American National Standard
for Financial Services

ANS X9.24 Part 2: 2006

Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

Secretariat

Accredited Standards Committee X9, Inc.

Approved: January 13, 2006

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

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.

Part 1 of ANS X9.24 deals exclusively with management of symmetric keys using symmetric techniques. This Part 2 addresses the use of asymmetric techniques for the distribution of symmetric keys. Asymmetric techniques utilize algorithms other than the DEA (e.g., Diffie-Hellman, RSA, Elliptic Curve, etc.). Those asymmetric algorithms are defined in other American National Standards Institute standards (e.g., ANS X9.42 Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Algorithm Keys Using Discrete Logarithm Cryptography, ANS X9.44 DRAFT Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Factoring-Based Cryptography, and X9.63 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Management Using Elliptic Curve-Based Cryptography). Those algorithms are also in the public domain, and the security and reliability are also dependent on the security and integrity of the asymmetric keys and the infrastructure under which those keys are created and managed.

This part of ANS X9.24 assumes the reader is familiar with the concepts behind asymmetric cryptography.

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 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 wrote 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, Editor
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

Special thanks to Jeanne Fagan, the technical editor of this standard.

Retail Financial Services
Symmetric Key Management
Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

1 Purpose

The financial services industry desires an additional and cost effective method of implementing symmetric Triple Data Encryption Algorithm (TDEA) key distribution at remote devices and between communicating pairs. Compliant implementation of the requirements stated in ANS X9.24 Part 1 for the secure management of symmetric TDEA keys requires (among other things) unique keys per device and strict enforcement of dual control and split knowledge processes for handling the full-length (i.e., not concatenated) keying material deployed to remote devices or established between communicating pairs. Historically, *compliant* implementation of key distribution has been a manually performed, physically on-site process that is difficult to manage, costly, and/or non-existent (i.e., not compliant). An automated rather than manual method of distributing symmetric keys could address these issues and could result in improved security of the financial services networked environment.

The use of public key cryptography and associated asymmetric key algorithms is one proposed solution for automated remote symmetric key distribution. Unlike clear TDEA keys which **SHALL** be protected from disclosure at all times during their key life cycle, the clear public keys of the asymmetric key pairs may be exchanged over open networks. This characteristic allows for automated distribution from a remote location and may eliminate the above issues associated with manual key loading. Once distributed, the protocols associated with the asymmetric algorithms may be used to establish the TDEA symmetric key, and may eliminate the manual symmetric key loading process and its associated risks. There are two such protocols for establishing the TDEA symmetric key. The key transport protocol may be used by the sender to encrypt and transport the TDEA symmetric key to the receiver. The key agreement protocol may be used to mutually derive the TDEA symmetric key.

The security and reliability of any process based on public key algorithms is directly dependent on the protection afforded to the secrecy of each key pair's associated private key and the integrity of the key pair and Public Key Infrastructure (PKI) environment under which those key pairs are created and managed. Key modulus sizes and the underlying mathematics of the asymmetric key algorithms **SHOULD** also be considered as factors in the overall security of the implementation. The public key validation is a very important security aspect. Implementation of the system **SHALL** include measures to prevent man-in-the-middle attacks on the system, and ensure the mutual authentication of the sender and receiver of the keys.

This part of ANS X9.24 establishes requirements and guidelines for the secure management and application-level interoperability of such automated keying operations. This part of this standard addresses symmetric keys managed with asymmetric keys, and asymmetric keys managed with symmetric keys (as in the storage of private keys encrypted with a TDEA master key for storage as cryptograms on a local database). This part of ANS X9.24 does NOT address using asymmetric keys to encrypt the Personal Identification Number (PIN) and does NOT address asymmetric keys managed with asymmetric keys.

2 Scope

This part of ANS X9.24 covers the management of keying material used for financial services such as point of sale (POS) transactions, automatic teller machine (ATM) transactions, messages among terminals and financial