



BSI Standards Publication

Information technology — Guidance for biometric enrolment

National foreword

This Published Document is the UK implementation of ISO/IEC TS 29196:2025. It supersedes PD ISO/IEC TR 29196:2018, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/44/-/4, Technical Implementation of Biometric Systems.

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

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 36287 9

ICS 35.240.15

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 December 2025.

Amendments/corrigenda issued since publication

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



Technical Specification

ISO/IEC TS 29196

Information technology — Guidance for biometric enrolment

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

**First edition
2025-12**

Reference number
ISO/IEC TS 29196:2025(en)

Full document details: PD ISO/IEC TS 29196:2025

© ISO/IEC 2025



Documents

Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	3
5 Role of biometric capture processing in a biometric system	3
6 Stakeholders and approaches for enrolment	6
6.1 Enrolment stakeholders	6
6.2 Enrolment approaches	8
7 Stakeholder interests	8
7.1 Key observations	8
7.2 Best practices and recommendations	10
7.2.1 General	10
7.2.2 Subject interests	10
7.2.3 Enrolment authority interests	13
7.2.4 Operator interests	21
7.2.5 Relying party interests	26
7.2.6 Designer and developer interests	27
7.2.7 Regulator interests	33
7.2.8 Auditor interests	34
8 Biometric enrolment capability development	34
8.1 General	34
8.2 Enrolment station architecture and design	34
8.3 System definition	35
9 Modality specific guidance	35
9.1 General	35
9.2 Facial biometric systems	36
9.2.1 General	36
9.2.2 Environment	36
9.2.3 Pose and position	36
9.2.4 Ethnicity	37
9.2.5 Improvements	37
9.2.6 Glasses	38
9.3 Fingerprint biometric systems	38
9.3.1 General	38
9.3.2 Fingerprint capture considerations	39
9.3.3 Single finger systems	39
9.3.4 Tenprint systems	40
9.4 Vascular (vein) authentication systems	40
9.4.1 General	40
9.4.2 Palm vein technology	40
9.4.3 Finger vein technology	41
9.5 Iris biometric systems	41
10 Mobile applications	43
10.1 Best practice guidelines	43
10.2 Fingerprint systems	44
10.3 Facial image systems	45
10.4 Iris systems	46
Bibliography	47

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

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

This first edition of ISO/IEC 29196 cancels and replaces ISO/IEC TR 29196:2018, which has been technically revised.

The main changes are as follows:

- recommendations added throughout the document;
- [Clause 3](#), some terms and references modified;
- information about enrolment updated to state of art;
- Annex A removed.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

One of the most important contributions to a successful biometric recognition system is a consistent biometric enrolment service ("biometric capture process") that stores biometric data captured from individuals for biometric comparison purposes. Biometric data captured for subsequent verifications or identifications are compared with the biometric data collected at enrolment time. If the quality of the biometric samples captured for enrolment is not consistently maintained, the performance of the biometric recognition system is likely to be unreliable. For those who are enrolled in a verification system, a poor quality enrolment is an inconvenience if they are not recognized.

NOTE Quality has a specific meaning when applied to biometric systems, see ISO/IEC 29794-1: 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.

Principles based on stakeholder requirements can guide the development of system policy to ensure that the quality of biometrics samples captured for enrolment are fit for purpose. Where biometric capture processing is outsourced to a third party, a shared understanding of quality is an extremely important basis for ensuring the relying party and the enrolment authority are aligned on what constitutes a biometric sample of acceptable quality.

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

Information technology — Guidance for biometric enrolment

1 Scope

This document gives guidance relating to successful, secure and usable implementation of biometric enrolment processes, while indicating risk factors that organizations which use biometric technologies can address during procurement, design, deployment and operation. Much of this document is generic to many types of applications, 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 taken into account when specifying an enrolment system and process.

This document specifies the differences in operation relating to specific types of application, e.g. where self-enrolment is more appropriate than attended enrolment. This document focuses on mandatory, attended enrolment at fixed locations. It ultimately consolidates information relating to better practices for the 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.

This 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.

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 terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

biometric capture service

process of capturing biometric data and submitting it to a back-end solution for either processing or biometric enrolment, or both

Note 1 to entry: Enrolment may happen directly or as a subsequent process of the backend solution.

3.2

biometric subject

individual seeking to be, or is enrolled in, a biometric enrolment database

3.3

breeder document

document used to support applications for identity, residence and travel documents, such as birth, marriage and death certificate

3.4

enrolment authority

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

3.5

enrolment officer

individual responsible for the operation of the biometric capture service and the enrolment in accordance with a system policy

Note 1 to entry: As an agent of the operator, the enrolment officer may be an employee or contracted by them.

Note 2 to entry: System policy can include requirements relating to legal, security, privacy, efficiency and effectiveness

Note 3 to entry: The enrolment officer can be responsible for the operation of the biometric enrolment service at one or more physical locations.

3.6

designer and developer

organization or individual responsible for the design, development, (and deployment, if applicable) of the biometric capture system

3.7

duty officer

trained individual acting on behalf of either the enrolment authority or operator.

Note 1 to entry: The duty officer is trained to provide advice and guidance to an enrolment officer in case of difficulty.

Note 2 to entry: The duty officer may be present in the vicinity of one or more enrolment stations, or available on line or by telephone.

Note 3 to entry: The duty officer may have a role in determining exception handling routines.

3.8

key performance indicator

KPI

metric quantifying one or more aspects of the successful operation of a process

3.9

operator

organization (or other entity) responsible for running the enrolment service on behalf of the enrolment authority

3.10

performance manager

individual responsible for assessing how well the biometric enrolment service satisfies the operational requirements of the enrolment authority

Note 1 to entry: This can include monitoring the quality of biometric samples captured and applying corrective measures where necessary, and reporting operating metrics to the enrolment authority as required.

3.11

personal assistant

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

Note 1 to entry: Such purposes can 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.

3.12**relying party**

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

3.13**service level agreement****SLA**

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

3.14**attendant****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, cultural and religious sensitivities, or age of the subject

3.15**vendor**

entity providing either the hardware or software biometric functionality, or both

4 Abbreviated terms

FMR	false match rate
FNMR	false non-match rate
FTAR	failure to acquire rate
FTER	failure to enrol rate
GUI	graphical user interface
NFIQ	NIST fingerprint image quality
OFIQ	open source face image quality

5 Role of biometric capture processing in a biometric system

Given the variety of applications and technologies, it can seem difficult to draw any generalizations about biometric systems. All such systems, however, have many elements in common. Biometric samples are captured from a subject using a biometric capture device which contains one or more sensors. 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. In other cases, the sample itself (without feature extraction) can 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.

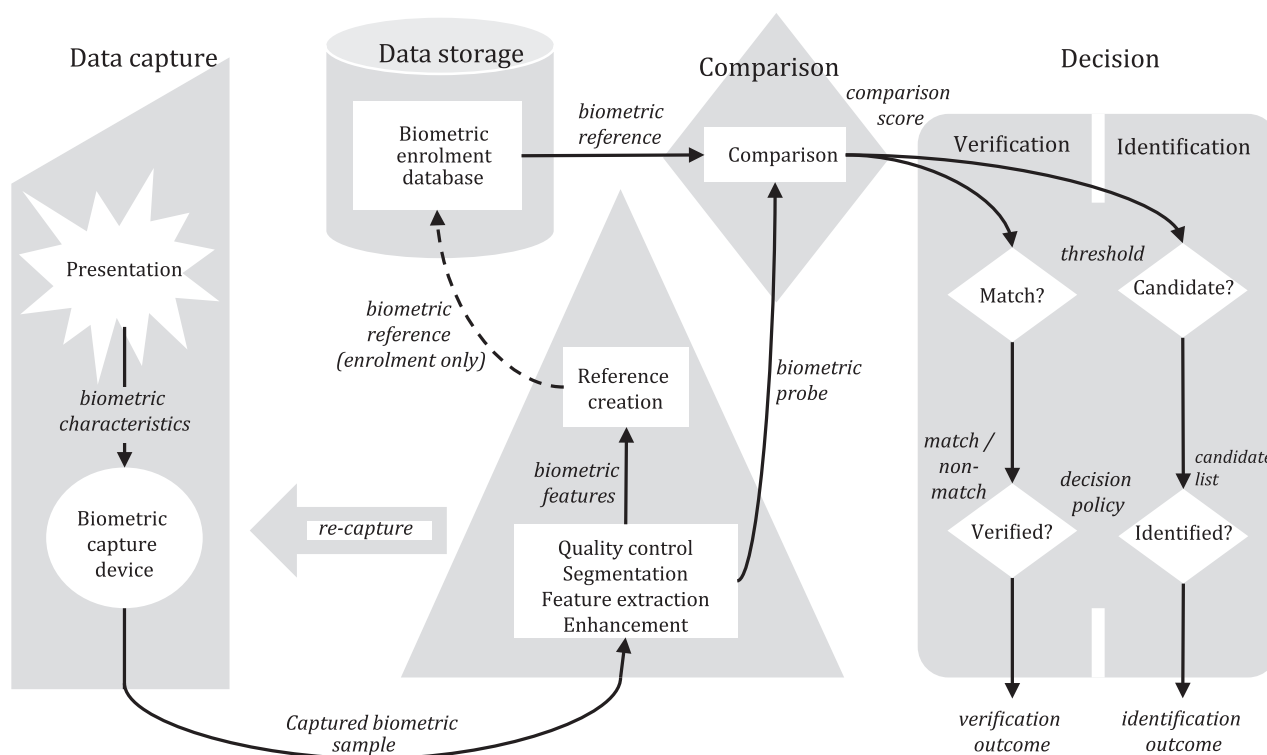


Figure 1 — Components of general biometric system

[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, in any implemented system, some of these conceptual components can be absent, or can potentially 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 biometric capture processing/enrolment, the signal processing subsystem creates a biometric reference. Sometimes the biometric capture 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 can be associated with some details of the enrolled subject or the capture process. 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 can 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 enrollee 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).

The administration subsystem (not portrayed in [Figure 1](#)) 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 can 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.

A subject can also be required to present additional data specific to the biometric capture process. This additional data can 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 biometric capture processing 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 can 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.

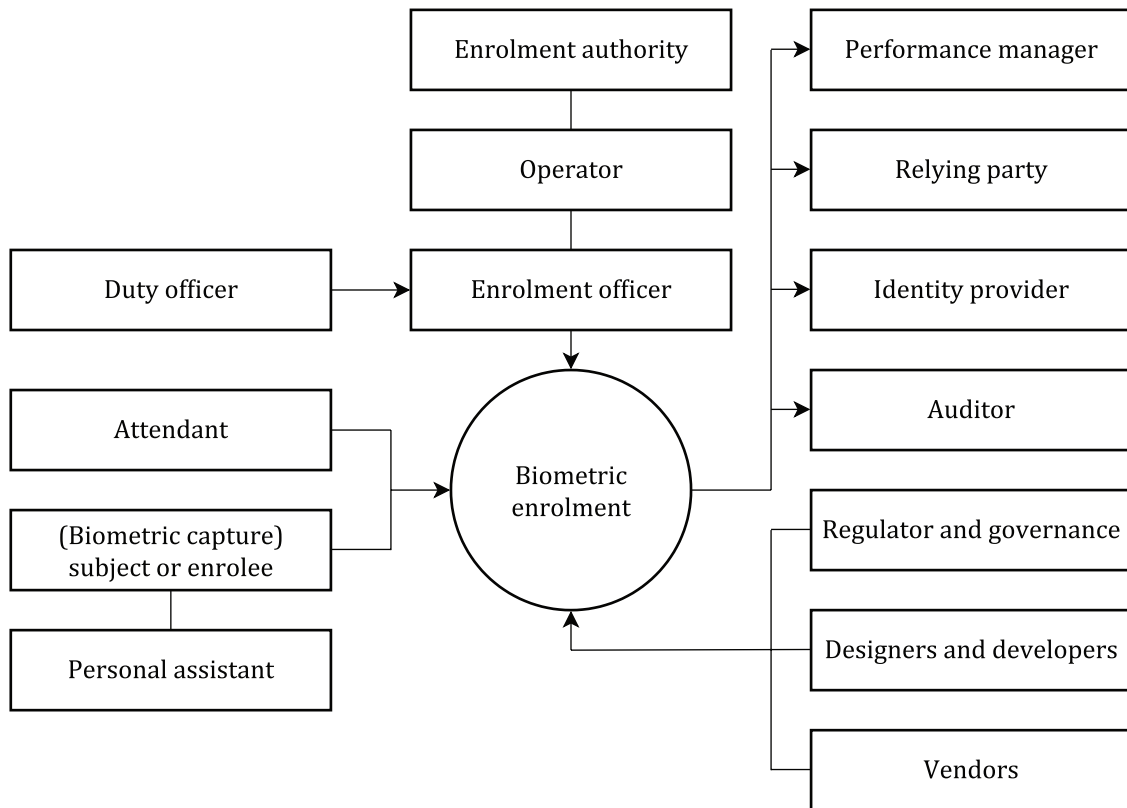


Figure 2 — Stakeholders at enrolment

Table 1 — Functional description of stakeholder roles

Stakeholder	Function description
Enrolment authority	<p>Is responsible for ensuring the quality of biometric enrolment samples and other KPIs are in accordance with SLA or contractual requirements.</p> <p>Is responsible for ensuring the operation of the enrolment service is in accordance with contractual requirements</p> <p>Initiates appropriate action if these fall outside the agreed targets.</p> <p>Ensures compliance with legal requirements.</p> <p>Ensures that the cultural sensitivities of operating an enrolment service are taken into consideration.</p> <p>As needed, engages an operator to run the enrolment service on its behalf.</p>
Operator	<p>Runs the enrolment service on behalf of the enrolment authority in accordance with the contractual arrangements in place.</p> <p>Takes remedial measures if KPIs, including quality and performance metrics, fall outside the agreed targets.</p>
Performance manager	Monitors, reviews and reports the performance of the enrolment service.
Enrolment officer	<p>Is responsible for the secure and effective enrolment service at one or more enrolment points.</p> <p>Ensures the day-to-day maintenance of equipment used in biometric capture processing.</p> <p>Interfaces with the subjects and provides any relevant information to them.</p> <p>Enters any biographical/contextual data (although some of these details may already be pre-populated).</p> <p>Ensures that the quality of the captured biometric sample collected by the sensor/camera meets the enrolment standards (usually through requesting the subject to re-capture if the standard is not achieved).</p> <p>Provides advice and support to the subject to achieve a quality enrolment.</p> <p>Notes any exceptional circumstances.</p>
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 cultural and religious sensitivities.
Biometric capture subject/enrolee	<p>Provides biometric sample to the system.</p> <p>Needs transparency and information on the system.</p> <p>Is interested in smooth operation.</p> <p>Is interested in maintaining their data privacy, wants to submit only that data that is absolutely necessary for the intended purpose.</p> <p>Prefers to have a system that is as usable and intuitive as possible.</p>
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 biometric data capturing of a child.
Designer and developer	<p>Designs the enrolment system as part of the enrolment service and processes using systems engineering principles wherever possible.</p> <p>Develops enrolment system, service and process.</p> <p>Develops an interaction protocol for the enrolee.</p> <p>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.</p>
Vendor	<p>Provides hardware and software.</p> <p>Provides (either directly or through an agent) technical support e.g. for upgrades or rectification of faults, if under contract to do so.</p>
Regulator and other governance bodies	Assures the enrolment process is operated according to laws, regulations, codes of practice, and contracts.

Table 1 (continued)

Stakeholder	Function description
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

Biometric capture processing can take different forms depending on the requirements of relying party including whether the service is:

- In-house or outsourced.
- Multiple or single location.
- Fixed, mobile or remote.
- Attended, semi-attended (one enrolment officer overseeing a number of biometric capture processes 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 or multiple modalities.
- Designed to provide biometric capture processing for either multiple applications or for a specific application. Enrolment is a required task in a biometric service. However, based upon the scale of the desired capture audience, enrolment can be costly, in terms of human capital and geographic locations to conduct the service. Self-enrolment capability can reduce the cost of personnel to observe enrolments, but can require more developmental and testing hours prior to deployment. In order to reduce costs, biometric data processing 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 biometric capture processes may be required to be more specific in design – e.g. access control 'offline' or 'batch' biometric capture process where the biometric sample capture is separate from the enrolment stage, or an integrated credential proofing/acquisition/enrolment process.
- Duration/complexity of the biometric capture process, from a simple single modality process (against pre-assigned identity) or a more complex process consisting of identity checks using breeder documents, followed by the collection of biometric samples for multiple modalities in accordance with quality requirements.

The operational policy and guidance for the enrolment service will be influenced by these requirements.

7 Stakeholder interests

7.1 Key observations

A repeatable biometric capture 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 sample(s) have been collected in line with best practice, but do not meet all quality criteria, can present difficulties when the reference created from

the sample(s) is subsequently compared with a biometric probe(s) for biometric comparison purposes. For example, if a thumb is presented and registered in a biometric capture process 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 be inconvenienced by having to use an exception handling process to gain access.

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 the biometric data captured 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 biometric capture process performance in any contracts or agreements between the 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](#). 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 for acceptance of the system(s) and performance management purposes.

The designers and developers of the biometric capture processing system use the requirements to define biometric capture processes, and source suitable hardware and software to collect biometric samples and assess their quality, create biometric references, and as required, check that biometric capture processing has been completed satisfactorily.

The security of the biometric enrolment service is critical to its success. All stakeholders have a part to play in specifying and addressing security requirements in the design of the service relating to subject interactions, processes and procedures, functions, components and points of integration with other systems.

When addressing the security requirements, consideration can be given to ISO/IEC standards for the protection of information and Information and Communication Technology (ICT), including generic methods, techniques and guidelines for security and privacy. Biometric specific International Standards that can be considered include:

- ISO/IEC 19792 — Security techniques — Security evaluation of biometrics
- ISO/IEC 24761 — Security techniques — Authentication context for biometrics
- ISO/IEC 30107 (all parts) — Biometric presentation attack detection

As the design of the enrolment service progresses, marketing and other awareness-raising activities should be started to support stakeholder engagement on the design at designated design checkpoints. This enables stakeholders including representatives of the subject population, media, regulators, and special interest groups to comment on the design proposals. These comments should be considered and any necessary changes to the design incorporated.

The enrolment authority/operator should ensure that the enrolment service is subject to appropriate testing prior to being piloted. The testing regime should be developed in accordance with Enrolment authority/operator testing policy and reference to ISO/IEC 19795. The testing should determine the extent to which the enrolment service meets requirements and whether it should be deployed for pilot and operational use.

Prior to operational deployment, the enrolment service can be piloted with a representative sample of the subject population and duty and enrolment officers. This provides the opportunity to address any unforeseen issues that would cause difficulties in a full operational deployment. Comments and observations collected during the pilot should be assessed and, where changes are made to the enrolment service, a further round of acceptance testing and pilot can be needed.

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.

An audit of the enrolment service may be requested periodically to evaluate whether it conforms to requirements. Guidelines for the audit process should take account of the particular characteristics of the enrolment service and the biometric modalities employed.

7.2 Best practices and recommendations

7.2.1 General

There are numerous stakeholders in any biometric capture process application, most of whom will benefit from a high quality, securely administered biometric capture 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 subclause describes some success factors for key characteristics of the enrolment service that would contribute to one or more stakeholders considering it to be successful.

A strategy for the design, development and deployment of a successful biometric capture processing 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 on the enrolment service characteristics that are relevant to service success^[6]:

- appropriateness, effectiveness and efficiency;
- convenience and price;
- look and feel;
- accessibility, usability and inclusion;
- personalization, localization and internationalization;
- governance arrangements;
- performance including speed, and accuracy;
- operational and environmental aspects;
- availability, reliability, maintainability and supportability;
- security, privacy and transparency;
- cultural and political aspects; and
- legal and cross-jurisdictional aspects.

7.2.2 Subject interests

7.2.2.1 General

The enrolment subject should be presented with a clear and understandable biometric capture process that allows the subject to feel safe and alleviate any concerns. The necessary information should be made available in a language known to the biometric subject, preferably in their native language.

The biometric capture process should flow well and be able to handle any possible exceptions. Prior identification of exceptional conditions (e.g. support for disabled persons, support for mentally challenged