

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 2 January 2026

R. Guthrie  
C. Wynn  
N. Gajcowski  
NSA  
1 July 2025

Using AES-GCM-SIV in the Internet Protocol Version 2 (IKEv2) and  
Encapsulating Security Payload (ESP) Protocols  
draft-guthrie-ipsecme-aes-gcm-siv-00

## Abstract

This document specifies the use of AES-GCM-SIV in the Internet Key Exchange Protocol version 2 (IKEv2) and the Encapsulating Security Payload (ESP) protocols. This document also adds AES-GCM-SIV to the IANA IKEv2 registry for "Transform Type 1 - Encryption Algorithm Transform IDs." AES-GCM-SIV is a nonce misuse-resistant authenticated encryption with associated data (AEAD) algorithm based on AES-GCM.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 2 January 2026.

## Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components

extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
1.1. Conventions Used in This Document . . . . .	3
2. AES-GCM-SIV Overview . . . . .	3
3. AES-GCM-SIV in IKEv2 . . . . .	4
3.1. IKEv2 Encrypted Payload Data . . . . .	4
3.2. IKEv2 Keying Material . . . . .	5
3.3. Associated Data Construction . . . . .	5
4. AES-GCM-SIV in ESP . . . . .	6
4.1. ESP Payload Data . . . . .	6
4.2. ESP Integrity Check Value (ICV) . . . . .	6
4.3. ESP Keying Material . . . . .	6
4.4. Additional Authenticated Data Construction . . . . .	7
5. Security Considerations . . . . .	7
6. Operational Considerations . . . . .	7
7. IANA Considerations . . . . .	7
8. References> . . . . .	7
8.1. Normative References . . . . .	7
8.2. Informative References . . . . .	8
Authors' Addresses . . . . .	8

## 1. Introduction

An authenticated encryption with associated data (AEAD) algorithm combines encryption and integrity into a single operation and returns ciphertext and an integrity check value (ICV) (also called an authentication tag) over the plaintext or ciphertext and the associated/additional data. A commonly used AEAD algorithm is AES-GCM (the Advanced Encryption Standard (AES) block cipher used in Galois/Counter mode)(GCM) [FIPS197], which offers certain performance advantages over other AES-based options that also provide both confidentiality and message authentication. However, AES-GCM fails catastrophically (i.e., exposes the authentication key) when two different plaintext messages are encrypted with the same key and nonce. While specifications of AES-GCM require a unique nonce per message, this can be difficult to guarantee in practice due to poor random number generation or failure to keep track of state, either of which can result in a nonce repeating. As a nonce-misuse-resistant AEAD, AES-GCM-SIV avoids this failure. In particular, when two messages are encrypted using the same AES-GCM-SIV nonce and key, the ICV/authentication tag associated with each message can only reveal whether it is probable that the two messages are equal.

This document specifies the use of AES-GCM-SIV in IKEv2 and ESP. This document also adds AES-GCM-SIV to the IANA IKEv2 registry for "Transform Type 1 - Encryption Algorithm Transform IDs."

### 1.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119][RFC8174] when, and only when, they appear in all capitals, as shown here.

## 2. AES-GCM-SIV Overview

Though AES-GCM-SIV is based on AES-GCM, there are several key differences between the two algorithms; these differences prevent the specifications for AES-GCM in IKEv2 and ESP from directly supporting AES-GCM-SIV. This section gives an overview of these differences and highlights how these differences manifest in the IKEv2 and ESP protocols.

The typical nonce construction for AES-GCM in IKEv2 and ESP is called "partially implicit" (Section 4 of [RFC5282]). It consists of a four-octet salt that is part of the IKEv2 keying material shared between parties (this is the implicit portion), followed by the eight-octet Initialization Vector (IV) included in the Encrypted payload (this is the explicit portion; hence "partially" implicit). It is required that the IV be eight octets and chosen in such a way that is only used once. Note in particular that the IV is defined as a component of this partially implicit nonce.

In contrast, the AES-GCM-SIV nonce is a component of the synthetic IV (SIV). Unlike the IV construction in [RFC5282], the SIV is a function of all the AEAD inputs: the 12-octet nonce, the key-generating key, the plaintext, and the associated data. For AES-GCM-SIV, the nonce is random, and does not contain a salt. Specifically, there is no need for a salt because the SIV is already a function of keying material (through the incorporation of the key-generating key).

Because of these structural differences, IKEv2 and ESP fields specified for AES-GCM nonce and IV cannot be used for the AES-GCM-SIV nonce and SIV without modification.

While the AES-GCM ciphertext (as described in [RFC5282]) and AES-GCM-SIV ciphertext both include an authentication tag, the authentication tag for AES-GCM can be 8, 12, or 16 octets. In contrast, the authentication tag for AES-GCM-SIV MUST be 16 octets. This is because the AES-GCM-SIV authentication tag is needed to decrypt ciphertext, so it must be transmitted in full (i.e., not truncated).

### 3. AES-GCM-SIV in IKEv2

The Internet Key Exchange version 2 [RFC7296] protocol is a component of IPsec [RFC4301] that establishes a Security Association (SA) with a shared session secret from which cryptographic keys are derived. This SA can facilitate the establishment of further SAs for Encapsulating Security Payload (ESP) [RFC4303] or Authentication Header [RFC4302], and the cryptographic keys are used to protect the traffic carried by each SA. [RFC7296] specifies generally how to negotiate and use cryptographic algorithms that provide properties such as encryption and integrity of the IKE SA. [RFC5282] specifies how to use AES-GCM as a Transform Type 1 algorithm to provide both encryption and integrity to the IKEv2 SA. This section specifies how to use AES-GCM-SIV for the same purpose and uses portions of [RFC5282] as a baseline.

#### 3.1. IKEv2 Encrypted Payload Data

The Encrypted payload (Section 3.14 of [RFC4106]) contains all the payloads of a given IKEv2 message in encrypted form. Section 3 (or Figure 1) of [RFC5282] updates the format of the Encrypted payload as depicted in Figure 21 of [RFC4106] in the case that one of the authenticated encryption algorithms AES-GCM or AES-CCM are used. This updated format contains two fields: an 8-octet Initialization Vector field followed by a variable-length Ciphertext field.

The Encrypted payload format for AES-GCM-SIV aligns with the modified format from [RFC5282] with one exception: instead of an Initialization Vector field, the AES-GCM-SIV Encrypted payload format includes a Nonce field in its place.

Then, the Encrypted payload has the following structure:

- \* Nonce: a twelve-octet AES-GCM-SIV nonce, followed by
- \* Ciphertext: a variable-length ciphertext.

The Nonce field contains a randomly-generated 96-bit (12-octet) value.

[EDNOTE: Is it acceptable to rename the IV field to Nonce, or should this guidance use the same field name and just clarify that the IV field contains the nonce instead of IV?]

The Ciphertext field contains the ciphertext as specified by [RFC8452]. The ciphertext as specified by [RFC8452] contains a 16-octet authentication tag, making it 16 octets longer than the corresponding plaintext. While the AES-GCM ciphertext (as described in [RFC5282]) and AES-GCM-SIV ciphertext both include an authentication tag, the authentication tag for AES-GCM can be 8, 12, or 16 octets. In contrast, the authentication tag for AES-GCM-SIV MUST be 16 octets. For both AES-GCM and AES-GCM-SIV, the presence of the authentication tag in the Ciphertext field makes it so that a separate Integrity Check Value field in the Encrypted payload is not needed. Note that the ciphertext calculation inputs described in Section 3 of [RFC5282] differ from the inputs used for the AES-GCM-SIV ciphertext calculation.

### 3.2. IKEv2 Keying Material

Parties in IKEv2 generate a quantity called SKEYSEED from which all keys used in the IKEv2 SA are derived (Section 2.14 of [RFC4106]).

AES-GCM-SIV uses one of these keys, SK\_e[i/r], as a key-generating key from which to derive further keying material. SK\_e[i/r] is either 128 or 256 bits, depending on whether AES-128 or AES-256 is in use. In particular, the key-generating key and the 96-bit nonce are used to derive a 128-bit message-authentication key and either a 128-bit or 256-bit (consistent with the length of the key-generating key, for use in AES-128 or AES-256 respectively) message-encryption key (see Section 4 of [RFC8452]).

Note that this process differs from the encryption method employed by AES-GCM, in which (SK\_e[i/r]) is used directly (instead of being used first to generate a message-encryption key).

The authentication keys SK\_a[i/r] from SKEYSEED are treated as having a length of zero octets and are not used, consistent with the treatment of SK\_a[i/r] for AES-GCM by Section 7.1 of [RFC5282].

### 3.3. Associated Data Construction

The construction of the associated data for AES-GCM-SIV (referred to as "additional data" by [RFC8452]) is as specified for AES-GCM in Section 5.1 of [RFC5282].

## 4. AES-GCM-SIV in ESP

### 4.1. ESP Payload Data

ESP packets contain a variable-length field, called Payload Data [RFC4303]. The format of the Payload Data field is dependent upon the encryption algorithm being used. In the case of AES-GCM-SIV, the ESP Payload Data field is composed of two subfields:

- \* Nonce: a twelve-octet AES-GCM-SIV nonce, followed by
- \* Ciphertext: a variable-length ciphertext.

The Nonce field contains a randomly-generated 96-bit (12-octet) value.

Note that the nonce is akin to the 8-octet Initialization Vector shown in Figure 1 of [RFC4106].

The instantiation of the Ciphertext field is consistent with the specification for AES-GCM in Section 3.2 of [RFC4106]. Note that while the AES-GCM-SIV ciphertext as per [RFC8452] contains a 16-octet authentication tag at the end, this tag MUST NOT be included in the Ciphertext field here; it is instead included as the Integrity Check Value (discussed in Section 4.2).

[EDNOTE: Is this the preferred way to format AEADs for ESP (vs. including the authentication tag in the Ciphertext field and leaving the ICV field empty)? It seems to be what other RFCs have done.]

### 4.2. ESP Integrity Check Value (ICV)

The ESP Packet Format depicted in Figure 1 of [RFC4303] includes a variable-length Integrity Check Value (ICV) field.

This field contains the AES-GCM-SIV 16-octet authentication tag (i.e., the last 16 octets of the AES-GCM-SIV ciphertext).

The ICV is the 16-octet AES-GCM-SIV Authentication Tag.

### 4.3. ESP Keying Material

The transform keys are extracted from the KEYMAT as defined in Section 2.17 of [RFC4106]. When AES-GCM-SIV with AES-128 is used, 16 octets are extracted; when AES-GCM-SIV with AES-256 is used, 32 octets are extracted.

#### 4.4. Additional Authenticated Data Construction

The construction of the Additional Authenticated Data (AAD) for AES-GCM-SIV is as specified for AES-GCM-SIV in Section 5 of [RFC4106].

#### 5. Security Considerations

This document inherits the security considerations of [RFC8452].

#### 6. Operational Considerations

Implementers of IPsec may assess the benefits and drawbacks of using AES-GCM-SIV in a given deployment scenario versus another AEAD algorithm. While AES-GCM-SIV decryption speed is comparable to that of AES-GCM, its encryption runs at about two thirds the speed of AES-GCM encryption. Because of this, it is not prudent to view AES-GCM-SIV as a blanket replacement for AES-GCM. [RFC8452] recommends that AES-GCM-SIV be used in any scenario where nonce uniqueness cannot be guaranteed, such as when there is no stateful counter, or when multiple encryptors use the same key.

#### 7. IANA Considerations

This document adds the following algorithm to the IANA "Transform Type 1 - Encryption Algorithm Transform IDs" registry for use in both IKEv2 and ESP:

+-----+	
Number	Name
+-----+	
TBD	ENCR_AES_GCM_SIV_16
+-----+	

#### 8. References

##### 8.1. Normative References

- [FIPS197] National Institute of Standards and Technology,  
"Recommendation for Block Cipher Modes of Operation:  
Galois/Counter Mode (GCM) and GMAC", November 2007.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate  
Requirement Levels", BCP 14, RFC 2119,  
DOI 10.17487/RFC2119, March 1997,  
<<https://www.rfc-editor.org/info/rfc2119>>.

- [RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, DOI 10.17487/RFC4106, June 2005, <<https://www.rfc-editor.org/info/rfc4106>>.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <<https://www.rfc-editor.org/info/rfc4301>>.
- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <<https://www.rfc-editor.org/info/rfc4303>>.
- [RFC5282] Black, D. and D. McGrew, "Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol", RFC 5282, DOI 10.17487/RFC5282, August 2008, <<https://www.rfc-editor.org/info/rfc5282>>.
- [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <<https://www.rfc-editor.org/info/rfc7296>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8452] Gueron, S., Langley, A., and Y. Lindell, "AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption", RFC 8452, DOI 10.17487/RFC8452, April 2019, <<https://www.rfc-editor.org/info/rfc8452>>.

## 8.2. Informative References

- [RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <<https://www.rfc-editor.org/info/rfc4302>>.

## Authors' Addresses

Rebecca Guthrie  
National Security Agency  
Email: [rmguthr@uwe.nsa.gov](mailto:rmguthr@uwe.nsa.gov)

Casey Wynn  
National Security Agency



Email: cwwynn@uwe.nsa.gov

Nicholas Gajcowski  
National Security Agency  
Email: nhgajco@uwe.nsa.gov