IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)		
Title	**TG9 KMP Minutes for November 2013 Plenary meeting, Dallas, TX USA**		
Date Submitted	2nd December 2013		
Source	[Paul Chilton] [NXP Semiconductors]	Voice: Fax: E-mail:	[+44-114-281-2655] [+44-114-281-2951] [paul.chilton@nxp.com]
Re:	TG9 KMP Minutes for November 2013 Plenary meeting		
Abstract	TG9 KMP Minutes for November 2013 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.

The meeting minutes were compiled from notes taken by Paul Chilton (NXP Semiconductors) and Peter Yee (Akayla).

Monday November 11th 2013 PM2 session

The meeting was opened by the Task Group Chair, Bob Moskowitz (Verizon) at 16:10 who gave a brief introduction to the aims of the Task Group for members of 802.1X attending the session. He also reminded all to complete their attendance. Slide describing the IEEE Patent Policy were displayed and a call was made by Bob for notification of any essential patents. There were no responses.

The Opening Report document 15-13-0663-00-0009 was displayed.
The minutes of the previous meeting were approved by acclamation.

The current version of the Recommended Practice is doc 15-13-0154-03-0009. In order to finish the document there are a number of things required, among them text on 802.1X for an appendix. Bob has to add more text on HIP and it is intended to make all KMP appendices follow a similar structure, which will require revisions to the existing text and possibly additional material.

Bob reported that the 802.15 Working Group Chair, Bob Heile (ZigBee Alliance) has asked the group to get the document finished with the target of starting a ballot at the January meeting. In order to meet this deadline, interim calls will be held in mid December and early January. Bob will arrange these using the Webex that is now available to the IEEE.

Bob asked if it would be possible to get a contribution for the 802.1X appendix in December. In the discussion that followed a number of questions were raised and points clarified.

It was stated that the goal of the Task Group is to describe how a KMP packet is transported and also the methods to initiate and control the transfer, and also how the KMP will be used but not how to use the 15.4 security mechanisms – it is sufficient enough to give a high level description, not the implementation. The biggest KMP frame that can be carried is 8 kbytes using the smallest packet sizes available in 802.15.4, described in section5 of the Recommended Practice.

Brian Weiss (Cisco) asked which use cases are under consideration. Bob replied that there are a number which range in size of implementation; the aim is to try to provide guidance on what would be a good fit a for a particular use case in terms of characteristics for each KMP. An example given was that 802.1X might be a good candidate for security between a home network using WiFi and a 802.15.4 network, since 802.1X is used in other parts of the infrastructure.

Mick Seaman (Self) asked how the transport mechanism is to be provided, and what the interface to use its services would look like. Bob explained that the mechanism provides a segmentation

and reassembly service into which the various packets of the KMP in use are fed. The interface will use a number of MLME calls which had not been defined so far. Bob stated that he would prepare a first draft of the MLME calls for discussion at a session later in the week and for subsequent inclusion in the document. The parameter will include the Destination Address, and some discussion ensued regarding the different types of address defined in the 802.15.4 specification, how they may be generated, which is the most appropriate to use and whether the cases where addresses are implied rather than explicitly stated in a 802.15.4 packet would be required to be supported.

It was also explained that the KMP transport effectively takes a type describing the KMP being carried and a payload which is opaque to the transport mechanism. The payload is introduced to the transport process at the sending device by the KMP and is delivered unchanged to the destination device. How the contents of the payload are interpreted at the destination is up to the actual KMP being carried. The result of the KMP process will be to set up the security parameters as needed by the destination.

Mick asked that a very precise description is provided in the Recommended Practice on things such things as the MLME calls which an implementor would need to use to initiate a KMP payload transfer and any other control operations.

A question was asked on why there are so many KMPs specified; it was explained that some are a better fit than others in particular situations or applications, for example energy harvesting vs line powered, sizing of memory or the opportunity to reuse crypto modules in several places when one in particular is required for a specific part of the stack or application as happens in ZigBee IP where PANA is present. Interoperability between KMPs is not required.

Bob explained how the fragmentation mechanism works and answered a number of questions asked by Mick regarding the state machines and timers involved. Mick was concerned that there should be no situations which could result in livelocks or deadlocks in the system and suggested that care is taken to analyse and avoid such problems.

Mick asked that the document be very clear on what is being added to the existing 15.4 protocol and which parts exist already in order to show which parts have already been scrutinized and which are new and require careful examination.

Brian asked when an update to the Recommended Practice be published. Bob stated he would work on changes to the document that evening and pass to Paul Chilton to include them in the document. Following on from this point, Bob showed document 15-13- 677-00-0009 on the proposed changes to the Recommended Practice.

The proposed changes were accepted and there was further discussion around other parts of the Recommended Practice document between those present.

It was suggested that text should be added in section 5.1 to make it explicit that there would be no attempt made by the transport mechanism to recover lost fragments. Tero Kivinen (INSIDE Secure) made the observation that even if a fragment loss is detected there is no mechanism to signal the transmitting device to stop sending the remaining fragments. All fragments of the KMP payload must be sent, but they will be discarded at the receiver.

Mick made the observation that there must be recovery paths from every state in the state machines which implements the KMP transport, even if the entry to the state was illegal.

Tero suggested that a specific check for the correct fragment number be made in the input state machine in order to make sure that it only accepts in-sequence fragment numbers.

Tero asked why in section 2 Normative References the PANA RFCs are listed. It was agreed that these references should be moved to the relevant annex of the document.

Tero commented that in Section 7 the text mentions a trigger value for initiating a rekey operation; currently this is set to 100, which he thought was too low and that 0xffff would be a more appropriate value to give more margin to initiate the rekey operation before the frame counter is in danger of wrapping. It was noted that the frame counter is incremented whenever a packet is sent, whether a data or command frame.

Bob indicated that he would work on text for the document that evening for the group to consider changes in the AM1 on Tuesday. He also asked all present to look over the document in order to present comments in following sessions.

The Task Group went into recess at 17:40

Tuesday 12th AM1

Bob Moskowitz (Verizon) has updated some of the terminology so that instead of using the term "Forced ACKs", the document will use the term "MAC Acknowledgement Frame". This change helps to specify at which layer (application vs. data link) the acknowledgement occurs.

Changes in the inbound and outbound state machines to match the implication of this terminology change were also proposed. Tero Kivinen (INSIDE Secure) will work on drawing the state machines. Additional text concerning the mechanism of rekeying and when it occurs was also added. An outstanding question remains about what to do if rekeying fails. Does that leave the system in a continuous loop, attempting to rekey?

Tero noted that a minimal (but complaint) IKEv2 implementation would not support rekeying. Thus, the semantics of rekeying in that case would actually be the same as doing a full key establishment. The system view diagram was updated to show where the KMP Service is

located and how the keys flow from there to the Information Element Shim. Finally, MLME (MAC Layer Management Entity) KMP-Data primitives were described, indicating the parameters passed through the send and receive interfaces. The initial values Moskowitz suggested were the KMP ID Value and KMP Payload. Additional values that should be passed are the (long form) source and destination addresses (to ensure all of the PDUs in a KMP exchange are part of a matching set), and the KMP payload length. We're not certain whether there is a need for confirm calls to indicate whether a PDU was transmitted or if its transmission timed out.

Tuesday 12th AM2

Bob Moskowitz (Verizon) opened the session; the aim of the session was to write and agree the closing report and to work further on additions and changes to the Recommended Practice document text.

Bob and Tero Kivinen (INSIDE Secure) worked on the document text.

The meeting was recessed and then adjourned