American National Standard for Financial Services

ANSI X9.79-2013

Public Key Infrastructure (PKI) — Part 4: Asymmetric Key Management — for the Financial Services Industry

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: February 5, 2013

American National Standards Institute

[NOTE: Only a document which is an American National Standard may use the special logos and may use the moniker "American National Standard". If this is a DSTU, simply state it as such.]

This page left intentionally blank

Contents

Page

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

Introduction

The use of asymmetric cryptography within the financial services industry has increased steadily since the original Diffie-Hellman paper [2] in 1976, the RSA paper [3] in 1978, and the ECC papers [4, 5] in 1985 and 1987. X9 standards have been developed addressing digital signature and hash algorithms, prime number generation, random number generation, key establishment schemes, public key infrastructure (PKI) policy and practices, certificate management, and both symmetric and asymmetric techniques for the distribution of symmetric keys. Several of these X9 standards have since been transformed into ISO standards. However there have been no standards directly addressing the requirements for utilizing asymmetric keys protecting financial information or other associated authentication data. This standard addresses the management and security of asymmetric keys for protecting financial information and other associated data.

Historically, as financial services migrated to electronic data and embraced common communication channels such as the Internet for online services, risks due to exploited information technology (IT) vulnerabilities correspondingly increased. Further, as regulatory bodies and industry organizations enhanced regulations and operating rules, the utilization of cryptography similarly grew. Today, asymmetric cryptography is often used across the enterprise for various security services (e.g., data confidentiality, data integrity, entity authentication and non-repudiation) in segregated departments with inconsistent key management policy and practices.

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, 1212 West Street, Suite 200, 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
Claudia Swendseid, 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	Diane C. 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. ..... Michael Knorr
Citigroup, Inc. ..... Karla McKenna
Citigroup, Inc. ..... Chii-Ren Tsai
Citigroup, Inc. ..... Gary Word
CUSIP Service Bureau ..... Gerard Faulkner
CUSIP Service Bureau ..... James Taylor
Deluxe Corporation ..... John FitzPatrick
Deluxe Corporation ..... Ralph Stolp
Diebold, Inc. ..... Anne Bayonnet
Diebold, Inc. ..... Bruce Chapa
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
FSTC, Financial Services Technology Consortium ..... Christine Nautiyal
FSTC, Financial Services Technology Consortium ..... Daniel Schutzer
FSTC, Financial Services Technology Consortium ..... Michael Versace
Harland Clarke ..... John McCleary
Hewlett Packard ..... Larry Hines
Hewlett Packard ..... Gary Lefkowitz
IBM Corporation ..... Todd Arnold
IFSA ..... Dexter Holt
IFSA ..... Dan Taylor
Ingenico ..... Alexandre Hellequin
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
RMG-SWIFT ..... Jamie Shay
RouteOne ..... Mark Leonard
SWIFT/Pan Americas ..... Jean-Marie Eloy

SWIFT/Pan Americas ..... James Wills
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

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

Ed Scheidt, X9F Chair
Sandra Lambert, X9F Vice Chair

Organization Represented — *Representative*

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 ..... John McGraw
Bank of America ..... Chris Schrick
Bank of America ..... Daniel Welch
Certicom ..... Daniel Brown
Certicom ..... John O. Goyo
Certicom ..... Sandra Lambert
Certicom ..... Scott Vanstone
Citigroup, Inc. ..... Susan Rhodes
Citigroup, Inc. ..... Gary Word
Communications Security Establishment ..... Alan Poplove
Communications Security Establishment ..... Bridget Walshe
Cryptographic Assurance Services LLC ..... Ralph Poore
Cryptographic Assurance Services LLC ..... 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. ..... Anne Bayonnet
Diebold, Inc. ..... Bruce Chapa
Diebold, Inc. ..... Laura Drozda
Diebold, Inc. ..... Scott Harroff
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
FSTC, Financial Services Technology Consortium ..... Christine Nautiyal
FSTC, Financial Services Technology Consortium ..... Daniel Schutzer
FSTC, Financial Services Technology Consortium ..... Michael Versace
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 ..... Mohammed Arif
Hypercom ..... Gary Zempich
IBM Corporation ..... Todd Arnold
IBM Corporation ..... Michael Kelly
IFSA ..... Dexter Holt
InfoGard Laboratories ..... Doug Biggs
InfoGard Laboratories ..... Ken Kolstad
Ingenico ..... Alexandre Hellequin

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
J.P. Morgan Chase & Co ..... Shawn Shifflett
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 ..... Dodd Roberts
Metavante Image Solutions ..... Ron Schultz
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
Rosetta Technologies ..... Jim Maher
Rosetta Technologies ..... Paul Malinowski
RSA, The Security Division of EMC ..... James Randall
RSA, The Security Division of EMC ..... Steve Schmalz
Surety, Inc. ..... Dimitrios Andivahis

Surety, Inc. ..... Tom Klaff
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

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 X9F4 Cryptographic Protocol and Application Security working group which developed this standard had the following active members:

Jeff Stapleton, X9F4 Chair
Sandra Lambert, X9F4 Vice Chair

Organization Represented *Representative*

Bank of America.....Andi Coleman
Bank of America..... Jeff Stapleton
Certicom .....Sandra Lambert
Certicom .....Scott Vanstone
Comet Capital .....Lawrence Levine
Cryptographic Assurance Services LLC .....Ralph Poore
Cryptographic Assurance Services LLC ..... Jeff Stapleton
DeLap LLP..... Steve Case
DeLap LLP.....Darlene Kargel
Diebold, Inc. .....Anne Bayonnet
Diebold, Inc. ..... Bruce Chapa
Diebold, Inc. .....Scott Harroff
Diebold, Inc. .....Jessica Wapole
Discover Financial Services .....Julie Shaw
Entrust, Inc.....Sharon Boeyen
Entrust, Inc..... Sheila Brand
Entrust, Inc.....Miles Smid
Ernst and Young.....Keith Sollers
Federal Reserve Bank ..... Darin Contini
Federal Reserve Bank ..... Pieralberto Deganello
Federal Reserve Bank .....Deb Hjortland
Federal Reserve Bank ..... Mike Ram
First Data Corporation .....Lilik Kazaryan
First Data Corporation ..... Brian Kean
First Data Corporation .....Todd Nuzum
Fiserv.....Dennis Freiburg
Fiserv.....Dan Otten
FSTC, Financial Services Technology Consortium .....Christine Nautiyal
FSTC, Financial Services Technology Consortium .....Michael Versace
Futurex.....Greg Schmid
GEOBRIDGE Corporation ..... Jason Way

Harland Clarke ..... John McCleary
Harland Clarke ..... John Petrie
Hewlett Packard ..... Larry Hines
Hypercom ..... Mohammed Arif
Hypercom ..... Gary Zempich
IBM Corporation ..... Todd Arnold
IBM Corporation ..... Phillip Griffin
IBM Corporation ..... Michael Kelly
IFSA ..... Dexter Holt
InfoGard Laboratories ..... Doug Biggs
InfoGard Laboratories ..... Ken Kolstad
Ingenico ..... Alexandre Hellequin
Ingenico ..... John Spence
J.P. Morgan Chase & Co ..... Sean Croston
J.P. Morgan Chase & Co ..... Leonid Vayner
KPMG LLP ..... Mark Lundin
MagTek, Inc. ..... Terry Benson
Merchant Advisory Group ..... Dodd Roberts
National Institute of Standards and Technology ..... Elaine Barker
National Institute of Standards and Technology ..... Lily Chen
National Security Agency ..... Greg Gilbert
National Security Agency ..... Tim Havighurst
National Security Agency ..... Paul Timmel
NCR Corporation ..... Charlie Harrow
NCR Corporation ..... Steve Stevens
NTRU Cryptosystems, Inc. ..... Ari Singer
NTRU Cryptosystems, Inc. ..... William Whyte
RSA, The Security Division of EMC ..... James Randall
Sun Microsystems PS ..... Joel Weise
Surety, Inc. ..... Dimitrios Andivahis
Thales e-Security, Inc. ..... Tim Fox
Thales e-Security, Inc. ..... James Torjussen
Transaction Network Services, Inc. ..... Kevin Gateman
Transaction Network Services, Inc. ..... Luc Saaka
Transaction Network Services, Inc. ..... Travis Lee
U.S. Bank ..... Peter Skirvin
U.S. Bank ..... Rush Wilson
Unisys Corporation ..... David J. Concannon
University Bank ..... Stephen Ranzini
University Bank ..... Michael Talley
VeriFone, Inc. ..... Dave Faoro
VeriFone, Inc. ..... Doug Manchester
VISA ..... Leon Fell
VISA ..... Tara Kissoon
VISA ..... Chackan Lai
VISA ..... Chris McDaniel
VISA ..... Richard Sweeney
VISA ..... Johan (Hans) Van Tilburg
Voltage Security, Inc. ..... Luther Martin

Wells Fargo Bank ..... Mick Bauer
Wells Fargo Bank ..... Jeff Jacoby
Wells Fargo Bank ..... Brian Keltner
Wells Fargo Bank ..... Eric Lengvenis
Wells Fargo Bank ..... Mike McCormick
Wells Fargo Bank ..... David Naelon
Wells Fargo Bank ..... Doug Pelton
Wells Fargo Bank ..... Mike Rudolph
Wells Fargo Bank ..... Ruven Schwartz
Wincor Nixdorf Inc ..... Matthias Runowski

This standard does not replace or update X9.24 [2.2] Symmetric Key Management using symmetric (Part 1) or asymmetric (Part 2) techniques for the distribution of symmetric keys, including PIN encryption keys and message authentication keys. Rather, this standard applies to all other areas where asymmetric keys and techniques are used within the financial services industry.

Public Key Infrastructure (PKI)

Part 4: Asymmetric Key Management

1 Scope

This standard addresses the management and security of asymmetric keys for protecting financial information and other associated data independent of the asymmetric algorithm, schemes or public key cryptography protocol. An asymmetric key pair consists of a mathematically related private key and public key that are jointly created using an asymmetric key generation algorithm. Only the public key (often encapsulated within an X.509 certificate issued by a certification authority) is distributed to the relying party. The corresponding private key must be retained by the originating party. Topics in scope of this standard include the following:

- Asymmetric key pairs utilized for the protection of financial data during transmission, in storage, or processing.
- Asymmetric key pairs utilized on computer systems, including mainframes, mid-range servers, client workstations, laptops, and other client platforms.
- Asymmetric key pairs utilized on network (wired) devices, including firewalls, routers, switches, load balancers, monitoring systems and other appliances.
- Asymmetric key pairs utilized on mobile (wireless) devices, including phones, pads, and tablets.
- Asymmetric key pairs utilized on cryptographic hardware and software modules.

Note that all public key certificates (e.g., X.509 certificates) are one type of public key credentials and for the purposes of this standard the term “certificate” includes all types of public key credentials. Refer to §6.1 Common Lifecycle Requirements for public key credential minimal requirements.

Related Topics out of scope for this standard include the following:

- Certificate Authority (CA) Certificate Policy (CP) and Certificate Practice Statement (CPS). Refer to ISO 21188 and RFC 5280 [1] for details.
- Using symmetric and asymmetric techniques for the distribution of symmetric keys, including ATM and POS. Refer to X9.24 [2.2] for details.
- Key establishment schemes for key transport or key agreement algorithms. Refer to X9.42 [2.3], X9.44 [2.4], and X9.63 [2.5] for details.
- Time stamp authority (TSA). Refer to X9.95 [2.20].
- Hardware Security Module (HSM) architecture, security requirements, and cryptographic application programming interfaces (API). These are vendor specific and proprietary. Refer to FIPS 140-2 [2.18].
- Entity authentication using knowledge, possession, or biometric factors.