Annex A:
Approved Security Functions for FIPS PUB 140-3, *Security Requirements for Cryptographic Modules*

July 10, 2009
Draft

NIST Computer Security Division

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

U.S. Department of Commerce
Secretary Gary Locke

Technology Administration
Under Secretary for Technology

National Institute of Standards and Technology
Deputy Director Patrick D. Gallagher

DRAFT

Annex A: Approved Security Functions for FIPS PUB 140-3, *Security Requirements for Cryptographic Modules*

1. Introduction

Federal Information Processing Standards Publication (FIPS PUB) 140-3, 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: Security Level 1, Security Level 2, Security Level 3 and Security 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 Interfaces
3. Roles, Authentication and Services
4. Software/Firmware Security
5. Operating Environment
6. Physical Security
7. Physical Security - Non-Invasive Attacks
8. Sensitive Security Parameter Management
9. Self-Tests
10. Life-Cycle Assurance
11. Mitigation of Other Attacks

The Cryptographic Module Validation Program (CMVP - www.nist.gov/cmvp) validates cryptographic modules for conformance to FIPS PUB 140-3 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 140-3 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated information (Canada).

Under 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 140-3.

Table of Contents

ANNEX A: APPROVED SECURITY FUNCTIONS

Annex A provides a list of the Approved security functions applicable to FIPS PUB 140-3. The categories include symmetric key, asymmetric key, message authentication and hashing.

Symmetric Key - Encryption

1. **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, May 2005.

   National Institute of Standards and Technology, *Counter with Cipher Block Chaining - Message Authentication Code (CCM)*, 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.

2. **Triple-DES**

   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, May 2005. Appendix E references Modes of Triple-DES.

   American Bankers Association, *Triple Data Encryption Algorithm Modes of Operation*, ANSI X9.52-1998.

3. **Skipjack**

   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 - Signature

1. **DSA, RSA and ECDSA**

   National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2 with Change Notice 1, October 05, 2001.

   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.

draft

Message Authentication

1. **Triple-DES MAC**

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

2. **Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality**

   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. **Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication**

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

4. **HMAC - Keyed-Hash Message Authentication Code**

   National Institute of Standards and Technology, *The Keyed-Hash Message Authentication Code (HMAC)*, Federal Information Processing Standards Publication 198-1, July, 2008

Hashing

1. **Secure Hash Standard (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 Bit Generators

1. **Approved Random Bit Generators**

   National Institute of Standards and Technology Special Publication 800-90, *Recommendation for Random Number Generation UsingDeterministic Random Bit Generators (revised)*, March, 2007.

draft

Document Revisions

Date	Change
03/02/2009	**Initial Draft**

draft

End of Document

draft