Jeffrey I. Schiller
July 2003

Cryptographic Algorithms for use in the Internet Key Exchange Version 2
<draft-ietf-ipsec-ikev2-algorithms-03.txt>

Status of this Memo

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 even 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 mandatory to implement algorithms for use of IKEv2 as well as specifying algorithms that should be implemented because they made 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. This requires that some set of algorithms be specified as "mandatory to implement."

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 3DES-CBC is a MUST implement and AES-128-CBC is a SHOULD+. For integrity HMAC-SHA1 is a MUST implement.

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 ~~references~~identified by group number. Any groups not listed here are considered as MAY implement.

Group Number	Bit Length	Status	Defined
2	1024	MUST	[RFC2409]
5	1536	SHOULD	[RFC2409]
14	2048 MODP Group	SHOULD+	[RFC3526]

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_DES_IV64	1	[RFC1827]	SHOULD-
ENCR_DES	2	[RFC2405]	SHOULD-
ENCR_3DES	3	[RFC2451]	MUST
ENCR_RC5	4	[RFC2451]	MAY
ENCR_IDEA	5	[RFC2451]	MAY
ENCR_CAST	6	[RFC2451]	MAY
ENCR_BLOWFISH	7	[RFC2451]	MAY
ENCR_3IDEA	8	[RFC2451]	MAY
ENCR_DES_IV32	9		MAY
ENCR_RC4	10		MAY
ENCR_NULL	11	[RFC2410]	MAY
ENCR_AES~~_128~~_CBC	12		SHOULD+
ENCR_AES~~_128~~_CTR	13		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	[RFC2104]	MAY

Name	Number	Defined In	Status
PRF_HMAC_SHA1	2	[RFC2104]	MUST
PRF_HMAC_TIGER	3	[RFC2104]	MAY
PRF_AES128_CBC	4	[CIPH-AES]	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	[RFC2403]	MAY
AUTH_HMAC_SHA1_96	2	[RFC2404]	MUST
AUTH_DES_MAC	3		MAY
AUTH_KPDK_MD5	4	[RFC1826]	MAY
AUTH_AES_XCBC_96	5		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.

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

[CIPH-AES] S. Frankel, S. Kelley, R. Glenn, "The AES Cipher Algorithm and its Use with Ipsec <draft-ietf-ipsec-ciph-aes-cbs-05.txt>", 2003

[IKEv2] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol <draft-

ietf-ipsec-ikev2-06.txt>",
[RFC1826] R. Atkinson, "IP Authentication Header", 1995
[RFC1827] R. Atkinson., "IP Encapsulating Security Payload (ESP)", 1995
[RFC2026] S. Bradner, "RFC2026 The Internet Standards Process -- Revision 3", 1996
[RFC2104] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", 1997
[RFC2119] S. Bradner, "RFC2119 Key words for use in RFCs to Indicate Requirement Levels.", 1997
[RFC2403] C. Madson, R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", 1998
[RFC2404] C. Madson, R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", 1998
[RFC2405] C. Madson, N. Doraswamy., "The ESP DES-CBC Cipher Algorithm With Explicit IV", 1998
[RFC2409] Harkins, D., Carrel, D., "RFC 2409 The Internet Key Exchange (IKE)", 1998
[RFC2410] R. Glenn, S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", 1998
[RFC2451] R. Pereira, R. Adams, "The ESP CBC-Mode Cipher Algorithms", 1998
[RFC3526] T. Kivinen, M. Kojo., "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", 2003

8. Authors 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

9. Full Copyright Statement