**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **Proposed Resolution for Key ID field** | |
| Date Submitted | January 2024 | |
| Sources | Rojan Chitrakar, Lei Huang (Huawei)  [rojan.chitrakar@huawei.com](mailto:rojan.chitrakar@huawei.com) |  |
| Re: |  | |
| Abstract |  | |
| Purpose | To propose resolution for Key ID field 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. | |

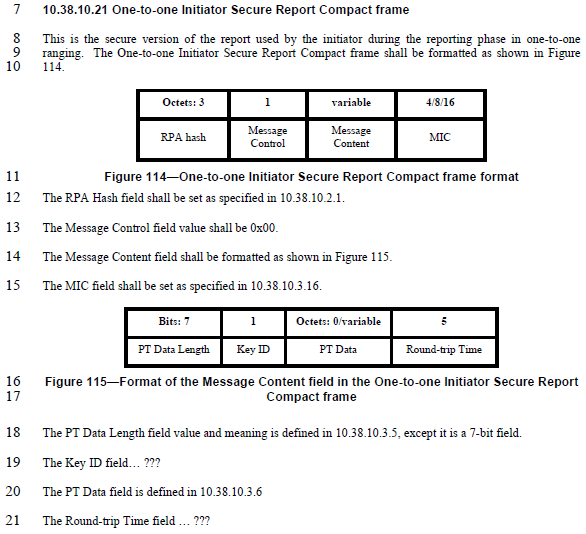
Rev 0: Initial version.

Rev 1: Added resolution for 168.

***Comment Indices in 15-24-0010-00-04ab-consolidated-comments-draft-c:***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Rojan Chitrakar | 634 | 71 | 10.38.10.3.19 | 2 | When the One-to-many Initiator Secure Report Compact frame is meant to be received by more than one responders, group Key may be used to secure the frame instead of a unicast Key. As such a 1 bit Key ID field is not enough. Suggest to use one octet for the Key ID field for all secure frames. Regardless, it is not necessary to desciribe the size of the field here and suggest to change to a general langugauage similar to the baseline. | Change to: "The Key ID field allows unique identification of different keys with the same originator." | Revised |
| Carl Murray | 824 | 98 | 10.38.10.21 | 19 | Field description missing | Add field description | Revised |
| Mickael Maman | 909 | 98 | 10.38.10.21 | 19 | The Key ID field… ??? | "The Key ID field is the KeyIndex parameter as defined in 10.38.10.3.19." | Revised |
| Carl Murray | 826 | 99 | 10.38.10.22 | 11 | Field description missing | Add field description | Revised |
| Carl Murray | 828 | 99 | 10.38.10.22 | 20 | Field description missing | Add field description | Revised |
| Rojan Chitrakar | 654 | 100 | 10.38.10.23 | 19 | When the One-to-many Initiator Secure Report Compact frame is meant to be received by more than one responders, group Key may be used to secure the frame instead of a unicast Key. As such a 1 bit Key ID field is not enough. Suggest to use one octet for the Key ID field for all secure frames. | Change the Key ID field to one octet and reposition as the first field of the Message Content field | Revised |
| Rojan Chitrakar | 655 | 100 | 10.38.10.23 | 21 | If a separate octet is used for the Key ID field, suggest to make the PT Data Length 1 octet for all secure compact frames, same as unsecure compact frames. | Delete ", except it is a 7-bit field" | Revised |
| Benjamin Rolfe | 169 | 100 | 10.38.10.23 | 22 | More missing field definitions (???) | Complete specification or remove clause | Revised |
| Carl Murray | 830 | 100 | 10.38.10.23 | 22 | Field description missing | Add field description | Revised |
| Benjamin Rolfe | 170 | 101 | 10.38.10.24 | 15 | More missing field definitions (???) | Complete specification or remove clause | Revised |
| Carl Murray | 832 | 101 | 10.38.10.24 | 15 | Field description missing | Add field description | Revised |
| Carl Murray | 834 | 102 | 10.38.10.24 | 4 | Field description missing | Add field description | Revised |

**Discussion**：



**Disposition: Revised**

**Disposition Detail:**

**Proposed text changes on P802.15.4ab™/D (pre-ballot) C:**

**10.38.10.3.19 The Key ID field (#634)**

The Key ID field allows unique identification of different keys with the same originator.

**10.38.10.21 One-to-one Initiator Secure Report Compact frame (#824, #909)**

***Change the subfield as follows (Track changes ON)***

…

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Octets: 1 | 1 |  | 0/variable | 5 |
| Key ID | PT Data Length |  | PT Data | Round-trip Time |

**Figure 115—Format of the Message Content field in the One-to-one Initiator Secure Report Compact frame**

The PT Data Length field value and meaning is defined in 10.38.10.3.5.

The Key ID field is defined in 10.38.10.3.19.

**10.38.10.22 One-to-one Responder Secure Report Compact frame (#826, #828)**

***Change the subfield as follows (Track changes ON)***

…

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Octets: 1 | 1 |  | 0/variable | 5 |
| Key ID | PT Data Length |  | PT Data | Round-trip Time |

**Figure 117—Format of the Message Content field in the One-to-one Responder Secure Report Compact frame when the Message Control field value is 0x00**

The PT Data Length field value and meaning is defined in 10.38.10.3.5.

The Key ID field is defined in 10.38.10.3.19.

…

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octets: 1 | 1 |  | 0/variable | 1 | 0/6 | 0/1 | 0/7 | 0/3 | 0/2 | 5 |
| Key ID | PT Data Length |  | PT Data | Presence Bitmap | NB Channel Map | Management PHY Configuration | Management MAC Configuration | Ranging PHY Configuration | Ranging MAC Configuration | Reply Time |

**Figure 118—** **Format of the Message Content field in the One-to-one Responder Secure Report Compact frame when the Message Control field value is 0x10**

The PT Data Length field value and meaning is defined in 10.38.10.3.5.

The Key ID field is defined in 10.38.10.3.19.

**10.38.10.23 One-to-many Initiator Secure Report Compact frame (#654, #655, #169)**

***Change the subfield as follows (Track changes ON)***

…

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Octets: 1 | 1 |  | 0/variable | 5 |
| Key ID | PT Data Length |  | PT Data | Round-trip Time |

**Figure 120—Format of the Message Content field in the One-to-many Initiator Secure Report Compact frame when the Message Control field value is 0x00**

The PT Data Length field value and meaning is defined in 10.38.10.3.5.

The Key ID field is defined in 10.38.10.3.19.

**10.38.10.24 One-to-many Responder Secure Report Compact frame (#170, #832, #834)**

***Change the subfield as follows (Track changes ON)***

…

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Octets: 1 | 1 |  | 0/variable | 5 |
| Key ID | PT Data Length |  | PT Data | Round-trip Time |

**Figure 122—Format of the Message Content field in the One-to-many Responder Secure Report Compact frame when the Message Control field value is 0x00**

The PT Data Length field value and meaning is defined in 10.38.10.3.5.

The Key ID field is defined in 10.38.10.3.19.

**…**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octets: 1 | 1 |  | 0/variable | 1 | 0/6 | 0/1 | 0/7 | 0/3 | 0/2 | 5 |
| Key ID | PT Data Length |  | PT Data | Presence Bitmap | NB Channel Map | Management PHY Configuration | Management MAC Configuration | Ranging PHY Configuration | Ranging MAC Configuration | Reply Time |

**Figure 123—Format of the Message Content field in the One-to-many Responder Secure Report Compact frame when the Message Control field value is 0x10**

The PT Data Length field value and meaning is defined in 10.38.10.3.5.

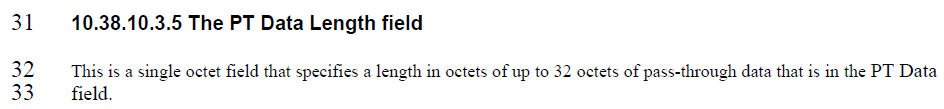
The Key ID field is defined in 10.38.10.3.19.

-------- 24/27r1--------

***Comment Indices in 15-24-0010-00-04ab-consolidated-comments-draft-c:***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Benjamin Rolfe | 168 | 99 | 10.38.10.22 | 10 | Incomplete definitions. Is PT e.g. type of integer (unsigned integer) for PT Data Length (why is it 7 bits when the max value defined is 32?); Reply time Field, Key ID field. Some of these are defined in the common clause? | Complete specification or remove clause | Revised |

**Discussion**：



**Disposition: Revised**

**Disposition Detail:**

**Proposed text changes on P802.15.4ab™/D (pre-ballot) C:**

**10.38.10.3.5 The PT Data Length field (#168)**

This is a single octet field that specifies the length of pass-through data that is in the PT Data field.

NOTE – The maximum length of the pass-through data is restricted by the Frame Length field of the PHR field as described in 13.1.3.2 (Frame Length field).