

{ The ideal biometric system offers high security combined with excellent user convenience }

3. Selecting identification technology

Anton Kuip & Hans Braskamp

Introduction

In physical access control systems, reliable identification of people is crucial. This article describes the most common ways in which people can be recognised using ID cards and Biometric identification when more security is needed. ID cards are available in many types, ranging from simple printed bar code cards to microprocessor-based RF cards. Biometric technology has grown in maturity, and many systems based on fingerprint, face, hand or eye recognition are performing well in combination with physical access control. Selecting the right system is a process that includes the consideration of criteria like convenience, reliability, accuracy, installation, and costs. This paper provides an overview of currently available technologies and their typical properties, which will hopefully be of assistance during your own selection process. The article starts with an introduction to several types of identification. The final section is about the selection process.

History

The oldest form of identification is in fact biometrics: to be more precise, face recognition by the human eye and brain: in mediaval times the guard decided whether he would provide access to his castle. A more objective and automated way to control acces is the use of the mechanical key, which is operated by manpower, so no electricity or software is needed. However, copying keys is relatively easy and their use does not fit in a fully automated access control system. Therefore, other equipment is required, which will be discussed in this document.

Some biometric history: the first person recognised to work in biometrics was an anthropologist named Alphonse Bertillion in the 1890s, who developed a method of bodily measurement. The problem with identifying repeated offenders was that the criminals often gave different aliases each time they were arrested. Bertillion realised that even if names changed, even if a person cut his hair or put on weight, certain elements of the body remained fixed, such as the size of the skull or the length of their fingers. His system was used by police authorities throughout the world, until it was discovered that some people shared the same measurements, and based on these measurements alone, two people could be mistaken for one another. After this, the police used finger printing instead, which was developed by Richard Edward Henry of Scotland Yard. Today we refer to biometrics (using a biometric reader) as the automated technology to identify people by looking at their faces, fingerprints, eyes, etc. In 1974 the first hand geometry reader was introduced, followed later by readers for fingerprint, face, and iris (1995).

Identification of people

When a person needs to be registered initially in an automated access control system, how do you know that they are really the person they claim to be? You have to rely on the information from identity papers like a passport or birth certificate they are carrying, or to get information from another registration or other people. This process is sensitive to fraud and mistakes, but is the most important step in setting up a reliable access control system.

Once you know the person's identity, you can issue a badge. The badge reader at the entrance will read the badge and access can be granted: the right person entered at the right time at the right place. Are you sure? Was the badge not lost or stolen? Or maybe a duplicate was made by listening to the RF signals of the original badge, or somebody could have made a copy of the mag stripe on the badge. Do you need to issue a badge? Why not use a PIN code? Or what about biometrics, is that really so secure?

Let's have a look at the different ways in which people can be identified automatically.

The figure on the next page shows the various alternatives.



Figure 1: identification alternatives.

“What you have”

This is the most common way for the automated identification of people, and in most cases this will be sufficient. In order to ensure that only the rightful owner is carrying the badge, you could print a photo on it. Or you could add more functionality to the card such as a payment function or logging in to a PC. This will prevent people from lending their cards to other people. However you can never be sure that somebody else will use the card, including all the rights that go along with this card.

“What you know”

If you really want to know if the carrier of the card is the rightful owner, a PIN code can be used to check this. We all know this from our banking cards when using an ATM to withdraw cash. This method is more reliable and is often implemented in special situations where higher security is required. Nevertheless, PIN codes can also fall into the wrong hands.

“Who you are”

Another form of identification is looking at the unique human characteristics of a person. Stealing someone’s fingerprint or face is virtually impossible, and copying someone’s signature is not so easy. This so called “Biometric Identification” is a very reliable way of establishing or verifying a person’s identity.

Card Technologies

In the following section, the most common card technologies will

be explored with a discussion of their pros and cons. The section begins with the simple and older types, before moving on to the more complex and new ones.

Magnetic stripe

The mag stripe can be ‘written’ because the tiny bar magnets can be magnetised in either a north or south pole direction. The mag stripe is very similar to a piece of cassette tape.

The magnetic stripe technology is most commonly used for access and banking activities. The use of this technology requires the user to swipe the card through a reader for each transaction. This requires physical contact between the card and the reader. This interaction causes wear to both the reader and the card; thereby causing an increase in card and reader replacements along with the need to clean the reader on a regular basis. The magnetic stripe technology is very cost effective simply because of its volume of use. There are three tracks on the magstripe, each track being about one-tenth of an inch wide, the data is specified in the ISO/IEC standard 7811. For access control applications, generally track 2 is used, and only numerical data is possible.

Nowadays, it is only suited for non critical applications because it is relatively easy to copy this card. The card is not really convenient to use, the user has to swipe it the right way because the magnetic stripe is only on one side of the card.

Wiegand

Wiegand is the trade name for a technology used in card readers and sensors, particularly for access control applications. A Wiegand card looks like a credit card, and it works according to a principle similar to that used in magnetic stripe cards. However, instead of a band of ferromagnetic material, the Wiegand card contains a set of embedded wires. The wires are made of a special alloy with magnetic properties that are difficult to duplicate. This makes Wiegand cards virtually counterfeit-proof. The set of wires can contain data such as credit card numbers or access control data. The card is read by passing it through a Wiegand swipe reader. In fact the Wiegand card is the first contactless card: the embedded wires are not in contact with the reading head. Wiegand is often referred to as an interface definition for readers, like RFID readers. The data output of this definition is equal to the original Wiegand card readers, but is nowadays generated by the processor of the reader.

Barcode

Barcode is an optical way to present and read data. The most well known standard is the linear barcode, of which many versions exist for different applications. Some examples are code 39, Codabar, EAN, UPC, etc. A more modern variation is the Data Matrix, which is a very area efficient 2D (two dimensional) barcode symbology that uses a unique perimeter pattern which helps the barcode scanner determine the cell locations. The cells are made up of square modules. Because it can encode letters, numbers, text and actual bytes of data, it can encode just about anything including text characters, unicode characters and photos. It is commonly used to encode data from a few digits to several hundred digits. Barcode is used extensively in retail and library applications, and also in access control. For demanding security applications barcode is not recommended, as copying the card is rather simple. To make cloning more difficult IR barcodes are invented which are only readable with infrared light. For visitor management it can be very convenient, because the low price of the barcode card means that no facility is needed to get visitor cards back.

RFID, Contactless technology

General

Contactless technology or Radio Frequency Identification (RFID) was developed in the late 1970s. It includes a broad variety of techniques and applications. A microchip attached to an antenna is packaged in a way that enables it to be applied to an object or human being. The tag or credential picks up signals from it and sends signals to a reader. The tag contains a unique serial number, but may have other information, such as a customers’ badge number. Tags come in many forms; for access control, cards and key fobs are the most popular. The use of contactless technology is particularly attractive for **secure physical access control**, where the ID credential and reader must work in harsh operating conditions, or with a high degree of user-convenience. The card can be presented to the reader without it having to be removed from a wallet or even without doing anything special in the case of real handsfree identification. Other applications of RFID are tracking of goods, cattle stock monitoring and vehicle identification.

Types

Concerning chip types, there are three types of contactless credentials on the market. The memory card (1) is the simplest form,

which stores data in the memory of the chip and is mostly protected by passwords. For access control the wired logic (2) version is more interesting: a fixed method to authenticate it to readers is available and communication to the reader can be encrypted.

This type of credential is widely used in access control, and Mifare Classic and Legic are good examples. A more complicated (3) and sophisticated type has a real microprocessor with memory on board, and an operating system to run general or custom-made applications. This type of credential is often used in public payment or governmental applications. All described technologies are passive, which means that the energy for the electronics in the card is derived from the electromagnetic field of the reader.

Technologies

In the following paragraph four main technologies are reviewed: 125 kHz, ISO/IEC 14443, ISO/IEC 15693 and microwave.

Low frequency

Low frequency (LF) 125 or 120 kHz read-only technology is used frequently in today’s RFID access control systems and is based on de facto industry standards rather than international standards. This means that credentials and readers of different manufacturers will not necessarily work together. Most of these types of credentials hold a fixed serial number (HID, Deister, Nedap), some have read/write memory to store variable information and authentication functionality (Hitag, Nedap NeXS). These low frequency products have proven to be very reliable and have a comfortable reading range of up to 1 meter, depending on the credential and reader type. The data transmission at this carrier frequency is not easily influenced by moisture and dirt.

13.56 MHz

Today, a very popular technology is the ISO 14443A standard for proximity cards working on 13.56 MHz with an operating range of maximum 10 centimeters. Because this is ISO standard equipment, devices from different manufacturers are interchangeable as far as the communication between the credential and reader is concerned. One well known commercial product is Mifare, developed by Mikron in Austria which was bought by Philips Semiconductors, now NXP. Read/write capability to the card is possible to store a custom format of personal identification or biometric template. Most types on the market have a form of authentication of card and reader, using encryption of data at the radio link.

This is available in custom algorithm or standard DES and 3DES. Memory sizes are available from 64 bytes to several kilobytes. In access control practice, Mifare Classic 1k and 4 kbyte cards have already been the standard solution for a long time. However, in the beginning of 2008 the security of these chips became questionable. For new applications DESFire is recommended with a 3DES security level. From Legic, Advant cards are available which are equipped with 3DES encryption as well.

ISO 15693 is a 13.56 MHz standard for passive vicinity identification, and it is able to operate at ranges of up to 1 metre. It was developed for the tracking of goods in logistic systems as an electronic alternative for the usual barcode identification. No authentication or encryption is standardised, so for demanding access control applications this will not be the most obvious choice.

Microwave

For some access control applications a greater reading distance is required, for example truck access or parking applications. This can be realised with microwave technology, functioning at a standardised frequency of 2.45 GHz. Detection distances of up to 10 metres are possible, depending on the antenna and tag dimensions. A typical property of these systems is that the tag is read in a narrow beam from the reader, this makes it possible to operate with lanes which are close together without interference.

Contact smart cards

These cards contain a chip, which can vary from a simple memory chip to an advanced processor running a specific application program. A well known example of the latter is the Java Card, with an operating system (JCOP, Multos) and Java applications running on a virtual machine. Advantages of the Java technology include security and portability, which means that an application can be used on different hardware platforms. In general contact cards are not ideal for physical access control, the card has to be inserted in a slot, metal contacts then land on the metal areas on the card and provide bi-directional communication. This is a vulnerable construction, especially in outside applications. The contact card is frequently used in banking and credit card applications. To avoid the use of contacts the dual-interface is introduced.

Dual-interface smart cards

To overcome the contact problem, a new card type is introduced with an additional contactless interface. Usually this interface complies with ISO 14443A standard, like the Mifare technology. The functions are comparable to the contact smart cards, but for practical reasons, these cards are more suitable for access control.

NFC technology

In a selection of recent mobile phones, NFC (Near Field Communication) technology is built in. With this 13.56 MHz technology, bi-directional short distance communication between the phone and a suitable reader is possible, if the right software is available on both sides. A simpler way is to make the phone act as a Mifare card, which can be read by a standard Mifare reader. This is possible because Mifare and NFC technologies are closely related.

Mobile phone

If identification from a long distance is required, the mobile phone itself comes into play. A special GSM modem with a serial communication output (RS232) can be connected to an access control controller. The number of the caller is transferred to the access control system and used as the identifier. Depending on the application, this can be an attractive solution.

Card technology characteristics

Cards, and other shapes like keyfobs, have a number specific characteristics. The most important will be discussed briefly.

Data size

It must be determined how much data is required to make access control possible. But in a multi-application environment more data space will be necessary, so a more broad investigation will be needed. For access control, normally only a few (4-10) bytes are sufficient.

Security

The major threats here are cloning and replay, which can be opposed by appropriate encryption and/or authentication. An advantage of a hands-free system is the impossibility of 'snatching' cards: the card can stay invisible in a bag or clothes.

Convenience

To make acceptance easier, the convenience of an access control system is an important factor. Convenience applies to the handling of the card at the reader and the speed of the transaction. The magnetic stripe is the least convenient, as a swiping action is required with much chance of error: too fast, too slow, wrong side of card, etc. The most convenient option is a real hands-free system, with identification at a distance of 0.5 to 1 meter. An additional economical advantage is the high throughput, which can result in a lower number of (parallel) doors.

Standardisation

An important factor is standardisation, which provides a greater independence from suppliers. It is desirable to have a second source for products you select in your access control system, so that at least a functional replacement is available. A suitable example is the ISO 14443A standard: a lot of Mifare products are on the market which comply with this standard.

Durability

Many access control badges are heavily used, so it is clear that wear is a factor. The common proximity and hands-free systems require no physical contact between card and reader, so wear will be low. In outdoor situations especially, these solutions will be favoured, as making RFID antennas weatherproof is much easier than slit readers.

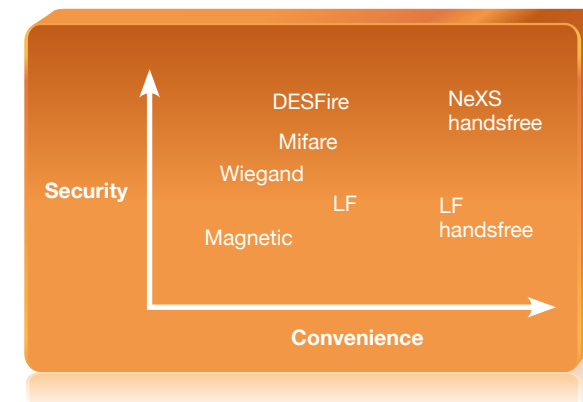


Figure 2: the positioning of several card technologies.

Biometric technologies

A general definition of biometrics is:

The automated recognition of individuals based on their behavioural or biological characteristics.

Biometric technologies are concerned with the physical parts of the human body like face or fingerprint, or the personal traits of human beings, like signature or voice pattern. It is important to note the term 'automatic' in the above definition. This essentially means that a biometric technology should recognise or verify a human characteristic quickly and automatically, in real time.

A wide variety of Biometric ID systems exists, but in all systems we can find the same basic elements. In the figure below, the schematics of a generic biometric system are represented.

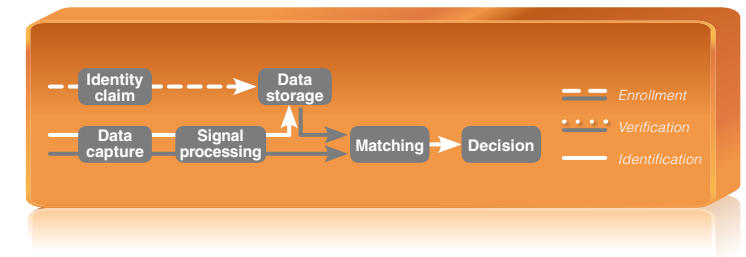


Figure 3: biometric system schematics.

- Identity claim: the person claims his/her identity by means of a card reader or keypad.
- Data capture: the data capture subsystem collects an image or signal of a person's biometric characteristics that is presented to the biometric sensor or camera, and outputs this image/signal as a biometric sample, e.g. a fingerprint image.
- Signal processing: the signal processing system extracts the distinguishing features from a biometric sample with such a quality that these features are likely to be distinguishing and repeatable. The signal processing subsystem creates a template from the extracted biometric features.
- Data storage: the processed biometric data, e.g. the enrolled templates are stored in the memory of a biometric reader, and/or in a central database. An alternative is to store the data on the ID card if privacy regulations require this. The size of a biometric template varies from 9 bytes for a hand geometry reader to 2k bytes for face recognition.

- Matching system: in the matching subsystem, the features are compared against one or more templates in the Data storage and comparison subsystem scores are passed to the decision subsystem. The scores indicate the degree of the fit between the features and references.
- Decision subsystem: the decision subsystem uses the comparison scores generated from one or more attempts to provide the decision outcome for a verification or identification transaction. The question is of course, how close the fit needs to be in order to conclude that the right person has been verified or identified, or how wide the fit needs to be to conclude that it is not the right person.
- Enrolment: this is the initial process in which a person's human characteristic is captured and processed into a biometric template and stored in a digital memory, together with the identity of the person.

The most popular biometric systems

Before we further explore the characteristics of biometric identification in general, we will review several biometric principles that are used in physical access control systems.

Face recognition

A video camera captures a digital image of a face. A proprietary algorithm or neural network within the biometric engine of the system will convert the facial image sample into a pattern and then a unique mathematical code. This is stored as a template (a biometric reference) for that individual. A typical characteristic of face recognition is the ease of use combined with a high recognition speed. All you need to do is to look into the camera for 2 seconds.

A 3D Face recognition system adds a third dimension to the facial image.

Three-dimensional maps of the face can be created through various means, such as the projection of an infrared grid ('structured light'), merging of multiple images, or using shading information in a single image.



A 3D image contains more unique facial characteristics, and this enables higher recognition accuracy. The drawback is that glasses and beards can have a negative effect on accuracy, leading to problems in recognising people with heavy beards or wearing big glasses.

In general, it can be said that face recognition is a user friendly and fast identification system. The accuracy is lower than fingerprint and eye (iris or retina) but this has improved significantly in the past few years, and will improve further in the near future.



Iris recognition

In most implementations, a greyscale image of the iris is acquired in the near-IR spectrum to maximise detail in dark-coloured eyes; some implementations capture irises in colour. Enrolment should be done in a well-lit environment. Non-patterned contact lenses

do not interfere with image capture. Sunglasses and glasses, however, should not be worn during enrolment as these can affect the capture process. Normally these glasses do not lead to problems during normal recognition at the door. Unique features of the iris are extracted from the captured sample by the biometric engine. These features are then converted into a unique mathematical code and stored as a biometric template for that person.

The impressive accuracy of these types of systems makes them very attractive for high security applications where only a limited number of (experienced) people are using the system.

In practice, the FAR (False Acceptance Rate) is zero meaning that one can be sure that only authorised people are allowed to enter. Recent developments, especially in iris identification are pushing this technology towards more user convenience. The latest iris ID product allows the user to present his/her face in front of a 3-camera unit at a distance of approx. 50 cm. Two cameras look for the exact position of the irises and the third camera takes a close picture of the iris, which is then processed further by the computer system.



Fingerprint recognition

The human fingerprint was accepted as a unique human identifier more than 100 years ago. It was logical that with the improvement of technology, automated reading of fingerprints should be possible. Today, there are many manufacturers offering fingerprint readers. In general the accuracy is good and for moderate numbers of people, it is even possible to identify people, so no additional card or PIN code is required. With regards to false rejects however, especially important in non-attended access control situations, many types of fingerprint readers still need improvement. In general, the recognition of very dry fingers causes problems. Moisture and dirt may also provide difficulties. New developments in contactless and/or multi spectral fingerprint capturing can solve the problems that occur when very dry or dirty fingers are presented. The relatively low price and high accuracy make fingerprint recognition a good choice in many access control applications.

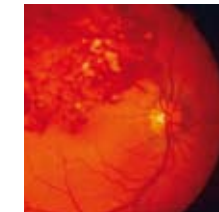


Hand geometry

Hand geometry takes a three-dimensional image of the hand and measures the shape and length of fingers and knuckles. It has been widely used since the early 1980s – predominantly for access control applications. Although hand geometry does not achieve the highest levels of accuracy, it is convenient to use and the primary advantage is that large volumes of subjects can be processed quickly. A person places a hand on the hand reader, aligning fingers with specially positioned guides. A mirror reflects light horizontally across the top of the hand, supplying a second two-dimensional shadow of the side of the hand. A camera positioned above the hand captures an image. The biometric engine extracts the 3-D measurements into a unique mathematical identifier and a template is created for that individual. Hand geometry is predominantly used for one-to-one verification and is very suitable in harsh environments since wet and or dirty hands hardly affect the performance of the hand reader.

Vein recognition

Biometric technologies that analyse vein patterns are considered to offer high authentication accuracy. The veins that exist in the hypodermic areas of the human body form a unique pattern for each person and can be captured using infra-red light. Any area of the skin where infra-red light is reflected produces a light image. On the other hand, a darker image is obtained for the vein pattern, as the reduced haemoglobin in the vein absorbs the infra-red light. The image-capturing system can therefore acquire the unique vein pattern made by the darker vein image. In actual products, the parts of body chosen (such as the palm, fingers, wrist and the back of the hands) are the parts where a user can easily present the blood vessel pattern to the sensor. The vein patterns are extracted, coded by the biometric engine and stored as a biometric template for that individual. Using image data processing techniques, we can get clear and constant vein patterns.



Retina vein recognition

This was the first product based on vein recognition and used in high security access control more than 20 years ago. The retina is the layer of blood vessels situated at the back of the eye and it forms a unique pattern. A precise enrolment procedure is necessary, which involves lining up the eye to achieve an optimum reading. The subject must look at a series of markers, viewed through the eyepiece, and line them up. When this is done, the eye is sufficiently focused for the scanner to capture the retina pattern. The retina is scanned and the unique pattern of the blood vessels is captured and converted into a template. The system requires accurate positioning of the eye, which may be difficult, and some users do not like the small (but harmless) light beam pointing into their eyes. The high accuracy and the fact that fraud is practically impossible makes this one of the most reliable biometric systems.



Hand vein recognition

The veins in the hand are easy to read by a camera system and can also be presented easily by the user. The first reader based on this principle came from Korea and it reads the veins on the top of the hand. When the hands are very cold the veins are narrower,

however the reader software offers sufficient compensation for this, and it does not generally lead to recognition problems. The camera in the unit points down and the hand must be placed under the camera. A newer version from Japan reads the veins in the palm of the hand. The inside of the hand can easily be presented and the vein picture is not obscured by hair growing on the hand. The camera points upwards and the palm of the hand must be presented on top at a distance of about 10 cm. The drawback is that dust can fall on the camera surface. A more vertical placement reduces this problem.



Finger vein recognition.

A relatively new product is the finger reader based on recognising the unique vein pattern in the finger. There are two ways of vein imaging: the reflection type and the transmission type. The reflection type directs the infra-red light onto the region to be photographed. The transmission type directs the infra-red light in such a way that the light passes through the part of the body that is being imaged. Using image data processing techniques, it is possible to get clear and constant vein patterns.

DNA

Analysis of human DNA, although now possible within ten minutes, is not yet sufficiently automated to rank DNA as a biometric technology. When technology advances so that DNA can be matched automatically in real time, DNA may emerge as a significant contender in the existing biometric industry

'Semi' biometrics

When biometrics is implemented in high security environments, extra measures have to be taken in order to ensure that only the right person is allowed access. There are several ways to make sure that only the person who is positively identified is standing at the door and is allowed to enter, and no other person is standing there as well.

Weight

By placing a weighing scale in front of the door; if the weight of a person is correct (allowing a small margin) then one can be sure that only one person is present.

Body measurement

Using several light beams and detecting if one or more of them are interrupted; this will give an indication that one or more people are present.

Video surveillance

Another way is to install a video camera at the door. An intelligent image processing algorithm can be used to determine if only one person is present.

If more people are detected, an alarm can be triggered. In unguarded situations, people can be physically separated using a lock or turnstile where one of the above mentioned pieces of equipment has been installed.

Biometric characteristics

A wide variety of biometric systems are available on the market today. The documentation of these products usually shows figures about security and reliability. It is good to know the meaning of these characteristics, as it will help you to make the right choice for a biometric system that fits best into your situation.

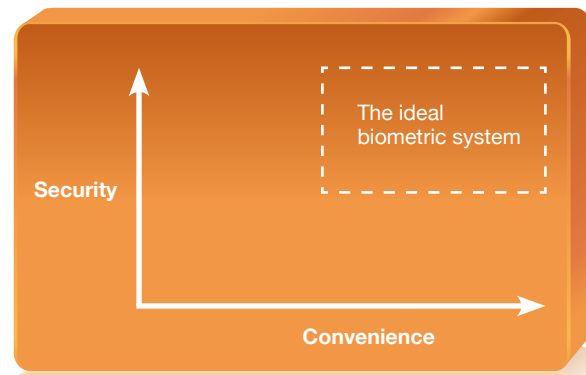


Figure 4: the ideal biometric system.

The ideal biometric system offers high security combined with excellent user comfort. Systems in practice unfortunately do not offer this perfect combination: there is always a trade-off between reliability and convenience. For access control they should both lie within the dotted frame on the above diagram, offering an acceptable combination of reliability and convenience.

Security

The level of security offered by biometric systems is not only related to accuracy: fraud and stability also play a role. The better you know the various benefits and shortcomings of a biometric system, the better prepared you are when it comes to the implementation of a biometric system.

Fraud

All systems are susceptible to fraud, but modern systems require significant knowledge and skills to compromise their security. If you're still interested here are some suggestions:

- Presenting a copy of a biometric characteristic, a fake fingerprint, iris, etc. You need a really good copy of the original and the relevance is different for the various biometric principles. A fingerprint can be left behind anywhere and can be stolen unnoticed. A good picture of an iris is much harder to get.
- The bloodier alternative: chopping a finger off or taking out one of the eyes is not successful anymore. The modern biometric readers demand 'live' fingers, faces, etc and on top of that, in almost all cases, the characteristics of a dead body part are different from the living version resulting in negative ID.
- Sniffing the data from the sensor and playback to the biometric system. Encryption of the data coming from the sensor can prevent this and can also help against changing biometric data on a card or in a database.

Stability

It is crucial that a biometric characteristic does not change over time; after a few months or years you should still be identified. Hands and fingers will change over time: a big change in weight may cause changes in the hand geometry leading to identification failures. Ageing can play a role in face recognition. In most cases this is not a problem and some systems can automatically store an updated template. A fingerprint or iris pattern remains consistent, but damages or illness may also cause changes here.

Accuracy

Failures: The system has to provide an authorised person's identity that rarely rejects authorised users (FRR, False Rejection Rate) and always detects fraudulent access attempts (FAR, False Acceptance Rate). Comparing the EER (Equal Error Rates where FRR = FAR) of the different systems can be instructive: it shows the relative strength of the various Biometric systems. However, there are more things that determine the quality of a system, and the real figures in practice can be quite different. First of all, it is very important to capture a good reference pattern preferably taken under different conditions. The system should also provide facilities to set individual acceptance levels to accommodate exceptional cases.

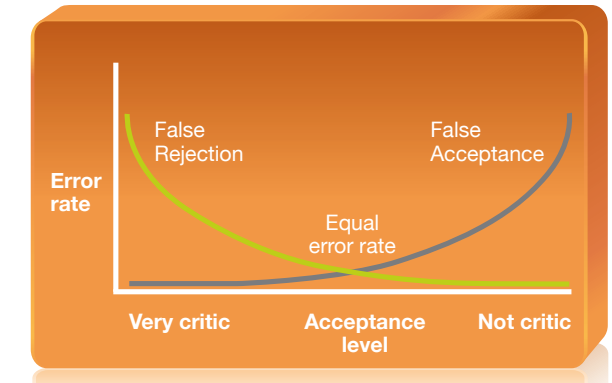


Figure 5: acceptance level versus Error rate.

Comfort

User convenience:

- Non invasive: the human body integrity is not to be discussed and systems should be absolutely non-invasive. Simple and quick body contact is acceptable, non contact systems seem to be less intrusive, but irritating lighting or an inconvenient set up can also have a negative influence on practical use.
- User friendly: the system should be easy to learn and simple to use in everyday practice.
- Speed: for convenient access control, the decision: access granted or denied, must be given within seconds; especially at locations where many people are involved or where people pass through many times a day.

Verification vs. identification

There are two different ways to recognise a person: verification and identification.

- Verification (am I who I claim I am?) involves confirming or denying a person's claimed identity, eg. the user presents an ID card and is then asked to present a finger or face to verify his/her identity.
- Identification: now the system has to recognise a person (who am I?) from a list of N users in the template database. Identification is a more challenging problem because it involves 1: N matching compared to 1:1 matching for verification.

Recently only eye identification, based on retina or iris identification offered enough accuracy to provide good identification results. Sufficient accuracy with other systems could only be achieved using verification, meaning that the user also has to present an ID card or enter a name or PIN code. Nowadays however, fingerprint systems and 3D face recognition also offer identification if N is not more than a few thousand.

Choosing the right biometric system

It is hard to make a good comparison between biometric systems, but the following figure places the systems in a chart of two hard-to-combine dimensions: reliability on the one hand, and convenience on the other. The ideal system does not exist but all biometrics show a tendency to creep slowly towards the ideal biometric equation. Depending on the application, sometimes reliability will prevail and sometimes convenience. Fingerprint and hand recognition are good alternatives when price is also an important issue.

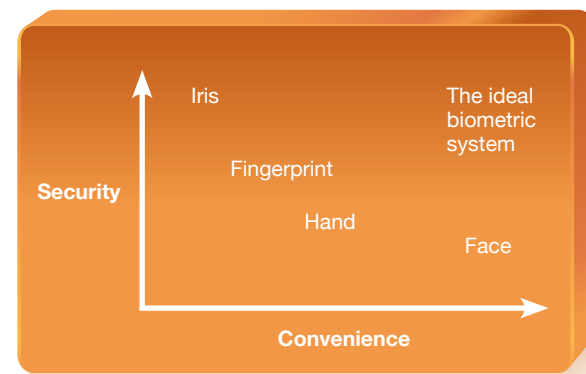


Figure 6: the positioning of several biometric systems.

General selection criteria

So far, we have introduced several forms of card technology and introduced the foundations of biometric identification. To decide which means of identification is appropriate in your organisation is not always an easy task. Vendors will focus on characteristics and criteria that are favourable to their own solutions or systems. Before starting to communicate with potential suppliers, it is very important to **clearly establish a prioritised list of criteria** for your specific organisation that you can use to assess the value of the product or system. A few possible criteria might be:

Security

The required level of security of the identification technology will depend on the value or importance of the protected object. A decision must be made which card type is suitable, and whether additional biometric verification is necessary. It is desirable to choose a proportional solution, so the security level of the physical aspects (locks, doors, windows) is also of concern. The card and/or biometrics should not be the weakest link, neither being significantly stronger than other elements of the system and therefore probably more expensive and complex.

Convenience

Ease of use is not only a benefit for acceptance but also increases the speed of the access transaction. All RFID cards operate by presenting the card to the reader, no inserting action is necessary. This will enable a high throughput of people, although the delay of the physical equipment (door, sliding door, revolving door, lock) sometimes remain a slow factor.

Legacy

The need to support existing, and possibly older card and reader technology in the security environment can be an important factor to consider in the card selection process. A way to deal with this situation is to select a combination card, with both the legacy and the preferred technology. Not all readers in existing buildings have to be replaced immediately this way. If this is combined with dual technology readers, a flexible and comfortable transition process can be realised.

Environmental

It is important to plan where the reader equipment will be installed. Slit readers and contact chip readers may cause problems for

outside use if no special protection measures are taken. Some biometrics (iris, face) are sensitive to environmental light, so in outdoor situations, care must be taken for this aspect.

Servicing

Maintenance is required during the full life cycle, so a good system supplier(s) is necessary. The availability of a good local representative and service organisation may influence the selection of identification type.

To be as future-proof as possible, a second alternative supplier is advisable but not always available. A functional replacement, although generating some rework, is then a possible alternative.

Financial

Although not a technical aspect, the financial part, the cost of ownership, is still a selection criterium. It is important to consider the total life cycle of the system, not just the initial procurement and installation costs. Maintenance and use can be serious parts of the total cost of ownership.

Manageability

Identification technology is seldom implemented independently from other systems. Most of the time the identification system will be part of an access control solution. Modern access control systems are capable of using multiple forms of identification in one security environment. Depending on the security needs and other criteria, a selection of one or more identification methods is applied to the entrance. The enrollment of biometric data or the registration of card specific information in the access control system should preferably be possible in a transparent and fully integrated way from within the user interface of the access control or security management system. When selecting identification technology, make sure that the system is well-documented and that it provides integration with the access control system of your choice, for example through a software interface.

Multi purpose

Are you selecting identification technology just for security purposes, or are you thinking of applying the technology elsewhere? Are you considering cashless vending? Would you like to combine logical and physical access control? We recommend that you ascertain whether the technology is fit for all required purposes.

Availability

A commercial strategy for some suppliers might be to limit the availability of the identification technology. Are you sure you can afford to depend on one supplier for the years to come? You may wish to make sure that your organisation has the freedom to choose technology and suppliers as much as possible.

Many more selection criteria can be considered. Although identification technology is only one part of the solution, it is a very critical part. It is the element of the security equation that users of your security systems are confronted with most. Finding the right balance between security and convenience related to identification technology is likely to be vital for the success of any security implementation.