PD ISO/IEC TR 29196:2018

BSI Standards Publication

# Information technology — Guidance for biometric enrolment

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 29196:2018

# National foreword

This Published Document is the UK implementation of ISO/IEC TR 29196:2018. It supersedes PD ISO/IEC TR 29196:2015, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/44, Biometrics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 51056 4

ICS 35.240.15

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2018.

**Amendments/corrigenda issued since publication**

| Date | Text affected |
|---|---|

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 29196:2018

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)

Documents
Document Sharing Hub
© ISO/IEC 2018

Full document details: PD ISO/IEC TR 29196:2018

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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



© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 29196:2018

# Contents

Page

**Foreword** ..... **v**
**Introduction** ..... **vi**
**1 Scope** ..... **1**
**2 Normative references** ..... **1**
**3 Terms and definitions** ..... **1**
**4 Abbreviated terms** ..... **3**
**5 Role of enrolment in a biometric system** ..... **3**
**6 Stakeholders and approaches for enrolment** ..... **6**
6.1 Enrolment stakeholders ..... 6
6.2 Enrolment approaches ..... 9
**7 Stakeholder interests** ..... **10**
7.1 Key observations ..... 10
7.2 Best practices and recommendations ..... 11
7.2.1 General ..... 11
7.2.2 Subject interests ..... 11
7.2.3 Enrolment Authority interests ..... 14
7.2.4 Operator interests ..... 22
7.2.5 Relying party interests ..... 25
7.2.6 Developer interests ..... 26
7.2.7 Regulator interests ..... 31
7.2.8 Auditor interests ..... 31
**8 Biometric enrolment capability development** ..... **32**
8.1 General ..... 32
8.2 Enrolment station architecture and design ..... 32
8.3 System definition ..... 33
**9 Modality specific guidance** ..... **33**
9.1 General ..... 33
9.2 Facial biometric systems ..... 34
9.2.1 General ..... 34
9.2.2 Environment ..... 34
9.2.3 Pose and position ..... 34
9.2.4 Ethnicity ..... 35
9.2.5 Improvements ..... 35
9.2.6 Glasses ..... 36
9.3 Fingerprint biometric systems ..... 36
9.3.1 General ..... 36
9.3.2 Fingerprint capture considerations ..... 37
9.3.3 Single finger systems ..... 37
9.3.4 Tenprint systems ..... 38
9.4 Vascular (vein) authentication systems ..... 38
9.4.1 General ..... 38
9.4.2 Palm vein technology ..... 39
9.4.3 Finger vein technology ..... 39
9.5 Iris biometric systems ..... 40
**10 Mobile applications** ..... **41**
10.1 Best practice guidelines ..... 41
10.2 Fingerprint systems ..... 42
10.3 Facial image systems ..... 43
10.4 Iris systems ..... 44
**Annex A** (informative) **Checklist of activities related to biometric enrolment** ..... **46**

Documents
Document Sharing Hub

© ISO/IEC 2018 – All rights reserved


Full document details: PD ISO/IEC TR 29196:2018

**Annex B** (informative) **Examples of good and bad face enrolment pictures** ..... **50**
**Bibliography** ..... **54**


© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018

# 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.

© ISO/IEC 2018 – All rights reserved


Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018

# 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.


© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018

# 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

Documents
Document Sharing Hub

© ISO/IEC 2018 – All rights reserved


Full document details: PD ISO/IEC TR 29196:2018

**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


© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018

**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.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018

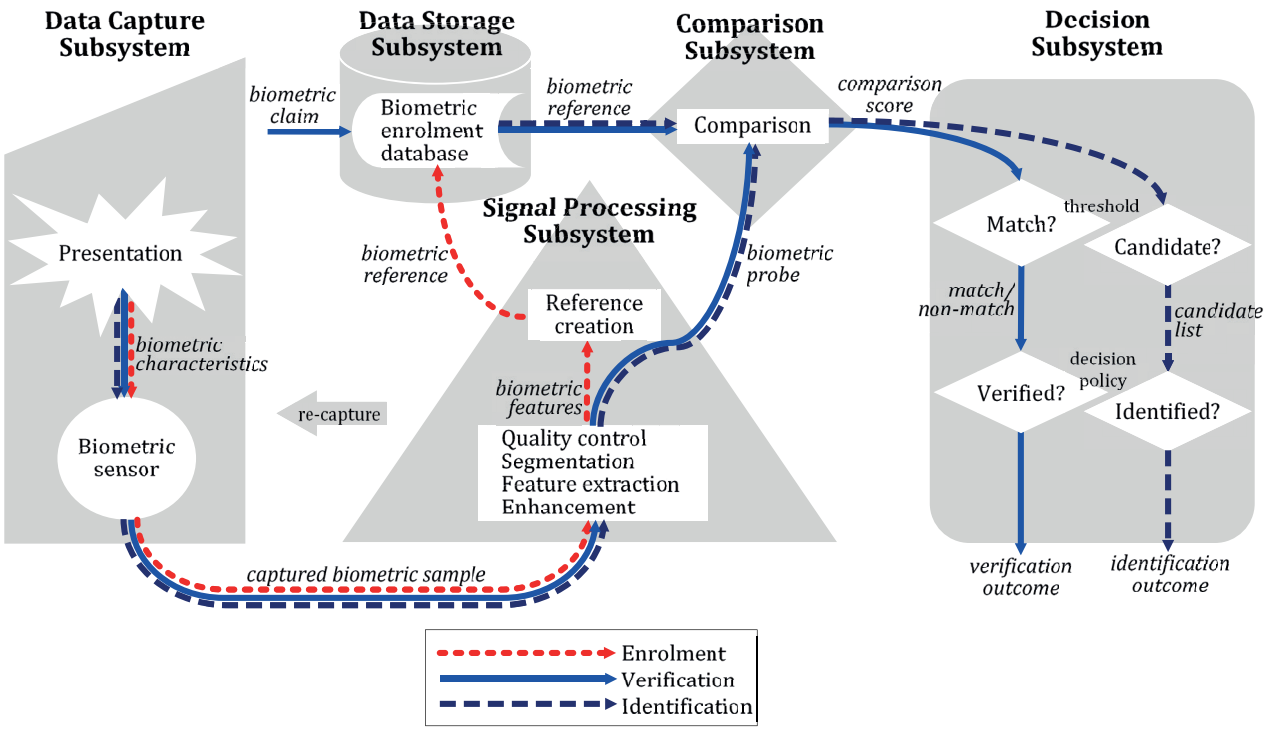


**Figure 1 — Components of general biometric system**

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


© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018

— *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,

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018

— 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.


© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018

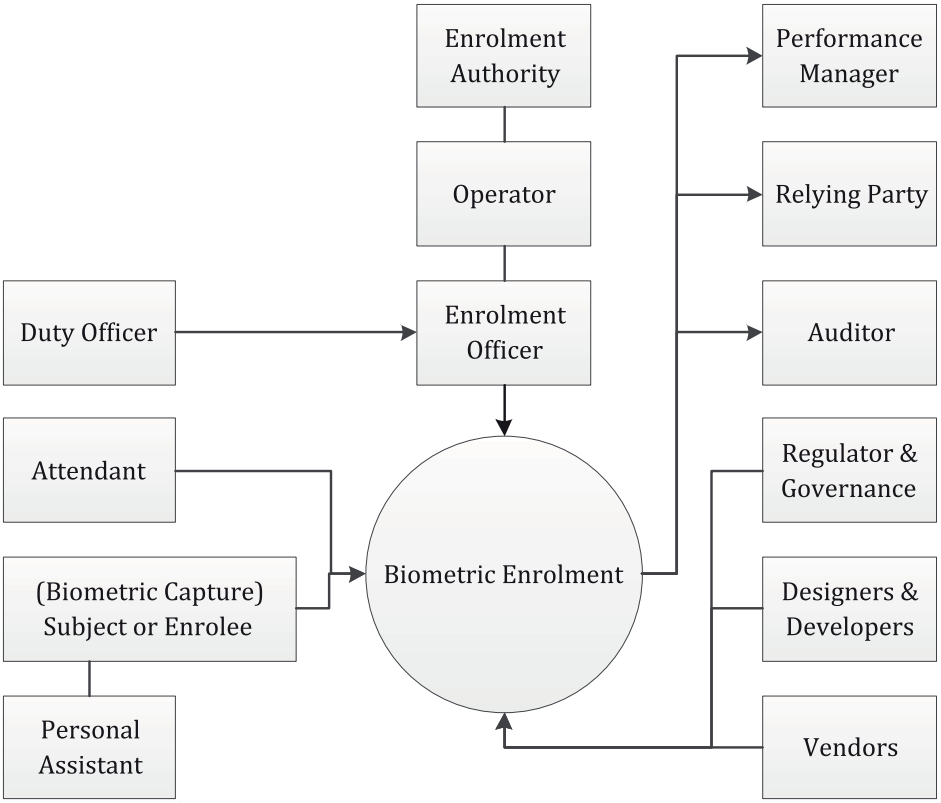


**Figure 2 — Stakeholders at enrolment**

**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.<br>Initiates appropriate action if these fall outside the agreed targets.<br>Ensures compliance with legal requirements.<br>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.<br>Is responsible to the Enrolment Authority for quality and security of the enrolment service.<br>Takes remedial measures if KPIs, including quality and performance metrics, fall outside the agreed targets. |
| Performance manager | Monitors the performance of the enrolment service.<br>Proposes corrective actions.<br>Reports back on the results of corrective actions. |

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018

**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.<br>Ensures the day-to-day maintenance of equipment used in enrolment.<br>Interfaces with the subjects and provides any relevant information to them.<br>Enters any biographical/contextual data (although some of these details may already be pre-populated).<br>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).<br>Provides advice and support to the subject to achieve a high standard of enrolment.<br>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.<br>Needs transparency and information on the system.<br>Is interested in smooth operation.<br>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.<br>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.<br>Develops enrolment system, service and process.<br>Develops an interaction protocol for the enrolee.<br>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. |


© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018

**Table 1** *(continued)*

| Stakeholder | Function description |
|---|---|
| Vendor | Provides hardware and software.<br>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.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018

# 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.


© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018

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.

Documents
Document Sharing Hub

© ISO/IEC 2018 – All rights reserved


Full document details: PD ISO/IEC TR 29196:2018

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).


© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29196:2018