

# A PRIMER ON BIOMETRICS FOR ID SYSTEMS

© 2022 International Bank for Reconstitution and Development/The World Bank  
1818 H Street, NW, Washington, D.C., 20433  
Telephone: 202-473-1000; Internet: [www.worldbank.org](http://www.worldbank.org)

## Some Rights Reserved

This work is a product of the staff of The World Bank with external contributions. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Nothing herein shall constitute or be considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, or of any participating organization to which such privileges and immunities may apply, all of which are specifically reserved.

## Rights and Permission



This work is available under the Creative Commons Attribution 3.0 IGO license (CC BY 3.0 IGO) <http://creativecommons.org/licenses/by/3.0/igo>. Under the Creative Commons Attribution license, you are free to copy, distribute, transmit, and adapt this work, including for commercial purposes, under the following conditions:

**Attribution**—Attribution—Please cite the work as follows: Ted Dunstone. 2021. A Primer on Biometrics for ID Systems, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO)

**Translations**—If you create a translation of this work, please add the following disclaimer along with the attribution: *This translation was not created by The World Bank and should not be considered an official World Bank translation. The World Bank shall not be liable for any content or error in this translation.*

**Adaptations**—If you create an adaptation of this work, please add the following disclaimer along with the attribution: *This is an adaptation of an original work by The World Bank. Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by The World Bank.*

**Third Party Content** — The World Bank does not necessarily own each component of the content contained within the work. The World Bank therefore does not warrant that the use of any third-party-owned individual component or part contained in the work will not infringe on the rights of those third parties. The risk of claims resulting from such infringement rests solely with you. If you wish to re-use a component of the work, it is your responsibility to determine whether permission is needed for that re-use and to obtain permission from the copyright owner. Examples of components can include, but are not limited to, tables, figures, or images.

All queries on rights and licenses should be addressed to World Bank Publications, The World Bank, 1818 H Street, NW, Washington, DC, 20433; USA; email: [pubrights@worldbank.org](mailto:pubrights@worldbank.org).

Cover images: Shutterstock.

# Contents

---

About ID4D	iv
Acknowledgments	v
About This Primer	vi
Acronyms and Abbreviations	viii
1. Biometric Fundamentals	ix
2. Common Biometric Modalities	6
3. Other Modalities	12
4. Multi modal Systems	16
5. Legal Considerations	18
6. Technical Considerations	26
7. Deployment and Operational Considerations	45
Appendix: Biometrics in ID Systems Frequently Asked Questions (FAQs)	54
General	55
Enrollment, Authentication, and Storage	62
Standards	68
Operations	70
Data Protection, Privacy, and Governance	72
Security and Accuracy	74
Costs and Procurement	81
Glossary	83

# About ID4D

---

The World Bank Group's Identification for Development (ID4D) initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals. It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, legal, among others.

The mission of ID4D is to enable all people to access services and exercise their rights, by increasing the number of people who have an official form of identification. ID4D makes this happen through its three pillars of work: thought leadership and analytics to generate evidence and fill knowledge gaps; global platforms and convening to amplify good practices, collaborate and raise awareness; and country and regional engagement to provide financial and technical assistance for the implementation of robust, inclusive and responsible digital identification systems and with civil registration.

The work of ID4D is made possible through support from the Bill & Melinda Gates Foundation, the UK Government, the French Government, Norad and the Omidyar Network.

To find out more about ID4D, visit [id4d.worldbank.org](https://id4d.worldbank.org). To participate in the conversation on social media, use the hashtag #ID4D.

# Acknowledgments

---

A Primer on Biometrics for ID Systems was prepared by Ted Dunstone under the supervision of Vyjayanti Desai. The Primer benefited greatly from reviews and inputs from: Adele Barzelay, Alan Gelb, Changqing Sun, David Satola, Fredes Montes, Henry Forero, James Neumann, Jerome Buchler, Jonathan Marskell, Julia Clark, Loreto Dingdong Sibayan II, Michiel van der Veen, Pablo Andres Guzman Abastoflor, Sam Jefferies, Sebastian Manhart, and Seth Ayers.

# About This Primer

---

The World Bank Group's Identification for Development (ID4D) Initiative prepared a *Primer on Biometrics for ID Systems (Primer)* as a reference document for practitioners, civil society organizations, development partners and other stakeholders on the responsible use of biometric recognition in official or government-recognized identification (ID) systems, such as national IDs, civil registration, population registers, and others. Over the past 30 years, countries have increasingly incorporated digital biometric recognition into these ID systems, either as part of identity proofing (de-duplication) and/or to provide verification and authentication to service providers. However, given the specialized and often proprietary nature of most biometric technology, the stakeholders mentioned above have not always had access to information they need to effectively consider the appropriate and responsible use of this technology. The Primer reflects experiences in a range of countries from different regions, with different legal systems, and at different stages of economic development. It also takes into account existing literature, international conventions, and norms and principles. It is based on evolving international good practice, as understood by ID4D.

## What is in the Primer?

This Primer aims to help fill this knowledge gap, serving as an introduction to key biometrics-related terms and concepts. It also provides good practices and approaches for determining whether or not biometric recognition is necessary for an ID system and—if so—how to use it responsibly, considering several domains (e.g. technical, deployment, operational, and legal). The Primer includes:

- Answers to frequently asked questions (FAQs) by practitioners during the design and implementation of incorporating biometrics in ID systems (*note: there is a user-friendly list of FAQs in the appendix*);
- An overview of how biometric recognition can be used in ID systems as part of the registration process and to provide people with proof of identity;
- Guidance on the responsible use of biometrics that are aligned with the [Principles on Identification for Sustainable Development](#) and data protection/privacy-by-design approaches; and
- Good practices for incorporating biometrics in ID systems in ways to ensure accessibility, inclusivity, security, and sustainability.

Despite the potential benefits of biometric recognition in detecting duplicate registrations and enabling authentication, including security and inclusion advantages over other authentication methods in some cases, deploying these technologies in ID systems presents various challenges. These challenges range from operational, technical, and legal to ethical considerations and include, for example, data protection, security, performance, inclusion, biometric recognition for children and elderly persons, implementation in harsh environments, technology and vendor selection, literacy, cost, and more.

We hope this Primer will help countries more carefully weigh these potential benefits, challenges, and risks, and where biometric recognition is used, adopt good practices for minimizing risk and safeguarding inclusion and data protection.

## What is not in the Primer?

The Primer does not advocate for the use of biometric recognition, or any particular biometric technology. Rather, it provides analysis and approaches for evaluating the use of the technology and design options for various contexts and applications. The use of biometrics for purposes beyond official ID systems—e.g., for the purpose of surveillance, law enforcement, public security—is outside the scope of this Primer. In addition, the Primer does not address the broader security and technological issues involved with ID systems, which are addressed in other materials, including in through international standards. As with any system that processes personal data, ID systems are vulnerable to attack or misuse given enough time, resources, and determination. The Primer is not intended to be a guide for planning World Bank operations. There is no guarantee that addressing all the issues raised in this Primer will result in successful use of biometrics in and ID system in a country—that will depend on many factors that must be considered, and which may be different from country to country. While every attempt has been made to be complete, there may be issues affecting the design, establishment of operation of the use of biometrics in an ID system that are not addressed in this Primer, or that are addressed in the context of certain assumptions, facts and circumstances that do not apply equally to every situation. Nothing in this Primer constitutes legal advice and no inference should be drawn as to the completeness, adequacy, accuracy or suitability of any of the analyses or recommendations as applied to any particular situation. This Primer is a reference tool only. As a result, when contemplating the use of biometric recognition for an ID system, policymakers, practitioners and other stakeholders must carefully balance these risks, as well as potential benefits and alternatives.

# Acronyms and Abbreviations

---

ABIS	Automated biometric identification system
ATM	Automated teller machine
API	Application programming interface
BIPA	Biometric Information Privacy Act
CCTV	Closed circuit television
DET	Detection error trade-off curve used to compare the accuracy of biometric systems by plotting FMR against FNMR
DPIA	Data Protection Impact Assessment
EER	Equal-error-rate (the operating point where the FMR equals the FNMR)
EU	European Union
FAR	False accept rate
FMR	False match rate
FNMR	False non-match rate
FRR	False-reject-rate
FRT	Facial recognition technologies
FTA	Failure-to-acquire rate
FTC	Failure-to-capture
FTE	Failure-to-enroll
GDPR	General Data Protection Regulation (EU)
HBV	Harmonized Biometric Vocabulary as defined by ISO Standard 2382-37 (2017)
ICAO	International Civil Aviation Organization
ID	Identification
ID4D	Identification for Development Initiative
IEC	International Electrotechnical Commission
IJOP	Integrated Joint Operations Platform (China)
ISO	International Organization for Standardization
IT	Information technology
ITU	International Telecommunication Union
KYC	Know Your Customer
M.I.T.	Massachusetts Institute of Technology
NIST	National Institute of Standards and Technology (US)
NGO	Non-governmental organization
OECD	Organization for Economic Co-operation and Development
OPM	Office of Personnel Management (US)
PAD	Presentation attack detection
PbD	Privacy-by-Design
PKI	Public key infrastructure
ROC	Receiver operating characteristic
TAR	True-accept rate ( $TAR = 1 - FRR$ )
UN	United Nations





# 1. Biometric Fundamentals

Biometric recognition is the automated recognition of individuals based on their physical, physiological, or behavioral characteristics, as indicated by biometric data (such as facial images or fingerprint data).

The most common physical and physiological traits used in biometric recognition across applications are face, fingerprint, iris, voice, and DNA. Behavioral characteristics used in biometric recognition include keystroke dynamics, gait recognition, or signature recognition. For the purpose of official ID systems, the most common modalities have been fingerprints, iris, and face, which are the subject of this guide.

The primary goal of a biometric system is to determine identity. This determination is undertaken by using a matching process that can be simplified into two phases:

- The capture and comparison of the biometric sample
- A decision as to whether to accept or reject the input as authentic

The capture of biometric data and the matching algorithm are specific to the biometric being used. Each biometric modality has specific requirements about the way the data needs to be processed. Examples of raw biometric input include audio data, images, and three-dimensional geometry.

The matching algorithms need to be tuned to look for the best features to distinguish individuals while coping with changes introduced due to aging or other variations. This requires them to be highly optimized for the type of biometric being matched.

The output of the biometric matching process is a similarity score. Although each algorithm may have quite different scoring characteristics and ranges, the output represents the common attempt to assign a relative likelihood that it is a particular person and not someone else.

## 1.1. Acquisition

**The capture of a biometric is known as acquisition, and this is accomplished using a biometric sensor. The sensor may be specialized like a fingerprint capture device or general like a camera or microphone.**

Biometric systems face specific acquisition challenges due to issues in the capture or acquisition process. For example, in cases where individuals do not have fingerprints or have poor quality fingerprints because of heavy manual labor. This may result in acquisition failures, which may result in individuals being excluded from the biometric system and, unless exception handling mechanisms are in place, from the ID system itself.




## Different types of acquisition failures include:

- *Failure to capture (FTC)*. The first potential failure is in the capture process; in which case it is not possible to measure the biometric (face, fingerprint, iris). This leads to what is known as "failure to capture" (FTC). An FTC can occur, for example, when a person does not have fingerprints or an iris or due to environmental conditions affecting the operating conditions of the capture device. FTC can occur in all the basic processes of a biometric system: enrollment, verification, and identification.
- *Failure to acquire (FTA)*. Failure to acquire is when meaningful information cannot be derived from a biometric sample after it has been captured. Infants and young children, elderly, and people who have done heavy manual labor may be overrepresented in FTAs. Like the FTC, a FTA can take place during the enrollment, verification, and identification processes of a biometric system.
- *Failure to enroll (FTE)*. An enrollment process is typically designed to minimize FTC and FTA, for example, by using state-of-the-art capture devices, active quality control, intuitive user-interface software with feedback mechanisms, and more. In such a process it is typically allowed to have multiple acquisition attempts. If the acquisition of the biometric data fails during the enrollment process, then this is referred to as "failure to enroll" (FTE). Because of the enrollment process, the FTE is usually smaller than the FTA. Note that FTE (and FTA) have an impact on false match rate (FMR) and false non-match rate (FNMR) (see Section 6.4.2 for details): Having stricter requirements on sample quality (i.e., rejecting a larger portion of low-quality samples) will increase FTE and at the same time improve FMR and FNMR. For this reason, all these parameters (FTE, FTA, FTC, FNMR, and FMR) are relevant when evaluating biometric systems.

The amount of acquisition failures depends on a range of factors, including the choice of face, fingerprint or iris as biometric characteristic(s), choice of technology (hardware and software), user interaction, environmental conditions, the target population, quality targets, and other influencing factors. For this reason, it is challenging to provide one single number for a specific biometric characteristic.

For example, a recent comparative FTC was evaluated on a sample of 4.5M records from 26 UNHCR country operations using the same UNHCR biometrics software. The FTC for each modality—excluding individuals who were not able to be enrolled with either modality whatsoever—were as follows: 4 percent of those enrolled were unable to record one or more irises. 5 percent of those enrolled were unable to record one or more fingerprints. The FTC of a minimum of two irises was calculated to be 14 percent, and a FTC of a minimum of 4 good fingerprints was 9 percent. Using both modalities together allowed UNHCR to significantly reduce the overall FTE rate.

**Figure 1.1. Typical Acquisition Failures per Modality**

	 <b>Face</b>	 <b>Fingerprint</b>	 <b>Iris</b>
<b>Failure to capture (FTC)</b>	The failure to capture the biometric characteristics from a capture device and create a biometric sample		
<b>Possible factors affecting FTC</b>	Occluded face image Environmental conditions (e.g., due to unfavorable light conditions)	Sensor not able to locate fingerprint, e.g., due to dirt or humidity, wear and tear of the sensor Individuals without fingers	Individuals without iris Can be higher for some equipment with younger subjects
<b>Failure to acquire (FTA)</b>	When the capture process was successful, a failure to acquire happens when there is a failure to accept the biometric sample for subsequent comparison.		
<b>Factors affecting FTA</b>	Insufficient quality of the captured biometric image (face, fingerprint, and iris) in combination with the quality threshold used for accepting a biometric sample The quality of the software in terms of user interaction end feedback mechanism The target population (a group of students aged 20–25 is expected to have better FTA than a group of people aged 60–65 who perform manual labor) The quality of the capture device		
<b>Failure to enroll (FTE)</b>	The failure to create and store a biometric enrollment data record.		
<b>Factors affecting FTE</b>	In addition to FTA and FTC, the enrollment strategy will affect the FTE. This may include, for example, the possibility of multiple acquisition attempts or the possibility for an operator to override acceptance criteria.		

## 1.2. Matching

**A matching algorithm fundamentally takes two biometric samples or templates and uses a mathematical process to determine how similar they are based on the most distinguishing characteristics.**

Modern matching algorithms need to be trained on data, both to create and tune the algorithm. This is done using large sets of labeled data that vendors have compiled. The output of this process is a model that can be used to predict similarity, but its robustness depends upon the data that was available for training as well as other pre-processing techniques.

**Biometric algorithms can exhibit bias based on different demographics.**

This bias can result in a higher chance of false acceptance or false rejection for population subgroups. The potential for this algorithm bias has recently raised public concerns over the use of face recognition

systems in particular. As most face recognition algorithms are generated by training the system to detect a number of faces from a database, bias can occur if the training database was not sufficiently diverse. See Section 6.4.5 for more information on the determination and consequences of bias.

## 1.3. Biometric Applications

**There are two biometric recognition processes used in typical ID systems: (1) identification (1:N matching), and (2) verification (1:1) matching both of which occur after biometric enrollment.** In general, the first process is used during registration into the ID system to duplicate new enrollments and ensure they are unique, while the second is used to authenticate the identity of a previously enrolled individual.

### 1.3.1. Biometric Enrollment

**Enrollment is the process by which individuals are registered and their identity data is recorded into the ID system.** This usually requires the individual to provide a strong link to their identity through one or more pieces of existing original documentation, such as a birth certificate, driver's license or passport, or, possibly, a qualified "introducer" for persons without documentation.<sup>1</sup>

For systems that use biometrics, biometric images are captured at this point to establish a link between the biometrics and the claimed identity. To be used most effectively and efficiently for automated or manual recognition, the images should comply with defined standards, such as the image format, quality, and specifications.

The biometric capture stage of enrollment acquires an image or images of the user's relevant biometric using a purpose-built device, ideally under quality-controlled conditions. The capture process can be fully automated via a kiosk, completed by an automated process supervised by a human system operator, or performed entirely by the human system operator. Where a poor-quality capture is detected, further attempts should be made to replace the poor quality images with those of better quality. In some cases, it is also necessary to have an override so that if a quality capture cannot be acquired, an operator can still submit a poorer quality image or enroll an individual without biometrics on an exceptional basis.

The biometric image is then transferred to an automated biometric identification system (ABIS) within the identity management system, where biometric features are extracted from the captured image in the form of a template and usually stored to enable matching. At this point, identification is frequently undertaken to ensure that the individual is not already enrolled under other details in a process known as "deduplication."

A biometric can be used by itself, in combination with other biometrics, or alongside other authentication factors (such as personal identification numbers [PIN] and secret phrases) to attest to a person's identity during a subsequent transaction or service.

The biometric authentication process is where a captured biometric is compared against a single individual's existing biometric data within a database or stored locally on a card or mobile device. This is known as a "one-to-one match" (1:1). This comparison produces a match score that is indicative of the likelihood of the match being from the same individual. The individual is then considered verified if the match score exceeds a system-defined threshold. Where the match verification fails, a manual verification check may be undertaken by a human operator. Particularly in cases where biometric verification is used for the delivery of basic services and entitlements, alternative authentication mechanisms or exception handling procedures are required to ensure that people are not excluded due to a false non-match.

---

<sup>1</sup> In the context of refugees, for example, the introducer may be the UNHCR.

### 1.3.2. Biometric Verification

The biometric verification process is where a captured biometric is compared against a single individual's existing biometric data within a database. This is known as a “one-to-one match” (1:1). This comparison produces a match score that is indicative of the likelihood of the match being from the same individual. The individual is then considered verified if the match score exceeds a system-defined threshold. Where the match verification fails, a manual verification check may be undertaken by a human operator.

Where a biometric is linked to biographic data in the foundational ID system, it can be used by itself, in combination with other biometrics, or alongside traditional security measures (such as personal identification number [PIN] and secret phrases) as proof of identification. This can apply both to the government agency and potentially for third-party service providers, such as telecommunications, utility providers, and banks.

### 1.3.3. Biometric Identification

Identification is traditionally defined as the process where a captured biometric is compared against multiple individuals' existing biometric data within a database. This is known as a “one-to-many match” (1:N)<sup>2</sup>. This will generate a list of the most likely match candidates, usually ordered by their similarity. The position of a candidate in this list is known as the “rank,” with the top candidate (most similar) known as “rank 1.”

- There are several ways this list can be used to adjudicate the matches:
- Top candidates. A human system operator looks at the topmost likely candidates (often the top 10) to determine if there might be the same individual with different credentials. This is often called “manual adjudication.”<sup>3</sup>
- Automated decisions and manual resolution and adjudication. The system may have two different thresholds such that when candidates are above the upper threshold, they are considered a match, and when they are below the lower threshold, they are not considered a match. In between these two thresholds, they are referred to operators for manual adjudication.

Deployments that implement widespread use of identification capabilities can introduce a variety of risks such as function creep related surveillance. It is, therefore, recommended that practitioners consult closely with biometric and legal experts on the implications if such use cases are to be involved in ID systems.

### 1.3.4. Biometric Deduplication

Enrollment into a foundational ID system occurs through users providing both their biographic and biometric data for registration. The captured biometric can then be compared against the enrollment database to ensure that the person is not already enrolled. This deduplication process lowers the risk of identity fraud by helping prevent people from obtaining multiple identities within the foundational ID system. This use case is currently used globally in most developed countries as part of the issuance process for passports and, in some cases, driver's licenses.

---

2 Note that in some cases the identification process may include an authentication step as well (1:N+1), since the 1:1 match may be explicitly performed.

3 Use of 1:N for the identification of individuals can assist with security, as matches can be compared against watchlists located in the database to identify persons of interest; however, this functionality must be balanced against data protection and function creep risks.

# 1.4. Conditional Suitability

Any ID system that plans to use biometrics must consider the suitability of the chosen biometric modality in the likely deployment conditions as well as data protection and governance requirements. Consideration also needs to be given to issues relating to accuracy, fraud, and risk, algorithm bias, integration with other systems, usability, and future utilization scenarios.

In 1999, Prof. Anil Jain and his team identified several factors that determine the suitability of a biometric modality to be used in a biometric system.<sup>4</sup> Table 1.1 expands on this foundation for key factors that decision-makers should consider when evaluating biometric systems for any particular application.

**Table 1.1. Suitability Factors for the Use of Specific Biometric Modalities in a Biometric System**

1	Universality	Every individual that makes use of a biometric system should possess a biometric trait. Failure to have such a biometric characteristic may lead to exclusion from the system.
2	Distinctiveness	The biometric characteristic should be sufficiently different between individuals in the relevant population (intervariability) and should be sufficiently stable for each individual in the relevant population (intravariability).
3	Stability	An individual's biometric characteristic should be sufficiently invariant over time with respect to the matching algorithm. A characteristic that changes significantly over time is unsuitable for biometric use. It should be noted that this is especially relevant in the context of biometric recognition for infants and the elderly.
4	Collectability	An individual's biometric characteristic should be simple to obtain and of high quality.
5	Performance	The biometric recognition accuracy should meet the requirements and constraints imposed by the application as well as required identification and verification speeds.
6	Acceptability	Individuals that will utilize the application should be willing to present their biometric traits to the system. This is particularly important to consider at a time where biometric recognition is becoming ubiquitous and security breaches and data protection concerns are increasing.
7	Resistance to circumvention	This refers to the ease with which the biometric system can be circumvented, e.g., through spoofing or other means of fraud.
8	Usability	The ease with which individuals can interact with the biometric system.
9	Interoperability	The ease with which the biometric characteristic can interact with third-party systems based on interchangeable data formats.
10	Cost	The total cost of a biometric system including the capture devices, software, and related processes.
11	Maturity	The technology has been proved to be stable in real-life conditions.

4 Jain, Anil K., Ruud Bolle, and Sharath Pankanti, eds. 1999. *Biometrics: Personal Identification in a Networked Society*. New York, NY: Springer.

## 1.5. Biometric Risk Factors

The adoption of biometrics has several significant advantages. These include detecting duplicate registrations (through identification) and verifying a claimed identity (through verification). Biometrics, when combined with other features, give a more accurate and secure manner of accomplishing this than the previous method of solely employing biographic attributes (i.e. name, date of birth). Biometrics can also improve usability when used to replace or enhance existing identification techniques.

As with any security technology, there are risks involved with it. Consideration of these risks is critical to guaranteeing the integrity of a biometric system and, as a result, retaining public trust by lowering the possibility of personal data compromise.

Security risks can exist in many areas of the use of biometrics with a system, including<sup>5</sup>:

- *Presentation attack.* The use of a false biometric during the enrollment process. Access to false biometric artefacts is becoming increasingly commonplace.
- *Identity claim.* The use of a fake identification artefact (such as a false passport or birth certificate) as proof of identity during the enrollment process.
- *Sensor.* The sensor that captures the biometric is compromised, for example, if a camera is modified to send a pre-existing image for matching instead of a captured image.
- *Transmission.* The captured biometric is intercepted in-transit between the various system components.
- *Quality control and feature extraction.* The enrolled biometric is of low-quality, making it easier to spoof the system.
- *Reference creation.* The attacker creates a compromised template that always returns the desired match score within the system.
- *Enrollment database.* The database that stores system data becomes compromised.
- *Comparison process.* Altering how the system handles verification, allowing the attacker to alter the scenarios where high match scores are produced.
- *Threshold process.* The threshold for matches is altered to allow for lower match scores to be accepted.
- *Candidate list.* The candidate list is modified to rank selected individuals lower than normal to ensure they are not flagged to the system operator.
- *Decision policy.* The system policy that produces accept or reject decisions is compromised.
- *Liveness detection.* The liveness detection system does not successfully identify liveness attacks.

Because of the ever-changing global technology landscape, new ways of attack are continually being devised. Attack artefacts like as realistic latex masks and 3D printed fingerprints, for example, are becoming increasingly affordable. As a result of this development, sophisticated attack scenarios that were previously limited by availability, resources, and talent will become more common.

---

<sup>5</sup> Adapted from Dunstone, Ted., and Yager, Neil. 2010. *Biometric System and Data Analysis: Design, Evaluation, and Data Mining*. New York, NY: Springer.



# 2. Common Biometric Modalities

## 2.1. Introduction

**This chapter provides an overview of the most common biometrics used in official ID systems**, including fingerprint, face, and iris recognition, along with other modalities such as voice recognition, 3D facial geometry, and vascular recognition. For each, it provides an overview of the modality and common uses, as well as advantages and specific risks.

## 2.2. Fingerprint Recognition

**Each of the intricate patterns on the finger is unique and fingerprints are a well-established and high performing biometric.** They have traditionally been used for identification purposes by law enforcement agencies, and over the past three decades have been commonly adopted in government-driven services such as national ID cards <sup>6</sup>(used in a dozen countries around the world), can increase difficulties with capture, as can other disabilities or missing appendages polling registration at elections (in about half of the countries in Africa and South America), or border and migration management (e.g., the European Union Entry-Exit System [EES] or UNHCR's refugee registration system). The introduction of fingerprint scanning capabilities in mobile devices has spilled over to the adoption of fingerprint recognition in the wider consumer market for access control to mobile devices.

### 2.2.1. Advantages

Fingerprint is considered the most mature biometric offering; it is the most established biometric for use at an enterprise scale. In addition, fingerprint recognition is highly distinctive and biometric performance is generally suitable for large-scale applications. Fingerprint is also attractive for reproofing activities where the source documentation is lost or stolen, given the fact that fingerprint has accuracy and robustness benefits over alternative modalities.

---

<sup>6</sup> World Bank. Forthcoming. *Global Identification Challenge by the Numbers*. Washington, DC: World Bank.



When all the user's fingers are registered (known as a "ten-print"), fingerprint recognition is one of the most accurate recognition techniques. Ten-print records are a very robust basis for large-scale de-duplication systems. Matching of both minutiae (minor or incidental details) and non-minutiae feature-based techniques further increases accuracy. International standards for fingerprint recognition are widespread and widely accepted. Capture devices include single fingerprint scanners, 4-4-2 scanners able to capture four fingers at a time, optical, and capacitive based fingerprint. Newer technological options include contactless based scanners that read the fingerprint without the user needing to make physical contact with the sensor but standards in this area are still emerging.

### 2.2.2. Disadvantages and Risks

Some key issues that can affect the use of finger biometrics for ID systems include:

- *Age.* Infants and small children below 5 may benefit from high resolution scanners and custom collection devices as subjects are rarely compliant and may require the use of child-specific algorithms. For children aged 5 and up standard scanners and algorithms can often be used. However UNHCR recommends updating every 2-3 years between the ages of 5-18 to accommodate changes in finger scale as the child grows.<sup>7</sup> Also, aging results in the loss of collagen, making the skin loose and dry, reducing the potential to collect high-quality fingerprints in elderly populations.
- *Inconsistent and unreproducible contact.* Each acquisition will be at a particular angle and level of pressure.
- *Noise.* Even under ideal conditions there will be some noise present, this can be increased by wet or dirty fingers.
- *Incomplete ridge structure.* If the entire ridge structure of the fingerprint is not captured this can affect the robustness of the matching.
- *Elastic distortions.* This occurs when a 3D finger is mapped to a 2D image. This is particularly the case for matching 3D contactless prints, against reference 2d pressed prints.
- *Medical conditions.* Medical conditions such as diabetes can increase difficulties with capture, as can other disabilities or missing appendages.
- *Occupation.* Some professions can cause fingerprints to wear.
- *Data protection concerns.* Fingerprints for identification has been affected by the linkage of fingerprints to criminality and law enforcement, which may create data protection concerns amongst the population.
- *Spoofing possibilities.* Fingerprints may be susceptible to creation of fake fingerprint artefacts, universal master print attacks, or other kinds of spoofing attacks.
- *The need for specialized capture equipment.* For fingerprint capture to be used effectively it must be acquired using hardware that can accurately read the fingerprint features. This cannot currently be reliably achieved using a phone camera<sup>8</sup> and proprietary sensors on mobile phones (such as Apple Touch ID) that do not typically allow access to the raw image or template for data protection reasons. This can limit its use in cases where remote authentication or unattended acquisition is required.

---

7 UNHCR's Guidance on Registration and Identity Management chapter 5.2 section 6.

8 NIST (National Institute of Standards and Technology). 2020. "NIST Study Measures Performance Accuracy of Contactless Fingerprinting Tech." Gaithersburg, MD: NIST. <https://www.nist.gov/news-events/news/2020/05/nist-study-measures-performance-accuracy-contactless-fingerprinting-tech>.

## 2.3. Face Recognition

The use of information collected from a face image for enrolment, verification, or identification is known as facial recognition. The majority of face matching algorithms rely on pattern recognition techniques such as machine learning or statistical learning, which are calibrated using large sets of data. Huge increases in accuracy have been made in the last five years, owing primarily to the use of better quality photographs and machine learning algorithms that are more resistant to environmental changes.

The advancement of facial recognition technologies (FRT) capabilities is resulting in the widespread deployment of FRT solutions for both fundamental and functional types of ID systems. For example, with ICAO requirements for e-passports, FRT is a vital component of international passport usage and is routinely employed as part of the passport issue process. Smartphone devices and applications are increasingly relying on FRT to unlock the phone or validate the owner's identification.

With regard to capture devices, FRT is easy to use and relatively cheap. With the recent accuracy and cost gains, face recognition is now adopted on a large scale in:

- Law enforcement and national security
- Video surveillance
- Automated border crossings using the digital facial image present in every ePassport
- Mobile devices (all the large smartphone manufacturers offer some version of face recognition)
- The financial sector

### 2.3.1. Advantages

Almost everyone can be enrolled in a face-based ID system (assuming a good quality image), whereas for fingerprint or iris-based ID systems there is a much higher failure-to-enroll rate (for example, due to injury). Older persons typically have challenges providing both adequate fingerprints and irises, and manual laborers will have challenges providing adequate fingerprints.

Face capture does not require more expensive hardware than cameras. High quality cameras are now cheap and commonly available. Additionally, FRT systems allow for facial capture and verification to have minimal intrusion on the user. Face capture offers a quick, automatic, and seamless user experience, allowing FRT to be deployed in cases where maintenance of business-as-usual is a high-priority or in high-transit areas.

In the current environment of increased awareness of the dangers of disease transmission, contactless biometrics, such as face and iris, have advantages over traditional contact biometrics, such as fingerprints. A current challenge to accuracy is posed by the wearing of masks.<sup>9</sup> However, in many government identity contexts, the brief removal of the mask for the purposes of identification in an appropriately controlled environment is generally acceptable.

Many existing ID documents and systems used to issue identity credentials, such as passports and drivers' licenses, already include or store the face as part of the document creation. This allows the match to take place against a high-quality image without necessitating recapture. Additionally, if existing systems are in place that possess the capacity for high-quality capture environments, proper equipment, and trained operators, this can reduce resource costs.

---

9 NIST. 2022. FRVT Face Mask Effects." Gaithersburg, MD: NIST. [https://pages.nist.gov/frvt/html/frvt\\_facemask.html](https://pages.nist.gov/frvt/html/frvt_facemask.html).

Recent algorithms have shown impressive levels of accuracy even for large databases and continue to rapidly become more accurate. For example, between June and November 2018, the most accurate algorithms tested by the US National Institute of Standards and Technology (NIST) had their false negative identification rate reduce from 0.0031 to 0.0028 when tested against 30.2 million still photographs of 14.4 million individuals. Furthermore, NIST expects this trend of rapid improvement to continue.

When compared to other biometrics such as iris and fingerprint, many FRT systems will take standard images in a variety of formats, providing flexibility and interoperability.

### 2.3.2. Disadvantages and Risks

Unlike other biometric modalities such as fingerprint or iris, facial images are more readily available in high volume online (such as through social media channels), giving rise to the risk of such images being used without the data subject's knowledge or authorization. Facial images can also be easily captured and matched with the subject from which the biometric was taken without any action or knowledge required directly by the data subject.

In addition, facial characteristics can be used to identify race, gender, ethnicity, and other characteristics that could potentially be used to discriminate or otherwise cause harm.

Algorithms for facial recognition can show varying degrees of bias against certain demographics of a population if they have not been trained on a sufficiently diverse gallery of face images or different environmental conditions.<sup>10</sup>

The use of facial recognition using uncontrolled capture devices such as mobiles has greatly increased. Using these uncontrolled devices can create a number of challenges including:

- Illumination
- Sharpness
- Detection confidence
- Inter-eye pixel measurement
- Pose deviation
- Resolution

For instances where the user is responsible for the acquisition process, there is limited opportunity to provide instruction or correction for presentation of the biometric. Any instructions should, therefore, focus on key aspects, pose, and lighting as that can have more significant impacts on the acquisition of a high-quality face image. In some unsupervised use cases, the acquisition process may also include liveness detection features for the purposes of presentation attack detection. Inclusion of this technology in the acquisition can have an impact on the ability to capture a high-quality biometric as it could require the user to alter behavior. The user instructions, including the use of presentation attack detection technology, should also address accessibility issues where it may prove more challenging for specific users to provide a high-quality biometric. These user instructions could be, for example, supported using both visual and audio cues.

---

<sup>10</sup> McLaughlin, Michael, and Daniel Castro. 2020. "The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist nor Sexist." ITIF (Information Technology & Innovation Foundation), January 27. <https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms>.

## The use of facial recognition technology therefore brings a unique set of risks, including:

- *Function creep.* The risk that a FRT system will be used for something other than its original purpose (or that it is used for new or additional purposes where the raw data is obtained from existing databases or sources, e.g., social media channels). This is a particular issue for identification use cases where a system designed for verification could, for instance, be expanded for surveillance or where a system established for deduplication is used to match against social media or using data acquired via closed circuit television (CCTV) or any smartphone camera.
- *Data breach.* The risk of biometric data being accessed, read or removed by an unauthorized source. FRT systems are often more sensitive to such breaches as the facial images can be more easily misused. This is especially concerning for databases that contain tagged images; however, even without labels a face can be potentially matched to social media images.
- *Potential discrimination.* Discrimination risks arise in different contexts including (1) positive discrimination, which includes the possibility that the biometric data held in FRT systems could be used to discriminate against people with certain identifying features (e.g., race or sex), and (2) the burden of inaccuracy falling disproportionately on particular races or genders.
- *Reputational damage.* The risk of public opinion and trust in the system being diminished by poor management or breaches of the system. For face systems this issue may be compounded compared to other modalities as the data can be widely used to match against other sources such as social media.
- *Spoofing (liveness detection).* Face recognition systems can be subject to a range of vulnerabilities including masks or presentation of photo or videos. Many systems today incorporate processes or algorithms to help detect and prevent this type of attack, however it is important to realize that this threat is on-going and attacks will likely become more sophisticated over time.
- *Morphing.* Taking two or more images of different people and creating a single look-alike facial image can be matched with either or both of the source facial image identities.
- *Privacy.* Better matching performance for certain groups of people may increase the risk of bias. Also, sharing of facial data is added to the risk of surveillance, while security breaches leave the data exposed to the perpetrators.
- *Genetic distinctiveness.* There is an intrinsic limitation of the distinctiveness of the face due to genetic factors (e.g., twins may be identified as the same individual).
- *Conditional suitability.* The stability and uniformity of performance is limited in unconstrained conditions.

## 2.4. Iris Recognition

Iris recognition is highly suitable as a technique for large-scale de-duplication systems due to its high accuracy, non-contact acquisition, and low number of exception cases. It can also be combined with fingerprint or face recognition. For example, during Somaliland voter registration and in exceptionally populous areas (e.g., in India), iris recognition proves to be a viable replacement or addition to fingerprinting.

Iris recognition utilises the distinct patterns of the iris muscle that contains a variety of features including collagenous fibers, crypts, color, rifts, and coronas. This pattern is set prior to birth and undergoes minimal change after the first two years of life. This makes it a typically very stable biometric. Iris recognition systems function on near-infrared (NIR) wavelengths. This is because melanin, the pigment that darkens

the eyes, is nearly transparent in NIR and, thus, the stromal structure behind becomes more visible. Iris recognition reads between the edge of the pupil and the outer edge of the iris. The unique shape and location of distinguishing features are marked on a "map."

- Iris recognition is a highly accurate and automated method of biometric identification of someone's unique and stable eye patterns using pattern-recognition techniques. Iris recognition may also provide good protection against spoofing and other attacks.

### 2.4.1. Advantages

**Iris recognition systems have several advantages including:**

- Higher levels of resistant against attack—protection against spoofing and other attacks.
- Iris information is more difficult to capture covertly. Iris data cannot be reliably extracted from normal optical photos.
- As the iris capture is non-contact, iris capture equipment is not subject to wear or damage as fingerprint systems.
- While the eye can suffer from a range of issues, a very high percentage of the population has at least one iris that can be reliably captured. Irises are also less affected by occupation than fingerprints.
- Iris patterns are very stable over time, which removes or reduces the need for recapture to keep the biometric templates current.

### 2.4.2. Disadvantages and Risks

**Iris systems can be expensive to implement, requiring relatively niche capture devices.** Capture for iris systems is more controlled than some other modalities. Potential issues include eye rotation, pupil dilation, occlusion, movement, environment, eyelash obscuration, glare, and height.

**Iris systems may also exclude subsets of the population, including those with medical conditions such cataracts and glaucoma.** Depending on the type, the use of glasses or contact lenses can also cause acquisition issues in some cases. Improving capture technology, both hardware and software, has reduced these issues.

Additionally, the ability of the iris to respond to light in the same way decreases with age and as such may require recapture. Some Iris systems can also have issues with usability (because of iris camera placement) as well as failures due to health conditions or contact lenses. Like facial recognition, it is possible to capture high-quality iris images from a distance without the knowledge of the user, however, it should be noted that this is more difficult to successfully accomplish for iris than for facial recognition.



# 3. Other Modalities

**Although face, finger, and iris are the most commonly used biometric modalities for ID systems, there are several other biometric modality options that have been used for specific purposes,** mostly in functional ID systems used to deliver benefits or authenticate people for specific transactions. The following modalities are in various stages of maturity and exhibit their own unique strengths and weaknesses.

Many of the challenges presented by these biometric modalities (usually a lack of reliability, accuracy, availability, or maturity) have resulted in a preference for face, finger, and iris recognition as the most widely used biometrics for foundational ID systems that generally seek to cover the entire population. As such, the following modalities might be considered as possible secondary or tertiary biometrics comprising a single part of a multi-modal system and not as the primary or sole biometric modality.

## 3.1. Voice Recognition

**Voice recognition is the use of the distinctive patterns of a person's speech for biometric verification.** Vocal characteristics are based on both the physical aspects of the vocal cords and the episodic nature of the local accent. One of its primary uses is for the verification of telephone transactions. As speaker verification is behavioral as well as physiological, there are two types:

1. Text-dependent recognition relies on the same word or words to be spoken as were enrolled.
2. Text-independent recognition that attempts to identify a speaker regardless of what is being said.

Many complex biological factors go into the production of speech including the movement of tongue, lips, and larynx and the relative sizes of the nasal and oral cavities. In addition, speech accent is affected by both regional and societal factors.

**Voice biometrics are commonplace in customer authentication systems for government agencies, banks, and other financial institutions.** The unique characteristics, variability, and types of passphrases used in these types of systems provide significant challenges in performance, vulnerability, and usability including:

- *Stress.* The fundamental frequency of voice can be significantly elevated under stress conditions. This is seen in raised pitch and a change in speaking cadence. Some systems have sought to use this as a simple lie detection mechanism; however, since the reaction to stress varies greatly, it is a rough guide at best.

- *Colds.* Colds that affect the nasal passage or the throat will have some impact on the quality of vocal data depending on severity. Where the vocal characteristics are dramatically changed, it makes recognition from a good quality enrollment almost impossible.
- *Background noise.* Most speaker systems do not operate in an acoustically isolated environment, and background noise is always likely to be present to some degree. Where the volume levels of the background are significant, the vocal frequencies can become obscured. Noises that operate in the same spectrum as the human voice will cause the worst distortion.
- *Mobile phones and voice over internet protocol (voice over IP or VoIP).* Mobile phones and calls made through the Internet are highly compressed to transmit vocal data efficiently. The compression codecs cause artifacts in the vocal signal that can reduce recognition performance. In addition, dropouts caused by transmission delays or blockages also create artifacts.
- *Channel mixing.* When a person enrolls on one type of device (e.g., a fixed-line phone) and then verifies on a different line type (e.g., a cellular phone), this is called "mixing channels." Because of the different characteristics of the channels, the frequency information can be quite different. For this reason, some systems require separate enrollments for each channel.
- *Speaker phones.* Speaker phones change the audio qualities of the voice and are more likely to be affected by background noise.
- *Text recognition.* Text-dependent recognition is concerned mainly with distinguishing one speaker from another as opposed to ensuring that the enrolled word or words are spoken. If a similar sounding but different word is spoken, it may still match successfully. To address this issue, it is often the case that a speech recognition system must be incorporated.
- *Mimics.* Some people are very talented at mimicking other voices. Whilst these individuals sound similar, the vocal signature still contains traces of the underlying physiology.
- *Relations.* People who are closely related to each other or are of the same gender and similar age may have very similar vocal physiology and speech style. Some testing results suggest that these individuals, while at an elevated risk of misidentification, can still be distinguished from one another.
- *Age and disability.* Speech changes with age for all people; however, it is particularly apparent for males during puberty. In addition, people who are deaf, hard of hearing, or non-verbal may have difficulties with voice recognition or using call-based services.

## 3.2. 3D Facial Geometry

**Three-dimensional face recognition uses various sensing technologies to determine the geometry of the face.** This structure reflects the underlying skeletal foundations of the face more directly than can be obtained using two-dimensional face data. Various sensing schemes have been used for acquisition, falling into three classes: (1) passive sensing—stereo cameras that look for pixel-to-pixel correlation using two cameras separated by a fixed distance, (2) active sensing—projecting a structured light onto the face (e.g., a grid) and noting the distortions in position that are caused by the facial geometry, and (3) hybrid sensing that combines aspects of both passive and active sensing. Challenges of three-dimensional (3D) facial recognition include:

- *3D rotation.* Depending on the geometry, reader information on range may be obtained from a single direction. This will cause occlusions as the head is rotated around its axis away from the camera.
- *Noise.* Depending on the technology used to sense the geometry, there may be spikes, pits, and holes in the acquired surface geometry.



- *Movement.* The sensing of 3D geometry may be slower than a camera frame rate, hence it may lead to artifacts if the subject moves during acquisition.
- *Expression.* Facial expressions can radically change the geometry of the cheeks, mouth, and nose. The effects of this are similar to two-dimensional face recognition, however in some cases the effects are more drastic since the information available is only structural not tonal.
- *Glasses.* Glasses cause the eye region to be occluded, since many range sensors are not able to sense through glass.
- *Beards and hair.* 3D geometry systems are more capable of effectively using the structure of the jaw for recognition than two-dimensional face recognition. As a result, beards may affect performance.
- *Antiquity.* During growth years, the facial bones and structure change significantly. Furthermore, the muscles of the face become less tight, which leads to sagging. Both of these effects will alter the apparent geometry of the face.
- *Weight change.* Significant weight change can alter the 3D geometry of the face, although the geometry of facial features around the nose and eyes are less affected.

### 3.3. Vascular Recognition

**The vascular network found just under the skin has been shown to be distinctive and systems using veins for recognition are increasing in popularity for applications such as authenticating banking customers at automated teller machines (ATMs).**<sup>11</sup> They work using a near infrared light transmitted or reflected through a biometric sample, such as a hand, palm, or finger, to map the pattern made by veins. As these systems are non-contact, they are less susceptible to damage than most fingerprint sensors. Possible challenges for vascular recognition systems include:

- *Exercise.* After and during exercise blood is pumped around the body faster. When this is the case, veins are more prominent and warmer, altering their appearance.
- *Stress.* When the body is under stress it can restrict the flow of blood to extremities. This will reduce the near infrared signature of the veins.
- *Environment.* A hot and humid environment, particularly where the user is sweating, may cause distortion of the near infrared signature.
- *Orientation and positioning.* The positioning of the veins under the sensor is subject to three-dimensional rotations that will distort their relative positions.
- *Clothing.* For palm vein recognition, the use of wrist straps or tight watches can change the amount of blood flowing through veins.
- *Weight change.* Changes in subcutaneous fat after enrollment can potentially alter the appearance and relative position of veins.
- *Dermatological damage.* Recent trauma, scars, and disease may all change the apparent position and location of the vein pattern.


---

<sup>11</sup> Korones, Sarah. 2012. "Japan's Palm-Reading ATM." ZDNet, April 14. <https://www.zdnet.com/article/japans-palm-reading-atm/>.



## 3.4. Palm Recognition

**The pattern of lines on the palm of a hand can be used as a biometric.** Traditionally this biometric has been used for forensic-style applications such as policing; however, there are now new technologies, including mobile phones techniques, that are able to read and use the palm for contactless ID-style applications. As this is an emerging field there is not currently significant information on its deployment or accuracy in the context of ID systems. As with all other biometrics, key challenges in its use will be obtaining high-quality images of the palm under a range of different real-world conditions.



# 4. Multi modal Systems

## 4.1. Overview

**The process of fusing (i.e., combining) different biometrics is called multibiometric or multimodal biometric.** It is particularly relevant for large-scale biometric identification and de-duplication systems with millions of enrollment records. For foundational ID systems where multiple biometrics are acquired, such as face, fingerprint, or iris, algorithms are used to fuse different biometric traits to enhance matching accuracy.

## 4.2. Advantages

There are three major benefits to multibiometric recognition:

1. *Improved matching performance.* Using multiple sources of biometric information will improve the overall matching performance leading to a lower FMR and FNMR. In particular for large-scale identification (e.g., de-duplication) systems, the use of multiple biometric sources is often required to yield an acceptable identification performance.
2. *Better inclusion and fault tolerance.* Combining different biometric traits such as fingerprint and iris will ensure that the system can still be used even when certain biometric data is not available or unreliable because of low quality. The improved acquisition performance (e.g., better FTE, FTA, and FTC) will improve the fault tolerance and biometric inclusion rate of individuals that are to be enrolled in a biometric system.
3. *Increased resilience to presentation attacks.* Using multiple sources of biometric information diminishes system vulnerability to presentation attacks as it is more difficult to set up forgeries for multiple modalities.

## 4.3. Disadvantages and Risks

**The improvements of multibiometric systems incur a cost in terms of added complexity, lower acquisition throughput, and increased price.** For example, capturing multiple biometric samples will add complexity

and increase the effort of the acquisition process. They also have the potential to create increased risk of misuse or unwarranted surveillance and exacerbates the severity of security breaches.

Capturing multiple biometric traits often requires additional capture devices increasing the overall cost of the system. After capture, multibiometric systems will require additional storage capacity and increased bandwidth and computation resources. Consequently, the benefits of a multimodal strategy need to be clear.

**In addition, given the unique sensitivity of biometric data used for identification purposes, such data should only be collected where necessary for a narrowly defined and lawful purpose.** Collecting more biometric data than necessary to establish uniqueness or for a specific use case would, therefore, not be justifiable and goes against general data minimization principles.



# 5. Legal Considerations

**A strong, comprehensive legal framework must be in place for biometric systems, as with any ID system.**<sup>12</sup>

Laws governing the operation of ID systems are dependent on a variety of emerging standards in local, national, regional, and international law. Most ID systems do, however, implicate data protection laws, and other human rights laws, conventions or covenants.

The policies, laws, and regulations that support an ID system can be divided into two categories:

1. *Enablers*. Laws and regulations that directly define and govern the ID system, including its design, management, operation, and relationships with stakeholders and other systems.
2. *Safeguards*. Laws and regulations that address potential risks surrounding the ID system, including those related to data protection, security, and non-discrimination.

Enabling legal frameworks are important to clearly articulate the scope and purpose of ID systems, as well as to specify governance, oversight, and accountability mechanisms. In terms of safeguards, enabling laws can be tailored to account for the unique risks associated with an ID system, or they can cross-reference existing laws or regulations that adapt generally applicable safeguards, including with respect to data protection, data security, and other civil and human rights protections (to the extent they exist in the relevant jurisdiction). When biometric technology is used, this should be incorporated into / appropriately covered by both these enablers and safeguards.

## 5.1. Enabling Laws and Regulations

In some jurisdictions, specific laws and regulations establish national ID systems, sometimes mandating the use of official national ID cards or documents. Examples include the National ID Card and Registry Law in Brazil,<sup>13</sup> the Aadhaar Act in India,<sup>14</sup> Uganda Citizenship and Immigration Control Act<sup>15</sup> and the Philippine

---

<sup>12</sup> United Nations. 1948. United Nations Declaration of Human Rights, Articles 9 and 10. <https://www.un.org/en/about-us/universal-declaration-of-human-rights> and the ID4D Practitioner's Guide. <https://id4d.worldbank.org/guide>.

<sup>13</sup> Identificação Civil Nacional Law no. 13444/2017.

<sup>14</sup> Ministry of Law and Justice. 2016. "Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016." *The Gazette of India*. New Delhi, India. March 16.

<sup>15</sup> Uganda Citizenship and Immigration Control Act. <https://immigration.go.ug/resources/citizenship-immigration-act-66>.

Identification System Act in the Philippines.<sup>16</sup> These laws typically include provisions on the scope of the relevant ID system, registration and eligibility requirements, the identification and jurisdiction of supervisory authorities, and offenses and penalties, among other provisions.

In other jurisdictions, national ID cards are optional rather than compulsory but can function like a mandatory requirement where their use is ubiquitous or required to access a wide array of important services. For example, the Public Services Card in Ireland, while not compulsory, has come under fire for being necessary to access social welfare payments or to apply for a driving license or passport.<sup>17</sup> Similarly, certain laws and regulations can indirectly impose a kind of national ID scheme by other means. In the United States, for example, advocacy groups have argued that the REAL ID Act,<sup>18</sup> which mandates uniform standards across state drivers' licenses, is a kind of de facto national ID law that would facilitate surveillance and discrimination.<sup>19</sup>

Even in the absence of national ID regulations, other laws and regulations may govern the use of systems relevant in the identity context. Examples include the regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) in Europe<sup>20</sup> and the emerging United Nations Commission on International Trade Law (UNCITRAL) framework for cross-border recognition of identity management and trust services.<sup>21</sup>

## 5.2. Data Protection Laws

### 5.2.1. Overview, Key Issues, and Emerging Trends

**One of the most important legal safeguards in the context of biometric-enabled national ID systems can be found in data protection laws.** The more comprehensive of these laws tend to differentiate between ordinary personal data and special or sensitive categories of personal data that require heightened protections and are subject to additional restrictions (or even prohibitions) on processing.<sup>22</sup>

**Biometric data used for identification purposes are almost always deemed special or sensitive<sup>23</sup> due to their ability to uniquely identify an individual.** Thus, ID systems that utilize biometrics are typically subject to heightened requirements and restrictions, in addition to all of the generally applicable requirements

---

16 An act establishing the Filipino Identification System, Republic Act No. 11055, July 24, 2017.

17 Privacy International. 2019. "The Irish Public Services Card, a de facto ID." <https://privacyinternational.org/examples/2877/irish-public-services-card-de-facto-id>.

18 The REAL ID Act of 2005, Pub. L. 109-13, 119 Stat. 302, enacted May 11, 2005.

19 EPIC.org (Electronic Privacy Information Center). 2020. "National ID and the REAL ID Act." [https://archive.epic.org/privacy/id\\_cards/](https://archive.epic.org/privacy/id_cards/).

20 Publications Office of the European Union. 2014. "Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 and repealing Directive 1999/93/EC." <https://op.europa.eu/en/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-en>.

21 UN Commission on International Trade Law. 2022. *Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services* (available at: <https://uncitral.un.org/en/commission>). This instrument was approved by the Commission in July 2022. A final version is not available at the time of writing.

22 The General Data Protection Regulation (GDPR) is one example of such a law. In order to process "special category data" (which includes data about race or ethnicity, religion, and sexual orientation), the GDPR requires a lawful basis to be met under Article 6 and a special condition for processing special category data to be met under Article 9. <https://gdpr.eu/article-9-processing-special-categories-of-personal-data-prohibited/>.

23 Argentina Presidencia: Boletín Oficial de la Republica Argentina. 2019. "Agencia de Acceso a la Información Pública. Resolution No. 4/2019." <https://www.boletinoficial.gob.ar/detalleAviso/primera/200224/20190116>.

under those laws.<sup>24</sup> While there may be exemptions that apply to the processing of sensitive biometric data, particularly in the context of the exercise of public authority or law enforcement, such exemptions should be very narrow and reliance on them should be carefully monitored and enforced.<sup>25</sup> In many cases, for example under General Data Protection Regulation (GDPR) in the European Union, the processing of sensitive (including biometric) data must be deemed "necessary" for narrowly prescribed purposes.<sup>26</sup> This means that, in order to rely on an exemption, there can be no other reasonable and less intrusive way to achieve the purpose.

**Most foundational ID systems mandate participation and enrollment; therefore, consent is unlikely to be a suitable lawful basis for the associated processing of biometric data.** The imbalance of power between individuals and public authorities also means that the former may feel pressured to give their consent even if not mandatory (especially if failure to give consent means they may not access a particular government service or benefit). Rather than relying on consent, a public authority should, therefore, be required to demonstrate that the collection of biometric data is necessary for a reason of substantial public interest on the basis of a law that contains adequate safeguards (such as an enabling law for an ID system).

### 5.2.2. Minimum Protections

**To ensure the legitimacy of an ID system incorporating biometrics, such a system should be necessary for a task carried out in the substantial public interest, with a clear basis in a law that applies to the ID system owner/operator and that provides adequate safeguards to data subjects.**<sup>27</sup> In practice, it should, therefore, be demonstrated at the outset that:

- The ID system will bring concrete and tangible benefits to the public.
- Incorporating biometrics in the ID system is a targeted and proportionate way of achieving such aims. To ensure that there are no other reasonable and less intrusive options, a clear justification for using certain biometrics over alternatives (including non-biometric modalities) should be articulated.
- The ID system has a clear basis in a law that applies to the ID system owner is proportionate to the public interest aims pursued and provides adequate data protection safeguards.

At a minimum, the applicable legal framework should contain the following safeguards: robust requirements in respect of key data protection principles (i.e., lawfulness and transparency, purpose limitation, data minimization, accuracy, storage limitation, and data security); data subject rights (including to access, rectification, and erasure of data where appropriate);<sup>28</sup> cross-border data transfers; third party access to data; data breach notification, remedies, and penalties; and independent oversight in terms of monitoring and enforcement.

---

24 European Data Protection Board. 2020. *Guidelines 3/2019 on Processing of Personal Data through Video Devices*. [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en).

25 South African Government. 2013. "Protection of Personal Information Act No. 4 of 2013, Section 6." <https://www.gov.za/documents/protection-personal-information-act>.

26 GDPR.

27 Mirroring the equivalent legal position under the GDPR (Articles 6(1)(e) and 9(2)).

28 Under the GDPR the right to erasure does not apply where data processing is necessary for a task carried out in the public interest or in the exercise of official authority, as would be the case for much data held in a foundational ID system.

The following safeguards should also be considered by the ID system owner, irrespective of whether they are expressly mandated by relevant laws:

- A data protection officer (DPO) should be appointed. A DPO is an independent expert in data protection law and practices, whose role is to advise on and monitor legal compliance, advise on data protection impact assessments, provide training to staff, and to cooperate with the applicable data protection authority.
- Individuals should not be subject to solely automated decisions based on the processing of their biometric data, where such decisions have legal or other significant effects (subject to limited exceptions).<sup>29</sup>
- Appropriate technical and organizational safeguards should be designed, documented, and implemented to protect biometric data collected, stored, and processed, including appropriate safeguards to prevent the unauthorized access, use, or disclosure of personal data.
- Data protection and privacy by design policy documents should be documented and implemented to guide the design, development, and evolving use of biometrics in the ID system.
- A written data breach notification policy should be designed, documented, and implemented.
- A data protection impact assessment (DPIA) should be undertaken prior to deploying biometrics in the context of the ID system. The DPIA should be reviewed by the DPO, and a new DPIA should be undertaken if there is a change to the nature, scope, context, or purposes of the data processing.<sup>30</sup>
- A policy document should be maintained, explaining what procedures are in place to ensure that the processing of biometric data as part of the ID system is in compliance with data protection law, particularly key principles around lawfulness and transparency, purpose limitation, data minimization, accuracy, storage limitation, and security.<sup>31</sup>
- Transparency and accountability should be facilitated through the use of clear privacy notices, policies, and other supplemental documents, including, where appropriate, the use of signs or symbols to indicate the use and purposes for using biometric data. See Transparency section below for more detail.
- A clear mechanism for the exercise of individual rights should be implemented, including rights of access, information, rectification, and erasure, where appropriate.
- A clear mechanism for human intervention should be implemented in the event of objections, refusal, concerns, malfunctions, or other issues that may arise with respect to the use of biometrics in a given ID system.
- Written policies should be implemented with respect to governance and oversight of all data protection and privacy requirements, policies, and procedures related to the use of biometric data.
- Cross-border transfers of biometric data should be reviewed and monitored to ensure compliance with relevant restrictions on transfers and other applicable laws.

---

29 See, e.g., Article 22 of the GDPR. <https://gdpr.eu/article-22-automated-individual-decision-making/>.

30 See, e.g., Article 35 of the GDPR. <https://gdpr.eu/article-35-impact-assessment/>.

31 Mirroring the requirement under Schedule 1, Part 4 of the UK Data Protection Act, for controllers undertaking certain special category data processing to have an “appropriate policy document” in place. <https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted>.

- Mechanisms should be implemented for the of biometric data by internal and external authorities, including any privacy or data protection supervisory authorities.

### **5.2.3. Transparency and Dialogue**

To maintain public trust, governments that implement biometric-enabled ID systems should provide additional transparency throughout all stages of the system life cycle, from the point of enrollment and data collection to participation and use of the system and including any ultimate exit from the system or destruction of data or records relating to an enrolled individual. Such transparency should address the types and nature of data collected (e.g., whether it is sensitive or a “special category” under the relevant laws, as should always be the case in respect of biometric data used for identification purposes), its intended uses, its intended recipients, the individual’s rights in respect of that data, and other relevant considerations.

This information might be presented in a separate, straightforward, and easily comprehensible notice or statement regarding the use of biometric data, in additional notices during the onboarding and intake process, and at relevant milestones. It should always include a clear statement on the mechanisms for users exercising their rights, including a relevant point of contact. That said, it is not sufficient to make the information available to the public. Further outreach and educational efforts should be undertaken to ensure the public truly understands the implications of the system and their rights in relation to it and have a mechanism for obtaining answers or further clarification. For more guidance, see forthcoming ID4D guides on CSO engagement and communications.

### **5.2.4. Data Sharing and Cross-Border Data Transfers**

Contractual protections should be implemented to ensure that any personal data in an ID system (including biometric) is not transferred to another country or accessed by third parties other than in limited circumstances and where this is in accordance with law. More detail on managing third parties is contained in Section 7.13.1.

### **5.2.5. External and Internal Access**

A range of government stakeholders such as the security services or police may wish to have access to biometric data. Therefore, different jurisdictions will have differing legal controls on the level and acceptability of access to an ID system data by these external bodies. Good data protection practice dictates, however, that the individual should know what access these agencies have and the circumstances under which it is provided. Uncontrolled search access to such a system by external policing agencies, in addition creating to data protection issues, is likely lead to a loss of faith in the system, thereby undermining it.



## 5.3. Oversight

### 5.3.1. Institutional Oversight

**Most government agencies that operate ID systems have review boards or other audit activities in place as part of standard operations.** As a best practice, these agencies should establish a dedicated review board to provide oversight of all aspects related to the ethics, privacy, and security of the ID system. Such a board should be concerned with all policies relating to retention, usage, and amendment of data in the biometric system. The board should have the power to ensure policies are being followed, investigate where there are concerns, and examine any new proposals or changes to the system's operation.

**The board should also be accountable to an independent oversight body.** Independent authorities should also be established to monitor and ensure compliance with the rules and regulations relating to the operation of ID systems. These agencies should be involved in (i) receiving and resolving complaints with respect to access to and usage of the system, errors, privacy, and security; (ii) conducting investigations; (iii) ensuring individuals are able to exercise their rights under the law; (iv) implementing remedies; and (v) resolving disputes.

### 5.3.2. Independent Government Authority

**Some countries (such as Israel and the United Kingdom) have appointed a biometric commissioner to provide independent oversight of specific government usages of biometric information, while other countries rely on an independent data protection authority** to regulate the processing of biometric data in both the public and private sectors.

The powers of such bodies vary, but in principle, the purpose is to provide confidence to the public that there is a truly independent and knowledgeable third party to ensure that policies are followed and to provide redress where they have been violated. For example, the UK Biometrics Commissioner has quite a narrow role in reviewing the use of DNA samples, profiles, and fingerprints by Police. The Commissioner provides oversight but has no regulatory powers. By and large most regulation of biometric data in the UK is done by the data protection authority, the Information Commissioner's Office (ICO).

They are established to be a voice and advocate for the public and so should not be controlled by governmental or departmental objectives. It is critical that engagement with the relevant independent government authority take place early in the process of establishing a foundational ID system.

The responsibilities of an independent government authority should include, inter alia:

- Monitoring and enforcing the application of data protection policies and regulations related to the use of biometric data.
- Promoting public awareness and understanding of the risks, rules, safeguards, and rights in relation to processing based on and data derived from biometric data.
- Advising on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing based on biometric data.
- Promoting the awareness of controllers and processors of their obligations.
- Upon request, providing information to any data subject concerning the exercise of their rights in respect of biometric data collected or processed via the ID system.

- Handling and investigating complaints and informing the complainant of the progress and the outcome of the investigation.
- Cooperating with other supervisory authorities with a view to ensuring the consistency of application and enforcement of privacy protection policies and regulations related to the use of biometric data.
- Conducting investigations on the application of data protection policies and regulations.
- Monitoring relevant developments that have an impact on the protection of biometric data.
- Fulfilling any other tasks related to the protection of biometric data.

For such bodies to be effective, they require a meaningful penalty mechanism as well as appropriate investigative powers. As a general matter, privacy and data protection regulators are quite well equipped to deal with the unique considerations associated with biometric data. The only independent regulatory body with oversight over use of biometrics in the UK is the ICO (the data protection authority). The UK Biometrics Commissioner has no regulatory powers and is narrowly focused on the use of DNA and fingerprints by police. It will be important to consider capacity risks and the potential for undue complexity if separate oversight mechanisms existed for data protection on the one hand and biometrics on the other. Many of the tasks listed above are standard functions of a general data protection regulator. Targeted regulation of biometrics may be warranted in certain circumstances, for example, in the case of live facial recognition technology used by law enforcement where issues around bias and discrimination and surveillance are particularly acute and the social license risks are particularly significant.

## 5.4. Civil, Political, Constitutional, and Human Rights Law

**The use of biometric data can implicate civil, political, and constitutional rights, as well as international human rights laws and norms, and national laws enshrining them.** For example, in addition to data protection rights, the misuse of facial recognition in particular can have an impact on individual rights to freedom of expression and to hold opinions without interference,<sup>32</sup> the right to freedom of peaceful assembly and association,<sup>33</sup> as well as rights to equality and non-discrimination.<sup>34</sup>

## 5.5. Inclusion

Most foundational ID schemes are primarily designed to provide access to services. Where such services are denied, segments of the population can be disenfranchised and prevented from accessing vital government services. Careful consideration must be given to the costs and processes for registration, particularly for those from rural or poorer areas. For example, with facial recognition systems, a technical barrier can be ensuring quality photographs in less controlled environments and the impacts of demographic bias (such as age, sex, ethnicity, etc.) and cultural barriers (such as obscuration of the face with religious or cultural clothing) on the inclusion must be considered. Options for those that wish to opt-out, or cannot be enrolled, should be considered at the design stage.

---

32 United Nations. 1948. United Nations Declaration of Human Rights, Article 19. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

33 United Nations General Assembly. 2017. Resolution adopted by the Human Rights Council on 23 March 2017 34/7 The right to privacy in the digital age. <https://digitallibrary.un.org/record/1307661>.

34 United Nations. 1976. International Covenant on Civil and Political Rights, Articles 2 and 26. [https://treaties.un.org/doc/Treaties/1976/03/19760323%2006-17%20AM/Ch\\_IV\\_04.pdf](https://treaties.un.org/doc/Treaties/1976/03/19760323%2006-17%20AM/Ch_IV_04.pdf).

## 5.6. External and Internal Access

Biometric systems are subject to a range of other government stakeholders from external departments, such as the security services or police, that may wish to have access to the biometric holdings. Different jurisdictions will have differing legal controls on the level and acceptability of access by these external bodies. Good data protection practice dictates, however, that the citizen should know what access these agencies have and the circumstances under which it is provided. Uncontrolled search access to such a system by external policing agencies, in addition to data protection issues, is likely lead to a loss of faith by citizens and, hence, undermine the core strength of a foundation ID system.

# 6. Technical Considerations

In addition to the legal aspects described above, this section describes a number of important technical considerations for biometrics in ID systems, including data security and storage, data protection/privacy-by-design features, data traceability, system performance, and interoperability and standards.

Technical mitigations that assist with protection of any data include:

- End-to-end encryption of data both in-transit and at rest
- Data anonymization and pseudonymization wherever possible
- System confidentiality and integrity
- Data backups
- Ongoing assurance mechanisms
- Digital certification and public key infrastructure (PKI)
- Access and control platforms
- Robust logging

**In addition, biometric specific technical risk mitigations include:**

- *Liveness (or suspicious presentation detection) mitigations.* These include sensors that detect liveness and aim to prevent the use of artifacts like silicon masks. Liveness algorithms can operate both on device and the server. The privacy-preserving aspect of this relates to the overall security of the system against attack.
- *Tamper mitigations.* The integrity of the capture device can be both electronically tested and physically secured to ensure that no modifications or substitution have been undertaken. Tamper-proofing might include digitally signing the image to associate it with the sensor or physically sealing all the internal hardware in resin and using electronic sensors to detect if tampering has occurred.
- *Biometric template protections.* Techniques to limit the use of the biometric matching data to preserve different aspects of privacy, including restrictions on identification and cross-matching.

**Biometric data should be securely stored and protected to prevent processing by unauthorized parties, loss, theft, and unwanted destruction and damage.** Given the increasing occurrence of large-scale cyber-attacks on IT systems (including well-documented cases of breached systems holding biometrics), it is vital to ensure that data is adequately secured. The biometric data must be protected throughout all system components and during all phases of the system lifecycle.

## 6.1. Data Security and Storage

**Biometric data used for identification purposes is especially sensitive and so needs to be protected with greater rigor than most types of personal data.** This is particularly the case for large-scale and government ID systems since they are an active target for sophisticated internal and external attacks, leading to potential data breaches. Many of the controls listed are the same as those needed for any large-scale identity system such as ISO/IEC 27001 and ISO/IEC 29100 from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). These standards support defining system security and data protection safeguarding requirements.

### 6.1.1. Raw Enrollment Data

**Raw biometric data (known as the biometric sample) is data gathered directly from the sensor before any processing has been carried out.** Biometric systems usually operate by taking the raw biometric data and converting this to a biometric template for storing and matching. The original raw data is then only required for two purposes:

- *Manual adjudication.* Human inspection of data, therefore, to make an informed judgement about the accuracy or quality of the algorithm match or matches.
- *Re-templating.* Templates are mostly unique both to specific algorithms from a vendor and to updated algorithms frequently also have different templates. This means that an upgrade is quite likely to involve the re-templating (converting all the images to templates) of the existing database.

**Both requirements mean that it is usually too impractical and expensive to remove the original raw data.** This original biometric data is sensitive and should be separated from the template and personal data.

### 6.1.2. ABIS and AFIS

Both ABIS (automated biometric identification system) and AFIS (automated fingerprint identification system) are software applications designed to undertake end-to-end enrollment, matching, and management of biometric information. AFIS relate mainly to policing systems as they are focused on fingerprints. More modern systems (ABIS) support multiple and different types of biometrics. Some common examples of ABIS systems include fingerprint, face, and iris.<sup>35</sup>

### 6.1.3. Cloud Storage

**Biometric data is considered sensitive personal information. As such, it is usually treated as sovereign data that must be stored onshore within a country.** Options exist (and are utilized by some major biometric implementations) that host data external to a government agency but still within private clouds established

---

<sup>35</sup> As an example of an ABIS system see UNHCR (United Nations High Commissioner for Refugees). 2015. "Biometric Identity Management System." <https://www.unhcr.org/uk/protection/basic/550c304c9/biometric-identity-management-system.html>.

onshore with the appropriate level of security and control. The choice to host the biometrics solution externally must be informed by strict data access controls and high levels of independent assessments for both physical and logical security solutions. Independent assurance should also be provided to ensure all data is stored in the country of origin and that no third parties can access or transmit this data.

#### 6.1.4. Biometric Template Protection and Biometric Encryption

Raw biometric data (known as the biometric sample) is data gathered directly from the sensor before any processing has been carried out. Almost all biometric system have or use templates which are derived from the raw biometric data. A template is the refined, processed, and stored representation of the distinguishing characteristics of a particular individual. The template is the data that gets stored during enrollment and which later will be used for matching. Because of variations in the way a biometric sample is captured, two templates from the same biometric will never be identical. This is the origin of the probabilistic nature of biometrics, as the matching process can only give a decision confidence, not an absolute assurance.

**Biometric template protection, or biometric encryption, is a method that increases the difficulty of accessing biometric information from stored data.** This involves mechanisms to restrict the use of the

biometric through active changes to the information stored. These mechanisms can introduce restrictions for the use of the biometric system for the purposes of

- *Identification.* The searching (1:N) of a database for a matching identity.
- *Authentication.* The validation of an identity (1:1) using a biometric.
- *Inspection.* Allowing a visual inspection of an image by an operator or officer.
- *Resolution and adjudication.* The process of manually examining the outcomes of close biometric matches.
- *Cross matching.* The cross-linking of biometric databases based on template-to-template matching.

**While it is technically possible to generate an image from a biometric template, it is not a practical attack vector in most cases.** This process, called "hill-climbing," relies on having access to the original algorithm that was used to generate the template and successively updating an initially random image until the new image is closer and closer to generating the same template. Hill-climbing is considered successful once the new image is close enough to the original template to pass as a biometric match, even when the image itself might look substantially different from the original image. The computing power and setup required to do this has traditionally meant this type of attack was more complex than alternative attack mechanisms (although with faster computing available this may not continue to be the case).

- *Crypto biometrics.* Cryptographic biometrics, or "crypto biometrics," refers to the practice of separately encrypting each template with a unique key. This ensures that the templates cannot be easily searched, since this involves decrypting each template that requires matching. It can provide an effective limitation against using a biometric system for unauthorised identification.
- *Unique template key.* To prevent the use of stolen templates, unique templates can be created that are specifically designed for the deployed algorithm. This means that any stolen templates would not be useful on any other system. It also restricts the ability to match templates across systems (this does not prevent such matching where the raw biometric is retained).
- *Homomorphic encryption.* Homomorphic encryption is an emerging technique that allows computations to be carried out on encrypted templates, thus generating a result without decrypting the templates. The value of this encryption is that stolen templates are of limited value since they

cannot be easily decrypted without the correct keys. While this does allow for identification, it prevents cross-matching against other data sources where the original biometric is still accessible. While a new standard (IEEE2410-2021) exists for this technology, commercial offerings are currently limited.

### 6.1.5. Digital Signatures and PKI

**All records should be stored on encrypted media so that physical removal of this media does not compromise security.** Transmission of any data should only be done using best-practice encryption techniques, and care should be taken to ensure that no residual data is cached. Backup storage and management must also be considered to ensure that no information is accidentally leaked during the backup or restore process. Digital signatures should be used whenever possible to detect data changes. ISO/IEC 27001 specifies the control mechanisms in some detail.

### 6.1.6. Personal Access and Control

**A foundational aspect of data protection principles, such as those enshrined in GDPR, is to ensure that individuals are made aware of how their personal data is collected and used and how to request corrections, changes or, in some circumstances, erasure of that data.** In a biometric system, individuals might be entitled to know when records of their biometric data have been changed or amended, access to any personal information stored against their records, and any matches or results of processing their biometric data. The system owner or operator should also provide a mechanism for redress through a request to exercise certain individual rights.

## 6.2. Data Protection/Privacy-by-Design Features

**Privacy-by-Design (PbD) embodies the concept that data protection considerations should be addressed ex-ante, at the heart of organizational operations, and not merely mitigated ex-post through regulation and enforcement.** PbD incorporates data protection into the design of the system, including architecture and design specifications. It is notable that, under the GDPR, PbD considerations must inform all data processing activities from their inception to conclusion.<sup>36</sup> The PbD framework has several core requirements (Table 1.2).<sup>37</sup>

---

<sup>36</sup> GDPR, Article 25. <https://gdpr.eu/article-25-data-protection-by-design/>.

<sup>37</sup> Cavoukian, Ann, Michelle Chibba, and Alex Stoianov. 2012. "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment." *Review of Policy Research* 29 (1): 37–61.

**Table 1.2. Requirements of Data Protection/Privacy-by-Design**

PbD requirement	General implications	Implications for biometrics
<b>1. Proactive not reactive; preventative not remedial</b>	Proactive not reactive; preventative not remedial: A system built around the PbD approach attempts to predict events that could impact user privacy before they occur. A true PbD framework does not dictate how to remediate breaches that have already occurred, as they are mitigated before they surface.	In the context of biometrics, this means ensuring that comprehensive risk analysis or Data Protection Impact Assessment (DPIA) is considered before, during, and after system implementation and informs the decision on whether/how to adopt biometrics. The security of biometric information is a constantly evolving technology, and a PbD biometric system will consistently attempt to stay ahead of the latest potential threats.
<b>2. Privacy as the default</b>	PbD systems are built to ensure that personal data is inherently protected. This is considered to be the default mode of operation for a system designed around the PbD framework. The system does not rely on the user to actively protect their own information, user information is already protected by default.	In the biometrics context, this means that a system will need to ensure sufficient security layers exist without the user having to opt-in. In essence, their biometric data will be safe as soon as it enters the system. Consider implementing default settings that minimize data collected, processed, and stored, the encryption of data both in transit and at rest, and maximizing localized processing on the individual's personal device(s), among other measures.
<b>3. Privacy embedded into design</b>	PbD systems must be designed using the PbD framework. PbD should not be inserted into the system post-hoc. The intent is to ensure that privacy is considered as a top priority at every stage, from development to production. This also requires having a plan for disaster recovery, resiliency, and alternative or "back-up" methods in the event of interruptions or unavailability of the ID system.	In the biometric context, particularly in cases with limited connectivity, this may require engineering for security and robustness in off-line settings. Consideration of how biometric data is protected and stored at each stage of acquisition and processing is key and should be a fundamental part of system design.
<b>4. Full functionality: positive sum, not zero-sum</b>	Traditionally, the belief has been that to increase security, there must be an equal loss of privacy or functionality. PbD framework aims to optimise outcomes by increasing both at the same time.	In a biometric context, this means that registering with an ID system must not come at the cost of the individual's privacy. Instead, the level of data protection must remain the same or increase using the system. For example, prevent unlawful or unintended correlation or identification of the individual through technical and organizational measures that segregate the biometric and biometric components of the ID system, e.g., avoid storing any other personal data related to the same individual in proximity to images of the individual's face or other biometrics.



PbD requirement	General implications	Implications for biometrics
<b>5. End-to-end security: lifecycle protection</b>	PbD framework dictates that data protection should be embedded into the system at every level, from when data enters the system, to when it is removed.	Biometric data must enter securely, transit securely, and be securely stored and deleted. For example, ensuring and monitoring appropriate authorizations and access controls, including through physical, technical, and organizational measures, applying encryption in transit and at rest to personal and sensitive data where possible, and ensuring that any personnel, entities, or vendors with access also delete their copies of any data at the end of the lifecycle.
<b>6. Visibility and transparency</b>	All moving system mechanics must be independently audited for the purposes of transparency. Stakeholders are assured that all technology implemented is working properly.	The choice of a biometric system and its implementation must be based on trust, but that trust must also be built by outlining how the system operates. Without compromising security, the system should allow transparency of its key operating parameters.
<b>7. Respect for individual privacy</b>	Every PbD system must be built from the belief that the individual's data protection must be respected. The system should empower individuals with a sense of control over their data with strong security, ease of use, and a human-centric design.	Biometrics should only be deployed in ID systems where necessary and proportional. There should be an option to opt-out or provide alternative measures to enroll in the system.

### 6.2.1. Data Separation and Anonymization

**A primary principle to help reduce the impact of data breaches is the separation of sensitive and personal data into different data stores.** The biometric data includes both the original raw data (the images) and the templates. The link between an individual's biometrics and other sensitive and personal data in these data stores should be a unique key that is not used for any other purpose. Should the biometric database be compromised, it should not be possible to link any data back to specific individuals.

**To be effective, the separation must be managed with other technical and organizational controls, including encryption and access controls, to prevent an attacker from easily taking all the data in a single breach.**

### 6.2.2. Limiting Functional Use Cases

**An effective control against function creep is ensuring the system interfaces and functionality are specifically designed to enable a segregation of duties for individuals operating the system and exclude use cases outside of the current functional requirements.** To do this, the system design must be built with an understanding of the specific risks of function creep.

General design considerations must apply both to the direct user interface of the system and any exposed application programming interface (API). Some questions around capabilities that could be limited include:

- *Restrict face biometrics for deduplication.* Some systems limit the use of face biometrics to verification (1:1 facial matching) or simply printing pictures on IDs for manual authentication and so do not feature 1:N type facial matching. This can address concerns about function creep and potential for surveillance.
- *Export.* How does the system prevent the unauthorized viewing, use, or extraction of data (biometrics or other personal data)?
- *Verification.* Can use of the system be limited to a verification functionality without enabling identification? If an identification function is required, could this be restricted to backend batch functionality only?
- *Identity matching and search.* Restrict search (1:N) capability to only deduplication. Other uses have the potential for function creep of surveillance and so should be only enabled where essential.
- *Access.* What data is exposed to different types of system operators? Not all system operators need access to the raw biometric image or other personal data.
- *Watchlist.* How large can a watchlist become, and who has access to the results?
- *Audit: How will inappropriate uses of the system be detected and resolved?*
- *Adjudication.* When close matches occur, how will such cases be decided? How does the system define “close,” and what is the threshold?
- *External matching.* How will access to the system by external parties be managed or restricted? Will it be possible to enable matches from other jurisdictions?

**It is extremely important to engage independent penetration tests against the operational system to ensure that, while a restriction has been put in place, it cannot be easily subverted.**

## 6.3. Data Traceability

### 6.3.1. Logging

**Accurate and complete logging is vital for any large-scale IT system, particularly those involving the management of identities.** Logging should be conducted on all system changes, identifying both the original and changed state, the exact time of the change, as well as identifying the user who made the change. These logs need to be stored and managed in a form that can ensure their integrity for the purpose of audits and other investigations.

**A regulator or independent oversight body should be provided with direct access to these logs and have the ability to check their integrity.** This should facilitate proactive reporting on usage and detect risks of function creep.

### 6.3.2. External Access Control

**Where a system can be accessed by third parties of any type, proactive monitoring for irregular use is vital.** It should be possible to trace precisely all transactions to a particular individual within an organization (not just an organization as a whole).

External users of the system must be warned as part of the terms of service that all transactions will be logged and regularly reviewed. For effective deterrence, the consequences of a detected breach should be in proportion with its severity.

## 6.4. Performance

**Assessed biometric performance can be complex, as performance depends on multiple highly technical factors.**

- *The data set.* Performance accuracy depends on the degree to which the underlying test data matches the real data that is expected to be seen by the system. Where the data is different, the performance results are unlikely to be fully valid. For example, a system that is tested on a population with one main ethnicity or other demographic is likely to perform quite differently when applied to a population with a different mix of demographics.
- *Statistical measures.* The two best-known accuracy statistics are false accept and false reject; however, there is also a range of other different types of statistics. These include the rank one correct identification rate, the false non-match identification rate, and the failure to enroll rate. Each of these aggregate statistics can be useful for interpreting performance; however, choosing the right statistic to meet your solution parameters is important, and it is suggested that expert advice may be required.
- *Configuration and tuning.* Biometric systems have several parameters that control accuracy, such as the threshold and quality settings. Assessed performance is dependent upon the configuration and tuning, and it is important to note this may change between a test system and production.
- *Population size (gallery size).* Performance of biometric systems when undertaking identification changes depending on the size of the gallery. As the gallery size increases the overall identification rate decreases, so performance figures for identification must be interpreted by understanding the size of the test gallery.

### 6.4.1. Configuration

Biometric systems have several parameters that control accuracy such as the threshold and quality settings. An incorrectly tuned biometric system may perform very poorly, either by being easily fooled or by rejecting too many of the correct individuals. For any large system, it is important to recognize the importance of tuning the various parameters after the operation has commenced to ensure optimal performance.

Many modern biometric systems use machine learning to train algorithms. When this is undertaken on enormous numbers of individuals, the algorithm learns to become better and better at recognition. Recently, some implementations have allowed customers to train on their own local data, resulting in more precise algorithms for local conditions. This can be beneficial but must be approached with caution as it is easy to “overfit” the training data so that performance is better on the training data but much worse for new data.

Although it is technically possible to include “online” learning to adjust their accuracy during operation, most implementations where learning is available do this as a batch process. This is because of risks associated with poor or misleading training data arising from mislabeled data (ground truth).

## 6.4.2. Accuracy and Quality

Unlike password-based systems, where a perfect match between two “password” strings is necessary to validate a user’s identity, a biometric system works differently. When measured twice, biometric data are seldom identical. The reasons for this variability may include:

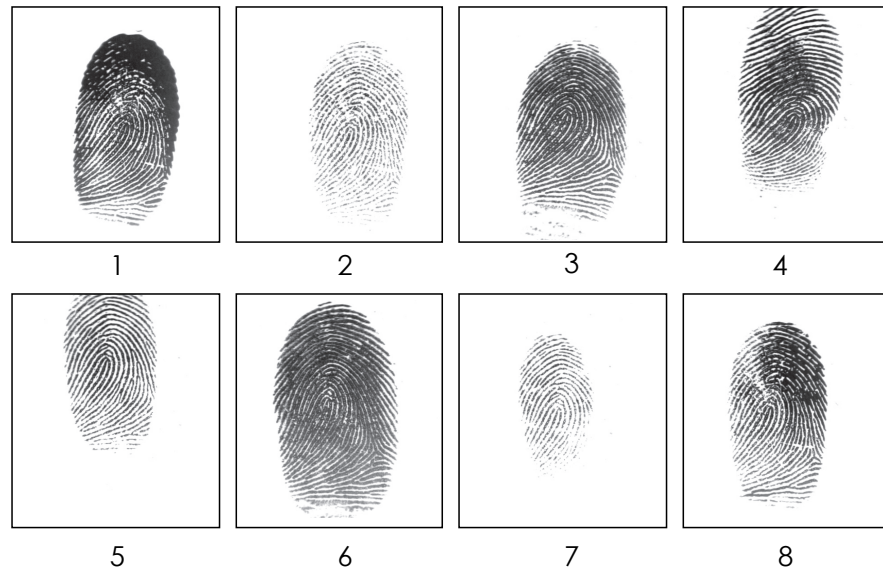
- The use of different scanner types for enrolment and verification.
- Differences in user interaction with the capture device (e.g., exercising more or less pressure on a fingerprint scanner).
- Alterations in the individual’s biometric characteristics (e.g., due to manual labor, accidents, or aging).
- Differences in environmental conditions (e.g., humidity, temperature).
- Differences in operational conditions (e.g., light conditions when capturing the face).
- Differences in operational procedures.

Biometric operations are inherently probabilistic; therefore, it is not possible to say with 100% certainty in most cases that an identity match has positively identified an individual. Sources of misidentification are modality dependant but can include twins, poor quality sample, or a poorly tuned algorithm. Handwritten signatures are currently used to “attest” a transaction for many legal purposes, and the traditional signature is just a type of biometric, while other biometrics have much higher accuracy than signatures. Ultimately, proof of a transaction rests with the legal framework in a jurisdiction and the risk tolerance of the organization using the biometrics.

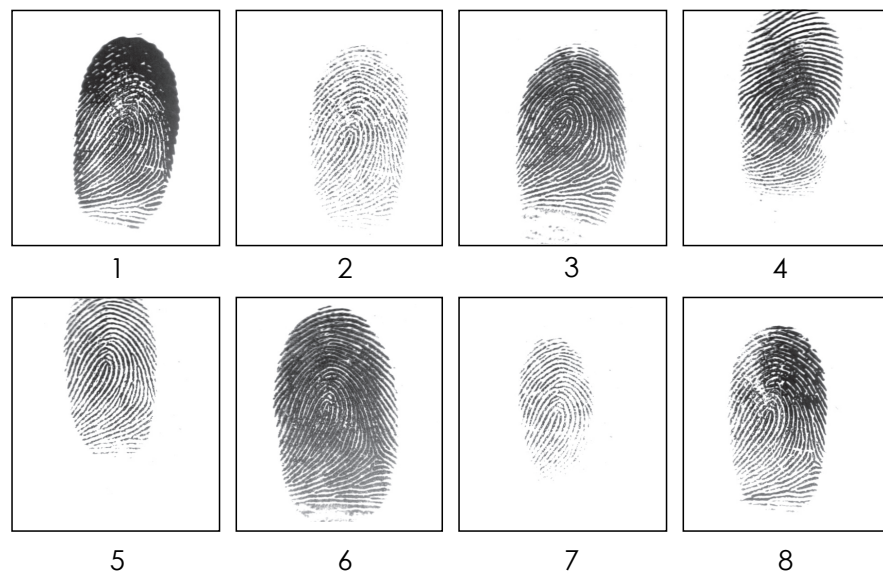
### Variation

**The variability that is observed in the biometric data of the same individual is referred to as the “intra-class variation,” whereas the variability between biometric data from two different individuals is known as “inter-class variation.”** Figures 1.2 and 1.3 give an impression of intra-class and inter-class variation, respectively, for fingerprint data. For successful biometric recognition, the intra-class variability must be as small as possible, while the inter-class variability should be large.

**Figure 1.2. Example of Intra-class Variation for Fingerprint Recognition Showing Eight Different Fingerprint Captures from the Identical Finger of the Same Individual (Biometric Data from the Third International Fingerprint Verification Competition [FVC2004]).<sup>38</sup>**



**Figure 1.3. Example of Inter-class Variation for Fingerprint Recognition Showing Eight Different Fingerprint Captures from Different Individuals (Biometric Data from FVC2004)**



<sup>38</sup> Beslay, Laurent., J. Galbally, and R. Haraksim. 2018. *Automatic Fingerprint Recognition: From Children to Elderly. Ageing and Age Effects*. Luxembourg: Publications Office of the European Union. doi:10.2760/809183.

## Biometric Verification Error Rates

**Comparing a newly captured biometric with a stored biometric will lead to a similarity score.** When the new biometric and stored biometric are from the same individual (i.e., a genuine comparison attempt), and the intra-class variability is small enough, a biometric comparison will likely lead to a high similarity score. However, if the biometric data comes from different individuals (i.e., through an imposter attempt), the biometric comparison is likely to yield a much lower similarity score. Figure 6.3(a) gives an impression of the genuine and imposter distributions, that is the distribution of the similarity scores for genuine and imposter comparisons, respectively. Using these distributions, a threshold can be used to distinguish between an imposter and a genuine matching attempt. Figure 6.3(a) also shows that, in case of an overlap of the genuine and imposter distribution, a given threshold may lead to falsely matched imposters and a falsely rejected genuine match.

The following terminology is used to describe biometric verification error rates:

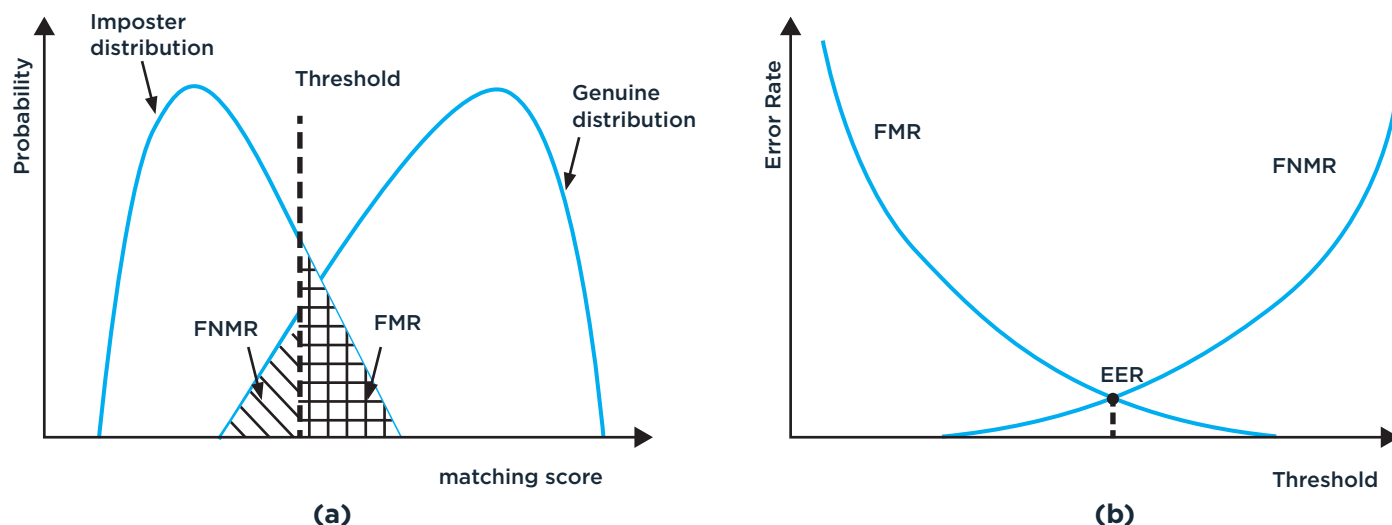
- *Match*. A comparison decision stating that a biometric probe and biometric reference are from the same source
- *Non-match*. A comparison decision stating that a biometric probe and biometric reference are not from the same source
- *False match rate (FMR)*. FMR is the percentage of completed imposter (non-mated) matching trials for which matching score is greater than the threshold.
- *False non-match rate (FNMR)*. FNMR is the percentage of completed genuine (mated) matching trials for which comparison is less than the threshold.
- *Equal error rate (EER)*. EER is the point where the FMR is identical to the FNMR.
- *False accept rate (FAR)*. FAR is the proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed. For example, during a verification transaction, if an impostor fingerprint happens to look sufficiently similar to the one enrolled that the algorithm decides that they are highly likely to be from the same characteristic and incorrectly verifies the user as the wrong identity. This is a false accept as an impostor has been allowed access.
- *False reject rate (FRR)*. FRR is the proportion of verification transactions with truthful claims of identity that are incorrectly denied. For example, during a verification transaction, if the finger is placed on the sensor such that only part of the fingerprint is visible and the algorithm incorrectly fails to verify the user, this is a false reject, as the legitimate user has been denied access.

**Note that false acceptance rate (FAR) versus FMR and false rejection rate (FRR) versus FNMR are often used interchangeably.** There is, however, a subtle difference in that FAR and FRR are system level errors, taking into account, for example, samples that failed to be acquired. Other terminology that is used in literature is the true acceptance rate (TAR), which is defined as  $1 - FRR$ , measuring the degree that a biometric system correctly matches the biometric from the same person.

**When changing the threshold, a trade-off between FMR and FNMR can be observed.** In figure 6.3(b), the dynamic of this trade-off is plotted for varying matching thresholds. Increasing the matching threshold will yield a lower FMR, meaning a lower percentage of imposters are falsely verified, and, as a result, the security of the system will increase. The downside of the trade-off, however, is that a larger percentage of genuine verifications are falsely rejected, and so the user convenience of the system drops. Setting the threshold of a biometric system in an optimal way depends on the application requirements but will always be a trade-off between security and convenience.

**An important performance indicator for biometric systems is the EER, which is the point where the FMR and the FNMR are identical.** The biometric system is rarely configured to operate at the EER point, but usually a more stringent threshold is chosen to set a pre-specified, typically lower FMR.

**Figure 1.4. (a). FMR and FNMR for a Given Threshold and a Given Genuine and Imposter Score Distribution. FMR Is the Percentage of Imposter Pairs Whose Matching Score Is Greater than the Threshold, and FNMR Is the Percentage of Genuine Pairs Whose Comparison Is Less than the Threshold. (b) Illustrative Example of FMR and FNMR as a Function of the Threshold also Indicating EER, Which Is the Point Where FMR Is Identical to FNMR.**



## Comparing the Accuracy of Biometric Verification Systems

The accuracy requirement of a biometric verification system is very much application dependent. For example, in a forensic application, the FNMR is more of a concern than the FMR as it is undesirable to miss a potential match with a criminal. For applications with a focus and function towards security, such as biometric verification to provide access to services, the primary objective is to deny all imposters, and the biometric systems are typically configured to operate at a certain security level specified by a fixed FMR.

In order to compare biometric systems, it is important to present the system accuracy at each operating point. This is typically done using a receiver operating characteristic (ROC) curve a detection-error trade-off (DET) curve. Both curves are threshold independent and allow for more easy comparison of different biometric systems. These graphs are generated by performing a large number of genuine matches and imposter matches on a particular biometric data set of single-fingerprint images. From these comparisons, the FMR and FNMR were derived as a function of the threshold. Then for each operating point (i.e., each threshold), the FNMR was plotted against the FMR.

It is important to mention that there is a strict dependency of the FMR and FNMR on the failure to acquire rate (FTA) or the failure to enroll rate (FTE). A stricter selection process of retaining biometric samples with high quality will lead to a higher number of exclusions (i.e., higher FTE) but at the same time will improve the FMR and FNMR. For this reason, the FTE and FTA need to be provided when comparing accuracy of biometric recognition algorithms and evaluating the risk of exclusion errors. As shown in table 6.2, the enrollment procedure of system (i) is such that only 0.61% of the individuals failed to enroll into the system compared to 1.45% for system (ii). So, while the biometric recognition algorithm (ii) has higher accuracy, more individuals are excluded from the system in the enrollment phase. In addition, note that a false non-match leads to the exclusion of an individual from a biometric system.

**It is important to mention that there is a strict dependency of the FMR and FNMR on the failure to acquire rate (FTA) or the failure to enroll rate (FTE).** A stricter selection process of retaining biometric



samples with high quality will lead to a higher number of exclusions (i.e., higher FTE) but at the same time will improve the FMR and FNMR. For this reason, the FTE and FTA need to be provided when comparing accuracy of biometric recognition algorithms and evaluating the risk of exclusion errors. As shown in table 6.2, the enrollment procedure of system (i) is such that only 0.61% of the individuals failed to enroll into the system compared to 1.45% for system (ii). So, while the biometric recognition algorithm (ii) has higher accuracy, more individuals are excluded from the system in the enrollment phase. In addition, note that a false non-match leads to the exclusion of an individual from a biometric system.

**Table 1.3. Example System Error Rates.**

Biometric recognition algorithm	(i)	(ii)
FNMR @ FMR = 0.01%	0.2%	0%
FNMR @ FMR = 0.001%	0.6%	0.2%
Failure to acquire (FTA)	11.5%	5.23
Failure to enroll (FTE)	0.61%	1.45%

Source: Biometric System Lab, University of Bologna. 2004. Fingerprint Verification Competition.(FVC 2004). <http://bias.csr.unibo.it/fvc2004/>

From the Test on FVR2004,<sup>37</sup> It Can Be Concluded That for an FMR of 1 out 100,000, System (ii) Outperforms System (i) with an FNMR of 2 out of 100 versus 6 out of 100, Respectively. That Is, at the Given Operating Point, the System (i) Falsely Misses 2 out of 100 Matches of Genuine Comparisons.

For more, please see forthcoming ID4D Evidence Note summarizing data from field studies of errors rates in biometric verification.

## Biometric Identification Error Rates

**In a biometric identification process, a biometric probe is matched with all biometric enrollment templates in a database to return a candidate list that may be empty (if no match is found) or contain one or more identifiers of matching enrollment templates.** If the database contains N biometric enrollment templates, then each of the N comparisons can lead to a match or non-match with related matching errors (FMR and FNMR). The overall process will lead to the following identification errors:

- False positive identification-error rate (FPIR). FPIR is the percentage of completed imposter (non-mated) searches where one or more enrolled candidates are returned at or above the threshold.
- False negative identification-error rate (FNIR). FNIR is the percentage of completed genuine (mated) searches where the enrolled mate has a matching score below threshold (or is outside the top R rank of the returned candidate list).

**The FPIR and FNIR are computed in the same way as the FMR and FNMR in the case of biometric verification.** The identification error rates are dependent on the number of biometric enrollment templates, N, that need to be searched. In several reports, the general rule of thumb for calculating FPIR is given: For very small FMR, the FPIR increases linearly with the size N of the database. The effect of this can be seen in the following example: when increasing the size N of the biometric enrollment database from 1,000 to 1,000,000 subjects, the probability for a false positive match will increase approximately by a factor of 1000.



**The dependency of the FPIR and FNIR on the size of the database has serious complications** regarding the design of biometric identification, including de-duplication systems. An increase in the size  $N$  leads not only to an increased requirement for higher computational power but also a decreased overall accuracy.

For example, consider an identification system intended to cover 1,000,000 people and assume that for an acceptable FNMR, the FMR of a chosen biometric algorithm is  $10^{-5}$  (i.e., a false match occurs in 1 out of 100,000 match attempts). For this system, the probability of falsely matching an individual during identification is approximately  $FPIR = 10^{-1}$  meaning that each search over the entire enrollment database will return 10 falsely matched candidates. When using such an identification system for de-duplication purposes, these falsely matched candidates would have to be (re-)examined through a so-called secondary (manual) adjudication process.

**For large-scale identification systems, the FPIR and FNIR are typically improved by using multiple fingers and multiple biometric traits, e.g., combining fingerprint, face, or iris.**

### 6.4.3. Algorithm Selection

**Choosing the best biometric algorithm for an ID system on an assessment of the following attributes:**

- *Accuracy.* The direct accuracy of the algorithm should be established by an independent testing authority. There are a range of publicly available reports that have tested a range of algorithms over varying conditions. Importantly, accuracy can vary significantly depending on the data quality, the number of biometrics being searched (gallery size), and demographics.
- *Cost.* Every vendor will have different costing parameters and charging models. It is common for a large system to be charged on volume.
- *Storage.* What will be storage requirements for the biometric templates?
- *Speed.* How fast will various operations such as enrollment, verification, or identification perform with the expected deployment infrastructure?
- *Vulnerability.* Does the algorithm check for any fake biometrics?
- *Quality.* How is quality managed to ensure that poor quality biometrics are rejected, asked for re-enrollment, or flagged?
- *Reliability.* What is the reliability of the software? Has it been shown in other deployments of similar scale to work well and minimize downtime?
- *Integration.* How will the algorithm work in the context of the entire ID system?

### 6.4.4. Multi-algorithmic Fusion

Secondary matching can improve the production matching outcomes in terms of quality of automated decision making and potential reductions in human workload. Fusion of algorithms with the primary matcher, with secondary algorithms and derived can also be effective in providing lower false positive or false negative identification rates. It is important to note that the fusion engine must be correctly configured to achieve positive results and may be vulnerable to model drift over time and as such must be actively managed.

### 6.4.5. Matching Algorithm Bias

**Most matching algorithms are trained on data, both to create and to tune the algorithm. This is accomplished using large sets of labeled data compiled by vendors.** The result of this process is a model that can be used to predict similarity, but its robustness is dependent on the data that was available for training. Even if the training data has the perfect demographic distribution, it is possible that bias cannot be completely eliminated from the system; thus, the goal is to minimize bias as much as possible.

**The possibility of bias in biometric systems that use FRT has recently raised public concern about their widespread use.** Bias is highly likely in systems where the database is not sufficiently diverse because most FRT algorithms are generated by training the system to detect a number of faces from a database, and, as such, sufficiently representative data sets must be utilized in order to minimize system bias. Early FRT algorithms were frequently biased and inaccurate. However, newer algorithms have corrected for much of this by ensuring that they use a larger and more diverse database for training algorithms.

**It is recommended that practitioners carefully assess the likelihood of bias in the local context as such bias can increase the risks of discrimination and exclusion** and, therefore, identify the optimal model for the given context. Bias can result in more false matches (misidentifications), more false non-matches (not being identified by the system), or failures to acquire (not even being able to be enrolled).

Bias can be measured in a test environment as well as through statistical analysis of operational outcomes. The identification of significant bias may necessitate the use of different settings depending on the demographic.

## 6.5. Interoperability and Standards<sup>39</sup>

### 6.5.1. Interoperability Standards

**Standards aim to establish generic sets of rules for different products and to facilitate interoperability, data exchange, consistency of use, and other desirable features.** International biometric standards on interoperability allow stability and consistency of biometric technologies and products that benefit consumers and investors.

Some well-known biometric standards for ensuring interoperability are listed in table 1.4.

**Table 1.4. Biometric Standards Ensuring Interoperability**

Standard	Main features of standard
ISO/IEC 19795-4:2008	Information technology—Biometric Performance Testing and Reporting—Part 4: Interoperability Performance Testing
ISO/IEC 19794-2	Information Technology—Biometric Data Interchange Format;—Part 2: Finger Minutiae Data
ISO/IEC 19794-4	Information Technology—Biometric Data Interchange Format—Part 4: Finger Image Data

39 For more information about standards for ID systems, please see the ID4D Standards Catalog. <https://id4d.worldbank.org/technical-standards>.

Standard	Main features of standard
ISO/IEC 19794-5	Information Technology—Biometric Data Interchange Format—Part 5: Face Image Data
ISO/IEC 19794-6	Information Technology—Biometric Data Interchange Format—Part 6: Iris Image Data
ISO/IEC 19794-10:2007	Information Technology—Biometric Data Interchange Formats—Part 10: Hand Geometry Silhouette Data
INCITS 378:2004	Fingerprint Minutiae Format American National Standard for Information Technology Biometric Application Programming Interface (BioAPI) defines the architecture and necessary interfaces to allow biometric applications to be integrated from different vendors
ISO/IEC 19784-1:2018	Information Technology—Biometric Application Programming Interface—Part 1: BioAPI Specification
ISO/IEC 29109-10:2010	Information Technology—Conformance Testing Methodology for Biometric Data Interchange Formats Defined In ISO/IEC 19794—Part 10: Hand Geometry Silhouette Data
ISO/IEC 19785-1	Information Technology—Common Biometric Exchange Formats Framework—Part 1: Data Element Specification
ISO/IEC 19785-3:2020	Information Technology—Common Biometric Exchange Formats Framework—Part 3: Patron Format Specifications
ISO/IEC 19785-4:2010	Information Technology—Common Biometric Exchange Formats Framework—Part 4: Security Block Format Specifications
ISO/IEC 24713-3:2009	Information Technology—Biometric Profiles for Interoperability and Data Interchange—Part 3: Biometrics-based Verification and Identification of Seafarers
ANSI/NIST-ITL 1-2011:Update 2015	NIST Special Publication 500-290e3, Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information (supports the exchange of biometric data, including fingerprints, faces, scars, marks, and tattoos, between law enforcement and related criminal justice agencies)
ANSI/NIST-ITL 1-2007/2-2008	Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information—Part 2: XML Version (defines a common format for exchanging and storing a variety of biometric data including faces, fingerprints, palm prints, irises, voices, and written signatures)
FBI-EBTS (FBI Electronic Biometric Transmission Specification)	Supports the exchange of biometric data with the US FBI

## 6.5.2. Quality Standards

**Biometric system performance heavily relies on the quality of the acquired input samples** and compliance with the corresponding international biometric standards advising that superior data quality ascertains a better-quality assurance management process. Hence, with the use of standards, great flexibility and modularity can be achieved.

Biometric standards for quality assurance are listed in table 1.5.

**Table 1.5. Biometric Standards for Quality Assurance**

Standard	Main features of standard
ISO/IEC 29794	Enables harmonized interpretation of quality scores from different vendors, algorithms, and versions by setting key factors to define quality in different biometric traits
ISO/IEC 29794-1:2016	Information Technology—Biometric Sample Quality—Part 1: Framework
ISO/IEC 29794-4:2017	Information Technology—Biometric Sample Quality—Part 4: Finger Image Data
ISO/IEC TR 29794-5:2010	Information Technology—Biometric Sample Quality—Part 5: Face Image Data
ISO/IEC 29794-6:2015	Information Technology—Biometric Sample Quality—Part 6: Iris Image Data
ISO/IEC-19794-5 (Annex)	Includes recommendations for taking photographs of faces for e-passport and related applications and includes indications about lighting, camera arrangement, and head positioning
ISO/IEC 30107	Biometric Presentation Attack Detection
ISO/IEC 19794-2:2005	Information Technology—Biometric Data Interchange Formats
ISO/IEC TR 29144:2014	Information Technology—Biometrics—The Use of Biometric Technology in Commercial Identity Management Applications and Processes
ISO/IEC 15444-1:2019	Information Technology—JPEG 2000 Image Coding System—Part 1: Core Coding System
NIST Special Publication 800-76-2	Biometric Specifications for Personal Identity Verification
NIST Federal Information Processing Standard Publication 201-1	Personal Identity Verification of Federal Employees and Contractors

### 6.5.3. General Standards

**With the digital identity space advancing at an accelerating pace, there has been an increase in biometric standards that are critical for identification systems to be robust, interoperable, and sustainable.**

Some international standards that apply to the use of biometrics in an ID system are listed in table 6.5.

**Table 6.5. International standards applying to biometrics in an ID system**

Standard	Main features of standard
ISO/IEC 29794	Biometric Performance Testing and Reporting
ISO/IEC 30107	Biometric Presentation Attack Detection
ISO/IEC 19794 Series (parts 1, 2, 3, 4 5, 6)	Biometric Data Interchange Formats
ISO/IEC 24745:2011	Information Technology—Security Techniques—Biometric Information Protection (Guidance for the Protection of Biometric Information for Confidentiality and Integrity during Storage or Managing Identities)
ISO 19092:2008	Financial Services—Biometrics—Security Framework
ISO/IEC 7501-1:2008	Identification Cards—Machine Readable Travel Documents—Part 1: Machine Readable Passport
ISO/IEC 30108-1:2015	Information Technology—Biometric Identity Assurance Services—Part 1: BIAS Services
ISO/IEC 24713-3:2009	Information Technology—Biometric Profiles for Interoperability and Data Interchange—Part 3: Biometrics-based Verification and Identification of Seafarers
ICAO 9303 travel document standard	International Travel Document (Passports) Standard
ISO/IEC 24760-1:2011	Information Technology—Security Techniques—A Framework for Identity Management—Part 1: Terminology and Concepts
ISO/IEC TR 30125:2016	Information Technology—Biometrics Used with Mobile Devices
ISO/IEC 2382-37:2017	Information Technology—Vocabulary Part 37: Biometrics
NIST SP 800-63	Digital Identity Guidelines
NIST Special Publication 800-76-2	Biometric Specifications for Personal Identity Verification
NIST Federal Information Processing Standard Publication 201-1	Personal Identity Verification of Federal Employees and Contractors
European Commission BEAT D6.5	Biometric Evaluation and Testing—Towards the Common Criteria Evaluations of Biometric Systems

## 6.6. Presentation Attack Detection

**A presentation attack is the use of a human or artificial instrument that mimics characteristics of a valid biometric to subvert a biometric system or cause missed identification in watch lists.** The resistance of biometric systems against biometric presentation attacks (PAD) is vital for the usefulness and reliability of biometrics within ID systems. This is a concept distinct from biometric recognition accuracy and has a different set of metrics and terminology. A biometric system with a false accept rate (FAR) of zero may still be highly vulnerable to presentation attacks.

**The market for presentation attack detection software and hardware is still relatively young.** However, there are a variety of techniques used for presentation attack detection with a wide range of effectiveness. Recently international standards have been developed for guidance on the types of approaches used for presentation attacks, the assessment of presentation attack in data formats, methods for performance assessment of presentation attack detection algorithms or mechanisms, and classification of known attack types.<sup>40</sup>

**PAD methods fall into one of two categories:**

1. *Through a data capture subsystem, which includes*

- Artifact detection

- Liveness detection

- Alteration detection

- Non-conformance detection

- Coercion detection

- Obscuration detection

2. *Through system-level monitoring, which includes*

- Failed attempt detection counters

- Geographic and temporal monitoring

- Video surveillance

---

<sup>40</sup> An international standard for PAD detection and assessment is given by BSI (British Standards Institution). 2016. *Biometric Presentation Attack Detection—Part 1: Framework*. ISO/IEC 30107-1.

# 7. Deployment and Operational Considerations

## 7.1. Operational Security

### 7.1.1. Operator Controls

**System operators should be provided with comprehensive system training, both on how to use the system and how to ensure that it is not misused.** Operators should also be regularly audited by a transparent and independent authority to ensure that individuals only have access to the functions they require for their specific job function or role. Additionally, the system design should limit the ability of any individual to alter or delete data or make changes to the system's operation (such as changing the matching threshold).

**Robust auditing processes will facilitate accountability and enable remediation where required.** The processing of sensitive and personal data should be monitored by an appropriate, independent oversight authority and, where possible, by data subjects themselves. Audit logs must be made easily accessible to the relevant authority while maintaining user privacy. A transparent audit system can also reinforce public support and uptake of the system.

**An effective control against function creep is ensuring the system interfaces and functionality are specifically designed to exclude use cases outside of the current functional requirements.** To do this, the system design must be built with an understanding of the specific risks of function creep.

## 7.2. Data Migration

**When establishing a new or upgraded deployment, the movement of existing biometric and identity data needs to be considered.** This process is often one of the most challenging aspects of a project as existing identity data stores frequently have a range of issues including:

- *Errors.* Data field errors arising from mistakes in data entry or issues with the previous application.
- *Fraud.* Fraudulent application with undetected multiple identities.
- *Quality.* Biometric quality issues, for instance, uncontrolled facial image capture or poor-quality fingerprints.

- *Duplicates.* As a result of the movement, records can become mistaken, linked, or delinked.
- *History.* Often moving from one system to another will mean not all historical transaction data will be available.
- *Transformation issues.* The data migration tools used to move data can also introduce errors especially where there are complex data business rules.
- *Templates.* In some cases, serious security and data protection concerns can arise if raw, unprotected data template is saved in the database to be migrated.
- *Template format.* If the raw biometrics cannot be accessed, the biometric templates may not be able to be used as they are specific to the current matching algorithm.
- *Parallel operations.* In some systems, the migration may need to run in parallel with the existing system and as such synchronization issues need to be considered.

**All data migration activities need to be undertaken in a way that is auditable and has appropriate control procedures to ensure accuracy and protect the migrated data.** Where data is coming from a third party outside of the implementing agency, it is essential to ensure all data protection considerations have been met.

It is recommended that the migration process is carefully planned and has some form of independent assurance process to detect and avoid issues both before and during migration. An initial step, known as data landscaping, can help to capture the types of errors and quality issues that might be expected by randomly sampling any existing data stores.

## 7.3. Manual Adjudication

**In ID systems, particularly with face, it is necessary to employ the use of human operators to assist the automated system when resolving matches that produce match scores that fall between the automatic rejection and acceptance thresholds.** This is generally focused on systems where there is identification/deduplication (1:N).

If the algorithm assessing the similarity between two images is unsuccessful in verifying the match, because the match score falls below a set threshold, the transaction can be referred to the manual resolution team for processing.

**As the capability and performance of the current biometric solutions improves, the frequency distributions of match scores for a matched and a non-matched identity will move further apart, and so less human processing is expected over time.** However, an important consequence of this trend is that the cases that absolutely do need humans to perform the identification process will become increasingly difficult in the sense that the amount and type of such cases requiring manual processing will require adjudicators within such systems to have special expertise in face comparison and document examination.

Using human adjudicators introduces several operational considerations that need to be managed by governance and policy.

### 7.3.1. Identity Adjudication Center

**To manage this manual resolution, best practice is to establish a dedicated center that can be staffed by trained experts.** These experts should have formal training in the relevant biometrics to be able to make informed decisions on any biometric candidates that are referred.



**These experts should be supported by appropriate software tools that allow such examination.** Such tools may be provided by the biometric vendor or sourced from a third party. They also require governance rules around the process of escalation in the case of potential fraud. One mechanism for structuring an identity resolution team involves the use of both primary experts for initial review and secondary more experienced experts for harder cases.

**Security controls for the identity resolution tools should be implemented including strong authentication** (non-repudiation) for adjudication operators, data segregation (demographics should not appear anywhere, ideally), and random allocation of jobs to prevent traceability of records.

## 7.4. Risk Management Frameworks

**Biometric systems are high-value targets for cybercriminals, and the consequences of system compromise are broad and serious.** Effectively managing risk is of critical importance for all identity systems, especially so for those that use biometrics. Although there are a multitude of different risk management frameworks—the choice of which will vary depending on region-specific practices (PDCA/PDSA, NIST RMF, ISO/IEC 31010 etc.)—any proposed risk management solution must be justified objectively by an examination of all possible factors, not just those governing technical performance metrics.

### 7.4.1. Data Protection Impact Assessment

**Some data protection legislation such as the GDPR requires a data protection impact assessment (DPIA) prior to any high-risk processing of personal data in use within biometric systems.** Biometric data used for identification purposes is a special category of personal data under the GDPR, and, as such, its processing or use within a ID system triggers the requirement to undertake a DPIA per Article 35 of the GDPR.<sup>41</sup>

Under Section 35 of EU GDPR, a DPIA must contain the following:

- A systematic description, including the purpose of all data processing operations implicated by the system
- Details concerning the necessity of the processing activities weighed against the purposes of such processing
- An assessment of the risks to the rights and freedoms of individuals whose data is processed by the ID system
- Measures undertaken to address these risks, safeguard personal data, and demonstrate compliance

**The purpose of conducting a DPIA is to identify risks and mitigatory actions relating to the processing of personal data (including sensitive biometric data required for the use of biometric systems).** The DPIA should be undertaken by the nominated data protection officer before processing begins. Required actions dictated by the results of the DPIA must be performed throughout system development. In addition, the DPIA should outline key stakeholders and seek their input throughout the lifecycle of the project.

---

41 Intersoft Consulting. 2016. *General Data Protection Regulation (GDPR)*. <https://gdpr-info.eu/>.

## 7.5. Threat Modeling

**Generating threat models can assist with identifying and understanding potential threats and developing subsequent mitigation strategies.** In the context of ID systems that use biometrics, threat modeling first requires a detailed description of the system. The use of a detailed system description facilitates the identification of potential system threats. Once the threats have been determined, strategies can be developed to mitigate the established risks. Threat modeling should be performed as soon as possible in the project lifecycle. Additionally, threat models should be reviewed whenever there is a substantial system change that could introduce further threats, such as when system architecture changes are made or new processes or dataflows are introduced.<sup>42</sup> Threat models can also assist with establishing user trust in the system, as well as subsequent system uptake.

## 7.6. Communication and engagement

**Communication is vital for the rollout of biometric systems.** This includes internal communications to staff around the use and benefit of the technology and a communications and marketing strategy to the wider population of users to ensure that they understand how and why biometrics are being used and where they can seek more information. As discussed above, it is also essential that communication be a two-way street, and that the public has regular and meaningful opportunities to provide feedback and raise concerns and solutions around the implementation of biometrics.

Good communication and engagement strategies need to address common concerns around the use of biometric technology without oversimplifying or downplaying risks. For guidance, see the forthcoming ID4D guides on communication and CSO engagement.

## 7.7. Risks and Challenges of the Political Context

Projects involving the use of biometrics can face specific challenges because they involve the introduction of new technology and there are often political sensitivities around privacy and security. Factors such as the political climate, existing legal frameworks relating to data protection and privacy, and lack of incentive to change existing systems can create challenges when implementing biometric identity systems. These factors result in a complex political environment that must be carefully navigated to mitigate risk and provide a successful and secure digital identity system.

The following recommendations provide a guide for stakeholders to mitigate political risk when developing a biometric identity system:

- *Assessment of existing identity infrastructure.* This includes legal frameworks, identity documents, and operational processes of agencies relating to biometrics and identity, especially in relation to practices that may disproportionately have an impact on vulnerable individuals or groups.
- *Development of strong political commitment from stakeholders.* Engage relevant ministries and stakeholders from the beginning and throughout the planning process in order to align outcomes with their incentives, to encourage support, and ultimately to adopt the proposed new system.
- *Revision of legislation and internal procedures.* Create or revise relevant legislation and internal procedures related to program implementation. In circumstances where existing legal frameworks

---

<sup>42</sup> Drake, Victoria. 2016. "Threat Modeling." Wakefield, MA: The Open Web Application Security Project (OWASP). [https://owasp.org/www-community/Threat\\_Modeling](https://owasp.org/www-community/Threat_Modeling).

were designed for non-digital data collection, significant revision may be required. This can be achieved by providing guidance to ministries and minimizes the risk of duplication or conflict in legislation. Throughout this process it is important to maintain protection of the individual's rights, particularly in relation to monitoring and enforcement. Legislation should also focus on the minimization of security risks, such as cyber-attacks causing data breaches.

- *Awareness of disproportionate impact on vulnerable populations.* Throughout the legislative revision process, awareness should be maintained of the possible exclusion of vulnerable populations and individuals when accessing identity services.

## 7.8. Governance

**The establishment of a robust governance structure is necessary to ensure that biometric systems stay in compliance with operational goals.** Governance structures should be designed to effectively implement and monitor the risk mitigation strategies outlined by threat modeling and data protection and other impact assessments. A robust governance framework will ensure that all governance roles are given specific, detailed, and transparent responsibilities. Additionally, strong governance structures to monitor system performance help to safeguard service delivery and quality. Several questions should be asked when designing a governance structure, including<sup>43</sup>:

- What skills are required to successfully meet the goals of the project?
- What system processes need to be understood so that the project's activities are sufficiently overseen?
- Are those within the governance structure being provided with the information required to properly oversee the project and make decisions?

## 7.9. Exclusion and Exception Handling

**Support for those unable to use a biometric system is critical to ensure inclusion.** Large scale systems have addressed this issue in a variety of ways:

- Noting in the database the missing biometric and requiring a password or other token (such as card)
- Retrying with relaxed quality standards
- Providing multiple biometrics (face, finger, and iris) so that if one or more biometrics are not present or unable to be enrolled there is still a biometric that can be used
- Continuously tracking and analyzing biometric performance and people's experiences with biometrics to identify and correct issues and adopt appropriate policies and appropriate exception mechanisms to prevent exclusion
- Carefully considering when and if biometric-based authentication is used to ensure that it is proportional to the required level of assurance and does not introduce a new risk of exclusion in service delivery.

---

<sup>43</sup> Deloitte Development. 2013. "Framing the Future of Corporate Governance." [https://deloitte.wsj.com/riskandcompliance/files/2013/05/US\\_AERS\\_Governance\\_-Framework\\_102412-Final.pdf](https://deloitte.wsj.com/riskandcompliance/files/2013/05/US_AERS_Governance_-Framework_102412-Final.pdf).

- Ensuring that--if biometrics are used for authentication--relying parties implement fair and clear exception handling mechanisms that staff are well-trained on to avoid denial of service due to difficulties with biometrics.
- Implementing accessible, effective grievance redress mechanisms

## 7.10.Acquisition Best Practice

There are several steps to improve biometric acquisition, including:

### Device and Environmental Setup

There are several simple steps that can be taken to ensure that devices and environments are set up for ensuring high-quality biometrics. Some factors to consider include the capture device, lighting, and backgrounds. Consideration to these can have one of the most significant impacts on ensuring a high-quality biometric and most are very simple to implement.

### Offline Environments

Biometric data can be captured offline by mobile or fixed devices. Where data is captured in an offline environment, the challenges are ensuring data is accurately synchronized, that any stored data is protected in case of theft or loss and that the data is protected against alteration.

### Enhanced Operator Guidance and User Instruction

There are several different quality aspects that operators could be trained to assess and acquire. While these can be documented and taught to operators, it is typically unlikely that all different quality characteristics will be able to be maintained in all instances, free of defects, degradations, and interferences. The training also needs to consider potential fringe cases and sensitivities to ensure they are handled appropriately.

### Enhanced User Instruction for Low Supervision Scenarios

For instances where the user is responsible for the acquisition process, there is limited opportunity to provide instruction or correction for the presentation of the biometric. The instructions should, therefore, focus on key aspects that can have more significant impacts on the acquisition of a high-quality biometric. In some unsupervised use cases, the acquisition process may also include liveness detection features for the purposes of presentation attack detection.

### Quality Assurance

There are several issues and challenges with capture quality that must be addressed. Ensuring robust quality assurance is critical to system performance and can be achieved in two ways:

- Manual inspections by operators, which is reliant on efficient training and operator guidance
- Automated quality assessment, which provides high efficiency and depth of analysis to improve outcomes.

## 7.11. Technical Performance Review and Reporting

**The technical performance of the identity system should be regularly measured. This allows the operating authority to**

- Compare current operations to best practice
- Ensure risk management and security processes are being carried out
- Proactively identify issues
- Identify when upgrades may be needed
- Manage and control settings

**Such metrics, reports, and performance reviews can include:**

- Biometric accuracy
- Biometric failures
- Speed of processing
- Vulnerability
- Usability
- Inclusiveness

**Ensuring that decision makers and operational staff have access to timely and accurate reporting on system performance should be a key metric around system development and deployment.**

These reviews can be particularly important in biometric systems as there are often issues managing both accuracy and vulnerabilities, particularly when they are first introduced. The frequency of such reviews should be approximately annually but may be more frequent during the first year. Some of this data can be collected automatically as part of the ID system processes (e.g., instances of FTE, throughput, etc.), while others may need supplementary data collection (e.g., via surveys or process auditing and observation).

- Transaction volumes and response times
- Identity resolution statistics
- System performance trends

## 7.12. Audit

**Robust auditing processes will facilitate accountability and enable remediation where required.** The processing of sensitive and personal data should be monitored by an appropriate, independent oversight authority and, where possible, by data subjects themselves. Audit logs must be made easily accessible to the relevant authority while maintaining user privacy. A transparent audit system can also reinforce public support and uptake of the system.

**It is recommended that biometric systems undergo regular audit at least yearly.** This audit should examine various measures of system performance, including failure rates, transaction performance, and acquisition quality. Another useful activity is to have biometric penetration attack testing undertaken. This can help ensure the system is operating as expected.

### 7.12.1. Transparency Portal

**The creation of a transparency portal can be implemented as a means of giving users control over their personal biometric data.** A transparency portal would allow system users to view details about their data, including:

- Which data was accessed?
- When was it accessed?
- Who accessed it?
- Who has the data been disclosed to?
- What was the purpose for which it was accessed or otherwise processed?
- How long will the data be stored?
- Are profiling or automated decision-making processes being applied to their data?
- How to lodge a complaint or seek redress?

This type of portal is becoming standard in many data protection regulations. For example Article 13 of the GDPR requires that this type of information be provided to individuals at the point at which their data is initially collected. Article 15 further requires access to such information upon an individual's request.<sup>44</sup> The transparency portal could also explain how the user can lodge a complaint with the supervisory authority and, where appropriate, request data rectification or erasure.<sup>45</sup> The integration of a transparency portal would also likely increase confidence in the system by users and possibly increase public uptake.

## 7.13. Data Sharing Controls

While the ability to securely share and verify data is once of the key benefits of an ID system the sharing of identity data, introduces the vulnerabilities of one system into another, multiplying the number of potential vulnerabilities for each additional introduced system. It is important to consider the potential gain of information sharing versus the potential compromise of system security and surveillance when designing the ability to share data between systems.

If a certain type of data sharing was not intended at the time data was originally collected, such processing should, as a general rule, be unlawful. In such circumstances, the GDPR, for example would only permit a public authority to share the data if this were authorised by law for limited reasons (concerning security, crime, judicial proceedings, and the like) or if the data sharing were compatible with the purpose it was originally collected (with extra caution expected to be taken in the case of biometric data).<sup>46</sup> This is consistent with the "purpose limitation" principle that is a fundamental aspect of many developed data protection laws.

### 7.13.1. Third-party Management

Some governments may seek to engage with private industry and other third-party organizations to enhance the functions of foundational ID systems. For example, banks, post offices, or telecommunications

---

44 European Union. 2016. General Data Protection Regulation (GDPR). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

45 Under the GDPR, the right to erasure does not apply where data processing is necessary for a task carried out in the public interest or in the exercise of official authority, as would be the case for much data held in a foundational ID system.

46 See GDPR Article 6(4). <https://gdpr-info.eu/art-6-gdpr/>

companies can be leveraged in order to provide identity verification using biometric data in combination with the foundational ID system.

It will be important, however, to ensure that third parties are only provided access to biometric data in the ID system in limited circumstances, supported by robust data protection laws and operational safeguards. In this context, it is worth making a distinction between two different types of third-party.

**1. Data processors.** A data processor processes personal data on behalf of a data controller. In the context of a foundational ID system, the owner of the ID system will likely be the data controller, while companies providing the underlying technological services (such as data storage and analysis) will be data processors. Data processors have no independent reason for processing the data. Under the GDPR, data processors are subject to a range of direct obligations, including to report security breaches to the data controller and to ensure a level of data security that is appropriate to the risks associated with the data processing they undertake (in the case of biometric data, the risk would be higher and so additional safeguards would be expected). In addition, certain contractual obligations must be in place between data controllers and data processors.<sup>47</sup> These clauses require, among other things, that a processor only acts on the controller's instructions, implements appropriate confidentiality and security measures, assists the controller in responding to data subject requests, and engages sub-processors only where authorized to do so.

**2. Data controllers.** A data controller is an organization that determines the purpose and means of data processing, i.e. the "why" and the "how." Crucially, they have their own independent reason for processing the personal data. In the circumstances described above, a bank or post office would likely be an independent data controller, as would an ID system owner. Under the GDPR, a public authority who owns an ID system could likely only share biometric data with a third-party data controller if this were authorized by law or in very narrow circumstances where individuals may be able to provide free consent (i.e., where they would suffer no detriment or loss of benefit as a result of having not consented). That said, a third-party data controller from the private sector could more readily share data with a public authority (assuming they were transparent and obtained a legally valid consent from individuals to do so). Where data sharing between data controllers is permissible, measures must be taken to ensure that robust legal, operational, and technical data protection practices of any engaged third-parties are in place, matching or exceeding those employed by the government implementing the system. Additional measures that should be considered include<sup>48</sup>:

- Data sharing agreements with strict contractual requirements outlining the minimum standards and requirements for accessing and using data (consider naming the specific individuals with access)
- Mandatory authorization processes
- Requirements that private sector providers are located within the country
- Government-retained control over any data collected and stored by the private sector provider on behalf of the ID system
- Prohibitions on further sharing or sub-contracting of requirements to additional individuals or entities

---

<sup>47</sup> See Article 28 of the GDPR. <https://gdpr-info.eu/art-28-gdpr/>

<sup>48</sup> The World Bank (2018), ID Enabling Environment Assessment (IDEEA) Guidance Note. <https://id4d.worldbank.org/sites/id4d.worldbank.org/files/2018-12/IDEEA%20Guidance%20Note%20-%20Consultation%20Draft%20V11142018.pdf>



# APPENDIX:

## Biometrics in ID Systems Frequently Asked Questions (FAQs)

The following provides a frequently asked questions for some commonly asked questions or misconceptions for the use of biometrics in ID systems.







# General

## 1. How are biometrics used in ID systems?

The primary purpose of a biometric system is to use automated recognition technology to accurately validate the identity of an individual. To do this, biometric systems utilize two phases:

1. Enrollment or acquisition
2. Matching and decision

And requires the following activities:

- Acquisition or Collection of the biometric
- Comparison of the biometric to one or more enrolled individuals
- The use of a matching algorithm to create a decision on identity

For more information on the workings of biometric systems, please see Section 1.

## 2. What is meant by biometric accuracy, false accepts, and false rejects?

Unlike password-based systems, where a perfect match between two “passwords” is necessary to validate a user’s identity, a biometric system works probabilistically because two biometric samples are never identical. Instead, a biometric system generates “scores” based on the level of confidence that two samples are a match. Because of this probabilistic nature, there is a trade-off between two types of errors:

- *False accept rate (FAR)*. The false accept rate is the proportion of verifications with wrongful claims of identity that are incorrectly confirmed. For example, during a verification transaction, if an impostor fingerprint happens to look sufficiently like the one enrolled, the algorithm decides that they are highly likely to be from the same characteristic and incorrectly verifies the user as the valid identity. This is a false accept as an impostor has been allowed access.

- *False reject rate (FRR)*. The false reject rate is the proportion of verification transactions with truthful claims of identity that are incorrectly denied. For example, during a verification transaction, if the finger is placed on the sensor such that only part of the fingerprint is visible and the algorithm incorrectly fails to verify the user, this is known as a false reject, as the legitimate user has been denied access.

For more information on biometric performance metrics, please see Section 6.5.

### 3. How do I establish if there is an operational need for integrating biometrics into an ID system?

Establishing a business or operational need involves investigating and documenting the costs, benefits, risks, and alternatives to biometric use. The primary role of biometrics as part of ID system is increased trust and confidence in a person's uniqueness and identity and as a potential authentication mechanism. This can be achieved by using biometrics to check for duplicate identities (identification) or using biometrics to validate a person against a previously stored biometric for that individual (e.g., for authentication during transactions). The requirements for each of these functions will be unique to the local environment, and benefits must be balanced against the costs and risks (both security and privacy)—such as those related to data protection and privacy, inclusivity and non-discrimination—both of the biometric systems and potential alternatives (e.g., relying on existing forms of identification and demographic deduplication for identity proofing).

Such an evaluation should be done during the project planning phase, and involve technical and legal experts, as well as consultations with the public and other potential stakeholders (e.g., the relying parties who will use the system for identity services).

### 4. What is the difference between enrollment, verification (1:1), identification (1:N), and deduplication?

Biometric recognition involves several distinct processes:

- *Enrollment* is the process by which individuals are processed and their identity data is recorded into the ID system. This usually requires the individual to provide a strong link to their identity through one or more pieces of existing original documentation such as a birth certificate, driver's license, or passport or possibly a qualified "introducer" for persons without documentation. Biometrics are captured at this point to establish a link, sometimes known as biometric binding, between the biometrics and the person.
- The identification process is where a captured biometric is compared against multiple individuals' existing biometric data within a database. This is known as a one-to-many match (1:N). This generates a list of the most likely match candidates, usually ordered by their similarity. The position of a candidate in this list is known as the rank, with the top candidate (most similar) known as rank 1.
- *Biometric deduplication* uses an identification process to compare captured data against the

enrollment database to ensure that the person is not already enrolled to ensure the removal of any duplicates of the biometric identity data enrolled into a system's database.

- *The verification process* is where a captured biometric is compared against a single individual's existing biometric data within a database or stored on a credential. This is known as a one-to-one match (1:1). This comparison produces a match score that is indicative of likelihood of the match being from the same individual. The individual is then considered verified if their match score exceeds a system defined threshold. Where the match verification fails, a manual verification check may be undertaken by a human operator.

For more information on biometric applications, please see Section 1.3.

## 5. What is the difference between biometric and non-biometric identification and deduplication?

Enrollment in an ID system occurs through users providing their biographic data for registration. That captured data can then be compared against the enrollment database to ensure that the person is not already enrolled. Deduplication can be performed by comparing biometric data, biographic data, or a combination of both. The deduplication process lowers the risk of identity fraud by helping prevent people from obtaining multiple identities within an ID system that seeks to establish the uniqueness of enrollees, such as most foundational ID system. Biometric deduplication is used globally in over 130 developed and developing countries as part of the issuance process for national IDs, population and civil registers, or similar foundational ID systems.

For more information on biometric applications, please see Section 1.3.

## 6. What is the difference between biometric and non-biometric authentication and verification?

The verification process is where captured data is compared against a single individual's existing data within a database. This is known as a one-to-one match (1:1). Verification can be performed by comparing biometric data, biographic data or a combination of both. Where biometrics are used, this comparison produces a match score that is indicative of likelihood of the match being from the same individual. The individual is then considered verified if their match score exceeds a system defined threshold. Where the match verification fails, a manual verification check may be undertaken by a human operator. Non-biometric authentication uses either something you know (e.g., passwords or personal Identification numbers [PINs]) or something you have (e.g., a smart card or passport).

For more information on biometric applications, please see Section 1.3.

## 7. What modality or modalities of biometrics can be used for an ID system?

A variety of different biometrics can be used in ID systems; however, the most commonly used traits are fingerprint and iris for identity deduplication, as well as face for identity verification.

Fingerprints are currently the most commonly used modality for biometric recognition in systems such

as foundational IDs. This technology relies on the unique minutiae of a fingerprint and requires specific technology (fingerprint readers) for use. A fingerprint pattern under normal circumstances is permanent and unchanging; however, there are factors that can influence the quality of a person's fingerprints such as employment types, age, and some medical conditions.

Iris recognition is a highly accurate and automated method of biometric identification of someone's unique and stable eye patterns using pattern-recognition techniques on video. In comparison to other biometric modalities, iris recognition may also provide better protection against spoofing and other attacks. The distinct iris pattern is made up of a number of features within the eye muscle, such as collagenous fibres, crypts, colour, rifts, and coronas. The high stability of the modality is based on the iris pattern's minimal change from formation prior to birth through the first two years of life.

Facial recognition technology (FRT) has undergone a technology revolution over the last five years. The greatly increased accuracy of FRT has led to the widespread adoption of FRT solutions for both foundational and functional types of ID systems particularly for 1:1 verification against a mobile device. This biometric technology is well-developed, and commonly engaged for many different use cases. For example, FRT is a fundamental component of international passport usage through International Civil Aviation Organization (ICAO) standards for e-passports and is commonly used as part of the passport issuance process. Smartphone devices and applications are increasingly using FRT to verify owners or users, which is leading to growing acceptance. However, there are some specific data protection and discrimination risks related to FRT---particularly when used for 1:N matching---due to the widespread availability of photos online, the ability to capture facial images at a distance, the increasing use of FRT for law enforcement, and bias in facial matching algorithms.

For more information on different biometric modalities, please see Sections 2, 3 and 4.

## 8. What are the pros and cons of a multi-modal ID system?

The process of fusing (i.e., combining) different sources of information is called multibiometric or multimodal biometrics. It is in particular relevant for large-scale biometric identification and de-duplication systems with millions of enrollment records (for example the foundational ID systems used in India, the Philippines, and Indonesia). There are two major benefits to multibiometric recognition:

1. *Improved matching performance.* Using multiple sources of biometric information will improve the overall matching performance leading to a lower FMR and FNMR. In particular for large-scale identification (e.g., de-duplication) systems, the use of multiple biometric sources is often required to yield an acceptable identification performance.
2. *Better inclusion and fault tolerance.* Combining different biometric traits will ensure that the system can still be used even when certain biometric data is not available or unreliable because of low quality. The improved acquisition performance (i.e., better FTE, FTA, and FTC) will improve the fault tolerance and inclusion rate of individuals that are to be enrolled in a biometric system.

Improvements of multibiometric systems also come at a cost, in terms of added complexity, lower acquisition throughput, or increased price. For example, capturing multiple samples of the same finger will add complexity and increase the effort of the acquisition process. In addition, capturing fingerprints from different fingers may require more expensive fingerprint scanners or the use of multiple biometric traits may require additional capture devices increasing the overall cost of the system. Also, multibiometric systems will require additional storage capacity and increased bandwidth and computation resources.

Given the unique sensitivity of biometric data used for identification purposes, such data should only be collected where necessary for a narrowly defined and lawful purpose. Collecting more biometric data than necessary to establish uniqueness or for a specific use case would, therefore, not be justifiable and goes

against general data minimization principles. The potential for re-identification through linked data is also increased as there is more personal data being stored.

For more information on multimodal systems, please see Section 4 of the Primer.

## 9. Where can I find information about the potential drawbacks for a particular modality?

**Fingerprints:** Infants and small children that have not fully developed cannot yet have their fingerprint taken, and aging results in the loss of collagen, making the skin loose and dry, negatively affecting the quality of fingerprints acquired by sensors. Manual laborers and persons with disabilities may also have difficulty with fingerprints. Furthermore, risks and challenges in the use of fingerprint recognition include a wide array of spoofing possibilities, universal master print attacks, replay attacks (where stolen fingerprint data is sent to the host remotely) or other kinds of attacks.

**Face:** Unlike other biometric modalities such as fingerprint or iris, facial images are easily available in high volume online through social media channels and can be silently acquired at a distance by cheap equipment (CCTV, smartphones). Facial characteristics can also be used to identify race, gender, ethnicity, and other characteristics that could potentially be used to discriminate or otherwise cause harm. Facial images can be easily captured and matched with the subject from which the biometric was taken without any action or knowledge required directly by the subject. Face recognition algorithms can show varying degrees of bias against certain demographics of a population if they have not been trained on a sufficiently diverse gallery of face images.

**Iris:** Iris systems can be expensive to implement, requiring relatively niche capture devices. Capture for iris systems is more controlled than some other modalities. Potential issues include eye rotation, pupil dilation, occlusion, movement, environment, eyelash obscuration, glare and height. Iris may also exclude subsets of the population, including those with common medical conditions such as cataracts and glaucoma and those that commonly use glasses or contact lenses as well as people with albinism. Additionally, there is the potential for a higher failure to acquire for younger subjects and some racial sub-groups have little visible iris structure which may make capture difficult.

**Voice:** An individual's unique voice print can be used for verification, validation, and authentication purposes but is generally not reliable for 1:N identification or deduplication. Because, an individual's voice prints can change over time and due to several factors, such as sickness, environmental conditions etc. therefore, regular updates of individuals' voice samples are generally necessary for voice recognition systems.

For more information on modality specific risks, please see Sections 2, 3 and 4.

## 10. How can biometric data be protected to help mitigate data protection and security risks?

Like other sensitive personal data, biometrics must be adequately protected from theft and misuse through a combination of legal, technical, and operational measures.

Technical mitigation methods include:

- Appropriate data security measures and controls to protect the integrity and confidentiality of biometric data, having regard to the increased risk associated with such data, including encryption, template protection, digital certificates, and public key infrastructure (PKI).

- Access controls must be securely managed.
- Data must be separated and anonymised.
- Data access and movement must be logged and traceable.
- Third Party external access restrictions must be in place for templated data.

Operational mitigation methods include:

- Operators must be sufficiently trained in use of the system.
- Robust governance structures and audit procedures must be in place.
- Data Protection Impact Assessments (DPIA) and threat modelling must take place.
- Regular technical performance reviews must be undertaken.
- Designating a data protection officer.

A comprehensive legal and regulatory framework will include data protection measures including:

- Demonstrating a clear lawful basis for the processing of biometric data
- Collecting biometric data only where necessary for limited, lawful purposes
- Minimizing collection of biometric data that is necessary
- Ensuring biometric data is kept accurate and for no longer than necessary
- Being transparent with users about the processing of biometric data
- Requiring appropriate organizational and technological security measures in respect of biometric data
- Carefully controlling external access to biometric data and ensuring appropriate contractual protections are in place with any third-party suppliers
- Creating mechanisms for external review and audit

For more information on mitigation methods, please see Sections 5, 6 and 7.

## 11. When might biometrics not be the best solution?

Some of the key questions when deciding whether or not to use biometrics for either 1:N identification (e.g., to establish uniqueness) or 1:1 verification (e.g., to authenticate for transactions) include:

- Is it possible to establish uniqueness of enrollees to the degree required for the purpose of the system using existing identity evidence and/or demographic deduplication (i.e., given the population size and the quality and ownership of existing IDs)? Is a higher level of authentication required for a specified purpose that can't be provided by other methods (e.g., using multi-factor authentication or a cryptographic authenticator)
- Is there a clear lawful basis for the use of biometrics, and are biometrics necessary for a narrowly defined purpose?

- Can biometric systems be effectively operated in the proposed environment with adequate security standards and sufficient legal, operational, and technical controls?
- Will biometrics be accepted by the intended users?
- Will the use of specific modalities or the requirement to provide biometrics for identification and/ or authentication exclude a significant percentage of the population?

## **12. What is an ABIS and AFIS, and what are the differences?**

Both ABIS (automated biometric identification system) and AFIS (automated fingerprint identification systems) are software applications designed to undertake the enrollment, matching, and management of biometric information focused on the permanent storage of biometric templates and matching. AFIS are focused on fingerprints only while more modern systems (ABIS) support multiple different types of biometrics. Common examples of ABIS system modalities include fingerprint, face, and iris.

For more information on ABIS and AFIS, please see Section 6.1.2.

## **13. What are some international biometric organizations for networking and discussions?**

There are several international not-for-profit membership-based organizations working on biometrics, including:

- The Biometrics Institute (<https://www.biometricsinstitute.org/>)
- The European Biometric Association (<https://eab.org/>)

# Enrollment, Authentication, and Storage

## 14. What are some techniques for acquiring good quality biometrics?

There are various procedures that may be followed to ensure good quality biometrics.

*Setup of devices and environments.* Consider the capturing device, lighting, and backgrounds. These can have a big impact on the quality of a biometric and may be easy to implement.

*Operator training and education.* Operators can be trained to assess and ensure many quality characteristics. While these can be documented and taught to operators, it is typically unlikely that all different quality characteristics will be able to be maintained in all instances, free of defects, degradations, and interferences. The training also needs to consider potential fringe cases and sensitivities to ensure they are handled appropriately.

*Quality assurance.* There are several issues and challenges with capture quality that must be addressed. Ensuring robust quality assurance is critical to system performance and can be achieved in two ways:

- Manual inspection by operators that is reliant on efficient training and operator guidance
- Automated quality assessment that provides high efficiency and depth of analysis to improve outcomes

For more information on acquisition best practice, please see Section 7.10.

## 15. How should cases be handled when a person is unable to provide biometrics to enroll in the ID system?

Support for those unable to use a biometric system is critical to ensure inclusion. Large scale systems have addressed this issue in a variety of ways:

- Providing multiple biometrics so that if one or more biometrics are not present or unable to be enrolled there is still a biometric that can be used



- Noting in the identity record any missing biometric, and providing an alternative authentication method
- Retrying with relaxed quality standards with appropriate logging
- Taking one or more photo(s) of missing biometrics (all exceptions declared) to deter abuses

For more information on acquisition issues, please see Section 1.1.1.

## 16. How and where should biometric data be stored?

Biometric data is considered to be sensitive personal data and so needs to be protected with greater rigor than less sensitive types of data. This is particularly the case for government ID systems since they are an active target for sophisticated internal and external attacks. Many of the controls listed are the same as those needed for any large-scale identity system such as ISO/IEC 27001 and ISO/IEC 29100 from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). These standards support defining system security and the data protection safe-guarding requirements.

Biometric data generally refers to either the raw biometric capture or the biometric template. Depending on the use this data can be stored and used either on a credential or device, inside a central system, with a node of a distributed application, or in a cloud storage bucket. The appropriate location for this data depends on the security requirements, data protection requirements, speed and network connectivity, the computing infrastructure available, and the type of application.

For more information on data storage, see Section 6.1.

## 17. Do I need hosting capacity within existing government infrastructure, or can biometrics solutions be hosted in the cloud?

Biometric data is considered sensitive personal information. Some countries treat this as sovereign data that must be stored onshore within a country. Options exist (and are utilized by some major biometric implementations) to host externally to a government agency but within private clouds established onshore with the appropriate level of security and control. The choice to host the biometrics solution externally must be informed by strict data access controls, high levels of independently assessed security, both physical and logical, the ability to ensure all data is stored in the country of origin, and that no third parties can access or transmit this data apart from the managing agency.

For more information on cloud storage, please see Section 6.1.3. For more information on third party management, please see Section 7.14.1.

## 18. What is the difference between raw biometric data and a biometric template? Which one should be kept?

The raw biometric data (known as the biometric sample) is data gathered directly from the sensor before any processing has been carried out. A template is the refined, processed, and stored representation of the distinguishing characteristics of a particular individual. The template is the data that gets stored during an enrollment and which later will be used for matching. Because of variations in the way a biometric

sample is captured, two templates from the same biometric will never be identical. This is the origin of the probabilistic nature of biometrics, as the matching process can only give a decision confidence, not an absolute assurance.

There are two primary reasons to store raw biometric data in addition to templates:

- *Manual adjudication.* Human inspection of raw data to make an informed judgement about the accuracy or quality of the algorithm match or matches.
- *Re-templating.* Templates are mostly unique both to specific algorithms from a vendor and to updated algorithms frequently also have different templates. This means that an upgrade is quite likely to involve the re-templating (converting all the images to templates) of the existing database.

Both requirements mean that it is usually too impractical and expensive to remove the original raw data—as this would have to be re-collected from the population to re-template. However, the original biometric data is also sensitive and should be separated from the template and personal data.

For more information on biometric templating, please see Section 6.1.1.

## 19. Can biometric data be captured in offline environments?

Biometric data can be captured offline by mobile or fixed devices. Where data is captured in an offline environment the challenges are ensuring that data is accurately synchronized, that any stored data is protected in case of theft or loss, and that the data is protected against alteration.

For more information on offline environments, please see Section 7.10.

## 20. What are the challenges in acquiring good quality facial images in mobile devices?

For face recognition—e.g., for 1:1 authentication against a mobile device—there are several challenges caused by uncontrolled capture devices such as mobiles including:

- Illumination
- Sharpness
- Detection confidence
- Inter-eye pixel measurement
- Pose deviation
- Resolution

For instances where the person enrolling is responsible for the acquisition process, there is limited opportunity to provide instruction or correction for presentation of the biometric. Any instructions should, therefore, focus on key aspects, pose, and lighting that can have more significant impacts on the acquisition of a high-quality face image.

In some unsupervised use cases, the acquisition process may also include liveness detection features for the purposes of presentation attack detection. Inclusion of this technology in the acquisition can have an impact on the ability to capture a high-quality biometric as it could require the user to alter

behavior. The user instructions, including the use of presentation attack detection technology, should also consider accessibility issues where it may prove more challenging for specific users to provide a high-quality biometric. These user instructions could be, for example, supported by both visual and audio cues.

For more information on face biometrics, please see Section 3.2.

## **21. What are some specific populations, such as children, that are known to have problems with for biometric systems? How can these issues be mitigated?**

UNICEF's 2019 guidance on the impact of biometrics on children,<sup>49</sup> they identifies that exclusion due to system design or technological constraints and faults, as well as unintentional usage of linked data are all concerns for children. In addition to the basic hazards associated with any identity management system, the possible influence on minors should be considered for some key reasons, including:

- Because biometric systems were meant to function with adults, they are not necessarily suitable for use in recognizing youngsters. Maybe the biometric property is difficult to capture (like an iris scan with young children), or the trait performs poorly in specific age groups (like facial recognition), or the user acceptance is low (DNA).
- Working with children poses more social and ethical hazards than working with adults. Children sometimes lack the agency or chance to participate in key decisions concerning services and programs. They also lack the information and comprehension of the risks and implications of processing their own personal data. While needing parental agreement is crucial, many parents or guardians may not completely comprehend the risks, increasing children's vulnerability.

Other populations that can have issues with biometric systems include:

- Persons with disabilities. Those with a cognitive or physical disability may have difficulty presenting a biometric.
- Persons with medical Issues. Some diseases or accidents ,as well as repetitive injuries due to manual labor, cause biometrics to not be present or to be of such low quality they cannot be used.
- Older persons. Some biometrics can be more difficult to collect from much older subjects as they may suffer from a variety of medical issues.

In all cases such individuals need to be provided alternate mechanisms for proof of identity. Multimodal biometric systems can also support individuals that cannot use one modality. Good governance ensures that reporting is made available on the reasons for failures to enroll in operation.

---

49 UNICEF (United Nations Children's Fund). 2019. Faces, Fingerprints & Feet. New York City, NY: UNICEF. [https://data.unicef.org/wp-content/uploads/2019/10/Biometrics\\_guidance\\_document\\_faces\\_fingersprint\\_feet-July-2019.pdf](https://data.unicef.org/wp-content/uploads/2019/10/Biometrics_guidance_document_faces_fingersprint_feet-July-2019.pdf).

## 22. What are some of the principal fraud vectors during the enrollment process?

A biometric system is composed of several different subsystems. Each subsystem may have several different points of attack, and for each point of attack there may be one or more potential exploits. Although such attack points exist in all matching systems, not all are equally vulnerable. Enrollment fraud can occur when an individual is able to procure fake foundational documents, take over another person's identity, subvert the enrollment by using a fake biometric, or corrupt the enrollment process (perhaps through a bribe).

For more information on risks during the enrollment process, please see Section 1.5.

## 23. How can systems be designed to mitigate the risks of biometric fraud?

*Technical risk mitigation* measures include presentation attack detection, tamper mitigation, and biometric template protection.

Biometric spoofs or fakes could be used to attack a system. Such spoofs can be produced from biometric data obtained directly or covertly from a person online or through hacked systems. This attack could involve a printed photo, an image or video of a person on a tablet, or the presentation of a 3D mask or a fake silicone fingerprint. Presentation attack detection (PAD) refers to detecting a biometric spoof when it is presented to a biometric sensor.

*Tamper mitigation* involves the integrity of the sensor being both electronically tested and physically secured to ensure that no modifications or substitution have been undertaken. Tamper-proofing might include physically sealing all the internal hardware in resin and using electronic sensors to detect if seals have been broken.

*Biometric template protection*, or biometric encryption, is a method that increases the difficulty of accessing biometric information from stored data. This involves mechanisms to restrict the use of the biometric through active changes to the information stored.

For more information on technical risk mitigation methods, please see Section 6.6.

## 24. What are the pros and cons of various common biometric scanner technologies (capacitive, optical, contactless, 4-4-2, etc.) for fingerprints, and how many fingerprints do I need to collect?

There are a wide range of biometric fingerprint acquisition devices, and new devices are constantly being developed. When comparing different scanner technologies, the following are the high-level considerations:

- *Accuracy.* Different scanners have different resolutions and different form factors. For the most accurate systems all 10 fingers need to be captured, but this process takes longer than simply acquiring two fingers.

- *Speed.* A scanner used for access control needs to be quick and easy (and so may be limited to one finger). A scanner used for enrollment for a population-wide ID will need higher accuracy and will need to collect more fingers (usually 10).
- *Durability.* Some scanners are inherently more scratch and damage resistant due to the hardness of the contact surface. Optical scanners tend to be more robust under high utilization than capacitive.
- *Vulnerability.* Vulnerability is how well a scanner can be used to detect a presentation attack (i.e., fake finger). Some readers are more resistant to common fake finger techniques.
- *Contact.* Contactless fingerprint sensors are now available that read the fingerprint from a distance. These readers are fast but may have poorer quality outcomes.

For more information on fingerprint modality, please see Section 2.2.



# Standards

## 25. What are the biometric standards for ensuring data quality and interoperability?

Standards aim to establish generic sets of rules for different products and to facilitate interoperability, data exchange, consistency of use, and other desirable features. International biometric standards on interoperability allow stability and consistency of biometric technologies and products.

Some well-known biometric standards for ensuring interoperability are referenced in Section 6.5.1.

Biometric system performance heavily relies on the quality of the acquired input samples. Compliance to the corresponding international biometric standards advising on data quality ascertains a better-quality assurance management process. Hence, with the use of standards, great flexibility and modularity can be achieved.

Biometric standards for quality assurance are referenced in Section 6.6.2.

For more information on standards for ID Systems, please see the Catalog of Technical Standards for Digital Identification Systems.<sup>50</sup>

## 26. Can an image be generated from a biometric template?

While it is technically possible to generate an image from a biometric template, it is not a practical attack vector in most cases. The process is called "hill-climbing." It relies on having access to the original algorithm that was used to generate the template, and then successively updating an initially random image until the new image is closer and closer to generating the same template. Once the original template is close enough, the new image would pass a biometric match, even when the image itself might look substantially different from the original image. The computing power and setup required to do this is usually more complex than other forms of attack.

---

<sup>50</sup> The World Bank. 2022. *The Catalog of Technical Standards for Digital Identification Systems*. Washington, DC: The World Bank. <https://id4d.worldbank.org/technical-standards>.

## 27. What is a facial token in the context of an ICAO passport?

A token is representation of the captured biometric data that has had some minimal amount of processing applied. For passports, the ICAO definition of the facial token to be stored on the passport chip is a cropped and scaled representation of the actual image. This is processed by the chosen matching algorithm. The reason for storing the image, rather than extracted features, is that any recognition algorithm can be used to process the "raw" data and advances in matching are not precluded. This is known as template interoperability. Another good reason for using a token is that advances in algorithms may discover new ways of extracting distinctive features from the original biometric sample. Using a token can allow seamless upgrading of algorithms.

For more information on biometric data protection methods, please see Section 7.0.

## 28. Which international common standards apply to the use of biometrics in an ID system?

With the digital identity space advancing at an accelerating pace, there has been an increase in biometric standards that are critical for identification systems to be robust, interoperable, and sustainable.

Some international standards that apply to the use of biometrics in an ID system are referenced in Section 6.5.3.

For more information on standards, please see Section 6.5.





# Operations

## **29. Are specific governance structures required to ensure the integrity for biometrics an ID system?**

The establishment of a robust governance structure is necessary to ensure that biometric systems stay in compliance with operational goals. Governance structures should be designed to effectively implement and monitor the risk mitigation strategies outlined by threat modeling and data protection and other impact assessments. A robust governance framework will ensure that all governance roles are given specific, detailed, and transparent responsibilities. Several questions should be asked when designing a governance structure, including:

- What skills are required to successfully meet the goals of the project?
- What system processes need to be understood so that the project's activities are sufficiently overseen?
- Are those within the governance structure being provided with the information required to properly oversee the project and make decisions?

In addition, robust auditing processes will facilitate accountability and enable remediation where required. The processing of sensitive and personal data should be monitored by an appropriate, independent oversight authority and, to the extent possible, by data subjects themselves. Audit logs must be made easily accessible to the relevant authority while maintaining user privacy. A transparent audit system can also reinforce public support and uptake of the system.

For more information on governance best practice, please see Section 7.8.

## **30. What considerations in terms of communications and engagement should be considered during the rollout of biometrics systems?**

Communications and public engagement are vital for the rollout of biometric systems. This includes internal communications to staff around the use and benefits of the technology and a communications and marketing strategy to the wider population of users to ensure that they understand how and why

biometrics are being used and where they can seek more information. Good communications strategies are needed to address common concerns around the use of biometric technology without oversimplifying or downplaying risks. Beyond one-way communications, effective engagement strategies are also essential for soliciting public feedback on concerns and solutions, and improving overall trust in the system.

For more guidance, see forthcoming ID4D guides on engaging with civil society organizations (CSOs) and communications strategies.

## 31. When migrating to a new or updated system what issues should be considered?

The migration of biometric and identity data to a new or upgraded biometric system can be complex and error prone. This is because of one or more the following factors:

- *Data errors.* There may be errors in the underlying data that are unknown and cause migration problems.
- *Poor quality.* A new biometric algorithm may handle quality differently. This can result in changes in what biometrics are able to be enrolled.
- *Biometric migration.* Due to the nature of biometric systems, in most cases the biometric will need to be re-enrolled from the original raw sample acquired to generate new templates. This can be a time-consuming process.
- *Data faults.* The infrastructure undertaking the migration may make mistakes or have other IT issues that result in a loss or corruption of data.
- *Scale up.* During the initial phases of implementation, the transition to full data load may need to be carefully managed to ensure the right amount of processing capability is available to ensure transactions are handled with appropriate speed.

To reuse the change of errors, it is recommended to ensure a comprehensive planning phase for migration is undertaken, including an analysis of the existing data as well as third-party audit mechanisms to provide assurance, that there is no data loss or corruption.



# Data Protection, Privacy, and Governance

## 32. What are some of the risks of an inadequately secured biometric ID system?

There are several possible risks that have caused a global concern over the use of biometric systems:

- *Function creep.* The risk that a biometric system will be used for something other than its original purpose (or that it is used for new or additional purposes where the raw data is obtained from existing databases or sources, e.g., social media channels). This is a particular issue for identification use cases where a system designed for verification could for instance be expanded for surveillance or where a system established for deduplication is used to match against social media or closed-circuit TV (CCTV).
- *Data breach.* The risk of biometric data being accessed, read, or removed by an unauthorized source. FRT systems are often more sensitive to such breaches as the facial images can be more easily misused. This is especially concerning for databases that contain tagged images; however, even without labels a face can be potentially matched to social media images.
- *Potential discrimination.* The possibility that the biometric data held in biometric systems could be used to discriminate against people with certain identifying features (e.g., race or sex).
- *Reputational damage.* The risk of public opinion and trust in the system being diminished by poor management or breaches of the system.

For more information on biometric risk factors, please see Section 1.5.

## 33. How can an ID system incorporate biometrics while minimizing data protection concerns?

In general, the use of biometrics must satisfy the principles of necessity and proportionality, meaning the measure is necessary to meet a specific and legitimate need (and would be effective in doing so) and there is no less intrusive way of achieving that end. A balancing test must be undertaken to strike a fair balance between the risks to and impact on the individual and the apparent benefit to society or the public interest.

This test can take the form of a data protection impact assessment and accompanying policy document.

Appropriate safeguards must also be implemented to ensure data minimization, purpose limitation, robust data security, the prevention of unauthorized access or use, and strict retention and disposal requirements. Data must not be repurposed or shared with third parties without their knowledge, and, in every case, there must be a lawful basis for the data processing. Finally, there should be a mechanism for human intervention and oversight, including an easy way to exercise individual rights, lodge complaints, and seek redress.

For more information on data protection, please see Section 5.2.

## **34. What sort of legal measures may be required before implementing biometrics in an ID system?**

Each country's legal system is unique and therefore, different measures may be required in different countries. In turn, there must be a clear lawful basis under the data protection legal and regulatory framework for processing biometric data in an ID system. Most ID systems mandate participation and enrollment; therefore, consent is unlikely to be a suitable lawful basis for the associated processing of biometric data. The imbalance of power between individuals and public authorities also means that the former may feel pressured to give their consent even if not mandatory (especially if failure to give consent means they may not access a particular government service or benefit). Rather than relying on consent, a public authority should, therefore, be able to demonstrate that the collection of biometric data is necessary for a reason of substantial public interest relating to the ID system, on the basis of a law that contains adequate safeguards (e.g., in respect of transparency, data security, data minimization, purpose limitation, and accuracy).

For more information on laws and regulations, please see Section 5.

## **35. Are biometrics considered to be personally identifiable information (PII)?**

The US Department of Labor defines PII as "Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."<sup>51</sup> Biometrics are almost always deemed to be PII due to their ability to uniquely identify an individual. Moreover, they are typically classified as "sensitive" PII, which entails greater risk to the individual if compromised or disclosed without authorization and therefore requires higher levels of protection.

---

<sup>51</sup> U.S. Department of Labor. 2022. "Guidance on the Protection of Personal Identifiable Information." Washington, DC: U.S. Department of Labor. <https://www.dol.gov/general/ppii>.

# Security and Accuracy

## 36. What are the metrics for measuring biometric systems technical performance?

The following terminology is used:

- *Match*. A comparison decision stating that a biometric probe and biometric reference are from the same source.
- *No-match*. A comparison decision stating that a biometric probe and biometric reference are not from the same source.
- *False accept rate (FAR)*. The proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed.
- *False reject rate (FRR)*. The proportion of verification transactions with truthful claims of identity that are incorrectly denied.
- *False match rate (FMR)*. FMR is the percentage of completed imposter (non-mated) matching trials whose matching score is greater than the threshold.
- *False non-match rate (FNMR)*. FNMR is the percentage of completed genuine (mated) matching trials whose comparison is less than the threshold.
- *Equal error rate (EER)*. EER is the point where the FMR is identical to the FNMR.
- *Failure-to-enroll rate (FTE)*. The number of people that cannot enroll a biometric at all.
- *Failure-to-acquire rate (FTA)*. The number of people that have difficulty using a biometric.

Note that in literature, FAR versus FMR and FRR versus FNMR are often used interchangeably. There is, however, a subtle difference in that FAR and FRR are system level errors, taking into account, for example, samples that failed to be acquired. Other terminology that is used in literature is the true acceptance rate (TAR), which is defined as  $1 - FRR$ , measuring the degree that a biometric system correctly matches the biometric from the same person.

For more information on biometric performance metrics, please see Section 6.4.

## 37. What other types of security technologies should be applied to ensure the security and integrity of a biometric ID system?

Biometric data should be securely stored and protected to prevent processing by unauthorized parties, loss, theft, unwanted destruction, and damage. Given the increasing occurrence of large-scale cyber-attacks on IT systems (including well-documented cases of breached systems holding biometrics), it is vital to ensure that data is adequately secured. The biometric data must be protected throughout all system components and during all phases of the system lifecycle.

Technical mitigations that assist with data protection include:

- *End-to-end encryption of data both in-transit and at rest*
- *Data anonymization and pseudonymization wherever possible*
- *System confidentiality and integrity*
- *Data backups*
- *Ongoing assurance mechanisms*
- *Digital certification and PKI*
- *Access and control platforms*
- *Robust logging*

For more information on technical mitigation measures, please see Section 6.

## 38. What information security issues need to be considered for a biometric ID system?

All physical and electronic security systems have vulnerabilities that require a variety of different levels of expertise to exploit. Any security system can be circumvented with enough access, time, and resources. No single security technique can remove all possible points of vulnerability in a system. As such, it is important to consider security infrastructure as a series of complementary interconnecting factors that are enforced by appropriate levels of governance.

In addition, new methods of attack are being constantly invented due to the evolving global technological landscape. For example, attack artifacts such as realistic latex masks and 3D printed fingerprints are now increasingly available. This trend will mean that sophisticated attack scenarios that were once restricted by availability, resources, and skill will become increasingly frequent.

It is important to note that concerns about risks vary by different stakeholders. For example, citizens may be concerned about their privacy, discrimination, and function creep, whereas governments may be more concerned about public trust and reputational damage.

For more information on technical mitigation measures, please see Section 6.

## **39. What does manual deduplication or manual identity resolution refer to in the context of an identification (1:N) system?**

Most foundational ID systems, particularly those based on face and fingerprint recognition, require the use of human operators to assist the automated system in resolving matches with match scores that fall between the automatic rejection and acceptance thresholds.

If the algorithm assessing the similarity of two images fails to verify the match because the match score falls below a predefined threshold, the transaction can be referred to the manual resolution team (sometimes called manual adjudication) for processing.

As the capability and performance of current biometric solutions improve, the cases that absolutely require humans to perform the identification process will become increasingly difficult, in the sense that the amount and type of such cases requiring manual processing will necessitate humans having improved training and tools.

Section 7 contains more information on the operation of biometric systems.

## **40. How can the integrity of biometric ID system operators be ensured?**

System operators should receive comprehensive system training, both on how to use the system and on how to avoid misusing it. Operators should also be audited on a regular basis by a transparent and independent authority to ensure that individuals only have access to the functions needed for their specific job function or role. Furthermore, the system design should restrict any individual's ability to alter or delete data or make changes to the system's operation (such as changing the matching threshold).

Strong auditing processes will facilitate accountability and allow for remediation where necessary. The processing of sensitive and personal data should be overseen by an appropriate, independent oversight authority, as well as, where possible, by the data subjects themselves. Audit logs must be easily accessible to the appropriate authority while protecting user privacy. A transparent audit system can also boost public support and adoption of the system.

Section 7.1 contains more information on operational security.

## **41. Can biometrics be spoofed?**

The integrity of a biometric system is obviously an important attribute in maintaining public trust and ensuring that sensitive and personal data is not compromised.

New methods of attack are being constantly invented due to the evolving global technological landscape. For example, attack artifacts such as realistic latex masks and 3D printed fingerprints are now increasingly available. This trend will mean that sophisticated attack scenarios that were once restricted by availability, resources, and skill will become increasingly frequent.

For more information on system compromise, please see Sections 7.4 and 7.5.



## **42. What sort of ongoing checks and reviews are needed to make sure the biometric components of my ID system are working effectively?**

It is recommended that biometric systems undergo regular audit at least yearly. This audit should look at various measures of system performance including failure rates, transaction performance, and acquisition quality. Another useful activity is to have a biometric penetration attack undertaken. This can help ensure the system is operating as expected.

A periodic and systematic (weekly and after each patch or change brought to automated biometric identification system [ABIS] configuration) accuracy testing of the ABIS by an independent third-party can ensure the ABIS is not “silently broken.”

In addition, it is recommendation to regularly collect data not only on system performance, but also to assess the efficacy of enrollment procedures, operator performance and adherence to procedures, and people’s experiences enrolling and using biometrics. This will help identify potential issues that could lead to exclusion, poor quality data, and/or reputational damage. This can be done via the ID and biometric systems and through periodic surveys, audits and mystery shoppers, and process observation.

## **43. What issues are there with third-party access to the biometric capability?**

To ensure that the legal, operational, and technical data protection practices of any third-parties with access to biometric systems match or exceed those employed by the implementing agency. Additional measures that should be considered include:

- Strict contractual requirements and data sharing agreements outlining the minimum standards and requirements for accessing data (consider naming the specific individuals with access)
- Mandatory authorization processes
- Requirements that private sector providers are located within the country
- Government-retained ownership and control over any data collected and stored by the private sector provider on behalf of the ID system
- Prohibitions on further sharing or subcontracting of requirements to additional individuals or entities
- For more information on third-party system access, please see Section 7.14.1.

## **44. What is logical separation of biometric data and why is it important?**

A primary principle to help reduce the impact of data breaches is the logical separation of biometric data into different data stores. The data includes both the original raw image and the template. The link between an individual’s biometrics and other sensitive personal data in these data stores should be a unique string that is not used for any other purpose. Should the biometric database be compromised, the attacker should not be able to link any data back to specific individuals.

To be effective, separation must be managed with other technical and organizational controls, including encryption and access controls, to prevent an attacker from easily taking all the data in a single breach.

For more information on data separation, please see Section 6.2.1.

## 45. Should biometric data be encrypted?

Biometric data is especially sensitive and so needs to be protected with greater rigor than less sensitive data. This is particularly the case for ID systems since they are an active target for sophisticated internal and external attacks. Biometric template protection, or biometric encryption, is a method that increases the difficulty of accessing biometric information from stored data. This involves mechanisms to restrict the use of the biometric through active changes to the information stored. These mechanisms can introduce restrictions for the use of the biometric system for the purposes of

- *Identification.* The mass searching (1:N) of a database for a matching identity
- *Authentication.* The validation of an identity (1:1) using a biometric
- *Inspection.* Allowing a visual inspection of an image by an operator or officer
- *Cross matching.* The cross-linking of biometric databases based on template-to-template matching
- *ID systems that use biometric data must include end-to-end encryption implemented for all data, both in-transit and at rest.*
- *For more information on biometric encryption, please see Section 6.1.4.*

## 46. What does it mean to “configure” a biometric system?

Biometric systems have several parameters that control accuracy such as the threshold and quality settings. An incorrectly tuned biometric system may perform very poorly either being easily fooled or by rejecting too many of the correct individuals. For any large system it is important to recognize the importance of tuning the various parameters after operation has commenced to ensure optimal performance.

For more information on biometric configuration, please see Section 6.4.1.

## 47. What is the role of algorithm training and how can it affect the actual performance of a biometric system in my implementation context? Will biometric systems learn and adjust their accuracy during operation?

All matching algorithms need to be trained on data, both to create and tune the algorithm. This is done using large sets of labeled data that vendors have compiled. The output of this process is a model that can be used to predict similarity, but its robustness depends upon the data that was available for training. Face recognition tends to be the main biometric modality that is subject to further training. This is because it is often more sensitive to demographics, capture technology, and environment than other modalities.

Many modern biometric systems use machine learning to train the algorithm what faces are from the same as compared to different people. When this is undertaken on enormous numbers of individuals, the algorithm learns to become better and better at recognition. Recently some implementations have allowed customers to train on their own local data, resulting in more precise algorithms for local conditions. This can be beneficial but must be approached with caution as it is easy to “overfit” the training data so that performance is better on the set of faces in the training but much worse for unseen faces.

While it is technically possible to include “online” learning to adjust their accuracy during operation, most implementations where learning is available do this as a batch process. This is because of risks associated with poor or misleading training data arising from mislabeled data (ground truth).

For more information on matching algorithms, please see Section 1.2.

## 48. What is bias and how can it be minimized?

While algorithmic bias—i.e., variation in the accuracy of biometric systems based on demographics such as ethnicity or race—may be technically present in all biometric systems, it is mainly systems that use facial recognition technologies (FRT) where most concern about the adverse consequences of system bias are found. As most FRT algorithms are generated by training the system to detect several faces from a database, bias is highly likely in systems where the database is not sufficiently diverse. Early FRT algorithms often had high bias and poor accuracy; however, newer algorithms have corrected for much of this by ensuring they employ a larger and more diverse database for training algorithms.

Current FRT systems are not bias free, however, and the risk of engineering systems that contain bias is still present. It may be possible that bias cannot be eliminated for the FRT, even where the training data has the perfect demographic distribution; therefore, the goal is to minimize bias as much as possible.

For more information on matching algorithms, please see Section 1.2.

## 49. What should I bear in mind when interpreting performance claims?

Assessed biometric performance claims can be complex for those without a statistical background. When assessing performance claims it is important to consider several factors:

- *The data set.* Performance accuracy only relates to the degree to which the underlying test data matches the data that is expected to be seen by the system. Where the data is different, the performance results are unlikely to be valid. For example, a system that is tested on a population with one main ethnic demographic is likely to perform quite differently when applied to a country with a different mix of demographics.
- *Statistical measures.* The two best known accuracy statistics are false accept and false reject; however, there are also a huge range of other different types of statistics, for example, the rank one correct identification rate, the false non-match identification rate, and the failure-to-enroll rate. Each of these aggregate statistics can be useful for interpreting performance; however, choosing the right statistic to meet your solution parameters is important, and it is suggested that expert advice is sought.
- *Configuration and tuning.* Biometric systems have several parameters that control accuracy such as the threshold and quality settings. Assessed performance is dependent on the configuration and tuning, and it is important to note this may change between a test system and production.

- *Population size (gallery size).* Performance of biometric systems when undertaking identification changes depends on the size of the gallery. As the gallery size increases, the overall identification rate decreases; so, performance figures for identification must be interpreted by understanding the size of the test gallery.

For more information on biometric accuracy, please see Section 6.4.2.

## 50. What does it mean for the individual if a biometric data breach occurs, and what should the ID authority do in the event of a biometric data breach?

The compromise of any system holding personal data is extremely serious. This is particularly the case for ID systems that hold biometric data, as a person's biometrics cannot be practically changed. For the individual, that can cause concern about identity theft and loss of control of personal information.

Each country will have different laws about what is required in terms of notification after a data breach. Best practice, however, involves outreach to all those affected, an attempt to track down those responsible for the breach, and to remove any copies found online. Additional watch mechanisms may be placed on the accounts of those affected to compensate for an elevated risk of attack.

The use of biometrics is as just one part of the overall identity confirmation process and helps to control risk, not eliminate risk. Modern biometric systems should have presentation attack detection to reduce the chance of a stolen biometric being used. To prevent data being stolen it is important to have state-of-the-art data encryption for data, both at rest and in transit, and not link biometric data to demographic data (including "public" personal identifiers).

For more information on securing biometric information, please see Section 6.1.

## 51. Does biometric authentication prove a transaction occurred (i.e., is it irrevocable)?

Biometric operations are by their very nature probabilistic. Therefore, it is not possible to say with 100% certainty in most cases that an identity match has positively identified an individual. Sources of misidentification are modality dependant but can include twins, poor quality sample, or a poorly tuned algorithm. Handwritten signatures are currently used to "attest" a transaction for many legal purposes, and the traditional signature is just a type of biometric. Other biometrics can have a significantly higher accuracy than signatures but they are not foolproof. Ultimately, proof of a transaction rests with the legal framework in a jurisdiction and the risk tolerance of the organization using the biometrics.

For more information on legal considerations, please see Section 5

# Costs and Procurement

## 52. What sort of human resources are needed to effectively operate an ID system that relies on biometrics?

A functioning biometric system requires all the standard personnel needed to ensure a functioning IT solution including but not limited to security, operations, governance, database, and performance. Biometric systems, however, do have some specific types of personnel that are different from a standard IT system. These individuals include identity resolution specialists (these need training for each different modality that is used), acquisition staff (the people that are capturing the biometrics), and performance and accuracy experts (experts in how to ensure the biometric system is running accurately).

## 53. How can vendors be best selected for the various components of an ID system (algorithm, sensors, etc.)?

There are three methods to evaluate vendors' past performance and quality that can be used in combination:

- Assessment of similar technology deployments
- Use of independent well-run public benchmarks such as those conducted by the US National Institute of Standards and Technology (NIST)
- Independent evaluation (ideally a formal ISO evaluation from a properly accredited laboratory)
- Proof of concept demonstration

## 54. What are some success factors for a good biometric tender process?

Biometric specific factors for a good tender include the following:

- A precise description of the business and operational environment
- The use of international standards

- Running a pilot (where practical) on the top selected vendors can be beneficial to identify how the technology performs in the local environment. Note: This should only be done with an experienced independent adviser to ensure that the testing is unbiased and accurate.
- Consideration of interoperability requirements
- Understanding of any data migration needs
- Flexibility in component architecture to allow replacement of biometric components devices and algorithms overtime
- The opportunity for down-selected vendors to undertake a well-defined proof of concept
- The use of independent expert advice during development
- Identification of target SLAs including accuracy, availability, and transaction times.

For more information, please see the ID4D Procurement Guide and Checklist for Digital Identification Systems.<sup>52</sup>

## 55. What are the biometric components most sensitive to vendor lock-in and how can this risk be mitigated?

Vendor lock-in occurs because of technology choices that are not sufficiently flexible and do not anticipate system changes. In a biometric system this may, for instance, relate to the templates that have been generated from a particular algorithm and cannot be used with another vendor. In most cases templates are proprietary and, therefore, not easily transferred between technologies (or even versions).

Consequently, it's extremely important for ID systems store and backup the original biometric images outside of the ABIS. Planning for how this data will be protected and used for re-enrollment is a critical part of the system lifecycle.

Systems that have highly modular architectures should also allow for the replacement of algorithms and the addition of new modalities.

For more information, please see the ID4D Procurement Guide and Checklist for Digital Identification Systems.<sup>53</sup>

## 56. What are open-source solutions? Should my biometric systems be open source?

Open-source solutions are solutions where the code is available for use without commercial restrictions and where the technology has been placed in the public domain. This can allow for significant advantages in terms of customization and integration. Its disadvantage is that it may not be as accurate or perform as well as commercial offerings that have had significant additional investment. Open source can be involved with many different components of a system from the algorithm through to the integration framework. Some solutions will mix both open and closed source solutions.

---

52 The World Bank. 2019. *Procurement Guide and Checklist for Digital Identification Systems*. Washington, DC: World Bank Group. <https://documents1.worldbank.org/curated/en/104171583178428889/pdf/Procurement-Guide-And-Checklist-For-Digital-Identification-Systems.pdf>.

53 Ibid.

# Glossary

---

<b>Acquisition</b>	The process of capturing sample information about a biological attribute of a subject.
<b>Artefact</b>	Fraudulent biometric traits that are presented to biometric identification systems in an attempt to either impersonate another subject or avoid being identified (e.g., a fake fingerprint or facial prosthetics).
<b>Authentication</b>	The comparison of a subject's presented data with the subject's stored biometric template for verification.
<b>Crypto biometrics</b>	Cryptographic biometrics, or "crypto biometrics," refers to the practice of separately encrypting each template with a unique key.
<b>Deduplication</b>	The process of eliminating redundant copies of stored biometric data.
<b>Elastic distortions</b>	The warping of fingerprints during fingerprint matching that can result in false non-match.
<b>Encryption</b>	The process of converting information or data into a code to prevent unauthorized access.
<b>End-to-end encryption</b>	A method of secure communication that prevents third parties from accessing data while it is transferred from one end system or device to another. Only the recipient can un-encrypt it.
<b>Fault tolerance</b>	The capacity of a system to continue to operate despite failures or malfunctions of software or hardware.
<b>Foundational ID system</b>	An identity system created to manage identity information for the general public and to provide identity for public and private services.
<b>Function creep</b>	When information is used for a purpose that it is not the specified purpose for which it was originally collected.
<b>Interoperability</b>	The ability of computer systems to exchange and make use of information.
<b>Liveness detection</b>	The ability of a biometric identification system to detect if a given biometric sample is from an alive and real person, not for instance a mask or picture.
<b>Matching algorithm</b>	The algorithm in a biometric identification system that matches a given sample to a stored template.
<b>Morphing</b>	A type of attack on a biometric identification system in which the stored biometric templates of multiple subjects are merged, so that these multiple subjects' templates are stored in the system as the one merged individual. For example, if such an image is used in an official identification document, all individuals whose templates have been merged will be able to use the one document successfully.

<b>Open source</b>	Code that is freely and publicly accessible for redistribution and modification.
<b>Presentation attack</b>	A type of attack on a biometric system in which obtained biometric data is used to create spoofs or fakes to try to fraudulently gain verification.
<b>Raw enrollment data</b>	The unprocessed data captured at enrollment.
<b>Similarity score</b>	The score that is generated when a captured biometric sample is compared to a stored template for the purposes of identification or verification.
<b>Spoof attack</b>	See presentation attack.
<b>Template</b>	A biometric template is a digital reference that has been extracted from a biometric sample.
<b>Throughput</b>	The amount of data that passes through a system.







[id4d.worldbank.org](https://id4d.worldbank.org)