Annex A:
Approved Security Functions for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*

July 26, 2011
Draft

Jean Campbell
Randall J. Easter

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick Gallagher, Director

Annex A: Approved Security Functions for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*

1. Introduction

Federal Information Processing Standards Publication (FIPS PUB) 140-2, *Security Requirements for Cryptographic Modules*, specifies the security requirements that are to be satisfied by the cryptographic module utilized within a security system protecting sensitive information within computer and telecommunications systems (including voice systems). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of the cryptographic module. These areas include the following:

1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)
9. Self Tests
10. Design Assurance
11. Mitigation of Other Attacks

The Cryptographic Module Validation Program (CMVP - www.nist.gov/cmvp) validates cryptographic modules to FIPS PUB 140-2 and other cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC - www.cse-cst.gc.ca). Modules validated as conforming to FIPS PUB 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated information (Canada).

In the CMVP, vendors of cryptographic modules use independent, accredited testing laboratories to have their modules tested. Organizations wishing to have validations performed would contract with the laboratories for the required services.

2. Purpose

The purpose of this document is to provide a list of the Approved security functions applicable to FIPS PUB 140-2.

Table of Contents

ANNEX A: APPROVED SECURITY FUNCTIONS 1

Transitions 1
Symmetric Key (AES, TDEA and EES) 1
Asymmetric Key (DSS – DSA, RSA and ECDSA) 2
Secure Hash Standard (SHS) 2
Random Number Generators (RNG and DRBG) 2
Message Authentication (Triple-DES, AES and SHS) 2

Document Revisions 4

End of Document 6

ANNEX A: APPROVED SECURITY FUNCTIONS

Annex A provides a list of the Approved security functions applicable to FIPS PUB 140-2. The categories include transitions, symmetric key, asymmetric key, message authentication and hashing.

Transitions

National Institute of Standards and Technology, *Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Special Publication 800-131A, January 2011. Sections relevant to this Annex: 1, 2, 3, 9 and 10.

Symmetric Key (AES, TDEA and EES)

1. **Advanced Encryption Standard (AES)**

   National Institute of Standards and Technology, *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, November 26, 2001.

   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*, Special Publication 800-38A, December 2001.

   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*, Addendum to Special Publication 800-38A, October 2010.

   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, Special Publication 800-38C, May 2004.

   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, Special Publication 800-38D, November 2007.

   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, Special Publication 800-38E, January 2010.

2. **Triple-DES Encryption Algorithm (TDEA)**

   National Institute of Standards and Technology, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, Special Publication 800-67, May 2004.

   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*, Special Publication 800-38A, December 2001. Appendix E references Modes of Triple-DES.

   American Bankers Association, *Triple Data Encryption Algorithm Modes of Operation*, ANSI X9.52-1998. Copies of X9.52-1998 may be obtained from X9, a standards committee for the financial services industry.

3. **Escrowed Encryption Standard (EES)**

   National Institute of Standards and Technology, *Escrowed Encryption Standard (EES)*, Federal Information Processing Standards Publication 185, February 9, 1984.

Skipjack and KEA Algorithm Specifications, Version 2.0, May 29, 1998.

Asymmetric Key (DSS – DSA, RSA and ECDSA)

1. **Digital Signature Standard (DSS)**

   National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-3, June, 2009. (DSA2, RSA2 and ECDSA2)

   National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, January, 2000 with Change Notice 1. (DSA, RSA and ECDSA)

   RSA Laboratories, *PKCS#1 v2.1: RSA Cryptography Standard*, June 14, 2002.
   Only the versions of the algorithms RSASSA-PKCS1-v1_5 and RSASSA-PSS contained within this document shall be used.

Secure Hash Standard (SHS)

1. **Secure Hash Standard (SHS) (SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512)**

   National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-3, October, 2008.

Random Number Generators (RNG and DRBG)

1. **Annex C: *Approved Random Number Generators***

   National Institute of Standards and Technology, *Annex C: Approved Random Number Generators for FIPS 140-2, Security Requirements for Cryptographic Modules*.

Message Authentication (Triple-DES, AES and SHS)

1. **Triple-DES**

   National Institute of Standards and Technology, *Computer Data Authentication*, Federal Information Processing Standards Publication 113, 30 May 1985.

2. **AES**

   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, Special Publication 800-38B, May 2005.

   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, Special Publication 800-38C, May 2004.

   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, Special Publication 800-38D, November 2007.

3. **SHS**

   National Institute of Standards and Technology, *The Keyed-Hash Message Authentication Code*

(HMAC), Federal Information Processing Standards Publication 198-1, July, 2008.

Document Revisions

Date	Change
05-13-2002	**Symmetric Key**, Number 1: Added: *Advanced Encryption Standard (AES)*
	Keyed Hash, Number 1: Added: *The Keyed-Hash Message Authentication Code (HMAC)*
02-19-2003	**Symmetric Key**, Number 1: Added: *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*
12-16-2003	**Asymmetric Key**, Number 1: Deleted: Removed Asymmetric Key references to ANSI X9.31-1998 and ANSI X9.62-1998. These are referenced FIPS 186-2.
03-11-2004	**Hashing,** Number 1: Added: *Secure Hash Standard* - SHA-256, SHA-384 and SHA-512
05-13-2004	**Hashing,** Number 1: Added: *Secure Hash Standard* - SHA-224
08-18-2004	**Asymmetric Key**, Number 1: Updated: Modified reference to include Change Notice 1 - *Digital Signature Standard (DSS)*
09-23-2004	**Message Authentication**, Number 3: Added: *Recommendation for BlockCipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*
05-19-2005	**Symmetric Key**, Number 2: Added: *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*
04-03-2006	**Message Authentication**, Number 4: Added: *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*
01-24-2007	**Random Number Generators**, Number 1: Updated: Modified reference document date - *Annex C: Approved Random Number Generators for FIPS 140-2, Security Requirements for Cryptographic Modules*
05/19/2007	**Symmetric Key**, Number 2: Deleted: References to DES removed.
	Message Authentication, Numbers 1 and 2: Deleted: References to DES removed.
10/18/2007	Updated: Modified URL's
12/18/2007	**Symmetric Key**, Number 1: Added: *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*
10/21/2008	**Hashing,** Number 1: Updated: FIPS 180-3 replaces FIPS 180-2 - *Secure Hash Standard*
06/18/2009	**Asymmetric Key - Signature,** Number 1: Updated: FIPS 180-3 replaces FIPS 180-2 - *Digital Signature Standard (DSS)*
07/21/2009	**Asymmetric Key - Signature,** Number 1: Added: Included reference to archived *Digital Signature Standard (DSS)* – FIPS 186-2 until transition plan from FIPS 186-2 to FIPS 186-3 ends.
10/08/2009	Updated: Editorial Changes to align with the CAVP
10/22/2009	**Key Management**, Number 1: Added: *Recommendation for Key Derivation Using Pseudorandom Functions*
01/27/2010	**Symmetric Key**, Number 1: Added: *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*

11/24/2010	**Symmetric Key**, Number 1: Added: *Addendum to Special Publication 800-38A, October 2010: Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*
	Message Authentication, Number 3: **Updated:** Revision date **-** *FIPS 198-1, July 2008: The Keyed-Hash Message Authentication Code (HMAC)*
01/04/2011	**Moved Key Management/Establishment references to FIPS 140-2 Annex D.**
07/26/2011	**Added new Section: Transitions** Added: *Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*

End of Document