Understanding Biometrics

Considerations for Implementing a Biometric System

18 September 2018

Understanding Biometrics

Considerations for Implementing a Biometric System

Table of Contents

Status of this Document

This is a live document which the Biometrics Institute intends to update once every two years to keep up with evolving technology, standards and guiding principles. This document has been prepared with the assistance of our Technology Innovation Expert Group, with additional reference material provided by other professionals in the field of biometrics.

We welcome suggestions for additional reference material that could be added to this guide. Please email your recommendations for consideration to manager@biometricsinstitute.org.

Isabelle Moeller
Chief Executive Officer
Biometrics Institute

1. Overview

Understanding Biometrics is a good practice guide published by the Biometrics Institute.

The Biometrics Institute

The Biometrics Institute is a not for profit organisation which promotes the *responsible* and *ethical* use of biometrics. It provides an *independent* and *impartial* international forum for biometric users and other interested parties. Its role is to educate and inform its members, key stakeholders and the public about biometrics; support the development and awareness of standards, policy and good practice, and promote the security and integrity of biometric systems and programmes.

The Institute was established in 2001 and has offices in London and Sydney. Its membership base of over 240 organisations from 30 different countries covers a wide range of users such as government agencies, borders, law enforcement authorities, banks and airlines, as well as researchers, vendors and privacy experts. It doesn't promote biometric technologies, its emphasis is on the responsible use of biometric systems, their security and integrity and most critically, privacy and data protection.

Disclaimer

The Biometrics Institute provides guiding material as a tool to help its members conduct due diligence. While the Institute has used reasonable care to ensure the accuracy of the material, due to the content and variable inputs during and after the process of implementing biometrics, the Institute cannot be held accountable for outcomes or compliance. The material has been prepared for informational purposes only and is not intended to provide legal or compliance advice. Organisations should consult industry experts should they require advice on the technical, legal or compliance aspects of the material.

Contact

Biometrics Institute
manager@biometricsinstitute.org
www.biometricsinstitute.org
Australasia: +61 2 9431 8688
Europe: +44 7887 414 887

What this Guide Covers

Biometrics is a complex subject involving many overlapping domains of interest. The aim of this guide is to assist interested parties to gain a more comprehensive and holistic understanding of the subject—to see the bigger picture, and how it fits together.

Biometrics are biological and/or behavioural **c**haracteristics of a person, which can be used in a system to recognise someone from those characteristics. Recognition encompasses **verification**—confirming that someone is who they claim to be, by comparing those characteristics on a one-to-one basis (1:1); and **identification**—the process of searching a database of such characteristics to find the biometric reference identifiers attributable to one individual, for example, in one-to-many searching (1:N).

At its core, the subject of biometrics is a technical and specialist discipline involving aspects of science, engineering, computing and medicine. It includes a large body of technical knowledge, including many precise terms. These need to be used and understood consistently, and are often defined by international standards bodies including the International Organization for Standardization (ISO), particularly Sub-Committee 37 (biometrics) of Joint Technical Committee 1 of ISO and IEC (ISO/IEC JTC 1/SC 37). Standards are set, for example, to achieve consistency in how biometric samples are collected in order to be stored in a biometric database, and how the accuracy of biometric recognition should be measured and tested. All ISO standards can be found here: https://www.iso.org/committee/313770/x/catalogue/p/0/u/1/w/0/d/0

Around this core are a great variety of businesses and users that use and depend on good biometric practices, but do not all share the same degree of understanding of the core discipline of biometrics. They may however have their own domains of knowledge relating to their own specialist practice. These groups have well-established uses of biometrics such as the maintenance of criminal records, the investigation of crime and the *identification* or *verification* processes used to assess a person seeking to enter a country. The rapidly expanding use of biometrics on mobile smartphones and in other devices is greatly increasing the use of biometrics in other areas of civil society, for example, for secure access to computer systems, to approve payments, or to verify that someone is entitled to use a travel ticket bought in advance.

For these businesses and organisations, the key need is to use the specialist learning and systems from the core of biometrics accurately to manage identity—to answer questions such as 'is the person trying to make this payment or enter my country, the person they claim to be?'. Or, from the user's perspective, 'how can I prove conveniently and reliably that I am *me* and be confident that no one else can make the same claim successfully? The critical task is to find the appropriate balance that authenticates legitimate users smoothly and efficiently with minimum friction, whilst ensuring adequate security to keep impostors from gaining entry to the system or location.

Using biometrics does not automatically guarantee success because biometric recognition is probabalistic. The technology installed must be fit for purpose and implemented properly. Users need to ask a series of questions before purchasing a new biometric system (and continue to ask them, even after it has been installed): Is the system the right one for my intended purpose? Is it being used in the right way, and only for the intended purpose? Is it reliable, efficient and accurate? Is it cost effective? Is it secure? Does it safeguard privacy? What are the system's vulnerabilities? *Understanding Biometrics* is particularly intended for anyone considering the use of biometrics who is new to the subject. It includes thinking from several experts in the field, brought together by the Biometrics Institute.

Some Examples of Biometric Modalities in Use

There are multiple modalities (types) of biometrics used, of which face, fingerprints, iris, voice recognition and DNA are perhaps the best known.

Face

- Used widely (and universally) for law enforcement to help verify identity; new search applications are increasingly being created.
- Widely used for border security: over 700 million e-Passports including facial images on secure chips have been issued; e-Gates widely used for automated facial recognition; extending to airport passenger management.
- With the explosion in the popularity of 'selfies', face recognition is now being expanded to commercial and consumer payment use cases and to access devices. Software to organise PC-based photo collections adds to the awareness of this technology.

Fingerprints

- Fingerprints are one of the oldest forms of biometric identification and, as a result, have developed the largest databases globally. Matching a fingerprint or fingerprints to a record held in a large database is known as 1 to Many matching (often abbreviated to 1:N). Fingerprint databases include:
    - FBI Next Generation Identification (NGI) has >160 million sets of fingerprints.
    - US DHS Office of Biometric Management (OBIM, formerly USVisit) has over 200 million unique identities - with 10-prints.
    - The Indian Aadhaar programme has enrolled the fingerprints of 1.2bn people.
    - Law Enforcement Fingerprint Databases usually feature sets of fingerprints taken from persons arrested for offences as well as finger marks (latents) recovered from crime scenes.
- Including fingerprint sensors on smartphones for commercial and banking use has helped increase public acceptance and reduce association solely with crime.

Iris

- Iris technology uses unique patterns of the iris and can be automated and searched in a similar way to fingerprints.
- Well-regarded and suitable for large collections (such as in some refugee camps), but still a newer modality which has not yet gained widespread adoption in commercial or consumer markets.

Speaker/ Voice Recognition

- There are two major applications of speaker recognition:
- Voice - Speaker Verification / Authentication: The use of the voice as a method of determining the identity of a speaker for access control.
  If the speaker claims to be of a certain identity and the voice is used to verify this claim. Speaker verification is a 1:1 match where one speaker's voice is matched to one template (also called a "voice print" or "voice model"). Speaker verification is usually employed as a "gatekeeper" in order to provide access to a secure system (e.g.: telephone banking). These systems operate with the user's knowledge and typically require their cooperation. For example, presenting a person’s passport at border control is a verification process - the agent compares the person’s face to the picture in the document.
- Voice - Speaker Identification: Auditory Biometric Identification is the task of determining an unknown speaker's identity.
  Speaker identification is a 1:N (many) match where the voice is compared against N templates. Speaker identification systems can also be implemented covertly without the user's knowledge to identify talkers in a discussion, alert automated systems of speaker changes, check if a user is already enrolled in a system, etc.
  For example, a police officer compares a sketch of an assailant against a database of previously documented criminals to find the closest match(es).
  In forensic applications, it is common to first perform a speaker identification process to create a list of "best matches" and then perform a series of verification processes to determine a conclusive match.
- Biometric identification of telephone callers is increasingly being used by banks and other call-based organisations, thus extending the applicability of biometrics. The technology is often introduced to speed up the authentication process when a user needs to prove their identity to a call centre.
- There is a difference between speaker recognition (recognising who is speaking, using the biometric for identification of the person) and speech recognition (recognising what is being said including but not limited to applications such as machine dictation, voice command

systems, integrated telephony automation, etc.). These two terms are frequently confused, as is voice recognition. Voice recognition is a synonym for speaker, and thus not speech, recognition. In addition, there is a difference between the act of authentication (commonly referred to as speaker verification or speaker authentication) and identification.

DNA Profiling

- Invented in 1984 and in use in many countries for law enforcement purposes such as linking crimes, identifying criminals, identifying victims of mass disasters and missing persons enquiries.
- DNA is not unique: in particular, identical twins can share the same DNA profile. However, it is highly effective in identifying unrelated persons and has non-criminal applications such as genetic medical uses, paternity testing and heredity/ancestry mapping.

Behavioural

- Using the unique characteristics of the manner that you perform an action as a means of identification—such as walking style or gait, handwriting style and signature, or the unique characteristics of typing, gestures on a smartphone and computer mouse use. This can be useful in detecting and blocking irregular login activity based on the manner in which the login credentials were entered.
- Behavioural biometrics can also be used to identify fraud as early as the new user/account registration process using annotated fraud data.

Multi-Modal Applications

- The use of two or more modalities in a system may improve accuracy and enable identification to be carried out in different ways, including providing accessibility to those people unable to use one specific modality'; e.g. the option of facial recognition or speaker recognition could make a biometrically enabled service accessible to amputees unable to use a fingerprint enabled service.
- This may include increasing the security of the process for certain applications or providing extra layers of scrutiny to detect irregularities in the data stored within the system.
- Aadhaar, the multi-modal biometric database of the Unique Identification Authority of India, reached 1.1 billion records in Jan 2017 and includes fingerprints, face images and iris patterns. Multi-modal systems must be carefully deployed to ensure that the match results of each modality are weighted or 'fused' in such a way to ensure the most accurate result.

2. The Business Case for Biometrics

Defining the Business Problem/Assessing the Need for a Recognition System

Biometric recognition is all about managing risk and about a balance of making things simpler for the customer while improving overall security.

It is important to understand the identity context that the business case will be working in:

- What is the identy problem?
- How is it currently solved?

Here are some business models that are typically used when biometrics is considered:

Replacement of an existing authentication mechanism:

Consider replacing an existing authentication mechanism with biometric, for example, moving from a pin to a fingerprint on a smart phone. This works quite well when the device is a personal device. As the system scales and migrates from 1:1 to 1:N, matching against many potential identities, it becomes a much harder problem.

Use of a biometric as part of improving overall security:
Existing identity processes may be kept as is, for example a pin but adding a biometric as an additional step in the process may improve overall security. This adds another factor to the current Identity process, not only making it more secure but it can also improve the experience for users.
Other considerations include:

Enrolment:
The process of enrolling and anchoring a person's identity can be costly. It is an activity in its own right and forms the basis of your biometric ecosystem. When performing the enrolment it is important to consider how users are added to the system. Ensuring that the right identity is matched to the enrolled biometric is critical and assurance needs to be build around the system, creating trust.

Privacy and data security:
When considering the business case for the use of biometrics, consider if such a technology choice could constitute a privacy risk and if that risk is proportional to the business benefits.
If biometric data is enrolled, security of this data is not only important but critical. Ensure that the correct security is in place to not only protect the data but that the system complies with local and international regulations on the management and handling of the information.

How is a biometric selected? Know the customer!
The choice of a biometric can be very reliant on the type of customer that will be serviced with the system. As biometrics is considered by many as a very personal attribute, some people are reluctant to be enrolled onto biometric systems. Most biometric systems require cooperation of the customer during the enrolment process. The ability to get good quality biometrics is very important for the verification or identification of the identity within the system. If the system is aimed at users who don't know how to use the system or find it difficult or perhaps are from demographic that don't work well with a particular biometric, then that is challenging.

Vendor Lock-in:
It is very easy with biometric solutions to get locked into a particular eco-system because vendors often have proprieteary algorithms and proprietary components. In some cases this may not pose a problem but it is important to understand the consequences of that lock-in and what can be done to avoid that lock-in.

Life-cycle:
During this process it is important to consider the life-cycle of the not only the biometric software which is responsible for the enrolment, verification and identification of the system, but also each the biometric hardware components. What will the process be if the biometric hardware that was initially used reaches end-of-life, is no longer supported by the vendor or a new model is released?

Cost:
Everyone one of the above considerations will add up to a potential additional cost, this can have a large impact on the value of the defined business case. Having a clear understanding of these costs will ensure that the value of biometrics is not only defined in terms of added security or improved user experience, but also in regards to cost.
As a rough guide, a relatively small, simple, commercial-off-the-shelf (COTS) biometric application may cost hundreds of thousands of pounds sterling to install and maintain. Larger, complex systems, such as those used by financial institutions or Governments can cost in the region of millions or even tens of millions of pounds sterling. Therefore, the cost of upgrading an existing system's performance capabilities or processing/storage capacity will be proportionate to the size and complexity of the system or network already in place.

Finding a partner:
There are many experienced partners who can help you along the journey. You may find the Biometrics Institute Supplier Directory (www.biometricsinstitute.org) a useful resource to search for the relevant experts.

3. Privacy and Security

Why These Factors are Critical with a Biometric System

Those responsible for accessing, managing and controlling any collection of personal information carry important obligations to safeguard privacy, ensure the accuracy of data and protect against unauthorised access, for example, from a cyber-attack or internal malfeasance. This is particularly critical in relation to biometrics since this personal data describes aspects of actual people . It may be possible to change a username or password after a data breach, but a person's face image or fingerprints remain the same for the rest of their lives. Compromising such data is therefore of great concern. It is for this reason that many biometric authentication vendors tend to use algorithm-derived biometric templates which are built in such a way that they cannot be reverse-engineered, and eliminate the need for any unnecessary storage of raw biometric data.

The Biometrics Institute Privacy Guidelines

The *Biometrics Institute Privacy Guidelines* are designed to guide all relevant parties; to assure the public that managers and controllers follow good practice privacy principles in biometric-based projects; to be a guide across many different countries and jurisdictions, and across the many diverse fields to which biometrics may apply.

The *Biometrics Institute Privacy Guidelines* and accompanying Privacy Awareness Checklist should be read in conjunction with *Understanding Biometrics*. The Privacy Guidelines include:

- **16 Key Principles**, including respect for individuals' privacy, proportionality, informed consent, truth and accuracy in business operations, protection of biometric data collected and non-discrimination.
- **15 Recommendations**, including: carry out a Privacy Impact Assessment (PIA), engage closely with users, adopt a communications plan, test the system design for privacy compliance before going live, conduct regular Privacy Audits and ensure the organisation keeps up to date with privacy concerns in relation to biometrics.

It is strongly recommended that managers/Data Controllers, (dealing with biometrics on an international level, familiarise themselves with the new European Union General Data Protection Regulation (EU GDPR) which extends both its territorial and compliance coverage (see http://www.eugdpr.org/). Managers/controllers must ensure that privacy is designed into all biometrics projects at the earliest possible planning stage. It should be noted that the GDPR introduces a specific role for Data Protection Officers.

The security of IT systems and business processes is essential for the safeguarding of privacy. A cyber-attack or other external or internal security breach is not only of concern if confidentiality is compromised, but can also have a significant impact on individuals if the integrity of information is affected (corrupting accurate information held on a system), or disrupt the availability of information and therefore the continuity of a service, as, for example, when a 'denial of service attack' takes place.

Pseudonymous Identity – Secure Biometric Assurance without Disclosing Identity

This situation (though paradoxical) can arise where an intermediary gives assurance to a third party confirming someone's existence and status, without disclosing their identity. This could arise where a

bank assures a seller that a customer has sufficient funds reserved to cover a forthcoming purchase without saying who they are; in a humanitarian situation where assurance is given that a person has a certain immigration or refugee status, without disclosing their name; or where a mobile ID solution based on a smartphone confirms to a point of sale terminal that a customer is over 18 and can legally buy alcohol or other controlled goods, without disclosing other personal information. In each case the intermediary knows who the person is and may use biometrics to confirm their identity, but gives an anonymous assurance about that person to the third party containing no more information than is needed.

4. Modality and Quality

Choosing the Right Biometric System

As we have already seen, there are multiple modalities or types of biometrics used, for example face, fingerprints, iris, voice and DNA. What are the respective advantages and disadvantages of each, and which modality — or modalities — should be selected in a particular case? The biometric modality (or modalities) appropriate for a particular biometric solution might take into account:

- The accuracy and usability of that biometric modality and its relevance to the type of use needed for the proposed system.
- The potential to combine two or more biometric modalities in the same system to potentially improve accuracy and performance and increase the possibility of identifying someone.
- The importance of the user experience depends on the application being considered. For example, in financial services the authentication process needs to be virtually invisible in the race to a customer-centric advantage but alternatively, in matters of national security, the need for accuracy and strict risk management may override the concepts of convenience and fluidity.
- The business needs to be able identify someone via multiple modalities, for example, in law enforcement from a face image or a fingerprint, because the data that is available may vary between cases.

Selecting the right biometric solution to meet your requirements can be complex, including the decision as to which biometric modality or modalities to employ. This decision may not be as simple as just considering the advantages or disadvantages of one biometric modality over another; and even listing these may not be clear-cut or obvious:

- Relative advantages of one modality over another can be dependent on the context, requiring several complex considerations to be taken into account.
- A relative ‘strength’ or ‘weakness’ may very much depend on how well the feature is implemented, which may depend on the investment made in research and development of the algorithms used, and perhaps the cost of the product chosen.
- Convenience, acceptability, usability and cost versus benefit will be important to the user.
- The situation at one point in time may change where a technical advance is made, improving the coding and search algorithm used, or liveness detection used—or where a better means of making a presentation attack (‘spoofing’ a recognition system) is discovered.
- The decision may be driven by external factors. For example, an immigration or policing solution may need to include fingerprint and facial biometrics for reasons of interoperability with existing systems and data; a biometric solution to give identity assurance for a telephone call-centre may well require the use of voice recognition.
- Accuracy may tend to be seen as the ultimate goal in selecting a biometric mode but this should not be the only consideration: simplicity, convenience, speed, availability and acceptability to the user and general public may also be material. Where multiple biometrics and other recognition factors are used, the ease of collecting an additional biometric that usefully

corroborates the identity may be seen as worthwhile, even if in isolation it does not deliver the highest possible accuracy.

- Response time is sometimes the most important aspect of the solution. Often, more accurate algorithms are slower. There are often architectural decisions that need to be made to help balance accuracy, system cost and speed. For example, an algorithm may take significant computational resources to extract templates to enable faster matching, and it may be appropriate to place this burden on the client to reduce network bandwidth as well. Matching may employ hierarchical matching strategies (including binning) to allow a solution to directly trade-off accuracy and matching. Binning allows a matcher to classify biometrics into categories (such as position or broad category) to reduce the identification population size, however, this speed improvement may be at the expense of increased classification error rates.
- Some strengths and weaknesses apply to all modalities. Some biometrics can be captured on the move or without direct contact. There is the risk of presentation attacks and challenges around the accuracy of the technology when the subject ages and finally, there is the risk of poor implementation.
- The impact of current and future regulation must also be taken into consideration. Privacy is a key concern, however regulation in financial services, for example, such as PSD2 requires very specific approaches to customer authentication that could not be serviced adequately by some biometric modalities.

With the caveat that such statements should not be taken to apply equally to every case, the following comments may be useful in thinking about some biometric modalities:

- **Fingerprints**—they are well established, widely used and are highly accurate, particularly when using all ten fingers. However, not everybody has equally high-quality fingerprints; it can be difficult to place fingers correctly on the scanner and mistakes can be made in the order of enrolling multiple fingers. Good supervision is needed to control this process. If all ten fingers are enrolled, a probe can be submitted to the entire database to attempt a match. Response times may vary slightly depending on the size of the database. The use of fingerprints has spread beyond law enforcement and border management functions and they are now used in a variety of ways to control access to premises, devices and systems throughout civil society.
- **Facial image**—this is well established for use as recorded images, for example, police photos of those taken into custody and on passports/ID cards and increasingly used for searching for individuals in the public/crowds (facial recognition technology). Face images may be regarded as less intrusive than fingerprints as they can be obtained without direct or close contact with the individual. However, the fact that face images can be captured at a distance or from online sources raises other privacy concerns in modern society. Automated face matching technology is more accurate in 1:1 situations as it requires specialised training of an individual to clarify and confirm the outcomes of a 1:Many search.
- **Iris**—this is a more recent biometric mode but it is considered to be a viable biometric and is sometimes used in combination with other biometrics to add assurance. Iris is highly accurate and facilitates fast searching of large databases – the AADHAAR database in India, with currently 1.2 billion identities, is de-duplicated using iris. For example, iris searches are performed to determine if a person has more than one registration on the AADHAAR system if, for example, their fingerprints are of poor quality.
- **Voice recognition**—this can be performed remotely, over the telephone, and is therefore increasingly of in interest and take up, particularly for call centres and in financial services.
- **Vascular (including Finger and palm vein)**—this is becoming popular in some regions and is considered to have advantages in resistance against presentation attacks as it is difficult to spoof. It is easy to use, placing the finger on a scanner without requiring precise alignment or

location. Finger or palm vein biometrics lack the cultural 'stigma' often attached to fingerprints and their widespread use in law enforcement to identify criminals.

- **Behavioural**—the process allows the user to carry on with their activity as they normally would and it provides continuous authentication, for example, while the user interacts with a website or interacts with their smartphone. Not as widely established as some other modalities, but is gathering momentum as a passive, continuous background authentication protocol. Generally considered less accurate as it can be subject to more variables (for example, the typing style depends on the keyboard, what is being typed and even the user's emotional or physical state—such as being tired. It is interesting to note, however, that some vendors are beginning to use Artificial Intelligence (AI) to derive 'clusters' of user behaviour to improve accuracy across a range of scenarios in this field.
- **DNA**—this is high in accuracy when full profiles are used for searching and comparisons. DNA from crime scenes may be degraded, contaminated, and generate only partial profiles. DNA is used extensively in criminal investigations and also in civil courts to determine parentage. It requires laboratory analysis and advanced scientific expertise to ensure evidence is presented correctly, for example, in court.

Selecting the most appropriate modality or modalities is important, but there are other decisions to be considered.

Quality: SAP/FAP Rating

The US National Institute of Science and Technology (NIST) has published a best practice recommendation on mobile identification, NIST (2016), which distinguishes the accuracy with which identification is required by many users in law enforcement and border management roles, and correspondingly, the precision that is obtained by using different numbers of images and different levels of quality (and in the case of fingerprints, one, two or ten fingers, for instance). This is known as Subject Acquisition Profile (SAP) as a general metric, or Fingerprint Acquisition Profile (FAP) in the case of fingers. For example, a FAP 10 fingerprint sensor would produce a single finger image at basic quality; FAP 30 at enhanced quality; and FAP 60 could capture four good fingerprint images in one 'slap' (multiple finger capture).

Fingerprints can be captured using a flat impression on a level surface, sensing the central features of the print, or a larger 'rolled' impression from one side of the finger to the other ('nail to nail' – N2N), increasing the area of the finger from which a match can be obtained—this is relevant to searching and matching with 'scene of crime' finger marks ('latent prints').

Biometric Templates and Reference Sets

A *biometric template* is a digital representation of the original, distinct characteristics of the biometric sample that have been extracted by the biometric recognition system at the time of acquisition. For example, in simple terms, a fingerprint image captured from an individual will be converted into a table of numbers that record the position of the fingerprint characteristics on an x, y axis as well as the relative orientation of each characteristic. It is this template that is used by the matcher in a biometric system for authentication and identification processing.

Where multiple, successive biometric templates are captured at different times, the system (possibly with operator assistance) may select the best possible sample to be used as the 'best' reference set, that is, the template generated from the best quality biometric image available that will be compared with a biometric probe to look for a match.

A choice can be made as to whether the system retains just the biometric template(s) or the template(s) *plus* the original biometric images or samples. Storing the template alone requires less storage, but can limit how flexibly the system can be used. Retaining the biometric images, on the

other hand, raises significant issues about privacy and security—there needs to be a justifiable operational reason if that is done.

Considerations include:

- If the template algorithm is upgraded later in the life of the system, this can often only be done if the original images have been retained, to be re-processed.
- If biometrics are to be exchanged between biometric systems from different vendors (or with different templating algorithms), for example, to search a second system for a match against a biometric held on the first, this can be done using images if there is no search compatibility between the templates from the different systems. Retaining images therefore has significant benefits for interoperability but again raises significant questions about security and privacy.
- There are some use cases where retention is essential. Without the original images, it is not possible for a qualified fingerprint expert to compare an enquiry fingerprint with those generated in the gallery of fingerprints generated during a search. The fingerprint expert may then need to use the fingerprint images to present in court his/her conclusion that the fingerprint images match, to a recognised standard of evidential proof. In law enforcement systems (for example, police and border security) the consequences of a match being declared may be adverse for the subject of that match (for example, arrest, detention, accusation, prosecution or maybe even conviction and penalty), raising significant issues of liberty. The view may therefore be taken that a match should only be declared in such a system if the images have been reviewed by a human expert qualified to make that confirmation.
- Retention of images has implications for privacy and the need to safeguard data securely. A key decision will be whether to store the data centrally or locally on smaller servers or devices. It is essential to protect such data and there are many commercial solutions available that use, for example, feature transformation techniques (altering the data so that the original features are not obtainable by unauthorised access) or biometric cryptosystems that use encoded auxiliary data to protect the original sample while still being able to perform searches and authentication tasks.
- It may be possible to mitigate privacy issues by limiting the data that can be viewed by the same person as part of an internal security policy for the application.
- Similar considerations may well apply in relation to other biometric modalities.

It is important to understand the context to strike the right balance between these factors.

Poor Quality Samples— Damaged or Missing Biometrics & Crime Scene Samples

Sub-standard biometric samples may not be of sufficient quality to enrol or search on a biometric recognition system. For example, some people who have engaged in heavy, manual labour or who used acidic or alkaline chemicals in their work may have damaged fingerprints that are difficult to capture onto a system and may present challenges for the search algorithm. The fingers and hands may be congenitally missing or may have been subject to amputation so that fingerprints cannot be used at all. This is also the case for other biometric modalities and often in large systems it is advisable to incorporate a multi-modal approach so that those excluded from using a specific biometric, for whatever reason, may be able to use the system by enrolling a different biometric.

Another consideration is, will the system process only fingerprints captured in optimum conditions by good quality sensors, or does the system need to process 'latent' prints which are left inadvertently such as at the scene of a crime. These latent prints (finger marks) may be incomplete and of poor quality. These set a much harder challenge for IT systems and human operators to match. Likewise, will face images, iris prints or video recordings be captured only in good conditions, for example, in a studio or laboratory, or can they also be captured under poor lighting or audio conditions?

Searching for a match using degraded biometric images is a far more challenging task than when using optimum samples. To continue the fingerprint example, latent, or scene of crime fingerprints may be smudged, incomplete, damaged by water or chemicals and may offer only a small sample area. Also, it may not be clear which finger has left a print. Forensic techniques may be needed to develop the latent print into something that can be seen. This also applies to other biometric samples, such as face images, DNA and voice recordings, retrieved from crime scenes or other sub-optimal environments. Vendors produce specific algorithms to undertake the enrolment and searching of such variable quality biometric data and these are different to the algorithms used for optimum quality biometric samples that are taken under controlled conditions usually using quality control procedures. It is therefore important to understand the types of data that will be used in any prospective biometric system or networks and obtain the correct algorithmic processing units to undertake the different forms of searching required.

5. Business Model—The Holistic View

Understanding How the Solution Will Operate—Who Does What?

Biometrics are an important technology, probably best thought of as an 'enabler' for the wider capability of identity management. It is important to understand the holistic business process for identity management and how it can best be used, including how a proposed new system will operate and integrate with the organisation and its existing IT systems.

Is the organisation able to explain the key benefits of the proposed system? For example, to enable the organisation to make much more effective use of identity, it may want to link the contact the organisation has with the person, whenever contact is made (known as a person-centric approach). This can apply in many types of organisations whether commercial or governmental. Organisations should ask whether they are aiming to do this efficiently, quickly and accurately? Are they communicating those benefits to all stakeholders involved in the system?

How Does the Proposed System Work Within the Context of the Organisation and its Existing Information Technology System?

Integration will be important too. If a biometric system is to act as a central 'hub' to link together information held on several other IT systems, then the overall strategy has to be clearly defined and adopted by all stakeholders, and committed to for the long-term. This can be very successful; however, it is more complicated than building a self-contained system that sits on its own. This integration process needs to be planned in detail in conjunction with the selection of the most appropriate biometric modality or modalities to support the business process.

Some of the broad elements the organisation may need to consider include:

- Data gathering and analysis to describe how the system will work holistically—this includes the data you will gather and process; the biometric modes you intend to use; business processes you will need (taking the opportunity to make improvements and not just automate what you have now); the roles you will need to run the system effectively (general, specialist and support/administrative); the systems and infrastructure you will need (including specialist biometric equipment such as sensors and how they will be integrated into host systems); and the interdependencies and interfaces you will have with other systems and organisations. In short, the business model for your complete system.
- The engagement you will need with users, managers and all stakeholders, going beyond superficial exchanges to genuine listening and understanding with an open mind.
- The volumes of data and transactions you expect and the performance you will need from the system to deliver the planned outcomes.

- How you project the system may grow during its lifecycle, for example, for new business areas, increases in volumes of data and volumes of transactions and the inclusion of new biometric modes, should they be required (or, a decision that these will not be provided for).
- How security and privacy will be protected and appropriately responded to with policy and operating procedures, for example, fall back mechanisms, emergency management and disaster mitigation, protection against cyber incidents or denial of service events, malicious attacks or system failure.
- Which channels you will be using to capture or deploy biometrics, for example across mobile, web or physical locations? Depending on the range of channels, you will need to consider whether an on-device, on-premises or server-side model is best suited.

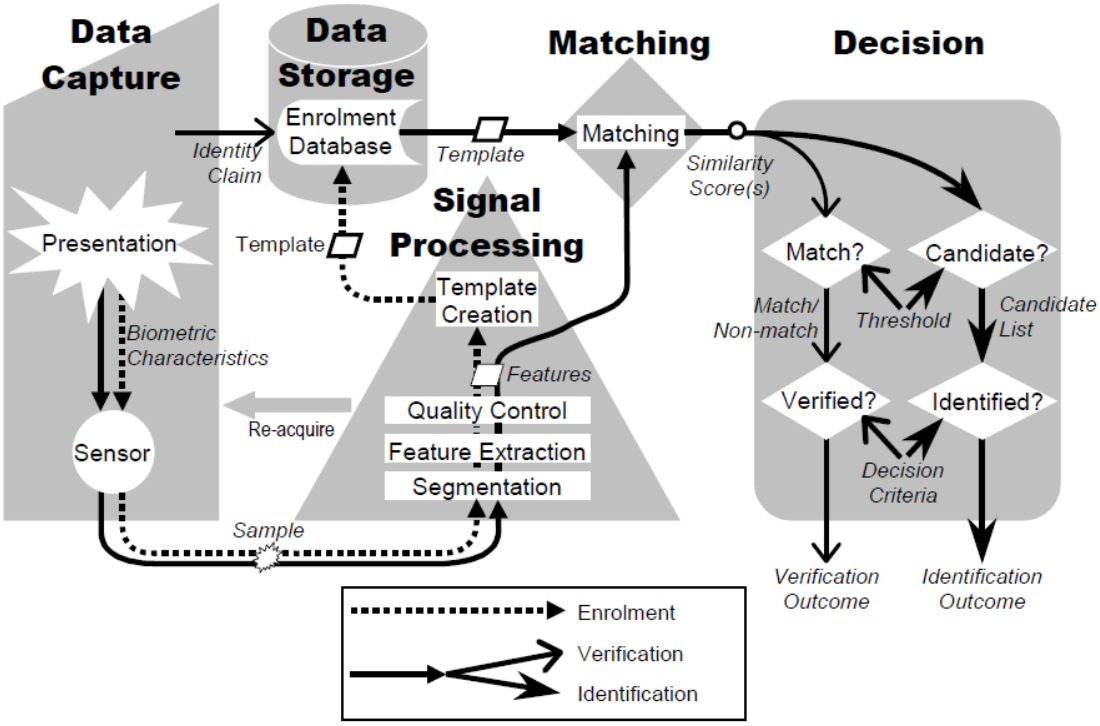
There are several other more detailed issues that may be useful to mention:

- **Usability**
  System functions need to work well, not just technically but when used in the real world of the user, as she or he experiences it. Piloting new functions with the involvement of real users, to ensure the solution works well in practice (not just on paper) is sound. This includes considering response times and acceptance criteria. Can the equipment be used properly and is it sufficiently ruggedized to be deployed in all the environmental conditions that are expected, for example, in bright light or at night; or in the rain, dust, heat or cold? What level of supervision is planned when the system is used? How well will users manage when a novel or innovative business solution is being provided—this includes solutions that are new in this context, even if the same practice is well established elsewhere.
- **Accessibility**
  Not all system users and subjects who may be asked to provide biometric samples are equally able to interact with the system. There are many factors, but some dominant ones are culture, race, disability and language. It is important that solutions include some adaptation if possible (or, at least, include appropriate exceptions or fall-back arrangements). Difficulties may arise at all points where the system is required to be used, from when biometrics are enrolled to when they are verified later. For example, older people, or, as mentioned earlier, those who undertake manual labour, may have difficulty providing clear fingerprint images. The positioning of biometric sensors needs to be suitable for people of widely differing height and by those who may have a disability.
- **Training**
  Any new system needs to be used correctly, particularly when it is introducing new ways of working. Appropriate training and support is essential, and should be designed and tested in advance to ensure all operating staff reach the required standard of skill.
- **Specialist Roles**
  Depending on the system being developed, some operating staff may need advanced skills that go beyond a normal level of aptitude that could be taught on a short course. Some skills require professional qualifications and experience – for example, for expert fingerprint or other biometric examiners – as well as good knowledge of the system they will be using. Some specialist roles may require special selection, such as facial super-recognisers.
- **Legal Requirements**
  Due to the nature of the personal information being managed on a biometric system, individual operating staff or the organisation may be held accountable for any breaches of privacy or security and face potential legal action. It is therefore important that suitable guidance and training is given to all staff operating and managing the biometric system.
- **User Administration**
  Making sure that users receive an efficient and professional service is important, for example, in being given access when they are correctly authorised. So too is an efficient and

professional response in the event of routine and urgent problems such as a breach of security or a member of the operating staff leaving their specialist post. Reporting on system use to highlight exceptions or investigate incidents is good practice. Grouping similar system use together to simplify administration is often efficient, for example, for Role Based Access Control (RBAC).

6. Testing

Testing is an essential part of any information technology system, but in the case of a biometric system there are extra considerations that are important to understand. A high-level description of the components of a general biometric system including the stages at which testing can be considered is shown in Figure 1.



ISO/IEC 19795-1 ed.1.0 "Copyright © 2006 IEC Geneva, Switzerland. www.iso.org. www.iec.ch.

Figure 1: Components of a general biometric system
Extract from standard ISO/IEC 19795-1:2006 Information technology—Biometric performance testing and reporting.

The Importance of Testing

Testing of a biometric system should not just be a one-off exercise undertaken before going live. Testing is essential, complex and needs to be considered throughout the life of a biometric system, illustrated with at least some of the detail to explain that assertion, and to promote a better understanding between experts and business managers.

Test Strategy and Planning

A substantial biometric system will need a comprehensive test strategy to define what needs to be tested and how, supported by test plans, test criteria, fault logs, test data and test environments – and this list is not exhaustive.

Field Trials
Owing to the complexity of the interaction between local environment conditions, differences in system setup and different demographics, it is usually important to conduct operational testing or trials prior to a system going live to establish how well the system works and to fine-tune operational parameters such as thresholds. A biometric match threshold is a measure of confidence and it is the point where there is reasonable expectation that the biometric probe (search sample) matches the corresponding reference biometric template in the database.

Roll-Out Testing
Final verification that a new system (or the release of an enhancement to one) is ready to be released into production – allowed to go live – should come after the culmination of a substantial test process including robust unit and integration testing, and a rigorous process to evaluate and resolve essential issues. The final stage is then to confirm the new release in the live environment under controlled conditions, with a formal Go/No Go decision.

Repeat Testing Over Time
Improvements will be made to different aspects of the system over time: the sensors, the encoding and searching algorithms, routine updates to the software managing the operation of the system, and even the design of the template itself (requiring a re-coding of the database to generate the new templates). Gallery growth, quality profile, demographics, etc. will change over time and re-benchmarking / tuning is recommended. Each such stage could potentially introduce errors that reduce biometric accuracy, so it is important to re-test biometric accuracy at regular intervals and particularly when significant changes such as software or system upgrades, or new biometric sensors are introduced. Biometric accuracy is also dependent on the attention that is given to ensuring good practice to maintain data quality and accuracy of samples that are enrolled onto the system; allowing poor quality samples to be enrolled will reduce the accuracy of the system in matching search requests to the database.

Biometric Accuracy Testing

As we have seen already, a biometric system operates by encoding a biometric sample to produce a digital representation of key distinguishing features; this is known as a template. The accuracy of the biometric matching algorithm is dependent on the algorithm's efficiency and utilisation of this encoding. Accuracy can also be dramatically affected by a wide range of operational factors including usability, the operational environment, the type of system and the demographics of the users. It is worth noting that many vendors provide a risk-based assessment of their system's key performance features. This can feed into the organisation's risk engine, so that different risk appetites can be attributed to different scenarios. The vendor shouldn't make the decision for the organisation, rather provide the numbers upon which an organisation can make their own judgement call based on their clearly defined business requirements.

Testing is therefore critical to confirm that the system delivers the correct results on accuracy. There are several key metrics of search accuracy, but the most common are:

For **verification** systems (1:1):

- False Acceptance Rate (FAR) – False acceptance occurs when the enquiry biometric template from one person is matched in error by the system to the biometric template of another person in the database i.e. a False Positive or Type 1 Error. The FAR is the number of false acceptances as a proportion or percentage of the total number of biometric enquiries that should have been rejected. For example, the number of non-matches generated and presented as matches by the system as a proportion of genuine non-matches.

- False Rejection Rate (FRR) – False rejection occurs when the enquiry biometric template is not matched to the correct database template even though they are from the same person i.e. a False Negative or Type 2 Error. The FRR is the number of false rejections as a proportion or percentage of the total number of biometric enquiries that should have been accepted. For example, the number of matches generated and presented as non-matches by the system as a proportion of genuine matches.
- *The FAR and FRR are interrelated. The higher the desired accuracy, the more likely it is that there will be false rejections. Similarly, if false rejections are reduced, false acceptances will increase. A professional judgement may be required to balance the accuracy and performance depending on the required security posture of the system.*
- **False Non Match Rate (FNMR) and False Match Rate (FMR):** These terms are approximately equivalent to the above FAR and FRR rates and are often used interchangeably. The primary difference relates to the fact that these terms are specifically per attempt, whereas FRR and FAR encompasses the entire transaction including all retries.

For **identification** systems (1:N):

- **Rank 1 identification:** The percentage of searches where the subject's correct identifier is returned at rank 1.
- **Rank N identification rate**: The percentage of searches where the subject's correct identifier is returned within the top N ranks.
- **False-negative identification-error rate (FNIR)**: The percentage of searches where the subject's correct identifier is not among those returned i.e. the subject's biometrics are filed in the database but do not appear on the candidate list generated by the search.
- **False-positive identification-error rate (FPIR):** The percentage of searches in which a biometric enquiry from an unenrolled subjects results in a non-empty subject return list i.e. the subject's biometrics have not previously been filed in the database but possible matches have been generated in the search candidate list by the matcher.

Other relevant metrics:

- **Failure to Enrol (FTE)**: The failure of to be able to enrol a person into the system. In production, this is often caused by physical disability.
- **Failure to Acquire (FTA)**: The ability of the system to acquire a sample when in use. Often this will mean the user may need to retry, or may need to use a fall-back mechanism.

A full description of relevant terms can be found in **ISO/IEC 19795-1:2006 Information technology – Biometric performance testing and reporting – Part 1: Principles and framework.**

Performance Testing

Searching a large biometric database to find matching templates is a heavy computational task. Special processing sections of the servers, known as matchers, are used to perform this task. If the system is required to allow a large number of simultaneous users to search a large database quickly at the same time, for example during peak demand, then performance testing may be advisable to confirm that the system will deliver the required performance at the heaviest specified loading.

Note also that over the lifetime of a biometric system, the size of the database is likely to grow progressively as new records are added before old records are demoted or deleted, and – assuming the system is regarded as a success – experience shows demand may well increase to add many more users over time. Both factors can add substantially to the performance demand on the system. This needs to be monitored through continued testing, with the possibility considered of future system upgrades to keep the system running effectively.

It is good practice, during the procurement of a biometric system, to agree staged performance and capacity upgrades with the vendor(s). This may take the form of annual reviews where pre-determined performance targets are evaluated and the vendor is contractually obliged to meet or exceed them. This builds a culture of continuous improvement between all parties and ensures that the biometric system stays fit for purpose and delivers the required business outcomes throughout its lifecycle.

How Do I Build a Test Biometric Database?

Testing needs to be undertaken at a representative scale, for performance (for example, speed of processing and consistent service delivery) and accuracy (for example, maintaining the required FAR and FRR). Test results may not be valid if based on a sample database that is tiny by comparison to the one to be used in production. That has implications: it is not always easy to obtain a realistic and representative test database of the size and mix of characteristics of the production database being built. If the new system being commissioned is a successor to an existing system already in use, re-use of a copy of the existing live database as a test database may be a suitable basis, perhaps expanded by adding 'new' records that include combinations of biometrics from other existing records. Extreme care is needed to safeguard the privacy of the individuals whose records are used in this way. In a traditional database which includes biographic records, random data can be synthesised to conceal the identity of each individual. However, a true fingerprint or facial image remains exactly that and can be identified to the individual concerned, even if it is copied into a test database and the 'name' is altered.

Not all biometric system testing needs to be carried out by the project team itself; considerable expert testing is possible using external and national experts such as NIST or FBI (US), BSI (the Germany Federal Office for IT Security) and the NPL (UK National Physical Laboratory), or by skilled testing 'houses'. Standards such as those highlighted in the Annex, Common Criteria Protection Profiles, certification of conformity against such standards, profiles and benchmarking, may all contribute to the overall testing of a new biometric system. It should also be noted that some vendors now provide a test environment for user project teams to run test integrations prior to embarking upon a Request for Proposal (RFP – part of the procurement bidding process) or full business requirements.

Organising Large-Scale Integration Testing

Testing a very large and complex system, which includes a biometric/identity management component, with other components is itself a complex undertaking, as well as being expensive and time-consuming. However, it is essential. A good first stage is to clarify the strategy for testing the combined system, including who is responsible for testing each component and how the integration testing of those components working jointly together will be managed—once the individual components are shown to be ready. Testing progressively at scale and with realistic data is also important, as mentioned above, components and systems may function correctly at a small scale but when the system is enlarged and operated under real-life conditions it may encounter different problems that have been masked during previous small-scale testing. Responsibilities need to be properly understood and formally agreed between the parties—and are more likely to succeed in a spirit of partnership, trust and mutual support.

Presentation Attacks—Threats and Defences

Biometric technology offers important advantages but an element of risk exists that someone presents a false biometric, to pretend to be someone else (an **Imposter Attack**) or to conceal their true identity (a **Concealer Attack**). Recognising that such an attack is taking place is called **Presentation Attack Detection (PAD)**. It is inappropriate to regard any system as 100% secure; so, organisations need to consider what is good enough for *their* application and seek independent, expert advice on the risks associated with their prospective biometric system.

How can risk be managed?

- *Ignoring the risk* would be to accept the possibility of identity fraud without considering the effects and whether, as a result, the risk may increase in the future.
- *Seriously considering the risk and devising appropriate countermeasures* is a more rational and balanced approach. This is highly recommended.

The Biometrics Security and Integrity Expert Group (BSIEG) of the Biometric Institute maintains a current and detailed overview of this topic. The attacks referred to above may be attempted by, for example, presenting a photograph to the camera in place of a live face—possibly one that has been altered falsely; using a carefully manufactured mask fitted precisely onto someone else's face; using someone who genuinely looks similar to the right person (a **l**ookalike or imposter)—this may particularly be a problem in the case of identical twins; using false fingerprints (known as gummies) over an imposter's fingertips; and even by the physical alteration of someone's features, for example, by injury or plastic surgery.

Experts such as the BSIEG, or ISO/IEC, who have been preparing an international standard on Presentational Attack Detection (PAD) (ISO/IEC 30107—Parts 1 and 3, dated 2017), are investigating how attacks may succeed and how they can be detected, including rigorous testing to explore possible vulnerabilities. Countermeasures to prevent attacks succeeding may include:

- **liveness detection**—important in preventing a photograph from being accepted in place of a live person; for example, this may take the form of a randomised challenge such as the blinking of eyes in the case of facial or iris recognition.
- **multi-factor authentication**—the use of two or more biometrics, or a combination of biometrics and other forms of authentication, for example, combining facial recognition with audio or lip movement.
- **research**—to understand how better to counter presentation attacks, including attempts to deceive the algorithm during its development.

7. Defining Requirements

This Guide has sought to illustrate the many considerations that need to be taken into account before specifying requirements and building a solution. The isn't a 'model' set of requirements that would be likely to work for all possible systems. Organisations need to reflect on the complexity of the different components of their system, which might form part of their requirements definition. For example, the storage time for biometric templates needs to be considered as biometrics may change or be challenged over time in relation to the human ageing process, damage or even new presentation attacks on the system. The factors below offer a possible framework, rating each from low to high complexity.

(1) Purpose

What is the system for? What benefit will biometrics bring?

- **Low**—intend to use biometrics to improve assurance, cost-effectiveness and/or user convenience in managing identity.
- **High**—critical need for effective identity management; essential for protection of life and public safety that the function is delivered to the highest standard possible within budget constraints.

(2) Size and Scale

How complex is the solution in terms of size?

- **Low**—single, moderate-sized organisation and/or user-base.

- **High**—large national or international solution supporting multiple agencies, companies or branches; a large population of users, clients or subjects.

(3) Modality

Modes, or types, of biometrics can include face, fingerprints, iris patterns, voice recognition, behavioural, DNA or others. Original images may be stored as well as templates where this is legally permissible, relevant and appropriate.

- **Low**—the system will support one biometric mode. Choice is determined by the business needs and the relative strengths and weaknesses of each modality.
- **High**—two or more biometric modes are required initially, and perhaps with the capability to add further modes in the future. Complex data model with templates and images.

(4) Business Process

What business processes need to be defined to manage the system correctly?

- **Low**—will use largely standard, 'out of the box' functionality (commercial-off-the-shelf); configuration of standard parameters with minimum programme customisation.
- **High**—substantial amount of bespoke development, workflow, special purpose tools and reports required for multiple national or international user communities/teams.

(5) Approach to Biometric Quality and Accuracy

How will the accuracy of biometric data be managed and tested?

- **Low**—quality is important but the aspiration is to rely on automation 'out of the box' and to run the system on a 'lights-out' (limited manual supervision and intervention) basis.
- **High**—high level of scrutiny and quality assurance with regular testing and intervention; use of subject matter experts in support and operational roles. All expert operational personnel should be subject to external accreditation and regular competency testing by their respective national standards bodies in terms of their technical and scientific competencies, knowledge and processes.

(6) Standardisation

How will the use of standards and standard components be adopted in the system?

- **Low**—every effort will be taken to keep to widely accepted international standards, taking advantage of commodity components and possibilities for interoperability.
- **High**—organisations will often need to adopt vendor specific standards (recognising the risk of vendor lock-in), or even develop bespoke products or standards for this solution. However, this can be avoided by specifying generic, international biometric standards at the procurement and contract stages or by using a systems integrator to source various elements of the biometric system from different suppliers. Some large organisations have the expertise to perform this task themselves and this eliminates the need for a systems integrator and their associated costs.

(7) Architecture

How will the system and its biometric components be structured and how and where will biometric data be structured?

- **Low**—biometric data will be stored and processed in a simple and consistent way with little or no workflow automation.
- **High**—data will be stored and processed in a number of different ways and places, with significant workflow and automation, reporting, quality review, and so on.

(8) Integration with Other Systems or Data

How will data accuracy, co-ordination and integration between components in the overall system be managed and tested?

- **Low**—the system is self-contained.
- **High**—the biometric capability will be used to link identities in other systems: extensive interdependencies; multiple interfaces required.

(9) Transition

Will the new system succeed an existing one? How will go-live be managed?

- **Low**—new build; the system introduces new functionality with limited or no existing data. Issues may arise for the organisation adapting to the new operation, for example, training, new business processes, support, and so on.
- **High**— existing system is being replaced with a major upgrade of functionality, an extensive, complex migration and conversion of data is needed (for example, converting a biometric database to use a new biometric algorithm/template), and data alignment needs to be tested and managed. A 'big bang' cutover involves switching off your old system and starting your new system and processes. This carries high risk because you are relying on your new system to work perfectly. The risk can be significantly reduced by comprehensive testing. Running the new system alongside the old system (Parallel Processing) is less risky but will be more complex, effort driven and expensive.

(10) Procurement and Operation

What various options are possible, such as your own build, package or bespoke.

- **Low**—package solution, cloud/managed service, configuring a service using Application Programming Interfaces (APIs) and facilities built into smartphone solutions which is easier and quicker but has less flexibility.
- **High**—substantial biometric solutions are more likely to require major infrastructure (industry-leading biometric solutions/algorithms, matcher arrays and co-ordination, workflow/business process automation with more bespoke customisation). There is a need for supplier and customer to have the requisite skills, technical knowledge and mature, adaptable business processes.

Overall Degree of Complexity

- Very great difference in complexity, as well as cost, risk and timescale to build the solution, depending on whether the answers to the questions above are predominantly at the 'low' or 'high' end of each spectrum described.
- How does this proposed solution rate overall in terms of complexity?
- Is the organisation and the project/programme team suitably equipped and able to manage the endeavour (using 'client-side' consultancy support if needed)? Is the solution affordable and economic? Is it deliverable? Are the risks adequately understood and addressed? Does the business case/outline proposition make sense? Should the proposition be approved to go ahead?

Defining the Requirements

- An assessment to rate parts of the solution, depending on complexity, should help to clarify the nature of the full solution required.
- *Understanding Biometrics* is not intended to stand as a detailed guide to requirements definition, but should help potential users comprehend the degree of effort required to specify the requirements.

8. Conclusion

Biometric systems can be complex in design, setup, delivery, implementation and daily use. Introducing a new biometric system that will be 'fit for purpose' can therefore be quite challenging.

The aim of the Biometrics Institute in writing *Understanding Biometrics* is to help put a clearer structure on the use of biometrics, in its own right and as part of larger business solutions such as for identity management; and to help those seeking to build such a solution to understand better what they need to do.

This Guide may also help organisations to form a basis for commercial negotiations and prepare a contract in preparation for appointing a suitable supplier.

9. Annex

Glossary & Acronyms

All numbered entries refer to ISO/IEC 2382-37:2017.

(1:1) One-to-one comparison: confirming that someone is who they claim to be, by comparing those characteristics on a one-to-one basis (verification). ISO/IEC 2382-37:2017: Process in which *biometric probe(s)* from one *biometric data subject* is compared to *biometric reference(s)* from one *biometric data subject* to produce a *comparison score.*

(1:N) One-to-many comparison: the process of searching a database of such characteristics to find the biometric reference identifiers attributable to one individual, in one-to-many searching (identification). ISO/IEC 2382-37:2017: Process in which *biometric probe(s)* of one *biometric data subject* is compared against the *biometric references* of more than one *biometric data subject* to return a set of *comparison scores.* DEPRECATED: one-to-few.

Aadhaar Means 'the foundation'—Indian biometric system for national identity holding face, fingerprints and iris.

AFIS Automatic Fingerprint Identification System. The generic name for any automated fingerprint system.

ABIS Automatic Biometric Identification System. The generic name for any automated system where one or more modality is used.

API Application Programming Interface—software that allows one programme/app to talk to another; as opposed to a user interface where a real live user is giving the directions or calling for something to be done.

Biometric data subject
(3.7.5) Individual whose individualised *biometric data* (3.3.6) is within the *biometric system* (3.2.3).

Biometric enrolment

(3.5.3) Act of creating and storing a *biometric enrolment data record* (3.3.10) in accordance with an enrolment policy.

Biometric identification

(3.8.2) Process of searching against a *biometric enrolment database* (3.3.9) to find and return the *biometric reference identifier(s)* (3.3.19) attributable to a single individual.

Biometric recognition/biometrics

(3.1.3) Automated recognition of individuals based on their biological and/or behavioral characteristics.

Biometric template/reference biometric feature set

(3.3.22) Set of stored *biometric features* (3.3.11) comparable directly to probe *biometric features* (3.3.11).

Biometric verification

(3.8.3) Process of confirming a *biometric claim* (3.6.4) through *biometric comparison* (3.5.7).

BPR Best Practice Recommendation (NIST).

CCTV Closed Circuit Television.

Contactless Enrolment of a biometric image/sample without physical contact with the sensor, for example, taking fingerprints when fingers are passed on front of a camera without stopping or touching the glass.

DNA Deoxyribonucleic acid—twin ribbons of organic molecules forming a double helix—used in the reproduction of all living organisms.

DNA Profile A biometric template derived from an organism's DNA which makes it possible to search for a match and verify whether two samples of DNA are from the same individual, or not. (Note: Under current standards, identical twins/triplets have identical DNA profiles, causing potential ambiguities. This problem is expected to be resolved in future DNA profile specification using additional types of DNA data, including epigenetic and 'copy number variations').

FAP Fingerprint Acquisition Profile (NIST).

FAR False acceptance occurs when the enquiry biometric template from one person is matched in error by the system to the biometric template of another person in the database. The FAR is the number of false acceptances as a proportion or percentage of the total number of biometric enquiries that should have been rejected. For example, the number of non-matches generated and presented as matches by the system as a proportion of genuine non-matches.

FNIR False-negative identification-error rate: Proportion of identification transactions by capture subjects enrolled in the system in which the subject's correct identifier is not among those returned (19795 Standard).

FPIR False-positive identification-error rate: Proportion of identification transactions by capture subjects not enrolled in the system, where an identifier is returned (19795 Standard).

FR Facial Recognition.

FRR False rejection occurs when the enquiry biometric template is not matched to the correct database template even though they are from the same person. The FRR is the number of false rejections as a proportion or percentage of the total number of biometric enquiries that should have been accepted. For example, the number of matches generated and presented as non-matches by the system as a proportion of genuine matches.

Fusion Managing the issues involved when bringing together multimodal biometrics in the same system, for example, relative weighting to be given to similarity scores achieved in different modalities.

GDPR General Data Protection Regulation (EU).

IEC International Electrotechnical Commission is an international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies (collectively known as "electrotechnology"). The IEC also manages three global conformity assessment systems that certify whether equipment, system or components conform to its International Standards.

ISO International Organization for Standardization develops and publishes standards across a wide range of industries including biometrics and forensic science. The ISO is a worldwide federation of national standards bodies, from 162 countries, who contribute to the production of standards through membership of the various subject-matter committees. Other countries may join as correspondent or subscriber members to receive information about standards.

ISO/IEC JTC1 Joint Technical Committee 1 established by ISO and IEC to develop information technology standards.

Latent, Latent Print (or Finger Mark)
An impression of the friction ridge surface of a finger deposited on a surface, for example, at a crime scene: it may be visible or may need special development techniques to make it visible and thus possible to detect. The friction ridge surface of the palms of the hand and the soles of the feet and toes can also be deposited in a similar manner. The friction ridge detail may be formed on or in a substrate in sweat or a contaminant (e.g. paint or blood), impressed into the surface (e.g. wax or putty) or by chemical action such as tarnishing on metallic objects.

N2N Nail-to-Nail—rolled fingerprint impression from the edge of the nail on one side to the other. This technique is used by law enforcement agencies to reveal the maximum amount of friction ridge detail for encoding, searching and comparison purposes.

NIST National Institute of Standards and Technology (US).

On the fly Biometric capture from a distance, possibly on the move, and without the subject necessarily being aware that the capture is taking place—for example, capture of multiple faces from a crowd by mobile camera, CCTV or VSS.

PIA Privacy Impact Assessment.

PAD Presentation Attack Detection. The presentation of an artefact or of human characteristics to a biometric capture subsystem in a fashion that could interfere with the intended policy of the biometric system is referred to as a presentation attack. The ISO/IEC 30107 series is concerned with mechanisms for the automated detection of presentation attacks. These mechanisms are called presentation attack detection (PAD) mechanisms.

Privacy audit An analysis by an independent third party of a project or entity's privacy environment, covering such issues as technical and procedural privacy protection, privacy awareness programmes, threats and risk, and incident reporting.

Privacy Impact Assessment
A pre-implementation assessment of the impact on privacy of a planned change in business activity (see ISO/IEC 29134).

Production environment
Live use of an IT-based system as opposed to a test or pilot site.

Pseudonymous identity
Giving assurance about someone's existence and identity via a trusted third party without disclosing the person's actual details. For example, in banking, confirming the person has funds for a proposed transaction, with a unique reference number for the transaction but without disclosing their actual name and identifying details.

RBAC Roll-Based Access Control.

Roll A rolled fingerprint impression is taken by rolling each finger in turn across the reader (or ink pad) to record the maximum surface area of the finger, even N2N, producing a characteristic rectangular shape of image.

SC37 Sub-committee 37 of JTC-1 which develops standards on the subject of biometrics**.**

Slap A slapped image is captured when multiple fingers are placed simultaneously on a fingerprint sensor, for example, four fingers or two thumbs. Software is used to separate the combined image to extract the prints for each finger. Produces characteristic oval-shaped images of each finger. Also used to quality assure the rolled fingerprint process (N2N & Roll q.v.), for example that the fingers have been rolled and recorded in the correct sequence.

SAP Subject Acquisition Profile (NIST).

VSS Video Surveillance System.

References—Standards and Guides

Some Key Standards

ISO standards relating to biometrics are at the following link:
https://www.iso.org/committee/313770/x/catalogue/

ISO/IEC 2382-37: Information technology — Vocabulary—Part 37: Biometrics, Dec 2012

ISO/IEC TR 24741: 2018 Information Technology – Biometrics – Overview and Application

BS ISO/IEC 29794: Information technology – Biometric data interchange formats (Part 5, Face image data; Part 2:2011: Finger minutiae data)

ISO/IEC 19795 Information technology – Biometric performance testing and reporting
(Part 6: Testing methodologies for operational evaluation)

ISO/IEC 30107 Series – Biometric Presentation Attack Detection

Proprietary standards exist for particular sectors or countries: for example: **ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290 Edition 3, dated August 22, 2016** (a standard for transferring biometrics between law enforcement and related criminal justice agencies). Further standards the FBI, US Military, US-Visit (DHS) and for vendor-neutral exchange of latents among disparate cross-jurisdictional AFIS systems.

Biometrics Institute Guiding Material
The Biometrics Institute has published several good practice guiding documents which are available free to members of the Institute. They include:

- Biometrics Privacy Guidelines, summarised in section 3 of this guide.
- Privacy Impact Assessment Checklist
- Top Ten Vulnerability Questions
- How to address Biometrics Vulnerabilities

See: www.biometricsinstitute.org.

Suggested Further Reading

Standards & Biometric Systems

International Organization for Standards http://www.iso.org

International Electrotechnical Commission http://www.iec.ch

European Committee for Standardisation https://www.cen.eu

National Institute of Standards and Technology (USA) http://www.nist.gov
PAS 92:2011 Code of Practice for the implementation of a biometric system – British Standards Institute www.bsigroup.com

Biometrics & Forensic Science

United Nations Office on Drugs and Crime (UNODC): 'Police: Forensic services and infrastructure' and 'Staff skill requirements and equipment recommendations for forensic science laboratories.' www.unodc.org

Forensic DNA Typing: Biology, Technology and Genetics of STR Markers – John M. Butler. Published by Elsevier Academic Press ISBN-13: 978-0-12-147952-7

ISO/IEC 17025:2017 The general requirements for the competence of testing and calibration laboratories

Biometric Systems – Vulnerabilities

ISO/IEC 30107-2_2017: Biometric presentation attack detection Series:
ISO/IEC 30107-1:2016
Information technology -- Biometric presentation attack detection -- Part 1: Framework
https://www.iso.org/standard/53227.html

ISO/IEC 30107-2:2017 Preview
Information technology -- Biometric presentation attack detection -- Part 2: Data formats
https://www.iso.org/standard/67380.html

ISO/IEC 30107-3:2017 Preview
Information technology -- Biometric presentation attack detection -- Part 3: Testing and reporting
https://www.iso.org/standard/67381.html

Frontex, Vulnerability Assessment and Testing for Automated Border Control (Abc) Systems (2017)

ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements

ISO 31000:2009 Risk management - Principles and guidelines

IEC 31010:2009 - Risk management -- Risk assessment techniques

NIST SP 800-30 Guide for Conducting Risk Assessments

NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach

Privacy

EU Agency for Fundamental Rights publication 'Under Watchful Eyes – Biometrics, EU-IT Systems & Fundamental Rights http://fra.europa.eu/en/publication/2018/biometrics-rights-protection

Biometrics Institute Supplier Directory
This resources offers you to search for potential partners for the implementation of biometrics.
See: www.biometricsinstitute.org.