Network Working Group
Request for Comments: 5282
Updates: 4306
Category: Standards Track

D. Black
EMC
D. McGrew

August 2008

Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol

Status of This Memo

Abstract

An authenticated encryption algorithm combines encryption and integrity into a single operation; such algorithms may also be referred to as combined modes of an encryption cipher or as combined mode algorithms. This document describes the use of authenticated encryption algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) protocol.

The use of two specific authenticated encryption algorithms with the IKEv2 Encrypted Payload is also described; these two algorithms are the Advanced Encryption Standard (AES) in Galois/Counter Mode (AES GCM) and AES in Counter with CBC-MAC Mode (AES CCM). Additional documents may describe the use of other authenticated encryption algorithms with the IKEv2 Encrypted Payload.

Table of Contents

1. Introduction

An authenticated encryption algorithm combines encryption and integrity into a single operation on plaintext data to produce ciphertext that includes an integrity check [RFC5116]. The integrity check may be an Integrity Check Value (ICV) that is logically distinct from the encrypted data, or the integrity check may be incorporated into the encrypted data that is produced. Authenticated encryption algorithms may also be referred to as combined modes of operation of a block cipher or as combined mode algorithms.

An Authenticated Encryption with Associated Data (AEAD) algorithm also provides integrity protection for additional data that is associated with the plaintext, but which is left unencrypted. This document describes the use of AEAD algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) protocol. The use of two specific AEAD algorithms with the IKEv2 Encrypted Payload is also described; the two algorithms are the Advanced Encryption Standard (AES) in Galois/Counter Mode (AES GCM) [GCM] and AES in Counter with CBC-MAC Mode (AES CCM) [CCM].

Version 1 of the Internet Key Exchange protocol (IKEv1) [RFC2409] is based on the Internet Security Association and Key Management Protocol (ISAKMP) [RFC2408]. The E (Encryption) bit in the ISAKMP header specifies that all payloads following the header are encrypted, but any data integrity verification of those payloads is handled by a separate Hash Payload or Signature Payload (see Sections 3.1, 3.11, and 3.12 of [RFC2408]). This separation of encryption from data integrity protection prevents the use of authenticated encryption with IKEv1, thus limiting initial specifications of AES combined mode usage for IPsec to the Encapsulating Security Payload (ESP) [RFC2406]. The current version of ESP is version 3, ESPv3 [RFC4303].

Version 2 of the Internet Key Exchange Protocol (IKEv2) [RFC4306] employs an Encrypted Payload that is based on the design of ESP. The IKEv2 Encrypted Payload associates encryption and data integrity protection in a fashion that makes it possible to use AEAD algorithms.

1.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The symbols or variables that designate authenticated encryption and decryption operation inputs and outputs (K, N, P, A, and C) are

defined in [RFC5116]. The SK_* symbols or variables that designate specific IKEv2 keys are defined in [RFC4306].

2. Structure of this Document

This document is based on the RFCs that describe the usage of AES GCM [RFC4106] and AES CCM [RFC4309] with ESP; hence, the introductory material and specification of the modes in those documents are not repeated here. The structure of this document follows the structure of those documents; many sections of this document indicate which sections of those two documents correspond, and call out any significant differences that implementers should be aware of. Significant portions of the text of this document have been adapted from those two documents.

This document is based on the authenticated encryption interfaces, notation, and terminology described in [RFC5116]. An important departure from [RFC4106] and [RFC4309] is that these two RFCs describe separate ciphertext and integrity check outputs of the encryption operation, whereas [RFC5116] specifies a single ciphertext (C) output that includes an integrity check. The latter more general approach encompasses authenticated encryption algorithms that produce a single, expanded ciphertext output into which the integrity check is incorporated, rather than producing separate ciphertext and integrity check outputs.

For AES GCM and AES CCM, the [RFC5116] ciphertext (C) output of authenticated encryption consists of the [RFC4106] or [RFC4309] ciphertext output concatenated with the [RFC4106] or [RFC4309] Integrity Check Value (ICV) output. This document does not modify the AES GCM or AES CCM authenticated encryption algorithms specified in [RFC4106] and [RFC4309].

3. IKEv2 Encrypted Payload Data

This section is based on [RFC5116] and Section 3.14 of [RFC4306].

For the use of authenticated encryption algorithms with the IKEv2 Encrypted Payload, this section updates Section 3.14 of [RFC4306] by replacing Figure 21 and the text that follows it (through the end of that section) with the contents of this section. In addition, Section 3.14 of [RFC4306] is also updated to allow the use of a single authenticated encryption algorithm instead of a block cipher and a separate integrity check algorithm. In contrast, Sections 3.1 and 3.2 of this document are specific to the AES GCM and AES CCM algorithms and hence do not update [RFC4306]. The updates to [RFC4306] made by this document have no effect when authenticated encryption algorithms are neither proposed nor used.

The IKEv2 Encrypted Payload Data structure applies to all authenticated encryption algorithms, and it is the same structure that is used with ESP. When an authenticated encryption algorithm is used, the IKEv2 Encrypted Payload is composed of the payload header fields, followed by an Initialization Vector (IV) field and a Ciphertext (C) field that includes an integrity check as shown in Figure 1.

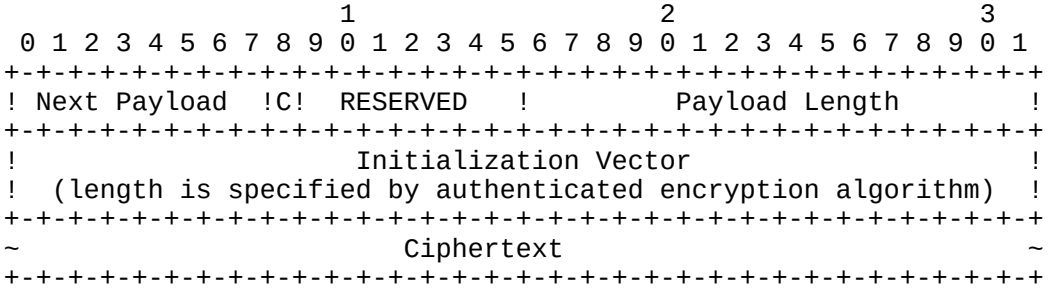

Figure 1. IKEv2 Encrypted Payload Data for Authenticated Encryption

The Next Payload, C bit, and Payload Length fields are unchanged from [RFC4306].

The contents of the Initialization Vector (IV) field are specified by the authenticated encryption algorithm; see Sections 3.1 and 4 (below) for AES GCM and AES CCM.

The Ciphertext field is the output of an authenticated encryption operation (see Section 2.1 of [RFC5116]) on the following inputs:

- The secret key (K) is the cipher key obtained from the SK_ei or SK_er key, whichever is appropriate, see [RFC4306]. The authenticated encryption algorithm describes how to obtain the cipher key from SK_ei or SK_er; for AES GCM and AES CCM, see Section 7.1 (below).

- The nonce (N) is specified by the authenticated encryption algorithm; for AES GCM and AES CCM, see Section 4 (below). When decrypting an Encrypted Payload, a receiver constructs the nonce based on the IV in the Encrypted Payload, using rules that are specific to the authenticated encryption algorithm; see Sections 3.1 and 4 (below) for AES GCM and AES CCM.

- The plaintext (P) consists of the concatenation of the IKE Payloads to be encrypted with the Padding (if any) and the Pad Length, as shown in Figure 2 (below). The plaintext structure in Figure 2 applies to all encryption algorithms used with the IKEv2 Encrypted Payload, and is unchanged from [RFC4306].

o The associated data (A) is described in Section 5 (below).

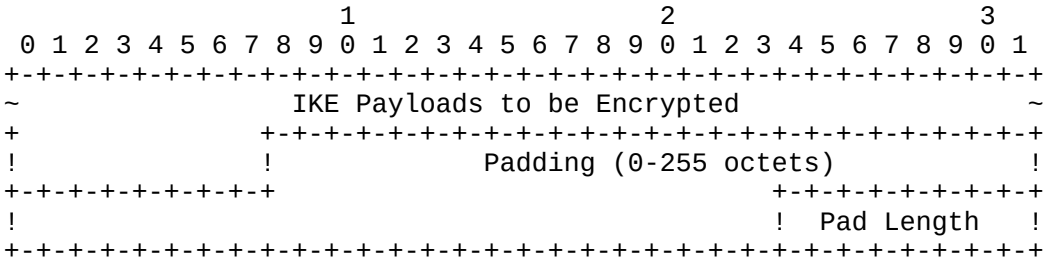

Figure 2. IKEv2 Encrypted Payload Plaintext (P)

The IKE Payloads are as specified in [RFC4306].

Padding MAY contain any value chosen by the sender.

Pad Length is the number of octets in the Padding field. There are no alignment requirements on the length of the Padding field; the recipient MUST accept any amount of Padding up to 255 octets.

The ciphertext output of authenticated encryption algorithms, as defined by [RFC5116], incorporates data that allows checks on the integrity and authenticity of the ciphertext and associated data. Thus, there is no need for a separate Integrity Check Value (ICV) field in the IKEv2 Encrypted Payload Data structure.

3.1. AES GCM and AES CCM Initialization Vector (IV)

This section is based on Section 3.1 of [RFC4106] and Section 3.1 of [RFC4309]. The Initialization Vector requirements are common to AES GCM and AES CCM, and are the same as the requirements for ESP.

The Initialization Vector (IV) MUST be eight octets. The IV MUST be chosen by the encryptor in a manner that ensures that the same IV value is used only once for a given key. The encryptor MAY generate the IV in any manner that ensures uniqueness. Common approaches to IV generation include incrementing a counter for each packet and linear feedback shift registers (LFSRs).

3.2. AES GCM and AES CCM Ciphertext (C) Construction

This section is based on Section 6 of [RFC4106] and Section 3.1 of [RFC4309] with generalizations to match the interfaces specified in [RFC5116]. The constructions for AES GCM and AES CCM are different, but in each case, the construction is the same as for ESP.

For AES GCM and AES CCM, the Ciphertext field consists of the output of the authenticated encryption algorithm. (Note that this field incorporates integrity check data.)

The AES GCM ICV consists solely of the AES GCM Authentication Tag. Implementations MUST support a full-length 16 octet ICV, MAY support 8 or 12 octet ICVs, and MUST NOT support other ICV lengths.

AES CCM provides an encrypted ICV. Implementations MUST support ICV sizes of 8 octets and 16 octets. Implementations MAY also support 12 octet ICVs and MUST NOT support other ICV lengths.

4. AES GCM and AES CCM Nonce (N) Format

Specific authenticated encryption algorithms MAY use different nonce formats, but they SHOULD use the default nonce format specified in this section.

The default nonce format uses partially implicit nonces (see Section 3.2.1 of [RFC5116]) as follows:

- The implicit portion of the nonce is the salt that is part of the IKEv2 Keying Material shared by the encryptor and decryptor (see Section 7.1); the salt is not included in the IKEv2 Encrypted Payload.

- The explicit portion of the nonce is the IV that is included in the IKEv2 Encrypted Payload.

When this default nonce format is used, both the encryptor and decryptor construct the nonce by concatenating the salt with the IV, in that order.

For the use of AES GCM with the IKEv2 Encrypted Payload, this default nonce format MUST be used and a 12 octet nonce MUST be used. Note that this format matches the one specified in Section 4 of [RFC4106], providing compatibility between the use of AES GCM in IKEv2 and ESP. All of the requirements of Section 4 of [RFC4106] apply to the use of AES GCM with the IKEv2 Encrypted Payload.

For the use of AES CCM with the IKEv2 Encrypted Payload, this default nonce format MUST be used and an 11 octet nonce MUST be used. Note that this format matches the one specified in Section 4 of [RFC4309], providing compatibility between the use of AES CCM in IKEv2 and ESP. All of the requirements of Section 4 of [RFC4309] apply to the use of AES CCM with the IKEv2 Encrypted Payload.

5. IKEv2 Associated Data (A)

This section is based on Section 5 of [RFC4106] and Section 5 of [RFC4309], both of which refer to associated data as Additional Authenticated Data (AAD). The associated data construction described in this section applies to all authenticated encryption algorithms, but differs from the construction used with ESP because IKEv2 requires different data integrity coverage.

5.1. Associated Data (A) Construction

The associated data (A) MUST consist of the partial contents of the IKEv2 message, starting from the first octet of the Fixed IKE Header through the last octet of the Payload Header of the Encrypted Payload (i.e., the fourth octet of the Encrypted Payload), as shown in Figure 3. This includes any payloads that are between the Fixed IKE Header and the Encrypted Payload.

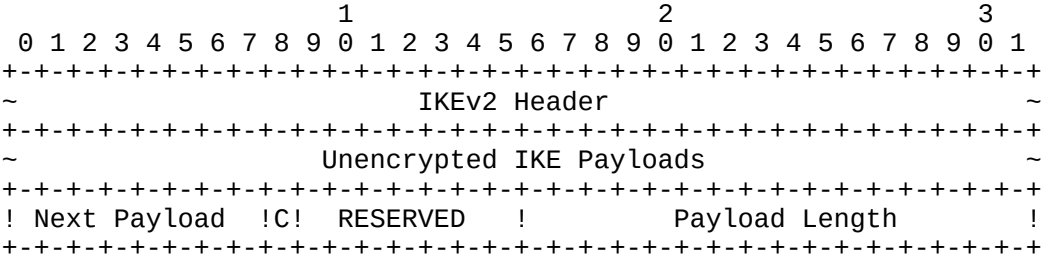

Figure 3. IKEv2 Encrypted Payload Associated Data (A) for Authenticated Encryption

The Initialization Vector and Ciphertext fields shown in Figure 1 (above) MUST NOT be included in the associated data.

5.2. Data Integrity Coverage

The data integrity coverage of the IKEv2 Encrypted Payload encompasses the entire IKEv2 message that contains the Encrypted Payload. When an authenticated encryption algorithm is used with the Encrypted Payload, this coverage is realized as follows:

1. The associated data (A) covers the portion of the IKEv2 message starting from the first octet of the Fixed IKE Header through the last octet of the Payload Header of the Encrypted Payload (fourth octet of the Encrypted Payload). This includes any Payloads between the Fixed IKE Header and the Encrypted Payload. The Encrypted Payload is always the last payload in an IKEv2 message [RFC4306].

2. The IV is an input to the authenticated encryption algorithm's integrity check. A successful integrity check at the receiver verifies that the correct IV was used, providing data integrity coverage for the IV.

3. The plaintext (IKE Payloads, Padding and Pad Length) is covered by the authenticated encryption algorithm's integrity check.

6. AES GCM and AES CCM Encrypted Payload Expansion

The expansion described in Section 7 of [RFC4106] and Section 6 of [RFC4309] applies to the use of the AES GCM and AES CCM combined modes with the IKEv2 Encrypted Payload. See Section 7 of [RFC4106] and Section 6 of [RFC4309].

7. IKEv2 Conventions for AES GCM and AES CCM

This section describes the conventions used to generate keying material and salt values for use with AES GCM and AES CCM using the IKEv2 [RFC4306] protocol. The identifiers and attributes needed to use AES GCM and AES CCM with the IKEv2 Encrypted Payload are also specified.

7.1. Keying Material and Salt Values

This section is based on Section 8.1 of [RFC4106] and Section 7.1 of [RFC4309]. The Keying Material and Salt Values for AES GCM and AES CCM are different, but have the same structure as the Keying Material and Salt Values used with ESP.

IKEv2 makes use of a Pseudo-Random Function (PRF) to derive keying material. The PRF is used iteratively to derive keying material of arbitrary size, from which keying material for specific uses is extracted without regard to PRF output boundaries; see Section 2.14 of [RFC4306].

This subsection describes how the key derivation specified in Section 2.14 of [RFC4306] is used to obtain keying material for AES GCM and AES CCM. When AES GCM or AES CCM is used with the IKEv2 Encrypted Payload, the SK_ai and SK_ar integrity protection keys are not used; each key MUST be treated as having a size of zero (0) octets. The size of each of the SK_ei and SK_er encryption keys includes additional salt bytes. The size and format of each of the SK_ei and SK_er encryption keys MUST be:

- For AES GCM, each encryption key has the size and format of the "KEYMAT requested" material specified in Section 8.1 of [RFC4106] for the AES key size being used. For example, if the AES key size

is 128 bits, each encryption key is 20 octets, consisting of a 16-octet AES cipher key followed by 4 octets of salt.

- For AES CCM, each key has the size and format of the "KEYMAT requested" material specified in Section 7.1 of [RFC4309] for the AES key size being used. For example, if the AES key size is 128 bits, each encryption key is 19 octets, consisting of a 16-octet AES cipher key followed by 3 octets of salt.

7.2. IKEv2 Identifiers

This section is unique to the IKEv2 Encrypted Payload usage of AES GCM and AES CCM. It reuses the identifiers used to negotiate ESP usage of AES GCM and AES CCM.

The following identifiers, previously allocated by IANA, are used to negotiate the use of AES GCM and AES CCM as the Encryption (ENCR) Transform for IKEv2 (i.e., for use with the IKEv2 Encrypted Payload):

14 for AES CCM with an 8-octet ICV;
15 for AES CCM with a 12-octet ICV;
16 for AES CCM with a 16-octet ICV;

18 for AES GCM with an 8-octet ICV;
19 for AES GCM with a 12-octet ICV; and
20 for AES GCM with a 16-octet ICV.

A 16-octet ICV size SHOULD be used with IKEv2, as the higher level of security that it provides by comparison to smaller ICV sizes is appropriate to IKEv2's key exchange and related functionality.

In general, the use of 12-octet ICVs (values 15 and 19) is NOT RECOMMENDED in order to reduce the number of options for ICV size. If an ICV size larger than 8 octets is appropriate, 16-octet ICVs SHOULD be used.

7.3. Key Length

This section is based on Section 8.4 of [RFC4106] and Section 7.4 of [RFC4309]. The Key Length requirements are common to AES GCM and AES CCM and are identical to the key length requirements for ESP.

Because the AES supports three key lengths, the Key Length attribute MUST be specified when any of the identifiers for AES GCM or AES CCM, specified in Section 7.2 of this document, is used. The Key Length attribute MUST have a value of 128, 192, or 256. The use of the value 192 is NOT RECOMMENDED. If an AES key larger than 128 bits is

appropriate, a 256-bit AES key SHOULD be used. This reduces the number of options for AES key length.

8. IKEv2 Algorithm Selection

This section applies to the use of any authenticated encryption algorithm with the IKEv2 Encrypted Payload and is unique to that usage.

IKEv2 (Section 3.3.3 of [RFC4306]) specifies that both an encryption algorithm and an integrity checking algorithm are required for an IKE SA (Security Association). This document updates [RFC4306] to require that when an authenticated encryption algorithm is selected as the encryption algorithm for any SA (IKE or ESP), an integrity algorithm MUST NOT be selected for that SA. This document further updates [RFC4306] to require that if all of the encryption algorithms in any proposal are authenticated encryption algorithms, then the proposal MUST NOT propose any integrity transforms.

9. Test Vectors

See Section 9 of [RFC4106] and Section 8 of [RFC4309] for references that provide AES GCM and AES CCM test vectors.

10. RFC 5116 AEAD_* Algorithms

This section adds new algorithms to the AEAD_* algorithm framework defined in [RFC5116] to encompass the usage of AES GCM and AES CCM with IKEv2. An AEAD_* algorithm does not have any attributes or parameters; each AEAD_* algorithm identifier defined in this document completely specifies the AES key size and the ICV size to be used (e.g., AEAD_AES_128_GCM uses a 128-bit AES key and a 16-octet ICV).

AEAD_* algorithm coverage of the AES GCM and AES CCM authenticated encryption algorithms used with IKEv2 requires specification of eight additional AEAD_* algorithms beyond the four algorithms specified in [RFC5116]:

- Four AEAD_* algorithms are specified to allow 8- and 12-octet ICVs to be used with the AES GCM and AEAD_* algorithms specified in [RFC5116].

- The version of AES CCM used with IPsec (see [RFC4309]) uses an 11-octet nonce instead of the 12-octet nonce used by the version of AES CCM specified in [RFC5116]. Six AEAD_* algorithms are specified for this short nonce version of AES CCM.

This document recommends against the use of 192-bit AES keys, and therefore does not specify AEAD_* algorithms for 192-bit AES keys.

10.1. AES GCM Algorithms with 8- and 12-octet ICVs

The following four AEAD_* algorithms are identical to the AEAD_* algorithms specified in [RFC5116], except that an 8-octet ICV is used instead of a 16-octet ICV.

10.1.1. AEAD_AES_128_GCM_8

This algorithm is identical to AEAD_AES_128_GCM (see Section 5.1 of [RFC5116]), except that the tag length, t, is 8, and an authentication tag with a length of 8 octets (64 bits) is used.

An AEAD_AES_128_GCM_8 ciphertext is exactly 8 octets longer than its corresponding plaintext.

10.1.2. AEAD_AES_256_GCM_8

This algorithm is identical to AEAD_AES_256_GCM (see Section 5.2 of [RFC5116]), except that the tag length, t, is 8, and an authentication tag with a length of 8 octets (64 bits) is used.

An AEAD_AES_256_GCM_8 ciphertext is exactly 8 octets longer than its corresponding plaintext.

10.1.3. AEAD_AES_128_GCM_12

This algorithm is identical to AEAD_AES_128_GCM (see Section 5.1 of [RFC5116]), except that the tag length, t, is 12, and an authentication tag with a length of 12 octets (64 bits) is used.

An AEAD_AES_128_GCM_12 ciphertext is exactly 12 octets longer than its corresponding plaintext.

10.1.4. AEAD_AES_256_GCM_12

This algorithm is identical to AEAD_AES_256_GCM (see Section 5.2 of [RFC5116], except that the tag length, t, is 12 and an authentication tag with a length of 12 octets (64 bits) is used.

An AEAD_AES_256_GCM_12 ciphertext is exactly 12 octets longer than its corresponding plaintext.

10.2. AES CCM Algorithms with an 11-octet Nonce

The following four AEAD algorithms employ the AES CCM algorithms with an 11 octet nonce as specified in [RFC4309].

10.2.1. AEAD_AES_128_CCM_SHORT

The AEAD_AES_128_CCM_SHORT authenticated encryption algorithm is identical to the AEAD_AES_128_CCM algorithm (see Section 5.3 of [RFC5116]), except that it uses a nonce that is one octet shorter. AEAD_AES_128_CCM_SHORT works as specified in [CCM]. It uses AES-128 as the block cipher by providing the key, nonce, associated data, and plaintext to that mode of operation. The formatting and counter generation function are as specified in Appendix A of [CCM], and the values of the parameters identified in that appendix are as follows:

the nonce length n is 11,

the tag length t is 16, and

the value of q is 3.

An authentication tag with a length of 16 octets (128 bits) is used. The AEAD_AES_128_CCM_SHORT ciphertext consists of the ciphertext output of the CCM encryption operation concatenated with the authentication tag output of the CCM encryption operation. Test cases are provided in [CCM]. The input and output lengths are as follows:

K_LEN is 16 octets,

P_MAX is 2^24 - 1 octets,

A_MAX is 2^64 - 1 octets,

N_MIN and N_MAX are both 11 octets, and

C_MAX is 2^24 + 15 octets.

An AEAD_AES_128_CCM_SHORT ciphertext is exactly 16 octets longer than its corresponding plaintext.

10.2.2. AEAD_AES_256_CCM_SHORT

This algorithm is identical to AEAD_AES_128_CCM_SHORT, but with the following differences:

K_LEN is 32 octets, instead of 16, and

AES-256 CCM is used instead of AES-128 CCM.

An AEAD_AES_256_CCM_SHORT ciphertext is exactly 16 octets longer than its corresponding plaintext.

10.2.3. AEAD_AES_128_CCM_SHORT_8

This algorithm is identical to AEAD_AES_128_CCM_SHORT, except that the tag length, t, is 8, and an authentication tag with a length of 8 octets (64 bits) is used.

An AEAD_AES_128_CCM_SHORT_8 ciphertext is exactly 8 octets longer than its corresponding plaintext.

10.2.4. AEAD_AES_256_CCM_SHORT_8

This algorithm is identical to AEAD_AES_256_CCM_SHORT, except that the tag length, t, is 8, and an authentication tag with a length of 8 octets (64 bits) is used.

An AEAD_AES_256_CCM_SHORT_8 ciphertext is exactly 8 octets longer than its corresponding plaintext.

10.2.5. AEAD_AES_128_CCM_SHORT_12

This algorithm is identical to AEAD_AES_128_CCM_SHORT, except that the tag length, t, is 12, and an authentication tag with a length of 12 octets (64 bits) is used.

An AEAD_AES_128_CCM_SHORT_12 ciphertext is exactly 12 octets longer than its corresponding plaintext.

10.2.6. AEAD_AES_256_CCM_SHORT_12

This algorithm is identical to AEAD_AES_256_CCM_SHORT, except that the tag length, t, is 12, and an authentication tag with a length of 8 octets (64 bits) is used.

An AEAD_AES_256_CCM_SHORT_12 ciphertext is exactly 12 octets longer than its corresponding plaintext.

10.3. AEAD_* Algorithms and IKEv2

The following table lists the AES CCM and AES GCM AEAD_* algorithms that can be negotiated by IKEv2 and provides the IKEv2 Encryption (ENCR) Transform Identifier and Key Length Attribute combination that is used to negotiate each algorithm.

AEAD algorithm	ENCR Identifier	Key Length
AEAD_AES_128_GCM	20	128
AEAD_AES_256_GCM	20	256
AEAD_AES_128_GCM_8	18	128
AEAD_AES_256_GCM_8	18	256
AEAD_AES_128_GCM_12	19	128
AEAD_AES_256_GCM_12	19	256
AEAD_AES_128_CCM_SHORT	16	128
AEAD_AES_256_CCM_SHORT	16	256
AEAD_AES_128_CCM_SHORT_8	14	128
AEAD_AES_256_CCM_SHORT_8	14	256
AEAD_AES_128_CCM_SHORT_12	15	128
AEAD_AES_256_CCM_SHORT_12	15	256

Each of the above AEAD_* algorithms is identical to the algorithm designated by the combination of the IKEv2 ENCR Identifier and Key Length Attribute shown on the same line of the table.

11. Security Considerations

For authenticated encryption security considerations, see the entirety of [RFC5116], not just its security considerations section; there are important security considerations that are discussed outside the security considerations section of that document.

The security considerations for the use of AES GCM and AES CCM with ESP apply to the use of these algorithms with the IKEv2 Encrypted Payload, see Section 10 of [RFC4106] and Section 9 of [RFC4309]. Use of AES GCM and AES CCM with IKEv2 does not create additional security considerations beyond those for the use of AES GCM and AES CCM with ESP.

For IKEv2 security considerations, see Section 5 of [RFC4306].

12. IANA Considerations

The Encryption Transform identifiers specified in Section 7.2 have been previously assigned by IANA for use with ESP. This document extends their usage to IKEv2 for the Encrypted Payload. No IANA actions are required for this usage extension.

IANA has added the following entries to the Authenticated Encryption with Associated Data (AEAD) Parameters Registry:

Name	Reference	Numeric Identifier
AEAD_AES_128_GCM_8	Section 10.1.1	5
AEAD_AES_256_GCM_8	Section 10.1.2	6
AEAD_AES_128_GCM_12	Section 10.1.3	7
AEAD_AES_256_GCM_12	Section 10.1.4	8
AEAD_AES_128_CCM_SHORT	Section 10.2.1	9
AEAD_AES_256_CCM_SHORT	Section 10.2.2	10
AEAD_AES_128_CCM_SHORT_8	Section 10.2.3	11
AEAD_AES_256_CCM_SHORT_8	Section 10.2.4	12
AEAD_AES_128_CCM_SHORT_12	Section 10.2.5	13
AEAD_AES_256_CCM_SHORT_12	Section 10.2.6	14

An IANA registration of an AEAD algorithm does not constitute an endorsement of that algorithm or its security.

13. Acknowledgments

See Section 13 of [RFC4106] and Section 12 of [RFC4309] for AES GCM and AES CCM acknowledgments.

Also, we thank Charlie Kaufman, Pasi Eronen, Tero Kivinen, Steve Kent, and Alfred Hoenes for their comprehensive reviews of this document.

This document was originally prepared using 2-Word-v2.0.template.dot, created by Joe Touch.

14. References

14.1. Normative References

[CCM] Dworkin, M., "NIST Special Publication 800-38C: The CCM Mode for Authentication and Confidentiality", U.S. National Institute of Standards and Technology, <http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf>, updated July 2007.

[GCM] Dworkin, M., "NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.", U.S. National Institute of Standards and Technology, November 2007, <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>, November 2007.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, June 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4306] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.

14.2. Informative References

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[RFC2408] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

Author's Addresses

David L. Black
EMC Corporation
176 South Street
Hopkinton, MA 10748

Phone: +1 (508) 293-7953
EMail: black_david@emc.com

David A. McGrew
Cisco Systems, Inc.
510 McCarthy Blvd.
Milpitas, CA 95035

Phone: +1 (408) 525-8651
EMail: mcgrew@cisco.com

Full Copyright Statement

Intellectual Property