American National Standard for Financial Services

ANSI X9.102-2020

Symmetric Key Cryptography For the Financial Services Industry— Wrapping of Keys and Associated Data

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: May 26, 2020

American National Standards Institute

Contents

Page

Figures

Tables

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

The protection of the integrity/authenticity of confidential data is often important and sometimes crucial to the security of an information system. However, the interaction of an encryption algorithm with a separate authentication algorithm can lead to unexpected vulnerabilities; see Bibliography item [3], for example. Therefore, recent years have seen the development of dedicated, single mechanisms for authenticated encryption. This standard specifies several such mechanisms, called key wrap mechanisms, that are intended for the protection of cryptographic keys and other sensitive data, whether in storage or in transport.

For general use, this standard specifies a particularly robust mechanism that is based on the AES algorithm; an analogue based on the Triple Data Encryption Algorithm (TDEA) is also specified. The conservative security of these mechanisms comes with a corresponding cost in performance. The rationale for this design choice is that the protection of keys is paramount, and in many systems the extra overhead for their management can be tolerated.

In addition, this standard specifies two other key wrap mechanisms. These two mechanisms are similar, except that one uses TDEA and the other uses AES. They are tailored to the needs of particular systems in the financial services industry.

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.

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.

The X9 committee had the following members:

Roy Decicco, X9 Chairman
Corby Dear, X9 Vice-Chairman
Steve Stevens, Executive Director
Janet Busch, Program Manager
Ambria Frazier, Program Manager

Organization Represented	*Representative*
ACI Worldwide	Doug Grote
Amazon	Igor Kleyman
American Bankers Association	Diane Poole
Bank of America	Daniel Welch
BDO	Tim Crawford
Bloomberg LP	Corby Dear

Citigroup, Inc.	Ellen Xu
Communications Security Establishment	David Smith
Conexxus, Inc.	Gray Taylor
CUSIP Global Services	Gerard Faulkner
Delap LLP	Andrea Beatty
Deluxe Corporation	Andy Vo
Diebold Nixdorf	Bruce Chapa
Digicert	Dean Coclin
Discover Financial Services	Diana Pauliks
Dover Fueling Solutions	Henry Fieglein
Federal Reserve Bank	Ainsley Hargest
First Data Corporation	Lisa Curry
FIS	Stephen Gibson-Saxty
Fiserv	Dan Otten
FIX Protocol Ltd - FPL	James Northey
Futurex	Ryan Smith
Gilbarco	Bruce Welch
Harland Clarke	Jonathan Lee
Hyosung TNS Inc.	Joe Militello
IBM Corporation	Todd Arnold
Ingenico	Steven Bowles
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	George Throckmorton
National Security Agency	Mike Boyle
NCR Corporation	Kevin Spengler
Office of Financial Research, U.S. Treasury Department	Thomas Brown Jr.
PCI Security Standards Council	Troy Leach
PricewaterhouseCoopers LLP	Michael Versace
PriVerify Corp	Adam Glynn
RouteOne	Chris Irving
SWIFT/Pan Americas	Karin DeRidder
Symcor Inc.	Debbi Fitzpatrick
TECSEC Incorporated	Ed Scheidt
The Clearing House	Sharon Jablon
U.S. Bank	Michelle Wright
U.S. Commodity Futures Trading Commission (CFTC)	Robert Stowsky
University Bank	Stephen Ranzini
USDA Food and Nutrition Service	Lisa Gifaldi
VeriFone, Inc.	Dave Faoro
Viewpointe	Richard Luchak
VISA	Adam Clark
Wells Fargo Bank	Mark Schaffer

The X9F subcommittee on Data and Information Security had the following members:

Dave Faoro, X9F Chairman
Steven Bowles, X9F Vice Chairman
Ed Scheidt, X9F Vice Chairman

Organization Represented	*Representative*
ACI Worldwide	Doug Grote
ACI Worldwide	Dan Kinney
ACI Worldwide	Julie Samson
Amazon	Sean Estrada
American Bankers Association	Tom Judd
American Express Company	Gail Chapman
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	Joel Kazin
Bank of America	Terry McKinney
Bank of America	Matt Sharp
Bank of America	Michael Smith
Bank of America	Daniel Welch
BBVA Compass	Omar Jarrar
BDO	Tim Crawford
BDO	Jeffrey Ward
BlackBerry Limited	Daniel Brown
Bloomberg LP	Erik Anderson
Bloomberg LP	Corby Dear
Capital One	Johnny Lee
comforte AG	Thomas Gloerfeld
comforte AG	Henning Horst
Communications Security Establishment	Jonathan Hammell
Communications Security Establishment	David Smith
Conexxus, Inc.	David Ezell
Conexxus, Inc.	Alan Thiemann
CUSIP Global Services	Scott Preiss
Delap LLP	Andrea Beatty
Delap LLP	Diane Bishop
Delap LLP	David Buchanan
Deluxe Corporation	Margiore Romay
Deluxe Corporation	Andy Vo
Diebold Nixdorf	Christoph Bruecher
Diebold Nixdorf	Bruce Chapa
Diebold Nixdorf	David Phister
Digicert	Tim Hollebeek
Discover Financial Services	Cheryl Mish
Discover Financial Services	Diana Pauliks
Discover Financial Services	Jordan Schaefer
Discover Financial Services	Jorge Vargas
Dover Fueling Solutions	Henry Fieglein
Federal Reserve Bank	Guy Berg

Federal Reserve Bank	Marianne Crowe
Federal Reserve Bank	Amanda Dorphy
Federal Reserve Bank	Ken Han
Federal Reserve Bank	Ainsley Hargest
Federal Reserve Bank	Daniel Maynard
Federal Reserve Bank	Susan Pandy
Federal Reserve Bank	Patti Ritter
First Data Corporation	Lisa Curry
First Data Corporation	Vinayak Kagalkar
First National Bank of Omaha	Robert Lamagna-Reiter
First National Bank of Omaha	Sherry Rewolinski
First National Bank of Omaha	Kristi White
Fiserv	Bud Beattie
Fiserv	Dan Otten
Futurex	Comron Moeni
Futurex	Ryan Smith
Futurex	Tim Weston
GEOBRIDGE Corporation	Jason Way
Gilbarco	Scott Turner
Gilbarco	Bruce Welch
Harland Clarke	Joseph Filer
Hyosung TNS Inc.	Joe Militello
Hyosung TNS Inc.	JaeWhan Shin
IBM Corporation	Todd Arnold
IBM Corporation	Richard Kisley
Ingenico	Steven Bowles
Ingenico	Wayne Burgess
Ingenico	Nabil Hamzi
Ingenico	Steve McKibben
Intralinks	Dominic Brown
Intralinks	William Klingenberg
Intralinks	Dario Lirio
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	Mukul Gupta
Level 10	Allan Elder
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Mimi Hart
MasterCard Europe Sprl	Mark Kamers
MasterCard Europe Sprl	Larry Newell
MasterCard Europe Sprl	Michael Ward
Micro Focus	Luther Martin
Micro Focus	Phil Smith III
Microsoft	Mike Reilly
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	Nick Gajcowski
National Security Agency	Paul Timmel
NCR Corporation	Charlie Harrow

NCR Corporation ..... Bradford Loewy
P97 Networks, Inc. ..... Steve Moses
PCI Security Standards Council ..... Leon Fell
PCI Security Standards Council ..... Troy Leach
PCI Security Standards Council ..... Ralph Poore
PriVerify Corp ..... Adam Glynn
SafeNet Infotech Pvt. Ltd..... Amit Sinha
SafeNet Infotech Pvt. Ltd..... Devesh Tewari
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
The Phoenix Group ..... Ron Davis
The Phoenix Group ..... Candice Hoft
U.S. Bank ..... Stephen Case
University Bank..... Stephen Ranzini
University Bank..... Michael Talley
Utimaco Inc. ..... Susan Langford
VeriFone, Inc. ..... John Barrowman
VeriFone, Inc. ..... Christophe Devaux
VeriFone, Inc. ..... Dave Faoro
VeriFone, Inc. ..... Indra Fitzgerald
VeriFone, Inc. ..... Joachim Vance
Viewpointe..... Richard Luchak
VISA ..... Adam Clark
VISA ..... Eric Le Saint
VISA ..... Kim Wagner
Wells Fargo Bank ..... Jason Buck
Wells Fargo Bank ..... David Cooper
Wells Fargo Bank ..... William Felts, IV
Wells Fargo Bank ..... Phillip Griffin
Wells Fargo Bank ..... Calvin Heng
Wells Fargo Bank ..... Rameshchandra Ketharaju
Wells Fargo Bank ..... Antoinette McCarthy
Wells Fargo Bank ..... Kelly O'Donnell
Wells Fargo Bank ..... Mark Schaffer
Wells Fargo Bank ..... Jeff Stapleton
Wells Fargo Bank ..... Tony Suarez
Wells Fargo Bank ..... Srinivas Voora
White and Williams LLP..... Richard Borden
White and Williams LLP..... Sandra Lambert
White and Williams LLP..... Joshua Mooney
White and Williams LLP..... Michael Olsan

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 Tools group which developed this standard had the following members:

Eric LeSaint, Chairman
Ralph Poore, Vice Chairman
Todd Arnold, Project Editor

Organization Represented	*Representative*
Amazon	Matthew Campagna
American Bankers Association	Tom Judd
American Express Company	Gail Chapman
Bank of America	Amanda Adams
Bank of America	Peter Capraro
Bank of America	Andi Coleman
Bank of America	Joel Kazin
Bank of America	Terry McKinney
Bank of America	Matt Sharp
Bank of America	Daniel Welch
BlackBerry Limited	Daniel Brown
Capital One	Johnny Lee
comforte AG	Henning Horst
Communications Security Establishment	Jonathan Hammell
Communications Security Establishment	David Smith
Diebold Nixdorf	Christoph Bruecher
Diebold Nixdorf	Rick Brunt
Diebold Nixdorf	Bruce Chapa
Diebold Nixdorf	Scott Harroff
Diebold Nixdorf	Anne Konecny
Diebold Nixdorf	Michael Nolte
Diebold Nixdorf	David Phister
Digicert	Tim Hollebeek
Discover Financial Services	Cheryl Mish
Discover Financial Services	Diana Pauliks
Discover Financial Services	Lakshmi Ramanathan
Discover Financial Services	Jorge Vargas
Dover Fueling Solutions	Henry Fieglein
Federal Reserve Bank	Guy Berg
Federal Reserve Bank	Pieralberto Deganello
Federal Reserve Bank	Amanda Dorphy
Federal Reserve Bank	Ken Han
Federal Reserve Bank	Ainsley Hargest
Federal Reserve Bank	Paul Nunnally
Federal Reserve Bank	John Rhodes
Federal Reserve Bank	Patti Ritter
Fiserv	Bud Beattie
Fiserv	Dan Otten
GEOBRIDGE Corporation	Jason Way
Gilbarco	Bruce Welch
IBM Corporation	Todd Arnold
IBM Corporation	Richard Kisley
Ingenico	Steven Bowles

Ingenico	Eric Brier
Ingenico	Nabil Hamzi
Ingenico	Regis Marcel
Ingenico	Vanessa Terrade
ISARA Corporation	Mike Brown
ISARA Corporation	Philip Lafrance
ISARA Corporation	Alexander Truskovsky
ITS, Inc. (SHAZAM Networks)	Janet LaFrence
J.P. Morgan Chase	Jackie Pagán
MasterCard Europe Sprl	Michael Ward
Member Emeritus	Darlene Kargel
Member Emeritus	Lawrence LaBella
Member Emeritus	Richard Sweeney
Micro Focus	Luther Martin
Micro Focus	Phil Smith III
National Institute of Standards and Technology (NIST)	Elaine Barker
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)	John Kelsey
National Security Agency	Mary Baish
National Security Agency	Mike Boyle
National Security Agency	Darryl Buller
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	Bradford Loewy
NCR Corporation	Brian Wotherspoon
PCI Security Standards Council	Troy Leach
PCI Security Standards Council	Doug Manchester
PCI Security Standards Council	John Markh
PCI Security Standards Council	Ralph Poore
PriVerify Corp	Adam Glynn
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
TokenEx	Ulf Mattsson
University Bank	Stephen Ranzini
University Bank	Michael Talley
University of Maryland	Jonathan Katz
Utimaco Inc.	Susan Langford
VeriFone, Inc.	Christophe Devaux
VeriFone, Inc.	Dave Faoro
VeriFone, Inc.	Indra Fitzgerald
VeriFone, Inc.	Joachim Vance
VISA	Naga Vinod Duggirala
VISA	Eric Le Saint
VISA	Kim Wagner
Wells Fargo Bank	Rao Abhijit
Wells Fargo Bank	Allen Ausec
Wells Fargo Bank	Sotos Barkas

Wells Fargo Bank ..... William Felts, IV
Wells Fargo Bank ..... Matthew Greenwell
Wells Fargo Bank ..... Phillip Griffin
Wells Fargo Bank ..... Calvin Heng
Wells Fargo Bank ..... Jeff Jacoby
Wells Fargo Bank ..... Amanda Judge
Wells Fargo Bank ..... Arun Kamath
Wells Fargo Bank ..... Brian Keltner
Wells Fargo Bank ..... Rameshchandra Ketharaju
Wells Fargo Bank ..... Jan Kohl
Wells Fargo Bank ..... Eric Lengvenis
Wells Fargo Bank ..... Antoinette McCarthy
Wells Fargo Bank ..... Olatunde Ojolola
Wells Fargo Bank ..... Doug Pelton
Wells Fargo Bank ..... Tim Plantand
Wells Fargo Bank ..... Mark Schaffer
Wells Fargo Bank ..... Jeff Stapleton
Wells Fargo Bank ..... Tony Stieber
Wells Fargo Bank ..... Tony Suarez
Wells Fargo Bank ..... Srinivas Voora
White and Williams LLP..... Clay Epstein
White and Williams LLP..... Sandra Lambert

Symmetric Key Cryptography for the Financial Services Industry —Wrapping of Keys and Associated Data

1 Scope

This standard specifies four key wrap mechanisms based on ASC X9-approved symmetric key block ciphers whose block size is either 64 bits or 128 bits. The key wrap mechanisms can provide assurance of the confidentiality and the integrity of data, especially cryptographic keys or other sensitive data.

2 Conformance

An implementation of the following mechanisms for authenticated encryption may claim conformance with this standard:

— AESKW (Section 7.1)

— TDKW (Section 7.2)

— AKW2 (Section 7.3)

— AKW3 (Section 7.4)

An implementation of AKW2 may only claim conformance with this standard in conjunction with TR-31 [Ref 1].

3 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.

1. ASC X9 TR 31-2018, Interoperable Secure Key Exchange Key Block Specification
   .

2. ANSI X9.24-1-2017, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques.

3. ANS X9.24-3, Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction