The CLEFIA Cipher Algorithm and Its Use with IPsec
draft-katagi-ipsecme-clefia-00

Abstract

This document describes the use of the CLEFIA block cipher algorithm in conjunction with several different modes of operation within IKE and IPsec.

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 http://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 April 24, 2012.

Copyright Notice

Copyright (c) 2011 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 (http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
Table of Contents

1. Introduction ......................................................... 3
   1.1. CLEFIA ......................................................... 3
2. Modes of Operation .................................................. 4
   2.1. Encryption ..................................................... 4
   2.2. Message Authentication Codes (MACs) .......................... 4
   2.3. Authenticated Encryption ...................................... 4
   2.4. Pseudo Random Functions (PRFs) .............................. 5
3. IKEv1 Conventions .................................................... 6
   3.1. Phase 1 Identifier ............................................. 6
   3.2. Phase 2 Identifier ............................................. 6
4. IKEv2 Conventions .................................................... 7
   4.1. Transform Type 1 ............................................... 7
   4.2. Transform Type 2 ............................................... 7
   4.3. Transform Type 3 ............................................... 7
5. Security Considerations .............................................. 8
6. IANA Considerations .................................................. 9
7. References ........................................................... 11
   7.1. Normative References ........................................... 11
   7.2. Informative References ......................................... 12
Authors’ Addresses ..................................................... 14
1. Introduction

This document describes the use of the CLEFIA block cipher algorithm [RFC6114] in conjunction with several different modes of operation within IKEv1 [RFC2409], IKEv2 [RFC5996], IPsec-v2 ([RFC2401], [RFC2402], [RFC2406]), and IPsec-v3 ([RFC4301], [RFC4302], [RFC4303]).

1.1. CLEFIA

CLEFIA is a 128-bit blockcipher algorithm, with key lengths of 128, 192, and 256 bits. The algorithm of CLEFIA was published in 2007 [FSE07]. Since AES was designed, cryptographic technologies have been advancing: new techniques on attack, design and implementation are extensively studied. CLEFIA is designed based on the state-of-the-art techniques on design and analysis of block ciphers. The security of CLEFIA has been scrutinized in the public community, and no security weaknesses have been reported so far.

CLEFIA is a general purpose blockcipher, and offers high performance in software and hardware. Especially, CLEFIA has an advantage in efficient hardware implementation over AES, Camellia, and SEED, which can be used in IPsec. Its gate efficiency, which is defined as the ratio of speed to gate size, is superior to these ciphers [ISCAS08].

Standardization of CLEFIA in other organizations is in progress. CLEFIA is proposed in ISO/IEC 29192-2 [ISO29192-2] and the CRYPTREC project for the revision of the e-Government recommended ciphers list in Japan [CRYPTREC]. ISO/IEC 29192 is a standardization project of "LightWeight Cryptography (LWC)", which is a cryptographic algorithm or protocol tailored for implementation in constrained environments including RFID tags, sensors, contactless smart cards and so on. LWC contributes to the security of the constrained devices connecting with IP.

The algorithm specification is described in RFC6114 [RFC6114]. Further information about CLEFIA, which includes design rationale, security evaluations, implementation results, and a reference code, is available from [CLEFIAWEB].
2. Modes of Operation

CLEFIA is a 128-bit blockcipher algorithm, with key lengths of 128, 192, and 256 bits. CLEFIA has a common interface with the Advanced Encryption Standard (AES) [FIPS-197] in terms of a block size and key lengths. Therefore, CLEFIA modes of operation are easily defined by replacing AES in modes of operation previously defined within IPsec/IKE without any limitation. The only difference is that the underlying encryption primitive is CLEFIA instead of AES.

2.1. Encryption

CBC mode and Counter mode are encryption modes that are based on a block cipher algorithm.

The use of CLEFIA in CBC mode (CLEFIA-CBC) and Counter mode (CLEFIA-CTR) for ESP is defined in the same manner as AES-CBC [RFC3602] and AES-CTR [RFC3686].

The use of CLEFIA-CBC for IKEv1 and IKEv2 is also defined in the same manner as [RFC3602] and [RFC5996], respectively. The use of CLEFIA-CTR for IKEv2 is defined in the same manner as [RFC5930].

2.2. Message Authentication Codes (MACs)

Cipher-based Message Authentication Code (CMAC) and Galois Message Authentication Code (GMAC) are message authentication codes that are based on a block cipher algorithm. CMAC and GMAC provide integrity protection of message.

The use of CLEFIA in CMAC mode (CLEFIA-CMAC) and GMAC mode (CLEFIA-GMAC) for ESP is defined in the same manner as AES-CMAC [RFC4494] and AES-GMAC [RFC4543]. The key size supported in CLEFIA-CMAC is 128 bits. CLEFIA-CMAC-96 is the CLEFIA-CMAC with 96-bit truncated output [RFC4494]. The key sizes supported in CLEFIA-GMAC are 128 bits, 192 bits, and 256 bits.

2.3. Authenticated Encryption

CCM mode and Galois/Counter mode are authenticated encryption modes that are based on a block cipher algorithm.

The use of CLEFIA in CCM mode (CLEFIA-CCM) and Galois/Counter mode (CLEFIA-GCM) for ESP is defined in the same manner as AES-CCM [RFC4309] and AES-GCM [RFC4106]. The use of CLEFIA-CCM and CLEFIA-GCM for IKEv2 is defined in the same manner as [RFC5282].

Based on [RFC4309], the size of integrity check value (ICV) in
CLEFIA-CCM also supports 8 octets, 12 octets, and 16 octets. In the similar way, the size of ICV in CLEFIA-GCM supports 8 octets, 12 octets, and 16 octets.

2.4. Pseudo Random Functions (PRFs)

IKEv2 uses pseudo-random functions (PRFs) to generate the secret keys that are used in IKE SAs and IPsec SAs.

In the same manner as AES-CMAC-PRF-128 [RFC4615], CLEFIA-CMAC-PRF-128 is identical to CLEFIA-CMAC defined in Section 2.2 except that the 128-bit key length restriction is removed.
3. IKEv1 Conventions

As mentioned in Section 2, CLEFIA has a common interface with AES. Identifiers in Phase 1 and Phase 2 are defined in Section 6.

3.1. Phase 1 Identifier

For IKE phase 1 negotiations, IANA is requested to assign an Encryption Algorithm Identifier for CLEFIA-CBC. The assigned identifier is shown in Section 6.

3.2. Phase 2 Identifier

For IKE phase 2 negotiations, IANA is requested to assign nine IPsec ESP Transform Identifiers for CLEFIA-CBC, CLEFIA-CTR, CLEFIA-CCM, and CLEFIA-GCM and three identifiers for CLEFIA-GMAC in the Authentication Algorithms registry. The assigned identifiers are shown in Section 6.
4. IKEv2 Conventions

As mentioned in Section 2, CLEFIA has a common interface with AES. Identifiers in IKEv2 Transform Types are defined in Section 6.

4.1. Transform Type 1

For IKEv2 negotiations, IANA is requested to assign Transform Type 1 identifiers for CLEFIA-CBC, CLEFIA-CTR, CLEFIA-CCM, and CLEFIA-GCM. The assigned identifiers are shown in Section 6.

4.2. Transform Type 2

For IKEv2 negotiations, IANA is requested to assign Transform Type 2 identifiers for CLEFIA-CMAC. The assigned identifier is shown in Section 6.

4.3. Transform Type 3

For IKEv2 negotiations, IANA is requested to assign Transform Type 3 identifiers for CLEFIA-CMAC and CLEFIA-GMAC. The assigned identifiers are shown in Section 6.
5. Security Considerations

The security of CLEFIA algorithm has been scrutinized in the public community since the algorithm was proposed, and no security weaknesses have been reported so far.

For other security considerations, please refer to the security considerations in previous RFCs ([RFC3602], [RFC3686], [RFC4106], [RFC4309], [RFC4494], [RFC4543], [RFC5930], and [RFC5996]). These apply to this document as well.
6. IANA Considerations

IANA is requested to allocate the Encryption Algorithm Class Values (Value 1) in the "Internet Key Exchange (IKE) attributes" registry:

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TBD1&gt;</td>
<td>CLEFIA-CBC</td>
</tr>
</tbody>
</table>

IANA is also requested to allocate the following values in the "Internet Security Association and Key Management Protocol (ISAKMP) Identifiers" registry:

### IPsec ESP Transform Identifiers

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TBD1&gt;</td>
<td>ESP_CLEFIA-CBC</td>
</tr>
<tr>
<td>&lt;TBD2&gt;</td>
<td>ESP_CLEFIA-CTR</td>
</tr>
<tr>
<td>&lt;TBD3&gt;</td>
<td>ESP_CLEFIA-CCM_8</td>
</tr>
<tr>
<td>&lt;TBD4&gt;</td>
<td>ESP_CLEFIA-CCM_12</td>
</tr>
<tr>
<td>&lt;TBD5&gt;</td>
<td>ESP_CLEFIA-CCM_16</td>
</tr>
<tr>
<td>&lt;TBD6&gt;</td>
<td>ESP_CLEFIA-GCM_8</td>
</tr>
<tr>
<td>&lt;TBD7&gt;</td>
<td>ESP_CLEFIA-GCM_12</td>
</tr>
<tr>
<td>&lt;TBD8&gt;</td>
<td>ESP_CLEFIA-GCM_16</td>
</tr>
<tr>
<td>&lt;TBD9&gt;</td>
<td>ESP_NULL_AUTH_CLEFIA-GMAC</td>
</tr>
</tbody>
</table>

### Authentication Algorithms sub-registry

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TBD1&gt;</td>
<td>CLEFIA-128-GMAC</td>
</tr>
<tr>
<td>&lt;TBD2&gt;</td>
<td>CLEFIA-192-GMAC</td>
</tr>
<tr>
<td>&lt;TBD3&gt;</td>
<td>CLEFIA-256-GMAC</td>
</tr>
</tbody>
</table>

IANA is also requested to allocate the following values in the "Internet Key Exchange Version 2 (IKEv2) Parameters" registry:

### Transform Type 1 - Encryption Algorithm Transform IDs

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TBD1&gt;</td>
<td>ENCR_CLEFIA_CBC</td>
</tr>
<tr>
<td>&lt;TBD2&gt;</td>
<td>ENCR_CLEFIA_CTR</td>
</tr>
<tr>
<td>&lt;TBD3&gt;</td>
<td>ENCR_CLEFIA_CCM_8</td>
</tr>
<tr>
<td>&lt;TBD4&gt;</td>
<td>ENCR_CLEFIA_CCM_12</td>
</tr>
<tr>
<td>&lt;TBD5&gt;</td>
<td>ENCR_CLEFIA_CCM_16</td>
</tr>
<tr>
<td>&lt;TBD6&gt;</td>
<td>ENCR_CLEFIA_GCM_8</td>
</tr>
<tr>
<td>&lt;TBD7&gt;</td>
<td>ENCR_CLEFIA_GCM_12</td>
</tr>
<tr>
<td>&lt;TBD8&gt;</td>
<td>ENCR_CLEFIA_GCM_16</td>
</tr>
<tr>
<td>&lt;TBD9&gt;</td>
<td>ENCR_NULL_AUTH_CLEFIA_GMAC</td>
</tr>
</tbody>
</table>
Transform Type 2 - Pseudo-random Function Transform IDs

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TBD1&gt;</td>
<td>PRF_CLEFIA128_CMAC</td>
</tr>
</tbody>
</table>

Transform Type 3 - Integrity Algorithm Transform IDs

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TBD1&gt;</td>
<td>AUTH_CLEFIA_128_CMAC_96</td>
</tr>
<tr>
<td>&lt;TBD2&gt;</td>
<td>AUTH_CLEFIA_128_GMAC</td>
</tr>
<tr>
<td>&lt;TBD3&gt;</td>
<td>AUTH_CLEFIA_192_GMAC</td>
</tr>
<tr>
<td>&lt;TBD4&gt;</td>
<td>AUTH_CLEFIA_256_GMAC</td>
</tr>
</tbody>
</table>
7. References

7.1. Normative References


7.2. Informative References


Authors’ Addresses

Masanobu Katagi
Sony Corporation
Phone: +81-3-5448-3701
Fax: +81-3-5448-6438
Email: Masanobu.Katagi@jp.sony.com

Shiho Moriai
Sony Corporation
Phone: +81-3-5448-3701
Fax: +81-3-5448-6438
Email: Shiho.Moriai@jp.sony.com