American National Standard for Financial Services

ANSI X9.97-2009

Financial services — Secure Cryptographic Devices (Retail) —

Part 1: Concepts, Requirements and Evaluation Methods —

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: May 22, 2009

American National Standards Institute

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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
1212 West Street Suite 200
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

This ANSI Standard is based on ISO 13491-1:2007(E) **Financial Services — Secure cryptographic devices (retail)** — Part 1: **Concepts, requirements and evaluation methods**. The ISO 13491-1:2007(E) has been reproduced in its entirety with the addition of "ANSI Note's" and other changes highlighted via dotted underlining (sample underlining) where required to adapt the text for use as an ANSI Standard. Where applicable, references to ANSI standards have been added and internal reference to this standard have been changed from ISO 13491-1:2007 to ANS X9.97-1:2008.

Annex A is an informative annex, unchanged from the original ISO standard.

Annex B is an informative annex, summarizing the changes made to this standard from the original ISO 13491-1:2007 standard.

ANS X9.97 consists of the following parts; under the general title Financial Services — Secure cryptographic devices (retail):

- Part 1: Concepts, requirements and evaluation methods
- Part 2: Security compliance check-lists for devices used in financial transaction environments

Introduction

ANS X9.97 describes both the physical and logical characteristics and the management of the secure cryptographic devices (SCDs) used to protect messages, cryptographic keys and other sensitive information used in a retail financial services environment.

The security of retail electronic payment systems is largely dependent upon the security of these cryptographic devices. This security is based upon the premise that computer files can be accessed and manipulated, communications lines can be "tapped" and authorized data or control inputs into system equipment can be replaced with unauthorized inputs. When Personal Identification Numbers (PINs), Message Authentication Codes (MACs), Cryptographic Keys and other sensitive data are processed, there is a risk of tampering or other compromise to disclose or modify such data. It must be ensured that the risk of financial loss is reduced through the appropriate use of cryptographic devices that have proper characteristics and are properly managed.

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.

The X9 committee had the following members:

Roy DeCicco, X9 Chairman
Vincent DeSantis, 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	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 & Information Security had the following members:

Richard Sweeney, Chairman

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	Todd	Inskeep
Bank of America	John	McGraw
Bank of America	Chris	Schrick
Bank of America	Daniel	Welch
Certicom Corporation	Daniel	Brown
Certicom Corporation	John O.	Goyo
Certicom Corporation	Sandra	Lambert
Certicom Corporation	Scott	Vanstone
Citigroup, Inc.	Mark	Clancy
Citigroup, Inc.	Susan	Rhodes
Citigroup, Inc.	Gary	Word
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.	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	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
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
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.)

The X9F6 group on Cardholder Authentication and ICC'swhich developed this standard had the following members:

John Sheets, Chairman

Organization Represented	*Representative*
ACI Worldwide	Doug Grote
ACI Worldwide	Jim Jeter
ACI Worldwide	Sid Sidner
Bank of America	Andi Coleman
DeLap LLP	Steve Case
DeLap LLP	Darlene Kargel
Diebold, Inc.	Bruce Chapa
Dresser Wayne	Tim Weston
Fagan and Associates, LLC	Jeanne Fagan
First Data Corporation	Lisa Curry
First Data Corporation	Lilik Kazaryan
First Data Corporation	Brian Kean
First Data Corporation	Scott Quinn
First Data Corporation	Andrea Stallings
Fiserv	Dan Otten
Futurex	Chris Hamlett
GEOBRIDGE Corporation	Jason Way
Gilbarco	Bruce Welch
Heartland Payment Systems	Roger Cody

Heartland Payment Systems	Glenda Preen
Hewlett Packard	Larry Hines
Hypercom	Gary Zempich
IBM Corporation	Todd Arnold
Ingenico	John Spence
K3DES LLC	James Richardson
Key Innovations	Scott Spiker
Mustang Microsystems, Inc.	Tom Galloway
NCR Corporation	Charlie Harrow
RP Kastner Consulting, Inc.	Rick (Richard P.) Kastner
SafeNet, Inc.	Brett Thompson
Thales e-Security, Inc.	Jose Diaz
Thales e-Security, Inc.	James Torjussen
VeriFone, Inc.	Doug Manchester
VISA	John Sheets
Wells Fargo Bank	Craig Shorter

Financial services — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods

1 Scope

This part of ANS X9.97 specifies the requirements for Secure Cryptographic Devices which incorporate the cryptographic processes defined in ISO 9564, ISO 16609 and ISO 11568.

This part of ANS X9.97 has two primary purposes:

1) to state the requirements concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their life cycle,

2) to standardize the methodology for verifying compliance with those requirements.

Appropriate device characteristics are necessary to ensure that the device has the proper operational capabilities and provides adequate protection for the data it contains. Appropriate device management is necessary to ensure that the device is legitimate, that it has not been modified in an unauthorized manner, e.g., by "bugging", and that any sensitive data placed within the device (e.g., cryptographic keys) has not been subject to disclosure or change.

Absolute security is not practically achievable. Cryptographic security depends upon each life cycle phase of the SCD and the complementary combination of appropriate management procedures and secure cryptographic characteristics. These management procedures implement preventive measures to reduce the opportunity for a breach of SCD security. These aim for a high probability of detection of any unauthorized access to sensitive or confidential data should device characteristics fail to prevent or detect the security compromise.

Annex A provides an informative illustration of the concepts of security levels described in this part of ANS X9.97 as being applicable to SCDs.

This part of ANS X9.97 does not address issues arising from the denial of service of an SCD.

Specific requirements for the characteristics and management of specific types of SCD functionality used in the retail financial services environment are contained in ANS X9.97-2.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ANS X9.8-1:2003: *Banking — Personal Identification Number Management and Security — Part 1: PIN protection principles and techniques for online PIN verification in ATM & POS systems*