**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 November 2014 Plenary meeting, San Antonio, TX** | |
| Date Submitted | 8th December 2014 | |
| Source | [Peter Yee] [NSA/IAD] | Voice: [+1-415-215-7733] Fax: [] E-mail: [ peter@akayla.com] |
| Re: | TG9 KMP Minutes for November 2014 Plenary meeting | |
| Abstract | TG9 KMP Minutes for November 2014 Plenary 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. | |

**Monday November 3rd 2014 PM1 session**

The agenda for IEEE 802.15 TG9 is found in [15-14/0625r0](https://mentor.ieee.org/802.15/dcn/14/15-14-0625-00-0009-tg9-agenda-san-antonio-2014.xls). More detailed information on the TG9 status is contained in the opening report ([15-14/0626r0](https://mentor.ieee.org/802.15/dcn/14/15-14-0626-00-0009-tg9-opening-report-nov-2014.ppt)). The minutes of the Athens meeting ([15-14/0611r0](https://mentor.ieee.org/802.15/dcn/14/15-14-0611-00-0009-tg9-meeting-minutes-athens-september-2014.docx)) were approved by acclamation.

Esko Vesala (INSIDE Secure) has agreed to serve as the (remote) editor for IEEE 802.15.9. A new draft (predraft8) has been uploaded to the members’ area of the IEEE 802.15 website. The images in the document may not be quite right as Vesala did not have sufficient time to completely convert them over to FrameMaker from Visio. All the changes that Tero Kivinen (INSIDE Secure) had planned to make have been incorporated into this draft. There’s a need to rename the “multipurpose layer” to something more like “multiplexing layer” because there is another use of multipurpose in IEEE 802.15.4. Multiplexing is a loaded term as well because it is already used in some IEEE 802.15 PHY layers. Ben Rolfe (Blind Creek Associates) suggests that the term “dispatch layer” might be an unambiguous alternative. Kivinen also explained his current thinking on the KMP-FINISHED primitives. This hits the area of rekeying – does rekey involve a new security association or does the security association (SA) remain the same with changed keying material (and a new key ID)? IKEv1 worked with the SA being deleted and created anew when rekeying was needed. Mick Seaman noted the IEEE 802.1AE does not do rekeying within an SA. He’s uncomfortable with such a concept, preferring an SA deletion/creation strategy using overlap (make-before-break) between the two SAs. Kivinen stated that the overlap period might be relatively long for group keys because it can take a while for sleeping nodes to become aware of the new SA and to switch over to the new key. He also notes that on transmission, the upper layer selects the SA to be used by IEEE 802.15.4 to protect data. The 802.15.4 MAC is not responsible for making the determination of the SA to be used. It would be nice to have a way to signal to the peer KMP entity that a particular key index is no longer needed (having been superseded by a new SA). Confirmation indications should be clearly understood not to indicate that the remote peer has agreed to do anything with the message sent. In some cases, the transmitting node immediately generates the confirmation, while in other cases it is generated after receipt of a MAC-layer acknowledgement, but such an acknowledgement does not indicate successful delivery of a PDU to the remote KMP entity. Bob Moskowitz (Verizon) has updated text to cover the previously agreed restriction that the KMP transport works in single-hop environments only. This text will be sent to the mailing list for agreement, not yet having been incorporated into the pre-draft. Updates will be made this week to incorporate as much new text as possible, with the goal being to have a ballot-ready document by the close of this meeting so that the IEEE 802.15 Working Group can be petitioned to initiate a working group ballot.

The group then went through the new pre-draft on a line-by-line basis to generate a list of changes needed. The document scope will be updated to include the single-hop restriction. The normative references have some (standard) boilerplate that needs to be updated to refer to IEEE 802.15.4-2014 (or 2015 if it takes that long for the new version to be approved) – it currently uses the 2011 version, but KMP Transport is reliant upon 2014 features. In Section 4.1, the overall system diagram will need revision to move the KM protocol block into the KM Information (IE) processing block. Currently, the blocks are separately connected through the DATA higher layer. This reflects that there is an expectation that the KMP configuration will “just be there” when the KMP is called and therefore a separate control block for passing in the configuration is unnecessary. The figure currently shows the KM IE passing keys back to the DATA higher layer in response to a key request. This would seem to be problematic for a FIPS 140-2/3 module, but Kivinen says that conceptually, this could really be handled by having the KMP pass a handle to the key to the DATA higher layer and directly emplace the key in the MIB so that the FIPS boundary is kept to a minimum. In Section 4.2, the concept of bi-directional SAs has been removed. While we are using the terms unicast and group SAs, we might want to mirror IEEE 802.15.4 usage and call them link and group SAs instead. Section 4.5 now shows that only 64-bit addresses are used for SAs. This aligns well with IEEE 802.15.4 usage and saves confusion that may arise when using the shorter addressing format. The Section 4.6 KMP payload size calculations now indicates that 9 KB is the typical maximum, but it should be noted that this is a PHY-dependent value. Section 5 discusses the multiplexing data service. As previously noted, this might be better described a dispatch service, but no decision on the name has been made. There has been some discussion within 802.15.4 for taking the multiplexing/dispatch service and directly incorporating it into IEEE 802.15.4, but there are no immediate plans to do so. In Section 5.2.1, the MPDataLength has been removed. James Gilb (Tensorcom) considers the interface to be a conceptual interface, not an API. Thus, the length isn’t really needed to get the concept across. Section 5.3 (MP-PURGE) is present because it mirrors IEEE 802.15.4 usage, but it’s not apparent how well it fits in with KMPs that may not have an abort processing capability. A new Section 6 covers the KMP transport service (as distinct from the dispatch service) to allow them to be wholly separable, should the need arise. An indication from the MAC layer to a higher layer indicating approaching frame counter exhaustion might be useful, although the higher layer might well pull that status rather than waiting for a push from the MAC layer. Kivinen will check figure 6.1.1 to see if the MP-DATA.confirm action is in the right place in the diagram. Section 6.1.1’s definition of KMP-CREATE.request needs to have selectors for the key index to be used and the key type/length to be generated by the KMP. The section 6.2 FINISHED primitives follow from Kivinen’s presentation from the March meeting. Another primitive that is needed (to be added to section 6.3) is a DELETE primitive. This allows for a clean signal to a peer that an SA should be torn down/cleaned up. It’s really a courtesy, not an operational requirement. Section 7.7 (KMP fragmentation) might be pushed to a new major section (8?) to separate it from the rest of the Section 7, which parallels the separation of the dispatch/multiplexing service from the actual KMP transport. In the state machine, Section 8.1, Figure 6 (inbound state machine) needs to be updated so that the “append to KMP list” action also includes a check to see that each fragment and PDU received uses a common security mode and key. The outbound state machine in Section 8.2 needs additional editing work – it’s not nearly as filled out as the inbound state machine. Section 9 (KMP Transport PIBs) is also in need of work to align with the current 802.15.4 draft. The MAC Specifics in Section 10 need to have more material added dependent on whether IEEE 802.15.4 or IEEE 802.15.7 is being used. Kivinen and Moskowitz have ideas for this area. The Appendices (which are specific to individual KMPs) need review and update, but have been neglected to date owing to concentration on the main body of the Recommended Practice. Currently, the appendices have widely varying levels of detail between them and none have been updated in light of changes within the main body of the document.

**Tuesday November 4th 2014 PM2 session**

For the Tuesday PM2 session, a new draft document (predraft8.1) was just posted. Moskowitz commented that his plan is to request approval to do a provisional ballot at the closing IEEE 802.15 plenary. The provisional status is because the task group will not have the final version of the draft ready at end of this meeting. This ballot will be a full working group ballot with a 30-day ballot period. The scope of comments is completely open and covers the entire document. The plan will be to form the ballot resolution committee during this meeting (a task group motion is needed to so) and set dates and times for conference calls. Moskowitz remarked on the need to avoid the holidays for calls in order to improve participation rates.

This session will look at the revised document, predraft 8.1. Aside from discussing them during the session, changes or new text should be posted to the email list for the editor to include in the next update. It was noted that the document covers only single hop – that could be coordinator-to-coordinator or coordinator-to-device or whatever. There is no concept of a relay in IEEE 802.15.4. Don Sturek asked to clarify that the document won’t preclude a multihop solution but just not prescribe how it would be done. If so, then text regarding out-of-sequence packets discussed yesterday may need to be removed from the document. Seaman commented that “not preclude” could raise some confusion/issues. Kivinen stated that the multiplexing level only works for single hop. There are no restrictions at the KMP level. Moskowitz took the action item to generate some text clarifying this state of affairs so it can be reviewed by the group. It was noted that the wrong predraft8.1 was uploaded to the IEEE 802.15 on-site meeting server. Moskowitz distributed the updated version manually. He then stepped through the revised draft to review the recent changes. In Section 4.7, (KMP Payload size), the 127 byte limit is for the PSDU (physical layer service data unit) only, it is not a hard limit for IEEE 802.15.4g. That can support up to 2047 bytes. Seaman thinks what is really meant is that even using 127-bit PSDUs, the maximum KMP payload is 9KB. Moskowitz will revise the text to turn around the emphasis of that text. In Section 5 (Multiplexed data service), the MP IE format uses up a very small value (1 byte identifier), which is a scarce resource. In terms of fragmentation control, the questions was for transmission, what would happen when a few fragments are sent and then purge is initiated. Does that stop all the rest of the fragments from being sent? That appears to be the case and the purge action removes the request from the transaction queue. Purge is currently missing from the state machine. The status of the appendices was reviewed next. Brian Weis (Cisco) commented that the IEEE 802.1X Appendix A specifies EAP and MKA but there is also a wireless IEEE 802.11 option. EAP authentication is the same but then the two methods (MKA, .11) differ, so he will need to add another (different) appendix to ensure coverage of both cases. PANA is included but it was suggested to remove the use of UDP. It was felt that PANA-UDP is indistinguishable from the IEEE 802.1X method. However, the PANA relay function is distinct from IEEE 802.1X. Kivinen commented that may be missing TLS or DTLS details. In any case, the state machine needs to be checked. Some things are obviously missing from it.

For the KMP create and KMP delete primitives there was a question of whether these necessitated a need to switch keys? Since there is a KMP running above the KMP transport, that entity is responsible for handling key switching. A key index is used and supported by IEEE 802.15) for SAs. The higher layer (where the KMP resides) owns the key indexes, so key switching is likewise an upper layer problem. There is, of course, a need to map between a key and a security association number to relate to the key index. This documents deals with the transport problem, not the actual key management.

Purge text still needs to be added to section 9.2. In the event of purge or timeout, it flushes all state / payload. Sections 11.1.2 and 11.1.3 can be removed.

While the plan for IEEE 802.15.9 was to provide support for both IEEE 802.15.4 and IEEE 802.15.7 MACs, to date only IEEE 802.15.4 has gotten real attention. This is partially owing to lack of participation by IEEE 802.15.7 experts as well as an issue of which under which conditions an IEEE 802.15.7 will convey IE. It is hoped that this document will provide impetus to IEEE 802.15.7 to fix the Information Element (IE) handling in such a way as to make IEEE 802.15.9 relevant to that MAC.

The plan for Wednesday session is to go through any additional changes and prepare the request for provisional balloting. The document has to be set on Thursday. The main reason to go to ballot (somewhat prematurely) is to get visibility in IEEE 802.15 and hopefully get comments from others in the full working group.

**Wednesday November 5th 2014 PM1 session**

A motion was presented to allow for a WG ballot of the next draft of the IEEE 802.15.9 draft once the edits agreed upon at this meeting are incorporated. Input from the IEEE 802.1 Security team on the IEEE 802.1X appendix is required to complete the edits. Karen Randall (Randall Consulting) indicated that the edits are minor, but input from IEEE 802.1 will likely not be complete by the close of the meeting. Brian Weis will take the action to update the IEEE 802.1 appendix. Passing a ballot-authorizing motion will require that the motion be predicated upon receipt of that input, so Moskowitz asked that IEEE 802.1 obtain a document number that can be referenced in the motion without the input actually having been written. A second motion was displayed that will empower a ballot resolution committee (BRC) that will handle the comments generated by the ballot requested in the previous motion. Members of the BRC include Robert Moskowitz, Tero Kivinen, Don Sturek (Grid2Home), Peter Yee (AKAYLA), Subir Das (Applied Communication Sciences, formerly known as Telcordia), and Brian Weis. The BRC will work via email and teleconferences to be held with at least 30 days’ notice. The BRC will be empowered until the next meeting at which time it will need to be renewed if its work is not completed. For planning purposes, teleconferences are planned to occur weekly on Mondays, starting December 8th at 5 p.m. EST for 1 hour each. Unneeded teleconferences will be cancelled ahead of time and it’s likely that the first meeting will be cancelled as it occurs almost immediately after the earliest potential close for the working group ballot. Both motions are working group motions, but require that the task group approve them. Moskowitz moved to approve submitting the ballot motion to the working group. Das seconded the motion. It was approved by acclamation. Moskowitz then moved to approve the request to the working group for formation of the BRC. Yee seconded the motion. This motion was also passed by acclamation. Karen Randall and Don Sturek both expressed the opinion that the document is not truly ready for ballot. Moskowitz responded that there was political pressure for the ballot to happen that was complicating the situation.

Five meeting slots will be requested for the January meeting in order to continue comment resolution.

Tero Kivinen then went through the newly generated predraft9, explaining the changes between that version and the previous one. In Section 4.6, the language was tightened up to clarify that 64-bit extended addresses are employed and authentication is based on these addresses. Section 4.7 still needs to be updated to indicate that 9 KB KMP PDUs can be accommodated, even with relatively small fragments. In Section 5.1 there seems to be dissension on whether KMP data should be transported via Data or Multipurpose frames. Flowing over Data frames can be a problem if the Coordinator has a minimum security level that requires all Data frames to be encrypted. Obviously, that would not be feasible for a KMP, since the KMP needs to run in the clear in order to establish keys that will then be used for Data frame encryption. Figure 2 in Section 5.2 has been corrected to show the proper sequencing of the ACK to the sender. Section 6.1.1 needs to have the key information added to the KMP-CREATE.request – Kivinen has not yet had an opportunity to specify the change. Section 6.3 now covers the KMP-DELETE request used to indicate that a security association is no longer needed. Some reordering of Table 6 is needed as it falls in the middle of Section 6.3 but it is related to Section 6.2. The inbound state machine diagram in Section 9.1 has been improved to match the text. Minor changes were made to the outbound state machine diagram in Section 9.2. Section 11 exists in skeletal form and mostly reserves minimum MAC-specific values with only a little bit of added color. The appendices could still use some cleanup. Moskowitz will look at Appendix B (Host Identification Protocol). All other edits (except for Brian Weis’ IEEE 802.1 input) need to be sent to the mailing list by 8 a.m. on Thursday morning in order to be incorporated into the draft that will be balloted. This will give the editor time to incorporate that input so that there will be a (mostly) completed document to be posted in time for the closing IEEE 802.15 plenary on Thursday evening.