Biometrics Guide for Access Control Applications

Version 1.0

Aug 2008

Table of Contents

Foreword

The Centre for the Protection of National Infrastructure (CPNI) is the recognised government authority for protective security advice across the national infrastructure. This guide has been produced by CESG on behalf of CPNI.

The guide is produced to meet an identified requirement to assist security managers when considering biometrics as part of the solution to physical access control. It is designed to stimulate thinking regarding the application and suitability of biometrics and provides an overview of the biometrics market.

SECTION 1 What are biometrics and why might they be useful?

This guide discuses biometric technologies and their application in access control systems. The term *biometric technologies* refers to automated systems for recognizing people based on bodily characteristics, both biological and behavioural. Examples include automatically recognizing people from fingerprint, face, voice or iris characteristics. The term *access control*, refers to systems intended to restrict entrance to physical spaces (such as rooms and buildings) or virtual spaces (such as computers and databases) to people with proper, prior authorizations. A successful access control system will ensure that access to physical or virtual spaces is granted only to people with the appropriate access rights. Biometric technologies can help to achieve this as a part of a system but many other aspects also need to be considered such as the other technology elements used, the security policy for the system, any network to which the system connects, and the vetting of system administrators etc. Since at least the 1970s both government and commercial organizations have implemented biometrics in access control applications. Some of these implementations have been successful, some less so. The purpose of this guide is to provide a brief overview of many of the available technologies, and to outline some of the benefits and implementation complexities encountered in practice.

Because biometric technologies recognise people from bodily characteristics, rather than from PINs, passwords or tokens, they are particularly useful for establishing a firm connection between a person and the record of their rights of access. Biometric characteristics are much harder to accidentally or deliberately transfer between persons than passwords or tokens. Biometric records can also leave a much stronger audit trail for access events, with less room for repudiation. Consequently, biometric technologies are most often thought of as appropriate primarily for access control to highly secure spaces or highly sensitive data. This paper however gives examples of the broader use of biometric technologies, extending to low security applications as well.

The term ‘identity management’ has recently come fashionable in reference to the collection and maintenance of information records about people for a broad array of purposes, access control being just one example[1]. In this broader context of identity management, biometric technologies can be used in two ways: (i) to limit connection of an information record to a single person and; (ii) to limit a single person to a single information record. In access control systems, the information record of each person contains his or her access authorizations. The biometric elements in an access control system are intended to limit an access authorization to a single person – the person to whom it was originally issued. But some access control systems may require use of biometrics in the second way, to prevent each person from being issued more than one authorization record. Passport systems, for instance, would want to limit use of a passport to the person to whom it was issued and to limit each person to issuance of a single passport.

[1] It is common to refer to information records about people as “identity records”

1.1 Biometric Enrolment

To be recognized, a person must first become known to the system through the process of enrolment. At a minimum, the enrolment process must collect biometric information, such as fingerprints, iris or face images. A person from whom data is collected will be referred to as a 'biometric data subject' and the stored data as a 'biometric reference'. It is important that the enrolled biometric references be unequivocally from the person to whom they are said to refer. This implies that the collection of biometrics during the enrolment process should be well supervised by trusted personnel, particularly for high security applications.

It is usual, although not always necessary[2], to collect additional information during enrolment, such as the data subject's name. Any such additional information required by policy as a condition for enrolment can only be verified through outside, trusted credentials, such as a birth certificate, passport or personnel security document. The use of biometrics within an access control system does not alleviate vetting requirements at the time access authorizations are conferred. The addition of biometric technologies to existing access control systems, with the requirement for "in person" enrolment, has been used as an opportunity to re-verify the credentials of existing system users. If the enrolment process is not done with due diligence, a person presenting false credentials can be granted a perfectly valid biometric enrolment or a valid access authorization can be transferred to an ineligible person.

During an enrolment process, the biometric characteristics collected during enrolment can be searched against all the biometric references in the existing database to check for previous enrolment and to enforce a one-person, one-enrolment policy.

The complexity of a carefully supervised enrolment process, and the resources that must be allocated to this should not be underestimated.

1.2 System Integration

The market for biometric solutions includes vendors of the hardware readers (e.g. cameras or fingerprint sensors); software for matching of biometric features; middleware suppliers who allow different biometric approaches to be integrated; and systems integrators (SIs) who draw together elements from a number of such vendors to offer a solution which meets the requirements of the organization planning to introduce a biometric-enabled access control system. System integrators who do not have experience in the design and operation of biometric system in an access control application may fail to appreciate the significance of the issues which are listed in this guide. For example, the interpretation of the performance of a 'biometric system' may differ for all of these parties, and the SI needs to operate to the requirements of the organization for which the system is being developed.

[2] An example of a system that does not collect names or personal information is that used by the Disney Corporation, explained in section 8.2.

A ‘lesson learned’ in biometric applications is the complexity of the systems integration process: making the biometric technologies fit into pre-existing information technology and business processes.

Biometric Basics

- Biometric technologies can automatically recognize people already known to the system.
- Biometric technologies never ‘stand alone’, but rather serve as one component in a larger system, such as for access control.
- The process of becoming ‘known to the system’ is called enrolment.
- Any personal information about enrolling persons (i.e., name, nationality, access authorizations) must be established through trusted, outside documentation, such as a passport or personnel security document.
- The complexity of the enrolment process, and the time required for trustworthy enrolment of each biometric data subject, must not be underestimated.
- Biometric systems can operate without any personal information about those enrolled. Consequently, biometric systems can be used for anonymous recognition.
- Biometric systems can determine that data subjects are not already known to the system, thus supporting a ‘one-person, one-enrolment record’ policy and preventing a second enrolment under a different identity.
- System integration is a hard task and having an appropriate supplier who understands your business needs is key to the success of the project.

SECTION 2 Types of Biometric Systems

Commercially-available biometric technologies are based on many different types of biometric measures: fingerprints, hand shape, iris pattern, voice characteristics, face images and hand or finger vein placement. Access control systems are available based on each of these types of biometric characteristics.

2.1 Fingerprints

Fingerprinting is perhaps the best known biometric technique. Historically, fingerprint records were collected by inking the finger and rolling it onto paper, but modern systems use cameras or silicon sensors instead. In access control applications, users place their fingers (usually a thumb or index finger) onto a glass platen of a fingerprint scanner. A light shining from underneath the platen reflects only where there is a fingerprint valley, but not where there is a ridge. This reflected fingerprint pattern is imaged with a camera-like device inside the scanner. The fingerprint ridges of interest are those between the first joint of the finger and the fingertip. The fingertip itself is not imaged. Figure 1 shows a fingerprint scanner.

Figure 1: Fingerprint Scanner (used with permission of Ingersoll Rand Security Technologies)

Usually at least two fingers from each user are enrolled, so that if one fingerprint is damaged, the other can be used. Fingerprinting systems for access control sometimes require the availability of moisturizers or drying agents to improve the quality of collected fingerprint images. Slap sensors, which image the four fingers placed on the platen at the same time with a ‘slapping’ motion of the hand, are just now also becoming common. Provided that international standards are used in the collection, formatting and transmission processes, fingerprint images taken with such devices can be referenced against existing law enforcement databases – a feature that can be either desirable or undesirable, depending upon the application. Accuracy rates for various commercial technologies against databases of fingerprints collected under a variety of conditions are published by the U.S. National Institute of Standards and Technology [1] and regularly updated.

2.2 Hand shape

Hand geometry systems, those measuring the shape of a user’s hand, have been the most ubiquitous biometric devices for access control over the last 20 years, performing well in a variety of environments. The technology is currently

available from only a single vendor and international biometric standards reference patented techniques. Users place their open palm down on a reflective surface, aligning pegs between the fingers. A light shines down on the hand from above, reflecting off of the exposed parts of the surface, creating a silhouette image of the hand which is captured by a camera. It is important to note that the fingerprint ridge patterns are not imaged. Figure 2 shows a hand geometry device. Figure 3 shows the silhouette of a hand captured by a hand geometry device.

Figure 2: Hand geometry device (used with permission of Ingersoll Rand Security Technologies)

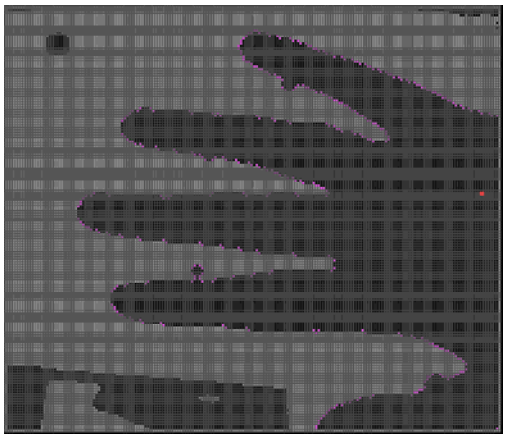

Figure 3: Hand silhouette as captured by hand geometry device (Courtesy of J.L.Wayman)

Accuracy rates for this technology with human volunteers in an access control environment were published in 2000 by the National Physical Laboratory[2].

2.3 Iris pattern

The coloured, iris area of the eye has long been recognized as distinctive. Iris recognition devices take high resolution, greyscale photographs of this pattern as the user looks into the camera with either one or both eyes. Illumination of the iris is from invisible and harmless infrared lights. Figure 4 shows an iris imaging device.

Image processing software isolates the iris within the eye image and converts the iris portion of the image to a binary code. Figure 5 shows a greyscale image of an iris segmented from the larger image of the eye. The resulting code is shown graphically in the upper left-hand portion of the image. Although iris images can be obscured by cosmetic designer contact lenses, standard contact lenses cause no issues.

Figure 4: (From LG iris, permission pending)

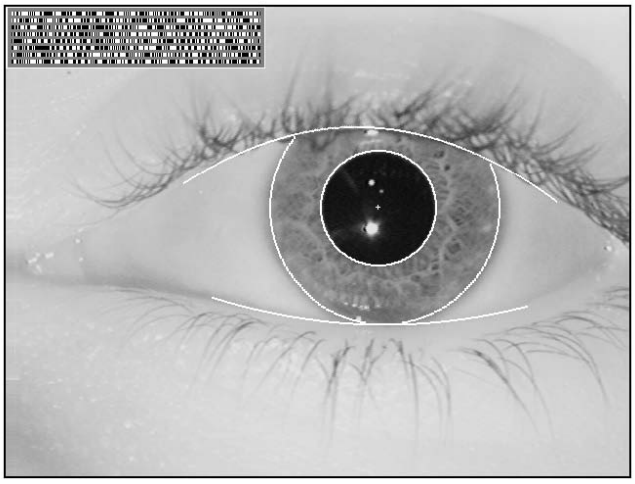

Figure 5: An iris segmented from the larger eye image with the resulting code in upper left. (Courtesy of Prof. John Daugman)

Iris recognition systems are available from a variety of vendors. A 2000 study by the National Physical Laboratory of biometric technologies for access control showed iris recognition to be the best performer among the technologies then available. Error rates published recently by the US National Institute of Standards and Technology do not relate to access control environments [3].

2.4 Voice characteristics

Use of voice characteristics for speaker recognition has a research history dating to the 1940s and remains a very active research topic. Speaker recognition has the attractive feature that telephones can be used as the input device. In access control applications, speakers choose a pass-phrase by which they will be recognized. To be recognized, the correct speaker must speak the correct pass phrase. Home incarceration programs have also used speaker recognition, asking callers to speak a randomly chosen ‘combination lock’ number (e.g. “25-56-32”) to prevent spoofing by recordings. Academic groups in a number of countries have been developing text independent speaker recognition algorithms for recognizing known persons speaking conversationally over the telephone. An annual competition in text-independent speaker recognition technologies is held by the US National Institute of Standards and Technology, but results are not published. There are no regular independent evaluations for use of speaker recognition in access control applications and no international standards yet exist.

2.5 Face images

Face recognition using standard digital or video cameras has become technically feasible over the last few years. Consistency of pose angle, illumination and facial expression are important for recognition, so cameras must be placed at head height, users must look directly into the camera with a consistent facial expression, and lighting must be controlled. Imaging conditions required for both reference images and at access control points are outlined in ISO 19795-5 [3]. One illustration from that standard showing the conditions required for optimal performance is shown as Figure 6. Successful use of facial recognition in surveillance applications has been limited by these requirements, but use of this technology for indoor access control has recently been shown to be quite feasible. Accuracy rates of multiple commercial technologies are regularly measured against recorded face images in periodic tests published by the U.S. National Institute of Standards and Technology [4]. These test results, however, do not translate into error rates for facial recognition biometrics in access control environments.

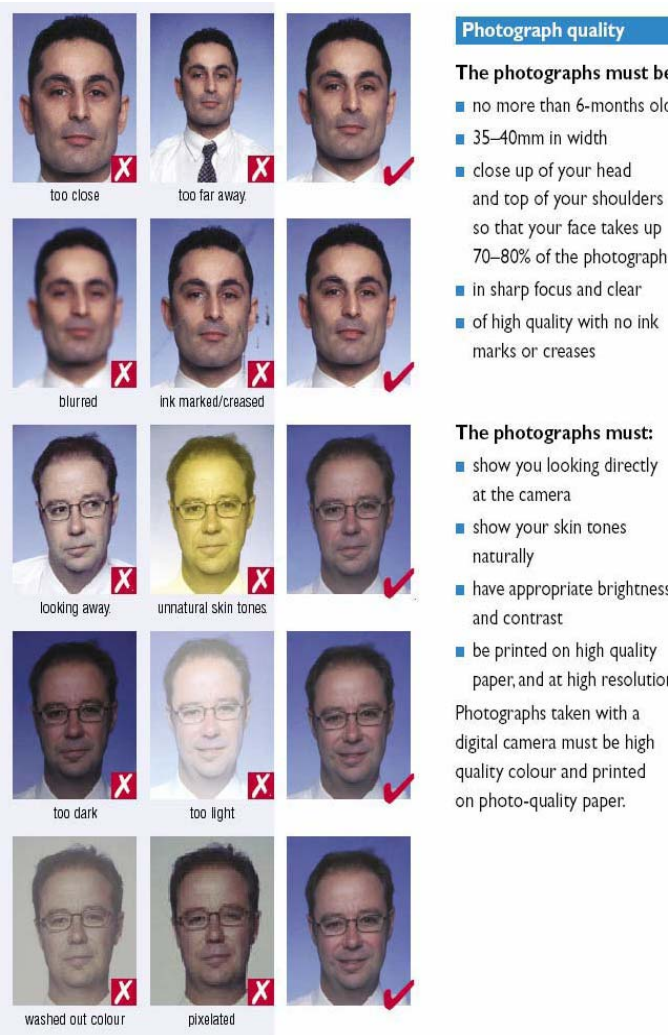

Figure 6. Optimal Imaging Conditions from ISO 19794-5 (Permission from BSI depending upon distribution)

2.6 Finger and hand veins

One of the newest biometric technologies to be marketed involves the imaging of veins in the hands or the fingers. These devices take advantage of the fact that veins absorb more near-infrared light than other types of tissue beneath the skin. The hand or finger can be illuminated with low intensity infrared light which, although invisible to the human eye, can be imaged with common CCD sensors. The light absorbing veins return a dark pattern against the more translucent skin and other tissue. The resulting patterns can be processed to determine similarity to stored references. Figure 7 shows a hand being imaged by a hand vein device.

Figure 7: Hand Vein Device (courtesy of Fujitsu)

2.7 Other Technologies

There are a number of lesser known biometric technologies that are commercially available, such as those based on dynamic signature analysis, computer keyboard keystroke patterns, and the electrical activity of the heart. There have been a number of unpublished tests on each of these technologies.

2.8 What About Retina Scanning?

In the 1980s and early 90s, before the commercialization of iris recognition, retinal scanning was a well-known biometric method. The retina is the light sensitive surface at the back of the eyeball containing blood vessels and nerves. Retina recognition was used in one of the first applications of biometrics by the U.S. Department of Defence for access control to highly secured spaces. Users looked closely into a lens system, while a rotating mirror directed a thin beam of infrared light onto the retina in a circular pattern. The intensity of the reflected light formed a one-dimensional pattern as it varied over the circle. Retina scanning did not produce an image of the retina and, contrary to persistent rumours, did not use laser light. There are now companies within the UK working with the technology to again develop a commercial market.

SECTION 3 Use of databases

Most biometric systems for multi-portal access control are networked in order to maintain a centralized record of transactions. Storage of the enrolment biometric data, however, can be centralized or decentralized, depending upon the system. There are strong differences between these approaches that must be considered.

3.1 Decentralized storage of biometric data

Some verification systems store data only on cards or tokens held by the data subjects of the system. This approach has the advantage of allowing each person control over her/his own data and eliminates the need for the creation and maintenance of an accessible, but secure, centralized infrastructure. The disadvantages are that losing an access control token or identity document will require the entire enrolment process to be repeated, this could lead to poor user perception. In addition, without a centralized database, there can be no checking for multiple enrolments in the system. The cards and tokens themselves, and the reference biometric data on them, may need protection against counterfeiting and forgery, for example using a cryptographic digital signature.

3.2 Centralized Storage of biometric data

Some verification systems and all identification systems store all data in a centralized database. In verification systems, this has the advantage of allowing re-issuance of lost documents by checking that the stored biometric data refers to the person applying for re-issuance. Centralized databases are required in identification systems and allow for a duplicate check, ensuring that each person in the database is enrolled only once. Such databases, however, have all the maintenance and security requirements of any database holding personal information/ appropriate information assurance must be gained and the system may well require the encryption of biometric data during storage and transmission.

3.3 Information Assurance

In either case protection of the biometric data both in the database and in transit is essential. Failure to do this may allow an attacker to defeat the system and also breach the confidentiality of the subjects' biometrics which would raise security and data protection issues.

SECTION 4 Modes of operation

The literature of biometric recognition talks about two modes of operation: verification and identification. Although developing precise definitions for these terms is difficult, the first (verification) refers to operations that require the subject to make an identity claim (often through the use of second factor such as a login, pin, password or token). The second mode (identification) applies to applications where the data subject does not supply an identifier to a stored reference. In applications of the first type, the system retrieves the biometric reference stored against this identifier and compares it to the current biometric characteristic supplied by the data subject to determine if they are adequately similar. In applications of the second type, the computer must make comparisons against all stored references that might be from the data subject to determine if any of them are approximately the same and, if so, return the located identifier.

Either approach, verification or identification, can be used for access control. In access control verification systems the user supplies a distinctive identifier, such as an ID number, smart card, RFID tag or pin prior to presenting the biometric characteristic. In access control identification systems (historically called ‘PINless verification’ systems) the user presents only the biometric characteristic; no keypad or card reading hardware is required. Access is allowed if the presented characteristic matches any reference characteristic enrolled in the system.

Ideally, the stored and currently presented biometric features would be identical. However, the nature of the interaction between the user and the technology means that an exact match is very unlikely, due to different presentation of the biometric characteristics to the sensor, ageing, changes in lighting, and other external environmental variations which can be difficult to control. This probabilistic nature is an area that marks biometrics out from other technologies and leads to the potential for matching errors, a subject that is discussed in the next section.

SECTION 5 Vulnerabilities and errors within biometric systems

All security systems can experience errors and biometric systems are no exception. The usage errors for biometric systems have been well studied in a variety of environments.

5.1 Types of errors

The three primary types of errors are:

- **False positive** a subject is falsely recognised as another subject.
- **False negative** a subject is not recognised as themselves.
- **Failure to enrol** the system is not being able to collect usable biometric images on an individual from the outset

5.2 Causes of errors

5.2.1 Matching errors

Most errors on biometric systems happen to normal users who are not acting maliciously, and are as a result of the probabilistic nature of a biometric system, design or environmental factors. Laboratory and *in situ* testing can establish rates for such errors with tested populations in tested environments. These rates, however, vary greatly from application to application, depending upon the data subjects, the enrolment conditions and the usage environment. The measured rates from this type of performance testing do not normally consider planned attacks on the system, but rather measure the probability of the system malfunctioning with subjects acting normally. The rates establish only the potential for an error, they do not alone allow us to predict how many such errors will be encountered.

5.2.2 Forced Errors

Another cause of error to be considered is that of a subject maliciously forcing an error through some form of vulnerability. There are ways subjects could force any of the errors above, for example:

- Forcing a false positive so that the subject is recognised as another subject (commonly termed impersonation), this can be though using a spoof artefact or in the case of a behavioural biometric, mimicking the other subjects biometric.
- Forcing a false negative so that a subject is not recognised as themselves (commonly termed disguise), this can be through lowering the quality of a biometric, presenting it in a non uniform manor, as well as using a spoof artefact.
- Forcing a failure to enrol so that a subject cannot be imaged. This can be through hiding the biometric, damaging the biometric or presenting in such a way as the image is so low quality it cannot be used.

5.2.3 Artefacts

Biometric characteristics are deemed to be stronger than traditional indirect mechanisms for recognition because they are linked intrinsically to the holder’s

body. If a fraudster can obtain, reproduce and enter into the biometric system an artefact of a biometric characteristic, such as a 'gummy' finger made of plastic or rubber, or photograph, this linkage can be broken. Research has shown that most biometric technologies will accept artefacts created by knowledgeable individuals if enough time is available at an unsupervised biometric sensor. Consideration should be given to whether the sensor would accept an artefact or whether the countermeasures in place would prevent and or detect this.

5.2.4 Damage

Biometrics, under the assumption that a fraudster cannot intentionally change or conceal their behavioural and biological characteristics, can be a reasonable solution. Unfortunately, biometric characteristics, such as fingerprints, can be intentionally covered or damaged, potentially allowing someone to obtain multiple enrolments in a single system. Some systems maintain a policy of denying enrolment to those whose body parts, such as fingerprints, appear intentionally damaged. Differentiating intentional from unintentional damage, however, is necessarily challenging, leading to the possibility that such a policy could have discriminatory impact on individuals with challenging characteristics because of age, disease or occupation. Another solution is to require that all enrolees verify their enrolment biometric characteristics in a subsequent visit, under the assumption that intentional damage will not be reproducible. Again, this might have a negative impact on those data subjects with naturally difficult characteristics.

5.2.5 Electronic Attack

All the errors discussed above can also be induced by electronic attack on the back end system. Biometric systems are commonly based on Commercial Off The Shelf (COTS) IT technology that can be vulnerable to a variety of different attacks. Suitable assurance must be sought of the security of the IT part of the system.

5.3 Impact of errors

The two types of systems, verification and identification, are impacted differently by these errors. A 1% false positive rate may be very acceptable for a verification system, but could be catastrophic for a large identification system with thousands of users. Understanding why different systems translate error rates differently into real errors is crucial to understanding biometric technology.

A lesson learnt is that all biometric systems must have quick, convenient, yet secure methods for adjudicating these errors and offering a fallback solution, which may need to be automated as well, if the access control system is designed to operate in an unattended mode.

5.3.1 Impact of errors on verification operations

Verification operations require the subject to make an identity claim (often through a the use of second factor such as a login, pin, password or token). False negatives result in a subject not matching the claimed identity and being denied the access granted to that identity. A false positive results in a subject

being allowed use the access right assigned to someone else. In an access control situation the motive of an attacker is to gain access to a protected space through claiming the identity of someone else and forcing a false match against their biometrics. Only legitimate subjects can be falsely rejected and only fraudulent subjects can be falsely accepted. The actual number of false rejections will be the product of the false negative rate and the number of legitimate subjects; the actual number of false acceptances will be the product of the false positive rate and the number of fraudulent subjects. Most users in verification systems will be legitimate; very few will be fraudsters. Consequently, there will be experiences of false rejections, even when the false negative rates are very low. These errors will be brought to the immediate attention of system administrators by the disgruntled legitimate users. A 1% false negative rate will imply that about 1 in every 100 transactions will result in an actual false rejection. This means that the fall back mechanism must be secure; or it will be open to exploitation by subjects fraudulently claiming to have been falsely rejected.

In verification systems, the false positive rate may not translate into any actual false positives (false acceptances). A 1% false positive rate will imply that about 99 out of every 100 different subjects attempting to use someone else's identity will be stopped, with one gaining access. Good system monitoring should alert system operators to un resolved non-matches, and subjects attempting to gain unauthorised access in this way. Attacks like this (termed zero-effort as the attacker is not exploiting a vulnerability) are high risk for the attacker and usually detected and so rarely tried in this type of system. It is important to note though that the figures quoted for the false positive rate normally only apply to a subject using the system as it should be used, and not a subject maliciously forcing an error through some form of vulnerability.

5.3.2 Impact of errors on in identification operations

In an identification system each submitted biometric sample is compared to every characteristic enrolled in the system. There are two common uses for identification operations within biometric system, one is to ensure the subject **is** enrolled on the system (positive identification) and one is to ensure the subject **isn't** enrolled on the system (negative identification). Positive identification may be used to make sure someone is allowed access, and negative identification may be used to stop duplicate enrolment.

Because every characteristic is searched in an identification operation, in systems with large numbers of enrolled characteristics, even very small false positive rates can result in actual false positives. For example, if biometric samples of 10 different individuals are searched exhaustively against a database of 1,000 records – resulting in 10 thousand comparisons – a false positive error will be expected even with a one-in-ten-thousand false positive rate. (Face recognition systems can operate at around this false positive error rate). For this reason, systems of this type must be carefully designed, basing the number, type and quality requirements for biometric characteristics on the anticipated ultimate size of the searched database. For the purpose of adjudicating errors, these systems generally store the complete biometric image and extensive biographical data of those in the database.

For access control systems using identification in lieu of requiring a PIN or a token, false negative error rates translate to false negative errors in the same way as in verification systems. For identification systems used to prevent multiple credential issuances to a single person, false negative error rates indicate the success potential for a person applying for a second credential.

Impact of Errors by Operation

Type of Operation		False Positive Rate	False Negative Rate	Failure to Enrol Rate
Verification		Potential for a fraudulent use of an identity NOT considering vulnerabilities	≈ percentage of falsely rejected subjects	Percentage of subjects routinely required to use a fall back system
Identification	Positive Identification (eg Access Control)	≈ percentage of the database wrongly matched to every search	≈ percentage of falsely rejected subjects	Percentage of subjects routinely required to use fall back system
	Negative Identification (Multiple Enrolment check)		Potential for issuing a allowing a second enrollment	Percentage of enrolees for whom other techniques to detect existing enrolment will be required

SECTION 6 Assessing the requirements for a biometrically enabled system

There is little doubt that the futuristic nature of biometric kit can be enticing, but all new technologies carry implementation challenges. Although highly successful applications have been documented above, not all applications of biometric technology have been completely positive. Several attempts in the 1990s to use biometric technologies within the UK Prison System proved to be of little value because the systems did not integrate with existing security processes. In 2005, an employee access control system employing fingerprinting was declared “dead on arrival” on the first day of implementation at a major US airport because of the failure of system designers to supply adequate fall back mechanisms for users encountering recognition problems.

The purpose of this section is to help potential implementers think through the justification for using biometrics, as opposed to more traditional (and often cheaper) forms of access control technologies, such as PINs, passwords, RFID, bar codes and mag-stripe cards. A more comprehensive document, “Biometrics for Identification and Authentication – Advice on Product Selection” has been published by CESG and is available on-line http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricsAdvice.pdf

The major areas of concern regarding the use of biometrics in access control are:

1. Establishing the business case in terms of money, time and convenience. Is the use of biometrics justified at all?
2. Complying with existing policies and legal requirements pertaining to both security and privacy.
3. Building support among both the data subjects and the system administrative personnel through an open dialogue.
4. Creating new policies for enrolment and use of the new technologies, including accommodation for users with biometric characteristics difficult to capture, such as those with damaged fingerprints, or those of unusual heights (e.g. using wheelchairs).
5. Phasing in a solution that can address unexpected problems as encountered, including the transition from legacy systems.
6. Establishing policies for recognizing and dealing gracefully with false negatives.
7. Teaming with a vendor who understands the application and the implications of the security and privacy requirements.

At a minimum, any organization considering the implementation of biometric technology should be able to give complete answers to a number of key questions, including:

1. Why are tokens, such as RFID and mag-stripe cards, or PINS/passwords alone unacceptable for your application?
    a. Possible answers supporting the use of biometric technologies include “Holders of tokens and passwords have an incentive to transfer them to others”; “Holders do not report lost tokens”; “Holders have no incentive to protect access to computers or facilities”.
2. What is the business case for using biometrics?
    a. How will the system be paid for?
    b. What cost savings can be anticipated by the use of biometrics?
    c. Establishing a business case may require estimation of both the database growth rates and the number of transactions required of the system, as some vendors base licensing payments upon number of comparisons made.
3. What current policies and legal requirements control your need for recognition technology?
4. Will the collection and use of biometric data cause additional policies and legal requirements to apply?
5. What privacy policies will be in place?
    a. Who will have access to the data?
    b. To what uses will the data be put?
    c. When and how will the data will be destroyed?
    d. What means will be in place to protect the data?
6. Are facilities and personnel available for the task of biometric enrolment?
    a. Enrolment generally requires verifying users’ current credentials, teaching proper use of the equipment, taking several biometric samples to serve as the stored reference.
7. Will the biometric system require PINs or tokens to serve as a pointer to the user reference?
    a. The answer may depend upon database size.
    b. If so, can existing PINs or tokens serve as a pointer or will new PINs/tokens need to be issued?
8. How will user difficulties with the system be resolved?
    a. The system must be designed with the certainty that some users will be wrongly denied services because of false positives or false negatives.
9. Will biometric technologies be needed to prevent multiple enrolment of a single individual?
    a. What risks, if any, exist in allowing a single individual to have multiple enrolments?
10. What will the application environment be like?
    a. Will the readers be in a controlled environment, will they be supervised, covered by CCTV etc? Will the environment by harsh?
    b. Will the users be under stress?
    c. Most biometric systems are designed and tested to be used indoors in office-like environments with office workers.

SECTION 7 Case Studies

Common applications of biometrics include access control to secure spaces, time and attendance logging, logical access to bank accounts, and computer system log-on. Here are three case studies:

7.1 Access control to secure spaces

San Jose State University in San Jose, California has been using hand geometry readers, for around-the-clock controlled, secure access to the Computer and Telecommunications Centre since 1993. About 125 employees are enrolled in the system and log a combined 500 entrance events each day at the three entrances. The system records all events on a central PC, allowing management to audit after-hour access to the Centre.

Employees permitted Centre access enter a 4 digit PIN into the system and place their right hand down on a reflective platen. At the time of enrolment of the employee, this vector is stored as a reference, pointed to by the PIN. Future measurements are compared to this reference vector. The use of the PIN as a pointer to the reference biometric characteristics requires every user to be assigned a different PIN, which may or may not be a secret. Users cannot pick their own PINs.

When an employee wishes to gain access to the Centre, they enter the PIN and place their right hand on the reflective platen. If the size and shape of the hand is “close enough” to the enrolled hand indexed by that PIN, the door opens and access is permitted. Upon successful use, the system automatically updates the stored reference by averaging in the newly acquired hand shape. The threshold used to determine “close enough” can be set individually, if necessary, to accommodate anyone having unusual difficulty using the system. The entire access process takes just a few seconds and false negatives with daily users of the system are exceedingly rare.

Impostors would need both a valid PIN and the correct hand shape to gain access to the system. PIN guessing can be prevented by locking the system or alarming after some number of consecutive access failures. The hand geometry technology has been widely tested in a number of openly published and commercial trials, so laboratory error rates are well understood.

The hand readers at each door now (2008) cost about US$1500. Some additional items, like electrically-activated door strikes, cabling and “request to exit” switches were purchased and installed, as well. The door strikes are controlled and powered directly from the hand reader unit. Although the units can stand alone, a central PC is used for event logging and for networking multiple units into a single reference database. University management has been quite pleased with the cost, efficiency, and security of the system.

San Francisco International Airport has been using hand geometry readers for employee access control to secured spaces since 1991. There are about 18,000 employees enrolled in the system, which logs approximately 186,000 transactions per day on the 280 networked readers in both the international and domestic areas of the terminal. Currently, this is the only large-scale application

of biometrics for general employee access control at an airport in the United States.

7.2 Access control in low security environments

Since 1996, the eight theme parks owned by the Walt Disney Corporation in Orlando, Florida, have used biometrics to link persons to tickets anonymously. Prior to 2006, finger geometry (a form of hand geometry using only the index and middle fingers) was the biometric technology employed. By 2006, that technology had become outdated, so Disney renewed the system with single-finger "finger scanning". Tickets with serial numbers encoded on magnetic stripes and bar-codes are sold to visitors on the condition that they may not be transferred. At the entry points to the various theme parks, visitors insert the tickets into a reader, and place any finger of choice on the fingerprint scanner. When the ticket is first used, the acquired fingerprint is linked to the serial number of the ticket and centrally stored. Whenever the ticket is used, the acquired fingerprint is compared to the stored fingerprint. If the match is considered 'close enough', it is presumed that the ticket is being used by the same person as first used the ticket and therefore the condition of 'non-transferability' has been met. If the fingerprint given at the entry point does not match that on file for the card's serial number or any other difficulty is encountered in the finger scanning process, a Guest Relations manager resolves the problem. Use of the system is optional for all guests.

At no point during the transaction is the user's name collected. Although it is true that entry transactions could theoretically be linked - via the ticket's serial number - to the credit card holder who paid for the ticket, some percentage of tickets are paid for in cash. Moreover, visitors are not required to buy their own ticket(s). Therefore, there is no way within the system to connect uses of the ticket to identified individuals. The use of anonymous biometric recognition enhances privacy far more than enforcing non-transferability by asking to see driving licences, passports or other identifying documentation. There have been over 21million successful fingerprint transactions since the fingerprint system was deployed and perhaps as many as 60 million biometric transactions since initial system deployment in 1996.

7.3 Logical access to bank accounts

Since 1997, Purdue Employees Federal Credit Union (PEFCU) in West Lafayette, Indiana, has been using fingerprint verification to replace PINs at nine Automatic Teller Machines (ATMs) kiosks. About 11,500 customers (20% of the PEFCU membership) are enrolled in the system, generating about 28,000 biometrically-enabled transactions per month. Customers electing to use fingerprinting can enrol in the system at the central office by presenting any two fingers to an optical scanner. Customers with poor fingerprints due to age or occupation, and customers not wishing to participate, can continue to use traditional PINs at all PEFCU ATMs.

The scanner takes a digital image of the fingerprint which is converted into a code based upon the patterns in the fingerprint ridges. The code, but not the

original fingerprint image, is stored in a central database[3]. After enrolment, customers can withdraw or deposit cash or apply for loans either by presenting their ATM card or by typing in their account number, then placing either enrolled fingerprint to the kiosk scanner. No further PIN entry is required. To guide users in the proper placement of the finger, a display screen on the kiosk shows the user the image of the presented fingerprint and an image of an ideally placed finger. The code extracted from the presented fingerprint is compared to that in the central database stored under the entered user name. Close similarity between the stored and presented codes verifies that the user is the source of the claimed enrolment record and is, therefore, the authorized ATM card holder.

The fingerprinting technology is estimated to represent only a small fraction of the total $70,000 cost of the ATM kiosk. No case of fraud owing to misuse of the fingerprinting system has ever been reported. Incidence of fraud originating from fingerprint-equipped ATMs is currently less than 5% of the fraud rate on other ATMs operated by PEFCU. The credit union is currently expanding the fingerprint system to traditional cashier desks to eliminate the need for enrolled users to present photo identification when making withdrawals.

This use of biometrics by PEFCU is to verify claims of identity with both habituated and non-habituated members of the general public in an unsupervised indoor or outdoor environment. One would expect the PEFCU application to be more challenging than the San Jose State University Computer Centre application with its more controlled population and environment.

[3] Because this code is not extracted or stored in a format recognized by international standards, it would be of no routine use by law enforcement.

SECTION 8 Existing and developing standards and bodies

In 2002, the International Standards Organization and the International Electrotechnical Commission established a standards body for biometrics, known officially as ISO/IEC JTC1 SC37. The UK contributes through the British Standards Institute shadow committee known as IST/44. Membership in IST/44 is open to all with interest in biometrics and a connection to British government, business (large or small), or academia.

As of this writing, SC37 has completed 20 international standards for biometrics, including standards for data storage and transmission, performance testing, and software application programming interfaces (API). Technical reports on the technology basics and privacy implications have also been completed.

Of the existing standards, those relating to data storage for fingerprint, face, and iris images allow:

1. Recognition of individuals across different systems;
2. Use of legacy data when changing vendors through technology refresh programmes;
3. Contractual decoupling of the data collection, processing and matching technology providers.

On the other hand, data standards are generally “lowest common denominator” – representing only those data elements common to all vendors. This implies that vendors can generally improve performance through use of proprietary approaches, storing images and codes relating to these in vendor-specific formats. Consequently, for “stand alone” access control applications with a limited lifespan, such that there will be no inheritance of legacy data by future systems, adherence to data storage and processing standards will not be the only path forward.

Lessons Learned

- The complexity of a carefully supervised enrolment process, and the resources that must be allocated, must not be underestimated.
- The complexity of the systems integration process -- making the biometric technologies fit into pre-existing information technology and business processes – must not be underestimated.
- Choose carefully your integrator – you will be spending a lot of time with them.
- All biometric systems must have quick, convenient, yet secure methods for adjudicating these errors and offering a fallback solution.
- Organisations planning to introduce biometric access control systems should consult with specialists in both the security and privacy of biometrics before committing to design and development.

References

[1] C. Watson, C. Wilson, M. Indovina, and B. Cochran, “Two finger matching with vendor SDK matchers” NISTIR 7249, July 2005, on-line at http://fingerprint.nist.gov/PFT/ir_7249.pdf. Testing updates are available at http://fingerprint.nist.gov/PFT/tables2f_110907.pdf

[2] A. Mansfield, G. Kelly, D. Chandler, and J. Kane, “Biometric Product Testing Final Report”, National Physical Laboratory, London, March 19, 2001, available online at www.cesg.gov.uk/technology/biometrics

[3] International Organisation for Standards, “Information technology -- Biometric data interchange formats -- Part 5: Face image data” ISO 19794-5:2005

[4] P. Jonathon Phillips, W. Todd Scruggs, Alice J. O’Toole, Patrick J. Flynn, Kevin W. Bowyer, Cathy L. Schott, and Matthew Sharpe. "FRVT 2006 and ICE 2006 Large-Scale Results." NISTIR 7408, March 2007, available on-line at http://iris.nist.gov/ice/FRVT2006andICE2006LargeScaleReport.pdf