**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 CIDs | |
| Date Submitted | 21, September, 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: | Sponsor\_Ballot\_Consolidated\_Comments | |
| Abstract | This document proposes comment resolution on Security CIDs for TG3e 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 |
| Jaewoo Park | ETRI |
| Jeeyon Choi | ETRI |
| Moon-Sik Lee | ETRI |
| Yeong Jin Kim | ETRI |

CID i-13

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| i-13 | 25 | 6.2.10 | 64 | The Number of subframes fields is 9-bit field, but this clams that up to 256 subframes can be aggregated into a single frame. Is this meaning that the values from 0-0x100 are valid for the Number of Subframes field, but values 0x101-0x1ff are not. | Also can the number of subframes be 0? I think the 256 subframes limitation was from the previous format of the secure aggregated data frame payload, where there was separate 8-bit secure subframe counter. I think this got removed in current version, so now we can have full 511 subframes in both non-secured and secured aggregated frames. Also as SFC is incremented for each subframe, the secure subframe counter is no longer used to generate nonce, this also does not set this requirement. | Revised  TG3e group has decided that 256 subframes are enough for aggregation, and the decision is regardless of the secure subframe counter. Since there is a frame with 0 subframe (such as Stk-ACK), 9 bit is allocated to indicate subframe number 0~256.  To improve the clarity of the sentence, it is better to indicate that other values are reserved.  See the proposed text change in 15-16-0687r2 |

**CID i-13: Proposed Text (based on 802.15.3e D04)**

***Change the following paragraph in clause 6.2.10 of 802.15.3e D04 as follows:***

**6.2.10 TX and ACK Information field for HRCP**

…..

The Number of Subframes field indicates the number of subframes included in the current frame. Up to 256 subframes can be aggregated into a single frame. The valid range of this field is [0-256] and other values are reserved.

CID i-217 and i-218

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| i-217 | 24 | 6.2.7.1 | 43 | "6.2.7.1 Frame Payload field" in the baseline should be amended to include pairnet. | Change "in the piconet" to "in the piconet or pairnet". Add reference to the secure MAC frame body format for HRCP. | Revised  See the proposed text change in 15-16-0687r2 |
| i-218 | 25 | 6.2.7.4 | 4 | "6.2.7.4 Secure Payload field" in the baseline should be amended to include pairnet. | Amend the baseline to inclulde secure payload for pairnet. | Revised.  See the proposed text change in 15-16-0687r2 |

**CID i-217 and i-218: Proposed Text (based on 802.15.3e D04 and 802.15.3-2016)**

***Amend the following paragraphs in clause 6.2.7.1 (Frame Payload field) and 6.2.7.4 (Secure Payload field) of 802.15.3-2016 as follows:***

**6.2.7.1 Frame Payload field**

The Frame Payload field is a variable-length field that carries the information that is to be transferred to a

DEV or group of DEVs in the piconet or to a DEV in the pairnet. In the case of a secure frame, it also includes the required security information and the secure payload, as illustrated in Figure 6-5 for piconet and as described in 6.2.7.9 for pairnet.

**6.2.7.4 Secure Payload field**

The Secure Payload field is a variable-length field that contains the information, protected by the symmetric key security operations, as defined in 9.3 for piconet and as defined in 9a for pairnet, that is to be transferred to a DEV or group of DEVs in the piconet or to a DEV in the pairnet. As illustrated in Figure 6-5 for piconet and as described in 6.2.7.9 for pairnet, the Secure Payload field is a part of the Frame Payload field and does not include the SECID, SFC, or Integrity Code fields.

CID i-227 and i-228

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| i-227 | 45 | 6.5 | 33 | Some security related commands (such as Distribute Key Request, Distribute Key Response, Security Information Request, Security Information, and Security Message) are not listed in the table 6-22a. | Check the security related commands that are used in HRCP and include them in the table 6-22a. | Revised  See the proposed text change in 15-16-0687r2 |
| i-228 | 47 | 6.5 | 9 | Security Message command is used in 15.3e, but it is marked "Not used" in table 6-22b | Change "Not used" to "Optional" | Accepted |

**CID i-227: Proposed Text (based on 802.15.3e D04)**

***Change Table 6-22a as follows:***

**Table 6-22a—Command types for pairnet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Command type**  **hex value**  **b15–b0** | **Command name** | **Subclause** | **Associated** |
| 0x0000 | Association Request command | 6.5.1.1 | - |
| 0x0001 | Association Response command | 6.5.1.2 | X |
| 0x0002 | Disassociation Request command | 6.5.1.3 | X |
| 0x0003 | Request Key command | 6.5.2.1 | X |
| 0x0004 | Request Key Response command | 6.5.2.2 | X |
| 0x0005 | Distribute Key Request command | 6.5.2.3 | X |
| 0x0006 | Distribute Key Response  command | 6.5.2.4 | X |
| 0x0007-0x000B | Reserved | - | - |
| 0x000C | Security Information Request  command | 6.5.4.3 | X |
| 0x000D | Security Information command | 6.5.4.4 | X |
| 0x000E | Probe Request command | 6.5.4.5 | X |
| 0x000F | Probe Response command | 6.5.4.6 | X |
| 0x0010–0x0017 | Reserved | - | - |
| 0x0018 | Transmit Power Change command | 6.5.7.5 | X |
| 0x0019 | Array Training command | 6.5.9.5 | X |
| 0x001A | Array Training feedback | 6.5.9.6 | X |
| 0x001B–0x001D | Reserved | - | - |
| 0x001E | Security Message command | 6.5.9.1 | X |
| 0x001F–0x00FF | Reserved | - | - |
| 0x0100–0x00FF | Vendor Defined | 6.5.9.2 | X |

CID i-245

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| i-245 | 65 | 8.1.2 | 8 | "8.1.2 Key tarnsport" in the baseline should be amended to include pairnet: Change "piconet group data key" to "piconet group data key or pairnet group data key" | As in the comment | Accepted  See the proposed text change in 15-16-0687r2 |

**CID i-245: Proposed Text (based on 802.15.3e D04 and 802.15.3-2016)**

***Amend the following paragraphs in clause 8.1.2 (Key transport) of 802.15.3-2016 as follows:***

**8.1.2 Key transport**

All keys that are transmitted from one DEV to another shall be encrypted as specified in the key request, as described in 8.4.3, and distribute key protocols, as described in 8.4.2. For example, key transport is used to provide a copy of the piconet group data key or pairnet group data key to a DEV.

CID i-246, i-247, i-248, and i-252

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| i-246 | 66 | 8.1.7 | 2 | "The last SFC received shall be only updated after ~" : Since the SFC for subframes that are not the 1st subframe are implicitly indicated in 15.3e, more description is needed for clarity. Change other related part in the security spec. | As in the comment | Revised  See the proposed text change in 15-16-0687r2 |
| i-247 | 69 | 8.3.5 | 19 | Change "send only frames that have increasing SFCs" to "send only frames or subrames that have increasing SFCs" since SFC is increased for each subframe in 15.3e. Apply similar changes to related part in the security spec. | As in the comment | Revised  See the proposed text change in 15-16-0687r2 |
| i-248 | 70 | 8.3.7 | 4 | "both of" should be struck out. | struck out "both of". | Accepted  See the proposed text change in 15-16-0687r2 |
| i-252 | 74 | 9a.2.4 | 52 | Delete "that is intended for a particular DEV address". Since target DEV address is not used in 15.3e nonce. | Delete "that is intended for a particular DEV address". | Accepted  See the proposed text change in 15-16-0687r2 |

**CID i-246, i-247 and i-248: Proposed Text (based on 802.15.3e D04)**

***Change the following paragraph in clause 6.2.7.3 (SFC field) of 802.15.3-2016 as follows:***

**6.2.7.3 Secure Frame Counter (SFC) field**

The Secure Frame Counter field (SFC) contains a counter that is used to ensure the uniqueness of the nonce in a secure frame. ~~A~~For non-HRCP, a DEV shall not reuse a frame counter with the same time token, as described in 6.3.1.1, and key, as described in 8.3.5. For HRCP, a DEV shall not reuse a frame counter with the same key, as described in 8.3.5. ~~T~~For non-HRCP, the DEV shall initialize the SFC to zero for the first frame sent and increment it for each successive secure frame sent. For HRCP, the DEV shall initialize the SFC value to zero for the first frame or subframe sent and increment it for each successive secure frame sent or each successive subframe sent in the aggregated frame. Only the SFC value of the first subframe is explicitly included in the transmitted aggregated frame. ~~W~~For non-HRCP, when the time token, as described in 6.3.1, is updated, the DEV shall reset the SFC to zero. For HRCP, the SFC value shall be increased even when the time token is updated. In the case where the DEV receives a new key, the DEV shall set the SFC to zero.

***Change the following paragraphs in clause 9a.2.4 (Nonce value) of 802.15.3-2016 as follows:***

**9a.2.4 Nonce value**

In order to preserve the security of the symmetric algorithms, the nonce used for GCM encryption and authentication shall be unique for a given key. As a result, the DEV shall not reuse any Secure Frame Counter (SFC) field value with a given key(as this would cause a repeated nonce).

This uniqueness is guaranteed by the use of the DEV address of the source DEV and the Secure Frame Counter (SFC). The DEV address is globally unique and guarantees that two different DEVs sharing the same key will use a different nonce. The DEV address of the source DEV and the secure frame counter guarantee uniqueness of the nonce for a given key as long as a DEV does not send more than 248 frames or subframes to the other DEV in the pairnet.

If a frame or a subframe is retransmitted and a single bit in the header or frame body has been changed, a new nonce shall be used. To implement this, each time a frame or a subframe is retransmitted, the value of the Secure Frame Counter shall be incremented.

…..

The Secure Frame Counter field is set to the value of the SFC corresponding to the transmitted frame or subframe that is being protected. SFC field is defined in 6.2.7.3. If the transmitted frame is an aggregated frame, only the Secure Frame Counter of the first subframe is explicitly included in the aggregated frame, and the Secure Frame Counter value for other subframes shall be incremented for each subframe in the aggregated frame, starting from the value explicitly indicated in the SFC field of the transmitted frame.

***Change the following paragraph in clause C.3.2 (Replay prevention) of 802.15.3-2016 as follows:***

**C.3.2 Replay prevention**

…..

For HRCP, the 6 octet SFC allows up to 248 frames or subframes to be sent in multiple superframes. In the worst case scenario described in C.3.1, the duration for transmitting 248 frames using 6 octet SFC is 4.17 days. 6 octet time token is used in HRCP. In the worst case scenario where a HRCP PNC keeps transmitting beacons and no DEV is associated, the time token will roll over every 254 years if we assume 28.5 μs beacon interval.

***Change the following paragraphs in clause 8.1.7 (Freshness protection) of 802.15.3-2016 as follows:***

**8.1.7 Freshness protection**

…..

To prevent replay of old messages, a strictly-increasing time token is included in the beacon. A DEV shall reject as invalid a received beacon with a time token less than or equal to the current time token. For HRCP, a DEV shall further check the SFC and the SECID included in the beacon and shall reject as invalid the beacon if the SFC value in the beacon is not strictly greater than the last SFC value received from that DEV corresponding to the key identified by the SECID. The last SFC value received shall be only updated after the received integrity code corresponding to the SFC value of the received frame or subframe is successfully verified. In addition, for non-HRCP, the time token is included in the nonce, as described in 9.2.4, for each secure frame, as described in 6.2, so the integrity check will fail if a frame is replayed in a different superframe. For HRCP, a DEV shall check the SECID included in each secure frame and the SFC value of each secure frame or subframe, and shall reject as invalid the received frame or subframe if the SFC value corresponding to the frame or subframe is not strictly greater than the last SFC value received from that DEV corresponding to the key identified by the SECID to detect whether the frame or subframe is replayed or not. The last SFC value received shall be only updated after the received integrity code corresponding to the SFC value of the received frame or subframe is successfully verified. A DEV maintains two values for freshness. The CurrentTimeToken is the time token value found in the beacon for the current superframe and is used to protect all messages sent and check all messages received during that superframe.

For HRCP, the values are used only to check beacon freshness and 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.

***Change the last paragraph in clause 8.3.5 (Secure frame generation) of 802.15.3-2016 as follows:***

**8.3.5 Secure frame generation**

…..

A non-HRCP DEV shall send only frames that have increasing SFCs in a superframe, except for frames that are retransmitted with the same SFC without any intervening frames having been sent. An HRCP DEV shall send only frames or subframes that have increasing SFC values for a single key corresponding to the SECID indicated in the transmitted frames.

***Change the following two paragraphs in clause 8.3.7 (Secure frame reception) of 802.15.3-2016 as follows:***

**8.3.7 Secure frame reception**

…..

When a DEV receives a secure beacon frame, as defined in 6.3.1.2, the DEV shall determine if the received time token is greater than the CurrentTimeToken and less than the LastValidTimeToken + *mMaxTimeTokenChange*. If not, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to BAD-TIME-TOKEN and shall not perform any additional operations on the received beacon. The DEV shall also determine if the SECID matches the SECID of the piconet group data key or pairnet group data key stored in the MAC/MLME, or the SECID of a valid old piconet group data key or old pairnet group data key, as described in 8.3.5. If the SECID matches, an HRCP DEV shall further check the SFC included in the beacon and the MLME shall return an MLME-SECURITYERROR.indication to the DME with the ReasonCode set to BAD-TIME-TOKEN and shall not perform any additional operations on the received beacon if the SFC value in the beacon is not strictly greater than the last SFC value received from that DEV corresponding to the key identified by the SECID. The last SFC value received shall be only updated after the received integrity code corresponding to the SFC value of the received frame or subframe is successfully verified. If the SECID does not match, the DEV may request a new piconet group data key or new pairnet group data key, as described in 8.3.2. If ~~both of~~these checks succeed, the DEV shall check the integrity code on the beacon using the piconet group data key or pairnet group data key. If this succeeds, the DEV shall accept the beacon and set the LastValidTimeToken and CurrentTimeToken to be the time token in the beacon.

When a DEV receives a secure non-Beacon frame, it shall use the appropriate keying material depending on the type of frame, SECID, and SrcID found in the frame. If the SECID in the frame does not correspond to known keying material in the receiving DEV, the MLME shall return an MLME-SECURITYERROR.indication to the DME with the ReasonCode set to UNAVAILABLE-KEY and shall not perform any additional operations on the received frame. ~~A~~For non-HRCP, a DEV shall reject all frames that do not have an SFC that is strictly greater than the last SFC received from that DEV in that superframe. For HRCP, a DEV shall reject all frames or subframes that do not have a corresponding SFC value that is strictly greater than the last SFC value received from that DEV corresponding to the key identified by the SECID in the received frames. The last SFC value received shall be only updated after the received integrity code corresponding to the SFC value of the received frame or subframe is successfully verified.

CID i-250 and i-251

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| i-250 | 71 | 8.3.9 | 24 | Array Training Feedback command is not listed in the table 8-1a. | Add "Array Training Feedback" command in the table. | Revised  See the proposed text change in 15-16-0687r2 |
| i-251 | 72 | 8.3.9 | 28 | PM Mode Change Response and PM Mode Change are not used in 15.3e | Remove PM Mode Change Response and PM Mode Change from the table 8-1a | Revised  See the proposed text change in 15-16-0687r2 |

**CID i-250 and i-251: Proposed Text (based on 802.15.3e D04)**

***Modify Table 8-1a as follows:***

Table 8-1a—Key selection for secure HRCP frames

| Frame type or command | None | HRCP PNC-DEV mgmt key | Pairnet group data key | Comment | |
| --- | --- | --- | --- | --- | --- |
| Beacon frame |  |  | X | All secure beacon frames shall be protected by the pairnet group data key. | |
| Stk-ACK frame | X |  |  | Stk-ACK frames shall not be secured with any key. | |
| Data frame |  |  | X | Only secure data frames shall be exchanged between DEVs that have a secure relationship. The Pairnet group data key shall be used for secure data frames between DEVs in pairnet. | |
| Association Request | X |  |  | Association Request commands shall not be secured with any key. | |
| Association Response | X |  |  | Association Response commands shall not be secured with any key. | |
| Disassociation Request | X | X |  | Disassociation Request commands shall not be secured with any key before the DEV establishes secure membership in the pairnet and shall be protected by the HRCP PNC-DEV management key otherwise. | |
| Request Key |  | X |  | The management key for the relationship shall be used for this command. | |
| Request Key Response |  | X |  | The management key for the relationship shall be used for this command. | |
| Distribute Key Request |  | X |  | The management key for the relationship shall be used for this command. | |
| Distribute Key Response |  | X |  | The management key for the relationship shall be used for this command. | |
| Security Information Request |  | X |  |  | |
| Security Information |  | X |  |  | |
| Probe Request | X | X | X | If the Probe Request command is sent to or from the HRCP PNC before the DEV becomes a secure member of the pairnet, the command shall not be secured by any key. If the DEVs do not share an individual relationship, the pairnet group data key shall be used. Otherwise, the HRCP PNC-DEV management key for the relationship shall be used. | |
| Probe Response | X | X | X | If the Probe Request command is sent to or from the HRCP PNC before the DEV becomes a secure member of the pairnet, the command shall not be secured by any key. If the DEVs do not share an individual relationship, the pairnet group data key shall be used. Otherwise, the HRCP PNC-DEV management key for the relationship shall be used. | |
| Transmit Power Change |  | X | X | If the DEVs do not share an individual relationship, the pairnet group data key shall be used. Otherwise, the HRCP PNC-DEV management key for the relationship shall be used. | |
| Array Training |  | X | X | If the DEVs do not share an individual relationship, the pairnet group data key shall be used. Otherwise, the HRCP PNC-DEV management key for the relationship shall be used. | |
| Array Training Feedback |  | X | X | If the DEVs do not share an individual relationship, the pairnet group data key shall be used. Otherwise, the HRCP PNC-DEV management key for the relationship shall be used. | |
| Security Message | X |  |  |  | |
| Vendor Defined |  | X | X | If the DEVs do not share an individual relationship, the pairnet group data key shall be used. Otherwise, the HRCP PNC-DEV management key for the relationship shall be used. | |