

Expires: July 2004

Cryptographic Algorithm Implementation Requirements For ESP And AH

<[draft-ietf-ipsec-esp-ah-algorithms-01.txt](#)>

Status of This Document

Distribution of this draft is unlimited. Comments should be sent to the authors.

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#). Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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." The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt> The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

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

Status of This Document.....	1
Copyright Notice.....	1
Abstract.....	1
Acknowledgement.....	2
Table of Contents.....	2
1 . Introduction.....	3
2 . Requirements Terminology.....	3
3 . Algorithm Selection.....	4
3.1 Encapsulating Security Payload.....	4
3.1.1 ESP Encryption and Authentication Algorithms.....	4
3.1.2 ESP Combined Mode Algorithms.....	5
3.2 Authentication Header.....	5
4 . Security Considerations.....	6
5 . IANA Considerations.....	6
Normative References.....	7
Informative References.....	7
Author's Address.....	9
Full Copyright Statement.....	10
Expiration and File Name.....	10

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 in 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.

D. Eastlake 3rd

[Page 3]

- SHOULD- This term 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 conformant ESP and AH implementations. The security algorithms actually used for any particular ESP or AH security association is determined by a negotiation mechanism, 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
-----	-----
MUST	NULL (1)
MUST-	TripleDES-CBC [RFC 2451]
SHOULD+	AES-CBC with 128-bit keys [RFC 3602]
SHOULD	AES-CTR [AES-CTR]
SHOULD NOT	DES-CBC [RFC 2405] (3)

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

SHOULD+

AES-XCBC-MAC-96 [[RFC 3566](#)]

D. Eastlake 3rd

[Page 4]

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 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 is in the process of being adopted as the preferred 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
-----	-----
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 isn't 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.

Normative References

- [AES CTR] - "Using AES Counter Mode With IPsec ESP", [draft-ietf-ipsec-ciph-aes-ctr](#)-.txt, R. Housley, July 2003.
- [AH] - "IP Authentication Header", [draft-ietf-ipsec-rfc2402bis](#)-.txt, S. Kent, September 2003.
- [ESP] - "IP Encapsulating Security Payload (ESP)", [draft-ietf-ipsec-esp-v3](#)-.txt, S. Kent, January 2004.
- [IPSEC] - "Security Architecture for the Internet Protocol", [draft-ietf-ipsec-rfc2401bis](#)-.txt, S. Kent, October 2003.
- [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 2406] - "IP Encapsulating Security Payload (ESP)", S. Kent, R. Atkinson, 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.

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/D7.0, October 2003.
- [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.

D. Eastlake 3rd

[Page 7]

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

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

Author's 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)
E-Mail: Donald.Eastlake@Motorola.com

Full Copyright Statement

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Expiration and File Name

This draft expires July 2004.

Its file name is [draft-ietf-ipsec-esp-ah-algorithms-01.txt](#).

