**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-2 (Key lookup and Source)** | |
| 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 security related comments to Key lookup and source 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.

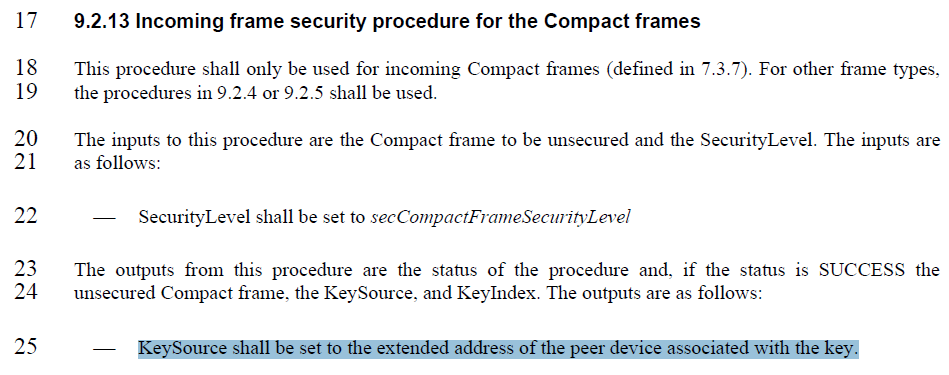
Rev 1: Editorial changes.

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

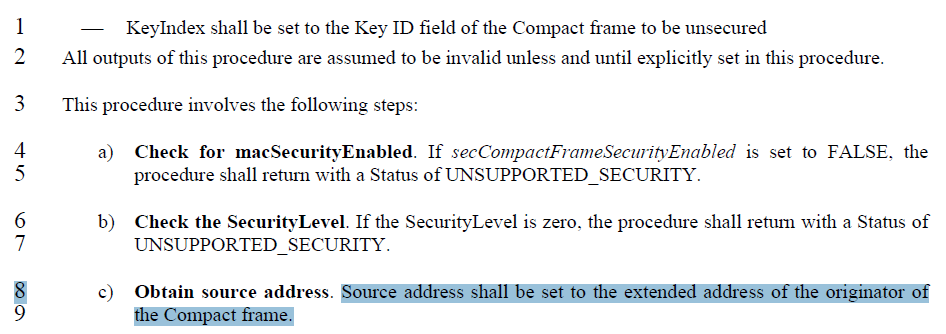
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Benjamin Rolfe | 138 | 24 | 9.2.12 | 10 | Key lookup procedure not specified. What "matching" means and success or failure criteria. Assuming the source address and Key ID are what must match? | Change to: The procedure shall obtain the matching Key from the secCompactFrameKeyList selecting the entry that has a matching value of KeySource and KeyIndex. If no matching entry is found, the Key lookup procedure fails, the procedure shall return  12 with a Status of UNAVAILABLE\_KEY. | Revised |
| Tero Kivinen | 499 | 25 | 9.2.13 | 25 | how is the KeySource known, i.e., how do you know which device is associationed with the key? | Remove compact frame format, and uses standard security processing. | Revised |
| Rojan Chitrakar | 579 | 25 | 9.2.13 | 25 | "KeySource shall be set to the extended address of the peer device associated with the key."  KeySource is required to identify the key, so this sentence is not correct. KeySource should be the extended address of the peer device that transmitted the compact frame. | Change the cited sentence to:  "KeySource shall be set to the extended address of the device originating the Compact frame." | Revised |
| Benjamin Rolfe | 143 | 26 | 9.2.13 | 8 | (Here and also line 30 in 9..2.4): How is the source address known? Addressing fields are elided in compact frames (not in the MAC header). This might be might be in 10.38.10.2.2? It is not at all clear how we get from 3 octet addresses in the frames to an extended address used here. | Provide a cross reference to where the source address is determined for the received frame | Revised |
| Tero Kivinen | 498 | 26 | 9.2.13 | 8 | there is no source address at all in the incoming frame, so we can't know the extended address of the originator of the compact frame. | Remove compact frame format, and uses standard security processing. | Revised |

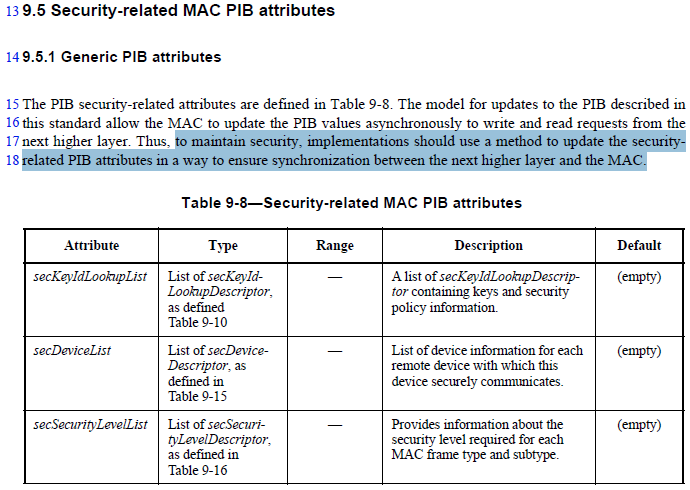
**Discussion**：A subclause is added (10.38.10.2.3 Extended Address) to clarify how the extended address is obtained for Compact frames.

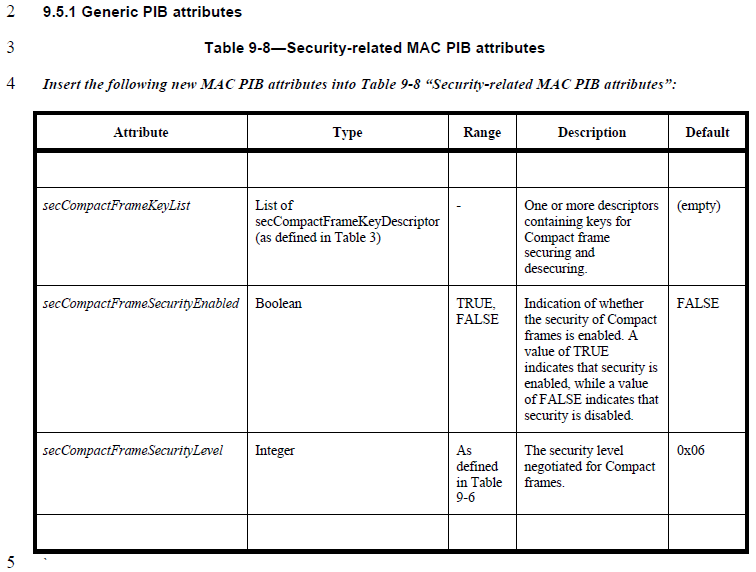
Comment index #499, #579:

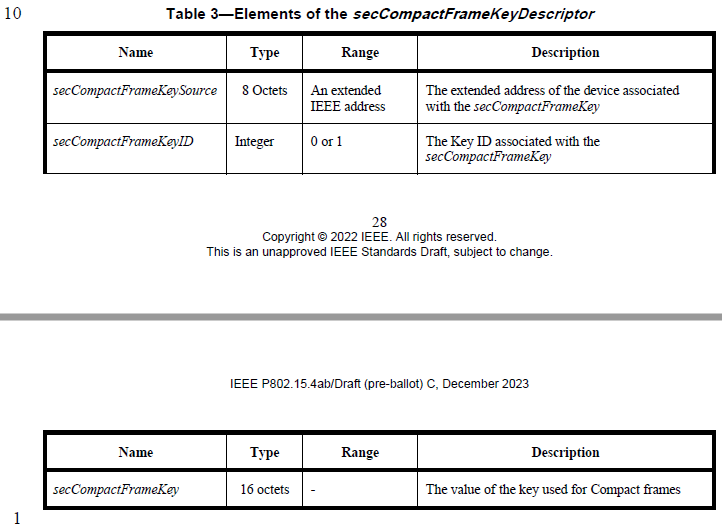


Comment index #498









**Disposition: Revised**

**Disposition Detail:**

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

**9.2.12 Outgoing frame security procedure for Compact frames (#138, #579)**

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

…

⎯ SecurityLevel shall be set to *secCompactFrameSecurityLevel*

⎯ KeySource shall be set to the extended address of the device to which the Compact frame is addressed (see 10.38.10.2.3).

…

d) Obtain Key. The procedure shall obtain the matching Key from the *secCompactFrameKeyList,* selecting the *secCompactFrameKey* of the *secCompactFrameKeyDescriptor* whose *secCompactFrameKeySource* matches the KeySource and *secCompactFrameKeyID* matches the KeyIndex. If a matching key is not found, the Key lookup procedure fails and the procedure shall return with a Status of UNAVAILABLE\_KEY.

**9.2.13 Incoming frame security procedure for the Compact frames (#138, #579)**

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

…

The outputs from this procedure are the status of the procedure and, if the status is SUCCESS the unsecured Compact frame, the KeySource, and KeyIndex. The outputs are as follows:

⎯ KeySource shall be set to the extended address of the device originating the Compact frame (see 10.38.10.2.3).

…

d) Obtain Key. The procedure shall obtain the matching Key from the *secCompactFrameKeyList,* selecting the *secCompactFrameKey* of the *secCompactFrameKeyDescriptor* whose *secCompactFrameKeySource* matches the KeySource and *secCompactFrameKeyID* matches the KeyIndex. If a matching key is not found, the Key lookup procedure fails and the procedure shall return with a Status of UNAVAILABLE\_KEY.

**10.38.10.2 Address formats**

***Add the following new subclause at the end of 10.38.10.2***

**10.38.10.2.3 Extended Address (#499, #143, #498)**

When an initiator and a responder intend to use secure compact frames (see 9.2.12 (Outgoing frame security procedure for Compact frames) and 9.2.13 (Incoming frame security procedure for the Compact frames)), each of the initiator and responder shall maintain one *secCompactFrameKeyDescriptor* in *secCompactFrameKeyList* (see 9.5.1) for each key negotiated between the initiator and the responder.

For an incoming compact frame that is marked as resolved (see 10.38.10.2.1), the corresponding extended address can be identified based on the IRK used to resolve the RPA\_hash of the frame.

Methods for the negotiation of the security key and the corresponding extended address and Key ID are not defined in this standard but may be carried out using higher layer methods.