**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | Comment resolutions for i-1389, i-2010, i-0146, i-2876, i-0293, i-1119, i-1756, i-2294, i-1124, i-1761, i-2340, i-0071, i-1123, i-1760, i-2800 |
| Date Submitted | [July 2019] |
| Source | Aditya V. Padaki (Samsung)Yi Yang (Samsung)Jong-Hoon Jang (Samsung)Jonghyo Lee (Samsung)Boon Loong Ng (Samsung)Mingyu Lee (Samsung)Seongah Jeong (Samsung)Zheda Li (Samsung)Rias Al-kadi (NXP)Ayman Nagiub (Apple)Benjamin Rolfe (Blind Creek) |  |
| Re: | Re: |  |
| Abstract | Text for possible inclusion in IEEE 802.15.4z MAC |
| Purpose | Provision of the text to facilitate its incorporation into the draft text of the IEEE 802.15.4z standard currently under development in the 802.15 TG4z. |
| 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 |  |
| Patent Policy | The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and<http://standards.ieee.org/guides/opman/sect6.html#6.3>.Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and<http://standards.ieee.org/board/pat>. |

***Goal of this submission:***

*The objective of this submission is to provide text, for inclusion into the 15.4z draft*

*The changes are based on 802.15.4.*

*This document addresses the following comments:*

**i-1389, i-2010, i-0146, i-2876, i-0293, i-1119, i-1756, i-2294, i-1124, i-1761, i-2340, i-0071, i-1123, i-1760, i-2800, rg-0004, rg-0010**

*Add the following normative reference in Clause 2*

IEEE 802.15.9-2016 - IEEE Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams

*Replace Section 6.9.7.9 with the following text*

**6.9.7.9 Ranging Enhanced Secure Service Transactions**

The enhanced ranging capabilities of the ERDEV can be used to protect by using ranging to check that the distance between the communicating devices is as expected. In such secure service transaction scenarios, the higher layer is often interfacing between the radio and a secure element used in validating the transaction. The MPX IE [B#] with the dispatch code for Ranging Enhanced Secure Service Transactions (allocation number and name TBD) shall be used to transfer information relevant to the Secure Element between the ERDEVs in conjunction with range measurements. The MPX IE shall be formatted with two fields, the first octet being Transaction Control and Upper-Layer Frame Fragment with variable number of octets (refer Figure 9 in [B#]). The Transaction Control field consists of a 3-bit Transfer Type field and a 5 bit Transaction ID field.

The Transfer Type shall be set to 1 (0b001) to indicate that Multiplex ID associated with the dispatch code for MPX IE is indicated by the 5 bit Transaction ID field of Transaction Control. Transaction ID field contains the 5 least significant bits of the Multiplex ID used as the dispatch code (see Table 20, Page 41 in 802.15.9 [B#]) and is used as an identifier to specify that this is IE/frame contains info used for Ranging Enhanced Secure Transactions.

The MPX IE with the dispatch code <ANA> (included in the Transaction ID field) for Ranging Enhanced Secure Service Transactions, is applicable to upper layer protocols that support transactions with a secure component in the device. When an MPX IE with the Transaction ID for Ranging Enhanced Secure Service Transactions is received in an RFRAME, the MAC delivers it to the higher layer with an associated ranging measurement, which the higher layer can use to limit access based on range. The Upper-Layer Frame Fragment field of the MPX IE contains fields to identify and distinguish transactions, and fields to carry information about the MAC payload that can be used by the higher layer to route the payload to different device components as shown in Figure X3. If the transaction takes place using multiple frames, all frames that transport data belonging to the particular transaction shall include the MPX IE with the same Transaction ID and USS ID value.



**Figure X3 – Format of Upper-Layer Frame Fragment field of MPX IE for Ranging Enhanced Secure Service Transactions**

The Payload Type field specifies the type of the content contained in the MAC Payload field. The Payload Type field shall have one of the values defined in Table T1.

**Table T1 – Payload Type field values**

|  |  |
| --- | --- |
| **Payload Type field value** | **Meaning** |
| 0 | Application specific payload |
| 1 | MAC Payload field contains an APDU as defined by ISO/IEC 7816-4 [B21] |
| 2 | MAC Payload field contains a Mifare Classic® command or response |
| 3 | MAC Payload field contains a Mifare Desfire® command or response |
| 4 | MAC Payload field contains an Information field as defined by JIS X 6319-4 [B20] |
| All other values | Reserved |

The USSID Length field specifies the number of octets in the USSSID field. The valid range USSID Length shall be 0 to 16.

The USSID field is used to identify and distinguish transactions. All frames that transport data belonging to the same transaction should use the same USSID value. The content of the USSID field depends on the Payload Type as per Table T2. The Secure Service IE cannot support differentiation of transactions with the same Payload Type value unless a USSID is provided. The USSID field includes an ID that identifies the target application for the transaction.

**Table T2—Permissible USSID depending on Payload Type field in Secure Service IE**

|  |  |
| --- | --- |
| **Payload Type Value** | **Permissible content of the USSID Length and USSID fields** |
| 0 | Either the USSID field shall contain an application identifier (AID) formatted as specified in Figure X4 or the USSID Length shall be set to 0, in which case the transaction is assumed to use implicit selection as defined in ISO/IEC 7816-4 [B21]. |
| 1 | USSID Length shall be set to 0. |
| 2 | Either the USSID field shall contain an AID formatted as specified in Figure X4 or the USSID Length shall be set to 0. |
| 3 | The USSID Length shall be set to 2 and the USSID field shall contain a system code (SC) formatted as specified in Figure X5. |



**Figure X4—Format of USSID field when carrying an AID**

The AID shall be an Application Identifier as defined in ISO/IEC 7816-5 [B22].



**Figure X5—Format of USSID field when carrying an SC**

The SC shall be a system code as defined by JIS X 6319-4 [B20].

The Additional Info Length field specifies the number of octets in the Additional Info field. The Additional Info field is used to provide a summary of the transaction, which can be used for user information and authorization. If present, the Additional Info field contains a string that can be used to provide additional information to the upper layer about the transaction to be performed. The encoding of characters into the Additional Info field shall be according to UTF-8 [B23]. Line breaks in the string shall be represented using a carriage return (CR) followed by a line-feed (LF), i.e. 0x0D, 0x0A in UTF-8. The Additional Info field should be present in the first frame used by a transaction.

*Delete Section 7.4.4.56 (Secure Service IE)*

**Bibliography**

*Additional references that are used in the new text above*

[B20] JIS X 6319-4:2016, “Specification of implementation for integrated circuit(s) cards-Part 4: High speed proximity cards”.

[B21] ISO/IEC 7816-4:2013, “Identification cards – Integrated circuit cards – Organization, security and commands for interchange”.

[B22] ISO/IEC 7816-5:2013, “Identification cards – Integrated circuit cards – Numbering system and

registration procedure for application identifiers”.

[B23] RFC3629, “UTF-8, a transformation format of ISO 10646”, F. Yergeau, 30 July 2018.

[B#] IEEE 802.15.9-2016 - IEEE Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams