**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **LB207/D01 comment resolution -- Clarifications -- CIDs 291, 488, 497, 501, 1019** |
| Date Submitted | February 4, 2025 |
| Sources | Alex Krebs (Apple)  krebs @ apple.com |
| Re: |  |
| Abstract |  |
| Purpose | To propose resolution for MMS related comments for “P802.15.4ab™/D (pre-ballot) C Draft Standard for Low-Rate Wireless Networks”. |
| Notice | This document does not represent the agreed views of the IEEE 802.15 Working Group or IEEE 802.15.4ab Task Group. It represents only the views of the participants listed in the “Sources” field above.It is offered as a basis for discussion and is not binding on the contributing individuals. The material in this document is subject to change in form and content after further study. The contributors reserve the right to add, amend or withdraw material contained herein. |

**Table of contents**

[CID 1019 (Revised) 3](#_Toc189060757)

[CID 291 (Reassign to Rojan) 4](#_Toc189060758)

[CID 488, 497, 501 (Revised) 5](#_Toc189060759)

# CID 1019 (Revised)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index #** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Billy Verso | 1019 | 13 | 3,1 | 23 | the term "hash" is used in the text, a definition should be added. | include a definition for the term "hash" |

Discussion: Agree that a lower-case "hash" is confusing. However, instead of (re)defining what a hash is, we should simply make sure that it is understood that the field name is "RPA Hash" and that computation thereof is accurately referenced. Note that there is another specific comment #1156 in 15-24-569-01-04ab that has already being agreed to resolve as proposed below.

Proposed Resolution: Revised

Disposition Detail:

Change the text on page p.63 l.24 as follows:

To establish a ranging session, HRP-ARDEVs may engage in an initialization and setup stage and perform

an initialization setup handshake as described in 10.38.3. After that, the HRP-ARDEVs enter the control

phase and the ranging session is started. The ranging session procedure is the same as described in 10.38.4

to 10.38.6, except for generating IRKs for the RPA Hash field specified in 10.38.3.6.2.

Change the text on page p.64 l.20 and l.22 as follows:

After ranging session is initialized using public addresses, private addresses described in 10.38.9.2.1 shall

be used during that ranging session. To handle private addresses, the IRK is generated by the initiator and

the responder(s) to generate the RPA Hash field value specified in 10.38.9.2.1. The initiator’s address and a

responder’s address which are exchanged during initialization shall be used to generate the IRK for

obtaining the RPA Hash field's value.

Change the text on page p.65 l.5 as follows:

For the ranging session after the initialization setup handshake using the Public Advertising Poll Compact

frame, Public Advertising Response Compact frame, Public Advertising Confirmation Compact frame and

Public Start of Ranging Compact frame, the IRK shall be formed, as shown in Figure 34, using the public

addresses which are known to both the initiator and the responder(s), and used to generate the value of the RPA Hash

field specified in 10.38.9.2.1 to use in poll, response and report messages.

Change the text on page p.65 l.14 as follows:

NOTE—Forming the IRK using public addresses is not intended to protect the privacy of a device. The primary

purpose is to generate the value of the RPA Hash field to allow reuse of the poll, response and report Compact frame formats.

In a one-to-many session, a One-to-many Poll Compact frame in the first sub-round shall be transmitted as

described in 10.38.8. To address multiple responders simultaneously, the IRK for the one-to-many POLL

compact frame with the Message Control field not set to 0x00 should be generated using a GroupID, which

represents a group of multiple devices in a one-to-many ranging session. By transmitting a Public

Advertising Poll Compact frame with the MessageControl field set to 0x21 on the initialization channel, a

GroupID is shared with responders. The GroupID shall be used to generate the IRK used for the computation of the value of the RPA Hash field that is used

in One-to-many Poll Compact frame in the one-to-many ranging session, as described in 10.38.8, in case

GroupID is shared with responders.

The GroupID is not shared if a Public Advertising Poll Compact frame with the MessageControl field value

is not set to 0x21 on the initialization channel. In this case, the value, 0xFFFFFF shall be used to generate

the IRK used for the computation of the value of the RPA Hash field used in the One-to-many Poll Compact frame with the Message Control field

not set to 0x00.

The initiator and responder devices maintain a resolving list by adding multiple IRKs. The resolving list

shall be used to resolve RPA\_hash in an incoming Compact frame. If multiple IRKs exists in the resolving

list, all the IRKs shall be iterated to resolve the value of the RPA Hash field, as described in 10.38.9.2.1.

Change the text on page p.79 l.3 as follows:

The value of a 3-octet RPA Hash field is then computed using an IRK and the initiator’s RPA\_prand. The value of the RPA Hash field is then

\_

given by bits 0 to 23 of *h*(key=IdentityResolvingKey, data=RPA\_prand) where *h( )* is the AES-128 block

cipher described in B.2.2, with an IRK and the initiator's RPA\_prand as inputs.

Depending on which compact message is used for transmission, the IRK used for calculating the value of the RPA Hash field

may be the initiator's IRK, a responder's IRK, or a group IRK associated with multiple devices. For details

see the description of the respective message. An RPA field consisting of an RPA Hash field and an RPA Prand field may

be used for OTA packet transmissions and can be resolved only at a receiving device that have knowledge

of the generating IRK.

To resolve the RPA of an incoming packet the receiving device shall compute the value of the RPA Hash field using one or

more IRKs that the receiver assumes to have been used by the sender device and the received RPA\_prand

communicated over the air by the transmitting device. If the result of the receiver's computation matches

the received RPA, the RPA is resolved. Otherwise, the RPA shall be marked as unresolved, and the

received packet shall be discarded by the receiver.

The generation and mutual exchange of IRKs among initiator(s) and responder(s) is a prerequisite for

private address resolution as described and is out of scope of this standard and may be conducted using

higher layer methods. Note that devices may carry multiple IRKs to, e.g., assert privacy among multiple

responders and/or ranging sessions. Again, methods for association and assignment of IRKs are not defined

in this standard but may be carried out using higher layer methods.

Change the text on page p.80 l.11 as follows:

For an incoming secure Compact frame that is marked as resolved (as described in 10.38.9.2.1), the

corresponding security key can be identified based on the extended address that is mapped to the IRK used

to resolve the value of the RPA\_hash field of the frame.

Change the text on page p.92 l.4 as follows:

The RPA Prand field shall be set as specified in 10.38.9.2.1. During initialization phase, the value of

RPA Prand as conveyed in this Compact frame shall be used to compute the values of the RPA Hash fields used in subsequent

Compact frames, until the initiator transmits another Advertising Poll Compact frame.

Change the text on page p.97 l.17 as follows:

The RPA Prand field shall be set as specified in 10.38.9.2.1. In the scope of a ranging round, the value of

RPA\_prand as conveyed in this frame shall be used to compute the values of the RPA Hash fields used in all subsequent

frames, until the initiator transmits another One-to-one Poll Compact frame or a One-to-many Poll

Compact frame.

Change the text on page p.101 l.22 as follows:

The Initiator RPA Hash field shall be calculated as specified in 10.38.9.2.1 using the initiator's IRK. Note

that if the Message Content field contains one or more Responder Address fields, each Responder Address

in the Message Content field shall represent an eligible responder's RPA Hash field value generated using the initiator's

RPA Prand field value from the preceding Advertising Poll Compact frame along with the responder's IRK.

Change the text on page p.103 l.4 as follows:

Note that if the Message Content field contains one or more Responder Address fields each Responder

Address field value in the Message Content field shall represent an eligible responder's RPA Hash field value generated

using the initiator's RPA Prand field value as conveyed in this frame along with that responder's IRK.

Change the text on page p.104 l.9 as follows:

The Responder Address field identifies a responder participating in the current one-to-many ranging. The

Responder Address field value shall contain an eligible responder’s RPA Hash field value generated using the

initiator’s RPA

Prand field value in the one-to-many Poll Compact frame along with the responder’s IRK.

Change the text on all p.106 l.3, p.107 l.3, and p.108 l.3 as follows:

The Responder Address field identifies a responder participating in the current one-to-many ranging. The

Responder Address field value shall contain an eligible responder’s RPAHash field value generated using the

initiator’s RPA Prand field value in the one-to-many Poll Compact frame along with the responder’s IRK.

# CID 291 (Reassign to Rojan)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index #** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Tero Kivinen | 291 | 17 | 7.3.7.1 | 3 | Adding a new frame format that does not allow security or privacy in 2024 is really bad. We must not do such thing. Security and privacy is required for the modern 802.15.4 operating environments, especially on the phones etc. Privacy cannot be provided without security, and the currently defined security and privacy features in compact frames are not suitable for the use these frames are intended for. | Define compact frame format so that it can use the 802.15.4 security and reuse the privacy to be defined in TG4ac. It is known that IEEE has long standing tradition of making insecure and broken standards, but lets try to get away from that tradition. |

Discussion: There is an ongoing work in " Proposed enhancements to secure Compact frames" DCN 15-24-587-00-04ab presented by Rojan at the Kobe F2F. This comment is likely to be resolved to the commenter's satisfaction alongside the other comments submitted to Rojan. I'd suggest to reassign this comment to Rojan, too. Update Feb 4, 2025: Work has been completed in DCN 15-24-381-03-04ab by introducing Compact frame ID 17 "Secured Compact frame" that allows for encryption of eligible Compact frames (where eligible in DCN 381r3 refers to frames that choose to take advantage of encryption).

Proposed Resolution: Revised.

Disposition Detail: As detailed in DCN 15-24-381-03-04ab (previously agreed by the group during Kobe F2F)

# CID 488, 497, 501 (Revised)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index #** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Tero Kivinen | 488 | 81 | 10.38.9.3.7 | 21 | The nbChannelBitmaskSet is not obtained from the bits 0 to 41, it is constructed from there by returning list of integers in such way that for each bit from 0 to 41 it returns the bit number which are set. | Properly define the generation of the NbChannelBitMaskSet. |
| Tero Kivinen | 497 | 82 | 10.38.9.3.8 | 25 | The nbChannelBitmaskSet is not obtained from the bits 0 to 9, it is constructed from there by returning list of integers in such way that for each bit from 0 to 9 it returns a channel number. | Properly define the generation of the NbChannelBitMaskSet. |
| Tero Kivinen | 501 | 83 | 10.38.9.3.9 | 15 | The nbChannelBitmaskSet is not obtained from the bits 0 to 31, it is constructed from there by returning list of integers in such way that for each bit from 0 to 31 it returns the bit number which are set. | Properly define the generation of the NbChannelBitMaskSet. |

Discussion: The referenced sentences are only the caption of the following text. The following text properly defines the generation of the NbChannelBitMaskSet. See here:

A screenshot of a paper

Description automatically generated

Here is the proper definition:

Comment is rightfully noting lack of proper definition here

Proposed Resolution: Revised

Disposition Detail: Add the words "as follows:" at the end of p.81 l.22, p.82 l.26, and p.83 l.16, respectively.