The Security Task Group met Tuesday 17th (a.m. & p.m.), Wednesday 18th (a.m. & p.m.), Thursday 19th (a.m.).
All TG meetings were chaired by Mick Seaman. The first session on Thursday was a joint meeting with 802.15.9.
No record of attendance separate from that for 802.1 as a whole for each meeting was kept.

1. Patent Policy

The chair showed the patent policy slides and issued the call for notification of essential patents at the start of each day's meetings (Tuesday 9.00 a.m, Wednesday 9.00 a.m., Thursday 8.00 a.m.) There were no responses at this time. On each occasion the TG chair noted that the patent policy slides could be found in the opening plenary slides (pointer distributed to the 802.1 email list by the 802.1 WG chair) if attendees wished to study them further, and that notifications of essential patents could be made to either the TG or WG chair at any time.

2. Agenda items

The work items for the week, previously notified briefly to the 802.1 opening plenary and reviewed at the beginning of the Tuesday TG meeting, were:

- P802.1AEbw WG recirc ballot resolution (passed, no outstanding negatives)
- P802.1Xbx ballot resolution
- ESS 0.5 spec - review of comments/responses/requests for clarification on the ESS 0.5 spec
- Discussion of potential interpretation request re Confidentiality Offset
- Other potential interpretation requests/maintenance items
- Meeting with 802.15.9 (chair Bob Moskowitz) re key agreement for 802.15.4

the following were also discussed:

- Future TG meetings

3. P802.1AEbw WG recirc ballot resolution

One set of comments (from Pat Thaler) had been received. Apart from one technical question (no change proposed) these were minor editorials, formally out of scope of the recirc, but none the less useful. In keeping with past WG practice these would be noted on the cover letter to the ballot along with similar items noted by Karen Randall [Note- for the P802.1Q Corrigenda the WG chair was able to submit a single brief comment requesting that all the cover letter edits be applied]. The ballot totals, Pat's comments and their resolution can be found at:

http://www.ieee802.org/1/files/private/bw-drafts/d1/802-1AEbw-D1-0-dis.pdf

Agreed to request 802.0 approval to forward P802.1AEbw D1.0 to Sponsor ballot.

A possible minor improvement to the Salt (to derive the 96-bit salt from the 128-bit Key Identifier (KI)) was discussed, together with not keeping the Salt secret even in P802.1Xbx (the Salt is not a secret in RTSP-Real Time Streaming Protocol). This would mean that P802.1Xbx could be completely aligned with P802.1AEbw+802.1X-2010. Brian Weis undertook to check the suggestion with David McGrew (GCM author), it might then be submitted as a sponsor ballot comment.

4. P802.1Xbx discussion

Brian Weis led a discussion of MKA suspension based on his document:

http://www.ieee802.org/1/files/public/docs2012/xbx-weis-mka-suspension-0713.pdf and undertook to update the document with some of the points made.

Mick Seaman reviewed the initial draft P802.1Xbx D0.1. In large part this comprised a set of place holders indicating where/how the results of technical discussion would/could be fitted into an amendment. A number of comments including updating of references were made. Mick will issue a new draft incorporating these.

5. ESS 0.5 spec review

The ESS (Ethernet Security Specification) had been prepared by the NSA (based on 802.1AE MACsec and its support by 802.1X-2010) and made available for public review. Mick and Brian had (independently) submitted comments and received responses and requests for further information. These were discussed by the group. In particular a number of potential interworking scenarios had been created (by 802.1ah and other amendments to 802.1Q) after the development of 802.1AE-2006 and these need to be addressed in further documentation (interpretation/maintenance/amendment or revision) for 802.1AE and/or 802.1X. While the authors of ESS 0.5 were not able to attend the meeting, four of their colleagues were and undertook to feedback some of the discussion.

6. Confidentiality Offset interpretation request

Brian Weis had received comments to implementers seeking clarification on what to do (integrity check or drop) frames received that were shorter than the Confidentiality Offset. The Confidentiality Offset feature had been intended to be a temporary provision, to be used prior to the availability of 'straight from the wire and prior to landing in memory' decryption. There was no evidence that it had in fact been used (while the feature has some customer appeal there remains no prospect of of striking/calculating the necessary balance between confidentiality and visibility from/to unauthenticated parties along the network path) and the original requirement was now moot (given available ship sets). The feature is not supported in the new XPN Cipher Suites. The issue is therefore one of providing clarity to implementers concerned to follow the letter of the specification, rather than to enable wider use, and an interpretation request (rather than some less timely but potentially more informative process) was appropriate. Agreed that the interpretation request needed to emphasize the receipt of the frame (rather than the potential for drop, which was not intended and is not in 1AE). Mick to clarify the question and draft a response for TG review before formal submission of the interpretation request.

7. Other items of 1AE/1X interpretation/maintenance

Karen had informally circulated some questions/observations made by others, and undertook to consolidate/clarify the list of these items so the TG could reach preliminary conclusions as to how to progress each.

Contradictions in the scope of the MKA Algorithm Agility parameter (1X-2010 6.2.4, 9.3.3, Fig 11-12, Fig 11-13) were noted (is the KEK and Key Wrap included or not?. At a minimum this should be clarified in 802.1Xbx as potential secure distribution of the Salt would take place within the Key Wrap.

8. Meeting with 802.15.9 (KMP (Key Management Protocol) Transport Proposal)

Bob Moskovitz presented

https://mentor.ieee.org/802.15/dcn/12/15-12-0373-00-0009-kmp-transport-joint-802-1.ppt

There was an initial draft for the project, though this was largely skeletal, and further progress would depend on identifying a technical editor for the draft. Mick indicated that .1 would likely be interested in contributing to ensure availability of .1X based solutions once the draft had progressed to the point where it was clear how such a contribution would fit in. This would of course be subject to identification of relevant use case scenarios.