JunHyuk Song
Jicheol Lee
Samsung Electronics

INTERNET DRAFT
Expires: November 24, 2005
May 25 2005

# The AES-CMAC-96 Algorithm and its use with IPsec
draft-songlee-aes-cmac-96-01.txt

## Status of This Memo



## Copyright Notice



## Abstract

National Institute of Standards and Technology (NIST) has newly specified the Cipher based MAC (CMAC) which is equivalent to the One-Key CBC-MAC1 (OMAC1) algorithm submitted by Iwata and Kurosawa. OMAC1 efficiently reduces the key size of Extended Cipher Block Chaining mode (XCBC). This memo specifies the use of CMAC mode on authentication mechanism of IPsec Encapsulating Security Payload (ESP) and the Authentication Header (AH) protocols. This new algorithm is named AES-CMAC-96.

## 1. Introduction

National Institute of Standards and Technology (NIST) has newly specified the Cipher based MAC (CMAC). CMAC [NIST-CMAC] is a keyed hashed function that is based on a symmetric key block cipher such as Advanced Encryption Standard [AES]. CMAC is equivalent to the One-Key CBC-MAC1 (OMAC1) algorithm submitted by Iwata and Kurosawa [OMAC1]. Although the OMAC1 algorithm is based on the eXtended Cipher Block Chaining mode (XCBC) algorithm submitted by Rogaway and Black [XCBC], OMAC1 efficiently reduces the key size of XCBC.
This memo specifies the usage of CMAC on authentication mechanism of IPsec Encapsulating Security Payload (ESP) and the Authentication Header (AH) protocols. This new algorithm is named AES-CMAC-96.
For further information on AH and ESP, refer to [AH] and [ROADMAP].

## 2. Specification of Language

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [3].

In addition, the following words are used to signify the requirements of the specification.

## 3. Basic definitions

| | |
|---|---|
| CBC | Cipher Block Chaining mode of operation for message authentication code. |
| MAC | Message Authentication Code.<br>A bitstring of a fixed length, computed by MAC generation algorithm, that is used to established the authority and hence, the integrity of a message. |
| CMAC | Cipher-based MAC based on an approved symmetric key block cipher, such as the Advanced Encryption Standard. |

| | |
|---|---|
| Key (K) | 128-bits (16bytes) long key for AES-128 cipher block. Denoted by K. |
| Message (M) | Message to be authenticated. Denoted by M. The total message M is denoted by sequence of M_i where M_i is the i'th block with size 128-bit. Message can be null message which means that the length of M is 0. |





| | |
|---|---|
| Length (len) | The length of message M in bytes. Denoted by len. Minimum value of the length can be 0. The maximum value of the length is not specified in this document. |
| truncate(T,l) | Truncate T (MAC) in msb-first order with l bytes. |
| T | The output of AES-CMAC-128. |
| Truncated T | The truncated output of AES-CMAC-128 in MSB first order. |
| AES-CMAC | CMAC generation function based on AES block cipher with 128-bits key |
| AES-CMAC-96 | IPsec AH and ESP MAC generation function based on CMAC-AES-128 which truncates MSB 96 bits of 128 bits output |

## 4. AES-CMAC-96

The underlying algorithm for AES-CMAC-96 are Advanced Encryption Standard cipher block [AES] and recently defined CMAC mode of operation [NIST-CMAC]. The output of AES-CMAC can validate the input message. Validating the message provide assurance of the integrity and authenticity over the message from the source. According to [NIST-CMAC] at least 64-bits should be used for against guessing attack.

For use in IPsec message authentication on AH and ESP, AES-CMAC-96 should be used. AES-CMAC-96 is a AES-CMAC with 96-bit-long truncated output in most significant bit first order. The output of 96 bits

MAC that will meet the default authenticator length as specified in [AH]. The result of truncation should be taken in most significant bits first order. For further information on AES-CMAC, refer to [AES-CMAC] and [NIST-CMAC].

Figure 1 describes AES-CMAC-96 algorithm:

In step 1, AES-CMAC is applied to the message 'M' in length 'len' with key 'K'

In step 2, Truncate output block, T with 12 byte in msb-first-order and return TT.





```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+                    Algorithm AES-CMAC-96                       +
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+                                                                +
+   Input    : K (128-bit Key described in section 4.1)         +
+            : M    ( message to be authenticated )             +
+            : len  ( length of message in bytes )              +
+   Output   : Truncated T  (Truncated output with length 12 bytes) +
+                                                                +
+----------------------------------------------------------------+
+                                                                +
+   Step 1.  T  := AES-CMAC-128 (K,M,len);                       +
+   Step 2.  TT := truncate (T, 12);                             +
+            return TT;                                          +
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Figure 1 Algorithm AES-CMAC-96

## 5. Test Vectors

These test cases same as defined in [NIST-CMAC] with one exception of 96 bits truncation

```
-------------------------------------------------
K               2b7e1516 28aed2a6 abf71588 09cf4f3c
Subkey Generation
AES_128(key,0) 7df76b0c 1ab899b3 3e42f047 b91b546f
K1              fbeed618 35713366 7c85e08f 7236a8de
K2              f7ddac30 6ae266cc f90bc11e e46d513b
```

```
Example 1: len = 0
M               <empty string>
AES_CMAC_96     bb1d6929 e9593728 7fa37d12

Example 2: len = 16
M               6bc1bee2 2e409f96 e93d7e11 7393172a
AES_CMAC_96     070a16b4 6b4d4144 f79bdd9d

Example 3: len = 40
M               6bc1bee2 2e409f96 e93d7e11 7393172a
                ae2d8a57 1e03ac9c 9eb76fac 45af8e51
                30c81c46 a35ce411
AES_CMAC_96     dfa66747 de9ae630 30ca3261

Example 4: len = 64
M               6bc1bee2 2e409f96 e93d7e11 7393172a
                ae2d8a57 1e03ac9c 9eb76fac 45af8e51
                30c81c46 a35ce411 e5fbc119 1a0a52ef
                f69f2445 df4f9b17 ad2b417b e66c3710
AES_CMAC_96     51f0bebf 7e3b9d92 fc497417
-------------------------------------------------
```





## 6. Interaction with the ESP Cipher Mechanism

As of this writing, there are no known issues which preclude the use of AES-CMAC-96 with any specific cipher algorithm.

## 7. Security Considerations

The security provided by AES-CMAC-96 is based upon the strength of AES. At the time of this writing there are no practical cryptographic attacks against AES or AES-CMAC-96.

As is true with any cryptographic algorithm, part of its strength lies in the correctness of the algorithm implementation, the security of the key management mechanism and its implementation, the strength of the associated secret key, and upon the correctness of the implementation in all of the participating systems. This document contains test vectors to assist in verifying the correctness of AES-CMAC-96 code.

## 8. IANA Consideration

TBD

## 9. Acknowledgement

Portions of this text were borrowed from [NIST-CMAC] and [AES-XCBC-MAC]. We would like to thank to OMAC1 author Tetsu Iwata and Kaoru Kurosawa, and CMAC author Morris Dworkin.

## 10. References

[NIST-CMAC] NIST, Special Publication 800-38B Draft,"Recommendation for Block Cipher Modes of Operation: The CMAC Method for Authentication," March 9, 2005

[AES] NIST, FIPS 197, "Advanced Encryption Standard (AES)," November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[OMAC1] "OMAC: One-Key CBC MAC," Tetsu Iwata and Kaoru Kurosawa, Department of Computer and Information Sciences, Ilbaraki University, March 10, 2003.

[AH] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[ROADMAP] Thayer, R., N. Doraswamy, and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.





[XCBC] Black, J. and P. Rogaway, "A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC," NIST Second Modes of Operation Workshop, August 2001. http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/xcbc-mac/xcbc-mac-spec.pdf

[AES-CMAC] JunHyuk Song and Jicheol Lee, "The AES-CMAC Algorithm" draft-songlee-aes-cmac-00.txt, May 2005

## 11. Author's Address

Junhyuk Song
Samsung Electronics
+82-31-279-3639
santajunman@hanafos.com

Jicheol Lee
Samsung Electronics
+82-31-279-3605
jicheol.lee@samsung.com

## Intellectual Property Statement





---



## Disclaimer of Validity

## Copyright Statement



## Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.