American National Standard
for Financial Services

ANS X9.24-1:2009

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

Secretariat

Accredited Standards Committee X9, Inc.

Approved: October 13, 2009

American National Standards Institute

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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
1212 West Street, Suite 200
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

Contents

Figures

Tables

Introduction

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). Specific examples of its use include standards for message authentication, personal identification number encryption, other data encryption, and key encryption.

The TDEA is in the public domain. The security and reliability of any process based on the TDEA is directly dependent on the protection afforded to secret numbers 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 of this standard will be welcome. They should be sent to the ASC X9 Secretariat, Accredited Standards Committee X9, Inc., 1212 West Street, Suite 200, Annapolis, MD 21401.

The standard was processed and approved for submittal to the American National Standards Institute by the Accredited Standards Committee X9 - Financial Services. Committee approval of the standard does not necessarily imply that all committee members voted for its approval. At the time it approved this standard, the X9 Committee had the following members:

Roy DeCicco, X9 Chairman
Vincent DeSantis, X9 Vice-Chairman
Cynthia Fuller, Executive Director
Janet Busch, Program Manager

Organization Represented	Representative	
ACI Worldwide	Doug	Grote
ACI Worldwide	Cindy	Rink
American Bankers Association	Tom	Judd
American Bankers Association	C. Diane	Poole
American Express Company	Ted	Peirce
Apriva	Len	Sutton
Bank of America	Andi	Coleman
Bank of America	Daniel	Welch
Certicom Corporation	Daniel	Brown
Citigroup, Inc.	Mark	Clancy
Citigroup, Inc.	Michael	Knorr

Citigroup, Inc.	Karla	McKenna
Citigroup, Inc.	Chii-Ren	Tsai
CUSIP Service Bureau	Gerard	Faulkner
CUSIP Service Bureau	James	Taylor
Deluxe Corporation	John	FitzPatrick
Deluxe Corporation	Ralph	Stolp
Diebold, Inc.	Bruce	Chapa
Diebold, Inc.	Anne	Konecny
Discover Financial Services	Dave	Irwin
Discover Financial Services	Deana	Morrow
Federal Reserve Bank	Deb	Hjortland
Federal Reserve Bank	Claudia	Swendseid
First Data Corporation	Todd	Nuzum
First Data Corporation	Rick	Van Luvender
Fiserv	Bud	Beattie
Fiserv	Kevin	Finn
Fiserv	Lori	Hood
Fiserv	Dan	Otten
Fiserv	Skip	Smith
FIX Protocol Ltd	Jim	Northey
Harland Clarke	John	McCleary
Hewlett Packard	Larry	Hines
Hewlett Packard	Gary	Lefkowitz
IBM Corporation	Todd	Arnold
IFSA	Dexter	Holt
IFSA	Dan	Taylor
Ingenico	Steve	McKibben
Ingenico	John	Spence
J.P. Morgan Chase & Co	Robert	Blair
J.P. Morgan Chase & Co	Roy	DeCicco
J.P. Morgan Chase & Co	Edward	Koslow
J.P. Morgan Chase & Co	Jackie	Pagan
J.P. Morgan Chase & Co	Charita	Wamack
Key Innovations	Scott	Spiker
Key Innovations	Paul	Walters
KPMG LLP	Mark	Lundin
MagTek, Inc.	Terry	Benson
MagTek, Inc.	Jeff	Duncan
MagTek, Inc.	Mimi	Hart
MasterCard International	Mark	Kamers
Merchant Advisory Group	Dodd	Roberts
Metavante Image Solutions	Stephen	Gibson-Saxty
NACHA The Electronic Payments Association	Nancy	Grant
National Association of Convenience Stores	Michael	Davis
National Association of Convenience Stores	Alan	Thiemann
National Security Agency	Paul	Timmel
NCR Corporation	David	Norris
NCR Corporation	Steve	Stevens
RouteOne	Mark	Leonard
SWIFT/Pan Americas	Jean-	Eloy

	Marie	
SWIFT/Pan Americas	James	Wills
SWIFT/Pan Americas	Jamie	Shay
TECSEC Incorporated	Ed	Scheidt
The Clearing House	Vincent	DeSantis
U.S. Bank	Brian	Fickling
U.S. Bank	Gregg	Walker
University Bank	Stephen	Ranzini
University Bank	Michael	Talley
VeriFone, Inc.	David	Ezell
VeriFone, Inc.	Dave	Faoro
VeriFone, Inc.	Allison	Holland
VeriFone, Inc.	Doug	Manchester
VeriFone, Inc.	Brad	McGuinness
VeriFone, Inc.	Brenda	Watlington
VISA	Brian	Hamilton
VISA	John	Sheets
VISA	Richard	Sweeney
Wells Fargo Bank	Andrew	Garner
Wells Fargo Bank	Mike	McCormick
Wells Fargo Bank	Mike	Rudolph
Wells Fargo Bank	Mark	Tiggas
Wincor Nixdorf Inc	Ramesh	Arunashalam
XBRL US, Inc.	Mark	Bolgiano

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

Dick Sweeney, Chairperson

Organization Represented	**Representative**	
Company	First Name	Last Name
ACI Worldwide	Doug	Grote
ACI Worldwide	Julie	Samson
ACI Worldwide	Sid	Sidner
American Bankers Association	Tom	Judd
American Express Company	William J.	Gray
American Express Company	Vicky	Sammons
Bank of America	Dion	Bellamy
Bank of America	Terrelle	Carswell
Bank of America	Andi	Coleman

Bank of America	Todd	Inskeep
Bank of America	John	McGraw
Bank of America	Chris	Schrick
Bank of America	Daniel	Welch
Certicom Corporation	Daniel	Brown
Certicom Corporation	John O.	Goyo
Certicom Corporation	Sandra	Lambert
Certicom Corporation	Scott	Vanstone
Citigroup, Inc.	Mark	Clancy
Citigroup, Inc.	Susan	Rhodes
Citigroup, Inc.	Gary	Word
Communications Security Establishment	Alan	Poplove
Communications Security Establishment	Bridget	Walshe
Cryptographic Assurance Services	Ralph	Poore
Cryptographic Assurance Services	Jeff	Stapleton
CUSIP Service Bureau	Scott	Preiss
CUSIP Service Bureau	James	Taylor
DeLap LLP	Steve	Case
DeLap LLP	Darlene	Kargel
Deluxe Corporation	John	FitzPatrick
Deluxe Corporation	Ralph	Stolp
Depository Trust and Clearing Corporation	Robert	Palatnick
Diebold, Inc.	Bruce	Chapa
Diebold, Inc.	Laura	Drozda
Diebold, Inc.	Scott	Harroff
Diebold, Inc.	Anne	Konecny
Diebold, Inc.	Jessica	Wapole

Discover Financial Services	Julie	Shaw
Entrust, Inc.	Sharon	Boeyen
Entrust, Inc.	Miles	Smid
Federal Reserve Bank	Darin	Contini
Federal Reserve Bank	Pieralberto	Deganello
Federal Reserve Bank	Deb	Hjortland
Federal Reserve Bank	Mike	Ram
Ferris and Associates, Inc.	J. Martin	Ferris
First Data Corporation	Lisa	Curry
First Data Corporation	Lilik	Kazaryan
First Data Corporation	Todd	Nuzum
First Data Corporation	Scott	Quinn
First Data Corporation	Andrea	Stallings
First Data Corporation	Rick	Van Luvender
Fiserv	Bud	Beattie
Fiserv	Mary	Bland
Fiserv	Kevin	Finn
Fiserv	Dennis	Freiburg
Fiserv	Dan	Otten
Futurex	Greg	Schmid
GEOBRIDGE Corporation	Jason	Way
Harland Clarke	Joseph	Filer
Harland Clarke	John	McCleary
Harland Clarke	John	Petrie
Heartland Payment Systems	Roger	Cody
Heartland Payment Systems	Glenda	Preen
Hewlett Packard	Larry	Hines

Hewlett Packard	Susan	Langford
Hewlett Packard	Gary	Lefkowitz
Hypercom	Mohammad	Arif
Hypercom	Gary	Zempich
IBM Corporation	Todd	Arnold
IBM Corporation	Michael	Kelly
IFSA	Dexter	Holt
Independent Community Bankers of America	Cary	Whaley
InfoGard Laboratories	Doug	Biggs
InfoGard Laboratories	Ken	Kolstad
Ingenico	John	Spence
J.P. Morgan Chase & Co	Robert	Blair
J.P. Morgan Chase & Co	Edward	Koslow
J.P. Morgan Chase & Co	Kathleen	Krupa
J.P. Morgan Chase & Co	Donna	Meagher
J.P. Morgan Chase & Co	Jackie	Pagan
K3DES LLC	Azie	Amini
Key Innovations	Scott	Spiker
KPMG LLP	Mark	Lundin
MagTek, Inc.	Terry	Benson
MagTek, Inc.	Jeff	Duncan
MagTek, Inc.	Mimi	Hart
MasterCard International	Jeanne	Moore
MasterCard International	Michael	Ward
Merchant Advisory Group	Brad	Andrews
Merchant Advisory Group	Dodd	Roberts
National Institute of Standards and Technology	Elaine	Barker

National Institute of Standards and Technology	Lawrence	Bassham III
National Institute of Standards and Technology	William	Burr
National Institute of Standards and Technology	Lily	Chen
National Institute of Standards and Technology	David	Cooper
National Institute of Standards and Technology	Morris	Dworkin
National Institute of Standards and Technology	Randall	Easter
National Institute of Standards and Technology	Sharon	Keller
National Institute of Standards and Technology	John	Kelsey
National Institute of Standards and Technology	Annabelle	Lee
National Institute of Standards and Technology	Fernando	Podio
National Security Agency	Mike	Boyle
National Security Agency	Greg	Gilbert
National Security Agency	Tim	Havighurst
National Security Agency	Paul	Timmel
National Security Agency	Debby	Wallner
NCR Corporation	Charlie	Harrow
NCR Corporation	Ali	Lowden
NCR Corporation	David	Norris
NCR Corporation	Ron	Rogers
NCR Corporation	Steve	Stevens
NCR Corporation	Ally	Whytock
NTRU Cryptosystems, Inc.	Nick	Howgrave-Graham

NTRU Cryptosystems, Inc.	Ari	Singer
NTRU Cryptosystems, Inc.	William	Whyte
Pitney Bowes, Inc.	Andrei	Obrea
Pitney Bowes, Inc.	Leon	Pintsov
Pitney Bowes, Inc.	Rick	Ryan
RBS Group	Dan	Collins
Rosetta Technologies	Jim	Maher
Rosetta Technologies	Paul	Malinowski
RSA, The Security Division of EMC	Steve	Schmalz
Surety, Inc.	Dimitrios	Andivahis
Surety, Inc.	Tom	Klaff
TECSEC Incorporated	Ed	Scheidt
TECSEC Incorporated	Dr. Wai	Tsang
TECSEC Incorporated	Jay	Wack
Thales e-Security, Inc.	Colette	Broadway
Thales e-Security, Inc.	Jose	Diaz
Thales e-Security, Inc.	Tim	Fox
Thales e-Security, Inc.	James	Torjussen
The Clearing House	Vincent	DeSantis
The Clearing House	Henry	Farrar
The Clearing House	Susan	Long
U.S. Bank	Glenn	Marshall
U.S. Bank	Peter	Skirvin
U.S. Bank	Robert	Thomas
Unisys Corporation	David J.	Concannon
Unisys Corporation	Navnit	Shah
University Bank	Stephen	Ranzini

University Bank	Michael	Talley
VeriFone, Inc.	John	Barrowman
VeriFone, Inc.	David	Ezell
VeriFone, Inc.	Dave	Faoro
VeriFone, Inc.	Doug	Manchester
VeriFone, Inc.	Brad	McGuinness
VeriFone, Inc.	Brenda	Watlington
VISA	Leon	Fell
VISA	Tara	Kissoon
VISA	Chackan	Lai
VISA	Stoddard	Lambertson
VISA	Chris	McDaniel
VISA	John	Sheets
VISA	Richard	Sweeney
VISA	Johan (Hans)	Van Tilburg
Voltage Security, Inc.	Luther	Martin
Voltage Security, Inc.	Terence	Spies
Wells Fargo Bank	Mick	Bauer
Wells Fargo Bank	Jason	Buck
Wells Fargo Bank	Andrew	Garner
Wells Fargo Bank	Jeff	Jacoby
Wells Fargo Bank	Brian	Keltner
Wells Fargo Bank	Israel	Laracuente
Wells Fargo Bank	Eric	Lengvenis
Wells Fargo Bank	Mike	McCormick
Wells Fargo Bank	David	Naelon
Wells Fargo Bank	Doug	Pelton

Wells Fargo Bank	Chuck	Perry
Wells Fargo Bank	Keith	Ross
Wells Fargo Bank	Mike	Rudolph
Wells Fargo Bank	Ruven	Schwartz
Wells Fargo Bank	Craig	Shorter
Wells Fargo Bank	Tony	Stieber
Wincor Nixdorf Inc	Ramesh	Arunashalam
Wincor Nixdorf Inc	Saul	Caprio
Wincor Nixdorf Inc	Joerg-Peter	Dohrs
Wincor Nixdorf Inc	Matthias	Runowski
Wincor Nixdorf Inc	Adam	Sandoval
Wincor Nixdorf Inc	Michael	Waechter

The X9F6 working group that revised this standard consisted of the following members:

John Sheets, Chairperson

Organization Represented	**Representative**	
ACI Worldwide	Doug	Grote
ACI Worldwide	Jim	Jeter
ACI Worldwide	Sid	Sidner
Bank of America	Andi	Coleman
DeLap LLP	Steve	Case
DeLap LLP	Darlene	Kargel
Diebold, Inc.	Bruce	Chapa
Dresser Wayne	Tim	Weston
Fagan and Associates, LLC	Jeanne	Fagan
First Data Corporation	Lisa	Curry
First Data Corporation	Lilik	Kazaryan
First Data Corporation	Scott	Quinn
First Data Corporation	Andrea	Stallings
Fiserv	Dan	Otten
Futurex	Chris	Hamlett
GEOBRIDGE Corporation	Jason	Way
Gilbarco	Bruce	Welch
Heartland Payment Systems	Roger	Cody
Heartland Payment Systems	Glenda	Preen
Hewlett Packard	Larry	Hines
Hypercom	Gary	Zempich
IBM Corporation	Todd	Arnold
Ingenico	John	Spence

K3DES LLC	James	Richardson
K3DES LLC	Azie	Amini
Key Innovations	Scott	Spiker
Mustang Microsystems, Inc.	Tom	Galloway
NCR Corporation	Charlie	Harrow
RP Kastner Consulting, Inc.	Rick (Richard P.)	Kastner
SafeNet, Inc.	Brett	Thompson
Thales e-Security, Inc.	Jose	Diaz
Thales e-Security, Inc.	James	Torjussen
VeriFone, Inc.	Doug	Manchester
VISA	John	Sheets
Wells Fargo Bank	Craig	Shorter

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

1 Purpose

This key management standard, utilized in conjunction with the American National Standard Triple Data Encryption Algorithm (TDEA) (see Reference 2), 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 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 Reference 5), for encrypting Personal Identification Numbers (PIN) (see Reference 4), for encrypting other data, and for encrypting other keys.

2 Scope

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 management of symmetric keys using symmetric techniques. This part of this standard specifies the minimum requirements for the management of keying material. Addressed are all components of the key management life cycle including 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. It is intended that two nodes, if they implement compatible versions of:

- the same secure key management method,
- the same secure key identification technique approved for a particular method, and
- the same key separation methodologies

in accordance with this part of this standard 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.

2.1 Application

This part of this standard is applicable for institutions implementing techniques to safeguard cryptographic keys used for authentication and encryption of messages and other sensitive data. Specifically, this applies to institutions in the financial services industry implementing References 4 and/or 5.