American National Standard for Financial Services

ANS X9.82: Part 3–2007 (R2017)

Random Number Generation

Part 3: Deterministic Random Bit Generators

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: September 11, 2007
Date Reaffirmed: January 27, 2017

American National Standards Institute

Foreword

The Accredited Standards Committee on Financial Services (ASC 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
275 West Street, Suite 107
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

Introduction

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

This part of ANS X9.82 (Part 3) defines mechanisms for the generation of random bits using deterministic methods.

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, 275 West Street, Suite 107, 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.

Discover Financial Services .... Katie Howser
Federal Reserve Bank .... Dexter Holt
First Data Corporation .... Elizabeth Lynn
Fiserv .... Skip Smith
FSTC, Financial Services Consortium .... Daniel Schutzer
Hewlett Packard .... Larry Hines
Hypercom .... Scott Spiker
IBM Corporation .... Todd Arnold
Ingenico .... John Spence
Intuit, Inc. .... Jana Hocker
iStream Imaging Bank of Kenney .... Ken Biel
JP Morgan Chase & Co .... Jacqueline Pagan
KPMG LLP .... Mark Lundin
Mag-Tek, Inc. .... Carlos Morales
MasterCard International .... William Poletti
National Association of Convenience Stores .... Michael Davis
National Security Agency .... Sheila Brand
NCR Corporation .... Steve Stevens
RMG SWIFT .... Jean-Marie Eloy
SWIFT/Pan Americas .... Malene McMahon
The Clearing House .... Vincent DeSantis
U.S. Bank .... Marc Morrison
University Bank .... Stephen Ranzini
VECTOR .... Ron Schultz
VeriFone .... Brad McGuinnes
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, X9F Chairman
Sandra Lambert, X9F Vice Chairman

Organization Represented — ***Representative***

ACI Worldwide .... Doug Grote
3PEA Technologies, Inc. .... Mark Newcomer
ACI Worldwide .... Jim Shaffer
American Financial Services Association .... Mark Zalewski
Bank of America .... Daniel Welch
Certicom Corporation .... Daniel Brown
Citigroup, Inc. .... Gary Word
Clearwave Electronics .... Mark Ross

CUSIP Servis Bureau .... Scott Preiss
DeLap, White, Caldwell and Croy, LLP .... Darlene Kargel
Deluxe Corporation .... John Fitzpatrick
Depository Trust and Clearing Corporation .... Robert Palatnick
Diebold, Inc. .... Bruce Chapa
Discover Financial Services .... Julie Shaw
Entrust, Inc. .... Miles Smid
Federal Reserve Bank .... Jeannine M. DeLano
Federal Reserve Bank .... Dexter Holt
Ferris and Associates, Inc. .... J. Martin Ferris
First Data Corporation .... Rick Van Luvender
First National Bank of Nebraska, Inc. .... Lisa Curry
Fiserv .... Bud Beattie
FSTC, Financial Services Technical Consortium .... Daniel Schutzer
Futurex .... Jason Anderson
Harland Clarke .... John McCleary
Hewlett Packard .... Larry Hines
Hypercom .... Scott Spiker
IBM Corporation .... Todd Arnold
InfoGuard Laboratories .... Tom Caddy
Ingenico .... John Spence
Innove .... Steven Teppler
Intel Massachusetts, Inc. .... Paul Posco
JP Morgan Chase & Co .... Edward Koslow
KPMG LLP .... Mark Lundin
Mag-Tek, Inc. .... Carlos Morales
MasterCard International .... Michael Ward
National Institute of Standards and Technology .... Lily Chen
National Security Agency .... Sheila Brand
NCR Corporation .... David Norris
NTRU Cryptosystems .... William Whyte
Pitney Bowes Inc. .... Leon Pintsov
Proofspace .... Paul F. Doyle
Rosetta Technologies .... Jim Maher
Rosetta Technologies .... Paul Malinowski
RSA, The Security Division of EMC .... James Randall
Surety, Inc. .... Dimitrios Andivahis
TECSEC Incorporated .... Ed Scheidt
Thales e-Security, Inc. .... James Torjussen
The Clearing House .... Vincent DeSantis
Triton Systems of Delaware .... Daryll Cordeiro
U.S. Bank .... Marc Morrison
Unisys Corporation .... David J. Concannon
University Bank .... Stephen Ranzini
VECTOR .... Ron Schultz

VeriFone .... Dave Faoro
VISA .... John Sheets
Voltage Security, Inc. .... Luther Martin
Wachovia Bank .... Ray Gatland
Wells Fargo Bank .... Ruven Schwartz

Under ASC X9, Inc. 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 the 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, and Elaine Barker, Project Editor

Organization Represented .... ***Representative***

ACI Worldwide .... Doug Grote
Certicom Corporation .... Dan Brown
Certicom Corporation .... Scott Vanstone
Communications Security Establishment of Canada .... Bridget Walshe
Entrust .... Don Johnson
Entrust .... Miles Smid
MasterCard .... Mike Ward
National Institute of Standards and Technology .... Elaine Barker
National Institute of Standards and Technology .... Lily Chen
National Institute of Standards and Technology .... Morris Dworkin
National Institute of Standards and Technology .... John Kelsey
National Security Agency .... Paul Timmel
National Security Agency .... Michael Boyle
NTRU .... William Whyte
Pitney Bowes, Inc. .... Matt Campagna
Pitney Bowes, Inc. .... Rick Ryan
RSA, The Security Division of EMC .... James Randall
RSA, The Security Division of EMC .... Burt Kaliski
RSA, The Security Division of EMC .... Steve Schmalz

Random Number Generation

Part 3: Deterministic Random Bit Generator Mechanisms

1 Scope

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 should be read for a basic understanding of this Standard before reading Part 3. This part of ANSI X9.82 (Part 3) defines mechanisms for the generation of random bits using deterministic methods. The DRBG mechanisms are not sufficient by themselves to define a Random Bit Generator (RBG); Parts 2 and 4 of this Standard provide further requirements for the design of an RBG.

Part 3 includes:

1. A model for a deterministic random bit generator (DRBG),
2. Requirements for DRBG mechanisms,
3. Specifications for DRBG mechanisms that are based on hash functions or block ciphers, or are based on number theoretic problems,
4. Implementation issues, and
5. Assurance considerations.

A DRBG is based on a DRBG mechanism as specified in this part of the Standard and includes a source of entropy input. Part 3 specifies several diverse DRBG mechanisms, all of which provided acceptable security when this Standard was approved. However, in the event that new attacks are found on a particular class of mechanisms, a diversity of approved mechanisms will allow a timely transition to a different class of DRBG mechanism.

Random number generation does not require interoperability between two entities, e.g., communicating entities may use different DRBG mechanisms without affecting their ability to communicate. Therefore, an entity may choose a single appropriate DRBG mechanism for its applications; see Annex D for a discussion of DRBG selection.

The precise structure, design and development of a random bit generator is outside the scope of this Standard.

2 Conformance

An implementation of a DRBG mechanism may claim conformance with ANS X9.82 if it implements the mandatory provisions of Part 1 and the mandatory requirements of one or more of the DRBG mechanisms specified in this part of the Standard. An implementation of a DRBG may claim conformance with ANS X9.82 as an RBG if the following are implemented: the mandatory provisions of Part 1, the mandatory requirements of one or more of the DRBG mechanisms specified in this part of the Standard, an entropy source from Part 2 and the appropriate mandatory requirements of Part 4.

