**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | List of changes to the 802.15.9 |
| Date Submitted |  September, 17 2019  |
| Source | [Tero Kivinen][] | Voice: []Fax: []E-mail: [kivinen@iki.fi] |
| Re: | TG9ma work |
| Abstract | Proposed list of changes to be included in the 802.15.9 standard compared to the current 802.15.9 recommended practice. |
| Purpose | Provide base editing instructions for 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. |

# Introduction

The TG9ma is moving the 802.15.9-2016 from Recommended practice to Standard, and at the same time fix some things there. This document contains the list of changes needed for this task.

Page 0 Change "Recommended Practice" to "Standard"

Page 2 In abstract line 3, change "Recommended Practice" to "Standard"

Page 2 In abstract line 4, change "Recommended Practice" to "Standard"

Page 2 In abstract line 6, change "Recommended Practice" to "Standard"

Page 8 In Introduction line 2, change "Recommended Practice" to "Standard"

Page 8 In Introduction add what was changed in this version.

Page 12 In Title, change "Recommended Practice" to "Standard"

Page 12 In section 1 line 1, change "Recommended Practice" to "Standard"

Page 12 In section 1.1 line 1, change "Recommended Practice" to "Standard"

Page 12 In section 1.1 line 3, change "Recommended Practice" to "Standard"

Page 12 In section 1.2 line 1, change "Recommended Practice" to "Standard"

Page 12 Add section 1.3 about deprecated features.

Page 12 Remove hanging paragraph 1. Overview.

Page 14 In section 4 2nd paragraph line 1, change "Recommended Practice" to "Standard"

Page 14 In section 4 3rd paragraph line 1, change "Recommended Practice" to "Standard"

Page 14 Hanging paragraph 4. Introduction.

Page 15 Section 4.1 last paragraph on page 15, change "The keys generated by the KMP " to "The keys generated and the algorithms negotiated by the KMP".

Page 16 In section 4.2 1st paragraph line 2, change "Recommended Practice" to "Standard"

Page 16 In section 4,3 2nd paragraph line 2, change "Recommended Practice" to "Standard"

Page 17 In section 4.7 1st paragraph line 2, change "Recommended Practice" to "Standard"

Page 18 Hanging paragraph 5.2 MPX data primitives.

Page 26 Hanging paragraph 5.3 MPX-PURGE primitives.

Page 28 Hanging paragraph 6. KMP transport service.

Page 29 Hanging paragraph 6.1 KMP-CREATE primitives.

Page 30 In section 6.1.1 add NewAlgorithmIdList after NewKeyIndex on semantics of KMP-CREATE.request

Page 30 In section 6.1.1 add NewAlgorithmIdList after NewKeyIndex in table 8 with type of "list of AlgoritmIds as defined in 802.15.4y", valid range of "as defined 802.15.4y" and description of "List of algorithm Ids allowed for this new key. The KMP will then negotiate the exact algorithm to be used."

Page 33 Section 6.2.1 add CreatedAlgorithmId before CreatedKey in KMP-FINISHED.indication semantics.

Page 33 Hanging paragraph 6.2 KMP-FINISHED primitives.

Page 34 Section 6.2.1 add CreatedAlgorithmId before CreatedKey in Table 12 with type, and valid range of "As defined 802.15.4y" and with Description of "The algorithm id of the negotiated algorithm for this key."

Page 34 In table 12 change Type of CreatedKey from "16 octets" to "variable".

Page 34 Hanging paragraph 6.3 KMP-DELETE primitives.

Page 37 Hanging paragraph 6.4 KMP-PURGE.primitives.

Page 38 Hanging paragraph 7. MPX IE format

Page 39 Hanging paragraph 7.2 MPX IE content.

Page 39 Hanging paragraph 7.2.1 Transaction Control field.

Page 42 In Table 21 mark PANA for deprecation,

Page 42 Hanging paragraph 8. KMP Service.

Page 47 Hanging paragraph A.1.2 Device authentication and cryptographic key agreement.

Page 47 Hanging paragraph A.1.2.1 IEEE 802.1X/MKA.

Page 50 Hanging paragraph A.2 Use cases.

Page 51 Hanging paragraph A.3.2 EAPOL-MKA.

Page 52 Annex A.3.3 add missing text how the material generated is formatted for 802.15.4 use.

Page 53 Annex A.3.3 add different Cipher Suite Selectors for other algorithms in addition to AES-CCM-128 (00-0f-ac-12).

Page 54 Hanging paragraph B.2 Use cases.

Page 55 Annex B.3.4 change "Octect" to "Octet" on last line of page 55.

Page 55 Annex B.3.4 1st paragraph remove last sentence saying "In IEEE Std 802.15.4, currently only the AES-CCM\* cipher is defined, so IKEv2 should use AES CCM with a 16-octet ICV (value 16 of the Transform Type 1 - Encryption Algorithm Transform IDs)."

Page 55 Hanging paragraph B.3 IKEv2 and IEEE 802.15 specifics.

Page 56 Annex B.3.5 last sentence, remove "16" from "first 16 octets".

Page 56 Annex B.3.6 if G-DOI IKEv2 is out soon, I will add text telling how to do broadcast / multicast using that.

Page 57 Hanging paragraph C.2 Use cases.

Page 58 Annex C.3.1 remove 2nd paragraph starting with "As the cipher algorithm ...".

Page 60 Annex D mark this PANA KMP for deprecation.

Page 63 Hanging paragraph E.1 Description.

Page 63 Hanging paragraph E.1.2 Device authentication and cryptographic key establishment.

Page 65 Hanging paragraph E.3 Dragonfly and IEEE 802.15 specifics.

Page 66 Hanging paragraph E.3.3 Message framing.

Page 69 Hanging paragraph F.3 Group keys.

57 annotation(s) found