**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-related MLME | |
| 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-related MLME 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 r01-68 and r01-69

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r01-68 | 34 | 5.3.7 | 42 | 5.3.7 Security management has to be updated to include pairnet | Amend 5.3.7 Security management in the baseline to include the pairnet. | Revised  See the proposed text change in 15-16-0733r0. |
| r01-69 | 34 | 5.3.10 | 58 | 5.3.10 Security Information retrieval has to be updated to include pairnet. | Amend 5.3.10 Security Information in the baseline to include the pairnet. | Revised  See the proposed text change in 15-16-0733r0. |

**CID r01-68 and r01-69: Proposed Text (based on 802.15.3-2016)**

***Amend clause 5.3.7 of 802.15.3-2016 as follows:***

**5.3.7 Security management**

……..

**Table 5-12—MLME-MEMBERSHIP-UPDATE and MLME-SECURITY-ERROR primitive parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| SECID | 2 octets | As defined in 6.2.7.2 | The identifier for the key. |
| OrigId | Integer | Any valid DEVID, as defined in 6.2.3 for piconet and as defined in 6.2.3a for pairnet, except for the BcstID, the McstID or the UnassocID | Either the PNCID or HRCP PNCID, if this key is for the DEV’s PNC or HRCP PNC personality, or the DEV’s DEVID. |
| TrgtId | Integer | Any valid DEVID, as defined in 6.2.3 for piconet and as defined in 6.2.3a for pairnet, except for the BcstID, the McstID or the UnassocID | The DEVID of the target DEV for this relationship. |
| MembershipStatus | Enumeration | MEMBER,  NON-MEMBER | Indicates the membership status for the provided SECID. If NON-MEMBER, KeyInfo is zero length. |
| KeyOriginator | Boolean | TRUE, FALSE | Indicates if the DEV is the key originator for this relationship. This is always true when the OrigId is the PNCID or HRCP PNCID. |
| KeyInfo | Octet string | Any valid symmetric key for the symmetric key security operations, as defined in 9.3 for piconet and as defined in 9a.3 for pairnet | The key used for protecting frames between this DEV and the TrgtId DEV. |
| SrcID | Integer | Any valid DEVID, as defined in 6.2.3 for piconet and as defined in 6.2.3a for pairnet, except for the BcstID, the McstID or the UnassocID | The DEVID of the DEV that is the source of a security error. |
| Timeout | Integer | 0–65535 | The time in milliseconds allowed for the primitive to complete. |
| ResultCode | Enumeration | SUCCESS, FAILURE | Indicates the result of the MLME request. |
| ReasonCode | Enumeration | NOT\_ASSOCIATED,  TARGET\_UNAVAILABLE,  UNAVAILABLE\_KEY,  FAILED\_SECURITY\_CHECK,  BAD\_TIME\_TOKEN,  INVALID\_SEC\_VALUE,  OTHER | The reason for a security error. |

....

**Table 5-13—MLME-SECURITY-MESSAGE primitive parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| TrgtId | Integer | Any valid DEVID, as defined in 6.2.3 for piconet and as defined in 6.2.3a for pairnet | Specifies the DEVID of the target of the MLME request. |
| OrigId | Integer | Any valid DEVID, as defined in 6.2.3 for piconet and as defined in 6.2.3a for pairnet | Specifies the DEVID of the originator of the MLME request. |
| UniqueId | Octet string | Any valid OUI or CID, as defined in 6.4.7 | A unique identifier for the entity that defines the format of the security information, as described in 6.4.7. |
| SecurityInformation | Octet string | Any valid octet string | Security information that will be passed from one DEV to another peer DEV in the piconet or pairnet. |
| Timeout | Integer | 0–65535 | The time in milliseconds allowed for the primitive to complete. |
| ResultCode | Enumeration | SUCCESS, FAILURE | Indicates the result of the MLME request. |
| ReasonCode | Enumeration | REQUEST\_TIMEOUT,  NOT\_ASSOCIATED,  TARGET\_UNAVAILABLE,  OTHER | The reason for a security error. |

….

**5.3.7.4 MLME-SECURITY-MESSAGE.request**

This primitive initiates the sending of a Security Message command, as described in 6.5.9.1, to the target DEV in the piconet or pairnet. The semantics of this primitive are as follows:

…

**5.3.7.6 MLME-SECURITY-MESSAGE.indication**

This primitive reports the reception of a Security Message command, as described in 6.5.9.1, from a DEV in the piconet or pairnet. The semantics of this primitive are as follows:

***Amend clause 5.3.10 of 802.15.3-2016 as follows:***

**5.3.10 Security information retrieval**

These primitives are used to request security information about other DEVs in the piconet or pairnet, as described in 8.4.1. The parameters used for the MLME-SECURITY-INFO primitives are defined in Table 5-16.

**5.3.10.1 MLME-SECURITY-INFO.request**

This primitive initiates a request to a DEV for security information regarding either a single DEV or all of the DEVs in the piconet or pairnet. The semantics of the primitive are as follows:

……..

**Table 5-16—MLME-SECURITY-INFO primitive parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| QueriedDevId | Integer | Any valid DEVID, as defined in 6.2.3 for piconet and as defined in 6.2.3a for pairnet, except for the McstID or the UnassocID | The DEVID of the DEV for which information is being requested. If it is set to the BcstID, then the information is being requested for all DEVs. |
| TrgtId | Integer | Any valid DEVID, as defined in 6.2.3 for piconet and as defined in 6.2.3a for pairnet | The DEVID of the DEV for which the security information request is intended. |
| OrigId | Integer | Any valid DEVID, as defined in 6.2.3 for piconet and as defined in 6.2.3a for pairnet | Specifies the DEVID of the DEV that initiated the MLME request. |
| NumSecurityRecords | Integer | 0–65535 | Number of entries in the SecurityRecordSet. |
| SecurityRecordSet | A set of Security Record fields, as defined in 6.5.4.4 | A set containing 0 or more instances of variable-length Security Record field. The maximum number of instances depends on the size of the records, *pMaxFrameBodySize* and the length of the secure command security fields, as defined in 6.3.3.2 for piconet and as defined in 6.3.3a for pairnet. | The SecurityRecordSet is returned to indicate the results of a Security Information Request command. |
| Timeout | Integer | 0–65535 | The time in milliseconds allowed for the primitive to complete. |
| ResultCode | Enumeration | SUCCESS, FAILURE | Indicates the result of the MLME request. |
| ReasonCode | Enumeration | REQUEST\_TIMEOUT,  NOT\_ASSOCIATED,  TARGET\_NOT\_ASSOCIATED,  OTHER | Indicates the reason for a ResultCode of FAILURE. |

……..

**5.3.10.2 MLME-SECURITY-INFO.confirm**

This primitive reports the result of the request to a DEV for security information regarding either a single DEV or all of the DEVs in the piconet or pairnet. The semantics of the primitive are as follows:

…

**5.3.10.3 MLME-SECURITY-INFO.indication**

This primitive indicates the reception of a request by a DEV for security information it manages regarding either a specific DEV or all of the DEVs in the piconet or pairnet. The semantics of the primitive are as follows: