

Internet Engineering Task Force	P. Hallam-Baker
Internet-Draft	VeriSign Inc
Intended status: Informational	November 05, 2007
Expires: May 8, 2008	

[TOC](#)

Cryptographic Algorithm Identifiers

draft-hallambaker-algorithm-identifiers-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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>.

This Internet-Draft will expire on May 8, 2008.

Abstract

Preferred identifiers for cryptographic algorithms currently in use in Internet standards.

Table of Contents

- [1.](#) Introduction
- [2.](#) Unkeyed Algorithms
 - [2.1.](#) Digest Algorithms
 - [2.1.1.](#) SHA2
 - [2.1.2.](#) RIPEMD-160
- [3.](#) Symmetric Algorithms
 - [3.1.](#) Encryption Algorithms
 - [3.1.1.](#) Block Ciphers

	3.1.1.1.	Triple Data Encryption Algorithm	
	3.1.1.2.	Advanced Encryption Standard	
	3.1.2.	Stream Ciphers	
	3.1.2.1.	RC4	
	3.2.	Message Authentication Codes	
	3.2.1.	HMAC	
	3.3.	One Time Password	
	3.4.	Combination Modes	
4.		Asymmetric Algorithms	
	4.1.	Key Agreement	
	4.1.1.	Diffie-Hellman	
	4.1.2.	RSA	
	4.2.	Signature	
	4.2.1.	RSA	
	4.3.	Encryption	
	4.3.1.	RSA	
5.		XML Tranformation	
	5.1.	Canonicalization	
6.		Encoding	
	6.1.	Binary	
	6.1.1.	Base 64	
7.		Security Considerations	
8.		IANA Considerations	
9.		Normative References	
§		Author's Address	
§		Intellectual Property and Copyright Statements	

1. Introduction

[TOC](#)

2. Unkeyed Algorithms

[TOC](#)

2.1. Digest Algorithms

[TOC](#)

[TOC](#)

2.1.1. SHA2

Standards Document: FIPS???

[Identifiers defined in xmldsig-core: XML-Signature Syntax and Processing]

Identifier: [SHA256] [length =256] [uri =http://www.w3.org/2001/04/xmlenc#sha256]

Identifier: [SHA512] [length =512] [uri =http://www.w3.org/2001/04/xmlenc#sha512]

[Identifiers defined in :]

Identifier: [DNSSEC Code=2] [length =256]

2.1.2. RIPEMD-160

[TOC](#)

[Identifiers defined in xmldsig-core: XML-Signature Syntax and Processing]

Identifier: [uri =http://www.w3.org/2001/04/xmlenc#ripemd160]

3. Symmetric Algorithms

[TOC](#)

3.1. Encryption Algorithms

[TOC](#)

3.1.1. Block Ciphers

[TOC](#)

3.1.1.1. Triple Data Encryption Algorithm

[TOC](#)

Alias: Triple DES

Standards Document: 800-67

Standards Document: X9.52

[Identifiers defined in xmlenc-core: XML Encryption Syntax and Processing]

Identifier: [Mode =cbc] [uri =http://www.w3.org/2001/04/xmlenc#tripledes-cbc]

Identifier: [Mode =kw] [uri =http://www.w3.org/2001/04/xmlenc#kw-tripledes]

3.1.1.2. Advanced Encryption Standard

[TOC](#)

Standards Document: FIPS 197

[Identifiers defined in xmlenc-core: XML Encryption Syntax and Processing]

Identifier: [length =128] [Mode =cbc] [uri =http://www.w3.org/2001/04/xmlenc#aes128-cbc]

Identifier: [length =192] [Mode =cbc] [uri =http://www.w3.org/2001/04/xmlenc#aes192-cbc]

Identifier: [length =256] [Mode =cbc] [uri =http://www.w3.org/2001/04/xmlenc#aes256-cbc]

Identifier: [length =128] [Mode =kw] [uri =http://www.w3.org/2001/04/xmlenc#kw-aes128]

Identifier: [length =192] [Mode =kw] [uri =http://www.w3.org/2001/04/xmlenc#kw-aes192]

Identifier: [length =256] [Mode =kw] [uri =http://www.w3.org/2001/04/xmlenc#kw-aes256]

3.1.2. Stream Ciphers

[TOC](#)

3.1.2.1. RC4

[TOC](#)

3.2. Message Authentication Codes

[TOC](#)

3.2.1. HMAC

[TOC](#)

Standards Document: RFC2104

[Identifiers defined in xmldsig-core: XML-Signature Syntax and Processing]

Identifier: [Mode =SHA1] [uri =http://www.w3.org/2000/09/xmlsig#hmac-sha1]

3.3. One Time Password

[TOC](#)

No algorithms registered yet.

3.4. Combination Modes

[TOC](#)

No algorithms registered yet.

4. Asymmetric Algorithms

[TOC](#)

4.1. Key Agreement

[TOC](#)

4.1.1. Diffie-Hellman

[TOC](#)

Standards Document: RFC2631

Standards Document: X9.42

[Identifiers defined in xmlenc-core: XML Encryption Syntax and Processing]

Identifier: [uri =http://www.w3.org/2001/04/xmlenc#dh]

4.1.2. RSA

[TOC](#)

Standards Document: RFC2437

[TOC](#)

4.2. Signature

4.2.1. RSA

[TOC](#)

Standards Document: RFC2437

[Identifiers defined in xmldsig-core: XML-Signature Syntax and Processing]

Identifier: [Mode =SHA1] [uri =http://www.w3.org/2000/09/xmldsig#rsa-sha1]

[Identifiers defined in :]

Identifier: [DNSSEC Code=5] [Mode =sha1]

Identifier: [DNSSEC Code=1] [Mode =md5]

4.3. Encryption

[TOC](#)

4.3.1. RSA

[TOC](#)

Standards Document: RFC2437

5. XML Transformation

[TOC](#)

5.1. Canonicalization

[TOC](#)

No algorithms registered yet.

6. Encoding

[TOC](#)

[TOC](#)

6.1. Binary

6.1.1. Base 64

[TOC](#)

Standards Document: Base64

[Identifiers defined in xmldsig-core: XML-Signature Syntax and Processing]

Identifier: [uri =http://www.w3.org/2000/09/xmldsig#base64]

7. Security Considerations

[TOC](#)

TBS

8. IANA Considerations

[TOC](#)

TBS

9. Normative References

[TOC](#)

[800-67]	"Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," May 2004.
[CSOR]	"Cryptographic Algorithm Object Registration."
[FIPS 197]	"Advanced Encryption Standard (AES)," November 2001.
[RFC2104]	"HMAC: Keyed-Hashing for Message Authentication," February 1997.
[RFC2119]	Bradner, S. , " Key words for use in RFCs to Indicate Requirement Levels ," BCP 14, RFC 2119, March 1997 (TXT , HTML , XML).
[RFC2437]	"PKCS #1: RSA Cryptography Specifications Version 2.0," October 1998.
[RFC2560]	Myers, M. , Ankney, R. , Malpani, A. , Galperin, S. , and C. Adams , " X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP ," RFC 2560, June 1999 (TXT).
[RFC2631]	"Diffie-Hellman Key Agreement Method," June 1999.
[RFC4034]	". "
[RFC4509]	". "
[RFC4868]	

	"Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec."
[X9.42]	"Agreement of Symmetric Keys Using Discrete Logarithm Cryptography."
[X9.52]	"Triple Data Encryption Algorithm Modes of Operation," 1998.
[XML-C14]	"XML Canonicalization."
[XML-XC14]	"Exclusive XML Canonicalization."
[xmldsig-core]	"XML-Signature Syntax and Processing," February 2002.
[xmlesc-core]	"XML Encryption Syntax and Processing."
[xpath]	"XML Path Language (XPath) Version 1.0," November 1999.
[xslt]	"XSL Transformations (XSLT) Version 1.0," November 16.

Author's Address

[TOC](#)

	Phillip Hallam-Baker
	VeriSign Inc
Email:	pbaker@verisign.com

Full Copyright Statement

[TOC](#)

Copyright © The IETF Trust (2007).

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, THE IETF TRUST 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.