American National Standard for Financial Services

ANSI X9.82: Part 2–2015

Random Number Generation

Part 2: Entropy Sources

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: September 25, 2015

American National Standards Institute

Table of Contents

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 of 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

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.

The X9 committee had the following members:
Roy DeCicco, X9 Chairman
Claudia Swendseid, X9 Vice-Chairman
Steve Stevens, Executive Director
Janet Busch, Program Manager

Organization Represented	***Representative***
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
Conexxus, Inc.	Michael Davis
Conexxus, Inc.	Gray Taylor
Delap LLP	Darlene Kargel
Deluxe Corporation	Angela Hendershott
Diebold Nixdorf	Bruce Chapa
Discover Financial Services	Michelle Zhang
eCurrency	David Wen
Federal Reserve Bank	Mary Hughes
Federal Reserve Bank	Janet LaFrence
First Data Corporation	Andrea Beatty
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
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:
Ed Scheidt, Chairman

Organization Represented	***Representative***
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

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	Vijay Bolina
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
Conexxus, 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 Nixdorf	Christoph Bruecher
Diebold Nixdorf	Andrea Carozzi
Diebold Nixdorf	Bruce Chapa
Diebold Nixdorf	Michael Nolte
Diebold Nixdorf	Michael Ott
Diebold Nixdorf	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	Guy Berg
Federal Reserve Bank	Marianne Crowe
Federal Reserve Bank	Amanda Dorphy
Federal Reserve Bank	Mary Hughes
Federal Reserve Bank	Heather Hultquist
Federal Reserve Bank	Janet LaFrence
Federal Reserve Bank	Susan Pandy
Federal Reserve Bank	Patti Ritter
Federal Reserve Bank	Daniel Rozycki

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
J.P. Morgan Chase	Darryl Scott
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
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	Jeffrey Singleton
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
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
Mary Baish, Michael Boyle, John Kelsey, Project Editor

Organization Represented	*Representative*
American Bankers Association	Tom Judd
American Express Company	Jonathan Gwynn
Bank of America	Amanda Adams
Bank of America	Peter Capraro
Bank of America	Andi Coleman
Bank of America	Lawrence LaBella
Bank of America	Daniel Welch
BlackBerry Limited	Daniel Brown
BlackBerry Limited	John O. Goyo
BlackBerry Limited	Sandra Lambert
Capital One	Johnny Lee
Cipherithm	Scott Spiker
comForte 21 GmbH	Henning Horst
Communications Security Establishment	Jonathan Hammell
Communications Security Establishment	David Smith
Delap LLP	Darlene Kargel
Diebold Nixdorf	Christoph Bruecher
Diebold Nixdorf	Rick Brunt
Diebold Nixdorf	Andrea Carozzi
Diebold Nixdorf	Bruce Chapa
Diebold Nixdorf	Scott Harroff
Diebold Nixdorf	Anne Konecny
Diebold Nixdorf	Michael Nolte
Diebold Nixdorf	Dave Phister
Diebold Nixdorf	Robert Simon
Discover Financial Services	Cheryl Mish
Discover Financial Services	Diana Pauliks
Discover Financial Services	Lakshmi Ramanathan
Discover Financial Services	Michelle Zhang
Federal Reserve Bank	Patrick Adler
Federal Reserve Bank	Guy Berg
Federal Reserve Bank	Pieralberto Deganello
Federal Reserve Bank	Amanda Dorphy
Federal Reserve Bank	Mary Hughes
Federal Reserve Bank	Heather Hultquist
Federal Reserve Bank	Janet LaFrence

Federal Reserve Bank	Paul Nunnally
Federal Reserve Bank	John Rhodes
Federal Reserve Bank	Patti Ritter
Federal Reserve Bank	Daniel Rozycki
Federal Reserve Bank	Charles Tsai
Fiserv	Bud Beattie
Fiserv	Dan Otten
GEOBRIDGE Corporation	Jason Way
Gilbarco	Bruce Welch
Harland Clarke	John McCleary
Hewlett Packard	Geoffrey Hird
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
KPMG LLP	Mark Lundin
MasterCard Europe Sprl	Michael Ward
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)	Lily Chen
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)	John Kelsey
National Security Agency	Mary Baish
National Security Agency	Mike Boyle
National Security Agency	Nick Gajcowski
National Security Agency	Paul Timmel
National Security Agency	Debby Wallner
NCR Corporation	Rick Fender
NCR Corporation	Charlie Harrow
NCR Corporation	Brian Wotherspoon
PCI Security Standards Council	Troy Leach
PCI Security Standards Council	Ralph Poore
Richard Sweeney	Richard Sweeney
RSA, The Security Division of EMC	Steve Schmalz
RSA, The Security Division of EMC	Ross Urban
SafeNet, Inc.	Amit Sinha
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 .....James Torjussen
Trustwave.....Tim Hollebeek
U.S. Bank .....Peter Skirvin
Vantiv LLC .....Gary Zempich
VeriFone, Inc. .....Dave Faoro
VeriFone, Inc. .....LeAnn Hostetler
VeriFone, Inc. .....Chris Madden
VeriFone, Inc. .....Doug Manchester
VeriFone, Inc. .....Joachim Vance
VISA .....Hap Huynh
VISA .....Shahzad Khan
VISA .....Johan ("Hans") Van Tilburg
VISA .....Kim Wagner
Wells Fargo Bank .....Sotos Barkas
Wells Fargo Bank .....William Felts, IV
Wells Fargo Bank .....Phillip Griffin
Wells Fargo Bank .....Jeff Jacoby
Wells Fargo Bank .....Brian Keltner
Wells Fargo Bank .....Jan Kohl
Wells Fargo Bank .....Eric Lengvenis
Wells Fargo Bank .....Doug Pelton
Wells Fargo Bank .....Jeff Stapleton
Wells Fargo Bank .....Tony Stieber

Random Number Generation
Part 2: Entropy Sources

1 Scope

ANS X9.82 is concerned with the generation of random bits, primarily for use in cryptographic applications. While there has been extensive research on the subject of generating (pseudo)random bits using a Random Bit Generator (RBG) and an unknown seed value, creating such an unknown value has not been as well documented. As Part 1 of this Standard establishes, the only way for this seed value to provide real security is for it to be obtained from a source that provides sufficient entropy. Directly or indirectly, the seeding of an RBG will rely upon a non-deterministic process – i.e., an entropy source. This part of ANS X9.82 describes the properties that an entropy source must have to make it suitable for use by cryptographic random bit generators. This part of ANS X9.82 includes:

1. An entropy source model,
2. Implementation issues,
3. Criteria and requirements for entropy source components, and
4. Tests for ensuring that the implementation continues to perform as expected (health tests).

The precise structure, design and development of an entropy source implementation are outside the scope of this Standard.

The development of entropy sources that provide suitable output is difficult, and providing guidance for their design and health testing is even more so. This part of the Standard is an initial attempt to provide design guidance for the development of entropy sources. The approach to health testing defined in this Standard assumes that the developer understands the behavior of the entropy source and has made a good-faith effort to provide a consistent source of entropy. It is expected that, over time, improvements to the guidance and health testing will be made, based on experience in using this Standard.

2 Conformance

An implementation of an entropy source may claim conformance with ANS X9.82 if it implements the requirements of this part of the Standard.

3 Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. Nevertheless, parties to agreements based on this document are encouraged to consider applying the most recent edition of the referenced