American National Standard
for Financial Services

ANS X9.24-2004

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

Secretariat

Accredited Standards Committee X9, Inc.

Approved: February 4, 2004

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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
P.O. Box 4035
Annapolis, MD 21403 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 ANS X9.24-2004 deals exclusively with management of symmetric keys using symmetric techniques. Additional parts may be created in the future to address other methods of key management.

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., P.O. Box 4035, Annapolis, MD 21403.

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:

Gene Kathol, X9 Chairman
Vincent DeSantis, X9 Vice Chairman
Cynthia L. Fuller, Executive Director
Isabel Bailey, Managing Director

Organization Represented	Representative
ACI Worldwide	Jim Shaffer
American Express Company	Mike Jones
American Financial Services Association	Mark Zalewski
Bank of America	Daniel Welch
Bank One Corporation	Jacqueline Pagan
BB and T	Woody Tyner
Cable & Wireless America	Kevin M. Nixon CISSP CISM
Citigroup, Inc.	Daniel Schutzer
Deluxe Corporation	Bill Ferguson
Diebold, Inc.	Bruce Chapa

Discover Financial Services	Jon Mills
eFunds Corporation	Cory Surges
Federal Reserve Bank	Dexter Holt
First Data Corporation	Gene Kathol
Fiserv	Bud Beattie
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
IBM Corporation	Todd Arnold
Ingenico	John Sheets
KPMG LLP	Alfred F. Van Ranst Jr.
MagTek, Inc.	Carlos Morales
MasterCard International	William Poletti
Mellon Bank, N.A.	David Taddeo
National Association of Convenience Stores	John Hervey
National Security Agency	Sheila Brand
NCR Corporation	David Norris
Niteo Partners	Michael Versace
Star Systems, Inc.	Michael Wade
Symmetricom	Sandra Lambert
The Clearing House	Vincent DeSantis
Unisys Corporation	David J. Concannon
VeriFone, Inc.	Brad McGuinness
VISA International	Patricia Greenhalgh
Wachovia Bank	Ray Gatland
Wells Fargo Bank	Terry Leahy

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**
3PEA Technologies, Inc.	Mark Newcomer
ACI Worldwide	Jim Shaffer
American Financial Services Association	Mark Zalewski
Bank of America	Mack Hicks
Bank One Corporation	Jacqueline Pagan
BB and T	Woody Tyner
Cable & Wireless America	Kevin M. Nixon CISSP CISM
Deluxe Corporation	Bill Ferguson
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Todd Douthat
Diversinet Corporation	Rick (Richard P.) Kastner
eFunds Corporation	Chuck Bram
Ferris and Associates, Inc.	J. Martin Ferris
First Data Corporation	Gene Kathol
Fiserv	Bud Beattie
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
IBM Corporation	Todd Arnold
Identrus	Brandon Brown

InfoGard Laboratories	Tom Caddy
Ingenico	John Sheets
International Biometric Group	Mcken Mak CISSP
Jones Futurex, Inc.	Ray Bryan
KPMG LLP	Alfred F. Van Ranst Jr.
MagTek, Inc.	Terry Benson
Mellon Bank, N.A.	David Taddeo
National Association of Convenience Stores	John Hervey
National Security Agency	Sheila Brand
NCR Corporation	David Norris
Niteo Partners	Michael Versace
NIST	Elaine Barker
NTRU Cryptosystems, Inc.	William Whyte
Orion Security Solutions	Miles Smid
Pitney Bowes, Inc.	Leon Pintsov
R Squared Academy Ltd.	Ralph Spencer Poore
RSA Security	Burt Kaliski
Star Systems, Inc.	Michael Wade
Surety, Inc.	Dimitrios Andivahis
TECSEC Incorporated	Ed Scheidt
Thales e-Security, Inc.	James Torjussen
VeriFone, Inc.	Dave Faoro
VISA International	Richard Hite
Wachovia Bank	Ray Gatland
Wells Fargo Bank	Terry Leahy

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

John Sheets, Chairperson

Organization Represented	**Representative**
ACI Worldwide	Julie Samson
ACI Worldwide	Jim Shaffer
Alliance Data Systems	Steve Case
Bank of America	Andi Coleman
DeLap, White, Caldwell and Croy, LLP	Darlene Kargel
Diebold, Inc.	Bruce Chapa
Diebold, Inc.	Anne Doland
Diversinet Corporation	Rick (Richard P.) Kastner
eFunds Corporation	Chuck Bram
Eracom Technologies	Berry Borgers
Fagan and Associates, LLC	Jeanne Fagan
First Data Corporation	Lisa Curry
First Data Corporation	Martha Keely
First Data Corporation	Bruce Sussman
First Data Corporation	Kristi White
Fiserv	Bud Beattie
Fiserv	Dan Otten
Gilbarco	Tim Weston
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
iS3	John Clark

iS3	Michael McKay
IBM Corporation	Todd Arnold
Ingenico	John Sheets
Ingenico	John Spence
KPMG LLP	Azita Amini
KPMG LLP	Jeff Stapleton
MagTek, Inc.	Terry Benson
nCipher Corporation Ltd.	Ron Carter
NCR Corporation	Charlie Harrow
Star Systems, Inc.	Hugh Burke
Star Systems, Inc.	Michael Wade
TECSEC Incorporated	Pud Reaver
Thales e-Security, Inc.	Brian Sullivan
Trusted Security Solutions, Inc.	Dennis Abraham
VeriFone, Inc.	Dave Faoro
VISA	Stoddard Lambertson
VISA International	Richard Hite

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 3), should be 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 ANS X9.24-2004 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 ANS X9.24-2004 deals exclusively with management of symmetric keys using symmetric techniques. Additional parts may be created in the future to address other methods of key management.

This part of ANS X9.24-2004 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 ANS X9.24-2004 will be interoperable at the application level. Other characteristics may be necessary for node interoperability; however, this part of ANS X9.24-2004 does not cover such characteristics as message format, communications protocol, transmission speed, or device interface.