

Cryptographic Algorithms for use in the  
Internet Key Exchange Version 2  
<[draft-ietf-ipsec-ikev2-algorithms-05.txt](#)>

Status of this Memo

This document is a submission by the IPSEC Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the [ipsec@lists.tislabs.com](mailto:ipsec@lists.tislabs.com) mailing list.

Distribution of this memo is unlimited.

This document is an Internet Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#) [[RFC2026](#)]. Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and 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."

To learn the current status of any Internet Draft, please check the "lid-abstracts.txt" listing contained in the Internet Drafts Shadow Directories on [ftp.is.co.za](ftp://ftp.is.co.za) (Africa), [nic.nordu.net](ftp://nic.nordu.net) (Europe), [munniari.oz.au](ftp://munniari.oz.au) (Australia), [ds.internic.net](ftp://ds.internic.net) (US East Coast), or [ftp.isi.edu](ftp://ftp.isi.edu) (US West Coast).

## [1.](#) Abstract

The IPSec series of protocols makes use of various cryptographic algorithms in order to provide security services. The Internet Key Exchange (IKE [[RFC2409](#)] and IKEv2 [[IKEv2](#)]) provide a mechanism to negotiate which algorithms should be used in any given association. However 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 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.

## [2.](#) Introduction

The Internet Key Exchange protocol provides for the negotiation of cryptographic algorithms between both end points of a cryptographic

association. Different implementations of IPSec and IKE may provide different algorithms. However the IETF desires that all implementations should have some way to interoperate. In particular, this requires that IKE define a set of mandatory-to-implement algorithms, since IKE itself uses such algorithms as part of its own negotiations. This requires that some set of algorithms be specified as "mandatory-to-implement" for IKE.

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 was removed from the main IKEv2 specification and 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 those algorithms (that 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.

### [3. 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](#)].

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 an algorithm marked as SHOULD- may be deprecated to a MAY in a future version of this document.

MUST-	This term means the same as MUST. However we expect at some point that this algorithm will no longer be a MUST in a future document. Although its status will be determined at a later time, it is reasonable to expect that if a future revision of a document alters the status of a MUST-algorithm, it will remain at least a SHOULD or a SHOULD-.
-------	---

### [4. Algorithm Selection](#)

#### [4.1. IKEv2 Algorithm Selection](#)

##### [4.1.1. Encrypted Payload Algorithms](#)

The IKEv2 Encrypted Payload requires both a confidentiality algorithm and an integrity algorithm.

For confidentiality, implementations MUST implement 3DES-CBC and SHOULD+ implement AES-128-CBC. For integrity, HMAC-SHA1 MUST be implemented.

#### [4.1.2.](#) Diffie-Hellman Groups

There are several MODP groups that are defined for use in IKEv2. They are defined in both the IKEv2 base document and in the MODP extensions document. They are identified by group number. Any groups not listed here are considered as "MAY be implemented".

Group Number	Bit Length	Status	Defined
2	1024 MODP Group	MUST-	[ <a href="#">RFC2409</a> ]
14	2048 MODP Group	SHOULD+	[ <a href="#">RFC3526</a> ]

#### [4.1.3.](#) IKEv2 Transform Type 1 Algorithms

IKEv2 Defines several possible algorithms for Transfer Type 1 (encryption). These are defined below with their implementation status.

Name	Number	Defined In	Status
RESERVED	0		
ENCR_3DES	3	[ <a href="#">RFC2451</a> ]	MUST-
ENCR_NULL	11	[ <a href="#">RFC2410</a> ]	MAY

ENCR_AES_CBC	12	[AES-CBC]	SHOULD+
ENCR_AES_CTR	13	[AES-CTR]	SHOULD

#### [4.1.4.](#) IKEv2 Transform Type 2 Algorithms

Transfer Type 2 Algorithms are pseudo-random functions used to generate random values when needed.

Name	Number	Defined In	Status
RESERVED	0		
PRF_HMAC_MD5	1	[ <a href="#">RFC2104</a> ]	MAY
PRF_HMAC_SHA1	2	[ <a href="#">RFC2104</a> ]	MUST
PRF_AES128_CBC	4	[AESPRF]	SHOULD+

#### [4.1.5.](#) IKEv2 Transform Type 3 Algorithms

Transfer Type 3 Algorithms are Integrity algorithms used to protect data against tampering.

Name	Number	Defined In	Status
NONE	0		
AUTH_HMAC_MD5_96	1	[ <a href="#">RFC2403</a> ]	MAY
AUTH_HMAC_SHA1_96	2	[ <a href="#">RFC2404</a> ]	MUST
AUTH_AES_XCBC_96	5	[AES-MAC]	SHOULD+

### [5.](#) 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 of the protocol used by the system to ensure that there are no non-cryptographic ways to bypass the security of the overall system.

Draft-ietf-ipsec-ikev2-algorithms-05.txt

April 2004

This document concerns itself with the selection of cryptographic algorithms for the use of IKEv2, 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.

## [6. IANA Considerations](#)

This document does not define any new registries nor elements in existing registries. Values given here for various algorithms are assigned in other documents and referenced here for convenience and clarity.

## [7. Normative References](#)

- [[RFC2026](#)] S. Bradner, "[RFC2026](#) The Internet Standards Process -- Revision 3", [RFC2026](#), 1996
- [[RFC2409](#)] Harkins, D., Carrel, D., "[RFC 2409](#) The Internet Key Exchange (IKE)", [RFC2409](#), 1998
- [IKEv2] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol", <[draft-ietf-ipsec-ikev2-06.txt](#)>, 2003
- [[RFC2119](#)] S. Bradner, "[RFC2119](#) Key words for use in RFCs to Indicate Requirement Levels.", [RFC2119](#), 1997
- [[RFC3526](#)] T. Kivinen, M. Kojo., "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exch", , 2003
- [[RFC2451](#)] R. Pereira, R. Adams, "The ESP CBC-Mode Cipher Algorithms", [RFC2451](#), 1998
- [[RFC2410](#)] R. Glenn, S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", [RFC2410](#), 1998
- [AES-CBC] S. Frankel, S. Kelly, R. Glenn, "The AES Cipher Algorithm and Its Use With IPsec", <[draft-ietf-ipsec-ciph-aes-cbc-05.txt](#)>, 2003
- [AES-CTR] R. Housley, "Using AES Counter Mode With IPsec ESP", <[draft-ietf-ipsec-ciph-aes-ctr-05.txt](#)>, 2003
- [[RFC2104](#)] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", [RFC2104](#), 1997

- [AESPRF] P. Hoffman, "The AES-XCBC-PRF-128 algorithm for IKE",  
<[draft-hoffman-ipsec-aes-prf-00.txt](#)>, 2003
- [[RFC2403](#)] C. Madson, R. Glenn, "The Use of HMAC-MD5-96 within ESP  
and AH", [RFC2403](#), 1998
- [[RFC2404](#)] C. Madson, R. Glenn, "The Use of HMAC-SHA-1-96 within ESP  
and AH", [RFC2404](#), 1998
- [AES-MAC] S. Frankel, H. Herbert, "The AES-XCBC-MAC-96 Algorithm and  
Its Use With IPsec", <[draft-ietf-ipsec-ciph-aes-xcbc-mac-04.txt](#)>, 2003

## [8.](#) Author's Contact Information

Jeffrey I. Schiller  
Massachusetts Institute of Technology  
Room W92-190  
[77](#) Massachusetts Avenue  
Cambridge, MA 02139-4307  
USA

Phone: +1 (617) 253-0161  
E-mail: [jis@mit.edu](mailto:jis@mit.edu)

## [9.](#) 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."