American National Standard for Financial Services

ANSI X9.102-2008 (R2017)

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

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: June 27, 2008

Date Reaffirmed: February 10, 2017

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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 Ref. [5], for example. Therefore, recent years have seen the development of dedicated, single mechanisms for authenticated encryption. This Standard specifies several such mechanisms, called key wraps, that are intended for the protection of cryptographic keys and other specialized 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 that are based on TDEA. One of them is specified to support the S/MIME protocol of the IETF. The other is tailored to the needs of particular legacy 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.

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	James Shaffer
American Bankers Association	C. Diane Poole
American Express Company	Mark Merkow
American Financial Services Association	Mark Zalewski
Bank of America	Daniel Welch
Certicom Corporation	Daniel Brown

Citigroup, Inc.	Gary Word
CUSIP Service Bureau	James Taylor
Deluxe Corporation	John Fitzpatrick
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Deana Morrow
Federal Reserve Bank	Dexter Holt
First Data Corporation	Rick Van Luvender
Fiserv	Skip Smith
FSTC, Financial Services Technology Consortium	Daniel Schutzer
Harland Clarke	John McCleary
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
IBM Corporation	Todd Arnold
Ingenico	John Spence
Intuit, Inc.	Jana Hocker
JP Morgan Chase & Co	Jacqueline Pagan
KPMG LLP	Mark Lundin
Mag-Tek, Inc.	Carlos Morales
Metavante Image Solutions	Ron Schultz
NACHA The Electronic Payments Association	Nancy Grant
National Association of Convenience Stores	Michael Davis
National Security Agency	Paul Timmel
NCR Corporation	Steve Stevens
SWIFT/Pan Americas	James Wills
The Clearing House	Vincent DeSantis
U.S. Bank	Brian Fickling
University Bank	Stephen Ranzini
VeriFone, Inc.	Brad McGuinness
VISA	Richard Sweeney
Wachovia Bank	Raymond 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 Represented	*Representative*
[3PEA Technologies, Inc.	Mark Newcomer
ACI Worldwide	Jim Shaffer
American Express Company	Mark Merkow
American Financial Services Association	Mark Zalewski
Bank of America	Daniel Welch
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Gary Word
ClearWave Electronics	Mark Ross
Communications Security Establishment	Alan Poplove
CUSIP Service Bureau	Scott Preiss
DeLap, White, Caldwell and Croy, LLP	Darlene Kargel
Deluxe Corporation	John Fitzpatrick
Depository Trust and Clearing Corporation	Robert Palatnik
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Julie Shaw
Entrust, Inc.	Miles Smid
Federal Reserve Bank	Dexter Holt
Ferris and Associates, Inc.	J. Martin Ferris
First Data Corporation	Rick Van Luvender
Fiserv	Bud Beattie
FSTC, Financial Services Technology Consortium	Daniel Schutzer
Futurex	Jason Anderson
Geobridge	Jeff Stapleton
Harland Clarke	John McCleary
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
IBM Corporation	Todd Arnold
InfoGuard Laboratories	Tom Caddy
Ingenico	John Spence
Innové, LLC	Steven Teppler
Intel Massachusetts, Inc.	Paul Posco
JP Morgan Chase & Co	Edward Koslow
KPMG LLP	Mark Lundin
Mag-Tek, Inc.	Carlos Morales
MasterCard International	Michael Ward
Metavante Image Solutions	Ron Schultz
National Institute of Standards and Technology	Elaine Barker
National Security Agency	Paul Timmel
NCR Corporation	David Norris
NTRU Cryptosystems	William Whyte
Pitney Bowes Inc.	Leon Pintsov
Rosetta Technologies	Jim Maher
RSA, The Security Division of EMC	James Randall
Surety, Inc.	Dimitrios Andivahis
Thales e-Security, Inc.	James Torjussen
The Clearing House	Vincent DeSantis

Triton Systems of Delaware, Inc.	Daryll Cordeiro
U.S. Bank	Robert Thomas
Unisys Corporation	David J. Concannon
University Bank	Stephen Ranzini
VeriFone	Dave Faoro
VISA	John Sheets
Voltage Security, Inc.	Luther Martin
Wachovia Bank	Raymond 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 which developed this standard had the following members:
Miles Smid, Chairman and Morris Dworkin, 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
Bank of New York Mellon	Indur Mandhyan
BlackBerry Limited	Daniel Brown
BlackBerry Limited	John O. Goyo
BlackBerry Limited	Sandra Lambert
Capital One	Johnny Lee
Certicom Corporation	Dan Brown
Cipherithm	Scott Spiker
comForte 21 GmbH	Henning Horst
Communications Security Establishment	Jonathan Hammell
Communications Security Establishment	David Smith
Delap LLP	Darlene Kargel
Diebold, Inc.	Rick Brunt
Diebold, Inc.	Bruce Chapa
Diebold, Inc.	Scott Harroff
Diebold, Inc.	Anne Konecny
Diebold, Inc.	Dave Phister
Diebold, Inc.	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	Jeremy Brotherton

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	Janet LaFrence
Federal Reserve Bank	Jackie Nugent
Federal Reserve Bank	Paul Nunnally
Federal Reserve Bank	Jim O'Connell
Federal Reserve Bank	Michael Ram
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	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)	William Burr
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	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
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
Wincor Nixdorf Inc	Christoph Bruecher
Wincor Nixdorf Inc	Andrea Carozzi
Wincor Nixdorf Inc	Michael Nolte

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 specialized data.

2 Conformance

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

— AESKW (Clause 7.1)

— TDKW (Clause 7.2)

— AKW1 (Clause 7.3)

— AKW2 (Clause 7.4)

— CCM (normative reference [3.6] below).

An implementation of AKW2 may only claim conformance with this Standard in conjunction with TR-31 [3.1].

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.

[3.1] Accredited Standards Committee X9, Incorporated, TR-31—2005: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms.

[3.2] ANS X9.24 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques: 2004.

[3.3] FIPS Publication 197, Advanced Encryption Standard (AES), U.S. DoC/NIST, November 26, 2001; ASC X9 Registry 00002.