TECHNICAL REPORT

ISO/IEC TR 29196

Second edition
2018-05

Information technology — Guidance for biometric enrolment

Technologies de l'information — Directives pour l'inscription biométrique

Reference number
ISO/IEC TR 29196:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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 second edition cancels and replaces the first edition (ISO/IEC TR 29196:2015), which has been technically revised.

Introduction

One of the most important contributions to a successful biometric-based recognition system is a consistent enrolment service that generates the biometric data required for subsequent recognition of individuals. Subsequent verifications or identifications will be compared with the biometric data collected at enrolment. If the quality of capture at enrolment is not maintained consistently, the operators of a recognition system which depends on a good enrolment are likely to experience unreliable performance. For those who are enrolled in a verification system, a poor quality enrolment will result in inconvenience should they fail to be recognized. (Readers of this document should note that quality has a specific meaning when applied to biometric systems; a high quality capture is one that results in biometric data that provides good comparison scores when compared with other high quality images from the same biometric feature.)

By analysing the requirements for a good enrolment from the perspectives of a range of stakeholders, it is possible to derive a set of principles to guide the development of a biometric enrolment policy and the deployment of a service. Where enrolment is outsourced to a third party, it is extremely important to be able to measure quality metrics rather than quantity metrics, since the technical and business objectives of the two organisations (the relying party and the Enrolment Authority as defined in this document) may, in general, not be aligned.

Although the recommendations and guidelines in this document are directed primarily to the parties responsible for the enrolment itself and for management of the enrolment service (noting that these two entities may be one and the same), they will also be of value to the designers and developers of enrolment systems.

Information technology — Guidance for biometric enrolment

1 Scope

This document consolidates information relating to successful, secure and usable implementation of biometric enrolment processes, while indicating risk factors that organisations proposing to use biometric technologies will should address during procurement, design, deployment and operation. Much of the information is generic to many types of application, e.g. from national scale commercial and government applications, to closed systems for in-house operations, and to consumer applications. However, the intended application and its purpose often have influence on the necessary enrolment data quality and are intended to be taken into account when specifying an enrolment system and process.

The document points out the differences in operation relating to specific types of application, e.g. where self-enrolment is more appropriate than attended operation. This document focuses on mandatory, attended enrolment at fixed locations. In summary, this document consolidates information relating to better practice implementation of biometric enrolment capability in various business contexts including considerations of process, function (system), and technology, as well as legal/privacy and policy aspects.

The document provides guidance on collection and storage of biometric enrolment data and the impact on dependent processes of verification and identification. This document does not include material specific to forensic and law enforcement applications.

This document does not contain any mandatory requirements. The following terms are used in this document to provide guidance.

The terms “should” and “should not” indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.

The term “may” indicates a course of action permissible within the limits of the publication.

The terms “can” and “cannot” indicate a possibility and capability, whether material, physical or causal.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and the following 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 https://www.iso.org/obp

3.1
biometric subject
individual seeking to be enrolled in a biometric enrolment database

3.2
designers and developers
organization or individuals responsible for the design, development, (and deployment, if applicable) of the enrolment system

3.3
duty officer
individual acting on behalf of either the Enrolment Authority or operator either present in the vicinity of one or more enrolment stations, or available on line or by telephone, trained to provide advice and guidance to an enrolment officer in case of difficulty

Note 1 to entry: The duty officer may also have a role in determining exception handling routines.

3.4
Enrolment Authority
organisation (or other entity) with legal and contractual responsibilities for the completion of enrolment processes

3.5
enrolment officer
agent of the operator responsible for the secure and effective enrolment service at one or more enrolment points

3.6
Identity Provider
entity storing and managing the biometric data obtained directly or indirectly from the biometric enrolment

3.7
operator
organization (or other entity) responsible for delivering the enrolment service on behalf of the Enrolment Authority

3.8
performance manager
person responsible for managing the enrolment service to ensure it meets its specified enrolment performance criteria

Note 1 to entry: This will typically include actions such as monitoring enrolment performance (quality as well as quantity metrics), applying corrective measures where necessary and reporting enrolment performance achievement to the Enrolment Authority.

3.9
personal assistant
individual accompanying the biometric subject at the enrolment session for one or more purposes

Note 1 to entry: Such purposes might include: translation of instructions from the enrolment officer into the native language of the subject; support for a disabled subject to enable the subject to undertake an enrolment successfully; to fulfil a legal requirement such as a parent present at the enrolment of a child.

3.10
relying party
entity operating a biometrically-enabled application for which the enrolment process provides biometric references

3.11
specialist support staff
trained attendant(s) present at the enrolment session on behalf of the Enrolment Authority or operator to assist with the enrolment of subjects with disabilities, or to fulfil service or legal requirements in respect of gender, religious observance, or age of the subject

3.12
vendor
entity providing hardware and/or software biometric functionality

4 Abbreviated terms

KPI	Key Performance Indicator. A metric quantifying one or more aspects of the successful operation of a process
NFIQ	NIST Fingerprint Image Quality
SLA	Service Level Agreement. An agreement between a service provider and a customer defining a target level of service, mutual responsibilities of service provider and customer, together with other requirements for the delivery of a service

5 Role of enrolment in a 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 sensor. The sensor output is sent to a processor that extracts the distinctive but repeatable measures of the sample (the biometric features), discarding all other components. The resulting features can be stored in the biometric enrolment database as a biometric reference or (in this case) a biometric template. In other cases the sample itself (without feature extraction) may be stored as the reference. A subsequent 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.

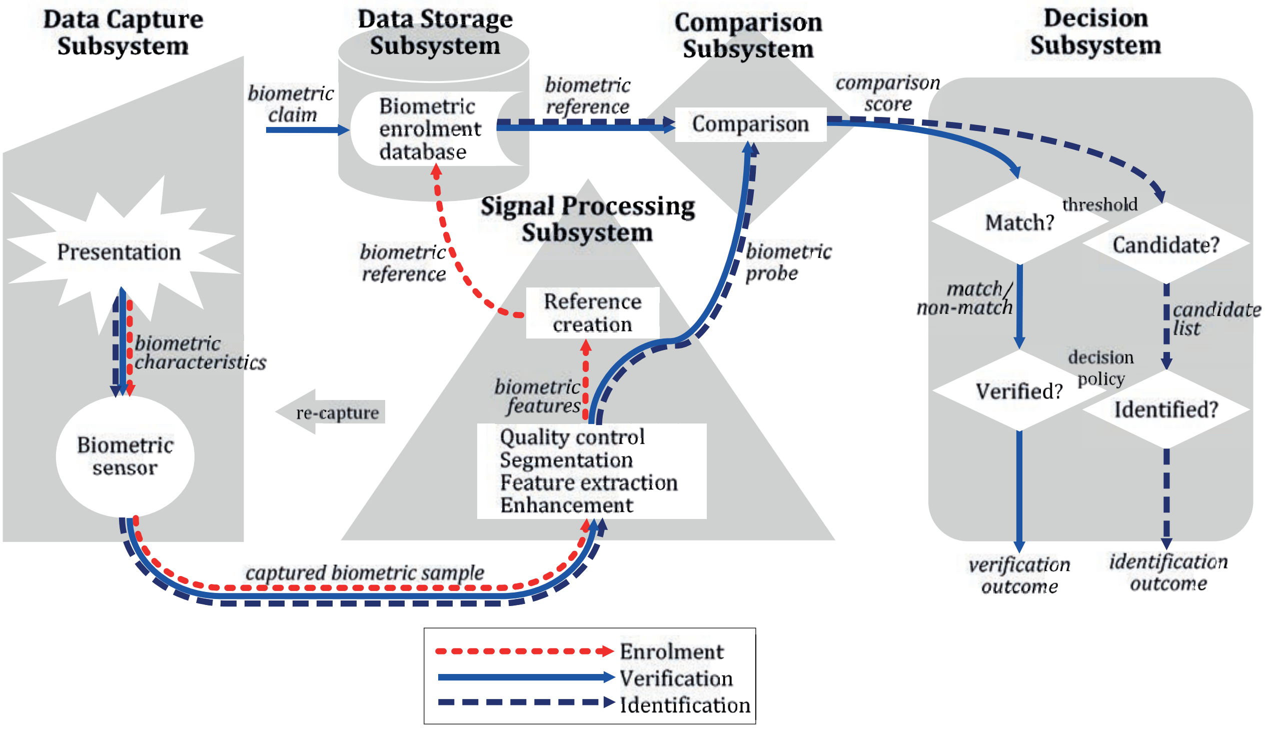

Figure 1 — Components of general biometric system

Figure 1 (which is functional in nature and has no implications for physical location) 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. The following sub-clauses 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.

The *data capture subsystem* collects an image or signal of a subject's *biometric characteristics* that they have presented to the *biometric sensor*, and outputs this image/signal as a *captured biometric sample*.

The *transmission subsystem* (not portrayed in the diagram and not always present or visibly present in a biometric system) will transmit *samples, features, probes* and *references* 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.

Signal processing may include 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, and references, and possibly affecting other processes, such as returning control to the data capture subsystem to collect further *samples*; or modifying parameters for segmentation, feature extraction, or 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 this 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.

References are stored within an *enrolment database* held in the *data storage subsystem*. Each reference might 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 on a personal computer or local server, or a central database.

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 *features* and *reference/s* compared. In some cases, the *features* may take the same form as the stored *reference*. For verification, a single specific claim of subject enrolment would lead to a single *comparison score*. For identification, many or all *references* may be compared with the *features*, and output a *comparison score* for each comparison.

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

In the case of verification, the *features* are considered to *match* a compared *reference* when (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 highest 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 multi-biometric systems in the same manner as uni-biometric systems, by treating the combined captured biometric *samples/references/scores* as if they were a single *sample/reference/score* and allowing the decision subsystem to operate score fusion or decision fusion as and if appropriate. (See also ISO/IEC TR 24722:2015.)

The *administration subsystem* (not portrayed in the diagram) governs the overall policy, implementation and usage of the biometric system, in accordance with the relevant legal, jurisdictional and societal constraints and requirements. Illustrative examples include

- Providing feedback to the subject during and/or after data capture,
- Requesting additional information from the subject,
- Storing and formatting of the biometric *references* and/or biometric interchange data,
- Providing final arbitration on output from decision and/or scores,
- Setting *threshold* values,

- Setting biometric system acquisition settings,
- Controlling the operational environment and non-biometric data storage,
- Providing appropriate safeguards for subject privacy, and
- Interacting with the application that utilizes the biometric system.

The biometric system may or may not interface to an external application or system via an application programming interface, a hardware interface or a protocol interface.

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

Enrolment typically involves

- Sample acquisition,
- Image pre-processing including sample restoration or enhancement, and segmentation,
- Feature extraction,
- Quality checks (which may reject the sample/features as being unsuitable for creating a reference, and require acquisition of further samples),
- Reference creation (which may require features from multiple samples), possible conversion into a biometric data interchange format,
- Storage,
- Test verification or identification attempts to ensure that the resulting enrolment is usable, and
- Allowing repeat enrolment attempts, should the initial enrolment be deemed unsatisfactory (dependent on the enrolment policy).

A subject can also be required to present additional data specific to the enrolment. This additional data might be a legal name, contact information, credentials, identity documents and the like. There are some biometric applications that may require no additional data whatsoever to be collected at the time of enrolment beyond the biological and behavioural characteristics.

6 Stakeholders and approaches for enrolment

6.1 Enrolment stakeholders

The successful operation of a biometric enrolment service depends on the co-operation of a large number of stakeholders as listed in Table 1. (See also Figure 2 below showing that enrolment officers work on behalf of the operator, which has a relationship with the Enrolment Authority; personal assistants support the subject of the enrolment). Note that systems may be far simpler than illustrated, for example, the Enrolment Authority may also be the operator of the service, as well as being the relying party in an enterprise access control system.

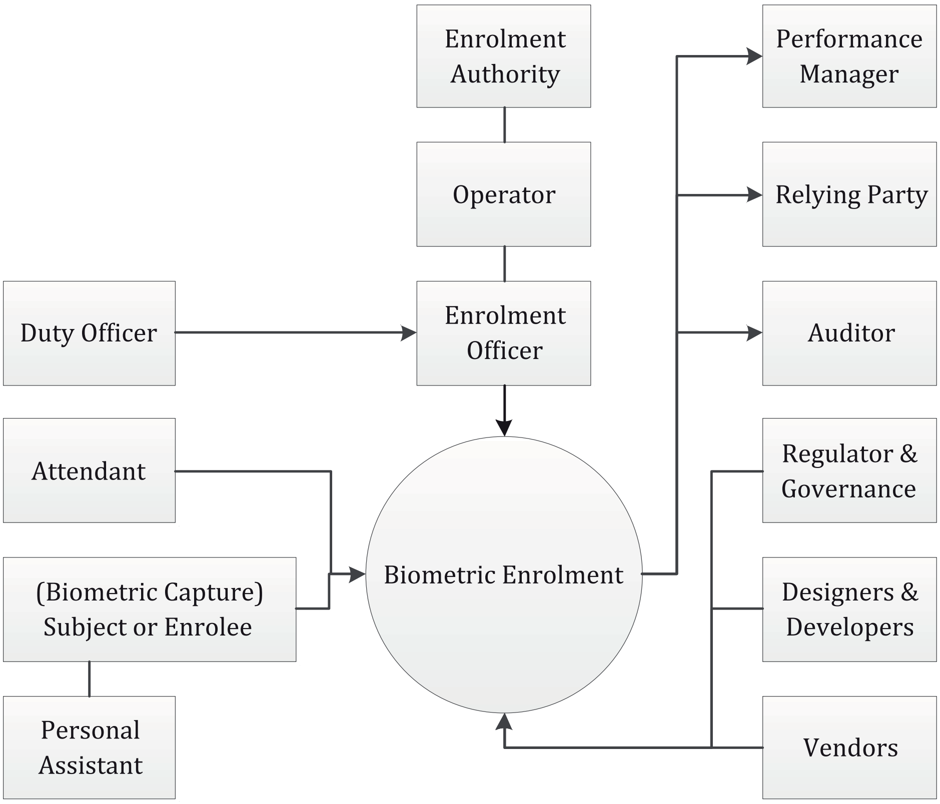

Figure 2 — Stakeholders at enrolment

Table 1 — Functional description of stakeholder roles

Stakeholder	Function description
Enrolment Authority	Is responsible for ensuring the quality of biometric enrolment samples and other KPIs are in accordance with SLA or contractual requirements. Initiates appropriate action if these fall outside the agreed targets. Ensures compliance with legal requirements. Ensures that the cultural implications of operating an enrolment service are taken into consideration.
Operator	Organizes delivering enrolment service on a day-to-day basis. Is responsible to the Enrolment Authority for quality and security of the enrolment service. Takes remedial measures if KPIs, including quality and performance metrics, fall outside the agreed targets.
Performance manager	Monitors the performance of the enrolment service. Proposes corrective actions. Reports back on the results of corrective actions.

Table 1 *(continued)*

Stakeholder	Function description
Enrolment officer	Is the agent of the operator responsible for the secure and effective enrolment service at one or more enrolment points. Ensures the day-to-day maintenance of equipment used in enrolment. Interfaces with the subjects and provides any relevant information to them. Enters any biographical/contextual data (although some of these details may already be pre-populated). Ensures that the quality of the enrolment feature collected by the sensor/camera meets the enrolment standards (usually through requesting the subject to re-enrol if the standard is not achieved). Provides advice and support to the subject to achieve a high standard of enrolment. Notes any exceptional circumstances.
Duty officer	Provides technical and/or operational advice and guidance to an enrolment officer.
Attendant	Assists the enrolment officer in obtaining the best available quality biometric sample through following procedures defined for subjects with accessibility needs or special requirements including age, gender, and religious observance.
Biometric capture subject / biometric enrolee, hereafter termed as subject or enrolee	Provides biometric sample to the system. Needs transparency and information on the system. Is interested in smooth operation. Is interested in maintaining their data privacy, wants to submit only that data that is absolutely necessary for the intended purpose, and prefers a system that is as usable as possible. Prefers to have a system that is as intuitive as possible.
Personal assistant	Provides support for the subject, e.g. translation of instructions from the enrolment officer, support for a disabled subject or to fulfil a legal requirement such as a parent present at the enrolment of a child.
Designer and developer	Designs the enrolment system as part of the enrolment service using systems engineering principles wherever possible. Develops enrolment system, service and process. Develops an interaction protocol for the enrolee. Develops the service for production and distribution of any token used as storage for biometric reference(s), or a pointer to where biometric reference(s) is/are stored.

Table 1 *(continued)*

Stakeholder	Function description
Vendor	Provides hardware and software. Provides (either directly or through an agent) technical support e.g. for upgrades or rectification of faults, if under contract to do so.
Regulator and other governance bodies	Assures the enrolment process is operated according to laws, regulations, codes of practice, and contracts.
Auditor	Audits the enrolment protocol.
Identity Provider	Processes the biometric features into references, performing any quality and de-duplication checks and storing references and images.
Relying party	Uses the biometric data obtained from the enrolment service in a biometric recognition service as part of a business-oriented application.

6.2 Enrolment approaches

Enrolment for biometric services can take the form of many differing approaches depending upon context, complexity, and requirements of the relying party such as:

- In-house or outsourced;
- Multiple or single location;
- Fixed, mobile or remote;
- Attended, semi-attended (one enrolment officer overseeing a number of enrolments in parallel) or unattended (e.g. self-enrolment);

  NOTE Self-enrolment can be with the active participation of the subject, or can even be acquired with stand-off systems not requiring direct interaction with the subject.

- Mandatory, optional (opt-in), or unaware (e.g. for surveillance/tracking);
- Using a single modality or multiple biometric modalities;
- Designed to provide enrolments for either multiple applications or for a specific application. Enrolment is an expensive part of a biometric service. In order to reduce costs, enrolment may at times be undertaken for multiple relying parties, each with differing business, technical and functional requirements. For example, the enrolled facial image for a passport may be re-used for a driver's licence application. Re-use of biometric data is mostly regulated by privacy law, which often requires informing the subject on the intended purpose preventing additional use without explicit consent of the subject. Other enrolment processes may be required to be more specific in design – e.g. access control 'offline' or 'batch' enrolment process where the biometric sample capture is separate from the enrolment stage, or an integrated credential proofing/acquisition/enrolment process;
- Duration/complexity of the enrolment process, from a simple single modality process (against pre-assigned identity), to a complex process consisting of identity checks using breeder documents, followed by collection of features relating to multiple modalities and a verification check on the effective operation of the collected features.

Based upon how the system is influenced by the above factors, there will be different requirements and operational guidance.

7 Stakeholder interests

7.1 Key observations

A repeatable biometric enrolment process is a prerequisite for the successful use of biometric recognition in one or more applications at a subsequent time.

A poor quality enrolment, e.g. one in which the subject's biometric features have been collected in line with best practice, but do not meet all quality criteria, can present difficulties when the reference derived from these features is compared with biometric data collected in the context of the application. For example, if a thumb is presented and registered in an enrolment for access control, and the subject uses one of the index fingers as instructed by a biometric verification unit at an access point, the biometric comparison will fail. The subject will therefore be inconvenienced, in having to use an exception-handling process provided by the operator of the access control system.

Such problems are likely to occur more often when the Enrolment Authority (and/or the operator) for the enrolment service is not the same as the party managing the subsequent application that uses biometric recognition (the relying party). In this case, the Enrolment Authority bears the costs of ensuring that the quality of enrolments is maintained while the benefits of good quality enrolments accrue to the relying party (or parties). Rather than setting this cost/benefit pivot at the interface between the two organizations, a better strategy is to move it to the enrolment service, incentivizing the Enrolment Authority to deliver high quality enrolments. This will usually entail clear and correct specification of metrics for the enrolment performance in any contracts or agreements between these two organizations.

In setting the requirements for an enrolment service, the Enrolment Authority should take account of the requirements of the relying party as well as other stakeholders as listed in Table 1 and represented schematically in Figure 2. (When these requirements are not known in full, e.g. because the recognition system of the relying party is still under development, designers of enrolment services should take appropriate measures to mitigate any risks.) The SLA between the Enrolment Authority and the operator of the enrolment service should include KPIs that relate to the business objectives of the Enrolment Authority as well as those of the relying party. Requirements should include quantitative performance measures capable of being tested either by the Enrolment Authority or by an independent testing organization during the acceptance phase of the project, as well as periodically afterwards.

The designers and developers of the enrolment system will use the requirements to define processes appropriately and to source suitable vendors of the biometric components, such as the hardware to collect biometric features, software to process these features and assess their quality, and - if required - verification software to check that the enrolment has been completed satisfactorily.

The security of the biometric enrolment process is also an essential aspect of its success. In preparing for a robust process design, all stakeholders are responsible for addressing security requirements, from the design of the logical technical architecture to the functional components, as well as procedures and checks that directly involve interaction with the subject.

The Enrolment Authority's designers and developers should address these requirements, as early as possible in the design, such as the ability to check the identity credentials presented by the subject and taking measures to counter spoofing attacks. For details on Presentation Attack Detection (PAD) see the multipart standard ISO/IEC 30107. Note that catering to the needs of subjects with language difficulties and disabilities will also feature in the design but may impact on the security procedures. These aspects of the enrolment process – and any requirements placed by regulators – should be included in the training materials for enrolment officers, attendants, duty officers and the performance manager.

After completion of the high level design, and prior to deployment, marketing and other awareness-raising activities should be started. This enables representatives of the subject population, mass media, regulators and special interest groups to comment on the enrolment service proposals. As a result, any necessary changes to the system design may be incorporated.

The enrolment service should be piloted with a representative sample of the subject population, both of subjects as well as enrolment officers. The performance manager should ensure that acceptance testing has been carried out and that the provisions of the SLA with the designers and developers have been met. Comments and observations collected from the subjects should be examined. If changes are made to the system or procedures in the light of these tests and comments, a further round of testing may be required.

At some time after the system is deployed, representatives of the relying party and the Enrolment Authority should review the performance of the enrolment service, assessing whether the KPIs continue to reflect the requirements of the relying party, and making any necessary adjustments.

A system audit may be requested periodically to ensure that the enrolment service operates in line with legal and business rules. Guidelines for the audit process should take account of the particular characteristics of biometric systems.

7.2 Best practices and recommendations

7.2.1 General

There are numerous stakeholders in any biometric enrolment application, most of whom will benefit from a high quality, securely administered enrolment process with due regard for the needs and expectations of the subjects of the enrolment.

For each stakeholder described in Table 1, there are specific reasons why the enrolment service should be successful. This Clause describes some of the benefits for these stakeholders.

A strategy for the design, development and deployment of a successful biometric enrolment should consider numerous issues in a structured manner. The approach favoured in this document is to itemise these issues against the principal stakeholders who are impacted by each issue. One way of examining the benefits to a stakeholder is to consider the operation of the enrolment service from a number of standpoints. Stakeholders will have different perspectives and not every standpoint will be relevant to every stakeholder:

- Appropriateness, effectiveness and efficiency,
- Convenience and price,
- Look and feel,
- Usability, personalisation and internationalization,
- Performance including speed, and accuracy,
- Operational and environmental aspects,
- Maintainability and support,
- Security, privacy and transparency,
- Cultural and political aspects, and
- Legal aspects.

7.2.2 Subject interests

The enrolment subject should be presented with a clear and understandable enrolment process that allows the subject to feel safe and alleviate any concerns.

The enrolment process should flow well and be able to handle any possible exceptions. Prior identification of exceptional conditions (e.g. support for disabled persons) can be flagged in the application process to allow for adjustments to be made in advance of enrolment.

It is important to ensure that the enrolment process is safe and provides a positive experience for the subject in order to enhance acceptance of the system. This includes that technical solutions should be as comfortable as possible within the constraints of application and enrolment system/process requirements.

Any situation where the enrolment may cause discomfort to the biometric capture subject needs a clear justification.

The enrolment subject should have easy access to information about the accessibility, privacy, usability and other consumer-relevant issues associated with the enrolment process and the biometric system preferably in advance of attending the enrolment session.

A strategy for the design, development and deployment of a successful biometric enrolment should consider numerous issues in a structured manner. The approach favoured in this report is to itemise these issues against the principal stakeholders who are impacted by each issue.

On the matter of issues relating to personal privacy, data protection, health and safety and accessibility, the reader of this report is referred to ISO/IEC TR 24714-1:2008.

NOTE This TR is freely available from: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

7.2.2.1 Provided information

When considering the information to be provided to a subject, several important considerations should be acknowledged. In particular, subjects:

- Should be notified about policies including, but not limited to, privacy, personal data protection and accessibility;
- Should be notified on the intended purpose of their collected biometric data, on the storage time frame and on de-enrolment and data removal;
- Should be notified about technical aspects including, but not limited to, security and data encryption;
- Should be informed that the security level depends on technology and processes and differs for different applications. In some applications, biometric technology may lead to specific legal assumptions with respect to non-repudiation. If this is the case, the subject should state that they fully understands and consents to the consequences of these legal assumptions;
- May expect to be notified about a contact point for further information;
- Where required, should be informed that they are asked to produce documents that can be authenticated with the Issuing Authority to satisfy the enrolment officer of their claimed identify;
- Some legislation requires that the subject shall always be informed when biometric data is captured, and that the captured data shall only be used for the intended purpose. A later extension of the purpose is not allowed without consent.

On occasion the subject may be unaware of the fact that a biometric enrolment is taking place, e.g. when submitting a photograph for a passport application. Advice should be sought as to whether a legal notice is required, or whether it would be prudent to provide more information to the subject.

Information about the enrolment should be provided in a way that is accessible and comprehensible to the subjects. It may be useful to include the possibility of a list of frequently asked questions (FAQ), including information regarding the purpose of enrolment and the organization’s privacy policy. Different kinds of information will be relevant at different stages of the enrolment: before the enrolment, during the process and afterwards. It should be updated as experience is gained so as to ensure that enrolments are an ongoing success.

At enrolment, provisions of specific information helps subjects to enrol in the system most effectively (e.g. whether they should stand or sit in a particular way, and whether there will be wipes or tissues to clean surfaces and improve the quality of images).

Subjects should be given the opportunity to supply information that may impact on the quality of enrolment, some of which may be regarded as personal or confidential. Recording of such information — and the measures taken during enrolment as a result of this information — should be undertaken in a secure manner.

7.2.2.2 Legal implications

Any specific local provision relating to documentation in support of proof of identity and authentication thereof, privacy, the protection of personal data, accessibility, security, etc. should be identified and incorporated during the requirements capture phase of the enrolment system lifecycle. The safeguarding of enrolment data provided by the subject in the enrolment system lifecycle is important, particularly if enrolment data is to be shared between organisations.

Therefore, requirements relating to access, use, disclosure and disposal of enrolment data should be carefully considered. Different parties, such as commercial and government, may consider legal implications differently and at times have conflicting requirements for addressing them. Governance procedures should be implemented that may in turn place specific requirements on audit logs.

Implications of enrolment also should be covered, e.g. if there are any non-repudiation ramifications to subjects enrolled in the system, these should be fully explained, understood, and consented to, by the subjects.

7.2.2.3 Inclusivity

In order to obtain optimal quality biometric data during the enrolment phase, it is particularly important to ensure that inclusivity issues are addressed. In many cases, it will be more effective to devote additional resources and time at enrolment with specialized equipment, staff and training for the subject. Also to avoid difficulties for the subject in attending and completing an enrolment, information should be provided regarding any accessibility conditions which might result in poor quality outcomes.

Provision should be made for personal assistants including guide dogs accompanying the subject to the enrolment facility.

Note that the enrolment process may reveal hitherto unrecognized conditions that may require sensitive handling by the attendants.

7.2.2.4 Usability

Enrolment systems should be designed for usability. ISO 9241-11:1998 and ISO 9241-210:2010 define usability as “the effectiveness, efficiency, and satisfaction with which the intended users can achieve their tasks in the intended context of product use.”

A guide to methods of assessing the usability of biometric systems is available that covers effectiveness, efficiency and user satisfaction[11][12].

In general, the enrolment system should attempt to obtain a biometric reference of the best quality for the target application, consistent with constraints of time allowed for enrolment, costs of arranging the enrolment and availability of equipment and attendants.

Quality is one of the aspects of effectiveness. This term does not necessarily relate to an aesthetically pleasing captured image. For example, if the system is required to ensure that a person is enrolled only once, a high quality capture is one that enables the matching system to other entries on the database to be carried out with the maximum confidence in identifying correct matches. Quality has many additional dimensions including consistency of presentation, sufficient distinguishing elements in the image.

The process of enrolment should be carried out in ways that enable the subjects to perform the task quickly and with as few errors as possible.

User satisfaction relates to subject attitudes, perceptions, feelings and opinions regarding the system, and includes aspects such as

- Whether the subjects are intimidated in any way by the equipment or process,
- Whether the subjects behave naturally, and the system interface is physically and cognitively ergonomically viable,
- Standard time,
- The quality of the information and support to subjects,
- The extent to which the user interface is designed as intuitive as possible to avoid subject discomfort and frustration, and
- The presence of an attendant (if the enrolment is manual), noting that the demeanour and helpfulness of the attendant is important.

Satisfaction levels can be measured in ways including surveys or focus groups, with the aim of maintaining and improving the user experience.

7.2.3 Enrolment Authority interests

For the Enrolment Authority, its principal objective is ensuring the collection of a representation of the biometric features of a qualified individual to fulfil the requirements of the relying party's application using biometrics. In helping to achieve its objective, the authority should develop an enrolment policy.

Note that the Enrolment Authority that enrols the subject and the relying party that operates the biometric-enabled application may be different organizations. The Enrolment Authority can have legal duties and obligations (e.g. in relation to provision for people with accessibility needs) of which it should make the operator aware, and ensure that the operator is in compliance. For example, the Enrolment Authority could define the specific duties of the attendant and special assistant and their role in obtaining a good enrolment as part of an inclusive design. Considerations for the Enrolment Authority include:

- Collection of the biometric samples that give (after further processing by an Identity Provider responsible for storage and matching of the samples) the best possible set of biometric references under the circumstances, which can be used for subsequent verification and identification processes. Such processes may include checks for duplicate enrolments.
- The establishment and monitoring of the characteristics of success for the end-to-end system.
- An enrolment process should reduce the cost of the end-to-end system (which covers enrolment, database, and the application operated by the relying party), especially for large scale systems, since enrolment costs are likely to be a significant component for such deployments.

7.2.3.1 Establishing the legal framework

The Enrolment Authority should, at an early stage of system design, establish the legal and cultural implications, which include privacy and data protection, compliance with codes of conduct, local laws and by-laws. Laws and regulations relating to these aspects may be both national and regional. ISO/IEC TR 24714-1:2008, 4.2.3 provides guidance on privacy principles for biometric systems.

Where appropriate, if the Enrolment Authority cannot be satisfied as to the claimed identity of the subject then services made available on the basis of enrolment may be withheld or otherwise constrained.

The Enrolment Authority should determine what auditing functions are required. Relevant terms of reference should be developed, together with frequency of audit and relationship to other governance activities.

Implications of enrolment also should be covered, e.g. if there are any non-repudiation ramifications to people enrolled in the system, these should be legally justified and enforceable, and processes developed to ensure that they are fully explained, understood, and consented to, by enrolees. Be aware that non-repudiation ramifications might cause subjects to refuse participation in voluntary applications.

Also there may be legal issues surrounding certain classes of enrolee, including gender, ethnicity, age, disability, culture, religion, and legal competence.

In many jurisdictions, procurement officials and operators should be aware of laws and regulations relating to inclusivity; capture of the relevant requirements at an early stage in the process is likely to lead to cost-effective solutions.

The Enrolment Authority (with the help of the auditors) should keep the legal framework under periodic review. As experience with deployment and operation of biometric applications grows, it is likely that new laws, regulations, and codes of practice will be introduced (or existing ones redrafted) and judicial decisions may affect the operation of services.

7.2.3.2 Independent service operation review

The Enrolment Authority may request an independent review of the delivery and operation of the enrolment service, both of its security and the biometric performance - either with a test group of enrolees before the start of an operation of the service, or during its operation using a representative sample of subjects. Assessment, testing and reporting the results of such tests for a biometric enrolment service requires specialized knowledge and experience. Only those organisations that can demonstrate their credentials in these areas should be considered. Testing should be undertaken against relevant national and international standards (such as those in the multi-part standard ISO/IEC 19795).

7.2.3.3 Success metrics

Enrolment is normally a prerequisite to operational use of a biometric system. The quality of enrolments will affect the performance and usability of the operational system. The subject experience at enrolment is likely to affect a subject's perception of the operational system and of the organization operating the system, which may also have a knock-on effect on the performance of the operational system.

The enrolment process/service will cost money, time and possibly other resources. Measures to improve enrolment quality or subject experience will probably have a cost/time implication for the enrolment service. Therefore an optimum balance between the cost of the enrolment service and the performance and usability of the operational system should be established.

In order to improve the quality of enrolment, it is vital to have access to data which can be used to monitor the various components of the service, both to ensure that the service is operating to initially developed performance levels, as well as helping to improve the service through addressing the most significant elements of the cost/benefit trade-off. This requires that the design of the biometric enrolment service allows for the right metrics to be collected (and analysed regularly at various levels of granularity).

The performance parameters divide into two broad categories:

— Parameters that relate to the performance of the enrolment service, e.g. failures to enrol, invalid enrolments, denied enrolments. These are the enrolment failure parameters.

— Parameters that affect the performance of the relying party's operational system using the enrolments from the enrolment service, e.g. FMR, FNMR, or FTAR. These are (largely) the enrolment quality-dependent parameters.

The two categories are distinct but interrelated and can be in conflict, e.g. a reduction in the FTER might lead to an increase in the FNMR. The possibility of conflict may create tension between the enrolment service and the operations of the relying party (or parties) which is likely to be amplified in cases where these are provided by different organisations.

A classification of enrolment failures is suggested in 7.2.3.4 based upon the definitions in ISO/IEC 2382-37 which provide definitions related to the enrolment process. Examples of common causes of enrolment failures are examined against this classification in 7.2.3.5.

In order to provide the data for such analysis, a requirements capture exercise should be undertaken before the design of the enrolment service which will include the following (some of which need data collated from relying parties under an SLA):

- Performance statistics from the relying party operating a service that is dependent on a successful enrolment of subjects, with a breakdown to help identify the impact of any variations in quality of the enrolment service.
- Subject satisfaction statistics, for example, extracted from analysis of surveys, numbers of complaints from enrolees or assessment from media reports. Identity proofing failure rates with a breakdown into rates where the Enrolment Authority detected suspicious (or proven) fraud, where it was unable to confirm identity to a sufficient (predetermined) level of confidence, and where subsequent evidence of inaccuracy or fraud came to light. Failure to enrol rates, analysed by demographic group, enrolment centre, time of day, the type of resolution procedure that was applied and the results of such actions.
- Distributions of image and enrolment quality analysed by demographic group, enrolment centre, time of day, etc.
- Number of retries required and whether or not an operator override (e.g. of quality threshold) was used.
- Statistical measures relating the duration of biometric enrolment (e.g. mean time from start of the process through to successful conclusion, maximum response times from a central database — if a check for duplicate enrolments is made). Note that terms should be defined clearly, e.g. ‘start time’ may refer to the earliest recorded interaction between the biometric capture device and the subject, or it may be the initiation of the process by the enrolment officer. Timings of the individual segments of the enrolment process may be recorded, for example, so that that the ‘dead time’ between individual transactions can be treated in accordance with a predetermined policy.
- Proportion of enrolments that fail the verification test (for services where these are implemented).
- Transaction logging of appropriate granularity.
- Auditing support consistent with a set of established requirements.

7.2.3.4 Error rates

A classification of failures encountered in enrolment processes is provided as an aid to the design and development of the enrolment services. Based upon the definitions in ISO/IEC 2382-37, this classification (which is not part of said document) will enable enrolment service designers to develop their own tabulation of failure types from Table 2 and Table 3 below in preparation for definitions of their performance metrics.

Table 2 — Classification of failures encountered in enrolment processes

Class	Failure mode	Definition	Comment
1	An ineligible person is denied service and hence does not commence an enrolment process	Not considered as a failure to enrol	Not enrolling someone ineligible to enrol is not a failure to enrol. Such a person may become eligible for enrolment at a later time. Reasons for ineligibility should be determined prior to commencement of the enrolment service.
2	Excluded biometric enrolment transactions	Transactions that failed to complete for non-biometric reasons	The proportion denominator is the number of biometric enrolment transactions, excluding those transactions that failed to complete for non-biometric reasons.
3	Failure to capture	Failure to accept for subsequent comparison the output of a biometric capture process, a biometric sample of the biometric characteristic of interest	A captured biometric sample contains a signal from a biometric characteristic, but it might not be the biometric characteristic of interest. A blank or empty sample represents a failure to capture, even if the failure is not discovered until the biometric acquisition process. A captured biometric sample might not be suitable for future processing.

Table 2 *(continued)*

Class	Failure mode	Definition	Comment
4	Failure to acquire	Failure to accept for subsequent comparison the output of a biometric capture process, a biometric sample of the biometric characteristic of interest	The failure to acquire rate (FTAR) is defined as the proportion of a specified set of biometric acquisition processes that were failures to acquire. Failure to acquire occurs if the captured data does not meet system policy requirements for processing. Failure to acquire can only occur if there has been a successful data capture event. Otherwise the event is a failure to capture. Possible causes of failure to acquire include poor biometric sample quality, algorithmic deficiencies and biometric characteristics outside the range of the system.
5	Failure to enrol	Failure to create and store a biometric enrolment data record for an eligible biometric capture subject, in accordance with a biometric enrolment policy	The failure to enrol rate (FTER) is defined as proportion of a specified set of biometric enrolment transactions that resulted in a failure to enrol. The proportion denominator is the number of biometric enrolment transactions, excluding those transactions that failed to complete for non-biometric reasons. Since the measure is based on the number of transactions, the FTER may result in a higher value than if it were based on the number of subjects. Note Enrolment transactions should be distinguished (includes the checking of credentials, acceptance for biometric enrolment as well as the biometric enrolment transaction) from biometric enrolment transactions

In defining contractual terms with the operator, the Enrolment Authority should take account of these definitions, referring to the Standard. If, after analysis of their requirements, the authority decides that these definitions do not apply, the contract (and any SLA policies) should make explicit reference to this fact and provide new definitions, and amend accordingly any definitions in the requirements for testing.

NOTE This document does not define the terms biometric enrolment policy, and (biometric enrolment) transaction.

When reviewing the failure to enrol rates, the Enrolment Authority (and or the operator) should adopt a systematic approach, noting sources of data and common classes of failure.

7.2.3.5 Failure analysis

The authority may require a detailed analysis of failed enrolment transactions from the operator, for example as part of a root cause analysis into changes in the FTER from certain enrolment locations. The capability to undertake such an analysis will depend on the availability of relevant data. Sources of data can be categorised as:

— Data that is available from records of enrolment transactions, e.g. the proportion of subjects who have enrolled successfully.

— Data that can be collected when the authority or the operator determines the need for an analysis of a representative set of enrolments but which would not be collected under normal circumstances. For example, the number of biometric enrolment transactions required for each enrolment may not be collected routinely, but a request can be made of attendants/enrolment officers to collect this data manually.

— Data that cannot be collected (without change to the enrolment software) when the authority or the operator determines the need for an analysis of a representative set of enrolments, but which can be subsequently derived from data accessible to the authority. For example, few, if any, enrolment systems would be able to account for the reasons for NFIQ scoring of the quality of a fingerprint image. Assignment of an NFIQ score is the results of applying a software algorithm to various aspects of the image. A major contribution to the assignment of this quality score is the number of minutiae detected in the image, together with the numbers with specified levels of 'minutiae quality'. It might be that the total number of minutiae in an image is of possible relevance, in which case the authority could request that an analysis be made of relevant stored images.

— Data that cannot be collected (without change to the enrolment software) when the authority or the operator determines the need for an analysis of a representative set of enrolments, and that cannot be subsequently derived from data accessible to the authority. An example is the levels and direction of ambient illumination during the enrolment of facial images, if such enrolments are made in a relatively uncontrolled environment, such as a room with windows to the external environment. Although some estimate of the predominant direction of lighting could be inferred from analysis of the photos, the levels of illumination could not be determined absolutely if cameras were set to optimize collection automatically.

The following listing of possible causes of poor enrolment indicates the range of circumstances which could be considered.

Table 3 — Causes of poor enrolment

Failure number	Failure type	Notes and examples	Failure class
1	An ineligible subject is not allowed to complete the enrolment		1
2	An ineligible subject completes the enrolment successfully		Exclude from analysis according to biometric enrolment failure class, but should still be recorded
3	A subject refuses to complete the enrolment process		2
4	A subject refuses to co-operate with the attendant in the capture of the biometric data in accordance with the authority's biometric enrolment policy and any other instructions	Exclusions may be allowed for medical conditions, but authority should offer guidance for people unwilling to touch surfaces as a result of obsessive-compulsive disorder and similar conditions. This should be covered in the biometric enrolment policy.	2
5	Failures in power supply, air conditioning or telecommunications links, strikes by operating staff, etc. result in abandonment of enrolments		2
6	Failure due to software or hardware malfunction		2
7	Absence of the body part	Missing iris (aniridia)	3
8	Body part is inaccessible due to medical condition	Bandaged finger or finger with psoriasis.	3
9	Body part is inaccessible on account of social, cultural or religious reasons	No female attendant present when a female subject presents with a face covering required for cultural or religious reasons	3
10	System triggers collection of biometric sample before subject is ready or before relevant body part is placed in contact/ proximity to capture device		3
11	The subject presents the wrong biometric modality		3
12	The subject presents the correct modality but the feature is not presented in the correct order	Placing the wrong hand on the fingerprint or palm vein reader. This presumes that such cases are detectable automatically by software or through observation by the enrolment officer.	3
13	The subject's medical condition prevents capture of the image through the required level of contact (or stability of position) not being made for sufficient time	Parkinson's disease, or conditions such as rheumatism preventing required area of contact with platen	3

Table 3 *(continued)*

Failure number	Failure type	Notes and examples	Failure class
14	Body adornment or treatment preventing the capture of a usable image	Henna, scars, marks, tattoos, and implants	3
15	Body part out of range of the specification for the enrolment device	Fingers too broad to enrol in a single finger device with guides	4
16	Biometric sample is wrongly assessed as a spoof attempt	Anti-spoofing alert triggered by unexpected characteristics of the biometric feature	4
17	Biometric sample from a feature which is damaged	Fingerprint quality software alerts to excessive damage	4
18	Insufficient detail in the biometric sample	Number of minutiae in fingerprint falls below a threshold, or finger is too dry	4
19	Biometric features fall out of range of the specification of the proprietary algorithm to create a usable biometric reference		5

7.2.3.6 Poor quality analysis

In addition to total failure of enrolment, the Enrolment Authority should develop metrics for measuring the incidence of poor quality enrolments. Standards and technical reports in the ISO/IEC 29794 series should be considered for that purpose.

This presupposes:

- The existence of a standard against which elements of quality can be assessed. In part, this may be supported by the multi-part standard ISO/IEC 19794;
- Experimentally-validated software which defines quality metrics for one or more biometric comparison algorithms. For fingerprint systems using minutiae, NIST have developed NFIQ and NFIQ 2.0 which have been tested on a number of comparison algorithms;
- Other specialist software, either from suppliers of comparison algorithms or from independent organisations, which often addresses specific elements of the specification for the modality in the multi-part standard ISO/IEC 19794.

It is worth noting that certain demographic groups present particular challenges during enrolment, as noted in ISO/IEC 19795-1. For example, experience shows that obtaining good quality fingerprint images from children and the very elderly can be difficult. Furthermore, certain activities, such as continued contact with abrasive materials, e.g. through working in the construction sector, can result in a greater proportion of poorer quality enrolments.

Where Enrolment Authorities permit glasses to be worn during collection of facial biometric images and the subject normally wears glasses, the glasses should not be thick framed glasses, allowing a clear view of the eyes. There should be no light reflections off the glasses.

7.2.3.7 Corrective actions

Analysis of the metrics relating to the enrolment service should highlight changes outside of the control parameters which have been determined for the service. Analysis of the metrics relating to the enrolment service may show changes outside of the control parameters. These should be investigated and remedial action agreed with the operator. As part of the contract(s) with the system designer(s) and developer(s), the Enrolment Authority may wish to negotiate for the production of guidance documentation for such eventualities.

7.2.3.8 Research

There are at least two reasons for retaining data for research purposes:

- Proving that a system operates correctly may require the temporary storage of biometric data, e.g. in order that false match rates can be determined.
- Biometric data relating to operational systems is often very difficult to obtain, yet improvements in technology need access to extensive data sets in order to validate novel ideas. Hence, data collected in one system can be used to improve the performance of other, totally unrelated, systems.

An Enrolment Authority should be aware of these opportunities and be prepared to develop security policies, privacy impact assessments, etc., if these are shown to be of long term value to their organization. Note that in some cases, this will require co-operation with relying parties, in order to track an individual's encounter with a biometric system from enrolment to recognition. In some countries, proposals for research should be presented to an ethics and/or privacy committee, and/or need the informed consent of all involved enrolees.

7.2.3.9 Contract termination and reassignment

Contracts with the operator (which delivers the enrolment service on behalf of the Enrolment Authority) may be designated for a specific term, after the expiry of which, the Enrolment Authority may want re-tender the service. Arrangements for handover may include the production of documentation capturing the knowledge of the operator and personnel about specific aspects relating to the successful delivery of the service at individual centres, and a detailed representation of the status of the biometric elements of the service. Note also that the Enrolment Authority may be engaged on a contract with the relying party (or parties) in which case, preparations for orderly transitioning should be in place well in advance of the handover period.

7.2.4 Operator interests

For the operator of the enrolment service (which in many cases will be the same organization as the Enrolment Authority), it is crucial that the procedures at enrolment fulfil the requirements set by the Enrolment Authority for a cost-effective, legal, quality and secure process, as expressed in a SLA.

Considerations for the operator include:

- The operator should consider how to collect the biometric features (such as optimising equipment and the number of attempts) that give the best available set of biometric references ('templates') so as to achieve targets for enrolment set by the relying party in its contract/agreement with the Enrolment Authority.
- A good experience for the subject should contribute to a lower drop-out rate from the appointment system for enrolment; otherwise, poor user experiences shared with the mass media may deter other potential subjects from keeping to their appointments.
- Provide the operator with a standard method of collection to ensure the process is efficient and consistent.
- A more efficient process will reduce operating costs.

7.2.4.1 Training programmes for personnel

Enrolment officers and attendants at attended enrolment points should be trained with the aim of delivering a secure, efficient and effective service to the Enrolment Authority. Such trained personnel may receive a certificate to indicate their level of qualification, and a periodic re-certification may be offered as well.

Human factors research and tests show that people vary greatly in their ability to recognize different images in a facial recognition gallery or image. Consideration should be given to enrolment officer's abilities to recognize images in galleries and image sets before being appointed to their role. If humans are to deal with the exceptions, then these individuals should be trained and have a high level of expertise and competence in the additional verification and identification tasks that may be required to establish identity. Selection of the training method should make use of best practice with regard to the placing of instruction, modality of delivery (e.g. written, face-to-face presentation, or online learning), frequency of refresher courses, etc. Some of the training material may be provided by suppliers of biometric components or systems. It is recommended that officers are periodically tested on competency after completion of the training.

Ongoing monitoring of enrolment quality, throughput rates and other relevant metrics may be used to indicate a need for refresher training; 'mystery shopping' and observational studies may be used periodically to ensure that officers continue to maintain a high standard of competency and practice.

A typical training programme may cover aspects such as:

— An explanation of the biometric process, indicating why a high quality and secure process — and strict adherence to the procedures of enrolment, is necessary for the successful use of the system in future recognition activities (through more reliable comparison with data in the database of biometric references);

— Practical enrolments under the supervision of a trainer covering all the relevant areas;

— Information about certain groups of subjects that may have difficulties with enrolment (disabled, children or elderly people, etc.), explaining how these groups may be assisted in providing a good quality biometric reference;

— Processes that should be followed in exceptional cases, e.g. bandaged or missing fingers or more than five fingers in a hand;

— Explanations that can be given to subjects of the enrolment service regarding the purpose of the enrolment and subsequent recognition services;

— Interpretation of error and other messages from either the hardware units or computer screen, together with actions to be taken;

— Regular maintenance activities (such as cleaning of fingerprint sensor units or checks to confirm that systems are operating within specified operating limits);

— Security-related procedures, such as the examination of fingers for unexpected modifications and artefacts;

— Instructions to the officer or attendant regarding maintaining notes in relation to unresolved problems;

— Procedures for closing down the enrolment session in a secure manner.

7.2.4.2 Performance monitoring and correction

The operation of enrolment service should be monitored in accordance with the requirements agreed with the Enrolment Authority or other governance body. If the authority responsible for enrolment is not the same as the relying party (for the application of the biometric system for recognition of individuals), the testing of the end-to-end system (encompassing enrolment and recognition services) is strongly recommended.

The operation of the enrolment service can be monitored at a number of levels of granularity, e.g. on a service-wide level, by geographical area or at the finest level of granularity. Among the data that can be collected are

— The distribution of quality measures, average quality measures for different demographic groups,

- Time taken for enrolment transactions (mean, mode, and other statistically relevant measures), and
- Percentage of enrolment transactions that are not completed satisfactorily, e.g. measuring the FTER (7.2.3.4).

Automated alerts can be triggered when performance metrics exceed permitted bounds, calling for investigation of the causes and corrective action.

In any case, aggregated data should be reviewed periodically by an official of the operator (optionally, with representatives of the authority) to note patterns of change and investigate accordingly.

7.2.4.3 Service improvement and periodic audit

The operation of the enrolment service should be monitored at frequent intervals as part of a general system quality improvement scheme. Such a scheme may draw upon the results of research, either by the developers, the vendors of hardware and software, academia or by the Enrolment Authority itself. Operational data obtained from other deployments may give insights into ways of improving the authority's processes. On the basis of these inputs, changes can be piloted on a certain group of enrolment stations, using existing performance data as the baseline against which to judge the impact of such changes.

Periodic audits of the operation of the enrolment service may be held on behalf of the authority, either to verify the secure operation of the processes, review the performance of the service or to confirm that the service is being delivered in accordance with a published mandate. Other types of audit may be undertaken on behalf of specific regulators, focusing on aspects such as compliance with legal requirements (e.g. in respect of privacy or personal data protection).

The outcomes of such audits should be in the form of actionable recommendations on the operator or Enrolment Authority, with internal governance arrangements identifying a responsible owner of each recommendation. Although the service may have functions and components other than those relating to the collection of biometric data, only audit actions relevant to biometric aspects of the service are considered here.

The operator or Enrolment Authority should dispose of each recommendation by one of the following actions:

- Agreeing to make changes in the enrolment service, determining what development work is required (if needed), contracting for its development and deployment, and testing the system in its new configuration to confirm that it still operates in accordance with the original mandate as amended by the recommendation;
- Deciding on the basis of an analysis of the impact of following the recommendation that the service would be compromised operationally or financially, and reporting back to the auditor accordingly;
- By proposing alternative means by which the audit recommendations could be addressed.

7.2.4.4 Contract termination and re-assignment

The operator may have a license for an agreed period of time; or be contracted to deliver against a number of metrics in the SLA with the Enrolment Authority. Consistent failure in meeting these metrics may result in recourse to remedies defined in the contract or even trigger contract reassignment processes. (Note that performance well above that expected may be rewarded in a graded manner.) The operator should work with the Enrolment Authority to develop processes for the orderly handover of assets and the management of the transition to a new operator.

The existing operator may have modified processes – and trained attendants accordingly, developed innovative solutions (for which they may have sought intellectual property protection) or modified quality assessment software, in order to improve the enrolment service. The Enrolment Authority should create an inventory of these changes, and establish transitioning procedures (which may entail support by the existing operator) for transfer of these practices to the new operator. After handover, the previous operator may be required to support the service over a period to help resolve problems such as deterioration in the performance of the service.

7.2.5 Relying party interests

Relying parties rely on the enrolment service to provide a reliable, repeatable, secure and consistent service. If the enrolment service delivers outputs of a lesser or variable quality than defined in an SLA, this may impact adversely on subsequent verification and identification processes. Such impacts will inconvenience relying parties and subjects of the enrolment as, for example, the exception handling options are exercised more frequently.

Two types of dependent parties can be identified:

- Type 1: The Identity Provider, the authority responsible for storage of the biometric references relating to individuals who have been enrolled successfully under the enrolment service;
- Type 2: Relying party, the party which relies on biometric recognition as part of an application or service.

For the first type, the requirements include

- Receipt of a file from the enrolment service formatted in accordance with the interface agreement with the authority, with ensured integrity and fit for purpose;
- The biometric data in the file to be in a form that permits the provider to make checks on biometric and data quality, and if inadequate to seek further actions from the Enrolment Authority or operator;
- Biometric data are usable in the proprietary processes for de-duplication (if required) and conversion into biometric references;
- When the authority declares a failure to enrol, to ensure that the exception handling procedures are followed and relevant data are received by the Identity Provider in the appropriate format (7.2.6.8);
- Acceptance testing and periodic testing afterwards to ensure that an acceptable performance level is achieved and maintained;
- Testing carried out by the Identity Provider on its accumulated data may reveal opportunities for improvement in the enrolment service, necessitating discussions with the Enrolment Authority;
- New customers of this Identity Provider may have additional requirements on the enrolment service, again necessitating discussions with the Enrolment Authority.

For the second type of dependent party (the operator of an application or service), requirements on the service include:

- Assurance that the enrolment service has delivered enrolments (including exception handling) to a level of integrity consistent with its risk profile and operational requirements;
- Co-operation with the Enrolment Authority in the assessment of end-to-end performance of the application or service;
- Capability to make adjustments to the enrolment service as and when the relying party changes its own requirements (e.g. adding new modalities, changing quality parameters, adding or subtracting biographic data, responding to amendments to standards);
- Capability to make adjustments to the enrolment service as and when a new relying party is introduced.

A useful principle in the design of IT systems (as well as a requirement relating to personal data protection in some jurisdictions) is that data which is no longer required should be disposed securely. For biometric systems, it is recommended that when the subject is no longer using any applications of a relying party, for example, because they have left the organization and no longer need access to its buildings, an exit process should be started by a relying party working in conjunction with the relevant Identity Provider. This process should define time limits for retention of biometric and other data on the live system and on any archive system, ideally referencing legal requirements or research that justifies the data retention periods. Removal of subject data and access rights is needed to protect the business as well as the subject.

7.2.6 Developer interests

Many individuals are involved in an enrolment process, each of whom will need training and support: the subject of enrolment, an attendant to support the quality acquisition of the biometric feature, representatives of the operator of the system (working on behalf of the Enrolment Authority), enrolment centre managers (who may not be employees of the operator), and call centre personnel who may interact with subjects before and after an enrolment. Design and development best practices should be employed to ensure that the system performs as required by the Enrolment Authority and regulators, and that the activities of these individuals are optimised to deliver a successful biometric enrolment service for all enrolees. Similar considerations relate to business processes.

7.2.6.1 Pre-enrolment and scheduling

Subjects for biometric enrolment will look to the operator to provide enough information ahead of time to understand what is required of them. If this information is part of a marketing campaign, the messages should be consistent with other information.

A pre-enrolment process can be used to collect data via a web application prior to appearing for capture of the biometrics as a way of reducing onsite enrolment time. (This can be done in conjunction with online appointment scheduling, providing directions to the enrolment centre, information on what documents to bring with the subjects, etc.).

A helpline (designed for inclusivity) may be offered to enable the subject to phone into the enrolment centre with any questions on the day of the session, e.g. whether the onset of a cold should postpone the enrolment into a voice verification system. This needs to be staffed with assistants with appropriate training.

Allocation of timeslots should take account of the time required for

- Pre-enrolment formalities (e.g. checking of the identity credentials supplied by the subject),
- Mean time for biometric enrolment, as well as the allowable maximum time for such enrolment,
- Allowing time for any cleaning and/or maintenance of any devices, and
- Allowing time in between the enrolments of subjects and providing for rest periods for attendants to ensure that they remain vigilant throughout an enrolment session.

7.2.6.2 Identity confirmation

A key purpose of most enrolment processes is to establish an individual’s identity by linking one or more biometric characteristics with their biographical data. In these cases, it is important that the identity is verified prior to this binding. This is typically done by performing “identity proofing” by inspection (and sometimes capture) of identity documents, sometimes referred to as “breeder documents”. Examples of such documents include birth certificates, driver’s licenses, passports, etc. For some subjects, e.g. minors lacking relevant identity documents, special processes may be required. The strength of the binding between persons and their biometric data should be appropriate according to the requirements of the intended use.

Where the security policy mandates this, the authenticity of these identification documents should be confirmed with the relevant issuing agencies, as well as using equipment and procedures to verify the documents as not being forgeries or altered. Acquiring high quality digital colour copies of these identity documents may be a requirement for audit processes, assuring the integrity of the enrolment process against human error and collusion. Some legislation does not allow capturing copies of ID documents without a well-defined justification.

This may also be the opportunity for persons with medical conditions that limit the quality of the biometric to show evidence.

7.2.6.3 Verification system

Multiple modalities could be used; fall-back systems and requirements from inclusive design should be developed. The intended purpose of the verification systems which rely on the enrolled data should be taken into account when determining the requirements of the data to be enrolled:

- How often is/are the system(s) used?
- Do the subjects accept deviations from their usual behaviour?
- What are the necessary error rates to be reached?
- What is the perfect balance between comfort and better technical performance reached by potential discomfort for the subjects?

7.2.6.4 Enrolment system selection and physical design

Equipment and software may be available that differs from that used in verification systems, e.g. in being more robust against repeated mechanical impact, having additional functionality and feedback information to the subject to optimize the positioning of the biometric feature or characteristic, etc. Assessment tools may be available and could help in determining whether the enrolment system has captured and processed an image or signal of sufficient quality to allow for subsequent comparison with the features of other enrolees (if it is important that no duplicate identities are recorded), or for use later in a verification system.

The sensor equipment should be positioned in ways that optimize the collection and processing of high quality images. Where enrolment takes place at large numbers of sites, the hardware should be designed to be as independent of the environment as is possible. Environments should only be modified where the enrolment solution cannot be adapted to the existing environment. Each modality will also have associated recommendations in respect of the ambient environment, e.g. acceptable background noise levels for enrolment in a voice verification system, and requirements of uniform illumination for facial image collection.

The importance of good ergonomic design cannot be overstated, for example, taking account of naturally occurring variations (e.g. height, size, left/right handedness), and where necessary the needs of disabled subjects and attendants, and subjects who are not native speakers. The illumination setup should take into consideration potential reflections from glasses and skin, and variations in skin tone.

Further information relating to ergonomics and inclusivity issues is to be found in ISO/IEC TR 24714-1:2008. In designing the hardware for enrolment, attention should be paid to user friendliness, ease of keeping the equipment clean, etc.

Provision for accompanying persons may be required, e.g. a translator or personal assistant with measures to reduce the chance of any interference in the biometric capture process, e.g. by collection of an additional face, or even the attendant's face only, in a facial enrolment system.

7.2.6.5 Subject guidance

Since the enrolment session may be the first time that enrolees have been in contact with biometric equipment, the developer should develop an interaction protocol with the enrolee. This may include elements of direct face-to-face support.

Written material (provided in an inclusive and comprehensible manner) in the form of posters, information leaflets in multiple (major) languages, etc., and video clips of an idealised enrolment session in action are helpful.

Even simple issues can cause additional problems which could be avoided by planning ahead, e.g. if a subject and attendant sit facing each other, they should have a mutually agreed view of “left” and “right” if this is significant in the comparison process.

NOTE In a test of 300 adults, NIST demonstrated that in presentation of enrolment information for optical tenprint collection, verbal and video methods of communicating the process were approximately equivalent. In contrast, a poster representation of the same information led to significantly more errors, as well as taking substantially longer. Subjects who were informed verbally of the process tended to anticipate continued support through the enrolment.

7.2.6.6 Training for enrolment officers and attendants

Enrolment officers and attendants should be able to support the subjects in achieving the most effective enrolment through answering their questions and addressing any difficulties. Operators should recognize that training is needed that acknowledges the range of both cultural expectations and specific requirements of individual subjects. This should reduce the chance of litigation and bad publicity.

Since they are in continual contact with enrolees, there should be provision for officers and attendants to note any problems and opportunities for process improvement, with a procedure for reviewing these insights and thereby improving the training (and re-training) of other attendants. Such provision could be made through additional fields in the forms or screens detailing information captured during the enrolment.

As early in the process as possible, the operator (or the Enrolment Authority) should take steps to identify and resolve issues such as health and safety considerations and negotiations with trade unions.

Provision for the training of maintenance and other personnel should be made. The content of the training material and its delivery should be prepared recognizing that personnel may not be familiar with biometric systems. Further general guidance about training of enrolment officers is found in 7.2.4.1.

7.2.6.7 Security

In designing the enrolment processes, specifying the equipment, software and user interfaces, operating environment, etc., the designer of the system will take into account known security threats and vulnerabilities relating to the biometric modality. For example, it may be prudent to confirm that the fingertips of subjects enrolling on a fingerprint sensor are examined visually by the attendant to note whether there is anything untoward, such as damage, concealment or artefacts that partially or totally obscure the subject’s own fingerprints.

Similarly, any replacement hardware may be required to have tamper evident features, and also to be validated as genuine - for example by digital certificate verification of software. Some knowledgeable subjects may require reassurance that the equipment is genuine, untampered with, accredited and certified to ensure that their biometric features cannot be reused for unlawful purposes.

Other security threats are common to all forms of registration process, e.g. collusion of the attendant with the subject in proofing of the identity of the person. Attendants and enrolment officers should be trained accordingly. The security of data both at enrolment centres and over transmission networks to centralised storage or monitoring centres (one of the relying parties) needs to be considered, as well as the delivery and installation of software updates.

In the special case where subjects for biometric service supply their own biometric samples (e.g. submitting facial photographs when applying for a passport), the designer of the system should be aware of the significant risks that the biometric sample may not reflect accurately the biometric characteristics of the individual.

For facial photographs, the subject or photographer may have made alterations for e.g. vanity or cultural reasons, or for subversive purposes. Such changes may not be detected by human examiners or automated systems (indeed such changes may impact on ease of human comparison). These changes could include digital alterations such as

- Removal of blemishes and scars,
- Change or removal of background colour or shadows,
- The whitening or darkening of skin pigmentation,
- Changes to eye colour, and
- The manipulation of image dimensions to make the subject look thinner or fatter.

If the aim is to subvert the enrolment system, the subject could enrol under multiple identities or avoid detection through biometric watch list checks.

In addition, conversion of printed photographs to digital formats can cause degradation of the image or addition of artefacts.

7.2.6.8 Exception handling and timeout

Many enrolment processes have been used that require a specific number of presentations (e.g. three separate placements of a finger on a sensor within a set period), from which the highest quality image(s) is/are obtained for subsequent processing. In order to improve the quality of the image between successive presentations, position sensing software may give an indication to the subject of any adjustments to the presentation of the biometric feature (e.g. to press down harder on the platen, or move the finger), or group of presentations. Alternatively, the sensor can collect samples of a biometric feature for a fixed time duration taking facial images in quick succession for 20 s to 30 s followed by an image quality assessment that selects the best representation(s); or declares that an image of sufficient quality has not been obtained. Such differences will impact upon the process of enrolment and equipment suppliers should be consulted as to the appropriate measures to be taken.

Some modalities require a more time consuming enrolment, e.g., speaker recognition. In such cases, it may be considered to split the enrolment into several sessions or to run additional enrolments in subsequent successful verification sessions.

Even after inclusive design, a certain proportion of the population may still have difficulties in enrolment. Such subjects will have to be offered an alternative procedure. This may be

- Another instance of the same modality (e.g. further attempts at enrolment of a thumb if one or other of the index fingers is inadequate),
- An alternative modality (such as collecting an iris image), or
- An entirely separate, non-biometric process that meets the same requirements of security and usability.

Enrolling multiple modalities should also be considered to allow for more choices during verification. An individual may find one biometric modality easier to use or prefer it for other reasons. This also provides the ability to use the “alternate biometric modality” when the preferred one is not available or working well due to a temporary injury, for example.

Wherever practicable, these alternatives should not disadvantage the subject, for example, by offering an inferior level of service or functionality.

Designers of systems should be aware that exception handling or fall-back processes are potential sources of security weaknesses, and appropriate measures and training for any specialist staff are required.

7.2.6.9 Post enrolment verification

In many systems, once the enrolment has been completed satisfactorily, the enrolee may have an opportunity to experience the verification process. There is an assumption that this will help a knowledgeable subject to understand why they should follow the recommended verification process and be able to try again if the verification was unsatisfactory in any way. A full or partial re-enrolment may be needed if repeated failures in such verifications are noted.

In some cases, the enrolment encounter is also an opportunity to train the subject on the use of the associated verification system. (For example, if the enrolment is for a physical access system, it is useful to have one of the door reader units available at the enrolment site for instructional and habituation purposes.) The environment of this check could reflect the operational use, e.g. through having similar signage.

This can also confirm that the biometric sample has been correctly associated with the biographic and other data in the database or token, that the transmitted file has been processed correctly by the Identity Provider, converted into references, and stored in a manner accessible for applications.

7.2.6.10 Token production and secure delivery

In many cases, the enrolment system could also start the process of issuing a token containing either the biometric reference model or template, or a unique alphanumeric identifier pointing to the entry in the database that stores this reference element. In the use of the token the security and privacy of the biometric data should be protected (e.g. through access controls, cryptographic mechanisms, etc.). The delivery of the token should be secure and this could offer a further opportunity for biometric verification of the identity of the subject. Policies for this should be developed by the designer, whether using biometric procedures or not.

At periodic intervals, the operator of the biometric enrolment service should review the KPIs to ensure that the quality of the service is being maintained. This requires that such a list of indicators is constructed during the system design, procurement testing and piloting phases. Such a list should also reflect the experience of people with impairments.

As a minimum, operators, through their performance manager, may wish to confirm that the proportion of failed enrolments is stable (or decreasing) over time, and that the mean time for enrolment is not increasing. User satisfaction with the process could also be assessed, since a poor perception of a service (as reported in mass media or through direct contact with previous enrolees) is likely to impact adversely on the confidence with which enrolees embark on their own session.

For larger scale deployments, where there are several offices, comparison of the KPIs can reveal opportunities for improvement to the enrolment process, particularly if, e.g., this data are associated with the maintenance logs.

If the enrolment service is associated with one or more verification services, the performance characteristics of the latter can be examined in relation to the KPIs of associated enrolment offices and periods of time. Any degradation in verification performance should be investigated as it may be an early pointer to problems with the design of the enrolment procedures and/or unexpected ageing of the biometric features. Such investigation is amenable to more detailed analysis by age group, ethnicity, disability, gender, specific attendants, enrolment office, etc.

Gathering this data should be approved by the subject to secure handling procedures, especially if the original biometric samples are to be retained. Other legal checks may be necessary to ensure that there is no suspicion of this data being used in a discriminatory manner.

7.2.6.11 System maintenance and performance monitoring

At specified intervals, attendants should be required to verify the correct operation of the hardware and/or software which may involve cleaning of surfaces and initiating self-calibration procedures, checking that tamper-resistant seals are intact, etc. It is recommended that the date and time of such routine activities be recorded. On occasion, enrolment subjects may request that any systems that require physical contact with equipment be cleaned; it is good practice to provide suitable wipes for this purpose. Other specialist measures based upon recommendations of the system supplier and on testing and piloting of the system will also be followed, for example, in fingerprint systems where the software advises that fingers are too dry or too moist. Only materials approved for use by the operator should be used, and the system designer should provide advice on such materials.

In some environments (e.g. a hospital) hygiene may require frequent use of disinfectants. Equipment should be selected or modified (e.g. sealed) to allow for such cleaning without damaging the electronics.

A programme of secure replacement of hardware at appropriate intervals can be developed.

7.2.6.12 Testing and piloting

Biometric enrolment is only one of a set of processes that taken together provide a benefit to an organization. The relying party may want to satisfy itself that the initial performance of the enrolment subsystem satisfies the requirements of the end-to-end system(s) of which it forms a part, and that subsequently the effectiveness of the subsystem does not drop to a point where it places the operation of the end-to-end system(s) at risk. Modelling of such system(s) can help identify the key metrics of the enrolment subsystem and justify investment in monitoring and testing of enrolment. Appropriate testing procedures should be followed using a demographically representative group of test subjects, and procedures that are described in the multi-part standard ISO/IEC 19795.

Piloting is best carried out in a location and environment that is representative of the application.

7.2.7 Regulator interests

7.2.7.1 Regulation

The operation of a biometric enrolment service may be subject to laws relating to data protection, privacy, discrimination and disability. Regulators for respective aspects may have in place codes of practice or regulations which may specify how to implement and manage their requirements.

7.2.7.2 Completeness of the governance processes

A Regulatory Authority may have best practice recommendations or legally mandated provisions for the governance of some aspects of the operation of the service, e.g. the nomination of an official responsible for the personal data protection aspects of the service. There may be other provisions of codes relating to health and safety, disability discrimination, etc. with separate requirements. A complete governance structure will ensure that these are woven into a wider framework that ensures that the authority’s interests are fully protected.

7.2.7.3 Logging integrity and audit

Logging of activities relating to significant actions in the operation of the enrolment service (e.g. setting of parameters for biometric quality software or to identify the enrolment officer on duty in a specific session) should be secured to an appropriate security level. Auditing requirements may surface after the system has been delivered, and provision for collection of such data should be added to the management information (MI) system after the MI system has already been completed. This has implications for an initial design of a secure system architecture that is extensible through change control, as well as affordable.

7.2.8 Auditor interests

Measures should be in place to ensure that terms of reference are appropriate, that the data and information is available in sufficient (but not excessive) detail and presentation mode, that reports and recommendations are made to the correct functions in organisations and that follow up on these recommendations is in place.

8 Biometric enrolment capability development

8.1 General

Successful biometric enrolment is key to the operation of applications and services that provide benefit to organisations. Authorities responsible for the delivery of enrolment systems should design, deploy and operate these in a quality way. The Enrolment Authority should consider the following phases (noting that agile project approaches to delivery may be used as well):

— System definition — requirements capture from stakeholders;

— Procurement — the acquisition of the enrolment system;

— System design — the process of defining the architecture, components, modules, interfaces, and data for the enrolment system to satisfy specified requirements;

— Development — creation of a service (hardware, software, business processes, training of staff, etc.);

— Testing — an investigation conducted to provide stakeholders with information about the quality of the enrolment system;

— Piloting — a small scale deployment of the enrolment system that is representative of the full scale system (some piloting can be done during the procurement stages);

— Deployment — the transformation of the enrolment system from the development environment to the operational environment;

— Operation — the day-to-day use of the enrolment system;

— Maintenance — the modification of the enrolment system for preventive and corrective actions;

— Governance — monitoring and process improvement, together with audit;

— Cessation or withdrawal of service.

Enrolment processes will, in general, include proofing of identity — measures to ensure that the subjects are indeed who they claim to be (e.g. before binding the identity to the enrolled biometrics).

8.2 Enrolment station architecture and design

In designing a biometric enrolment capability, the architecture is an important consideration for many of the stakeholders. The architecture not only affects the initial procurement and deployment, it also affects decisions made downstream with regard to system maintenance, upgrade, etc. Some considerations for enrolment station architecture are given below.

— **Form factor.** Enrolment stations may take the form of a desktop workstation, an “across the counter” setup, a kiosk, or a mobile enrolment kit. Selection of the configuration will depend on the facility, space considerations, cost, and the enrolment process.

— **Ergonomics and Accessibility.** The configuration should take into consideration how the subjects and operators will interact with the equipment (and the operator) in terms of both comfort (physical and psychological) and facilitation of the best quality biometric capture. The configuration should minimize unnecessary discomfort for the subject and/or the operator.

— **Connectivity.** The enrolment station may operate in a stand-alone fashion, but is most often connected to a back-end system — either continuously or periodically. In either event, the station should be able to work in both an online and offline mode. The latter should support a batch upload capability (e.g. after collection in a remote area) or a “store and forward” capability. When the station includes a storage requirement, both the storage capacity and data security should be considered. The enrolment station/application should be able to be integrated within a services oriented architecture (e.g. via a Web services interface).

— **Security.** The enrolment station should incorporate security mechanisms to protect the confidentiality and integrity of the biometric data, as well as provide for auditing for incident investigation and non-repudiation purposes. Operator access controls are needed to protect access to functionality and data.

— **Standards based.** Enrolment stations should collect biometric data in a format that allows it to be interchanged (e.g. using one of the parts of the multi-part standard ISO/IEC 19794). Interface and messaging standards may also be applicable.

— **Flexibility.** The architecture of the enrolment application should be flexible so that it can be easily modified in the future as requirements and environments evolve over time. For example, it should provide configurable workflow, user interface, and policies/rules; support multi-modality (even if not implemented initially), and be vendor/device neutral to the extent possible.

8.3 System definition

A robust system to deliver an enrolment service should be designed in line with best practice in systems engineering. For a biometric system, the system definition may entail some or all of the following:

— Developing a system that meets the needs of the relying party in a legal, secure and cost-effective way;

— Taking into account at an early stage in the design and development process, non-functional requirements such as privacy-compliance, inclusivity (for the disabled, subjects who are not native speakers of the language(s) used in the country where enrolment sessions are held), user acceptance and usability, etc.;

— Interoperating with systems of other organisations in the same sector, to allow for future sharing of resources;

— Allowing for substitution of biometric hardware and software from other vendors, in case the suppliers retire their current components from the market, or the authority requires to re-compete the system at a future date.

9 Modality specific guidance

9.1 General

Information about best practices for successful enrolment of subjects is available from various sources. For example, experience gained in practical applications is distilled in data format standards in the multi-part standard ISO/IEC 19794, in particular in the informative Annexes.

There is a scarcity of publicly-available information about enrolment where more than one modality is used. An exception is the UK Passport Service enrolment trial for face, fingerprint and iris (May 2005), but the information in this report needs to be treated with some caution, since the trial predates much of the ISO standardization activity and experience with large scale enrolments for biometric visas and passports.

There is growing interest in enrolling subjects on mobile systems, and these require specialist design. In general, the quality of biometric data obtained from enrolments using mobile systems is likely to be inferior to that obtained in fixed systems where the environment can be controlled more consistently, computer systems with more processing power can be deployed, etc. However, the use of a mobile enrolment terminal may be the only practical way of collecting biometric data when subjects are unable or unwilling to travel to a dedicated facility. Further information is provided in Clause 10.

9.2 Facial biometric systems

9.2.1 General

This Clause discusses recommendations for co-operative enrolment in a dedicated facility. It uses the results of studies that were undertaken for the introduction of electronic passports and summarized in ISO/IEC 19794-5:2011, as well as Australian and US studies that quantified the negative impact that wearing glasses has on automated face recognition. Some of the advice is applicable to other situations, where the subject is not necessarily co-operating or when the relying party is unable to control environmental conditions and/or the behaviour of the subject.

9.2.2 Environment

Further detailed information about enrolment of facial biometric images can be found in 10.3. For specific applications specific guidance might be available. One example is the ICAO TR on Portrait Quality for passports and similar ID documents.

For subjects to be recognized using a facial biometric system in an application in which the environment is controlled and the subject co-operates in being recognized, images captured at enrolment and recognition should be as similar as is possible. More specifically, this means that:

- The pose of the face should be similar in terms of roll, pitch, and yaw angles. Conventionally, enrolment images are taken with a 'full-frontal pose' and the standard for passport photographs quotes a maximum rotation of no more than ±8 ° from frontal in roll. Research has shown that collecting a three-dimensional image may be beneficial if appropriate software is used. Alternatively, a number of images taken at different angles may assist in successful comparison if suitable software is available keeping in mind that research has shown that using a number of images taken at different angles may reduce the false reject rate (FRR) it may also increase the false accept rate (FAR).

- The illumination of the face should be similar, in terms of angle, diffusion, etc. In typical enrolment scenarios, the recommendation is for an even illumination with no visible shadows across the face.

- Eyes should be open and visible in both cases, since most algorithms use the centres of the eyes in photographs to reference the face.

- The expression in each image should be similar (e.g. if the expression in the enrolment image is neutral, it will be more difficult to compare it successfully using biometric software to a smiling facial image).

9.2.3 Pose and position

Although the emphasis has been on attaining similarity between enrolment and recognition conditions, many applications require that high quality images be captured with the subject posed in a standardised mode (facing the camera directly, with a neutral expression, evenly illuminated, etc.). In addition:

- The face should be uncovered with the subject not wearing headgear such as caps.

- Hair should not obscure the main part of the face.

- If the Enrolment Authority permits glasses during enrolment of facial biometric images and the subjects normally wear glasses, there should be no reflections of flash or lamps visible on the glasses. It is suggested that if the subject wears glasses, they may be asked to remove the glasses for the enrolment, if this doesn't prevent them from following visual instructions. Research has shown that this has negligible effect on the recognition while enrolling a subject wearing glasses may create similarity to other people wearing the same glasses, resulting in increased false accept rate (FAR).

- If the Enrolment Authority does not permit glasses during enrolment of facial biometric images, the subject should remove their glasses during the enrolment process. The subject should be informed that glasses have negative impact on the recognition in the intended application.

- A high resolution image should be captured — with the resolution often expressed in terms of the numbers of pixels between the eyes with a figure of 90 pixels offering good matching performance in studies supporting this requirement within ISO/IEC 19794-5. Guidelines for best practice from the Facial Identification Scientific Working Group (FISWG) recommend that cameras should be four megapixels or above of effective resolution, with the camera mounted for portrait mode capture.
- The camera should be positioned at the same height as the subject's eyes and positioned about two meters from the subject.
- The depth of field in the image should allow all visible parts of the face to be in focus.
- The background of the enrolment image should be such that the face and hair is easily distinguishable from it. Ideally there should be no shadows on the background surface and a uniform light colour with a plain smooth surface is recommended for certain applications.
- The camera settings for the images to be captured should be an industry acceptable format such as JPEG, and the highest possible quality setting should be used to minimize image quality loss and distorting factors such as image artefacts. The camera's digital zoom should not be used.
- Colour-balanced techniques should be used to avoid unnatural colours.

9.2.4 Ethnicity

Human facial images can provide demographic information, such as ethnicity, age, and gender.

Humans are generally found to be better at recognizing faces of individuals with similar demographic factors, e.g. ethnicity/race, age and gender. Machine algorithms will develop recognition tendencies similar to human visual system.

Images that are used to develop or train the facial recognition algorithms and systems should replicate as much as possible the operational conditions under which the system will perform in terms of the characteristics of the individuals in the images (ethnicity, race, gender, age, etc.) and the conditions under which the images were captured (illumination, pose, etc.).

Consideration should also be given to how the various parts of the task are distributed between humans and computers. If humans are used to deal with the exceptions, then these individuals should be trained and have a high level of expertise and competence in the additional verification and identification tasks that may be required to establish identity.

9.2.5 Improvements

Towards the end of the enrolment session, it is recommended that the subject is offered the opportunity to be recognized in a simulation of the application that the relying party intends to use. This familiarises the subject with the context of application and provides a measure of confidence that the enrolment has been carried out successfully. It allows for an on-the-spot re-enrolment if the simulation indicates problems with collection and/or encoding of the facial image. Ideally, the simulation should be carried out in a different environment, and not directly after the enrolment.

Usability studies can offer insight into improvements that can improve the performance of a facial biometric enrolment, improvements that can be made without imposing additional tasks on attendants or making changes in the environment. A NIST study on improvements in the collection of images at the US-VISIT primary line showed that all participants would be imaged correctly if five interventions were introduced:

- The cameras were changed from a webcam (unfamiliar to some travellers at immigration) to appear as a traditional camera;
- The camera should click as the picture was taken to provide feedback that the process had been completed;
- The camera should be positioned in portrait mode;

- — The attendant should face towards the subject (and the monitor) when adjusting the camera position;
- — Indicate to the subject where to stand (e.g. by placing images of footprints on the floor in front of the camera).

9.2.6 Glasses

Studies have quantified the negative impact that wearing glasses has on both automated and human operated facial recognition systems. Images with glasses can dominate the candidate list when subjects are wearing glasses. Some Enrolment Authorities do not permit glasses to be worn during image capture. However where Enrolment Authorities permit glasses to be worn during collection of facial biometric images and the subject normally wears glasses, the glasses should not be thick framed glasses, allowing a clear view of the eyes. There should be no light reflections on the glasses.

Australian and U.S. studies quantified the negative impact that wearing glasses has on automated face recognition and found the following:

- — Glasses are detrimental to automated face recognition. The Australian study also found that there was a negative effect of wearing glasses on human-operated face recognition.
- — When a subject wears glasses in one image, but not in another image, there is an elevated Type I error rate (that the subject will not be identified).
- — When a subject wears glasses and the images in the database contain subjects with glasses, the rate of false matches (Type II error) to others is elevated.
- — Presence of glasses increases similarity scores in imposter comparisons.
- — Images with glasses dominate candidate lists when probes are wearing glasses.
- — Imposter retrievals from the database exhibit higher levels of facial similarities when subjects are not wearing glasses.
- — Glasses can occlude facial features and interfere with eye location.
- — Glasses can be detected automatically with reasonable accuracy.

9.3 Fingerprint biometric systems

9.3.1 General

Four tiers of fingerprint enrolment have been discussed:

- — A full tenprint set of rolled and plain (alternatively known as flat or slap) prints from both hands — generally used only in law enforcement applications;
- — A set of plain tenprints — for other government and public sector applications;
- — Capture of images from a smaller number of fingerprints, with one or (preferably two, for resilience) flat prints — in general for commercial applications or where small closed user group identification is required;
- — Self-enrolment, e.g. by using a swipe sensor on a laptop or Smartphone.

The requirements for a successful enrolment in each of these use cases will depend to a great extent on the application. There will be trade-offs, such as those between high accuracy, low cost, and high speed throughput, so that an optimization of all three parameters for the specific context of operation will require careful planning.

Self-enrolment in an unattended environment is not recommended at present, except for situations where the security aspect of an implementation is secondary to convenience in operation.

Further detailed information about enrolment of fingerprint biometric images can be found in Clause 10 which relates to their enrolment in mobile systems.

9.3.2 Fingerprint capture considerations

High quality fingerprint systems generally enrol on optical scanners, for which there seems to be optimum moisture of the finger. Experience shows that overly moist fingers should be wiped with a cloth or paper towel. A number of strategies have been suggested for fingers that are too dry; asking the subject to breathe on the finger(s), sliding it across the forehead (or the side of the nose) to pick up traces of oil, or applying a surface dab of a skin-moisture lotion have all been used.

9.3.3 Single finger systems

Based upon experience gained from tests on 1 100 people in the autumn of 2006, and using three different sensors, Bausinger and Seidel[24] developed the enrolment procedures for fingerprints in German e-Passports. This example of a procedure which may be implemented differently in other countries consisted of the following:

— The standard process is the enrolment of two fingers, one from the right and one from the left hand.

— Fingers that are not available (e.g. due to injuries or disability) are not part of the standard process. It is up to the officer to decide if a finger is suited for enrolment or not.

— Attempts at enrolment follow a pre-defined order, starting with the index finger, then thumb, middle finger, and finally the ring finger (*designations are conventional*). In the study, 89 % of both right and left index fingers were enrolled, with the right thumb enrolled for 2,5 % and the left thumb enrolled for 2,8 % of subjects.

— A process is mandated, requiring the subject to try two fingers of one hand before the option to switch to the other hand is offered.

— From each hand, the best finger is selected for storage (according to the quality scoring method).

— From each fingerprint, three separate images are captured (by placing the finger three times on the scanner).

— For each image, the quality score is calculated.

— The system compares the three images against each other to avoid substitutions.

— The best image, according to comparison score, is selected for storage.

Quality assurance software is used in the following way:

— The software has to model the control flow so that the fingers are taken in the correct order;

— Pre-qualification of single fingerprints by NIST Fingerprint Image Quality (NFIQ) algorithm,

— There is always a series of three enrolled images per finger;

— The image with the best Bozorth3 reference comparison score average is chosen, rather than relying on NFIQ, since experience shows that the NFIQ values of fingers taken in succession are very similar. The first image was used for 21 % of fingerprint captures, whereas nearly 48 % of stored images came from the final of the three images for a single finger.

In order to reduce the subject's fears about the transmission of diseases and to improve the experience, fingerprint sensors should be regularly cleaned and disinfected. The image capture quality should also improve with regular cleaning. Enquiries should be made of the suppliers with regard to any religious connotations of using alcohol based cleaning solutions and whether any components contain materials known or suspected of causing allergies.

Although it is generally recommended that full size optical and semiconductor sensors are deployed, there are applications for which 'swipe sensors' such as those found on certain laptop computers can be specified. Initial guidance on specification of these devices is to be found in the NIST biometric specification for Personal Identity Verification[13].

9.3.4 Tenprint systems

Tenprint systems are mostly designed for large scale identification applications, often with de-duplication functionality at the Identity Provider's data centre to ensure that a database of single identities is maintained. ISO/IEC TS 20027[23] should be considered for tenprint systems. It should be considered that several sets of tenprints may be retained against a single individual's identity for operational reasons. In such cases, it is important to reduce the failure to enrol rate (FTER) to a minimum through:

- Optimised fingerprint capture hardware and environment (e.g. positioning of devices as mentioned above, cleaning contact surfaces in accordance with the suppliers schedule);
- Auto-capturing software which collects images of the fingerprints on an automated cycle, performing quality checks at each capture, and retaining the best images (either singly, if segmentation and sequencing software is reliable — or otherwise as a single image);
- Use of trained attendants who can address problems as they arise, share their experience in quality improvement circles and are motivated to obtain the best images;
- Upgrades to the system as improved quality analysis software, hardware, etc. are introduced.

The FTER (and associated operating parameters, such as total biometric collection time, quality measures) should be monitored at a number of levels of granularity, from the global statistics for all enrolment stations, to a specific enrolment unit operated during a specific shift of an attendant. It is important that these parameters are tracked over time, taking corrective actions in accordance with a predefined policy once critical parameters drift out of permitted bands.

The root cause analysis of problem areas is helped immeasurably if more detailed data are available relating distributions of quality scores to specific age and ethnic groupings, analysed by gender and quality scores from previous enrolments (if available). NFIQ/NFIQ 2.0 or quality data from proprietary quality software may be considered. Attendants may be encouraged to note any untoward circumstances in a free text file which can be collected as part of the metadata for the enrolment session.

In these systems, alternative biometric modalities may be collected, and tracking the KPIs related to these modalities (e.g. FTER, throughput time, quality scores) may support the root cause analysis of problems with tenprint collection.

9.4 Vascular (vein) authentication systems

9.4.1 General

Vascular authentication uses the blood vessel patterns of the vein in the subcutaneous tissue of the human body to discriminate between individuals. Vein patterns are read using near-infrared light. When a hypodermic vein is illuminated with near-infrared light, the reduced haemoglobin contained in the vein absorbs near-infrared light and the hypodermic vein creates a shadow on an image. Using image processing technology, the shadow pattern of the venous blood is processed from the captured image. The resulting patterns are used in biometric comparison, referencing features such as flow directions and bifurcations, or using the patterns themselves. In practice, veins in the hand, such as that those in a palm, the back of a hand, or a finger, are used for authentication because such these are easy to capture by a sensor.

9.4.2 Palm vein technology

Palm vein authentication systems generally use optical palm vein sensors for capture of the image pattern. Palm vein authentication is used normally without a cradle for the hand. However, especially for those who are not familiar with this modality, a cradle for the hand may be offered. If a cradle for the hand is used in enrolment, the cradle should be appropriately positioned so that it does not obstruct the imaging of the palm by the sensor. Guidance from the GUI or audio prompts is the most effective way to provide support for subjects in placing their hands correctly.

If there is only one hand available, then only the palm vein image or pattern from this hand will be enrolled. Quality check algorithms and/or a verification test after enrolment should be used in the enrolment process. The following should be considered when placing the hand on the sensor:

- Open the fingers lightly and position the hand over the sensor.
- Keep the hand horizontal over the sensor in the same way that you would when resting your hand on the surface of a desk.
- When viewing your hand from directly above, position it over the sensor such that the middle finger is aligned with the central axis of the sensor and the hand is straight.
- Try to keep the distance between palm and the sensor surface at an appropriate distance. Be careful not to bring the palm too close to the sensor surface.
- The recognition accuracy of the system is affected considerably by the quality of the enrolled palm vein pattern data. If the quality of enrolled data is not sufficient, there may be repeated false rejections even if the hand is positioned correctly for verification.
- The pattern of veins in the palm may not be enrolled correctly, and the recognition accuracy of the system may be impaired if:
  a) An adhesive or other type of bandage is applied to, or wrapped around, the palm;
  b) The palm is soiled, wet or injured.
- If problems are encountered when using the device on cold mornings, performance can be improved by warming the hands by for example, rubbing them together.
- Subjects should take care that their sleeves do not obscure any part of the palm.

9.4.3 Finger vein technology

Enrolment devices should be installed at a height between one’s chest and waist, so as to improve their usability. Finger vein patterns of the frontal side (fingerprint side) of a finger are enrolled. Biometric references from the veins of two or more fingers are enrolled to make at least one finger available for authentication should one be unavailable due to physical injury.

At enrolment, subjects can select fingers from both hands for enrolment. Index fingers, middle fingers and ring fingers are recommended for enrolment because these fingers can be positioned on the device in a steady position during enrolment or recognition.

Attended enrolment is essential to optimize the capture process and to enrol high quality references. Some subjects may place a fingertip on the image capture sensor in the belief that the device is a fingerprint sensor.

For each finger, more than three finger vein images are captured, with a quality assessment performed for each image, and repeating the transaction if the quality threshold has not been reached. Features are extracted from the images as candidates for inclusion in a biometric reference with features of the highest quality being selected.

Verification is recommended after enrolment to confirm that the reference is of an adequate and repeatable quality.

9.5 Iris biometric systems

ISO/IEC 29794-6:2015 defines iris image quality components and specifies the measurements, as well as acceptable values/thresholds, for each. Iris images, iris image quality records, and iris cameras should meet their respective requirements as outlined in the conformance clause of that document.

The first of several iris exchange (IREX) evaluations found that "iris recognition accuracy is highly dependent on the quality of the iris samples"[19]. IREX V provides guidance material for the proper collection and handling of iris images that comprises a poster[20], a final report[21], and a collection of instructional slides for iris camera operators[22]. IREX V outlines simple procedures for iris camera operators to follow to ensure that the images they collect are good quality.

For a high quality iris image collection, the poster demonstrates

- Eyes wide open,
- Iris centred and fully visible,
- Eyes looking at camera,
- Sharp, in focus,
- Few reflections or specular highlights, and
- Correct left and right labels.

For a low quality iris image collection, the poster demonstrates

- Occlusion of the iris — ask the subject to open their eyes wide,
- Eyeglasses — ask the subject to remove eyewear,
- Iris absent — align the camera with the eyes,
- Focus and motion blur — hold the camera still and at the proper distance from the subject,
- Background reflections on the iris — avoid bright scenes in front of the subject,
- Upside down iris image — align the camera properly with the subject,
- Improper gaze angle — ask the subject to look directly at the camera or fixation point,
- Iris close to the edge of the image — align the camera axis with the eye(s),
- Rotation — align the camera with the subject,
- Excessive dilation — increase ambient light and/or wait for drugs to wear off,
- Uneven illumination and/or low contrast — verify illumination is uncovered and working, and
- Patterned or coloured contact lens — ask the subject to remove the patterned contact lens or do not acquire the iris image.

The final report provides comprehensive recommendations for avoiding the collection of poor quality iris images. It decomposes common iris capture problems into three categories: those caused by the camera operator, those cause by subject behaviour, and those attributable to the iris camera. Examples of each problem detail the effect it has on the iris image, as well as how to mitigate each problem for capture of a high quality iris image. The summaries of recommendations are:

- Capture environment: Ideally, ambient lighting is diffuse and reflective of typical daytime conditions. If the iris camera does not block ambient sources of illumination, neither the subject nor the camera operator should be facing bright sources of light, such as the sun. Ensure all LEDs are emitting light.

- Prior to capture: Ensure the subjects have their eyeglasses or patterned contact lenses removed. Instruct the subjects to remain still and to face, and look at, the camera. The subjects may use their fingers to open their eyes wider if necessary.
- During capture: Ensure the camera is held still, is properly aligned with the subject's face, and that the operator's fingers are not obscuring any part of the camera lens or illumination array.
- Post capture: Ensure the iris is present and centred in the image, is not blurry, and is well illuminated. Ensure the upper-eyelid does not cross into the pupil and that the iris is not severely rotated (i.e. is greater than approximately 15°).

The collection of instructional slides for iris camera operators instructs readers to detect the most common problems that can occur during iris image capture. Though many commercial iris cameras produce high quality enrolment images in the majority of cases without human intervention, there are cases where recapturing of the images is necessary. When an enrolment officer is present in these cases, they can apply knowledge and judgment to the human review of iris images to determine whether recapture is necessary and, if so, how to mitigate the problem that cause recapture to be necessary. Like the poster, the instructional slides provide examples of high and low quality iris images, with particular emphasis and direction on how to mitigate issues that cause low quality iris images.

10 Mobile applications

10.1 Best practice guidelines

In 2009, NIST published best practice recommendations for the use of biometric mobile identification devices using fingerprint, face and iris modalities. Such devices could be used for a number of government or private sector applications, but the report focused on the needs of government organisations in the law enforcement, defence and homeland security sectors. Mobile systems are more challenging both for the device supplier as well as attendants, since the units usually are portable and robust, the environment of operation is less controlled and the design of hardware, software and enrolment processes has to take account of uncooperative subjects. Extensive experience has been gained in the use of mobile biometric capture systems on the battlefield.

The recommendations include advice on systems for verification and identification. In this report, the most significant guidance for enrolment is extracted and re-ordered.

The modality (or combinations of modalities) to be used and the specifications for the mobile identification device depend on the requirements of the recognition system. The report classifies these according to three levels of risk to public safety (other systems, not related to use of biometrics in support of public safety will have analogous risk profiles, and that in these cases, operators should use appropriate risk management practices to develop a categorization to suit their specific circumstances).

Table 4 — Recommended biometric modalities for US government use in mobile contexts

Risk to public safety	Use case example	Recommended capture of biometric features (facial images are used as supplementary to either of core modalities)		
		Face	**Finger**	**Iris**
Severe	Field enrolment into databases with applications where there is a high risk of loss of life or assets. Enrolment should achieve an equivalent level of quality as if conducted in a controlled environment using non-mobile devices	Multiple views of faces including full-face and three to five profiles. Attempts should be made to control backgrounds, expression and lighting where it is practical to do so.	All 10 fingerprints enrolled. Fingerprint sensors should meet EBTS Appendix F requirements to support human examiners making a full 10-print comparison	Both irises
		Multiple instances of each biometric feature may provide additional search capabilities Some applications may require multi-modal enrolment.		
Moderate	Mobile booking; cite and release when the violation is not high enough to ensure incarceration until arraignment without bail	Ideal lighting should be used; otherwise irises or fingerprints should be used additionally	6+	Both left and right irises
Mild	The biometric enrolment is of sufficient quality to allow later verifications (e.g. e-citations)		4+	Both left and right irises

An additional recommendation is for attendants making use of mobile hand-held devices to be authenticated to the device using two factor authentication, one factor of which should be a biometric modality.

10.2 Fingerprint systems

The objective should be to obtain high quality fingerprint images, with the standard recommending that images with NFIQ values of 4 or 5 should not be used for enrolment unless multiple capture attempts fail to yield a lower NFIQ value and the application requirements permit enrolling poor quality fingerprints. At an early stage during each enrolment the attendants should be provided with feedback (preferably on the mobile device) to alert them to instances of poor quality images.

Recommendations regarding the mobile devices include:

— The area of the sensitive surface should allow for the capture of a sufficient proportion of the fingerprint to allow for subsequent applications. For single finger images, the minimum size should be 12,7 mm wide by 16,5 mm height, although corresponding larger platen sizes up to 20,3 mm × 25,4 mm may be specified for more demanding uses.

— Single finger readers should have an integrated finger guide to optimize finger placement, and of sufficient length to allow capture of both the core of the fingerprint and the first crease of large thumbs.

— Optical fingerprint readers may have special coatings to improve the capture of dry fingers.

— Optical systems may have replaceable contact surfaces to avoid replacement of the total unit.

Considerations for the software include:

— The minimum scanning resolution is set at 197 pixels per centimetre (500 pixels per inch), with tolerances of 2 ppcm to 4 ppcm (5 ppi to 10 ppi) depending on the application.

- The compression algorithm should be WSQ for the 197 ppcm (500 ppi) resolution with a maximum compression ratio of 10:1.
- If the application requires a higher resolution scanner, then 394 ppcm (1 000 ppi) devices are available, although for these the recommended compression algorithm is JPEG2000[18].
- For the least demanding applications, direct minutiae extraction using a certified minutiae extraction algorithm is allowed. For all other uses, an image of the fingerprint should be transferred to the application.
- Software should be developed, with a user interface to show the subjects of enrolment or the attendants how to move fingers or hands to optimize the capture of good quality images, moving them left/right, or up or down as necessary. A displayed image of the fingerprints may be of use in some cases.
- Provision of a check on the quality of the image, using a combination of
  - a) Image size,
  - b) Measurements of light or dark parts of the image,
  - c) Numbers of minutiae,
  - d) Location of the core, and
  - e) Image quality scores using NFIQ.
- Design for auto-capture of fingerprint images, so that the on-board software can continually monitor quality on each scan frame, collecting the image once a quality threshold has been exceeded.

Determination of how many, and which fingers to capture depends primarily on the requirements of the recognition system, but factors to consider include:

- Configurability of the device to cater for different numbers of fingers, if the enrolment is undertaken for different authorities.
- If all ten fingers are not mandated, the default is to include both index and middle fingers of both hands, with an observation that in future the middle fingers will be the default for two finger capture, since these offer better matching than the traditionally used index fingers.

In operation of these devices, the attendant should note:

- Some systems do not work in full sunlight or under other intense sources of illumination;
- Any advice regarding periodic cleaning of surfaces, using the correct cleaning method, while avoiding touching the platen unnecessarily;
- Where multiple instances of fingerprints have to be collected (e.g. if a single fingerprint reader is used to collect a number of images of fingertips) the attendant should pay particular attention that the correct sequence is followed.

10.3 Facial image systems

Of the three modalities applied in a mobile setting, the enrolment of a good quality facial image, of sufficiently good quality to give reliable results at a later time is by far the most challenging. Indeed, it is not recommended as the primary biometric modality - used for automated comparison - in any of the use cases in Table 4. Nevertheless, a well-captured facial image at enrolment can be of considerable value in subsequent face comparison by human operators, who can contribute to the recognition system with far less training than that required to visually match fingerprints.

The enrolment of images that are useful for both automated and human comparison at a later time requires an integrated solution consisting of a well-designed camera and a user interface (possibly with custom designed fill-in illumination). Additionally, it requires quality assessment software with feedback to well-trained operators of the mobile device.

Although a similar requirement on quality is placed on systems collecting facial images there is no equivalent of the non-proprietary NFIQ fingerprint quality standard. Nevertheless, the same recommendation is made for feedback to attendants as to quality, albeit using a proprietary system, to alert them to unsatisfactory aspects of the lighting, expression, pose angle, centrality of image, background, etc.

The basic camera requirements are similar for all three risk levels in the Table above, with the exception of the inter-eye distance which is specified as more than 90 pixels for the ‘mild risk’ level, and more than 150 pixels for the ‘moderate’ and ‘severe’ use cases.

Mobile biometric systems using facial recognition are generally used with a camera-to-subject distance of between 60 cm and 200 cm (preferably operated at the longer end of this range), and with the lower end requirement also used to verify the identity of the attendant at the start of an enrolment session.

If there is an intention to use automated face comparison as part of a recognition process, it is recommended that the requirements for a successful enrolment are developed alongside those in the recognition process. Design of the user interface to the camera unit (which is likely to be integrated with other modalities in an enrolment device) should take account of the guidance in ISO/IEC 19794-5:2011. Markings and information on the visual display may

- Help with centring of the face and alerting to excessive pose angles,
- Display the results of a quality assessment, highlighting gross unevenness in illumination across the face and other causes of the eyes not being properly imaged,
- Warn of clutter in the background,
- Remind the operator of the unit to make any manual adjustments, and
- Advise on taking further images in the profile.

The design of supplementary illumination in cases of highly directional or uneven lighting, or in low ambient lighting situations, will be critical, and the NIST recommendations of fill-in Xenon flash or LEDs may not be sufficient.

10.4 Iris systems

Collection of iris images (whether singly or as a pair) is a useful supplemental modality in mobile systems to cater for instances of problematic enrolments of fingerprint images and for other specialized recognition systems, such as those using a co-operative ‘iris-on-the-move’ verification service. For enrolment, both eyes should be enrolled, even if the recognition application requires just one eye for verification.

The small size of the iris and the requirement to illuminate it in the infrared dictates the use of a camera customised for this application. The specialized lighting (Light Emitting Diodes) should allow imaging in range of wavelengths of 700 nm to 900 nm, with at least 35 % of the power output of the illuminator in the 800 nm to 900 nm sub-band, and with limits on the maximum irradiance specified by appropriate health and safety standards.

In the absence of a standard for the assessment of the quality of the image, designers should select a proprietary implementation which should be tested against the algorithms used in the comparison part of the recognition system.

To avoid the impact of camera movements (‘camera shake’) and to collect the requisite biometric data from the iris, the NIST recommendations offer the following minimum specifications for resolution and exposure for the three use cases outlined in 10.1.

Table 5 — Specifications for iris recognition in US government mobile applications

Use case	Iris diameter in true, non-upscaled pixels	Exposure time
Severe	>210	<10 ms
Moderate	>170	<15 ms
Mild	>140	<33 ms

Additional requirements on the iris imaging in the camera are:

— Capture distance from camera to iris > 10 cm;

— ‘Capture volume’, the tolerance in horizontal, vertical and axial dimensions of the position of the iris:

a) For single iris systems: 11 mm width × 9 mm height × 20 mm depth;

b) For dual iris systems (which take both at the same time): 9 mm width × 14 mm height × 20 mm depth;

c) If the camera uses a mechanical system of positioning the head in relation to the camera (e.g. providing a head rest and head forehead stop), the depth volume specification allows for a minimum of 12 mm;

— The imaging of the area surrounding the iris should allow for margins to the left and right of the iris of half the iris diameter, and above and below the iris of one quarter of the iris diameter;

— Sensor signal-to-noise ratio should be greater than 36 db.

In order that images are interoperable with other recognition applications, it is recommended that the images are formatted in the rectilinear system as described in ISO/IEC 19794-6:2011, noting that the standard has been amended several times.

Annex A
(informative)

Checklist of activities related to biometric enrolment

A.1 Introduction

This listing is offered as a service to those parties involved in the delivery and operation of biometric enrolment systems and services. It points to some of the activities described in more detail in the relevant sections. Those intending to launch new deployments may wish to develop their own checklists using this format as a guide.

As a minimal response, the official(s) responsible for each phase of the enrolment service should sign and date against each action line, to indicate that the specific action has been considered and a decision taken. Officials may wish to provide further information, referencing against each action line any other relevant documents.

A.2 Activities during the procurement phase

Number	Name	Clause in this document	Action
1	Capture of legal provisions relating to privacy, protection of personal data, accessibility, security, etc. (at a high level)	7.2.2.2	
2	Determine remit of regulators of enrolment systems and whether systems should be developed in accordance with regulations or certified	7.2.7.1, 7.2.7.2	
3	Enrolment Authority and potential operators to consider end of contract conditions	7.2.3.9, 7.2.4.4	
4	Definition of specialist technical terms in the contract, especially if internationally standardised terms are not to be used	7.2.2.3	
5	Contract to include service improvement actions	7.2.4.3	

A.3 Activities during the design and development phases

Number	Name	Clause in this document	Action
1	Development using best practices in systems engineering	Clause 8	
2	Capture of legal provisions relating to privacy, protection of personal data, accessibility, security, etc. (Detailed level)	7.2.2.2, 7.2.3.1	
3	Requirements capture in respect of non-repudiation	7.2.3.1	
4	Authority to ascertain whether there are likely to be requirements for retention of biometric data (and associated biographic data and metadata) for research, whether for future services or to measure the end-to-end performance of the dependent application. If needed, to set up an ethics committee	7.2.3.5, 7.2.3.8	

Number	Name	Clause in this document	Action
5	Establishing governance procedures and development of audit functions and logging which support these	7.2.2.2, 7.2.7.2, 7.2.7.3	
6	Addressing of inclusivity issues, provision of facilities for personal attendants (and assistant animals)	7.2.2.3, 7.2.3.1	
7	Actions to protect information revealed by the enrolment process	7.2.2.2, 7.2.2.3	
8	Establishment of principles for achieving the best quality for the target application, consistent with constraints of time allowed for enrolment, costs of arranging the enrolment and availability of equipment and attendants	7.2.3, 7.2.4	
9	Development of procedures for biometric subjects (hereafter termed subjects) to enable them to perform task quickly and with few errors as possible	7.2.2.3, 7.2.2.4	
10	Determination of specific demographic groups who may cause problems during enrolment	7.2.2.3	
11	Determination of the SLA between Enrolment Authority and operator of the enrolment service	7.2.2.3, 7.2.4.2	
12	Strategy for the remedial measures to be undertaken if the provisions under the SLA between Enrolment Authority and operator of the enrolment service are not met	7.2.2.3, 7.2.3.9, 7.2.4.4	
13	Determination of the requirements of the application(s) which will depend on the enrolment and which relate to a secure, consistent and robust enrolment	7.2.5, 7.2.6.4	
14	Architectural considerations in enrolment station design	8.2	
15	Selection of the enrolment system and any assessment tools	7.2.6.4	
16	Environmental design of the enrolment facility	7.2.6.4	
17	IT interconnection	8.2	
18	Formatting of biometric and biographic data into files for transmission to data centre/database, and receipt of acceptance or requests for further action from the Identity Provider	Clause 5, 7.2.5	
19	Development of an interaction protocol of the subject with the enrolment process	7.2.6.5	
20	Development of training programme for enrolment officer	7.2.4.1, 7.2.6.6	
21	Development of training programme for support staff	7.2.6.6	
22	Development of training programme for attendants	7.2.4.1	
23	Design of the security services, taking account of specific vulnerabilities of biometric systems	7.2.6.7	
24	Determine the number of attempts at enrolment during a session, or the maximum duration before abandonment of a session	7.2.6.8	
25	Design and development of a fall-back solution should the main enrolment system fail	7.2.6.8	
26	Integration of a verification service directly after the completion of enrolment	7.2.6.9	
27	Production of tokens using references obtained at enrolment, and secure delivery to the subject	7.2.6.10	

Number	Name	Clause in this document	Action
28	Development of a performance monitoring system to measure KPIs	7.2.6.11	
29	Development of testing procedures for enrolment	7.2.2.3, 7.2.6.12	
30	Development of a system acceptance approach, through modelling of the integrated service (with authorities managing the dependent recognition services), and piloting the tests	6.2.6.12	
31	Enrolment Authority and operator to determine end of contract handover terms	7.2.3.9, 7.2.4.4	

A.4 Activities during testing phase

Number	Name	Clause in this document	Action
1	Testing of user satisfaction	7.2.2.4	
2	Conformance testing of the formatting and transmission of biographic and biometric data	Clause 5	
3	Piloting and development of an enrolment process	7.2.6.12	
4	Acceptance testing	7.2.6.12	

A.5 Activities during deployment phase

Number	Name	Clause in this document	Action
1	Determine whether a certification of the service is required and ensure that testing is undertaken	7.2.3.2	
2	Determine what technical and system information is to be made available publicly as part of the marketing and awareness-raising campaigns	7.2.2.4, 7.2.6.5	

A.6 Activities during biometric enrolment of subjects

Number	Name	Clause in this document	Action
1	Establishing the information which can be collected ahead on the web ahead of the enrolment, and setting up a helpline to support persons with disabilities	7.2.2.3, 7.2.6.1	
2	Provision of legal information to subjects	7.2.2.1, 7.2.2.2	
3	Collection of information from subject regarding accessibility issues	7.2.2.3	
4	Development of the scheduling of appointments for enrolments	7.2.6.1	
5	Determination of biographic identity ahead of enrolment	7.2.6.2	
6	Training attendants and enrolment officers	7.2.4.1	
7	Activation of the exception handling procedure if a failure to enrol is declared	7.2.6.8	
8	Receipt of the acceptance check from data centre/database or request for enrolment centre to take remedial actions	Clause 5, 7.2.5	

A.7 Activities during operation of enrolment systems

Number	Name	Clause in this document	Action
1	System maintenance procedures	7.2.6.11	
2	System performance monitoring and correction actions	7.2.6.11	
3	Enrolment Authority responding to change requests from Identity Providers and relying parties	7.2.5	
3	Service improvement actions	7.2.4.3	

A.8 Checklist for auditors of enrolment systems

Number	Name	Clause in this document	Action
1	Confirm that appropriate information is being made available to subjects	7.2.2.1	
2	Check that legal provisions relating to privacy, protection of personal data, accessibility, security, etc. captured at the detailed level during the design and development phases have been implemented and are being adhered to in operation, alerting the Enrolment Authority as to imminent changes in the legal framework	7.2.2.2, 7.2.3.1	
3	Ensure that audit provisions under the SLA between Enrolment Authority and operator of the enrolment service are in place	7.2.3.3	
4	Periodic audit of the service	7.2.4.3	
5	Integrity of the logging and audit processes	7.2.7.3	
6	Auditor’s perspective on a successful biometric enrolment	7.28	

Annex B
(informative)

Examples of good and bad face enrolment pictures

This annex provides examples of good face pictures for enrolment in Figure B.1 and examples of bad face pictures in Figures B.2 to B.10.

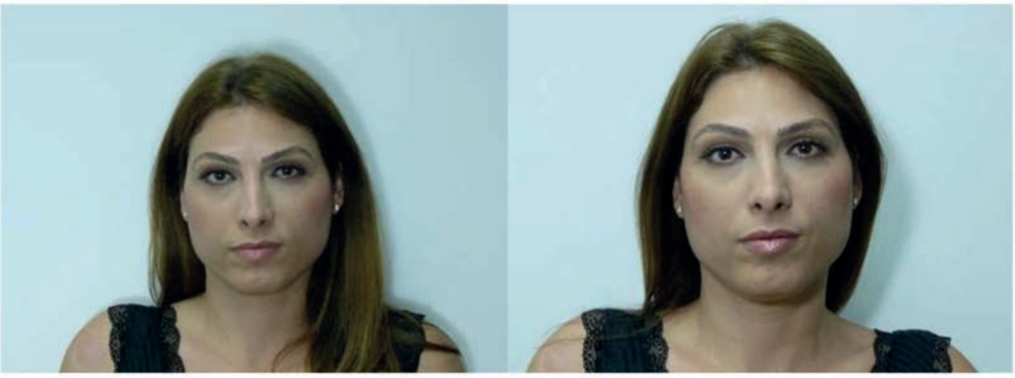

Figure B.1 — Samples of good images

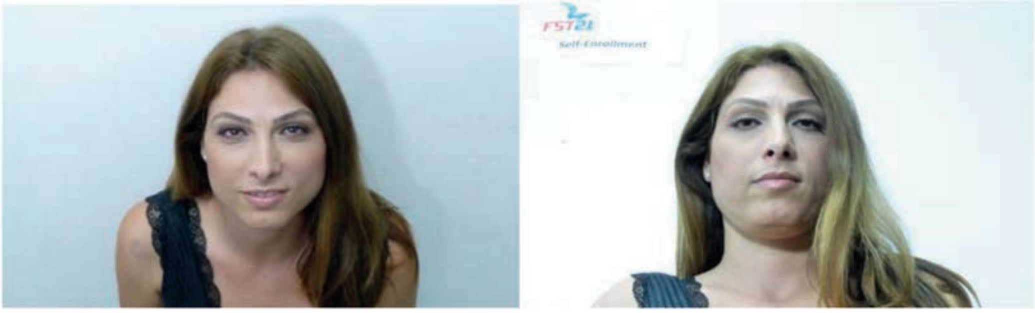

Figure B.2 — Persons looking up and looking down to the camera

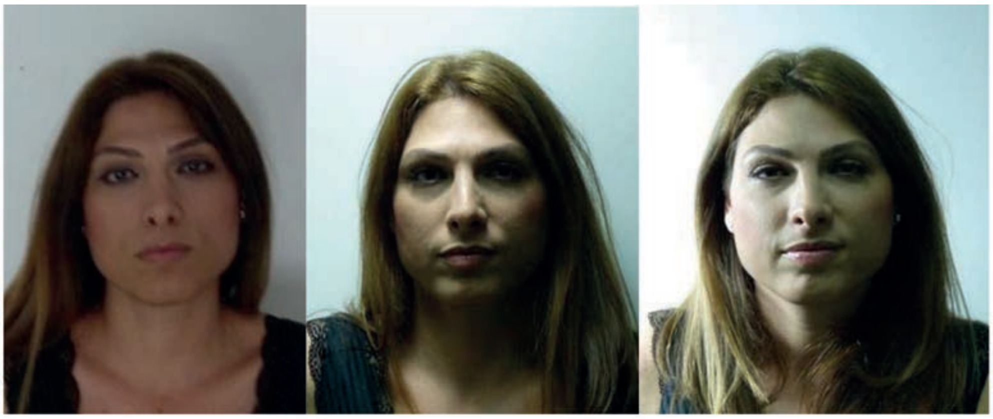

Figure B.3 — Dark face, dark eye socket, and uneven light

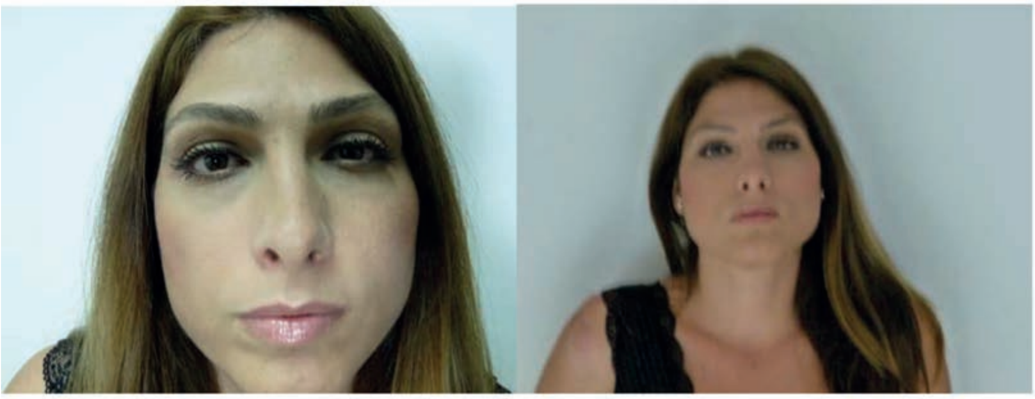

Figure B.4 — Fish eye and blurry image

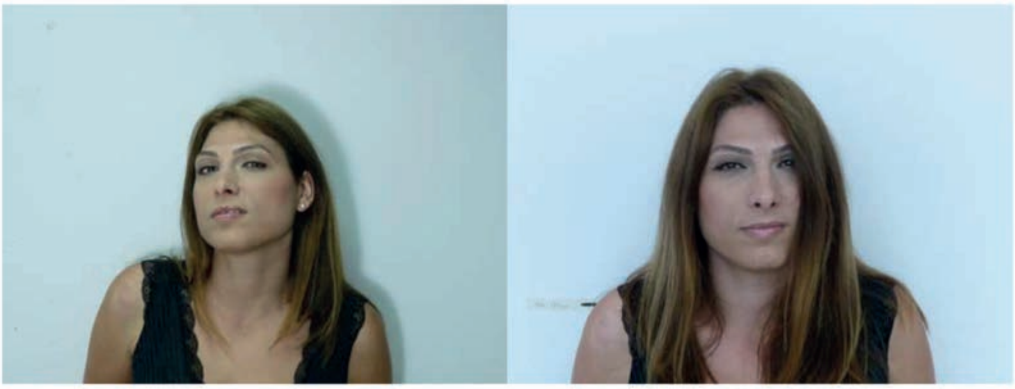

Figure B.5 — One ear only visible, and hair covering the face

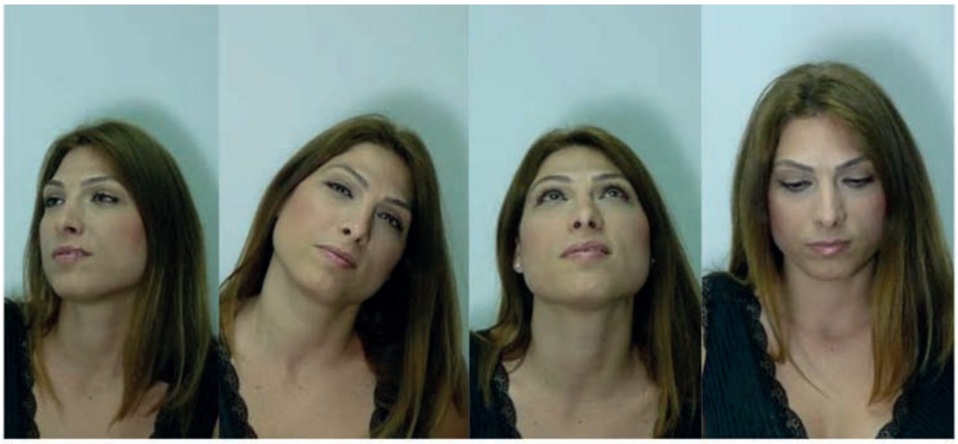

Figure B.6 — Faces not frontal

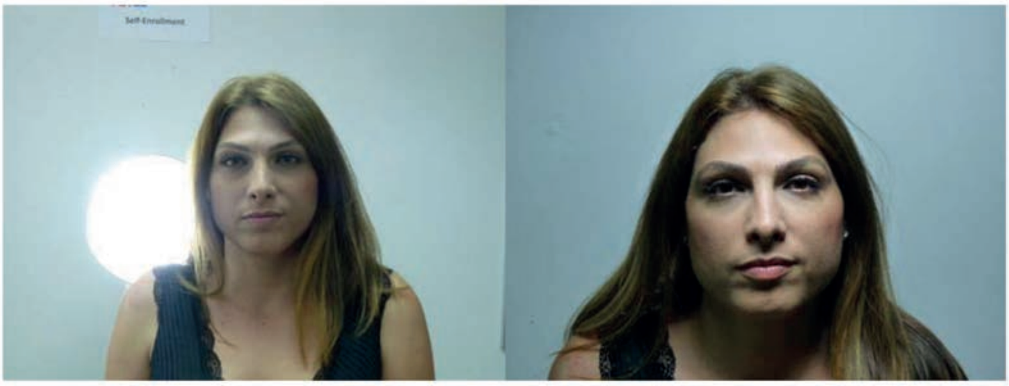

Figure B.7 — Backlight and hotspot

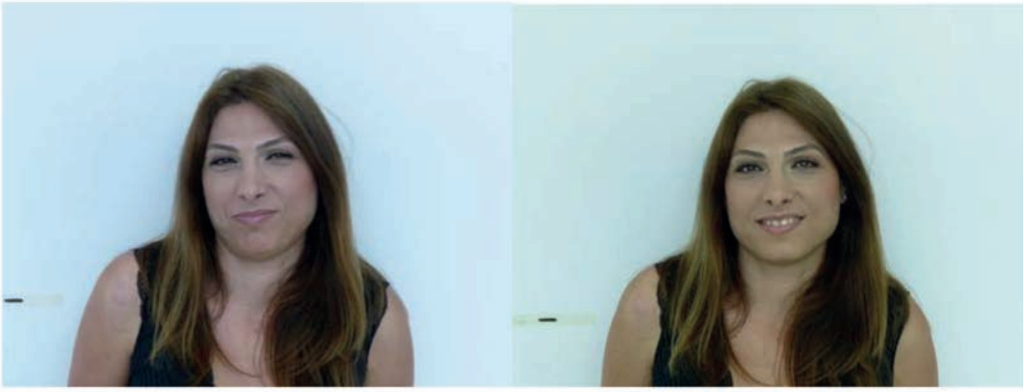

Figure B.8 — Non-neutral expression

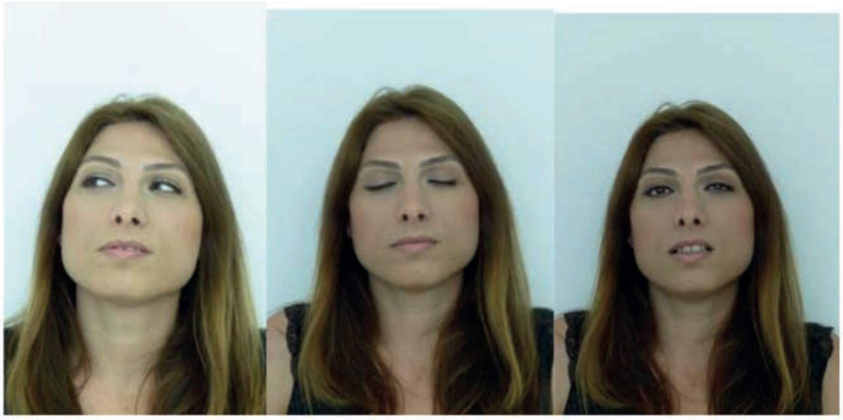

Figure B.9 — Subject not looking to the camera, subject with closed eyes, and subject with opened mouth

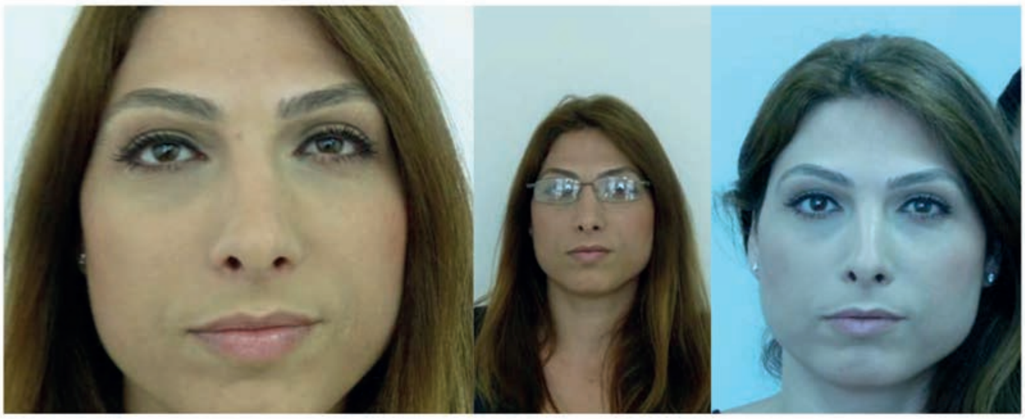

Figure B.10 — Cropped face, reflections on glasses, several people

Bibliography

[1] ISO 9241-11:1998, *Ergonomic requirements for office work with visual display terminals (VDTs) — Part 11: Guidance on usability*

[2] ISO 9241-210:2010, *Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems*

[3] ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

[4] ISO/IEC 19794 (all parts), *Information technology — Biometric data interchange formats*

[5] ISO/IEC 19795 (all parts), *Information technology — Biometric performance testing and reporting*

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

[7] ISO/IEC/TR 24722:2015, *Information technology — Biometrics — Multimodal and other multibiometric fusion*

[8] ISO/IEC 29794 (all parts), *Information technology — Biometric sample quality*

[9] Tabassi E. Fingerprint Image Quality, NISTIR 7151 (August 2004) http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905710

[10] Tabassi E., & Grother P. Quality Summarization. Recommendations on Biometric Quality Summarization across the Application Domain, NISTIR 7422 (May 2007), http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=51149

[11] Theofanos M. *et al* Automated Face Acquisition NISTIR 7540 (September 2008), http://zing.ncsl.nist.gov/biousa/docs/face_IR-7540.pdf

[12] National Institute of Standards and Technology. Usability & Biometrics, Ensuring Successful Biometric Systems (June 2008), http://zing.ncsl.nist.gov/biousa/docs/Usability_and_Biometrics_final2.pdf

[13] Grother P. Biometric Specifications for Personal Identity Verification, NIST Special Publication 800-76-2, July 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf

[14] Orandi S., & Michael McCabe R. Mobile ID Device Best Practice Recommendation Version 1.0, NIST Special Publication 500-280 (August 2009), http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=903169

[15] Rahmun F. Biometric Enrolment for the European Visa Information System (VIS). German Experiences. http://www.icao.int/Meetings/AMC/MRTDsymposium2010/Documentation/Rahmun.pdf

[16] Schumacher G. Recognition Performance in the Case of Juvenile Fingerprints, IBPC 2010 conference, https://www.nist.gov/sites/default/files/documents/2016/11/30/schumacher_guenter_juvenile_fingerprinting.pdf

[17] Drahansky M. Fingerprint Recognition Influenced by Skin Diseases, *International Journal of Bio-Science and Bio-Technology*. 2010 December, **2** (4), http://www.sersc.org/journals/IJBSBT/vol2_no4/2.pdf

[18] NIST Special Publication 500 –289: "Compression Guidance for 1000 ppi Friction Ridge Imagery”, http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.500-289.pdf

[19] NIST IREX V. https://www.nist.gov/itl/iad/image-group/irex-v-homepage

[20] IREX IRIS EXCHANGE Guide to Capturing Iris Images, June 12, 2014, https://www.nist.gov/sites/default/files/documents/2017/02/23/irex_v_poster_20140612.pdf

[21] QUINN G.W. IREX V Guidance for Iris Image Collection NIST Interagency Report 8013, July 2, 2014, http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=915751

[22] IREX V – BEST PRACTICES FOR IRIS IMAGE CAPTURE TRAINING GUIDE SLIDES FOR ENROLLMENT STATION OPERATORS. June 12, 2014, https://www.nist .gov/sites/default/files/documents/2017/02/23/irex_v_slides_20140612.pptx

[23] ISO/IEC TS 20027, *Biometric interoperability profiles – Best Practises for slap tenprint capture*

[24] BAUSINGER O., & SEIDEL U. Next Generation German e-Passport Fingerprint Enrolment – Quality vs. Time. NIST Biometric Quality Workshop, October 31, 2007. https://www.nist.gov/sites/default/files/documents/2016/12/07/bausinger_seidel_v10.pdf

[25] ISO/IEC 30107 (all parts), *Information technology — Biometric presentation attack detection*

ICS 35.240.15

Price based on 55 pages