.aa.8 New IRMK Request frame format**

The New IRMK Request 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 frame Action field is shown in Figure 9-iii.

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

 Octets: 1 1 1

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

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined 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 | Duplicate Key exists |
| 3 | Key not random  |
| 3-255 | 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.

A non-AP STA generates an 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 an IRMA as its TA, and sends an IRM element to the AP. The IRM element includes an IRM Hash. The IRM Hash 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, supporting IRM, associates to an AP, that also supports IRM, using an identifiable random MAC address (IRMA). An IRMA is a random MAC address with the “I/G” bit set to 0 and the “U/L” bit set to 1 (see Figure 9-1) with the remaining 46 bits randomly selected.

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

The IRM Hash 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 is included 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. If the non-AP STA has not previously provided an IRMK to the AP, then the IRM Indicator field value 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”.

An AP recognizes that the non-AP STA has used an IRMA as its TA, and that the non-AP STA has set the IRM Capability sub-field to 1 in the Extended Capabilities field. The first time that a non-AP STA associates to an AP using an IRMA, the non-AP STA chooses an IRMK and calculates the IRM Hash (see 11.xx.2). In the IRM element, the non-AP STA sets the IRM Indicator field value in the IRM element to “Unknown”, and the IRM Hash field to the calculated value. 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 the IRM Indicator field value is set to “Known”, or “Change”, 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 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 that the non-AP STA included in the IRM element. Optionally, after the non-AP STA has assocated, the AP may transmit an IRMK Confirm frame 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 set to 1. The non-AP STA shall then transmit an IRMK Response frame with the new IRMK. The AP shall then use this IRMK as the identifier for the non-AP STA.

A non-AP STA may request the AP for an IRMK. Once associated, either in response to an IRMK Request frame, or at any time, a non-AP STA may send a Provide IRMK Request frame to the AP and the AP shall respond with a Provide IRMK Response frame that contains an IRMK selected by the AP. An AP may set the IRMK field in the Provide IRMK Response frame to 0, indicating that the AP has chosen to not provide an IRMK. The non-AP STA shall send a Provide IRMK Confirm frame setting the Result field to indicate accept or not accept (see Table 9.ccc).

An AP may request an associated non-AP STA to provide a new IRMK by sending a New IRMK Request 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 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.

When associated, a non-AP STA may send an IRMK Response frame to the AP at any time in order to change its 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 calculated using the IRMA and the IRMK, such that the AP can identify the non-AP STA pre association.

*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

P3035.42

Unless the non-AP STA is using identifiable random MAC (IRM) (see 11.xx), ~~A~~ a non-AP STA that receives from an AP an Extended Capabilities field with the Local MAC Address Policy