**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | Sponsor Ballot Comment resolution on Security in Clause 6 and 9 | |
| Date Submitted | 20, October, 2016 | |
| Source | Jae Seung Lee ETRI  218 Gajeong-ro, Yuseong-gu, Daejeon, 305-700, Korea | Voice: +82 42 860 1326 Fax: +82 42 860 1326 E-mail: jasonlee@etri.re.kr |
| Re: | Recirculation\_Sponsor\_Ballot\_Consolidated\_Comments | |
| Abstract | This document proposes comment resolution on Security CIDs in Clause 6 and 9 for TG3e Recirculation Sponsor Ballot. | |
| Purpose | To be used by the technical editor to apply the necessary changes to the draft. | |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. | |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. | |

**List of contributors**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Jae Seung Lee | ETRI |
| Moon-Sik Lee | ETRI |
| Yeong Jin Kim | ETRI |

CID r01-73

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r01-73 | 39 | 6.2 | 48 | Security overhead should be considered in the maximum frame size when the security option is enabled. | Add a description on the maximum frame size when the security option is enabled. | Rejected  Baseline already has the text on the max frame size when the security option is enabled as follows: “The maximum length of the MAC Frame Body field includes the length of the security fields, if  present.” |

CID r01-74 and r01-75

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r01-74 | 53 | 6.3.4a.2 | 36 | Padding should be added to Figure 6-58g. | Add Padding to Figure 6-58g. | Revised  See the proposed change in 15-16-0734r0. |
| r01-75 | 53 | 6.3.4a.2 | 46 | There is no description on the HRCP MAC Subheader field and the Payload field in this sub-clause. | Add description on the HRCP MAC Subheader field and the Payload field for the secure aggregated data frame. | Revised  See the proposed text change in 15-16-0734r0. |

**CID r01-74 and r01-75: Proposed Text (based on 802.15.3e D05)**

***Change clause 6.3.4a.2 of 802.15.3e D05 as follows:***

**6.3.4a.2 Secure HRCP Aggregated Data frame**

….

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octets: 4 | variable | 16 | 4 | variable | … | 4 | variable | 16 | 4 | variable |
| HRCP  MAC Subheader 1 | Secure Payload 1 | Integrity Code | FCS | Padding |  | HRCP  MAC Subheader  *n* | Secure Payload *n* | Integrity Code | FCS | Padding |
| Secure MAC Subframe Body 1 | | | |  | Secure MAC Subframe Body *n* | | | |

**Figure 6-58g—Secure HRCP Aggregated Data Frame Payload field format**

The HRCP MAC Subheader field is defined in 6.3.4a.1. The Payload Length field in the HRCP MAC Subheader includes the length of the secure payload not including the Integrity Code, FCS and padding octets.

The Secure Payload field is a variable-length field that contains the information, protected by the symmetric key security operations as defined in 9a, that is to be transferred to a DEV.

The Integrity Code field is defined in 6.2.7.5.

The FCS field is defined in 6.2.7.6.

The Padding is defined in 7.8.3.

CID r01-76

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r01-76 | 55 | 6.3.5a.2 | 40 | Do we need these redundant descriptions on the SECID, SFC, Data ID, Integrity Code, FCS field? We did not introduce new figure on the frame format in this sub-clause. | Consider to delete these field descriptions. | Revised  It is better to provide a figure for clarity.  See the proposed change in 15-16-0xxxr0. |

**CID r01-76: Proposed Text (based on 802.15.3e D05)**

***Change clause 6.3.5a.2 of 802.15.3e D05 as follows:***

**6.3.5a.2 Secure HRCP Aggregated Multi-protocol Data frame**

….

The Secure HRCP Aggregated Multi-protocol Data frame uses the same frame format as Figure 6-58g but the Payload 1 through n fields are replaced by the HRCP Multi-protocol Data Payload format illustrated in Figure 6-61a. Figure 6-xx illustrates the Secure HRCP Aggregated Multi-protocol Data frame.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octets: 4 | 1 | variable | variable | 16 | 4 | variable | … | 4 | 1 | variable | variable | 16 | 4 | variable |
| HRCP  MAC Subheader 1 | Data ID | Data Header | Data Payload 1 | Integrity Code | FCS | Padding |  | HRCP  MAC Subheader  *n* | Data ID | Data Header | Data Payload *n* | Integrity Code | FCS | Padding |
| Secure MAC Subframe Body 1 | | | | | |  | Secure MAC Subframe Body *n* | | | | | |

**Figure 6-xx—Secure HRCP Aggregated Multi-protocol Data Frame Payload field format**

The SECID field is defined in 6.2.7.2.

The SFC field is defined in 6.2.7.3.

The HRCP MAC Subheader field is defined in 6.3.4a.1. The Payload Length field in the HRCP MAC Subheader includes the sum of the lengths of the Data ID field, Data Header field, and Data Payload field, not including the Integrity Code, FCS and padding octets.

The Data ID field and the Data Header field are defined in 6.3.5.1.

The Data Payload field is a variable-length field that contains the information that is to be transferred to a DEV. The Data ID field, Data Header field, and Data Payload field are encrypted by the symmetric key security operations as defined in 9a.

The Integrity Code field is defined in 6.2.7.5.

The FCS field is defined in 6.2.7.6.

The Padding is defined in 7.8.3.

CID r01-78

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r01-78 | 91 | 8.1.7 | 1 | Change "the values are used" to "the value is used" | Change "the values are used" to "the value is used" | Revised  See the proposed change in 15-16-0734r0. |

**CID r01-78: Proposed Text (based on 802.15.3e D05)**

***Change clause 8.1.7 of 802.15.3e D05 as follows:***

**8.1.7 Freshness protection**

….

(Page 90, line 62)

A DEV maintains two values for freshness. The CurrentTimeToken is the time token value found in the beacon for the current superframe. ~~and~~ For non-HRCP, the CurrentTimeToken is used to protect all messages sent and check all messages received during that superframe. For HRCP, the CurrentTimeToken together with the SFC value is used to check beacon freshness , and only the SFC value is used to check freshness of other frames. The LastValidTimeToken is used by the DEV to ensure that the security of the beacons have not been compromised.

CID r01-81

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r01-81 | 101 | 9a.3.2 | 40 | It is better to specify that the padding octets in the subframes and HCS for the frame header are not included in the GCM input for clarity. | Specify that the padding octets in the subframes and HCS for the frame header are not included in the GCM input | Revised  See the proposed change in 15-16-0734r0. |

**CID r01-81: Proposed Text (based on 802.15.3e D05)**

***Change clause 9a.3.2 of 802.15.3e D05 as follows:***

**9a.3.2 Symmetric cryptographic operations**….

….

(Page 101, line 40)

The data input to GCM for each subframe shall be taken in the order it is received in the frame, omitting the FCS, Integrity Code, and Padding in the subframe. The HCS for the Frame Header shall be also omitted.

CID r01-82

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r01-82 | 101 | 9a.3.2 | 65 | Since multi-protocol data frame is used in 15.3e, it is better to add description on GCM input for multi-protocol data frame for clarity. | Add description on GCM input for secure multi-protocol data frame in this sub-clause. | Revised  See the proposed change in 15-16-0734r0. |

**CID r01-82: Proposed Text (based on 802.15.3e D05)**

***Add followings at the end of clause 9a.3.2 of 802.15.3e D05:***

**9a.3.2 Symmetric cryptographic operations**….

….

(add at the end of the clause)

Figure 9a-x specifies the length information and data input to the GCM operation for Secure Multi-Protocol Data frames. The GCM operation is applied to each subframe in the data frame separately. For the first subframe, the Auth Data Length 1, *l1(a)*, which is the Auth Data Length for the first subframe, shall be set to 22 which is the length of the Frame Header, SECID, SFC, and the MAC Subheader of the first subframe, and the Enc Data Length 1, *l1 (p)*, which is the Enc Data Length for the first subframe, shall be set to the sum of the lengths of the Data ID field, Data Header field, and Data Payload field in the first subframe.

For the *n*-th subframe, the Auth Data Length *n*, *ln(a)*, which is the Auth Data Length for the *n*-th subframe, shall be set to 4 which is the length of the MAC Subheader of the *n*-th subframe, and the Enc Data Length *n*, *ln (p)*, which is the Enc Data Length for the *n*-th subframe, shall be set to the sum of the lengths of the Data ID field, Data Header field, and Data Payload field in the *n*-th subframe.

The data input to GCM for each subframe shall be taken in the order it is received in the frame, omitting the FCS, Integrity Code, and Padding in the subframe. The HCS for the Frame Header shall be also omitted.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octets: 10 | 2 | 6 | 4 | L1 | | |  | 2 | 2 |
| Frame Header | SECID | SFC | MAC Subheader 1 | Data ID | Data Header | Data  Payload 1 |  | Auth Data Length 1 | Enc Data Length 1 |

***…………..***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Octets: 4 | L*n* | | |  | 2 | 2 |
| MAC Subheader *n* | Data ID | Data Header | Data  Payload *n* |  | Auth Data Length *n* | Enc Data Length *n* |

**Figure 9a-x—GCM input for Secure Multi-Protocol Data frames**