IEEE P802.15

Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)	
Title	Frame examples for AES-CCM-256, AES-GCM-128 and AES-GCM-256.	
Date Submitted	17, January 2019	
Source	Tero Kivinen Finland	Voice: +358 40 547 4476 E-mail: kivinen@iki.fi
Re:	Examples matching current Annex C, but using different encryption algorithms.	
Abstract	This contains sections to be added to 802.15.4y document as example frames using new algorithms. This includes examples using AES-CCM-256, AES-GCM-128, and AES-GCM-256.	
Purpose	Provide annex material for 802.15.4y standard.	
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.	

Table of Contents

C.4 AES-CCM-256 examples

C.4.1 Beacon frame

This is same example as C.2.1.

MHR of the Beacon Frame with Frame Version of 0b01, Security Enabled, Destination address is using Omitted, Source address is using Extended Address. 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

C.4.2 MAC Command frame

This is same example as C.2.2.

MHR of the MAC Command Frame with Frame Version of 0b01, Security Enabled, Ack Requested, Destination address is using Extended Address, Source address is using Extended Address. 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

C.4.3 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, IE Present, Destination address is using Short Address, Source address is using Extended Address. 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

C.4.4 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, IE Present, Destination address is using Short Address, Source address is using Extended Address. 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

C.4.5 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 0x123456.

MHR of the Beacon Frame with Frame Version of 0b10, Security Enabled, PAN ID Compression, IE Present, Destination address is using Short Address, Source address is using Extended Address. 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, Frame counter suppressed, ASN In Nonce, using key of 0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecfc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

Nonce:

ac de 48 00 00 00 00 01 00 12 34 56 07

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 56 34 12 00 00 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 56 34 12 00 00 04 01 1c 01 0a 1b 01 01 64 00 01 00 00 00 00 0f 01 c8 00 || b7 34 eb 99 60 63 7c 9b 3d 00 7f e7 90 69 4a 53

C.4.6 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.

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

C.4.7 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, IE Present, Destination address is using Extended Address, Source address is using Extended Address. 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

C.5 AES-GCM-128 examples

C.5.1 Beacon frame

This is same example as C.2.1.

MHR of the Beacon Frame with Frame Version of 0b01, Security Enabled, Destination address is using Omitted, Source address is using Extended Address. 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 0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

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 || 6a 21 48 47 71 f5 c9 a2

C.5.2 MAC Command frame

This is same example as C.2.2.

MHR of the MAC Command Frame with Frame Version of 0b01, Security Enabled, Ack Requested, Destination address is using Extended Address, Source address is using Extended Address. 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 0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

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 78 || 2d c1 f9 01 29 6d d2 6c

C.5.3 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, IE Present, Destination address is using Short Address, Source address is using Extended Address. 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 0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

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 || 1c eb b9 3c 9c 3b 16 2f || f8 8c 60 a1 b0 2d e4 ec b4 72 7d 75 30 43 7b a1

C.5.4 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, IE Present, Destination address is using Short Address, Source address is using Extended Address. 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 0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

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 || 9b 5c 0d 01 5c 03 a6 14 || 66 fc 44 e1 2f cc f9 90 e1 61 64 ba 0b 59 fd ed

C.5.5 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 0x123456.

MHR of the Beacon Frame with Frame Version of 0b10, Security Enabled, PAN ID Compression, IE Present, Destination address is using Short Address, Source address is using Extended Address. 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, Frame counter suppressed, ASN In Nonce, using key of 0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

Nonce:

ac de 48 00 00 00 00 01 00 12 34 56 07

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 56 34 12 00 00 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 56 34 12 00 00 04 01 1c 01 0a 1b 01 01 64 00 01 00 00 00 00 0f 01 c8 00 || 3d bb d1 92 57 d6 6c 55 b9 a4 0b 15 cb a6 94 d3

C.5.6 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.

MHR of the Data Frame with Frame Version of 0b10, Security Enabled, Ack Requested, PAN ID Compression, IE Present, Destination address is using Extended Address, Source address is using Extended Address. 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 0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

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 || 5b 50 1c 01 ce 49 f5 9c 1a 90 6c a5 48 d5 5f a3 e9 e6 79 f2 2d 2b 27 || 50 99 4e a9 d1 7e 68 97

C.5.7 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, IE Present, Destination address is using Extended Address,

Source address is using Extended Address. 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 0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

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 || d5 52 c3 || 33 4a 82 8b

C.6 AES-GCM-256 examples

C.6.1 Beacon frame

This is same example as C.2.1.

MHR of the Beacon Frame with Frame Version of 0b01, Security Enabled, Destination address is using Omitted, Source address is using Extended Address. 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 || 1c 78 62 81 53 4c b5 64

C.6.2 MAC Command frame

This is same example as C.2.2.

MHR of the MAC Command Frame with Frame Version of 0b01, Security Enabled, Ack

Requested, Destination address is using Extended Address, Source address is using Extended Address. 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 7a || 45 5d 32 73 c0 13 0c ad

C.6.3 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, IE Present, Destination address is using Short Address, Source address is using Extended Address. 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 || 07 8b 72 38 1e fd 24 c7 || 6f d4 f5 16 a7 ff 42 59 e3 d0 01 f9 bc dd 8e 65

C.6.4 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, IE Present, Destination address is using Short Address, Source address is using Extended Address. 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 || e2 84 7b fe 8c 99 ce 0c || ae f9 f1 35 aa 45 c9 4a f4 05 58 c3 fc 62 af 67

C.6.5 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 0x123456.

MHR of the Beacon Frame with Frame Version of 0b10, Security Enabled, PAN ID Compression, IE Present, Destination address is using Short Address, Source address is using Extended Address. 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, Frame counter suppressed, ASN In Nonce, using key of 0xc0c1c2c3c4c5c6c7c8c9cacbcccdcecfc0c1c2c3c4c5c6c7c8c9cacbcccdcecf.

Nonce:

ac de 48 00 00 00 00 01 00 12 34 56 07

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 56 34 12 00 00 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 56 34 12 00 00 04 01 1c 01 0a 1b 01 01 64 00 01 00 00 00 00 0f 01 c8 00 || ee 60 3a 18 b1 70 3d d0 b9 d2 b9 8a f9 0f df ab

C.6.6 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.

MHR of the Data Frame with Frame Version of 0b10, Security Enabled, Ack Requested, PAN ID Compression, IE Present, Destination address is using Extended Address, Source address is using Extended Address. 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 || 38 b6 ba 3c c0 12 91 55 a0 06 06 7d 6a 8b 3c 57 ee 3f 07 51 cd d6 e0 || ac 5a 07 a2 9a d3 2c f2

C.6.7 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, IE Present, Destination address is using Extended Address, Source address is using Extended Address. 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 || 87 7e 47 || fc ef 9a c3