TECHNICAL REPORT

ISO/IEC TR 24741

First edition
2007-09-15

Information technology — Biometrics tutorial

Technologies de l'information — Tutoriel biométrique

Reference number
ISO/IEC TR 24741:2007(E)

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) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

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

ISO/IEC TR 24741, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics.*

Introduction

“Biometric authentication” is the automatic recognition of individual persons based on distinguishing biological and behavioural traits. The field is a subset of the broader field of human identification science. Example technologies include fingerprinting, face recognition, hand geometry, speaker recognition and iris recognition.

At the current level of technology, DNA analysis is a laboratory technique not fully automated and requiring human processing, so it is not considered “biometric authentication” under this definition (it is not currently automatic and fast, but may become so in the near future).

Some techniques (such as iris recognition) are more biologically based and some (such as signature recognition) are more behaviourally based, but all techniques are influenced by both behavioural and biological elements. There are no purely “behavioural” or “biological” biometric systems.

Biometric authentication is frequently referred to as simply “biometrics”, although this latter word has historically been associated with the statistical analysis of general biological data. The word “biometrics”, like “genetics”, is usually treated as singular. It first appeared in the vocabulary of physical and information security around 1980 as a substitute for the earlier descriptor “automatic personal identification”, in use in the 1970s. Biometric systems recognize “persons” by recognizing “bodies”. The distinction between person and body is subtle, but is of key importance in understanding the inherent capabilities and limitations of these technologies. In our context, biometrics deals with computer recognition of patterns created by human behaviours and biological structures, and is usually associated more with the field of computer engineering and statistical pattern analysis than with the behavioural or biological sciences.

Today, biometrics is being used to recognize individuals in a wide variety of contexts, such as computer and physical access control, law enforcement, voting, border crossing, social benefit programs and driver licensing.

Information technology — Biometrics tutorial

1 Scope

This Technical Report provides a tutorial on biometrics.

It contains a description of the architecture of biometric processes and of the processes themselves.

An annex provides further details of International Standards' activity in the field of biometrics.

A further annex provides terms and definitions that are in use in these International Standards.

2 Introduction and general history

2.1 What are biometric technologies?

The all-encompassing term 'biometrics' refers to the quantification or statistical analysis of biological characteristics. In this context, we are concerned with technologies that analyze human characteristics for recognition security purposes. The statistical science of biometrics, usually used in biomedical contexts, is a separate discipline. A broadly accepted definition of biometrics for recognition states that:

A biometric is a unique, measurable characteristic or trait for automatically recognizing or verifying the identity of a human being.

The agreed SC37 definition comes in two parts, and broadly agrees with the above. It is recommended that the word biometric be normally used only as an adjective, and not where the fuller term biometric characteristic (as above) would be more appropriate. We have for adjectival use:

biometric
of or having to do with biometrics

and for noun use:

biometrics
automated recognition of individuals based on their behavioural and biological characteristics

So, biometric technologies are concerned with the physical parts of the human body or the personal traits of human beings, and the recognition of individuals based on either or both of those parts or traits. It is important to note the term 'automatic' in the above definition. This essentially means that a biometric technology must recognize or verify a human characteristic quickly and automatically, in real time. (A fuller explanation of the various biometric technologies is given in clause 3.) In summary the most common *physical biometric characteristics* are the eye, face, fingerprints, hand and voice; while signature, typing rhythm and gait are the most common *behavioural biometric characteristics*. Use of DNA is excluded today, as it is not yet a fast automated process, although that is likely to change in the next few years.

2.2 History

In a non-sophisticated way, biometric characteristics have been used for centuries. Parts of our bodies and aspects of our behaviour have historically been used, and continue to be used, as a means of identification. The study of fingerprinting dates back to ancient China; we often remember and identify a person by their face or by the sound of their voice; and a signature is the established method of authentication in banking, for legal contracts and many other walks of life.

The modern science of recognizing people based on physical measurements owes much to the French police clerk, Alphonse Bertillon, who began his work in the late 1870s (Beavan, 2001 [3]; Cole, 2001 [11]). The Bertillon system involved multiple measurements, including height, weight, the length and width of the head, width of the cheeks, and the lengths of the trunk, feet, ears, forearms, and middle and little fingers. Categorization of iris colour and pattern was also included in the system. By the 1880s, the Bertillon system was in use in France to identify repeat criminal offenders. Use of the system in the United States for the identification of prisoners began shortly thereafter and continued into the 1920s.

Although research on fingerprinting by a British colonial magistrate in India, William Herschel, began in the late 1850s, knowledge of the technique did not become known in the western world until the 1880s (Faulds, 1880 [13]; Herschel, 1880 [18]) when it was popularized scientifically by Sir Francis Galton (1888) [16] and in literature by Mark Twain [47] (1893). Galton's work also included the identification of persons from profile facial measurements.

By the mid-1920s, fingerprinting had completely replaced the Bertillon system within the U.S. Bureau of Investigation (later to become the Federal Bureau of Investigation). Research on new methods of human identification continued, however, in the scientific world. Handwriting analysis was recognized by 1929 (Osborne, 1929 [36]) and retinal identification was suggested in 1935 (Simon and Goldstein, 1935 [44])

None of these techniques was "automatic", however, so none meets the definition of "biometric authentication" being used in this Technical Report. Automatic techniques require automatic computation (and are expected to be fast). Work in automatic speaker recognition can be traced directly to experiments with analogue filters done in the 1940s (Potter, Kopp and Green, 1947 [38]) and early 1950s (Chang, Pihl, and Essignmann, 1951 [10]). With the computer revolution picking up speed in the 1960s, speaker (Pruzansky, 1963 [39]) and fingerprint (Trauring, 1963 [46]) pattern recognition were among the very first applications in automatic signal processing. By 1963, a "wide, diverse market" for automatic fingerprint recognition was identified, with potential applications in "credit systems", "industrial and military security systems" and for "personal locks". Computerized facial recognition research followed (Bledsoe, 1966 [6]; Goldstein, Harmon, and Lesk, 1971 [17]). In the 1970's, the first operational fingerprint and hand geometry systems were fielded (for example, the Identimat system), results from formal biometric system tests were reported (Wegstein, 1970 [52] ;), measures from multiple biometric devices were being combined (Messner, Cleciwa, Kibbler, and Parlee, 1974 [27]; Fejfar, 1978 [14]) and government testing guidelines were published (NBS, 1977 [28]).

Running parallel to the development of hand technology, fingerprint biometrics were making progress in the 60s and 70s. During this time a number of companies were involved in automatic identification of fingerprints to assist law enforcers. The manual process of matching prints against criminal records was laborious and used up far too much manpower. Various fingerprint systems developed for the FBI in the 1960s and 70s increased the level of automation, but these were ultimately based on human fingerprint comparisons. Automated Fingerprint Identification Systems (AFIS) were first implemented in the late 70s, most notably the Royal Canadian Mounted Police AFIS in 1977. The role of biometrics in law enforcement has mushroomed since then and Automated Fingerprint Identification Systems (AFIS) are used by a significant number of police forces throughout the globe. Building on this early success, fingerprinting is now exploring a range of civilian markets.

In the 1980s, fingerprint scanners and speaker recognition systems were being connected to personal computers to control access to stored information. Based on a concept patented in the 1980s (Flom and Safir, 1987 [15]), iris recognition systems became available in the mid-1990s (Daugman, 1993 [12]). Today there are close to a dozen approaches used in commercially-available systems, utilizing hand and finger geometry, iris and fingerprint patterns, face images, voice and signature dynamics, computer keystroke, and hand vein patterns.

Today's speaker verification systems have their roots in technological achievements of the 1970s, while biometric technologies such as signature verification and facial recognition are relative newcomers to the industry. The migration from R&D towards commercialization continues today. Research in universities and by biometric vendors throughout the globe is essential for refining the performance of existing biometric technologies, while developing new and more diverse techniques. The hard part is bringing a product to market and proving its operational performance. It does take time for a system to become fully operational. However, such systems are now in place and proving themselves across a range of diverse applications.

3 Technology overview

Biometric systems now come in many shapes and sizes. This can range from hardware, software, OEMs, software development kits or complete solutions. Systems may be marketed and sold by vendors directly or through various distribution channels, such as systems integrators, strategic partners or value added resellers. All biometric systems have the principles of capture, extraction, and comparison in common. Yet, biometric technologies focus on different parts of the human make-up, so the workings of each technology and each vendor's specific system will differ. This clause looks at the operation of each biometric technology within the four stages of capture, extraction, comparison and decision.

3.1 Eye technologies

Biometric technologies that analyze the eye are generally thought to offer the highest levels of accuracy at present, and differ even between identical twins. They can be divided into two specific technologies: iris biometric characteristics and retina biometric characteristics.

3.1.1 Iris characteristics

The iris is the coloured ring of textured tissue that surrounds the pupil of the eye. Each iris is a unique structure, featuring a complex pattern. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, radial furrows and striations. It is claimed that artificial duplication of the iris is virtually impossible because of its unique properties and that no two irises are alike. The iris is closely connected to the human brain and is thought to be one of the first parts of the body to be rendered unusable for biometric recognition after death. It is therefore very unlikely that an artificial iris could be recreated or that a dead iris could be used to fraudulently by-pass the biometric system. (Equally, this means that identification of a dead body using recorded iris data is unlikely to work as well as DNA, which survives death very well under most conditions - heat and salt-water excluded.)

In most implementations, a grayscale image of the iris is acquired in the near-IR spectrum to maximize detail in dark-colored eyes; some implementations capture irises in color. This should be done in a well-lit environment. Non-patterned contact lenses do not interfere with image capture. Sunglasses and glasses, however, should not be worn as these can affect the capture process.

Unique features of the iris are extracted from the captured sample by the biometric engine. These features are then converted into a unique mathematical code and stored as a template (a biometric reference) for that individual.

3.1.2 Retina characteristics

The retina is the layer of blood vessels situated at the back of the eye. As with the iris, the retina forms a unique pattern and is thought to be one of the first parts of the body to be rendered unusable for biometric recognition after death. A precise enrolment procedure is necessary, which involves lining up the eye to achieve an optimum reading.

The eye is positioned in front of the system, The eye is positioned in front of the system, at a capture distance ranging from 8 cm to one metre.. The subject must look at a series of markers, viewed through the eyepiece,

and line them up. When this is done, the eye is sufficiently focused for the scanner to capture the retina pattern. The retina is scanned and the unique pattern of the blood vessels is captured.

The biometric engine maps out the position of the blood vessels; a unique mathematical representation is extracted and stored as a template (a biometric reference) for that individual.

3.2 Face technologies

The face is a key component in determining the way human beings remember and recognize each other. Automatically identifying an individual by analyzing a face is a complex process which can require sophisticated artificial intelligence and machine learning techniques. A number of biometric vendors and research institutions have developed facial recognition systems, using either standard video or thermal imaging to capture facial images. Because people change over time, and facial hair, glasses and the position of the head can affect the way a biometric system can match one face with another, machine learning is important in order to adapt to changes and accurately compare new samples with previously recorded templates.

Standard video techniques use a facial image, or collection of images, captured by a video camera. The precise position of the subject's face and the surrounding lighting conditions may affect the system's performance. The complete facial image is usually captured and a number of points on the face can then be mapped out. For example, the position of the eyes, mouth and nostrils may be plotted so that a unique template is built. Three-dimensional maps of the face can be created through various means, such as the projection of an infrared grid ("structured light"), merging of multiple images, or using shading information in a single image.

Thermal imaging analyzes heat caused by the flow of blood under the face. A thermal camera captures the hidden, heat-generated pattern of blood vessels underneath the skin. Because infrared cameras are used to capture facial images, lighting is not important, and systems can capture images in the dark. However, such cameras are significantly more expensive than standard video cameras.

A proprietary algorithm or neural network within the biometric engine will convert the facial image sample into a pattern and then a unique mathematical code. This is stored as a template (a biometric reference) for that individual.

3.3 Finger ridge technologies

3.3.1 Finger scanning

Finger image biometrics are largely regarded as an accurate method of biometric identification and verification. Most one-to-many AFIS and one-to-one fingerprint systems analyze small unique marks on the fingerprint – which are known as minutiae. These may be defined as fingerprint ridge endings, or bifurcations (branches made by fingerprint ridges). Some fingerprinting systems also analyze tiny sweat pores on the finger which, in the same way as minutiae, are uniquely positioned to differentiate one person from another. Finger image density, or the distance between ridges, may also be analyzed.

Certain conditions may affect the prints of different individuals. For example, dirty, dry or cracked prints will all reduce the quality of image capture. Age, gender and ethnic background are also found to have an impact on the quality of finger images. The way a subject interacts with a finger scanner is another important consideration. By pressing too hard on the scanner surface, for example, an image can be distorted. Vendors are addressing these problems so that scanners are ergonomically designed to optimize the fingerprinting process.

A key difference between the various fingerprint technologies on the market is the means of capturing an image. One-to-one fingerprint verification systems use four main capture techniques: optical, thermal or tactile, capacitance and ultra-sound. Most one-to-many systems capture finger images using the optical technique or by electronically scanning images from paper.

3.3.2 Finger image verification

The optical image technique typically involves generating a light source, which is refracted through a prism. Subjects place a finger on a glass surface, known as a platen. Light shines on the fingerprint and the impression made by the print is captured.

Tactile or thermal techniques use sophisticated silicon chip technology to acquire fingerprint data. A subject places a finger on the chip sensor which senses heat or pressure from the finger. Fingerprint data is then captured.

Capacitance silicon sensors measure electrical charges and give an electrical signal when a finger is placed on the sensor surface. The core element of capacitance techniques, as with tactile and thermal methods, is the chip sensor. Using capacitance, the peaks and troughs of fingerprint ridges and valleys are analyzed. An electrical signal is given when fingerprint ridges contact the sensor. No signal is generated by the valleys. This variance in electrical charge produces an image of the fingerprint.

Ultra-sound image capture uses sound waves beyond the limit of human hearing. A finger is placed on a scanner and acoustic waves are used to measure the density of the fingerprint pattern.

The biometric engine extracts fingerprint data contained in the print. A unique mathematical representation of the print is then stored as a template (a biometric reference) for that individual.

3.3.3 Finger image identification

For one-to-many identification, individuals are enrolled using the optical live-scan capture process described above for finger image verification. Law enforcement AFIS systems, also known as booking stations, capture all ten fingerprints. A civil AFIS, however, need not capture all fingerprints and can operate effectively using one or two. Latent prints, those taken from the scene of a crime, or inked images on paper can also be captured by the AFIS using a flatbed scanner.

For an AFIS, the process of binning fingerprints refines the extraction process. Minutiae data is extracted and is stored as a template (a biometric reference) for that individual.

A new sample, captured by either live-scan, latent or paper scanning techniques, is compared against the database of references. If binning has taken place the comparison will be against the bin that holds similar features as the newly presented print.

3.3.4 Palm technologies

Palm biometrics can be closely aligned with fingers-canning, and in particular AFIS technology. Ridges, valleys and minutiae data are found on the palm, as with fingerprints. These are usually analyzed using optical capture techniques. This area of the biometrics industry is particularly focused on the law enforcement community, as latent palm prints are equally as useful in crime detection as latent fingerprints. However, certain vendors are also looking at the access control market and hope to migrate to civil applications, following in the footsteps of fingerprinting.

Palm biometric characteristics are predominantly used for one-to-many identification and the capture process is essentially the same as the optical technique described for fingerprinting. A palm print system captures prints when a hand is placed on a scanner. Latent or ink palm prints can also be scanned into the system in the same way as an AFIS.

Minutiae data are extracted by the biometric engine and the palm print data is stored as a template (a biometric reference) on a database.

A newly captured print, by either live-scan, latent or paper scanning techniques, is compared against the database of reference templates.

3.4 Hand geometry technologies

Hand geometry takes one or more two-dimensional images of the hand and measures the shape and length of fingers and knuckles. It has been widely used since the early 1980s – predominantly for access control applications. Although hand geometry, like finger geometry (see below), does not achieve the highest levels of accuracy, it is convenient to use and the primary advantage is that large volumes of subjects can be processed quickly. For this reason, hand and finger geometry are often used for repeat accesses to theme parks.

A subject places a hand on the hand reader, aligning fingers with specially positioned guides. A mirror reflects light horizontally across the top of the hand, supplying a second two-dimensional shadow of the side of the hand. A camera, positioned above the hand, captures an image. Measurements of selected points on the hand are then taken.

The biometric engine extracts the measurements into a unique mathematical identifier and a template (a biometric reference) is created for that individual.

Hand geometry is predominantly used for one-to-one verification. A new sample is compared against a database of templates (references).

3.5 Finger geometry technologies

A handful of biometric vendors use finger geometry, or the measurement of finger shape, to determine identity. This technology uses similar principles to hand geometry. The geometry of one or two fingers may be analyzed, depending on the biometric system being used. Measurements of unique finger characteristics, such as finger width, length, thickness and knuckle size are then taken. Finger geometry systems can perform one-to-one verification or one-to-many identification. The main advantage is that systems are robust and can accommodate a high throughput of subjects.

As with fingerprint verification, the method of capture depends on the system being used. There are currently two main techniques on the market.

The first measures the geometry of two or more fingers. A mirror reflects light horizontally across the top of the hand, supplying a second two-dimensional shadow of the side of the hand. A camera, positioned above the hand, now takes a three-dimensional measurement when a subject places the index and middle finger, of either the right or left hand, onto the reader.

The second technique requires a subject to insert a finger into a tunnel so that three-dimensional measurements of the finger can be taken.

The three-dimensional measurements are then extracted by the biometric engine and a template (a biometric reference) is then created for that individual.

3.6 Dynamic signature technologies

Signature biometrics is often referred to as *dynamic signature verification* (DSV) and look at the way we sign our names or initial a document. It is the method of signing rather than the finished signature that is important. Thus DSV can be differentiated from the study of static signatures on paper. A number of characteristics can be extracted and measured by DSV. For example, the angle at which the pen is held, the time taken to sign, the velocity and acceleration of the signature, the pressure exerted when holding the pen and the number of times the pen is lifted from the paper – can all be extracted as unique behavioural characteristics. DSV is not based on a static image, so even if a signature is traced, a forger would need to know the dynamics of that signature. This makes forgery very difficult.

The other advantage of signature biometric technologies is that the signature is one of the most accepted means of asserting identity. It is also used in a number of situations to legally bind an individual, such as the signing of a contract. These factors have taken signature biometrics to a number of diverse markets and applications, ranging from checking welfare entitlement, to document management and pen-based computing.

Note that dynamic signature data can be captured using an electronic signature pad without the subject's knowledge.

Signature data can be captured via a special sensitive pen or tablet. The pen-based method incorporates sensors inside the pen. The tablet method relies on the tablet to sense the unique signature characteristics. Another variation on these two techniques is acoustic emission which measures the sound that a pen makes against paper. Typically for DSV systems, as for all other biometrics, a subject will enrol a number of times so that the system can build a profile of the signing characteristics.

The unique signature characteristics are extracted, coded by the biometric engine and stored as a template (a biometric reference) for that individual.

3.7 Speaker recognition technologies

Speaker recognition is a biometric technology used to verify or identify a speaker through the sound of the voice. Speaker recognition should not be confused with the related non-biometric technology of speech recognition, which is used to recognize words for dictation or automate instructions given over the telephone.

The sound of a human voice is caused by resonance in the vocal tract. The length of the vocal tract, the shapes of the mouth and nasal cavities are all important. Sound is measured, as affected by these specific characteristics. The technique of measuring the voice may use either text-independent or text-dependent methods. In other words, the voice may be captured with the subject uttering a specifically designated response to a challenge, combining phrases, words or numbers (text-dependent) or by speaking any form of phrase, words or numbers without a specific challenge (text-independent). Currently, text-dependent (challenge-based) techniques are dominant in commercially available speaker recognition systems.

Speaker recognition technologies are particularly useful for telephone-based applications. We are all used to speaking on the telephone and biometric systems can be easily incorporated into private or public telephone networks. However, environmental background noise and interference over these networks can affect the performance of speaker recognition systems.

Subjects speak into a microphone and utter a previously selected (text-dependent) or random (text-independent) phrase. This process is usually repeated a number of times during enrolment to build a sufficient profile of the voice.

The biometric engine extracts the unique voice signal and a model (a biometric reference) is created.

One-to-one verification is the preferred method. The subject speaks into a microphone; the new voice sample and biometric reference are then compared.

3.8 Vein patterns

Biometric technologies that analyze vein patterns are considered to offer high authentication accuracy. The veins that exist in the hypodermic areas of the human body form a unique pattern for each person. Even the patterns of genetically identical twins differ. Furthermore, the vein pattern is information within a human body, so it is safe information that cannot be easily stolen by other persons by use of normal photography or from objects that the person has been in contact with (compare fingerprints).The underlying vein pattern can be captured using infra-red light. Any area of the skin where infra-red light is reflected produces a light image. On the other hand, a darker image is obtained for the vein pattern, since the reduced haemoglobin in the vein absorbs the infra-red light. The image capturing system can therefore acquire the unique vein pattern made by the darker vein image.

In actual products, the parts of body chosen (such as the palm, fingers, wrist and the back of the hands) are the parts where a user can easily present the blood vessel pattern to the sensor. The vein patterns are extracted, coded by the biometric engine and stored as a template (a biometric reference) for that individual.

There are two types of vein imaging methods. They are the reflection type and the transmission type. The reflection type directs the infra-red light onto the region to be photographed. The transmission type directs the infra-red light in such a way that the light passes through the part of the body that is being imaged.

Using image data processing techniques, we can get clear and constant vein patterns.

3.9 Keystrokes

Keystroke biometrics, more commonly referred to as keystroke dynamics, analyze typing rhythm. Keystroke dynamics are behavioural and evolve over time as subjects learn to type and develop their own unique typing pattern. The ultimate aim is to be able to continually check the identity of a person as they type on a keyboard. This is obviously a difficult task as subjects often become tired or distracted during the course of a day, which in turn affects typing rhythm.

3.10 Possible future biometric technologies

Biometric technologies of the future are likely to be advanced versions of the biometric technologies described above. For all biometric technologies, there are remaining needs for improvement in capture (including speed, ergonomics, accuracy, and improving capture quality), as well as matching (including improved accuracy, speed, and tolerance of poor-quality data). Despite the success to date of existing biometric technologies, research and development of some more varied and interesting technologies continues to progress.

3.10.1 Scent

A system that analyzes the chemical make-up of body scent is currently in development. Here sensors are capable of capturing the scent from non-intrusive parts of the body such as the back of the hand. Each unique human smell is made up of chemicals known as volatiles. These are extracted by the system and converted into a template.

3.10.2 DNA

Analysis of human DNA, although now possible within ten minutes, is not yet sufficiently automatic to rank DNA as a biometric technology. When technology advances so that DNA can be matched automatically, in real time, DNA may emerge as a significant contender against the existing biometric industry. However DNA sampling is at present extremely intrusive and usually requires some form of tissue, blood or other bodily sample. This method of capture will have to be refined.

3.10.3 Ear shape

Identifying individuals by ear shape is used in law enforcement applications where ears are visible in photographs, but this is currently a manual process. Research is progressing into using ear shape as a biometric, which would presumably be used in conjunction with face recognition, especially for profile images.

3.10.4 Body potential differences

An interesting new technique being researched involves measuring the (small) potential differences that exist between the left and right sides of the body. These potential differences vary in a unique pattern that repeats every heart-beat (due to blood surges through the body). The measurement technique is by a simple credit-card-sized card with contacts on it for the left and right hands.

4 A general biometric system

NOTE See A.2 for a layered model of biometric standards.

4.1 Conceptual diagram of a general biometric system

Given the variety of applications and technologies, it might seem difficult to draw any generalizations about biometric systems. All such systems, however, have many elements in common. Biometric samples are acquired from a subject by a sensor. The sensor output can be sent to a processor which extracts the distinctive but repeatable measures of the sample (the "features"), discarding all other components. The resulting features can be stored in the database as a "reference", sometimes called a "biometric reference" or (in this case) a biometric "template". In other cases the sample (without feature extraction) may be stored as the biometric reference. A new sample can be compared to a specific reference, to many references or to all references already in the database to determine if there is a match. A decision regarding the identity claim is made based upon the similarity between the sample features and those of the reference or references compared.

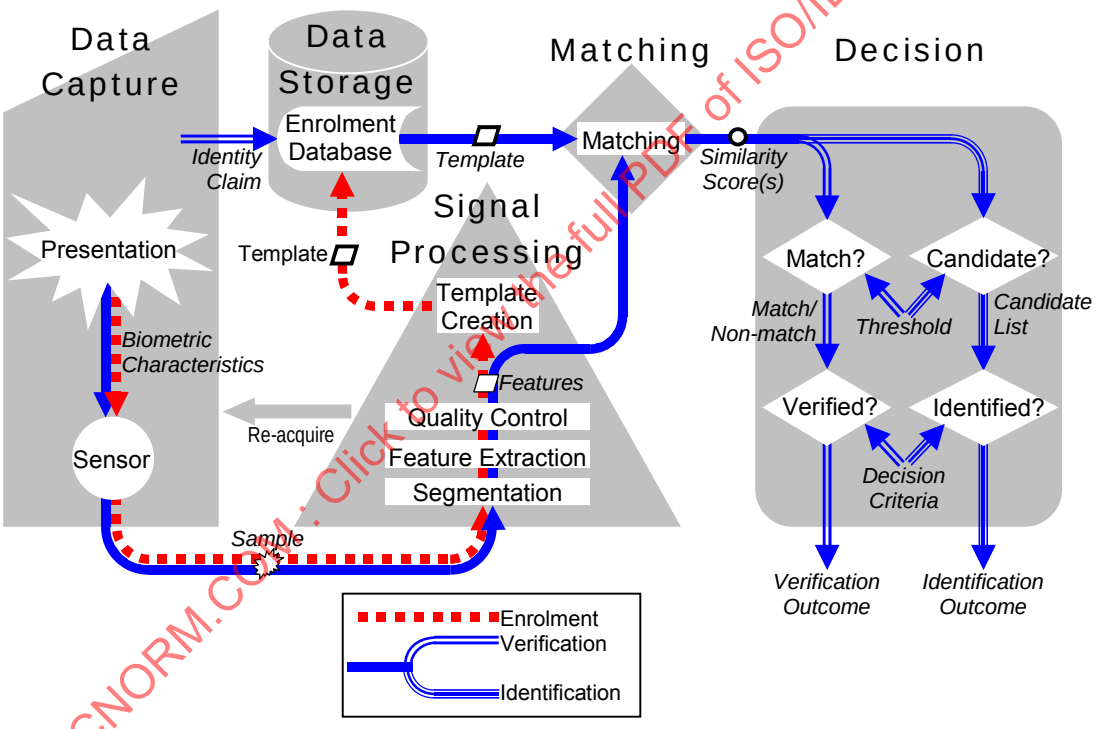

Figure 1 — Components of a general biometric system

Figure 1 illustrates the information flow within a general biometric system, showing a general biometric system consisting of *data capture*, *signal processing*, *storage*, *matching* and *decision* subsystems. This diagram illustrates both enrolment, and the operation of verification and identification systems. The following subclauses describe each of these subsystems in more detail. It should be noted that, in any real biometric system, these conceptual components may not exist or may not directly correspond to the physical components.

4.2 Conceptual components of a general biometric system

4.2.1 Data capture subsystem

The *data capture subsystem* collects an image or signal of a subject's *biometric characteristics* that they have *presented* to the *biometric sensor*, and outputs this image/signal as a *biometric sample* (also known as a *biometric data block (BDB)* − see 6.1).

Biometric systems begin with the collection of a signal from a behavioural/biological characteristic. As data from a biometric sensor can be one- (speech), two- (fingerprint) or multi-dimensional (handwriting dynamics), we are not generally dealing with "images". To simplify our vocabulary, we refer to raw signals simply as "samples".

Key to all systems is the underlying assumption that the signal from the biometric characteristic being observed is both distinctive between individuals and repeatable over time for the same individual. Therefore, it is desirable that there be as much variation between individuals and as little variation within an individual as possible. The challenges of measuring and controlling these variations begin in the data collection subsystem.

The subject's characteristic must be observed by a sensor, such as a microphone, CCD-based fingerprint scanning chip, digital camera, or computer keyboard. In systems where a subject seeks verification of a positive claim to an enrolled identity, the subject can cooperatively present the characteristic to the sensor. The act of presenting a biometric characteristic to a sensor introduces a behavioural component to every biometric method as the subject must interact with the sensor in the collection environment. The output of the sensor is the combination of: 1) the biometric characteristic; 2) the way the characteristic is presented; and 3) the technical characteristics of the sensor. All measurements and decisions made by the system will be based on this sensor output. Both the repeatability and the distinctiveness of the measurement are negatively impacted by changes in any of these three factors. If a system is to exchange data with other systems, the presentation and sensor characteristics must be standardized to ensure that biometric characteristics collected with one system will match those collected on the same individual by another system.

4.2.2 Transmission subsystem

NOTE This is not shown in figure 1

The *transmission subsystem* (not always present or visibly present in a biometric system) will transmit *samples, features,* and/or *references* between different subsystems. *Samples, features* or *references* may be transmitted using *biometric information records* (BIRs) consisting of standard biometric data interchange formats for *biometric data blocks - BDBs* with additional metadata (see 6.1). The biometric *sample* may be compressed and/or encrypted before transmission, and expanded and/or decrypted before use. A biometric *sample* may be altered in transmission due to noise in the transmission channel as well as losses in the compression/expansion process. It is advisable that cryptographic techniques be used to protect the authenticity, integrity, and confidentiality of stored and transmitted biometric data.

Some biometric systems collect data at one location but process it at another (see 6.3). If a great amount of data is involved, data compression may be required to conserve transmission bandwidth. Those systems requiring storage of the biometric samples usually do so in a compressed format. Figure 1 shows compression and transmission occurring before signal processing or sample storage. In the BioAPI/BIP architecture (see 6.3 and 6.4), the BIR would be processed locally before transmission to a remote application using the *BioAPI Interworking Protocol*. The transmitted or stored compressed data could be expanded before further use, or could be obtained by feature extraction. There are no current SC37 standards for general compression, only feature extraction as the result of processing a BDB to produce another type of BDB. The process of general compression and expansion generally causes quality loss in the restored signal, with loss increasing with higher compression ratios. An interesting area of research is in finding, for a given biometric technique, compression methods with minimum negative impact on the subsequent signal processing activities. Interestingly, limited compression has been seen in some fingerprint matching cases to improve the performance of the pattern recognition software (see Watson, C.I. and Wilson, C.L. (2005) [50] table 6), as information loss in the original signal is generally in the less repeatable high frequency components.

4.2.3 Signal processing subsystem

The *signal processing subsystem* extracts the distinguishing *features* from a biometric *sample*. This may involve locating the signal of the subject's *biometric characteristics* within the received *sample* (a process known as *segmentation*), *feature extraction*, and *quality control* to ensure that the extracted features are likely to be distinguishing and repeatable. Should *quality control* reject the received *sample/s*, control may return to the *data capture subsystem* to collect a further *sample/s*.

In the case of enrolment, some systems, such as those used with current e-passports, may simply store the acquired sample as the reference characterizing the subject. In other systems, such as some ID cards, the *signal processing subsystem* creates a *template* from the extracted biometric *features* to be used as the reference. Often the enrolment process requires *features* from several presentations of the individual's *biometric characteristics* for the creation of a template usable as a reference. Yet other systems, such as speaker and face recognition systems, may create as the reference more mathematically abstract "models" from the extracted features. Regardless of whether consisting of samples, templates or models, the reference will serve as the basic characterization of the subject for all further recognition.

The biometrics signal processing subsystem is composed of four modules: segmentation, feature extraction, quality control, and (for enrolment only) template creation. This is all encompassed by the "processing BSP" concept in BioAPI. The segmentation module must determine if biometric signals exist in the received data stream (signal detection) from the device and, if so, extract the signal from the surrounding noise. If the segmentation module fails to properly detect or extract a biometric signal, we say that a "failure-to-acquire" has occurred. In the BioAPI architecture, this is reported as an event (through the BioAPI Framework) to the controlling application.

The feature extraction module (the same or a different Biometric Service Provider (BSP), in BioAPI terms - see 6.3) must process the signal in some way to preserve or enhance the between-individual variation (distinctiveness) while minimizing the within-individual variation (non-repeatability). The output of this module is a set of numbers which, although called biometric "features", may not have direct biological or behavioural interpretation. For example, the numerical values developed by a facial recognition system do not indicate the width of the lips, length of the nose, or the distances between the eyes and the mouth, but rather represent the face in a more abstract, mathematically-based way. The Basic Data Block (BDB) formats (see 6.1) that record the results of feature extraction are an important part of SC37 standardization.

The quality control module analyzes the extracted features to make sure that they contain a sufficient quality and quantity of features to be processed effectively. If the quality check fails, the system may be able to alert the subject to recapture the biometric sample(s). If the biometric system is ultimately unable to produce an acceptable feature set from a subject, a "failure-to-enrol" or a "failure-to-acquire" will be said to have occurred, and will be sent via the BioAPI Framework to the controlling application. "Failure-to-enrol/acquire" may be due to failure of the segmentation algorithm, in which case no feature set will be produced. The quality control module might even impact the decision process, directing the decision subsystem to adopt higher requirements for matching a poor quality input sample, for instance.

The template creation module (on the enrolment path only - see figure 1) produces a biometric template (also called a reference template, a biometric reference, a model, or just a reference) that is a BDB in a defined (usually standardised) format that is suitable for storage and future use in the matching subsystem. It provides an unambiguous pointer or "reference" to the human being that was enrolled.

4.2.4 Data storage subsystem

References are stored within an *enrolment database* held in the *data storage subsystem*. Each *reference* is associated with details of the enrolled subject. It should be noted that prior to being stored in the *enrolment database*, *references* may be re-formatted into a standardized biometric data interchange format - a Biometric Information Record (BIR) consisting of a Biometric Data Block together with some metadata. *References* may be stored within a biometric capture device, on a portable medium such as a smart card, locally such as on a personal computer or local server, or in a central database.

In BioAPI terminology (see 6.3), this is an archive *biometric service provider (BSP)*. The processed features or the feature generation model of each subject will be stored or "enrolled" in a database for future comparison by the pattern matcher (*comparison BSP*) to incoming feature samples. Systems for verifying negative claims of identity require a centralized database of all enrolled templates (or the equivalent, linked decentralized databases, probably using the *BioAPI Interworking Protocol (BIP)* (see 6.4) to access them) to verify a claim that a person is not enrolled in the system. Such systems generally return the records of any previous enrolments found, so are called "identification" systems. Large-scale identification systems may partition the database using factors such as gender or age so that not all centrally-stored templates need be examined to establish that a person is not in the database. Such systems are sometimes loosely called "one-to-N" to indicate that a submitted sample must be compared to multiple enrolment (reference) templates or models.

For systems that only verify positive claims to a specific identity, the database of templates may be distributed on magnetic stripe, optically-read or smart cards carried by each enrolled subject. Although no centralized database needs to exist in this case, the absence of a central database makes checking for multiple enrolments impossible and complicates the replacement of lost or damaged cards. Such positive verification systems are sometimes loosely called "one-to-one" to indicate that biometric samples might be compared to the reference templates or models of only the single claimed identity. However, verification systems based on likelihood estimation techniques compare samples not only to the claimed enrolment (reference) templates, but also to the templates of other subjects or to "background models" so might not really be "one-to-one".

Although distributed or card storage is possible, positive claim verification systems might still use a centralized, encrypted database to prevent creation of counterfeit cards or to reissue lost cards without re-collecting the biometric measures.

The original biometric measurement, such as a fingerprint pattern, is generally not reconstructable from the stored reference templates. However, if access can be had to unencrypted templates, it is quite possible for a knowledgeable hacker in possession of an identical system to construct an artefact capable of re-generating the accessed template. Although this artefact will not have exactly the same visible pattern as the original biometric sample, the biometric system will generate the same template. For this reason, biometric templates are always treated as sensitive data and will generally require restricted access and (especially during transmission) cryptographic means to prove their integrity and authenticity. The decision to maintain a centralized reference template database for verification applications should be done with an assessment of the privacy and security risks should the database be compromised, as well as any associated privacy issues.

Biometric templates are usually created using the proprietary feature extraction algorithms of the system vendor, although the standardized BDB formats that record features provide considerable guidance on how to do feature extraction for these formats. Table 1 shows some typical examples of unencrypted template sizes for various biometric technologies.

Table 1 — Typical Biometric Template Sizes

Device	Size in Bytes
Fingerprint	200 – 2,000
Speaker	2,000 upwards (text dependent) 4,000 - 50,000 (text independent)
Finger Geometry	14
Hand Geometry	9
Face	100 – 3,500
Iris	512
Vascular	256 - 1,000

4.2.5 Matching subsystem

In the *matching subsystem*, the *features* are compared against one or more *references* and *comparison scores* are passed to the *decision subsystem*. The *scores* indicate the degree of fit between the *features* and *reference/s* compared. For verification of a claim of enrolment in a simple system, a single specific claim of a subject would lead to the comparison of a submitted sample to a single reference, resulting in a single *comparison score* between the submitted sample and the claimed reference. For identification of an unknown

individual without a claim to a specific reference, many or all *references* in the database may be compared with the *features*, resulting in the output of a *score* for each comparison, or a list of "candidate" matches from the database.

The pattern matching module compares sample feature data with previously enrolled feature data (“reference templates”) from the database and produces a numerical “comparison score”. When both template and features are vectors, the comparison may be as simple as a Euclidean distance. Neural networks or statistical measures, such as likelihood ratios, might be used instead. Comparison algorithms are not currently being standardized in SC37, as many are "company confidential" or subject to Intellectual Property Rights (IPR) and patent rights, but the concept of a "comparison BSP" is fully recognised. Regardless of what pattern matching technique is used, templates and features from samples will never exactly match because of the repeatability issues already discussed (see 4.2.1). Consequently, the comparison scores determined by the pattern matching module will have to be interpreted by the decision subsystem.

In some systems, such as speaker verification, the enrolment “templates” might be “models” of the feature generation process – very different data structures than the observed features. The pattern matching module determines the consistency of the observed features with the stored model. Some pattern matching modules may even direct the adaptive recomputation of features from the input data to see if better matches might be made through small adjustments to the input data. This can be accomplished within the BioAPI model through appropriate provision of BSPs.

4.2.6 Decision subsystem

The *decision subsystem* uses the *comparison scores* generated from one or more attempts to provide the decision *outcome* for a verification or identification transaction.

In the case of verification, the *features* are considered to match a compared *reference* when the *comparison score* exceeds a specified *threshold*. A claim about the subject’s enrolment can then be verified on the basis of the *decision policy*, which may allow or require multiple attempts.

In the case of identification, the enrolee reference is a potential *candidate* for the subject when the *comparison score* exceeds a specified *threshold*, and/or when the *comparison score* is among the highest k values generated during comparisons across the entire database. The *decision policy* may allow or require multiple attempts before making an identification decision.

NOTE Conceptually, it is possible at this level of abstraction to treat multibiometric systems (see A.11.1.13) in the same manner as uni-biometric systems, by treating the combined biometric *samples/references/scores* as if they were a single *sample/reference/score* and allowing the *decision subsystem* to operate score fusion or decision fusion as and if appropriate.

The decision subsystem is considered independently from the pattern matching module, and would, in BioAPI architecture terms, be a separate processing BSP (possibly provided by a different vendor). The decision subsystem might make a simple “match” or “no match” determination by comparing the output score from the pattern matching module against a pre-determined threshold value. The ultimate “acceptance” or “rejection” of a subject’s identity claim might be based on multiple “match/no match” decisions from multiple measures or from some dynamically-determined, user-dependent or measure-dependent decision criteria. For instance, common decision policies will accept a transaction if a match occurs in any of three attempts or against any one of several stored templates.

The decision module might also direct operations to the stored database, storing features as templates during enrolment, updating templates in the database after a successful transaction, calling up additional templates for comparison in the pattern matching module, or directing a database search.

Because input samples and stored templates will never exactly match, the decision modules will make mistakes – wrongly rejecting a correctly claimed identity of an enrolled subject or wrongly accepting the identity claim of an impostor. Thus, there are two types of errors: false non-matches and false matches. These errors can be traded off against one another to a limited extent: decreasing false non-matches at the

cost of increased false matches and vice versa. In practice, however, inherent within-individual variation (non-repeatability) limits the extent to which false non-matches can be reduced, short of accepting all comparisons. The decision policies regarding “match/no match” are specific to the operational and security requirements of the system and reflect the ultimate cost and likelihood of errors of both types.

Because of the inevitability of errors (both false non-matches and false matches), all biometric systems must have “exception handling” mechanisms in place. If exception handling mechanisms are not as strong as the basic biometric security system, vulnerability will result. High numbers of falsely rejected comparisons may overload even strong exception handling mechanisms and lower the responsiveness of system management to potential attacks on the system. Consequently, a high false non-match rate can lead not only to user inconvenience and operational delays, but to a compromise in system security as well. False matches and false non-matches are closely related to the system concepts of false accepts and false rejects.

Different systems can require dramatically different tradeoffs between error rates. For example, a biometric portal can be effective with even a 20% false match rate (an 80% probability of intercepting an impostor), which may be low enough to decrease the frequency of attacks on the biometric system to the point that there are no successful impostor transactions. Truly determined fraudsters might find other entry points, including the exception handling mechanism, more appealing than the biometric portal. Conversely, in a criminal identification system a false match may result in a false arrest or imprisonment, so false match rates must be reduced as much as possible.

4.2.7 Administration subsystem

NOTE This is not shown in figure 1.

The *administration subsystem* governs the overall policy, implementation and usage of the biometric system, in accordance with the relevant legal, jurisdictional and societal constraints and requirements. Illustrative examples include:

— providing feedback to the subject during and/or after data capture;

— requesting additional information from the subject;

— storage and format of the biometric references and/or biometric interchange data;

— provide final arbitration on output from decision and/or scores;

— set threshold values;

— set biometric system acquisition settings;

— control the operational environment and non-biometric data storage;

— provide appropriate safeguards for the privacy of the subject;

— interact with the application that utilizes the biometric system.

4.2.8 Interfaces

The biometric system may or may not interface to an external application or system via an Application Programming Interface (see 6.3), hardware interface or a protocol interface (see 6.4).

4.3 Functions of a general biometric system

4.3.1 Enrolment phase

In enrolment, a transaction by a subject is processed by the system in order to generate and store an enrolment record for that individual. The enrolment record will consist of the biometric reference (a stored

sample, template or model) for the individual and perhaps other information, such as a name. At the time of enrolment, the veracity of this other information must be ascertained from external source documentation, such as birth certificates, passports or other trusted documents. The use of biometrics does not obviate the need for care in ascertaining the validity of these documents at the time of enrolment. Note that in some identification systems enrolment may not be a distinct phase; an encounter with an individual who is not found in the database results in an enrolment.

Enrolment typically involves:

— sample acquisition,

— segmentation and feature extraction,

— quality checks, (which may reject the sample/features as being unsuitable for creating a template, and require acquisition of further samples),

— reference creation (which may require features from multiple samples), possible conversion into a biometric data interchange format and storage,

— test verification attempts to ensure that the resulting enrolment data can be successfully used to match another sample obtained from the subject and

— should the initial enrolment be deemed unsatisfactory, repeat enrolment attempts may be allowed (dependent on the enrolment policy).

4.3.2 Recognition phase

4.3.2.1 Verification (or authentication)

In verification, a transaction by a subject is processed by the system in order to verify a positive specific claim about the subject's enrolment (e.g. "I am enrolled as subject X"). Verification will either accept or reject the claim. The verification decision outcome is considered to be erroneous if either a false claim is accepted (false accept) or a true claim is rejected (false reject). Note that some biometric systems will allow a single person to enrol more than one instance of a biometric characteristic (for example, an iris system may allow a person to enrol both iris images, while a fingerprint system may support the enrolment of two or more fingers as backup, in case one finger gets damaged).

Verification typically involves:

— sample acquisition,

— segmentation and feature extraction,

— quality checks, (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples),

— comparison of the sample features against the reference for the claimed identity producing a similarity score,

— judgment on whether the sample features match the reference based on whether the similarity score exceeds a threshold, and

— a verification decision based on the match result of one or more attempts as dictated by the decision policy.

EXAMPLE In a verification system allowing up to three attempts to be matched to an enrolled reference, a false rejection will result with any combination of failures-to-acquire and false non-matches over three attempts. A false acceptance will result if a sample is acquired and falsely matched to the enrolled reference for the claimed identity on any of three attempts.

4.3.2.2 Identification

In identification, a transaction by a subject is processed by the system in order to find the identifier of the subject's enrolment record. Identification provides a candidate list of enrolment records. This list may be empty or may contain only one record. The identification process is considered successful when the subject is enrolled, and at least one enrolment record is in the candidate list. The identification is considered to be erroneous if either an enrolled subject's enrolment record is not in the resulting candidate list (false-negative identification error), or if a transaction by a non-enrolled subject produces a non-empty candidate list (false-positive identification error). There are two approaches to producing a candidate list, closed-set identification and open-set identification (see 7.1).

Identification typically involves:

— sample acquisition,

— segmentation and feature extraction,

— quality checks, (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples),

— comparison against some or all references in the enrolment database, producing a comparison score for each comparison,

— judgment on whether each compared reference is a potential candidate identifier for the subject, based on whether the similarity score exceeds a threshold and/or is among the highest k scores returned, producing a candidate list,

— an identification decision based on the candidate lists from one or more attempts, as dictated by the decision policy.

5 Fundamental concepts

It has been recognized since 1970 that the three pillars of automated personal recognition are (IBM 1970 [19]) recognition by:

— something known or memorized

— something carried

— a personal physical characteristic (a biometric characteristic)

We now say that a person can be automatically recognized by what he/she "knows, has or is", that is by PINs and passwords, tokens, or biometrics. Biometric technology, this last pillar, and the most secure of the three, can be used alone, but is generally combined in access control systems with the other forms of identification (PINs, passwords, or physical tokens). Physical access control applications using biometrics can currently be found at airports, amusement parks, consumer banking kiosks, international ports of entry, universities, office buildings and secured government facilities. When used to control access to information systems, biometrics becomes a technology important to the field of information security. It cannot be forgotten, nor lost.

The perfect biometric measure for all applications would be:

Distinctive: different across all subjects;

Repeatable: similar across time for each subject, over a long time period (several years);

Accessible: easily displayed to a sensor (for example, camera or finger-print scanner or finger geometry measurement device);

Acceptable: the subject is prepared to use the biometric measure in the given application;

Universal: possessed and observable on all people.

Unfortunately, no biometric measure has all of the above properties: there are great similarities among different individuals; biometric characteristics change over time; some physical limitations prevent display; "acceptability" is in the mind of the subject; not all people have all characteristics. Practical biometric technologies must compromise on every point. Consequently, the challenge of biometric deployment is to develop robust systems to deal with the vagaries and variations of human beings.

Biometric systems verify claims (test hypotheses) regarding the source of a biometric pattern in a database. The claim can be made by the person presenting a biometric sample (One example: "I am the source of a biometric data record in the database") or about the source by another actor in the system ("She is the source of a biometric data record in the database"). The claims can be positive ("I am the source of a biometric record in the database") or negative ("I am not the source of a biometric record in the database"). Claims can be specific ("I am the source of biometric record A in the database") or unspecific ("I am not the source of any biometric record in the database"). Any combination of specific or unspecific, positive or negative, first-person or third-person is possible in a claim. To introduce International Standard's terminology, we can look for a "match" between the biometric characteristics of an individual and an identified biometric reference stored in the database (verification), or we can search a population of biometric references in a database for a match with the supplied biometric samples of an individual (identification). In both cases, we have to set thresholds for how close the match has to be before we can consider the supplied biometric sample and the biometric reference to have come from the same individual. Of course, errors can be made: either by a "false non-match" - failing to correctly declare a "match" when the patterns are indeed from the same individual, or a "false match" - incorrectly declaring a match when the patterns are from different individuals. We talk about the percentage of such errors over the total number of comparisons - the "false match rate" (FMR) and the "false non-match rate" (FNMR) for a given technology and a given population in a given application environment.

Systems requiring a positive claim to a specific enrolled reference treat the biometric pattern as an attribute of the enrolment record. These systems "verify" that the biometric attribute in the claimed enrolment record matches the sample submitted by the subject and are called "verification" systems. Some systems, such as those for social service and driver licensing, verify negative claims of no biometric pattern already in the database by treating the biometric pattern as a record identifier or pointer. These systems search the database of biometric pointers to find one matching the submitted sample and are called "identification" systems. However, the act of finding an identifier (or pointer) in a list of identifiers also verifies an unspecific claim of enrolment in the database, and not finding a pointer verifies a negative claim of enrolment. Consequently, the differentiation between "identification" and "verification" systems is not always clear and these terms are not mutually exclusive.

In the simplest systems, "verification" of a positive claim to a specific enrolment record might require the comparison of submitted samples to only the biometric attributes in the single claimed record. For example, a subject might claim to be the source of the fingerprint record stored on an immigration card. To prove the claim to being the source of the enrolled record, the subject would insert the card into a card reader which reads the record, then place his/her finger on the fingerprint reading device. The system compares the fingerprint reference recorded on the card to that of the finger placed on the reader. If the two patterns are reasonably close, the system concludes that the subject is indeed the source of the record on the card and therefore should be afforded the rights and privileges associated with the card. (This does, of course, assume that the card has not been forged. All that the biometric verification achieves is to determine that the human being has presented a biometric that is a close match to that recorded on the card.)

Simple “identification” might require the comparison of the submitted biometric sample with all of the biometric identifiers stored in the database. The State of California requires applicants for social service benefits to verify the negative claim of no previously enrolled identity in the system by submitting fingerprints from both index fingers. Depending upon the specific automated search strategy, these fingerprints might be searched against the entire database of enrolled benefit recipients to verify that there are no matching fingerprints already in the system, or perhaps just the part of the database corresponding to subjects of the same sex as the applicant. If matching fingerprints are found, the enrolment record pointed to by those fingerprints is returned to the system administrator to confirm the rejection of the applicant’s claim of no previous enrolment.

These are examples of the simplest systems. More advanced systems might use comparisons with multiple enrolled records for verification of a claimed identity or only a very limited number of comparisons for identification among all the enrolled records. There is no dependable relationship between “verification” or “identification” and the number of comparisons that the system is required to make.

Information security systems generally use biometrics to verify positive claims to be the source of a specific or unspecific enrolment record in the database. These systems are commonly called “verification” systems regardless of the search strategy and architecture employed. If a claim to enrolment is verified, authorizations associated with the verified or identified enrolment record can then be applied with confidence to the requested activities, such as computer logon. Although hybrid systems – verifying at the time of enrolment the negative claim that a subject is not already in the database, then verifying in later encounters positive claims of enrolment – are also possible, they are not currently widespread.

Biometric technologies are playing a growing role in information security systems today to connect users to system authorizations through verification of claims of enrolled identity. The argument can be made that biometric characteristics more closely link the authentication process to the human user than “what you have” or “what you know”.

Biometric characteristics are not as easy to transfer, forget or steal as PINs, passwords and tokens, so they may increase the security level of systems employing them. Biometrics can be combined with PINs and tokens into “multifactor” systems for added security should the PINs or tokens be stolen or compromised. In case the PIN, password or token are stolen or compromised or the biometric is compromised, the PIN, password or token can be blocked.

6 International Standards for biometrics technical interfaces

6.1 BDBs and BIRs

There are two key concepts in International Standards for biometrics technical interfaces.

The first is that of a "Biometric Data Block" (BDB). A biometric data block is a standardized data interchange format for recording a particular biometric such as a finger-print image, a record of "finger minutiae" (ridge and valley merging or bifurcation), an iris image, etc.

There are biometric data interchange format standards (ISO/IEC 19794 - see A.3) for various biometric technologies, each specifying one or more BDB formats (e.g. compact smart card formats as well as normal formats). Each technology has one or more associated BDB format identifiers that enable the associated format to be interpreted and processed by any system that has knowledge of that format

The second is that of a "Biometric Information Record" (BIR). A BIR is a BDB with added metadata, such as when it was captured, its expiry date, the equipment capturing it, whether it is encrypted, and so on. A number of different BIR formats are defined by ISO/IEC 19785-3 (see A.11.2.3) as part of ongoing work in this area, based both on the amount of information included in the BIR and on the compactness of the encoding scheme used. Again, BIR formats have an identifier, called in this case a "CBEFF Patron Format Identifier".

The BIR is the unit used in most International Standards for the storage and movement between software modules and computer systems, for example using the BioAPI Interfaces (within a system) or the Biometric Interworking Protocol (BIP) (between systems).

The BioAPI and BIP architectures are important for any work involving the movement of biometric information (BDBs, BIRs) within a system or between systems.

6.2 Common Biometric Exchange Formats Framework (CBEFF)

This International Standard (see A.11.2.1) promotes interoperability of biometric-based applications and systems by specifying standard structures for biometric information records (BIRs) - BDBs plus metadata - and a set of abstract data elements and values that can be used to create the header part of a CBEFF-compliant BIR.

A biometric information record (BIR) is an encoding in accordance with a CBEFF patron format (see below). It is a unit of biometric data for storage in a database or for interchange between systems or parts of systems. A BIR always has at least two parts: a standard biometric header (SBH) and at least one biometric data block (BDB). It may also have a third part called the security block (SB). CBEFF places no requirements on the content and encoding of a BDB except that its length shall be an integral number of octets; the several parts of ISO/IEC 19794 specify standardized BDB formats for a number of biometric types.

The primary purpose of CBEFF is to define abstract data elements (data elements with a set of defined abstract values, with their semantics) that are expected to be of general utility as parts of the standard biometric header (SBH) in biometric information records (BIRs).

A CBEFF patron format is defined for a particular domain of use. A CBEFF patron format is a full bit-level specification of encodings that can carry some or all of the abstract values of some or all of the CBEFF data elements defined in this International Standard (possibly with additional abstract values determined by the CBEFF patron), together with one or more biometric data blocks (BDBs) containing biometric data.

ISO/IEC 19785 consists of three Parts. The first specifies a full set of (metadata) data elements and their abstract values (without determining any particular encoding). The second Part specifies the procedures for the operation of a Registration Authority that registers identifiers for biometric organizations, BDBs, patron formats (BIR formats) and security block formats. The third part defines a number of useful patron formats that vary from minimal to maximal metadata and include both binary and XML encodings of the meta-data.

6.3 The BioAPI International Standard

BioAPI (ISO/IEC 19784 - see A.11.3.1) is an important International Standard that provides an implementation architecture that supports these functions using software (and hardware) modules from multiple vendors.

The basic concept is of applications (from multiple vendors) interacting with a BioAPI Framework (from a single vendor, but with defined interfaces), which in turn interacts with *Biometric Service Providers (BSPs)* (from multiple vendors) to perform the biometric functions. The BioAPI architecture is shown in Figure 2.

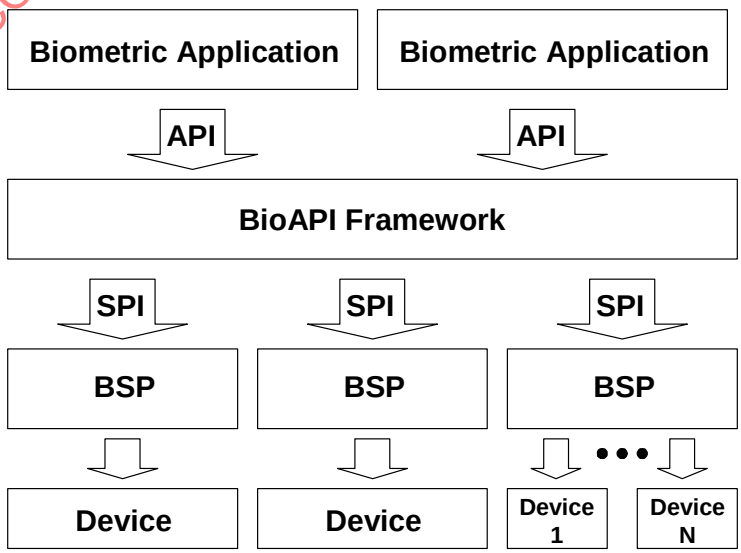

Figure 2: BioAPI architecture

Interaction between these various components is by passing a BIR.

BSPs can perform capture, comparison, archiving, or processing of a BIR.

In a recent addition to the BioAPI architecture, the BSP may consist of code from one vendor interacting with a "BioAPI Unit" provided by a different vendor - typically a hardware device and its driver, thus minimizing the work needed by hardware suppliers to become part of a biometric system.

6.4 The BIP International Standard

The BIP Standard (ISO/IEC 24708 - see A.11.4) provides bits-on-the-line communication to enable an application in one BioAPI system to interact with BSPs in a remote BioAPI system. This extension of the BioAPI architecture is an important piece of additional standardization that forms part of the transmission subsystem described in clause 4.2.2 (see figure 3).

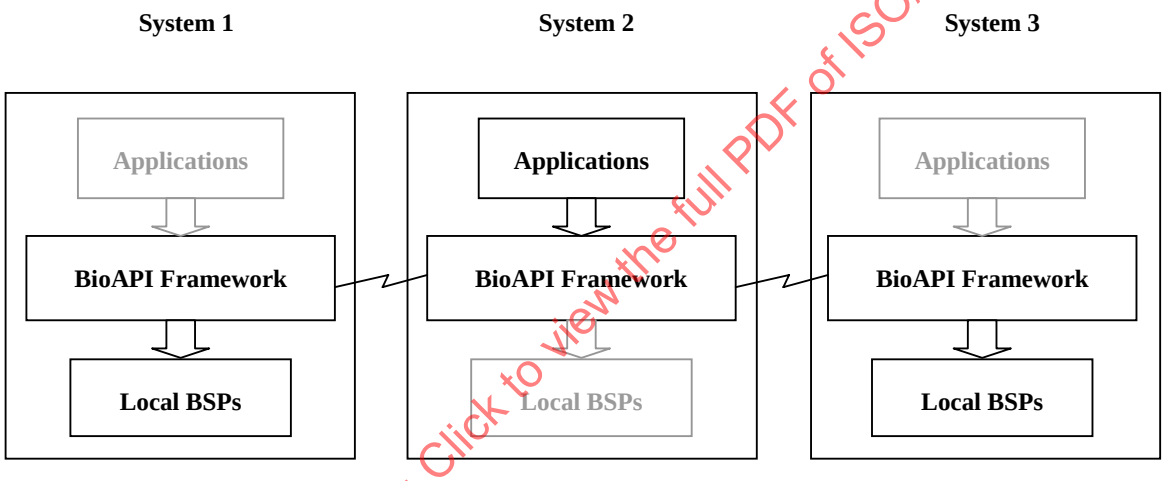

Figure 3: Use of the BIP for communication between systems

7 Performance testing

7.1 General

Biometric devices and systems might be tested in many different ways. Types of testing (see also A.11.5) include:

— Technical performance (in terms of error rates and throughput rates);

— Reliability, Availability and Maintainability (RAM);

— Vulnerability;

— Security;

— User acceptance;

— Human factors;

— Cost/benefit;

— Privacy regulation compliance.

Technical performance has been the most common form of testing in the last three decades. Technical tests are generally conducted with the goal of predicting system performance with a target population in a target environment, but historically, extrapolation of results from a test environment to the "real world" has been difficult. To make test results more predictive of real world performance, testing standards are being developed (ISO/IEC 19795 - see also A.11.5).

Technical tests can be either "closed-set" or "open-set". A "closed-set" test assumes that all subjects are enrolled in the system and does not acknowledge the existence of impostors. A closed set test returns the rank of the true comparison when an input sample is compared to all of the enrolled references. Closed-set tests measure the probability that the true pattern was found at rank k or better in the search against the database of size N. In any test, the rank k probability is dependent upon the database size, decreasing as the database size increases.

An "open-set" test does not require that all input samples be represented by a reference in the enrolled data base and measures all comparison scores against a score threshold. An open-set test returns, as a function of the threshold, the probability of either missing a true comparison (the false non-match rate) or matching a wrong comparison (the false match rate). Open-set measures are independent of the size of the database searched, converging to the correct estimator as the test size increases. Examples of both open-set and closed-set tests are found in the literature, but as most applications must acknowledge the potential for impostors, open-set results are of the greater practical value to the system designer or analyst.

Metrics generally collected in open-set technical tests are: failure-to-enrol, failure-to-acquire, false acceptance, false rejection and throughput rates. Failure-to-enrol rate is determined as the percentage of all persons presenting themselves to the system for enrolment who are unable to do so because of system or human failure. Failure-to-acquire rate is determined as the percentage of presentations by all enrolled subjects that are not acknowledged by the system. The false rejection rate is the percentage of all subjects whose claim to identity is not accepted by the system; the inverse of this is often stated as the true acceptance rate. This will include failed enrolments and failed acquisitions, as well as false non-matches against the subject's stored template. The false acceptance rate is the rate at which "zero-effort" impostors making no attempt at emulation are incorrectly matched to a single, randomly chosen false identity. Because false acceptance/rejection and false match/non-match rates are competing measures, they can be displayed together on a "Decision Error Trade-off" (DET) curve. False acceptance and true acceptance rates can be displayed on a "Receiver Operator Characteristic" (ROC) curve.

The throughput rate is the number of persons processed by the system per minute, and includes both the human-machine interaction time and the computational processing time of the system.

7.2 Types of technical tests

Three types of technical tests have been described: Technology, Scenario, and Operational (Philips, Martin, Wilson and Przybocki, 2000 [37]).

Technology test: The goal of a technology test is to compare competing algorithms from a single technology, such as fingerprinting, against a standardized database collected with a sensor compliant with a stated standard (a "universal" sensor). There are competitive technology tests in speaker verification (NIST, 1996-2006 [29]), facial recognition (NIST, 1993-1997 [30] and NIST, 2000-2006 [32]), fingerprinting (Fingerprint Verification Competition, 2000-2006 [4] ; NIST, 2003. [31] ; NIST, 2004-2006 [33] ; NIST - 2004-2006 [34]), and iris (International Biometric Group, 2005 [20] ; NIST, 2004-2006 [35]).

Scenario test: While the goal of technology testing is to assess the algorithm, the goal of scenario testing is to assess the performance of the subjects as they interact with the complete system in an environment that models a "real-world" application. Each system tested will have its own acquisition sensor and so will receive slightly different data. Scenario testing has been performed by a number of groups, but few results have been published openly (Rodriguez, Bouchier and Ruehie, 1993 [41]; Bouchier, Ahrens and Wells, 1996 [7]; Mansfield, Kelly, Chandler and Kane, 2000 [25])

Operational test: The goal of operational testing is to determine the performance of a target population in a specific application environment with a complete biometric system. In general, operational test results will not be repeatable because of unknown and undocumented differences between operational environments. Further, "ground truth" (i.e. who was actually presenting a "good faith" biometric measure) will be difficult to ascertain. Because of the sensitivity of information regarding error rates of operational systems, few results have been reported in the open literature (Wayman, 2000 [51]).

All biometric recognition techniques require human interaction with a data collection device. Technology testing generally attempts to limit the effect of human interaction, while scenario and operational testing must account for and may attempt to measure these effects. Match errors, failure-to-enrol/acquire and throughput rates are determined by human interaction, which in turn depends upon the specifics of the collection environment. Human factors of biometric collection is an emerging discipline.

8 Biometrics and information security

Hopefully it is clear by this point that biometrics can have an important role in information security, being much more closely linked to a subject and more difficult to forget, give away or lose than a token, a PIN or a password. Use of biometrics can provide additional evidence that an authorization credential is being presented by the person to whom it was issued. However, biometric technologies do not represent a "silver bullet" eliminating PINS, passwords and tokens while resolving all security issues.

In architecting a system for verifying a positive claim to identity, we must decide whether each person's biometric reference will be carried by the person themselves on a token (and if so, whether the reference will be stored in processed form as a template or in the same form as acquired, such as an image), or whether the reference will be stored centrally in a database linked to the point of service by a communications system (see 6.4). The former approach has positive implications for privacy (Kent and Millett, 2003 [21]), but if biometric references are stored centrally, several different questions arise:

— Will the acquired sample be sent to the central system or will the central system pass the reference to the point of service for processing? In either case, some strong form of encryption will be required to protect the data during transmission.

— If the data is sent from the point of service to the central site, will it be in raw form or processed into features? If processed into features prior to transmission, computational power and knowledge of the feature extraction algorithm will be required at each point of service but transmission bandwidth will be reduced.

— How will the encrypted data be unencrypted when necessary for comparison?

— How will the subject trust the point of service to be legitimate and not to be storing the biometric data after transmission?

Although these issues are not insurmountable, they demonstrate that use of biometrics does not eliminate the usual security issues.

It has been well known since the 1970s that biometric devices can be fooled by forgeries (Lummis and Rosenberg, 1972 [23]; Raphael and Young, 1974 [40]; NBS, 1977[28]). "Spoofing" is the use of a forgery of another person's biometric characteristics, in order to be recognized as that person. It is also possible to disguise one's own biometric characteristics to avoid recognition. Forging the biometric characteristics of another person is more difficult than disguising one's own characteristics, but is quite possible nonetheless.

Several studies (Blackburn, et al 2001 [5]; van der Putte and Keuning, 2000 [48]; Matsumoto, Matsumoto, Yamada and Hoshino, 2002 [26]; Thalheim, Krissler and Ziegler, 2002 [45]; BSI, 2003 [8]) and BSI, 2005 [9]) discuss ways by which facial, fingerprint and iris biometrics can be forged. Liveness testing (testing for forgeries) is possible for several biometric modes. For example, speaker recognition systems can make forgery difficult by requesting that the subject say numbers randomly chosen by a computer; iris systems can check for the presence of pupillary oscillation; fingerprint systems can check for blood flow. However, liveness testing is a research area, and effective liveness testing without increasing false rejection rates is problematic. The likelihood of forgery can be reduced through the collection of multiple biometric instances or modes (e.g. ten fingers, or iris and face), along with trained operators.

The use of biometrics does not reduce the need to fully vet all applicants for authorizations. A biometric system can neither verify the external truth of the enrolled identity itself nor establish the link automatically to an external identity with complete certainty. Determining a subject's "true" identity, if required, is done at the time of enrolment through trusted external documents, such as a birth certificate or (depending on national regulations) an identity card or driver's licence. The biometric characteristics link the subject to an enrolled identity and associated authorizations that are only as valid as the original determination process.

Not all systems, however, have a requirement to know a subject's "true" name or identity. Biometric characteristics can be used as pseudo-anonymous identifiers and consequently have intriguing potential for privacy enhancement of authorization systems.

All biometric characteristics may change over time, due to aging of the body, injury or disease. Therefore, re-enrolment may be required. If "true" identity or continuity of identity is required by the system, re-enrolment must necessitate presentation of trusted external documentation. Both enrolment and reenrolment also require the physical presence of the enrolling person before the enrolling authority. Otherwise, there is no way to determine that the enrolled biometric characteristic came from the body of the person presenting it.

9 Example applications

Applications of biometric technologies are extremely diverse. Yet biometric applications can be simply categorized as either being for law enforcement or for some form of civilian access control to physical or logical resources.

9.1 Law enforcement

The law enforcement community uses many of the world's largest biometric systems, comparable in size only to some immigration control systems (see 9.2.4). The two main biometric functions in law enforcement agencies involve identification of arrestees (usually through sets of fingerprints), and identification of forensic evidence (often through latent fingerprints or DNA left at crime scenes). In the US, fingerprints are searched against the FBI's IAFIS, which currently contains fingerprint sets from approximately 50 million individuals with criminal histories. Police forces throughout the world use AFIS technology to process criminal suspects, match fingerprints, and bring guilty criminals to justice.

9.2 Civilian applications

All other biometric applications, not involving crime detection, utilize some form of access control. Whether it is securing benefit systems from fraud, preventing illegal immigrants from entering a country or prisoners from leaving a prison – controlling access to a physical or logical resource is the underlying principle. Access control ensures that authorized individuals can gain access to a particular area or resource and that unauthorized individuals cannot. This is a rapidly expanding market. Fraud is an ever-increasing problem and security is becoming a necessity in many walks of life. Access control, therefore, will not be restricted to the application areas mentioned below and will branch out to other market opportunities, as soon as a need is identified.

9.2.1 Banking applications

Banks have been evaluating a range of biometric technologies for many years. Fraud and general breaches of security must be controlled if banks are to remain competitive in the ever-diversifying financial services industry. Biometrics can implement this element of control in a number of situations. Weak links such as Automated Teller Machines (ATMs) and transactions at the point of sale are particularly vulnerable to fraud and can be secured by biometric technologies. Other emerging markets such as telephone banking and Internet banking must also be totally secure for bank customers and bankers alike. A variety of biometric technologies are now striving to prove themselves throughout this range of diverse market opportunities.

9.2.2 Benefit systems

Benefit systems, as well as banks, are particularly vulnerable to fraud. The battle against fraud has been strongly fought by welfare departments in many countries for a number of years. The main problem here is to avoid multiple registrations of the same individual, so 1-many checks at enrolment time are a key feature of this application, but one-to-one checks when benefits are paid out is also important. Again, a variety of technologies are being evaluated, though the use of fingerprinting is particularly widespread. Here, AFIS technology and one-to-one verification can be used to ensure that the benefit claimant legitimately receives a benefit cheque. Another development that looks set to revolutionize the payment of benefit is Electronic Benefit Transfer (EBT) which involves loading funds onto a plastic card. The card can then be used to purchase food and other essentials in shops fitted with special point of sale readers. Biometric technologies are well-placed to capitalize on this market opportunity and vendors are building on the strong relationship currently enjoyed with the benefits community.

9.2.3 Computer systems access

Computer systems access (also known as logical access control) is important because fraudulent access to computer systems affects private computer networks and the expansive Internet in the same way. Confidence is lost and the network is unable to perform at full capacity until the hole in security is patched. Biometric technologies are proving to be more than capable of securing computer networks. This market area has a lot of potential, especially if the biometrics industry can migrate to large-scale Internet applications. As banking data, business intelligence, credit card numbers, medical information and other personal data become the target of attack, the opportunities for biometric vendors are increasing.

9.2.4 Immigration control

Terrorism, drug-running, illegal immigration and an increasing throughput of legitimate travellers is putting a strain on immigration authorities throughout the world. These authorities need to quickly and automatically process travellers in order to identify those with criminal histories or fraudulent visas and others that are deemed inadmissable. Biometric technologies are being employed in a number of diverse applications to make this possible. Many Immigration and Naturalization Services are becoming major users and evaluators of a number of biometric technologies. Systems are currently in place in many countries to automate the flow of legitimate travellers and to deter illegal immigrants.

9.2.5 National identity cards

Biometrics are beginning to assist governments as they record population growth, identify citizens and prevent fraud occurring during local and national elections. Often this involves storing a biometric template (reference) on a card, which in turn acts as a national identity document. Fingerprinting is particularly strong in this area and schemes are already under way in many countries.

9.2.6 Physical access control

The general application area of physical access control can be used to illustrate the deployment of biometrics that cannot be categorized in any other way. Many different organizations are using biometrics to secure the physical movement of people. Schools, nuclear power stations, military facilities, theme parks, hospitals, offices and supermarkets, across the globe, employ biometric technologies to minimize security threats.

9.2.7 Prisons and police applications

The prisons and police application area differs from law enforcement in that here biometrics are not used to catch criminals, but to make sure that they are securely detained. In other words, this is about physical access control for prison and police environments. A surprising number of prisoners simply walk out of prison gates before they are officially released. A wide range of biometrics are now being used worldwide to secure prison access, police detention areas, enforce home confinement orders and regulate the movement of probationers and parolees. Speaker recognition systems are becoming of increasing interest to enable prisoners on parole to automatically record their presence (via a land-line telephone) without the manually intensive need to physically present themselves at a police station.

9.2.8 Telephone systems

Global communication expanded over the past decade. Cellular telephones, Dial Inward System Access (DISA) and a range of telecommunication services are now available. Yet these are all under attack from fraudsters. Cellular companies are vulnerable to cloning (where a new phone is created using stolen code numbers) and new subscription fraud (where a phone is obtained using a false identity). Meanwhile, Dial Inward System Access – which allows authorized individuals to contact a central exchange and make free calls – is being targeted by telephone hackers. Once again, biometrics is being called upon to defend against such attacks. Voice biometrics are obviously well suited to the telephone environment and are making in-roads into these markets, and speaker recognition systems have the potential to make stolen mobile phones unusable.

9.2.9 Time, attendance and monitoring applications

Recording and monitoring the movement of employees as they arrive at work, have breaks and leave for the day was traditionally performed by 'clocking-in' machines. However, the manual clocking-in process can be circumvented. This defeats the purpose of clocking-in and disrupts time management and unit costing exercises. Replacing the manual process with biometrics reduces abuses of the system and can be incorporated with time management software to produce management accounting and personnel reports.

9.2.10 Civil background checks

A large and growing use of biometric systems is in civil background checks, in which fingerprints are used to check for a criminal background. Traditionally, these checks were limited to security clearances, but now are required for many diverse occupations, such as attorneys (applications to the bar), teachers, or school bus drivers and school caretakers. In the United States, these checks are run against the FBI's IAFIS, which processes tens of thousands of such transactions daily. There are legal requirements for such criminal background checks in other countries, although biometrics are not always currently used.

10 Biometrics and privacy

10.1 General

The concept "privacy" is highly culturally dependent. Legal definitions vary from country to country and, in the United States, even from state to state (Alderman and Kennedy, 1995 [1]). A classic definition is the intrinsic "right to be let alone" (Warren and Brandeis, 1890 [49]), but more modern definitions include informational privacy: the right of individuals "to determine for themselves when, how and to what extent information about them is communicated to others" (Westin, 1967 [53]) and the right of informational self-determination as the right to know who gets which information, when and for which purpose. A third, more recent, concern is to protect the individual from having his identity stolen, or to be reliably and quickly identified after an accident or incident. All three types of privacy can be impacted, both positively and negatively by biometric technology.

10.2 Biometric technology acceptability

There are differences between the acceptability of different biometric technologies. Some require physical contact (for example, with a finger-print reader), but this is no different from the use of a keypad to enter a PIN. Some require a light to shine into the eye (retina images). But many technologies are very non-intrusive, such as face recognition and iris scans.. Nonetheless, there are some cultures where it is objectionable to display a face to a camera. Hand biometrics have been considered by some as the Biblical “the sign of the beast”. Thus a range of biometric technologies will need to be employed if all cultures are to be accommodated.

It can be argued (Locke, 1690 [22]; Baker, 2000 [2]) that a physical body is not identical to the person that inhabits it. Whereas PINs and passwords identify persons, biometrics identifies the body. Biometric measures could allow linking of the various “persons” or psychological identities that each of us manifests in our separate dealings within our social structures. Biometrics, if universally collected without adequate controls, could aid in linking, for example, employment records to health history and/or church membership. Whilst the investigation of such linkages may be a valid research activity, it is normal for such research to make the data involved anonymous, so that no actual individual can be identified. Similar safeguards are needed when use of biometric technologies becomes wide-spread.

10.3 Protection from identity theft

Identity theft and identity fraud are serious, growing problems. There are many mechanisms in use today to ensure that no one person can operate under many different identities, and to ensure that a person's privacy, rights, and privileges cannot be compromised by others masquerading under their identity. The use of biometric technologies and central databases of biometric references provides the best means available today to ensure that identity documents (such as passports) can only be obtained once, and cannot be misused by someone other than the person to whom they have been issued. The use of strong encryption to ensure the integrity of biometric references on cards, and the use of checks of a central database for attempts at duplicate enrolment gives biometric technologies an important strength in all activities related to identity.

10.4 Privacy

With increasing numbers of biometric implementations worldwide, the aspect of privacy gains importance. As a result it is necessary to understand what the objectives of data protection law and policy intend. Stated simply, it is the protection of the personal rights of those whose data are processed, and the protection of data subjects and not simply the protection of data. Using a biometric system means in most cases using personal data, thus the privacy regime of national laws apply. Depending on how a system is deployed, use of biometrics can either threaten or protect a data subject’s privacy. The possibility of protection is especially valid in view of the special properties of biometric characteristics, which for an entire life are linked to the subject, unlike PINs and passwords, which are only indirectly and weakly linked to a person. Therefore, by using biometric technologies, other types of personal data can be better protected from theft and misuse than by traditional means. Biometrics can therefore be both an object and a tool in the different aspects of this discussion. In all applications, the principle of proportionality should be applied. That means that biometric data used should be adequate, relevant and non excessive with regard to the purposes for which it is collected and further processed.

Biometrics can thus also be used as a Privacy Enhancing Technology (PET). The principle of PETs applies to biometrics from two standpoints: first, the implementation and application of biometrics has to follow a correct privacy regime in order to be privacy enhancing. Second, biometrics itself can be a privacy enhancing method. The main question, with regards to the concept of PETs, (and in general in the application of biometrics, following the proportionality principle) is whether or not identification is necessary for each of the processes of the conventional information system. In most cases it is not necessary to know the data subject’s identity in order to grant privileges. Yet there are some situations in which the data subject will have to reveal his or her identity to allow verification.

11 Conclusions

Biometric systems are well-developed and mature in some applications, such as criminal investigation, civil background checks, or immigration control. In other areas, biometric solutions are making increasing inroads, such as physical or logical access control or benefits systems. For decades, mass adoption of biometric technologies in consumer markets has appeared to be just a few years away (Raphael and Young, 1974 [40]), yet even today, difficulties remain in establishing a strong business case, in motivating consumer demand, and in creating a single system usable by all sizes and shapes of persons. Nonetheless, the biometric industry has grown at a steady pace as consumers, industry, and government have found appropriate applications for these technologies. Although the privacy implications continue to be debated, biometrics can be used in privacy enhancing applications. Only time will tell if biometric technologies will receive widespread application in the area of information security.

Annex A

(informative)

A brief summary of International Standards activity

NOTE This Annex is correct as of mid-2006. Work is, however, continually being added to the SC37 programme of work, and that should be consulted for more up-to-date information.

A.1 Background on biometrics standardization

NOTE Some key acronyms and terms and abbreviations used in the biometric work are provided in Annex B.

A.1.1 Much of biometrics standardization was initiated in the USA, but in 2002 a new ISO/IEC JTC1 Subcommittee was established - SC37, and first met in Orlando in December 2002. The following is from the SC37 Web site.

A.1.2 ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National Bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity.

A.1.3 ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, government and non-governmental, in liaison with ISO and IEC also take part in the work.

A.1.4 In the field of information technology, ISO and IEC have established a Joint Technical Committee 1: ISO/IEC JTC 1 on Information Technology. In June 2002, JTC 1 established a new Subcommittee 37 on Biometrics. The goal of this new JTC 1 SC is to ensure a high priority, focused, and comprehensive approach worldwide for the rapid development and approval of formal international biometric standards. These standards are necessary to support the rapid deployment of significantly better, open systems standard-based security solutions for purposes such as homeland defence and the prevention of ID theft.

A.1.5 The intended area of work is the standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects.

A.2 Layers or areas of biometric standardization and Working Groups

A.2.1 There is not yet an agreed layered model for the SC 37 biometrics work (but see clause 4 for a model of a biometric system), but the following is used in this tutorial. For a slightly different layered relationship of SC 37 standards, please refer to ISO/IEC 24713-1: Biometric Profiles for Interoperability and Data Interchange: Biometric Reference Architecture (see A.11.6.1 below).

A.2.2 For the purposes of this tutorial, we recognise six levels of biometric standardization, plus other areas related to societal and privacy issues. The layering is largely based on dependencies for implementation of the Standards, with implementation of those in a higher layer dependent on implementation of a lower layer Standard. Societal and privacy issues are outside this layering structure. Figure A.1 shows the structure of the standards as an "onion-skin" diagram.

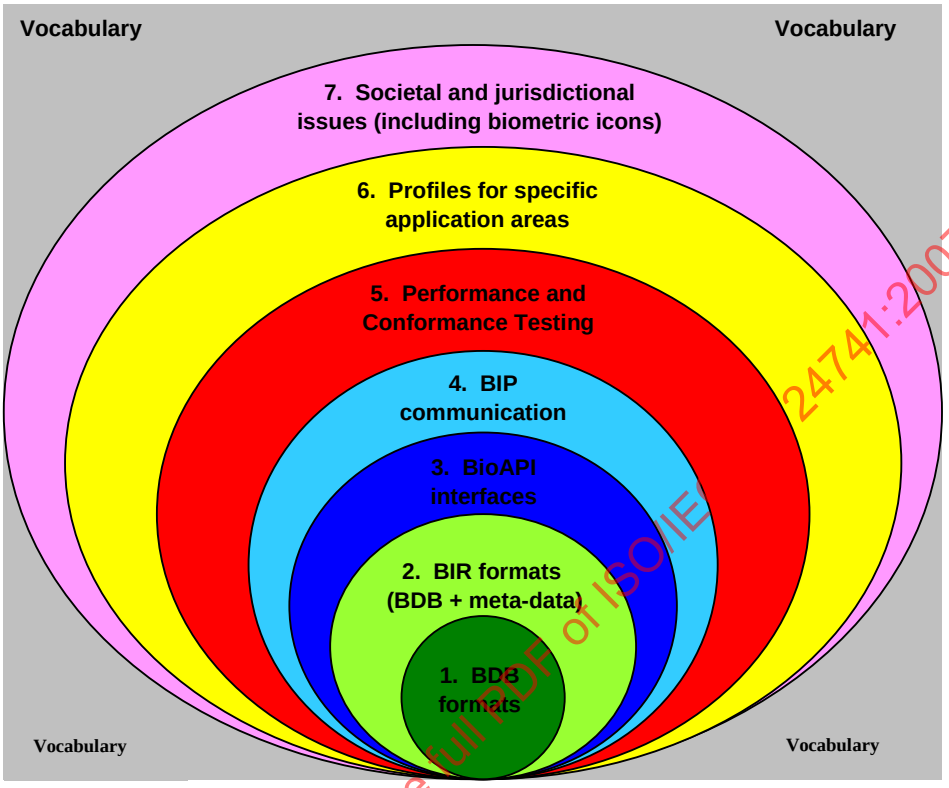

Figure A.1 — Layered model of biometrics standards

A.2.3 This tutorial recognises:

— **(Layer 1)** BDB (Biometric Data Block) format standards

— **(Layer 2)** BIR (Biometric Information Record) formats (BDBs plus CBEFF metadata)

— **(Layer 3)** BioAPI interfaces between applications, framework, and Biometric System Providers

— **(Layer 4)** BIP (BioAPI Interworking Protocol) for communication between biometric systems

— **(Layer 5)** Performance and Conformance testing standards

— **(Layer 6)** Biometric profiles for specific application areas

— **(Layer 7)** Societal and jurisdictional issues

— With vocabulary standardization underlying everything.

A.2.4 The work is organized into the following Working Groups:

WG1 - Harmonized Biometric Vocabulary and Definitions

WG2 - Biometric Technical Interfaces (Layer 2, 3, 4 and 5 Standards)

WG3 - Biometric Data Interchange Formats (Layer 1 Standards)

WG4 - Profiles for Biometric Applications (Layer 6 Standards)
WG5 - Biometric Testing and Reporting (Layer 5 Standards)
WG6 - Cross-Jurisdictional and Societal Aspects (Layer 7 Standards)

A.3 Layer 1 Standards (approved or in preparation for initial standards)

ISO/IEC 19794-1, *Information technology — Biometric data interchange formats — Part 1: Framework*

ISO/IEC 19794-2, *Information technology — Biometric data interchange formats — Part 2: Finger minutiae data*

ISO/IEC 19794-3, *Information technology — Biometric data interchange formats — Part 3: Finger pattern spectral data*

ISO/IEC 19794-4, *Information technology — Biometric data interchange formats — Part 4: Finger image data*

ISO/IEC 19794-5, *Information technology — Biometric data interchange formats — Part 5: Face image data*

ISO/IEC 19794-6, *Information technology — Biometric data interchange formats — Part 6: Iris image data*

ISO/IEC 19794-7, *Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data*

ISO/IEC 19794-8, *Information technology — Biometric data interchange formats — Part 8: Finger pattern skeletal data*

ISO/IEC 19794-9, *Information technology — Biometric data interchange formats — Part 9: Vascular image data*

ISO/IEC 19794-10, *Information technology — Biometric data interchange formats — Part 10: Hand geometry silhouette data*

ISO/IEC 19794-11, *Information technology — Biometric data interchange formats — Part 11: Signature/sign processed dynamic data*

ISO/IEC 29794-1, *Information technology — Biometric sample quality — Part 1: Framework*

ISO/IEC 29794-4, *Information technology — Biometric sample quality — Part 4: Fingerprint sample quality*

ISO/IEC 29794-5, *Information technology — Biometric sample quality — Part 5: Face image data sample quality*

A.4 Layer 2 Standards (approved or in preparation for initial standards)

ISO/IEC 19785-1, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

ISO/IEC 19785-2, *Information technology — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority*

ISO/IEC 19785-3: *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

A.5 Layer 3 Standards (approved or in preparation for initial standards)

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

ISO/IEC 19784-2, *Information technology — Biometric application programming interface — Part 2: Biometric archive function provider interface*

ISO/IEC TR 24722, *Information technology — Biometrics — Multimodal and other multibiometric fusion*

A.6 Layer 4 Standards (approved or in preparation for initial standards)

ISO/IEC 24708, *Information technology — Biometrics — Biometric Interworking Protocol (BIP)*

A.7 Layer 5 Standards (approved or in preparation for initial standards)

ISO/IEC 19795-1, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*

ISO/IEC 19795-2, *Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation*

ISO/IEC TR 19795-3, *Information technology — Biometric performance testing and reporting — Part 3: Modality-specific testing*

ISO/IEC 19795-4, *Information technology — Biometric performance testing and reporting — Part 4: Performance of biometric access control systems*

ISO/IEC 24709-1, *Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 1: Methods and procedures*

ISO/IEC 24709-2, *Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 2: Test assertions for biometric service providers*

ISO/IEC 24709-3, *Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 3: Test assertions for frameworks*

ISO/IEC 24709-4, *Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 4: Test assertions for applications*

A.8 Layer 6 Standards (approved or in preparation for initial standards)

ISO/IEC 24713-1, *Information technology — Biometric profiles for interoperability and data interchange — Part 1: Biometric system reference architecture*

ISO/IEC 24713-2, *Information technology — Biometric profiles for interoperability and data interchange — Part 2: Physical access control for employees at airports*

ISO/IEC 24713-3, *Information technology — Biometric profiles for interoperability and data interchange — Part 3: Biometric-based verification and identification of seafarers*

A.9 Layer 7 Standards (approved or in preparation for initial standards)

ISO/IEC TR 24714-1, *Cross-jurisdictional and societal aspects of implementations of biometric technologies — Part 1: Guide to the accessibility, privacy and health and safety issues in the deployment of biometric systems for commercial application*

ISO/IEC TR 24714-2, *Cross-jurisdictional and societal aspects of implementations of biometric technologies — Part 2: Practical application to specific contexts*

A.10 Vocabulary work (approved or in preparation for initial standards)

Harmonized Biometric Vocabulary (an ISO/IEC JTC1/SC37 Standing Document)

ISO 2382-37, *Information processing systems — Vocabulary — Part 37: Biometrics*

A.11 A brief summary of the above Standards or Technical Reports

A.11.1 Layer 1 Standards

A.11.1.1 Biometric Data Interchange Format: Framework (ISO/IEC 19794-1)

This International Standard sets the context for the standardization of BDBs and their use in other biometrics data structures. It discusses the issues involved in the capture, feature extraction, and use of biometric data at the BDB level, including the distinction between a BDB containing image data and one based on feature extraction. It also discusses some of the requirements for a sensor, some of the terminology used in multimodal work (multiple BDBs, possibly using different biometrics), and the BDB format identifier registration mechanism.

A.11.1.2 Biometric Data Interchange Format: Finger Minutiae Data (ISO/IEC 19794-2)

This International Standard defines a data structure (called a Biometric Data Block format) that contains a digital record of the features that can be identified and extracted from a digitised fingerprint, and recorded.

These features are called finger minutiae. Most people are aware that if you examine a finger you will find a pattern of ridges and valleys, with points where a single ridge splits into two ridges, creating a new valley (ridge bifurcation) or where a ridge ends, with the valleys on either side merging into a single valley. The points where this occurs are called finger minutiae. A typical fingerprint is shown in figure A.2.

Figure A.2 — A typical fingerprint

By identifying these minutiae, and then recording their position relative to each other, particularly a count of the number of ridges between pairs of them, a very compact digital representation can be obtained which can be used to compare two fingerprints to see if they are virtually certain to have been produced by the same individual. The use of finger minutiae is a very mature technique for matching fingerprints.

The Standard specifies how the minutiae are to be identified, and their relative positions recorded, but most importantly the data format to be used to record this information. (Note that this is not a full digital image of the finger-print, merely a record of the relative positions of its minutiae, but it is sufficient for very accurate matching.

This Standard enables equipment from one vendor to produce a finger minutiae data block format that can be compared directly with a finger minutiae data block produced by equipment from a different vendor without any collaboration between the two vendors (open interworking).

Associated comparison algorithms are not standardized, but there are examples and guidelines for comparison algorithms in an Annex.

Normally a BDB would be "captured" (produced) when a human subject (a person) is "enrolled" (registered with an organization), and archived (stored) with some additional metadata about the time of capture, the equipment used, and so on. It might be (only) archived on a smart-card to be carried by the human subject, or it might be (only) archived on a central database, or it might be archived on both. These options for archiving are subject to privacy concerns that might be expressed by the individual or in national legislation, and to the need to maintain backups.

This Standard defines two main data formats. The first provides rapid and easy comparison, the second is a more compressed format that is more suitable where the BDB is stored on a smart card (and the comparison perhaps performed by the card).

A.11.1.3 Biometric Data Interchange Format: Finger Pattern Spectral Data (ISO/IEC 19794-3)

This International Standard is based on the highly mathematical transformation of an image into so-called "spectral components" for uniform-sized regions of the image. Spectral components are obtained using Discrete Fourier Transforms and (single-scale) Gabor Filter components, extracted from both overlapping and non-overlapping uniform-sized regions of the original image. The discussion of these mathematical concepts is beyond the scope of this text.

(There are fingerprint recognition algorithms that use spectral data directly for comparing a stored template with a newly-captured template.)

A.11.1.4 Biometric Data Interchange Format: Finger Image Data (ISO/IEC 19794-4)

This International Standard defines a data structure (called a Biometric Data Block format) that contains a digital record of the image of one or more fingers (or of a palm).

It specifies how the image is to be acquired, and how it is to be converted to a digital representation, with a full specification of the digital format.

This Standard enables equipment from one vendor to produce a finger image data block format that can be compared directly with a finger image data block produced by equipment from a different vendor without any collaboration between the two vendors (open interworking).

Associated comparison algorithms are not standardized, and are generally company confidential.

Normally a BDB would be "captured" (produced) when a human subject (a person) is "enrolled" (registered with an organization), and archived (stored) with some additional metadata about the time of capture, the equipment used, and so on. It might be (only) archived on a smart-card to be carried by the human subject, or it might be (only) archived on a central database, or it might be archived on both. These options for archiving are subject to privacy concerns that might be expressed by the individual or in national legislation, and to the need to maintain backups.

A.11.1.5 Biometric Data Interchange Format: Face Image Data (ISO/IEC 19794-5)

This International Standard defines a data structure (called a Biometric Data Block format) that contains a digital record of the image of a face.

It specifies how the image is to be acquired (including lighting, pose of the subject, facial expression, head-dress, etc.), and how it is to be converted to a digital representation, with a full specification of the digital format.

This Standard enables equipment from one vendor to produce a face image data block format that can be compared directly with a face image data block produced by equipment from a different vendor without any collaboration between the two vendors (open interworking).

Associated comparison algorithms are not standardized, and are generally company confidential.

Normally a BDB would be "captured" (produced) when a human subject (a person) is "enrolled" (registered with an organization), and archived (stored) with some additional metadata about the time of capture, the equipment used, and so on. It might be (only) archived on a smart-card to be carried by the human subject, or it might be (only) archived on a central database, or it might be archived on both. These options for archiving are subject to privacy concerns that might be expressed by the individual or in national legislation, and to the need to maintain backups.

Figure A.3 shows some of the measurement points on a face:

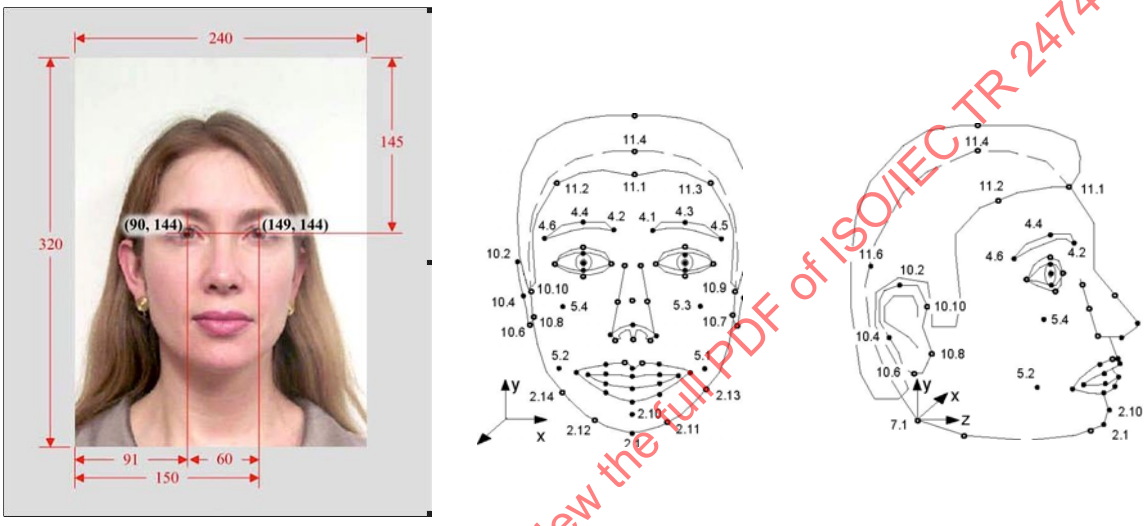

Figure A.3 — Some of the measurement points on a face

A.11.1.6 Biometric Data Interchange Format: Iris Image Data (ISO/IEC 19794-6)

This Standard defines a data structure (called a Biometric Data Block format) that contains a digital record of the image of an iris (see Figure A.4).

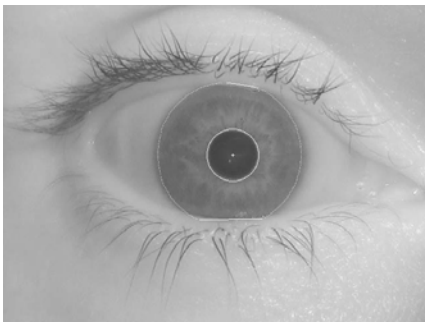

Figure A.4 — Picture of an iris

It specifies how the image is to be acquired, and how it is to be converted to a digital representation, with a full specification of the digital format.

Two BDB formats are defined. The first is relatively verbose, but requires minimal processing of the image to produce it. The second is more compact and requires more processing to produce it.

This Standard enables equipment from one vendor to produce an iris image data block format that can be compared directly with an iris image data block produced by equipment from a different vendor (provided that they both produce either the verbose or the compact format) without any collaboration between the two vendors (open interworking).

Associated comparison algorithms are not standardized, and are generally company confidential.

Normally a BDB would be "captured" (produced) when a human subject (a person) is "enrolled" (registered with an organization), and archived (stored) with some additional metadata about the time of capture, the equipment used, and so on. It might be (only) archived on a smart-card to be carried by the human subject, or it might be (only) archived on a central database, or it might be archived on both. These options for archiving are subject to privacy concerns that might be expressed by the individual or in national legislation, and to the need to maintain backups.

A.11.1.7 Biometric Data Interchange Format: Signature/Sign Time Series Data (ISO/IEC 19794-7)

This International Standard specifies a BDB format for data captured when a person writes a signature or a personal sign (a generalization of the concept of a signature) using a digitizing tablet or an advanced pen system (see figure A.5).

The signature/sign time series data interchange format can be used for both intermediate data (serving as the starting point for further feature extraction) and feature data (to be compared using dynamic time warping algorithms).

The data recorded is a sequence of values at successive points in time, including values such as the position of the tip of the pen, the pressure exerted, the velocity and acceleration, and the "tilt" of the pen. Inclusion of the pen coordinates at each sample point is mandatory; the inclusion of other values is optional. The sampling may happen at fixed or varying time intervals.

The Standard defines two main formats, an expressive and flexible record format and a more compressed card format (with fewer options) that is especially suitable for storing BDBs on smart cards.

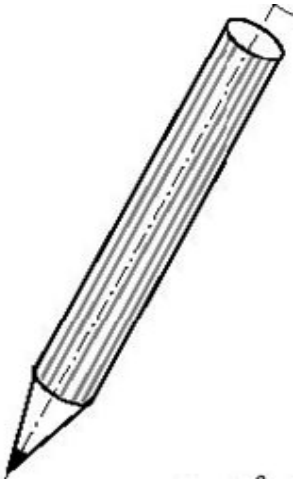

Figure A.5 — Pen

A.11.1.8 Biometric Data Interchange Format: Finger pattern Skeletal Data (ISO/IEC 19794-8)

The term "skeletal" here means that the BDB is based on reducing the image to a series of one-pixel-wide lines (see figure A.6) that represent the ridges of a finger print, and then producing either minutiae or spectral data from that "skeleton".

It thus incorporates much of the text and concepts of both the Finger Minutiae Data and the Finger Spectral Pattern Data standards.

Figure A.6 — A fingerprint skeleton

A.11.1.9 Biometric Data Interchange Format: Vascular Image Data (ISO/IEC 19794-9)

This International Standard defines a BDB format for recording "vascular data" taken from any of several parts of the human body. "Vascular data" means an image (usually taken using sensors operating in the near-infra-red) of the pattern of blood-vessels in that part of the human body. The parts of the human body considered are the palm, fingers, wrist and the back of the hands.

A.11.1.10 Biometric Data Interchange Format: Hand Geometry Silhouette Data (ISO/IEC 19794-10)

This International Standard defines a BDB format for the recording of the silhouette of a hand. Imagine shining a bright light onto a hand with the fingers spread-out, positioned over a light-sensing surface and record black or white for the image on the surface. In practice, a camera placed above a hand placed on a "platen" with pins to separate the fingers is commonly used. The BDB records a simple line that traces the outline of the silhouette from a start-point to an end-point. Both top-bottom and side silhouettes are supported.

The outline of the silhouette is what is recorded in the data, producing a relatively small BDB, but permitting measurements to be made of various characteristics of the silhouette for the purpose of comparison.

Figure A.7 — A hand silhouette

A.11.1.11 Biometric Data Interchange Format: Signature/Sign processed dynamic data (ISO/IEC 19794-11)

This is essentially an extension of ISO/IEC 19794-7 that records a variety of statistics related to the captured data.

A.11.1.12 Biometric Sample Quality (ISO/IEC 29794-1, 4, and 5)

This multi-part International Standard is intended to clarify the measurement of the quality of biometric samples corresponding to the parts of ISO/IEC 19794. Currently only Part 1 (Framework), Part 4 (Fingerprint Sample Quality), and Part 5 (Face Image Data Sample Quality) are under development.

A.11.1.13 Multimodal and Other Multibiometric Fusion (ISO/IEC 24722)

It is recognised today that biometric identification can be better performed if more than one biometric is involved in the comparison process. This is called a multibiometric approach. This can relate to multiple samples of the same biometric, or (more commonly) to the use of different biometrics (such as a finger-print combined with an iris image). The way comparison scores should be combined when multiple biometric templates are available is difficult and is called "fusion" of the scores. This is a Technical Report that is defining multibiometric terminology and recommending the way multibiometrics should be supported in BDBs, CBEFF and BioAPI. It will in due course result in amendments to some Standards, and probably a few new Standards.

A.11.2 Layer 2 Standards

A.11.2.1 Common Biometric Exchange Formats Framework (CBEFF): Data Element Specification (ISO/IEC 19785-1)

A number of International Standards specify the detailed format of a digital representation of various parts of the human body (finger prints, face, iris, etc - see ISO/IEC 19794) - a Biometric Data Block (BDB), but BDBs normally can only be processed by vendor-supplied biometric service provider (BSP) modules rather than by application-level code (as described, for example, in the BioAPI architecture). But while the application level typically treats the BDB as opaque data that it passes to or receives from a BSP, the application does need

information about the BDB so that, for example, it can determine which BSP (in a multi-BSP system) should process a particular BDB.

This Standard specifies an architecture for specifying biometric data structures that include both the BDB and the metadata about the BDB that can be accessed at the application level. The metadata is located in a substructure called the Standard Biometric Header (SBH), and the combination of an SBH and a BDB is called a Biometric Information Record (BIR). A BIR can also include a third substructure, called the Security Block (SB) which also contains data accessible to the application that describes any encryption or integrity attributes of the BIR.

This Standard specifies a range of data elements (metadata) that can be included in a SBH, and it specifies rules for defining BIRs that contain only one BDB (a simple BIR) and for BIRs that contain more than one BDB (a complex BIR).

The specification in this Standard is of a series of abstract types (data elements) and their semantics. It does not define their bit-level encoding. An organization that meets the requirements to be a CBEFF Patron can publish bit-level BIR specifications (BIR structure and content of the SBH) that conform to the requirements of this Standard. JTC 1 SC 37 is developing CBEFF Patron Formats (see A.11.2.3) to completely specify several generally useful BIR formats for storage or transfer or as examples for other organizations that want to develop their own.

This Standard also specifies transformation rules between BIR formats that support different sets of CBEFF data elements or different BIR structures.

A.11.2.2 Common Biometric Exchange Formats Framework (CBEFF): Procedures for the Operation of the Biometrics Registration Authority (ISO/IEC 19785-2)

This is quite a short Standard. ISO/IEC 19794 defined a variety of Biometric Data Block formats (a digital record of a fingerprint, palm, face, or iris etc.). ISO/IEC 19785-1 defined some metadata elements that could be associated with the BDB to form a Biometric Information Record (BIR). ISO/IEC 19785-3 will define a number of BIR formats (see A.11.2.3).

It is necessary to allocate world-wide globally unique identifiers for BDB formats, BIR formats, and biometric product types (software and hardware) of various sorts. This Standard specifies the operation of a Biometric Registration Authority that provides the registration (and publication) of the unique identification (using an ASN.1 Object Identifier - see ISO/IEC 8824 and ISO/IEC 9834) of such formats and products, and their definition.

A.11.2.3 Common Biometric Exchange Formats Framework (CBEFF): Patron Format Specifications (ISO/IEC 19785-3)

This Standard recognises the varying needs for particular domains of use to incorporate a minimum set or a full set of CBEFF data elements in their BIRs. This Standard specifies six (currently) BIR formats (CBEFF Patron Formats). These include formats that use both byte-orientation and more compact formats that use bit-fields for data elements, formats that include only a minimal set of CBEFF data elements and formats that include them all, and formats that include a bit-map to indicate which elements are present and which are absent.

Some are defined in English text with tables (tabular notation), some are defined more formally using ASN.1.

A.11.3 Layer 3 Standards

A.11.3.1 BioAPI - Biometric Application Programming Interface: BioAPI Specification (ISO/IEC 19784-1)

This (quite large) Standard specifies internal interfaces in a computer system using biometrics, and allows system integration of software components from different vendors (some with associated hardware).

The first and major software component is the BioAPI Framework (one BioAPI Framework per computer system). This is responsible for routing C programming-language calls from one or more applications running on the system - the second set of software components - to one or more Biometric Service Provider modules (that may have associated hardware) - the third set of software components.

The Biometric Service Provider modules are dedicated to biometric functions such as capturing a Biometric Data Block (a digital representation of a human finger, palm, face, or iris etc - see ISO/IEC 19794), or comparing a captured image with an archived image captured some time earlier, for the purposes of biometric authentication of an individual.

The interface between applications and the BioAPI Framework is called the API (Application Programming Interface), which gives the name to the Standard. The interface between the BioAPI Framework and Biometric Service Provider modules is called the SPI (Service Provider Interface).

Both the API and the SPI are specified in detail as a series of C (programming language) function calls and parameters of those function calls. (But modules can be written in Java or C++, for example, so long as they exhibit the defined C programming interface in their API and SPI interactions.)

A.11.3.2 BioAPI - Biometric Application Programming Interface: Biometric Archive Function Provider Interface (ISO/IEC 19784-2) and Biometric Capture Function Provider Interface (ISO/IEC 19784-3)

These parts of the BioAPI standard are the first of what is intended to be a series of Parts, each defining the interface to a particular type of Biometric Function Provider (BFP). A more detailed discussion is outside the scope of this text, and requires an understanding of the BioAPI architecture.

A.11.4 Layer 4 Standards

Biometric Interworking Protocol (BIP) (ISO/IEC 24708)

This is an International Standard that essentially provides bits-on-the-line communication from an application in one system to BSPs (for example, capture devices or biometric databases) in remote systems.

In essence, it takes the C-function calls of BioAPI and converts them into messages defined using ASN.1. Conformance only requires that the correct bits-on-the-line are used, but the text relies heavily on the BioAPI architecture and function calls. It could be described as providing a "distributed BioAPI".

It enables a complete biometric application (for example, turn-style control at a sports event or theme park to be provided by systems from multiple vendors at the different access points and at the central site. It also enables a central (probably government-operated) database repository of biometric templates to interwork with capture and verification or comparison systems at geographically remote sites, provided by different vendors.

A.11.5 Layer 5 Standards

A.11.5.1 Biometric Performance Testing and Reporting: Principles and Framework (ISO/IEC 19795-1)

This International Standard describes the principles and provides a framework for the scientific 'technical performance testing' of biometric systems and devices. Technical performance testing seeks to determine error and throughput rates, with the goal of understanding and predicting the real-world error and throughput

performance of a biometric system. The error rates include both false positive (false match) and false negative (false non-match) decisions, as well as failure-to-enrol and failure-to-acquire rates across the test population. Throughput rates refer to the number of subjects processed per unit time based both on computational speed and human–machine interaction.

It is concerned with the way in which performance testing should be conducted (size of sample population, etc), but also with the way in which the results should be reported in statistical and graphical form.

A.11.5.2 Biometric Performance Testing and Reporting: Testing Methodologies for Technology and Scenario Evaluation (ISO/IEC 19795-2)

This International Standard identifies approaches to performance testing, and provides guidelines for the organization and conduct of tests, and the reporting of results.

A.11.5.3 Biometric Performance Testing and Reporting: Modality Specific Testing (ISO/IEC TR 19795-3)

This International Standard provides a taxonomy for classifying biometric applications related to the way their performance should be tested. (Note that here "application" is used in a very general sense - "the use of biometrics for some purpose", not in the BioAPI computer-oriented sense of the application program part of a biometric system.) It identifies the appropriate testing method for each element in the taxonomy.

A.11.5.4 Biometric Performance Testing and Reporting: Performance of Biometric Access Control Systems (ISO/IEC 19795-4)

This International Standard establishes requirements for the performance-based assessment of systems that embed interoperable modular components. This includes comparison of acquisition devices, biometric data block generators, and comparison subsystems. The standard specifically addresses two performance issues: Do systems using standardized data perform as well as those using proprietary formats, and does a supplier's system perform as well on other suppliers' standardized biometric data blocks as on its own. The standard was developed after SC37 Working Group 3 were successful in producing a flight of data interchange standards most prominently the fingerprint templates (ISO/IEC 19794-2,3,8) and iris image (ISO/IEC 19794-6) standards.

A.11.5.5 BioAPI Conformance Testing: Methods and Procedures (ISO/IEC 24709-1)

This International Standard provides the notation and methodology for specifying conformance test suites that will enable the conformance of BioAPI components (particularly BSPs) to be tested by embedding them in a test-harness on the platform they are designed for.

A.11.5.6 BioAPI Conformance Testing: Test Assertions for BSPs (ISO/IEC 24709-2), Test Assertions for Frameworks ISO/IEC 24709-3), and Test Assertions for Applications (ISO/IEC 24709-4)

These International Standards give a detailed specification of the tests to be performed.

A.11.6 Layer 6 Standards

A.11.6.1 Biometric Profiles for Interoperability and Data Interchange: Biometric Reference Architecture (ISO/IEC 24713-1)

This International Standard discusses a biometric system in terms of the base functions it performs (rather than in the BioAPI architecture terms of software components) and includes administrative functions related to the operation of that system. **It is in some ways another tutorial on biometric applications**, and interestingly includes the concept of a "Watchlist" that is not present in other SC37 Standards.

It contains a layer diagram (not the same as that in this tutorial!) showing the relationship of the different SC 37 Standards. It is recommended supplementary reading for those that want a broader view of the SC 37 Standards and architecture.

A.11.6.2 Biometric Profiles for Interoperability and Data Interchange: Physical Access Control for Employees at Airports (ISO/IEC 24713-2)

One of the concerns in this International Standard is with the process of issuing "tokens" (typically a smart-card) to employees wanting access to secure areas, including the use of Watchlists.

A.11.6.3 Biometric Profiles for Interoperability and Data Interchange: Biometric-based verification and identification of Seafarers (ISO/IEC 24713-2)

This International Standard supports the work of the International Labour Organization (ILO) in providing biometric identification of ship-board employees.

A.11.7 Layer 7 Standards

Cross Jurisdictional and Societal Aspects of Biometric Technologies: Guide to the Accessibility, Privacy and Health and Safety issues in deployment of Biometric Systems for Commercial Applications (ISO/IEC TR 24714-1) and Practical application to specific contexts (ISO/IEC TR 24714-2)

These Technical Reports intend to provide guidance, examples of best practice and pointers to further information regarding the cross-jurisdictional and societal aspects in the introduction and use of biometrics.

They aim to address issues of:

— Accessibility (challenges posed by those who are sufficiently impaired to affect their usage of a biometric solution).

— Health and safety (including misconceptions of the risks involved in the use of biometrics and inferences about ethnic grouping, medical condition and gender from the biometric feature).

— Support of legal requirements and acknowledgement of cross-jurisdictional and societal considerations pertaining to personal information and privacy.

The documents are designed specifically for operators and system integrators who are considering the introduction of such systems in the private sector.

A.11.8 Vocabulary Standards

A.11.8.1 Harmonized Biometric Vocabulary

This work is attempting to agree (harmonize) definitions of biometric terms used in the various SC37 Standards. It concentrates on terms that are used in multiple Standards, and seeks to achieve a common definition.

A.11.8.2 Biometric Vocabulary Corpus, leading to Part 37 of ISO 2382 - Vocabulary

This work attempts to relate the concepts behind various biometric definitions, and to present them in a structured way so that relationships between different terms can be clearly identified, and their definitions coordinated prior to producing a final Biometrics Vocabulary Standard.

Annex B
(informative)

Terms and definitions used in International Biometric Standards

B.1 General concepts

B.1.1
authenticate
to prove or show to be of undisputed origin or veracity; genuine

B.1.2
authentication (deprecated)
(No definition provided)

NOTE 1 Use of this term as a synonym for biometric verification or biometric identification is deprecated.

NOTE 2 This term has been used in biometrics as a synonym primarily for biometric verification application and biometric verification function, but also as a synonym for biometric identification application and biometric identification function.

B.1.3
biometric
of or having to do with biometrics

NOTE The use of biometric as a noun, to mean biometric characteristic or biometric modality, is deprecated.

EXAMPLE Incorrect usage #1: ICAO resolved that face is the biometric most suited to the practicalities of travel documents.

EXAMPLE Correct usage #1: ICAO resolved that face recognition is the biometric modality most suited to the practicalities of travel documents.

EXAMPLE Incorrect usage #2: My face biometric was encoded in my passport.

EXAMPLE Correct usage #2: My facial biometric characteristics were encoded in my passport.

B.1.4
biometric characteristic
biometric (deprecated)
biological and behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable features can be extracted for the purpose of automated recognition of individuals

NOTE 1 Biological and behavioural characteristics are physical properties of body parts, physiological and behavioural processes created by the body and combinations of any of these.

NOTE 2 Distinguishing does not necessarily imply individualization.

EXAMPLE Examples of biometric characteristics are: Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, etc.

B.1.5
biometrics
automated recognition of individuals based on their behavioural and biological characteristics

NOTE "Individual" is restricted in scope by SC37 to humans.

B.1.6
system
an organized scheme or method; a complex whole; a set of things working together as a mechanism or interconnected network

B.2 Data-related terms

B.2.1
biometric data
biometric sample at any stage of processing, biometric reference, biometric feature or biometric property

B.2.2
Biometric Data Block (BDB)
block of data with a defined format that contains one or more biometric samples or biometric templates

NOTE Definition according to CBEFF.

B.2.3
biometric feature
output of a completed biometric feature extraction process

NOTE 1 The use of this term should be consistent with its use by the pattern recognition and mathematics communities.

NOTE 2 An uncompleted biometric feature extraction process might be an error message or a NULL vector.

NOTE 3 A biometric feature set can also be considered a processed biometric sample.

B.2.4
Biometric Information Record (BIR)
data structure containing one or more BDBs together with information identifying the BDB formats, and possibly further information such as whether the BDBs are encrypted

NOTE Definition according to CBEFF.

B.2.5
biometric property
descriptive attributes of the subject estimated or derived from the biometric sample

EXAMPLE Fingerprints can be classified by the biometric properties of ridge-flow (i.e. arch, whorl, and loop types); In the case of facial recognition, this could be estimates of age or gender.

B.2.6
biometric model
stored function (dependent on the individual) generated from one or more biometric features

NOTE 1 Comparison applies the function to the biometric features of a recognition biometric sample to give a comparison score.

NOTE 2 The function may be determined through training.

EXAMPLE Examples for the stored function could be a Hidden Markov Model or Artificial Neural Networks.

B.2.7
biometric reference
one or more stored biometric samples, biometric templates or biometric models attributed to a subject and used for comparison

EXAMPLE Face image on a passport; Fingerprint minutiae template on a National ID card; Gaussian Mixture Model, for speaker recognition, in a database.

NOTE A biometric reference may be created with implicit or explicit use of auxiliary data, such as Universal Background Models.

B.2.8
biometric sample
analog or digital representation of biometric characteristics prior to the biometric feature extraction process and obtained from a biometric capture device or biometric capture subsystem

NOTE A biometric capture device is a biometric capture subsystem with a single component.

B.2.8.1
captured biometric sample
raw biometric sample (deprecated)
biometric sample that is input to intermediate biometric sample processing

B.2.8.2
intermediate biometric sample
biometric sample that is the output intermediate biometric sample processing

EXAMPLE Intermediate biometric samples may have been enhanced for biometric feature extraction, compressed for compact storage purposes, etc.

B.2.8.3
recognition biometric sample
biometric sample that is used for recognition by comparison with a biometric reference

B.2.9
biometric template
set of stored biometric features comparable directly to biometric features of a recognition biometric sample

NOTE 1 A biometric reference consisting of an image, or other captured biometric sample, in its original, enhanced or compressed form, is not a biometric template.

NOTE 2 The biometric features are not considered to be a biometric template unless they are stored for reference.

B.2.10
data object
discrete data, considered as a unit, representing an instance of a data structure that is known or assumed to be known

NOTE Definition source: ISO 2382-17, term 17.01.11

B.2.11
database
collection of data organized according to a conceptual structure describing the characteristics of these data and the relationship among their corresponding entities, supporting one or more applications

B.2.12
record (in databases)
data object that is an instance of a record type

NOTE Definition source: ISO 2382-17, term 17.05.12

B.3 Capture-related terms

B.3.1
biometric capture device
device that collects a signal from a biometric characteristic and converts it to a biometric sample

NOTE 1 A signal can be generated by the biometric characteristic or generated elsewhere and affected by the biometric characteristic, for example, face illuminated by incident light.

NOTE 2 A device can be any piece of hardware (and supporting software and firmware).

B.3.2
biometric capture process
process of collecting or attempting to collect a signal from a biometric characteristic and converting it to a biometric sample

NOTE A signal can be generated by the biometric characteristic or generated elsewhere and affected by the biometric characteristic, for example, face illuminated by incident light.

B.3.3
biometric capture subsystem
components and sub-processes required to execute a biometric capture process

EXAMPLE In some systems, converting a signal from a biometric characteristic to a biometric sample may include multiple components such as a camera, photographic paper, printer, digital scanner, ink and paper.

B.3.4
capture
record or express accurately in words or pictures; cause data to be stored in a computer

B.4 Enrolment-related terms

B.4.1
biometric reference adaptation
automatic incremental updating of a biometric reference to mitigate performance degradation

NOTE For example, degradation may be from minor changes in the biometric characteristic, channel or sensor.

B.4.2
duplicate enrolment check
comparison of a recognition biometric sample / biometric feature / biometric model to some or all of the biometric references in the enrolment database to determine if any similar biometric reference exists

B.4.3
enrol
create and store, for an individual, an enrolment data record associated with an individual and including biometric reference(s) and, typically, non-biometric data

B.4.4
enrolment data record
record created upon enrolment, associated with a subject and including one or more biometric references

B.4.5
enrolment
registration (deprecated)
the action of enrolling or being enrolled

B.4.6
enrolment data record
record created upon enrolment, associated with a subject and including one or more biometric references and typically non-biometric data

B.4.7
re-enrolment
process of establishing a new biometric reference for an individual already enrolled in the database

NOTE 1 Re-enrolment requires one or more new captured biometric samples.

NOTE 2 For example, re-enrolment may be required as a result of performance degradation due to major changes in the system or biometric characteristics.

B.4.8
registration
the action or process of registering or of being registered; exact correspondence of the position of printed matter on the two sides of a leaf

NOTE 1 Register – v – enter in or place on a register.

NOTE 2 Register – n – an official list of record.

NOTE 3 Definition source for registration and register (verb and noun): Oxford dictionary.

B.5 Process and system-related terms

B.5.1
biometric feature extraction process
algorithm applied to a biometric sample with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from other biometric samples

NOTE 1 Filters applied to biometric samples are not themselves biometric features, however the output of the filter applied to these samples may be. Therefore, for example, eigenfaces are not biometric features.

NOTE 2 Repeatable implies low variation between outputs generated from samples of the same individual.

NOTE 3 Distinctive implies high variation between outputs generated from samples of different individuals.

B.5.2
biometric system
system used for the purpose of the automated recognition of individuals based on their behavioural and biological characteristics