INTERNATIONAL STANDARD

ISO 19092

First edition
2008-01-15

Financial services — Biometrics — Security framework

Services financiers — Biométrie — Cadre de sécurité

Reference number
ISO 19092:2008(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 19092 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This first edition of ISO 19092 cancels and replaces ISO 19092-1:2006, of which it constitutes a minor revision, notably to remove references to the ISO 19092-2 project.

Introduction

This International Standard replaces ISO 19092-1:2006. When ISO 19092-1:2006 was published, it was expected that a second part of ISO 19092 (ISO 19092-2, *Financial services — Biometrics — Part 2: Message syntax and cryptographic requirements*) would subsequently be published. However, ISO 19092-2 was not completed due to a lack of consensus. As a result, ISO 19092-1:2006 has been updated into this International Standard, removing all references to ISO 19092-2 and incorporating some minor editorial corrections.

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 on systemically important payment systems and other financial systems 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 into these environments has elevated the awareness for strong authentication and created the need for alternate forms of authentication. The financial community is responding to these needs.

Biometrics, the “something you are or are able to do” identity factor, has come of age, and includes such technologies as finger image, voice identification, eye scan and facial image. 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 International Standard describes adequate controls and proper procedures for using biometrics as an authentication mechanism for secure remote electronic access or local physical access controls for the financial industry.

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

The success of a biometric system with the public is based on a number of factors, and these factors differ among the available biometric technologies:

— convenience and ease of use;

— level of apparent security;

— performance;

— non-invasiveness.

The authentication systems discussed in this International Standard are those for a closed user group in which the group members have agreed to use biometric identification or perform identification themselves. Such agreements might be explicit (e.g. service agreement) or implicit (e.g. entering a facility indicating a clear intent to conduct a transaction). Such systems that will be used to monitor an indefinite number of people are excluded from the scope of this International Standard.

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

Financial services — Biometrics — Security framework

1 Scope

This International Standard describes the security framework for using biometrics for authentication of individuals in financial services. It introduces the types of biometric technologies and addresses issues concerning their application. This International Standard also describes the architectures for implementation, specifies the minimum security requirements for effective management, and provides control objectives and recommendations suitable for use by a professional practitioner.

The following are within the scope of this International Standard:

— usage of biometrics for the authentication of employees and persons seeking financial services by:

  — verification of a claimed identity;

  — identification of an individual;

— validation of credentials presented at enrolment to support authentication as required by risk management;

— management of biometric information across its life cycle comprised of the enrolment, transmission and storage, verification, identification and termination processes;

— security of biometric information during its life cycle, encompassing data integrity, origin authentication and confidentiality;

— application of biometrics for logical and physical access control;

— surveillance to protect the financial institution and its customers;

— security of the physical hardware used throughout the biometric information life cycle.

The following are not within the scope of this International Standard:

— the individual's privacy rights and ownership of biometric information;

— specific techniques for data collection, signal processing and matching of biometric data, and the biometric matching decision-making process;

— usage of biometric technology for non-authentication convenience applications such as speech recognition, user interaction and anonymous access control.

This International Standard provides the mandatory means whereby biometric information may be encrypted for data confidentiality or other reasons.

Although this International Standard does not address specific requirements and limitations of business applications employing biometric technology, other standards may address these topics.

2 Conformance

A biometric authentication system may claim compliance to this International Standard if the implementation satisfies the management and security requirements identified in this International Standard.

A biometric authentication system that utilizes the cryptographic message requirements recommended in this International Standard and that has implemented appropriate policies, practices and operational procedures shall comply with this International Standard.

Compliance of many of the aspects of a biometric authentication system can be achieved by satisfying the management and security requirements specified in Clauses 9 and 10, and verified if the implementation and its associated policies, practices and operational procedures meet the validation control objectives identified in Clause 11. An organization can document compliance to many operational aspects of this International Standard using the biometric event journal specified in Annex A.

3 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.

ISO 10202-3, *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 3: Cryptographic key relationships*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

4.1
adaptation
process of automatically updating or refreshing a reference template

4.2
attempt
submission of a biometric sample on the part of an individual for the purposes of enrolment, verification, or identification in a biometric system

NOTE An individual can be permitted several attempts to enrol, to verify, or to be identified.

4.3
binning
database partitioning based on information contained within (endogenous to) the biometric patterns

4.4
biometrics
measurable biological or behavioural characteristic, which reliably distinguishes one person from another, used to recognize the identity, or verify the claimed identity, of an enrolee

4.5
biometric authentication
process of confirming an individual's identity, either by verification or by identification

4.6
biometric data
extracted information taken from the biometric sample and used to generate either a reference template or a match template

4.7
biometric identification
one-to-many process of comparing a submitted biometric sample against some or all enrolled reference templates to determine an individual's identity

4.8
Biometric Policy
BP
named set of rules that indicate the applicability of a biometric template to some community or class of application having common security requirements

4.9
Biometric Practice Statement
BPS
statement of the practices which an organization follows during the biometric template life cycle (e.g. creation, management, and destruction), including business, legal, regulatory and technical matters

4.10
biometric sample
initial (raw) biometric data that is captured and processed

4.11
biometric system
automated system capable of capturing, extraction, matching and returning a decision (match/non-match)

4.12
biometric verification
process of comparing a match template against a specific reference template based on a claimed identity (e.g. user ID, account number)

4.13
capture
acquisition of a biometric sample

4.14
claim of identity
name or index of a claimed reference template or enrolee used by a biometric system for verification

4.15
claimant
person submitting a biometric sample for verification

4.16
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/TR 13569:2005, 3.15; ISO/IEC 13335-1:2004, 2.6]

4.17
cryptographic exchange
secure transport or storage of data or cryptographic materials under the protection of a cryptographic key

4.18
decision policy
logic through which a biometric system provides match/no match decisions, inclusive of the following elements:

— the biometric system's matching threshold;

— the number of match attempts permitted per transaction;

— the number of reference templates enrolled per claimant;

— the number of distinct biometric samples (e.g. different fingerprints) enrolled per claimant;

— the number of biometric technologies (e.g. fingerprint, voice) in which the claimant is enrolled;

— the use of internal controls in the matching process to detect like or non-like biometric samples.

NOTE Serial, parallel, weighted or fusion decision models in biometric systems utilize more than one reference template in the match process for a given user (e.g. multiple-biometric systems as well as systems in which reference templates are created and stored from multiple fingerprints).

4.19
encryption
reversible transformation of plain text (readable) by a cryptographic algorithm to produce cipher text (unreadable) to hide the information content of the plain text

4.20
enrolment
process of collecting biometric samples from a person and the subsequent generation and storage of biometric reference templates associated with that person

NOTE See also **initial enrolment** (4.36) and **re-enrolment** (4.47).

4.21
Equal Error Rate
EER
probability or percentage of errors when the decision threshold of a system is set such that the false match rate is equal to the false non-match

NOTE Historically, this was referred to as "crossover rate".

4.22
extraction
feature extraction
process of converting raw biometric data into processed biometric data for use in template comparison or reference template creation

4.23
face biometrics
biometric technology based on the distinctive characteristics of the face, inclusive of features in the visible spectrum, the infrared spectrum, or both

4.24
failure to acquire
failure of a biometric system to capture a biometric sample, or to extract biometric data from a biometric sample, sufficient to generate a reference template or match template

4.25
failure to enrol
failure of a biometric system to capture one or more biometric samples, or to extract data from one or more biometric samples, sufficient to generate a reference template

4.26
False Acceptance Rate
FAR
probability, in a one-to-one system, that a biometric system will incorrectly identify an individual, or will fail to reject an impostor

NOTE For a positive (verification) system, it can be estimated from the number of false acceptances divided by the number of impostor verification attempts.

4.27
False Match Rate
FMR
rate for incorrect positive matches by the matching algorithm for single template comparison attempts

NOTE For a biometric system that uses just one attempt to decide acceptance, FMR is the same as FAR. When multiple attempts are combined in some manner to decide acceptance, FAR is more meaningful at the system level than FMR.

4.28
False Non-Match Rate
FNMR
rate for incorrect negative matches by the matching algorithm for single template comparison attempts

NOTE For a biometric system that uses just one attempt to decide acceptance, FNMR is the same as **FRR** (4.29). When multiple attempts are combined in some manner to decide acceptance, FRR is more meaningful at the system level than FNMR.

4.29
False Rejection Rate
FRR
probability that a biometric system will fail to identify a genuine enrolee

NOTE For a positive (verification) system, it can be estimated from the number of false rejects divided by the number of enrolee verification attempts.

4.30
filtering
partitioning a database through the use of exogenous information about the user not discernible from the biometric patterns, such as sex, age or race

4.31
finger geometry
biometric technology based on the distinctive characteristics of the shape and dimensions of one or more fingers

4.32
fingerprint biometrics
biometric technology (e.g. finger minutia or finger pattern matching) based on the distinctive characteristics of the friction ridges and valleys present on an individual's fingertips

4.33
hand geometry
hand identification
biometric technology based on the distinctive characteristics of the shape and dimensions of the hand

4.34
impostor
person who submits a biometric sample in either an intentional or inadvertent attempt to be authenticated as another person who is an enrolee

4.35
information security
preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

[ISO/IEC 17799:2005, 2.5]

4.36
initial enrolment
process of enrolling an individual's biometric data for the first time, such that the individual shall provide a means of authentication, such as a password or ID in order to establish or confirm an identity

NOTE See also **enrolment** (4.20) and **re-enrolment** (4.47).

4.37
integrity
property of safeguarding the accuracy and completeness of assets

[ISO/IEC 13335-1:2004, 2.15]

4.38
iris biometrics
biometric technology based on the distinctive characteristics of features found in the iris

4.39
match
process of comparing a match template against a previously stored reference template and scoring the degree of similarity or correlation between the two

4.40
match template
data, which represents the biometric measurement of a claimant, extracted from a claimant's biometric sample and used by a biometric system for comparison against one or more stored reference templates

4.41
multi-biometric authentication
biometric authentication using two or more different biometric types

NOTE For example, finger biometrics with iris biometrics or voice biometrics with face biometrics.

4.42
multi-factor authentication
authentication using two or more of the following factors:

— knowledge factor, "something an individual knows";

— possession factor, "something an individual has";

— biometric factor, "something an individual is or is able to do".

4.43
one-to-many
biometric identification

4.44
one-to-one
biometric verification

4.45
palm biometrics
biometric technology based on the distinctive characteristics of features found in the palm of the hand, inclusive of ridge/minutiae information and/or palm lines

4.46
raw biometric data
captured, unprocessed biometric data (e.g. fingerprint image or audio stream) from a sensor device, in digital form, suitable for subsequent processing to create a biometric sample or template

4.47
re-enrolment
process of enrolling an individual's biometric data where the same or other biometric data has been enrolled at least once

NOTE See also **enrolment** (4.20) and **initial enrolment** (4.36).

4.48
reference template
data, which represents the biometric measurement of an enrolee, extracted from an enrolee's biometric sample and typically stored and used by a biometric system for comparison against subsequently submitted match templates

4.49
registration
process in which a person proves his/her identity by presenting credentials to the biometric service provider before being allowed to enrol and is assigned an electronic identifier

4.50
retinal biometrics
biometric technology based on the distinctive characteristics of features found in the retina

4.51
risk management
coordinated activities to direct and control an organization with regard to risk

[ISO/IEC Guide 73:2002, 3.1.7]

4.52
score
numerical representation of the degree of similarity between two matched templates

NOTE The specific method by which a biometric score is generated, as well as the probability of its correctly indicating a true or false match, is generally propriety to each biometric vendor.

4.53
signature verification biometrics
biometric technology based on the distinctive characteristics of features found in the dynamics of a hand-written signature or other signed symbols

4.54
single-factor authentication
authentication using only one of the following factors:

— knowledge factor, "something an individual knows";

— possession factor, "something an individual has";

— biometric factor, "something an individual is".

4.55
template
data, which represents the biometric measurement of an individual, used by a biometric system to execute biometric matches

NOTE See **match template** (4.40) and **reference template** (4.48).

4.56
threshold
point above which the degree of similarity between two compared templates is sufficiently high to constitute a "match", and below which the degree of similarity between two compared templates is sufficiently low to constitute a "non-match"

NOTE Thresholds can often be adjusted at an administrative level to decrease the **False Match Rate** (4.27) or to decrease the **False Non-Match Rate** (4.28).

4.57
voice biometrics
biometric technology based on the distinctive characteristics of acoustic information found in the voice of a speaker

5 Symbols and abbreviated terms

ADF Application Data File

AES Advanced Encryption Standard

ATM Automated Teller Machine

BISMS Biometrics Information Security Management System

CA Certification Authority

CDF Common Data File

DEA Data Encryption Algorithm

DES Data Encryption Standard

DSV Dynamic Signature Verification

IC Integrated Circuit

ICC Integrated Circuit Card

ID Identification

KEK Key Encryption Key

PKI Public Key Infrastructure

6 Biometric technology overview

6.1 General

Biometric technology addresses the problems associated with confirming the identity of an individual for the purposes of financial transactions. The registration processes are a prerequisite for any formal biometric enrolment. Each person shall prove his/her identity to the biometric service provider using credentials before being allowed to enrol. This provides assurance that the biometric reference template is actually bound to the identity of the individual who has enrolled.

Biometric identification leverages the universally recognized fact that certain physiological or behavioural characteristics can reliably distinguish one person from another. Biometric technology includes both the automatic collection and the comparison of these characteristics. The digital representations of these characteristics are stored in an electronic medium and later used to confirm the identity of an individual. A typical authentication process utilizing biometric technology consists of the following basic steps:

a) capturing the biometric data;

b) evaluating the quality of the captured biometric data and recapturing it if necessary;

c) processing the captured biometric data; and

d) matching the processed biometric data with previously enrolled template(s) to determine if a match exists; this matching can be done for biometric verification or biometric identification.

There are three basic biometric processes, as described below.

— Enrolment is the process of collecting biometric samples from a person and the subsequent generation and storage of biometric reference templates associated with that person. Enrolment may entail the collection of other information about the individual, which links them to an organization, an account, or a set of privileges. In cases where duplicate enrolment is not allowed, enrolment may be preceded by a one-to-many comparison to make sure that the individual is not already in the database, perhaps under another name. If no match is found, the template and its associated information may be added to the individual's respective database entries. (See also 9.3.)

— Verification is a "one-to-one" comparison. This process entails the comparison of a match template generated from a newly captured sample with a previously generated reference template stored in a database or on an ID card. If the newly captured sample matches the previously generated template, the claim of identity is confirmed or verified.

— Identification is a "one-to-many" comparison. This process entails the comparison of a match template generated from a newly captured sample with all of the templates in the database. It is most often used to determine whether a person has previously enrolled in the system. Some systems use an external qualifier (e.g. telephone number) to narrow the search and subsequent identification to "one-to-few".

The advent of modern computing techniques is making the use of biometric technology for the purposes of identification a viable option in many areas. The characteristics, which can be used to represent an individual, include fingerprints, voiceprints, iris patterns, hand geometry, facial image, retinal patterns, and signature verification. These seem to be the current mainstream biometric technologies, and a brief description of these techniques is given in the following paragraphs. However, these are not the only biometric characteristics available today. Others include palm identification, head acoustics, wrist vein geometry, body odour, ear shape and keystroke dynamics. As technology advances, the list of viable characteristics may well expand.

6.2 Fingerprint biometrics

Friction ridges and valleys on an individual's fingertips are considered unique to that individual. For over one hundred years, law-enforcement agencies have been classifying fingerprint images into one of several main Henry types and sub-types (i.e. fingerprint patterns such as loops, whorls, and arches) as well as determining

identity by matching key points of ridge endings and bifurcations. Fingerprints appear unique for each finger on the same hand, as well as between identical twins.

Most modern fingerprint matching technology focuses on the unique points within the finger image, the minutiae. These minutiae are the points where individual friction ridges branch apart (bifurcate) or end. Imaging algorithms extract the minutiae and create a proprietary template that codes these minutiae. Pattern matching systems are based on overall ridge flow as opposed to minutiae. Systems can also analyse the finger's tiny sweat pores or the number of ridges between two key points (such as the core and the deltas). Fingerprint biometrics is capable of both verification and identification.

Conditions that may affect the prints of different individuals and reduce the quality of image capture include dirty, dry or cracked prints. Age, gender and body size are also found to have an impact on the quality of finger images, as well as the placement (rotation, shift and pressure) of the finger on the scanner. The public may see the historical use of fingerprinting by government law-enforcement organizations as a negative, although the capture of the fingerprint is generally regarded as non-invasive. Many fingerprint systems are being marketed by many companies, and significant advances have been made in the cost, size and speed of this technology in this competitive environment.

6.3 Voice biometrics

Voice biometrics (also called “speaker recognition”) dates back five decades. Early systems, pre-dating digital computing, used the output of several analogue filters, which were averaged over time for matching. Current digital speaker recognition systems model the acoustic features of speech that have been found to differ between individuals, yet remain stable over time for a single individual. These acoustic patterns reflect both anatomy (e.g. size and shape of the throat and mouth) and learned behavioural patterns (e.g. voice pitch, speaking style).

Speaker recognition systems can employ any of three styles of spoken input: text-dependent, text-prompted, and text-independent speech. Most speaker verification applications use text-dependent input, which involves selection and enrolment of one or more voice passwords. Text-prompted systems ask users to repeat specific words, phrases, or numbers. Text-prompted input is used where there is concern regarding tape-recorded impostors. Text-independent input is free-flowing speech.

Voice biometrics can be used for challenge-response type speaker verification, categorized in ISO/IEC 7816-11 as “dynamic biometric verification”. Applications of speaker identification by law-enforcement agencies typically use text-independent input because it does not require enrolment or input of specific words. Input speech is “digitized” to create a series of numbers. From these numbers, a reduced set of “features” is extracted mathematically. Voice biometrics is commonly used for verification, but rarely for identification.

Ambient noise levels can be an impediment to the collection of initial and subsequent voice samples. Voice changes due to ageing also need to be addressed by voice biometrics systems; adaptation can be employed to evolve the voice template along with changes in the verified speaker’s voice. Many companies market speaker recognition engines, often as part of large voice processing, control and switching systems. Capture of the biometrics is seen as non-invasive. The technology needs little additional hardware and can leverage existing microphones and voice-transmission technology. This provides functionality over long distances via ordinary telephones (wire line or wireless). However, performance is negatively affected by changes, between enrolment and sampling, in the microphone type or the transmission path.

6.4 Iris biometrics

The iris of the eye is the coloured portion of the eye surrounding the pupil. Iris imaging uses distinctive anatomical features such as corona, crypts, filaments, freckles, pits, radial furrows, and striations that make up the complex iris patterns. Iris biometrics entails illumination of the eye, capture of the resulting image, and location of distinctive features through specialized video cameras. Iris biometrics is capable of both verification and identification.

Iris images can be acquired automatically and with reasonably little effort from a distance of more than 0,33 m from the camera. Iris biometrics systems utilize automatic eye detection and advanced camera technology. Iris biometrics systems are much easier for the public to use than retinal systems.

The iris, being naturally well protected behind the cornea, appears to be stable over long periods (decades) according to medical literature. Iris imaging is not perceived as highly invasive, since the minimum distance, even for less-sophisticated iris identification systems, is between 75 mm and 100 mm (between 3 in and 4 in) from the sensor. Iris images are unaffected by common contact lenses but can be affected by “designer” contacts. Reflections caused by eyeglasses and sunglasses can also be a problem.

6.5 Retina biometrics

The retina is a structure in the interior of the eye. Retinal biometrics leverages the pattern of blood vessels on the retina. Retinal biometrics entails illumination of the eye, capture of the resulting image, and location of distinctive features through specialized video cameras.

Accurate retinal imaging requires almost perfect alignment of the eye with the scanning device, which requires the eye to be in close proximity to the scanner. This requires a great deal of effort and training, and can lead to high levels of enrolment and non-matching errors. At the same time, this contributes to the technology’s historically low false match rate. Retina biometrics is capable of both verification and identification.

Retinal patterns are highly distinctive, but the retinal structure may change during the life of the person. The requirement for close proximity to the retinal imager, as well as the beam of light shone into the eye, is perceived as unpleasant by many.

6.6 Face biometrics

The identification or verification of a person by their facial image is a common use of biometric technology. Most face biometrics solutions utilize images captured in the visible spectrum using standard camera technology. An alternative approach, known as facial thermography, uses an infrared camera to capture the unique heat emission patterns made by people’s faces.

The visible light systems extract features from captured facial image(s). Approaches to modelling facial images in the visible spectrum include Principal Component Analysis, Local Feature Analysis, neural networks, elastic graph theory, and multi-resolution analysis. Principal Component Analysis, or the “Eigenface” technique, models a particular face as a weighted combination of other “basis” faces. The set of basis faces is constructed by collecting many face images, then mathematically determining the set that optimally models them all. Local Feature Analysis locates and maps key feature points of the face, similar to fingerprint minutiae extraction. Face biometrics is capable of both verification and identification.

Challenges for facial identification in the visual spectrum include reducing the impact of changes in pose, expression, hairstyle, facial hair, makeup and lighting. Some facial biometrics systems may require a stationary or posed user in order to capture the image, though some systems use motion imagery. All systems process the images to detect a person's head and locate the face automatically. Major advantages of facial identification are that it is non-intrusive, hands-free, continuous and accepted by most users. In the visible spectrum, an untrained operator can also assist the system when identification is uncertain.

6.7 Hand geometry biometrics

Hand geometry has been used for physical access control and time and attendance systems for over two decades. Hand geometry systems use a camera array to scan the shape of the hand from different directions. Sensors determine when the hand is in correct alignment.

Hand geometry uses the dimensions and shape of the hand, fingers and knuckles to form an identifying series of numbers. This template is one of the smallest, requiring only 9 bytes for storage. Operation requires use of a token or a PIN, as the technology operates only in verification mode.

Users with arthritis and rheumatism, as well as those with missing fingers or excessively large hands, could have difficulties. Hand geometry is convenient to use and requires little training. The process of using a hand scanner is perceived as non-invasive and acceptable to the public. A related biometric technology is finger geometry, scanning and extracting features only from a few fingers, as opposed to the entire hand.

6.8 Signature biometrics

Hand-written signatures can be identified from the way the signature looks or the way the hand of the signer moves during the signing. Signature recognition based upon the biometric characteristics related to movement of the hand is referred to as Dynamic Signature Verification (DSV). These systems capture the way we sign our names, utilizing features such as the angle of the pen, the time to complete the signature, the acceleration and velocity of the pen, the pressure while signing, and how often the pen is lifted from the page. Electronic pens, tablets or both can be used to capture the signature biometrics. Digitized signatures are generally used in verification as opposed to identification mode.

The sensing equipment can be highly sensitive and prone to wear and tear over time and therefore may prove to be maintenance intensive. Since DSV is not based on a static image, forgery is very difficult. Several companies market DSV systems, and public acceptance of signature verification is high since hand-written signatures are currently one of the most accepted means of asserting identity.

6.9 Vein biometrics

Vein authentication uses the blood vessel pattern of the veins in the subcutaneous tissue of the human body to discriminate between individuals. A vein pattern is read using near-infrared light. When a hypodermic vein is irradiated with near-infrared light, the reduced haemoglobin contained in the vein absorbs near-infrared light and the hypodermic vein creates a shadow on an image. The shaded part is extracted from the captured image as the blood vessel pattern of the vein using image processing technology. The resulting blood vessel pattern is compared using vessel structure features such as directions and bifurcations, or using the pattern itself.

In practical terms, a blood vessel pattern of a hand, such as that of a palm, the back of a hand, or a finger, are used for authentication because such parts of the hand are easy to present to a sensor, and various products have been developed for such hand parts. Because the products have many functions to support and guide users in proper usage, such as detection of hand position based on image processing technology, high usability is achieved and the accuracy of authentication is very stable. Since the blood vessel pattern used by vein authentication is information that is hidden in a body, it is generally not known by others in typical usage environments, and therefore forgery is very difficult.

Many products for vein authentication of a palm, a finger or the back of a hand are already employed by ATMs of multiple financial service companies[1)] and as access control systems.

7 Technological considerations

7.1 Biometric system properties

For applications in the financial services, the following biometric system properties should be considered:

— public acceptance and policy considerations,

— resistance to fraud (see Annex C for further information),

— universality of the chosen biometric characteristic,

— uniqueness of the chosen biometric characteristic,

— accuracy of the biometric system,

— stability of the biometric characteristic,

1) In Japan, since December 2005, the vein authentication technology of a palm or a finger has been employed on ATMs of financial institutions, including some major banks and several regional banks.

— template storage requirements (i.e. template size),

— system validation ability,

— speed of comparison between the claimant sample and the enrolled template, and

— environmental and interface factors.

7.2 Universality

In order for a biometric system to be of value, nearly all people in the target population should be able to successfully use that system. A small number of exceptions may be possible, providing that an alternative method is available to authenticate or recognize those people who are unable to use the biometric system. Care shall be taken in the design and administration of that alternative method, so that it does not become a point of weakness or vulnerability in the system.

While vendor claims may be misleading, measurable error rates are associated with all biometric technologies. Most of these errors come from two classes of users:

a) individuals who cannot provide the biometric feature required by the sensor;

b) individuals who are unable to give consistent or high-quality samples, resulting in false non-matches.

Such individuals are referred to as “outliers” in the biometric industry. Experience suggests that they either do not have a repeatable biometric measurement, or chronically experience a “failure to acquire” system error.

The percentage of outliers differs by technology and vendor. The use of multiple biometrics is a potential solution to the outlier problem, since the overall probability of an individual being an outlier across two or more biometrics is smaller than the probability for a single biometrics system. Alternatively, other identification factors can be used as a fall-back, such as the PIN, for users not possessing the biometric feature of interest.

While alternative methods are often necessary to provide for universal authentication, these alternatives might undermine overall system security. The use of passwords as a fall-back, for example, may provide incentive for an attacker purposely to fail his/her biometric match in order to access a less robust authentication mechanism.

7.3 Distinctiveness

Distinctiveness describes how reliably the biometric characteristic is measurably different for each individual in the population. In an ideal system, there would be no ambiguity; the measured biometric feature from each individual in the population would be different from that of every other individual. This can only occur if the feature itself is unique to each individual, who at least requires that the number of permutations be large enough[2)] to accommodate the population, and if the biometric system can measure the feature with enough detail and repeatability to produce a unique electronic analogue of that feature.

Experience and studies provide some idea of the distinctiveness of most of the popular biometric characteristics. For example, fingerprints have been studied for many years, and there is a consensus that fingerprint patterns are unique among individuals. More recent studies suggest that iris and retinal patterns are also unique. In contrast, as an example, the facial features of identical twins may not be unique. Therefore, the properties of each biometric technology are different and should be evaluated to determine which provide the level of distinctiveness required for a given application.

2) A template size of at least $2^{32} \approx 4$ billion permutations would theoretically accommodate the earth’s population.

7.4 Accuracy

Biometric techniques are subject to statistical error, such that impostors may be granted access to protected resources that legitimate users are prevented from accessing. The probability that a biometric system will fail to reject an impostor in a 1:1 verification attempt, or will incorrectly identify an individual in a 1:N identification attempt, is the system's False Match Rate (FMR). The probability that a biometric system will fail to verify an enrolled individual in a legitimate 1:1 verification attempt, or will fail to identify an enrolled individual in a 1:N identification attempt, is the system's False Non-Match Rate (FNMR). The techniques discussed in this International Standard are all prone to some level of false matching and false non-matching.

A system's FMR and FNMR are inversely related, such that adjusting biometric system security settings to reduce the FMR results in an increased FNMR, and vice versa. Two biometric templates are determined to "match" or "non-match" based on a comparison between

a) the score that results from the match attempt, and

b) the system's match threshold.

Strictly speaking, a system's FMR and FNMR are not "adjusted" by an administrator. Instead, the administrator adjusts a single threshold above which two templates are declared a match and below which two templates are declared a non-match. It is therefore impossible to adjust one error rate without impacting the other. Both error rates are a function of a single threshold.

A deployer's operating environment will generally dictate which of the error types should be limited, at the expense of potentially increasing the other error type. For example, a high-security facility will usually minimize the system FMR at the expense of increasing the system FNMR, whereas a customer service facility will usually minimize the FNMR at the risk of increasing the FMR.

Because of the relationship between FMR and FNMR, a system's FMR is only meaningful when provided in conjunction with its FNMR, and vice versa. Any system can claim a FMR of 0 % by simply rejecting every attempt, or a FNMR of 0 % by accepting every attempt. An ideal biometric system will offer simultaneously low FMR and FNMR.

The point at which a biometric system's FMR equals its FNMR is the Equal Error Rate (EER) or Crossover Error Rate.

NOTE 1 Some biometric systems do not allow threshold adjustments and do not use EER (see Reference [16]).

This rate provides a useful snapshot of overall matching accuracy, as a system with a low EER is more likely to operate accurately than one with a high EER. However, few deployers will actually implement a system in which false match and false non-match rates are identical. Most will choose to emphasize either convenience or security based on their operating environment. When comparing the accuracy of different biometric technologies, deployers should evaluate what levels of false matching *and* false non-matching are acceptable, and then determine what technology or technologies are capable of providing the required level of performance for both metrics.

NOTE 2 FMR and FNMR cannot be used alone to determine overall system accuracy: a system's failure-to-enrol rate, or the percentage of users unable to provide sufficiently distinctive or replicable biometric data for enrolment, is a critical element not captured by matching error rates.

Capabilities of certain biometrics allow them to be deployed for the purposes of identification, or "single-factor authentication." Single-factor authentication does not require that the individual provide a unique identifier in the form of a card, token or username, with major implications for system security and convenience. These issues are discussed further in Clause C.8.

Error rates can be generated through independent testing or through vendor-provided testing. In either case, published error rates may only be reflective of operation in a strictly controlled test environment, and may not be indicative of performance in a deployment environment, subject to decision policy. Decision policy is the logic through which a biometric system provides match/no match decisions, inclusive of implementation-

specific factors. In order to gauge a biometric system's real-world performance, the system's error rates should be evaluated in conjunction with its decision policy.

One of the major factors in a biometric system's decision policy is the number of attempts permitted for verification or identification. In biometric systems, an "attempt" is the act of an individual providing a usable biometric sample (a single fingerprint, voice pattern or iris image) to a biometric system.

NOTE 3 In certain biometric systems, an attempt consists of comparison of multiple biometric samples acquired over a brief period. Facial-scan systems can acquire multiple facial images over the period of several seconds, generate match templates with each image, and declare a match if any of the acquired images exceed the required threshold. In this case, the "attempt" can continue until the system times out after a certain duration.

Most biometric systems allow an individual multiple attempts to be verified or identified before timing out or preventing further attempts, e.g. an individual may be permitted to place a fingerprint on a scanner up to three times in order to verify against his or her enrolment. A common decision policy is to grant access if any of the three attempts is successful. Under this decision policy, the system's effective FNMR may be lower than its single-attempt FNMR, i.e. the user is more likely to be verified at some point in the verification sequence given the additional attempts. However, this decision policy increases a system's effective FMR, as an impostor may have multiple chances to provide biometric data in an effort to defeat the system.

Another factor in a biometric system's decision policy is the number of enrolment templates associated with a given user. Many biometric systems acquire two enrolment templates from a user, such as from the right and left fingerprints, in order to mitigate the impact of injuries and to reduce incidents of false non-matching of authorized users. If a system allows a user to verify against either of his or her enrolled templates, the system's effective FNMR may be lower than its single-attempt FNMR, i.e. the user is more likely to be verified against one of his or her enrolled templates. However, this decision policy increases a system's effective FMR, as an impostor may have multiple chances to match against enrolled biometric data.

Other decision policy elements that can impact a system's accuracy include the following:

— the number of distinct biometric samples (e.g. different fingerprints) enrolled per claimant;

— the number of biometric technologies (e.g. fingerprint, voice) in which the claimant is enrolled;

— the use of internal controls in the matching process to detect like or non-like biometric samples, e.g. comparing templates derived from two subsequent match attempts to determine if the individual is placing different fingers in an attempt to falsely match;

— the use of serial, parallel, weighted or fusion decision models in biometric systems that utilize more than one reference template in the match process for a given user (e.g. multiple-biometric systems, as well as systems in which reference templates are created and stored from multiple fingerprints).

Secure biometric system implementation requires that deployers evaluate the impact of decision policy on the FMR and FNMR in order to determine how well their system will perform when deployed. A biometric system's *effective* FMR and its *effective* FNMR represent its error rates with all elements of a deployer's decision policy taken into consideration. The overall decision policy (including thresholds) is set according to the needs of the organization, based upon a risk assessment.

7.5 Performance evaluation

When evaluating the performance of biometric products, it is important to understand the different factors that can influence the measured FMR and FNMR (see Clause C.5 for further information). Reported performance numbers for different products may have been measured under different circumstances, and thus they cannot be directly compared. The factors below should be taken into consideration.

— **Who were the users in the test, and how were they selected?** Ideally, the users should be chosen at random from a population that is representative of the people who will use the system in the real application environment. In some cases, however, the test users do not accurately represent the real-world users. If the test group comes from the vendor's employee population, they may differ significantly

from the target users in terms of educational level, cultural background and other factors that can influence the performance with the chosen biometric system.

— **How were the test users trained?** The training for the testers should be as close as possible to that anticipated for users of the real system. The testers are often more carefully coached than the real users will be, either intentionally (to improve measured performance) or unintentionally (due to the enthusiasm of the vendor for his/her own product). A related issue is how long the test group used the system before the formal measurement period began. Typically, performance will be lower when the users begin using the system, and will rise and stabilize as they get accustomed to it.

— **What thresholds were used during the test?** Because false match and false non-match rates between samples and stored templates are dependent upon threshold settings, system FMR and FNMR encountered during testing will similarly be affected by the chosen thresholds. FMR and FNMR should be reported together at a common threshold.

— **How many attempts are allowed per verification session?** Most measurements are based on single attempts to verify identity with the biometric system. Some, however, are based on the overall results of a "session" in which the user is permitted several tries. The system decision policy, including the number of allowed attempts per verification session, will allow for various system FNMR and FMR to result from the same single-comparison false match and false non-match rates. Clearly, the FNMR will be lower and the FMR will be higher if the user is given more than one try at verification.

— **Were problem users systematically eliminated from the test?** It is common for some users to experience a "failure to acquire" during enrolment. This is often called a "failure to enrol." If enrolment requirements are placed high, problem users can be systematically eliminated from the test at enrolment. Of course, eliminating problem users will lower measured false non-match rates later in the test and result in better system performance.

— **What is the motivation to succeed at impersonating another user?** In some biometric systems, a user has a better chance of achieving a False Match if motivated to do so, e.g. the user may have a better chance of impersonating another user's signature, voice or keyboard dynamics if he/she is trying very hard to do so. Measurements of FMR can therefore be influenced by the testing method. In some tests, users are directly rewarded if they can successfully forge another user's identity. In other tests, there is no reward. Finally, some False Match tests are carried out simply by cross-testing a database of collected biometric data, in order to see if any of the samples can be verified as a match to any other sample which came from a different person.

— **How did the test conditions compare with those for the real application?** Did the test subjects use the system while seated in a comfortable room? If so, will the real application involve verification outdoors in potentially bad weather or in the dark? Will users have to verify while standing? Will they be clothed differently in some way, such as in heavy winter coats, that might in some way affect verification performance? These are important factors in determining whether the test results will accurately match those obtained in the real world.

— **Was the test organization impartial?** Some tests are run by independent organizations. Others are run by the vendor who sells the biometric product or by some other organization with a stake in making the product look good, or perhaps bad. An independent test organization is more likely to test products in a way that is unbiased, rather than performing the test under the best-case circumstances for that particular product or technology.

— **Has there been a change in the product since the test was performed?** Products constantly change. The test results you see may have been measured with a version of the product that differs from what is available today. Frequently this means that performance will improve, or that performance will be the same, but with a reduction in cost. Although less likely, it is also possible, however, that changes in hardware or software can reduce performance.

It is important to understand these issues before choosing a biometric product for your application. Biometric performance depends upon the precise conditions of the installation and the users, can be difficult to measure, and may be subject to much more variation than performance measurements of other products, e.g. it is much

easier to measure the number of transactions per hour that a computer system can support, or the access time for a disk drive. When selecting a biometric system, be sure you understand how performance was measured, and how that method relates to the way the system will be used in your application.

There is no substitute for testing in an environment that replicates the actual application environment. Biometrics vendors cannot replicate the conditions of all potential customers, and it should be expected that the vendors have a natural bias to portray their products favourably. Thus, the customer should ultimately test a system to understand how it would perform under their specific conditions.

7.6 Interoperability

Biometric templates issued by financial institutions should be used in a manner that is consistent with the biometric information management policy and practices of the institution.

8 Basic principles of biometric architectures

8.1 Biometric system model

All biometric systems have the common function of recognizing individuals by matching some personal physical characteristic with the stored information about that same characteristic. The methods, applications, and implementations of biometric systems vary widely, and in the context of biometric standards it is important to understand the biometric system model and basic approaches that are common to most applications.

All biometric systems are composed of the following subsystems:

— data collection;

— signal processing (feature extraction);

— matching;

— storage;

— decision;

— transmission.

NOTE For dynamic biometric verification, a “challenge presentation” subsystem is used.

Transmission is the movement of biometric data between two components that are not physically collocated within the same tamper-resistant security module. Transmission can occur between any two components, depending on the specific vendor implementation, and may not exist in some systems.

Any biometric system operates in an environmental context, which shall be taken into consideration when evaluating security aspects of the system. Subclause 11.2 illustrates the two major domains of any biometric system, i.e.

a) the physical domain, in which resides the subject to be verified or identified, and

b) the logical domain, in which the computational processing of the biometric data takes place.

The data collection device provides the bridge from the physical domain to the electronic processing domain.

Furthermore, some biometric technologies may have low enough crossover error rates to be suitable for large-scale single-factor authentication. Single-factor authentication has major implications from a security and convenience standpoint (see C.4.3).

Each of the major components is described in more detail in 8.2 and 8.3.

8.2 Data collection subsystem

The data collection subsystem contains the input device or sensor that reads the biometric information from the user and converts it to a form suitable for processing by the remainder of the biometric system.

It is the link from the physical domain to the logical domain. Examples include a variety of transducers, such as a video camera, a fingerprint scanner, a special signature pen or tablet, a microphone and other input devices specific to the chosen biometric characteristic to be measured. The output of this subsystem is raw biometric data, which may be processed locally or may be transmitted to another location.

To recognize a user successfully, the sampled biometric characteristic shall always be similar to the user's enrolled template to which it is compared. This imposes requirements on the design of the data collection sensor, and may impose training requirements for the users. Some characteristics change slowly over time, and biometric systems may employ adaptation in order to keep the stored reference template in step with those changes (see Clause C.7 for further information). Re-enrolment of a user's record by provision of a new enrolment template for that individual on an overt basis (usually initiated by the application) may also be performed.

In use, the biometric feature is presented to a sensor, which converts the feature into an electronic signal suitable for further processing. All sensors in a given system shall be similar enough that a feature measured by one sensor will closely match the same feature measured at other sensors, so that the user can be recognized equally well at any location. This includes the requirement that the sensors shall be consistent over time, either by virtue of inherent stability, or through use of automatic calibration. Some systems include automatic quality control features in the sensors or signal processing paths, and these systems can detect poor-quality signals that might otherwise increase the false non-match rate.

The performance and output of the data collection subsystem is impacted by changes in any of the following:

— the underlying biometric pattern;

— the presentation of the pattern to the sensor;

— the performance of the sensor itself; and

— the surrounding environmental conditions (e.g. lighting, background noise).

8.3 Transmission subsystem

The transmission subsystem provides the ability to send information between the data collection, signal processing, decision, storage and matching components. The connectivity provided may be point-to-point or networked, allowing one system to connect to multiple subsystems.

The system components that are communicating may be local or remote to each other, within the same secure envelope, e.g. tamper-resistant security module (see Annex D), or in separate secure envelopes. The transmission subsystem may not necessarily be monolithic, but may actually be composed of a number of different transmission mediums such as Ethernet, leased line, wireless, etc. These media may or may not provide security services, such as data confidentiality, data integrity and authentication of origin between the connected subsystems.

8.4 Signal processing subsystem

The signal processing subsystem receives the raw biometric data from the data collection subsystem, and transforms that data into the form required by the matching subsystem. The exact processing that takes place varies for different biometric characteristics that are measured, and for different vendors' biometric systems.

The system may perform a quality analysis on the input signal to determine it if is satisfactory for use. If the signal fails the quality tests, it is rejected and, depending upon the enrolment policy, the user may need to supply another presentation of the biometrics.

Filtering may be applied to the signal in order to remove noise or other information that is extraneous to the matching process. This may include, for example, removing high- or low-frequency data from the signal.

The signal may be normalized in some way, e.g. the voltage level of an analogue signal may be adjusted to be within accepted limits, and a video image may be adjusted to standard levels of brightness and contrast.

Once the input signal has been satisfactorily adjusted, it will be analysed to extract features that are used by the matching subsystem. Some biometric systems compare raw data, and this step is not required. Feature extraction is performed to transform the raw data into a set of characteristics that will represent it to the matching process. The types of features vary with different biometric techniques. A fingerprint system typically looks for physical characteristics such as branch and end points of the ridges; the system would extract a set of values where each one contained an indication of the type of feature found, the coordinates where it was found on the finger, and the angle of the ridge at that point. A voice biometrics system, on the other hand, might record such things as the energy in the different frequency components of the signal. The result of feature extraction is data that is much smaller and simpler to use than the original raw data signal.

Typically, once raw biometric data has been processed, it is not feasible to reconstruct the raw data from the processed sample or template.

8.5 Matching subsystem

The matching subsystem receives the processed biometric data from the signal processing subsystem and compares it with the biometric template from the storage subsystem. The matching subsystem has a key role in the biometric architecture.

The matcher is composed of the following sub-components:

— sequencer,

— match-scoring module, and

— adaptation module (optional).

The sequencer handles the sequencing of the activation of the match and adaptation modules and the transfer of matching scores to the decision subsystem to perform different functions.

The match-scoring module measures the similarity of a claimant sample with a template. Each comparison of a sample with a particular template yields a *score*, which is a numeric value indicating how closely the sample and template match. The method of computing the score differs among biometric technologies, but typical methods include distance metrics (see Reference [14]), probabilistic measures and normalized correlation. Ultimately, the score should be related to a given confidence of positive identification for the biometric subject, which can be factored into the overall business rules and risk policy for the financial institution authorization policy. This confidence value will be considered by the decision subsystem in implementing the administrator's authorization policy for the transaction, employing the biometrics as an authentication factor.

In the simplest form of verification, the sequencer provides the claimant sample and enrolment templates to the matcher, and passes this result to a decision subsystem, which returns a binary decision regarding whether the claimant is who he/she claims to be.

However, the interplay between the match-scoring module and the sequencer may be quite involved in systems that carry out identification, e.g. in an identification mode, the sequencer may take into account additional indexing or binning information about the claimant sample, in order to focus the computations of the matcher onto templates that are most likely to match the claimant sample. Feedback from the decision subsystem might also be invoked during the identification process to guide the search towards the likeliest match enrolment templates.

Some systems use the sequencer and matcher, with feedback from the decision subsystem to perform adaptation, to keep the enrolment templates up to date with gradually changing biometric characteristics for the user (see also Clause C.7).

An application program (e.g. a transaction authorization system) uses the decision process result. It may be used in various ways, depending on the purpose of that application program. The actions at this level are not a part of the decision subsystem itself, but are a part of that application program. Most often, the application program will grant the user some level of privilege if the decision indicates a match with the template belonging to the claimed identity. In other systems, however, the goal is to verify that the user is *not* in the template database, e.g. when a financial services employee attempts to enrol in a benefits program in which he/she is already a member, thus avoiding duplicate records. In this case, the application program will "accept" the user only if the decision subsystem indicates that there are *no* matches between the user's sample and any template in the current database.

8.6 Decision subsystem

The decision subsystem receives a score from the matching subsystem and, using a confidence value based on business risks and risk policy, interprets the results of the score.

The decision subsystem returns a binary yes or no regarding the positive identification of the claimant, based on the score computed by the pattern matching subsystem. In the most common case, the decision is based on a single threshold. If the score is above the threshold, the system concludes that the user is indeed the individual owning the template. If not, the system indicates that the user is *not* that individual. In more complicated cases, the decision subsystem may require matches in one out of three submitted samples, or in higher security scenarios, for two out of three multi-biometric characteristics.

An application program (e.g. a transaction authorization system) uses this decision process result in various ways, depending on the purpose of that application program. The actions at this level are not a part of the decision subsystem itself, but are a part of that application program. Most often, the application program will grant the user some level of privilege if the decision indicates a match with the template belonging to the claimed identity. In other systems, however, the goal is to verify that the user is *not* in the template database, e.g. when an individual attempts to enrol in a benefits program. In this case, the application program will "accept" the user only if the decision subsystem indicates that there are *no* matches between the user's sample and any template in the current database.

8.7 Storage subsystem

The storage subsystem maintains the templates for the enrolled users. It provides for the addition, deletion and retrieval of an enrolled template (or templates), as needed by the matching subsystem. The storage subsystem may contain a single template for a single user, or thousands of templates, depending on the system architecture and intended function.

For example, templates may be stored in:

— physically protected storage within the biometric device,

— a conventional database on a computer system, or

— portable tokens, such as smart cards.

The data stored for each user always includes that user's template, but it may also include other information. It may also contain data that is completely unrelated to the biometric system, if the same database is used for purposes other than user authentication.

8.8 Portable tokens

When portable tokens, such as smart cards, are used in conjunction with biometrics, then any (or none) of the biometric subsystems described in this clause may reside within the token. The most common card deployment models are (from lowest to highest token cost):

— "identity on card", in which the token contains no biometric template or subsystem, and is used with an external biometric verification system to provide two-factor authentication;

— “off-card matching”, in which the biometric storage subsystem contains one or more reference templates stored in the token, and where all other biometric subsystems are external to the token;

— “on-card matching”, in which the matching and storage subsystems are in the token and data collection is external to the token; the signal processing or decision subsystems may be in or external to the token;

— “self-contained card”, in which all the biometric subsystems (including the sensor) are in the token, and verification can be performed without any external system interaction.

The “identity on card” model does not differ significantly from a cardless biometric implementation with a central database. The token contains a unique value that has been associated with the reference template of the individual. The individual possessing the token provides this value to claim an identity. This value is used to simplify location of the individual's reference template in a template database, without the need to search by biometric matching. Together, the token and biometrics provide two-factor authentication. This model minimizes the risk of a cardless implementation and token cost, but does not provide the benefits of decentralized template management.

The other three models remove the need for centralized template management and database support by housing the reference template in the token. However, decentralized template storage increases the risk of alteration or substitution of the template by an attacker.

The additional risks and confidentiality concerns that come with publicly sharing reference templates apply to the “off-card matching” model. In this model, the token shall emit the individual's reference template to an external verification system. This exposure makes the template vulnerable to theft by “skimming” or other attacks.

The “on-card matching” model avoids the risks of template exposure associated with the “off-card matching” model. This model does not emit the reference template to external systems. Instead, the token receives biometric samples or matching templates, and emits only biometric match results and decision control information.

The “self-contained card” model largely avoids tampering and skimming risks, since the token does not transfer the reference template across an interface to external systems during verification. However, self-contained tokens are prone to frequent sensor failure due to rough handling and storage of tokens, poor-quality sampling due to dirty or damaged sensors, and higher failure rates (both FMR and FNMR) due to poor sample quality and limited processing power.

9 Management and security requirements

9.1 Basic applications

There are three basic applications in a biometric system:

a) enrolment (creating the biometric template used in later verification or identification functions),

b) verification (the user claims an identity and offers a biometrics sample to prove that identity), and

c) identification (the system searches a database looking for a match with the offered biometrics).

9.2 Core security requirements

This subclause defines the requirements for managing and securing biometric information for each application, for the transmission and storage of biometric information, and for maintaining the event journal for purposes of compliance and audit. The core requirements that apply to all applications and environments wherever biometric information is used are the following:

a) mechanisms shall be in place to maintain the integrity of biometric data and authentication results between any two components;

b) mechanisms shall be in place to mutually authenticate the source and destination of the biometric data and authentication results, between the sender and receiver component;

c) if desired, mechanisms may be in place to ensure the confidentiality of the biometric data between any two components and within any component.

Each of these biometric applications is comprised of the components described in 8.1.

9.3 Enrolment

9.3.1 General

Enrolment is the process through which the user's identity (either as claimed by the user, or known through a prior business relationship, or as verified through collateral documentation, such as a passport, national identification card, driving licence or birth certificate) is bound with biometric template data and entered into the system database or an appropriate portable token. The bound information is discretionary to the organizations and may be the hash of some representation of one or more collateral documents.

NOTE There can also be a need to establish the validity of a business and the authority of individuals to perform transactions on its behalf. Consequently, financial institutions typically review articles of incorporation, business credit reports, board resolutions identifying officers and authorized signers, and other business credentials as part of the identity verification process.

The enrolment process consists of the initial biometric data being captured during data collection. Signal processing generates a template, and the template is placed securely into storage. Optionally, the sample data may be forwarded to a matching subsystem for identification to determine whether the enrolee has already been registered. The matching subsystem component would retrieve as many templates as necessary. Other enrolment variations may also be implemented, such as storing the initial data from numerous enrolees and forwarding the data for template generation in a batch mode.

9.3.2 Initial enrolment

Initial enrolment is the first time an enrolee's biometric data is captured for creating the biometric template. In addition to the core requirements in 9.2, the following requirements for enrolment apply.

a) Mechanisms and procedures shall be in place to ensure the enroller has the proper permissions (e.g. access control for the enrolment function) to enrol the enrolee.

b) Mechanisms and procedures shall be in place to verify the identity of the enrolee before his/her biometric data is collected. Collateral material, such as photo identification, may be useful.

c) Mechanisms and procedures shall be in place to ensure a binding of the biometric information to the enrolee, such that the biometric information captured during the enrolment process belongs to the enrolee, using:

   — physical protection, such as a token where no transmission is involved and all components reside within the same tamper-resistant unit, as described in ISO/IEC 19790;

NOTE ISO 13491-1 contains similar materials and has particular relevance for the financial services.

   — manual procedures, such as reference numbers where the biometric information is traceable to existing enrolee information.

d) Each biometric component shall at least meet the minimum security level of the application system, and shall meet or exceed the equivalence of Level 2 physical security requirements in a controlled

environment and at least Level 3 physical security requirements in an uncontrolled environment, as specified in Annex D.

e) The integrity and authenticity of biometric data shall be maintained throughout its life cycle, beginning with the enrolment process. Furthermore, the issuance date of the template shall be captured and its integrity maintained throughout the biometric life cycle.

9.3.3 Re-enrolment

Re-enrolment is for subsequent updates to the biometric template, such as

— updating the biometric data (e.g. per a security policy addressing the biometric life cycle),

— changing biometric sources (e.g. use a different finger),

— changing biometric technology (e.g. switch from finger image to iris scanning), and

— changing biometric devices when they are not interoperable (e.g. move from fingerprint sensor A to fingerprint sensor B).

The security requirements for re-enrolment are the same as for enrolment. Note that the requirements for authenticating the enrolee can be satisfied by the re-enrolment process in any one of the following ways.

a) Use the original credential material and do not use the existing biometric template. Depending upon the reliability and availability of the existing biometric template and technology, this may provide a sufficient level of assurance.

b) Use the biometric template and do not use the existing collateral material. Depending upon the reliability and availability of the existing biometric template and technology, this may provide a higher level of assurance than relying solely on the collateral material.

c) Use both the biometric template and the collateral material. This provides a higher level of assurance than relying solely upon either the collateral material or the biometric template.

Some biometric technologies and authentication systems do not require updating the biometric data within the template, such that the previous template and the new template are essentially equivalent except for the issuance date (see also Clause C.7 for information about the security risk differences between updates and adaptation). Termination of the previous template is required and archiving may be required when re-enrolment occurs.

9.4 Verification

In the verification process, the user presents a claimed identity and presents the required biometric characteristic for measurement. The system retrieves the user's template, usually based on the claimed identity, and compares that template to the features derived from the measured characteristic in order to determine whether that user is in fact the owner of the claimed identity.

The verification process consists of the raw biometric data being captured in the data collection subsystem, the sample biometric features being generated by the signal processing subsystem, a specific biometric template being retrieved from storage, and the comparison of sample features to the template being made by the matching subsystem. The resulting score from matching might be forwarded to a decision process or optionally to the application, where the score is evaluated and a Boolean "Yes/No" is determined.

If the decision process were separate from the application, then the application would only receive the Boolean result. Although adaptation of the biometric template is performed in the matching subsystem, the judgement as to whether or not to accept the adaptation and update the enrolled template in storage may also involve the decision subsystem (see also Clause C.7).

The biometric data includes the raw biometric data, the processed sample data, and the biometric template. In addition to the core requirements in 9.2, the following requirements, recommendations and other considerations for verification apply.

a) The matching subsystem shall be performed within the physical confinement of a tamper-resistant security module meeting at least the Level 3 requirements in Annex D, or in a physical environment that provides a comparable level of security, as determined by the institution. These requirements can be met by various architectures not related to “on-card matching”.

b) Error rates differ among various biometrics. Due to the variable nature of physical characteristics and human behaviour, it is difficult to arrive at a consistent, common biometric error rate. The variables involved in determining an accurate error rate include issues relating to correct use of the biometrics, environmental conditions and user training/acceptance. This International Standard assumes that the biometrics is presented under ideal conditions.

c) For verification systems, the corresponding false non-match rate of the biometrics shall be consistent with requirements for convenient operations, and shall not exceed 10^{-2} (see Clause C.6).

d) Enrolment error rates shall also be taken into consideration, so as not to lead to significant customer service issues.

When evaluating overall system security, deployers shall bear in mind the decision policy issues addressed in 7.4. There is a critical difference between the single-attempt False Match Rate and False Non-Match Rate required in this International Standard and the effective False Match Rate and False Non-Match Rate. A system’s effective False Match Rate and False Non-Match Rate represent its error rates with all elements of a deployer’s decision policy taken into consideration.

For example, a system whose decision policy allows for multiple attempts against multiple enrolment templates for a given user will have a higher effective False Match Rate than its single-attempt False Match Rate. This is due to the increased likelihood of an impostor's template matching an enrolled template at some point in the verification process. Consequently, a biometrics may have, as an example, an FMR of 10^{-4} but be susceptible to higher real-world false match rates due to the manner in which it is implemented.

Due to the nature of biometrics, users shall carefully balance security risks, prudent business practices, and application specifics when determining the specific accuracy requirements for the systems to be implemented, and should additionally work with vendors to ensure that optimum testing procedures are followed.

9.5 Identification

The identification process is used to recognize an individual within a large group, based on a set of biometric templates. The user presents the required biometric characteristic, and the system compares that biometric data to a set of templates in the system database. In the simplest case, the system stops checking templates as soon as the first one is found. It returns the identity associated with that matching template as the identity of the user.

Variations that are more complex are also possible, e.g. the system may compare the user’s biometric sample to all templates in the system data set, in order to verify that the user does not match more than one. In the case of multiple matches, the system may identify the user as the owner of the template with the closest correspondence to the sample data, or it may use other approaches.

The identification process consists of the raw biometric data being captured in data collection, the sample biometric features being generated by signal processing, multiple biometric templates being retrieved from storage, and multiple sample-template comparisons being made by a matching subsystem. The resulting candidate list from matching might be forwarded to a decision process or optionally to the application, where the candidate list is evaluated and an assumed identity is determined. If the decision process were separate from the application, then the application would only receive the result.

The security requirements for identification are the same as in 9.4, with the additional consideration for identification: this International Standard recommends that significantly lower system False Match and False

Non-Match Rates should be employed for systems that employ a single biometrics for authentication as opposed to multi-factor authentication. Determining the proper false non-match and false match rates in single-factor authentication systems is contingent on the number of identification attempts, the size of the database against which attempts are executed, and the overall decision policy (see also Clause C.8).

In order to ensure the highest possible system accuracy in an identification system (especially in the case of large databases), it may be necessary to utilize high-quality sensors (typically higher than needed for verification systems) to generate high-quality sample data. Higher threshold settings may also be necessary.

If the biometric system is being used to prohibit enrolment by certain individuals, it is critical that the enrolment be of sufficient quality to enable an accurate search. Low-quality enrolment is more likely to allow the individual to be registered in the system on multiple occasions.

9.6 Transmission and storage

9.6.1 General

Transmission is the process subsequent to enrolment and prior to verification or identification, where the biometric template is transferred to its storage location. Subclause 9.1 describes the relationship between the various subsystems.

The template is created in the enrolment process and transferred to one or more storage sites that are accessed by the verification and identification applications. The storage sites can be a central database, local storage or a removable token, such as a smart card.

It is important that templates reflect a common schema, so that the template created by one financial services institution can be used by another. A common standardized schema facilitates application solutions by multiple vendors, which can help to increase competition and drive down costs to customers.

9.6.2 Transmission

The locations where the enrolment process occurs, the biometric template is generated and the template is stored might be different and therefore include transmission. The requirements for transmission are the core requirements in 9.2.

9.6.3 Central database

In this model, biometric data (raw biometric data, sample biometric data and the biometric template) are stored in a central database, and verification or identification is performed online. In addition to the core requirements in 9.2, the requirement for storage is that access control mechanisms shall be in place to prevent unauthorized access to stored biometric data (see Clause C.4 for risk issues).

9.6.4 Biometric tokens

In this model, the biometric template is stored in a portable device, such as a smart card, whereby verification or identification can be performed non-centrally. A system external to the card may load the reference template to the card. At this time, the card shall authenticate the external system, or the reference template shall be an integrity object.

At verification time, the user claims an identity by presenting the token and their biometric sample at the point of presence. The system cryptographically authenticates the reference template, or authenticates the token, and then retrieves the user's reference template from the token. The system then compares that reference template to the biometric sample to determine whether that user is the owner of the claimed identity. In some cases, identification may be used where several templates are stored on the token, such as family members.

The verification (or identification) process is the same as previously described, but the system architecture of the biometric components may differ between implementations. The token boundary may be limited to storage, in which case the token only provides the storage of the biometric template and all other system components

are external to the token. In this implementation, the template shall be exported from the token. Other token boundaries may include all of the system components, except the data collection and application components. In this implementation, the template is never exposed outside the confines of the token and only the verification result is exported from the token. In other implementations, the token may encompass the entire verification and application process.

If any part of the verification process occurs outside the secure token boundary, then any reference template stored in the token shall be protected as defined in this International Standard. Without cryptographic protection to provide data integrity and origin authentication, biometric templates are vulnerable to alteration or substitution attacks.

The processes of enrolment, authentication and the surrounding security framework for IC cards are detailed in ISO/IEC 7816-11, and additional guidance can be obtained from ISO 10202. In addition to the core requirements in 9.2 and the additional requirements in 9.4 and 9.5, the requirement for tokens is that access control mechanisms shall be in place to prevent unauthorized access to stored biometric data (see Clause C.4 for risk issues).

9.7 Termination and archiving

9.7.1 Termination

Termination is the process of expunging a user's biometric data or making the data obsolete. The termination of the biometric data is dependent on various factors:

a) employment termination reasons that might legally preclude job employment in the future;

b) the enrolment period for the user has expired (e.g. a smart-card user whose card has reached its expiration date);

NOTE Termination is required before re-enrolment.

c) technology of the biometrics has become outdated in favour of a newer version;

d) a different biometrics will be used in place of the previous one;

e) the biometric data has changed enough to warrant a new sample;

f) a different means of authentication has been developed;

g) the biometric data has been compromised;

h) legal or regulatory measures.

Where biometric information is used, the following termination requirements and recommendations apply to all applications and environments.

— The required period for keeping biometric data depends on the application. Business applications may require that the biometric data be archived for an extended period. For this and other reasons, an audit history of these events is recommended and is covered in Annex A.

— The possibility exists that the use of biometric data could be put "on hold" or "restricted" for a period. This would be analogous to a credit-card authorization being restricted for reasons such as fraudulent activity. Depending upon the outcome of an investigation, the biometric data could be "activated" again or be assigned a termination status.

9.7.2 Archiving

Archiving is the process of storing biometric data for either a predetermined or an indeterminate period. Expiration dates are a part of the enrolment process. The expiration date signals the date by which re-enrolment should occur.

In addition to the core requirements in 9.2, there is an archiving requirement that access control mechanisms shall be in place to prevent unauthorized access to archived biometric data (see Clause C.4 for risk issues).

9.8 Compliance and event journal

The compliance of any authentication system in terms of its consistency and accuracy requirements is often ascertained by an audit trail in an event journal. This International Standard makes the following recommendations.

— Compliance of the biometric system to this International Standard should be periodically validated according to the organization's Biometric Information Security Management System (BISMS) policy, practices and procedures. This activity is part of the “Check” function employed in a “Plan – Do – Check – Act (PDCA)” model.

— Clause 11 should be used in the compliance process.

Compliance can be validated internally by an organization or by an external third party. The results of the validation are typically kept confidential within the organization. Independent third parties can validate compliance or issue a formal attestation report that can be made public.

10 Security infrastructure

10.1 Components

10.1.1 Security architecture

The biometric functions necessary to construct the components described in Clause 8 may be contained in a biometric service provider (BSP). The cryptographic functions necessary to protect biometric information may be contained in a separate cryptographic service provider (CSP), or within the BSP, an application layer or an intermediate architectural layer [3)].

In one possible implementation, the application submits a biometric function call to the architectural layer. The architectural layer insulates the BSP from the application and submits the biometric function call to the BSP. The BSP processes the biometric function call and manages all cryptography by communicating directly with the CSP. The call response is returned from the BSP to the architectural layer and then to the application.

In an alternative approach, the application submits a biometric function call to the architectural layer. The architecture manages the cryptographic functions with the CSP and the biometric functions with the BSP [4)]. The call responses from the CSP and the BSP are returned to the application by the architectural layer.

In a third approach, the application submits cryptographic function calls directly to the CSP and the biometric function calls directly to the BSP. No intermediate architecture is used. The call responses from the CSP and the BSP are returned directly to the application.

---

3) The Common Data Security Architecture (CDSA) is one example of an intermediate architecture (See Reference [12]).

4) The BSP described is consistent with the BioAPI specification in ISO/IEC 19784-1.

10.1.2 Digital signature

The following requirements apply for employing a digital signature to protect biometric information with integrity.

— Hash algorithms shall be as specified in a relevant ISO (or equivalent national) standard.

— Key management techniques, as identified in Table 1, shall be as specified in a relevant ISO (or equivalent national) standard, such as ISO 11568, or in an ISO/IEC standard, such as ISO/IEC 11770.

10.1.3 Encryption for purposes of data confidentiality

The following requirements apply for employing encryption to protect biometric information.

— Encryption algorithms shall be as specified in a relevant ISO (or equivalent national) standard.

— Key management techniques shall be as specified in a relevant ISO (or equivalent national) standard.

10.2 Physical techniques

10.2.1 Protection mechanisms

Protection mechanisms are physical techniques to prevent and/or detect the unauthorized disclosure, modification or substitution of sensitive information, e.g. a tamper-resistant security module (TRSM) is designed never to reveal a symmetric or asymmetric private key in clear text form. Physical techniques, such as those described in ISO/IEC 19790 and discussed in Reference [15], include the following:

— tamper-evident mechanisms that result in visual evidence that an attack has been attempted, such as smooth, moulded casing, discoloration due to chemical attacks, evidence tape, or holographic seals;

— tamper-responsive mechanisms that detect unauthorized access and initiate countermeasures, such as zeroizing memory or placing the system into a security state;

— tamper-resistant mechanisms that resist physical penetration, such as hardened casing to resist drilling, or compounds that resist acid washings.

10.2.2 Types of attack

The type of attack the mechanism is designed to thwart is related to the sophistication of the attacker, as described in the following taxonomy of attackers (see Reference [17]).

— Class I (clever outsiders) are often very intelligent, but may have insufficient knowledge of the system. They may have access to only moderately sophisticated equipment, and often try to take advantage of an existing weakness in the system, rather than try to create one.

— Class II (knowledgeable insiders) have substantial specialized technical education and experience. They have varying degrees of understanding of parts of the system but potential access to most of it. They often have highly sophisticated tools and instruments for analysis.

— Class III (funded organizations) are able to assemble teams of specialists with related and complementary skills, backed by great funding resources. They are capable of in-depth analysis of the system, designing sophisticated attacks and using the most advanced analysis tools. They may use Class II adversaries as part of the attack team.

10.2.3 Risk analysis

The actual design and implementation of such protection mechanisms is problematic. A risk analysis should be performed to determine the appropriateness of the physical techniques in the design of the biometric equipment, in the implementation's environment and for the business application. Consideration in the design

should recognize that physical techniques based solely on ISO/IEC 19790 may not address the risk of being attacked from outside the biometric security perimeter, through the peculiar weaknesses to biometric systems, such as spoofing by artificial counterfeit.

For the purposes of this International Standard, the following requirements for physical protection apply.

— Biometric devices shall meet or exceed the Level 3 security requirements specified in Annex D, or the Level 2 security requirements specified in Annex D, within a physically secure environment.

— Cryptographic devices shall meet or exceed ISO/IEC 19790 Level 3 security requirements, or the ISO/IEC 19790 Level 2 security requirements, within a physically secure environment.

11 Biometric validation control objectives

11.1 Periodic review and audit considerations

Like other organizations, financial services rely heavily on the use of information technology (IT) and need to protect and manage the security of these assets, including biometric information. To fulfil these management responsibilities, security shall be provided for biometric information, and the management of information security shall become an important component of the organization's management plan.

The goal of financial services organizations shall be to meet or exceed industry standards and practices by using biometric technology in a responsible manner, and by managing the security of biometric technology as part of an overall policy-based information security management programme. This programme should include imposing and monitoring the effectiveness of proper controls. Compliance with the organization's policies, practices and procedures can only be assured by systematic, periodic security reviews. There are two primary types of security reviews:

— internal security reviews, and

— external reviews conducted by an independent information security professional.

The control criteria used for internal or external security reviews may be internally generated or originate from recognized standards, such as this International Standard. Consequently, this clause contains guidelines for assessing the compliance of a biometric system with the requirements contained in this International Standard, for the purposes of an internal or an external audit.

The control objectives in this clause represent control criteria against which a biometric system may be evaluated or audited. The control criteria described in this clause represent recommended practices for business, operational, and technical use by an organization which has implemented a biometric system. The security policies and practices of an existing information security management programme, such as that described in ISO/TR 13569, and in more general terms in ISO/IEC 17799, may already address some of these control objectives.

A biometric system may reside within or employ an IT infrastructure, and therefore environmental controls are applicable to the secure implementation of any biometric technology.

A biometric system may employ some form of cryptographic protection, such as encryption for data confidentiality, digital signatures for data integrity and authentication of origin. If cryptographic protection is used, key management controls are applicable to the secure implementation of biometric technology.

A biometric system enrols individuals by capturing biometric data to generate, distribute, use, and eventually terminate templates. This is analogous to the certificate registration process (see ISO 15782) for public key infrastructure (PKI) and, in some instances, biometric technology incorporated into a PKI.

11.2 Environmental controls

11.2.1 Security policy

The organization maintains controls to provide reasonable assurance that security policy and practices regarding biometric information exist and are maintained by a recognized policy management authority (see Table 1).

Table 1 — Security policy

	Control criteria: Information security policy
1.	A Biometric Information Security Management System (BISMS) Biometric Policy (BP) document is approved by management, published and communicated, as appropriate, to all employees, customers, and users of the biometric system. There may be more than one BP in an organization.
2.	As a minimum, the BP contains the following: a) definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing; b) a statement of management intent, supporting the goals and principles of information security; c) a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization, including: — compliance with legislative, regulatory and contractual requirements, — security education requirements, — prevention and detection of viruses and other malicious software, — cryptography requirements, — business continuity management, and — consequences of security policy violations; d) a definition of general and specific responsibilities for information security management, including reporting security incidents; and e) references to documentation that may support the policy.
3.	There is a defined review process, including responsibilities and review dates, for maintaining the biometric security policy.
	Control criteria: Policy management authority
4.	The organization has a management group with final authority and responsibility for specifying and approving the BP.
5.	The policy management authority (or equivalent group) has performed an assessment to evaluate business, legislative and regulatory risks to determine the security requirements and operational procedures to be included in the applicable policies and practices for a) environmental controls as detailed in this subclause, b) key management controls, as detailed in 11.3, and c) biometric management controls as detailed in 11.4.
	Control criteria: Policy management
6.	The BP is approved and modified in accordance with a defined review process, including responsibilities and review dates for maintaining the BP.
7.	The organization publishes the applicable public sections of the BP to all appropriate users.
8.	Significant revisions to the biometric security policy are made available to users.

11.2.2 Security organization

The organization maintains controls to provide reasonable assurance that:

— management direction and support for information security is provided;

— information security is properly managed within the organization;

— the security of facilities, systems and information assets accessed by third parties is maintained; and

— the security of information is maintained when the responsibility for functions has been outsourced to another organization or entity.

See Table 2.

Table 2 — Security organization

	Control criteria: Information security infrastructure
9.	Senior management and/or a high-level management information security committee ensure there is clear direction and visible management support for security initiatives.
10.	A management group or security committee exists to coordinate the implementation of information security practices and procedures.
11.	Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined.
12.	A management authorization process for new information-processing facilities exists and is followed.
	Control criteria: Security of third-party access
13.	Procedures exist and are followed to control access to organizational biometric information-processing facilities by third parties.
14.	Where there is a business need to connect to a third-party location, a risk assessment is performed to determine security implications and specific control requirements.
15.	Arrangements involving third-party access to organizational biometric information-processing facilities are based on a formal contract containing all necessary security requirements.
	Control criteria: Outsourcing
16.	If the organization outsources the management and control of all or some of its information systems, networks and/or desktop environments, the security requirements of the organization are addressed in a contract agreed between the parties.

11.2.3 Asset classification and management

The organization maintains controls to provide reasonable assurance that biometric assets and information receive an appropriate level of protection (see Table 3).

Table 3 — Asset classification and management

	Control criteria: Accountability for assets
17.	Owners are identified for all major assets, such as — biometric data (especially templates), — biometric hardware and/or software (including biometric readers at the point of presence), and — cryptographic hardware and/or software, and assigned responsibility for the maintenance of appropriate controls.
18.	Inventories of important assets are maintained by the organization.
	Control criteria: Information classification
19.	The organization has implemented biometric information classification and associated protective controls for this information that take account of business needs for sharing or restricting information, and the business impacts associated with such needs (e.g. unauthorized access or damage to the information).

20.	Procedures are defined to ensure that biometric information labelling and handling are performed in accordance with the organization's classification scheme and associated protective controls, e.g. the authorization to read or modify an event journal.

11.2.4 Personnel security

The organization maintains controls to provide reasonable assurance that personnel and hiring practices enhance and support the trustworthiness of the organization's operations (see Table 4).

Table 4 — Personnel security

	Control criteria: Personnel security
21.	Security roles and responsibilities are specified in the organization's biometric security policy, which is documented in job descriptions where appropriate.
22.	Verification checks on permanent staff are performed at the time of job application.
23.	Employees sign a confidentiality (non-disclosure) agreement as part of their initial terms and conditions of employment.
24.	Controls on contracting personnel are documented, and include a) bonding requirements on contract personnel, b) contractual requirements, including indemnification for damages due to the actions of the contractor personnel, and c) audit and monitoring of contractor personnel.
25.	All employees of the organization and, where relevant, third-party users receive appropriate training in organizational policies and procedures. The organization's policies and procedures specify the following: a) the training requirements and training procedures for each role; and b) any retraining period and retraining procedures for each role.
26.	Periodic reviews occur to verify the continued trustworthiness of personnel involved in the activities related to key management and biometric information management.
27.	A formal disciplinary process exists. This process is followed for employees who have violated organizational security policies and procedures. The organization's policies and procedures specify the sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems. Appropriate and timely actions are taken when an employee's contract is terminated so that controls and security are not impaired by such occurrences.

11.2.5 Physical and environmental security

The organization maintains controls to provide reasonable assurance that:

— physical access to facilities housing biometric systems not otherwise protected (e.g. by the requirements in Annex D) is limited to properly authorized individuals, and facilities are protected from environmental hazards;

— loss, damage or compromise of assets and interruption to business activities are prevented; and

— compromise or theft of information and information-processing facilities are prevented.

See Table 5.

Table 5 — Physical and environmental security

	Control criteria: Secure areas
28.	Physical protection is achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the business premises and facilities housing biometric systems.
29.	The perimeter of the building or site containing biometric systems is physically sound (i.e. there should be no gaps in the perimeter where a break-in could easily occur).
30.	A manned reception area, or other means to control physical access, is in place to restrict access to the building or site housing biometric systems to authorized personnel only.
31.	To prevent unauthorized access and damage, critical or sensitive biometric system components are housed in secure areas with appropriate physical barriers in place.
32.	Secure areas are used in accordance with the security policy to protect offices, rooms and facilities with special security requirements.
33.	Intruder detection systems are installed and regularly tested to cover all external doors leading to secure areas.
34.	Unoccupied secure areas are alarmed at all times.
35.	All personnel are required to wear visible identification and are encouraged to challenge anyone not wearing visible identification.
36.	Access to facilities is controlled and restricted to authorized persons only.
37.	All personnel entering and leaving the facility housing biometric systems are logged (i.e. an audit trail of all access is securely maintained).
38.	Visitors to the facility housing biometric systems are supervised and their date and time of entry and departure are recorded.
39.	Third-party support services personnel are granted restricted access to secure facilities housing biometric systems only when required, and such access is authorized and monitored.
40.	Access rights to the facility housing biometric systems are regularly reviewed and updated.
	Control criteria: Equipment security
41.	Equipment is sited or protected such as to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
42.	Equipment is protected from power failures and other electrical anomalies.
43.	Power and telecommunications cabling carrying data or supporting biometric services are protected from interception or damage.
44.	Equipment is maintained in accordance with the manufacturer's instructions and/or other documented procedures to ensure its continued availability and integrity.
45.	Security procedures and controls are used to secure equipment used outside an organization's premises.
46.	All items of equipment containing storage media (i.e. fixed hard disks) are checked to determine whether they contain any sensitive data prior to disposal or reuse. Storage devices containing sensitive information that are no longer in operational use are physically destroyed or securely overwritten.
47.	Equipment, information and software belonging to the organization cannot be taken off-site without authorization.

11.2.6 Operations management

The organization maintains controls to provide reasonable assurance that:

— correct and secure operation of the organization's information processing facilities is ensured;

— risk of systems failure is minimized;

— integrity of systems and information is protected against viruses and malicious software;

— damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures; and

— media are securely handled to protect media from damage, theft and unauthorized access.

See Table 6.

Table 6 — Operations management

	Control criteria: Operational procedures and responsibilities
48.	Biometric system operating procedures are documented and maintained.
49.	Formal management responsibilities and procedures exist to control all changes to biometric system equipment, software and operating procedures.
50.	Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorized modification or misuse of information or services.
51.	Development and testing facilities are separated from operational facilities.
	Control criteria: System planning and acceptance
52.	Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.
53.	Acceptance criteria for new information systems, upgrades and new versions are established, and suitable tests of the system are carried out prior to acceptance.
	Control criteria: Protection against malicious software
54.	Detection and prevention controls to protect against viruses and malicious software and appropriate user awareness procedures are implemented.
	Control criteria: Incident reporting and response
55.	A formal incident reporting procedure exists and this is followed, together with an incident response procedure, setting out the action to be taken on receipt of an incident report.
56.	Users of biometric systems are required to note and report observed or suspected security weaknesses in, or threats to, systems or services.
57.	Procedures exist and are followed for reporting hardware, software and firmware malfunctions or new feature requirements.
58.	Procedures exist and are followed to ensure that faults are reported and corrective action is taken.
59.	Incident management responsibilities and procedures exist and are followed to ensure quick, effective and orderly response to security incidents.
	Control criteria: Media handling and security
60.	Procedures for the management of removable computer media require the following: a) if no longer required, the previous contents of any reusable media that are to be removed from the organization are erased; b) authorization is required for all media removed from the organization and a record is kept of all such removals to maintain an audit trail; c) all media are stored in a safe, secure environment, in accordance with manufacturers' specifications.
61.	Media is disposed of securely and safely when no longer required.
62.	Procedures for the handling and storage of information exist and are followed in order to protect such information from unauthorized disclosure or misuse.
63.	System documentation is protected from unauthorized access.

11.2.7 System access management

The organization maintains controls to provide reasonable assurance that access to the management component of a biometric system and access to a resource that is controlled by a biometric access control system is limited to properly authorized individuals (see Table 7).

Table 7 — System access management

	Control criteria: User access management
64.	Business requirements for access control are defined and documented in an access control policy which includes at least the following: a) roles and corresponding access permissions, b) authentication process for each user, c) segregation of duties, and d) number of persons required to perform specific operations (e.g. n of m rule).
65.	A formal user registration and deregistration procedure for granting access to all multi-user information systems and services is followed.
66.	The allocation and use of privileges is restricted and controlled.
67.	The allocation of passwords is controlled through a formal management process.
68.	Users' access rights are reviewed at regular intervals.
	Control criteria: Network access control
69.	Users are provided direct access to only those services that they have been specifically authorized to use.
70.	The path from the user terminal to computer services is controlled.
71.	If permitted, access by remote users is subject to authentication.
72.	Connections to remote computer systems are authenticated.
73.	Access to diagnostic ports is securely controlled.
74.	Controls (e.g. firewalls) are in place to protect the organization's internal network domains from external network domains accessible by third parties.
75.	Controls are in place to limit the services (e.g. HTTP, FTP, etc.) available to users, in accordance with the organization's access control policies.
76.	Routing controls are in place to ensure that computer connections and information flows do not breach the access control policy of the organization's business applications.
77.	The security attributes of all network services used by the organization are documented by the organization.
	Control criteria: Operating system access control
78.	Automatic terminal identification is used to authenticate connections to specific locations and to portable equipment.
79.	Access to the organization's systems uses a secure logon process.
80.	All users have a unique identifier (user ID) for their personal and sole use, so that activities can be traced to the individual responsible.
81.	A password management system is in place to provide an effective, interactive facility, which ensures quality passwords.
82.	Use of system utility programs are restricted and tightly controlled.
83.	If required, based on a risk assessment, duress alarms are provided for users who might be the target of coercion.
84.	Inactive terminals serving biometric systems time out after a defined period of inactivity to prevent access by unauthorized persons.
85.	Restrictions on connection times are used to provide additional security for high-risk applications.
	Control criteria: Application access control
86.	Access to information and application system functions are restricted in accordance with the access control policy.
87.	Access to program source libraries is restricted and controlled.

11.2.8 Systems development and maintenance

The organization maintains controls to provide reasonable assurance that systems development and maintenance activities are properly authorized to maintain system integrity (see Table 8).

Table 8 — Systems development and maintenance

	Control criteria: Systems development and maintenance
88.	Business requirements for new systems, or enhancements to existing systems, specify the requirements for controls.
89.	Change control criteria exist and these are followed for the implementation of software on operational systems.
90.	Change control criteria exist and these are followed for scheduled software releases and modifications.
91.	Change control criteria exist and these are followed for emergency software fixes.
92.	Test data is protected and controlled.
93.	Strict control is maintained over access to program source libraries.
94.	The implementation of changes is strictly controlled by the use of formal change control criteria, to minimize the risk of corruption of information systems.
95.	Application systems are reviewed and tested when operating system changes occur.
96.	Modifications to software packages are discouraged and essential changes are strictly controlled.
97.	The purchase, use and modification of software is controlled and checked to protect against possible covert channels and Trojan code.
98.	Controls are applied to secure outsourced software development.

11.2.9 Business continuity management

The organization maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster or key compromise (see Table 9).

Table 9 — Business continuity management

	Control criteria: Business continuity management process
99.	The organization has a managed process for developing and maintaining its business continuity plans.
100.	The organization has a business continuity planning strategy based on an appropriate risk assessment.
101.	A single framework of business continuity plans is maintained to ensure that all plans are consistent and to identify priorities for testing and maintenance.
102.	Business continuity plans are tested regularly and maintained by regular reviews to ensure that they are up to date and effective.
103.	The organization's business continuity plans include disaster recovery processes for all critical components of a biometric system, including the hardware, software and keys, in the event of a failure of one or more of these components.
104.	Disaster recovery processes are in place to provide for the event that a critical security component is compromised.
105.	Backup copies of essential business information and software are regularly made. The security requirements of these copies are consistent with the controls for the information backed up.
106.	Fall-back equipment and backup media are sited at a safe distance to avoid damage from disaster at the main site.
107.	The recovery procedures used, if computing resources, software, and/or data are corrupted or suspected to be corrupted, describe: a) how a physically secure environment is re-established, b) which biometric templates are terminated, c) under what circumstances the system cryptographic keys are destroyed or archived, d) how the new cryptographic keys (if any) are securely distributed, and e) how the subjects are re-enrolled.
108.	The biometric system continuity plan includes procedures for securing its facility during the period of time following a natural or other disaster, and before a secure environment is re-established, either at the original site or a remote hot site.
	Control criteria: Key compromise
109.	The organization's business continuity plan for key compromise addresses who is notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures and encrypted data.

11.2.10 Monitoring and compliance

The organization maintains controls to provide reasonable assurance that:

— the organization complies with legal requirements;

— compliance with the organization's security policies and procedures is ensured;

— the effectiveness of the system audit process is maximized and interference to/from the system audit process is minimized; and

— unauthorized system usage is detected.

See Table 10.

Table 10 — Monitoring and compliance

	Control criteria: Compliance with legal and regulatory requirements
110.	The organization has procedures to ensure that all relevant statutory, regulatory and contractual requirements are explicitly defined and documented for each information system.
111.	Appropriate procedures are implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products.
112.	Important records of an organization are protected from loss, destruction and falsification (see 9.7).
113.	Procedures exist to ensure that personal information is protected in accordance with relevant legislation.
114.	Management authorizes the use of information-processing facilities, and controls are applied to prevent the misuse of such facilities.
115.	Controls are in place to ensure compliance with national agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls.
116.	The organization's biometric system confidentiality policies and procedures address the following: a) the types of information that shall be kept confidential; b) the types of information that are not considered confidential; c) the policy on release of information to law-enforcement officials; d) information that can be revealed as part of civil discovery; e) the conditions upon which information may be disclosed upon the owner's request; and f) any other circumstances under which confidential information may be disclosed.
	Control criteria: Review of security policy and technical compliance
117.	Managers are responsible for ensuring that security procedures within their area of responsibility are carried out correctly.
118.	The organization's biometric system is subject to regular review to ensure compliance with security policies and standards.
119.	The organization's biometric system is periodically checked for compliance with security implementation standards.
	Control criteria: System audit considerations
120.	Audits of operational systems are planned and performed such as to minimize the risk of disruptions to business processes.
121.	Access to system audit tools is protected to prevent possible misuse or compromise.
	Control criteria: Monitoring system access and use
122.	Procedures for monitoring the use of biometric systems are established and the results of the monitoring activities are reviewed regularly.
123.	Audit logs recording exceptions and other security-relevant events are produced and retained for an agreed period, to assist in future investigations and access control monitoring.
124.	Procedures for monitoring the use of biometric information-processing facilities are established and the result of the monitoring activities are reviewed regularly.

11.2.11 Event journaling

The organization maintains controls to provide reasonable assurance that:

— significant environmental, key management and biometric information life-cycle events are accurately and completely logged;

— the confidentiality and integrity of active and archived event journals is maintained;

— event journals are completely and confidentially archived in accordance with disclosed business practices; and

— authorized personnel review event journals periodically.

See Table 11.

Table 11 — Event journaling

	Control criteria: Event journals
125.	The biometric system generates automatic (electronic) and manual event journals as appropriate.
126.	Elements to be included in all journal entries include (synchronise with 9.8): a) date and time of the entry; b) serial or sequence number of entry; c) type of entry; d) source (terminal, port, location, customer, etc.); e) identity of the entity making the journal entry.
	Control criteria: Events logged
127.	Biometric enrolment information to be journalized includes: a) type of identification document(s) presented by the applicant; b) a record of unique identification data, numbers, or a combination thereof (e.g. applicant's driving licence number) of identification documents, if applicable; c) storage location of copies of applications and identification documents; d) identity of entity accepting the application; e) method used to validate identification documents, if any; and f) name of enroller, if applicable.
128.	Events to be journalized in the event journal(s) concerning keying material include the following: a) generation and installation of cryptographic keys; b) backup and/or recovery of cryptographic keys; c) withdrawal, destruction, or termination of keying material from service; d) deposit or withdrawal of archived cryptographic keys; and e) compromise of a symmetric key or asymmetric private key.
129.	Events to be journalized in the event journal(s) concerning cryptographic and biometric device life-cycle management include the following: a) device receipt; b) entering or removing a device from storage; c) device usage; d) device de-installation; e) designation of a device for service and repair; and f) device retirement.

Table 11 (*continued*)

130.	Security-sensitive events to be journalized: a) security-sensitive files or records read or written, including the event journal; b) deletion of security-sensitive data; c) security profile changes; d) use of authentication mechanisms, both successful and unsuccessful (including multiple failed authentication attempts); e) system crashes, hardware failures and other anomalies; f) actions taken by computer operators and system administrators and/or system security officers; g) change of affiliation of an entity; h) decisions to bypass encryption/authentication processes or procedures; and i) access to the biometric system or any component thereof.
131.	Additional considerations for high-risk applications where non-repudiation is necessary, concerning verification and identification: a) retention of the biometric sample captured and used in the authentication; b) deletion of the retained biometric sample on a predetermined basis; c) ability to validate the original verification or identification results; and d) protection mechanisms to prevent replay of a legitimate biometric sample.
132.	Event journals do not record the plain text values of any symmetric keys, asymmetric private keys, or biometric information.
133.	Computer clocks are synchronized for accurate recording.
	Control criteria: Event journal protection
134.	Current and archived event journals are maintained in a form that prevents unauthorized modification or destruction.
135.	Current and archived automated event journals are protected from modification or substitution.
136.	The private key used for signing event journals is not used for any other purpose.
	Control criteria: Event journal archival
137.	The biometric system archives event journal data on a periodic basis.
138.	A periodic risk assessment has been performed to determine the appropriate length of time for retention of archived event journals, as part of a continuous programme for the assessment of threats and mitigating processes.
	Control criteria: Review of event journal
139.	Current and archived event journals may only be retrieved by authorized individuals for valid business or security reasons.
140.	Event journals are reviewed periodically.
141.	The review of current and archived event journals includes a validation of the event journals' integrity, and the identification and follow-up of exceptional, unauthorized or suspicious activity.

11.3 Key management life-cycle controls

11.3.1 Key generation

The organization maintains controls to provide reasonable assurance that keys are generated in accordance with industry standards (see Table 12).

Table 12 — Key generation

	Control criteria: Key generation
142.	Key generation uses a random bit generator (RBG) or pseudo random bit generator (PRBG), as specified in ISO/IEC 18031.
143.	When prime numbers are needed, key generation uses a prime number generator, as specified in ISO/IEC 18032.
144.	Key generation occurs within a secure cryptographic device meeting the equivalent of — Level 3 requirements from ISO/IEC 19790, or — Level 2 requirements from ISO/IEC 19790 contained within a physically secure environment.
145.	Key generation takes place in a physically controlled environment.
146.	Key generation requires dual control by authorized personnel.
147.	Key generation uses a key generation algorithm, as specified in an ISO (or equivalent national) standard.
148.	Key generation results in key sizes in accordance with the applicable BISMS practices and procedures.
149.	The trustworthiness of the hardware/software used for key generation and the interfaces to the hardware/software are tested and verified before usage.
150.	Key generation is recorded in the event journal.

11.3.2 Key storage, backup and recovery

The organization maintains controls to provide reasonable assurance that private keys remain confidential and maintain their integrity (see Table 13).

Table 13 — Key storage, backup and recovery

	Control criteria: Key storage, backup and recovery
151.	If an asymmetric private key or symmetric key is exported from a secure cryptographic module and moved to secure storage for purposes of backup and recovery, then the cryptographic key is exported using a secure key management scheme: a) as cipher text under a key encryption key, used solely for the purpose as a KEK, with at least the equivalent cryptographic strength of a double length DEA key using Triple DES, or the strength of AES; b) as encrypted key fragments using dual control and split ownership, with the encryption used solely for that purpose, with at least the equivalent cryptographic strength of a double length DEA key using Triple DES, or the strength of AES; c) as clear text that is directly injected into another secure cryptographic module, such as a key transportation device using dual control; or d) as symmetric key components under dual control and split knowledge.
152.	If an asymmetric private key or symmetric key is backed up, it is stored and recovered by authorized personnel using dual control in a physically secured environment.
153.	If an asymmetric private key or symmetric key is backed up, recovery of the key is conducted in the same secure schema used in the backup process, using dual control.
154.	Procedures are in place to ensure that the integrity of the asymmetric private key or symmetric key is maintained throughout its life cycle.
155.	The permissible backup and recovery period for an asymmetric public key or symmetric key is in accordance with the BISMS policy, practices, and procedures.
156.	Backup and recovery procedures are tested on a periodic basis in accordance with the BP and BPS.
157.	Key storage, backup and recovery actions are recorded in the event journal.

11.3.3 Key distribution

The organization maintains controls to provide reasonable assurance that the integrity and authenticity of keys are maintained during initial and subsequent distribution (see Table 14).

Table 14 — Key distribution

	Control criteria: Public key distribution
158.	The integrity and authentication of origin of a biometric system's public keys, and any associated parameters, are provided via the use of a public key certificate.
159.	The distribution mechanism for the public key certificate is established and documented.
160.	The public key certificate shall be changed (re-keyed) periodically according to the BISMS policy, practices and procedures.
	Control criteria: Private key distribution
161.	The integrity and authenticity of an asymmetric private key and any associated parameters shall be maintained throughout the distribution process, such as the injection of the key into a biometric reader device within a physically secure key generation/loading facility.
162.	The distribution mechanism for the private key is established and documented.
163.	Private key distribution actions by the biometric systems are recorded in the event journal.
	Control criteria: Symmetric key distribution
164.	The integrity and authenticity of a symmetric key and any associated parameters shall be maintained throughout the distribution process, such as the injection of the key into a biometric reader device within a physically secure key generation/loading facility.
165.	The distribution mechanism for the symmetric key is established and documented.
166.	Symmetric key distribution actions by the biometric system are recorded in the event journal.

11.3.4 Key usage

The organization maintains controls to provide reasonable assurance that keys are used only for their intended functions in their intended locations (see Table 15).

Table 15 — Key usage

	Control criteria: Key usage
167.	Cryptographic keys are generated and used solely for their intended purpose, which is specified and documented during key generation, including: — asymmetric key pairs for biometric data integrity and authentication of origin; — asymmetric key pairs for biometric device authentication of origin; — symmetric keys for biometric data integrity and authentication of origin; — symmetric keys for biometric device authentication of origin; and — symmetric keys for biometric data confidentiality.

11.3.5 Key destruction and archival

The organization maintains controls to provide reasonable assurance that

— keys are completely destroyed at the end of their life cycle, and

— archived keys remain confidential and are never put back into production.

See Table 16.

Table 16 — Key destruction and archival

	Control criteria: Key destruction
168.	The BP and BPS specify who is authorized to destroy the cryptographic keys, and how the cryptographic keys are destroyed (e.g. token surrender, token destruction, or key overwrite).
169.	All copies and fragments of cryptographic keys are destroyed at the end of the key life cycle (with the noted exception of any archived keys).
170.	Key destruction actions taken by the biometric system are recorded in the event journal.
	Control criteria: Key archival
171.	The BP and BPS specify: a) the identity of the archival agent(s); b) the form in which the key is archived (e.g. encrypted, secret shares, components); and c) the security controls specified on the archival mechanism.
172.	Archived CA keys are subject to the same or greater level of security controls as keys currently in use.
173.	All archived keys are destroyed at the end of the archive period using dual control in a physically secure environment.
174.	Mechanisms are in place to ensure that archived keys are never put back into production.
175.	Mechanisms are in place to ensure that the archived keys are recoverable for the shortest time period technically permissible.
176.	Archived keys are periodically verified to ensure that they are properly destroyed at the end of the archive period.
177.	All archival access is recorded in the event journal.

11.3.6 Cryptographic device life cycle

The organization maintains controls to provide reasonable assurance that:

— access to cryptographic hardware is limited to properly authorized individuals, and

— cryptographic hardware is functioning correctly.

See Table 17.

Table 17 — Cryptographic device life cycle

	Control criteria: device shipment [a]
178.	Policies and procedures require that cryptographic hardware be sent from the manufacturer via registered mail using tamper-evident packaging.
	Control criteria: Device receipt [b]
179.	Upon the receipt of cryptographic hardware from the manufacturer, authorized personnel inspect the tamper-evident packaging to determine whether the seal is intact.
180.	Upon the receipt of cryptographic hardware from the manufacturer, acceptance testing and verification of firmware settings is performed.
181.	Devices used for private key storage and recovery, and the interfaces to these devices, are tested before usage for integrity.
182.	Device receipt is recorded in an event journal.
	Control criteria: Device pre-use storage [c]
183.	To prevent tampering, the cryptographic hardware shall be stored in a secure site, the access to which is limited to authorized personnel, and which has the following characteristics: — inventory control processes and procedures to manage the origination, arrival, condition, departure and destination of each device; — access control processes and procedures to limit physical access to authorized personnel; — reporting of all successful or failed physical access attempts in an event journal; — incident processes and procedures to handle abnormal events, security breaches, and investigation and reports; and — audit processes and procedures to verify the effectiveness of the controls.
184.	Cryptographic hardware is stored in tamper-resistant packages.
185.	The handling of cryptographic hardware is performed in the presence of no less than two trusted employees.
186.	Entering or removing a device from storage is recorded in an event journal.
	Control criteria: Device installation [d]
187.	The installation of cryptographic hardware is managed procedurally by authorized personnel to prevent tampering or substitution, such that: — installation is performed in the presence of no less than two trusted employees; — installation is performed using automated initialization processes capable of remotely authenticating the device.
188.	Device installation is recorded in an event journal.
	Control criteria: Device usage [e]
189.	Documented policies and procedures exist and these are followed to verify correct processing on a periodic basis.
190.	Diagnostic support is provided during troubleshooting of CA cryptographic hardware, in the presence of no less than two trusted employees.
191.	Device usage is recorded in an event journal.
	Control criteria: Device de-installation [f]
192.	The removal of cryptographic hardware is performed in the presence of no less than two trusted employees.
193.	Device de-installation is recorded in an event journal.
	Control criteria: Device service and repair [g]
194.	The service or repair site is a secure site with inventory control and access limited to authorized personnel.
195.	The process whereby cryptographic hardware is serviced or repaired with new hardware, firmware or software is performed in the presence of no less than two trusted employees, unless the keys have been removed.
196.	The designation of a device for service and repair is recorded in an event journal.
197.	Upon the receipt of cryptographic hardware that has been serviced or repaired, acceptance testing and verification of firmware settings are performed.

Table 17 (*continued*)

	Control criteria: Device retirement [h]
198.	The process whereby cryptographic hardware is disassembled and permanently removed from use is performed in the presence of no less than two trusted employees.
199.	If the device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose is erased from the device.
200.	If the device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, then the case is destroyed.
201.	The device case is securely stored until its destruction.
202.	Device retirement is recorded in an event journal.

[a] This stage is where the cryptographic device is shipped from the manufacturer to the organization.

[b] This stage is where the biometric system accepts the cryptographic device received from the manufacturer.

[c] This stage is where the cryptographic device has been received from the manufacturer, prior to installation, and stored in a controlled environment.

[d] This stage is where the cryptographic device has been removed from storage, installed into its production site, and readied for use. Installation includes the loading of all cryptographic keying material.

[e] This stage is where the cryptographic device is in full operational mode.

[f] This is the process whereby the cryptographic device is physically removed from production.

[g] This is the process whereby the cryptographic device is serviced or repaired with new hardware, firmware, or software.

[h] This is the process whereby the cryptographic device is disassembled and thus permanently removed from use.

11.4 Biometric information life cycle

11.4.1 Enrolment

The organization maintains controls to provide reasonable assurance that

— enrolees are properly identified and authenticated, and

— enrolment of the enrolee's biometric data is accurate, authorized and complete.

See Table 18.

Table 18 — Enrolment

	Control criteria: Enrolment request
203.	The authentication procedures for individual enrolment and reference template creation conform to the BP and BPS.
204.	The enrolment procedure requires that an individual enrolee shall prepare and submit the appropriate identification credentials, commensurate with an appropriate level of assurance, as specified in the BP and BPS.
205.	The enrolment procedure verifies the identity of the individual enrolee, in accordance with the BP and BPS.
206.	The enrolment procedure verifies the authority of the enrolee, in accordance with the BP and BPS.
207.	The enrolment procedure verifies the identity and the authority of the enroller, in accordance with the BP and BPS.
	Control criteria: Checking the enrolment data for errors and changes
208.	The enrolment procedure shall check the biometric data for quality and the enrolee’s identification credentials for errors or omissions.
209.	If required by the BP and BPS, the biometric system verifies the uniqueness of the enrolee's biometric data and claimed identity, and takes appropriate action, as specified in the BP and BPS.
	Control criteria: Enrolee notification
210.	The biometric system issues an out-of-band notification to the enrolee when a reference template has been generated and distributed.
211.	Where the biometric system could passively initiate an identification process as the customer activates the application (e.g. insertion of an ATM card), the applicant enrolling in such a biometric verification system is made aware of, and agrees to the use of, this procedure.

11.4.2 Template life cycle

The organization maintains controls to provide reasonable assurance that biometric templates are properly and securely generated, validated, stored, transmitted, distributed and terminated (see Table 19).

Table 19 — Template life cycle

	Control criteria: Template generation
212.	The biometric reference template components used by the biometric system conform to and do not conflict with the BP and BPS.
213.	The biometric system generates a biometric reference template that includes an identifier of the BP and may include BPS identification.
214.	The biometric system generates a biometric reference template that includes a unique user identifier in a critical template extension.
215.	The biometric system generates a biometric reference template that includes a unique reference template issuer identifier in a critical template extension.
216.	The biometric system ensures that the minimum number and type of authentication factors required for use of the biometric reference templates it generates can be enforced by applications and devices that conform to the security policies and practices of the organization.
217.	The biometric system ensures that the minimum number and type of biometric identifiers required for use of the biometric reference templates it generates can be enforced by applications and devices that conform to the security policies and practices of the organization.
218.	The biometric system does not generate reference templates for two users with the same unique user identifier.
219.	The biometric system does not generate reference templates for two users with the same biometric data.
	Control criteria: Template validation
220.	The biometric system validates the newly generated template against the enrolee's biometric data prior to acceptance and/or distribution of the template.
221.	The biometric system validates that the newly generated template is relatively unique within the domain of existing templates.
222.	The biometric system validates that the newly generated template contains sufficient data points to achieve the False Match Error Rate for verification or identification, in accordance with the BP and BPS.
223.	The biometric system ensures that the minimum number and type of alternate, fall-back authentication factors [a], when the biometric reference templates it generates cannot be used for any reason, are enforced by applications and devices that conform to the security policies and practices of the organization.
224.	The biometric system ensures that the minimum number and type of alternate, fall-back biometric factors [a], when the biometric reference templates it generates cannot be used for any reason, are enforced by applications and devices that conform to the security policies and practices of the organization.
	Control criteria: Template storage and transmission
225.	The biometric system ensures the integrity and authentication of origin of the template during transmission.
226.	The biometric system ensures the integrity and authentication of origin of the template whilst in storage.
227.	The biometric system ensures the access controls to the template during storage.

Table 19 (*continued*)

	Control criteria: Template distribution
228.	Templates are distributed within the biometric system using one or more of the following mechanisms. a) The central model is where the template is stored in a single location, such as a database, containing all other templates and accessed for verification or identification. b) The distributed model is where the template is transmitted to one or more locations, containing some or all other templates and accessed for verification or identification. c) The token model is where the template is stored in removable media, such as a smart card, containing one or more templates for an individual that are accessed for verification or identification.
229.	If the central model is used, the biometric system has policies and procedures to acknowledge the secure delivery of the template to the central storage site.
230.	If the distributed model is used, the biometric system has policies and procedures to acknowledge the secure delivery of the template to all storage sites.
231.	If the token model is used, the biometric system has policies and procedures to acknowledge the secure injection of the template into the device and the issuance of the token to the enrolee.
232.	Distribution acknowledgements are recorded in the event journal.
	Control criteria: Template termination
233.	The BP and BPS specify who may terminate a template.
234.	The BP and BPS specify under what circumstances a template may be terminated.
235.	The BP and BPS specify under what circumstances a template shall be terminated.
236.	The biometric system verifies the identity and authority of the individual (e.g. enrolee) requesting the termination of a template.
237.	When feasible to do so, the biometric system notifies the enrolee in the event of a template termination.
238.	Template termination requests are processed and validated in accordance with the requirements of the BP and BPS.
239.	Template termination is recorded in an event journal as described in Annex A.
240.	When a template is terminated, all instances of the template are destroyed.

[a] In cases where the alternate, fall-back authentication factors are deemed to provide a weaker level of assurance, it is the responsibility of the organization to ensure that applications adjust access and entitlements accordingly.

11.4.3 Verification and identification process controls

The organization maintains controls to provide reasonable assurance that verification and identification are securely performed in accordance with parameters agreed upon (see Table 20).

Table 20 — Verification and identification process controls

	Control criteria: Sample capture (raw data)
241.	Procedures and/or mechanisms are in place to ensure that the raw data can be accurately processed to create the sample data with sufficient data points for entity authentication in accordance with the BP and BPS.
242.	Mechanisms are in place to ensure that alternate authentication is made available when the biometric mechanism has failed, in accordance with the BP and BPS, which should consider that there is a risk of creating a serious security hole when alternative mechanisms are used.
	Control criteria: Sample transmission
243.	The integrity of the sample data during transmission is protected from modification.
244.	The authenticity of the sample data during transmission is protected from substitution.
245.	The non-repudiation of the sample data during transmission is protected from masquerading, where applicable, as determined by BP and BPS.
	Control criteria: Template transmission
246.	The integrity of the template during transmission is protected from deliberate or accidental modification.
247.	The authenticity of the template during transmission is protected from substitution.
248.	The non-repudiation of the template during transmission is protected from masquerading, where applicable, in accordance with the BP and BPS.
	Control criteria: Matching (scoring)
249.	The False Match Error Rate is in accordance with the BP and BPS.
250.	The results of the matching (score) are protected from modification and substitution.
	Control criteria: Decision
251.	The results of the decision (yes/no) are protected from modification and substitution.

11.4.4 Biometric device life-cycle controls

The organization maintains controls to provide reasonable assurance that

— access to biometric devices is limited to properly authorized individuals, and

— biometric devices are functioning correctly.

See Table 21.

Table 21 — Biometric device life-cycle controls

	Control criteria: Device shipment [a]
252.	Practices and procedures require that biometric devices be sent from the manufacturer via a reliable shipping process, using tamper-evident packaging.
	Control criteria: Device receipt [b]
253.	Upon the receipt of biometric devices from the manufacturer, practices and procedures require that authorized personnel inspect the tamper-evident packaging to determine whether the seal is intact.
254.	Device receipt is recorded in an event journal.
	Control criteria: Device pre-use storage [c]
255.	To prevent tampering, the biometric device shall be stored in a controlled environment within the storage facility, access to which is limited to authorized personnel, and which has the following characteristics: — inventory control practices and procedures to manage the origination, arrival, condition, departure and destination of each biometric device; — access control practices and procedures to prevent physical access to the controlled environment by unauthorized personnel; — incident practices and procedures to handle abnormal events, security breaches, and investigation and report; and — audit practices and procedures to verify the effectiveness of the controls.
256.	An audit of the inventory control process to verify its accuracy and account for the location and status of each biometric device is performed on a periodic basis.
257.	All successful or failed physical access attempts are recorded in the event journal.
258.	All incidents and their resolutions are recorded in the event journal.
259.	An audit of the event journal is performed on a periodic basis to verify the access controls and incident controls.
	Control criteria: Device installation [d]
260.	The installation of a biometric device is performed by an authorized individual.
261.	The verification or identification capabilities of the biometric device are tested prior to activation.
262.	The cryptographic capabilities of the biometric device are tested prior to activation.
263.	Device installation is recorded in an event journal.
	Control criteria: Device usage [e]
264.	Documented practices and procedures exist and are followed to verify correct processing on a periodic basis.
265.	Documented practices and procedures exist and are followed to provide diagnostic support during troubleshooting.
266.	Biometric devices meet or exceed the equivalent of Level 3 requirements from Annex D.
	Control criteria: Device de-installation [f]
267.	The de-installation of a biometric device is performed by an authorized individual.
268.	All biometric and/or cryptographic material is deleted from the biometric device.
269.	Device de-installation is recorded in an event journal.
	Control criteria: Device service and repair [g]
270.	The service or repair site is a controlled environment, with inventory control and access limited to authorized personnel.
271.	The designation of a device for service and repair is recorded in an event journal.

Table 21 (*continued*)

	Control criteria: Device retirement [h]
272.	The retirement of a biometric device is performed by an authorized individual.
273.	All biometric and/or cryptographic material is deleted from a retired biometric device.
274.	If the device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, then the case is destroyed.
275.	Device retirement is recorded in an event journal.

[a] This stage is where the biometric device is shipped from the manufacturer to a storage facility, either under the direct control of the biometric system or to a third-party storage facility.

[b] This stage is where the storage facility accepts the biometric device received from the manufacturer.

[c] This stage is where the biometric device has been received from the manufacturer, prior to installation, and stored in a storage facility with a controlled environment.

[d] This stage is where the biometric device has been removed from storage, installed into its production site, and readied for use. Installation includes the loading of all cryptographic keying material and biometric templates.

[e] This stage is where the biometric device is in full operational mode.

[f] This is the process whereby the biometric device is physically removed from production.

[g] This is the process whereby the biometric device is serviced or repaired with new hardware, firmware, or software.

[h] This is the process whereby the biometric device is permanently removed from service.

11.4.5 Integrated Circuit Card (ICC) life-cycle controls

The organization maintains controls to provide reasonable assurance that

— ICC preparation is securely controlled,

— ICC application preparation is securely controlled,

— ICC usage is enabled prior to ICC issuance,

— ICCs are securely stored and distributed,

— ICC deactivation and reactivation are securely controlled, and

— the use of ICCs is securely terminated for ICCs returned to the organization.

See Table 22.

A more detailed description of life-cycle controls is provided in ISO/IEC 7816-11. Additional guidance on ICC use can be found in ISO 10202.

Table 22 — Integrated Circuit Card (ICC) life-cycle controls

	Control criteria: ICC manufacturing [a]
276.	Prior to the stage when proprietary data enters the manufacturing process of the ICC (smart card), the security of the manufacturing procedures is in accordance with the level of security as requested by the card issuer.
277.	From the stage when proprietary data (e.g. a proprietary cryptographic algorithm or a cryptographic key) and/or other secret elements are combined with an IC, the following security requirements shall apply. — All processes are conducted in a secure environment, where access is controlled and confidentiality of proprietary data is maintained. — Access to controlled areas of an IC is only through use of a production key (as specified in ISO 10202-3). (Between each stage of manufacture, there may be a different production key.) — During storage and transport, ICs and ICCs (e.g. smart cards) are physically protected or cryptographically protected.
278.	The following data is recorded in an IC for security audit purposes: — IC manufacturer identifier, — manufacturer's IC type identifier, and — embedder/IC assembler identifier.
279.	As part of the manufacturing process, the integrity of an IC is verified (e.g. by examining a statistical sample) to confirm that it corresponds to the agreed reference specifications.
280.	Production of ICCs (e.g. smart cards) is properly authorized.
281.	Documented procedures exist and these are followed to ensure that ICCs (e.g. smart cards) are securely and accurately processed and documented.
	Control criteria: ICC personalization [b]
282.	The card issuer is responsible for the card personalization process.
283.	The personalization process is under the control of the appropriate cryptographic key(s) (as specified in ISO 10202-3) and involves the loading of Common Data File (CDF) data and its IC-related cryptographic keys.
284.	A card personalizer shall be recorded in an IC for security audit purposes.
	Control criteria: Common Data File (CDF) activation [c]
285.	CDF activation is the responsibility of the card issuer.
286.	CDF activation is conducted by a securely controlled process.
287.	CDF activation takes place at the end of the CDF personalization process, or as a separate process later.
288.	CDF activation is indicated in the ICC (e.g. smart card).
289.	The CDF activator identifier, date of activation and the CDF activator serial number should be recorded in the ICC (e.g. smart card) for security audit purposes.
	Control criteria: Application Data File (ADF) allocation [d]
290.	This process is only conducted under the control of the card issuer.
291.	For protection against unauthorized ADF allocation, a cryptographic exchange is performed using the appropriate cryptographic key (as specified in ISO 10202-3).
	Control criteria: Application Data File (ADF) personalization [e]
292.	The application supplier is responsible for the ADF personalization process.
293.	For protection against unauthorized personalization, a cryptographic exchange is performed using the appropriate cryptographic key.

Table 22 (*continued*)

	Control criteria: Application Data File (ADF) activation [f]
294.	ADF activation is the responsibility of the application supplier.
295.	ADF activation is conducted by a securely controlled process.
296.	ADF activation takes place at the end of the ADF personalization process, or as a separate process later.
297.	ADF activation is indicated in the ICC (e.g. smart card).
298.	An ADF can only be activated when the CDF is either in a activated or in a reactivated state.
	Control criteria: Smart card use
299.	An ICC (e.g. smart card) is not issued unless the card has been personalized.
300.	The IC is not usable for a financial transaction unless the CDF is in an activated or a reactivated state.
301.	Updating of ADF security parameters is not possible without approval of the application supplier.
302.	For protection against unauthorized modification, a cryptographic exchange is performed using the appropriate cryptographic key (as specified in ISO 10202-3).
	Control criteria: Application Data File (ADF) deactivation
303.	ADF deactivation is indicated in the ICC (e.g. smart card).
304.	Only the application supplier is able to deactivate or define the conditions for the deactivation of the ADF.
305.	While the ADF is deactivated, the ADF cannot perform any financial transaction.
306.	Reading of an ADF and ADF reactivation may be performed under the direct control of the application supplier.
307.	For protection against unauthorized deactivation of an ADF, a cryptographic exchange is performed using the appropriate cryptographic key (as specified in ISO 10202-3).
	Control criteria: Common Data File (CDF) deactivation
308.	CDF deactivation is indicated in the ICC (e.g. smart card).
309.	Only the card issuer is able to deactivate or define the conditions for the deactivation of the CDF.
310.	While the CDF is deactivated, an ICC (e.g. smart card) cannot perform any financial transaction.
311.	Reading of the CDF or CDF reactivation may be performed under the direct control of the card issuer.
312.	For protection against unauthorized deactivation of the CDF, a cryptographic exchange is performed using the appropriate cryptographic key (as specified in ISO 10202-3).
	Control criteria: Common Data File (CDF) reactivation
313.	CDF reactivation is indicated by an active status in the ICC (e.g. smart card).
314.	The process of reactivating the CDF, so that the ICC (e.g. smart card) may again be used for financial transactions, is conducted under the control of the card issuer.
315.	For protection against unauthorized reactivation of the CDF, a cryptographic exchange is performed using the appropriate cryptographic key (as specified in ISO 10202-3).
	Control criteria: Application Data File (ADF) reactivation
316.	ADF reactivation is indicated by an active status in the ICC (e.g. smart card).
317.	The process of reactivating an ADF, so that it may again be used for financial transactions, is conducted under the control of the application supplier.
318.	For protection against unauthorized reactivation of an ADF, a cryptographic exchange is performed using the appropriate cryptographic key (as specified in ISO 10202-3).

Table 22 (*continued*)

	Control criteria: ICC distribution
319.	Documented procedures exist and are followed to ensure that smart cards are securely distributed.
320.	ICCs (e.g. smart cards) are securely stored prior to distribution.
321.	Distribution of ICCs (e.g. smart cards) is logged in an event journal.
	Control criteria: Application Data File (ADF) termination
322.	ADF termination is indicated in the ICC (e.g. smart card).
323.	ADF termination is the responsibility of the application supplier.
324.	In this state, an ADF is permanently disabled (no possible reactivation) from use for a financial transaction.
325.	Preventing the termination of an ADF is the responsibility of the application supplier.
326.	For protection against unauthorized termination of an ADF, a cryptographic exchange is performed using the appropriate cryptographic key (as specified in ISO 10202-3).
	Control criteria: Common Data File (CDF) termination
327.	CDF termination is indicated in the ICC (e.g. smart card).
328.	CDF termination is the responsibility of the card issuer.
329.	In this state, the CDF is permanently disabled (no possible reactivation) from use for a financial transaction.
330.	Preventing the termination of the CDF is the responsibility of the card issuer.
331.	For protection against unauthorized termination of the CDF, a cryptographic exchange is performed using the appropriate cryptographic key (as specified in ISO 10202-3).
	Control criteria: Key termination
332.	After ADF termination, all cryptographic keys remaining in the ADF are disabled under the control of the application supplier.
333.	This process does not preclude the subsequent reading of previously readable information (as specified in ISO 10202-3).
334.	After CDF termination and the transfer of any residual values from an IC, all cryptographic keys remaining in the CDF are disabled under the control of the card issuer.
335.	This process does not preclude the subsequent reading of the previously readable CDF information (as specified in ISO 10202-3).
336.	After the termination of all the keys, the cryptographic functions are disabled in such a way that they cannot be used again.

[a] The smart-card manufacturing process includes IC semi-conductor design and software design, IC manufacturing, IC assembling and IC embedding.

[b] Smart-card preparation consists of two steps: card personalization and CDF activation.

[c] The CDF activation process prepares the ICC (smart card) for use in financial transactions by the cardholder.

[d] ADF preparation consists of three steps: ADF allocation, ADF personalization, and ADF activation. ADF allocation involves the allocation of memory areas in an IC.

[e] ADF personalization involves the loading of ADF-related keys and data.

[f] ADF activation prepares an ADF for use in financial transactions by the cardholder.

Annex A
(informative)

Event journal

A.1 General

The compliance of any authentication system as to its consistency and accuracy are validated by evidence of an event journal providing an audit trail. An event journal is considered to have two states:

— the active state, where events are captured in the event journal by the authentication mechanism;

— the archive state, where a journal has been removed from the active state and placed in storage.

A.2 Management requirements

This International Standard requires that an event journal, whether electronic or manual, be generated and maintained to meet the control objectives specified in 11.2.11. The following are suggestions for maintaining the event journal.

a) Mechanisms should be in place to maintain the integrity of the active event journal, such that

   — the deletion of an event entry can be detected,

   — the addition of an event entry can be detected, and

   — the modification of an event entry can be detected.

b) Mechanisms should be in place to provide authentication of the event journal's origin.

c) The active event journal should be archived no less than every 30 days or every 3 000 events, whichever occurs first.

d) Mechanisms should be in place to provide access control over the active event journal, such that

   — the active event journal cannot be replaced by an archived event journal,

   — only authorized processes can add entries to the event journal,

   — only authorized processes can delete entries from the event journal,

   — only authorized processes can modify the event journal, and

   — only authorized personnel can read the event journal.

e) The archive event should be captured in both the new active journal and the new archive journal, with at least the following information:

   — indicator denoting the archive event;

   — date and time of the archive event;

   — total number of event entries (optional);

— subtotals by event type (optional);

— sequence numbers of the new archive journal and the new active journal.

f) The archive journal should be kept up to a maximum time consistent with security policies and prudent business practices, and legislative and regulatory requirements.

A.3 Content requirements

A.3.1 Enrolment

The following are journal recommendations for enrolment events.

a) The following information shall be captured for each successful enrolment:

— successful enrolment event record indicator;

— date and time of the enrolment;

— template description (e.g. biometric header);

— enrolee identifier;

— enroller identifier;

— Biometric Policy under which the enrolment occurred;

— certificate serial number (optional);

— discretionary data (e.g. usage flags).

b) The following information should be captured for each failed enrolment:

— failed enrolment event record indicator;

— date and time of the enrolment failure;

— template description (e.g. biometric header);

— enrolee identifier;

— enroller identifier;

— enroller comments;

— discretionary data (e.g. usage flags).

A.3.2 Verification and identification

The following are journal recommendations for verification events.

The following information shall be captured for each failed verification:

— failed verification event record indicator;

— date and time of the verification failure;

— template description (e.g. biometric header);

— discretionary data (e.g. usage flags).

A.3.3 Termination and revocation

The following are journal recommendations for termination and revocation events.

The following information shall be captured for each termination and revocation:

— failed termination and revocation event record indicator;

— date and time of the termination and revocation;

— reference template;

— discretionary data (e.g. usage flags).

A.3.4 Transmission and storage

The following are journal recommendations for distribution events.

a) The following information shall be captured for each addition to a storage system:

   — addition to the database event record indicator;

   — date and time of the addition;

   — template description (e.g. biometric header);

   — enrolee identifier;

   — enroller identifier;

   — certificate identification (optional);

   — discretionary data (e.g. usage flags).

b) The following information shall be captured for each modification to a template in a storage system:

   — modification of a template event record indicator;

   — date and time of the modification;

   — template description (e.g. biometric header);

   — reference template identifier;

   — enrolee identifier;

   — enroller identifier;

   — certificate identification (optional);

   — discretionary data (e.g. usage flags).

c) The following information should be captured for each deletion in a storage system:

- indicator denoting a deletion from the database;
- date and time stamp of the deletion;
- reference template description;
- enrolee identifier;
- enroller identifier;
- certificate identification (optional);
- discretionary data (e.g. usage flags).

d) The following information shall be captured for each injection of biometric information into a token:

- indicator denoting an issuance of a token;
- date and time stamp;
- reference template description (e.g. biometric object identifier);
- enroller identifier;
- enrolee identifier;
- certificate identification (optional);
- discretionary data (e.g. usage flags).

e) The following summary information should be captured daily:

- date and time stamp of when the summary record was generated;
- total number of additions, deletions and modifications to the storage system;
- total number of successful enrolments;
- total number of failures to enrol;
- total number of tokens issued with a biometric template;
- total number of successful verifications;
- total number of failed verifications;
- total number of successful identifications;
- total number of failed identifications;
- total number of adds and reads to the event journal, including the current summary record.

Annex B
(normative)

Biometric enrolment

B.1 General

Enrolment is the process whereby an individual's biometric data is captured for intended use in accessing the institution's financial services or for internal use by employees. To meet the requirements of this International Standard, it is necessary for applicants to be enrolled at an authorized capture site. There shall be verification that the biometrics being recorded is that of the actual user. It is crucial that all biometric data be validated as emanating from an authorized capture site in order to preclude the possibility of insertion of false, spoofed or otherwise unwanted biometric data into the system. The enrolment process consists of the following steps:

a) individual identity verification;

b) biometric profile capture;

c) quality check and verification of ability to match; and

d) biometric data transmission and storage.

B.2 Identification criteria for an individual

The registration authority at the authorized capture station is responsible for verifying that the individuals enrolling with a biometric identification profile are "who they say they are". The level of documentation required to verify identification is dependent on the value/risk involved in the financial services that will be accessible to the enrolee. These documents and the collection mechanism are chosen based on the risk level of the financial service, as in the following recommendations.

a) Low-risk financial services should require the registration authority to collect from the user personal information (e.g. name, address, driving licence number) and other financially related information (e.g. income, employer, work address). In addition, at least two other forms of personal identification should be required (e.g. credit cards, state-issued driving licence, passport, utility bills).

b) Medium-risk financial services should require the registration authority to collect from the user personal and financial information. In addition, at least two other forms of personal identification should be required, one of which should contain the applicant's photograph (e.g. credit cards, state-issued driving licence, passport, utility bills).

c) High-risk financial services should require a senior registration authority to collect the user's personal and financial information in person, with photo identification, multiple identification documents and a recognized third-party notarized testimonial. A court officer, minister or medical doctor who has known the applicant for at least two years should write this testimonial letter. The senior registration authority shall verify the validity of at least two of the supplied identification documents and make verbal contact with the individual authoring the testimonial letter. Copies of the legal documents, identification documents supplied and the user's original written signature attesting to the accuracy and truthfulness of the information should be kept on file at the biometric capture location, or at the site of the registration authority if the enrolment point is at a third-party or remote location.

B.3 Quality check and verification of ability to match

It is imperative that the biometric data captured be automatically checked for acceptable quality before the applicant leaves the site. Experience has shown that human judgement of the acceptability of the captured sample is not always accurate with many biometric systems. To guarantee that the biometric profile has been accurately recorded and stored, a live match should be made of the applicant's biometrics to the newly stored biometric template.

Annex C
(normative)

Security considerations

C.1 General

This annex identifies security considerations and possible attacks or weaknesses in biometric systems. The possible points of attack and a set of possible solutions are described when applicable. Further information can be found in Reference [16].

C.2 Registration of an individual using false identity

Each user shall prove their identity to the biometric system owner before being allowed to enrol. This provides assurance that the biometric reference template is actually bound to the identity of the individual who has enrolled, and not to a different person who the enrolee claims to be. Security is compromised if any individual can enrol using a false identity (see Table C.1).

Table C.1 — False identity registration

Points of entry or attack	Protection mechanisms	Relevant component
enrolment process	well-defined and controlled enrolment process	— capture — process — transmission — storage

C.3 Fraud susceptibility within data collection “Synthetic attack”

An attacker fabricates an analogue of the real user’s biometric characteristic using captured information. The fabrication is subsequently used to impersonate the user to the biometric system. This attack involves two separate steps:

a) collection of biometric information representing one or more other users’ biometric characteristic;

b) use of the collected biometric information to fabricate a model or facsimile of the biometric characteristic, and use of that model in a biometric reader.

It is impractical to prevent collection of biometric information from an individual, so the preventive measures apply to the possible use of the fabricated model of the user’s biometric characteristic (see Table C.2).

Table C.2 — Synthetic attack

Points of entry or attack	Protection mechanisms	Relevant component
a) standard biometric capture device, for application of attack b) various methods for capturing the data necessary to build the synthetic device — capture from the individual (photograph face, capture fingerprint from water glass) — capture raw biometric data or template data from the biometric system (wiretaps, access to database, etc.) — install fake biometric readers that users believe are part of the real system, and collect the entire biometric sample data entered through those readers	a) biometric capture devices that can detect synthetic biometric features (e.g. fingerprint readers that detect warmth and pulse) b) verification stations that are monitored by a live attendant, or electronically by means such as a video camera	— capture

C.4 Protection of the data during transmission

C.4.1 Overview

The biometric data is vulnerable when transmitted between components or stored within components of the system. It can be intercepted and recorded or manipulated, or substitute data can be injected in its place. When biometric systems are used in financial applications, it is essential that the data be protected from such attacks. This requires assurance of data integrity throughout the transmission system. If integrity mechanisms are used to guarantee that no altered or replayed data is accepted, then interception and substitution attacks will not be possible.

In some applications, proof of origin may also be important. Typically, this would be used to verify that the data was collected at a valid biometric reader.

The processed signal serves a different purpose in the enrolment and verification operations. In enrolment, the processed signal is written to template storage. Additional limitations may be imposed, such as a search to first verify that the same individual is not already enrolled. In verification, the processed signal is compared to one or more templates in the current database of enrolled users. This may be one-to-one verification to determine whether the user matches a template for the person he claims to be, or it may be a one-to-many verification, in order to try to identify which enrolled template matches the unknown user.

The templates shall be protected against substitution, either by replacing the stored template itself, or by substituting a template in the path between the storage medium and the matching subsystem. The degree and type of protection depends on the nature of the storage subsystem and the overall biometric system. No additional protection is needed if the entire biometric system, including template storage, is contained in a single physically secure unit.

If the templates are stored in a database on a separate computer, however, integrity measures are required to ensure that the template received at the matching subsystem is the intended one. Likewise, if the templates are stored in physically secure tokens but other biometric subsystems utilized during verification reside on a separate device, integrity measures are required to ensure data integrity and origin authentication of the template. Such protection provides assurance that the template in the token has not been altered or replaced, and that it was created by a trusted party.

C.4.2 Injection of false/replayed biometric data

An attacker captures biometric data that can later be injected into the system, identifying the attacker as the individual whose data was captured (see Table C.3).

Table C.3 — False/replayed data

Points of entry or attack	Protection mechanisms	Relevant component
a) communications interfaces (local or remote) b) template database or token	a) cryptographic integrity protection b) physical protection of interfaces and cables	— capture — transmission — storage

C.4.3 Search for match between chosen sample and templates

The attacker tries to verify his own biometric characteristic against a large number of templates in the system database in an attempt to find one or more other individuals whose biometric data is similar enough that he can successfully verify himself as those other people. This is a possibility with many biometric technologies; any non-zero false match rate indicates that there will be individuals who can verify against each other's templates.

In a related attack, the attacker tries to find a template that matches a selected person's biometric data. The attacker might choose a person with a high level of authority or another characteristic that makes them an attractive target. The attacker tries to find a template that matches the target person. If one is found, he colludes with the owner of the matching template in order to defraud the target person (see Table C.4).

Table C.4 — Chosen sample match search

Points of entry or attack	Protection mechanisms	Relevant component
a) normal biometric authentication interface b) injection of biometric data electronically into the system c) direct access to comparison process	a) restrict access to the template data: — restrict access to database or directory — require successful authorization via second factor before allowing access to the individual's biometric template data — use portable storage (e.g. smart card) for template data b) restrict the ability to issue verification requests against data in the template database	— storage

C.4.4 Search for match between pairs of templates

This attack is similar to the one described in C.4.3, except that the attacker looks for matches between any two templates in the database, rather than looking for a match with a specific user's data. If two sufficiently similar templates are found, the attacker attempts to convince one of the two people to collude in defrauding the other person in the matching pair (see Table C.5).

Table C.5 — Match between template pairs

Points of entry or attack	Protection mechanisms	Relevant component
a) normal biometric authentication interface b) injection of biometric data electronically into the system c) direct access to comparison process	a) restrict access to the template data: — restrict access to database or directory — require successful authorization via second factor before allowing access to the individual's biometric template data — use portable storage (e.g. smart card) for template data b) restrict the ability to issue verification requests against data in the template database	— storage

C.5 Modification of verification result

The biometric device correctly acquires the sample and the template, and performs the comparison, but the attacker is able to change the answer before the verification result is used (see Table C.6).

Table C.6 — Verification result modification

Points of entry or attack	Protection mechanisms	Relevant component
a) transmission path of verification result to system/equipment that will act on that result b) unprotected software involved in biometric decision, or in transmission of result	a) cryptographic integrity checks of the binary verification result b) protected environment for software execution	— transmission — match — decision

C.6 False Match (FM) versus False Non-Match (FNM)

C.6.1 Overview

When a submitted biometric sample and a stored template are compared by the matching subsystem, the resulting score can be said to represent a "match" if it exceeds a particular threshold, and a "non-match" if it does not. The most simple system decision policy that might be used in verification applications would be to "accept" the user's claim to an identity if a "match" occurs, and reject the claim if a "non-match" is determined. However, all operational biometric systems use more sophisticated decision policies, e.g. most verification systems allow a user at least three attempts to produce a score exceeding the "match" threshold, thus producing a decision to "accept" the claimed identity if one out of three trials results in a sufficient score. Consequently, for verification systems, the "False Acceptance" rate is determined by both the "False Match" (FM) rate and the decision policy, while the "False Rejection" rate is determined by both the "False Non-Match" (FNM) rate and the decision policy.

The relationship between FM and FNM is inversely proportional, because there is an overlap between good and bad matches. Another indicator is the value when FM equals FNM, the Equal Error Rate. The better the biometric system, the lower the value. Bad matches generally form a bell-shaped distribution curve. Good matches also form a similar curve with an additional grouping of FNM in the bad-match region, which is termed a bi-modal distribution. Setting a high threshold eliminates all bad reads (everything below the threshold) from good reads (everything above the threshold), but allows false non-matches. Setting a lower threshold eliminates most bad matches (everything below the threshold) from the good matches (everything above the threshold), but allows false matches.

C.6.2 Improper threshold settings

An improperly adjusted False Reject Rate (FRR) or False Acceptance Rate (FAR) may result in an unauthorized individual gaining access, or an authorized individual being denied access (see Table C.7).

Table C.7 — Improper threshold

Points of entry or attack	Protection mechanisms	Relevant component
a) enrolment process b) verification process c) identification process	a) policy, controls and audit procedures for well-defined FRR and FAR parameters	— match — decision

C.6.3 Improper device calibration

A legitimate operator (maintenance person) may compromise or damage the biometric device during routine maintenance or installation. Likewise, an adversary could physically access the biometric device and modify the device's configuration. Either situation could lead to a loss of service, an increased FFR, or an increased FAR (see Table C.8).

Table C.8 — Improper calibration

Points of entry or attack	Protection mechanisms	Relevant component
a) enrolment process b) verification process c) identification process	a) policy, controls and audit procedures for well-defined FRR and FAR parameters	— capture

C.6.4 Illicit device or system performance

A biometric device or the system may allow a higher FRR or FAR due to a hardware or software flaw, or environmental conditions where a device is operating outside its normal parameters (see Table C.9).

Table C.9 — Illicit device or system performance

Points of entry or attack	Protection mechanisms	Relevant component
a) verification process b) identification process	a) monitoring mechanisms to detect unacceptable levels of FRR and/or FAR b) quality controls for hardware and software components c) rigorous formal and/or informal testing of biometric systems	— capture — process — match — decision

C.7 Scores and thresholds

C.7.1 Attacks

An attacker may utilize the results of a match to gain information to compromise the system systematically. Two such attacks are described in C.7.2 and C.7.3.

C.7.2 Hillclimbing attack

The result of a verification operation may be a Boolean “yes” (for a positive match) or “no” (for a negative match), based on a given threshold setting, or may be the actual match score.

The biometric sample is compared with an enrolled template within the biometric technology module to create a score. This score is then compared with a predefined threshold, and the subject who provided the sample is either verified to be the legitimate holder of the template or not. The release of scores from the biometric technology to the application becomes a security issue when passed through open standardized means (such as an API). In this case, an attacker can write a rogue application that systematically interrogates the biometric technology by providing a sample that is randomly perturbed and monitoring the output score to maintain only changes in the sample which move it closer to the raw input data represented by the template. The attacker can thus systematically modify the sample to obtain progressively higher scores until the decision threshold is met. Such an attack can be labelled a “hillclimbing” attack (see Table C.10).

See Reference [18] for further information.

Table C.10 — Hillclimbing attack

Points of entry or attack	Protection mechanisms	Relevant component
a) interface between application and biometric technology	a) return of incremental scores of sufficient step size, rather than continuous scores b) mutual authentication between application and biometric technology	— capture — transmission — match

C.7.3 Update and adaptation

A template update is generally initiated by the application and is the same as a re-enrolment in the same technology, perhaps using the original template as an input. Adaptation is performed automatically by the biometric technology upon a successful verification match.

When an update is performed, the possibility exists for an attacker (as a rogue application) to submit a sample of an unauthorized individual into the update function to cause the return of a compromised new template, which would then be stored in the user database for the authorized individual. With adaptation, since the new sample and enrolled template would have already passed the verification match, they are known to belong to the same individual (see Table C.11).

Table C.11 — Update and adaptation

Points of entry or attack	Protection mechanisms	Relevant component
a) interface between application and biometric technology b) database interface	a) access controls on database b) authorization controls on performance of update function (i.e. only an administrator may perform this function, same controls as for an enrolment) c) mutual authentication between application and biometric technology	— transmission — storage

These systems may use a three-tiered decision process with two separate thresholds.

— If the score exceeds the upper threshold, the system indicates that the sample data matches the template, and nothing else is done.

— If the score exceeds the lower threshold, but not the upper threshold, the system indicates that the sample data matches the template, and the template is updated in some way using the sample data.

— If the score is below the lower threshold, the system indicates that the sample data does not match the template, and no other action is taken.

For these systems, one needs to be concerned about a “hillclimbing attack” (see Reference [18]).

C.8 Single- versus multi-factor authentication

Using multiple authentication factors is generally thought to improve system security, since multiple authentication factors must be compromised in order to defeat the authentication process. However, increasing the number of authentication factors may result in a number of problems. These include:

— more customer frustration, due to having to carry, remember and use additional authentication factors;

— increased institutional maintenance costs in administering multiple identification factors such as cards and pins;

— lost productivity by workers when they cannot access resources (i.e. higher False Rejection Rates);

— system circumvention when fall-back verification mechanisms allow an impostor to intentionally be rejected or to intentionally fail to enrol in a biometric system, in order to attack a secondary authentication mechanism.

Too many authentication factors can also lead to decreased system security if users resort to insecure techniques to manage the complexity of multiple authentication factors, e.g. users may write passwords down for a multiple-password system in order not to forget them. However, an excessively lax authentication policy may bring material loss, potential data confidentiality breaches, loss of faith in an institution due to fraud, lost customer time restoring stolen identities, and other intangibles. When determining the number of authentication factors in an authentication system, it is therefore important to consider the trade-offs in terms of achieved security versus other costs, such as customer frustration and maintenance costs for the combined system.

Some biometric systems achieve a low enough False Match Rate that they can carry out both verification and identification using a single biometric measure. Other biometric systems require multiple measures to achieve a low False Match Rate. This capability makes these technologies ideal candidates for use in systems where there is only a single authentication factor – the biometric. As an example, consider a single-measure biometric system, which is operated at a threshold such that the single-comparison False Match Rate is Pr[FM]. Assume we wanted to employ this biometrics with a banking population of N enrolled users. In general, biometric systems will "partition" the database, separating the enrolled users into separate groups based on either information within the biometric measure (such as fingerprint classification), or other information, such as age or gender. The "penetration rate", P, is the average percentage of the enrolled database that will be searched during every transaction. Consequently, each transaction will require, on average, $P * N$ comparisons of the submitted biometric sample to stored biometric templates.

Using a simple probability model for a single-measure biometric system (see Reference [19]), the resulting probability for system False Match, Pr[System False Match], not to occur in a population of N users is

$$\text{Pr[System False Match]} = 1 - (1 - \text{Pr[FM]})^{P*N} \tag{C.1}$$

For example, given the single-comparison False Match Rate of 10^{-6}, and a penetration rate of 0,5, the corresponding system False Match Rate for a population of $N = 1\,000$ users is 1:100. In other words, using a biometrics, which has a single-comparison False Match Rate of 1:100 000 and running it against a partitioned biometric database of 1 000 users would give a System False Match Rate of 1:200. This underscores the tremendous accuracy requirements for any single-factor identification system that uses only a single biometric measure.

The next issue relates to the fact that the single-factor used in authentication shall have a high level of integrity to prevent software component replacement and spoofing attacks. This criterion is met when the biometric system meets the security requirements enumerated in this International Standard, in particular the requirements regarding a "synthetic biometric feature": those regarding replayed or fake data and "proof of origin" are especially relevant. This is because a single-measure biometric system relies solely on the integrity of the single biometric template used to "unlock" the system. Authentication system security is weakened unless strong techniques are put in place in these areas.

To summarize, when deciding whether to implement an authentication system based on a single, biometric-based factor, a number of other elements should be taken into account. These include the accuracy of the biometrics in terms of False Match, target population size and system security, so that user convenience is maximized while still meeting system security objectives.

C.9 Testing

Assessing error rates for biometric devices is clearly part of the technical testing process. Beyond that, however, there is little agreement. A review of the technical literature on biometric device testing reveals a wide variety of conflicting nomenclature and protocols. Hoping to address this problem and rationalize the field of error rate testing, the British government has released a document called "Best Practices in Testing and Reporting Performance of Biometric Devices" (see Reference [20]). Its purpose is to propose, for general review by the biometrics community, "best practices" for conducting and reporting technical testing for the purpose of error-rate estimation.

The wide variety of biometric devices, sensors, vendor instructions, data acquisition methods, target applications and populations makes it impossible to present precise uniform testing protocols. On the other hand, some specific terms, philosophies and principles can be applied over a broad range of devices and test conditions.

The first question relates to nomenclature. Traditionally, errors have been described as “false acceptance” and “false rejection”. Unfortunately, these terms have opposite meanings to the access control and large-scale identification communities, leading to confusion when comparing documents across applications. The terms “false match” and “false non-match”, like the terms “false positive” and “false negative”, do not have this problem. The former terms are preferred only because they are slightly shorter and more descriptive of the problem.

The second question is whether error rates should be reported as

a) the probability of an error of each of the above types for single comparison, or

b) a “rank order statistic”, indicating the average rate at which a sample is correctly found to be in the top m candidates over a database of n enrolled templates.

Approach a) is preferred by most researchers because it does not convolve the reported errors with the database size, and it conveys more information. For any database size, the expected “rank order statistics” can be derived from the false match and non-match error rates, but not vice versa.

The final and most important question concerns how these error rates should be assessed. This question dominates most of the “Best Practices” document; however, it will only be briefly summarized here. One general principle is that biometric devices, by themselves, do not have error rates. Errors are only made when devices are used by a population of users in a specific application. This means that the question “What are the error rates for fingerprint devices?” is ill posed. A better question would be “What error rates can be expected when a fingerprint device is used by habituated working people in an unsupervised, indoor environment?” This cannot be predicted without testing the impact of habituation, supervision and an indoor environment on the error rates of adults using fingerprinting systems. This implies that a complete answer to the question of error rates and biometric devices will require testing of all possible populations.

Testing is so expensive that it is rarely done even for a single device in a single application with a single population. However, the following general impacts of environment and population on error rates are known: infrequent users make more errors than habituated users; young people make fewer errors with fingerprinting devices than older people; outdoors is a more challenging environment than indoors. Therefore, if we have results for habituated working adults in an indoor environment, we know that error rates for an infrequently used, outdoor device at a retirement facility will be substantially higher.

A second general principle is that system policy also drastically affects error rates. For instance, system false non-match error rates can be decreased at the expense of false match error rates by enrolling two measures (such as two index fingers) and allowing a system match if a match against either measure occurs. Using mathematics, test error rates can be approximately (and sometimes very inaccurately owing to unknown data correlations) translated to system error rates under a variety of system policies, such as “three-strikes-you’re-out” or multiple-template enrolment. Other system policies, such as allowing only “good” users to enrol by rejecting poor-quality enrolment images, will keep some people from ever using the system, but will result in much lower system error rates of both kinds.

A final principle is that testing is always performed with volunteering, supervised, and therefore cooperating, users. Volunteers might even be provided an incentive to correctly use the system, thereby lowering false non-match rates. False match rates are determined by the coincidental matching of two individuals' measures. These are called “zero-effort” impostors. The vulnerability of the false match rate to determined impostors and the effect on the false non-match rate of uncooperative users is never measured. Consequently, the psychological environment of the test may not match that of the target “real-world” application.

In conclusion, false match and false non-match rate testing gives only an approximate look at the potential for errors with biometric systems. No matter how carefully designed and extensive the testing, results can never be said to predict definitively “real-world” performance.

C.10 Open versus closed systems

This clause describes two types of authentication systems employing biometric technology: open systems and closed systems (see Table C.12).

Table C.12 — Closed versus open systems

Characteristic	Closed (proprietary) system	Open system
Software	Knowledge of which biometrics are used (e.g. fingerprint, voice, iris) is kept proprietary or secret from the public.	Knowledge of which biometrics are used is non-sensitive or public information.
	Users are discouraged from using the same biometric technique and biometric data in different systems.	Users are allowed to make use of the same biometric technique and data across many different systems.
Hardware	Biometric readers are located in private and controlled spaces.	Biometric readers are located in public places.
Data	Biometric information is not shared outside the system, because doing so could diminish or potentially compromise the system.	Biometric information is shared among many biometric systems under the control of different organizations, and across different jurisdictions.
	Biometric information is kept confidential, and thus shall be encrypted when transmitted over communication lines and/or in storage.	Biometric information is treated as non-secret data, and hence encryption is unnecessary when transmitted or stored for reasons of confidentiality.
	Biometric information becomes invalid when a user's biometric data has been disclosed in an unauthorized manner.	Unauthorized disclosure of a user's biometric data does not invalidate the biometric information.

In a closed system (self-contained, limited number of users, single enterprise), the following characteristics apply.

— The security afforded by a biometric protection mechanism may be enhanced by keeping details of the biometric system secret, by keeping the identity of the users of the biometric system secret, and by keeping the biometric data itself secret.

— It may be possible to keep biometric data secret, and hence a closed system may be able to derive the security benefit by keeping biometric data secret. Consequently, mechanisms such as cryptographic encryption or physical protection may be used to ensure the confidentiality of the biometric data between any two components, and within any component.

— Mechanisms may be used to ensure that biometric information is not shared outside the system and users are not using the same biometric technique and biometric data in different systems.

— Mechanisms may be used to ensure that biometric readers are located in private and controlled spaces.

— Mechanisms may be used to ensure that the knowledge of a specific biometrics, which is used in the system, is kept secret.

— Mechanisms may be used to ensure that biometric information of a user, upon termination, is securely erased from any component of an authentication system to prevent unauthorized disclosure of the biometric information.

In an open system (global and ubiquitous, large number of users, same biometric technique employed by multiple vendors and organizations), the following characteristics are found.

a) The quality of protection when biometric information is shared by two or more systems will not undermine or diminish the biometric security in any of these systems, i.e. if the quality of protection is undermined in one system because of poor implementation, this will not affect or undermine the quality of protection in any other system.

b) The security of biometric solutions constructed using the “proprietary model” is inherently undermined. The security assumptions of the “proprietary model” are in conflict with an open-systems environment.

NOTE The details of the biometric system, and the biometric method, cannot be kept secret (see Reference [8])

— where biometric reader devices are sometimes located in public places,

— where the users of the biometric system are known or knowable,

— where an adversary may be able to collect biometric samples outside the biometric system, and

— where sampled biometric data based on “like” biometric techniques, and even biometric templates, can be shared among different systems, among different organizations, on a worldwide basis.

c) The biometric technique shall be robust, such that “like” biometric data sampled from one user in one biometric system will not undermine the security of another biometric system. The quality of protection afforded by one biometric system is not diminished or undermined by another biometric system (e.g. where biometric information for a set of users is shared across many biometric systems).

d) The security of any one biometric system shall be independent of the number of different biometric systems that employ the same biometric technique or that sample “like” biometric data from the same selection of users.

e) The security of the global biometric infrastructure shall not be diminished if users of one biometric system are also users of another biometric system.

C.11 Compromise/loss of biometric data

This addresses issues, such as the biometric data confidentiality, which are not required in order to ensure the integrity and accuracy of the biometric identification system, but which may be required due to other factors, such as privacy laws, liability protection or customer satisfaction (see Table C.13).

Table C.13 — Compromise/loss

Points of entry or attack	Protection mechanisms	Relevant component
a) all interfaces that carry raw biometric data, processed (e.g. feature-extracted) biometric samples or biometric templates b) storage media holding biometric templates	a) use encryption to prevent unauthorized disclosure of the biometric information b) physically protect all interfaces (e.g. do all processing in a single physically secure module)	— capture — process — transmission — storage

C.12 Data compression

In order to reduce the amount of data transmitted, many systems employ compression algorithms for the raw biometric data, the template data, or both. The data is decompressed prior to use at the receiving end.

There are two distinct classes of compression algorithms:

— lossy, and

— lossless.

With a lossless system, the decompressed signal is identical to the original input signal in every detail. With a lossy system, however, some data fidelity is sacrificed in order to achieve significantly greater reduction in data size. Lossy compression is acceptable with some biometric techniques, and unacceptable with others. There is a trade-off between the amount of signal degradation due to compression and the accuracy of the biometric verification.

C.13 System circumvention

The presence of a fall-back authentication mechanism, such as a password or a secondary biometrics, may impel an impostor to fail an authentication attempt intentionally or to fail to enrol in a biometric system intentionally. By failing the primary authentication or enrolment method, normally the stronger of the two methods, the would-be impostor can attack the secondary biometric or authentication technology.

Annex D
(normative)

Security requirements for biometric devices

D.1 Physical security

This International Standard specifies the security requirements that will be satisfied by a biometric device utilized within a security system protecting sensitive information. There are three increasing, qualitative levels of security: Level 1, Level 2, and Level 3. The intention of having these three levels is to cover a wide range of potential applications and environments that employ biometric devices.

A biometric device shall employ physical security mechanisms in order to restrict unauthorized physical access to the contents of the device and to deter unauthorized use or modification of the device (including substitution of the entire device) when installed. All hardware, software, firmware and data components within the device shall be protected.

A biometric system that is implemented completely in software, such that the physical security of the biometric components is provided solely by the host platform, is not subject to the physical security requirements of this International Standard.

Depending on the physical security mechanisms of a biometric device, unauthorized attempts at physical access, use or modification will have a high probability of being detected subsequent to an attempt, because they leave visible signs (i.e. tamper evidence), and/or during an attempt, so that appropriate actions can be taken by the biometric device to protect secret and private information and any critical security parameters within the biometric device (i.e. tamper response).

This International Standard defines the general physical security requirements for each of three security levels of a biometric device. In general,

— Security Level 1 requires minimal physical protection,

— Security Level 2 requires the addition of tamper-evident mechanisms, and

— Security Level 3 adds requirements for the use of strong enclosures with tamper detection and response mechanisms for removable covers and doors.

Tamper detection and tamper response are not substitutes for tamper evidence.

Security requirements are specified for a maintenance access interface when a biometric device is designed to permit physical access (e.g. by the device vendor or other authorized individuals).

D.2 General physical security requirements

The following requirements shall apply to all biometric devices.

— Documentation shall specify the security level for which the physical security mechanisms of a biometric device are implemented.

— Documentation shall specify the physical security mechanisms of a biometric device.

If a biometric device includes a maintenance role that requires physical access to the contents of the device, or if the device is designed to permit physical access (e.g. by the device vendor or other authorized individual), the following shall apply:

a) a maintenance access interface shall be defined;

b) the maintenance access interface shall include all physical access paths to the contents of the biometric device, including any removable covers or doors;

c) any removable covers or doors included within the maintenance access interface shall be safeguarded using the appropriate physical security mechanisms;

d) all secret and private information and critical security parameters shall be zeroized when the maintenance access interface is accessed;

e) documentation shall specify the maintenance access interface, and how secret and private information and critical security parameters are zeroized when the maintenance access interface is accessed.

D.3 Security levels

D.3.1 Security Level 1

The following requirements shall apply to all biometric devices for Security Level 1.

— The biometric device shall consist of production-grade components that shall include standard passivation techniques (e.g. a conformal coating or a sealing coat applied over the device's circuitry to protect against environmental or other physical damage).

— When performing physical maintenance, secret and private information and other unprotected critical security parameters contained in the biometric device shall be zeroized. Zeroization shall either be performed procedurally by the operator or automatically by the biometric device.

If the biometric device is contained within an enclosure or removable cover, a production-grade enclosure or removable cover shall be used.

D.3.2 Security Level 2

In addition to the general requirements for Security Level 1, the following requirement shall apply to all biometric devices for Security Level 2.

The biometric device shall provide evidence of tampering (e.g. on the cover, enclosure, and seal) when physical access to the device is attempted. This may be achieved by covering the biometric device with a tamper-evident coating (e.g. a tamper-evident passivation material or a tamper-evident material covering the passivation) or by protecting the biometric device with a tamper-evident enclosure to deter direct observation, probing, or manipulation of the device, and to provide evidence of attempts to tamper with or remove the device. If a tamper-evident coating or tamper-evident enclosure is used, it shall be opaque within the visible spectrum.

If a tamper-evident enclosure is used, and the enclosure includes any doors or removable covers, then the doors or covers shall be locked with pick-resistant mechanical locks employing physical or logical keys, or shall be protected with tamper-evident seals (e.g. evidence tape or holographic seals).

Tamper-evident enclosures of biometric devices shall be opaque within the visible spectrum.

D.3.3 Security Level 3

In addition to the general requirements for Security Levels 1 and 2, the following requirements shall apply to all biometric devices for Security Level 3.

If the biometric device contains any doors or removable covers, or if a maintenance access interface is defined, then the device shall contain tamper response and zeroization circuitry. The tamper response and zeroization circuitry shall immediately zeroize all secret and private information and critical security parameters when a door is opened, a cover is removed, or when the maintenance access interface is accessed. The tamper response and zeroization circuitry shall remain operational when secret or private information or critical security parameters are contained within the biometric device.

If the biometric device contains ventilation holes or slits, then the holes or slits shall be constructed in a manner that prevents undetected physical probing inside the enclosure (e.g. there shall be at least one 90° bend or obstruction with a substantial blocking material).

Either the biometric device shall be covered with a hard, opaque, tamper-evident coating (e.g. a hard, opaque epoxy covering the passivation) or the enclosure shall be implemented so that attempts at removal or penetration of the enclosure shall have a high probability of causing serious damage to the biometric device (i.e. the device will not function).

Annex E
(informative)

Existing applications

E.1 Cash desks

Payments that cannot be effected by automated dispensers such as ATMs are made at secure cash desks operated by an authorized teller. In some regulatory environments, access to cash-desk areas are granted to tellers by a supervisor. Once access to the controlled area is granted, the cash desk is manned continuously by the teller. This system ensures that only authorized persons enter the controlled cash-desk environment, and requires that the supervisor monitor the teller to ensure that he/she remains in the controlled area.

If biometric technology were used to control access to this environment, access to the controlled area and operation of the cash desk could be limited only to authorized staff, and constant monitoring by a supervisor could be eliminated. The cash desk would only need to be manned for the time it takes a customer to conduct a transaction. The cash drawer could be automatically disabled and secured when the teller leaves the cash-desk area, and not enabled again until an authorized teller is present.

Access to the cash-desk area could be better controlled using biometrics, since tellers may share PINs or keys, but cannot share their biometrics. Each cash-drawer transaction could be linked to an individual teller, since access by biometrics could reveal who entered or exited the controlled area, not just which key or PIN was used. Since access could be limited to a small number of authorized persons, the biometric system could employ one-to-many matching to identify authorized tellers. The access control system could correlate an individual's entry to and exit from the controlled area, by including a time and date along with employee identification information when creating an audit trail of cash-drawer access control event journal records.

E.2 Dispensing banknotes

Some staff-operated banknote dispensers (cash drawers) require dual control for normal operation. These devices should only be operated when at least two staff are continuously present in the customer service area, and within each other’s field of vision. Biometric technology can be employed to ensure that only staff authorized to pay out withdrawals can access or exit the customer service area, remain continuously present, and are positioned as required for the exercise of dual control.

Additional biometrics-based technical features on banknote dispensers could be employed to ensure that these devices only operate when at least two authorized staff members are present in the customer service area and within each other’s field of vision. The addition of biometrics could create a controlled teller environment that would not require monitoring by bank management. Through event logging, a biometrics-based automated dispenser and service area could automatically monitor and control activities. This could then limit the period of continuous staff attendance from a constant period to only the time required to pay out withdrawals to meet customer demand.

E.3 Cheque fraud detection

Some financial institutions have implemented biometrics-based fraud detection systems, in which a bank customer signature on a cheque is matched against a previously enrolled reference signature. In these systems, when a bank customer opens an account, part of the enrolment process involves the customer signing his/her name to create a reference signature. This reference signature is then stored in a database linked to the customer’s account number or other identifier.

When the enrolled customer writes a cheque for payment, the signature on the cheque is extracted along with the account information. Cheque verification is completed using automated biometric signature verification technology. If the signature presented scores below an application-dependent threshold, a warning condition is raised and the cheque is placed on an exception list. A manual verification is then performed by a bank employee to determine if there are any obvious discrepancies in the signature.

If the bank employee believes the signature on the cheque could be fraudulent, the bank customer may be notified in an attempt to determine if they did indeed write the cheque. A “yes” response from the bank customer attesting to writing the cheque would lead to clearing the cheque. But a “no” response could lead to the bank refusing payment.

In the case of a fraudulent cheque, the account number would be added to a database (cheque verification service) of “bad cheques”, which could be used to detect the bad-cheque writer in the future for the purpose of denying future payments. In addition, the bank may close the account if it determines the cheque was fraudulently signed and cashed.

Bibliography

[1] ISO/IEC 7816-11, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

[2] ISO 10202 (all parts), *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards*

[3] ISO 11568 (all parts), *Banking — Key management (retail)*

[4] ISO/IEC 11770 (all parts), *Information technology — Security techniques — Key management*

[5] ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

[6] ISO 13491-1, *Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

[7] ISO/TR 13569:2005, *Financial services — Information security guidelines*

[8] ISO 15782 (all parts), *Certificate management for financial services*

[9] ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

[10] ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

[11] ISO/IEC 18032, *Information technology — Security techniques — Prime number generation*

[12] ISO/IEC 19784-1:2006, *Information technology — Biometric application programming interface — Part 1: BioAPI specification*

[13] ISO/IEC Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*

[14] PANKANTI, JAIN et al. *Personal Electronic Identification In A Networked Society*, Kluwer, 1999

[15] ANDERSON, ROSS and KUHN, MARKUS, *Tamper Resistance — A Cautionary Note*, Proceedings of the Second USENIX Workshop on Electronic Commerce, November 1996

[16] DR. MAYTAS, STEPHEN M. and STAPLETON, JEFF, A Biometric Standard for Information Management and Security, *Computer and Security*, July 2000

[17] ABRAHAM, D.G., DOLAN, G.M., DOUBLE, G.P. and STEVENS, J.V., Transaction Security System, *IBM Systems Journal*, vol. 30 No. 2, 1991

[18] DR. SOUTAR, COLIN, *Biometric System Performance and Security*, Presented at IEEE Workshop on Automatic Identification Advanced Technologies, September 1999

[19] WAYMAN, J.L. Error Rate Equations for the General Biometric System, *IEEE Robotics and Automation Magazine*, March 1999

[20] Biometrics Working Group (BWG), Best Practices in Testing and Reporting Performance of Biometric Devices, version 2.01, August 2002, http://www.cesg.gov.uk/biometrics/

ICS 03.060; 35.240.40

Price based on 77 pages