**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **TG9 KMP Minutes for teleconference 27th March 2014** |
| Date Submitted | 16th April 2014  |
| Source | [Paul Chilton][NXP Semiconductors] | Voice: [+44-114-281-2655]Fax: []E-mail: [ paul.chilton@nxp.com] |
| Re: | TG9 KMP teleconference March 27th 2014  |
| Abstract | Minutes from the TG9 KMP teleconference March 27th 2014 |
| 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**

Robert Moskowitz (Verizon) - Chair, Tero Kivinen (INSIDE Secure), Brian Weiss (Cisco), Karen Randall (Randall Associates), Paul Chilton (NXP Semiconductors)

Called to order at 22:03 GMT

Chair showed document 15-14-0215-00 to introduce the call. Chair made a call for essential patents as per the IEEE patent policy and procedures. No responses were heard.

Chair reviewed the Agenda for the meeting, which was to review Service Access Point (SAP) comments from the Beijing meeting, and to define a work plan leading up to the next call.

Tero Kivinen walked through the slides in document 15-14-0184-01, produced from material discussed in the meeting with James Gilb in Beijing.

In the following section Sx corresponds to Slide x in the presentation.

The following comments were made and points raised:

S4 – Where is the data to be stored - some of the parameters will be held in the underlying calls for MLME

S5 – Multipurpose SAP will be called MP-SAP.

S6 – Multipurpose SAP primitives and attributes will be renamed to begin with prefix “MP-“

S7 – Noted that although KMP transport does not need all the addressing parameters they will be needed for others. Underlying primitives such as MCPS-DATA also have lots of other arguments, some needed and some not

S9 – MP-DATA.confirm will show data has been sent

S10 – Noted that some fragments may have different security levels for different flows

S11 – Consequences of above comment – may have to send all fragments at same security level

Comment that it may be possible to store some parameters in the MP-SAP layer eg those which are PHY related

S17 – Tero indicated that a new interest group is being formed in 15.4 in order to fix the security layer in 15.4-2011 to allow more MAC frame counters than the current single one. Brian asked which entity decides that encryption needed; Tero answered that this is a question for a higher layer.

S18 – Tero suggested that we may not need the error notification. There is a need for more work to be done on group key management. Brian suggested that the group look at MKA from 802.1X. Bob noted that ZigBee–IP uses group keys and they are now trying to work out how to rekey groups using PANA

S19 – Noted that KMP-FINISHED may need to be a different name

S20 – Noted that KmpId is the identifier of the KMP in use

S23 – The Handle is only known at the initiating end so can’t be used in Indication or Response primitives

S26 – Need to work out which parameters to put in AllowOperation

S27 – Discussed question of whether a status parameter is needed in the indication, or whether it only gets generated if the result is a success – needs resolving

S34 – Noted that it is necessary to perform all KMP transactions without security so that there is no possibility that there is not a mismatch of keys when rekeying between the different ends

Bob outlined the plan for the next three weeks up to the next call, and asked all to use the mailing list for discussions. With input from the discussions on the list in the first week, we should be able to write text for adding into the document in the second week and then integrate it during the third week to produce a new draft.

Chair closed the call at 22:58 GMT