**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **TG9 KMP Minutes for the January 2015 Interim meeting, Atlanta, GA** |
| Date Submitted | 27th January 2015  |
| Source | [Peter Yee][NSA/IAD] | Voice: [+1-415-215-7733]Fax: []E-mail: [ peter@akayla.com] |
| Re: | TG9 KMP Minutes for January 2015 Interim meeting |
| Abstract | TG9 KMP Minutes for January 2015 Interim meeting |
| Purpose | Official Minutes |
| 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. |

The agenda for IEEE 802.15 TG9 is found in [15-15/0005r1](https://mentor.ieee.org/802.15/dcn/15/15-15-0005-01-0009-tg9-agenda-atlanta-2015.xls).  More detailed information on the TG9 status is contained in the opening report ([15-15/0004r0](https://mentor.ieee.org/802.15/dcn/15/15-15-0004-00-0009-tg9-opening-report-jan-2015.ppt)). The minutes of the San Antonio meeting ([15-14/0708r1](https://mentor.ieee.org/802.15/dcn/14/15-14-0708-01-0009-tg9-meeting-minutes-san-antonio-november-2014.docx)) were approved by acclamation.

Attendees were asked to write their names and affiliations on a pad of paper being circulated through the room because the IEEE network is not functioning reliably.  The chair noted the IEEE 802 patent policy.

The meeting will be dedicated to the resolution of comments from the initial working group ballot on the draft.  The current comment resolution status at the beginning of the meeting is found in [15-14/0718r4](https://mentor.ieee.org/802.15/dcn/14/15-14-0718-04-0009-p802-15-9-comment-entry-form.xls).

Discussion of select CIDs is listed below.

In reference to CID 132, Phil Beecher (Wi-SUN Alliance) requested that SAPs be explicitly noted in Figure 1.  Thus DATA MCPS will be labeled as MCSP-SAP (Data Services), for example.  Tero Kivinen (INSIDE Secure) countered that it would be better to label it “MAC Data Services”.  And the MLME interface would be labeled “MAC Management Service”.  Further discussion combined the two points of view, with the arrow between the MAC Services and the Data Higher Layer labeled as the MCPS SAP.

The related CID 133 was satisfied by indicating that the KMP Transport mechanism itself does not use MLME services.  MLME services would be used by the KMP running in the higher layer in order to emplace negotiated keys and perform other MAC-specific operations.

With the restoration of network access, Gary Stuebing (Cisco) gave a briefing ([15-14/0711r0](https://mentor.ieee.org/802.15/dcn/14/15-14-0711-00-0009-ieee-802-15-9-for-securing-wireless-mesh-networks.doc)) that gives a better presentation of the message flows in 802.15.9, Annex A (and potentially the main body of the document as well), particularly as to how they can be used to support mesh networks as used in smart metering scenarios.  Key management in this proposal remains single-hop, with multi-hop to be supported in commercial product extensions.  In the node-to-node (N2N) case, [ETSI TS102-887-2](http://www.etsi.org/deliver/etsi_ts/102800_102899/10288702/01.01.01_60/ts_10288702v010101p.pdf) is the controlling reference for new session creation messages that are operated over EAPOL-KEY messages.  The scheme proposed in the document will need to be assigned a new protocol number.  The authors of this proposal will supply actual text for either a new annex or an extension to Annex F – further discussion of the best place for the new text is needed to make this determination.  There was substantial discussion on what level of autonomy the KMP has to handle rekeying events.  As currently specified, the KMP has very limited autonomy to do anything that affects the data layer, such as generating new keys due to exhaustion of the cryptoperiod.  The KMP can autonomously send PDUs that affect only the KMP state, such as IKEv2’s rekeying of the keys used to protect IKEv2 message.  It would be helpful for the body of the document to indicate what the annexes can and cannot specify for each KMP along with what the KMP is required to provide in order to be driven within the 802.15.9 framework.

CID 298 was rejected.  That CID asked about the basis for inclusion of KMP annexes.  The simple answer is that protocols were included when participants brought them to the task group.  New protocols may be added to the Recommended Practice, when there is interest and willing parties to do the work to generate the relevant text.

 Don Sturek (Silver Spring Networks) presented Phil Beecher’s (Wi-SUN Alliance) proposal ([15-14/0710r0](https://mentor.ieee.org/802.15/dcn/14/15-14-0710-00-0009-fragmentation-replacement-text.docx)) for alternate fragmentation text.  In table 17 in the draft, the multiplex ID comes out of the same octet used to indicate the fragment counter.  Owing to the limited number of multiplex IDs available, they feel that it would be better to use an expanded information element (named the DTC IE) that adds a two-octet protocol ID, a full one-octet fragment ID, a fragment count, and an optional CTS/RTS (clear-to-send/ready-to-send) signal.  A separate Fragmented Data IE is used to transmit fragments.  Bob Moskowitz asked that the authors attempt to make do with one information element, as there are very few of them available (or more correctly very few IE identifiers available).  The authors are not wedded to the exact wording of their proposal, but they do feel that features such as CTS/RTS and expanded ID spaces are important to incorporate into the draft.  They will take another pass on their proposal and bring it back to the task group.  CIDs 45 and 46 reference this presentation, so their resolution is deferred.

CID 252 will be accepted with minor revisions, as it reasonably explains that although the transport is hop-by-hop, if things are done in multi-hop environments, fragmentation is done a hop-by-hop basis and not end-to-end.

CID 300 is believed to be resolved by improving the use of mandatory “shall” language in the referenced text.  Bob Moskowitz will attempt to provide revisions.

CID 301 is really out of scope for the core of the document, but is an issue for individual KMPs/annexes.

CID 184 is rejected.  The Recommended Practice doesn’t impact data payloads; thus use of short addresses or long addresses is immaterial to the draft.

CID 299 is rejected.  The behavior described in the comment is the expected behavior if the network topology changes.

CID 158 is based off of CID 45, so the resolution for CID 45 will apply to CID 158 as well.

CID 254 questions the typical size of a KMP message and whether the expectation of 127-byte PDUs is realistic.  If a 9 KB payload is desired, then more fragments need to be supported if each PDU carries less than 127 bytes.  Kivinen noted that a typical KMP message was less than a KB, so a reduced PDU size would generally require more fragments.

CID 135 is rejected for the same reason as CID 254.

CID 136 will be accepted with the revision that the text will show 96 bytes as the effective KMP fragment size sent per PDU.  This will have the effect of reducing the maximum KMP message size that can be transmitted unless the number of allowed fragments is increased.

CID 304 questions the apparent absence of IEEE 802.15.7 support.  In fact, the task group has not had any substantive input on IEEE 802.15.7 and it may be necessary to remove reference to it from the draft.  IEEE 802.15.7 would need to change how their Information Elements work in order to leverage IEEE 802.15.9 services.  The task group agreed to remove references to IEEE 802.15.7 because that standard will not be revised to be compatible with IEEE 802.15.9 in any time frame (if at all) that would be helpful to the IEEE 802.15.9 ballots.  IEEE 802.15.7 is being considered by the WG for update work that might be leveraged to make the needed change, but the timeline remains unacceptable for use by IEEE 802.15.9.

CID 305 will be resolved along the lines of CID 136.

CID 43 is resolved the same as CID 45, which adds flexibility to the multiplexing mechanism.

CID 138 mistakes the IEEE 802.15.4 PHY (Physical Layer) PDU fragmentation/reassembly mechanism for the MAC fragmentation/reassembly mechanism that is found in IEEE 802.15.9, so it is rejected.

CID 69 is accepted as the recommended deletion of lines does not cause any harm and may aid clarity.  CID 47 is covered by the resolution to CID 69, but may also be covered if the alternate fragmentation text is accepted in principal.

CID 108 will be assigned to Kivinen for a revised response.

The ballot resolution committee (BRC) plans to hold future teleconferences at 4 p.m. ET on Tuesdays 30 days from now.  Up to that point, the teleconferences will be held on Mondays at 5 p.m. as previously announced.  The BRC comprises Robert Moskowitz, Tero Kivinen, Kunal Shah, Peter Yee, Subir Das, and Brian Weis.

A motion to the WG will be made to empower the BRC to initiate a recirculation ballot upon completion of comment resolution and the resulting document edits.

CID 307 – the commenter may have been looking at an earlier version of the draft, because there are no TBDs in the referenced section.

CID 308 – no length field to be added because this is a conceptual interface, per James Gilb.  (Or was it Ben Rolfe?)

CID 309 – rejected because there is no PHY switching capability; the one PHY used by the MAC for a particular sequence of PDUs is selected by the MLME-Start request.

CID 57/160 – a purge capability is needed because a fragmented sequence of PDUs may take a long time to transmit, but the KMP may decide not to continue the negotiation because of a timeout or other reason that obviates the need to continue the negotiation.  Note that the purge only affects the local device – it has no effect over the air other than the cessation of transmission of queued PDUs.  It should be clarified that a purge should be done at the highest layer (KMP) and cascaded down to the MP and MCPS layers.

CID 279 – rejected because the text used actually originates in the 802.15.4-2015 draft.

CID 280 – rejected as well, because the proper reference to 802.15.4-2015 will subsume 802.15.4e-2012.

CID 262 – text to describe the new TRANSACTION\_OVERFLOW is indeed needed.  Kivinen supplied suggested text as shown in the updated comment resolution spreadsheet.

CID 312 is covered by the resolution CID 160.  In reference to the specifics of the comment, if 13 fragments have been sent, 13 have probably been received.  The purge will simply prevent further transmission of the remaining queued fragments.

CID 113 – text is needed to show that the KMP-FINISHED.indication can be sent to the higher layer after the final MP.confirm is received.  Otherwise the sender might want to wait some period of time after receipt of the KMP-FINISHED.indication before transmitting encrypted data PDUs in order to give the receiver time to complete KMP processing and emplacement of the negotiated key.  The concern with immediate transmission of data after an early receipt of a KMP-FINISHED.indication is that the far side might receive encrypted data that it can’t handle until it has finished the KMP processing.  The MAC wouldn’t know that a key is about to be emplaced by the KMP and would therefore fail the decryption due to the “missing” key.

All remaining comments not otherwise resolved during the meeting were assigned to members of the BRC for resolution. The status of these resolutions and assignments is available in the meeting’s final updated comment resolution spreadsheet ([15-14/718r10](https://mentor.ieee.org/802.15/dcn/14/15-14-0718-10-0009-p802-15-9-consolodated-comments.xls)). These remaining resolutions will be debated during the BRC teleconferences.