**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **TG9 KMP Minutes for September 2012 Interim meeting, Palm Springs CA USA** |
| Date Submitted | 30 October 2012  |
| Source | [][NXP Semiconductors] | Voice: [+44-114-281-2655]Fax: [+44-114-281-2951]E-mail: [ paul.chilton@nxp.com] |
| Re: | TG9 KMP Minutes for September 2012 Plenary meeting |
| Abstract | TG9 KMP Minutes for September 2012 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. |

**Attendance:**

Attendance Log used.

**Discussion**

Thanks to Peter Yee for the notes used to prepare these minutes

The TG9 agenda is found in [15-12-0488-00](https://mentor.ieee.org/802.15/dcn/12/15-12-0488-00-0009-tg9-agenda-palmsprings-2012.xls).

The opening report (document 15-12-0520-00) was displayed, containing slides on IEEE patent policy as regards the duty of participants to inform if they know of any essential patents; the Chair called for anyone with knowledge of essential patents to advise the group.

Minutes from the San Diego meeting in July are found in [15-12-0456-01](https://mentor.ieee.org/802.15/dcn/12/15-12-0456-01-0009-tg9-meeting-minutes-san-diego-july-2012.docx), and were approved by acclamation.

Bob Moskowitz (Verizon) briefed the group on document [15-12/0458r0](https://mentor.ieee.org/802.15/dcn/12/15-12-0458-00-0009-moving-kmp-forward.ppt), updated to [15-12/0458r2](https://mentor.ieee.org/802.15/dcn/12/15-12-0458-02-0009-moving-kmp-forward.ppt)) on what has been agreed in the task group to date and what it will take to make progress.  At this point, he has concluded that Command frames must be used for both 802.15.4 and 802.15.7 key management.

New areas of work since the last meeting include the state machines for KMP Command frame processing and the KMP Transport Mechanism.  The state machine for KMP Command frame processing deals with fragmentation support and in particular the retransmission of unacknowledged fragments.  The KMP Transport Mechanism state machine deals with triggers to start KMP processing and to cause the KMP to rekey when a certain number of frames have been encrypted.  The former trigger is used to start the key management protocol, presumably through a notification to the KMP implementation in a higher layer.  The latter trigger is used to prevent too much traffic being passed over any one key.  Moskowitz has noticed that the 2011 version of 802.15.4 has had the text describing the major security association tables (key table and device table) removed.  It was in previous versions, although the tables themselves remain in the document.  This last trigger could conceivably be rendered moot if we consider the KMP responsible for population of the security association tables.  To do so would greatly simplify the work that 802.15.9 is responsible for.  Moskowitz will adjust his slides to reflect that the KMP is responsible for population of the security association tables and such behavior is outside of the realm of the KMP transport.

Next steps will be the development of state machine drawings, adding text to the draft document tocover both the general KMP data format and state machines, and generating specific appendices for individual KMPs.

Bob Moskowitz noted that René Struik’s presentation on PUFs (physically unclonable functions) makes a lot of sense for protecting keys in 802.15.4 coordinator devices.  While not relevant to the bits-on-the-wire protocol, the technology should be of interest to implementers.

Yoshihiro Ohba (Toshiba) discussed an update ([15-12-0109-01](https://mentor.ieee.org/802.15/dcn/12/15-12-0109-01-0009-pana-over-802-15-9-presentation.docx)) to his PANA appendix to 802.15.9.  The update aligns the appendix with the current version of the main body text.  There are no actual technical changes as the methodology used to adapt PANA to 802.15.9 KMP transport remains the same.  Moskowitz will work with Ohba in mid-October to roll the PANA appendix text into the main document.  Dr. Ohba will supply the diagrams from the document in an importable format.

The task group will hold a conference call on October 30, 2012 at 10 a.m. EDT.

The meeting was adjourned by acclamation on September 20th at 12:17.