

Cryptographic Algorithm Implementation Requirements for
Encapsulating Security Payload (ESP) and Authentication Header (AH)

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

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 that there is 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.

Table of Contents

1. Introduction	2
2. Requirements Terminology	3
3. Algorithm Selection	3
3.1. Encapsulating Security Payload	3
3.1.1. ESP Encryption and Authentication Algorithms	4
3.1.2. ESP Combined Mode Algorithms	4
3.2. Authentication Header	5
4. Security Considerations	5
5. Acknowledgement	5
6. Changes from RFC 2402 and 2406	6
7. Normative References	6
8. Informative References	7

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 that there is 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 [RFC2119].

We 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 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 that 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 are determined by a negotiation mechanism, such as the Internet Key Exchange (IKE [RFC2409, 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 [RFC2451]
SHOULD+	AES-CBC with 128-bit keys [RFC3602]
SHOULD	AES-CTR [RFC3686]
SHOULD NOT	DES-CBC [RFC2405] (3)

Requirement	Authentication Algorithm (notes)
-----	-----
MUST	HMAC-SHA1-96 [RFC2404]
MUST	NULL (1)
SHOULD+	AES-XCBC-MAC-96 [RFC3566]
MAY	HMAC-MD5-96 [RFC2403] (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 affect 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 that 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 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 (notes)
-----	-----
MUST	HMAC-SHA1-96 [RFC2404]
SHOULD+	AES-XCBC-MAC-96 [RFC3566]
MAY	HMAC-MD5-96 [RFC2403] (1)

Note:

(1) Weaknesses have become apparent in MD5; however, these should not affect 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 and the strength of the keys used with those algorithms. The security also depends on 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. Acknowledgement

Much of the wording herein was adapted from [RFC 4307](#), "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2", by Jeffrey I. Schiller.

6. Changes from RFC 2402 and 2406

[RFC2402] and [RFC2406] defined the IPsec Authentication Header and IPsec Encapsulating Security Payload. Each specified the implementation requirements for cryptographic algorithms for their respective 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 [RFC2405] (1)
MUST	2402 2406	MAY	HMAC-MD5-96 [RFC2403]
MUST	2402 2406	MUST	HMAC-SHA1-96 [RFC2404]

Note:

- (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 [RFC2407]). 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.

7. Normative References

- [AH] Kent, S., "IP Authentication Header", RFC 4302, December 2005.
- [ESP] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.
- [IPsec] Kent, S., "Security Architecture for the Internet Protocol", RFC 4301, December 2005.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

- [RFC2403] Madson, C. and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", [RFC 2403](#), November 1998.
- [RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", [RFC 2404](#), November 1998.
- [RFC2405] Madson, C. and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", [RFC 2405](#), November 1998.
- [RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", [RFC 3566](#), September 2003.
- [RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", [RFC 3602](#), September 2003.
- [RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", [RFC 3686](#), January 2004.

8. 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.
- [JIS] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", [RFC 4307](#), December 2005.
- [CCM] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", [RFC 3686](#), January 2004.
- [IKEv2] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", [RFC 4306](#), December 2005.
- [RFC791] Postel, J., "Internet Protocol", STD 5, [RFC 791](#), September 1981.
- [RFC2402] Kent, S. and R. Atkinson, "IP Authentication Header", [RFC 2402](#), November 1998.
- [RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", [RFC 2406](#), November 1998.

- [RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", [RFC 2407](#), November 1998.
- [RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", [RFC 2409](#), November 1998.

Author's Address

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

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

Full Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.