IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed Text for incorporating MAAD, IRM and RRCM into TGbh Draft 0.2 | | | | |
| Date: 2022-09 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

Device ID indication, MAAD and IRM and RRCM will be covered.

IRM and RRCM support is to accomodate non-AP STAs that prefer to allocate their MAC addresses rather than have the AP allocate. The AP can still not support IRM or RRCM if it insists on being the allocater.

AP and STA can advertise support for any, combinations or all.

Device ID – AP sends ID in msg 3, STA sends ID back in msg 2 on every association

MAAD – AP sends MAAD MAC in msg 3 on every association, STA uses MAAD MAC as TA on next association.

IRM – STA sends IRMA in msg 2 on every association. STA uses the IRMA as TA on the next association.

RRCM - a non-AP STA and AP generate the same non-AP STA Random MAC address or addresses (RMA(s)) to be used in the next association(s) through following the same procedure

NOTE: If AP sees IRMA or RRCM in msg 2, AP does not send MAAD in msg 3.

See 22/0908r1 for detailed discussion on how the schemes simply co-exist.

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 IRM scheme uses an ID allocated by the STA during a previous RSN association as the TA for a new association. The TA is changing every association

In the RRCM scheme a non-AP STA and AP generate the same non-AP STA Random MAC address or addresses (RMA(s)) to be used in the next association(s) through following the same procedure. The non-AP STA can use the RMA(s) in its next association(s) and will be identified by the AP.

The following provides the instructions for inserting the new text into Draft 0.2.

Instructions:

802.11 bh Draft 0.2 is base

*Add the following definitions t o 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).

**Rule-based Random and Changing MAC Address (RRCM):** A privacy enhancement mechanism for non-AP STA and AP to generate one or more Random Mac Addresses (RMA) for use by non-AP STA in order to prevent non-AP STA from being tracked (by third parties) and still allow the non-AP STA to be identified by the AP in subsequent message exchanges. “Rule-based” implies that the non-AP STA and AP apply the same procedures for generating RMA or RMAs locally at their sides.

**RMAK (RMA Key):** RMAK is the key that is used to generate one or more Random Mac Addresses (RMA) for RRCM procedure

*Add following Acronym to 3.4.*

MAAD MAC Address Designation

*At 4.5.4.10, edit last sentence to read*

Such a STA, when reconnecting to a network, can opt-in to exchange a device identifier that allows the network to recognize the device and/or use a MAC address that has been allocated by the network or the STA, whilst still protecting the information from third parties.

***Clause 6.3***

***We might need an “MLME-RCM” primitive so that the SME can instruct the MLME to set up which schemes (device ID, MAAD, IRM, RRCM) the STA will support. Work in ARC and TGme will probably change the way this is written. The primitive will consist of a single MLME-RCM.request. Discussions in TGbh to decide if MIB or MLME.***

*At 9.3.3.5 Association Request frame format*

*Insert new row in Table 9-62 Association Request frame body P23*

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | Device ID | The Device ID element is optionally present when using FILS authentication; otherwise, it is not present. |
| <ANA> | MAAD | The MAAD element is optionally present when using FILS authentication; otherwise, it is not present |
| <ANA> | IRM | The IRM element is optionally present when using FILS authentication; otherwise, it is not present |
| <ANA> | RRCM | The RRCM element is present when using FILS authentication; otherwise, it is not present. |

*At 9.3.3.6 Assocaition Response frame format*

*Insert new row in Table 9-63 Association Response frame body P1031*

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | Device ID | The Device ID element is optionally present when using FILS authentication; otherwise, it is not present. |
| <ANA> | MAAD | The MAAD element is optionally present when using FILS authentication; otherwise, it is not present |
| <ANA> | IRM | The IRM element is optionally present when using FILS authentication; otherwise, it is not present |
| <ANA> | RRCM | The RRCM element is present when using FILS authentication; otherwise, it is not present. |

*Insert new rows 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 |
| <ANA> | IRM | The IRM element is optionally present when using FILS authentication; otherwise, it is not present |
| <ANA> | RRCM | The RRCM element is present when using FILS authentication; otherwise, it is not present. |

*Insert new rows 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 |
| <ANA> | IRM | The IRM element is optionally present when using FILS authentication; otherwise, it is not present |
| <ANA> | RRCM | The RRCM element is present when using FILS authentication; otherwise, it is not present. |

*At 9.4.2.1 Insert new rows in Table 9-128 Element IDs P23*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element | Element ID | Element ID Extension | Extensible | Fragmentable |
| Device ID (see 9.4.2.x (Device ID element)) | 255 | <ANA> | No | No |
| MAAD (see 9.4.2.xx MAAD element) | 255 | <ANA> | No | No |
| IRM (see 9.4.2.xxx IRM element) | 255 | <ANA> | No | No |
| RRCM (see 9.4.2.xxxx RRCM element) | 255 | <ANA> | No | No |

*At 9.4.2.241 Insert new rows in Table 9-363 Extended Capabilities field, P24*

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| <ANA> | Device ID support | The STA sets the Device ID Support field to 1 to indicate support for Device ID indication. Otherwise, the STA sets the Device ID field to 0. |
| <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. |
| <ANA> | IRM Capability | A STA sets IRM Capability subfield to 1 to indicate support for MAAD and sets to 0 if IRM is not supported. |
| <ANA> | RRCM Capability | The STA sets RRCM Capability subfield to 1 to indicate support for RRCM Capability and sets to 0 if not supported. |

*Insert following subclauses after 9.4.2.296a “Device ID element” P 24*

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.

**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

**9.4.2.xxx RRCM element**

The RRCM element contains Seed and Counter fields that are used in RRCM procedure. The format of the RRCM element is shown in Figure 9-xxx (RRCM element format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | Seed | Counter |

Octets 1 1 1 16 2

Figure 9-xxx - RRCM element format

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

Seed and Counter are values to generate one or more RMA for RRCM procedure. For details, see subclause **12.2.11.4.**

**.**

**12. Security**

*Add the following new subclause after 12.2.10*

**12.2.11 Mitigation of random and changing changing MAC address**

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. Device ID indication, MAAD, IRM and RRCM may be used to identify the non-AP STA whilst still being unidentifiable to a third party.

When using device ID indication, an AP may provide a device ID, contained in a device ID KDE in EAPOL Key-message 3 of the 4-way handshake, to a non-AP STA and the non-AP STA may provide that same device ID, in a device ID KDE in EAPOL Key-message 2 of the 4-way handshake, to any AP in the same ESS to allow the network to recognize the same non-AP STA when it returns to the ESS even if it changes its MAC address.

When using MAAD, an AP may provide a random MAC address (MAAD MAC address) contained in a MAAD KDE in EAPOL Key-message 3 of the 4-way handshake, to a non-AP STA when it associates, and the non-AP STA may then use that MAAD MAC address as its TA when associating the next time to that ESS or AP. Hence, that AP or ESS can also recognize that non-AP STA pre-association.

When using IRM, a non-AP STA, when associating, may provide a random identifiable random MAC address (IRMA), contained in an IRMA KDE in EAPOL Key-message 2 of the 4-way handshake, to an AP. The non-AP STAA may then use that IRMA as its TA when associating the next time to that ESS or AP. Hence, that AP or ESS can also recognize that non-AP STA pre-association.

When using RRCM, a non-AP STA and AP generate the same non-AP STA Random MAC address or addresses (RMA(s)) to be used in the next association(s) through following the same procedure. The non-AP STA can use the RMA(s) in its next association(s) and will be identified by the AP.

A non-AP STA and an AP may indicate support for device ID indication, MAAD, IRM or RRCM either individually or in combination. An MLME-RCM.request may be used to set which scheme(s) the STA supports. A non-AP STA and an AP may indicate support for device ID indication, MAAD, IRM or RRCM either individually or in combination.

No combination of MAAD, IRM or RRCM can be used at the same time. If the AP and non-AP STA indicate support for MAAD, IRM and/or RRCM then if the non-AP STA includes an IRMA KDE or an RRCM KDE in EAPOL Key-message 2 of the 4-way handshake, then the AP shall not include a MAAD KDE in EAPOL-Key message 3 of the 4-way handshake. A non-AP STA shall not include an IRMA KDE and an RRCM KDE in EAPOL Key-message 2 of the 4-way handshake.

***Renumber Device ID indication clause 12.2.11 as 12.2.11.1. Then delete the first paragraph and retain the rest (with changes as appropriate from the CID resolutions)***

**12.2.11.1 Device ID indication**

~~An AP may provide an identifier to a non-AP STA and the non-AP STA may opt-in to providing that identifier to any AP in the same ESS to allow the network to recognize the same non-AP STA when it returns to the ESS even if it changes its MAC address. Exchanges of this identifier information are protected from third parties to limit the tracking capability to the APs in an ESS~~.

***Following existing text subject to change from CIDs***

A non-AP STA indicates support for this capability in the Device ID Support subfield in the Extended RSN Capabilities field (see 9.4.2.241 (RSN Extension Element)). An AP shall not send an identifier to a non-AP STA that does not indicate support for this capability.

When using FILS authentication, the non-AP STA sends the identifier, if it has one and opts-in to using it, in the Association Request frame and the AP sends a new identifier in the Association Response frame. When using FT, the non-AP STA sends the identifier, if it has one and opts-in to using it, during the initial mobility domain association the EAPOL-Key message 2/4 and the AP sends a new identifier in the EAPOL-Key message 3/4; the identifier or a new identifier are not exchanged during the FT protocol reassociations within the same ESS. For other cases, the non-AP STA sends the identifier, if it has one and opts-in to using it, during the initial 4-way handshake in the EAPOL-Key message 2/4 and the AP sends a new identifier in the EAPOL-Key message 3/4. When the non-AP STA sends the opaque identifier, it shall send the most recently received value from an

AP in the ESS without modification.

***Insert following sub clauses 12.2.11.2 and 12.2.11.3***

**12.2.11.2 MAC Address Designation (MAAD) operation**

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 may allocate a new MAAD MAC address to the non-AP STA by including a MAAD KDE in EAPOL-Key message 3 of 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 next associates to that same AP or another AP in the same ESS. In so doing, the AP/ESS will identify the non-AP STA. When reassocating to the same AP or another AP in the same ESS, the non-AP STA uses the MAAD MAC address that it used for the association.

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.

The MAAD MAC address is 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. 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 should 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.

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 can identify the non-AP STA before association is started or completed. A non-AP STA should use a random MAC address when sending Probe Requests. 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 when directed by the AP or ESS such that, for example, the ESS may steer the non-AP STA to an appropriate AP. Such steering applications are outside of scope. A non-AP STA that has been allocated a MAAD MAC address, may use that address in an ANQP packet so that the AP that allocated that MAAD MAC may identify the non-AP STA, i.e., the non-AP STA had previously associated with that AP.

**12.2.11.3 Identifiable random MAC (IRM) operation**

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 message 2 of the 4-way handshake. When using FILS authentication, the IRMA is sent in the (Re)Association Request frame. When using FT, the IRMA is sent during the initial mobility domain association EAPOL-Key message 2 of the 4-way handshake, 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.

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). 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 so 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.

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. An AP might delete IRMAs from its stored list for various reasons e.g., time, capacity. If, preassociation, or after association, the AP does not find a corresponding IRMA, then the AP may use the device ID 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.

When a non-AP STA sends an Association Request using an IRMA as the TA, then that AP can identify the non-AP STA before association is started or completed. A non-AP STA should use a random MAC address when sending Probe Requests. A non-AP STA may use an IRMA when directly probing the AP or ESS that knows that IRMA when directed by the AP or ESS such that the ESS may steer the non-AP STA to an appropriate AP. Such steering applications are outside of scope. A non-AP STA using an IRMA, may use that address in an ANQP packet so that the AP which nows that IRMA may identify the non-AP STA, i.e., that non-AP STA had previously associated with that AP.

**12.2.11.4 Rule-based Random and Changing MAC Address (RRCM)**

**12.2.11.4.1 General**

To improve its privacy, a non-AP STA may desire to use a random MAC address (RMA) while still being identifiable by the same AP in subsequent associations. Rule-based Random and Changing MAC address (RRCM) allows for identification despite randomly changed MAC address at later associations., When a non-AP STA associates to an AP with one MAC address, it can still be recognized by the AP and ESS after the non-AP STA changes its MAC address before reconnecting to the same AP and ESS.

Through RRCM, a non-AP STA and AP can generate the same ‘randomized’ MAC address or addresses to be used by the non-AP STA in the next association(s) based on a common procedure through a total of three parameters. Among these parameters, two of them (Seed, Counter) are exchanged between the non-AP STA and AP, and one of them (the key – RMAK) is generated locally at both sides.

A non-AP STA and AP may generate a single RMA, which the non-AP STA can use in all message exchanges, or multiple RMAs (RMA1, RMA2 etc.), which the non-AP STA can use in different message exchanges (e.g., RMA1 in probe request frame, RMA2 in other frames).

The STA advertises the support for RRCM by setting the RRCM Capability subfield to 1 in the Extended Capabilities Element.

The relevant items (the generation of RMA(s) and RMAK) for RRCM are explained in 12.2.11.4.2. The identification procedure is explained in 12.2.11.4.3.

**12.2.11.4.2 RMA, Keys, and Tag Generation**

The procedures to generate the RMA(s) and key, RMAK, are as follows:

**RMAK** = KDF-Hash-256(KDK, "RMA Key", Min(ANonce, SNonce) || Max(ANonce, SNonce)

**RMAn** = KDF-Hash-48(RMAK, "Next RMAs", seed || n)

Where,

* KDF-Hash-256 will generate 256 bits key, RMAK. Hash is the Hash algorithm used in the AKM that the STA and AP agreed upon. KDK is derived from PTK for RRCM procedure. ANonce and SNonce are the generated values from 4-way Handshake. “RMA Key” is the string name for RMAK and is treated as an ASCII string.
* KDF-Hash-48 will generate 48-bit RMA. Seed is a 128-bit random bit string generated at non-AP STA. n is initialized with 1 and incremented by 1 until n is equal to Counter, which is the number of generated RMA(s). As an example, if three RMAs are generated, Counter=3 implies that n=1 is used to generate RMA1, n=2 is used to generate RMA2, n=3 is used to generate RMA3. The length of the counter is 16 bits, resulting in maximum 2^16 different RMA(s) generation in each association.

NOTE1-- In each association, the non-AP STA may decide to generate one or more RMA(s), where each parameter {RMAK, Seed} is re-generated and Counter is reset to one.

NOTE2-- I/G = 0 and U/L = 1 bits shall be replaced in each generated RMA, see subclause 12.2.10.

NOTE3--RMA(s) may be saved on non-AP STA and AP/ESS side until new RMA(s) are generated.  
NOTE4 – When RRCM is negotiated, The PTK is partitioned into KCK, KEK, TK, and a KDK. KDK is used to derive RMAK.

**12.2.11.4.3 Identification Procedure**

During the association procedure, the non-AP STA and AP derive RMAK from KDK (see RMAK generation in subclause **12.2.11.4.2**).

Non-AP STA behaviour:

The non-AP STA initializes {Seed, Counter} values to locally generate one or more RMAs (see RMA generation in subclause **12.2.11.4.2**). When using FILS authentication, the non-AP STA sends the {Seed, Counter} in IE in the Association Request frame. When using FT, the non-AP STA sends the {Seed, Counter} during the initial mobility domain association in enctypted Key Data field (RRCM KDE) in the EAPOL-Key message 2 of 4-way handshake. {Seed, Counter} is not exchanged during the FT protocol reassociations within the same ESS. For other cases, the non-AP STA sends the {Seed , Counter } in enctypted Key Data field (RRCM KDE) in the EAPOL-Key message 2 of 4-way handshake.

AP behaviour:

After receiving {Seed, Counter} from the non-AP STA in the the EAPOL-Key message 2 of 4-way handshake or Association Request frame in FILS authentication mode, the AP first checks the {Counter} value to determine the number of RMA(s) it needs to generate locally. The AP generates the same number of RMA(s) that non-AP STA generated (see RMA generation in subclause **12.2.11.2**).

After the non-AP STA have been disassociated, {RMAK, Seed} are deleted and {Counter} is reset to 1, while RMA(s) are stored at non-AP STA and at the (previously) associated AP or ESS.

The non-AP STA may use the generated RMAs for messaging, preparing, and establishing the next association. The AP or ESS can then identify the non-AP STA despite changing MAC addresses through comparison of the MAC addresses with its stored RMAs.

Note— The usage of which RMA(s) for which frame is based on implementation.

.

* EAPOL-Key frames

*Add a new row into Table 12-10 (KDE selectors) P26 as shown below:*

|  |  |  |  |
| --- | --- | --- | --- |
| * KDE selectors | | | |
| OUI | | Data type | Meaning |
| 00-0F-AC | | <ANA> | Device ID KDE |
| 00-0F-AC | | <ANA> | MAAD KDE |
| 00-0F-AC | | <ANA> | IRMA KDE |
| 00-0F-AC | | <ANA> | RRCM KDE |

*Make following additions for the new KDE at the end of 12.7.2 as shown below:*

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

|  |
| --- |
| MAAD  MAC |

Octets 6

Figure 12-48b—MAAD KDE format

The MAAD MAC field contains a MAC address.

The format of the IRMA KDE is shown in Figure 12-48c (IRMA KDE format).

|  |
| --- |
| IRMA |

Octets 6

Figure 12-48c—MAAD KDE format

The IRMA field contains a MAC address.

The format of the RRCM KDE is shown in Figure 12-49 (RRCM KDE format).

|  |  |
| --- | --- |
| Seed | Counter |

Octets 16 2

Figure 12-49—RRCM KDE format

Seed and Counter are values to generate one or more RMA(s) through RRCM procedure. For details, see subclause **12.2.11.4.**

* EAPOL-Key frame notation

*Insert following text after OCI KDE (shown for reference)*

OCI KDE is a KDE containing operating channel information

Device ID KDE is a KDE containing a device identifier

MAAD KDE is a KDE containing a MAAD MAC

IRMA KDE is a KDE containing an IRMA

RRCM KDE is a KDE containing {Seed, Nonce, Counter, Tag} to be used for RRCM procedure

* 4-way handshake
* General

*Modify 12.7.6.1 P27 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} or

{RSNE, OCI KDE, RSNXE} or {RSNE, Device ID KDE} or {RSNE, OCI KDE, Device ID KDE} or {RSNE, RSNXE, Device ID KDE} or {RSNE, OCI KDE, RSNXE, Device ID KDE} or  
{RSNE, OCI KDE, RSNXE} or {RSNE, Device ID KDE, IRM KDE} or {RSNE, OCI KDE, Device ID KDE, IRM KDE} or {RSNE, RSNXE, Device ID KDE, IRM KDE} or {RSNE, OCI KDE, RSNXE, Device ID KDE, IRM KDE} or

{RSNE, OCI KDE, RSNXE} or {RSNE, IRM KDE} or {RSNE, OCI KDE, IRM KDE} or {RSNE, RSNXE, IRM KDE} or {RSNE, OCI KDE, RSNXE, IRM KDE}) or

{RSNE, OCI KDE, RSNXE} or {RSNE, Device ID KDE, RRCM KDE} or {RSNE, OCI KDE, Device ID KDE, RRCM KDE} or {RSNE, RSNXE, Device ID KDE, RRCM KDE} or {RSNE, OCI KDE, RSNXE, Device ID KDE, RRCM KDE} or

{RSNE, OCI KDE, RSNXE} or {RSNE, RRCM KDE} or {RSNE, OCI KDE, RRCM KDE} or {RSNE, RSNXE, RRCM KDE} or {RSNE, OCI KDE, RSNXE, RRCM KDE})

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], Device ID KDE} or {RSNE, GTK[N], OCI KDE, Device ID KDE} or  
{RSNE, GTK[N], RSNXE, Device ID KDE} or {RSNE, GTK[N], OCI KDE, RSNXE, Device ID KDE} 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} or  
{RSNE, GTK[N], MAAD KDE} or {RSNE, GTK[N], OCI KDE, MAAD KDE} or   
{RSNE, GTK[N], RSNXE, Device ID, MAAD KDE} or   
{RSNE, GTK[N], OCI KDE, RSNXE, Device ID, MAAD KDE})

Message 4: Supplicant  Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,{}).

**12.7.6.3 4-way handshake message 2**

*At P 28.39 Modify 12.7.6.3 as shown below:*

* Additionally, contains an OCI KDE when dot11RSNAOperatingChannelValidationActivated is true on the Authenticator.
* Additionally, may include a Device ID KDE
* Additionally, may include an IRM KDE or an RRCM KDE
* The RSNXE that the Authenticator sent in its (Re)Association Request frame, if this element is present in the (Re) Association Request frame that the Authenticator sent.

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

Key Ack = 0

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

Secure = 0 – same as message 1

Error = 0 – same as message 1

Request = 0 – same as message 1

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

Reserved = 0 – unused by this protocol version

* Key Data =
  + - * Additionally, contains RRCM KDE to carry the {Seed, Nonce, Counter, Tag} for RRCM KDE procedure
* 4-way handshake message 3

*At P 28 Modify 12.7.6.4 as shown below:*

* Additionally, contains an OCI KDE when dot11RSNAOperatingChannelValidationActivated is true on the Authenticator.
* Additionally, may include a Device ID KDE
* 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.