**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **TG9 KMP Minutes for September 2014 Interim meeting, Athens, GR** | |
| Date Submitted | 19th October 2014 | |
| Source | [] [NSA/IAD] | Voice: [+1-415-215-7733] Fax: [] E-mail: [ peter@akayla.com] |
| Re: | TG9 KMP Minutes for September 2014 Plenary meeting | |
| Abstract | TG9 KMP Minutes for September 2014 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. | |

**Monday September 15th 2014 PM2 session**

The chair, Bob Moskowitz, opened the meeting at 4:17 p.m. on Monday, September 14, 2014. He reminded attendees to record their attendance. He also displayed the patent policy slides.

The agenda for IEEE 802.15 TG9 is found in 15-14/0530r0. The minutes of the San Diego meeting (15-14/0503r0) were approved by acclamation. Peter Yee continues as the acting task group secretary. Tero Kivinen has volunteered a colleague of his who will be able to do some of the document editing remotely. This colleague (Esko Vesala) is a technical editor at INSIDE Secure. Bob Moskowitz will plan a stopover in Helsinki in conjunction with other travel to meet with Vesala in October.

There have been no changes to the draft specification since the July meeting owing to the previous lack of an editor. The plan for this week is to walk through the document and annotate changes that need to be reflected in the next draft in order to have a useful document for the November plenary in San Antonio.

Text will be added to the document indicating that it covers key management protocol transport over single hops. Multiple hops will not be covered because that conflicts with also doing fragmentation, which is a critical feature of the specification. The necessary text will be added to the scope. IEEE 802.15.7 will continue to be referenced in the document, but cannot actually support KMP transport as is because it is unable to transport an Information Element (IE) by itself. In 802.15.7 IEs can only be sent within a Command frame. The last two sentences in the first paragraph of section 4.2 can be dropped – specifying the nature of a security association (SA) is unnecessary since the transmitter simply sends its packets out to an address without really being aware of how many recipients are covered by that address. Thus, there are no such things as broadcast SAs or paired unicast SAs in this context. An SA is bidirectional. In section 4.5, the text should be clarified that the SA is associated with 64-bit extended addresses and authenticates based on those addresses. Use of 16-bit addresses for transmission purposes should not present a problem as long as the previous two restrictions are followed. In section 5, the Multi-Purpose data service should be renamed so as not to cause confusion with the similarly named multi-purpose frames. A possible replacement name might be multiplexing payload service, but it needs to be confirmed that this name doesn’t cause further confusion. In section 5.1, last paragraph, it will be clarified how fragments can become lost even when they are acknowledged by the MAC layer: 802.15.4 may be unable to further process a fragment owing to problems in the receiver (overload, lack of resources) such that the acknowledgement should only be taken to indicate that the fragment made it to the recipient, not that the recipient passed the fragment to the reassembly service and on to the key management protocol. Tero Kivinen has previously submitted comments to the list on the content of section 6.1. Those comments (from May 13, 2014) will be incorporated into the next draft and cover things like SAs not actually being paired. Section 6.2.4 will have its numbers changed to hexadecimal to align with other 802.15 usage. Section 7.1’s inbound state machine should handle the error case where fragments are received in both cleartext and ciphertext forms – these should not be mixed and receipt of mixed forms might indicate an attack. The frame should be dropped in such a case. Section 8 will need to be revisited after the core of the 802.15.4 is amended to correct many errors in the PIBs (PAN Information Bases) in regards to how rekey is handled when frame counters hit certain levels. As mentioned in previous meeting notes, the current rekey handling is badly broken, conflating rekeying for one key to mean that all keys must be rekeyed. There are a number of other issues that Kivinen has found and is fixing as part of the 802.15.4 maintenance process. This Recommended Practice will be aligned to 802.15.4-2015 when that document is issued. Section 9.1.2 (6lowpan support) will be dropped due to the frame counter issues that are only fixed in 802.15.4-2015.

The task group recessed at 17:43. The next session will be used to address issues with the annexes.

**Tuesday September 16th 2014 AM1 session**

Tuesday morning at 8:07 a.m., the chair called the meeting to order. The patent policy information was shown and a call was made for potentially essential patents.

Work continued on the annexes. Questions raised were whether there was commonality between each of the KMPs given in the annexes that could be factored out and if examples of each KMP in use would be helpful. Tero Kivinen explained the changes that are coming out of the 802.15 Security Interest Group that will affect the base 802.15.4 standard in terms of how security associations are populated in the PIB. The commonality between the KMPs likely includes what is in a group key payload information element and for unicast keys, the key derivation/generation/distribution process.

A teleconference is proposed for October 23, 2014 at 12 – 1 p.m. EDT.

Bob Moskowitz will work up a submission of the changes to be made to the draft and post it to the task group mailing list to prompt a discussion of those plans.

TG9 adjourned at 9:27 a.m.