**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **LB213 - Proposed Resolutions for Security – Part 2** | |
| Date Submitted | July 2025 | |
| Sources | Rojan Chitrakar, Lei Huang (Huawei)  [rojan.chitrakar@huawei.com](mailto:rojan.chitrakar@huawei.com) |  |
| Re: |  | |
| Abstract |  | |
| Purpose | To propose resolution for “P802.15.4ab™/D01 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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| VERSO, BILLY | 365 | 50 | 10.32.3.5 | 7 | I am not sure what this is "the address of the network" is, this term does not appear elsewhere in 4ab or the base standard. Is it the PAN, i.e., the PAN ID, or what? Please clarify, or delete. | delete "or the address of the network it belongs to" | **Revise** |
| Shellhammer, Steve | 293 | 79 | 10.39.4.1 | 18 | What is the expected behaviour when the responder does not receive Poll? In this case, there is no point for the responder to send the response compact frame. | Add this sentence in line 18: "If the responder does not receiver the Poll, it shall skip sending the response Compact frame." | **Reject**  There is normative behaviour specified in Page 80 Line 12 that covers this:  “A responder shall discontinue the MMS UWB ranging round if the responder fails to receive the poll Compact frame at the beginning of the expected ranging round,” |
| Kivinen, Tero | 95 | 96 | 10.39.11.1.2.3 | 36 | This text is confusing and mixed extended addresses and key source fields in a way which is hard to understand. | Change the text to say that devices are always identified using the extended address of the originator or destination, but the key id mode of 0x03 is used, where each key is identified with 64-bit KeySource which matches the owner of the key. I.e., use term KeySource when talking about the key identifier. | **Revise** |
| VERSO, BILLY | 499 | 97 | 10.39.11.1.2.3 | 5 | This sentence says mapping of extended address to the IRK are not defined in this standard, but we have added macIrkDescriptorElement which seems to allow for mapping between IRK and extended address, so I am not sure if this statemet is correct.. | Probably should revise the statement to add some description about this mapping, and/or reference where it is described.. | **Revise** |
| VERSO, BILLY | 530 | 110 | 10.39.11.2 | 8 | The Secured Compact frame itself, is not lised as eligible (or not eligible) for securing. It is inside the ranging block but proably should say that it is not eligible. | State that the secured frame itself shall not be iteratively/recursively secured into another secured frame. | **Revise** |
| VERSO, BILLY | 531 | 110 | 10.39.11.2 | 9 | The criteria for securing seems to be whether the slot index is available, to act as the nonce. For the ineligible frames we could we optionally include a nounce frame counter, e.g. using the Secured Control field reserved bit 15 to signal its presence. Would take no additional space when not needed. Number could be continmued as slot inex when slotted mode is established. | Consider allowing this, to make a more rounded spec | **Reject**  There is no strong motivation to enable security for securing of frames sent before the ranging slot structure is established. |
| VERSO, BILLY | 532 | 110 | 10.39.11.2 | 9 | Vendor specific frames are not covered here, they could be used in slotted mode or not. Woulld be good to have a way to secure therm. Vendor specific IE can be secured in 15.4 data frames. It is very likely that vendor specifc compact frames will have content that also needs to be secured. Such securing is a normal function of the MAC so it should really be done here. | Add mechanism incorporate vendor specific frames into thise securing process. Possibly will need have option to include RPA hash and other fields into the vendor specific frames to allow for this, which might be a good thing to allow common handling in the MAC. | To be discussed |
| VERSO, BILLY | 581 | 143 | 10.39.11.3.21 | 10 | All other vendor specific messages within in 802.15.4 are within properly addressed MAC frames. Here there is no addressing so the frames are passed to the upper layer without any notion whether they are for this device or not. If the frames have RPA/HASH they have already passed that part of the MAC where secret keys etc. reside (possibly hidden from the upper layer). Similarly CRC is not part of the definition so if there is one, then the higher layer has to check it separately from any H/W there may have been to do it in the lower MAC. This will make extending the compact messaging scheme less straightforward. Doing this would also facilitate carrying them in the secure compact frame, and it is likely that MAC level security processing will be needed for many vendor specific use cases. | To allow for common MAC processing of the low level parts of the frame, specify RPA HASH and PRAND fields and CRC as fields as part of the Vendor Specific Compact frame format. This would allow the entities using vendor specific format to use same IRK etc in common way. | Transfer to Alex? |
| Kivinen, Tero | 99 | 143 | 10.39.11.3.22 | 21 | The section 9.3.4.3 uses MHR which is not defined for the compact frames. | Add new figure that defines MHR. The MHR needs to include the first octet of the frame i.e., the compact frame id and frame type, security control field, RPA Hash and RPA Prand fields. The rest can be marked as Private Payload field. | **Reject**  MHR for Compact frame is defined in 9.3.4.3 (a data and m data) and (9.3.5.3 c data and a data). |
| Kivinen, Tero | 97 | 143 | 10.39.11.3.22 | 23 | The Security Compact Frame ID is 8-bit field, but it contains Compact Frame ID that is only 5 bits long. | Reduce the size of the Secured Compact Frame ID to match Compcat Frame Id Size. | **Reject**  There is no need to match the field sizes; Also the Compact Frame ID may be extended in future. |
| Kivinen, Tero | 98 | 143 | 22 line 23 |  | There is KeyIndex and Key ID terms used by the draft and I assume they are trying to mean same. | If Key ID and KeyIndex are supposed to be same, use the same term. Also the Key ID and KeyIndex fields are used as 4 bit or 8 bit fields in different places, make sure they are consistent. | **Revise** |
| Kivinen, Tero | 100 | 144 | 10.39.11.3.22 | 15 | The MIC field is not really set to those values. | The output of the AEAD transformation is c data. The Private Payload field of the original unsecured frame shall be replaced by the right-concatenation of that field and the c field if data confidentiality is not provided and shall be replaced by the c field otherwise. There should not be separate MIC field at all. This text requires rewrite to match what 9.3.4/9.3.5 does. | **Revise** |
| Kivinen, Tero | 101 | 146 | 10.39.12 | 5 | The macIrkAssocEuiPresent should point out that if it is FALSE, then no secure communication to or from this device is possible. | Add text explaining that if it is set to FALSE then no extended address is stored and no security communication to the device is possible. | **Reject**  If an associated Extended address is not found, the Outgoing/Incoming frame security procedure for Compact frames will return with error, so no further explanation is required. |
|  |  |  |  |  |  |  |  |

**9.2.12 Outgoing frame security procedure for Compact frames [#365]**

***Change the sub-clause as follows (Track changes ON)***

…

After receiving the block assignment(s), if the controlee finds its address or the PAN ID of the PAN it belongs to in the Scheduling IE, it will know the block that is assigned to it.

**10.39.11.1.2.3 Extended Address [#95]**

***Change the sub-clause as follows (Track changes ON)***

…

For an outgoing secure Compact frame the KeySource and the KeyIndex elements of the CompactSecurityParams element of the CompactFrameDescriptor parameter provided in the MCPS-DATA.request primitive is used as *secCompactFrameKeySource* and secCompactFrameKeyID respectively to identify the security key in *secCompactFrameKeyDescriptor*.

For an incoming secure Compact frame whose RPA is marked as resolved (as described in 10.39.11.1.2.1), the corresponding security key in secCompactFrameKeyDescriptor can be identified based on the Key ID field of the frame and the *macIrkAssociatedEui* corresponding to the IRK in the macIrkDescriptor used to resolve the RPA of the frame.

**10.39.11.2 Security of MMS Compact frames [#530]**

***Change the sub-clause as follows (Track changes ON)***

A Secured Compact frame is used to cryptographically protect another Compact frame. Only those Compact frames used within a ranging block structure are eligible for security, while those used outside the ranging block structure are not eligible for security. These are listed in Table 23 and Table 24 respectively. The Secured Compact frame itself shall not be iteratively/recursively secured in another Secured Compact frame.

…

**10.39.11.3.22 Secured Compact frame [#98, #100]**

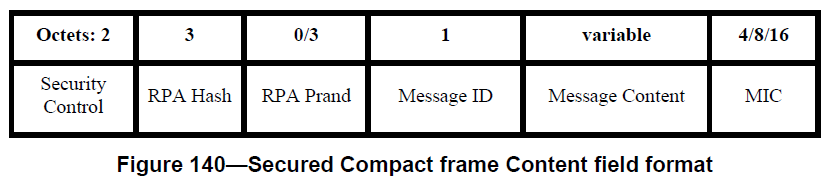
***Change the sub-clause as follows (Track changes ON)***

…

The Key ID field identifies the index of the key that is used for cryptographic protection of the Compact frame.

…

***Delete the MIC field in Figure 140:***



…

**10.39.11 Messages for MMS UWB operation [#100]**

**10.39.11.1 Overview**

**10.39.11.1.1 General**

Compact frames are used in MMS UWB operation. These have a one-octet header that includes the Compact 16 Frame ID field which identifies the Compact frame, (as specified in Table 10), and content which is specific 17 to the Compact Frame ID. Each frame ends with either a 2-octet FCS, which shall be the 16-bit ITU-T CRC 18 generated as described in 7.2.11, or with a MIC which shall be one of MIC-32, MIC-64, MIC-128, 19 ENC-MIC-32, ENC-MIC-64 or ENC-MIC-128 as defined by Table 9-6.