American National Standard for Financial Services

ANSI X9.82: Part 1–2006

(R2013)

Random Number Generation

Part 1: Overview and Basic Principles

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: July 26, 2006

American National Standards Institute

Contents

Figures

Foreword

The Accredited Standards Committee on Financial Services (ANSI X9) has developed several cryptographic standards to protect financial information. Many of these standards require the use of Random Number Generators to generate random and unpredictable cryptographic keys and other critical security parameters. This Standard, *Random Number Generation*, defines techniques for the generation of random numbers that are used when other ASC standards require the use of random numbers for cryptographic purposes.

While the techniques specified in this Standard are designed to generate random numbers, the Standard does not guarantee that a particular implementation is secure. It is the responsibility of the financial institution to put an overall process in place with the necessary controls to ensure that the process is securely implemented. Furthermore, the controls should include the application with appropriate validation tests in order to verify compliance with this Standard.

Approval of an American National Standard requires verification by ASC that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ASC Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this Standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to reaffirm, revise, or withdraw this Standard no later than five years from the date of approval.

Published by

Accredited Standards Committee X9 Incorporated
Financial Industry standards
1212 West Street, Suite 200
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

Introduction

NOTE The user's attention is called to the possibility that compliance with this Standard may require use of an invention covered by patent rights.

By publication of this Standard, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the standards developer.

Suggestions for the improvement or revision of this Standard are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, 1212 West Street, Suite 200, Annapolis, MD 21401 USA.

This Standard was processed and approved for submittal to ANSI by the Accredited Standards Committee on Financial Services, X9. Committee approval of the Standard does not necessarily imply that all the committee members voted for its approval.

The X9 committee had the following members:
James Shaffer, X9 Chairman
Vincent DeSantis, X9 Vice-Chairman
Cynthia Fuller, Executive Director

Organization Represented	Representative
ACI Worldwide	Jim Shaffer
American Bankers Association	C. Diane Poole
American Express Company	John Allen
American Financial Services Association	Mark Zalewski
Bank of America	Daniel Welch
Capital One	Scott Sykes
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Mike Halpern
Clarke American Checks, Inc.	John W. McCleary
Deluxe Corporation	John Fitzpatrick
Diebold, Inc.	R. David Nein
Discover Financial Services	Katie Howser
Federal Reserve Bank	Dexter Holt
First Data Corporation	Connie Spurgeon
Fiserv	Skip Smith
FSTC, Financial Services Technology Consortium	Daniel Schutzer
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker

iStream Imaging	Ken Biel
IBM Corporation	Todd Arnold
Identrus	Mack Hicks
Ingenico	John Spence
Intuit, Inc.	Jana Hocker
J.P. Morgan Chase & Co	Jacqueline Pagan
KPMG LLP	Mark Lundin
MagTek, Inc.	Carlos Morales
MasterCard International	William Poletti
National Association of Convenience Stores	Gray Taylor
National Security Agency	Sheila Brand
NCR Corporation	Steve Stevens
SWIFT/Pan Americas	Malene McMahon
The Clearing House	Vincent DeSantis
U.S. Bank	Marc Morrison
University Bank	Stephen Ranzini
VeriFone, Inc.	Brad McGuinness
VECTORsgi	Ron Schultz
VISA	Richard Sweeney
Wachovia Bank	Ray Gatland
Wells Fargo Bank	Ruven Schwartz

The X9F subcommittee on Data and Information Security had the following members:
Richard J. Sweeney, Chairman

Organization Represented	**Representative**
3PEA Technologies, Inc.	Mark Newcomer
ACI Worldwide	Jim Shaffer
American Bankers Association	C. Diane Poole
American Express Company	John Allen
American Financial Services Association	Mark Zalewski
Bank of America	Andi Coleman
Capital One	Scott Sykes
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Paul Gubiotti
Citigroup, Inc.	Mike Halpern
Clarke American Checks, Inc.	John W. McCleary
Clarke American Checks, Inc.	John Petrie
Deluxe Corporation	John Fitzpatrick
DeLap, White, Caldwell and Croy, LLP	Darlene Kargel
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Julie Shaw
Entrust, Inc.	Robert Zuccherato
Federal Reserve Bank	Neil Hersch
Ferris and Associates, Inc.	J. Martin Ferris

Fidelity Investments	Michael Versace
First Data Corporation	Connie Spurgeon
Fiserv	Bud Beattie
FSTC, Financial Services Technology Consortium	Daniel Schutzer
FTI Consulting	Roger Nebel
Futurex	Jason Anderson
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
IBM Corporation	Todd Arnold
Identrus	Mack Hicks
InfoGard Laboratories	Tom Caddy
Ingenico	John Spence
Intel Massachusetts, Inc.	John Cyr
J.P. Morgan Chase & Co	Edward Koslow
MagTek, Inc.	Terry Benson
National Institute of Standards and Technology	Elaine Barker
National Security Agency	Sheila Brand
NCR Corporation	David Norris
NTRU Cryptosystems, Inc.	William Whyte
Pi R Squared Consulting LLP	Ralph Spencer Poore
Pitney Bowes, Inc.	Leon Pintsov
Proofspace	Paul F. Doyle
RSA Security, Inc.	James Randall
Surety, Inc.	Dimitrios Andivahis
TECSEC Incorporated	Ed Scheidt
Thales e-Security, Inc.	James Torjussen
Triton Systems of Delaware, Inc.	Daryll Cordeiro
U.S. Bank	Marc Morrison
University Bank	Stephen Ranzini
VeriFone, Inc.	Dave Faoro
Verisign, Inc.	Joseph Adler
VECTORsgi	Ron Schultz
VISA	Richard Sweeney
Wachovia Bank	Ray Gatland
Wells Fargo Bank	Ruven Schwartz

Under ASC X9 procedures, a working group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A working group exists only to develop standard(s) or guideline(s) in a specific area and is then disbanded. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the standard or guideline. (Note: Per X9 policy, company names of non-member participants are listed only if, at time of publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

The X9F1 Cryptographic Tool Standards and Guidelines group that developed this Standard had the following members:

Miles Smid, Chairman

Don Johnson and Miles Smid, Project Editors

Organization	**Representative**
Certicom Corporation	Dan Brown
Communications Security Establishment of Canada	Bridget Walshe
Entrust	Don Johnson
HP	Susan Langford
Microsoft	Niels Furguson
National Institute of Standards and Technology	Elaine Barker
	Lily Chen
	Morris Dworkin
	John Kelsey
National Security Agency	Paul Timmel
	Michael Boyle
NTRU	William Whyte
Orion Security Solutions	Miles Smid
Pitney Bowes, Inc	Matt Compagna
RSA Security	James Randall
	Steve Schmalz
University Bank	Michael Talley

Random Number Generation, Part 1: Overview and Basic Principles

1 Scope

This Standard defines techniques for the generation of random numbers that **shall** be used whenever ASC X9 Standards require the use of a random number or bitstring for cryptographic purposes. The Standard consists of four parts:

- Part 1: Overview and Basic Principles
- Part 2: Entropy Sources
- Part 3: Deterministic Random Bit Generator Mechanisms
- Part 4: Random Bit Generator Construction

Part 1 contains:

1. A functional model for random bit generators,
2. The general properties necessary for random bit generators to produce bitstrings that are suitable for cryptographic use, and
3. Approved methods for converting a random number into a random bitstring and vice versa.

Part 2 contains:

1. An Entropy Source model,
2. Entropy Source properties, requirements and design criteria,
3. Examples of Entropy Sources, and
4. Implementation validation and health testing of Entropy Sources.

Part 3 contains:

1. A model for deterministic random number generators (DRBGs),
2. Requirements for DRBG mechanisms,
3. Specifications for Approved DRBG mechanisms, and