**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **TG9 KMP Minutes for July 2013 Plenary meeting, Geneva, Switzerland** |
| Date Submitted | 26th August 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 July 2013 Plenary meeting |
| Abstract | TG9 KMP Minutes for July 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 provided by Peter Yee (Akayla)

**Monday July 15th 2013 PM2 session**

The TG9 agenda is found in [15-13/361r0](https://mentor.ieee.org/802.15/dcn/13/15-13-0361-00-0009-tg9-agenda-geneva-2013.xls).  The opening report is found in [15-13/405r1](https://mentor.ieee.org/802.15/dcn/13/15-13-0405-01-0009-tg9-opening-report-july-2013.ppt).  Minutes from the Waikoloa meeting in May are found in [15-13/364r0](https://mentor.ieee.org/802.15/dcn/13/15-13-0364-00-0009-tg9-meeting-minutes-waikoloa-may-2013.docx) and were approved by acclamation.

The session was called to order by Bob Moskowitz (Verizon), TG chair. The standard patent disclosure information was presented and the chair made a call for essential patents according to the IEEE patent policy.  None were noted.

The minutes for May 2013 meeting were approved by acclamation.

The updated draft document (15-13-0154-02-0009-p802-15-9-d01.pdf) was discussed with a focus on IKEv2 additions. A tangential discussion noted that IKEv2 changes to work with 15.9 are aligned with IKEv2 changes to support TCP-AO (TCP Authentication Option). Tero Kivinen (INSIDE Secure) stated that he was seeing to that as the TCP-AO work was coming out of the KARP (Keying and Authentication for Routing Protocols) working group in the IETF.

The TG discussed the need for cipher negotiation as 15.4 is based on a single cipher/key length but that the MIC (Message Integrity Code) size can actually be varied by a higher layer setting the security level. In particular, IKEv2 has a potentially suitable 'childless negotiation' that does not include cipher negotiation and thus is included in the IKEv2 content.

Bob Moskowitz pointed out that HIP is similar in that cipher negotiation is optional.

Peter Yee asked why this content is needed in the document, since the information is not used when carrying IKEv2 (or HIP) over 15.9.

Karen Randall (Randall Consulting) raised a concern about crypto agility as this functionality is built into 801.1X.

Bob Moskowitz said that 15.4 has no crypto agility beyond the MIC size. Any change would require a PAR and a linked PAR could be to amend 15.9 as needed. It was noted that this is a common practice in 802. No resolution was reached on this topic.

The meeting recessed for the day with the comment that the Wednesday AM2 session would cover decisions on technical comments from May and PM2 would be more on KMPs with a presentation on Dragonfly by Dan Harkins (Aruba Networks), any discussions for 802.1X inclusion, and writing assignments. Finally there will not be a September session, so we need to select times for teleconferences in October before adjourning the meetings this week.

**Wednesday July 17th 2013 AM2 session**

The session covered the decisions found in document 15-13-0442-01-0009-tg9-technical-decisions.ppt

***Item 1: Address format***

Tero Kivinen pointed out that the security associations (SAs) need to be bound to the long address form for authentication purposes, not to the short address. As long as the KMP gets the long address for the SA, it is okay that short addresses were sent over the air.

We will add clarifying text for this.

***Item 2: ACK is no proof of processing***

If a fragment is lost, that is, the inbound state machine registers a skipped fragment, then the inbound processing fails; this is considered an acceptable behavior. A KMP SHOULD be able to handle a lost message, therefore no effort will be made within the 15.9 mechanism to recover a loss fragment.

Text will be added to clarify this behavior.

***Item 3: MACFrameCounter triggering rekey***

Bob Moskowitz recalled that James Gilb (Tensorcom) had noted in a previous meeting that we could have an MLME SAP that actually monitors MACFrameCounter and triggers the rekey, as opposed to the way currently described where the 15.9 shim needs to monitor and trigger this. More clarification is needed.

Will add the PIB MACRekeyThreshold, an MLME SAP to set it, and change the text accordingly.

***Item 4: Crypto Agility***

Add a section in the general part of 15.9 on cipher negotiation (or lack thereof), if there are no choices on ciphers rather than require each KMP description to include text on this.

***Item 5: KMP sections as Annexes***

Accepted. Paul Chilton is rearranging the document already to accommodate this decision.

No other items were raised and TG9 recessed.

**Wednesday July 17th 2013 PM2 session**

Dan Harkins presented his document ([15-13/419r0](https://mentor.ieee.org/802.15/dcn/13/15-13-0419-00-0009-dragonfly-over-802-15-9.doc)) describing the Dragonfly protocol for use within the TG9 KMP transport. Dragonfly is also specified for use with other protocols including 802.11s, TLS (as TLS-PWD), and IKEv2. Dragonfly takes a relatively simple passphrase or other shared secret and uses it as a credential. It is based on elliptic curve cryptography. Operations are peer-to-peer, and either side may initiate the protocol, even simultaneously. The Dragonfly specification will need to be modified to signal the ECDH (Elliptic Curve Diffie-Hellman) group being used since 802.15.9 does not support negotiation of KMPs and their parameters. Alternatively, it might be possible to simply specify the SHA-256 algorithm and the P-256 elliptic curve for use with Dragonfly which would then remove the need to signal the information.