**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **Proposed Resolution for Security: Part-1 (Key-ID)** |
| Date Submitted | January 2024 |
| Sources | Rojan Chitrakar, Lei Huang (Huawei)rojan.chitrakar@huawei.com |  |
| Re: |   |
| Abstract |  |
| Purpose | To propose resolution for Key ID field related security 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. Addresses the following comments:

…

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Benjamin Rolfe | 137 | 24 | 9.2.12 | 23 | KeySource and KeyIndex depend on information not present in every compact frame. If security is enabled, but the frame has no Key ID field, what Key ID is used?  | Add text: When the Key ID is not present in the frame, the Key ID value of zero is used.  | Revised |
| Tero Kivinen | 501 | 24 | 9.2.12 | 23 | not every compact frame has key id field. | Remove compact frame format, and uses standard security processing. | Revised |
| Benjamin Rolfe | 142 | 26 | 9.2.13 | 1 | What value is used for KeyIndex when the Key ID field is not present in the frame being processed? | Change to: When the Key ID field is present in the Compact frame to be unsecured, KeyIndex shall be set to the Key ID field value; otherwise KeyIndex is set to zero.  | Revised |
| Tero Kivinen | 500 | 26 | 9.2.13 | 1 | There is no Key Id field in every compact frame, thus there is no way of knowing keyindex. | Remove compact frame format, and uses standard security processing. | Revised |

**Discussion**：





Key ID field is present in all Secure compact frames so there is no need to handle the case when the Key ID field is not present. However, it is good to clarify that 9.2.12 (Outgoing frame security procedure for Compact frames) and 9.2.13 (Incoming frame security procedure for the Compact frames) only apply to the four Secured Compact frames: One-to-one Initiator Secure Report Compact frame, One-to-one Responder Secure Report Compact frame, One-to-many Initiator Secure Report Compact frame, and One-to-many Responder Secure Report Compact frame.



**Disposition: Revised**

**Disposition Detail:** Key ID field is present in all Secure compact frames so there is no need to handle the case when the Key ID field is not present. However, it is good to clarify that 9.2.12 (Outgoing frame security procedure for Compact frames) and 9.2.13 (Incoming frame security procedure for the Compact frames) only apply to the four Secured Compact frames: One-to-one Initiator Secure Report Compact frame, One-to-one Responder Secure Report Compact frame, One-to-many Initiator Secure Report Compact frame, and One-to-many Responder Secure Report Compact frame.

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

**9.2.12 Outgoing frame security procedure for Compact frames (#137, #501, #142, #500)**

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

This procedure shall be used to secure the Compact frames listed below:

* One-to-one Initiator Secure Report Compact frame
* One-to-one Responder Secure Report Compact frame
* One-to-many Initiator Secure Report Compact frame
* One-to-many Responder Secure Report Compact frame

This procedure does not apply to Compact frames that are not listed above.

To secure other frame types, the procedure in 9.2.2 shall be used.

…

**9.2.13 Incoming frame security procedure for the Compact frames (#137, #501, #142, #500)**

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

This procedure shall only be used for incoming Compact frames listed below:

* One-to-one Initiator Secure Report Compact frame
* One-to-one Responder Secure Report Compact frame
* One-to-many Initiator Secure Report Compact frame
* One-to-many Responder Secure Report Compact frame

This procedure does not apply to Compact frames that are not listed above.

For other frame types, the procedures in 9.2.4 or 9.2.5 shall be used.

…

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Rojan Chitrakar | 583 | 28 | 9.5.11 | 10 | It is not necessary to specify the range as 0 or 1 here. It is better to reference to 10.38.10.3.19 (The Key ID field) where the field is described. | "Change the Range column to:"As described in 10.38.10.3.19 (The Key ID field)" | Accepted |

**Discussion**：



**Disposition: Accepted**

**Disposition Detail:** Another comment resolution is proposing to change the Key ID field to 1 octet, hence the Range is not limited to 0 or 1. In any case, it is better to refer to the Key ID field for the range.