MACsec GCM-AES Test Vectors

April 11, 2011

Provided for IEEE P802.1 Security Task Group
consideration by Karen Randall

Contents

1 Overview

This document provides a set of test vectors designed to demonstrate the use of GCM-AES encryption [1] within the MACsec protocol [2]. A number of packet sizes will be examined. The test data provided will include examples for GCM-AES-128 and GCM-AES-256. These examples include authentication only test data as well as confidentiality with authentication test data.

2 Test Data

In this section we will document the operation of Galois/Counter mode (GCM) on a number of different data sizes. In the examples that follow a data set will be specified. This data set will then be processed through the GCM module first using a 128-bit AES encryption key. The example will then be repeated using a 256-bit AES encryption key. Examples demonstrating the authentication only and confidentiality with authentication capabilities of GCM-AES are provided.

The examples presented here will use the notation developed in [1]. These conventions are summarized in Table 2.1. These conventions are also followed in [2].

K	The AES key (either 128-bit or 256-bit)
IV	initial value used by GCM
A	additional authenticated data
P	plaintext (user data)
C	encrypted data
T	integrity check value (ICV)

Table 2.1: GCM-AES Notation

In the examples provided we will follow the practices set forth in the MACsec standard [2].

Authentication without Encryption:

- A is MAC DA, MAC SA, SecTAG, and the user data concatenated in this order.
- P is null (which implies that C is null).
- The secure data used to form the output packet is the user data unmodified.

Confidentiality with Authentication:

- A is MAC DA, MAC SA, and SecTAG concatenated in this order.
- P is the user data.
- The secure data C is the encrypted data.

In each of the examples that follows we will associate the IP EtherType with the user data to form a single data unit. This will simplify our description of the GCM processing. We will not describe the data elements used to construct the MACsec packets in complete detail. For the complete details of the flags and encoding used in the MACsec data we refer the reader to [2].

The MACsec packets used in these examples are identical to those presented in [3].

2.1 54-byte Packet Authentication

This 54-byte example begins with an IP packet containing a 6-byte destination address, a 6-byte source address, and 42 bytes of user data (including the IP EtherType). These values are shown in Table 2.2. Table 2.3 contains the MACsec data elements required to process the packet. This packet will be processed to provide authentication only; no data confidentiality will be provided.

Field	Value
MAC DA	D6 09 B1 F0 56 63
MAC SA	7A 0D 46 DF 99 8D
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 00 01

Table 2.2: Input Data Elements

The input packet before MACsec processing is:

```
D609B1F0 56637A0D 46DF998D 08000F10
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 0001
```

The security tag consists of the MACsec EtherType, the TCI, the AN, the SL, the PN, and the optional SCI.

Field	Value
MAC DA	D6 09 B1 F0 56 63
MAC SA	7A 0D 46 DF 99 8D
MACsec EtherType	88 E5
TCI and AN	22
SL	2A
PN	B2 C2 84 65
SCI	12 15 35 24 C0 89 5E 81
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 00 01

Table 2.3: MACsec Data Elements

```
88E5222A B2C28465 12153524 C0895E81
```

The additional data A to be authenticated is formed by concatenating the MAC DA, the MAC SA, the security tag, and the user data. This input is then processed through the authentication only operation of the GCM module. A is shown below.

```
D609B1F0 56637A0D 46DF998D 88E5222A
B2C28465 12153524 C0895E81 08000F10
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 0001
```

The SCI and the PN form the 96-bit IV used by GCM within MACsec.

```
12153524 C0895E81 B2C28465
```

This authentication process is shown in sections 2.1.1 and 2.1.2.

2.1.1 54-byte Packet Authentication Using GCM-AES-128

This example performs authentication without confidentiality using GCM-AES-128. This process produces a 128-bit integrity check value (ICV).

```
key size = 128 bits
```

```
P: 0 bits
A: 560 bits
IV: 96 bits
ICV: 128 bits

Key:
AD7A2BD03EAC835A6F620FDCB506B345

P:

A:
D609B1F056637A0D46DF998D88E5222A
B2C2846512153524C0895E8108000F10
1112131415161718191A1B1C1D1E1F20
2122232425262728292A2B2C2D2E2F30
313233340001

IV:
12153524C0895E81B2C28465

GCM-AES Authentication
H: 73A23D80121DE2D5A850253FCF43120E
Y[0]: 12153524C0895E81B2C2846500000001
E(K,Y[0]): EB4E051CB548A6B5490F6F11A27CB7D0
X[1]: 6B0BE68D67C6EE03EF7998E399C01CA4
X[2]: 5AABADF6D7806EC0CCCB028441197B22
X[3]: FE072BFE2811A68AD7FDB0687192D293
X[4]: A47252D1A7E09B49FB356E435DBB4CD0
X[5]: 18EBF4C65CE89BF69EFB4981CEE13DB9
GHASH(H,A,C): 1BDA7DB505D8A165264986A703A6920D

C:

T: F09478A9B09007D06F46E9B6A1DA25DD

ICV: F09478A9B09007D06F46E9B6A1DA25DD
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the unmodified user data, and the ICV.

```
D609B1F0 56637A0D 46DF998D 88E5222A
```

```
B2C28465 12153524 C0895E81 08000F10
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 0001F094 78A9B090 07D06F46
E9B6A1DA 25DD
```

2.1.2 54-byte Packet Authentication Using GCM-AES-256

This example performs authentication without confidentiality using GCM-AES-256. This process produces a 128-bit integrity check value (ICV).

```
key size = 256 bits
P: 0 bits
A: 560 bits
IV: 96 bits
ICV: 128 bits

Key:
E3C08A8F06C6E3AD95A70557B23F7548
3CE33021A9C72B7025666204C69C0B72

P:

A:
D609B1F056637A0D46DF998D88E5222A
B2C2846512153524C0895E8108000F10
1112131415161718191A1B1C1D1E1F20
2122232425262728292A2B2C2D2E2F30
313233340001

IV:
12153524C0895E81B2C28465

GCM-AES Authentication
H: 286D73994EA0BA3CFD1F52BF06A8ACF2
Y[0]: 12153524C0895E81B2C2846500000001
E(K,Y[0]): 714D54FDCFCEE37D5729CDDAB383A016
X[1]: BA7C26F578254853CF321281A48317CA
X[2]: 2D0DF59AE78E84ED64C3F85068CD9863
X[3]: 702DE0382ABF4D42DD62B8F115124219
X[4]: DAED65979342F0D155BFDFE362132078
```

```
X[5]: 9AB4AFD6344654B2CD23977E41AA18B3
GHASH(H,A,C): 5E4691528F50E5AB5EC346A7BC264A46

C:

T: 2F0BC5AF409E06D609EA8B7D0FA5EA50

ICV: 2F0BC5AF409E06D609EA8B7D0FA5EA50
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the unmodified user data, and the ICV.

```
D609B1F0 56637A0D 46DF998D 88E5222A
B2C28465 12153524 C0895E81 08000F10
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 00012F0B C5AF409E 06D609EA
8B7D0FA5 EA50
```

2.2 60-byte Packet Encryption

This 60-byte example begins with an IP packet containing a 6-byte destination address, a 6-byte source address, and 48 bytes of user data (including the IP EtherType). These values are shown in Table 2.4. Table 2.5 contains the MACsec data elements required to process the packet. This packet will be processed to provide both confidentiality and authentication.

Field	Value
MAC DA	D6 09 B1 F0 56 63
MAC SA	7A 0D 46 DF 99 8D
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 00 02

Table 2.4: Input Data Elements

The input packet before MACsec processing is:

```
D609B1F0 56637A0D 46DF998D 08000F10
```

```
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 35363738 393A0002
```

Field	Value
MAC DA	D6 09 B1 F0 56 63
MAC SA	7A 0D 46 DF 99 8D
MACsec EtherType	88 E5
TCI and AN	2E
SL	00
PN	B2 C2 84 65
SCI	12 15 35 24 C0 89 5E 81
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 00 02

Table 2.5: MACsec Data Elements

P, the user data to be encrypted, is extracted as:

```
08000F10 11121314 15161718 191A1B1C
1D1E1F20 21222324 25262728 292A2B2C
2D2E2F30 31323334 35363738 393A0002
```

The security tag consists of the MACsec EtherType, the TCI, the AN, the SL, the PN and the optional SCI.

```
88E52E00 B2C28465 12153524 C0895E81
```

The additional data A to be authenticated is formed by joining the MAC DA, the MAC SA, and the security tag. A is shown below.

```
D609B1F0 56637A0D 46DF998D 88E52E00
B2C28465 12153524 C0895E81
```

This additional data will be processed with the encrypted data to form the integrity check value (ICV) as specified in [1].

The SCI and the PN form the 96-bit IV used by GCM within MACsec.

```
12153524 C0895E81 B2C28465
```

The results of the encryption operations are shown in sections 2.2.1 and 2.2.2.

2.2.1 60-Byte Packet Encryption Using GCM-AES-128

This example performs authenticated encryption using GCM-AES-128. It produces a 128-bit integrity check value (ICV).

```
key size = 128 bits
P: 384 bits
A: 224 bits
IV: 96 bits
ICV: 128 bits

Key:
AD7A2BD03EAC835A6F620FDCB506B345

P:
08000F101112131415161718191A1B1C
1D1E1F202122232425262728292A2B2C
2D2E2F303132333435363738393A0002

A:
D609B1F056637A0D46DF998D88E52E00
B2C2846512153524C0895E81

IV:
12153524C0895E81B2C28465

GCM-AES Encryption
H: 73A23D80121DE2D5A850253FCF43120E
Y[0]: 12153524C0895E81B2C2846500000001
E(K,Y[0]): EB4E051CB548A6B5490F6F11A27CB7D0
Y[1]: 12153524C0895E81B2C2846500000002
E(K,Y[1]): 781AF50CD12BD3C370049D7E44B17238
C[1]: 701AFA1CC039C0D765128A665DAB6924
Y[2]: 12153524C0895E81B2C2846500000003
E(K,Y[2]): 2587A05339EEFFA5ECB53A895694A5F1
C[2]: 3899BF7318CCDC81C9931DA17FBE8EDD
```

```
Y[3]: 12153524C0895E81B2C2846500000004
E(K,Y[3]): 5039E4BB7D14CFB5D61E78134680713F
C[3]: 7D17CB8B4C26FC81E3284F2B7FBA713D
X[1]: 9CABBD91899C1413AA7AD629C1DF12CD
X[2]: B99ABF6BDBD18B8E148F8030F0686F28
X[3]: 8B5BD74B9A65A459150392C3872BCE7F
X[4]: 934E9D58C59230EE652675D0FF4FB255
X[5]: 4738D208B10FAFF24D6DFBDDC916DC44
GHASH(H,A,C): A4C350FB66B8C960E83363381BA90F50

C:
701AFA1CC039C0D765128A665DAB6924
3899BF7318CCDC81C9931DA17FBE8EDD
7D17CB8B4C26FC81E3284F2B7FBA713D

T: 4F8D55E7D3F06FD5A13C0C29B9D5B880

ICV: 4F8D55E7D3F06FD5A13C0C29B9D5B880
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the encrypted user data, and the ICV.

```
D609B1F0 56637A0D 46DF998D 88E52E00
B2C28465 12153524 C0895E81 701AFA1C
C039C0D7 65128A66 5DAB6924 3899BF73
18CCDC81 C9931DA1 7FBE8EDD 7D17CB8B
4C26FC81 E3284F2B 7FBA713D 4F8D55E7
D3F06FD5 A13C0C29 B9D5B880
```

2.2.2 60-byte Packet Encryption Using GCM-AES-256

This example performs authenticated encryption using GCM-AES-256. It produces a 128-bit integrity check value (ICV).

```
key size = 256 bits
P: 384 bits
A: 224 bits
IV: 96 bits
ICV: 128 bits
```

Key:
E3C08A8F06C6E3AD95A70557B23F7548
3CE33021A9C72B7025666204C69C0B72

P:
08000F101112131415161718191A1B1C
1D1E1F202122232425262728292A2B2C
2D2E2F303132333435363738393A0002

A:
D609B1F056637A0D46DF998D88E52E00
B2C2846512153524C0895E81

IV:
12153524C0895E81B2C28465

GCM-AES Encryption
H: 286D73994EA0BA3CFD1F52BF06A8ACF2
Y[0]: 12153524C0895E81B2C2846500000001
E(K,Y[0]): 714D54FDCFCEE37D5729CDDAB383A016
Y[1]: 12153524C0895E81B2C2846500000002
E(K,Y[1]): EA0061A43E406416388D0E8A42DE02CB
C[1]: E2006EB42F5277022D9B19925BC419D7
Y[2]: 12153524C0895E81B2C2846500000003
E(K,Y[2]): B88C794CB37DC1CB54A893CB21C5C18B
C[2]: A592666C925FE2EF718EB4E308EFEAA7
Y[3]: 12153524C0895E81B2C2846500000004
E(K,Y[3]): E8091409702AB53E6ED49E476F917834
C[3]: C5273B394118860A5BE2A97F56AB7836
X[1]: D62D2B0792C282A27B82C3731ABCB7A1
X[2]: 841068CDEDA878030E644F03743927D0
X[3]: 224CE5247BE62FB2AC5932EFAC5D1991
X[4]: EB66718E589AB6472880D1A2C908CB72
X[5]: 6D109A3C7F34085754FDDFF0EB5D4595
GHASH(H,A,C): 2DE8C33074F038F04D389C30B9741420

C:
E2006EB42F5277022D9B19925BC419D7
A592666C925FE2EF718EB4E308EFEAA7
C5273B394118860A5BE2A97F56AB7836

T: 5CA597CDBB3EDB8D1A1151EA0AF7B436

```
ICV: 5CA597CDBB3EDB8D1A1151EA0AF7B436
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the encrypted user data, and the ICV.

```
D609B1F0 56637A0D 46DF998D 88E52E00
B2C28465 12153524 C0895E81 E2006EB4
2F527702 2D9B1992 5BC419D7 A592666C
925FE2EF 718EB4E3 08EFEAA7 C5273B39
4118860A 5BE2A97F 56AB7836 5CA597CD
BB3EDB8D 1A1151EA 0AF7B436
```

2.3 60-byte Packet Authentication

This 60-byte example begins with an IP packet containing a 6-byte destination address, a 6-byte source address, and 48 bytes of user data (including the IP EtherType). These values are shown in Table 2.6. Table 2.7 contains the MACsec data elements required to process the packet. This packet will be processed to provide authentication only; no data confidentiality will be provided.

Field	Value
MAC DA	E2 01 06 D7 CD 0D
MAC SA	F0 76 1E 8D CD 3D
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 00 03

Table 2.6: Input Data Elements

The input packet before MACsec processing is:

```
E20106D7 CD0DF076 1E8DCD3D 08000F10
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 35363738 393A0003
```

The security tag consists of the MACsec EtherType, the TCI, the AN, the SL, and the PN. (The optional SCI is omitted.)

Field	Value
MAC DA	E2 01 06 D7 CD 0D
MAC SA	F0 76 1E 8D CD 3D
MACsec EtherType	88 E5
TCI and AN	40
SL	00
PN	76 D4 57 ED
SCI	F0 76 1E 8D CD 3D 00 01
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 00 03

Table 2.7: MACsec Data Elements

```
88e54000 76D457ED
```

The additional data A to be authenticated is formed by concatenating the MAC DA, the MAC SA, the security tag, and the user data. This input is then processed through the authentication only operation of the GCM module. A is shown below.

```
E20106D7 CD0DF076 1E8DCD3D 88E54000
76D457ED 08000F10 11121314 15161718
191A1B1C 1D1E1F20 21222324 25262728
292A2B2C 2D2E2F30 31323334 35363738
393A0003
```

The SCI and the PN form the 96-bit IV used by GCM within MACsec.

```
F0761E8D CD3D0001 76D457ED
```

This authentication process is shown in sections 2.3.1 and 2.3.2.

2.3.1 60-byte Packet Authentication Using GCM-AES-128

This example performs authentication without confidentiality using GCM-AES-128. This process produces a 128-bit integrity check value (ICV).

```
key size = 128 bits
```

```
P: 0 bits
A: 544 bits
IV: 96 bits
ICV: 128 bits

Key:
071B113B0CA743FECCCF3D051F737382

P:

A:
E20106D7CD0DF0761E8DCD3D88E54000
76D457ED08000F101112131415161718
191A1B1C1D1E1F202122232425262728
292A2B2C2D2E2F303132333435363738
393A0003

IV:
F0761E8DCD3D000176D457ED

GCM-AES Authentication
H: E4E01725D724C1215C7309AD34539257
Y[0]: F0761E8DCD3D000176D457ED00000001
E(K,Y[0]): FC25539100959B80FE3ABED435E54CAB
X[1]: 8DAD4981E33493018BB8482F69E4478C
X[2]: 5B0BFA3E67A3E080CB60EA3D523C734A
X[3]: 051F8D267A68CF88748E56C5F64EF503
X[4]: 4187F1240DB1887F2A92DDAB8903A0F6
X[5]: C7D64941A90F02FA9FCDECC083B4B276
GHASH(H,A,C): F02428563BB7E67C378044C874498FF8

C:

T: 0C017BC73B227DFCC9BAFA1C41ACC353

ICV: 0C017BC73B227DFCC9BAFA1C41ACC353
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the unmodified user data, and the ICV.

```
E20106D7 CD0DF076 1E8DCD3D 88E54000
```

```
76D457ED 08000F10 11121314 15161718
191A1B1C 1D1E1F20 21222324 25262728
292A2B2C 2D2E2F30 31323334 35363738
393A0003 0C017BC7 3B227DFC C9BAFA1C
41ACC353
```

2.3.2 60-byte Packet Authentication Using GCM-AES-256

This example performs authentication without confidentiality using GCM-AES-256. This process produces a 128-bit integrity check value (ICV).

```
key size = 256 bits
P: 0 bits
A: 544 bits
IV: 96 bits
ICV: 128 bits

Key:
691D3EE909D7F54167FD1CA0B5D76908
1F2BDE1AEE655FDBAB80BD5295AE6BE7

P:

A:
E20106D7CD0DF0761E8DCD3D88E54000
76D457ED08000F101112131415161718
191A1B1C1D1E1F202122232425262728
292A2B2C2D2E2F303132333435363738
393A0003

IV:
F0761E8DCD3D000176D457ED

GCM-AES Authentication
H: 1E693C484AB894B26669BC12E6D5D776
Y[0]: F0761E8DCD3D000176D457ED00000001
E(K,Y[0]): 87E183649AE3E7DBF725659152C39A22
X[1]: 20107B262134C35B60499E905C532004
X[2]: D7A468F455F09F947884E35A2C80CD7F
X[3]: A82D607070F2E4470FD94C0EECA9FCC1
X[4]: 03C3C8725883EB355963BD53B515C82D
```

```
X[5]: 8FF6F0311DDE274FFA936965C0C905B4
GHASH(H,A,C): B2C0FF13D15FD66DC643D96886687725

C:

T: 35217C774BBC31B63166BCF9D4ABED07

ICV: 35217C774BBC31B63166BCF9D4ABED07
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the unmodified user data, and the ICV.

```
E20106D7 CD0DF076 1E8DCD3D 88E54000
76D457ED 08000F10 11121314 15161718
191A1B1C 1D1E1F202 1222324 25262728
292A2B2C 2D2E2F303 1323334 35363738
393A0003 35217C774 BBC31B6 3166BCF9
D4ABED07
```

2.4 54-byte Packet Encryption

This 54-byte example begins with an IP packet containing a 6-byte destination address, a 6-byte source address, and 48 bytes of user data (including the IP EtherType). These values are shown in Table 2.8. Table 2.9 contains the MACsec data elements required to process the packet. This packet will be processed to provide both confidentiality and authentication.

Field	Value
MAC DA	E2 01 06 D7 CD 0D
MAC SA	F0 76 1E 8D CD 3D
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 00 04

Table 2.8: Input Data Elements

The input packet before MACsec processing is:

```
E20106D7 CD0DF076 1E8DCD3D 08000F10
```

```
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 0004
```

Field	Value
MAC DA	E2 01 06 D7 CD 0D
MAC SA	F0 76 1E 8D CD 3D
MACsec EtherType	88 E5
TCI and AN	4C
SL	2A
PN	76 D4 57 ED
SCI	F0 76 1E 8D CD 3D 00 01
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 00 04

Table 2.9: MACsec Data Elements

P, the user data to be encrypted, is extracted as:

```
08000F10 11121314 15161718 191A1B1C
1D1E1F20 21222324 25262728 292A2B2C
2D2E2F30 31323334 0004
```

The security tag consists of the MACsec EtherType, the TCI, the AN, the SL, and the PN. (The optional SCI is omitted.)

```
88E54C2A 76D457ED
```

The additional data A to be authenticated is formed by joining the MAC DA, the MAC SA, and the security tag. A is shown below.

```
E20106D7 CD0DF076 1E8DCD3D 88E54C2A
76D457ED
```

This additional data will be processed with the encrypted data to form the integrity check value (ICV) as specified in [1].

The SCI and the PN form the 96-bit IV used by GCM within MACsec.

```
F0761E8D CD3D0001 76D457ED
```

The results of the encryption operations are shown in sections 2.2.1 and 2.2.2.

2.4.1 54-byte Packet Encryption Using GCM-AES-128

This example performs authenticated encryption using GCM-AES-128. It produces a 128-bit integrity check value (ICV).

```
key size = 128 bits
P: 336 bits
A: 160 bits
IV: 96 bits
ICV: 128 bits

Key:
071B113B0CA743FECCCF3D051F737382

P:
08000F101112131415161718191A1B1C
1D1E1F202122232425262728292A2B2C
2D2E2F30313233340004

A:
E20106D7CD0DF0761E8DCD3D88E54C2A
76D457ED

IV:
F0761E8DCD3D000176D457ED

GCM-AES Encryption
H: E4E01725D724C1215C7309AD34539257
Y[0]: F0761E8DCD3D000176D457ED00000001
E(K,Y[0]): FC25539100959B80FE3ABED435E54CAB
Y[1]: F0761E8DCD3D000176D457ED00000002
E(K,Y[1]): 1BB4C83B298FD6159B64B669C49FBECF
C[1]: 13B4C72B389DC5018E72A171DD85A5D3
Y[2]: F0761E8DCD3D000176D457ED00000003
E(K,Y[2]): 683C6BF3813BD8EEC82F830DE4B10530
C[2]: 752274D3A019FBCAED09A425CD9B2E1C
```

```
Y[3]: F0761E8DCD3D000176D457ED00000004
E(K,Y[3]): B65CC1D7F8EC4E66B3F7182C2E358591
C[3]: 9B72EEE7C9DE7D52B3F3
X[1]: A0AE6DFAE25C0AE80E9A1AAC0D5123D3
X[2]: EAEA2A767986B7D5B9E6ED37A3CBC63B
X[3]: 8809F1263C02DC9BD09FDF0F34575BA6
X[4]: A173C5A2C03DE08C025C93945B2E74B7
X[5]: 65D113682551614E556BFAA80AA2FA7A
GHASH(H,A,C): 2A807BDE4AF8A462D467D2FFA3E1D868

C:
13B4C72B389DC5018E72A171DD85A5D3
752274D3A019FBCAED09A425CD9B2E1C
9B72EEE7C9DE7D52B3F3

T: D6A5284F4A6D3FE22A5D6C2B960494C3

ICV: D6A5284F4A6D3FE22A5D6C2B960494C3
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the encrypted user data, and the ICV.

```
E20106D7 CD0DF076 1E8DCD3D 88E54C2A
76D457ED 13B4C72B 389DC501 8E72A171
DD85A5D3 752274D3 A019FBCA ED09A425
CD9B2E1C 9B72EEE7 C9DE7D52 B3F3D6A5
284F4A6D 3FE22A5D 6C2B9604 94C3
```

2.4.2 54-byte Packet Encryption Using GCM-AES-256

This example performs authenticated encryption using GCM-AES-256. It produces a 128-bit integrity check value (ICV).

```
key size = 256 bits
P: 336 bits
A: 160 bits
IV: 96 bits
ICV: 128 bits

Key:
```

691D3EE909D7F54167FD1CA0B5D76908
1F2BDE1AEE655FDBAB80BD5295AE6BE7

P:
08000F101112131415161718191A1B1C
1D1E1F202122232425262728292A2B2C
2D2E2F30313233340004

A:
E20106D7CD0DF0761E8DCD3D88E54C2A
76D457ED

IV:
F0761E8DCD3D000176D457ED

GCM-AES Encryption
H: 1E693C484AB894B26669BC12E6D5D776
Y[0]: F0761E8DCD3D000176D457ED00000001
E(K,Y[0]): 87E183649AE3E7DBF725659152C39A22
Y[1]: F0761E8DCD3D000176D457ED00000002
E(K,Y[1]): C9623045621E80472581BAC2CB4C7F8A
C[1]: C1623F55730C93533097ADDAD2566496
Y[2]: F0761E8DCD3D000176D457ED00000003
E(K,Y[2]): 7C3B2A0B628F8F9944E3C812E02170C2
C[2]: 6125352B43ADACBD61C5EF3AC90B5BEE
Y[3]: F0761E8DCD3D000176D457ED00000004
E(K,Y[3]): BFB2CB533F95AC58E51D6608DBEBDBC2
C[3]: 929CE4630EA79F6CE519
X[1]: F268EF5B38A96261A139D06CD7F43A33
X[2]: 9AE3BF42A20F4FB773EEFD5B5C5DBDD3
X[3]: 22A7FA0F7E5FC49715374D6B72EC7FBB
X[4]: 2FE103C6651C845A71217C1C7E80D559
X[5]: FA94D93A0A7D235AEED7891F5E381A17
GHASH(H,A,C): 954EBAA64B1E25DEE8AE1EADCFFAE4D0

C:
C1623F55730C93533097ADDAD2566496
6125352B43ADACBD61C5EF3AC90B5BEE
929CE4630EA79F6CE519

T: 12AF39C2D1FDC2051F8B7B3C9D397EF2

```
ICV: 12AF39C2D1FDC2051F8B7B3C9D397EF2
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the encrypted user data, and the ICV.

```
E20106D7 CD0DF076 1E8DCD3D 88E54C2A
76D457ED C1623F55 730C9353 3097ADDA
D2566496 6125352B 43ADACBD 61C5EF3A
C90B5BEE 929CE463 0EA79F6C E519
```

2.5 65-byte Packet Authentication

This 65-byte example begins with an IP packet containing a 6-byte destination address, a 6-byte source address, and 53 bytes of user data (including the IP EtherType). These values are shown in Table 2.10. Table 2.11 contains the MACsec data elements required to process the packet. This packet will be processed to provide authentication only; no data confidentiality will be provided.

Field	Value
MAC DA	84 C5 D5 13 D2 AA
MAC SA	F6 E5 BB D2 72 77
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 00 05

Table 2.10: Input Data Elements

The input packet before MACsec processing is:

```
84C5D513 D2AAF6E5 BBD27277 08000F10
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 35363738 393A3B3C 3D3E3F00
05
```

The security tag consists of the MACsec EtherType, the TCI, the AN, the SL, the PN, and the optional SCI.

Field	Value
MAC DA	84 C5 D5 13 D2 AA
MAC SA	F6 E5 BB D2 72 77
MACsec EtherType	88 E5
TCI and AN	23
SL	00
PN	89 32 D6 12
SCI	7C FD E9 F9 E3 37 24 C6
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 00 05

Table 2.11: MACsec Data Elements

```
88E52300 8932D612 7CFDE9F9 E33724C6
```

The additional data A to be authenticated is formed by concatenating the MAC DA, the MAC SA, the security tag, and the user data. This input is then processed through the authentication only operation of the GCM module. A is shown below:

```
84C5D513D2AAF6E5BBD2727788E52300
8932D6127CFDE9F9E33724C608000F10
111213141516171819 1A1B1C1D1E1F20
212223242526272829 2A2B2C2D2E2F30
313233343536373839 3A3B3C3D3E3F00
05
```

The SCI and the PN form the 96-bit IV used by GCM within MACsec.

```
7CFDE9F9 E33724C6 8932D612
```

This authentication process is shown in sections 2.5.1 and 2.5.2.

2.5.1 65-byte Packet Authentication Using GCM-AES-128

This example performs authentication without confidentiality using GCM-AES-128. This process produces a 128-bit integrity check value (ICV).

```
key size = 128 bits
P: 0 bits
A: 648 bits
IV: 96 bits
ICV: 128 bits

Key:
013FE00B5F11BE7F866D0CBBC55A7A90

P:

A:
84C5D513D2AAF6E5BBD2727788E52300
8932D6127CFDE9F9E33724C608000F10
111213141516171819 1A1B1C1D1E1F20
212223242526272829 2A2B2C2D2E2F30
313233343536373839 3A3B3C3D3E3F00
05

IV:
7CFDE9F9E33724C68932D612

GCM-AES Authentication
H: EB28DCB361EE1110F98CA0C9A07C88F7
Y[0]: 7CFDE9F9E33724C68932D61200000001
E(K,Y[0]): 4EAAF8E4DF948ACAC7F3349C1006A91F
X[1]: 279344E391DB8834EFA68FD3F1BA5CD8
X[2]: DC35B123F4D387BBB076D0822BD60816
X[3]: 8AB3B52963CC15C9C2DB3E4C801CB65A
X[4]: CAB6A261225F42578E6B86ABA9F0DD18
X[5]: 6ABDBB3ECAC0458F116A82AA0DAC563F
X[6]: 8F39EF45985C691E35814202B6BB6EF6
GHASH(H,A,C): 6FD29F01D3B927BE057F0FCCBBD9C045

C:

T: 217867E50C2DAD74C28C3B50ABDF695A

ICV: 217867E50C2DAD74C28C3B50ABDF695A
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the unmodified user data, and the ICV.

```
84C5D513 D2AAF6E5 BBD27277 88E52300
8932D612 7CFDE9F9 E33724C6 08000F10
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 35363738 393A3B3C 3D3E3F00
05217867 e50c2dad 74c28c3b 50abdf69
5a
```

2.5.2 65-byte Packet Authentication Using GCM-AES-256

This example performs authentication without confidentiality using GCM-AES-256. This process produces a 128-bit integrity check value (ICV).

```
key size = 256 bits
P: 0 bits
A: 648 bits
IV: 96 bits
ICV: 128 bits

Key:
83C093B58DE7FFE1C0DA926AC43FB360
9AC1C80FEE1B624497EF942E2F79A823

P:

A:
84C5D513D2AAF6E5BBD2727788E52300
8932D6127CFDE9F9E33724C608000F10
1112131415161718191A1B1C1D1E1F20
2122232425262728292A2B2C2D2E2F30
3132333435363738393A3B3C3D3E3F00
05

IV:
7CFDE9F9E33724C68932D612

GCM-AES Authentication
H: D03D3B51FDF2AACB3A165D7DC362D929
Y[0]: 7CFDE9F9E33724C68932D61200000001
E(K,Y[0]): E97EA8EE4455AE79EC4225CAC340E326
X[1]: 22C28F4DF8D09267EA3E11F019F5932C
```

```
X[2]: 3D02CFE5FC6A8A9E65B8FFD63E525083
X[3]: 78466AE4A3490819A08645DDC95B143B
X[4]: 6FE4921A6F0A1D5DD90A100A40206142
X[5]: C880DEC2FF2C44F8AD611692AF6D1069
X[6]: CF4D709A4D020BA876F4371BAA788444
GHASH(H,A,C): 879FC806BEB90ACA80C497FE514C4A53

C:

T: 6EE160E8FAECA4B36C86B234920CA975

ICV: 6EE160E8FAECA4B36C86B234920CA975
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the unmodified user data, and the ICV.

```
84C5D513 D2AAF6E5 BBD27277 88E52300
8932D612 7CFDE9F9 E33724C6 08000F10
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 35363738 393A3B3C 3D3E3F00
056EE160 E8FAECA4 B36C86B2 34920CA9
75
```

2.6 61-byte Packet Encryption

This 61-byte example begins with an IP packet containing a 6-byte destination address, a 6-byte source address, and 49 bytes of user data (including the IP EtherType). These values are shown in Table 2.12. Table 2.13 contains the MACsec data elements required to process the packet. This packet will be processed to provide both confidentiality and authentication.

The input packet before MACsec processing is:

```
84C5D513 D2AAF6E5 BBD27277 08000F10
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 35363738 393A3B00 06
```

P, the user data to be encrypted, is extracted as:

Field	Value
MAC DA	84 C5 D5 13 D2 AA
MAC SA	F6 E5 BB D2 72 77
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 00 06

Table 2.12: Input Data Elements

Field	Value
MAC DA	84 C5 D5 13 D2 AA
MAC SA	F6 E5 BB D2 72 77
MACsec EtherType	88 E5
TCI and AN	2F
SL	00
PN	89 32 D6 12
SCI	7C FD E9 F9 E3 37 24 C6
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 00 06

Table 2.13: MACsec Data Elements

```
08000F10 11121314 15161718 191A1B1C
1D1E1F20 21222324 25262728 292A2B2C
2D2E2F30 31323334 35363738 393A3B00
06
```

The security tag consists of the MACsec EtherType, the TCI, the AN, the SL, the PN, and the optional SCI.

```
88E52F00 8932D612 7CFDE9F9 E33724C6
```

The additional data A to be authenticated is formed by joining the MAC DA, the MAC SA, and the security tag. A is shown below.

```
84C5D513 D2AAF6E5 BBD27277 88E52F00
```

```
8932D612 7CFDE9F9 E33724C6
```

This additional data will be processed with the encrypted data to form the integrity check value (ICV) as specified in [1].

The SCI and the PN form the 96-bit IV used by GCM within MACsec.

```
7CFDE9F9 E33724C6 8932D612
```

The results of the encryption operations are shown in sections 2.6.1 and 2.6.2.

2.6.1 61-byte Packet Encryption Using GCM-AES-128

This example performs authenticated encryption using GCM-AES-128. It produces a 128-bit integrity check value (ICV).

```
key size = 128 bits
P: 392 bits
A: 224 bits
IV: 96 bits
ICV: 128 bits

Key:
013FE00B5F11BE7F866D0CBBC55A7A90

P:
08000F101112131415161718191A1B1C
1D1E1F202122232425262728292A2B2C
2D2E2F303132333435363738393A3B00
06

A:
84C5D513D2AAF6E5BBD2727788E52F00
8932D6127CFDE9F9E33724C6

IV:
7CFDE9F9E33724C68932D612

GCM-AES Encryption
H: EB28DCB361EE1110F98CA0C9A07C88F7
```

```
Y[0]: 7CFDE9F9E33724C68932D61200000001
E(K,Y[0]): 4EAAF8E4DF948ACAC7F3349C1006A91F
Y[1]: 7CFDE9F9E33724C68932D61200000002
E(K,Y[1]): 324DE9EA230B0300CEA514C137F9B2F4
C[1]: 3A4DE6FA32191014DBB303D92EE3A9E8
Y[2]: 7CFDE9F9E33724C68932D61200000003
E(K,Y[2]): BCAB86E16C00D82C25B0C61038AB4110
C[2]: A1B599C14D22FB080096E13811816A3C
Y[3]: 7CFDE9F9E33724C68932D61200000004
E(K,Y[3]): B1B5E04C2AA9A5EEB5A433DAA4341176
C[3]: 9C9BCF7C1B9B96DA809204E29D0E2A76
Y[4]: 7CFDE9F9E33724C68932D61200000005
E(K,Y[4]): 44491285F0FCF957EB73F79AC5D4E273
C[4]: 42
X[1]: BA7749648FCB954F95B5933AC87D5AA3
X[2]: A78C78463850956BF8939E6D8314DED1
X[3]: 18EB5A2C2541C14DD668468C26D2CD8A
X[4]: 32C49AA9AD2B7025767B14F37740A2E8
X[5]: 59CEE3A487F7ACAA9531883B31B11561
X[6]: 3FC125EEEC404708A0D8B9998FE0DE9B
GHASH(H,A,C): F179E8405CE80BA6085698BFBB069097

C:
3A4DE6FA32191014DBB303D92EE3A9E8
A1B599C14D22FB080096E13811816A3C
9C9BCF7C1B9B96DA809204E29D0E2A76
42

T: BFD310A4837C816CCFA5AC23AB003988

ICV: BFD310A4837C816CCFA5AC23AB003988
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the encrypted user data, and the ICV.

```
84C5D513 D2AAF6E5 BBD27277 88E52F00
8932D612 7CFDE9F9 E33724C6 3A4DE6FA
32191014 DBB303D9 2EE3A9E8 A1B599C1
4D22FB08 0096E138 11816A3C 9C9BCF7C
1B9B96DA 809204E2 9D0E2A76 42BFD310
A4837C81 6CCFA5AC 23AB0039 88
```

2.6.2 61-byte Packet Encryption Using GCM-AES-256

This example performs authenticated encryption using GCM-AES-256. It produces a 128-bit integrity check value (ICV).

```
key size = 256 bits
P: 392 bits
A: 224 bits
IV: 96 bits
ICV: 128 bits

Key:
83C093B58DE7FFE1C0DA926AC43FB360
9AC1C80FEE1B624497EF942E2F79A823

P:
08000F101112131415161718191A1B1C
1D1E1F202122232425262728292A2B2C
2D2E2F303132333435363738393A3B00
06

A:
84C5D513D2AAF6E5BBD2727788E52F00
8932D6127CFDE9F9E33724C6

IV:
7CFDE9F9E33724C68932D612

GCM-AES Encryption
H: D03D3B51FDF2AACB3A165D7DC362D929
Y[0]: 7CFDE9F9E33724C68932D61200000001
E(K,Y[0]): E97EA8EE4455AE79EC4225CAC340E326
Y[1]: 7CFDE9F9E33724C68932D61200000002
E(K,Y[1]): 19022DEF9142D8F8F37C9622C98068F1
C[1]: 110222FF8050CBECE66A813AD09A73ED
Y[2]: 7CFDE9F9E33724C68932D61200000003
E(K,Y[2]): 678417BC3149B6B7AC30A9FEC143A585
C[2]: 7A9A089C106B959389168ED6E8698EA9
Y[3]: 7CFDE9F9E33724C68932D61200000004
E(K,Y[3]): 2FC53D47EADE1D5CD14522622C9DE1EE
C[3]: 02EB1277DBEC2E68E473155A15A7DAEE
```

```
Y[4]: 7CFDE9F9E33724C68932D61200000005
E(K,Y[4]): D2541F9E6E5ABAB19C0341912287646B
C[4]: D4
X[1]: 0B75EC495656426640FD4E24ABA3ED1E
X[2]: 4BC3618F5864A86E9F4EE84504DE347C
X[3]: F67E393EC69D2D6FFD54C4EFA6F5FF88
X[4]: C7FE302C946CC29D1EFAAA22B7F587DD
X[5]: 87FCCA374A2EAFC6FD08FE08F919FB8E
X[6]: 0A648461F8E051A0B03165459D5E6F59
GHASH(H,A,C): 4871E6EB57C98DA6ECF18F16B2B0BA4C

C:
110222FF8050CBECE66A813AD09A73ED
7A9A089C106B959389168ED6E8698EA9
02EB1277DBEC2E68E473155A15A7DAEE
D4

T: A10F4E05139C23DF00B3AADC71F0596A

ICV: A10F4E05139C23DF00B3AADC71F0596A
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the encrypted user data, and the ICV.

```
84C5D513 D2AAF6E5 BBD27277 88E52F00
8932D612 7CFDE9F9 E33724C6 110222FF
8050CBEC E66A813A D09A73ED 7A9A089C
106B9593 89168ED6 E8698EA9 02EB1277
DBEC2E68 E473155A 15A7DAEE D4A10F4E
05139C23 DF00B3AA DC71F059 6A
```

2.7 79-byte Packet Authentication

This 79-byte example begins with an IP packet containing a 6-byte destination address, a 6-byte source address, and 67 bytes of user data (including the IP EtherType). These values are shown in Table 2.14. Table 2.15 contains the MACsec data elements required to process the packet. This packet will be processed to provide authentication only; no data confidentiality will be provided.

The input packet before MACsec processing is:

Field	Value
MAC DA	68 F2 E7 76 96 CE
MAC SA	7A E8 E2 CA 4E C5
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 00 07

Table 2.14: Input Data Elements

```
68F2E776 96CE7AE8 E2CA4EC5 08000F10
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 35363738 393A3B3C 3D3E3F40
41424344 45464748 494A4B4C 4D0007
```

Field	Value
MAC DA	68 F2 E7 76 96 CE
MAC SA	7A E8 E2 CA 4E C5
MACsec EtherType	88 E5
TCI and AN	41
SL	00
PN	2E 58 49 5C
SCI	7A E8 E2 CA 4E C5 00 01
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 00 07

Table 2.15: MACsec Data Elements

The security tag consists of the MACsec EtherType, the TCI, the AN, the SL, and the PN. (The optional SCI is omitted.).

```
88E54100 2E58495C
```

The additional data A to be authenticated is formed by concatenating the MAC DA, the

MAC SA, the security tag, and the user data. This input is then processed through the authentication only operation of the GCM module. A is shown below.

```
68F2E776 96CE7AE8 E2CA4EC5 88E54100
2E58495C 08000F10 11121314 15161718
191A1B1C 1D1E1F20 21222324 25262728
292A2B2C 2D2E2F30 31323334 35363738
393A3B3C 3D3E3F40 41424344 45464748
494A4B4C 4D0007
```

The SCI and the PN form the 96-bit IV used by GCM within MACsec.

```
7AE8E2CA 4EC50001 2E58495C
```

This authentication process is shown in sections 2.7.1 and 2.7.2.

2.7.1 79-byte Packet Authentication Using GCM-AES-128

This example performs authentication without confidentiality using GCM-AES-128. This process produces a 128-bit integrity check value (ICV).

```
key size = 128 bits
P: 0 bits
A: 696 bits
IV: 96 bits
ICV: 128 bits

Key:
88EE087FD95DA9FBF6725AA9D757B0CD

P:

A:
68F2E77696CE7AE8E2CA4EC588E54100
2E58495C08000F101112131415161718
191A1B1C1D1E1F202122232425262728
292A2B2C2D2E2F303132333435363738
393A3B3C3D3E3F404142434445464748
494A4B4C4D0007
```

```
IV:
7AE8E2CA4EC500012E58495C

GCM-AES Authentication
H: AE19118C3B704FCE42AE0D15D2C15C7A
Y[0]: 7AE8E2CA4EC500012E58495C00000001
E(K,Y[0]): D2521AABC48C06033E112424D4A6DF74
X[1]: CA0CAE2BEE8F19845DCB7FE3C5E713AB
X[2]: 5D3F9C7A3BC869457EA5FDFD404A415F
X[3]: 760E6A2873ACC0515D4901B5AC1C85E4
X[4]: 5A40A8425165E3D1978484F07AFC70D8
X[5]: D9687630FC4436EE582A90A8E4AFC504
X[6]: 311CE361065F86403CDA5DB00798B961
GHASH(H,A,C): D5C03125787D0DB11764ACEE98C79A57

C:

T: 07922B8EBCF10BB2297588CA4C614523

ICV: 07922B8EBCF10BB2297588CA4C614523
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the unmodified user data, and the ICV.

```
68F2E776 96CE7AE8 E2CA4EC5 88E54100
2E58495C 08000F10 11121314 15161718
191A1B1C 1D1E1F20 21222324 25262728
292A2B2C 2D2E2F30 31323334 35363738
393A3B3C 3D3E3F40 41424344 45464748
494A4B4C 4D000707 922B8EBC F10BB229
7588CA4C 614523
```

2.7.2 79-byte Packet Authentication Using GCM-AES-256

This example performs authentication without confidentiality using GCM-AES-256. This process produces a 128-bit integrity check value (ICV).

```
key size = 256 bits
P: 0 bits
A: 696 bits
```

```
IV: 96 bits
ICV: 128 bits

Key:
4C973DBC7364621674F8B5B89E5C1551
1FCED9216490FB1C1A2CAA0FFE0407E5

P:

A:
68F2E77696CE7AE8E2CA4EC588E54100
2E58495C08000F101112131415161718
191A1B1C1D1E1F202122232425262728
292A2B2C2D2E2F303132333435363738
393A3B3C3D3E3F404142434445464748
494A4B4C4D0007

IV:
7AE8E2CA4EC500012E58495C

GCM-AES Authentication
H: 9A5E559A96459C21E43C0DFF0FA426F3
Y[0]: 7AE8E2CA4EC500012E58495C00000001
E(K,Y[0]): 316F5EDB0829AC9271A6AFF79F3600BF
X[1]: 06A9019B44B76FFEC18978E8B21513E2
X[2]: 89A6401E39EAB6EE5B8159570139F54D
X[3]: 0A5E22BA54F282CE464C334D1AF598EF
X[4]: 4514D8A5C15E15CABC3D2A0E24FC758E
X[5]: 6F98DE3369B88F25AACBF3A993003E78
X[6]: 8183B21C0A932A2D5F598E1B2967564B
GHASH(H,A,C): 31D2FF6CE05FA42ECEE1A0E58A494CB8

C:

T: 00BDA1B7E87608BCBF470F12157F4C07

ICV: 00BDA1B7E87608BCBF470F12157F4C07
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the unmodified user data, and the ICV.

```
68F2E776 96CE7AE8 E2CA4EC5 88E54100
```

```
2E58495C 08000F10 11121314 15161718
191A1B1C 1D1E1F20 21222324 25262728
292A2B2C 2D2E2F30 31323334 35363738
393A3B3C 3D3E3F40 41424344 45464748
494A4B4C 4D000700 BDA1B7E8 7608BCBF
470F1215 7F4C07
```

2.8 75-byte Packet Encryption

This 75-byte example begins with an IP packet containing a 6-byte destination address, a 6-byte source address, and 63 bytes of user data (including the IP EtherType). These values are shown in Table 2.16. Table 2.17 contains the MACsec data elements required to process the packet. This packet will be processed to provide both confidentiality and authentication.

Field	Value
MAC DA	68 F2 E7 76 96 CE
MAC SA	7A E8 E2 CA 4E C5
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 00 08

Table 2.16: Input Data Elements

The input packet before MACsec processing is:

```
68F2E776 96CE7AE8 E2CA4EC5 08000F10
11121314 15161718 191A1B1C 1D1E1F20
21222324 25262728 292A2B2C 2D2E2F30
31323334 35363738 393A3B3C 3D3E3F40
41424344 45464748 490008
```

P, the user data to be encrypted, is extracted as:

```
08000F10 11121314 15161718 191A1B1C
1D1E1F20 21222324 25262728 292A2B2C
2D2E2F30 31323334 35363738 393A3B3C
3D3E3F40 41424344 45464748 490008
```

Field	Value
MAC DA	68 F2 E7 76 96 CE
MAC SA	7A E8 E2 CA 4E C5
MACsec EtherType	88 E5
TCI and AN	4D
SL	00
PN	2E 58 49 5C
SCI	7A E8 E2 CA 4E C5 00 01
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 00 08

Table 2.17: MACsec Data Elements

The security tag consists of the MACsec EtherType, the TCI, the AN, the SL, and the PN. (The optional SCI is omitted.)

```
88E54D00 2E58495C
```

The additional data A to be authenticated is formed by joining the MAC DA, the MAC SA, and the security tag. A is shown below.

```
68F2E776 96CE7AE8 E2CA4EC5 88E54D00
2E58495C
```

This additional data will be processed with the encrypted data to form the integrity check value (ICV) as specified in [1].

The SCI and the PN form the 96-bit IV used by GCM within MACsec.

```
7AE8E2CA 4EC50001 2E58495C
```

The results of the encryption operations are shown in sections 2.8.1 and 2.8.2.

2.8.1 75-byte Packet Encryption Using GCM-AES-128

This example performs authenticated encryption using GCM-AES-128. It produces a 128-bit integrity check value (ICV).

```
key size = 128 bits
P: 504 bits
A: 160 bits
IV: 96 bits
ICV: 128 bits

Key:
88EE087FD95DA9FBF6725AA9D757B0CD

P:
08000F101112131415161718191A1B1C
1D1E1F202122232425262728292A2B2C
2D2E2F303132333435363738393A3B3C
3D3E3F404142434445464748490008

A:
68F2E77696CE7AE8E2CA4EC588E54D00
2E58495C

IV:
7AE8E2CA4EC500012E58495C

GCM-AES Encryption
H: AE19118C3B704FCE42AE0D15D2C15C7A
Y[0]: 7AE8E2CA4EC500012E58495C00000001
E(K,Y[0]): D2521AABC48C06033E112424D4A6DF74
Y[1]: 7AE8E2CA4EC500012E58495C00000002
E(K,Y[1]): CB1F5CC98F4494E323470EA02BC8B1FB
C[1]: C31F53D99E5687F7365119B832D2AAE7
Y[2]: 7AE8E2CA4EC500012E58495C00000003
E(K,Y[2]): 1A5FCAB3D0DBC18F117350B32EA493D2
C[2]: 0741D593F1F9E2AB3455779B078EB8FE
Y[3]: 7AE8E2CA4EC500012E58495C00000004
E(K,Y[3]): 81F1C32FBF0C6143CD2E3C7B0F255E2E
C[3]: ACDFEC1F8E3E5277F8180B43361F6512
Y[4]: 7AE8E2CA4EC500012E58495C00000005
E(K,Y[4]): 908F526E7916C96834DBFD3A61D848B2
C[4]: ADB16D2E38548A2C719DBA7228D840
X[1]: A9845CAED3E164079E217A8D26A600DA
X[2]: 09410740B1204002F754119A976F31C8
X[3]: CB897D3B71442B121E77CEA5416D3931
X[4]: 5F3A6A2D049FF2337096523ECAA1BD30
```

```
X[5]: 0C95908AEEBDAF1B1C279837AE498000
X[6]: 1ACA99E1E46D2395BC610D21BB4216A0
GHASH(H,A,C): 5AAA6FD11F06A18BE6E77EF2BC18AF93

C:
C31F53D99E5687F7365119B832D2AAE7
0741D593F1F9E2AB3455779B078EB8FE
ACDFEC1F8E3E5277F8180B43361F6512
ADB16D2E38548A2C719DBA7228D840

T: 88F8757ADB8AA788D8F65AD668BE70E7

ICV: 88F8757ADB8AA788D8F65AD668BE70E7
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the encrypted user data, and the ICV.

```
68F2E776 96CE7AE8 E2CA4EC5 88E54D00
2E58495C C31F53D9 9E5687F7 365119B8
32D2AAE7 0741D593 F1F9E2AB 3455779B
078EB8FE ACDFEC1F 8E3E5277 F8180B43
361F6512 ADB16D2E 38548A2C 719DBA72
28D84088 F8757ADB 8AA788D8 F65AD668
BE70E7
```

2.8.2 75-byte Packet Encryption Using GCM-AES-256

This example performs authenticated encryption using GCM-AES-256. It produces a 128-bit integrity check value (ICV).

```
key size = 256 bits
P: 504 bits
A: 160 bits
IV: 96 bits
ICV: 128 bits

Key:
4C973DBC7364621674F8B5B89E5C1551
1FCED9216490FB1C1A2CAA0FFE0407E5
```

```
P:
08000F101112131415161718191A1B1C
1D1E1F202122232425262728292A2B2C
2D2E2F303132333435363738393A3B3C
3D3E3F404142434445464748490008

A:
68F2E77696CE7AE8E2CA4EC588E54D00
2E58495C

IV:
7AE8E2CA4EC500012E58495C

GCM-AES Encryption
H: 9A5E559A96459C21E43C0DFF0FA426F3
Y[0]: 7AE8E2CA4EC500012E58495C00000001
E(K,Y[0]): 316F5EDB0829AC9271A6AFF79F3600BF
Y[1]: 7AE8E2CA4EC500012E58495C00000002
E(K,Y[1]): B28AEC0BD4145B797D65F3E4FD7AFCC0
C[1]: BA8AE31BC506486D6873E4FCE460E7DC
Y[2]: 7AE8E2CA4EC500012E58495C00000003
E(K,Y[2]): 4A4700D02733D0381D12D9342D87AB9A
C[2]: 57591FF00611F31C3834FE1C04AD80B6
Y[3]: 7AE8E2CA4EC500012E58495C00000004
E(K,Y[3]): 452D80FF6A15D5070A904BA1E37DF9CC
C[3]: 6803AFCF5B27E6333FA67C99DA47C2F0
Y[4]: 7AE8E2CA4EC500012E58495C00000005
E(K,Y[4]): F3E8B2135A9502ED0689B0EE383BD81D
C[4]: CED68D531BD741A943CFF7A6713BD0
X[1]: 1F7477283AA77457BD0C161CB6F179C5
X[2]: 617F112B72DF67BC42218163B73AF025
X[3]: 20A91ADD33433324DBE7822A5BC98013
X[4]: 84D320FCB3B7AF10A66A48BADD00CFA1
X[5]: 52F52D34BC031431185DB9A617FCE98C
X[6]: 57E7CFDDBA0BA07415FD58BCEE906CAC
GHASH(H,A,C): 177E93A6A2287A8E2D2EC236372101B8

C:
BA8AE31BC506486D6873E4FCE460E7DC
57591FF00611F31C3834FE1C04AD80B6
6803AFCF5B27E6333FA67C99DA47C2F0
CED68D531BD741A943CFF7A6713BD0
```

```
T: 2611CD7DAA01D61C5C886DC1A8170107

ICV: 2611CD7DAA01D61C5C886DC1A8170107
```

The final MACsec processed packet combines the MAC DA, the MAC SA, the security tag, the encrypted user data, and the ICV.

```
68F2E776 96CE7AE8 E2CA4EC5 88E54D00
2E58495C BA8AE31B C506486D 6873E4FC
E460E7DC 57591FF0 0611F31C 3834FE1C
04AD80B6 6803AFCF 5B27E633 3FA67C99
DA47C2F0 CED68D53 1BD741A9 43CFF7A6
713BD026 11CD7DAA 01D61C5C 886DC1A8
170107
```

References

[1] NIST Special Publication 800-38D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007.

[2] IEEE Std 802.1AE. Media Access Control (MAC) Security, June 2006.

[3] Guy Hutchison. MACsec Sample Packets, July 2006.