National Standard
for Financial Services

X9.84-2003

Biometric Information Management and Security for the Financial Services Industry

Secretariat:
Accredited Standards Committee X9, Incorporated

Approved July 29, 2003:
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, directly and materially affected interests have reached substantial agreement. 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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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, Incorporated
Financial Industry Standards
P. O. Box 4035
Annapolis, MD 21403
www.x9.org

Contents

List of Figures

List of 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 accidental or deliberate alteration, substitution or destruction of data. Interconnected networks, and the increased number and sophistication of malicious adversaries compound this risk.

The inevitable advent of electronic communications across uncontrolled public networks, such as the Internet, is also increasing risk to the financial industry. The necessity to expand business operations onto these environments has elevated the awareness for strong identification and authentication (I&A) and created the need for alternate forms of I&A. The financial community is responding to these needs.

Biometrics, the “something you are” identity factor, has come of age, and includes such technologies as finger image, voice identification, eye scan, facial image, and the like. The cost of biometric technology has been decreasing while the reliability has been increasing, and both are now acceptable and viable for the financial industry.

This Standard, ANSI X9.84-2002, *Biometrics Management and Security*, describes adequate controls and proper procedures for using biometrics as an identification mechanism and authentication mechanism for secure remote electronic access or local physical access controls for the financial industry.

Biometrics can be used for human identification and authentication for physical and logical access. Logical access can include access to applications, services, or entitlements. This standard promotes the integration of biometrics into the financial industry. It positions biometric technology to strengthen public key infrastructures (PKI) for higher I&A by providing stronger methods as well as multi-factor authentication. In addition, this Standard allows continuous reassurance that the entity about to generate a digital signature is, in fact, the person authorized to access the private key.

This standard assumes that the identity of the individual is recognized as part of the transaction process and that the use of the biometric is solely for the purpose of facilitating a financial transaction. It also assumes that any individual using a biometric form of identification for a legitimate financial transaction does so willingly and with the full knowledge of both when a biometric measurement is being taken and what is being measured.

The techniques specified in this Standard are designed to maintain the integrity and confidentiality of biometric information and provide strong authentication. However, 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 with this Standard.

Suggestions for the improvement or revision of this Standard are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9 Incorporated, Financial Industry Standards P. O. Box 4035, Annapolis MD 21403.

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:
Gene Kathol, Chairman, First Data Corporation
Vincent DeSantis, Vice Chairman, The Clearing House

Cindy Fuller, Executive Director, ASC X9, Inc.
Isabel Bailey, Managing Director, ASC X9, Inc.

Organization	Representative
ACI Worldwide	Cindy Rink
ACI Worldwide	Jim Shaffer
American Bankers Association	Doug Johnson
American Bankers Association	Don Rhodes
American Bankers Association	Stephen Schutze
American Bankers Association	Michael Scully
American Express Company	Mike Jones
American Express Company	Barbara Wakefield
American Financial Services Association	John Freeman
American Financial Services Association	Mark Zalewski
BancTec, Inc.	Rosemary Butterfield
BancTec, Inc.	Christopher Dowdell
BancTec, Inc.	David Hunt
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.	Daniel Schutzer
Citigroup, Inc.	Mark Scott
Citigroup, Inc.	Skip Zehnder
Deluxe Corporation	Maury Jansen
Diebold, Inc.	Bruce Chapa
Diebold, Inc.	Anne Doland
Diebold, Inc.	Judy Edwards
Discover Financial Services	Pamela Ellington
Discover Financial Services	Masood Mirza
eFunds Corporation	Chuck Bram
eFunds Corporation	Richard Fird
eFunds Corporation	Daniel Rick
eFunds Corporation	Joseph Stein
eFunds Corporation	Cory Surges
Electronic Data Systems	Linda Low
Federal Reserve Bank	Jeannine M. DeLano
Federal Reserve Bank	Dexter Holt
Federal Reserve Bank	Laura Walker
First Data Corporation	Gene Kathol
Fiserv	Bud Beattie
Fiserv	Kevin Finn

Fiserv	Dan Otten
Hewlett Packard	Larry Hines
Hewlett Packard	Gary Lefkowitz
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
Silas Technologies	Andrew Garner
Silas Technologies	Ray Gatland
Star Systems, Inc.	Elizabeth Lynn
Star Systems, Inc.	Michael Wade
Symmetricom	Sandra Lambert
Symmetricom	Jerry Willett
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 International	Patricia Greenhalgh
Wells Fargo Bank	Terry Leahy
Wells Fargo Bank	Gordon Martin

The X9F Subcommittee on Information Security had the following members:
Richard Sweeney, Chairman, Inovant
Sandra Lambert, Vice Chairman, Lambert and Associates

Organization	Representative
3PEA Technologies, Inc.	Mark Newcomer
3PEA Technologies, Inc.	Daniel Spence
ACI Worldwide	Cindy Rink
ACI Worldwide	Jim Shaffer
American Bankers Association	Don Rhodes
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
BancTec, Inc.	Christopher Dowdell
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
Communications Security Establishment	Mike Chawrun
Communications Security Establishment	Alan Poplove
Deluxe Corporation	Maury Jansen
Diebold, Inc.	Bruce Chapa
Diebold, Inc.	Anne Doland
Diebold, Inc.	Judy Edwards
Discover Financial Services	Pamela Ellington
Discover Financial Services	Masood Mirza
Diversinet Corporation	Michael Crerar
eFunds Corporation	Chuck Bram
Electronic Industries Alliance	Edward Mikoski
Electronic Industries Alliance	Donald L. Skillman
Entrust, Inc.	Miles Smid
Federal Reserve Bank	Neil Hersch
Ferris and Associates, Inc.	J. Martin Ferris
First Data Corporation	Gene Kathol
Fiserv	Bud Beattie
Fiserv	Dan Otten

Hewlett Packard	Larry Hines
Hewlett Packard	Gary Lefkowitz
IBM Corporation	Todd Arnold
IBM Corporation	Michael Kelly
IBM Corporation	Allen Roginsky
Identrus	Brandon Brown
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	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
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
Wells Fargo Bank	Terry Leahy
Wells Fargo Bank	Gordon Martin
Wells Fargo Bank	Ruven Schwartz

The X9F4 Working Group on Applications Security had the following members:
Jeff Stapleton, Chairman, KPMG LLP

Organization	Representative
American Bankers Association	Don Rhodes
American Express Company	Mike Jones
American Financial Services Association	Mark Zalewski
BancTec, Inc.	Christopher Dowdell
BancTec, Inc.	Alex Parkov
Bank of America	Mack Hicks
Bank of America	Todd Inskeep
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
Diebold, Inc.	Bruce Chapa
Diebold, Inc.	Anne Doland
Diebold, Inc.	Judy Edwards
Entrust, Inc.	Miles Smid
Entrust, Inc.	Robert Zuccherato
Federal Reserve Bank	Neil Hersch
First Data Corporation	Lisa Curry
First Data Corporation	Michael Hodges
First Data Corporation	Gene Kathol
First Data Corporation	Lynn Wheeler
Fiserv	Dan Otten
Gilbarco	Timothy Dickson
Gilbarco	Tim Weston
Hewlett Packard	Larry Hines
IBM Corporation	Todd Arnold

IBM Corporation	Michael Kelly
Identrus	Brandon Brown
Ingenico	John Sheets
Ingenico	John Spence
Inovant	Richard Sweeney
International Biometric Group	Mcken Mak CISSP
KPMG LLP	Tim Gartin
KPMG LLP	Eric Longo
KPMG LLP	Mark Lundin
KPMG LLP	Jeff Stapleton
KPMG LLP	Alfred F. Van Ranst Jr.
Landgrave Smith, Jr.	Landgrave Smith
MasterCard International	William Poletti
National Security Agency	Greg Gilbert
NCR Corporation	Wayne Doran
Niteo Partners	Charles Friedman
Niteo Partners	Michael Versace
NTRU Cryptosystems, Inc.	Ari Singer
NTRU Cryptosystems, Inc.	William Whyte
RSA Security	Burt Kaliski
Sun Microsystems PS	Yvonne Humphery
Sun Microsystems PS	Joel Weise
Surety, Inc.	Dimitrios Andivahis
Symmetricom	Ron Holm
Symmetricom	Sandra Lambert
Symmetricom	Jerry Willett
TECSEC Incorporated	Pud Reaver
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Dr. Wai Tsang
Thales e-Security, Inc.	Tim Fox
Thales e-Security, Inc.	Brian Sullivan
Thales e-Security, Inc.	James Torjussen
TimeCertain, LLC	Steven Teppler
TimeCertain, LLC	John Tomaszewski
VeriFone, Inc.	Dave Faoro
Wells Fargo Bank	Gordon Martin
Wells Fargo Bank	Ruven Schwartz

The X9F4 Working Group had the following liaison relationships:

Liaison Organization	Representative
ANSI B10.8 Drivers License / Identification	Michael Hodges (liaison)
BioAPI Consortium	Catherine Tilton (liaison)
Biometric Consortium	Fernando Podio (co-chair)
INCITS M1 on Biometrics	Fernando Podio (chair)
INCITS M1 on Biometrics	Jeff Stapleton (liaison)
INCITS T4 on Information Security	Phillip H. Griffin (liaison)
International Biometric Industry Association (IBIA)	Paul Collier (liaison)

Liaison Organization	Representative
ISO TC68 Subcommittee 2 Security And General Banking Operations	Michael Versace (chair)
OASIS XML Common Biometric Format (XCBF) Technical Committee	Phillip H. Griffin (chair)

Biometric Information Management and Security for the Financial Services Industry

1 Scope

This Standard specifies the minimum security requirements for effective management of biometric data. Within the scope of this Standard the following topics are addressed:

- Security for the collection, distribution, and processing, of biometric data, encompassing data integrity, authenticity, and non-repudiation.
- Management of biometric data across its life cycle comprised of the enrollment, transmission and storage, verification, identification, and termination processes.
- Usage of biometric technology, including one-to-one and one-to-many matching, for the identification and authentication of banking customers and employees.
- Application of biometric technology for internal and external, as well as logical and physical access control.
- Encapsulation[1] of biometric data.
- Techniques for the secure transmission and storage of biometric data.
- Security of the physical hardware used throughout the biometric data life cycle.
- Techniques for integrity and privacy protection of biometric data.

Items considered out of scope and not addressed in this Standard include the following:

- The individual's privacy and ownership of biometric data.
- Application specific requirements and limitations for employing biometric technology.

This standard does not require nor recommend confidentiality of biometric information for purposes of security, however §9 Techniques provides the mandatory means whereby biometric information may be encrypted for reasons of privacy or other perceived liabilities.

This standard assumes that identification of an individual is on a voluntary basis whereby the individual is recognized as part of the transaction process and is not intended for surreptitious activity.
This standard is organized as follows:

2 Conformance and Organization

A biometric authentication system may claim compliance to this standard if the implementation satisfies the management and security requirements identified in §8 *Management and Security Requirements*.

A biometric authentication system that utilizes the methods recommended in §9 *Techniques* and has implemented appropriate policies, practices and operational procedures should comply with this standard.

Compliance of a biometric authentication systems can be verifed if the implementation and its associated policies, practices and operational procedures meet the the validation control objectives identied in Annex F: *(Informative) Biometric Validation Control Objectives*.

[1] Analogous to the ANSI PIN Block, refer to ANSI X9.8 and ISO 9564 PIN Management and Security standards.