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 | 15 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.

Attendance:

* Tero Kivinen (self)
* Ann T Krieger (U.S. DoD)
* Clint Powell (HID Global)
* Harry Bims (Bims Laboratories)
* Radhakrishna Canchi (Kyocera International)
* Goran Selander (Ericsson)

1. 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
* 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, just 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, or just refer to the 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** Meeting was recessed.

**Tuesday 14 May 2024**

**1:35pm** TG chair Tero Kivinen (self) called the meeting to order.

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

Attendance:

* Tero Kivinen (self)
* Ann T Krieger (U.S. DoD)
* Harry Bims (Bims Laboratories)
* Tim Godfrey (EPRI)
* Goran Selander (Ericsson)
* Yeong Min Jang (Kookmin University)
* Clint Powell (HID Global)
* Mick Seaman (self)
* Stephan Jechel (Fraunhoffer HHI)

There was discussion about EDHOC is lightweight key management protocol.

* Ephemeral Diffie-Hellman Over COSE (EDHOC)
* Provides mutual authentication, forward secrecy and identity protection.
* Intended for usage in constrained scenarios.
* Three messages, small message sizes.

Presentation from Goran Selander (Ericsson) – (doc # [15-24-0281-00](https://mentor.ieee.org/802.15/dcn/24/15-24-0281-00-cryp-background-to-par-edhoc-for-802-15-9.pdf))

* IETF Lightweight Security Background.
  + General background on some COSE, COSE, ACE, EDHOC
  + “Keying of MACsec with EAP-EDHOC (draft-ietf-emu-eap-edhoc)” – a customer in the automotive industry is using MACsec.
    - Q: IETF liaison – 802.1 would like to know who is using our standards (i.e. MACsec).
    - A: just reporting on what EDHOC was on top of, no change to MACsec
    - GDOI wants to use MACsec – similar to the MACsec key agreement.
* Keying 802.15.4 with EDHOC
  + EDHOC has analogous properties as other CMPs in 802.15.9 allowing a straightforward addition.

Should we create an 802.15.9 amendment that adds EDHOC to 802.15.9?

* Allocate new KMP ID value for 802.15.9.
* Add new Annex that defines how EDHOC is used inside 802.15.4 frames. Needs to define how keys are derived, and how the keys are identified.
* Not sure if there is a way to transport broadcast and/or multicast keys

Looked through the 802.15.9 standard at what is there and what we need to do.

Worked on PAR/CSD for EDHOC and for the Ascon (4ae) from yesterday.

**3:27pm:** Meeting was recessed.

**Wednesday 15 May 2024**

**1:34pm** TG chair Tero Kivinen (self) called the meeting to order.

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

Attendance:

* Tero Kivinen (self)
* Ann T Krieger (U.S. DoD)

PARs and CSDs

* 802.15.9a – PAR ([15-24-0284-00](https://mentor.ieee.org/802.15/dcn/24/15-24-0284-00-cryp-par-for-tg9a-edhoc-for-802-15-9.pdf)) CSD – ([15-24-0286-01](https://mentor.ieee.org/802.15/dcn/24/15-24-0286-01-cryp-csd-for-tg9a.docx))
* 802.15.4ae – PAR ([15-24-0267-01](https://mentor.ieee.org/802.15/dcn/24/15-24-0267-01-cryp-par-for-tg4ae-ascon-for-802-15-4.pdf)) CSD – ([15-24-0268-01](https://mentor.ieee.org/802.15/dcn/24/15-24-0268-01-cryp-csd-for-tg4ae.docx))
* IG motions for the PARs and CSDs were passed and WG motions were created.

Worked on the closing report (doc # [*15-24-0219-02*](https://mentor.ieee.org/802.15/dcn/24/15-24-0219-02-cryp-may-opening-and-closing.pptx)):

* July – one meeting for IG crypto to process the comments received to PARs and CSDs
* September - one meeting for each to start working on the documents.

**2:23pm** Meeting adjourned.