**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-3 (Misc)** |
| Date Submitted | January 2024 |
| Sources | Rojan Chitrakar, Lei Huang (Huawei)rojan.chitrakar@huawei.com |  |
| Re: |   |
| Abstract |  |
| Purpose | To propose resolution for miscellaneous security 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: Editorial changes made during presentation: added “field” to Round-trip time and Reply Time.

Rev 2: Modified the dispositions for comment indices #581 and #582 to Revised: defined the MHR for compact frames.

Rev 3: Added resolution for 627.

Rev 4: Revised the dispositions for comments #581, #582

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Tero Kivinen | 502 | 24 | 9 |  | The security processing for compact frames is not properly defined, for example it does not include policy checking etc. | Remove compact frame format, and uses standard security processing. | Rejected |

**Disposition: Rejected**

**Disposition Detail:** Policy checking is not applicable for compact frames.

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Benjamin Rolfe | 141 | 25 | 9.2.13 | 18 | "shall only" is poor specification language and unnecessary here. Don't need the "only". | Delete "only" | Accepted |
| Benjamin Rolfe | 140 | 25 | 9.2.12 |  | The value TurnAroundTime is not (as far as I can find) defined in this draft. Unfortunately, the term TurnAroundTime is defined and used in the base standard to mean the time it takes for a transceiver to switch from transmit to receive and receive to transmit operations, which is not I think the intended meaning of TurnAroundTime in this draft (I don thin this term means what you thin it means). I think what is meant in this draft is the time it takes to "turn around" e.g. loop back, a reply which is called reply time in the base standard. If in deed this is intended to be something other than what turn around time means in the base standard we need to use a different term. | Change TurnAroundTime to ReplyTime here and in 10.38.6.  | Revised |
| Rojan Chitrakar | 581 | 27 | 9.3.4.3 | 17 | """For Compact frames, the MHR is composed of the ID field, the RPA\_hash field, the RPA\_prand field if present and the Message Control field of the Compact frame.""The original ID field is now split into the Frame Type field and ID field, so Frame Type should also be included in the MHR." | "Change the cited sentence to:""For Compact frames, the MHR is composed of the Frame Type field, the Compact Frame ID field, the RPA\_hash field, the RPA\_prand field if present and the Message Control field of the Compact frame.""" | Revised |
| Rojan Chitrakar | 582 | 27 | 9.3.5.3 | 23 | """For Compact frames, the MHR is composed of the ID field, the RPA\_hash field, the RPA\_prand field if present and the Message Control field of the Compact frame.""The original ID field is now split into the Frame Type field and ID field, so Frame Type should also be included in the MHR." | "Change the cited sentence to:""For Compact frames, the MHR is composed of the Frame Type field, the Compact Frame ID field, the RPA\_hash field, the RPA\_prand field if present and the Message Control field of the Compact frame.""" | Revised |
| Rojan Chitrakar | 584 | 29 | 9.5.11 | 1 | It is not necessary to specify the Type as 16 octets. This is better to use a more general language similar to the baseline. | Change the Type column as:"Set of octets." | Accepted |

**Discussion**：

Comment# 140 is on this:





Field names used in Draft-C:





Comment# 584 is on this:



The length of the Key can vary depending on the security AEAD algorithm used. It is better not to specify the length and rather follow the baseline style:



**Disposition (#**140**): Revised**

**Disposition Detail:**

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

**9.2.12 Outgoing frame security procedure for Compact frames (#140)**

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

**Table 2—Compact frame exceptions to Private Payload field and Open Payload field definitions**

|  |  |  |
| --- | --- | --- |
| **Compact frame type**  | **Private Payload field**  | **Open Payload field**  |
| One-to-one Initiator Secure Report | Round-trip Time field | All other fields in the Message Content field |
| One-to-one Responder Secure Report | Reply Time field | All other fields in the Message Content field |
| One-to-many Initiator Secure Report | Round-trip Time field | All other fields in the Message Content field |
| One-to-many Responder Secure Report | Reply Time field | All other fields in the Message Content field |

**10.38.6 UWB MMS report phase (#140)**

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

…

A report primarily serves to provide ranging results obtained during the ranging phase. The values Reply Time field (as described in xxx 10.38.10.3 Common message fields (comment index#66, 67)) and Round-trip Time field (as described in xxx 10.38.10.3 Common message fields (comment index#66, 67))shall be reported as measured by its sender's local clock without CFO compensation to the receiver's side.

------------------- 24/20r4 -------

**9.2.12 Outgoing frame security procedure for Compact frames (#581, #582)**

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

**Table 2—Compact frame exceptions to Private Payload field and Open Payload field definitions**

|  |  |  |
| --- | --- | --- |
| **Compact frame type**  | **Private Payload field**  | **Open Payload field**  |
| One-to-one Initiator Secure Report | TurnAroundTime | The Message Control field and all other fields in the Message Content field except the Round-trip time field. |
| One-to-one Responder Secure Report | ReplyTime  | The Message Control field and all other fields in the Message Content field except the Reply Time field. |
| One-to-many Initiator Secure Report | TurnAroundTime | The Message Control field and all other fields in the Message Content field except the Round-trip time field. |
| One-to-many Responder Secure Report | ReplyTime  | All other fields in the Message Content field except the Reply Time field. |

**9.3.4.3 a data and m data (#581, #582)**

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

In the AEAD transformation process, the data fields shall be applied as in Table 9-3. For frames other than Compact frames, MHR is as defined in 7.2. For secure Compact frames, MHR, as used in Table 9-2, is represented by the right-concatenation of the Frame Type field and the Compact Frame ID field (as shown in Figure 2), the RPA Hash field and, if present, the RPA Prand field (as shown in Figure 61).

NOTE—The MHR for frames other than Compact frames contains the Auxiliary Security Header field, as defined in 7.2.



**9.3.5.3 c data and a data (#581, #582)**

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

In the AEAD inverse transformation process, the data fields shall be applied as in Table 9-5. For frames other than Compact frames, MHR is as defined in 7.2. For secure Compact frames, MHR, as used in Table 9-5, is represented by the right-concatenation of the Frame Type field and the Compact Frame ID field (as shown in Figure 2), the RPA Hash field and, if present, the RPA Prand field (as shown in Figure 61).



NOTE—The MHR for frames other than Compact frames contains the Auxiliary Security Header field, as defined in 7.2.

-------- 24/20r3--------

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Rojan Chitrakar | 627 | 64 | 10.38.10.1 | 5 | """each PSDU ends with a 2-octet FCS, which …""Secure compact frames do not carry FCS, they carry MIC instead." | "Change the sentence as:"" each PSDU either ends with a 2-octet FCS, which shall be …., or ends with a MIC field as described in 10.38.10.3.16." | Revised |

**Discussion**：



**Disposition: Revised**

**Disposition Detail:**

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

**10.38.10.1 Overview (#627)**

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

Compact frames are employed for the control channel messages. This PSDU format only contains a 1-octet header that conveys the message ID. The PSDU content is message specific to the message ID, however each PSDU ends either with a 2-octet FCS, which shall be the 16-bit ITU-T CRC generated as described in 7.2.11, or with a MIC field as described in 10.38.10.3.16.