**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | Alternative Draft Text for Inclusion of UWB Secure Service Information Element | |
| Date Submitted | [January 2019] | |
| Source | Yi Yang (Samsung)  Jong-Hoon Jang (Samsung)  Jonghyo Lee (Samsung)  Aditya V. Padaki (Samsung)  Boon Loong Ng (Samsung)  Rias Al-kadi (NXP)  Klaus Roehrle(Sony) |  |
| 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, to standardize the Secure Service IE to allow the UL to route traffic belonging to secure transactions to one or more hosts inside the receiver (some of which may be Secure Elements).*

*The changes are based on 802.15.4-2015.*

### Nested IEs

*Add a new row for the Secure Service IE in Table 7-16.*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sub-ID**  **value** | **Name** | **Enhanced Beacon** | **Enhanced ACK** | **Data** | **Multipurpose** | **MAC Command** | **Format subclause** | **Use description** | **Used by** | **Created by** |
| 0x?? | Secure Service IE |  |  | X | X |  | X.X.X:X | X.X.X.X | UL | UL |

*New section to be inserted in the list of Nested IEs (7.4.4.x).*

#### Secure Service IE

The Secure Service IE is applicable if the UL uses a protocol that supports transactions with a secure component in the receiver device (in this section, UL refers to the layers above the MAC). The Secure Service IE provides additional information about the MAC payload that can be used by the receiver to route the payload device internal to different components. The proposal allows the UL to perform multiple transactions in parallel on a single 802.15.4 communication link. The Secure Service IE is applied in both communication directions All frames that transport data belonging to a corresponding transaction shall include the Secure Service IE.

The Secure Service IE shall be formatted as illustrated in **Figure 1**.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Bits : 0­-2** | **3-5** | **6-10** | **11-15** | **Octets: 0-16** | **0-31** |
| Payload Type | Reserved | USSID Length | Additional Info Length | USSID (UWB Secure Service ID) | Additional Info |

**Figure 1 – Secure Service IE Content field format**

The Payload Type field indicates the type of the content contained in the MAC Payload field. The Payload Type field shall have one of the values defined in **Table 1**.

**Table 1 – Payload Type field values**

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

The USSID field is used to identify and distinguish transactions. All frames that transport data belonging to the same transaction have to use the same USSID value.

The Additional Info fields provides a summary of the transaction, which can be used for user information and authorization.

The USSID Length field specifies the number of octets in the USSSID field. If its value is zero, the USSID field is omitted. Values above 16 shall be reserved.

The content of the USSID Length and USSID fields depend on the Payload Type:

* If the Payload Type value is equal to 0, either the USSID field shall contain an AID as defined in **Table 2** or the USSID Length shall be set to 0. In the latter case the transaction is assumed to use implicit selection as defined in ISO/IEC 7816-4 [B##].
* If the Payload Type value is equal to 1, the USSID Length shall be set to 0.
* If the Payload Type value is equal to 2, the USSID field shall contain an AID as defined in **Table 2** or the USSID Length shall be set to 0.
* If the Payload Type value is equal to 3, the USSID field shall contain a SC as defined in **Table 3**. The USSID Length shall be set to 2.

The Secure Service IE does not support to differentiate between multiple transactions with the same Payload Type value and using a USSID Length of 0.

The Additional Info Length field specifies the number of octets in the Additional Info field. If its value is zero, the Additional Info field is omitted.

The USSID field includes an ID that identifies the target application for the transaction. If present, the value of the USSID field shall be one of the types defined in **Table 2** or **Table 3**.

**Table 2 –AID type USSID field value**

|  |
| --- |
| **Octets : 5­-16** |
| AID (Application IDentifier) |

The AID field shall contain an Application Identifier as defined in ISO/IEC 7816-5 [B\*\*].

**Table 3 –SC type USSID field value**

|  |
| --- |
| **Octets : 2** |
| SC (System Code) |

The SC field shall contain a system code as defined by JIS X 6319-4 [B#].

If present, the Additional Info field contains a string that can be used to provide additional information to the user about the transaction to be performed. The encoding of characters into the Additional Info field shall be according to UTF-8 [B\*]. Line breaks in the string shall be represented using the CRLF (0x0D,0x0A in UTF-8).

The Additional Info field should be present in the first frame used by a transaction.

***Change section number for “Vendor Specific Nested IE” and “Channel hopping IE” from 7.4.4.30 and 7.4.4.31 to 7.4.4.31 and 7.4.4.32 due to new sections 7.4.4.30.***

#### Vendor Specific Nested IE

#### Channel hopping IE

**Bibliography**

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

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

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

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

registration procedure for application identifiers”.

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