**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **TG9 KMP Minutes for May 2012 Interim meeting, Atlanta** | |
| Date Submitted | 21 May 2012 | |
| Source | [] [] | Voice: [+44-114-281-2655] Fax: [+44-114-281-2951] E-mail: [ paul.chilton@nxp.com] |
| Re: | TG9 KMP Minutes for May 2012 Interim meeting | |
| Abstract | TG9 KMP Minutes for May 2012 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. | |

**Attendance:**

Attendance Log used.

**Discussion**

*Monday 14th May, AM2 session*

The meeting was called to order at 10:30 a.m. by the Chair, Bob Moskowitz (Verizon).

The IEEE Patent Policy was presented and reviewed and a call for essential patents made. No patents issues were raised from the floor. The attendance was taken.

Minutes from March meeting. Tero Kivinen (AuthenTec) made a motion to approve the minutes, with Yoshihiro Ohba (Toshiba) seconding. The minutes were approved unanimously.

Document review. The documents to be reviewed over the course of the meeting were listed: An Overview of the KMP transport (15-12/0024r8), a review of the Draft Document (15-12/0116r2), and KMP presentations (currently only HIP).

Bob Moskowitz presented the Overview of the KMP Transport document. He re-iterated the goals of the TG, which is to produce a Recommended Practice for KMP Transport. This will be done by using Information Elements (IEs) for traffic selector and providing fragmentation of large KMP PDUs over smaller 802.15 MPDUs. There will be a simple state machine for sending and receiving KMP IE payloads and managing fragmentation. The state machine triggers need to be fleshed out, for example, what starts the KMP and when? What happens when an unsecured frame is received or if a secured frame is received using an unknown key?

802.15.7 will transport the KMP IE in the COMMAND frame. However, it seems

that an IE cannot be sent without an actual command in the frame. Moskowitz is going to file a maintenance issue to allow for the use of command-less COMMAND frames. Since 15.7 is looking into a PAR for new work on LED-based communications, this will serve as an opportunity to modify the base standard to support IE-only command frames.

TG9 needs to specify how many retries are performed when a fragment has not been acknowledged. The number of retries may need to be specified as a function of the MAC/PHY over which the fragments are being sent.

The group reviewed the state of the draft specification document (15-12/0116r3) which is currently rudimentary. An editor is still needed and is solicited. A candidate has made himself known, but he requires funding to participate. The Chair asked for anyone who can supply funding to contact him.

The meeting went into recess at 11:54 a.m.

*Wednesday May 15th AM1 session*

The meeting was called to order at 8:03 a.m.

Review of HIP KMP document. Bob Moskowitz discussed the HIP KMP over TG9 document (15-12/0231r1). HIP (Host Identity Protocol) is a key management scheme between peers and contains both Base Exchange (BEX) and Diet Exchange (DEX) variants. The basic protocol is defined in Experimental RFC 5021. Identities in HIP are the public key (of a device). BEX supports a variety of algorithms, while DEX is limited to static ECDH. A hash of the public key is used as a short form identity which is more convenient for managing security associations. It was suggested that HIP is particularly well suited for constrained sensors where code size and computation are limited. Such devices (e.g., light switches) are well within the realm of what 802.15.4/802.15.7 cover. HIP supports keying for multiple protocols at multiple layers in the network stack. To make it conform to 802.15 needs, BEX would need to be tailored such that it can generate more than one key as it currently only generates a single key. Both BEX and DEX would have their ESP (Encapsulating Security Protocol) transformations dropped as those are irrelevant in an 802.15 environment. In those environments, either Access Control Lists (ACLs) or a RADIUS back end can be used for authentication, depending on the PAN topology. ACLs are reasonable in a star PAN (Personal Area Network) arrangement, while RADIUS is more general. X.509 certificates could be used with HIP-BEX if desired. Bob expects to have HIP-specifying text ready for incorporation into the draft specification within two weeks of this meeting.

Bob Moskowitz has updated his KMP transport proposal (15-12/0024r9). It now has additional information on what triggers would make sense for the state machine. Since he doesn’t believe that the state machine will be looking at MAC MIB values, it will need to have its own trigger values and mechanisms for things like frame counts reaching certain levels that would require rekeying.

René Struik (Struik Security Consultancy) showed portions of 802.15.4-2011 to assist in determining what should be done when an unsecured packet is received by a station that is

expecting a secured packet. This falls within the larger discussion of packet processing and how things are supposed to flow with the insertion of a KMP into the picture.

Bob Moskowitz has also updated the draft specification document (15-12/0116r3). The document remains rudimentary and does not incorporate the HIP-specific text. Karen Randall (Randall Consulting) pointed out that Bob should incorporate definitions for things like key management protocol and security association from existing 802 sources such as 802.1X instead of using Wikipedia definitions that he had currently copied. Based on his present thinking, Bob believes that the transport will support carriage of KMP PDUs of up to 9 KB.

The meeting went into recess at 10:00 a.m.

## Thursday 17th May AM1 session

The meeting was called to order at 8:19 a.m.

 Tero Kivinen (AuthenTec) spoke on IKEv2 over TG9 ([15-12/0257r1](https://mentor.ieee.org/802.15/dcn/12/15-12-0257-01-0009-ikev2-over-tg9.ppt)).  This presentation is similar in nature to Bob Moskowitz’s HIP presentation.  IKEv2 is specified in IETF RFC 5996 for use with IPsec.  It is a peer-wise key management protocol using a 4-packet session key establishment scheme.  Tero presented the protocol flow.  The traffic selector payloads in those flows will need to be specified for 802.15.9.  Additionally, for use in 802.15.9, the TG will need to specify group key distribution as well as which features are not needed, e.g., NAT traversal and cookie exchange.  He suggested that suitable use cases for IKEv2 would be in devices that already support the required strong cryptographic primitives and probably have them implemented in hardware.  Such devices could share the IKEv2 for all suitable network layers.

The meeting went into recess at 8:50 a.m.

## Thursday 17th May AM2 session

The meeting was called to order at 10:38 a.m.

Bob Moskowitz will work on text to show how management messages for events such as counter exhaustion or decryption failure work between the MLME (MAC Layer Management Entity) and upper layer management. These messages would essentially bypass the KMP transport that this TG is working on. He expects to post his thoughts to the mailing list within about two weeks.

Bob then showed the draft closing report (15-12/0290r0) for comment and modification. Major efforts during this meeting centered on dealing with trigger events, refocusing on using command frames instead of data frames, and hearing presentations on HIP and IKEv2 as KMPs that will be transported by the 802.15.9 mechanism.

In terms of planning for the July plenary meeting, an ad hoc teleconference is posited for June 27, 9 a.m. EDT. Moskowitz will send out a meeting request with LiveMeeting or WebEx details. A test call a couple of weeks prior to the actual teleconference will be attempted in order to make sure that the online portion of the meeting works correctly.

During the plenary meeting in July, TG9 expects to have a joint session with the 802.1 security group as well as participating in the LED IG (Light Emitting Diode Interest Group) session. An update to the whole 802.15 working group is also planned, either during a plenary or WNG slot.

The revised timeline for TG9 expects TG balloting to start in November 2012. Working group balloting would start in March 2013, followed by Sponsor balloting in July 2013. That draft would go to RevCom in November 2013 assuming smooth sailing through the balloting process.

The meeting was adjourned at 10:58 a.m.