IEEE P802.11
Wireless LANs

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
| Control frame protection test vectors |
| Date: 2025-09-12 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel  |  |  | po-kai.huang@intel.com |
| Danny Ben-Ari |  |  | danny.ben-ari@intel.com |
| Shapira Guy |  |  | guy.shapira@intel.com |
| Ido Ouzieli |  |  | ido.ouzieli@intel.com |
| Danny Alexander |  |  | danny.alexander@intel.com |
| Nehru Bhandaru | Broadcom |  |  | nehru.bhandaru@broadcom.com |
| Garima Bansal |  |  | garima.bansal@broadcom.com |

 |

Abstract

This submission proposes resolutions for the following comments from comment collection on P802.11-REVmf D1.0:

194

**Revision History:**

R0: Initial version.

# CID xxxx

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page.Line** | **Comment** | **Proposed Change** | **Resolution** |
| 194 | Annex J | 6767.01 | Suggest to add test vectors of CFP. At least 2 examples for Trigger frame, 2 examples for MBA, and 2 examples for BAR. | Contribution 11-25-1442 will be submitted to resolve this CID. | **REVISED –**Agree in principle with the commenter. Instruction to TGmf Editor:Implement the proposed text updates in this document. |

## Proposed Text:

**TGmf Editor: *Instruction: Insert new subclause to Annex J as shown below:***

**J.15 Control frame protection test vectors**

**J.15.1 CIP with Trigger frame**

**======= CIP-GMAC-256 with EHT variant Basic Trigger frame without padding==========**

FC = 24 00

DUR = 20 06

RA = 48 1a e9 28 4b 88

TA = 1a f4 1d 73 20 8f

Common Info = 80 47 a4 b9 08 00 00 3f

Special User = d7 07 a2 ff 0f 00

User Info = 1f 25 21 4c 4a 84

PN User Info 1 = d9 07 fd 0c 1f 00

PN User Info 2 = d9 07 b7 e3 f3 00

MIC User Info 1 = da 07 6e b7 50 00

MIC User Info 2 = da 07 1c 59 db 00

MIC User Info 3 = da 07 5d b3 23 00

MIC User Info 4 = da 07 b7 39 25 00

MIC User Info 5 = da 07 84 a4 e7 00

MIC User Info 6 = da 07 fb 00 00 00

FCS = 07 bf 2e bd

Entire frame:

24 00 20 06 48 1a e9 28 4b 88 1a f4 1d 73 20 8f 80 47 a4 b9 08 00 00 3f d7 07 a2 ff 0f 00 1f 25 21 4c 4a 84 d9 07 fd 0c 1f 00 d9 07 b7 e3 f3 00 da 07 6e b7 50 00 da 07 1c 59 db 00 da 07 5d b3 23 00 da 07 b7 39 25 00 da 07 84 a4 e7 00 da 07 fb 00 00 00 07 bf 2e bd

key:

2b a7 27 f6 ea 53 ce 3b e8 14 c7 bb c0 b1 fa b6 39 01 0c 4b 62 9e 5b b7 c5 8d 33 ac 91 26 a6 a4

CIP AAD: 24 00 20 06 48 1a e9 28 4b 88 1a f4 1d 73 20 8f

payload:

80 47 a4 b9 08 00 00 3f d7 07 a2 ff 0f 00 1f 25 21 4c 4a 84 d9 07 fd 0c 1f 00 d9 07 b7 e3 f3 00

nonce:

1a f4 1d 73 20 8f f3 e3 b7 1f 0c fd

GMAC MIC: 6e b7 50 1c 59 db 5d b3 23 b7 39 25 84 a4 e7 fb

**======= CIP-GMAC-256 with EHT variant Basic Trigger frame with padding============**

FC = 24 00

DUR = 3c 00

RA = 00 00 18 01 02 00

TA = 00 00 18 e1 e2 00

Common Info = 80 08 9c 00 10 00 00 30

Special User = d7 87 00 c4 01 00

User Info = 89 91 b8 41 00 1c

PN User Info 1 = d9 07 df 30 fd 00

PN User Info 2 = d9 07 da 5b fb 00

MIC User Info 1 = da 07 7a 2f 59 00

MIC User Info 2 = da 07 11 ce 62 00

MIC User Info 3 = da 07 41 07 91 00

MIC User Info 4 = da 07 f3 f7 78 00

MIC User Info 5 = da 07 88 ce 7c 00

MIC User Info 6 = da 07 60 00 00 00

Padding = ff ff ff ff ff ff ff ff

FCS = db 31 3d ac

Entire frame:

24 00 3c 00 00 00 18 01 02 00 00 00 18 e1 e2 00 80 08 9c 00 10 00 00 30 d7 87 00 c4 01 00 89 91 b8 41 00 1c d9 07 df 30 fd 00 d9 07 da 5b fb 00 da 07 7a 2f 59 00 da 07 11 ce 62 00 da 07 41 07 91 00 da 07 f3 f7 78 00 da 07 88 ce 7c 00 da 07 60 00 00 00 ff ff ff ff ff ff ff ff db 31 3d ac

Key:

40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 44 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 44

CIP AAD:

24 00 3c 00 00 00 18 01 02 00 00 00 18 e1 e2 00

payload:

80 08 9c 00 10 00 00 30 d7 87 00 c4 01 00 89 91 b8 41 00 1c d9 07 df 30 fd 00 d9 07 da 5b fb 00

nonce:

00 00 18 e1 e2 00 fb 5b da fd 30 df

GMAC MIC:

7a 2f 59 11 ce 62 41 07 91 f3 f7 78 88 ce 7c 60

**J.15.2 CIP with Multi-STA BlockAck frame**

**======= CIP-GMAC-256 with individually addressed Multi-STA BlockAck frame =========**

FC = 94 00

DUR = 0000

RA = 84 D9 d7 7b d3 96

TA = b6 f1 30 21 cd 1f

BA Control = 36 00

AID TID Info = 5f 32

BA SSC = 10 4f

BA Bitmap = ff 03 00 00 00 00 00 00

AID TID Info = d9 07

BA SSC = 04 00

PN = 5a 5f 9c 40 28 f8

MIC = 0c f9 45 42 21 45 81 d5 46 c2 81 2e 61 75 b4 34

Reserved = 00 00 00 00 00 00 00 00 00 00

AID TID Info = ff 07

BA SSC = 00 00

Padding = ff ff ff ff ff ff ff ff

FCS = 5b 56 11 d8

Entire frame:

94 00 00 00 84 d9 d7 7b d3 96 b6 f1 30 21 cd 1f 36 00 5f 32 10 4f ff 03 00 00 00 00 00 00 d9 07 04 00 5a 5f 9c 40 28 f8 0c f9 45 42 21 45 81 d5 46 c2 81 2e 61 75 b4 34 00 00 00 00 00 00 00 00 00 00 ff 07 00 00 ff ff ff ff ff ff ff ff 5b 56 11 d8

key:

84 3f 8b 5e 97 8f af be 28 03 cc f2 6a 8e 03 98 e8 b8 00 63 d0 c7 4b ca 5f 61 98 b6 63 80 12 34

CIP AAD: 94 00 00 00 84 d9 d7 7b d3 96 b6 f1 30 21 cd 1f

payload: 36 00 5f 32 10 4f ff 03 00 00 00 00 00 00 d9 07 04 00 5a 5f 9c 40 28 f8

nonce: b6 f1 30 21 cd 1f f8 28 40 9c 5f 5a

GMAC MIC: 0c f9 45 42 21 45 81 d5 46 c2 81 2e 61 75 b4 34

**======= CIP-GMAC-256 with group addressed Multi-STA BlockAck frame ============**

FC = 94 00

DUR = 00 00

RA = ff ff ff ff ff ff

TA = 01 00 18 e1 e2 00

BA Control = 16 00

AID TID Info = d6 57

BA SSC = 10 42

BA Bitmap = 62 c2 98 a0 32 0d 73 6b

AID TID Info = d6 67

BA SSC = 32 3e

BA Bitmap = 12 cc 68 40 c2 dc 1d ab 1f 03 98 7d ad ee 54 c2

AID TID Info = 89 01

BA SSC = 00 00

BA Bitmap = 0f 00 00 00 00 00 00 00

AID TID Info = d9 07

BA SSC = 04 00

PN = 96 28 5d bf c0 f7
MIC = f9 e5 83 8c bc 33 47 5f fb 6e 3a 9b 14 af 34 ab

Reserved = 00 00 00 00 00 00 00 00 00 00

AID TID Info = ff 07

BA SSC = 00 00

Padding = ff ff ff ff ff ff ff ff

FCS = 0f df d5 73

Entire frame:

94 00 00 00 ff ff ff ff ff ff 01 00 18 e1 e2 00 16 00 d6 57 10 42 62 c2 98 a0 32 0d 73 6b d6 67 32 3e 12 cc 68 40 c2 dc 1d ab 1f 03 98 7d ad ee 54 c2 89 01 00 00 0f 00 00 00 00 00 00 00 d9 07 04 00 96 28 5d bf c0 f7 f9 e5 83 8c bc 33 47 5f fb 6e 3a 9b 14 af 34 ab 00 00 00 00 00 00 00 00 00 00 ff 07 00 00 ff ff ff ff ff ff ff ff 0f df d5 73

key:

40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 44 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 44

CIP AAD:

94 00 00 00 ff ff ff ff ff ff 01 00 18 e1 e2 00

payload:

16 00 d6 57 10 42 62 c2 98 a0 32 0d 73 6b d6 67 32 3e 12 cc 68 40 c2 dc 1d ab 1f 03 98 7d ad ee 54 c2 89 01 00 00 0f 00 00 00 00 00 00 00 d9 07 04 00 96 28 5d bf c0 f7

nonce:

01 00 18 e1 e2 00 f7 c0 bf 5d 28 96

GMAC MIC:

f9 e5 83 8c bc 33 47 5f fb 6e 3a 9b 14 af 34 ab

**J.15.3 CIP with BlockAckReq frame**

**======= CIP-GMAC-256 with Compressed BlockAckReq frame without padding============**

FC = 84 00

DUR = 2c 00

RA = 80 6f f6 d3 89 ca

TA = 10 da db a0 7c 6a

BAR Control = 24 10

BAR Info = 80 34

PN = 42 c8 bd ee 6b f8

MIC = 4d b3 d2 7e 03 f2 e4 8d 98 b7 b3 a5 67 be 3d ba

FCS = 30 68 0a af

Entire frame:

84 00 2c 00 80 6f f6 d3 89 ca 10 da db a0 7c 6a 24 10 80 34 42 c8 bd ee 6b f8 4d b3 d2 7e 03 f2

e4 8d 98 b7 b3 a5 67 be 3d ba 30 68 0a af

key: 77 16 cc ce fb 66 40 55 b9 9b 2a d7 85 23 9c 53 4a e0 4d 95 9e c7 af d9 d5 60 cc bf ee c2 e7 0b

CIP AAD: 84 00 2c 00 80 6f f6 d3 89 ca 10 da db a0 7c 6a

payload: 24 10 80 34 42 c8 bd ee 6b f8

nonce: 10 da db a0 7c 6a f8 6b ee bd c8 42

GMAC MIC:

4d b3 d2 7e 03 f2 e4 8d 98 b7 b3 a5 67 be 3d ba

**======= CIP-GMAC-256 with Compressed BlockAckReq frame with padding============**

FC = 84 00

DUR = 28 00

RA = 00 00 18 01 02 00

TA = 00 00 18 e1 e2 00

BA Control = 24 00

BAR Info = 80 00

PN = d6 87 82 c6 d9 fc

MIC = fb 6d 92 b4 b0 f7 1a cf 71 cb ec a3 d7 3d 85 26

Padding = ff ff ff ff

FCS = 47 58 ce e2

Entire frame:

84 00 28 00 00 00 18 01 02 00 00 00 18 e1 e2 00 24 00 80 00 d6 87 82 c6 d9 fc fb 6d 92 b4 b0 f7 1a cf 71 cb ec a3 d7 3d 85 26 ff ff ff ff 47 58 ce e2

Key:

40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 44 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 44

CIP AAD:

84 00 28 00 00 00 18 01 02 00 00 00 18 e1 e2 00

Payload:

24 00 80 00 d6 87 82 c6 d9 fc

Nonce:

00 00 18 e1 e2 00 fc d9 c6 82 87 d6

GMAC MIC:

fb 6d 92 b4 b0 f7 1a cf 71 cb ec a3 d7 3d 85 26