**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **TG9 KMP Conference Call Notes for February 9, 2015** |
| Date Submitted | 9th February 2015  |
| Source | [Peter Yee][NSA/IAD] | Voice: [+1-415-215-7733]Fax: []E-mail: [ peter@akayla.com] |
| Re: | TG9 KMP Notes for February 9, 2015 conference call |
| Abstract | TG9 KMP Notes for February 9, 2015 conference call |
| Purpose | Call Notes |
| 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. |

Brian Weis (Cisco) presented his [updates](https://mentor.ieee.org/802.15/dcn/15/15-15-0127-00-0009-lb98-resolutions-weis.doc) to Annex A based on the agreed upon comment resolutions. This covers CIDs 98, 99, 102, 103, 122, 157, 100, 130, 131, 182, 234 and 294. CIDs 98, 99, 157, 100 cover a desire to have independent multiplex protocol IDs for EAP, 802.1X/MKA, 802.11/4WH, 802.11/GKH. CID 182 is resolved by joining Annex F with Annex A so that the clarification in Annex A on EAPOL frame placement covers both. CIDs 130, 102, and 103 are fixed in the update to Annex A at the end of Weis’ document. CID 122, 131, 294, and 234 are accepted in principle, although the specifics of the 802.11/4WH and 802.11/GWH cipher suite selector needs to be resolved – Weis suggests using a 3-octet OUI and 1-octet cipher suite value at the 802.15 level. James Gilb indicated that this would have to be done by the 802.15 WG – perhaps at the next meeting or in a separate letter ballot. Moskowitz should be able to make this request of Heile during the Berlin meeting. Gilb questioned the need to have a unique namespace for the cipher suites; while 802.11 went this route, it might be good to know why they did so, since we could do “our own thing” without a globally unique OUI as a protocol ID if the value is not interpreted outside of our own uses. It appears that use of an OUI (really a Company ID, not truly an OUI) would be useful and a request should be made of the RAC. Weis will work with Moskowitz to determine how to make the request of the 802.15 WG. Moskowitz (who will not be present at the next meeting) will work with Heile and Gilb to get this all set up. Pages 6-10 contain the replacement text for Annex A (covering and combining both the old A and the old F). A few changes remain to be made to the annex. There is a new Figure (Y) showing the combination of 802.1X/EAP and 802.1X/MKA in sequence using the KMP transport primitives. 802.1X/MKA may continue to run after the completion of the steps shown in Figure Y as it is sometimes used to verify liveness. Kivinen inquired how the KMP-FINISHED.indication could be used with 802.1X/EAP when EAP doesn’t create an 802.15.4 KEY, it only handles the authentication. Modifying the KMP-FINISHED text to allow this use of the primitive for 802.1X/EAP would solve that problem, with the understanding that the FINISHED indication for 802.1X/EAP is used to get to a final state once 802.1X/MKA is used. 802.1X/EAP might be returning keying materials that would be used internal to the KMP process to generate the actual 802.15.4 traffic keys. There’s some trickiness around all of this because an upper layer will not be aware of the state of the 802.1X/EAP run when 802.1X/MKA is called subsequently. The KMP will know the state of 802.1X/EAP before subsequently calling on 802.1X/MKA, but other upper layer elements almost certainly would not. It’s unlikely that upper layer elements would have the necessary states to keep track of 802.1X/EAP status.

Tero Kivinen next showed his [proposal](https://mentor.ieee.org/802.15/dcn/15/15-15-0126-00-0009-fragmentation-format-proposal.doc) for fragmentation. He believes that 16-bits for the transaction ID is excessive and reduced it to a 6-bit value. He also doesn’t like the RTS/CTS scheme, preferring to use a size returned in an abort message for signaling. Sturek inquired whether his requirement for several hundred simultaneous neighbors. Kivinen said that each device could have 64 simultaneous transactions to the coordinator; the limit of 64 is not for the set of all nodes talking to the coordinator. Since KMP PDUs are transported in IEs, optimizations can be made in carrying certain subelements since their presence can be intuited from the length of the IE itself. Kivinen believes that this allows for minimal transmission of data. The abort message can optionally be paired with a maximum length value to cover the facility supplied by the RTS/CTS mechanism. No timeout values are specified in Kivinen’s presentation – it only covers the frame formats. Sturek would like to see a MAC PIB value that covers the timeout. Kivinen believes that’s fine, but it doesn’t have to specified by 802.15.9 – this value would not be transmitted to the other side, so it can be implementation specific. Sturek clarified with Kivinen that the maximum size for a PDU was the same between Sturek’s and Kivinen’s proposals.

The discussion did not finish, but will be continued on the mailing list. Next week’s call will be on Tuesday, with the chair to send out details to the 802.15.9 mailing list.