



American National Standard for Financial Services

ANS X9.82: Part 3–2007

Random Number Generation Part 3: Deterministic Random Bit Generators



Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved:

American National Standards Institute

American National Standards, Technical Reports and Guides developed through 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.....	vii
Introduction	viii
1 Scope	1
2 Conformance	1
3 Normative References	2
4 Terms and Definitions.....	2
5 Abbreviations and Symbols	5
6 General Discussion and Organization.....	7
7 Functional Model.....	9
7.1 General Discussion	9
7.2 Functional Model Components	9
7.2.1 Entropy Input	9
7.2.2 Other Inputs	10
7.2.3 The Internal State	10
7.2.4 The DRBG Mechanism Functions	10
8. DRBG Mechanism Concepts and General Requirements	11
8.1 Introduction.....	11
8.2 DRBG Mechanism Functions and a DRBG Instantiation.....	11
8.2.1 DRBG Mechanism Functions	11
8.2.2 DRBG Instantiations	11
8.2.3 Internal States	11
8.2.4 Security Strengths Supported by an Instantiation	12
8.3 DRBG Mechanism Boundaries	13
8.4 Seeds	14
8.4.1 General Discussion	14
8.4.2 Generation and Handling of Seeds	15
8.5 Other Inputs to the DRBG Mechanism.....	17
8.5.1 Discussion	17
8.5.2 Personalization String.....	17
8.5.3 Additional Input.....	18

ANS X9.82, Part 3 –2007

8.6	Prediction Resistance and Backtracking Resistance	18
9	DRBG Mechanism Functions	19
9.1	General Discussion	19
9.2	Instantiating a DRBG.....	19
9.3	Reseeding a DRBG Instantiation	22
9.4	Generating Pseudorandom Bits Using a DRBG	24
9.4.1	The Generate Function.....	25
9.4.2	Reseeding at the End of the Seedlife.....	27
9.4.3	Handling Prediction Resistance Requests	28
9.5	Removing a DRBG Instantiation	28
10	DRBG Algorithm Specifications	30
10.1	Overview	30
10.2	Deterministic RBG Based on Hash Functions	30
10.2.1	Discussion	30
10.2.2	HMAC_DRBG.....	31
10.2.2.1	Discussion.....	31
10.2.2.2	Specifications	32
10.2.2.2.1	HMAC_DRBG Internal State.....	32
10.2.2.2.2	The Update Function (CTR_DRBG_Update)	32
10.2.2.2.3	Instantiation of HMAC_DRBG.....	33
10.2.2.2.4	Reseeding an HMAC_DRBG Instantiation	34
10.2.2.2.5	Generating Pseudorandom Bits Using HMAC_DRBG	34
10.3	DRBG Mechanisms Based on Block Ciphers	36
10.3.1	Discussion	36
10.3.2	CTR_DRBG	36
10.3.2.1	CTR_DRBG Description	36
10.3.2.2	Specifications	38
10.3.2.2.1	CTR_DRBG Internal State.....	38
10.3.2.2.2	The Update Function (CTR_DRBG_Update)	39
10.3.2.2.3	Instantiation of CTR_DRBG.....	39
10.3.2.2.4	Reseeding a CTR_DRBG Instantiation	41
10.3.2.2.5	Generating Pseudorandom Bits Using CTR_DRBG.....	43

10.4	DRBG Mechanisms Based on Number Theoretic Problems	47
10.4.1	Discussion	47
10.4.2	Dual Elliptic Curve Deterministic RBG (Dual_EC_DRBG)	47
10.4.2.1	Discussion	47
10.4.2.2	Specifications	49
10.4.2.2.1	Dual_EC_DRBG Internal State	49
10.4.2.2.2	Instantiation of Dual_EC_DRBG	50
10.4.2.2.3	Reseeding of a Dual_EC_DRBG Instantiation	51
10.4.2.2.4	Generating Pseudorandom Bits Using Dual_EC_DRBG	51
10.5	Auxiliary Functions	54
10.5.1	Discussion	54
10.5.2	Derivation Function Using a Hash Function (Hash_df)	54
10.5.3	Derivation Function Using a Block Cipher Algorithm (Block_Cipher_df)	55
10.5.4	BCC Function	57
11	Assurance	58
11.1	Overview	58
11.2	Minimal Documentation Requirements	58
11.3	Implementation Validation Testing	59
11.4	Health Testing	59
11.4.1	Overview	59
11.4.2	Known-Answer Testing	60
11.4.3	Testing the Instantiate Function	60
11.4.4	Testing the Generate Function	60
11.4.5	Testing the Reseed Function	61
11.4.6	Testing the Uninstantiate Function	61
11.4.7	Error Handling	61
11.4.7.1	General Discussion	61
11.4.7.2	Errors Encountered During Normal Operation	61
11.4.7.3	Errors Encountered During Health Testing	62
Annex A:	(Normative) Application-Specific Constants	63
A.1	Constants for the Dual_EC_DRBG	63
A.1.1	Curves over Prime Fields	63

ANS X9.82, Part 3 –2007

A.1.1.1 Curve P-256.....	63
A.1.1.2 Curve P-384.....	64
A.1.1.3 Curve P-521.....	64
A.2 Using Alternative Points in the Dual_EC_DRBG()	65
A.2.1 Generating Alternative P, Q	65
A.2.2 Additional Self-testing Required for Alternative P, Q	66
ANNEX B : (Normative) Conversion and Auxiliary Routines.....	67
B.1 Bitstring to an Integer.....	67
B.2 Integer to a Bitstring.....	67
B.3 Integer to a Byte String.....	67
B.4 Byte String to an Integer.....	68
Annex C: (Informative) Security Considerations.....	69
C.1 Extracting Bits in the Dual_EC_DRBG (...).....	69
C.1.1 Potential Bias Due to Modular Arithmetic for Curves Over F_p	69
C.1.2 Adjusting for the Missing Bit(s) of Entropy in the x Coordinates.	69
ANNEX D: (Informative) DRBG Mechanism Selection	73
D.1 Choosing a DRBG Algorithm	73
D.2 HMAC_DRBG	73
D.3 CTR_DRBG.....	74
D.4 DRBGs Based on Hard Problems.....	75
D.5 Summary for DRBG Selection	76
ANNEX E: (Informative) Example Pseudocode for Each DRBG Mechanism	77
E.1 Preliminaries.....	77
E.2 HMAC_DRBG Example	77
E.2.1 Discussion	77
E.2.2 Instantiation of HMAC_DRBG	78
E.2.3 Generating Pseudorandom Bits Using HMAC_DRBG.....	79
E.3 CTR_DRBG Example Using a Derivation Function	81
E.3.1 Discussion	81
E.3.2 The CTR_DRBG_Update Function	82
E.3.3 Instantiation of CTR_DRBG Using a Derivation Function.....	82

E.3.4	Reseeding a CTR_DRBG Instantiation Using a Derivation Function	84
E.3.5	Generating Pseudorandom Bits Using CTR_DRBG	85
E.4	CTR_DRBG Example Without a Derivation Function	87
E.4.1	Discussion	87
E.4.2	The CTR_DRBG_Update Function	88
E.4.3	Instantiation of CTR_DRBG Without a Derivation Function	88
E.4.4	Reseeding a CTR_DRBG Instantiation Without a Derivation Function	88
E.4.5	Generating Pseudorandom Bits Using CTR_DRBG	89
E.5	Dual_EC_DRBG Example.....	89
E.5.1	Discussion	89
E.5.2	Instantiation of Dual_EC_DRBG	90
E.5.3	Reseeding a Dual_EC_DRBG Instantiation	Error! Bookmark not defined.
E.5.4	Generating Pseudorandom Bits Using Dual_EC_DRBG	91
ANNEX F: (Informative) DRBG Provision of RBG Security Properties		94
F.1	Introduction.....	94
F.2	Security Strengths.....	94
F.3	Entropy and Min-Entropy.....	94
F.4	Backtracking Resistance and Prediction Resistance	94
F.5	Indistinguishability and Unpredictability	94
F.6	Desired RBG Output Properties.....	94
F.7	Desired RBG Operational Properties	95
ANNEX G:.....		97
G.1	Overview	97
G.2	HMAC_DRBG	97
G.3	CTR_DRBG.....	97
G.4	Dual_EC_DRBG.....	98
Bibliography		101

ANS X9.82, Part 3 –2007

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
P.O. Box 4035
Annapolis, MD 21403 USA
X9 Online <http://www.x9.org>

Copyright © 2007 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.

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, P.O. Box 4035, Annapolis, MD 21403 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
Susan Yashinskie, Managing Director

Organization Represented

ACI Worldwide
American Banker's Association
American Express Company
American Financial Services Association
Bank of America
Capital One
Certicom Corporation
Citigroup, Inc.
Clarker American Checks, Inc.
CUSIP Service Bureau
Deluxe Corporation
Diebold, Inc.
Discover Financial Services
Federal Reserve Bank
First Data Corporation
Fiserv
FSTC, Financial Services Consortium

Representative

James Shaffer
C. Diane Poole
John Allen
Mark Zalewski
Daniel Welch
Scott Sykes
Daniel Brown
Mike Halpern
John W. McCleary
James Taylor
John Fitzpatrick
Bruce Chapa
Katie Howser
Dexter Holt
Elizabeth Lynn
Skip Smith
Daniel Schutzer

ANS X9.82, Part 3 –2007

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 sgi	Ron Schultz
VeriFone	Brad McGuinness
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

3PEA Technologies, Inc.
ACI Worldwide
American Financial Services Association
Bank of America
Certicom Corporation
Citigroup, Inc.
Clearwave Electronics
CUSIP Servis Bureau
DeLap, White, Caldwell and Croy, LLP
Deluxe Corporation
Depository Trust and Clearing Corporation
Diebold, Inc.
Discover Financial Services
Entrust, Inc.
Federal Reserve Bank
Federal Reserve Bank
Ferris and Associates, Inc.
First Data Corporation
First National Bank of Nebraska, Inc.
Fiserv
FSTC, Financial Services Technical Consortium
Futurex
Harland Clarke

Representative

Mark Newcomer
Jim Shaffer
Mark Zalewski
Daniel Welch
Daniel Brown
Gary Word
Mark Ross
Scott Preiss
Darlene Kargel
John Fitzpatrick
Robert Palatnick
Bruce Chapa
Julie Shaw
Miles Smid
Jeannine M. DeLano
Dexter Holt
J. Martin Ferris
Rick Van Luvender
Lisa Curry
Bud Beattie
Daniel Schutzer
Jason Anderson
John McCleary

Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
IBM Corporation	Todd Arnold
InfoGuard Laboratories	Tom Caddy
Ingenico	John Spence
Innove	Steven Tepler
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
VECTORsgi	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

Certicom Corporation
Certicom Corporation
Communications Security Establishment of Canada
Entrust

Representative

Dan Brown
Scott Vanstone
Bridget Walshe
Don Johnson

ANS X9.82, Part 3 –2007

Entrust
MasterCard
National Institute of Standards and Technology
National Institute of Standards and Technology
National Institute of Standards and Technology
National Institute of Standards and Technology
National Security Agency
National Security Agency
NTRU
Pitney Bowes, Inc.
Pitney Bowes, Inc.
RSA, The Security Division of EMC
RSA, The Security Division of EMC
RSA, The Security Division of EMC

Miles Smid
Mike Ward
Elaine Barker
Lily Chen
Morris Dworkin
John Kelsey
Paul Timmel
Michael Boyle
William Whyte
Matt Campagna
Rick Ryan
James Randall
Burt Kaliski
Steve Schmalz

This is a preview of "ANSI X9.82: Part 3 -...". [Click here to purchase the full version from the ANSI store.](#)

ANS X9.82, Part 3 –2007

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.