**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | **IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)** |
| Title | **SECN March, 2019 Plenary Notes** |
| Date Submitted | [March 14, 2019] |
| Source | [Don Sturek][Itron][San Jose, CA] | Voice: 669 770-4790Fax: [ ]E-mail: [don.sturek@itron.com] |
| Re: |  |
| Abstract | [IEEE 802.15 4y SECN Minutes.] |
| Purpose | [Report progress to WG.] |
| 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. |

IEEE 802.15.4y SECN Vancouver Plenary Meeting

Tuesday AM1:

Attendees:

Don Sturek - Chair

See Imat for full attendance

The meeting was called to order at 8:10 a.m. by the chair, Don Sturek (Itron).  Attendees were reminded to log their attendance.  The IPR slides were displayed and described aloud.  The chair request that anyone who had essential patents to disclose to do so.  There was no response from those present.

The TG4y agenda is found in [15-19/0098r01](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.15_dcn_19_15-2D19-2D0098-2D01-2D004y-2Dagenda-2Dmar-2D2019-2Dplenary.pptx&d=DwMFaQ&c=pqcuzKEN_84c78MOSc5_fw&r=1GV4MJ6HR9AwKcKCAJ4QKhw_mH0MdGOWvJPdW-K8IoU&m=kepxQXXDSokPbPTG5F0mfL5E5LPNGF3MqSk3Mw6q8BQ&s=fB4nW_PTRS69v3zuuaEnZAZxP2wFCgZk83L8rr1MBHw&e=).  The agenda was accepted by unanimous consent.

Sturek has created editor’s instructions for the revision of Annex B for coverage of AES-256-CCM.  Tero Kivinen (self) has updated Annex C.  Sturek will reach out to Robert Cragie (ARM), who did the original Annex C, to see if he would be interested in reviewing Kivinen’s updates.  Kivinen noted that his Annex C updates are available in Wireshark format.

The meeting minutes of the St. Louis meeting ([15-19/0032r00](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.15_dcn_19_15-2D19-2D0032-2D00-2D004y-2Djan-2D2019-2Dinterim-2Dminutes.docx&d=DwMFaQ&c=pqcuzKEN_84c78MOSc5_fw&r=1GV4MJ6HR9AwKcKCAJ4QKhw_mH0MdGOWvJPdW-K8IoU&m=kepxQXXDSokPbPTG5F0mfL5E5LPNGF3MqSk3Mw6q8BQ&s=fu6VQj0R_-CwcPpjAOTTqCbl16fbdpPN0mENWCorlQM&e=)) were approved by unanimous consent after Chris Calvert (Landis+Gyr) moved to do so.  Kivinen seconded the motion.

Sturek presented his updates ([15-19/0081r00](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.15_dcn_19_15-2D19-2D0081-2D00-2D004y-2Ddraft-2Dtext-2Dfor-2D4y.docm&d=DwMFaQ&c=pqcuzKEN_84c78MOSc5_fw&r=1GV4MJ6HR9AwKcKCAJ4QKhw_mH0MdGOWvJPdW-K8IoU&m=kepxQXXDSokPbPTG5F0mfL5E5LPNGF3MqSk3Mw6q8BQ&s=mbky6R7FJJ_SUn2a9LqgRVZWuuvQmm-rGIbPUklsOF8&e=)) to Annex B.  It now covers CCM and CCM\*, in key lengths of both 128 bits and 256 bits.  Kivinen would prefer to leave Annex B intact and then replicate it in a new Annex that has pointers to the source NIST FIPS and IETF RFCs in which the algorithms are specified.  Aside from covering both modes and key sizes, Sturek’s changes also require that the length of the M authentication field not be 0 (meaning encrypt without authentication).  Kivinen suggests that Annex B retain sections B.1 and B.2.  Then, for each algorithm and mode, new sections will be created that will point off to the appropriate source document.  The new sections will describe how IEEE 802.15.4 uses each algorithm with appropriate parameter values.  This is similar to the approach used in [RFC 5282](https://urldefense.proofpoint.com/v2/url?u=https-3A__tools.ietf.org_html_rfc5282&d=DwMFaQ&c=pqcuzKEN_84c78MOSc5_fw&r=1GV4MJ6HR9AwKcKCAJ4QKhw_mH0MdGOWvJPdW-K8IoU&m=kepxQXXDSokPbPTG5F0mfL5E5LPNGF3MqSk3Mw6q8BQ&s=VZKrHXpAcKiXIpUu9zx6Es8aJPZ_C4n0Why-oufS288&e=), Section 10.  [RFC 5116](https://urldefense.proofpoint.com/v2/url?u=https-3A__tools.ietf.org_html_rfc5116&d=DwMFaQ&c=pqcuzKEN_84c78MOSc5_fw&r=1GV4MJ6HR9AwKcKCAJ4QKhw_mH0MdGOWvJPdW-K8IoU&m=kepxQXXDSokPbPTG5F0mfL5E5LPNGF3MqSk3Mw6q8BQ&s=vBUNz8bdURIejcw_y6sZDU__pX4We8NW0OoewP-5Ldk&e=) also uses a similar method to describe generic AEAD algorithms.  Sturek will put together a slide to describe this new approach for Annex B and present it to the group on Thursday.

Sturek displayed the initial version ([15-19/0082r00](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.15_dcn_19_15-2D19-2D0082-2D00-2Dwng0-2D802-2D15-2D9a-2Dpar-2Ddraft.docx&d=DwMFaQ&c=pqcuzKEN_84c78MOSc5_fw&r=1GV4MJ6HR9AwKcKCAJ4QKhw_mH0MdGOWvJPdW-K8IoU&m=kepxQXXDSokPbPTG5F0mfL5E5LPNGF3MqSk3Mw6q8BQ&s=0_B3pMlE3zq3oTNEgvzMJHjQDk7Pd1JCKSa0ZHqgq_c&e=)) of a PAR for a revision to IEEE 802.15.9 that is related to the work being done in SECN.  IEEE 802.15.9 needs revision because it was written during the time when AES-128-CCM\* was the only specified encryption algorithm.  Additional key management methods that are suitable for use with IEEE 802.15.4 will be solicited for addition to the specification – the TLS handshake, for example, might be a candidate.  The new PAR will also deal with session key generation methods and how the key index is supposed to work – both areas where the original IEEE 802.15.9 is a bit thin.  Also within scope are broadcast/multicast key creation and security algorithm selection.  Kivinen will discuss the PAR revision with IEEE 802.15 chair Bob Heile (Decawave).  IEEE 802.15.12 (Upper Layer Interface) will be taking the multicasting and fragmentation portions of IEEE 802.15.9, so coordination with that task group is needed to ensure that the new task group’s efforts are aligned with what happens in IEEE 802.15.12.  Kivinen will check in with IEEE 802.15.12 chair Pat Kinney to determine what, if any, changes are needed to the PAR.  Kivinen will be volunteering to chair the newly created task group, although the timeline to spin up the task group doesn’t see that happening until September.  Prior to that, Bob Heile has indicated that the group can meet informally.

Sturek indicated that he will not be able to attend the interim meeting in Atlanta in May.  In his stead, vice-chair Peter Yee will convene the meeting.  The timeline (see slide 3 of the January closing report ([15-19/0031r00](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.15_dcn_19_15-2D19-2D0031-2D00-2D004y-2Djan-2D2019-2Dinterim-2Dclosing.pptx&d=DwMFaQ&c=pqcuzKEN_84c78MOSc5_fw&r=1GV4MJ6HR9AwKcKCAJ4QKhw_mH0MdGOWvJPdW-K8IoU&m=kepxQXXDSokPbPTG5F0mfL5E5LPNGF3MqSk3Mw6q8BQ&s=x07PMPnTyeN3xiWoZ0KJkv9ooiugCpxS2lZHEtmRiAg&e=))) will remain unchanged.

The group will look at the list ([15-18/0324r02](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.15_dcn_18_15-2D18-2D0324-2D02-2D004y-2Djuly-2D2018-2Dmeeting-2Dminutes.doc&d=DwMFaQ&c=pqcuzKEN_84c78MOSc5_fw&r=1GV4MJ6HR9AwKcKCAJ4QKhw_mH0MdGOWvJPdW-K8IoU&m=kepxQXXDSokPbPTG5F0mfL5E5LPNGF3MqSk3Mw6q8BQ&s=L29qkXdpJKYI7iDEwfTYlIMS7Wm6b-m-SBZjb-w20u8&e=)) of changes to the base specification that was generated last July to see what section 9 changes to IEEE 802.15.4 are editorial and therefore the purview of IEEE 802.15.4md, and what parts are technical and belong to IEEE 802.15.4y.  This review might actually end up bringing about changes to the timeline.

The meeting was recessed at 9:22 a.m.  The meeting will reconvene at 8:30 a.m. on Thursday.

Thursday AM1:

Attendees:

Don Sturek - Chair

See Imat for full attendance

The meeting was reconvened at 8:34 a.m. on Thursday.

The agenda ([15-19/0098r03](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.15_dcn_19_15-2D19-2D0098-2D03-2D004y-2Dagenda-2Dmar-2D2019-2Dplenary.pptx&d=DwMFaQ&c=pqcuzKEN_84c78MOSc5_fw&r=1GV4MJ6HR9AwKcKCAJ4QKhw_mH0MdGOWvJPdW-K8IoU&m=sMEZl1uqSFO7fy-2Ly7f_ge8Yu0kZAf3f6PqmY1k-zs&s=8knd8HXw6mqpZbLqbQ6BiXb6KUNRk2te0gLrZp9i-h0&e=)) has been amended to show all of the work that was completed on Tuesday (and in the joint session with TG13 on Wednesday).

Sturek led a discussion of updated text in [15-19/0081r01](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.15_dcn_19_15-2D19-2D0081-2D01-2D004y-2Ddraft-2Dtext-2Dfor-2D4y.docm&d=DwMFaQ&c=pqcuzKEN_84c78MOSc5_fw&r=1GV4MJ6HR9AwKcKCAJ4QKhw_mH0MdGOWvJPdW-K8IoU&m=sMEZl1uqSFO7fy-2Ly7f_ge8Yu0kZAf3f6PqmY1k-zs&s=FDn9YctknhzsqZog3v5d5i-J7K4225OL9a3HFzBPKKk&e=) reflecting the outcomes of Tuesday’s agreements.  He also proposed that rather than rework Annex B in the form of RFC 5282 or RFC 5116, he suggested that Annex B marked as deprecated and a new annex be created that is structured like the RFCs with individual sections for parameter selections and pointers to the base specifications for the algorithms.

The notes ([15-19/0324r02](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.15_dcn_18_15-2D18-2D0324-2D02-2D004y-2Djuly-2D2018-2Dmeeting-2Dminutes.doc&d=DwMFaQ&c=pqcuzKEN_84c78MOSc5_fw&r=1GV4MJ6HR9AwKcKCAJ4QKhw_mH0MdGOWvJPdW-K8IoU&m=sMEZl1uqSFO7fy-2Ly7f_ge8Yu0kZAf3f6PqmY1k-zs&s=mT2NglwLunQwDNoPk4gPLSJL6X8-Elo_Jix_MwZmTG4&e=)) from the San Diego meeting were displayed in order to make sure that all the desired changes have been made or are in progress.  Tero Kivinen asked that we verify that his “rogue comments” are reflected as well.  The “Identify an ANA process to…” change will be deferred until the July meeting when Sturek will next be attending a SECN meeting.  Kivinen and Sturek will work to effect most of the listed changes into the draft specification.  This work should be done by the May meeting.  It might possible to even ballot the draft coming out of that meeting and form a CRG (Comment Resolution Group) to resolve any comments that are submitted during the balloting.  Kivinen notes that the state machine references sections like 9.3.4, but it does not currently handle differences in algorithms.  In these places, a new input for algorithm ID is needed.  New text will then use the algorithm ID as a switch to point to algorithm-specific processing.  Similar changes are needed in section 9.3.5.

The draft closing report is found in [15-19/0139r00](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.15_dcn_19_15-2D19-2D0139-2D00-2D004y-2Dsecn-2Dmar-2D2019-2Dclosing.pptx&d=DwMFaQ&c=pqcuzKEN_84c78MOSc5_fw&r=1GV4MJ6HR9AwKcKCAJ4QKhw_mH0MdGOWvJPdW-K8IoU&m=sMEZl1uqSFO7fy-2Ly7f_ge8Yu0kZAf3f6PqmY1k-zs&s=u2WBT2tsqDfEPyUdWhFLtuvEsMmzvz54HSZRydXnh-w&e=).  One change needed is that Tero Kivinen has been assigned to update the key descriptor and work on the section 9 text for IEEE 802.15.4.  The timeline is now revised to show Annex C changes in May, an initial WG ballot in July, and a recirculation ballot in September.  That would mean a first Sponsor Ballot in January 2020.  For the IEEE 802.15.9 revision, the PAR (15-19/0082r00) and CSD (15-19/0086r00) have been drafted by Sturek.  Kivinen has volunteered to chair the group.

The May agenda will be a review of IEEE 802.15.4 Section 9 text, and Annex B and Annex C changes.  An assembled draft for the SECN amendment will be placed in the private area and an internal WG review will be carried out prior to the July meeting.

The meeting was adjourned at 9:18 a.m.