**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 2013 Interim meeting, Waikoloa HI, USA** | |
| Date Submitted | 2nd July 2013 | |
| Source | [] [NXP Semiconductors] | Voice: [+44-114-281-2655] Fax: [+44-114-281-2951] E-mail: [ paul.chilton@nxp.com] |
| Re: | TG9 KMP Minutes for May 2013 Interim meeting | |
| Abstract | TG9 KMP Minutes for May 2013 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.

The meeting minutes were compiled from notes provided by Peter Yee (Akayla)

The TG9 agenda is found in [15-13/256r1](https://mentor.ieee.org/802.15/dcn/13/15-13-0256-01-0009-tg9-agenda-waikoloa-2013.xls).  The opening report is found in [15-13/266r0](https://mentor.ieee.org/802.15/dcn/13/15-13-0266-00-0009-tg9-opening-report-may-2013.ppt).  Minutes from the Orlando meeting in March are found in [15-13/254r0](https://mentor.ieee.org/802.15/dcn/13/15-13-0254-00-0009-tg9-meeting-minutes-orlando-march-2013.docx) and were approved by acclamation.

The chair made a call for essential patents according to the IEEE patent policy.  None were noted.  The agenda was approved without modification.

Bob Moskowitz (Verizon) gave a technical overview ([15-13/265r0](https://mentor.ieee.org/802.15/dcn/13/15-13-0265-00-0009-tg9-techincal-review.ppt)) of the key management protocol (KMP) transport draft.  The material is fairly similar to that previously presented, with an improved description of the problem space.  Within 802.15.4, key management is left up to the individual implementations to define.  802.15.9 will provide a more uniform means for carriage of KMP PDUs.  Problems that are being addressed are highly constrained systems (power, CPU, memory) and control of critical infrastructure via the 802.15 MACs.  The 802.15.9 solution does not require a higher layer protocol to carry the KMP.  It supports multiple KMPs and hides any issues that might occur because some KMPs do not fit within the PDU limitations of 802.15 MACs.  Which KMPs are utilized is not negotiated – it is believed that most controllers will support one KMP and will only operate within that context.  The general method for 802.15.9 is to define a new Information Element (IE) that describes its payload (KMP or other data) and handles carrying of split KMP PDUs.  KMP PDUs are split if they exceed the 2047-octet IE limit for 802.15.4 or the 255-octet IE limit for 802.15.7.

James Gilb (Tensorcom) asked why there was a requirement to use long MAC addresses.  Moskowitz replied that short addresses wouldn’t have been assigned prior to association, which is one of the times when the KMP might be operating.  Tero Kivinen (INSIDE Secure) said that since 802.15 MACs don’t allow selective encryption, there would have to be plaintext exchanges (for the KMP) before the short addresses could have been assigned.  Gilb rightly points out that use of long vs. short addresses does not affect the KMP, to which Kivinen agreed.  Gilb believes that frames can be sent prior to association and that might be a means to run the KMP prior to the association. Association is when short addresses are assigned.  Gilb remains unconvinced of the need for pre-association key management.  The failure cases for unauthenticated associations do not appear to be particularly problematic.

The state machine diagrams are split between the simpler outbound and more complex inbound processing.  Gilb noted that forced ACKs were no guarantee that the receiving node had actually processed the received KMP PDU.  It could drop the PDU after sending the ACK if, for example, the receiver’s buffer became full.  ACKs occur before the inbound processing occurs on a PDU, so an ACK is only indicative of receipt of a PDU, not of successful processing of that PDU.

The MACFrameCounter threshold for rekeying may need to be rethought to a larger number.  The current threshold is set to 100 frames prior to the MAC frame counter rollover.  Gilb suggests having an MLME (MAC Layer Management Entity) SAP (Service Access Point) added that allows a PIB (PAN Information Base) entry to be set so that the threshold is configurable, in order to avoid burying a hard constant within the document for this value.

The currently targeted KMP list contains 802.1X, HIP, IKEv2, and PANA.  SAE remains of interest.  Each KMP described within the 802.15.9 Recommended Practice will be given a justification for its use, examples, deployment advice, and a description of its key lifecycle management.  Specific text will describe items such as what backend processing the KMP requires to operate, profiling of the KMP parameters, and how a security association is identified.  There will also need to be text supplied indicating how the 802.15 use of a particular KMP differs from its definition in its native environment.  For example, changes to KMP encapsulation or the management of group keys are typically different between the native environment and 802.15.  Gilb states that the KMP-specific text might be best covered as informative annexes, understanding that the whole document is informative since it is a recommended practice, not a standard.

The current target is to have the document assembled with the initial set of KMPs and primary body text ready for the July plenary meeting.

Rene Struik (Struik Security Consultancy) presented his “Any over 802.15.9” presentation ([15-13/259r0](https://mentor.ieee.org/802.15/dcn/13/15-13-0259-00-0009-any-over-802-15-9.docx)).  He noted that 802.15.9 is suitable for transporting other protocols than KMPs (and has explicit provisions for doing so).  Struik is proposing to generalize the IE fragmentation and general protocol carrying capabilities of 802.15.9.  He defines Conceptual Objects that are identified with higher-layer protocols but are not otherwise understood by 802.15.9.  The objects are broken down into IEs that are used to allow fragmentation/reassembly when the objects are large.  A registry of the identifiers for higher-layer protocols is posited in the proposal, although the specifics of which body would administer that registry need to be decided.  Struik’s work would replace and augment elements of the existing draft.

Tero Kivinen then spoke on adapting IKEv2 as a KMP ([15-13/255r0](https://mentor.ieee.org/802.15/dcn/13/15-13-0255-00-0009-ikev2-over-802-15-9.doc)) for use with 802.15.9.  His proposed text would be added into the current draft where the placeholder section 9.2 appears.  IKEv2 features that are included in the proposal include the basic IKEv2 exchange ([RFC 5996](http://tools.ietf.org/rfc/rfc5996.txt)), childless initiation of IKEv2 ([RFC 6023](http://tools.ietf.org/rfc/rfc6023.txt)), and use of AEAD (Authenticated Encryption with Associated Data) with IKEv2 ([RFC 5282](http://tools.ietf.org/rfc/rfc5282.txt)).  Specifically excluded IKEv2 features or options include negotiation of multiple protocols with the same proposal, and the capability to handle multiple outstanding KMP requests, both of which seem unnecessary for 802.15 environments.  Also excluded are the use of IKEv2 cookies, configuration payloads, and the ability to handle NAT traversal.  The latter feature is at a networking layer above IEEE 802’s interest.  Kivinen lists some IKEv2 features for which a decision on whether to include them needs to be taken.  These features include: commonality of algorithm negotiation between IKEv2 and 802.15, whether multicast security associations should be supported (802.15.4 doesn’t currently do multicast, so this is mostly moot), and some of the IKEv2 exchanges (certain child creation modes and informational payloads).

Another protocol that is being adapted to the 802.15.9 framework is PANA (Protocol for carrying Authentication for Network Access).  Yoshihiro Ohba (Toshiba) gave an update to his previous presentation on how PANA can be made to work with 802.15.9.  Two modes of operation are specified.  One involves a PANA client (PaC) and a PANA Authentication Agent (PAA) as “adjacent” nodes.  The other involves a PANA Relay Element (PRE) that facilitates multi-hop communications between non-adjacent PaCs and PAAs.  If a PRE is present, the communication between the PRE and PAA are out of scope of 802.15.9.  802.15.9 is only used between a PaC and the next hop.

No conference calls are planned between this meeting and the July IEEE 802 Plenary meeting.