KMIP-UG 3.0 Rev 1 References

[DoD5220.22M] *National Industrial Security Program Operating Manual*, February 2006 (Incorporating Change 1 March 28, 2013), <http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf>

[ECC-Brainpool] *ECC Brainpool Standard Curves and Curve Generation v. 1.0.19.10.2005*, <http://www.ecc-brainpool.org/download/Domain-parameters.pdf>.

[KMIP-SPEC] *Key Management Interoperability Protocol Specification Version 3.0*. Edited by Greg Scott and Charles White. Latest version: <https://docs.oasis-open.org/kmip/kmip-spec/v3.0/kmip-spec-v3.0.html>.

[KMIP-PROF] *Key Management Interoperability Protocol Profiles Version 3.0.* Edited by Tim Hudson and Tim Chevalier. Latest version: <https://docs.oasis-open.org/kmip/kmip-profiles/v3.0/kmip-profiles-v3.0.html>.

[KMIP-TC] *Key Management Interoperability Protocol Test Cases Version 3.0.* Edited by Tim Chevalier and Tim Hudson. Latest version: <https://docs.oasis-open.org/kmip/kmip-testcases/v3.0/kmip-testcases-v3.0.html>.

[FIPS 180-4] *Secure Hash Standard (SHS)*, FIPS PUB 180-4, March 2012, <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>

[FIPS 186-4] *Digital Signature Standard (DSS)*. FIPS PUB 186-4. July 2013. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[FIPS 197] *Advanced Encryption Standard (AES)*. FIPS PUB 197. November 26, 2001. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

[FIPS 198-1] *The Keyed-Hash Message Authentication Code (HMAC)*. FIPS PUB 198-1. July 2008. <http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf>

[PKCS#1] RSA Laboratories. PKCS #1 v2.1: RSA Cryptography Standard. June 14, 2002. <http://www.preserveitall.org/emc-plus/rsa-labs/standards-initiatives/pkcs-rsa-cryptography-standard.htm>.

[PKCS#10] RSA Laboratories. PKCS #10 v1.7: Certification Request Syntax Standard. May 26, 2000. <http://www.preserveitall.org/emc-plus/rsa-labs/standards-initiatives/pkcs10-certification-request-syntax-standard.htm>.

[PKCS#11] OASIS PKCS#11 Cryptographic Token Interface Base Specification Version 3.0

[RFC1321] R. Rivest, *The MD5 Message-Digest Algorithm*, IETF RFC 1321, Apr 1992, <http://www.ietf.org/rfc/rfc1321.txt>

[RFC1421] J. Linn, *Privacy Enhancement for Internet Electronic Mail:**Part I: Message Encryption and Authentication Procedures*, IETF RFC 1421, Feb 1993, <http://www.ietf.org/rfc/rfc1421.txt>

[RFC3647] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. *RFC3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. November 2003. <http://www.ietf.org/rfc/rfc3647.txt>

[RFC4210] C. Adams, S. Farrell, T. Kause and T. Mononen, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*, IETF RFC 2510, Sep 2005, <http://www.ietf.org/rfc/rfc4210.txt>

[RFC4211] J. Schaad, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*, IETF RFC 4211, Sep 2005, <http://www.ietf.org/rfc/rfc4211.txt>

[RFC4949] R. Shirey. *RFC4949: Internet Security Glossary, Version 2*. August 2007. <http://www.ietf.org/rfc/rfc4949.txt>

[RFC4880] J. Callas, L. Donnerhacke, H. Finney, D. Shaw and R. Thayer. *RFC4880: OpenPGP Message Format. November 2007*. <http://www.ietf.org/rfc/rfc4880.txt>

[RFC5272] J. Schaad and M. Meyers, *Certificate Management over CMS (CMC)*, IETF RFC 5272, Jun 2008, <http://www.ietf.org/rfc/rfc5272.txt>

[RFC5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. *RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* May 2008. <http://www.ietf.org/rfc/rfc5280.txt>

[RFC5639] M. Lochter, J. Merkle, *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*, IETF RFC 5639, March 2010, <http://www.ietf.org/rfc/rfc5639.txt>.

[RFC7292] K. Moriarty, M. Nystrom, S. Parkinson, A. Rusch, M. Scott, PKCS#12: Personal Information Exchange Syntax v1.1, IETF RFC 7292, July 2014, <https://tools.ietf.org/html/rfc7292>

**[RFC7748]** Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>

**[****SAM-TSS]** *SAM Threshold Sharing Schemes Version 1.0*, Edited by Tim Chevalier and Tim Hudson. Latest versions: <http://docs.oasis-open.org/sam/sam-tss/v1.0/sam-tss-v1.0.html.>

[SEC2] SEC 2: Recommended Elliptic Curve Domain Parameters, <http://www.secg.org/SEC2-Ver-1.0.pdf>.

[SP800-38A] M. Dworkin. *Recommendation for Block Cipher Modes of Operation – Methods and Techniques*. NIST Special Publication 800-38A, Dec 2001. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf>

[SP800-38D] M. Dworkin. *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. NIST Special Publication 800-38D. Nov 2007. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf>.

[SP800-38E] M. Dworkin, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices*, NIST Special Publication 800-38E, January 2010, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf>.

[SP800-56A] E. Barker, L. Chen, A. Roginsky, and M. Smid, *Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, NIST Special Publication 800-56A Revision 2, May 2013, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf>

[SP800-57-1] E. Barker, W. Barker, W. Burr, W. Polk and M. Smid, *Recommendations for Key Management – Part 1: General (Revision 3)*, NIST Special Publication 800-57 Part 1 Revision 3, July 2012, <http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf>

[SP800-67] W. Barker and E. Barker, *Recommendations for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, NIST Special Publication 800-67 Revision 1, January 2012, <http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf>

[SP800-88] R. Kissel, A. Regenscheid,M. Scholl, K. Stine, *Guidelines for Media Sanitization*, NIST Special Publication 800-88 Revision 1, December 2014, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

[X.509] International Telecommunications Union (ITU)-T, *X.509: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*, November 2008, <https://www.itu.int/rec/T-REC-X.509/recommendation.asp?lang=en&parent=T-REC-X.509-200811-S>

[X9.31] ANSI, *X9.31: Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry* *(rDSA)*. September 1998.

[X9.42] ANSI, *X9.42: Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*. 2003.

[X9.62] ANSI, *X9.62: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 2005.

References that have been updated, superseded or moved (strikethrough indicate might be OK)…

[DoD5220.22M] *National Industrial Security Program Operating Manual*, February 2006 (Incorporating Change 1 March 28, 2013), <http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf>

[ECC-Brainpool] *ECC Brainpool Standard Curves and Curve Generation v. 1.0.19.10.2005*, <http://www.ecc-brainpool.org/download/Domain-parameters.pdf>.

~~[KMIP-SPEC]~~ *~~Key Management Interoperability Protocol Specification Version 3.0~~*~~. Edited by Greg Scott and Charles White. Latest version:~~ [~~https://docs.oasis-open.org/kmip/kmip-spec/v3.0/kmip-spec-v3.0.html~~](https://docs.oasis-open.org/kmip/kmip-spec/v3.0/kmip-spec-v3.0.html)~~.~~

~~[KMIP-PROF]~~ *~~Key Management Interoperability Protocol Profiles Version 3.0.~~* ~~Edited by Tim Hudson and Tim Chevalier. Latest version:~~ [~~https://docs.oasis-open.org/kmip/kmip-profiles/v3.0/kmip-profiles-v3.0.html~~](https://docs.oasis-open.org/kmip/kmip-profiles/v3.0/kmip-profiles-v3.0.html)~~.~~

~~[KMIP-TC]~~ *~~Key Management Interoperability Protocol Test Cases Version 3.0.~~* ~~Edited by Tim Chevalier and Tim Hudson. Latest version:~~ [~~https://docs.oasis-open.org/kmip/kmip-testcases/v3.0/kmip-testcases-v3.0.html~~](https://docs.oasis-open.org/kmip/kmip-testcases/v3.0/kmip-testcases-v3.0.html)~~.~~

[FIPS 180-4] *Secure Hash Standard (SHS)*, FIPS PUB 180-4, March 2012, <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>

~~[FIPS 186-4]~~ *~~Digital Signature Standard (DSS)~~*~~. FIPS PUB 186-4. July 2013. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf~~

~~[FIPS 197]~~ *~~Advanced Encryption Standard (AES)~~*~~. FIPS PUB 197. November 26, 2001.~~ [~~http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf~~](http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf)

~~[FIPS 198-1]~~ *~~The Keyed-Hash Message Authentication Code (HMAC)~~*~~. FIPS PUB 198-1. July 2008.~~ [~~http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1\_final.pdf~~](http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf)

[PKCS#1] RSA Laboratories. PKCS #1 v2.1: RSA Cryptography Standard. June 14, 2002. <http://www.preserveitall.org/emc-plus/rsa-labs/standards-initiatives/pkcs-rsa-cryptography-standard.htm>.

[PKCS#10] RSA Laboratories. PKCS #10 v1.7: Certification Request Syntax Standard. May 26, 2000. <http://www.preserveitall.org/emc-plus/rsa-labs/standards-initiatives/pkcs10-certification-request-syntax-standard.htm>.

[PKCS#11] OASIS PKCS#11 Cryptographic Token Interface Base Specification Version 3.0

~~[RFC1321] R. Rivest,~~ *~~The MD5 Message-Digest Algorithm~~*~~, IETF RFC 1321, Apr 1992,~~ [~~http://www.ietf.org/rfc/rfc1321.txt~~](http://www.ietf.org/rfc/rfc1321.txt)

~~[RFC1421] J. Linn,~~ *~~Privacy Enhancement for Internet Electronic Mail:~~**~~Part I: Message Encryption and Authentication Procedures~~*~~, IETF RFC 1421, Feb 1993,~~ [~~http://www.ietf.org/rfc/rfc1421.txt~~](http://www.ietf.org/rfc/rfc1421.txt)

~~[RFC3647] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu.~~ *~~RFC3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework~~*~~. November 2003.~~ [~~http://www.ietf.org/rfc/rfc3647.txt~~](http://www.ietf.org/rfc/rfc3647.txt)

~~[RFC4210] C. Adams, S. Farrell, T. Kause and T. Mononen,~~ *~~Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)~~*~~, IETF RFC 2510, Sep 2005,~~ [~~http://www.ietf.org/rfc/rfc4210.txt~~](http://www.ietf.org/rfc/rfc4210.txt)

~~[RFC4211] J. Schaad,~~ *~~Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)~~*~~, IETF RFC 4211, Sep 2005,~~ [~~http://www.ietf.org/rfc/rfc4211.txt~~](http://www.ietf.org/rfc/rfc4211.txt)

~~[RFC4949] R. Shirey.~~ *~~RFC4949: Internet Security Glossary, Version 2~~*~~. August 2007.~~ [~~http://www.ietf.org/rfc/rfc4949.txt~~](http://www.ietf.org/rfc/rfc4949.txt)

~~[RFC4880] J. Callas, L. Donnerhacke, H. Finney, D. Shaw and R. Thayer.~~ *~~RFC4880: OpenPGP Message Format. November 2007~~*~~.~~ [~~http://www.ietf.org/rfc/rfc4880.txt~~](http://www.ietf.org/rfc/rfc4880.txt)

~~[RFC5272] J. Schaad and M. Meyers,~~ *~~Certificate Management over CMS (CMC)~~*~~, IETF RFC 5272, Jun 2008,~~ [~~http://www.ietf.org/rfc/rfc5272.txt~~](http://www.ietf.org/rfc/rfc5272.txt)

~~[RFC5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk.~~ *~~RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.~~* ~~May 2008.~~ [~~http://www.ietf.org/rfc/rfc5280.txt~~](http://www.ietf.org/rfc/rfc5280.txt)

~~[RFC5639] M. Lochter, J. Merkle,~~ *~~Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation~~*~~, IETF RFC 5639, March 2010,~~ [~~http://www.ietf.org/rfc/rfc5639.txt~~](http://www.ietf.org/rfc/rfc5639.txt)~~.~~

~~[RFC7292] K. Moriarty, M. Nystrom, S. Parkinson, A. Rusch, M. Scott, PKCS#12: Personal Information Exchange Syntax v1.1, IETF RFC 7292, July 2014,~~ [~~https://tools.ietf.org/html/rfc7292~~](https://tools.ietf.org/html/rfc7292)

**~~[RFC7748]~~** ~~Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016,~~ [~~https://www.rfc-editor.org/info/rfc7748~~](https://www.rfc-editor.org/info/rfc7748)

**[SAM-TSS]** *SAM Threshold Sharing Schemes Version 1.0*, Edited by Tim Chevalier and Tim Hudson. Latest versions: <http://docs.oasis-open.org/sam/sam-tss/v1.0/sam-tss-v1.0.html.>

~~[SEC2] SEC 2: Recommended Elliptic Curve Domain Parameters,~~ [~~http://www.secg.org/SEC2-Ver-1.0.pdf~~](http://www.secg.org/SEC2-Ver-1.0.pdf)~~.~~

~~[SP800-38A] M. Dworkin.~~ *~~Recommendation for Block Cipher Modes of Operation – Methods and Techniques~~*~~. NIST Special Publication 800-38A, Dec 2001.~~ [~~http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf~~](http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf)

~~[SP800-38D] M. Dworkin.~~ *~~Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC~~*~~. NIST Special Publication 800-38D. Nov 2007.~~ [~~http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf~~](http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf)~~.~~

~~[SP800-38E] M. Dworkin,~~ *~~Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices~~*~~, NIST Special Publication 800-38E, January 2010,~~ [~~http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf~~](http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf)~~.~~

[SP800-56A] E. Barker, L. Chen, A. Roginsky, and M. Smid, *Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, NIST Special Publication 800-56A Revision 2, May 2013, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf>

[SP800-57-1] E. Barker, W. Barker, W. Burr, W. Polk and M. Smid, *Recommendations for Key Management – Part 1: General (Revision 3)*, NIST Special Publication 800-57 Part 1 Revision 3, July 2012, <http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf>

[SP800-67] W. Barker and E. Barker, *Recommendations for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, NIST Special Publication 800-67 Revision 1, January 2012, <http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf>

[SP800-88] R. Kissel, A. Regenscheid,M. Scholl, K. Stine, *Guidelines for Media Sanitization*, NIST Special Publication 800-88 Revision 1, December 2014, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

[X.509] International Telecommunications Union (ITU)-T, *X.509: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*, November 2008, <https://www.itu.int/rec/T-REC-X.509/recommendation.asp?lang=en&parent=T-REC-X.509-200811-S>

~~[X9.31] ANSI,~~ *~~X9.31: Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry~~**~~(rDSA)~~*~~. September 1998.~~

~~[X9.42] ANSI,~~ *~~X9.42: Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography~~*~~. 2003.~~

~~[X9.62] ANSI,~~ *~~X9.62: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)~~*~~, 2005.~~

References KNOWN to have issues (from list above)

[DoD5220.22M] *National Industrial Security Program Operating Manual*, February 2006 (Incorporating Change 1 March 28, 2013), <http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf>

[ECC-Brainpool] *ECC Brainpool Standard Curves and Curve Generation v. 1.0.19.10.2005*, <http://www.ecc-brainpool.org/download/Domain-parameters.pdf>.

[FIPS 180-4] *Secure Hash Standard (SHS)*, FIPS PUB 180-4, March 2012, <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>

[PKCS#1] RSA Laboratories. PKCS #1 v2.1: RSA Cryptography Standard. June 14, 2002. <http://www.preserveitall.org/emc-plus/rsa-labs/standards-initiatives/pkcs-rsa-cryptography-standard.htm>.

[PKCS#10] RSA Laboratories. PKCS #10 v1.7: Certification Request Syntax Standard. May 26, 2000. <http://www.preserveitall.org/emc-plus/rsa-labs/standards-initiatives/pkcs10-certification-request-syntax-standard.htm>.

**[SAM-TSS]** *SAM Threshold Sharing Schemes Version 1.0*, Edited by Tim Chevalier and Tim Hudson. Latest versions: <http://docs.oasis-open.org/sam/sam-tss/v1.0/sam-tss-v1.0.html.>

SP800-56A] E. Barker, L. Chen, A. Roginsky, and M. Smid, *Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, NIST Special Publication 800-56A Revision 2, May 2013, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf>

[SP800-57-1] E. Barker, W. Barker, W. Burr, W. Polk and M. Smid, *Recommendations for Key Management – Part 1: General (Revision 3)*, NIST Special Publication 800-57 Part 1 Revision 3, July 2012, <http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf>

[SP800-67] W. Barker and E. Barker, *Recommendations for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, NIST Special Publication 800-67 Revision 1, January 2012, <http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf>

[SP800-88] R. Kissel, A. Regenscheid,M. Scholl, K. Stine, *Guidelines for Media Sanitization*, NIST Special Publication 800-88 Revision 1, December 2014, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

[X.509] International Telecommunications Union (ITU)-T, *X.509: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*, November 2008, <https://www.itu.int/rec/T-REC-X.509/recommendation.asp?lang=en&parent=T-REC-X.509-200811-S>

References that still need to be checked:

RFCs may have been superceded, so they should be examined further.

[X9.31] ANSI, *X9.31: Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry* *(rDSA)*. September 1998.

[X9.42] ANSI, *X9.42: Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*. 2003.

[X9.62] ANSI, *X9.62: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 2005.