

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

ANS X9.84-2003

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

Copyright © 2002 by Accredited Standards Committee X9, Incorporated
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of the publisher. Printed in the United States of America

ANS X9.84-2003

Contents

Foreword	i
Introduction	vi
1 Scope	1
2 Conformance and Organization	1
3 Normative References	2
4 Terms and Definitions	4
5 Symbols and Abbreviated Terms	9
6 Overview of Biometric Technology	11
6.1 Introduction	11
6.2 Fingerprint Biometrics	11
6.3 Voice Biometrics	12
6.4 Iris Biometrics	12
6.5 Retina Biometrics	13
6.6 Face Biometrics	13
6.7 Hand Geometry Biometrics	13
6.8 Signature Biometrics	14
6.9 Technology Considerations	14
6.9.1 Introduction to Consideration	14
6.9.2 Universality	14
6.9.3 Distinctiveness	15
6.9.4 Accuracy	15
6.9.5 Performance Evaluation	17
7 Basic Principles of Biometric Architectures	19
7.1 Introduction	19
7.2 The Data Collection Subsystem	20
7.3 The Transmission Subsystem	21
7.4 The Signal Processing Subsystem	21
7.5 Matching Subsystem	22
7.6 The Decision Subsystem	23
7.7 The Storage Subsystem	23
8 Management and Security Requirements	24
8.1 Introduction	24
8.2 Core Security Requirements	24
8.3 Enrollment	24
8.3.1 Initial Enrollment	25
8.3.2 Re-enrollment	26
8.4 Verification	26
8.5 Identification	28
8.6 Transmission and Storage	29
8.6.1 Transmission	29
8.6.2 Central Data Base	29
8.6.3 Tokens	30
8.7 Termination and Archive	30
8.7.1 Termination	30
8.7.2 Archiving	31
8.8 Compliance and the Event Journal	31
9 Techniques	31
9.1 Biometric Information Objects	31
9.2 ASN.1 Syntax	36
9.2.1 Biometric Object	36
9.2.2 Biometric Header	36
9.2.3 Biometric Objects	39

ANS X9.84-2003

9.2.4	Integrity Objects	39
9.2.5	Privacy Objects	44
9.2.6	Integrity and Privacy Objects	47
9.2.7	Biometric Syntax Sets	48
9.3	Cryptographic Techniques	49
9.3.1	Security Architecture	49
9.3.2	Key Management	49
9.3.3	Digital Signatures	50
9.3.4	Message Authentication Codes (MAC).....	50
9.3.5	Encryption for Purposes of Privacy.....	50
9.4	Physical Techniques	51
Annex A:	(Normative) Biometrics Syntax and Encoding Rules	52
A.1	Introduction	52
A.2	X9-84-Biometrics ASN.1 Module	52
A.3	X9-84-CMS ASN.1 Module	57
A.4	X9-84-ObjectIdentifiers ASN.1 Module	60
A.5	Object Identifiers	70
Annex B:	(Informative) Bibliography	72
Annex C:	(Informative) Data Flow Diagrams	73
Annex D:	(<i>Informative</i>) Biometric Enrollment.....	76
D.1	Identification Criteria for an Individual.....	76
D.2	Quality Check and Verification of Matchability.....	76
Annex E:	(<i>informative</i>) Security Considerations	78
E.1	Registration of individual using false identity.....	78
E.2	Fraud Susceptibility within Data Collection "Synthetic Attack"	78
E.3	Protection of the data.....	79
E.3.1	Injection of false/replayed biometric data	79
E.3.2	Search for match between chosen sample and templates.....	79
E.3.3	Search for match between pairs of templates	80
E.4	Modification of verification result	80
E.5	False Match versus False Non-Match	81
E.5.1	Improper Threshold Settings	82
E.5.2	Improper Device Calibration	82
E.5.3	Illicit Device or System Performance.....	82
E.6	Scores and Thresholds.....	82
E.6.1	Hillclimbing Attack.....	83
E.6.2	Update and Adaptation.....	83
E.7	Single versus Multi-Factor Authentication	84
E.8	Testing.....	85
E.9	Open Versus Closed Systems.....	86
E.10	Compromise/loss of biometric data	87
E.11	Data compression.....	88
E.12	System circumvention.....	88
Annex F:	(Informative) Biometric Validation Control Objectives	89
F.1	Introduction	89
F.2	Environmental Controls.....	89
F.2.1	Security Policy.....	90
F.2.2	Security Organization.....	90
F.2.3	Asset Classification and Management.....	91
F.2.4	Personnel Security.....	91
F.2.5	Physical and Environmental Security.....	93
F.2.6	Operations Management.....	94
F.2.7	System Access Management	95
F.2.8	Systems Development and Maintenance	96
F.2.9	Business Continuity Management	96
F.2.10	Monitoring and Compliance	97

ANS X9.84-2003

F.2.11	Event Journaling	98
F.3	Key Management Life Cycle Controls.....	100
F.3.1	Key Generation	101
F.3.2	Key Storage, Backup and Recovery	101
F.3.3	Key Distribution	102
F.3.4	Key Usage.....	102
F.3.5	Key Destruction and Archival.....	103
F.3.6	Cryptographic Device Life Cycle Controls	103
F.4	Biometric Information Life Cycle Controls.....	105
F.4.1	Enrollment	105
F.4.2	Template Life Cycle	106
F.4.3	Verification and Identification Process Controls	107
F.4.4	Biometric Device Life Cycle Controls.....	109
F.4.5	Integrated Circuit Card (ICC) Life Cycle Controls.....	110
	Annex G: (Informative) Public Acceptance and Policy Considerations	114
	Annex H: (Informative) Encoding Examples	115
H.1	Introduction	115
H.1	Unprotected Biometric Object	115
H.1.1	Examples: Reduced Biometric Header	115
H.1.2	Examples: Complete Biometric Header	116
H.2	Biometric Objects with Integrity	117
H.3	Biometric Objects with Privacy	121
	Annex I: (Informative) Event Journal.....	125
I.1	Management Requirements.....	125
I.2	Content Requirements	125
I.2.1	Enrollment	125
I.2.2	Verification and Identification	126
I.2.4	Transmission and Storage	126
	Annex J: (Informative) Biometric Identification Record (BIR)	128
	Annex K: (Informative) X9.84 Relationship to X9.73	132
K.1	Signed Data	132
K.2	Authenticated Data	133
K.3	Enveloped Data	133
K.4	Other Types	134

ANS X9.84-2003

List of Figures

Figure 1 Major Components of a Generalized Biometric Architecture	20
Figure 2 Environmental Context for a Biometric System	20
Figure 3 Enrollment Model	25
Figure 4 Verification Model	27
Figure 5 Identification Model	28
Figure 6 Distribution Model	29
Figure 7 Token Verification Model	30
Figure 8 - Biometric Header	32
Figure 9 - Biometric Object	33
Figure 10 - Integrity Object.....	33
Figure 11 - Privacy Object.....	34
Figure 12 - Integrity and Privacy Object.....	34
Figure 13 - Biometric Syntax Set	34
Figure 14 - Biometric Objects.....	35
Figure 15 - Integrity Objects.....	35
Figure 16 - Privacy Objects.....	35
Figure 17 - Integrity and Privacy Objects.....	36
Figure 18 Security Architectures	49
Figure 19 CBEFF Entity Relationships	128
Figure 20 BioAPI BIR.....	130

List of Tables

Table 1 Organization of X9.84	2
Table 2 Key Management Techniques	50
Table 3 Closed versus Open Systems.....	86
Table 4 CBEFF to X9.84 Data Element Mapping	129
Table 5 Biometric Identification Record (BIR).....	129

ANS X9.84-2003

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

ANS X9.84-2003

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

Organization

ACI Worldwide
ACI Worldwide
American Bankers Association
American Bankers Association
American Bankers Association
American Bankers Association
American Express Company
American Express Company
American Financial Services Association
American Financial Services Association
BancTec, Inc.
BancTec, Inc.
BancTec, Inc.
Bank of America
Bank of America
Bank of America
Bank One Corporation
BB and T
BB and T
Cable & Wireless America
Cable & Wireless America
Cable & Wireless America
Cable & Wireless America
Citigroup, Inc.
Citigroup, Inc.
Citigroup, Inc.
Deluxe Corporation
Diebold, Inc.
Diebold, Inc.
Diebold, Inc.
Discover Financial Services
Discover Financial Services
eFunds Corporation
eFunds Corporation
eFunds Corporation
eFunds Corporation
eFunds Corporation
Electronic Data Systems
Federal Reserve Bank
Federal Reserve Bank
Federal Reserve Bank
First Data Corporation
Fiserv
Fiserv

Representative

Cindy Rink
Jim Shaffer
Doug Johnson
Don Rhodes
Stephen Schutze
Michael Scully
Mike Jones
Barbara Wakefield
John Freeman
Mark Zalewski
Rosemary Butterfield
Christopher Dowdell
David Hunt
Mack Hicks
Richard Phillips
Daniel Welch
Jacqueline Pagan
Michael Saviak
Woody Tyner
Dr. William Hancock CISSP CISM
Shannon Myers
Kevin M. Nixon CISSP CISM
Jonathan Siegel
Daniel Schutzer
Mark Scott
Skip Zehnder
Maury Jansen
Bruce Chapa
Anne Doland
Judy Edwards
Pamela Ellington
Masood Mirza
Chuck Bram
Richard Fird
Daniel Rick
Joseph Stein
Cory Surges
Linda Low
Jeannine M. DeLano
Dexter Holt
Laura Walker
Gene Kathol
Bud Beattie
Kevin Finn

ANS X9.84-2003

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
Symmetricon	Sandra Lambert
Symmetricon	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

ANS X9.84-2003

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

Organization

3PEA Technologies, Inc.
3PEA Technologies, Inc.
ACI Worldwide
ACI Worldwide
American Bankers Association
American Express Company
American Express Company
American Express Company
American Financial Services Association
American Financial Services Association
BancTec, Inc.
Bank of America
Bank of America
Bank of America
Bank of America
Bank of America
Bank of America
Bank One Corporation
BB and T
BB and T
Cable & Wireless America
Cable & Wireless America
Cable & Wireless America
Cable & Wireless America
Certicom Corporation
Communications Security Establishment
Communications Security Establishment
Deluxe Corporation
Diebold, Inc.
Diebold, Inc.
Diebold, Inc.
Discover Financial Services
Discover Financial Services
Diversinet Corporation
eFunds Corporation
Electronic Industries Alliance
Electronic Industries Alliance
Entrust, Inc.
Federal Reserve Bank
Ferris and Associates, Inc.
First Data Corporation
Fiserv
Fiserv

Representative

Mark Newcomer
Daniel Spence
Cindy Rink
Jim Shaffer
Don Rhodes
William J. Gray
Mike Jones
Mark Merkow
John Freeman
Mark Zalewski
Christopher Dowdell
Andi Coleman
Mack Hicks
Todd Inskeep
Richard Phillips
Daniel Welch
Craig Worstell
Jacqueline Pagan
Michael Saviak
Woody Tyner
Dr. William Hancock CISSP CISM
Shannon Myers
Kevin M. Nixon CISSP CISM
Jonathan Siegel
Daniel Brown
Mike Chawrun
Alan Poplove
Maury Jansen
Bruce Chapa
Anne Doland
Judy Edwards
Pamela Ellington
Masood Mirza
Michael Crerar
Chuck Bram
Edward Mikoski
Donald L. Skillman
Miles Smid
Neil Hersch
J. Martin Ferris
Gene Kathol
Bud Beattie
Dan Otten

ANS X9.84-2003

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

ANS X9.84-2003

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

American Bankers Association
American Express Company
American Financial Services Association
BancTec, Inc.
BancTec, Inc.
Bank of America
Bank of America
BB and T
Cable & Wireless America
Cable & Wireless America
Cable & Wireless America
Cable & Wireless America
Certicom Corporation
Diebold, Inc.
Diebold, Inc.
Diebold, Inc.
Entrust, Inc.
Entrust, Inc.
Federal Reserve Bank
First Data Corporation
First Data Corporation
First Data Corporation
First Data Corporation
Fiserv
Gilbarco
Gilbarco
Hewlett Packard
IBM Corporation

Representative

Don Rhodes
Mike Jones
Mark Zalewski
Christopher Dowdell
Alex Parkov
Mack Hicks
Todd Inskeep
Michael Saviak
Dr. William Hancock CISSP CISM
Shannon Myers
Kevin M. Nixon CISSP CISM
Jonathan Siegel
Daniel Brown
Bruce Chapa
Anne Doland
Judy Edwards
Miles Smid
Robert Zuccherato
Neil Hersch
Lisa Curry
Michael Hodges
Gene Kathol
Lynn Wheeler
Dan Otten
Timothy Dickson
Tim Weston
Larry Hines
Todd Arnold

ANS X9.84-2003

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
Symmetricon	Ron Holm
Symmetricon	Sandra Lambert
Symmetricon	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:

<u>Liaison Organization</u>	<u>Representative</u>
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)

ANS X9.84-2003

Liaison Organization

ISO TC68 Subcommittee 2
Security And General Banking Operations
OASIS XML Common Biometric Format
(XCBF) Technical Committee

Representative

Michael Versace (chair)

Phillip H. Griffin (chair)

ANS X9.84-2003

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.
- Encapsulation¹ 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 verified if the implementation and its associated policies, practices and operational procedures meet the the validation control objectives identified 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.