



American National Standard for Financial Services

ANSI X9.82: Part 4–2011 (R2017)

Random Number Generation Part 4: Random Bit Generator Constructions



Developed by
Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: November 11, 2011

Date Reaffirmed: February 2, 2017

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., 275 West Street, Suite 107, Annapolis, Maryland 21401.

This is a preview of "ANSI X9.82: Part 4-2...". [Click here to purchase the full version from the ANSI store.](#)

ANSI X9.82-4-2011 (R2017)

Table of Contents

1	Scope.....	1
2	Conformance.....	1
3	Normative References.....	2
4	Terms and Definitions.....	3
5	Symbols and Abbreviated Terms.....	9
6	General Discussion	11
6.1	Introduction.....	11
6.2	RBG Security.....	12
6.3	Assumptions.....	13
6.4	Document Organization.....	13
7	Random Bit Generator Concepts	15
7.1	RBG Boundaries and Distributed RBGs.....	15
7.2	Full Entropy	17
7.3	Entropy Sources and Full Entropy Sources	17
7.4	Live Entropy Source	17
7.5	Backtracking and Prediction Resistance.....	18
7.6	Deterministic Random Bit Generators (DRBGs)	19
7.7	Non-deterministic Random Bit Generators (NRBGs).....	20
7.7.1	NRBG Discussion.....	20
7.7.2	Basic NRBGs.....	20
7.7.3	Enhanced NRBGs	21
8	Step By Step: How to Construct an RBG	22
9	RBG Interfaces and Primary Components.....	25
9.1	RBG Interfaces.....	25
9.1.1	General Discussion of RBG Interfaces	25
9.1.2	Pseudocode Conventions	25
9.2	Sources of Entropy Input (SEI).....	32
9.2.1	Primary SEI Components	32
9.2.2	General SEI Requirements.....	33
10	DRBG Construction.....	36
10.1	Overview	36

10.2	DRBG Functions.....	37
10.3	DRBGs with Live Entropy Sources.....	38
10.4	DRBGs without Live Entropy Sources.....	39
10.5	DRBGs with Intermittent Access to an Entropy Source.....	39
10.6	Non-volatile, Modifiable Storage	39
10.7	Sources of Other DRBG Inputs	40
10.7.1	Discussion.....	40
10.7.2	Nonces for DRBG Instantiation.....	40
10.7.3	Personalization Strings for DRBG Instantiation.....	40
10.7.4	Additional Input During Generate and Reseed Functions	40
10.7.5	Seedfiles.....	40
10.8	Considerations for DRBG Chains.....	42
10.9	DRBG Configurations	43
11	NRBG Construction.....	46
11.1	Introduction.....	46
11.2	Enhanced NRBGs vs. Basic NRBGs.....	46
11.3	The DRBG Mechanism within the NRBG	47
11.4	Construction: Enhanced NRBG – XOR Construction.....	47
11.4.1	Discussion	47
11.4.2	NRBG Instantiation	48
11.4.3	NRBG Generation.....	49
11.4.4	Direct DRBG Access	50
11.4.5	Entropy Required for NRBG Output.....	50
11.5	Construction: Enhanced NRBG – Oversampling Construction	50
11.5.1	Discussion	50
11.5.2	NRBG Instantiation	51
11.5.3	NRBG Generation.....	51
11.5.4	Direct DRBG Access	52
11.5.5	Entropy Required for NRBG Output.....	52
12	Combining RBGs.....	53
12.1	Discussion.....	53
12.2	Construction to Combine RBGs	53

ANSI X9.82-4-2011 (R2017)

12.2.1	Overview	53
12.2.2	Combined RBG Instantiation.....	54
12.2.3	Combined RBG Reseeding.....	56
12.2.4	Combined RBG Generation.....	57
13	Additional Constructions	59
13.1	Overview	59
13.2	Constructions Using an RBG as an SEI.....	60
13.2.1	Discussion.....	60
13.2.2	General Construction Using an RBG as an SEI.....	62
13.2.3	Constructions Using a DRBG as an SEI.....	62
13.2.4	Construction for Using an NRBG as an SEI.....	64
13.3	Constructions Using an Entropy Source as an SEI.....	65
13.3.1	Discussion	65
13.3.2	Construction for Using Any Entropy Source.....	66
13.3.3	Construction for Using a Full Entropy Source	67
13.3.4	Constructions for Accumulating and Condensing Entropy Source Output External to the Entropy Source.....	67
13.4	Construction for the External Conditioning of Entropy Sources.....	69
13.5	Constructions for Obtaining Entropy when an Entropy Source is Available Intermittently.....	70
13.5.1	Discussion	70
13.5.2	Insertion by Reseeding.....	70
13.5.3	Insertion as Additional Input	70
14	Testing.....	72
14.1	Introduction.....	72
14.2	Health Testing.....	72
14.2.1	Discussion.....	72
14.2.2	Testing Components Recursively	72
14.2.3	Known-Answer Testing for Part 4 Components.....	73
14.2.4	Handling Failure	73
14.3	Implementation Validation	73
14.3.1	Introduction.....	73
14.3.2	Minimum Documentation Requirements.....	74

Annex A (Normative) Conversion Routines.....	75
A.1 Introduction.....	75
A.2 Converting Bits into Integers.....	75
A.2.1 The Simple Discard Method.....	75
A.2.2 The Complex Discard Method.....	76
A.2.3 The Simple Modular Method.....	76
A.2.4 The Complex Modular Method.....	77
A.3 Converting a Random Integer into Random Bits.....	77
A.3.1 The No Skew (Variable Length Extraction) Method.....	77
A.3.2 The Negligible Skew (Fixed Length Extraction) Method.....	78
Annex B (Informative) RBG Examples.....	80
B.1 Example of the XOR Construction.....	80
B.1.1 Description.....	80
B.1.2 NRBG Instantiation.....	81
B.1.3 NRBG Generation.....	81
B.1.4 DRBG Generation.....	82
B.1.5 DRBG Reseeding.....	83
B.2 Example of the Oversampling Construction.....	83
B.2.1 Description.....	83
B.2.2 NRBG Instantiation.....	84
B.2.3 NRBG Generation.....	85
B.2.4 DRBG Generation.....	86
B.2.5 DRBG Reseeding.....	86
B.3 Alternative Example of the Oversampling Construction.....	87
B.3.1 Description.....	87
B.3.2 RBG Startup.....	88
B.3.3 RBG Generation.....	89
B.3.4 Reseeding.....	89
B.4 Example of a DRBG Without a Live Entropy Source.....	90
B.4.1 Description.....	90
B.4.2 DRBG Instantiation.....	90
B.4.3 DRBG Generation.....	91
B.4.4 DRBG Reseeding.....	91

ANSI X9.82-4-2011 (R2017)

B.5	Example of a DRBG with a Live Entropy Source	91
B.5.1	Description	91
B.5.2	DRBG Instantiation	92
B.5.3	DRBG Generation.....	92
B.5.4	DRBG Reseeding.....	92
B.5.5	Obtaining Full Entropy Output	93
B.6	A Chain of DRBGs without a Live Entropy Source.....	94
B.6.1	Description.....	94
B.6.2	DRBG Instantiation	95
B.6.3	DRBG Generation.....	97
B.6.4	DRBG Reseeding.....	97
B.7	A Chain of DRBGs with a Live Entropy Source.....	98
B.7.1	Description.....	98
B.7.2	DRBG Instantiation	99
B.7.3	DRBG Generation.....	100
B.7.4	DRBG Reseeding.....	100
B.7.5	Obtaining Full Entropy Output	101
B.8	A DRBG with a Live Entropy Source and a Seedfile.....	103
B.8.1	Description.....	103
B.8.2	DRBG Instantiation	104
B.8.3	DRBG Generation.....	104
B.8.4	DRBG Reseeding.....	105
B.9	Combined RBG.....	106
B.9.1	Description.....	106
B.9.2	RBG Instantiation	106
B.9.3	RBG Generation.....	107
B.9.4	RBG Reseeding.....	107
Annex C (Informative)	Security Considerations	108
C.1	Enhanced NRBG Constructions	108
C.1.1	Discussion	108
C.1.2	XOR Construction	108
C.1.3	Oversampling Construction	109
C.2	Seedfiles.....	110

C.3	Full Entropy, Prediction Resistance, and Security.....	111
C.3.1	A DRBG without a Live Entropy Source	111
C.3.2	A DRBG with a Live Entropy Source	112
C.3.3	An NRBG with Full Entropy Output.....	113
C.4	Combining Multiple SEIs to Provide Entropy Input	114
C.4.1	All SEIs are RBGs	114
C.4.2	All SEIs are Entropy Sources	115
C.4.3	The SEIs are a Combination of RBGs and Entropy Sources.....	116
C.5	RBG Security Strength	117
Annex D (Normative)	Implementation Considerations.....	118
D.1	DRBG Interaction with an SEI During Instantiation and Reseeding	118
D.1.1	Scenarios	118
D.1.2	Making the SEI Characteristics Known to the (Target) DRBG	124
D.2	Real-life Scenarios.....	125
D.2.1	An RBG in Smart Cards	125
D.2.2	An RBG in a Laptop	126
D.2.3	A Self-contained RBG.....	126

ANSI X9.82-4-2011 (R2017)

Foreword

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

Copyright © 2017 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.

ANSI X9.82-4-2011 (R2017)

Introduction

NOTE The user's attention is called to the possibility that compliance with this Standard may require the 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.

The X9 committee had the following members:

- X9 Chairman, Roy DeCicco
- Vincent DeSantis, X9 Vice-Chairman
- Steve Stevens, Executive Director

<i>Organization Represented</i>	<i>Representative</i>
ACI Worldwide.....	Doug Grote
ACI Worldwide.....	Dan Kinney
American Bankers Association.....	Diane Poole
American Express Company.....	David Moore
Bank of America.....	Daniel Welch
Blackhawk Network.....	Anthony Redondo
Bloomberg LP.....	Corby Dear
Capital One.....	Marie LaQuerre
Citigroup, Inc.	Karla McKenna
CLS Bank.....	Ram Komarraju
Conexus, Inc.	Michael Davis
Conexus, Inc.	Gray Taylor
Delap LLP.....	Darlene Kargel
Deluxe Corporation.....	Angela Hendershott
Diebold, Inc.....	Bruce Chapa
Discover Financial Services.....	Michelle Zhang
eCurrency.....	David Wen
Federal Reserve Bank.....	Mary Hughes
Federal Reserve Bank.....	Janet LaFrence
FIS.....	Stephen Gibson-Saxty
Fiserv.....	Dan Otten
FIX Protocol Ltd - FPL.....	Jim Northey
Futurex.....	Ryan Smith
Gilbarco.....	Bruce Welch

Harland Clarke	John McCleary
Hewlett Packard	Susan Langford
IBM Corporation.....	Todd Arnold
Independent Community Bankers of America	Cary Whaley
Ingenico.....	Rob Martin
ISITC.....	Jason Brasile
J.P. Morgan Chase	Roy DeCicco
KPMG LLP.....	Mark Lundin
MagTek, Inc.....	Roger Applewhite
MagTek, Inc.....	Mimi Hart
MasterCard Europe Sprl	Mark Kamers
NACHA The Electronic Payments Association	Priscilla Holland
National Security Agency.....	Paul Timmel
Nautilus Hyosung.....	Joe Militello
NCR Corporation.....	David Norris
Office of Financial Research, U.S. Treasury Department	Justin Stekervetz
PCI Security Standards Council.....	Troy Leach
RouteOne	Chris Irving
RouteOne	Jenna Wolfe
State Street Corporation.....	Jason Brasile
SWIFT/Pan Americas	Frank Vandriessche
Symcor Inc.....	Debbi Fitzpatrick
TECSEC Incorporated	Ed Scheidt
The Clearing House	Sharon Jablon
U.S. Bank.....	John King
U.S. Commodity Futures Trading Commission (CFTC).....	Robert Stowsky
USDA Food and Nutrition Service.....	Kathy Ottobre
Vantiv LLC.....	Gary Zempich
VeriFone, Inc.....	Dave Faoro
VISA	Kim Wagner
Wayne Fueling Systems.....	Steven Bowles
Wells Fargo Bank	Mark Schaffer

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

<i>Organization Represented</i>	<i>Representative</i>
[ACI Worldwide	Doug Grote
ACI Worldwide.....	Dan Kinney
ACI Worldwide.....	Julie Samson
American Bankers Association.....	Tom Judd
American Express Company.....	Farid Hatefi
American Express Company.....	John Timar
American Express Company.....	Kevin Welsh
Bank of America.....	Amanda Adams

ANSI X9.82-4-2011 (R2017)

Bank of America	Peter Capraro
Bank of America	Andi Coleman
Bank of America	Lawrence LaBella
Bank of America	Will Robinson
Bank of America	Michael Smith
Bank of America	Daniel Welch
BlackBerry Limited	Daniel Brown
BlackBerry Limited	Sandra Lambert
Blackhawk Network.....	Anthony Redondo
Bloomberg LP	Erik Anderson
Bloomberg LP	Corby Dear
Capital One	Marie LaQuerre
Capital One	Johnny Lee
Cipherithm	Scott Spiker
comForte 21 GmbH	Thomas Gloerfeld
comForte 21 GmbH	Henning Horst
Communications Security Establishment	Jonathan Hammell
Communications Security Establishment	David Smith
Conexus, Inc.	Alan Thiemann
CUSIP Service Bureau.....	Scott Preiss
Delap LLP	David Buchanan
Delap LLP	Darlene Kargel
Deluxe Corporation.....	Angela Hendershott
Deluxe Corporation.....	Margiore Romay
Deluxe Corporation.....	Andy Vo
Diebold, Inc.....	Bruce Chapa
Diebold, Inc.....	Michael Ott
Diebold, Inc.....	Dave Phister
Discover Financial Services.....	Cheryl Mish
Discover Financial Services.....	Diana Pauliks
Discover Financial Services.....	Jordan Schaefer
eCurrency	David Wen
Federal Reserve Bank	Patrick Adler
Federal Reserve Bank	Cynthia Baxter
Federal Reserve Bank	Guy Berg
Federal Reserve Bank	Julia Cheney
Federal Reserve Bank	Marianne Crowe
Federal Reserve Bank	Sandeep Dhameja
Federal Reserve Bank	Amanda Dorphy
Federal Reserve Bank	Mary Hughes
Federal Reserve Bank	Heather Hultquist
Federal Reserve Bank	Janet LaFrence
Federal Reserve Bank	Jackie Nugent
Federal Reserve Bank	Jim O'Connell
Federal Reserve Bank	Susan Pandy
Federal Reserve Bank	Patti Ritter

Federal Reserve Bank	Daniel Rozycki
Federal Reserve Bank	Rick Sullivan
First Data Corporation	Andrea Beatty
First Data Corporation	Lisa Curry
First National Bank of Omaha	Kristi White
FIS.....	Chelsea Lopez
FIS.....	John Soares
FIS.....	Sunny Wear
Fiserv.....	Bud Beattie
Fiserv.....	Dan Otten
Futurex	Ryan Smith
GEOBRIDGE Corporation	Donna Gem
GEOBRIDGE Corporation	Jason Way
Gilbarco.....	Scott Turner
Gilbarco.....	Bruce Welch
Harland Clarke	Joseph Filer
Heartland Payment Systems	Scott Meeker
Hewlett Packard	Susan Langford
Hewlett Packard	Luther Martin
Hewlett Packard	Terence Spies
IBM Corporation.....	Todd Arnold
Independent Community Bankers of America	Cary Whaley
Ingenico.....	Rob Martin
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Bruce Geller
J.P. Morgan Chase	Kathleen Krupa
J.P. Morgan Chase	Jackie Pagán
K3DES LLC.....	Azie Amini
KPMG LLP	Mark Lundin
MagTek, Inc.....	Jeff Duncan
MagTek, Inc.....	Mimi Hart
MasterCard Europe Sprl	Mark Kamers
MasterCard Europe Sprl	Joshua Knopp
MasterCard Europe Sprl	Larry Newell
MasterCard Europe Sprl	Adam Sommer
MasterCard Europe Sprl	Michael Ward
National Institute of Standards and Technology (NIST)	Elaine Barker
National Institute of Standards and Technology (NIST)	Lily Chen
National Security Agency	Mike Boyle
National Security Agency	Paul Timmel
Nautilus Hyosung.....	Joe Militello
Nautilus Hyosung.....	Jay Shin
NCR Corporation	Tanika Eng
NCR Corporation	Charlie Harrow
NCR Corporation	David Norris
PCI Security Standards Council.....	Leon Fell

ANSI X9.82-4-2011 (R2017)

PCI Security Standards Council.....	Troy Leach
PCI Security Standards Council.....	Ralph Poore
RSA, The Security Division of EMC	Steve Schmalz
SafeNet, Inc.....	Amit Sinha
Security Innovation.....	Mark Etzel
Security Innovation.....	William Whyte
Security Innovation.....	Lee Wilson
Security Innovation.....	Zhenfei Zhang
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Dr. Wai Tsang
TECSEC Incorporated	Jay Wack
Thales UK Limited	Larry Hines
Thales UK Limited	James Torjussen
The Clearing House	Henry Farrar
Trustwave.....	John Amaral
Trustwave.....	Tim Hollebeek
U.S. Bank	Stephen Case
U.S. Bank	Peter Skirvin
Vantiv LLC	Bill Weingart
Vantiv LLC	Gary Zempich
Vantiv LLC	James Zerfas
VeriFone, Inc.	John Barrowman
VeriFone, Inc.	David Ezell
VeriFone, Inc.	Dave Faoro
VeriFone, Inc.	Doug Manchester
VeriFone, Inc.	Brad McGuinness
VeriFone, Inc.	Joachim Vance
VISA	Shahzad Khan
VISA	Kim Wagner
Wayne Fueling Systems.....	Steven Bowles
Wells Fargo Bank	William Felts, IV
Wells Fargo Bank	Phillip Griffin
Wells Fargo Bank	Jan Kohl
Wells Fargo Bank	Garrett Macey
Wells Fargo Bank	Kelly O'Donnell
Wells Fargo Bank	Mark Schaffer
Wells Fargo Bank	Jeff Stapleton
Wincor Nixdorf Inc.....	Christoph Bruecher
Wincor Nixdorf Inc.....	Andrea Carozzi
Wincor Nixdorf Inc.....	Michael Nolte
XYPRO Technology.....	Steve Tcherchian

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 part of the Standard had the following members:

Terence Spies, Chairman
 Elaine Barker, Project Editor

<i>Organization Represented</i>	<i>Representative</i>
ACI Worldwide.....	Doug Grote
ACI Worldwide.....	Dan Kinney
ACI Worldwide.....	Julie Samson
American Bankers Association.....	Tom Judd
American Express Company.....	Gail Chapman
American Express Company.....	Alan Fong
American Express Company.....	Michael Hyzer
American Express Company.....	Kenneth Mealey
American Express Company.....	David Moore
American Express Company.....	Clyde Van Blarcum
American Express Company.....	Kevin Welsh
Bank of America.....	Amanda Adams
Bank of America.....	Dion Bellamy
Bank of America.....	Peter Capraro
Bank of America.....	Terrelle Carswell
Bank of America.....	Andi Coleman
Bank of America.....	Lawrence LaBella
Bank of America.....	Chris Schrick
Bank of America.....	Michael Smith
Bank of America.....	Daniel Welch
Bank of America.....	Terri Willis
BetterBuyDesign.....	Steve Mott
BlackBerry Limited.....	Daniel Brown
BlackBerry Limited.....	John O. Goyo
BlackBerry Limited.....	Sandra Lambert
Blackhawk Network.....	Vari Bindra
Blackhawk Network.....	Anthony Redondo
Bloomberg LP.....	Erik Anderson
Capital One.....	Johnny Lee
Cipherithm.....	Scott Spiker
Cirque Inc.....	Jared Bytheway
Cirque Inc.....	Brian Monson
comForte 21 GmbH.....	Henning Horst
comForte 21 GmbH.....	Michael Horst

ANSI X9.82-4-2011 (R2017)

Conduent.....	Jennifer Baur
Conexxus, Inc.	Ann Seki
Conexxus, Inc.	Alan Thiemann
Conexxus, Inc.	Linda Toth
CUSIP Service Bureau.....	Scott Preiss
Delap LLP.....	David Buchanan
Delap LLP.....	Darlene Kargel
Diebold, Inc.....	Rick Brunt
Diebold, Inc.....	Bruce Chapa
Diebold, Inc.....	Scott Harroff
Diebold, Inc.....	Anne Konecny
Diebold, Inc.....	Michael Ott
Diebold, Inc.....	Dave Phister
Discover Financial Services.....	David Kloser
Discover Financial Services.....	Cheryl Mish
Discover Financial Services.....	Diana Pauliks
Discover Financial Services.....	Julie Quandt
Discover Financial Services.....	Lakshmi Ramanathan
Discover Financial Services.....	Jordan Schaefer
Discover Financial Services.....	Michelle Zhang
eCurrency.....	David Wen
Federal Reserve Bank.....	Patrick Adler
Federal Reserve Bank.....	Cynthia Baxter
Federal Reserve Bank.....	Guy Berg
Federal Reserve Bank.....	Jeremy Brotherton
Federal Reserve Bank.....	Julia Cheney
Federal Reserve Bank.....	Pieralberto Deganello
Federal Reserve Bank.....	Sandeep Dhameja
Federal Reserve Bank.....	Amanda Dorphy
Federal Reserve Bank.....	Mary Hughes
Federal Reserve Bank.....	Heather Hultquist
Federal Reserve Bank.....	Bob Hunt
Federal Reserve Bank.....	Janet LaFrence
Federal Reserve Bank.....	Joonho Lee
Federal Reserve Bank.....	Jackie Nugent
Federal Reserve Bank.....	Paul Nunnally
Federal Reserve Bank.....	Jim O'Connell
Federal Reserve Bank.....	Susan Pandy
Federal Reserve Bank.....	Michael Ram
Federal Reserve Bank.....	John Rhodes
Federal Reserve Bank.....	Patti Ritter
Federal Reserve Bank.....	Daniel Rozycki
Federal Reserve Bank.....	Rick Sullivan
Federal Reserve Bank.....	Charles Tsai
First Data Corporation.....	Andrea Beatty
First Data Corporation.....	Lisa Curry

ANSI X9.82-4-2011 (R2017)

First Data Corporation	Kerry Deardorff
First Data Corporation	Jacqueline Dill
First Data Corporation	Angela Ghetu
First Data Corporation	Brian Kean
First Data Corporation	Venkatesh Patil
First Data Corporation	Randall Rieth
First National Bank of Omaha	Kristi White
FIS.....	Tami Harris
FIS.....	Chelsea Lopez
Fiserv.....	Bud Beattie
Fiserv.....	Dan Otten
Futurex	Chris Hamlett
Futurex	Ryan Smith
GEOBRIDGE Corporation	Donna Gem
GEOBRIDGE Corporation	Dean Macinkas
GEOBRIDGE Corporation	Jason Way
Gilbarco.....	Scott Turner
Gilbarco.....	Bruce Welch
Harland Clarke	John McCleary
Heartland Payment Systems	Kevin Halliburton
Heartland Payment Systems	Randy Ison
Heartland Payment Systems	John Masden
Heartland Payment Systems	Scott Meeker
Hewlett Packard	Susan Langford
Hewlett Packard	Terence Spies
IBM Corporation.....	Todd Arnold
ID TECH.....	Eric Lecesne
Independent Community Bankers of America	Cary Whaley
Ingenico.....	Rob Martin
Ingenico.....	Steve McKibben
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Bruce Geller
J.P. Morgan Chase	Kathleen Krupa
J.P. Morgan Chase	Jackie Pagán
J.P. Morgan Chase	Darryl Scott
K3DES LLC.....	Azie Amini
K3DES LLC.....	James Richardson
KPMG LLP.....	Mark Lundin
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Sean Gately
MagTek, Inc.	Mimi Hart
Mainsail Trim, Inc.	Norman Cecil
MasterCard Europe Sprl	Mark Kamers
MasterCard Europe Sprl	Joshua Knopp
MasterCard Europe Sprl	Susie Thompson
MasterCard Europe Sprl	Michael Ward

ANSI X9.82-4-2011 (R2017)

MasterCard Europe Sprl	Gregory Williamson
Merchant Advisory Group	Brad Andrews
Merchant Advisory Group	Liz Garner
National Institute of Standards and Technology (NIST)	Elaine Barker
National Institute of Standards and Technology (NIST)	Lawrence Bassham
III	
National Institute of Standards and Technology (NIST)	William Burr
National Institute of Standards and Technology (NIST)	Lily Chen
National Institute of Standards and Technology (NIST)	David Cooper
National Institute of Standards and Technology (NIST)	Morris Dworkin
National Institute of Standards and Technology (NIST)	Randall Easter
National Institute of Standards and Technology (NIST)	Sharon Keller
National Institute of Standards and Technology (NIST)	Annabelle Lee
National Institute of Standards and Technology (NIST)	Fernando Podio
National Security Agency	Paul Timmel
Nautilus Hyosung.....	Joe Militello
Nautilus Hyosung.....	Jay Shin
NCR Corporation	Tanika Eng
NCR Corporation	Charlie Harrow
NCR Corporation	David Norris
NCR Corporation	Brian Wotherspoon
PCI Security Standards Council.....	Leon Fell
PCI Security Standards Council.....	Troy Leach
PCI Security Standards Council.....	Ralph Poore
Richard Sweeney	Richard Sweeney
RSA, The Security Division of EMC	Steve Schmalz
SafeNet, Inc.....	Chris Dunn
SafeNet, Inc.....	Kuldeep Saini
SafeNet, Inc.....	Amit Sinha
Security Innovation.....	Mark Etzel
Security Innovation.....	Jeff Hoffstein
Security Innovation.....	William Whyte
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Dr. Wai Tsang
TECSEC Incorporated	Jay Wack
Thales UK Limited	Colette Broadway
Thales UK Limited	Larry Hines
Thales UK Limited	James Torjussen
The Clearing House	Henry Farrar
The Clearing House	Sharon Jablon
Trustwave.....	John Amaral
Trustwave.....	Tim Hollebeek
U.S. Bank	Stephen Case
U.S. Bank	Peter Skirvin
USDA Food and Nutrition Service.....	Erin McBride
USDA Food and Nutrition Service.....	Kathy Ottobre

ANSI X9.82-4-2011 (R2017)

Vantiv LLC	Chris Doyle
Vantiv LLC	Bill Weingart
Vantiv LLC	Gary Zempich
Vantiv LLC	James Zerfas
VeriFone, Inc.	John Barrowman
VeriFone, Inc.	David Ezell
VeriFone, Inc.	Dave Faoro
VeriFone, Inc.	LeAnn Hostetler
VeriFone, Inc.	Chris Madden
VeriFone, Inc.	Doug Manchester
VeriFone, Inc.	Brad McGuinness
VeriFone, Inc.	Joachim Vance
VISA	Adam Clark
VISA	Hap Huynh
VISA	Shahzad Khan
VISA	Chackan Lai
VISA	Stoddard Lambertson
VISA	Sekhar
Nagasundaram	
VISA	Michael Stefanich
VISA	Johan ("Hans") Van
Tilburg	
VISA	Kim Wagner
VISA	Sue Zloth
Wayne Fueling Systems.....	Steven Bowles
Wayne Fueling Systems.....	Tim Weston
Wells Fargo Bank	Sotos Barkas
Wells Fargo Bank	William Felts, IV
Wells Fargo Bank	Andrew Garner
Wells Fargo Bank	Phillip Griffin
Wells Fargo Bank	Sam Grosby
Wells Fargo Bank	Jeff Jacoby
Wells Fargo Bank	Brian Keltner
Wells Fargo Bank	Jan Kohl
Wells Fargo Bank	Eric Lengvenis
Wells Fargo Bank	Garrett Macey
Wells Fargo Bank	Brian Parks
Wells Fargo Bank	Doug Pelton
Wells Fargo Bank	Marv Peterson
Wells Fargo Bank	Keith Ross
Wells Fargo Bank	Mike Rudolph
Wells Fargo Bank	Jeff Stapleton
Wells Fargo Bank	Tony Stieber
Wincor Nixdorf Inc.....	Christoph Bruecher
Wincor Nixdorf Inc.....	Andrea Carozzi
Wincor Nixdorf Inc.....	Michael Nolte

ANSI X9.82-4-2011 (R2017)

Wincor Nixdorf Inc.....Matthias Runowski
XYPRO Technology.....Steve Tcherchian

This is a preview of "ANSI X9.82: Part 4-2...". [Click here to purchase the full version from the ANSI store.](#)

Random Number Generation

Part 4: Random Bit Generator Constructions

1 Scope

Cryptography and security applications make extensive use of random numbers and random bits. However, the generation of random bits is problematic in many practical applications of cryptography. The purpose of American National Standard (ANS) X9.82 is to specify a standard for the design of random bit generators (RBGs) and to provide methods for converting the random bits to random numbers when required. By matching the security requirements of the application using the random bits with the security claims of the RBG generating those bits, an application can safely use the random bits produced by an RBG conforming to this Standard.

The preceding parts of this Standard have addressed the development of components and base concepts for the construction of RBGs:

- Part 1, *Overview and Basic Principles*, provides definitions of fundamental concepts, such as entropy, randomness, and security strengths, and frames the problem of random bit generation for cryptographic and security applications. Part 1 should be read for a basic understanding of this Standard before reading Part 4.
- Part 2, *Entropy Sources*, provides guidance for developing Approved entropy sources – mechanisms that provide truly unpredictable bits from some nondeterministic process.
- Part 3, *Deterministic Random Bit Generator Mechanisms*, specifies several Deterministic Random Bit Generator (DRBG) mechanisms containing cryptographic algorithms that, when used correctly, are expected to produce bits that are indistinguishable from an ideal random sequence, up to the specified security strength of the instantiation.

Part 4 specifies how Approved RBGs **shall** be constructed, using components from Parts 2 and 3 of the Standard. Part 4 specifies constructions for an RBG, and constructions for building components that are used within those RBG constructions. The information in Part 4 is intended to be combined with the information in the Parts 2 and 3 in order to:

- Construct an RBG with the required security properties that will be compliant with the Standard, and
- Verify that an RBG has been constructed in compliance with the Standard.

The precise structure, design and development of an RBG is outside the scope of this Standard.

2 Conformance

An implementation of an RBG may claim conformance with ANS X9.82 if the following are implemented: a source of entropy bits (e.g., an appropriate entropy source from Part 2), the mandatory requirements of one or more of the Deterministic Random Bit Generator (DRBG) mechanisms specified in Part 3, and the appropriate mandatory requirements of Part 4.

Conformance can be assured by a testing laboratory associated with the Cryptographic Module Validation Program (CMVP) (see <http://csrc.nist.gov/cryptval>). Although an implementation may claim conformance with the Standard apart from such testing, implementation testing through the CMVP is strongly recommended.