**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **LB213 - Proposed Resolutions for remaining security CIDs** | |
| 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 | 333 | 31 | 9.2.1 | 9 | Reading the pre-existing part of this paragraph coming from the base standard, there is a notion of a device that does not implement security…. Do we want 4ab devices without security? If not we should state that the EMDEV shall support security. | Add statement somewhere that the HRP-EMDEV shall support securing of MAC frames, including compact frames as used for MMS UWB control and reporting . | **Reject**  It is preferable to leave the Security of Compact frames as optional. |
| 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. | **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** |

**10.39.11.2 Security of MMS Compact frames [#532]**

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

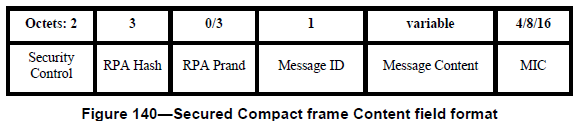
A Secured Compact frame is used to cryptographically protect another Compact frame. Only those Compact frames used within a ranging block structure are eligible for security, while those used outside the ranging block structure are not eligible for security. These are listed in Table 23 and Table 24 respectively. The Secured Compact frame itself shall not be iteratively/recursively secured in another Secured Compact frame. The security of Vendor Specific Compact frames is left to individual vendors/organisations to define and manage and is outside of the scope of this standard.

…

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

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

…



…

If data confidentiality is not provided by the selected Security Level, the Message Content field shall be set as the Message Content field of the corresponding Compact frame indicated by the Secured Compact Frame ID field with the same value of the Message ID field. Otherwise, if data confidentiality is provided by the selected Security Level, the Message Content field shall be set as the Encrypted Private Payload field portion of the c data field from the AEAD transformation process as listed in Table 9-4 in 9.3.4.4.

If data confidentiality is not provided by the selected security level, the MIC field shall be set to the c data field from the AEAD transformation process as listed in Table 9-4 in 9.3.4.4. Otherwise, if data confidentiality is provided by the selected Security Level, the MIC field shall be set to one of MIC-32, MIC-64 or MIC-128 portion of the c data field from the AEAD transformation process as listed in Table 9-4 in 9.3.4.4, the MIC size being determined by the selected Security Level.

**9.2.12 Outgoing frame security procedure for Compact frames**

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

…

g) **Secure the Compact frame**. The Private Payload field shall be set to the Message Content field, and Open Payload field shall be empty. The procedure shall then use the Private Payload field, the Open Payload field, the source address, the frame counter, and the Key to produce the c data field, according to the transformation process described in 9.3.4.