IEEE P802.15

Wireless Personal Area Networks

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | May24 Session Minutes for IG Crypt | |
| Date Submitted | 16 May 2024 | |
| Source | Ann T Krieger | E-mail: AnnKrieger.dod@gmail.com |
| Re: | May 2024 Wireless Interim Session | |
| Abstract | Meeting minutes for the IG Crypt | |
| Purpose | Provide meeting 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. | |

# IEEE 802.15 IG Crypt

## Monday 13 May 2024

1. **1:30pm** The TG chair Tero Kivinen (self) called the meeting in order.
2. Displaying the opening report (doc # [*15-24-0219-00*](https://mentor.ieee.org/802.15/dcn/24/15-24-0219-00-cryp-may-opening-and-closing.pptx)):

* A call was made for essential patents. No one had anything to disclose.
* The agenda was approved

Agenda:

* Discuss and verify the interest of creating task groups for crypto additions
* Work on PAR(s) and CSD(s)

Two main topics

* Ascon cipher algorithms for 802.15.4 –(doc # [15-24-0168-00](https://mentor.ieee.org/802.15/dcn/24/15-24-0168-00-wng0-ascon-the-lightweight-cryptography-standard-for-iot.pptx))
  + Ascon is lightweight crypto algorithm and would be quite suitable for 802.15.4 use.
  + It is AEAD algorithm, uses 128-bit nonce etc, thus can be quite easily added to the 802.15.4 which uses same construct.
  + Two versions Ascon-128 and Ascon-128a, most likely we want to pick one (more efficient Ascon-128a?)
  + What would we need to do?
    - Add Ascon to secAeadAlgorithm assignment table.
    - Create annex to describe how Ascon is used, most likely very short just refer to the external references.
    - Create annex to provide test vectors similar to Annex C.
* Ephemeral Diffie-Hellman Over COSE (EDHOC) [RFC9528](https://datatracker.ietf.org/doc/rfc9528/) KMP for 802.15.9
  + We will discuss this more on Tuesday

Worked on the PAR and CSD for the Ascon addition to 802.15.4

* Draft PAR was started in myProject, current pdf version is (doc #[15-24-0267-00](https://mentor.ieee.org/802.15/dcn/24/15-24-0267-00-cryp-par-for-tg4ae-ascon-for-802-15-4.pdf))
* [Template](https://mentor.ieee.org/802-ec/dcn/18/ec-18-0064-01-0PNP-csd-template-in-doc-format.doc) for CSD was found in the EC documents, Policy and procedures) Current version of CSD is (doc #[15-24-0268-00](https://mentor.ieee.org/802.15/dcn/24/15-24-0268-00-cryp-csd-for-tg4ae.docx))

**3:26 pm** This meeting was recessed.

**Tuesday 14 May 2024**

**1:xxpm** TG chair Tero Kivinen (self) called the meeting to order.

Worked on the closing report:

**2:xxpm** Meeting adjourned.

**Wednesday 15 May 2024**

**1:xxpm** TG chair Tero Kivinen (self) called the meeting to order.

Worked on the closing report (doc # [*15-24-0149-01*](https://mentor.ieee.org/802.15/dcn/24/15-24-0149-01-04ac-march-opening-and-closing.pptx)):

* Will meet in May for 2 slots.
* Coordinate that we don’t overlap with TG4ab, 802.11 TGbi
  + If not, then have at least 1 meeting not overlapped with TG4ab.
* Plan on working on draft.

**2:xxpm** Meeting adjourned.