Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol

Abstract

This document describes the usage of Advanced Encryption Standard Counter Mode (AES-CTR), with an explicit Initialization Vector, by the Internet Key Exchange version 2 (IKEv2) protocol, for encrypting the IKEv2 exchanges that follow the IKE_SA_INIT exchange.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5930.
1. Introduction

The Internet Key Exchange version 2 (IKEv2) protocol [RFC4306] is a component of IPSec used for performing mutual authentication and establishing and maintaining security associations (SAs). [RFC4307] defines the set of algorithms that are mandatory to implement as part of IKEv2, as well as algorithms that should be implemented because they may be promoted to mandatory at some future time. [RFC4307] requires that an implementation "SHOULD" support Advanced Encryption Standard [AES] Counter Mode [MODES] (AES-CTR) as a Transform Type 1 algorithm (encryption).

Although [RFC4307] specifies that the AES-CTR encryption algorithm feature SHOULD be supported by IKEv2, no existing document specifies how IKEv2 can support the feature. This document provides the specification and usage of AES-CTR Counter Mode by IKEv2.

Implementers need to carefully consider the use of AES-CTR over the mandatory-to-implement algorithms in [RFC4307], because the performance improvements of AES-CTR are minimal in the context of...
IKEv2. Furthermore, these performance improvements may be offset by the Counter Mode specific risk of a minor, hard-to-detect implementation issue resulting in total security failure.

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].

2. IKEv2 Encrypted Payload

Section 3.14 of IKEv2 [RFC4306] explains the IKEv2 Encrypted Payload. The Encrypted Payload, denoted SK(...), contains other IKEv2 payloads in encrypted form.

The payload includes an Initialization Vector (IV) whose length is defined by the encryption algorithm negotiated. It also includes Integrity Checksum data. These two fields are not encrypted.

The IV field MUST be 8 octets when the AES-CTR algorithm is used for IKEv2 encryption. The requirements for this IV are the same as what is specified for the Encapsulating Security Payload (ESP) in Section 3.1 of [RFC3686].

IKEv2 requires Integrity Check Data for the Encrypted Payload as described in Section 3.14 of [RFC4306]. The choice of integrity algorithms in IKEv2 is defined in [RFC4307] or documents that update it in the future.

When AES-CTR is used in IKEv2, no padding is required. The Padding field of the Encrypted Payload SHOULD be empty, and the Pad Length field SHOULD be zero. However, according to [RFC4306], the recipient MUST accept any length that results in proper alignment. It should be noted that the ESP [RFC4303] Encrypted Payload requires alignment on a 4-byte boundary while the IKEv2 [RFC4306] Encrypted Payload does not have such a requirement.

The Encrypted Payload is the XOR of the plaintext and key stream. The key stream is generated by inputting counter blocks into the AES algorithm. The AES counter block is 128 bits, including a 4-octet Nonce, 8-octet Initialization Vector, and 4-octet Block Counter, in that order. The Block Counter begins with the value of one and increments by one to generate the next portion of the key stream. The detailed requirements for the counter block are the same as those specified in Section 4 of [RFC3686].
3. IKEv2 Conventions

The use of AES-CTR for the IKE SA is negotiated in the same way as AES-CTR for ESP. The Transform ID (ENCR_AES_CTR) is the same; the key length transform attribute is used in the same way; and the keying material (consisting of the actual key and the nonce) is derived in the same way. See Section 5 of [RFC3686] for detailed descriptions.

4. Security Considerations

Security considerations explained in Section 7 of [RFC3686] are entirely relevant to this document as well. The security considerations on fresh keys and integrity protection in Section 7 of [RFC3686] are totally applicable to using AES-CTR in IKEv2; see [RFC3686] for details. As static keys are never used in IKEv2 for IKE_SA and integrity protection is mandatory for IKE_SA, these issues are not applicable for AES-CTR in IKEv2 when protecting IKE_SA.

Additionally, since AES has a 128-bit block size, regardless of the mode employed, the ciphertext generated by AES encryption becomes distinguishable from random values after $2^{64}$ blocks are encrypted with a single key. Since IKEv2 SA cannot carry that much data (because of the size limit of the message ID of the IKEv2 message and the requirements for the message ID in Section 4 of [RFC4306]), this issue is not a concern here.

For generic attacks on AES, such as brute force or precalculations, the key-size requirements provide reasonable security [Recommendations].

5. IANA Considerations

IANA [IANA-Para] has assigned an Encryption Algorithm Transform ID for AES-CTR encryption with an explicit IV for IKEv2: 13 as the number, and ENCR_AES_CTR as the name. IANA has added a reference to this RFC in that entry.

6. Acknowledgments

The authors thank Yaron Sheffer, Paul Hoffman, Tero Kivinen, and Alfred Hoenes for their direction and comments on this document.

This document specifies usage of AES-CTR with IKEv2, similar to usage of AES-CTR with ESP as specified in [RFC3686]. The reader is referred to [RFC3686] for the same descriptions and definitions. The authors thank Russ Housley for providing the document.
During the production and modification of this document, both Huawei and CNNIC supported one of the authors, Sean Shen. Both are appreciated as affiliations of the author.

7. References

7.1. Normative References


7.2. Informative References


Authors’ Addresses

Sean Shen
Huawei
4, South 4th Street, Zhongguancun
Beijing 100190
China
EMail: shenshuo@cnnic.cn

Yu Mao
Hangzhou H3C Tech. Co., Ltd.
Oriental Electronic Bld., No. 2 Chuangye Road Shang-Di Information Industry Hai-Dian District Beijing 100085 China
EMail: yumao9@gmail.com

N S Srinivasa Murthy
Freescale Semiconductor
UMA PLAZA, NAGARJUNA CIRCLE, PUNJAGUTTA HYDERABAD 500082 INDIA
EMail: ssmurthy.nittala@freescale.com