IEEE P802.15

Wireless Personal Area Networks

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | AES-256 Test Vectors | |
| Date Submitted | 10, January 2021 | |
| Source | Tero Kivinen Finland | E-mail: kivinen@iki.fi |
| Re: | Annex C | |
| Abstract | This is test vectors for AES-256 similarly than what is in the IEEE Std 802.15.4 Annex C.3, i.e., providing short examples of different frames and showing them both before and after outbound security processing. | |
| Purpose | To be included as bibliography to P802.15.4y | |
| 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. | |

## 1 AES-CCM-256 Examples

### 1.1 Beacon frame

This is same example as Annex C.2.2 of IEEE Std 802.15.4-2020.

MHR of the Beacon Frame with Frame Version of 0b01, and Security Enabled. Destination address is omitted. Source address is 0xacde480000000001 with Pan ID of 0x4321.

Auxiliary Security Header using security level of Mic64, Key Id Mode 0 - Implicit, Frame Counter of 0x00000005, using key of:

0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecfc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

Nonce:

ac de 48 00 00 00 00 01 00 00 00 05 02

Beacon frame:

08 d0 84 21 43 01 00 00 00 00 48 de ac || 02 05 00 00 00 || 55 cf 00 00 51 52 53 54

Secured beacon frame:

08 d0 84 21 43 01 00 00 00 00 48 de ac || 02 05 00 00 00 || 55 cf 00 00 51 52 53 54 ||

9e e6 d5 8c d7 43 6f fb

### 1.2 MAC Command frame

This is same example as Annex C.2.3 of IEEE 802.15.4-2020.

MHR of the MAC Command Frame with Frame Version of 0b01, Security Enabled, and Ack Requested. Destination address is 0xacde480000000002 with Pan ID of 0x4321. Source address is 0xacde480000000001 with Pan ID of 0xffff.

Auxiliary Security Header using security level of Encrypted Mic64, Key Id Mode 0 - Implicit, Frame Counter of 0x00000005, using key of:

0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecfc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

Nonce:

ac de 48 00 00 00 00 01 00 00 00 05 06

MAC Command frame:

2b dc 84 21 43 02 00 00 00 00 48 de ac ff ff 01 00 00 00 00 48 de ac || 06 05 00 00 00 ||

01 ce

Secured MAC Command frame:

2b dc 84 21 43 02 00 00 00 00 48 de ac ff ff 01 00 00 00 00 48 de ac || 06 05 00 00 00 ||

01 82 || 92 0f 0f ca fa 5f 1a 2c

### 1.3 MAC Command frame

This is an example of Enhanced Beacon command using Enhanced Beacon Filter IE.

MHR of the MAC Command Frame with Frame Version of 0b10, Security Enabled, and IE Present. Destination address is 0xffff with Pan ID of 0x4321. Source address is 0xacde480000000001 with Pan ID of 0x4321.

Auxiliary Security Header using security level of Encrypted Mic128, Key Id Mode 0 - Implicit, Frame Counter of 0x00000006, using key of:

0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecfc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

Nonce:

ac de 48 00 00 00 00 01 00 00 00 06 07

MAC Command frame:

0b ea 85 21 43 ff ff 21 43 01 00 00 00 00 48 de ac || 07 06 00 00 00 || 00 3f ||

03 88 01 1e 01 00 f8 07

Secured MAC Command frame:

0b ea 85 21 43 ff ff 21 43 01 00 00 00 00 48 de ac || 07 06 00 00 00 || 00 3f ||

5a 26 0b 79 5d e5 5b a0 || 60 8e fd d8 c5 eb 3d 77 5a 20 c8 c4 99 2b b2 15

### 1.4 MAC Command frame

This is same example as last one, but this one is using Pan ID Compression and will omit the source PAN ID.

MHR of the MAC Command Frame with Frame Version of 0b10, Security Enabled, PAN ID Compression, and IE Present. Destination address is 0xffff with Pan ID of 0x4321. Source address is 0xacde480000000001.

Auxiliary Security Header using security level of Encrypted Mic128, Key Id Mode 0 - Implicit, Frame Counter of 0x00000007, using key of:

0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecfc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

Nonce:

ac de 48 00 00 00 00 01 00 00 00 07 07

MAC Command frame:

4b ea 86 21 43 ff ff 01 00 00 00 00 48 de ac || 07 07 00 00 00 || 00 3f ||

03 88 01 1e 01 00 f8 07

Secured MAC Command frame:

4b ea 86 21 43 ff ff 01 00 00 00 00 48 de ac || 07 07 00 00 00 || 00 3f ||

a6 3b 5c 78 a4 67 39 df || c7 99 c0 7f fb 1b 0f 81 72 a1 de c9 4c 84 8f 65

### 1.5 Enhanced Beacon frame

This is example of Enhanced Beacon used in the TSCH. This is just authenticated not encrypted, as TSCH beacons cannot be encrypted as the data in them is needed for joining the network. The security processing is bit more difficult as the recipient needs to know the ASN before it can verify the MIC of the frame. As this is TSCH Beacon this will include TSCH Synchronization IE inside which will tell the ASN. This frame is using ASN of 0x123456789a.

MHR of the Beacon Frame with Frame Version of 0b10, Security Enabled, PAN ID Compression, and IE Present. Destination address is 0xffff with Pan ID of 0x4321. Source address is 0xacde480000000001.

Auxiliary Security Header using security level of Mic128, Key Id Mode 1 with key index of 1, ASN 0x123456789a In Nonce, using key of:

0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecfc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

Nonce:

ac de 48 00 00 00 00 01 12 34 56 78 9a

Beacon frame:

48 ea 87 21 43 ff ff 01 00 00 00 00 48 de ac || 6b 01 || 00 3f ||

1a 88 06 1a 9a 78 56 34 12 04 01 1c 01 0a 1b 01 01 64 00 01 00 00 00 00 0f 01 c8 00

Secured Beacon frame:

48 ea 87 21 43 ff ff 01 00 00 00 00 48 de ac || 6b 01 || 00 3f ||

1a 88 06 1a 9a 78 56 34 12 04 01 1c 01 0a 1b 01 01 64 00 01 00 00 00 00 0f 01 c8 00 ||

b0 59 27 59 1b 20 e2 51 4f 8b d9 aa 0b f8 33 28

### 1.6 Data frame

This is example of Data frame using both header (not encrypted) and payload IEs (encrypted). This also uses PAN ID Compression of extended addresses, meaning there is no PAN ID at all. The header IE is Global Time IE, and the Payload IE is the Mac Metrics IE telling the number of octets sent. The contents of the data frame is string "This is data".

MHR of the Data Frame with Frame Version of 0b10, Security Enabled, Ack Requested, PAN ID Compression, and IE Present. Destination address is 0xacde480000000002. Source address is 0xacde480000000001.

Auxiliary Security Header using security level of Encrypted Mic64, Key Id Mode 1 with key index of 1, Frame Counter of 0x00000008, using key of:

0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecfc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

Nonce:

ac de 48 00 00 00 00 01 00 00 00 08 06

Data frame:

69 ee 85 02 00 00 00 00 48 de ac 01 00 00 00 00 48 de ac || 0e 08 00 00 00 01 ||

84 14 34 ff 3f 5c 00 3f ||

07 88 05 1f 01 e8 03 00 00 00 f8 54 68 69 73 20 69 73 20 64 61 74 61

Secured Data frame:

69 ee 85 02 00 00 00 00 48 de ac 01 00 00 00 00 48 de ac || 0e 08 00 00 00 01 ||

84 14 34 ff 3f 5c 00 3f ||

4e 45 38 85 88 0d 47 f6 3e 07 b3 6b 8b de 97 0a 08 c4 44 fa 57 bf af ||

0b c9 1f 8c 43 26 29 2d

### 1.7 Ack frame

This is an example of Ack frame using Header IEs and Data. The header IE used is the TSCH Time Correction IE, but this is not using the ASN in Nonce feature, so this is not exact TSCH ACK frame. The data in Ack simply says "ACK".

MHR of the Ack Frame with Frame Version of 0b10, Security Enabled, PAN ID Compression, Sequence Number Suppression, and IE Present. Destination address is 0xacde480000000002. Source address is 0xacde480000000001.

Auxiliary Security Header using security level of Encrypted Mic32, Key Id Mode 1 with key index of 1, Frame Counter of 0x00000009, using key of:

0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecfc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

ACK Payload: 41 43 4b

Nonce:

ac de 48 00 00 00 00 01 00 00 00 09 05

Data frame:

4a ef 02 00 00 00 00 48 de ac 01 00 00 00 00 48 de ac || 0d 09 00 00 00 01 ||

02 0f 01 00 80 3f || 41 43 4b

Secured ACK frame:

4a ef 02 00 00 00 00 48 de ac 01 00 00 00 00 48 de ac || 0d 09 00 00 00 01 ||

02 0f 01 00 80 3f || 01 15 24 || f9 cd 66 dd