American National Standard for Financial Services

ANSI X9.24-1-2017

Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: June 8, 2017

American National Standards Institute

This page left intentionally blank

Contents

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

Today, billions of dollars in funds are transferred electronically by various communication methods. Transactions are often entered remotely, off-premise from financial institutions, by retailers or by customers directly. Such transactions are transmitted over potentially non-secure media. The vast range in value, size, and the volume of such transactions expose institutions to severe risks, which may be uninsurable.

To protect these financial messages and other sensitive information, many institutions are making increased use of the American National Standards Institute Triple Data Encryption Algorithm (TDEA) and the Advanced Encryption Standard (AES). Specific examples of its use include standards for message authentication, personal identification number encryption, other data encryption, and key encryption.

AES and the TDEA are in the public domain. The security and reliability of any process based on AES or the TDEA is directly dependent on the protection afforded to secrets called cryptographic keys. This part of this standard deals exclusively with management of symmetric keys using symmetric techniques. ANS X9.24-2 addresses management of symmetric keys using asymmetric techniques.

A familiar analogy may be found in the combination lock of a vault. The lock design is public knowledge. Security is provided by keeping a number, the combination, a secret. Secure operation also depends on protective procedures and features which prevent surreptitious viewing or determination of the combination by listening to its operation. Procedures are also required to ensure that the combination is random and cannot be modified by an unauthorized individual without detection.

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 Chairman
Angela Hendershott, X9 Vice-Chairman
Steve Stevens, Executive Director

Organization Represented	***Representative***
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
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

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

Dave Faoro, 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	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	Bruce Chapa
Diebold Nixdorf	Michael Ott
Diebold Nixdorf	Dave Phister
Diebold Nixdorf	Christoph Bruecher
Diebold Nixdorf	Andrea Carozzi
Diebold Nixdorf	Michael Nolte
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
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
Ingenico	John Spence
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
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, 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 X9F6, Cardholder Authentication and ICC's group which developed this standard had the following active members:

Scott Spiker, X9F6 Chairman
Darlene Kargel, X9F6 Vice Chairman
Andrea Beatty, Technical Editor
John Spence, Technical Editor

Organization Represented	***Representative***
American Express Company	Alan Fong
Bank of America	Andi Coleman
Delap LLP	David Buchanan

Delap LLP	Darlene Kargel
Diebold Nixdorf	Bruce Chapa
Diebold Nixdorf	Anne Konecny
Federal Reserve Bank	Amanda Dorphy
First Data Corporation	Andrea Beatty
First Data Corporation	Lisa Curry
First National Bank of Omaha	Kristi White
Fiserv	Dan Otten
Futurex	Ryan Smith
GEOBRIDGE Corporation	Donna Gem
GEOBRIDGE Corporation	Dean Macinskas
GEOBRIDGE Corporation	Jason Way
Gilbarco	Scott Turner
Gilbarco	Bruce Welch
Heartland Payment Systems	John Masden
Hewlett Packard	Susan Langford
IBM Corporation	Todd Arnold
Ingenico	Rob Martin
Ingenico	Steve McKibben
Ingenico	John Spence
J.P. Morgan Chase	Kathleen Krupa
J.P. Morgan Chase	Darryl Scott
K3DES LLC	Azie Amini
K3DES LLC	James Richardson
Mainsail Trim, Inc.	Norman Cecil
National Institute of Standards and Technology (NIST)	Elaine Barker
PCI Security Standards Council	Ralph Poore
Thales UK Limited	Colette Broadway
Thales UK Limited	Larry Hines
Thales UK Limited	James Torjussen
Trustwave	Tim Hollebeek
U.S. Bank	Stephen Case
Vantiv LLC	Gary Zempich
VeriFone, Inc.	Dave Faoro
VeriFone, Inc.	Doug Manchester
VeriFone, Inc.	Joachim Vance
VISA	Adam Clark
VISA	Shahzad Khan
VISA	Michael Stefanich
VISA	Kim Wagner
Wayne Fueling Systems	Steven Bowles
Wells Fargo Bank	Jeff Jacoby
XYPRO Technology	Steve Tcherchian

This document cancels and replaces the 2009 version of X9.24 Part 1.

As part of the ANSI 5-year review process, this standard underwent significant modifications that resulted in an extensive rewrite. It reflects updates in key management security requirements, includes AES algorithm use, and leverages advancements in hardware devices used for protecting cryptographic keys.

Implementation details for TDES and AES DUKPT have been moved to part three of X9.24.

Retail Financial Services
Symmetric Key Management
Part 1: Using Symmetric Techniques

1 Purpose

This key management standard, utilized in conjunction with the National Institute for Standards and Technology Triple Data Encryption Algorithm (TDEA) (see Reference 1) and the Advanced Encryption Standard (AES) (see Reference 5), is used to manage symmetric keys that can be used to protect messages and other sensitive information in a financial services environment. The security and reliability of any process based on AES or the TDEA is directly dependent on the protection afforded to secret parameters called cryptographic keys.

This standard establishes requirements and guidelines for the secure management and application-level interoperability of keying operations. Such keys could be used for authenticating messages (see References 11, 14, and 16), for encrypting Personal Identification Numbers (PIN) (see Reference 10), for encrypting other data, for encrypting other keys, or for other purposes.

2 Scope

2.1 General

This part of this standard covers both the manual and automated management of keying material used for financial services such as point-of-sale (POS) transactions (debit and credit), automated teller machine (ATM) transactions, messages among terminals and financial institutions, and interchange messages among acquirers, switches and card issuers. This part of this standard deals exclusively with the management of symmetric keys using symmetric techniques. Requirements for symmetric keys protected by asymmetric keys are addressed in X9.24-2. Any requirements stated in this part are not meant to invalidate the requirements provided for in Part 2. This part of the standard specifies the minimum requirements for the management of keying material. Addressed are all components of the key management life cycle, including the generation, distribution, utilization, storage, archiving, replacement and destruction of the keying material. An institution's key management process, whether implemented in a computer or a terminal, is not to be implemented or controlled in a manner that has less security, protection, or control than described herein. The intention is that if two nodes implement compatible and secure versions of key management methods, key identification techniques, and key separation methods in accordance with this part of this standard, they will be interoperable at the application level. Other characteristics may be necessary for node interoperability; however, this part of this standard does not cover such characteristics as message format, communications protocol, transmission speed, or device interface.

The definition of the DUKPT algorithm is addressed in X9.24 Part 3. Information contained in previous versions of this standard related to the implementation of DUKPT has been moved to that standard.

2.2 Application

This part of this standard is applicable for institutions implementing techniques to safeguard the cryptographic keys used for the authentication and encryption of messages and other sensitive data. For example, this applies to institutions in the financial services industry implementing References 10, 11, or 18.

Mandatory standard techniques and procedures are indicated by the word '**SHALL**'. Guidelines are indicated by the word '**SHOULD**'.