AES Mode for 802.16

IEEE 802.16 Presentation Submission

Document Number:

IEEE S802.16e-04/12

Date Submitted:

2004-01-09

Source:

David Johnston
Intel
2111 NE 25th
Hillsboro, OR 97124

Voice: 503 264 3855
Fax: 503 202 5047
E-mail: dj.johnston@intel.com, david.johnston@ieee.org

Venue:

January 2004 802.16 Interim, Vancouver, BC

Base Document:

Purpose:

Description of proposed amendments to the 802.16 privacy layer to introduce AES based encryption and authentication.

AES mode for 802.16

David Johnston, Intel,
dj.johnston@intel.com

What This Submission Is Not

- An authorization method
- An enhancement of PKM
  - Beyond necessary capability declarations
- Anything to do with EAP

This Submission Is

- A new authenticated encryption mode and ciphersuite.
- Based on Federal standards based algorithms FIPS-197 (AES) and CCM mode.
- An optional and runtime negotiable cipher mode

Privacy/Security

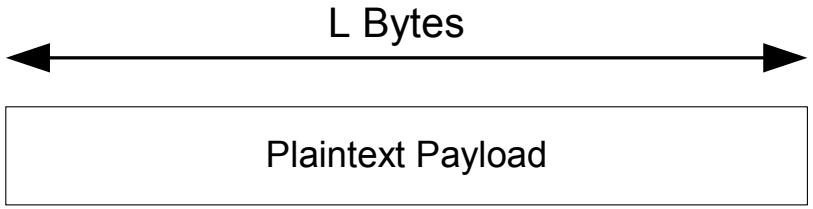
- Diversity in the choice of ciphersuite entries means that the privacy sublayer may now offer more than just privacy.
  - Change name to security sublayer to accommodate new crypto capabilities.

AES-CCM

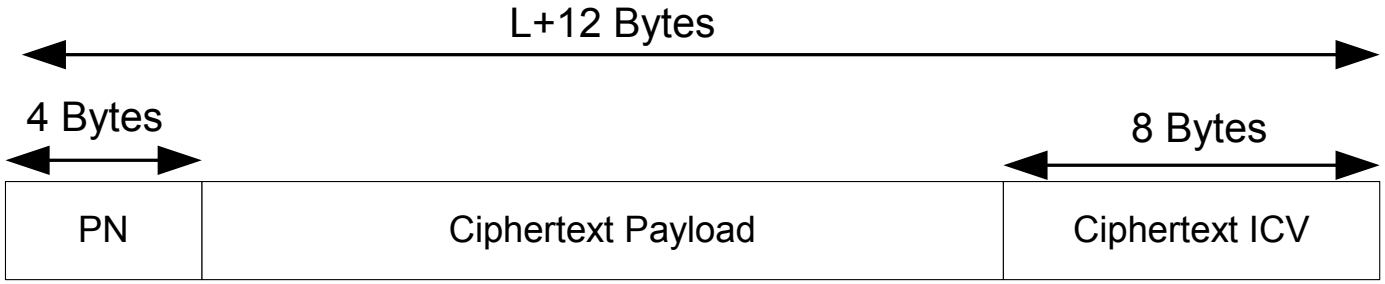
- Frames may be encrypted and authenticated with an AES-CCM mode.
- AES-CCM is a FIPS compliant security mode and as such is the default choice for an authenticated encryption mode.

AES-CCM Payload Format

PDU Payload Before Encryption:



PDU Payload After Encryption:



AES-CCM Algorithm

- The NIST CCM mode is flexible
- 802.16 must define the particular mode that CCM is used in:
  - M=8 (coded as $_b$011)
  - Length Field is 2 octets
  - DLEN size field coded as $_b$001
  - Nonce built from GMH and PN as described in 7.5.1.2.3 in the text

PKM Changes

Data Encryption Algorithm Identifier

- There is a new data encryption algorithm identifier

Value	Description
0	No data encryption
1	CBC-Mode, 56-bit DES
2	CCM-Mode, 128 bit AES
3-255	*Reserved*

Table 287—Data encryption algorithm identifiers

Data Authentication Algorithm Identifier

- There is a new data authentication algorithm identifier
  - This is the same instance as the encryption mode, since CCM combined authentication and encryption.
  - The ciphersuite selectors prevent selection of CCM crypto with anything other than CCM authentication

Value	Description
0	No data authentication
1	CCM-Mode, 128 bit AES
2-255	*Reserved*

Table 288—Data authentication algorithm identifiers

TEK Encryption Algorithm Identifier

- There is a new TEK encryption algorithm identifier
  - 128 bit strong TEK encryption is required.

Value	Description
0	*Reserved*
1	3-DES EDE with 128-bit key
2	RSA with 1024-bit key
3	ECB mode AES with 128-bit key
4-255	*Reserved*

Table 289—TEK encryption algorithm identifiers

Cryptographic Suites

- One new ciphersuite selection

Value	Description
0x000001	No data encryption, no data authentication & 3-DES,128
0x010001	CBC-Mode 56-bit DES, no data authentication & 3-DES,128
0x000002	No data encryption, no data authentication & RSA, 1024
0x010002	CBC-Mode 56-bit DES, no data authentication & RSA, 1024
0x020103	CCM-Mode 128 bit AES, CCM-Mode, 128 bit AES, ECB mode AES with 128-bit key
All remaining values	*Reserved*

Table 290—Allowed cryptographic suites

OFDM PMP Profile

TEK encryption algorithms: 3-DES EDE with 128-bit key (type 1) RSA with 1024-bit key (type 2) ECB mode AES with 128-bit key (type 3)	Yes No No	

- Switch required/not required between RSA and 3-DES for TEK encryption

IVs

- For AES-CCM mode, the CBC IV is not required in the TEK parameters:

11.2.8
[…]
The CBC-IV attribute is required when the data encryption algorithm identifier in the SA ciphersuite is 0x01 (DES in CBC mode).

The CBC-IV attribute is not required when the data encryption algorithm identifier in the SA ciphersuite is 0x02 (AES).

TEK Size

- Encrypted TEK will be larger with CCM mode

Type	Length	Value (string)
8	8 or 16	Encrypted TEK.

When the TEK encryption algorithm identifier in the SA is 0x01, the length shall be 8 and the TEK shall be encrypted with 3DES in EDE mode according to the procedure defined in 7.5.2.1.

When the TEK encryption algorithm identifier in the SA is 0x03, the length shall be 16 and the TEK shall be encrypted with AES in ECB mode according to the procedure in 7.5.2.3

TEK Encryption

- TEK Encryption defined, using AES in ECB mode.

encryption: C = Ek1[P]
decryption: P = Dk1[C]
P = Plaintext 128-bit TEK
C = Ciphertext 128-bit TEK
k1 = the 128-bit KEK
E[ ] = 128-bit AES ECB mode encryption
D[ ] = 128-bit AES ECB decryption

Packet numbers

- SAs may be bound both to uplink and downlink CIDs as well as bi-directional CIDs such as the secondary management channel

- So each SA should maintain an uplink PN and a downlink PN.

- The MSB of the PN is always 1 on uplink traffic and 0 on downlink traffic
  - Prevents the need for separate uplink/downlink keys