Reference number of working document: ISO/IEC JTC 1/SC 37/N0000

Date: 2021-08-16

Reference number of document: **ISO/IEC CD 24741:2021**

Committee identification: **ISO/IEC JTC 1/SC 37/WG 4**

Secretariat: ANSI

Information technology — Biometrics — Overview and application

Technologies de l'information — Aperçu général et applications

Contents

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, SC 37, *Biometrics*.

This third edition cancels and replaces the second edition (ISO/IEC TR 24741:2017), which has been technically revised with the following changes:

– guidance on the international standards that underpin the use of biometric recognition systems;

— ...

Introduction

“Biometric recognition” is the automated recognition of individuals based on their biological and behavioural characteristics. The field is a subset of the broader field of human identification science. Example technologies include, among others: fingerprinting, face recognition, hand geometry, speaker recognition and iris recognition.

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

“Biometric recognition” 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 — Overview and application

1 Scope

This document describes the history of biometrics and what biometrics does, the various biometric technologies in general use today (for example, fingerprint recognition, face recognition and iris recognition) and the architecture of the systems and the system processes that allow automated recognition using those technologies. It also provides information about the application of biometrics in various business domains such as border management, law enforcement and driver licensing, the societal and jurisdiction considerations that are typically taken into account in biometric systems.

Additionally, this document identifies and provides guidance on the use of the international standards that underpin the use of biometric recognition systems.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

4 Introduction and fundamental concepts

4.1 What are biometric technologies?

The definition of biometrics in ISO/IEC 2382-37 is “automated recognition of individuals based on their biological and behavioural characteristics”.

NOTE 1 The all-encompassing term “biometrics” refers to “the application to biology of the modern methods of statistics”. In the context of this document, we are concerned with automated technologies that analyse human characteristics for recognition purposes; the general application of statistics to biological systems is a separate discipline.

The term “biometric characteristic” is defined as “biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition”. So, biometric technologies are related to physical parts of the human body or the behavioural traits of human beings, and the recognition of individuals based on either or both of those parts or traits. A fuller explanation of the various biometric technologies is given in Clause 6.

NOTE 2 ISO/IEC 2382-37 recommends the use of the term “biometric” only as an adjective and deprecates its use as a noun in places where the fuller term biometric characteristic (as above) would be more appropriate.

The perfect biometric characteristic 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 presented to a sensor (for example, camera or fingerprint scanner or finger-geometry measurement device);
- *Universal*: observable on all people;
- *Acceptable:* the subject is prepared to use the biometric characteristic in the given application.

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

4.2 What biometric systems do

It has been recognized since 1970 that for some applications there are three pillars of automated personal recognition (IBM 1970[25]):

a) something known or memorized;

b) something carried;

c) a personal physical characteristic.

The original context for this concept was secure access control to computer data. The underlying assumptions were that persons authorized to access secure data would cooperatively make positive claims (e.g. "I am authorized to access data on the system") and could be counted on to protect their Personal Identification Numbers (PINs) and passwords. In such applications, biometric technologies do indeed compete with PINs, passwords and tokens, but have received less acceptance. For example, most web-based access control requires a User ID and an associated password, not biometrics. Passwords have been more widespread than biometrics in such applications because they are easily replaced, can vary across applications, require no specialized acquisition hardware, can be created with different levels of security and are exactly repeatable under conscious control.

However, in many applications, PINs, passwords and tokens cannot logically meet the security requirements. For example, PINs, passwords and tokens cannot logically be used in applications where enrolled individuals have little motivation to protect their accounts against use by others, such as with amusement parks. Similarly, in applications where the claim is negative (e.g. "I am not enrolled in the system as Pat") PINs, passwords and tokens cannot logically meet the requirements of demonstrating the truth of the claim.

Biometric systems recognize persons by observing physical and behavioural characteristics of their bodies. Biometric characteristics are not as easy to transfer, forget or steal as PINs, passwords and tokens, so they can be used in applications for which these other authentication methods are inappropriate. Biometrics can be combined with PINs and tokens into "multifactor" systems for added security.

Although biometric technologies cannot directly "identify" persons, they can link bodies to records of attributes, which we will call "identities". Consequently, biometric recognition can become part of an identity management system.

Biometric recognition is used in two main classes of applications: 1) those that use biometric comparison to verify a biometric "claim of identity"; and 2) those that search a database of the biometric characteristics of known individuals to find and return the identifier attributable to a single individual. The former applications are called "biometric verification" and the latter, "biometric identification". Biometric systems can also be used to "cluster" characteristics, labelling together those that come from the same bodily source (i.e. from the same person and biometric instance), even when the bodily source cannot be attributed to any known individual. Such types of systems are gaining application in law enforcement.

Biometric verification systems verify claims (test hypotheses) regarding the source of a biometric data record in a database. The claim can be made by the person presenting a biometric sample (e.g. "*I am the source of a biometric data record in the database"*) or the claim can be made 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"*; *"These two samples came from the same bodily source"*) 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 the terminology of ISO/IEC 2382-37, an individual's biometric data record in a database is referred to as a "biometric reference" and the biometric sample used for comparison with the stored biometric reference is referred to as a "biometric probe". We can look for a "match" between the biometric probe of an individual and an identified biometric reference stored in the database, or we can search a population of biometric references in a database for a match with the supplied biometric probe and return an identifier for any reference that matches. In both cases, we have to set thresholds for how close the comparison has to be before we can consider the biometric probe and the biometric reference to have come from the same bodily source (a "match"). Of course, errors can be made: either by a "false non-match", failing to correctly declare a "match" when the probe and reference are indeed from the same bodily source, or by a "false match", incorrectly declaring a match when the probe and reference are from different bodily sources. We talk about the proportion 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 reference as an attribute of the enrolment record. These systems "verify" that the biometric reference in the claimed enrolment record matches the probe sample submitted by the subject. Some systems, such as those for social service and driver licensing, verify negative claims of no biometric data record already in the database by treating the biometric reference as a record identifier or pointer. These systems search the database of biometric pointers to find one matching the submitted biometric probe (and the process is one of biometric identification). 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 biometric probe to only the biometric reference in the single claimed record.

For example, a subject might claim to be the source of the fingerprint biometric reference stored on an immigration card. To prove the claim, the subject would insert the card into a card reader which reads the reference record, then place their finger on the fingerprint reading device. The system compares the biometric characteristics of the fingerprint on the reader with those of reference recorded on the card. The system may conclude, in accordance with defined thresholds, that the subject is indeed the source of the reference 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 biometric characteristics that are 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 references 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.

The number of comparisons to be made, and the "prior" probabilities that those comparisons will result in a "match" (determination that biometric probe and reference have the same bodily source) will depend upon both the claim and the system architecture. The security risk posed by a wrong determination will also vary by system function. Consequently, some systems are very sensitive to false matches (false positives), while some systems are very sensitive to false non-matches (false negatives) for any comparison. Depending upon the claim, either a false positive or a false negative might result in either a "false acceptance" or "false rejection" of the claim.

5 History

In a non-automated 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 use 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 (Bertillon 1889[4]). 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, began in the late 1850s, knowledge of the technique did not become known in the western world until the 1880s (Faulds, 1880[15]; Herschel, 1880[23]) when it was popularized scientifically by Sir Francis Galton (1888[18]) and in literature by Mark Twain (1893[71]). 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[57]) and retinal identification was suggested in 1935 (Simon and Goldstein, 1935[67]). However, at this time none of these techniques were automated.

Work in automated speaker recognition can be traced directly to experiments with analogue filters done in the 1940s (Potter, Kopp and Green, 1947[61]) and early 1950s (Chang, Pihl, and Essignmann, 1951[13]). With the computer revolution picking up speed in the 1960s, speaker (Pruzansky, 1963[62]) and fingerprint (Trauring, 1963a[69]) pattern recognition were among the very first applications in automated signal processing. By 1963, a "wide, diverse market" for automated fingerprint recognition was identified, with potential applications in "credit systems", "industrial and military security systems" and for "personal locks" (Trauring, 1963b[70]). Computerized facial recognition research followed (Bledsoe, 1966[6]; Goldstein, Harmon, and Lesk, 1971[19]). In the 1970s, 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[77]), measures from multiple biometric devices were being combined (Messner, Cleciwa, Kibbler, and Parlee, 1974[52]; Fejfar, 1978[16]) and government testing guidelines were published (Meissner, 1977[51]).

Running parallel to the development of hand technology, fingerprint recognition was making progress in the 1960s and 1970s. During this time a number of companies were involved in automated 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 identification systems developed for the FBI in the 1960s and 1970s increased the level of automation, but these were ultimately based on fingerprint comparisons by trained examiners. Automated Fingerprint Identification Systems (AFIS) were first

implemented in the late 1970s, most notably by the Royal Canadian Mounted Police AFIS in 1977. The role of biometrics in law enforcement has mushroomed since then and AFIS are used by a significant number of police forces throughout the globe. Building on this early success, biometric usage is now being explored in 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[17]), iris recognition systems became available in the mid-1990s (Daugman, 1993[14]). 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/finger vein patterns.

Today's speaker verification systems have their roots in technological achievements of the 1960s, while biometric technologies such as iris, finger vein, and facial recognition are relative newcomers to the industry. 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 any laboratory technology to migrate to a fully operational system. However, such systems are now in place and proving themselves across a range of diverse applications.

6 Overview of biometric standardisation

6.1 Standards Developing Organisations

A standard is a document, established by consensus and approved by a recognized body, that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits.

There are a number of Standards Developing Organizations (SDOs) developing biometric standards. Most are private sector organizations. There are presently around 200 biometric standards published or under development. Almost all of these biometric standards have been developed, revised, amended, or corrected as a result of innovation, and feedback from testing and implementation over the last twenty years.

Under ISO (the International Organization for Standardization) the following technical committees develop standards for biometrics:

- ISO/IEC JTC 1 SC 37 Biometrics;
- ISO/IEC JTC 1 SC 17 Cards and security devices for personal identification;
- ISO/IEC JTC 1 SC 27 Information security, cybersecurity and privacy protection.

Other SDOs developing biometric standards include:

- CEN/TC 224, the European Committee for Standardization, Technical Committee 224, Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment;
- FIDO (Fast IDentity Online) Alliance;
- IEEE, the Institute of Electrical and Electronics Engineers;
- ICAO, the International Civil Aviation Organization;
- ISO/TC 68, ISO Technical Committee 68, Financial Services;
- ITU-T, the International Telecommunication Union Telecommunication Standardization Sector;
- NIST, the National Institute of Standards and Technology of the United States Department of Commerce;

– OASIS, and the Organization for the Advancement of Structured Information Standards.

Clause 6.2 provides a representative snapshot of the types of biometric standards and the SDOs involved. These standards are periodically reviewed and reaffirmed, revised, or withdrawn. Moreover, amendments or corrections can occur at any time. Therefore, the SDOs' web pages should be checked for the latest status of these standards.

6.2 Types of biometric standards

6.2.1 Biometric data interchange format standards

These standards specify the common content, meaning, and representation of biometric data formats of biometric modalities (e.g., fingerprint, iris, face, DNA). See Table 1.

Table 1 — Example standards: Biometric and data interchange formats

Published & under development	SDO
ISO/IEC 19794 Series (Parts 1-11, 13-15) Biometric data interchange formats	ISO/IEC JTC 1/SC 37
ISO/IEC 39794 Series (Parts 1-2, 4-6, 9, 16, 17) Extensible biometric data interchange formats	ISO/IEC JTC 1/SC 37
ANSI/NIST-ITL 1 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information	NIST ITL

6.2.2 Biometric technical interface standards

These standards specify interfaces and interactions between biometric components and sub-systems, as well as the possible use of security mechanisms to protect stored data and data transferred between systems. See Table 2.

Using biometric data interchange format and biometric technical interface standards allows for data interchange and interoperability between biometric systems, which can include components of different design or manufacture.

Table 2 — Example standards: Biometric technical interfaces

Published & under development	SDO
ISO/IEC 19784 Series (Parts 1-2, 4), Biometric application programming interface	ISO/IEC JTC 1/SC 37
ISO/IEC 19785 Series (Parts 1-4), Common Biometric Exchange Formats Framework	ISO/IEC JTC 1/SC 37

6.2.3 Biometric conformance testing standards

These standards specify the concepts, framework, test types, test methods, and criteria required to test conformity of biometric products claiming conformance to biometric data interchange records or biometric technical interfaces. See Table 3

Table 3 — Example standards: Biometric conformance testing

Published & under development	SDO
ISO/IEC 24709 Series (Parts 1-3), Conformance testing for the biometric application programming interface (BioAPI)	ISO/IEC JTC 1/SC 37
ISO/IEC 29109 Series (parts 1-2, 4-10), Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794	ISO/IEC JTC 1/SC 37
ISO/IEC 18584, Conformance test requirements for on-card biometric comparison	ISO/IEC JTC 1/SC 17

applications	

6.2.4 Biometric sample quality standards

These standards specify the use and testing of image quality metrics for a particular modality (e.g., face, iris), which impacts the accuracy of a biometric comparison. See Table 4.

Table 4 — Example standards: Biometric sample quality

Published & Under development	SDO
ISO/IEC 29794-1, Biometric sample quality — Part 1: Framework	ISO/IEC JTC 1/SC 37
ISO/IEC 29794-4, Biometric sample quality — Part 4: Finger image data	ISO/IEC JTC 1/SC 37
ISO/IEC TR 29794-5, Biometric sample quality — Part 5: Face image data	ISO/IEC JTC 1/SC 37
ISO/IEC 29794-6, Biometric sample quality — Part 6: Iris image data	ISO/IEC JTC 1/SC 37

6.2.5 Biometric application profile standards

These standards define conforming subsets or combinations of base standards used to provide specific functions (e.g., enrolment, verification, identification). Profiles facilitate implementations of the base standards (e.g. biometric data interchange format and biometric interface standards) for defined applications. These profile standards define the functions of an application (e.g. physical access control for employees at airports) and then specify use of options in the base standards to ensure biometric interoperability. See Table 5.

Table 5 — Example standards: Biometric application profiles

Published & under development	SDO
ISO/IEC 24713 Series (Parts 1-3), Biometric profiles for interoperability and data interchange	ISO/IEC JTC 1/SC 37
ISO/IEC 30137 Series (Parts 1 and 4), Use of biometrics in video surveillance systems	ISO/IEC JTC 1/SC 37
ISO/IEC TR 20027, Biometric interoperability profiles – Best practices for slap tenprint capture	ISO/IEC JTC 1/SC 37
ISO/IEC TR 29195, Traveller processes for biometric recognition in automated border control systems	ISO/IEC JTC 1/SC 37
ISO/IEC TR 30125, Biometrics used with mobile devices	ISO/IEC JTC 1/SC 37
ISO/IEC WD TS 22604, Biometric recognition of subjects in motion in access related systems	ISO/IEC JTC 1/SC 37
ISO/IEC WD 24358, Face-aware capture subsystem specifications	ISO/IEC JTC 1/SC 37

6.2.6 Biometric performance testing and reporting standards

These standards specify testing methodologies to determine error and throughput rates. This provides an empirical basis for predicting the real-world error and throughput performance of biometric systems. The error rates include both false positive and false negative decisions, as well as failure-to-enrol and failure-to-acquire rates across the test population. Throughput rates refer to the number of users processed per unit time based both on computational speed and human-machine interaction. These measures are generally applicable to all biometric systems and devices. See Table 6.

Table 6 — Example standards: biometric performance testing and reporting

Published & under development	SDO
ISO/IEC 19795 Series (Parts 1-7, 9) Biometric performance testing and reporting	ISO/IEC JTC 1/SC 37
ISO/IEC TR 29156:2015, Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics	ISO/IEC JTC 1/SC 37
ISO/IEC 29197:2015, Evaluation methodology for environmental influence in biometric system performance	ISO/IEC JTC 1/SC 37
ISO/IEC 30136:2018, Performance testing of biometric template protection schemes	ISO/IEC JTC 1/SC 37

6.2.7 Biometric security standards

These standards deal with various biometric-specific aspects of security. These include 1) principles to be considered during the security evaluation of a biometric system and 2) guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. See Table 7.

Table 7 — Example standards: Biometric security

Published & under development	SDO
ISO/IEC 19792, Security techniques — Security evaluation of biometrics	ISO/IEC JTC 1/SC 27
ISO/IEC 19989 series (Parts 1 to 3), Information security — Criteria and methodology for security evaluation of biometric systems	ISO/IEC JTC 1/SC 27
ISO/IEC 24745, Security techniques — Biometric information protection	ISO/IEC JTC 1/SC 27
IEEE 2790, IEEE Standard for Biometric Liveness Detection	IEEE Biometric Liveness Detection Working group
ISO/IEC 30107 Series (Parts 1-4), Biometric presentation attack detection	ISO/IEC JTC 1/SC 37
ITU-T X.1092, Integrated framework for telebiometric data protection in e-health and telemedicine	ITU-T SG 17
ITU-T X.1091, A guideline for evaluating telebiometric template protection techniques	ITU-T SG 17
ITU-T X.1087, Technical and operational countermeasures for telebiometric applications using mobile devices	ITU-T SG 17
ITU-T X.1086, Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security	ITU-T SG 17
ITU-T X.1081, The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics	ITU-T SG 17

6.2.8 Biometric authentication standards

These standards define requirements to establish corroboration that an entity is the one claimed. This includes requirements for checking the validity of the result of a biometric enrolment and verification process executed at a remote site via a network or a web-based service. See Table 8.

Table 8 — Example standards: Biometric authentication

Published & under development	SDO
ISO/IEC 30108-1, Biometric Identity Assurance Services — Part 1: BIAS services	ISO/IEC JTC 1/SC 37

ISO/IEC WD 30108-2, Biometric Identity Assurance Services — Part 2: REST-based implementation	ISO/IEC JTC 1/SC 37
ISO/IEC 7816-11, Integrated circuit cards — Part 11: Personal verification through biometric methods	ISO/IEC JTC 1/SC 17
ISO/IEC 17839-1, Biometric System-on-Card — Part 1: Core requirements	ISO/IEC JTC 1/SC 17
ISO/IEC 17839-3, Biometric System-on-Card — Part 3: Logical information interchange mechanism	ISO/IEC JTC 1/SC 17
ISO/IEC 24787, On-card biometric comparison	ISO/IEC JTC 1/SC 17
ISO/IEC TR 30117, Guide to on-card biometric comparison standards and applications	ISO/IEC JTC 1/SC 17
ISO/IEC 24761, Authentication context for biometrics	ISO/IEC JTC 1/SC 27
ISO/IEC 17922, Telebiometric authentication framework using biometric hardware security module	ISO/IEC JTC 1/SC 27 ITU-T SG 17
2410-2019 - IEEE Standard for Biometric Open Protocol	IEEE BOP - Biometrics Open Protocol WG
Biometric Identity Assurance Services (BIAS) SOAP Profile Version 2.0 Committee Specification 01, 11 July 2017	OASIS Biometric Services (BIOSERV) TC
WS-Biometric Devices Version 1.0 Committee Specification 01, 11 July 2017	OASIS Biometric Services (BIOSERV) TC
ISO 19092:2008, Financial services — Biometrics — Security framework	ISO/TC 68/SC 2
FIDO Universal Authentication Framework (UAF) Reference Architecture Feb 2017	FIDO
ITU-T X.1094 (03/2019): Telebiometric authentication using biosignals	ITU-T SG 17
ITU-T X.1093 (11/2018): Telebiometric access control with smart ID cards	ITU-T SG 17
ITU-T X.1090 (05/2011): Authentication framework with one-time telebiometric templates	ITU-T SG 17
ITU-T X.1089 (05/2008): Telebiometrics authentication infrastructure (TAI)	ITU-T SG 17
ITU-T X.1086 (11/2008): Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security	ITU-T SG 17
ITU-T X.1084 (05/2008): Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems	ITU-T SG 17
Doc 9303 Machine readable travel documents — Part 9: Deployment of biometric identification and electronic storage of data in MRTDs (Eighth Edition, 2020)	ICAO

6.2.9 Standards on cross-jurisdictional and societal aspects of biometrics

These standards provide guidance on the design and implementation of biometric technologies with respect to usability, accessibility, health and safety, taking into account legal, cultural, ethical and societal considerations. See Table 9.

Table 9 — Example standards: Cross-jurisdictional and societal aspects of biometrics

Published & under development	SDO
ISO/IEC 24779 series (Parts 1, 4, 5, and 9), Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems	ISO/IEC JTC 1/SC 37
ISO/IEC 24714, Information technology — Cross-jurisdictional and societal aspects of biometrics — General guidance	ISO/IEC JTC 1/SC 37

ISO/IEC TR 29194, Information Technology — Biometrics — Guide on designing accessible and inclusive biometric systems	ISO/IEC JTC 1/SC 37
ISO/IEC TR 30110, Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and children	ISO/IEC JTC 1/SC 37

6.2.10 Biometric vocabulary standards

A general biometric vocabulary standard provides a systematic description of the concepts in the field of biometrics pertaining to recognition of human beings and reconciles variant terms in use in pre-existing biometric standards against the preferred terms, thereby clarifying the use of terms in this field. Specific biometric standards may also include other definitions for terms that apply to that standard. See Table 10.

Table 10 — Example standards: Biometric vocabulary

Published & under development	SDO
ISO/IEC 2382-37:2017, Vocabulary — Part 37: Biometrics	ISO/IEC JTC 1/SC 37

7 Overview of biometric technologies

7.1 Finger and palm ridge technologies

7.1.1 Fingerprint imaging

Historically, fingerprints were collected by placing inked fingers onto collection cards. In the early days of automated fingerprint recognition, those cards were then scanned into a computer. With the advent of technologies that collect fingerprints without the use of ink, previous methods are considered obsolete. However, there may be occasions when an inked collection is still necessary, e.g. when the capture device is unable to acquire the biometric subject's fingerprint or is unavailable. Very recently, contactless systems have been developed that use either laser or standard lighting that do not require the fingers to touch any surface.

Fingerprints derived from finger friction ridges may vary from instance to instance for many reasons. For example, finger moisture, angle of placement, pressure and ridge damage will all change the images captured. The way a subject interacts with a finger scanner is of utmost importance. This includes the height and angle of the fingerprint scanner in relationship to the data subject. Vendors are addressing these problems so that scanners are ergonomically designed to optimize the fingerprinting process.

A key difference between the various contact-based fingerprint technologies on the market is the means of capturing an image. Most large-scale systems capture finger images using the optical technique or by electronically scanning inked images from paper. Other capture techniques include capacitive, thermal and ultra-sonic devices.

In contact fingerprint systems, the optical image technique is based on the concept of "frustrated total internal reflection". A glass platen is illuminated from below at an angle of incidence just beyond the critical angle at which light becomes reflected. If nothing is touching the topside of the platen, all of the light is reflected into the camera sensor. But where a finger ridge is touching the platen, the internal reflection is "frustrated", i.e. the light rays are not reflected but pass through to the finger. Consequently, the resulting fingerprint image is dark where there are ridges and light where there are valleys, replicating the pattern obtained through traditional ink impressions.

With capacitive fingerprint sensors, the platen comprises an array of tiny cells, each smaller than the width of a fingerprint ridge. Measurement of capacitance over the cells in the array indicates where the finger ridges are in contact with the sensor, generating a fingerprint image.

Thermal techniques use silicon chip technology to acquire fingerprint data as the subject moves a finger across the sensor. Variation in temperature between the ridges and the valleys are sensed and converted into a black and white image.

Ultra-sonic imaging 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.

Fingerprints can be imaged one at a time, or in combinations of two or four. An image of four fingers (index through little finger) is known as a “slap”. Two “slaps” (one from each hand) are taken, followed by a single image of both the thumbs to create a “ten-print” image. In large-scale identification systems, individuals are enrolled using the optical live-scan capture process using multiple fingers, often taken as “slaps” as described above. Law enforcement AFIS capabilities may include a biometric collection kit or “booking station” that will capture prints of all ten fingers. A booking station may operate in a standalone capability without connection to an AFIS system. A civil AFIS, however, need not capture all fingerprints and can operate effectively using as few as two.

Regardless of the fingerprint imaging technology employed, the fingerprint scanner develops a matrix of numbers, each corresponding to a pixel, representing the fingerprint. The standard resolution for fingerprint images is 500 pixels per inch. The numbers in the matrix generally range from 0 (dark) to 255 (light), but some non-optical scanners may output only a matrix of 0s and 1s.

Fingerprint imaging is a special case of the more general biometric trait of friction ridges. Just as a fingerprint’s friction ridges can be captured by an appropriate technology, so can the friction ridges of palms, feet, and toes.

7.1.2 Fingerprint comparison

There are many ways to compare fingerprints computationally (the word “computationally” is added here to indicate exclusion of optical comparison methods developed in the 1960s and 1970s, which will not be covered in this document). The major computational approaches are: 1) transform-based; 2) local correlation; and 3) minutiae-based. All three have been used in commercial systems. While minutiae-based systems were once the most popular, new uses of fingerprint recognition (for example on smartphones with small area sensors) and breakthrough in accuracy due to Convolutional Neural Networks have made transform-based approaches at least as common.

We start with the premise that no two fingerprints are alike. That is, even the same finger placed twice on a fingerprint platen will produce two different images of the ridge structure. We will never be in a position of comparing two identical fingerprints even from the same finger. The within-class variation of fingerprints from the same finger has many causes including changes in pressure and orientation of finger placement, finger moisture and ridge damage, as well as changes of imaging device.

So how can we compare fingerprints under such circumstances? Transform-based methods were generally based on two-dimensional Fourier transforms and Hough transforms applied to the matrix of pixels representing the fingerprint. In recent years, Convolutional Neural Networks have been successfully used to significantly increase accuracy. The idea is to mathematically transform the image in some way, then compare coefficients of the transformed images. In this context, the fingerprints’ “features” are the transform coefficients. ISO/IEC 19794-3[33] was developed as a standard for transform-based fingerprint transmission and storage.

Correlation-based methods recognize that fingerprints, and their representative matrices from the scanner, cannot simply be overlaid owing to all the variation. However, small areas of two fingerprints, when overlaid, might be correlated. If the geometrical relationship between centres of the small areas remains about the same when overlaid to maximize correlation between the two images, maybe the images are of the same finger friction ridges.

Minutiae-based methods analyse small friction ridge features of the finger and emulate what forensic fingerprint examiners do. The minutiae are the ridge endings, and bifurcations (branching of fingerprint ridges). Minutiae also have a direction associated with the ridge at the point they occur, and the distance between ridges may also be analysed. The mathematical algorithm moves over the image looking for ridges and where they split or end and creating a minutiae map. To compare two fingerprints, we lay their minutiae maps on top of each other and spin/slide them around. If we can get some number of minutiae to overlay in position and direction, we call it a “match”.

7.1.3 Palm technologies

Palm biometrics can be closely aligned with finger-scanning, and in particular AFIS technology. As with fingers, friction ridges containing minutiae points are found on the palm. These can be captured using optical techniques as with fingerprinting. This area of the biometrics industry is particularly focused on the law enforcement community, as latent palm prints are as useful in criminal investigation as latent fingerprints. The capture and comparison processes for palm prints are essentially the same as those for fingerprints. Some collection platforms are suitable for both fingerprint and palmprints.

Other palm biometrics based not on the friction ridge structures but on the palm creases have been developed in laboratory programs.

7.1.4 International standards for finger and palm ridge biometrics

- ISO/IEC 19794-2:2005 Information technology — Biometric data interchange formats — Part 2: Finger minutiae data (+AMD 1:2010, COR 2:2014)
- ISO/IEC 19794-2:2011 Information technology — Biometric data interchange formats — Part 2: Finger minutiae data (+AMD 2:2015)
- ISO/IEC 19794-3:2006 Information technology — Biometric data interchange formats — Part 3: Finger pattern spectral data
- ISO/IEC 19794-4:2011 Information technology — Biometric data interchange formats — Part 4: Finger image data (+AMD 2: 2015)
- ISO/IEC 19794-8:2011 Information technology — Biometric data interchange formats — Part 8: Finger pattern skeletal data (+AMD 1:2014)
- ISO/IEC 19794-15:2017 Information technology — Biometric data interchange format — Part 15: Palm crease image data
- ISO/IEC 20027:2018 Information technology — Guidelines for slap tenprint fingerprint capture
- ISO/IEC 24779-4:2017 Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems — Part 4: Fingerprint applications
- ISO/IEC 29109-2:2010 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 2: Finger minutiae data
- ISO/IEC 29109-4:2010 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 4: Finger image data
- ISO/IEC 29109-8:2011 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 8: Finger pattern skeletal data
- ISO/IEC 29141:2009 Information technology — Biometrics — Tenprint capture using biometric application programming interface (BioAPI)
- ISO/IEC 29794-4:2017 Information technology — Biometric sample quality — Part 4: Finger image data
- ISO/IEC 39794-4:2019 Information technology — Extensible biometric data interchange formats — Part 4: Finger image data

7.2 Face technologies

7.2.1 Overview

Automatically identifying an individual by analysing a face is a complex process for which there are a variety of algorithmic approaches. A number of biometric vendors and research institutions have developed facial recognition systems that use digital photographs or video to capture images in visible, near IR or far IR (thermal) wavelengths. Facial recognition is made difficult by changes in images of the same face owing to

pose angle, lighting, facial expression or adornment, and by the basic structural similarity of all faces (generally a mouth placed under a nose placed below and between two eyes). Facial recognition is also subject to ageing effects, more strongly than most other modalities, a large timespan between the acquisition of the probe and reference samples can significantly degrade recognition accuracy.

Algorithms often start the identification process with image enhancement and normalization: finding eye centres, reposing the facial image to a full-frontal orientation, and adjusting for shadows etc. On the normalized image, a variety of image processing techniques are available to extract abstract measures from the image by the placement of filters over all or parts of the face. The extracted “facial features” are abstract measures not related directly to distances between “landmarks” on the face, such as nose, mouth and ears. Such measures, however, need to be both stable (not changing much for each person from image to image) and distinctive (varying greatly between persons).

At the current level of development, facial recognition technology can work quite accurately with high resolution (more than 100 pixels between the eye centres), full frontal images in good lighting. However performance degrades as resolution reduces or pose angle increases. Lighting variations also cause a decrease in accuracy. In the mid-2010s, the usage of Convolutional Neural Networks (CNN) to detect and encode face data provided a major technological breakthrough in the accuracy of facial recognition algorithms; Error rates dropped by orders of magnitude in the span of a few years, and this fast improvement is still ongoing at time of writing. This improvement has allowed facial recognition to be used effectively in previously challenging settings. At the current level of development, facial recognition technology can work quite accurately even with limited resolution (from 30 pixels between the eye centres) and is resilient to most defects (lighting, pose angle). Only when several strong defects are present simultaneously a decrease in accuracy will be noticed.

Three-dimensional maps of the face can be created through various means, such as through laser ranging, the projection of a grid on to the face to observe grid distortion owing to facial structure, merging of multiple images, or using shading information in a single image.

Thermal imaging analyses 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 and facial recognition systems based on this technology have not been commercially available since the 1990s.

7.2.2 International standards for face recognition

7.2.2.1 Biometric data interchange format standards for face

Biometric facial recognition systems rely upon standardized biometric data interchange formats for face images that can be stored, transmitted and processed.

The International Civil Aviation Organization (ICAO) develops standards for travel documents such as passports. These travel documents use internationally standardized biometric data interchange formats for traveller verification by face, fingerprint, or iris.

The present ICAO implementation uses the first generation of facial data interchange format standards developed by ISO/IEC JTC 1/SC 37, Biometrics. These standards remain valid as long as needed for the transition to ISO/IEC 39794-5 in ePassports.

- ISO/IEC 19794-1:2006 Information technology — Biometric data interchange formats — Part 1: Framework
- ISO/IEC 19794-5:2005 Information technology — Biometric data interchange formats — Part 5: Face image data
- ISO/IEC 29109-5:2019 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 5: Face image data

— Implementations wishing to conform to the present ICAO requirements for ISO/IEC biometric data interchange format standards for face should use the above standards.

The second generation of biometric data interchange format standards for face developed by ISO/IEC JTC 1/SC 37 are also available for more recent implementations.

— ISO/IEC 19794-1:2011 Information technology — Biometric data interchange formats — Part 1: Framework

— ISO/IEC 19794-5:2011 Information technology — Biometric data interchange formats — Part 5: Face image data (+AMD 2:2015)

Implementations wishing to conform to the second generation of ISO/IEC biometric data interchange format standards for face should use the above standards.

— ISO/IEC 39794-5 Information technology — Extensible biometric data interchange formats — Part 5: Face image data

ISO/IEC 39794-5 provides a face image data interchange format capable of being extended in a defined way. An extensible specification in ASN.1 (Abstract Syntax Notation One) and the distinguished encoding rules (DER) of ASN.1 form the basis for encoding face image data in binary tag-length-value format. An XSD (XML schema definition) forms the basis for encoding face image data in XML (eXtensible Markup Language).

7.2.2.2 Biometric sample quality standards for face

Quality metrics are useful for understanding and enhancing the performance of biometric recognition systems. While ISO/IEC 29794-1 specifies a structure and gives guidelines for quality score categorization, Parts 1 and 5 of ISO/IEC 29794 define and specify methodologies for objective, quantitative quality score expression, interpretation, and interchange for face.

— ISO/IEC 29794-1:2016 Information technology — Biometric sample quality — Part 1: Framework

— ISO/IEC TR 29794-5:2010 Information technology — Biometric sample quality — Part 5: Face image data

7.2.2.3 Other standards for face biometrics

— ISO/IEC 24779-5:2020 Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems — Part 5: Face applications

7.3 Iris recognition

7.3.1 Overview

Iris recognition technology is now available from a variety of commercial sources and has been used successfully in border crossing, benefit programs and access control environments. Iris recognition has been successfully used in access control applications without the need for any form of identification or claim of identity by the data subject. The data subject can be verified as allowed system access by searching through the entire database of enrolled persons. Technologies vary by vendor, with some systems collecting images from a single eye and some systems collecting images of both eyes simultaneously. Technologies are now available that can collect iris images from distances of over a metre or from persons walking through a portal.

In most implementations, a grayscale image of the iris is acquired in the near-infrared (IR) spectrum to maximize detail in eyes of all colours. To ensure pupil constriction to maximize the area of the iris, acquisition should be done in a well-lit environment. Non-patterned contact lenses and glasses do not interfere significantly with image capture. Sunglasses, however, should not be worn as these can affect the capture process. The computer algorithms unwrap these images to form a rectangular matrix of pixels over which a smaller filter is placed in multiple locations. The filter represents a smooth wave with a frequency and direction. At every filter placement, the phase of the same frequency and direction in iris image is observed

relative to the filter and used to create a pattern of 0s and 1s. These 0s and 1s are the iris "features" and do not directly represent any of the visible patterns on the iris such as crypts, filaments and freckles. Features of two iris patterns are compared by counting the percentage of 0s and 1s that coincide over the length of this binary vector, a function that can be performed by a computer at the bit level with extreme efficiency. If over about ⅔ of the 0s and 1s coincide, the patterns are assumed to be from the same eye. This value of ⅔ represents a threshold that can be varied to aid in balancing the false negatives and false positives.

7.3.2 International standards for iris recognition

7.3.2.1 Biometric data interchange formats standards

Biometric iris recognition systems rely upon standardized biometric data interchange formats for iris images that can be stored, transmitted and processed.

The International Civil Aviation Organization (ICAO) develops standards for travel documents such as passports. These travel documents use internationally standardized biometric data interchange formats for traveller verification by face, fingerprint, or iris.

The present ICAO implementation uses the first generation of iris data interchange format standards developed by ISO/IEC JTC 1/SC 37, Biometrics. These standards remain valid as long as needed for the transition to ISO/IEC 39794-6 in ePassports.

- ISO/IEC 19794-1:2006 Information technology — Biometric data interchange formats — Part 1: Framework
- ISO/IEC 19794-6:2005 Information technology — Biometric data interchange formats — Part 6: Iris image data
- ISO/IEC 29109-6:2011 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 6: Iris image data

Implementations wishing to conform to the present ICAO requirements for ISO/IEC biometric data interchange format standards for iris should use the above standards.

The second generation of biometric data interchange format standards for iris developed by ISO/IEC JTC 1/SC 37 are also available for use in more recent implementations.

- ISO/IEC 19794-1:2011 Information technology — Biometric data interchange formats — Part 1: Framework
- ISO/IEC 19794-6:2011 Information technology — Biometric data interchange formats — Part 6: Iris image data (+ AMD 1: 2015, AMD 2:2016)

Implementations wishing to conform to the second generation of ISO/IEC biometric data interchange format standards for iris should use the above standards.

- ISO/IEC 39794-6:2021 Information technology — Extensible biometric data interchange formats — Part 6: Iris image data

ISO/IEC 39794-6 provides an iris image data interchange format capable of being extended in a defined way. An extensible specification in ASN.1 and the DER of ASN.1 form the basis for encoding iris image data in binary tag-length-value format. An XSD forms the basis for encoding iris image data in XML.

7.3.2.2 Biometric sample quality standards for iris

Quality metrics are useful for understanding and enhancing the performance of biometric recognition systems. While ISO/IEC 29784-1 specifies a structure and gives guidelines for quality score categorization, Parts 1 and 6 of ISO/IEC 29794 define and specify methodologies for objective, quantitative quality score expression, interpretation, and interchange for iris.

- ISO/IEC 29794-1:2016 Information technology — Biometric sample quality — Part 1: Framework

— ISO/IEC 29794-6:2015 Information technology — Biometric sample quality — Part 6: Iris image data

7.4 Dynamic signature technologies

7.4.1 Overview

Dynamic signature verification (DSV) is based on the hand movements made during the signing of our names. 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. The technology was developed in the 1960s and is one of the oldest forms of automated personal recognition.

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 distinctive signature characteristics.

A number of characteristics can be extracted and measured by DSV. For example, 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 distinctive characteristics. DSV is not based solely on the static image, so even if a signature is traced, a forger would need to know the dynamics of that signature.

A further 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.

7.4.2 International standards for signature recognition

— ISO/IEC 19794-7:2014 Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data (+AMD 1:2015)

— ISO/IEC 29109-7:2011 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 7: Signature/sign time series data

— ISO/IEC 19794-11:2013 Information technology — Biometric data interchange formats — Part 11: Signature/sign processed dynamic data (+AMD 1:2014)

7.5 Vascular patterns

7.5.1 Overview

The blood vessels (veins) that exist in the subcutaneous areas of the human body form a distinctive pattern for each person. Furthermore, as blood vessels are within a human body, their vascular pattern cannot be easily obtained by other persons through use of normal photography. The underlying vascular pattern can be captured using infra-red illumination either directed onto the region to be photographed or transmitted through the body part being imaged. The blood vessels absorb infra-red light more than the surrounding tissue and appear darker in the acquired image. The vascular pattern can then be extracted and encoded for reference or comparison by the biometric system.

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.

7.5.2 International standards for vascular biometrics

— ISO/IEC 19794-9:2011 Information technology — Biometric data interchange formats — Part 9: Vascular image data (+ AMD 2:2014)

— ISO/IEC 29109-9:2011 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 9: Vascular image data

- ISO/IEC 24779-9:2015 Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems — Part 9: Vascular applications

7.6 Hand geometry technologies

7.6.1 Overview

Hand geometry techniques have been widely used in access control applications since the 1980s. The most common commercial approach takes one or more two-dimensional silhouette images of the hand and processes those images using a proprietary algorithm to develop a 9-byte code.

A subject places a hand on a reflective platen, aligning fingers with specially positioned guides. The platen is illuminated with infrared light and returns a reflection only where the hand is not covering the platen, thus producing a silhouette image of the hand. A mirror reflects light horizontally across the top of the hand, supplying a second two-dimensional silhouette of the side of the hand.

7.6.2 International standards for hand geometry technologies

- ISO/IEC 19794-10:2007 Information technology — Biometric data interchange formats — Part 10: Hand geometry silhouette data
- ISO/IEC 29109-10:2010 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 10: Hand geometry silhouette data

7.7 Speaker recognition technologies

7.7.1 Overview

Speaker recognition is a biometric technology based on 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 mainly 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).

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 unguided (text-independent) phrase. The process is usually repeated a number of times during enrolment to build a sufficient model of the voice generally based on biometric features such as “cepstral coefficients” which capture the resonance characteristics of the vocal tract.

7.7.2 International standards for speaker recognition

- ISO/IEC 19794-13:2018 Information technology — Biometric data interchange formats — Part 13: Voice data

7.8 DNA

7.8.1 Overview

There are many types of semi-automated DNA analysis, some taking as little as fifteen minutes to implement. Given a sufficient number of loci, DNA analysis can not only identify individuals, it can identify heredity relationships. Because DNA requires some form of tissue, blood or other physical biological sample, it is likely to remain exclusively a forensic technique, as opposed to a significant contender in the access control market.

7.8.2 International standard for DNA biometrics

— ISO/IEC 19794-14:2013 Information technology — Biometric data interchange formats — Part 14: DNA data (+ AMD 1:2016)

7.9 Gait and full body recognition

7.9.1 Overview

Gait is defined as the style or manner of walking. Gait recognition systems record video of a person walking and analyse distinctive features of the shape and dynamics of the silhouette, and/or relative positions and dynamics of joints and limbs.

7.9.2 International standards

— ISO/IEC 39794-16:2021 Information technology — Extensible biometric data interchange formats — Part 16: Full body image data

— ISO/IEC 39794-17:2021 Information technology — Extensible biometric data interchange formats — Part 17: Gait image sequence data

7.10 Retina recognition

The retina is the light-sensitive layer of nerves and blood vessels on the inner surface of the eye. During the 1980s and 1990s, retinal recognition systems that mapped the vein patterns on the retina were commercially available. Such systems did not develop images of the vein patterns, but rather scanned an IR light beam in a circular pattern over the retina and recorded the intensity of the returned light. This resulted in a one-dimensional pattern with high values of reflected light over portions of the circle for which no blood vessel was encountered and low values of reflected light where blood vessels absorbed the IR beam. Despite rumours to the contrary, no health information was known to exist in these patterns and no laser light was ever used. Because of the requirement to shine the imperceptible IR light onto the back surface of the eye, data subjects were required to look into the scanner at a very close proximity, in near contact with the device. Today, retinal recognition devices are no longer commercially available.

7.11 Keystroke dynamics

Keystroke dynamics analyse typing rhythm. An individual's keystroke dynamics evolve over time as they learn to type and develop their own distinctive typing habits. The algorithms may need to cope with subjects becoming distracted or tired during the course of the day.

7.12 Scent/Odour

Recognition of persons through personal odour has long been suggested based on the proven ability of dogs in this area. Although no devices have ever been commercially marketed, they have been under development. A "sniffing" device will draw the odour onto an electronic sensor with receptor proteins that react to specific odour molecules. The variations in the proportions of the various molecules may be distinctive enough to enable recognition.

7.13 Cardiogram

Physical differences between heart muscles and circulatory systems give rise to distinctiveness in the fine details in cardiac rhythm as displayed in electrical signals or by blood flow. There have been many research projects in this area, some resulting in commercial products.

7.14 Multimodal biometrics

7.14.1 Overview

Multimodal biometrics is the combination of different modalities. This combination can be used to increase accuracy and/or improve flexibility. The modalities are typically used in the same context, with the application deciding how to best combine the results to make the best decision given the context of the solution.

7.14.2 International standards

- ISO/IEC TR 24722:2015 Information technology — Biometrics — Multimodal and other multibiometric fusion
- ISO/IEC 29159-1:2010 Information technology — Biometric calibration, augmentation and fusion data — Part 1: Fusion information format

8 Example applications

Editor's notes: Standards relevant to specific applications include:
ISO/IEC 24713-1:2008 Information technology — Biometric profiles for interoperability and data interchange — Part 1: Overview of biometric systems and biometric profiles
ISO/IEC 24713-2:2008 Information technology — Biometric profiles for interoperability and data interchange — Part 2: Physical access control for employees at airports
ISO/IEC 24713-3:2009 Information technology — Biometric profiles for interoperability and data interchange — Part 3: Biometrics-based verification and identification of seafarers
ISO/IEC TR 29195:2015 Traveller processes for biometric recognition in automated border control systems
ISO/IEC TR 29196:2018 Information technology — Guidance for biometric enrolment
ISO/IEC TR 24714-1:2008 Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance
ISO/IEC TR 29194:2015 Information Technology — Biometrics — Guide on designing accessible and inclusive biometric systems
ISO/IEC TR 30110:2015 Information technology — Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and children
ISO/IEC TR 30125:2016 Information technology — Biometrics used with mobile devices
ISO/IEC 30137-1:2019 Information technology — Use of biometrics in video surveillance systems — Part 1: System design and specification

Applications of biometric technologies are extremely diverse and occur in a broad range of government, commercial and personal applications and therefore are difficult to distinctly categorize. This clause is organized by function of the application (e.g. "time and attendance", automated payments) as opposed to the implementing sector (e.g. banking, healthcare), while recognizing that a single biometric application may be used in multiple sectors.

8.1 Physical access control

Some of the earliest applications of automated human recognition were for opening doors. These applications continue at health clubs, theme parks and workplaces for allowing members and employees to pass through portals with minimal staff supervision. In the 1990s and early 2000s, hand geometry was the primary biometric modality used for low to moderate security applications, but recently fingerprint recognition has become dominant. In the 1980s and 1990s, some high security applications for both government and business

were built around retinal recognition, but since then, iris recognition and multi-finger fingerprinting has come to dominate.

Disney World in Orlando, Florida, US, began using finger geometry (a form of hand geometry) in the mid-1990s as a multi-factor access control solution for season pass holders. By the mid-2000s, the system transitioned to fingerprinting and was applied to all holders of any access pass to Disney World to prevent transference of passes.

8.2 Logical access control

Use of biometrics to control access to computer records was strongly advocated in the 1970s. By the late 1980s, many commercial fingerprint, retinal, and voice systems were being marketed. By the late 1990s, fingerprint readers were being built into computer keyboards and cell phones, but uptake was slow. “Match on Card” technology was available by the late 2000s. This technology stored the reference (generally, a fingerprint) and did all computer calculations required for recognition on a smart card controlled by the data subject. This solution was thought to be a privacy protective technology. Although the data subject was required to submit a biometric sample to a host computer, that sample was not stored, but was passed immediately to the smart card for comparison with the stored reference.

The rapid uptake of smart phones in the 2010s allowed extension of the “match on card” concept to the cell phone, but now with all aspects, e.g. biometric data collection, storage and matching, under complete control of the biometric data subject. Apps for voice, face, sclera-vein and fingerprints became readily available for unlocking the phone and other apps on the phone, with no transfer of biometric data out of the direct possession of the data subject.

8.3 Time and attendance

Biometric systems for recording the entry and exit of employees from work sites date at least to the early 1990s, with current use extending to small business, industry and government. A variety of devices are available based on fingerprint, hand geometry and iris recognition. In addition to tracking time for payroll purposes, the systems can give supervisors immediate access to data about which employees are at the job site at any time, information useful in the event of an emergency.

8.4 Accountability

Biometric recognition can be used in applications requiring accountability and non-repudiation. Some hospitals and pharmacies use biometrics as a requirement for access to narcotics. The collection of a biometric characteristic assures that the dispensing of each dosage can be attributed to a registered person in a way that cannot be later repudiated.

8.5 Electronic authorizations

A number of banks have released smart phone apps using biometric characteristics to authorize purchases and transfers of funds. Bank customers can be given a choice of biometrics, such as fingerprint, face or voice, or may choose to not use biometrics at all.

8.6 Government/citizen services

eGovernment services in a number of countries recognize citizens and residents using biometrics. The largest such application is the Unique Identification Authority India (UIDAI). Indian residents apply for an “Aadhaar” number at any of thousands of enrolment sites, supplying two iris images, ten fingerprints and a face image. The iris and fingerprint images are used for “de-duplication”, meaning a search of the entire database to avoid issuance of multiple Aadhaar numbers to a single individual. The issued number may be used with one of the biometric characteristics (generally fingerprint) for multifactor recognition for the dispensing of government benefits and services. The original purpose of the system was to promote economic participation, including the creation of bank accounts, for persons who otherwise have no identity documents or government identity records.

The use of biometrics in voting has presented multiple challenges. The Mexican government has used facial images, along with biographic information, to de-duplicate voter registrations on a precinct by precinct basis. Use of biometrics at a national level on election day to connect voters with registrations has proven problematic because of the throughput and bandwidth requirements and the need for exception handling mechanisms for those not recognized.

The Australian Department of Human Services uses speaker recognition to verify the identity of phone callers to the Centrelink benefits offices. Speaker reference models are indexed by telephone number, so that an incoming call from a recognized phone number needs only be compared to a very few speaker models to verify the identity of the caller. This system operates in both text-dependent and text-independent modes.

8.7 Border protection

8.7.1 ePassports and machine-readable travel documents

In the 1990s, the International Civil Aviation Organization (ICAO), which is responsible for specifying international passport standards, began an initiative for the creation of "Machine Readable Travel Documents" (MRTDs) and in 2003 established face images, supplemented as necessary with fingerprint and iris images, as the preferred biometric characteristic for use on MRTDs. Since the around 2006, nearly all developed nations have been issuing ePassports which contain a computer chip compliant with ICAO MRTD specifications. The face image is stored on the computer chip as a JPEG file. Some countries have augmented this data with the inclusion of fingerprint minutiae templates. This has enabled use of ePassports with biometric Automated Border Crossing (ABC) systems, allowing passengers to transit through systems on which they have not been previously enrolled.

8.7.2 Automated border crossing (ABC) systems

By the mid-2010s, at least 15 countries have implemented ABC systems for some international travellers, replacing primary line inspection with a biometric gate. The ABC system verifies the connection of the traveller to the travel document (generally a passport) by capturing the biometric characteristic presented by the traveller and comparing it with that encoded in the MRTD (either the face image or on some passports, fingerprints) or with an enrolment reference previously created specifically for this ABC system and linked to the identity document. In the case of a traveller not being recognized against the reference image, the traveller is referred for processing by a border control officer.

Typically, ABC systems include other border control processing as required by a border control authority, such as a check on the currency and authenticity of the travel document, and the name or document-number against a watchlist. ABC systems are not intended to replace all manual/human border control policies and procedures, and are generally supported by human oversight.

8.7.3 Visas

Most countries require travellers from at least some other countries to acquire visas from local consulates prior to entry. Some visa issuance processes collect face and fingerprint images for comparison to those of persons previously denied visas and for comparison to the traveller upon arrival to prevent transference of the visa.

8.7.4 EURODAC

EURODAC is a European Union (EU) fingerprint database of asylum seekers which has been operational since 2003. The fingerprints of all EU asylum seekers over 14 years of age are compared to fingerprints of previous EU asylum seekers, then stored in the EURODAC central system for 10 years. The purpose of this system is to detect persons applying multiple times for asylum within the EU within this 10 year period.

8.8 Law enforcement

The law enforcement community uses many of the world's largest biometric systems. The two main biometric functions in law enforcement agencies involve identification of arrestees (usually through sets of fingerprints

but also in some applications through facial images), 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 NGI system, which currently contains fingerprint sets from over 70 million individuals. Police forces throughout the world use AFIS or ABIS technology to identify the source of fingerprints from crime scenes and to identify arrestees. Law enforcement databases will also frequently hold the fingerprints of persons not associated with any criminal activity, such as those in law enforcement, the military, or government positions of trust.

8.9 Civil background checks

Many types of government and private employment require background checks on the criminal history of applicants. These checks are usually implemented by searching applicant fingerprints against the fingerprints held in the criminal portion of law enforcement databases.

8.10 Clustering

Biometrics has traditionally been associated with "identification" and "verification", but other applications follow from the definition of biometrics as "automated methods of recognizing individuals". Biometric systems can be used to "cluster" biometric samples (for example, face images), grouping samples likely to have come from the same person without requirement for "enrolment" or knowledge of the person being recognized.

Social media has begun to cluster and mark faces of single individuals. Those individuals can then be linked to clusters of other individuals appearing in the same images, allowing mappings of social networks.

In the same way, an audio recording containing the voices of multiple individuals can be segmented and clustered into the speech segments associated with each individual, even if the individuals are otherwise unknown.

9 General biometric system

9.1 Conceptual representation of 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. Captured biometric samples are acquired from a subject by a biometric capture device and are sent to a processor that extracts the distinctive but repeatable measures of each sample (the biometric features), discarding all other components. The resulting features may be stored in the biometric enrolment database as a biometric reference. In other cases, the sample itself (without feature extraction) may be stored as the reference. A subsequent query or probe biometric 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 biometric claim is made based upon the similarities or dissimilarities between the features of the biometric probe and those of the reference or references compared.

Figure 1 illustrates the information flow within a general biometric system consisting of data capture, signal processing, data storage, comparison and decision subsystems. This diagram illustrates both enrolment and the operation of verification and identification systems.

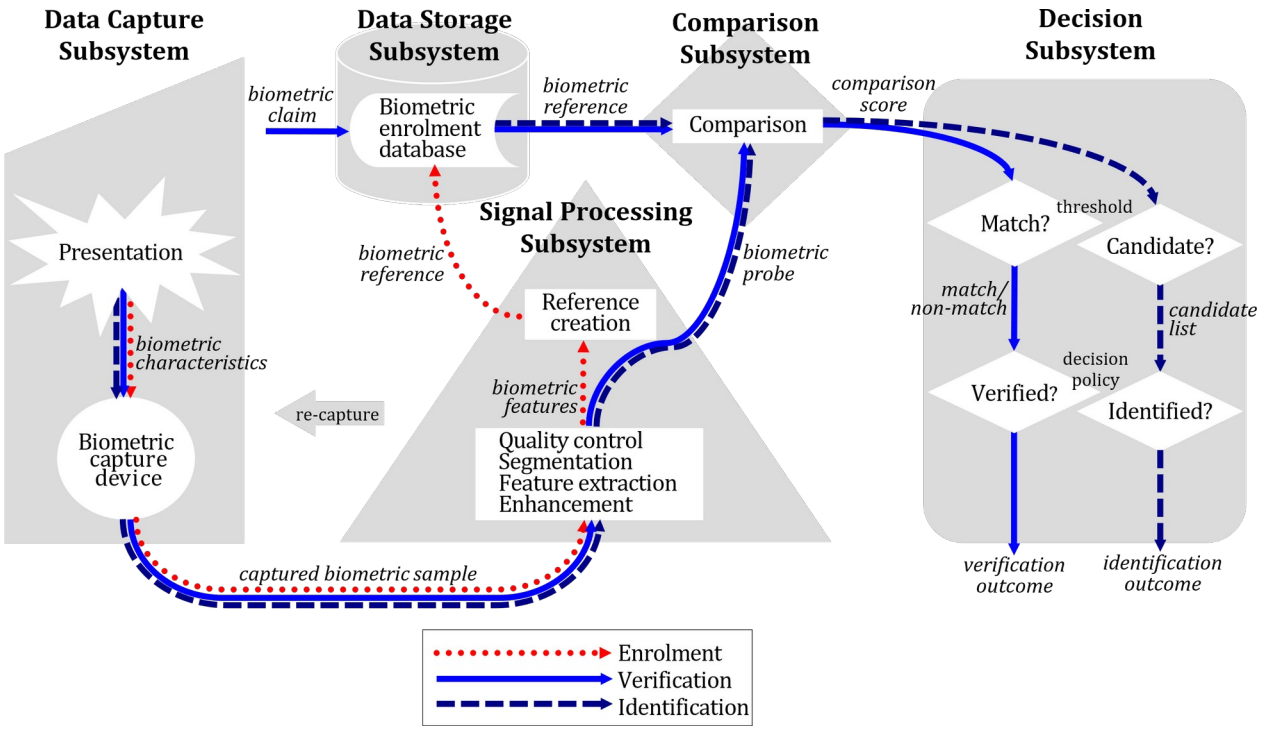

Figure 1 — Components of a general biometric system

The following subclauses describe each of these subsystems in more detail. However, it should be noted that in any implemented system, some of these conceptual components may be absent, or may not have a direct correspondence with a physical or software entity.

9.2 Conceptual components of a general biometric system

9.2.1 Data capture subsystem

The data capture subsystem collects an image or signal of a subject's biometric characteristics presented to the biometric capture device, and outputs this image or signal as a captured biometric sample.

9.2.2 Transmission subsystem

The transmission subsystem (not always present or visibly present in a biometric system) transmits samples, features, probes, references, comparison scores and outcomes between different subsystems. The captured biometric sample may be compressed and/or encrypted before transmission and expanded and/or decrypted before use. A captured biometric sample may be altered in transmission due to noise in the transmission channel as well as losses in the compression/expansion process. Data may be transmitted using standard biometric data interchange formats, and cryptographic techniques may be used to protect the authenticity, integrity, and confidentiality of stored and transmitted biometric data.

NOTE The transmission subsystem is not portrayed in Figure 1.

9.2.3 Signal processing subsystem

Signal processing includes processes such as:

— enhancement, i.e. improving the quality and clarity of the captured biometric sample;

— segmentation, i.e. locating the signal of the subject's biometric characteristics within the captured biometric sample;

- feature extraction, i.e. deriving the subject's repeatable and distinctive measures from the captured biometric sample; and
- quality control, i.e. assessing the suitability of samples, features, references, etc. and possibly affecting other processes, such as returning control to the data capture subsystem to collect further samples (recapture), or modifying parameters for segmentation, feature extraction, or comparison. Quality can also be used in biometric fusion where the comparison scores are combined with a consideration of the associated quality values of the samples used for each comparison.

In the case of enrolment, the signal processing subsystem creates a biometric reference. Sometimes the enrolment process requires features from several presentations of the individual's biometric characteristics. Sometimes the reference comprises just the features, in which case the reference may be called a "template". Sometimes the reference comprises just the sample, in which case feature extraction from the reference occurs immediately before comparison.

In the case of verification and identification, the signal processing subsystem creates a biometric probe.

Sequencing and iteration of the above-mentioned processes are determined by the specifics of each system.

9.2.4 Data storage subsystem

References are stored within an enrolment database held in the data storage subsystem. Each reference may be associated with some details of the enrolled subject or the enrolment process. It should be noted that prior to being stored in the enrolment database, references may be reformatted into a biometric data interchange format. 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, in a central database, or in the 'cloud'.

9.2.5 Comparison subsystem

In the comparison subsystem, probes are compared against one or more references and comparison scores are passed to the decision subsystem. The comparison scores indicate the similarities or dissimilarities between the probe(s) and reference(s) compared. For verification, a single specific biometric claim of would lead to a single comparison score. For identification, many or all references may be compared with the probes and output a comparison score for each comparison.

9.2.6 Decision subsystem

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

In the case of verification, the probes are considered to match a compared reference when (assuming that higher scores correspond to greater similarity) the comparison score exceeds a specified threshold. A biometric claim 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 (assuming that higher scores correspond to greater similarity) the comparison score exceeds a specified threshold, and/or when the comparison score is among the predetermined number of ranked 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 to treat multibiometric systems in the same manner as unibiometric systems, by treating the combined captured biometric samples, references or scores as if they were a single sample, reference or score and allowing the decision subsystem to operate score fusion or decision fusion as and if appropriate. (See also ISO/IEC TR 24722 Multimodal and other multibiometric fusion[Error: Reference source not found].)

9.2.7 Administration subsystem

The administration subsystem governs the overall policy, implementation, configuration and operation of the biometric system. Illustrative examples include:

a) interacting with the subject including providing guidance feedback to the subject during and/or after data capture, and requesting additional information from the subject;

b) storing and formatting of the biometric references and/or biometric interchange data;

c) providing final arbitration on output from decision and/or scores;

d) setting threshold values;

e) setting biometric system acquisition settings;

f) controlling the operational environment and non-biometric data storage;

g) providing appropriate safeguards for subject privacy and subject data security;

h) interacting with the application that utilizes the biometric system.

NOTE The administration subsystem is not portrayed in Figure 1.

9.2.8 Interface to external application

The biometric system may or may not interface to an external application or system via a Web Services Interface, an Application Programming Interface (API), a Hardware Interface or a Protocol Interface.

NOTE Interfaces to external application are not portrayed in Figure 1.

9.3 Functions of general biometric system

9.3.1 Enrolment

In enrolment, a transaction by a capture subject is processed by the system in order to generate and store an enrolment reference for that individual.

Enrolment typically involves:

a) sample capture;

b) sample optimization or enhancement;

c) segmentation;

d) feature extraction;

e) quality checks (which may reject the sample/features as being unsuitable for creating a reference, and require capture of further samples). Sample quality scores may also be stored with the biometric reference for subsequent use in biometric comparison;

f) presentation attack detection checks (which may reject the sample/features as being ineligible for use as an enrolment reference);

g) (where system policy so requires) comparison against existing biometric references to ensure the subject is not already enrolled;

h) reference creation (which may require features from multiple samples) and possibly generation of a database index;

i) storage of the biometric reference data record, possibly after conversion to a biometric reference data interchange format;

j) test verification or identification attempts by the capture subject to ensure that the resulting biometric reference is usable;

k) allowing repeat enrolment attempts, should the initial enrolment be deemed unsatisfactory (dependent on the enrolment policy).

9.3.2 Verification of a positive biometric claim

In applications such as access control, a transaction by a subject may be 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"). Note that some biometric systems allow a single subject to enrol more than one instance of a biometric characteristic (for example, an iris system may allow subjects to enrol both iris images, while a fingerprint system may require enrolment of additional fingers for fallback in case a primary finger is damaged).

Verification of a specific positive claim typically involves:

a) sample capture;

b) sample optimization or enhancement;

c) segmentation;

d) feature extraction;

e) quality checks (which may reject the sample/features as being unsuitable for comparison, and require capture of further samples); the sample quality may also be considered at biometric comparison;

f) presentation attack detection checks (which may reject the sample/features as being ineligible for use)

g) probe creation (which may require features from multiple samples), possible conversion into a biometric data interchange format;

h) comparison of the probe and the reference for a biometric claim producing a comparison score;

i) determination of whether the biometric features of the probe match those of the reference based on whether the comparison score exceeds a threshold (in cases where higher scores correspond to greater similarity);

j) decision to verify a claim based on the comparison result of one or more attempts as dictated by the decision policy.

The verification function either accepts or rejects the specific positive 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). In this application, a false acceptance occurs if the submitted sample is wrongly matched to a stored reference not created by the data subject. A false rejection occurs if the submitted sample is not matched to a reference actually created by the data subject.

NOTE Verification of an unspecific positive claim is also quite possible with a biometric system. Such applications have been called "PIN-less verification" because no Personal Identification Number (PIN) or other identifier was necessary to establish that the data subject was indeed enrolled in the database. The process is as above through steps a) – g). However, steps h) – j) are somewhat different when the claim is unspecific:

h) comparison of the probe against all the references producing a score for each comparison;

i) determination of whether the biometric features of the probe match those of any reference based on whether the comparison score exceeds a threshold (in cases where higher scores correspond to greater similarity);

j) decision to verify a claim based on the comparison results of one or more attempts as dictated by the decision policy.

9.3.3 Identification

In identification, biometric samples from a capture subject are processed to generate a probe, and the enrolment database is searched to return identifiers of references similar to that probe. Identification provides a candidate list of identifiers containing zero, one, or more identifiers. Identification is considered correct when the subject is enrolled and an identifier for their enrolment is in the candidate list. The identification is considered to be erroneous if either an enrolled subject's identifier 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).

Identification typically involves:

a) sample capture;

b) sample optimization or enhancement;

c) segmentation;

d) feature extraction;

e) quality checks (which may reject the sample/features as being unsuitable for comparison, and require capture of further samples); the sample quality may also be considered at biometric comparison;

f) presentation attack detection checks (which may reject the sample/features as being ineligible for use);

g) probe creation (which may require features from multiple samples) and possible conversion into a biometric data interchange format);

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

i) determination of whether each compared reference is a potential candidate identifier for the capture subject, based on whether the comparison score exceeds a threshold and/or is among the highest ranked scores returned, producing a candidate list (higher scores correspond to greater similarity);

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

10 Performance testing

10.1 General

Biometric devices and systems might be tested in many different ways. Types of testing include:

a) functional capability;

b) technical performance (in terms of error rates and throughput rates);

c) reliability, availability and maintainability;

d) vulnerability;

e) security;

f) user acceptance;

g) human factors;

h) cost/benefit;

i) legislative compliance including that relating to privacy and transparency of the biometric data recorded for an individual.

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 have been developed (ISO/IEC 19795[34]).

Technical tests can be either “closed-set” or “open-set”. In closed-set testing all test subjects are enrolled in the system. Closed-set tests cannot measure performance of the system when used by people who are not enrolled. 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 database, and measures all comparison scores against a score threshold. An open-set test returns, as a function of the threshold, the probabilities of (i) declaring a non-match for a mated comparison of probe and reference from the same subject (the false non-match rate) and (ii) declaring a match for a non-mated comparison of probe and reference from different individuals (the false match rate).

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. The failure-to-enrol rate is determined as the proportion of enrolment transactions in which the enrolment could not be completed because of system or human failure. The failure-to-acquire rate is determined as the proportion of acquisition processes by all enrolled subject that are not acknowledged by the system. The false rejection rate is the proportion of all verification transactions with true biometric claims erroneously rejected by the system. The false acceptance rate is the proportion of verification transactions with untrue biometric claims erroneously accepted by the system. Because false acceptance rate and false rejection rate (or false match rate / and false non-match rate) are competing measures, they can be displayed together on a "Detection Error Trade-off" (DET) 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.

10.2 Types of technical tests

Three types of technical tests are described: Technology, Scenario, and Operational (Philips, Martin, Wilson and Przybocki, 2000[58]).

- *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, 1996-2012[54]);
  - facial recognition (NIST FERET, 1993-1997[55] and NIST FRVT 2000-2013[5][59][60][21][22]);
  - fingerprinting (Fingerprint Verification Competition 2000-2006,[47][48][11][12] NIST FpVTE 2003-2012[79] [75]; NIST, 2004-2006[74]; NIST MINEX, 2004-2006[20]);
  - iris (International Biometric Group, 2005[26]; NIST ICE 2004-2006[60]).
- *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[65]; Bouchier, Ahrens and Wells, 1996[7]; Mansfield, Kelly, Chandler and Kane, 2000[49]).
- *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 uncontrolled differences of operational environments. Further, "ground truth" (i.e. who was actually presenting a "good faith" biometric characteristic) 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[76]).

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. Comparison error rates, failure-to-enrol/acquire

rates 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.

Results of technical performance tests can vary depending on:

- the type of test (technology, scenario, or operational);
- the composition of the corpus of test data and controls on data quality (see ISO/IEC 29794-1[39]);
- application environment (which can affect the relative difference between mated probe and reference, making these harder to match (see ISO/IEC TR 29198[40]);
- decision policy of the application (e.g. how many retries are permitted).

These issues can make comparison of test results and prediction of real-world performance difficult.

10.3 International standards for biometric performance testing

- ISO/IEC 19795-1:2006 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework
- ISO/IEC 19795-2:2007 Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation (+ AMD 1: 2015)
- ISO/IEC TR 19795-3:2007 Information technology — Biometric performance testing and reporting — Part 3: Modality-specific testing
- ISO/IEC 19795-4:2008 Information technology — Biometric performance testing and reporting — Part 4: Interoperability performance testing
- ISO/IEC 19795-5:2011 Information technology — Biometric performance testing and reporting — Part 5: Access control scenario and grading scheme
- ISO/IEC 19795-6:2012 Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation
- ISO/IEC 19795-7:2011 Information technology — Biometric performance testing and reporting — Part 7: Testing of on-card biometric comparison algorithms
- ISO/IEC TS 19795-9:2019 Information technology — Biometric performance testing and reporting — Part 9: Testing on mobile devices
- ISO/IEC TR 29189:2015 Information technology — Biometrics — Evaluation of examiner assisted biometric applications
- ISO/IEC 29120-1:2015 Information technology — Machine readable test data for biometric testing and reporting — Part 1: Test reports
- ISO/IEC 29197:2015 Information technology — Evaluation methodology for environmental influence in biometric system performance
- ISO/IEC 30136:2018 Information technology — Performance testing of biometric template protection schemes
- ISO/IEC TR 29198:2013 Information technology — Biometrics — Characterization and measurement of difficulty for fingerprint databases for technology evaluation

11 Biometric technical interfaces

11.1 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 block of data with a defined format that contains one or more biometric samples or biometric templates such as a fingerprint 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[32]) for various biometric technologies, each specifying one or more BDB formats (e.g. compact smart card formats as well as normal formats). Each BDB format has a BDB format identifier that enables the 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, e.g. when it was captured, its expiry date, the equipment capturing it, whether it is encrypted. A number of different BIR formats are defined by ISO/IEC 19785-3[31] 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 Common Biometric Exchange Formats Framework “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 Biometrics Identity Assurance Services (BIAS) and the BioAPI Interfaces (within a system) or the Biometric Interworking Protocol (BIP) (between systems).

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

11.2 Service architectures

Service-oriented architecture (SOA) is a software design pattern based on discrete pieces of software called services. Services are independent software programs designed to fulfil a specific function and comprise a set of capabilities to realize that function. The service is typically expressed in service contracts, which are technical service descriptions designed for runtime consumption (for example: a Web Services Description Language (WSDL) definition and an XML schema definition). Services are akin to Application Programming Interfaces (APIs). The SOA design pattern provides for services to be aggregated through service compositions the effect of which is to provide automated support to any business process that requires the functionality of the service composition.

Biometric software services are designed to provide a generic set of biometric and identity-related functions and associated data definitions to facilitate the collection, storage, use and disclosure of biographic and biometric data in a variety of business contexts and domains. These services typically do not contain logic specific and unique to a particular business operation as such logic is more appropriately contained within the application logic layer. Rather, the services contain the logic required to enable biometric services to be applied agnostic to the operating environment.

There are currently two standards of interest which specify biometric services:

a) WS Biometric Devices (WS-BD), described in NIST Special Publication 500-288[53], which defines a number of primitive and aggregate services for the integration of biometric sensor devices into biometric systems that have a biometric acquisition component;

b) Biometric Identity Assurance Services, described in ISO/IEC 30108[42], which defines a number of primitive and aggregate biometric identity assurance services. In essence, these services provide for the storage and retrieval of biographic and biometric data collected from an individual where the biometric data is collected via a biometric sensor of some sort.

11.3 Common Biometric Exchange Formats Framework (CBEFF)

— ISO/IEC 19785-1:2015 Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification

- ISO/IEC 19785-2:2006 Information technology — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority
  +Amendment 1:2010 Additional registrations
- ISO/IEC 19785-3:2015 Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications
- ISO/IEC 19785-4:2010 Information technology — Common Biometric Exchange Formats Framework — Part 4: Security block format specifications

The International Standard for CBEFF (ISO/IEC 19785[30]) promotes interoperability of biometric-based applications and systems by specifying standard structures for 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 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 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 needs to be an integral number of octets; the parts in the ISO/IEC 19794[32] series 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 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 document (possibly with additional abstract values determined by the CBEFF patron), together with one or more BDBs containing biometric data.

The ISO/IEC 19785 series consists of four parts. ISO/IEC 19785-1 specifies a full set of (metadata) data elements and their abstract values (without determining any particular encoding). ISO/IEC 19785-2, which defined procedures for the operation of the Biometric Registration Authority, was withdrawn in order to avoid conflicts with the contract established between ISO/IEC and the Biometric Registration Authority. ISO/IEC 19785-3 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. ISO/IEC 19785-4 defines the security block (SB) to provide for both integrity and encryption of the biometric data.

11.4 The BioAPI International Standard

- ISO/IEC 19784-1:2018 Information technology — Biometric application programming interface — Part 1: BioAPI specification
- ISO/IEC 19784-2:2007 Information technology — Biometric application programming interface — Part 2: Biometric archive function provider interface
- ISO/IEC 19784-4:2011 Information technology — Biometric application programming interface — Part 4: Biometric sensor function provider interface
- ISO/IEC 24709-1:2017 Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 1: Methods and procedures
- ISO/IEC 24709-2:2007 Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 2: Test assertions for biometric service providers
- ISO/IEC 24709-3:2011 Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 3: Test assertions for BioAPI frameworks
- ISO/IEC 29164:2011 Information technology — Biometrics — Embedded BioAPI

— ISO/IEC 30106-1:2016 Information technology — Object oriented BioAPI — Part 1: Architecture + Amendment 1:2016 Additional specifications and conformance statements

— ISO/IEC 30106-2:2016 Information technology — Object oriented BioAPI — Part 2: Java implementation

— ISO/IEC 30106-3:2016 Information technology — Object oriented BioAPI — Part 3: C# implementation

— ISO/IEC 30106-4:2019 Information technology — Object oriented BioAPI — Part 4: C++ implementation

BioAPI (ISO/IEC 19784[29]) provides an implementation architecture that supports biometric applications using software (and hardware) modules from multiple vendors.

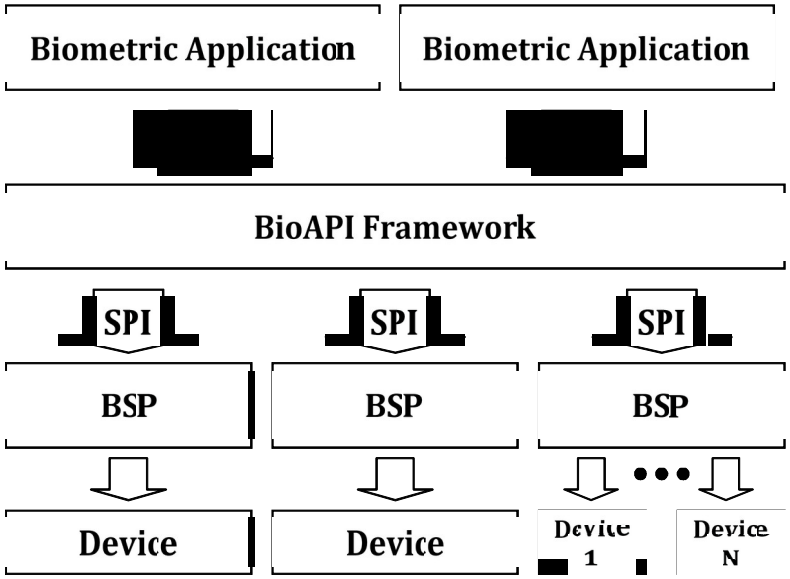

Figure 2 — BioAPI architecture

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.

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).

11.5 The BIP International Standard

— ISO/IEC 24708:2008 Information technology — Biometrics — BioAPI Interworking Protocol

The BIP International Standard (ISO/IEC 24708[35]) 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 forms part of the transmission subsystem described in 8.2.2 (see Figure 3 below).

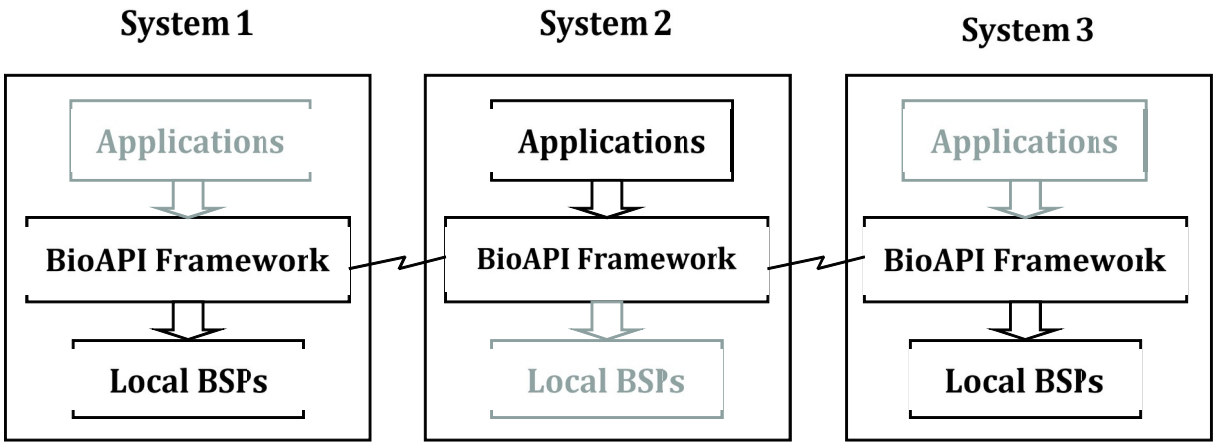

Figure 3 — Use of the BIP for communication between systems

12 Biometrics and information security

12.1 General

It should be 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 a 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 biometric claim, 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 10.5). The former approach has positive implications for privacy (Kent and Millett, 2003[43]), but if biometric references are stored centrally, several different questions arise.

a) Will the acquired biometric 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.

b) If the biometric sample is sent from the point of service to the central site, will it be in raw form or as biometric features? If the latter, computational power and knowledge of the feature extraction algorithm will be required at each point of service but transmission bandwidth will be reduced.

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

d) How will the person 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.

12.2 Security of biometric data

The requirements for the use of biometrics to verify the claim of an individual for authorizations are well documented.

Firstly, a person's biometric data should be confidential and not be subject to unauthorized access, use and modification or disclosed to unauthorized entities. Ideally, the encryption of the biometric data should occur immediately upon creation of the biometric file as this is an important consideration for both the transmission and storage of biometric data.

Secondly, the integrity of the biometric data across the various processing subsystems in the biometric system is also critical. For example, if the integrity of the data is compromised resulting in an untrustworthy biometric reference, subsequent verification and identification processing results are also untrustworthy.

Thirdly, if an individual's biometric reference is the subject of an identity theft and therefore compromised, the persistence of the biometric characteristics from which the reference is derived means that it is very difficult to revoke the stolen reference and enrol a new one. Therefore, methods for mitigating the risk of compromised biometric references including provisions for revocable/renewable biometric references are considered.

Confidentiality, integrity and renewability and revocability of biometric data are achieved through the application of cryptographic techniques (ISO/IEC 24745:2011[38] pages 13-14).

Various forms of cryptographic encryption algorithms (ciphers) can be used for providing confidentiality of stored data. The encryption algorithms are applied to the biometric data to produce encrypted data and are designed such that the encrypted data yields no information about the biometric data. There is a corresponding decryption algorithm, which transforms the encrypted data into its original form. Ciphers work in association with keys. Where the key is the same for both encryption and decryption the cipher is symmetric. Where they are different for encryption and decryption the cipher is asymmetric. The public key infrastructure for encrypting biographic and biometric face image data on e-Passports uses asymmetric ciphers.

To safeguard the integrity of transmitted biometric data, Message Authentication Code (MAC) algorithms are used to verify that biometric data has not been subject to unauthorized alteration. These algorithms provide integrity and authenticity assurances on a transmitted message by detecting message changes and also affirming the origin of the message. As a MAC does not provide non-repudiation, where this is required digital signature schemes are employed.

There are also methods available for processing data to provide both confidentiality and integrity protection. They typically involve either specific combination of encryption and a MAC computation or the use of an encryption algorithm in a special way. ISO/IEC 19772[28] specifies six methods for authenticated encryption with the following security objectives:

- *Data confidentiality:* protection against unauthorized disclosure of data;
- *Data integrity:* protection that enables the recipient of data to verify that it has not been modified;
- *Data origin authentication:* protection that enables the recipient of data to verify the identity of the data originator.

All six methods require the originator and the recipient of the protected data to share a secret key.

Renewable and revocable biometric references are achieved through the concept of pseudo identities (PIs). PIs are anonymous and renewable biometric identity verification strings in a predefined context (Breebart et al, 2009[8] page 302). A PI is derived from a data subject's biometric characteristics. Features extracted from a data subject's captured biometric sample are processed by a pseudonymous identified encoder, which generates a pseudonymous identifier and auxiliary data (AD) providing a Renewable Biometric Reference (RBR). Once this reference is generated it can be stored and the captured biometric sample and extracted features discarded. For subsequent verification processes, features are extracted from a captured biometric sample and a pseudo identity re-coder is applied generating a probe PI based on the extracted features and the AD component of the RBR. The reference PI and probe PI are then compared. All things being equal, they will only match if the correct biometric characteristics are presented and the correct AD is used.

In addition to enabling the reference probe comparison, the AD component of the RBR can be used to serve a number of purposes including:

- generation of multiple independent PIs from the same captured biometric sample to provide a sufficient number of diversifications for the biometric characteristics of an individual and therefore a renewable biometric reference capability within the same application context;
- generation of independent PIs from the same captured biometric sample with minimal common information between the PIs to prevent biometric comparisons and linking across applications where they are used.

Depending on the security requirements for the biometric system, RBRs may or may not be employed. Where RBRs are not used, the generalized model for the biometric system at Figure 1 applies. Where RBRs are used, the generalized model is varied as shown in Figure 4 below (adapted from ISO/IEC 24745[38] page 18):

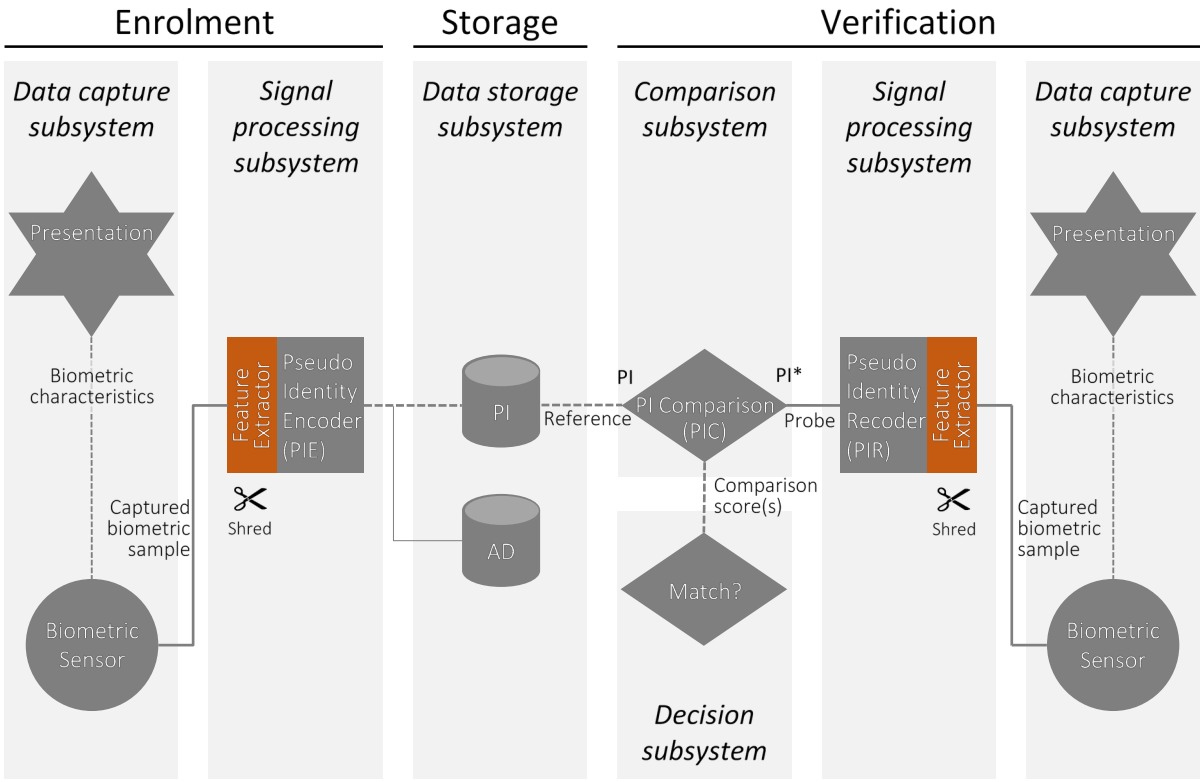

Figure 4 — Generalized model of biometric system using renewable biometric references

The generalized model and RBR models may be implemented in various ways based on where the biometric reference is stored and where the comparison of the reference with the probe is made and, in the case where RBRs are implemented, where the PI and AD components are stored. In this context, possible topologies include (ISO/IEC 24745:2011[38] pages 25-38):

- Model A: Store on server and compare on server;
- Model B: Store on token and compare on server;
- Model C: Store on server and compare on client;
- Model D: Store on client and compare on client;
- Model E: Store on token and compare on client;
- Model F: Store on token and compare on token;
- Model G: Store distributed on token and server, compare on server;
- Model H: Store distributed on token and client, compare on client;

Each model has its own security and privacy advantages and disadvantages.

12.3 Presentation attacks (Spoofing)

Notwithstanding the methods for biometric data protection, it has been well known since the 1970s that biometric devices can be fooled by forgeries (Lummis and Rosenberg, 1972[46]; Raphael and Young, 1974[63]; Meissner, 1977[51]). “Spoofing” is a term that has been commonly used in literature for presenting a forgery of another person’s biometric characteristics, in order to be recognized as that person. ISO/IEC 30107-1[41] which focuses on biometric-based attacks on the biometric data capture subsystem, uses the term “presentation attack”, which points to what can be done with a biometric presentation to subvert the intended operation of a biometric system.

Two basic types of presentation attack are identified:

- where a person intends to be recognized as an individual other than him/herself;
- where a person intends not to be recognized as any individual known to the system and so conceal their biometric characteristics

In both cases, the person is termed a subversive user.

To be recognized as another person by a biometric system, a subversive user may perform a biometric sensor attack by coercing another person to present their biometric characteristics or through impersonation. In a coercive attack, the biometric data subject’s biometric characteristics are presented to the sensor without their permission. This may be through force or some other means. In an impersonation attack, a person changes their biological or physical characteristics, for example their appearance, in an effort to match that of an enrolled data subject. A person may also conceal or disguise their biometric characteristics to avoid recognition. For example, in a facial recognition system, concealment may be by the wearing of caps and sunglasses to conceal the face. A person may also distort their biometric characteristics, for example by placing glue on fingers or wearing artificial or patterned contact lenses. 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[72]; Matsumoto, Matsumoto, Yamada and Hoshino, 2002[50]; Thalheim, Krissler and Ziegler, 2002[68]; BSI, 2003[9] and BSI, 2005[10]) 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.

- ISO/IEC 30107-1:2016 Information technology — Biometric presentation attack detection — Part 1: Framework
- ISO/IEC 30107-2:2017 Information technology — Biometric presentation attack detection — Part 2: Data formats
- ISO/IEC 30107-3:2017 Information technology — Biometric presentation attack detection — Part 3: Testing and reporting
- ISO/IEC 30107-4:2020 Information technology — Biometric presentation attack detection — Part 4: Profile for testing of mobile devices

12.4 Integrity of the enrolment process

The use of biometrics does not reduce the need to appropriately confirm applicants' identity information or 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 passport,

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 and affordances 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. Enrolment template update mechanisms might also be employed to periodically update enrolment references from biometric samples acquired in transactions subsequent to enrolment. The aim of template updating is to automatically adapt a biometric reference over time. This takes into account the variation of the biometric data presented on each occasion, including from ageing, to minimize the impact of such variations on recognition performance.

13 Biometrics and privacy

Editor's Note: Standard:
ISO/IEC TR 24714-1:2008 Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance
ISO/IEC 24745:2011 Information technology — Security techniques — Biometric information protection

13.1 General

Recognition by close observation of the body causes discomfort in some people who may react by stating that "biometrics invades my privacy". Privacy is a legally and culturally determined concept which is extremely important and can directly affect the success of any biometric deployment.

Legal definitions of "privacy" vary from country to country and, in the United States, even from state to state (Alderman and Kennedy, 1995[2]). A classic definition is the intrinsic "right to be let alone" (Warren and Brandeis, 1890[73]), 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[78]) 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 their identity stolen, or to be reliably and quickly identified after an accident or incident.

The increasing pervasiveness of web and mobile technologies sees more individuals transacting electronically for social and economic reasons on the basis of personal information that they are required to provide, including biometric information. How this information is safeguarded and what controls are in place for the access, use, disclosure and discarding of that information is a fundamental concern for many.

Various national and international legal and normative instruments relating to the privacy of personal data are based on a set of principles including that individuals be informed (Robinson et al, 2009[64] page 1):

- when and for what purpose (scope) personal data is collected;
- who is requesting the data and the reason for their request to help them decide whether to provide and release control of all or part of such data;
- of the parties that the data they provide might be disclosed to and under what circumstances;
- how they can access data about themselves in order to verify its accuracy and request changes;
- how their data will be protected from unauthorized access, modification, use and disclosure;

- how long the data provided will be stored in all of the places is stored, including the parties to whom the data has been disclosed to, before it is required to be permanently deleted.

NOTE In some jurisdictions, biometric information is considered to be sensitive personal information, placing more stringent obligations on entities using biometrics. For example, in the European Union, Directive 2016/680 on the processing of personal data, and in Australia, the 2014 update to the Privacy Act 1988, both specifically identify biometric information as sensitive personal information.

The objectives of these various instruments 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 to be safeguarded and a tool to enhance the safeguarding.

The key privacy protections that are generally considered for the applications of biometrics are:

- the proportionality of the application of the biometric data collected;
- the acceptability in the candidate population of the biometrics employed given cultural, religious and therefore privacy sensitivities;
- the confidentiality of the biometric data provided by the individual;
- the integrity of the biometric data provided by the individual;
- the irreversibility of the biometric data generated from the biometric samples provided by the individual;
- the unlinkability of the biometric data in contexts outside of permissions agreed to when the biometric samples were provided by the individual;
- the renewability of the biometric reference created from the biometric samples provided by the individual should they be compromised.

In general terms the implementations of these protections are guided by a number of general principles, which are considered privacy enhancing including (ISO/IEC 24714-1:2008[36] page 5):

- limit the storing and use of personal data;
- use encryption if using personal data;
- destroy raw data as soon as possible;
- anonymize personal data wherever possible;
- do not use central databases where they are not required;
- give subjects control over their personal data;
- use a means of evaluation and certification to verify that an application delivers a guarantee of an appropriate level of trust.

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.

13.2 Proportional application of biometrics

In all biometric 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. In practice this means that a biometric application is used to link the biometric reference with the necessary and sufficient attributes of the identity of an individual to assign the rights or authorizations that the specific individual is entitled to in the application context. Such assignment occurs upon verification of a biometric claim made by the individual concerned. However, there are applications, especially in the context of border protection, fraud and forensics where individuals must be subject by law to identification processes and they may or may not be cooperative. Further, right or authorizations may be denied if the identification process results in an assessment by an authority that there is an unacceptable risk to the community if the rights or authorizations are afforded. So, the notion of proportionality has to be extended to the basic purpose of the identification process (Kindt and Müller, 2007 [44] page 75).

13.3 Biometric technology acceptability

The acceptability of biometric technology is deeply related to personal preferences, values and norms which are influenced by historical, societal and cultural background. Not surprisingly, there are differing preferences values and norms across geographic areas and populations resulting in differences between the acceptability of different biometric technologies.

Some biometric technologies require physical contact (for example, with a fingerprint 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 preferences, values and norms are to be accommodated.

It can be argued (Locke, 1690[45]; Baker, 2000[3]) that a physical body is not identical to the person that inhabits it. Whereas PINs and passwords identify persons, biometrics identifies the body. Biometric characteristics 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 widespread.

13.4 Confidentiality of biometric data

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. Therefore, it is an essential privacy requirement that the biometric data stored as part of an individual’s identity data record or otherwise transmitted be kept confidential.

Confidentiality of the biometric data is typically achieved by (ISO/IEC 24745:2011[38] page 23):

- storing biometric references (or parts thereof) on a personal token or card instead of using centralized databases to prevent privacy threats resulting from a security breach of the centralized database (for example when an adversary obtains illegitimate access to a centralized database and publishes its contents);
- encryption of biometric references using a key only known to the operator of the application and/or data subject.

13.5 Integrity of biometric data

Given rights and authorization may be afforded or denied an individual in decision making processes following the assessment of biometric comparison results, it is critical for the operator of the biometric

system, decision makers and the individual concerned that the integrity of the biometric data is maintained at all times. Decisions based on untrustworthy biometric data have the potential to deny individual rights and authorizations and lead to unnecessary intrusions into their personal and private lives.

As discussed in 12.2, employing MAC algorithms or digital signature algorithms can achieve integrity of the biometric data.

13.6 Irreversibility of biometric data

It is possible that an observer of the biometric information, particularly raw biometric information as might be contained in a captured biometric sample, may interpret it to mean that an individual has certain medical conditions or the individual is of a particular race or religion. This is generally considered personal and highly sensitive information.

When creating biometric templates from captured biometric samples for reference or comparison purposes, feature extraction algorithms perform data reduction and redundancy removal thereby increasing the difficulty of using the extracted features to obtain medical or ethnic data. These data minimization approaches seek to mitigate the risk of information leakage from the biometric data. However, at least until 2007 no systematic research has been carried out with respect to remaining additional information in templates and the extent to which information such as health conditions could still be derived (Kindt and Müller, 2007[44] page 83). It is known that the knowledge of a trained PCA eigenspace coupled with the PCA eigenvalues for an individual allows reconstruction of the individual's face (Adler 2003[1]). Fingerprint minutia information can also be reverse engineered from templates and used to create artificial fingerprints (Hill 2001[24] page 116).

In recent times, significant research effort has been directed to methods to make it computationally harder to retrieve biometric features from the stored templates. Current methods to achieve this include[38]:

- Encryption using a key only known by the operator of the system and/or data subject prevents external observers having access to the biometric data;
- Using PIs and irreversible transforms to provide a means to prevent access to the biometric characteristics of the data subject.

13.7 Unlinkability of biometric information

Using biometric data for purposes other than that communicated to an individual at the time of collection presents various risks for that individual. For example, the biometric data may be used to identify links in information held by various organizations that are not within the scope of the purpose for which the data was originally collected. This may result in an individual being disadvantaged in some way. For example, being denied credit on the basis of credit information obtained from financial institution data holdings using the biometric data as the linking mechanism.

To mitigate risks to the individual from unauthorized linking attempts, various mechanisms might be employed either separately or in combination including (ISO/IEC 24745:2011[38] page 23):

- encryption of biometric references employing different (secret) keys or mechanisms across applications;
- independent PIs created from a biometric reference (diversification);
- logical or physical separation of the enrolment data record and the corresponding biometric reference data record, or PI and AD components where RBRs are employed;
- the use of incompatible feature extraction algorithms or biometric data exchange formats across applications.

Bibliography

confN0N0[1] ADLER A. 2003. Sample images can be independently restored from face recognition templates. *Proc. Canadian Conference on Electrical and Computer Engineering 2003*, pp.1163–1166conf

bokN0N0[2] ALDERMAN, E. and KENNEDY, C. 1995. *The Right to Privacy.* New York: Vintage Booksbok

bokN0N0[3] BAKER, L.R. 2000. *Persons and Bodies: A Constitution View.* Cambridge: Cambridge University Pressbok

bokN0N0[4] BERTILLON, A. 1889. *Alphonse Bertillon's Instructions For Taking Descriptions For The Identification Of Criminals And Others, By Means Of Anthropometric Indications*, translated by Gallus Muller. Whitefish: Kessinger Publishingbok

otherN0N0[5] BLACKBURN D., BONE M., GROTHER P., PHILLIPS P.J. 2001. Facial Recognition Vendor Test 2000: Evaluation Reportother

otherN0N0[6] BLEDSOE W.W. 1966. *Man-machine facial Recognition: Report on a large-scale experiment*, Technical Report PRI22, Panoramic Research Inc, Palo Alto, CAother

otherN0N0[7] BOUCHIER F., AHRENS J., WELLS G. 1996. *Laboratory evaluation of the Iriscan prototype biometric identifier.* Technical report SAND96-1033, Sandia National Laboratoriesother

confN0N0[8] BREEBART J., BUSCH C., GRAVE J., KINDT E. 2008. A reference architecture for biometric template protection based on pseudo identities. In: *BIOSIG 2008. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*. Editor: Brömme, A. Bonn: Gesellschaft für Informatik, 2008, pp.25-37conf

erefN0N0[9] Bundesamt für Sicherheit in der Informationstechnik. 2004. *An investigation into the performance of facial recognition systems relative to their planned use in photo identification documents — BioP I: Public final report.* Available online at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/BioP/BioPfinalreport_pdf.pdf?__blob=publicationFile (Date of Access 25 Jul 2016)eref

erefN0N0[10] Bundesamt für Sicherheit in der Informationstechnik. 2005. *Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen — BioP II Öffentlicher Abschlussbericht* https://www.bsi.bund.de/DE/Publikationen/Studien/BioPII/BioPII.html (Date of Access 25 Jul 2016)eref

jrnN0N0 _issn="0162-8828"[11] CAPPELLI, R., MAIO, D., MALTONI, D., WAYMAN, J.L. and JAIN, A.K. 2006. Performance evaluation of fingerprint verification systems. *IEEE Trans. on Pattern Analysis and Machine Intelligence.* **28**, pp.3-18jrn

jrnN0N0[12] CAPPELLI, R., FERRARA, M., FRANCO A. and MALTONI, D. 2007. Fingerprint verification competition 2006, *Biometric Technology Today*, **vol.15, no.7-8**, pp.7-9jrn

jrnN0N0 _issn="0731-5996"[13] CHANG, S.H., PIHL, G.E., and ESSIGNMANN, M.W 1951. Representations of Speech Sounds and Some of Their Statistical Properties, *Proc. Institute of Radio Engineers*, 147jrn

jrnN0N0 _issn="0162-8828"[14] DAUGMAN, J. 1993. High confidence visual recognition of persons by a test of statistical independence, *IEEE Trans. on Pattern Analysis and Machine Intelligence* **15**, 1148-1161jrn

jrnN0N0 _issn="0028-0836"[15] FAULDS, H. 1880. On the Skin Furrows of the Hand, *Nature,* **22**, 605jrn

confN0N0[16] FEJFAR A. 1978. Combining techniques to improve security in automated entry control, *Carnahan Conference on Crime Countermeasures*conf

otherN0N0[17] FLOM L., SAFIR A. 1987. Iris recognition system, U.S. Patent 4,641,349other

jrnN0N0 _issn="0028-0836"[18] GALTON, F. 1888. On personal identification and description, *Nature* **38,** 173-177, 201-202jrn

jrnN0N0[19] GOLDSTEIN, A.J., HARMON, L.D., LESK, A.B. 1971. Identification of human faces, *Proc. Institute of Electrical and Electronic Engineers*, **59**, 748-760jrn

unknownN0N0[20] GROTHER, P.J., MCCABE, R., WATSON, C.I., INDOVINA, M.D., SALAMON, W.J., Flanagan, P.A., Tabassi, E., Newton, E.M., WILSON C.L. 2006. *MINEX Performance and Interoperability of the INCITS 378 Fingerprint Template.* National Institute of Standards and Technology, Tech. Report, NISTIR 7296unknown

unknownN0N0[21] GROTHER, P., QUINN, G.W., PHILLIPS, P.J. 2010. *Evaluation of 2-D still-image face recognition algorithms*. National Institute of Standards and Technology, Tech. Report, NISTIR 7709unknown

unknownN0N0[22] GROTHER, P. and NGAN, M. 2014. *Face recognition vendor test (FRVT): Performance of face identification algorithms.* National Institute of Standards and Technology, Tech. Report, NISTIR 8009unknown

JRNN0N0 _ISSN="0028-0836"[23] HERSCHEL, W.J. 1880. Skin Furrows of the Hand, *Nature,* **23**, 76jrn

jrnN0N0[24] HILL, C.J. 2001. *Risk of masquerade arising from the storage of biometrics*. Australian National University, 2001, p.116jrn

otherN0N0[25] IBM. 1970. *The Considerations of Data Security in a Computer Environment*, Technical Report G520-2169, White Plains, NYother

bokN0N0[26] International Biometric Group 2005. *Independent testing of iris recognition technology (ITIRT)*bok

stdN0N0[27] ISO/IEC 2382-37:2012, *Information technology — Vocabulary — Part 37: Biometrics*std

stdN0N0[28] ISO/IEC 19772:2009, *Information technology — Security techniques — Authenticated encryption*std

stdN0N0[29] ISO/IEC 19784-1:2006, *Information technology — Biometric application programming interface — Part 1: BioAPI specification*std

stdN0N0[30] ISO/IEC 19785-1:2006, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*std

stdN0N0[31] ISO/IEC 19785-3:2007, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*std

stdN0N0[32] ISO/IEC 19794-1:2011, *Information technology — Biometric data interchange formats — Part 1: Framework*std

stdN0N0[33] ISO/IEC 19794-3:2006, *Information technology — Biometric data interchange formats — Part 3: Finger pattern spectral data*std

stdN0N0[34] ISO/IEC 19795-1:2006, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*std

stdN0N0[35] ISO/IEC 24708:2008, *Information technology — Biometrics — BioAPI Interworking Protocol*std

stdN0N0[36] ISO/IEC 24714-1:2008, *Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance*std

stdN0N0[37] ISO/IEC 24722:2007, *Information technology — Biometrics — Multimodal and other multibiometric fusion*std

stdN0N0[38] ISO/IEC 24745:2011, *Information technology — Security techniques — Biometric information protection*std

stdN0N0[39] ISO/IEC 29794-1:2016, *Information technology — Biometric sample quality — Part 1: Framework*std

stdN0N0[40] ISO/IEC/TR 29198:2013, *Information technology — Biometrics — Characterization and measurement of difficulty for fingerprint databases for technology evaluation*std

stdN0N0[41] ISO/IEC 30107:2016, *Information technology — Biometric presentation attack detection — Part 1: Framework*std

stdN0N0[42] ISO/IEC 30108-1:2016, *Information technology — Biometric Identity Assurance Services — Part 1: BIAS services*std

bokN0N0[43] KENT, S.T. and MILLETT, L.I. 2003. *Who goes there? Authentication through the lens of privacy*, Washington, D.C.: National Academies Pressbok

otherN0N0[44] KINDT E., MÜLLER L., eds. 2007. *Biometrics in identity management*, Report D3.10, Future of Identity in the Information Society (FIDIS)other

bokN0N0[45] LOCKE, J. 1690. *An essay concerning human understanding*, Book 2, Chapter 27,bok

jrnN0N0 _issn="0001-4966"[46] LUMMIS, R.C., and ROSENBERG, A. 1972. Test of an ASV method with intensively trained professional mimics, *Journal of the Acoustical. Society of America* 51, 131jrn

jrnN0N0 _issn="0162-8828"[47] MAIO, D., MALTONI, D., Cappelli, R., Wayman, J.L. and Jain, A.K. 2002. FVC2000: Fingerprint verification competition. *IEEE Trans. on Pattern Analysis and Machine Intelligence.* **24**, pp.402-412jrn

confN0N0[48] MAIO D., MALTONI D., CAPPELLI R., WAYMAN J.L., JAIN A.K. 2002. FVC2002: Second fingerprint verification competition. *Proceedings of the 16th International Conference on Pattern Recognition (ICPR'02)* volume 3, pp.811-814conf

unknownN0N0[49] MANSFIELD, A.J., KELLY, G., CHANDLER, D. and KANE, J. 2000. Biometric product testing final reportunknown

jrnN0N0 _issn="0277-786X"[50] MATSUMOTO, T., MATSUMOTO, H., YAMADA, K., and HOSHINO, S. 2002. Impact of Artificial 'Gummy' Fingers on Fingerprint Systems, *Proceedings SPIE,* 4677jrn

unknownN0N0[51] MEISSNER, P. 1977. Guidelines on evaluation of techniques for automated personal identification, National Bureau of Standards, FIPS PUB 48unknown

confN0N0[52] MESSNER W.K., CLECIWA C.A., KIBBLER G.O.T.H., PARLEE W.L. 1974. Research and Development of Personal Identity Verification Systems, *Proceedings 1974 Carnahan and International Crime Countermeasures Conference*, University of Kentuckyconf

unknownN0N0[53] MICHAELS, R.J., MANGOLD, K., ARONOFF, M., KWONG, K. and MARSHALL, K. 2012. *Specification for WS-Biometric Devices (WS-BD), Version 1,* National Institute of Standards and Technology, Tech. Report, NISTSP 500-288unknown

unknownN0N0[54] National Institute Of Standards And Technology Multimodal Information Group. (1996-2012). *Speaker Recognition Evaluation*.[1] unknown

unknownN0N0[55] National Institute of Standards and Technology. (1993-1997). Facial Recognition Technology (FERET) Database Evaluation.unknown[2]

unknownN0N0[56] National Institute of Standards and Technology (2004-2006). Fingerprint Software Development Kit Testingunknown

bokN0N0[57] OSBORN, S. 1929. *Questioned Documents.* Chicago: Nelson-Hallbok

jrnN0N0 _issn="0018-9162"[58] PHILLIPS, P.J., MARTIN, A., WILSON, C.L. and Przybocki, M. 2000. An introduction to evaluating biometric systems, *Computer,* **33**, 56-63jrn

unknownN0N0[59] PHILLIPS, P., GROTHER, P., MICHEALS, R., BLACKBURN, D., TABASSI, E. AND BONE, J. 2003. *Face recognition vendor test 2002: Evaluation report*, National Institute of Standards and Technology, Tech. Report, NISTIR 6965unknown

unknownN0N0[60] PHILLIPS, P.J., SCRUGGS, W.T., O'TOOLE, A.J., FLYNN, P.J., BOWYER, K.W., SCHOTT, C.L., and SHARPE, M. 2007. *FRVT 2006 and ICE 2006 Large-scale results*. National Institute of Standards and Technology, Tech. Report NISTIR 7408unknown

unknownN0N0[61] POTTER, R.K., KOPP, G.A., and GREEN, H.C. 1947. *Visible Speech*, New York: van Nostran Counknown

jrnN0N0 _issn="0001-4966"[62] PRUZANSKY, S. 1963. Pattern-matching procedure for automatic talker recognition, *Journal of the Acoustical Society of America*, **26**, 403-406jrn

bokN0N0[63] RAPHAEL, D.E. and YOUNG, J.R. 1974. *Automated Personal Identification*, Palo Alto: SRI Internationalbok

unknownN0N0[64] ROBINSON, N., GRAUX, H., BOTTERMAN, M., VALERI, L. 2009. *Review of the European Data Protection Directive*. Rand Europeunknown

otherN0N0[65] RODRIGUEZ J.R., BOUCHIER F., RUEHIE M. 1993. Performance Evaluation of Biometric Identification Devices, Report SAND93-1930, Sandia National Laboratory Albuquerqueother

edbN0N0[66] ROETHENBAUGH, G. (Ed) 1998. *Biometrics Explained.* ICSA Commercial Biometric Developers Consortium[3]edb

jrnN0N0 _issn="0028-7628"[67] SIMON, C. and GOLDSTEIN, I. 1935. A new scientific method of identification. *New York State Journal of Medicine*, **35**, 901-906jrn

1 https://nist.gov/itl/iad/mig/sre.cfm

2 https://www.nist.gov/itl/iad/ig/feret.cfm

3 Parts of this tutorial are based, with permission, on text in this publication.

unknownN0N0[68] THALHEIM, L., KRISSLER, J. and ZIEGLER, P. 2002. Biometric Access Protection Devices and their Programs Put to the Test, *C'T Magazine* 11unknown

jrnN0N0 _issn="0028-0836"[69] TRAURING, M. 1963a. On the automatic comparison of finger ridge patterns, *Nature*, **197**, 938-940jrn

bokN0N0[70] TRAURING, M. 1963b. *Automatic comparison of finger ridge patterns*, Hughes Research Laboratory Report, 190, Malibubok

bokN0N0[71] Twain, M. 1893. *Pudd'nhead Wilson*, The Century, serialized 47(2) – 48(2), New York: The Century Companybok

confN0N0[72] VAN DER PUTTE T., KEUNING J. 2000. Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned, *IFIP TC8/WG.8., Fourth Working Group Conference on Smart Card Research and Advanced Applications*, 289-303conf

jrnN0N0 _issn="0017-811X"[73] WARREN, S. AND BRANDEIS, L. 1890. The Right to Privacy, *Harvard Law Review*, **4**, 193-220jrn

unknownN0N0[74] WATSON, C.I. AND WILSON, C.L 2005. *Effect of Image Size and Compression on One-to-One Fingerprint Matching*. National Institute of Standards and Technology, Tech Report, NISTIR 7201unknown

unknownN0N0[75] WATSON. C., FIUMARA, G., TABASSI, E., CHENG, S.L., FLANAGAN, P., SALAMON, W. 2014. *Fingerprint vendor technology evaluation 2012: Evaluation of fingerprint matching algorithms*, National Institute of Standards and Technology, Tech Report, NISTIR 8034unknown

edbN0N0[76] WAYMAN, J.L. 2000. Evaluation of the INSPASS Hand Geometry Data. In J.L. Wayman (Ed.), U.S. *National Biometric Test Center Collected Works: 1997-2000*, San Jose: San Jose State Universityedb

bokN0N0[77] WEGSTEIN, J. 1970. *Automated Fingerprint Identification*, Technical Note 538, National Bureau of Standardsbok

bokN0N0[78] WESTIN, A. 1967. *Privacy and Freedom*, Boston: Atheneumbok

unknownN0N0[79] WILSON, C.L., GROTHER, P.J., MICHAELS, R.J., OTTO, S.C., WATSON, C.I., HICKLIN, R.A., KORVES, H., ULERY, B., ZOEPFL, M. 2004. *Fingerprint vendor technology evaluation 2003: Summary of results and analysis report*. National Institute of Standards and Technology, Tech. Report NISTIR 7123unknown

EDITOR'S NOTE Listed here are the current SC37 standards, and additionally standards from SC17 and SC27 pertaining to biometrics

Relevant standards from ISO/IEC JTC 1/SC 17, Cards and security devices for personal identification

ISO/IEC 7816-11:2017 Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods

ISO/IEC 11694-6:2014 Identification cards — Optical memory cards — Linear recording method — Part 6: Use of biometrics on an optical memory card

ISO/IEC 17839-1:2014 Information technology — Biometric System-on-Card — Part 1: Core requirements

ISO/IEC 17839-3:2016 Information technology — Identification cards — Biometric System-on-Card — Part 3: Logical information interchange mechanism

ISO/IEC 18584:2015 Information technology — Identification cards — Conformance test requirements for on-card biometric comparison applications

ISO/IEC 24787:2018 Information technology — Identification cards — On-card biometric comparison

ISO/IEC TR 30117:2014 Information technology — Guide to on-card biometric comparison standards and applications

Relevant standards from ISO/IEC JTC 1/SC 27, Information security, cybersecurity and privacy protection

ISO/IEC 17922:2017 Information technology — Security techniques — Telebiometric authentication framework using biometric hardware security module

ISO/IEC 19792:2009 Information technology — Security techniques — Security evaluation of biometrics

ISO/IEC 24745:2011Information technology — Security techniques — Biometric information protection

ISO/IEC 24761:2019 Information technology — Security techniques — Authentication context for biometrics

Standards from ISO/IEC JTC 1/SC 37

ISO/IEC 2382-37:2017 Information technology — Vocabulary — Part 37: Biometrics

ISO/IEC 19784-1:2018 Information technology — Biometric application programming interface — Part 1: BioAPI specification

ISO/IEC 19784-2:2007 Information technology — Biometric application programming interface — Part 2: Biometric archive function provider interface

ISO/IEC 19784-4:2011 Information technology — Biometric application programming interface — Part 4: Biometric sensor function provider interface

ISO/IEC 19785-1:2015 Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification

ISO/IEC 19785-2:2006 Information technology — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority
+Amendment 1:2010 Additional registrations

ISO/IEC 19785-3:2015 Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications

ISO/IEC 19785-4:2010 Information technology — Common Biometric Exchange Formats Framework — Part 4: Security block format specifications

ISO/IEC 19794-1:2011 Information technology — Biometric data interchange formats — Part 1: Framework
+ Amendment 1:2013 Conformance testing methodology
+Amendment 2:2015 Framework for XML encoding

ISO/IEC 19794-2:2011 Information technology — Biometric data interchange formats — Part 2: Finger minutiae data (+COR1:2012)
+Amendment 1:2013 Conformance testing methodology
+Amendment 2:2015 Framework for XML encoding

ISO/IEC 19794-3:2006 Information technology — Biometric data interchange formats — Part 3: Finger pattern spectral data

ISO/IEC 19794-4:2011 Information technology — Biometric data interchange formats — Part 4: Finger image data
+ Amendment 1:2013 Conformance testing methodology
+ Amendment 2:2015 XML encoding

ISO/IEC 19794-5:2011 Information technology — Biometric data interchange formats — Part 5: Face image data
+Amendment 1:2014 Conformance testing methodology
+Amendment 2: 2915 XML encoding

ISO/IEC 19794-6:2011Information technology — Biometric data interchange formats — Part 6: Iris image data
+ Amendment 1:2015 Conformance testing methodology
+ Amendment 2:2016 XML encoding

ISO/IEC 19794-7:2014 Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data
+ Amendment 1:2015 XML encoding

ISO/IEC 19794-8:2011 Information technology — Biometric data interchange formats — Part 8: Finger pattern skeletal data
+ Amendment 1:2014 Conformance testing methodology

ISO/IEC 19794-9:2011 Information technology — Biometric data interchange formats — Part 9: Vascular image data
+ Amendment 1:2013 Conformance testing methodology
+ Amendment 2:2014 XML Encoding

ISO/IEC 19794-10:2007 Information technology — Biometric data interchange formats — Part 10: Hand geometry silhouette data

ISO/IEC 19794-11:2013 Information technology — Biometric data interchange formats — Part 11: Signature/sign processed dynamic data
Amendment 1:2014 Conformance test assertions

ISO/IEC 19794-13:2018 Information technology — Biometric data interchange formats — Part 13: Voice data

ISO/IEC 19794-14:2013 Information technology — Biometric data interchange formats — Part 14: DNA data
+ Amendment 1:2016 Conformance testing

ISO/IEC 19794-15:2017 Information technology — Biometric data interchange format — Part 15: Palm crease image data

ISO/IEC 19795-1:2006 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework

ISO/IEC 19795-2:2007 Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation
+ Amendment 1:2015 Testing of multimodal biometric implementations

ISO/IEC TR 19795-3:2007 Information technology — Biometric performance testing and reporting — Part 3: Modality-specific testing

ISO/IEC 19795-4:2008 Information technology — Biometric performance testing and reporting — Part 4: Interoperability performance testing

ISO/IEC 19795-5:2011 Information technology — Biometric performance testing and reporting — Part 5: Access control scenario and grading scheme

ISO/IEC 19795-6:2012 Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation

ISO/IEC 19795-7:2011 Information technology — Biometric performance testing and reporting — Part 7: Testing of on-card biometric comparison algorithms

ISO/IEC TS 19795-9:2019 Information technology — Biometric performance testing and reporting — Part 9: Testing on mobile devices

ISO/IEC 20027:2018 Information technology — Guidelines for slap tenprint fingerprint capture

ISO/IEC 24708:2008 Information technology — Biometrics — BioAPI Interworking Protocol

ISO/IEC 24709-1:2017 Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 1: Methods and procedures

ISO/IEC 24709-2:2007 Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 2: Test assertions for biometric service providers

ISO/IEC 24709-3:2011 Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 3: Test assertions for BioAPI frameworks

ISO/IEC 24713-1:2008 Information technology — Biometric profiles for interoperability and data interchange — Part 1: Overview of biometric systems and biometric profiles

ISO/IEC 24713-2:2008 Information technology — Biometric profiles for interoperability and data interchange — Part 2: Physical access control for employees at airports

ISO/IEC 24713-3:2009 Information technology — Biometric profiles for interoperability and data interchange — Part 3: Biometrics-based verification and identification of seafarers

ISO/IEC TR 24714-1:2008 Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance

ISO/IEC TR 24722:2015 Information technology — Biometrics — Multimodal and other multibiometric fusion

ISO/IEC TR 24741:2018 Information technology — Biometrics — Overview and application (Previous version of this document !)

ISO/IEC 24779-1:2016 Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems — Part 1: General principles

ISO/IEC 24779-4:2017 Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems — Part 4: Fingerprint applications

ISO/IEC 24779-5:2020 Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems — Part 5: Face applications

ISO/IEC 24779-9:2015 Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems — Part 9: Vascular applications

ISO/IEC 29109-1:2009 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 1: Generalized conformance testing methodology

ISO/IEC 29109-2:2010 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 2: Finger minutiae data

ISO/IEC 29109-4:2010 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 4: Finger image data

ISO/IEC 29109-5:2019 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 5: Face image data

ISO/IEC 29109-6:2011 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 6: Iris image data

ISO/IEC 29109-7:2011 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 7: Signature/sign time series data

ISO/IEC 29109-8:2011 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 8: Finger pattern skeletal data

ISO/IEC 29109-9:2011 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 9: Vascular image data

ISO/IEC 29109-10:2010 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 10: Hand geometry silhouette data

ISO/IEC 29120-1:2015 Information technology — Machine readable test data for biometric testing and reporting — Part 1: Test reports

ISO/IEC 29141:2009 Information technology — Biometrics — Tenprint capture using biometric application programming interface (BioAPI)

ISO/IEC TR 29144:2014 Information technology — Biometrics — The use of biometric technology in commercial Identity Management applications and processes

ISO/IEC TR 29156:2015 Information technology — Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics

ISO/IEC 29159-1:2010 Information technology — Biometric calibration, augmentation and fusion data — Part 1: Fusion information format

ISO/IEC 29164:2011 Information technology — Biometrics — Embedded BioAPI

ISO/IEC TR 29189:2015 Information technology — Biometrics — Evaluation of examiner assisted biometric applications

ISO/IEC TR 29194:2015 Information Technology — Biometrics — Guide on designing accessible and inclusive biometric systems

ISO/IEC TR 29195:2015 Traveller processes for biometric recognition in automated border control systems

ISO/IEC TR 29196:2018 Information technology — Guidance for biometric enrolment

ISO/IEC 29197:2015 Information technology — Evaluation methodology for environmental influence in biometric system performance

ISO/IEC TR 29198:2013 Information technology — Biometrics — Characterization and measurement of difficulty for fingerprint databases for technology evaluation

ISO/IEC 29794-1:2016 Information technology — Biometric sample quality — Part 1: Framework

ISO/IEC 29794-4:2017 Information technology — Biometric sample quality — Part 4: Finger image data

ISO/IEC TR 29794-5:2010 Information technology — Biometric sample quality — Part 5: Face image data

ISO/IEC 29794-6:2015 Information technology — Biometric sample quality — Part 6: Iris image data

ISO/IEC 30106-1:2016 Information technology — Object oriented BioAPI — Part 1: Architecture + Amendment 1:2016 Additional specifications and conformance statements

ISO/IEC 30106-2:2016 Information technology — Object oriented BioAPI — Part 2: Java implementation

ISO/IEC 30106-3:2016 Information technology — Object oriented BioAPI — Part 3: C# implementation

ISO/IEC 30106-4:2019 Information technology — Object oriented BioAPI — Part 4: C++ implementation

ISO/IEC 30107-1:2016 Information technology — Biometric presentation attack detection — Part 1: Framework

ISO/IEC 30107-2:2017 Information technology — Biometric presentation attack detection — Part 2: Data formats

ISO/IEC 30107-3:2017 Information technology — Biometric presentation attack detection — Part 3: Testing and reporting

ISO/IEC 30107-4:2020 Information technology — Biometric presentation attack detection — Part 4: Profile for testing of mobile devices

ISO/IEC 30108-1:2015 Information technology — Biometric Identity Assurance Services — Part 1: BIAS services

ISO/IEC TR 30110:2015 Information technology — Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and children

ISO/IEC TR 30125:2016 Information technology — Biometrics used with mobile devices

ISO/IEC 30136:2018 Information technology — Performance testing of biometric template protection schemes

ISO/IEC 30137-1:2019 Information technology — Use of biometrics in video surveillance systems — Part 1: System design and specification

ISO/IEC 39794-1:2019 Information technology — Extensible biometric data interchange formats — Part 1: Framework

ISO/IEC 39794-4:2019 Information technology — Extensible biometric data interchange formats — Part 4: Finger image data

ISO/IEC 39794-5:2019 Information technology — Extensible biometric data interchange formats — Part 5: Face image data