IEEE P802.15

Wireless Personal Area Networks

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | SecurityParams changes |
| Date Submitted | 11, November 2019 |
| Source | Tero KivinenFinland | Voice: +358 40 547 4476E-mail: kivinen@iki.fi |
| Re: | Move all Security related parameters to separate substructure and create new section describing them. |
| Abstract | This document proposes a change for 802.15.4 draft to be done either now, or in the next revision cycle. |
| Purpose | Clarify the 802.15.4 standard and make it easier to understand. |
| 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. |

#  Overview

Most of the MLME calls in the 802.15.4 have 4 common security related parameters in them. In 802.15.4-2015 descriptions were harmonized to reference the MCPS-DATA primitives, but the parmeters were left intact. This document proposes a change that would remove all separate security related paramaters and would replace them with one SecurityTxParams or SecurityRxParams structure and provide reference to new subsection describing those fields.

These changes only affect the sections 8 and Annex F. No changes anywhere else is needed.

# MLME-ASSOCIATE.request example

Current MLME-ASSOCIATE.request semantics:

MLME-ASSOCIATE.request (

 ChannelNumber,

 ChanllePage,

 CoordAddrMode,

 CoordAddress,

 CapabilityInformation,

 SecurityLevel,

 KeyIdMode,

 KeySource,

 KeyIndex,

 ChannelOffset,

 HoppingSequenceId,

 DsmeSequenceId,

 Direction,

 AllocationOrder,

 HoppingSequenceRequest

 )

New semantics:

MLME-ASSOCIATE.request (

 ChannelNumber,

 ChanllePage,

 CoordAddrMode,

 CoordAddress,

 CapabilityInformation,

 SecurityTxParams,

 ChannelOffset,

 HoppingSequenceId,

 DsmeSequenceId,

 Direction,

 AllocationOrder,

 HoppingSequenceRequest

 )

Current parameter table entries for SecurityLevel, KeyIdMode, KeySource, KeyIndex:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| SecurityLevel | Integer | As defined in Table 8-75 | As defined in Table 8-75 |
| KeyIdMode | Integer | As defined in Table 8-75 | As defined in Table 8-75 |
| KeySource | Set of octets | As defined in Table 8-75 | As defined in Table 8-75 |
| KeyIndex | Integer | As defined in Table 8-75 | As defined in Table 8-75 |

New parameter table entry for SecurityTxParams

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| SecurityTxParams | Structure | As defined in Section 8.y.z.1 | Provides security related parameters. |

Same change to every MLME primitive which refers to Table 8-75.

# MLME-ASSOCIATE.indication example

Current MLME-ASSOCIATE.indication semantics:

MLME-ASSOCIATE.indication (

 DeviceAddress,

 CapabilityInformation,

 SecurityLevel,

 KeyIdMode,

 KeySource,

 KeyIndex,

 ChannelOffset,

 HoppingSequenceId,

 DsmeAssociation,

 Direction,

 AllocationOrder,

 HoppingSequenceRequest

 )

New semantics:

MLME-ASSOCIATE.indication (

 DeviceAddress,

 CapabilityInformation,

 SecurityRxParams,

 ChannelOffset,

 HoppingSequenceId,

 DsmeAssociation,

 Direction,

 AllocationOrder,

 HoppingSequenceRequest

 )

Current parameter table entries for SecurityLevel, KeyIdMode, KeySource, KeyIndex:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| SecurityLevel | Integer | As defined in Table 8-77 | As defined in Table 8-77 |
| KeyIdMode | Integer | As defined in Table 8-77 | As defined in Table 8-77 |
| KeySource | Set of octets | As defined in Table 8-77 | As defined in Table 8-77 |
| KeyIndex | Integer | As defined in Table 8-77 | As defined in Table 8-77 |

New parameter table entry for SecurityTxParams

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| SecurityRxParams | Structure | As defined in Section 8.y.z.2 | Provides security related parameters. |

Same change to every MLME primitive which refers to Table 8-77.

# Section 8.x.y.1 SecurityTxParams

This structure is included in the MLME call sending data out and it provides security parameters required to send the frame out. Parameters included in this substructure are:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| SecurityLevel | Integer | As defined in Table 9-6 | The security level to be used. |
| KeyIdMode | Integer | As defined in Table 9-7 | The mode used to identify the key to be used. This parameter is ignored if the SecurityLevel parameter is set to 0x00. |
| KeySource | Set of octets | As specified by the KeyIdMode parameter | The originator of the key to be used, as described in 9.4.3.1. This parameter is ignored if the KeyIdMode parameter is ignored or set to 0x00 or 0x01. |
| KeyIndex | Integer | 0x01-0xff | The index of the key to be used, as described in 9.4.3.2. This parameter is ignored if the KeyIdMode parameter is ignored or set to 0x00. |

# Section 8.x.y.2 SecurityRxParams

This structure is included in the MLME call which has received frame and needs to indicate the security parameters from the frame to upper layer. Parameters included in this substructure are:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| SecurityLevel | Integer | As defined in Table 9-6 | The security level purportedly used by the received frame. |
| KeyIdMode | Integer | As defined in Table 9-7 | The mode used to identify the key purportedly used by the originator of the received frame. This parameter is invalid if the SecurityLevel parameter is set to 0x00. |
| KeySource | Set of octets | As specified by the KeyIdMode parameter | The originator of the key purportedly used by the originator of the received frame, as described in 9.4.3.1. This parameter is invalid if the KeyIdMode parameter is invalid or set to 0x00 or 0x01. |
| KeyIndex | Integer | 0x01-0xff | The index of the key purportedly used by the originator of the received frame, as described in 9.4.3.2. This parameter is invalid if the KeyIdMode parameter is invalid or set to 0x00. |