



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

American National Standards, Technical Reports and Guides developed through the Accredited Standards Committee X9, Inc., are copyrighted. Copying these documents for personal or commercial use outside X9 membership agreements is prohibited without express written permission of the Accredited Standards Committee X9, Inc. For additional information please contact ASC X9, Inc., 1212 West Street, Suite 200, Annapolis, Maryland 21401.

Contents

Foreword.....	iv
Introduction	vi
1 Scope	1
2 Conformance	2
3 Normative references.....	2
4 Terms and definitions	2
5 Symbols and Abbreviations	10
6 General Discussion.....	11
6.1 Overview of Document	11
6.2 The Need for Random Numbers.....	12
6.3 Examples of Cryptographic Use of Random Numbers	13
7 Overview of Random Bit Generators.....	15
7.1 Secure RBG	15
7.2 Idealized Coin Flipping – The Canonical RBG	15
7.2.1 Coin Flipping Preliminaries	15
7.2.2 Properties of Idealized Coin Flipping	15
7.2.3 Possible Problems with Actual Coin Flipping	16
7.2.4 von Neumann Unbiasing	17
7.3 Random Bit Generation Functional Model	17
7.3.1 Entropy Source.....	19
7.3.2 Algorithmic Processing	19
7.3.3 Interfacing with the RBG	20
7.4 Types of Random Bit Generators	20
7.4.1 Non-deterministic Random Bit Generator (NRBG).....	21
7.4.2 Deterministic Random Bit Generator (DRBG).....	21
7.4.3 The RBG Spectrum	22
7.4.4 Summary of an Approved RBG.....	23
8 Security Properties of a Random Bit Generator	23
8.1 General Discussion.....	23
8.2 Security Strengths	23
8.3 Entropy and Min-Entropy	24
8.4 Backtracking Resistance and Prediction Resistance	25
8.5 Indistinguishability Versus Unpredictability.....	26
8.6 Prediction Resistance and Backtracking Resistance Considerations	27
8.7 Desired RBG Output Properties.....	28
8.8 Desired RBG Operational Properties.....	29

9 Converting Random Bits to/from Random Numbers	30
9.1 The Need for Conversion Routines	30
9.2 Converting Random Bits into a Random Number	30
9.2.1 The Simple Discard Method	31
9.2.2 The Complex Discard Method	31
9.2.3 The Simple Modular Method.....	32
9.2.4 The Complex Modular Method	32
9.3 Converting a Random Number into Random Bits.....	33
9.3.1 The No Skew (Variable Length Extraction) Method.....	33
9.3.2 The Negligible Skew (Fixed Length Extraction) Method.....	34
Annex A (Informative) Security Considerations	36
A.1 Attack Model	36
A.2 RBG Security Analysis.....	36
A.3 Computationally-Indistinguishable Randomness Theorems.....	37
A.4 Min-Entropy as the Measure of Entropy	38
A.4.1 Why Shannon Entropy Is Not Appropriate	39
A.4.2 Why Guessing Entropy Is Not Appropriate	40
A.4.3 Min-Entropy Tutorial.....	41
Annex B (Informative) Bibliography	43

Figures

Figure 1: Random Bit Generation Functional Model.....	18
Figure 2: Sequence of DRGB States.....	26

ANS X9.82, Part 1-2006

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>

Copyright © 2004 ASC X9, Inc.
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of the publisher. Published in the United States of America.

ANS X9.82, Part 1-2006

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

ACI Worldwide
American Bankers Association
American Express Company
American Financial Services Association
Bank of America
Capital One
Certicom Corporation
Citigroup, Inc.
Clarke American Checks, Inc.
Deluxe Corporation
Diebold, Inc.
Discover Financial Services
Federal Reserve Bank
First Data Corporation
Fiserv
FSTC, Financial Services Technology
Consortium
Hewlett Packard
Hypercom

Representative

Jim Shaffer
C. Diane Poole
John Allen
Mark Zalewski
Daniel Welch
Scott Sykes
Daniel Brown
Mike Halpern
John W. McCleary
John Fitzpatrick
R. David Nein
Katie Howser
Dexter Holt
Connie Spurgeon
Skip Smith

Daniel Schutzer
Larry Hines
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
VECTORsg	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

3PEA Technologies, Inc.
ACI Worldwide
American Bankers Association
American Express Company
American Financial Services Association
Bank of America
Capital One
Certicom Corporation
Citigroup, Inc.
Citigroup, Inc.
Clarke American Checks, Inc.
Clarke American Checks, Inc.
Deluxe Corporation
DeLap, White, Caldwell and Croy, LLP
Diebold, Inc.
Discover Financial Services
Entrust, Inc.
Federal Reserve Bank
Ferris and Associates, Inc.

Representative

Mark Newcomer
Jim Shaffer
C. Diane Poole
John Allen
Mark Zalewski
Andi Coleman
Scott Sykes
Daniel Brown
Paul Gubiotti
Mike Halpern
John W. McCleary
John Petrie
John Fitzpatrick
Darlene Kargel
Bruce Chapa
Julie Shaw
Robert Zuccherato
Neil Hersch
J. Martin Ferris

ANS X9.82, Part 1-2006

Fidelity Investments
First Data Corporation
Fiserv
FSTC, Financial Services Technology
Consortium
FTI Consulting
Futurex
Hewlett Packard
Hypercom
IBM Corporation
Identrus
InfoGard Laboratories
Ingenico John Spence
Intel Massachusetts, Inc.
J.P. Morgan Chase & Co
MagTek, Inc.
National Institute of Standards
and Technology
National Security Agency
NCR Corporation
NTRU Cryptosystems, Inc.
Pi R Squared Consulting LLP
Pitney Bowes, Inc.
Proofspace
RSA Security, Inc.
Surety, Inc.
TECSEC Incorporated
Thales e-Security, Inc.
Triton Systems of Delaware, Inc.
U.S. Bank
University Bank
VeriFone, Inc.
Verisign, Inc.
VECTORsgi
VISA
Wachovia Bank
Wells Fargo Bank

Michael Versace
Connie Spurgeon
Bud Beattie

Daniel Schutzer
Roger Nebel
Jason Anderson
Larry Hines
Scott Spiker
Todd Arnold
Mack Hicks
Tom Caddy

John Cyr
Edward Koslow
Terry Benson

Elaine Barker
Sheila Brand
David Norris
William Whyte
Ralph Spencer Poore
Leon Pintsov
Paul F. Doyle
James Randall
Dimitrios Andivahis
Ed Scheidt
James Torjussen
Daryll Cordeiro
Marc Morrison
Stephen Ranzini
Dave Faoro
Joseph Adler
Ron Schultz
Richard Sweeney
Ray Gatland
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

Certicom Corporation

Communications Security Establishment of Canada

Entrust

HP

Microsoft

National Institute of Standards and Technology

National Security Agency

NTRU

Orion Security Solutions

Pitney Bowes, Inc

RSA Security

University Bank

Representative

Dan Brown

Bridget Walshe

Don Johnson

Susan Langford

Niels Furguson

Elaine Barker

Lily Chen

Morris Dworkin

John Kelsey

Paul Timmel

Michael Boyle

William Whyte

Miles Smid

Matt Compagna

James Randall

Steve Schmalz

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