American National Standard for Financial Services

ANSI X9.124-2-2018

Symmetric Key Cryptography For the Financial Services Industry — Format Preserving Encryption- Part 2: Key Stream with Counter Mode

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: February 14, 2018

American National Standards Institute

This page left intentionally blank

Contents

Page

Foreword

Approval of an American National Standard requires verification by ANSI 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 ANSI 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 interpretation 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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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.
At the time this standard was approved, the X9 committee had the following members:

Roy DeCicco, X9 Chair
Angela Hendershott, X9 Vice-Chair
Steve Stevens, Executive Director
Janet Busch, Program Manager

Organization Represented	*Representative*
ACI Worldwide	Doug Grote
American Bankers Association	Diane Poole
American Express Company	David Moore
Bank of America	Daniel Welch
Bank of New York Mellon	Arthur Sutton
Blackhawk Network	Anthony Redondo
Bloomberg LP	Corby Dear
Capital One	Marie LaQuerre
Citigroup, Inc.	Karla McKenna
CLS Bank	Ram Komarraju
Conexxus, Inc.	Gray Taylor
CUSIP Service Bureau	Gerard Faulkner
Delap LLP	Andrea Beatty
Delap LLP	Darlene Kargel
Deluxe Corporation	Angela Hendershott
Diebold Nixdorf	Bruce Chapa
Discover Financial Services	Michelle Zhang
Dover Fueling Solutions	Bradford Loewy
eCurrency	David Wen
Federal Reserve Bank	Mary Hughes
First Data Corporation	Lisa Curry
FIS	Stephen Gibson-Saxty

Fiserv	Dan Otten
FIX Protocol Ltd - FPL	Jim Northey
Futurex	Ryan Smith
Gilbarco	Bruce Welch
Harland Clarke	John McCleary
IBM Corporation	Todd Arnold
Ingenico	Rob Martin
ISARA Corporation	Alexander Truskovsky
ISITC	Lisa Iagatta
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Roy DeCicco
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	Thomas Brown Jr.
PCI Security Standards Council	Troy Leach
RouteOne	Chris Irving
RouteOne	Jenna Wolfe
SWIFT/Pan Americas	Karin DeRidder
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	John Hall
VeriFone, Inc.	Dave Faoro
Viewpointe	Richard Luchak
VISA	Kim Wagner
Wells Fargo Bank	Mark Schaffer

At the time this standard was approved, the X9F subcommittee on Data and Information Security had the following members:

Dave Faoro, Chairman
Steven Bowles, Vice Chairman

Organization Represented	*Representative*
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	Farid Hatefi
American Express Company	David Moore
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
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	Andrea Beatty
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
Digicert	Tim Hollebeek
Discover Financial Services	Cheryl Mish
Discover Financial Services	Diana Pauliks
Discover Financial Services	Jordan Schaefer
Dover Fueling Solutions	Steven Bowles
Dover Fueling Solutions	Bradford Loewy
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
First Data Corporation	Lisa Curry
First Data Corporation	Kalli Davidson
First National Bank of Omaha	Sherry Rewolinski
First National Bank of Omaha	Kristi White
FIS	Saman Amighi
FIS	John Soares
FIS	Sunny Wear
Fiserv	Bud Beattie
Fiserv	Dan Otten
Futurex	Ryan Smith
Futurex	Tim Weston
GEOBRIDGE Corporation	Donna Gem
GEOBRIDGE Corporation	Jason Way
Gilbarco	Scott Turner
Gilbarco	Bruce Welch
Harland Clarke	Joseph Filer
Heartland Payment Systems	Scott Meeker
IBM Corporation	Todd Arnold
IBM Corporation	Richard Kisley
Ingenico	Nabil Hamzi
Ingenico	Rob Martin
ISARA Corporation	Mike Brown
ISARA Corporation	Philip Lafrance
ISARA Corporation	Alexander Truskovsky
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Kathleen Krupa

J.P. Morgan Chase	Jackie Pagán
J.P. Morgan Chase	Darryl Scott
K3DES LLC	Azie Amini
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
Micro Focus	Luther Martin
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
Onboard Security	Mark Etzel
Onboard Security	Virendra Kumar
Onboard Security	William Whyte
Onboard Security	Lee Wilson
Onboard Security	Zhenfei Zhang
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 Infotech Pvt. Ltd.	Amit Sinha
SafeNet Infotech Pvt. Ltd.	Devesh Tewari
Safeway	Gary Zempich
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	Mark Fitlin
The Clearing House	Sharon Jablon
The Clearing House	Hirak Patel
The Clearing House	Miguel Sanchez
Trustwave	John Amaral
U.S. Bank	Stephen Case
U.S. Bank	Peter Skirvin
Vantiv LLC	John Hall
Vantiv LLC	Jeffrey Singleton

Vantiv LLC ..... Bill Weingart
VeriFone, Inc..... John Barrowman
VeriFone, Inc..... David Ezell
VeriFone, Inc..... Dave Faoro
VeriFone, Inc..... Doug Manchester
VeriFone, Inc..... Brad McGuinness
VeriFone, Inc..... Saxon Noh
VeriFone, Inc..... Joachim Vance
VISA..... Shahzad Khan
VISA..... Eric Le Saint
VISA..... Kim Wagner
Wells Fargo Bank..... Allen Ausec
Wells Fargo Bank..... David Cooper
Wells Fargo Bank..... William Felts, IV
Wells Fargo Bank..... Matthew Greenwell
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..... Maria Schuett
Wells Fargo Bank..... Jeff Stapleton
White and Williams LLP ..... Emma Bechara
White and Williams LLP ..... Richard Borden
White and Williams LLP ..... Joshua Mooney
White and Williams LLP ..... Laura Schmidt
White and Williams LLP ..... Kate Woods
XYPRO Technology ..... Steve Tcherchian

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.)

At the time this standard was approved, the X9F1 Cryptographic Tools group which developed this standard had the following active members:

Eric LeSaint, Chairman and Kim Wagner, Project Editor

Organization Represented *Representative*

American Bankers Association ..... Tom Judd
American Express Company..... Gail Chapman

American Express Company ..... Jonathan Gwynn
American Express Company ..... David Moore
Atlantic BT ..... Ulf Mattsson
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
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
Digicert ..... Tim Hollebeek
Discover Financial Services ..... Cheryl Mish
Discover Financial Services ..... Diana Pauliks
Discover Financial Services ..... Lakshmi Ramanathan
Discover Financial Services ..... Michelle Zhang
Dover Fueling Solutions ..... Steven Bowles
Dover Fueling Solutions ..... Bradford Loewy
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 ..... Charles Tsai
Fiserv ..... Bud Beattie
Fiserv ..... Dan Otten
GEOBRIDGE Corporation ..... Jason Way

Gilbarco	Bruce Welch
Harland Clarke	John McCleary
IBM Corporation	Todd Arnold
IBM Corporation	Richard Kisley
Ingenico	Eric Brier
Ingenico	Nabil Hamzi
Ingenico	Rob Martin
ISARA Corporation	Mike Brown
ISARA Corporation	Philip Lafrance
ISARA Corporation	Alexander Truskovsky
MasterCard Europe Sprl	Michael Ward
Micro Focus	Susan Langford
Micro Focus	Luther Martin
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
Onboard Security	William Whyte
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 Infotech Pvt. Ltd.	Amit Sinha
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Dr. Wai Tsang
TECSEC Incorporated	Jay Wack
Thales UK Limited	Colette Broadway
Thales UK Limited	James Torjussen
U.S. Bank	Peter Skirvin
Vantiv LLC	John Hall
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 .....Eric Le Saint
VISA .....Johan ("Hans") Van Tilburg
VISA .....Kim Wagner
Wells Fargo Bank .....Sotos Barkas
Wells Fargo Bank .....William Felts, IV
Wells Fargo Bank .....Matthew Greenwell
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

Symmetric Key Cryptography for the Financial Services Industry — Format Preserving Encryption — Part 2: Counter Mode

1 Scope

This document defines requirements for Format Preserving Encryption - Counter Mode (FPCM). FPCM methods encrypt data strings of a specific length and character set into ciphertext of the same length using the same character set and using the equivalent of Counter Mode (CTR) defined in NIST SP38B. Format Preserving Encryption is useful in situations where fixed-format data, such as Primary Account Numbers (PANs) or Social Security Numbers, must be encrypted, but there is a requirement to limit changes to existing communication protocols, database schemata or application code. FPCM is a particularly simple and efficient mechanism to achieve format preserving encryption, which shares many of the strengths and challenges of CTR.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

X9 SD-34, *Registry of Approved Cryptographic Resources for Financial Services Industry Standards*, Registry Item 00002, *Advanced Encryption Standard*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

AES
The Advanced Encryption Standard, a block cipher with a 128-bit wide block and either a 128-bit or 256-bit key.

alphabet
A finite nonempty set.

block
A block is a fixed-length sequence of binary bits.