American National Standard
for Financial Services

X9.92-1–2009

Public Key Cryptography for the Financial Services Industry

Digital Signature Algorithms Giving Partial Message Recovery

Part 1: Elliptic Curve Pintsov-Vanstone Signatures (ECPVS)

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: August 12, 2009
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 interpretations 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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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, Inc.
Financial Industry Standards
1212 West Street, Suite 200
Annapolis, MD 21401
X9 Online http://www.x9.org

Contents

Figures

Tables

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 the 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 through the use of symmetrically keyed encryption algorithms (e.g. ANS X9.52, Triple-DEA) in combination with public-key cryptography-based key management techniques.

Some of the conventional “due care” controls used with paper-based transactions are unavailable in electronic transactions. Examples of such controls are safety paper which protects integrity, and handwritten signatures or embossed seals which indicate the intent of the originator to be legally bound. In an electronic-based environment, controls must be in place that provide the same degree of assurance and certainty as in a paper environment. The financial community is responding to these needs.

This Standard, X9.92-1–2009, Public Key Cryptography For The Financial Services Industry: Digital Signatures Algorithms Giving Partial Message Recovery: Elliptic Curve Pintsov-Vanstone Signatures (ECPVS), defines a mechanism designed to facilitate the secure authentication and non-repudiation of data.

While the techniques specified in this Standard are designed to facilitate authentication and non-repudiation applications, the Standard does not guarantee that a particular implementation is secure. 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.

NOTE The user's attention is called to the possibility that compliance with this Standard may require the 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., 1212 West Street, Suite 200, Annapolis, Maryland 21401.

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:

Roy DeCicco, X9 Chairman
Vincent DeSantis, X9 Vice-Chairman
Cynthia Fuller, Managing Director
Janet Busch, Program Manager

Organization	Representative	
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
Bank of America	Andi	Coleman
Bank of America	Daniel	Welch
Certicom Corporation	Daniel	Brown
Citigroup, Inc.	Mark	Clancy
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:

Richard Sweeney, X9F Chairman
Sandra Lambert, X9F Vice-Chairman

Organization	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	Andi	Coleman
Bank of America	Daniel	Welch
Certicom Corporation	Daniel	Brown
Certicom Corporation	Sandra	Lambert
Citigroup, Inc.	Mark	Clancy
Citigroup, Inc.	Susan	Rhodes
Communications Security Establishment	Alan	Poplove
Communications Security Establishment	Bridget	Walshe
Cryptographic Assurance Services	Ralph	Poore
Cryptographic Assurance Services	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.	Bruce	Chapa
Discover Financial Services	Julie	Shaw
Entrust, Inc.	Sharon	Boeyen
Entrust, Inc.	Miles	Smid
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	Mohammad	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
K3DES LLC	Azie	Amini
Key Innovations	Scott	Spiker
Key Innovations	Paul	Walters
KPMG LLP	Mark	Lundin
MagTek, Inc.	Terry	Benson
MagTek, Inc.	Jeff	Duncan
MagTek, Inc.	Mimi	Hart
Merchant Advisory Group	Dodd	Roberts
National Institute of Standards and Technology	Elaine	Barker
National Institute of Standards and Technology	Lily	Chen
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
RBS Group	Dan	Collins
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	John	Sheets
VISA	Richard	Sweeney
Voltage Security, Inc.	Luther	Martin
Voltage Security, Inc.	Terence	Spies
Wells Fargo Bank	Mike	McCormick
Wells Fargo Bank	Ruven	Schwartz
Wells Fargo Bank	Mark	Tiggas
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 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 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 Daniel Brown Project Editor

Organization	Representative
Certicom Corporation	Daniel Brown
	Scott Vanstone
	Matt Campagna
Communications Security Establishment of Canada	Mike Chawrun
Entrust	Don Johnson
	Miles Smid
Microsoft	Niels Ferguson
National Institute of Standards and Technology	Morris Dworkin

	Elaine Barker
	John Kelsey
	Lily Chen
National Security Agency	Paul Timmel
	Michael Boyle
NTRU	William Whyte
Pitney Bowes, Inc	Rick Ryan
RSA Security	James Randall
	Burt Kaliski
	Steve Schmalz

At the time of the publication of this Standard, the X9F1 Cryptographic Tool Standards and Guidelines group was headed by Terence Spies, Chair, and Ralph Spencer Poore, Vice Chair.

Public Key Cryptography for the Financial Services Industry Digital Signature Algorithms Giving Partial Message Recovery Part 1: Elliptic Curve Pintsov-Vanstone Signatures (ECPVS)

1 Scope

This Standard defines methods for digital signature generation and verification for the protection of messages and data giving partial message recovery.

This document is Part 1 of this Standard, and it defines the Elliptic Curve Pintsov-Vanstone Signature (ECPVS) digital signature algorithm. Part 2 of this Standard defines the Finite Field Pintsov-Vanstone Signature (FFPVS) digital signature algorithm.

ECPVS is a signature scheme with low message expansion (overhead) and variable length recoverable and visible message parts. ECPVS is ideally suited for short messages, yet is flexible enough to handle messages of any length.

The ECPVS shall be used in conjunction with an Approved hash function and an Approved symmetric encryption scheme. In addition, this ECPVS Standard provides the criteria for checking the message redundancy.

Supporting examples are also provided.

2 Conformance

An implementation of elliptic curve Pintsov-Vanstone signatures may claim conformance with this Standard if it implements the mandatory provisions in Part 1.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. Nevertheless, parties to agreements based on this document are encouraged to consider applying the most recent edition of the referenced documents indicated below. For undated references, the latest edition of the referenced document (including any amendments) applies.

ANS X9.52, *Triple Data Encryption Algorithm Modes of Operation*

ANS X9.62, *Public-Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*

ANS X9.63, *Public-Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*

ASC X9 Registry Item 00002, Advanced Encryption Standard

ASC X9 Registry Item 00003, Secure Hash Standard