**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **TG9 KMP Minutes for March 2013 Plenary meeting, Orlando FL, USA** | |
| Date Submitted | 16th April 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 March 2013 Plenary meeting | |
| Abstract | TG9 KMP Minutes for March 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.

**Monday March 18th 2013 PM1 session**

Bob Moskowitz (Verizon), Chair of TG9, opened the session at 13:35 by showing the opening report (document 15-13-0137-01). He invited all present to record their attendance, displayed the IEEE Policy on Essential Patents and invited anyone with knowledge of essential patents to declare it. The minutes of the Vancouver meeting were accepted by acclamation.

Bob notified the group that the May and September meeting overlap with Jewish holidays, making it difficult for him to attend. He may be able to attend the May meeting in Waikoloa for one day on the Monday so will try to arrange sessions for then.

The target for the group should be to get a first full draft of the Recommended Practice completed in June in order to be able to ballot it and then undertake comment resolution during the July meeting.

Bob showed the latest revision of the “Moving Forward” (document 15-12-0458-06). He noted that the overall system view shown in the presentation has been reviewed by parties outside of the TG and is accepted as being the correct approach.

A slight change to the content of the IE has been made; now only the first frame carries the KMP Identifier to indicate which KMP is carried in the payload. This is valid because a stream of KMP fragments cannot be interrupted by other frames due to the use of the forced ACK between fragments.

It is likely there will be no change required to the state machines as already conceived. There may be changes or additions required to the PIB and also deciding which entity is responsible for reading and writing security elements in the PIB. *macSecurityEnabled* already exists, and is currently set by the higher layer. The State Machine Engine will need to set this variable, and also the *macFrameCounter* as well. There is a Frame Counter for each sender which may result in lots to reset when a rekey event occurs. We will also likely need to introduce attributes *macSecRequired* and *macRekeyNeeded;* the question is whether these belong in the MAC PIB or a separate KMP PIB (in which case they will be *kmpSecRequired*, *kmpRekeyNeeded*). The Next Higher Layer is responsible for specifying if security is required; we may need to get help on writing MLME calls to sort this interface out. Since the *macFrameCounter* attribute is in the existing PIB, we need to find out with other groups if changes are allowed to be made here.

It will be prudent to perform a rekey before rollover of the MAC Frame Counter occurs for a given SA. There should be a threshold prior to rollover which triggers the rekey operation; the value of the threshold needs to take into account the control messages as well as data messages being sent. The threshold is typically a policy driven by an organization, but the Recommended Practice can give guidelines on values. The threshold must also take account of data rates on a PHY; for high data rate PHYs rekeying could be needed very frequently as the Frame Counter becomes exhausted. This will not be a problem with 802.15 protocols as they operate at low data rates.

Bob called on the authors of the various KMP sections to provide text for the document. The following people have agreed to author sections of the document:

* HIP – Bob Moskowitz (Verizon)/Jussi Haapola (University of Oulu),
* IKEv2 – Tero Kivinen (InsideSecure),
* PANA - Yoshi Ohba (Toshiba),
* 802.1x - needs input from the group
* SAE – no author identified

Tero mentioned that the Core working group in the IETF may require TLS and DTLS so this may also need to be considered. It was suggested that it might be useful to contact Zach Shelby or Hannes Tschofenig to discuss possible requirements.

Vendor specific KMPs will require some form of identifier or reserved number. It was suggested that we provide an index in the KMP identifier number space, which would then be followed immediately by an identifier which specifies the vendor or protocol.

In the document we should include a Use Case section containing examples of possible deployments and how to employ particular KMPs, in order to give guidance on selection. This kind of information is not usually found in the KMP definition docs.

Bob encouraged participation in the SC-MAN activity to look at the security section of 15.4. The current way it is written is unclear and needs fixing

The KMPs descriptions may need to show how they will be adapted to run over the transport – for example IKEv2 was intended to run over UDP so what must be done to adapt it. We should also consider what additions are needed for SA management eg how to supply keys and how to broadcast and groupcast.

Want to get comments on stuff that authors contribute – Bob.

Tero commented that some problems are generic amongst all the KMPs, therefore there may be some text needed to define common requirements.

There was discussion of the problems which might be found in the RFID mode of 15.4e, in terms of how to do groupcast and rekeying of RFID tags, and also how 802.1AE deals with the problem of multiple senders of a group key.

The group went into recess at 14:34.

**Monday March 18th 2013 PM2 session**

The Chairman called the meeting to order at 16:00 to work on the text of the Recommended Practice.

Paul Chilton (NXP Semiconductors) walked through the document (15-13-0154-00) and the group reviewed the current state and made a few changes.

It was suggested that since the TG9 sessions will be complete by Tuesday afternoon, the closing report can be given at the midweek plenary.

The goal for the Geneva meeting in July is to have a solid document ready for ballot in June for comment resolution during the meeting.

Bob will request 2 slots for the Task Group on the Monday of the May meeting in Waikoloa so he can attend.

The group went into recess at 16:45.

**Tuesday March 19th 2013 AM1 session**

The Chairman called the meeting to order at 08:10. He reminded all present to register their attendance.

Yesterday Bob was asked by James Gilb where 15.9 fits into the 802 architecture. He sent a reply to James and forwarded to the TG9 list, suggesting that he refer to the architecture diagram in the draft document 15-13-0154 which shows that the layer sits above the MAC and below the LLC.

Arrangements for a teleconference were discussed with suggested dates around the end of Apr or early May to discuss progress on the document. Arrangements concerning the number of slots for the May meeting and when they should be scheduled were also discussed. The consensus was that at least the Monday PM1 & 2 slots should be requested.

The group went into recess at 8:30 to continue with document editing and preparation of the closing report.

**Tuesday March 19th 2013 AM2 session**

The Chairman called the meeting to order at 10:43, and invited all present to record their attendance.

During the recess, Bob discussed the procedures for balloting the Recommended Practice with experienced members of the Working Group. There is a reasonable amount of latitude available to the Task Group in how they wish to proceed with developing and balloting the document in the Task Group. We will use a formal process in this TG, with a goal to complete the first TG ballot by the July meeting. This means the document must be in a sufficiently complete state by then to put forward to the TG members. Bob set a deadline of having major contributions submitted by 26th April, with the contributions integrated into the document and ready to be discussed and amended during the May members meeting.

Up until the document is submitted for Letter Ballot within the Working Group, procedurally it will be known as a Contribution to the Recommended Practice. It can only become a formal draft (with subsequent access restrictions in Mentor) when it goes for WG ballot.

Bob asked the members of the group for their opinion on how long a ballot should run. The consensus was for a 14-day ballot.

Karen Randall (Randall Consulting) noted that there may be a problem getting content for the 802.1X section, since they met last month and are not due to meet soon; there needs to be a formal request for contributions to the document to be made to the 802.1X group.

*Action: Bob Moskowitz to send a formal request for contribution to the Recommended Practice to the 802.1X group.*

During the period up to the ballot, Bob will be soliciting review and comments from experts on the 802.15.4 MAC to check that the proposed transport mechanism is feasible

The Closing Report (doc 13-15-0171) was prepared in the meeting and approved by the Task Group members.

Bob sent a request for the Monday PM1 and PM2 slots during the May meeting. The TG will probably want to ask for some more time later in the week to allow for more work after reviewing the updated contribution draft in the Monday sessions.

The timetable for reaching TG ballot is as follows

* Major contributions to be received by end of 26th April
* Update document and post to Mentor for teleconf to discuss on the 29th April
* 14-day task group ballot commencing 28th June, closing 12th July
* Comment consolidation 13th – 16th July
* Comment resolution and review during the July meeting sessions on the 17th and 18th July

*Action: Bob Moskowitz to send out arrangements for the call on 29th April by the end of the 22nd April*

It was suggested that there may be a need for a conference call during the week of the 24th June to discuss the document prior to the Letter Ballot beginning. This can be arranged with the usual one week notice period if it becomes necessary.

It was suggested that any further revisions to the contribution to the recommended practice should be published as a pdf on Mentor.

The Chairman adjourned the meeting at 11:21