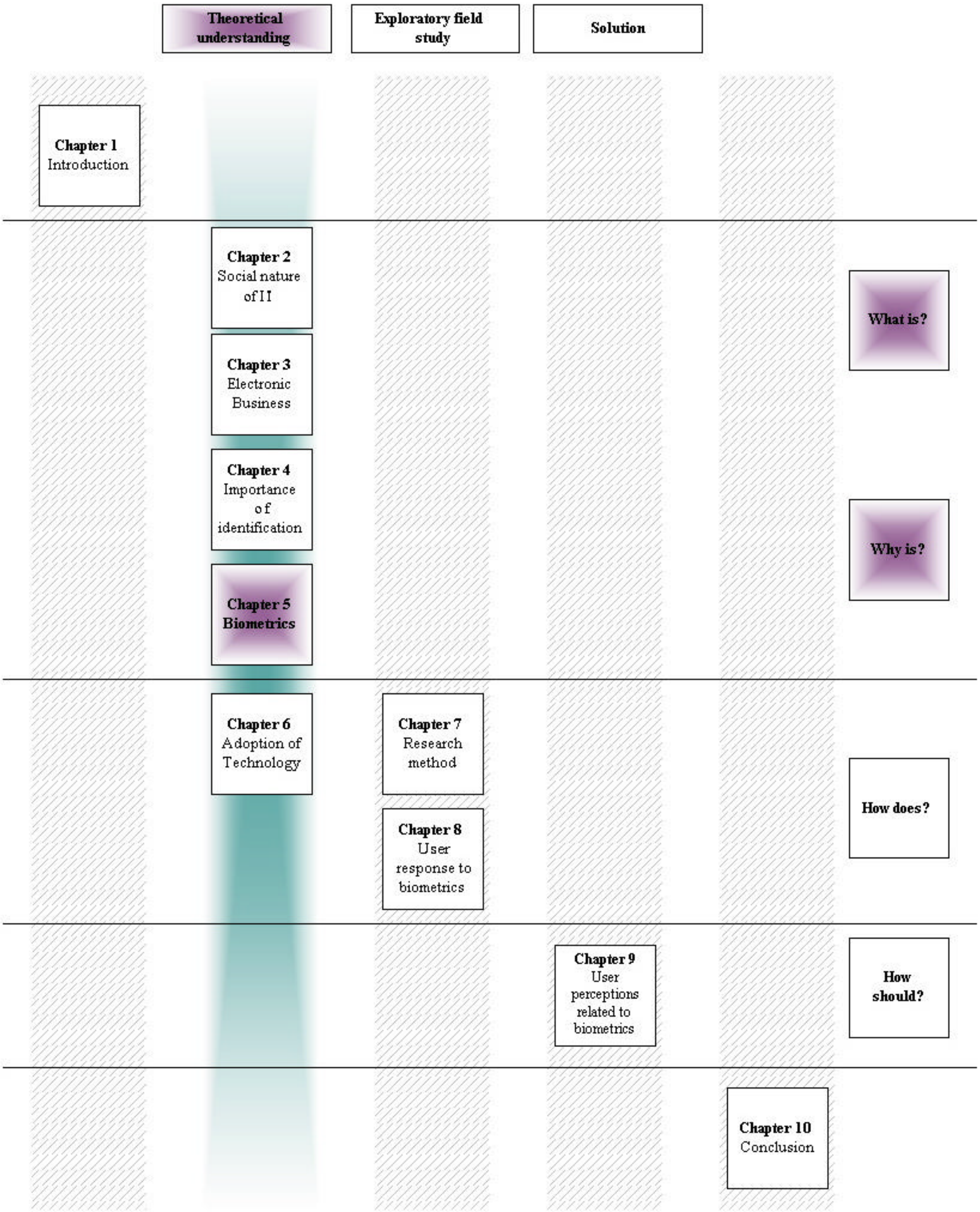
5. CHAPTER 5: BIOMETRICS

"Many people make the mistake of trying harder instead of trying differently."

Mark Twain

Figure 5-1: Thesis roadmap – Chapter 5


Theoretical understanding
Exploratory field study
Solution
Chapter 1 Introduction
Chapter 2 Social nature of II
Chapter 3 Electronic Business
Chapter 4 Importance of identification
Chapter 5 Biometrics
Chapter 6 Adoption of Technology
Chapter 7 Research method
Chapter 8 User response to biometrics
Chapter 9 User perceptions related to biometrics
Chapter 10 Conclusion
What is?
Why is?
How does?
How should?

CHAPTER 5: Biometrics

5.1 Introduction

This chapter provides a theoretical understanding of the term "Biometrics", addressing the research question: "What does biometrics comprise?" This chapter has the following sections:

- Defining the term biometrics.
- Providing a brief biometric history.
- Clarifying important biometric terminology.
- Explaining how a biometric system works.
- Listing **two** categories of biometric methodologies.
- Summarizing some biometric identification system advantages and disadvantages.
- Discussing some social factors that will impact on user perceptions related to biometrics and providing some social factor solutions proposed by other researchers before moving on to the chapter's summary and conclusion sections.

5.2 Biometrics defined

The term biometrics or biometry, also called a biometric characteristic or a biometric trait, (Allan 2002b and Prabhakar *et al*. 2003) can be seen as a scientific discipline – a "life measurement" and comes from the Greek words **bios** meaning life and **metron or metrikos** meaning measure. Biometrics can be defined as measurable physiological and/or behavioural characteristics that can be utilized to verify the identity of an individual, and include fingerprint verification, hand geometry, retinal scanning, iris scanning, face recognition and signature verification (Ashbourn 1999). Biometric research (2003) adds to this definition by referring to biometrics as an automatic identification of an individual based on his or her physiological or behavioural characteristics. Biometric research (2003) further states that a biometric system is essentially a pattern recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristic possessed by the individual. Biometrics is a general term for the measurement of humans, to identify them or authenticate that they are who they claim to be (Clarke 2001). Biometrics is of interest in any area where it is important to verify the true identify of an individual. Biometrics was previously only used in specialist high security applications, but is currently being used in a much broader range of public facing applications (Ashbourn 1999) such as prison visitor systems, drivers' licences, canteen administration, benefit payment systems, border control, voting systems, school areas, etc. According to Ashbourn (1999) future biometric identification applications could include ATM use, workstation and network access, travel and tourism, Internet transactions, telephone transactions, public identity cards, etc.

5.3 A brief history of biometrics

According to Ashbourn (1999) personal identification numbers (PINs) were one of the first automated recognition identifiers. However, the actual PIN was recognized and not the individual who provided the PIN. The same pitfalls apply to the use of cards and other tokens. Using a card or token together with a PIN provides a slightly higher confidence level, but it is seemingly easily compromised if one is determined to do so. Biometrics, on the other hand, cannot easily be transferred between individuals and represents a unique identifier, which means that verifying an individual's identify can become more accurate and streamlined.

Ashbourn (1999) states that it is tempting to think of biometrics as being a sci-fi futuristic technology that will be used some time in the near future, but in actual fact the basic principles of biometric verification were understood and practiced somewhat earlier. Thousands of years ago people in the Nile region routinely employed biometric verification in a number of everyday situations. Their techniques included identifying individuals via unique physiological parameters such as scars, measured physical criteria or a combination of features such as complexion, eye colour and height. The people of the Nile did not have automated electronic biometric readers and computer networks, and they were not dealing with the numbers of individuals that exist today, but the basic principles were similar.

Later, in the nineteenth century, researchers attempted to relate physical features and characteristics with criminal tendencies, resulting in a variety of measuring devices being produced. In parallel to this, fingerprinting became the international methodology amongst police forces for identity verification. The absolute uniqueness or otherwise of fingerprints is often debated, nevertheless, this was the best methodology on offer and still the primary one for police forces. With this background, it is hardly surprising that for many years a fascination with the possibility of using electronics and the power of microprocessors to automate identity verification had occupied the minds of individuals and organizations, both in the military and commercial sectors. Various projects were initiated to look at the potential of biometrics and one of these eventually led to a large and rather ungainly hand geometry reader being produced. Eventually, a much smaller and considerably enhanced hand geometry reader became one of the cornerstones of the early biometric industry. This device worked well and found favour in numerous biometric projects around the world. In parallel, other biometric methodologies such as fingerprint verification were being steadily improved and refined to the point where they would become reliable, easily deployed devices.

In recent years, much interest has been seen in iris scanning and facial recognition techniques, which offer the potential of a non-contact technology, although there are additional issues involved in this respect. The last decade has seen the biometric industry mature from a handful of specialist manufacturers struggling for sales, to a global industry shipping respectable numbers of devices and poised for significant growth as large scale applications start to unfold (Ashbourn 1999).

5.4 Clarifying certain terms

This section found within Chapter 5 – Biometrics, will discuss some important biometric terminology such as verification vs. identification and authentication vs. recognition.

5.4.1 Verification vs. identification

The terms "verification" and "identification" are often used when discussing biometrics, but are easily confused. Verification and identification are **two** different ways to resolve an individual's identity:

1. **Verification** involves confirming or denying an individual's claimed identity (Biometric research 2003) – Am I whom I claim I am? Most available biometric devices operate in a verification mode (Ashbourn 1999). This means that an identify is claimed by calling a particular template from memory and then performing a live sample for comparison, resulting in a match or no match according to predefined parameters. Verification can be seen as a one-to-one match that may be performed quickly and generate a binary yes or no result (Ashbourn 1999). Prabhakar *et al*. (2003) sees the verification process as a process whereby an individual's identity is validated by comparing the captured biometric characteristic with the individual's biometric template pre-stored in the system's database.
2. With **identification**, the identity of an individual has to be established (Biometric research 2003) – Who am I? Clarke (2001) sees identification as a process whereby a real-world entity is recognized, and its "identity established". Only a few devices claim to offer biometric identification whereby the individual submits a live sample and the system attempts to identify it within a database of templates. This can be seen as a more complex one-to-many match, which may generate multiple results according to the number and similarity of stored templates (Ashbourn 1999). Put in a different way, a new measurement is compared against a database obtaining information about large numbers of entities (Clarke

2001). In other words, the individual was in a particular location at a particular time, and conducted a transaction or provided data.

5.4.2 Authentication vs. recognition

The terms "authentication" and "recognition" may easily be confused. Authentication and recognition are **two** different ways (modes) that a biometric identification system can function (Allan 2002b):

1. Clarke (2001) sees **authentication** as a process whereby a degree of confidence is established about the truth of an assertion. In authentication mode the biometric system verifies an individual identity by comparing the trial template generated from the sample to a reference template, referred to as a one-to-one matching process (1:1). Put in a different way a new measurement that purports to belong to a particular entity is compared against the data stored in relation to that entity (Clarke 2001). In other words, the authentication of the identity of an individual who performs, or seeks to perform, a particular act e.g. gaining access to premises or gaining access to data. Allan (2002b) states that biometrics have an advantage over other authentication methods because a biometric identification system recognize an individual without the need for him or her to key in an identifier.
2. According to Allan (2002b) in **recognition** mode the biometric system combines identification within a single-step process; the biometric system determines an individual's identity by performing matches against multiple biometric templates, referred to as a one-to-many matching process (1:N).

There is, however, a middle ground between authentication and recognition referred to as one-to-few (1:few); it involves identifying an individual from a small database (Allan 2002b).

5.5 How do biometric systems work?

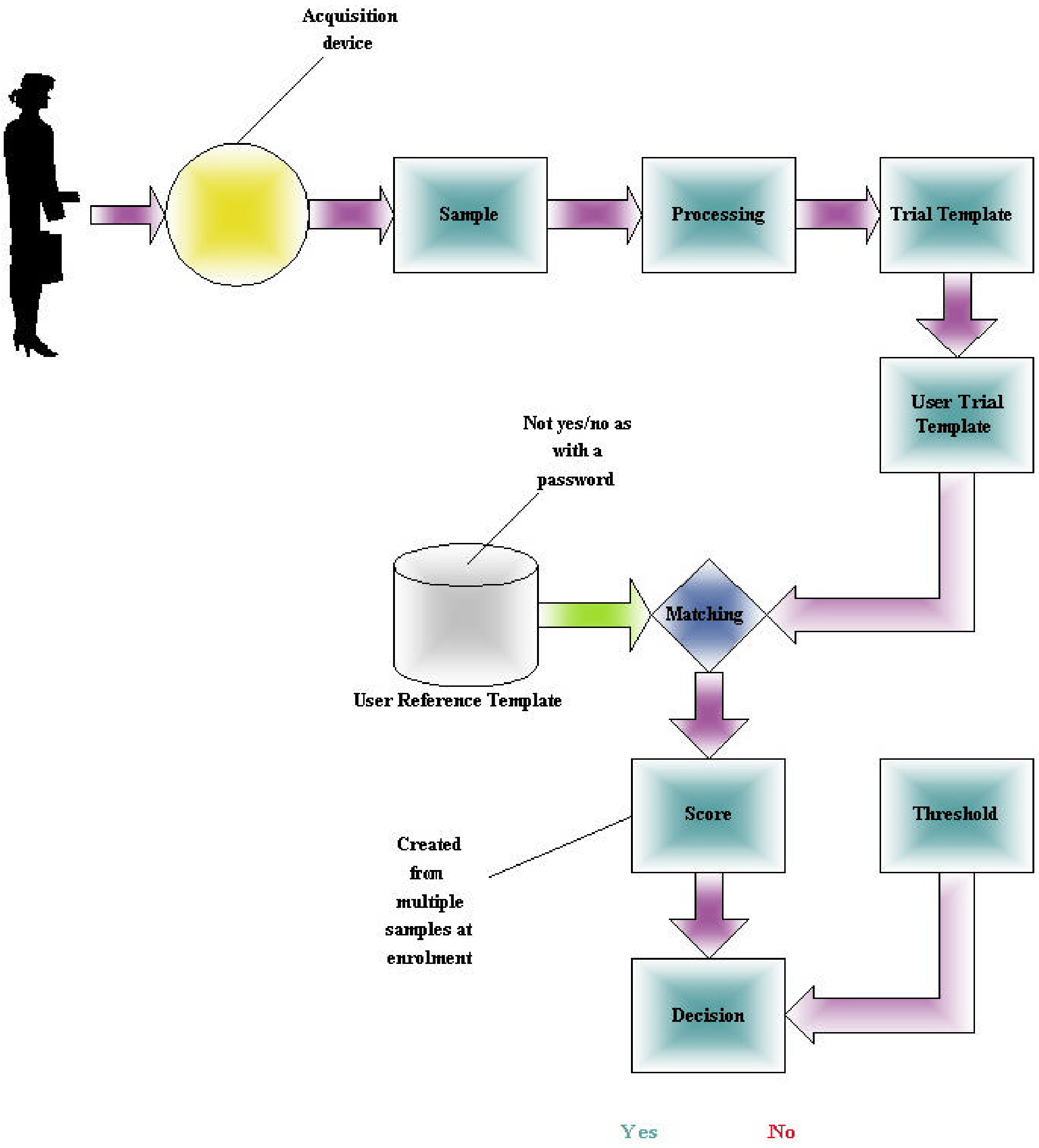
Allan (2002b), states that although biometric technologies differ in terms of what and how they measure, all biometric systems work in a similar way and the process can be summarized in the following steps:

1. The individual submits a sample (an identifiable, unprocessed image or recording of the physiological biometric or behavioural biometric) to the acquisition device e.g. a scanner or camera.
2. The biometric sample is processed to extract information about distinctive features to create a trail template or verification template, which is essentially large number sequences and it is impossible to reconstruct the biometric sample from the template, known as the individual's "password".
3. Verifying a memorized password or a one-time password, generated by an authentication token, is a simple yes or no decision; however, verifying a trial template is not. A trail template is compared against a reference template or enrolment template that was created from multiple images when the individual was enrolled into the biometric system.
4. No **two** templates are ever the same, so the biometric system must decide if there is a "close enough" match – the matching score must exceed the configured threshold. In other words, biometric identification systems can err e.g. a trial template might be matched incorrectly against another individual's reference template, or it might not be matched even though the user is enrolled in the biometric identification system.
5. Therefore, the accuracy of a biometric system is measured by:
   - ❑ **FMR** (False match or acceptance rate) – the lower the biometric identification system's FMR, the better the security. FMR means mistaking the biometric measurements from **two** different individual's to be from the same individual (Prabhakar *et al*. 2003).

- **FNMR** (False non-match or rejection rate) – the lower the biometric identification system's FNMR, the easier the system is to use. FNMR means mistaking **two** biometric measurements from the same individual to be from **two** different individuals (Prabhakar *et al*. 2003).

Both methods focus on the biometric identification system's ability to allow limited access to authorized individuals. In general, for any given biometric system, the lower the FMR (False match rate), the greater the FNMR (False non-match rate) and there has to be a trade-off between the biometric system's security and its ease of use to the individual (Allan 2002b). The following figure provides a schematic representation of a typical biometric system (Allan 2002b):

Figure 5-2: A biometric system



Source: Adapted from source - ALLAN, A. 2002b. Biometrics: How do they measure up? *Gartner Research*, 2002, p.1-5.

To conclude, all biometric systems works in a similar way, but it is important to remember that the ease of enrolment and quality of the template are critical success factors in the overall success of any biometric system (Allan 2002b).

5.6 Biometric methodologies

This section discusses **two** different biometric methodology categories, namely physiological biometrics and behavioural biometrics (Allan 2002b). The section further lists some strengths and weaknesses, as well as suitable applications per biometric methodology as summarized by Allan (2002b).

5.6.1 Physiological biometrics

Physiological biometrics, also called physical biometrics or static biometrics, is based on data derived from the measurement of a part of an individual's anatomy (Allan 2002b) e.g.:

1. At present there are a greater variety of **fingerprint verification** approaches available than any other biometric method and include (Ashbourn 1999) the emulation of the traditional police method of matching minutiae, straight pattern matching devices, and some that can even detect if a live fingerprint is presented or not. Potentially capable of good accuracy (low instances of false acceptance) fingerprint devices can suffer from usage errors among insufficiently disciplined individuals (higher instances of false rejection) especially within a large user base. The user interface (Ashbourn 1999) and how it will be affected by larger scale usage in a variety of environments should also be considered. According to Allan (2002a) it has been established that the chance of **two** individuals having the same fingerprint is less than one in a hundred billion. It is known that fingerprints form in the womb at around **five** months and remain constant even after death. Fingerprints have even been successfully taken from well-preserved mummies more than **two** thousand years after their death (Allan 2002a).
2. **Hand geometry**, as the name suggests, is concerned with measuring the physical characteristics of the individual's hand and fingers (Ashbourn 1999). The method offers a good balance of performance characteristics and is relatively easy to use. This methodology, according to Ashbourn (1999) may be suitable on larger individual bases or individuals who may

access the system infrequently and may therefore, be less disciplined in their approach to the system. Accuracy can be very high if desired, whilst flexible performance tuning and configuration can accommodate a wide range of applications (Ashbourn 1999). Ease of integration into other systems and processes, coupled with ease of use, makes hand geometry an obvious first step for many biometric implementation projects (Ashbourn 1999). According to Allan (2002a) virtually every individual's hands are shaped differently from everyone else's and the shape does not significantly change over time. A biometric template can be built from measurements of geometrical characteristics of an individual's hand (Allan 2002a).

3. **Retinal scanning** is an established technology where the unique patterns of the retina are scanned by a low intensity light source via an optical coupler (Ashbourn 1999) and has proved to be quite accurate in use. However, it does require the individual to look into a receptacle and focus on a given point. This is not particularly convenient if the individual is a spectacle wearer or has concerns about intimate contact with the reading device (Ashbourn 1999). According to Allan (2002a), along with iris recognition technology, retinal scanning is perhaps the most accurate and reliable biometric technology.
4. **Iris scanning** is undoubtedly the least intrusive of the eye-related biometric methodologies (Ashbourn 1999). Iris scanning utilizes a fairly conventional CCD camera element and requires no intimate contact between the individual and reader. In addition, it has the potential for higher than average template matching performance and has been demonstrated to work with spectacles in place and with a variety of ethnic groups. It is one of the few methods that can work well in identification mode (Ashbourn 1999). According to Allan (2002a) the uniqueness of eye identification is well established. The iris is a robust biometric, as it remains unchanged throughout an individual's life and is not subject to wear and injury, although damage to the cornea, disease and so forth might

obscure the iris. The iris has **six** times as many distinct identifiable features as a fingerprint (Allan 2002a).

5. **Face recognition** is a technique that has attracted considerable interest and whose capabilities have often been misunderstood. Extravagant claims have been made for facial recognition devices, which have been difficult to substantiate in practice. It is one thing to match **two** static images; it is quite another to unobtrusively detect and verify the identity of an individual within a group. It is easy to understand the attractiveness of facial recognition from an individual's perspective, but the expectations of the technology (Ashbourn 1999) need to be realistic. According to Allan (2002a) an obvious limitation of face verification is that, because it generally disregards changeable characteristics like hair colour and style, it cannot differentiate between monozygotic siblings. To date, facial recognition systems have had limited success in practical applications. However, progress continues to be made and if the technical obstacles can be overcome, facial recognition could become a primary biometric methodology (Ashbourn 1999) in the near future.

5.6.2 Behavioural biometrics

Behavioural biometrics, also called dynamic biometrics, is based on data derived from measurements of an action performed by an individual and distinctively incorporating time as a metric; the measured action has a beginning, middle and end (Allan 2002b) e.g.:

1. According to Ashbourn (1999) **voice verification** is an interesting technique bearing in mind how much voice communication takes place with regard to everyday business transactions. Some designs have concentrated on wall-mounted readers whilst others have sought to integrate voice verification into conventional telephone handsets. According to Allan (2002a) voice is less accurate than other biometrics, but its main attraction is its suitability for telephone applications and

interactive voice response (IVR) systems, where it can be deployed with no additional hardware costs.

2. **Signature verification** enjoys a synergy with existing processes that other biometric methodologies do not have; individuals are used to signatures as a means of transaction-related identity verification and would mostly see nothing unusual in extending this to encompass biometrics (Ashbourn 1999). Signature verification devices have proved to be reasonably accurate in operation and lend themselves to applications where the signature is an accepted identifier (Ashbourn 1999). According to Allan (2002a) signature identification systems analyze **two** different areas of an individual's signature: the specific features of the signature itself (visual image) and the specific features of the process of signing. Features that are taken into account and measured include speed, pen pressure, directions, stroke length and the points in time when the pen is lifted from the paper (Allan 2002a). With sufficient practice, an individual might be able to duplicate the visual image of someone else's signature, but it is difficult if not impossible to duplicate the dynamics (Allan 2002a).

5.6.3 Strengths, weaknesses and suitable applications

The following table (Allan 2002a) provides a summary per biometric methodology, listing some strengths, weaknesses and suitable applications:

Table 5-1: Strengths, weaknesses and suitable applications

Biometric	**Strengths**	**Weaknesses**	**Suitable applications**
Fingerprint verification	Very stable over time Uniqueness	Potential user resistance Requires user training	IS access control Workstation access control Physical access control ATMs Automotive
Hand geometry	Small template Low failure-to-enrol Unaffected by skin condition	Size of device Physical contact required Juvenile finger growth	IS access control Physical access control Time and attendance
Voice verification	Good user acceptance Low training	Unstable over time Changes with time	Mobile phones Telephone banking
Retina scanning	Stable over time Uniqueness	Requires user training High user resistance Slow read time	IS access control Physical access control
Iris scanning	Very stable over time Uniqueness	Potential user resistance Requires user training Dependant on a single vendor's technology	Physical access control ATMs and airline tickets
Signature verification	High user acceptance Minimal training	Unstable over time Changes over time Enrolment takes long	Portable devices stylus input Applications where a "wet signature" ordinarily would be used

Biometric	**Strengths**	**Weaknesses**	**Suitable applications**
Facial recognition	Universally present	Can not distinguish between identical siblings Religious or cultural prohibitions	Physical access control

Source: Adapted from source - ALLAN, A. 2002a. Biometric Authentication: Perspective. *Gartner Research*, 2002, p.1-31.

To summarize, physiological biometrics is unchanging and unalterable, but is perceived as being more invasive and raises privacy concerns more quickly. On the other hand, behavioural biometrics are partly derived from physiology; an individual's voice depends on the shape of the vocal chords, an individual's signature depends on the dexterity of hands and fingers and an individual's face might depend or change based on the individual's behaviour (Allan 2002b). In other words, behavioural biometrics is less stable, changes with stress and sickness and is less secure (Allan 2002b), but has a significant advantage over physiological-based biometrics because the verification process can be potentially "invisible" to the user (Deane *et al*. 1995). Deane *et al*. (1995) further state that behavioural-based biometric security systems are more acceptable to users than physiological-based biometric security systems because they are perceived to be less obtrusive and less intrusive e.g.:

1. There have been some concerns over the widespread acceptance of **fingerprint verification** due to its association with crime (Torbet *et al*. 1995). Torbet *et al*. (1995) mentions that although fingerprint verification seems to be socially doubtful, it appears to be legally acceptable.
2. It is interesting to note that some characteristic of physiological-based biometric methods makes them more acceptable than behavioural-based biometric methods e.g. **voice verification** appears to be more acceptable than other behavioural-based biometric methods. The reason could be that the verification of an individual's voice is perceived to have more in common with fingerprint and

retina verification procedures (physiological) than signature verification procedures (behavioural). This "salient" characteristic may result in a relatively higher acceptability rating for voice verification (Deane *et al*. 1995). According to Torbet *et al*. (1995), voice verification seems to be socially acceptable and requires no literacy skills.

3. **Retina scanning** appears to be less acceptable than other physiological-based biometric methods. This could be due to the high level of intrusiveness associated with the procedure. Individuals are highly sensitive and protective of their eyes, and retina scanning may be thought of as an unacceptable intrusion and/or threat (Deane *et al*. 1995). Torbet *et al*. (1995) states that retina scanning is invasive, expensive and invokes fears about security.

Other biometric methodologies include the use of scent, ear lobes and various other parameters. Whilst these may be technically interesting, they are not considered at this stage to be workable solutions in everyday applications (Allan 2002a). New biometric technologies using other physiological and behavioural features are under development and include (Allan 2002a):

1. **DNA matching** is the "ultimate" biometric technology that can produce proof-positive identification of an individual.
2. **Keystroke dynamics** is an innovative biometric technology. The system measures **two** distinct variables: dwell time (the length of time an individual holds down a particular key) and flight time (the length of time it takes an individual to move between keys).
3. **Palm print** uses the patterns of line on an individual's palm in much the same way as with fingerprint verification.
4. With **vascular patterns** the patterns or veins on various parts of an individual's body as well as the face are used.

To conclude, there is no single "best" biometric methodology, different biometric methodologies vary widely in cost and performance and the various characteristics of the biometric method will suit different applications e.g.:

1. Iris scanning, fingerprint verification and face recognition biometrics will likely have the widest applicability.
2. Voice recognition and signature verification would generally be reserved for interactive voice response and document systems, respectively (Allan 2002a).

The **bottom line** is that biometrics offer a strong method of authentication in a wide variety of applications and can help recognize individuals and speed up access processes.

5.7 Biometric identification system: advantages and disadvantages

Biometrics does have some drawbacks, but it also has some outstanding benefits. An organization must consider user perceptions related to biometrics, security (accuracy, reliability and resistance to track), intrusiveness, cost (expense), effortlessness (ease of use) and template storage (location and capacity planning) when selecting a specific biometric identification method (Allan 2002a and 2002b).

Based on the views of Allan (2002a) and Harris and Yen (2002) a biometric identification system advantages and disadvantages can be summarized in the following **two** tables:

5.7.1 Biometric identification system advantages

Table 5-2: Summary of biometric advantages

Advantages	**Why?**	**Improvements**
No PINs	Cuts down on support costs	Efficiency
Known user	Confidence in information	Decision making
Cannot be sheared	Integrity of information upheld	Reliability
Use of template	Cannot recreate biometric	Security
Levels of security	Adjust to needs of business	Customizability
Increased security	Biometric information cannot be lost	Security
Increased convenience	Biometric information always present	User acceptance
Reduced costs	Eliminate the overhead of password management	Economical

Source: Adapted from source - ALLAN, A. 2002a. Biometric Authentication: Perspective. *Gartner Research*, 2002, p.1-31. and HARRIS, A.J. and YEN, D.C. 2002. Biometric authentication: assuring access to information. *Information Management and Computer Security*, 2002, vol.10, no.1, p.12-19.

Albrecht (2003) states that biometrics can provide:

1. **Conventional security –** Biometric methods can provide greater security within the verification system. A verification system based on the principle of possession and knowledge normally requires verification using a token (e.g. smart card) in conjunction with a PIN. The primary weaknesses of this traditional identification method are that it can be easily lost or forgotten, the card or code can be stolen, and their transferability (whether voluntary or forced) means they lack distinct personal verification. The security of a knowledge-based method depends primarily on the individual keeping their code secret.
2. **Unforgettable –** Biometric characteristics cannot be forgotten.

3. **Secure from theft –** Under normal circumstances, biometric characteristics cannot be stolen.
4. **Transferable –** Biometric characteristics are not transferable.

Biometric identification methods, according to Biometric research (2003), are preferred over traditional methods involving passwords and PINs for various reasons. These include that the individual to be identified is required to be physically present at the point-of-identification, and identification based on biometric techniques obviates the need to remember a password or carry a token.

5.7.2 Biometric identification system disadvantages

Table 5-3: Summary of biometric disadvantages

Disadvantages	**Why?**	**Decreases**	**Alternatives**
Biometric is public	Access to others	Security	Protect biometric
Faulty scans	More time for authentication	Efficiency	Improve process
Inconvenience	Upset users	Productivity	Use alternative biometric
Cost	Deter business from using	Security	Show gains from systems
Education	Time is needed for this	Productivity	Whitepaper availability
People's views	Must overcome issues	Productivity	Address before implementation
Default threshold	Some can be beaten	Security	Raise threshold
Privacy concern	Misuse of data	User acceptance	Protect information
Personal, cultural and religious concern	Criminal connotation and hygiene	User acceptance	Use alternative biometric

Disadvantages	Why?	Decreases	Alternatives
Suitability for all users	Missing body part	User acceptance	Use a "**fallback**" system

Source: Adapted from source - ALLAN, A. 2002a. Biometric Authentication: Perspective. *Gartner Research*, 2002, p.1-31. and HARRIS, A.J. and YEN, D.C. 2002. Biometric authentication: assuring access to information. *Information Management and Computer Security*, 2002, vol.10, no.1, p.12-19.

To summarize, the biometric identification system advantages and disadvantages need to be evaluated by the organization in order to select the most applicable methods for their business purposes.

5.8 Social factor influence

As mentioned in Chapter 3 – Electronic Business, social factors are aspects that describe intrinsic human values that cannot be changed fundamentally in any way and relate to human behaviour that links with human perceptions and attitudes. There are always factors, which could be of a technological nature or of a social nature, that obstruct emerging technology adoption. In the case of biometrics these include user perceptions related to biometrics, the potential loss of privacy, false acceptance rates, device deployment difficulties (Wheatman 2002) and according to Shankar *et al.* (2002), trust is important in the adoption of new technologies such as biometrics. The pursuit of high-quality identification through biometrics involves significant technical, organizational, social, legal and political issues (Davies 1994) and the tie between the actual identity of an individual and the use of biometrics is subtle and provokes many debates, particularly relating to privacy and other societal issues (Soutar 2002). A high-integrity biometric system appears, from the perspective of the organization, to be an ideal solution to identification problems – yet, from the perspective of the user, any move toward a biometric identifier carries enormous risk (Davies 1994).

Biometrics have been seen on the verge of market acceptance for several years, providing (Wheatman 2002) "something you are", e.g. fingerprint or retina scan, in addition to "something you know", e.g. use identification or password, and "something you have", e.g. security token, smart card or dongle. Biometrics is appealing because if it works correctly it identifies the user requesting access rather than raising the question (Wheatman 2002): "Did someone else use the password or token?"

But, according to Albrecht (2002b and 2003), individuals have many concerns when considering the use of biometrics. Albrecht's (2002b) survey conducted in 2002 shows that an individual when first introduced to the concept of biometrics, tends to have a spontaneous positive attitude towards it. At a second glance, however, individuals become sceptical, especially towards the use of the new technology in their private lives e.g. at home. On the other hand, users were more receptive to the idea of using biometrics in their work environment. In general, there is a feeling of being at the mercy of a procedure that has not yet been correctly classified and where security, reliability and robustness cannot yet be ultimately evaluated. Contact with biometrics and therefore, with personal human characteristics, appears to make people more sensitive towards adopting biometrics as an identification system (Albrecht 2003).

5.8.1 Security and privacy considerations

"The real danger is the gradual erosion of individual liberties, through the automation, integration, and interconnection of many small, separate record keeping systems, each of which alone may seen innocuous, even benevolent, and wholly justifiable."

U.S. Privacy Protection Study Commission, 1977

As most biometric systems are deployed within security systems, or as part of an identification program, implementation issues relating to security and privacy need to be considered (Soutar 2002). User perceptions of security systems in general are of paramount importance for successful biometric identification system implementation; an inaccurate perception of a security system may have considerable implications for the climate of organizational trust, morale and employer-employee and employee-employee relationships (Deane *et al*. 1995).

Privacy can be defined as the ability to lead your life free of intrusions, to remain autonomous and to control access to personal information (Prabhakar *et al*. 2003). Privacy in its simplest form, according to Electronic Commerce policy (2002b) can be described as the "right to be left alone". This right is made up of several different elements, such as the right to enjoy private space, the right to expect confidentiality and the right to individual autonomy. According to Phillips (2001), user perceptions with regard to privacy concerns is the leading inhibitor to user adoption of biometric technology and can be divided into **three** systematic privacy concerns (Prabhakar *et al*. 2003):

1. **Unintended functional scope** – biometric identifiers are biological in origin and might provide additional personal information from scanned biometric measurements e.g. malformed fingers might be statistically correlated with certain genetic disorders. With the rapid advances in human genome research, fear of inferring further information from biological measurements might be on the rise. Such derived medical information could become the basis for systematic discrimination against segments of the population perceived as "risky". According to Phillips (2001) specific biometric data can be linked with information beyond that used for identification, such as AIDS, diabetes, blood pressure and sexual orientation.
2. **Unintended application scope** – strong biometric identifiers such as fingerprints allow the possibility of unwanted identifications e.g.

individuals legally maintaining aliases for safety purposes could be identified based on their fingerprints. In addition, biometric identifiers could link behavioural information about individuals enrolled in a wide range of different applications; detractors often construe this potential as a means for organizations (governmental or corporate) to accumulate power over individuals and their autonomy. According to Phillips (2001) template databases may be made available to law-enforcement agencies and may be crosschecked against other databases by a credit provider.

3. **Covert recognition** – biometric characteristics are not secret. It is easy to obtain a biometric sample such as individual's face, without that individual's knowledge. This permits covert recognition of previously enrolled individuals. Consequently those who desire to remain anonymous in any particular situation could be denied their privacy by biometric recognition.

Clark (2001) identified the following threats embodied in biometric identification methods with regard to privacy consideration:

1. **Privacy of the user** – biometrics does not simply involve collection of information **about** an individual, but rather information **of** the individual, intrinsic to them. This statement alone makes the idea of biometrics distasteful to individuals in many cultures and of many religious persuasions. Each individual has to submit "something" for examination, in some cases in a manner that many individuals regard as demeaning, e.g. in providing a quality fingerprint, one's forearm and hand are grasped by a specialist and rolled firmly and without hesitation across a piece of paper or a platen, and an iris or retina scan requires the eye to be presented in a manner compliant with the engineering specifications of the supplier's machine.
2. **Privacy of user data** – many organizations require the provision of user personal data to assist in the administration of their business. Some are operated in close conjunction with other data-rich systems such as

personnel or welfare administration. This consolidation of data enhances the opportunity for the organization to exercise control over the population for whom it holds biometrics.

3. **Privacy of user behaviour –** the monitoring of individuals' movements and actions through the use of biometrics increases the transparency of individuals' behaviours to organizations. These organizations are in a better position to anticipate actions that they would prefer to prevent and communicate warnings to the predicted perpetrators.

The use of biometrics is seen as an invasion of privacy because the individual has to enrol with an image of a body part and once acquired, it is possible that the biometric might be used for other purposes, unknown to the individual (Bolle *et al*. 2001). Biometric characteristics are personal data and therefore, especially worth protecting; in many cases surplus information can be gained from biometric data e.g. diseases like diabetes can be recognized by viewing the retina of the eye or people's age can be estimated by analyzing their fingerprints (TeleTrust 2003b). This surplus information is almost never necessary for the actual purpose and should not be analyzed and evaluated, but since it is part of the biometric data, it has to be protected from any further unauthorized evaluation (TeleTrust 2003b). There is also the possibility of comparing biometric data from different applications and gaining additional information (Gundermann and Probst 2001).

RSA Security (2002) states that any identification system (whether it makes use of biometrics or not) should adhere to **four** key elements of a privacy policy:

1. **Notice** – users need to receive prior notification of information practices.
2. **Choice** – users need to be in a position to provide specific consent to the gathering and use of information pertaining to them.
3. **Access** – users need to have the ability to access their own personal information whenever needed.

4. **Security** – users need to have assurance that the organization has taken and is taking measures to prevent unauthorized access to and use of their personal information. This definition is similar to the definition given earlier in the research study to privacy by Ratnasingham (1998) because security also includes a confidentially factor – to keep information private (e-Security 2000).

With regard to security, from an individual point of view, the greater security that biometrics may offer over conventional identification methods is seen as a distinct advantage. Individuals are well aware of the disadvantages of traditional identification methods and prefer biometric methods to passwords and PINs, but at the same time the need for security of biometric data needs to be addressed (Albrecht 2003). Due to the fact that biometric data is more or less "public", the security of biometric systems cannot depend on the "secrecy" of biometric data (Gundermann and Probst 2001).

To conclude, user perceptions related to biometrics with regard to privacy concerns are the leading inhibitor to user adoption of biometric technology; individuals are concerned about their own privacy and the privacy of their data – in other words, the security of the biometrics data needs to be addressed. The question to be answered is then: How can security and privacy considerations be addressed with regard to user perceptions related to biometrics? With regard to security and privacy considerations Albrecht (2003) stresses that individuals have a pronounced need for information on biometric identification methods. In particular, they want to know how the technology works, where the data is stored, which data is registered, how the data is protected, who has access to the data and who is operating the system. An experienced and trustworthy institution or operator, addressing "who is operating the system", should perform the enrolment process. User guidance, in person or by means of a user guide, is important and the way the individual needs to present his or her biometrics information e.g. fingerprint, voice, retina, etc. must be explained in detail because of the necessary active co-operation from the individual (Albrecht 2003). If this need for information can be addressed, it will lead to individuals' security and privacy considerations being reduced tremendously. To secure authentic data transfer and to provide for a safe connection between the user ID and the saved template, cryptographic techniques can be used (Gundermann and Probst 2001), addressing individual concerns around "how the data is protected". Biometric features can be used for encryption as well as for security, providing better means to control access to or manipulation of data than conventional password systems.

Gundermann and Probst (2001) state that biometrics should not be seen as a threat, but rather as a means to improve and enhance privacy. They further suggest that biometrics should be promoted (Tomko 1998) as a privacy enhancing technology (PET), the principle of which can be summarized as (Albrecht 2002a):

"*Different measures in the areas of communication – and information technologies which aim to protect privacy by means of elimination or reduction of personal data without loss of functionality of the Information Technology system.*"

Electronic Commerce policy (2002a) defines privacy-enhancing technology (PET) as a technology that protects personal identities and is designed to provide individuals with control over their personal information. They further state that privacy-enhancing technology (PET) may provide technological answers to the protection of personal information, as tools complimentary to privacy legislation. In other words, information privacy refers to an individual's right to determine when, how and to what extent they will share personal information about themselves with others (Electronic Commerce policy 2002b). According to Albrecht (2002a) biometrics in terms of being promoted as a privacy-enhancing technology (PET) means that:

1. Biometrics must use as little personal data as necessary for the aim of its authentication process.
2. If biometrics does use personal data, it must make use of data encryption as part of the process.
3. Raw data, not being used, should be destroyed as soon as possible.
4. The biometric database should be decentralized.
5. Individuals must have control over their personal data.
6. Means of evaluation and certification must be used to create a guaranteed level of trust amongst the participants making use of the biometric process.

Lastly, biometric identification methods should be portrayed to individuals as a "privacy protector": biometric authentication can provide a personal binding of a right to access personal data and as a protector of identity theft (Albrecht 2002a). In the end, the actual outline of applications will ultimately determine whether a biometric identification system should be considered as a threat to privacy or not.

5.9 Summary

This chapter first defined the term biometrics as measurable physiological and/or behavioural characteristics that can be utilized to verify the identity of an individual (Ashbourn 1999). Biometric methodologies were categorized as physiological or behavioural biometrics. These can offer a strong method of authentication in a wide variety of applications that can help to recognize individuals and speed up the access processes (Allan 2002b). Individuals' pronounced need for information on biometric identification methods should be addressed, which will lead to their security and privacy considerations being reduced tremendously.

5.10 Conclusion

It was concluded in this chapter, **Chapter 5 – Biometrics**, that all biometric systems function in a similar way, but it is important to remember that the ease of enrolment and quality of the template are critical success factors in the overall success of any biometric system (Allan 2002b). Furthermore, user perceptions with regard to security and privacy considerations were identified as social factors that need to be addressed as part of user adoption when making use of biometrics as an identification method within Electronic business (Soutar 2002). It was concluded that biometric identification methods should be sold to individuals as a privacy-enhancing technology (PET), convincing them that it will act as a privacy protector instead of a privacy invasion technology (Albrecht 2002a).

This chapter has therefore, addressed the research question: "What does biometrics comprise?" The last chapter within the literature study section of the research study will provide a theoretical understanding of "Adoption of technology".