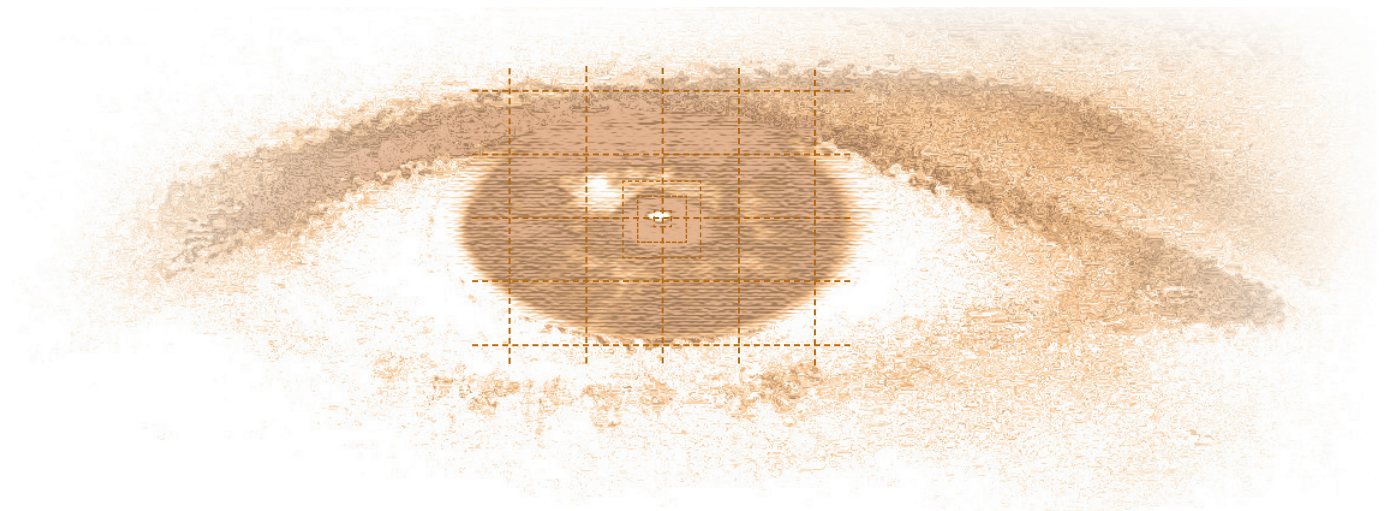


access control
biometrics
user guide



April 2006

For other information please contact:

British Security Industry Association
t: 0845 389 3889
f: 0845 389 0761
e: info@bsia.co.uk
www.bsia.co.uk

Why biometrics?

The purpose of this guide is to provide sound and practical advice to those who are considering Biometrics as part of a security solution. Some questions to be asked are:

- What level of security does your organisation require?
- Which biometric suits your requirement?
- Will your staff be willing to accept it?

Understanding Biometrics

A biometric is the automated means of recognising a living person by either a physiological or behavioural trait, which is unique to an individual and cannot therefore be passed on, or duplicated easily. Some of the more familiar biometrics are fingerprint, facial recognition, hand geometry and iris recognition. At present fingerprint technology is the most widely used and accepted. Many other biometric technologies are also available. These include voice recognition, retina, signature, finger geometry, typing characteristics (Behavioural) and DNA matching. Some of these methods have been superseded but many are still available. Due to the massive growth in the biometrics sector, a number of new technologies & methods are likely to become available in the future.

Choosing the right biometric

First of all you will need to ensure that your chosen security system supports biometrics. Each technology has advantages and disadvantages according to the application and the personnel using it. A number of factors need to be considered including ease of use, user acceptance and cost. It is important to compare the various manufacturers data for False Acceptance Rate (FAR) and False Reject Rate (FRR) to ensure the system meets the security requirements of the organisation.

Understanding technology

What is the difference between identification and verification?

There are two methods by which a user can be matched to their biometric sample; "one to one" and "one to many". These are sometimes referred to as "One to One" technology is where the user's biometric sample is compared to a single template stored by the biometric system. The term used to describe this identification method is *verification* because the user is verifying a known template. The user identifies themselves to the system (e.g. via a keypad, smartcard, etc), and then a biometric feature is scanned. This method is usually quick because the biometric system does not need to search through all records stored to find the user's template.

"One To Many" technology is where the recorded biometric feature is compared to all biometric data saved in a system. This method is referred to as *identification* due to the user being unknown to the system prior to providing a biometric sample. If there is a match, the identification is successful, and the corresponding user name or user ID may be processed subsequently. This method is usually fairly quick for small numbers of enrolled users but the speed of identification can deteriorate proportionally with the greater number of users enrolled. For small numbers of enrolled users it is possible to use biometrics only, making the use of a card or pin unnecessary.

Other relevant definitions

False Acceptance Rate (FAR)

The FAR is the frequency that a non-authorized person is accepted as authorized. Because a false acceptance can often lead to a lapse in security, FAR is a security relevant measure.

False Rejection Rate (FRR)

The FRR is the frequency that an authorized person is rejected access. FRR is generally thought of as a comfort criteria, because a false rejection can cause frustration to the user and delays in entry.

Enrolment

Enrolment is the process of recording the biometric into the system. All users must be enrolled to register their biometric. Good enrolment is critical to the successful operation of a biometric solution. Enrolment can be a time consuming process. Poor enrolment will lead to a higher False Acceptance Rate (FAR) and False Rejection Rate (FRR).

The enrolled biometric will be stored either on a card, the reader, or in a central database. Some systems will store the biometric in more than one of these locations.

As of the end of 2004 fingerprint technology is the most widely used and accepted. This is followed by facial recognition and hand geometry technology.

What are the advantages of a biometric system?

A biometric, unlike a pin or card, cannot be obtained from or given to another person. Biometric systems rely on a user providing a personal biometric sample to gain access. This increases the probability that it is the authorised person entering and removes the possibility of card sharing, "buddy punching" or similar system abuses.

Factors to be considered

Before implementing a biometric solution a risk assessment of the premises should be conducted. This assessment will determine the level of security you require and in turn influence your choice of which biometric to use. The risk assessment should be carried out by a suitably qualified organisation with specialist knowledge of biometrics and the installation of security systems. For a list of suitable installers refer to the BSIA web site at www.bsia.co.uk.

At present most biometric readers are suited for internal installation, as they are susceptible to environmental conditions, particularly rain and workplace contamination.

There can be difficulties when trying to enrol certain users or when trying to utilise certain technologies. For example a small proportion of users do not have a suitable fingerprint and cannot be enrolled with a high level of success. There may be occasions when it is inappropriate for a user to provide a Biometric because of a disability; in these circumstances an alternative method must be used.

User acceptance is crucial to implementing a successful biometric system, as some biometric technologies are perceived to be more acceptable than others. For example Iris technology is considered to be an invasive procedure but in fact is completely safe.

The use of a biometric device for identity verification does not, in itself, affect your privacy. Most biometric systems store the template as a mathematical algorithm and not as a readable image. It is virtually impossible to reverse engineer a stored template to produce an image of a user's biometric sample.

Account should be taken of the structure of the proposed system and its database. Biometric readers can be "stand-alone" with a local database or linked to a centralised server. Biometric information on this server can be sent to connected readers as required. The disadvantage of a "stand alone" system is that if the reader fails and the database is lost, all users will be required to re-enrol. It is also true that a loss of data communications on a system that relies solely on a centralised database will delay or prevent access.

Acknowledgements

We would like to acknowledge the support of the International Association for Biometrics.

Further information

For information on standards for Biometrics and further information visit their website: www.iafb.org.uk