IEEE P802.15

Wireless Personal Area Networks

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | Responses to the PAR comments | |
| Date Submitted | 15th July 2024 | |
| Source | Tero Kivinen | E-mail: kivinen@iki.fi |
| Re: | PAR and CSD comments | |
| Abstract | Provide responses to the PAR and CSD comments. | |
| Purpose | Responses to TG4ae and TG9a PAR and CSD comments | |
| 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. | |

# TG4ae comments

|  |  |  |
| --- | --- | --- |
| **Comment** | **Text in PAR/CSD** | **Remarks / Answers to the Comments** |
| **In response to the comments from IEEE 802.3:** | | |
| **PAR 5.4:**  5.4 Does this amendment delete the purpose clause of the base standard, since the “change to purpose” section is stricken out? | **5.4 Purpose:** This document will not include a purpose clause. | When we select “This document will not include a purpose clause” because we belived this meant for “this document” as it says. We have now heard that “this document” actually means “base standard”, so we will now say that this project will have purpose clause. |
| **CSD 1.1.2:**  1. improve clarity of the response. Change “Yes.” To “Yes, the definitions will be part of the project.” | **1.1.2 Coexistence**  **...**  a) The definitions will be part of this project.  Yes. | **Comment Accepted, used proposed text as is.**  a) The definitions will be part of this project.  Yes, the definition will be part of the project. |
| **CSD 1.1.2:**  2. grammatical error. Change “No CA document needed...” to “No CA document is needed...” | **1.1.2 Coexistence**  **...**  b) If not, explain why the CA document is not applicable.  No CA document needed, as this amendment only adds new cryptographic algorithms to existing IEEE Std 802.15.4. | **Comment Accepted, used proposed text as is.**  b) If not, explain why the CA document is not applicable.  No CA document is needed, as this amendment only adds new cryptographic algorithms to existing IEEE Std 802.15.4. |
| **CSD 1.2.1:**  1.2.1 There is a asterisk character after “AES-CCM” which may be spurious. If it references a note, the note is missing. | **1.2.1 Broad market potential**  …  IEEE Std 802.15.4 was designed using AES-CCM\*. | The AES-CCM\* is the name of the algorithm. The IEEE Std 802.15.4 uses a modified version of the AES-CCM called AES-CCM\*. The star is part of the name, and is not a note. |
| **CSD 1.2.1:**  Also, the second sentence in the first paragraph of the response is confusing to the reader and difficult to parse. Consider changing it to “Adding the more efficient drop in replacement cipher Ascon-128 and/or Ascon-128a will make more lightweight implementations available.”  Also, readability in the last sentence of the first paragraph. Consider changing to “…as the NIST…” or “…as a NIST…” please clarify in this sentence if there is a group or only one algorithm, etc. | **1.2.1 Broad market potential**  …  IEEE Std 802.15.4 was designed using AES-CCM\*. Adding more efficient drop in replacement cipher Ascon-128 and/or Ascon-128a allows making more lightweight implementations available. Ascon is selected as NIST lightweight cryptographic algorithm, making its use in the future more widespread. | **Comment Accepted, used proposed text as is, clarified ascon to be family of algorithms selected by NIST.**  IEEE Std 802.15.4 was designed using AES-CCM\*. Adding the more efficient drop in replacement cipher Ascon-128 and/or Ascon-128a will make more lightweight implementations available. The Ascon family has been selected as the NIST lightweight cryptographic algorithm, making its use in the future more widespread. |
| **CSD 1.2.2:**  1.2.2 Is this the “no” response from the IEEE 802.1 WG? | **1.2.2 Compatibility**  ...  a) Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q?  b) If the answer to a) is no, supply the response from the IEEE 802.1 WG.  No. While the amendment shall comply with IEEE Std 802, it cannot comply with IEEE Std 802.1Q and IEEE Std 802.1AC because IEEE Std 802.15.4 uses 64-bit MAC addresses. | **This is the response that as been agreed for IEEE Std 802.15.4 amendments.** |
| **CSD 1.2.3:**  1.2.3 Improve readability of the last sentence in the response, as it is difficult to parse. Change to “Adding Ascon-128 and/or Ascon-128a will allow using the more lightweight cryptographic algorithm and offers functionality not available in AES (like hashing and key material extraction) that supports more use cases than AES.” | **1.2.3 Distinct Identity**  IEEE Std 802.15.4 was developed specifically to optimally address the needs of IoT networks and is broadly used in that application. It remains unique in that regard. Adding Ascon-128 and/or Ascon-128a will allow using the more lightweight cryptographic algorithm and because it offers functionality not available in AES, like hashing and key material extraction, it can be used in more cases than AES. | **Comment Accepted, used proposed text as is.**  IEEE Std 802.15.4 was developed specifically to optimally address the needs of IoT networks and is broadly used in that application. It remains unique in that regard.  Adding Ascon-128 and/or Ascon-128a will allow using the more lightweight cryptographic algorithm and offers functionality not available in AES (like hashing and key material extraction) that supports more use cases than AES. |
| **CSD 1.2.4:**  1.2.4 Typo. Change “competetion" to “competition” | 1.2.4 Technical Feasibility  Ascon was announced as winner of the NISTs lightweight cryptographic standard competetion. During the competition it received a large number of third party reviews, and verifications. There are multiple existing implementations of it.  It uses the same AEAD framework as used in the IEEE Std 802.15.4, thus dropping it in to the existing IEEE Std 802.15.4 security framework should be straightforward. | **Accepted.**  Ascon was announced as winner of the NISTs lightweight cryptographic standard competition. During the competition it received a large number of third party reviews, and verifications. There are multiple existing implementations of it.  It uses the same AEAD framework as used in the IEEE Std 802.15.4, thus dropping it in to the existing IEEE Std 802.15.4 security framework should be straightforward. |
| **CSD 1.2.5:**  1.2.5 Change “cheaper” to “lower cost”. Change “impementations” to “implementations” | 1.2.5 Economic Feasibility  Ascon provides a smaller footprint than AES for hardware implementatons, and it is faster on pure software implementations, thus it allows making cheaper impementations than currently possible. The cost of the implementation should be same in both coordinators and devices, and there is no special installation or operational costs. | **Accepted.**  Ascon provides a smaller footprint than AES for hardware implementatons, and it is faster on pure software implementations, thus it allows making lower cost implementations than currently possible. The cost of the implementation should be same in both coordinators and devices, and there is no special installation or operational costs. |
| **In response to the comments from IEEE 802.11:** | | |
| **PAR 5.2.b:**  5.2b Make a complete Sentence: -- Change to “This amendment adds the Ascon-128 and Ascon-128a cryptographic algorithms to the IEEE Std 802.15.4.” | **5.2.b Scope of the project:** Add additional cryptographic algorithms Ascon-128/Ascon-128a for the IEEE  Std 802.15.4 for link encryption and authentication. | **Comment Accepted, used proposed text as is.**  This amendment adds the Ascon-128 and Ascon-128a cryptographic algorithms to the IEEE Std 802.15.4. |
| **PAR 5.5:**  5.5 Why is Ascon needed? Just because NIST selected it, why did it need to be added. Clarify the Need.  8.1 Move the comment for 5.5 to 5.5 as it a better explanation for Why.  “5.5 Ascon provides functions like hashing and extracting key material, which are not provided by AES. These functions are not currently used by IEEE Std 802.15.4, but key management protocols defined in IEEE Std 802.15.9 need such functions and providing one algorithm that supports encryption, authentication, hashing, and key material extraction allows more lightweight implementations in the future.”  alternatively: “IEEE Std 802.15.4 is widely used in IoT applications. Use of the Ascon-128 and Ascon128a lightweight cryptographic algorithms enables 802.15.4 devices to support even more demanding IoT applications. “ | **5.5 Need for the Project:** NIST has selected Ascon as its lightweight cipher, thus providing it in the IEEE  Std 802.15.4 is needed.  In addition Ascon provides functions that are not available in the Advanced Encryption Standard (AES). | **Comment Accepted, used alternate text as is.**  **5.5 Need for the Project:** IEEE Std 802.15.4 is widely used in IoT applications. Use of the Ascon-128 and Ascon128a lightweight cryptographic algorithms enables 802.15.4 devices to support even more demanding IoT applications. |
| Question is this trying to support 802.15.9? |  | This project adds Ascon to IEEE Std 802.15.4.  IEEE Std 802.15.9 reuses key management protocols (KMPs) defined elsewhere. The decision to define how Ascon is used in any of the IEEE Std 802.15.9 KMPs happens in those other standardization bodies defining those KMPs. |
| **PAR 8.1 for 5.2.b:**  8.1 first comment for #5.2 – “Ascon-128/Ascon-128a” should be “Ascon-128 and Ascon-128a”. And change “had been selected” to “has been selected”  Also at the end of the sentence : “allowing it to be a drop in “ change to “allowing an Ascon algorithm to be a drop-in”  Whether your move the comment 5.5 to section 5.5 or not, 802.15.9 should be fully identified in 8.1. | 5.2.b Ascon-128/Ascon-128a: Ascon is a family of lightweight authenticated ciphers that had been selected by US National Institute of Standards and Technology (NIST) for  future standardization of the lightweight cryptography.  Ascon provides the same Authenticated Encryption with Associated Data (AEAD) functionality as Advanced  Encryption Standard (AES), allowing it to be a drop in replacement. | **Comment Accepted, used proposed text as is.**  5.2.b Ascon-128 and Ascon-128a: Ascon is a family of lightweight authenticated ciphers that has been selected by US National Institute of Standards and Technology (NIST) for future standardization of the lightweight cryptography. Ascon provides the same Authenticated Encryption with Associated Data (AEAD) functionality as Advanced Encryption Standard (AES), allowing an Ascon algorithm to be a drop-in.  IEEE Std 802.15.9: IEEE Standard for Transport of Key Management Protocol (KMP) Datagrams |
| **CSD 1.2.1:**  CSD 1.2.1 the two paragraphs are sentence fragments. Rewrite with better grammar to complete the sentences. | IEEE Std 802.15.4 was designed using AES-CCM\*. Adding more efficient drop in replacement cipher Ascon-128 and/or Ascon-128a allows making more lightweight implementations available. Ascon is selected as NIST lightweight cryptographic algorithm, making its use in the future more widespread.  There are many silicon and system vendors already producing devices and systems using IEEE Std 802.15.4 for use in IoT applications. This includes things like consumer electronics, mobile devices, building automation, medical applications, SmartGrid and Smart Community applications, industrial control, etc., and therefore has a very large end user community. |  |
| **CSD:**  CSD – Expand first use of acronyms – AES, NIST, AEAD, etc.. | 1.2.1 Broad market potential  IEEE Std 802.15.4 was designed using AES-CCM\*. Adding more efficient drop in replacement cipher Ascon-128 and/or Ascon-128a allows making more lightweight implementations available. Ascon is selected as NIST lightweight cryptographic algorithm, making its use in the future more widespread.  There are many silicon and system vendors already producing devices and systems using IEEE Std 802.15.4 for use in IoT applications. This includes things like consumer electronics, mobile devices, building automation, medical applications, SmartGrid and Smart Community applications, industrial control, etc., and therefore has a very large end user community.  1.2.4 Technical Feasibility  Ascon was announced as winner of the NISTs lightweight cryptographic standard competetion. During the competition it received a large number of third party reviews, and verifications. There are multiple existing implementations of it.  It uses the same AEAD framework as used in the IEEE Std 802.15.4, thus dropping it in to the existing IEEE Std 802.15.4 security framework should be straightforward. | **Expanded acronyms:**  1.2.1 Broad market potential  IEEE Std 802.15.4 was designed using advanced encryption standard extension of counter mode encryption and cipher block chaining message authentication code  (AES-CCM\*). Adding more efficient drop in replacement cipher Ascon-128 and/or Ascon-128a allows making more lightweight implementations available. Ascon is selected as US National Institute of Standards and Technology (NIST) lightweight cryptographic algorithm, making its use in the future more widespread.  There are many silicon and system vendors already producing devices and systems using IEEE Std 802.15.4 for use in Internet of Things (IoT) applications. This includes things like consumer electronics, mobile devices, building automation, medical applications, SmartGrid and Smart Community applications, industrial control, etc., and therefore has a very large end user community.  1.2.4 Technical Feasibility  Ascon was announced as winner of the NISTs lightweight cryptographic standard competetion. During the competition it received a large number of third party reviews, and verifications. There are multiple existing implementations of it.  It uses the same authenticated encryption with associated data (AEAD) framework as used in the IEEE Std 802.15.4, thus dropping it in to the existing IEEE Std 802.15.4 security framework should be straightforward. |

# TG9a comments

|  |  |  |
| --- | --- | --- |
| **Comment** | **Text in PAR/CSD** | **Remarks / Answers to the Comments** |
| **In response to the comments from IEEE 802.3:** | | |
| **PAR 5.4:**  5.4 Does this amendment delete the purpose clause of the base standard, since the “change to purpose” section is stricken out? | **5.4 Purpose:** This document will not include a purpose clause. | When we select “This document will not include a purpose clause” because we belived this meant for “this document” as it says. We have now heard that “this document” actually means “base standard”, so we will now say that this project will have purpose clause. |
| **CSD 1.1.2:**  1. improve clarity of the response. Change “Yes.” To “Yes, the definitions will be part of the project.” | **1.1.2 Coexistence**  **...**  a) The definitions will be part of this project.  Yes. | **Comment Accepted, used proposed text as is.**  a) The definitions will be part of this project.  Yes, the definition will be part of the project. |
| **CSD 1.1.2:**  2. grammatical error. Change “No CA document needed...” to “No CA document is needed...” | **1.1.2 Coexistence**  **...**  b) If not, explain why the CA document is not applicable.  No CA document needed, as this amendment only adds new cryptographic algorithms to existing IEEE Std 802.15.4. | **Comment Accepted, used proposed text as is.**  b) If not, explain why the CA document is not applicable.  No CA document is needed, as this amendment only adds new cryptographic algorithms to existing IEEE Std 802.15.4. |
| **CSD 1.2.2:**  1.2.2 Is this the “no” response from the IEEE 802.1 WG? | **1.2.2 Compatibility**  ...  a) Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q?  b) If the answer to a) is no, supply the response from the IEEE 802.1 WG.  No. While the amendment shall comply with IEEE Std 802, it cannot comply with IEEE Std 802.1Q and IEEE Std 802.1AC because IEEE Std 802.15.4 uses 64-bit MAC addresses. | **This is the response that as been agreed for IEEE Std 802.15.4 amendments.** |
| **In response to the comments from IEEE 802.11:** | | |
| ‍**PAR 2.1:**  2.1 Title needs to expand acronym COSE | **2.1 Project Title:** IEEE Standard for Transport of Key Management Protocol (KMP) Datagrams  Amendment: Ephemeral Diffie-Hellman Over COSE (EDHOC) KMP | The full expansion of the COSE will make the title really long and difficult to parse:  IEEE Standard for Transport of Key Management Protocol (KMP) Datagrams  Amendment: Ephemeral Diffie-Hellman Over Concise Binary Object Representation (CBOR) Object Signature and Encryption (COSE) (EDHOC) KMP  Those acronyms are already expanded in 8.1, and for the EDHOC the COSE is not really an acronym it is the name of the protocol used. |
| **PAR 5.2.b:**  5.2b. Change to “This amendment specifies the use of EDHOC (RFC 9528) KMP for the IEEE Std 802.15.9.” | **5.2.b Scope of the project:** Specify the use of EDHOC (RFC 9528) KMP for the IEEE Std 802.15.9. | **Comment Accepted, used proposed text as is.**  This amendment specifies the use of EDHOC (RFC 9528) KMP for the IEEE Std 802.15.9. |
| **PAR 5.5:**  5.5 Change “objectives for IEEE 802.15.” to “objectives for IEEE 802.15.9” . Just saying 802.15 seems too broad.  Is this what you mean? 802.15.9 needs a non-fragmented algorithm to be defined. 802.15.9 needs to add EDHOC so that it has a non-fragment method. | **5.5 Need for the Project:** Existing methods in IEEE Std 802.15.9 cannot be used without IEEE Std  802.15.9 fragmentation. EDHOC is a lightweight key management protocol whose messages can be sent in  frames without fragmentation, and has a low code footprint matching the objectives for IEEE 802.15. | Low code footprint is one of the objectives for IEEE 802.15 working group as whole. |
| **CSD 1.2.1:**  CSD 1.2.1b Add “(KMP)” after “key management protocols” and use KMP in the second line. | 1.2.1 Broad market potential  IEEE Std 802.15.9 was designed to include multiple key management protocols, so different environments could select suitable key management protocol for their use case. One of the problems with existing KMPs is that all of them use messages that require fragmentation in typical IEEE 802.15.4 PHY. EDHOC has a mode of operation where each message is less than 50 bytes, meaning it does not need fragmentation. | **Comment Accepted, used proposed text as is.**  IEEE Std 802.15.9 was designed to include multiple key management protocols (KMP), so different environments could select suitable KMP for their use case. One of the problems with existing KMPs is that all of them use messages that require fragmentation in typical IEEE 802.15.4 PHY. EDHOC has a mode of operation where each message is less than 50 bytes, meaning it does not need fragmentation. |
| **CSD 1.2.1:**  CSD 1.2.1b second paragraph: Change “combination of IEEE Std 802.15.9” to “combination with IEEE Std 802.15.9“ | 1.2.1 Broad market potential  There are multiple silicon and system vendors producing devices and systems using IEEE Std 802.15.4 in combination of IEEE Std 802.15.9 for use in IoT applications. This includes things like consumer electronics, mobile devices, building automation, medical applications, SmartGrid and Smart Community applications, industrial control, etc., and therefore has a very large end user community. | **Comment Accepted, used proposed text as is.**  There are multiple silicon and system vendors producing devices and systems using IEEE Std 802.15.4 in combination with IEEE Std 802.15.9 for use in IoT applications. This includes things like consumer electronics, mobile devices, building automation, medical applications, SmartGrid and Smart Community applications, industrial control, etc., and therefore has a very large end user community. |