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

Abstract

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

Table of Contents

---

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/xmldsig#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 Tranformation

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.
[xmlenc-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

Intellectual Property

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.