INTERNET-DRAFT
Obsoletes RFCs 2402 and 2406
Expires: February 2005

Donald E. Eastlake 3rd
Motorola Laboratories

August 2004

# Cryptographic Algorithm Implementation Requirements For ESP And AH

<draft-ietf-ipsec-esp-ah-algorithms-02.txt>

## Status of This Document



## Abstract

The IPsec series of protocols makes use of various cryptographic algorithms in order to provide security services. The Encapsulating Security Payload (ESP) and the Authentication Header (AH) provide two mechanisms for protecting data being sent over an IPsec Security Association (SA). To ensure interoperability between disparate implementations it is necessary to specify a set of mandatory-to-implement algorithms to ensure at least one algorithm that all implementations will have available. This document defines the current set of mandatory-to-implement algorithms for ESP and AH as well as specifying algorithms that should be implemented because they may be promoted to mandatory at some future time.

Acknowledgement

Much of the wording herein was adapted from "Cryptographic Algorithms for use in the Internet Key Exchange Version 2" <draft-ietf-ipsec-ikev2-algorithms-*.txt> by Jeffrey I. Schiller.

Table of Contents

## 1. Introduction

The Encapsulating Security Payload (ESP) and the Authentication Header (AH) provide two mechanisms for protecting data being sent over an IPsec Security Association (SA) [IPsec, ESP, AH]. To ensure interoperability between disparate implementations it is necessary to specify a set of mandatory-to-implement algorithms to ensure at least one algorithm that all implementations will have available. This document defines the current set of mandatory-to-implement algorithms for ESP and AH as well as specifying algorithms that should be implemented because they may be promoted to mandatory at some future time.

The nature of cryptography is that new algorithms surface continuously and existing algorithms are continuously attacked. An algorithm believed to be strong today may be demonstrated to be weak tomorrow. Given this, the choice of mandatory-to-implement algorithm should be conservative so as to minimize the likelihood of it being compromised quickly. Thought should also be given to performance considerations as many uses of IPsec will be in environments where performance is a concern.

Finally we need to recognize that the mandatory-to-implement algorithm(s) may need to change over time to adapt to the changing world. For this reason the selection of mandatory-to-implement algorithms is not included the main IPsec, ESP, or AH specifications. It is instead placed in this document. As the choice of algorithm changes, only this document should need to be updated.

Ideally the mandatory-to-implement algorithm of tomorrow should already be available in most implementations of IPsec by the time it is made mandatory. To facilitate this we will attempt to identify such algorithms as they are known today in this document. There is no guarantee that the algorithms we believe today may be mandatory in the future will in fact become so. All algorithms known today are subject to cryptographic attack, and may be broken in the future.

## 2. Requirements Terminology

Keywords "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT" and "MAY" that appear in this document are to be interpreted as described in [RFC 2119].

In addition we will define some additional terms here:

SHOULD+  This term means the same as SHOULD. However it is likely that an algorithm marked as SHOULD+ will be promoted at

some future time to be a MUST.

| | |
|---|---|
| SHOULD- | This terms means the same as SHOULD. However it is likely that an algorithm marked as SHOULD- will be deprecated to a MAY or worse in a future version of this document. |
| MUST- | This term means the same as MUST. However we expect at some point in the future this algorithm will no longer be a MUST. |

## 3. Algorithm Selection

For IPsec implementations to interoperate, they must support one or more security algorithms in common. This section specifies the security algorithm implementation requirements for standards comformant ESP and AH implementations. The security algorithms actually used for any particular ESP or AH security association is determined by a negotiation mechahism, such as the Internet Key Exchange (IKE [RFC 2409, IKEv2]), or pre-establishment.

Of course, additional standard and proprietary algorithms beyond those listed below can be implemented.

### 3.1 Encapsulating Security Payload

The implementation conformance requirements for security algorithms for ESP are given in the tables below. See section 2 for definitions of the values in the "Requirement" column.

#### 3.1.1 ESP Encryption and Authentication Algorithms

These tables list encryption and authentication algorithms for the IPsec Encapsulating Security Payload protocol.

| Requirement | Encryption Algorithm (notes) |
|---|---|
| MUST | NULL (1) |
| MUST- | TripleDES-CBC [RFC 2451] |
| SHOULD+ | AES-CBC with 128-bit keys [RFC 3602] |
| SHOULD | AES-CTR [RFC 3686] |
| SHOULD NOT | DES-CBC [RFC 2405] (3) |

| Requirement | Authentication Algorithm (notes) |
|---|---|
| MUST | HMAC-SHA1-96 [RFC 2404] |
| MUST | NULL (1) |

SHOULD+ AES-XCBC-MAC-96 [RFC 3566]

| | |
|---|---|
| MAY | HMAC-MD5-96 [RFC 2403] (2) |

Notes:

1. Since ESP encryption and authentication are optional, support for the two "NULL" algorithms is required to maintain consistency with the way these services are negotiated. NOTE that while authentication and encryption can each be "NULL", they MUST NOT both be "NULL".
2. Weaknesses have become apparent in MD5, however these should not effect the use of MD5 with HMAC.
3. DES, with its small key size and publicly demonstrated and open design special purpose cracking hardware, is of questionable security for general use.

### 3.1.2 ESP Combined Mode Algorithms

As specified in [ESP], combined mode algorithms are supported which provide both confidentiality and authentication services. Support of such algorithms will require proper structuring of ESP implementations. Under many circumstances, combined mode algorithms provide significant efficiency and throughput advantages. Although there are no suggested or required combined algorithms at this time, AES-CCM [CCM], which has been adopted as the prefered mode for security in IEEE 802.11 [802.11i], is expected to be of interest in the near future.

## 3.2 Authentication Header

The implementation conformance requirements for security algorithms for AH are given below. See section 2 for definitions of the values in the "Requirement" column. As you would suspect, all of these algorithms are authentication algorithms.

| Requirement | Algorithm (notes) |
|---|---|
| MUST | HMAC-SHA1-96 [RFC 2404] |
| SHOULD+ | AES-XCBC-MAC-96 [RFC 3566] |
| MAY | HMAC-MD5-96 [RFC 2403] (1) |

Notes:

1. Weaknesses have become apparent in MD5, however these should not effect the use of MD5 with HMAC.

## 4. Security Considerations

The security of cryptographic based systems depends on both the strength of the cryptographic algorithms chosen, the strength of the keys used with those algorithms and the engineering and administration of the protocol used by the system to ensure that there are no non-cryptographic ways to bypass the security of the overall system.

This document concerns itself with the selection of cryptographic algorithms for the use of ESP and AH, specifically with the selection of "Mandatory-to-Implement" algorithms. The algorithms identified in this document as MUST implement or SHOULD implement are not known to be broken at the current time and cryptographic research so far leads us to believe that they will likely remain secure into the foreseeable future. However, this is not necessarily forever. We would therefore expect that new revisions of this document will be issued from time to time that reflect the current best practice in this area.

## 5. IANA Considerations

This document does not define any new registries nor elements in existing registries.

## 6. Changes from RFC 2402 and 2406

[RFC 2402] and [RFC 2406] defined the IPsec Authentication Header and IPsec Encapsulating Security Payload. Each specified the implementation requirements for cryptogrpahic algorithms for their respectively protocols. They have now been replaced with [AH] and [ESP], which do not specify cryptographic algorithm implementation requirements, and this document which specifies such requirements for both [AH] and [ESP].

The implementation requirements are compared below:

| Old Req. | Old RFC(s) | New Requirement | Algorithm (notes) |
|---|---|---|---|
| MUST | 2406 | SHOULD NOT | DES-CBC [RFC 2405] (1) |
| MUST | 2402 2406 | MAY | HMAC-MD5-96 [RFC 2403] |
| MUST | 2402 2406 | MUST | HMAC-SHA1-96 [RFC 2404] |

Notes:

1. The IETF deprecated the use of single DES years ago and has not

included it in any new standard for some time (see IESG note on the first page of [RFC 2407]). But this document represents the first standards track recognition of that deprecation by specifying that implementations SHOULD NOT provide single DES. The US Government National Institute of Standards and Technology (NIST) has formally recognized the weakness of single DES by a notice published in the 26 July 2004 US Government Federal Register (Docket No. 040602169-4169-01) proposing to withdraw it as a US Government Standard. Triple DES remains approved by both the IETF and NIST.

## Normative References

[AH] - "IP Authentication Header", draft-ietf-ipsec-rfc2402bis-*.txt, S. Kent, work in progress.

[ESP] - "IP Encapsulating Security Payload (ESP)", draft-ietf-ipsec-esp-v3-*.txt, S. Kent, work in progress.

[IPsec] - "Security Architecture for the Internet Protocol", draft-ietf-ipsec-rfc2401bis-*.txt, S. Kent, work in progress.

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

[RFC 2403] - "The Use of HMAC-MD5-96 within ESP and AH", C. Madson, and R. Glenn, November 1998.

[RFC 2404] - "The Use of HMAC-SHA-1-96 within ESP and AH", C. Madson, and R. Glenn, November 1998.

[RFC 2405] - "The ESP DES-CBC Cipher Algorithm With Explicit IV", C. Madson, and N. Doraswamy, November 1998.

[RFC 3566] - "The AES-XCBC-MAC-96 Algorithm and Its Use With IPSec", S. Frankel. H. Herbert, September 2003.

[RFC 3602] - "The AES-CBC Cipher Algorithm and Its Use with IPsec", S. Frankel, R. Glenn, S. Kelly, September 2003.

[RFC 3686] - "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", R. Housley, July 2003.

## Informative References

[802.11i] - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements, IEEE Std 802.11i, June 2004.

[AES CCM] - "Using AES CCM Mode With IPsec ESP", draft-ietf-ipsec-ciph-aes-ccm-05.txt which is in the RFC Editor Queue, R. Housley, November 2003.

[IKEv2] - "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-*.txt, C. Kaufman, October 2003.

[RFC 791] - "Internet Protocol", J. Postel, September 1981.

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

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

[RFC 2407] - "The Internet IP Security Domain of Interpretation for ISAKMP", D. Piper, november 1998.

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

Authors Address

Donald E. Eastlake 3rd
Motorola Laboratories
155 Beaver Street
Milford, MA 01757 USA

Telephone:  +1-508-786-7554 (w)
            +1-508-634-2066 (h)
EMail:      Donald.Eastlake@Motorola.com

## Full Copyright Statement



## Expiration and File Name

This draft expires February 2005.

Its file name is draft-ietf-ipsec-esp-ah-algorithms-02.txt.