American National Standard for Financial Services

X9.42–2003

(R2013)

Public Key Cryptography for the Financial Services Industry:

Agreement of Symmetric Keys Using Discrete Logarithm Cryptography

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: November 19, 2003

American National Standards Institute

Contents

Tables

Forward

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

Introduction

Business practice has changed with the introduction of computer-based technologies. The substitution of electronic transactions for their paper-based predecessors has reduced costs and improved efficiency. Trillions of dollars in funds and securities are transferred daily by telephone, wire services, and other electronic communication mechanisms. The high value or sheer volume of such transactions within an open environment exposes the financial community and its customers to potentially severe risks from accidental or deliberate disclosure, alteration, substitution, or destruction of data. These risks are compounded by interconnected networks, and the increased number and sophistication of malicious adversaries. Electronically communicated data may be secured using symmetrically-keyed encryption algorithms (e.g. ANS X9.52, Triple-DEA) in combination with public key cryptography-based key management techniques.

This standard, ANS X9.42-2003, *Public Key Cryptography For The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*, defines the secure establishment of cryptographic data for the keying of symmetrically-keyed algorithms (e.g. TDEA). Schemes are provided for the agreement of symmetric keys using Diffie-Hellman and MQV algorithms. The Diffie-Hellman key agreement mechanism is a well-understood and widely implemented public key technique that facilitates cost-effective cryptographic key agreement across modern distributed electronic networks such as the Internet. The MQV algorithm is a variation of the Diffie-Hellman algorithm that has more security attributes and may provide better performance over analogous Diffie-Hellman methods. Because the Diffie-Hellman and the MQV techniques are based on the same fundamental mathematics as the Digital Signature Algorithm (DSA) (see [4]), additional efficiencies and functionality may be obtained by combining these and other cryptographic techniques.

While the techniques specified in this standard are designed to facilitate key management applications, the standard does not guarantee that a particular implementation is secure (even though the techniques specified in the standard are a basis for security). It is the responsibility of the financial institution to put an overall process in place with the necessary controls to ensure that the process is securely implemented. Furthermore, the controls should include the application of appropriate audit tests in order to verify compliance.

This standard also does not guarantee interoperability (though, again, the techniques specified in this standard are a basis for interoperability). ANS X9.42 is not a standard for interoperability, but a set of ASC X9-approved key establishment schemes with varying attributes.

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, P.O. Box 4035, Annapolis, MD 21403 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:
Harold Deal, X9 Chairman
Vincent DeSantis, X9 Vice-Chairman
Cynthia Fuller, Executive Director
Isabel Bailey, Managing Director

Organization Represented	Representative
ACI Worldwide	Cindy Rink
ACI Worldwide	Jim Shaffer
American Express Company	Mike Jones
American Express Company	Barbara Wakefield
American Financial Services Association	John Freeman
American Financial Services Association	Mark Zalewski
Bank of America	Mack Hicks
Bank of America	Richard Phillips
Bank of America	Daniel Welch
Bank One Corporation	Jacqueline Pagan
BB and T	Michael Saviak
BB and T	Woody Tyner
Cable & Wireless America	Dr. William Hancock CISSP CISM
Cable & Wireless America	Shannon Myers
Cable & Wireless America	Kevin M. Nixon CISSP CISM
Cable & Wireless America	Jonathan Siegel
Citigroup, Inc.	Paul Gubiotti
Citigroup, Inc.	Daniel Schutzer
Citigroup, Inc.	Mark Scott
Deluxe Corporation	Bill Ferguson
Deluxe Corporation	John Fitzpatrick
Deluxe Corporation	Alain Rault
Deluxe Corporation	John Toedter
Deluxe Corporation	Mike Valiquet
Diebold, Inc.	Bruce Chapa
Diebold, Inc.	Anne Doland
Diebold, Inc.	Judy Edwards
Discover Financial Services	Todd Douthat
Discover Financial Services	Pamela Ellington
Discover Financial Services	Matt Johanson
Discover Financial Services	Dan Kniola
Discover Financial Services	Jon Mills
eFunds Corporation	Chuck Bram
eFunds Corporation	Richard Fird
eFunds Corporation	Daniel Rick

eFunds Corporation	Joseph Stein
eFunds Corporation	Cory Surges
Federal Reserve Bank	Jeannine M. DeLano
Federal Reserve Bank	Dexter Holt
Federal Reserve Bank	Lori Hood
First Data Corporation	Gene Kathol
First Data Corporation	Todd Nuzum
Fiserv	Bud Beattie
Fiserv	Kevin Finn
Fiserv	Dan Otten
Fiserv	William Saffici
Fiserv	Linda Weber
Hewlett Packard	Larry Hines
Hewlett Packard	Gary Lefkowitz
Hypercom	Scott Spiker
Hypercom	Dennis Sullivan
Hypercom	Gary Zempich
IBM Corporation	Todd Arnold
Ingenico	John Sheets
Ingenico	John Spence
Inovant	Richard Sweeney
KPMG LLP	Tim Gartin
KPMG LLP	Mark Lundin
KPMG LLP	Jeff Stapleton
KPMG LLP	Alfred F. Van Ranst Jr.
MagTek, Inc.	Terry Benson
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Mimi Hart
MagTek, Inc.	Carlos Morales
MasterCard International	Caroline Dionisio
MasterCard International	Naiyre Foster
MasterCard International	Ron Karlin
MasterCard International	William Poletti
Mellon Bank, N.A.	Richard H. Adams
Mellon Bank, N.A.	David Taddeo
National Association of Convenience Stores	John Hervey
National Association of Convenience Stores	Teri Richman
National Association of Convenience Stores	Robert Swanson
National Security Agency	Sheila Brand
NCR Corporation	David Norris
NCR Corporation	Steve Stevens
Niteo Partners	Charles Friedman
Niteo Partners	Michael Versace
Star Systems, Inc.	Elizabeth Lynn
Star Systems, Inc.	Michael Wade
Symmetricom	Sandra Lambert

The Clearing House	Vincent DeSantis
The Clearing House	John Dunn
Unisys Corporation	David J. Concannon
Unisys Corporation	Navnit Shah
VeriFone, Inc.	David Ezell
VeriFone, Inc.	Dave Faoro
VeriFone, Inc.	Allison Holland
VeriFone, Inc.	Brad McGuinness
VeriFone, Inc.	Brenda Watlington
VISA	Brian Hamilton
VISA International	Patricia Greenhalgh
Wachovia Bank	Andrew Garner
Wachovia Bank	Ray Gatland
Wells Fargo Bank	Terry Leahy

The X9F subcommittee on Data and Information Security had the following members:

Richard Sweeney, Chairman

Organization Represented	Representative
3PEA Technologies, Inc.	Mark Newcomer
3PEA Technologies, Inc.	Daniel Spence
ACI Worldwide	Cindy Rink
ACI Worldwide	Jim Shaffer
American Express Company	William J. Gray
American Express Company	Mike Jones
American Express Company	Mark Merkow
American Financial Services Association	John Freeman
American Financial Services Association	Mark Zalewski
Bank of America	Andi Coleman
Bank of America	Mack Hicks
Bank of America	Todd Inskeep
Bank of America	Richard Phillips
Bank of America	Daniel Welch
Bank of America	Craig Worstell
Bank One Corporation	Jacqueline Pagan
BB and T	Michael Saviak
BB and T	Woody Tyner
Cable & Wireless America	Dr. William Hancock CISSP CISM
Cable & Wireless America	Shannon Myers
Cable & Wireless America	Kevin M. Nixon CISSP CISM
Cable & Wireless America	Jonathan Siegel
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Paul Gubiotti
Communications Security Establishment	Mike Chawrun
Communications Security Establishment	Alan Poplove
Deluxe Corporation	Bill Ferguson
Deluxe Corporation	John Fitzpatrick
Deluxe Corporation	Alain Rault
Deluxe Corporation	John Toedter
Deluxe Corporation	Mike Valiquet
Diebold, Inc.	Bruce Chapa
Diebold, Inc.	Anne Doland
Diebold, Inc.	Judy Edwards
Discover Financial Services	Todd Douthat
Discover Financial Services	Pamela Ellington
Discover Financial Services	Matt Johanson
Discover Financial Services	Dan Kniola
Discover Financial Services	Jon Mills
Diversinet Corporation	Rick (Richard P.) Kastner
Diversinet Corporation	David Simonetti

eFunds Corporation	Chuck Bram
Federal Reserve Bank	Neil Hersch
Ferris and Associates, Inc.	J. Martin Ferris
First Data Corporation	Gene Kathol
First Data Corporation	Todd Nuzum
Fiserv	Bud Beattie
Fiserv	Dan Otten
Hewlett Packard	Larry Hines
Hewlett Packard	Gary Lefkowitz
Hypercom	Scott Spiker
Hypercom	Dennis Sullivan
Hypercom	Gary Zempich
IBM Corporation	Todd Arnold
IBM Corporation	Michael Kelly
IBM Corporation	Allen Roginsky
Identrus	Brandon Brown
InfoGard Laboratories	Tom Caddy
InfoGard Laboratories	Ken Kolstad
Ingenico	John Sheets
Ingenico	John Spence
Inovant	Richard Sweeney
International Biometric Group	Mcken Mak CISSP
International Biometric Group	Mike Thieme
Jones Futurex, Inc.	Ray Bryan
Jones Futurex, Inc.	Scott Davis
Jones Futurex, Inc.	Barry Golden
Jones Futurex, Inc.	Steve Junod
KPMG LLP	Azita Amini
KPMG LLP	Tim Gartin
KPMG LLP	Mark Lundin
KPMG LLP	Jeff Stapleton
KPMG LLP	Alfred F. Van Ranst Jr.
MagTek, Inc.	Terry Benson
MagTek, Inc.	Mimi Hart
MasterCard International	Ron Karlin
MasterCard International	William Poletti
Mellon Bank, N.A.	David Taddeo
National Association of Convenience Stores	John Hervey
National Association of Convenience Stores	Robert Swanson
National Security Agency	Sheila Brand
NCR Corporation	Wayne Doran
NCR Corporation	Charlie Harrow
NCR Corporation	David Norris
NCR Corporation	Steve Stevens
Niteo Partners	Charles Friedman

Niteo Partners	Michael Versace
NIST	Elaine Barker
NIST	Lawrence Bassham III
NIST	Morris Dworkin
NIST	Annabelle Lee
NTRU Cryptosystems, Inc.	Ari Singer
NTRU Cryptosystems, Inc.	William Whyte
Orion Security Solutions	Santosh Chokhani
Orion Security Solutions	Miles Smid
Pitney Bowes, Inc.	Matthew Campagna
Pitney Bowes, Inc.	Andrei Obrea
Pitney Bowes, Inc.	Leon Pintsov
R Squared Academy Ltd.	Richard E. Overfield Jr.
R Squared Academy Ltd.	Ralph Spencer Poore
RSA Security	Burt Kaliski
Star Systems, Inc.	Elizabeth Lynn
Star Systems, Inc.	Michael Wade
Surety, Inc.	Dimitrios Andivahis
Symmetricom	Sandra Lambert
TECSEC Incorporated	Pud Reaver
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Dr. Wai Tsang
TECSEC Incorporated	Jay Wack
Thales e-Security, Inc.	Paul Meadowcroft
Thales e-Security, Inc.	Brian Sullivan
Thales e-Security, Inc.	James Torjussen
VeriFone, Inc.	Dave Faoro
VeriFone, Inc.	Brad McGuinness
VISA International	Patricia Greenhalgh
VISA International	Richard Hite
Wachovia Bank	Andrew Garner
Wachovia Bank	Ray Gatland
Wells Fargo Bank	Terry Leahy
Wells Fargo Bank	Gordon Martin
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 Elaine Barker, Project Editor

Organization Represented	Representative
ACI Worldwide	Jim Shaffer
American Express Company	Mike Jones
BB and T	Michael Saviak
Cable & Wireless America	Dr. William Hancock CISSP CISM
Cable & Wireless America	Shannon Myers
Cable & Wireless America	Kevin M. Nixon CISSP CISM
Cable & Wireless America	Jonathan Siegel
Certicom Corporation	Daniel Brown
Certicom Corporation	Scott Vanstone
Communications Security Establishment	Mike Chawrun
Communications Security Establishment	Alan Poplove
DeLap, White, Caldwell and Croy, LLP	Darlene Kargel
Diebold, Inc.	Bruce Chapa
Diebold, Inc.	Anne Doland
Diebold, Inc.	Judy Edwards
Discover Financial Services	Todd Douthat
Discover Financial Services	Jon Mills
Diversinet Corporation	Rick (Richard P.) Kastner
Diversinet Corporation	David Simonetti
eFunds Corporation	Chuck Bram
Entrust, Inc.	Don Johnson
Entrust, Inc.	Robert Zuccherato
Federal Reserve Bank	Neil Hersch
First Data Corporation	Lisa Curry
First Data Corporation	Michael Hodges
First Data Corporation	Todd Nuzum
First Data Corporation	Lynn Wheeler
Fiserv	Bud Beattie
Fiserv	Dan Otten
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
Hypercom	Dennis Sullivan
Hypercom	Gary Zempich
IBM Corporation	Todd Arnold
IBM Corporation	Michael Kelly
IBM Corporation	Allen Roginsky
Identrus	Brandon Brown
InfoGard Laboratories	Tom Caddy
InfoGard Laboratories	Ken Kolstad
Ingenico	John Sheets
Ingenico	John Spence
Inovant	Richard Sweeney

KPMG LLP	Tim Gartin
KPMG LLP	Mark Lundin
KPMG LLP	Jeff Stapleton
Landgrave Smith, Jr.	Landgrave Smith
MasterCard International	William Poletti
National Security Agency	Mike Boyle
National Security Agency	Sheila Brand
National Security Agency	Paul Timmel
NCR Corporation	Charlie Harrow
NCR Corporation	Ali Lowden
NCR Corporation	Ally Whytock
Niteo Partners	Charles Friedman
Niteo Partners	Michael Versace
NIST	Elaine Barker
NIST	Lawrence Bassham III
NIST	William Burr
NIST	Morris Dworkin
NIST	Randall Easter
NIST	Sharon Keller
NIST	John Kelsey
NTRU Cryptosystems, Inc.	Nick Howgrave-Graham
NTRU Cryptosystems, Inc.	Ari Singer
NTRU Cryptosystems, Inc.	William Whyte
Orion Security Solutions	Santosh Chokhani
Orion Security Solutions	Miles Smid
Pitney Bowes, Inc.	Matthew Campagna
Pitney Bowes, Inc.	Leon Pintsov
R Squared Academy Ltd.	Richard E. Overfield Jr.
R Squared Academy Ltd.	Ralph Spencer Poore
Relyco Sales Inc	Christopher Dowdell
RSA Security	Burt Kaliski
RSA Security	Mark McCutcheon
Symmetricom	Sandra Lambert
TECSEC Incorporated	Pud Reaver
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Dr. Wai Tsang
Thales e-Security, Inc.	Tim Fox
Thales e-Security, Inc.	Doug Grote
Thales e-Security, Inc.	Brian Sullivan
Thales e-Security, Inc.	James Torjussen
Unisys Corporation	David J. Concannon
VeriFone, Inc.	Dave Faoro
VISA International	Richard Hite
Wells Fargo Bank	Gordon Martin

This document cancels and replaces ANS X9.42—2001, the previous edition of this Standard. The technical changes to the 2001 edition are described in Annex F.

ANS X9.42 – 2003, Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography

1 Scope

This standard, partially adapted from ISO 11770-3 (see [13]), specifies schemes for the agreement of symmetric keys using Diffie-Hellman and MQV algorithms. It covers methods of domain parameter generation, domain parameter validation, key pair generation, public key validation, shared secret value calculation, key derivation, and test message authentication code computation for discrete logarithm problem based key agreement schemes. These methods may be used by different parties to establish a piece of common shared secret information such as cryptographic keys. The shared secret information may be used with symmetrically-keyed algorithms to provide confidentiality, authentication, and data integrity services for financial information, or used as a key-encrypting key with other ASC X9 key management protocols.

The key agreement schemes given herein do not provide certain desired assurances of security, such as key confirmation and entity authentication. However, these schemes may be used in conjunction with key confirmation and entity authentication mechanisms in key establishment protocols that are specified in other ASC X9 standards. These key agreement schemes may be used as subroutines to build key establishment protocols (see [8]). The key establishment methods specified in ANS X9.63 provide examples of mechanisms for obtaining these additional security properties. Further references for key agreement can be found in [33].

2 Normative References

ANS X3.92 –1981 (Revised 1998): *American National Standard - Data Encryption Algorithm*.

ANS X9.30 - Part 1 (Revised) - 1997: *Public Key Cryptography For the Financial Services Industry: The Digital Signature Algorithm (DSA)*.

ANS X9.30 - Part 2 (Revised) - 1997: *Public Key Cryptography For the Financial Services Industry: Secure Hash Algorithm (SHA-1)*.

ANS X9.52-1998: *Triple Data Encryption Algorithm Modes of Operation*.

ANS X9.57-1997: *Public Key Cryptography For the Financial Services Industry: Certificate Management*.

IEEE P1363-2000, *Standard Specifications for Public Key Cryptography*.