Annex C:
Approved Random Number Generators for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*

July 26, 2011
Draft

Jean Campbell
Randall J. Easter

DRAFT

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, Deputy Director

Annex C: Approved Random Number Generators 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 Approved random number generators applicable to FIPS PUB 140-2.

Table of Contents

DRAFT

ANNEX C: APPROVED RANDOM NUMBER GENERATORS

Annex C provides a list of Approved random number generators applicable to FIPS PUB 140-2. There are two basic classes: deterministic and nondeterministic. A deterministic RNG consists of an algorithm that produces a sequence of bits from an initial value called a seed. A nondeterministic RNG produces output that is dependent on some unpredictable physical source that is outside human control.

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 and 4.

Deterministic Random Number Generators

1. National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 27, 2000 with Change Notice – Appendix 3.1.

2. National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 27, 2000 with Change Notice – Appendix 3.2.

   Note: Please review National Institute of Standards and Technology, Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program, Sections 8.1, 8.7 and 8.9 for additional guidance.

3. American Bankers Association, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA),* ANSI X9.31-1998 - Appendix A.2.4.

4. American Bankers Association, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),* ANSI X9.62-1998 – Annex A.4

5. National Institute of Standards and Technology, *NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms*, January 31, 2005.

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

Nondeterministic Random Number Generators

There are no FIPS Approved nondeterministic random number generators**.**

draft

Document Revisions

Date	Change
03-17-2003	**Deterministic Random Number Generators**, Number 3: Updated: corrected reference to Appendix A.2.4 - *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*
01-31-2005	**Deterministic Random Number Generators**, Number 5: Added*: NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms*
01-24-2007	**Deterministic Random Number Generators**, Number 6: Added*: Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
03-19-2007	**Deterministic Random Number Generators**, Number 6: Updated: Revision date - *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)*
10/18/2007	Updated: Modified URL's
07/21/2009	Updated: Modified URL to archived FIPS 186-2.
11/24/2010	**Deterministic Random Number Generators**, Number 4: Updated: Revision date - *ANSI X9.62-2005 – Annex D*: *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*
06/14/2011	**Deterministic Random Number Generators**, Number 4: Removed - *ANSI X9.62-2005 – Annex D*: *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)* and replaced with *ANSI X9.62-1998 – Annex A.4*: *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)* Note: *ANSI X9.62-2005 – Annex D*: *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)* is incorporated in NIST SP 800-90 (Number 6) HMAC_DRBG
07/26/2011	**Added new Section: Transitions** Added: *Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*

draft

End of Document

draft