**<http://lists.w3.org/Archives/Public/public-xmlsec/2009Jun/att-0044/xmlenc-ref.html>**

**10** **References**

**10.1** **Normative References**

TRIPLEDES

1. ANSI X9.52: Triple Data Encryption Algorithm Modes of Operation. 1998.  \*\*\*HERE
	1. <http://www.ansi.org/>
2. AES-WRAP, [RFC3394: Advanced Encryption Standard (AES) Key Wrap Algorithm](http://www.ietf.org/rfc/rfc3394.txt). J. Schaad and R. Housley. Informational, September 2002.
	1. <http://www.rfc-editor.org/rfc/rfc3394.txt> \*\*\*HERE
3. DRAFT-HOUSLEY-KW-PAD [Advanced Encryption Standard (AES) Key Wrap Algorithm With Padding](http://tools.ietf.org/html/draft-housley-aes-key-wrap-with-pad-02). R. Housley, M. Dworkin. Internet-Draft (Work in Progress), 15 June 2009.
	1. <http://tools.ietf.org/html/draft-housley-aes-key-wrap-with-pad-03> . \*\*\*HERE
4. SHA
	1. [FIPS PUB 180-3](http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf). *Secure Hash Standard.* U.S. Department of Commerce/National Institute of Standards and Technology.
	2. <http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf> \*\*\*HERE
5. XML-DSIG
	1. [XML-Signature Syntax and Processing](http://www.w3.org/TR/xmldsig-core/). D. Eastlake, J. Reagle, and D. Solo. W3C Recommendation, 10 June 2008. \*\*\*HERE
	2. <http://www.w3.org/TR/xmldsig-core/>
6. XMLDSIG11
	1. [XML Signature Syntax and Processing Version 1.1](http://www.w3.org/TR/2009/WD-xmldsig-core1-20090226). D. Eastlake, J. Reagle, D. Solo, F. Hirsch, T. Roessler. K. Yiu. W3C Working Draft, February 2009.
	2. <http://www.w3.org/TR/2009/WD-xmldsig-core1-20090226/> \*\*\*HERE

**10.2** **Informative References**

1. Glossary
	1. [RFC 4949: Internet Security Glossary](http://www.ietf.org/rfc/rfc2828.txt), Version 2. R Shirey. Informational, May 2000. \*\*\*HERE
	2. ftp://ftp.rfc-editor.org/in-notes/rfc4949.txt \*\*\*HERE
2. MIME [RFC 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies](http://www.ietf.org/rfc/rfc2045.txt). N. Freed and N. Borenstein. Standards Track, November 1996. <http://www.ietf.org/rfc/rfc2045.txt>
	1. RFC 5335 Internationalized Email Headers, ftp://ftp.rfc-editor.org/in-notes/rfc5335.txt \*\*\*HERE
3. MIME-REG [RFC 2048: Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures](http://www.ietf.org/rfc/rfc2048.txt). N. Freed, J. Klensin, and J. Postel. Best Current Practice, November 1996. <http://www.ietf.org/rfc/rfc2048.txt>
	1. RFC 3023 XML Media Types, ftp://ftp.rfc-editor.org/in-notes/rfc3023.txt \*\*\* HERE
4. UTF-8
	1. [RFC 3629: UTF-8, a transformation format of ISO 10646F.](http://www.ietf.org/rfc/rfc2279.txt) F. Yergeau. Standards Track, November 2003. \*\*\*HERE
	2. ftp://ftp.rfc-editor.org/in-notes/rfc3629.txt \*\*\*HERE
5. URN
	1. [RFC 3406: **Uniform Resource Names (URN) Namespace Definition Mechanisms**.](http://www.ietf.org/rfc/rfc2611.txt) Best Current Practices. L. Daigle, D. van Gulik, R. Iannella, P. Faltstrom. October 2002. \*\*\*HERE
	2. ftp://ftp.rfc-editor.org/in-notes/rfc3406.txt \*\*\*HERE
6. X509v3
	1. ITU-T Recommendation X.509 version 3 (1997). "Information Technology - Open Systems Interconnection - The Directory Authentication Framework"  ISO/IEC 9594-8:2001. \*\*\*HERE
	2. <http://www.iso.org/iso/catalogue_detail.htm?csnumber=34551> \*\*\*HERE