American National Standard for Financial Services

ANSI X9.98 - 2010

Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: 10/15/2010

American National Standards Institute

This page left intentionally blank

Contents

Flows

Tables

Algorithms

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

Introduction

This Standard specifies key establishment techniques using public-key cryptography based on the problems of finding short vectors or close vectors in a lattice. The keying material established may be used to obtain one or more individual keys used to provide other cryptographic services outside the scope of this Standard, e.g. data confidentiality, data integrity, or symmetric-key-based key establishment

There are two primary reasons to consider the use of the techniques in this Standard:

1. The techniques are based on a different hard problem than other X9 approved public key algorithms. If the integer factorization problem, the finite field discrete logarithm problem and the elliptic curve discrete logarithm problem were all to be broken (for example, by the realization of a quantum computer of sufficient size), this method might remain unbroken.
2. The techniques may have performance advantages in some environments, provided that the stated security levels for domain parameters and key sizes specified herein are accurate.

The techniques described in this Standard were developed more recently than the techniques described in other X9 standards that use public key cryptography. As such, although this standard reflects the state of the art in knowledge about the security of these techniques, they may be considered to face a greater risk than other public key techniques that improved attacks will be discovered. Implementers who are considering implementing this system should determine for themselves how to balance this potentially greater risk with the benefits described above.

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 CeCicco, X9 Chairman
Vincent DeSantis, X9 Vice-Chairman
Cynthia L. Fuller, Executive Director
Janet Busch, Program Manager

The X9 Committee had the following members:

Company	First Name	Last Name
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

BAFT/IFSA	Dexter	Holt
BAFT/IFSA	Joseph	Pawelczyk
BAFT/IFSA	Dan	Taylor
Bank of America	Andi	Coleman
Bank of America	Jeff	Stapleton
Bank of America	Daniel	Welch
Certicom Corporation	Daniel	Brown
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	Deb	Lynch
Deluxe Corporation	Ralph	Stolp
Diebold, Inc.	Bruce	Chapa
Diebold, Inc.	Anne	Konecny
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
Independent Community Bankers of America	Viveca	Ware
Independent Community Bankers of America	Cary	Whaley
Ingenico	Steve	McKibben
Ingenico	John	Spence
ISITC	Tara	Gonzales
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	Kathleen	Krupa
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
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
Symantec Corportation	Alex	Deacon
Symcor Inc.	Brian	Salway
TECSEC Incorporated	Ed	Scheidt
The Clearing House	Vincent	DeSantis
The Clearing House	Sharon	Jablon
U.S. Bank	Brian	Fickling
U.S. Bank	Gregg	Walker
University Bank	Stephen	Ranzini
University Bank	Michael	Talley
USDA Food and Nutrition Service	Kathy	Ottobre
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	Kim	Wagner
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 Information Security had the following members:

Company	Last Name, First Name
American Bankers Association	Judd, Tom
Bank of America	Coleman, Andi
Certicom Corporation	Brown, Daniel
Citigroup, Inc.	Tsai, Dr. Chii-Ren
Communications Security Establishment	Poplove, Alan
Cryptographic Assurance Services	Poore, Ralph

CUSIP Service Bureau	Preiss, Scott
DeLap LLP	Kargel, Darlene
Deluxe Corporation	FitzPatrick, John
Depository Trust and Clearing Corporation	Palatnick, Mr. Robert
Diebold, Inc.	Chapa, Bruce
Discover Financial Services	Schaefer, Mr. Jordan
Entrust, Inc.	Smid, Miles
Federal Reserve Bank	Hjortland, Deb
Ferris and Associates, Inc.	Ferris, J. Martin
First Data Corporation	Curry, Lisa
Fiserv	Beattie, Bud
GEOBRIDGE Corporation	Way, Jason
Harland Clarke	Petrie, John
Heartland Payment Systems	Preen, Glenda
Hewlett Packard	Hines, Larry
Hypercom	Zempich, Gary
IBM Corporation	Arnold, Todd
InfoGard Laboratories	Biggs, Doug
Ingenico	Spence, John
ITS, Inc. (SHAZAM Networks)	Nathwani, Mr. Manish
J.P. Morgan Chase & Co	Koslow, Edward
Key Innovations	Spiker, Scott
KPMG LLP	Lundin, Mark
MasterCard International	Ward, Michael
Merchant Advisory Group	Roberts, Dodd
Merchant Link	Franklin, Scott
National Institute of Standards and Technology	Barker, Elaine
National Security Agency	Timmel, Paul
NCR Corporation	Norris, David
Pitney Bowes, Inc.	Ryan, Rick
RBS Group	Collins, Dan
Rosetta Technologies	Maher, Jim
Rosetta Technologies	Malinowski, Paul
Security Innovation	Whyte, William
STAR	Kazaryan, Lilik
Surety, Inc.	Andivahis, Dimitrios
Symcor Inc.	Salway, Brian
TECSEC Incorporated	Scheidt, Ed
Thales e-Security, Inc.	Torjussen, James
The Clearing House	DeSantis, Vincent
Trustwave	Amaral, John
Unisys Corporation	Concannon, David J.
University Bank	Ranzini, Stephen
VeriFone, Inc.	Faoro, Dave
Voltage Security, Inc.	Martin, Luther
Wells Fargo Bank	Tiggas, Mark
Wincor Nixdorf Inc	Nolte, Michael

The X9F1 Working Group on Applications Security had the following members:

Terence Spies, Voltage Security, Inc., Chairman

Organization Represented	Representative
Bank of America	Andi Coleman
Certicom Corporation	Daniel Brown
Communications Security Establishment	Bridget Walshe
Cryptographic Assurance Services	Ralph Poore
Entrust, Inc.	Miles Smid
Hewlett Packard	Susan Langford
Hypercom	Mohammad Arif
IBM Corporation	Todd Arnold
InfoGard Laboratories	Doug Biggs
MasterCard International	Michael Ward
National Institute of Standards and Technology	Elaine Barker
National Security Agency	Mike Boyle
RSA, The Security Division of EMC	Steve Schmalz
Security Innovation	William Whyte
Voltage Security, Inc.	Terence Spies

ANSI X9.98-2010

Lattice-Based Polynomial Public Key Encryption Algorithm for the Financial Services Industry, Part 1: Key Establishment

1 Scope

This Standard specifies the cryptographic functions for establishing symmetric keys using a lattice-based polynomial public key encryption algorithm and the associated parameters for key generation (see Note 1). The mechanism supported is *key transport*, where one party selects keying material and conveys it to the other party with cryptographic protection. The keying material may consist of one or more individual keys used to provide other cryptographic services outside the scope of this Standard, e.g. data confidentiality, data integrity, or symmetric-key-based key establishment. The standard also specifies key pair generators and corresponding key pair validation methods supporting the key transport schemes (see Note 2).

This standard does not address the distribution of the public and private keys, associated parameters and other keying material. The integrity and authenticity of the public key and its associated parameters is outside the scope of this standard, and are assumed to be securely managed using the appropriate X9 standards. The confidentiality of the private key and its associated parameters is outside the scope of this standard, and are assumed to be securely managed using the appropriate X9 standards.

This version of the Standard is limited to a small number of possible lattice-based polynomial public key establishment schemes and key pair generators and validation methods. Future versions may include additional schemes with different attributes (see Note 3).

NOTE: A key pair validation method determines whether a candidate public-key/private-key pair meets the constraints for key pairs produced by a particular key generation method. A *public-key validation method* determines whether a candidate public key meets those constraints, without knowledge of the private key. Full public-key validation methods are not specified in this version of the Standard, but are expected to be developed in future X9 work.

2 Conformance to this Standard

An implementation may claim conformance with this Standard if it implements at least one key pair generator, public key validation, or key transport scheme in this Standard with at least one approved set of parameters. An implementation claiming conformance with this Standard shall indicate the specific techniques with which conformance is claimed and the parameter sets for which conformance is claimed.

Key pair generators with which conformance may be claimed are: lbp-kgp-3 (see section 11.3.1.1).

Key transport mechanisms with which conformance may be claimed are: kts1-basic (see section 15.2.3) and kts1-receiver-confirmation (see section 15.2.4).

Key pair validation mechanisms with which conformance may be claimed are: kpv3 (see section 13.4.3.1).

Public key validation mechanisms with which conformance may be claimed are described in section 13.4.5.2.

Parameter sets with which conformance may be claimed are: ees401ep1, ees541ep1, ees659ep1, ees449ep1, ees613ep1, ees761ep1, ees677ep1, ees887ep1, ees1087ep1, ees1087ep2, ees1171ep1, ees1499ep1.
.

