



## **BIOMETRICS WHITE PAPER**

### **Introduction**

**A biometric is defined as "a measurable, physical characteristic or personal behavioural trait used to recognise the identity, or verify the claimed identity, of an enrollee".**

With an ever increasing awareness of security and identity theft, there is a need to have a method to identify specific individuals uniquely and accurately. Biometrics are seen as a technology to provide such accurate identification. There are many biometrics in use today, with the most popular being:

- Fingerprints
- Iris scans
- Retina scans
- Voice prints
- Facial features
- Hand Geometry
- Signatures

Biometrics can either be used to confirm a specific individual is who they say they are (one to one matching) or identifying an individual from their biometric data (one to many matching). Using a biometric to link an individual to an ID card is an example of one to one matching whilst the best example of one to many matching is using a fingerprint to track down a criminal.

In all walks of life the identification of the valid user is now a key issue and is being driven by increased security threats and the rising problem of identity theft. The debate about ID cards has raised the profile of biometrics as a method of user identification. This white paper looks at the use of different biometrics for user identification, how well they perform and how they may be applied.

### **Available Biometrics**

#### **Fingerprints**

A fingerprint is defined by the patterns found on a fingertip. These patterns are unique to an individual and the main use of fingerprints is by the police. There are a variety of methods for using fingerprints to identify an individual. Some emulate the traditional police method of visually matching minutiae, whilst others use pattern-matching techniques.

There are also some unusual techniques, including moiré fringe patterns or ultrasonics.

### **Iris**

The iris is the coloured ring of tissue surrounding the pupil of the eye. Again, the iris is unique to an individual. To use the iris as a biometric it needs to be scanned by a device similar to a camera. An iris scan can then be matched against a library of templates to identify or authenticate an individual.

### **Retina**

The retina biometric is based on the analysis of the blood vessels at the back of the eye which are again unique to the individual. To take a retina scan, a low intensity light is used to capture the unique patterns of the retina.

### **Voice**

The voice biometric is based on the frequency and/or time analysis of the voice. A template of the user's voice is taken by effectively recording the voice. As with most other biometrics the recording can be compared with a series of templates to perform the biometric check.

### **Face**

The face can be analysed by geometry of facial characteristics. The geometry is captured by taking a digital image of the face and then using software to analyse the characteristics.

### **Hand Geometry**

In the same way as the face, the geometry of a user's hand can be analysed.

### **Signature**

A signature biometric can be based on the image of the signature or the way it is written. A static signature biometric is solely based on image comparison, whilst dynamic analysis uses both the image and the dynamics of the signature.

## **Approaches to User Identification**

There are three different approaches to user identification:

- Something you know – a password, PIN or piece of personal information
- Something you have – a token, a swipe card, a smart card or a passport
- Something you are (a biometric) – a fingerprint, a signature or an iris scan

Often the methods are combined for increased security, for example a swipe card will also have a PIN. Such combinations are sometimes referred to as 'two factor authentication'. 'Three factor' authentication could be a smart card containing the user's biometric data that also required the user to disclose their PIN. As various methods are combined to increase security, there is a trade off between a high level of security and usability.

PINs and passwords are vulnerable to being forgotten, given away, observed by others, or otherwise obtained (social engineering). Cards can be stolen and/or forged. A combination of these can help against fraud, however, combine either with a biometric and usability as well as security is improved. This is provided that the performance and capability of the biometric technology is sufficiently high

## **Use of Biometrics in Electronic Systems**

The use of biometric identification has a number of driving factors:

- Level of security required
  - Physical environment
  - User acceptance
  - Cost
- } Performance  
} Capability

Performance of biometrics is a measurement of 'False Negatives' against 'False Positives'. A false negative is when the biometric of the correct individual is deemed to be erroneous by the system and therefore refusing legitimate entry to the system. A false positive is when the biometric of the wrong individual is identified by the system as being correct and therefore allowing illegitimate entry to the system.

Statistically 'False Positives' can never be zero, but need to be sufficiently low to meet the level of security required. The acceptable level of 'False Negatives' is generally driven by user acceptance, but is also a function of the level of security required and the physical environment the biometric identifier is performing in. As a 'rule of thumb' a level of 0-20% for false negatives is considered acceptable by most people for most electronic processes, providing this results in close to 0% within a few authorisation attempts.

In the past it has proved difficult to produce biometric identification solutions with adequate performance within a cost to enable ubiquity of use. As a result, biometric identification has been used for specialised purposes, and most commonplace electronic user identification is implemented by giving users an ID and a password or PIN.

PINs and passwords offer minimal levels of security and are often changed on a regular basis to increase security. However this further increases the occurrence of passwords and PINs being forgotten, with it being well reported that IT help desk time is dominated by re-setting passwords.

More importantly PINs and passwords get given away. A recent survey revealed that 7 out of 10 users asked at a London railway station gave out their passwords in return for a bar of chocolate. PINs and passwords are also open to being stolen; especially if they are written down to avoid forgetting them. PINs are particularly subject to 'over the shoulder' gazing and capture by criminals. All these factors have driven the electronic biometric identification developers to drive performance up and cost down, to establish common use of biometric identification for all electronic processes.

The general increasing awareness of security and the rising problem of identity theft has meant that biometrics are now seen as the preferred method of user identification in electronic systems, and are being seriously considered in many environments. This, linked with improvements in biometric technology, means that biometrics as part of an electronic system is now a reality.

For any biometric a major issue is that of user acceptance. In a recent Mori poll 4 out of 5 users expressed a preference to use biometrics instead of passwords. This is driven by the myriad of passwords and PINs we each have to remember. However, there still are cultural and environmental issues on the selection of particular types of biometrics. Generally people will associate fingerprints with law enforcement rather than everyday identification. Some cultures object to physical contact to devices (like fingerprint readers) that are used by the general public.

Some physical environments also make the selection of biometric identification restricted. For example, in healthcare where many processes are performed with individuals wearing gloves, fingerprints are not practical. In noisy environments voice recognition proves very difficult. Poorly lit environments make facial recognition difficult.

## **Comparison of Biometrics for Electronic User Identity**

It is useful to look in more detail at some of the more common biometrics being considered for incorporation into the electronic identification processes. In some cases, for example the UK Identity Card, a combination of biometrics is being considered. Such approaches aim to overcome environmental and usability issues, while maintaining acceptable security levels.

### **Fingerprints**

Fingerprints are often seen as the optimal biometric because of their wide acceptance of uniqueness. Fingerprints used for law enforcement identification use all fingers and a 'rolled' fingerprint. This provides maximum data input for analysis comparison. Commercial fingerprint readers and solutions generally do not use all fingers or a 'rolled image'. Such readers have now been incorporated in a range of devices including keyboards, mice and Personal Digital Assistants (PDAs). This approach lowers the cost but does decrease the performance in comparison with law

enforcement solutions. For example, most commercial solutions suffer from problems with finger orientation. Many devices will suffer from dirty environments and generally deteriorate in performance as users leave dirt on the reader.

## **Where fingerprints fail**

In terms of the number of products available, fingerprints must be considered as the leading biometric. However, due to criminal justice implications, fingerprints have certain connotations which make some users wary. On a more practical note there are certain environments, such as hospitals where gloves are worn, where fingerprints are not practical. Also, about 2% of the world population have problems with fingerprint systems as their prints have become worn due to manual labour or their patterns are too small to recognise.

Fingerprints also do not provide a clear intention to authorise because that can be obtained from latent prints left on objects or forced onto readers by un-authorized users. More gruesomely many readers do not check for a 'live' finger.



Tsutomu Matsumoto a Japanese cryptographer along with his students at the Yokohama National University published a paper in January 2002, showing that they could reliably fool 11 commercially available fingerprint readers, with both optical and capacitive sensors, and some with "live finger detection" features – 80% of the time with artificial fingers made out of gelatine. These are sometimes referred to as "Gummy Fingers". He first of all gained the cooperation of users to mould their fingers. Later his trial lifted latent fingerprints from glasses, etc. (Just like police do at a scene of crime.), and using simple enhancement, digital photography, and PC photo software and printing was able to etch the fingerprint onto copper to then create a mould.

## **Fooling the fingerprint reader**

A team of journalists at the European computer magazine C'T tested nine fingerprint readers. The team were able to fool them all with a variety of methods.



- Breathing on readers can re-activate the last latent

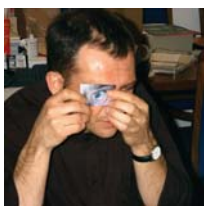


- Simply pressing a copy of a latent can fool some readers
- Water in a bag being pressed can re-activate the last latent

All of these approaches were not sophisticated attacks from professionals. Although Tsutomu Matsumoto is a cryptographer, he didn't have to use any challenging crypto-analysis to gain access. This work showed that fingerprint readers will often need to be in controlled environments to ensure they are not being fooled, or combined with additional ID methods to form 2 or 3 factor authentication.

## **Iris**

Iris scanners are coming down in price, opening up their consideration, yet the infrastructure costs for associated workflow processes would still be prohibitive. Environmental lighting and user positioning are important factors in performance. Physical characteristics of the population also have an effect. Dark iris colour intensity can affect the ability to correctly distinguish pattern markings, along with the use of coloured or tinted contact lenses. Long eyelashes can make the iris less visible. Enrolment difficulties together with user acceptance are the important factors in adoption.



- Again the computer magazine C'T team, while testing fingerprint readers checked out one Iris scanner, and was able to fool it using a simple photo with a hole cut for the pupil.

## **Face**

Facial recognition probably has greatest user acceptance because many of us already have photographs in passports, driving licenses, or on employee ID cards. However, facial biometric identification solutions are susceptible to environmental problems such as lighting and positioning of cameras. They also have great difficulty in handling our everyday changes in appearance, such as cosmetics, hats, earrings, hair, glasses, beards, etc. Performance issues can lead to poor user experience and general distrust. Facial recognition also deteriorates over time due to the natural process of aging. It is estimated that there is on average a 5% drop in accuracy per year due to aging. This means that regular annual registrations would have to take place.



- Facial recognition was simply fooled by the team at C'T magazine by the simple replay of a video clip.

## **Voice**

This would appear an obvious choice of biometric where microphones are already part of the electronic infrastructure (e.g. Mobile phones, PDAs, and PCs). However, the quality of data captured by such devices is poor, making exploitation of the voice as a biometric difficult. To overcome this, current voice biometric solutions use additional higher quality sound equipment, raising the infrastructure costs.

The performance of all voice biometric solutions is influenced by environmental background noise, making their deployment restricted. With commercial levels of computer power, voice verification has to be combined with a PIN or pass phrase to provide recognition. This means they are susceptible to misspoken phrases. They are also susceptible to conditions of poor health (colds, laryngitis), breathlessness, stress, etc.

## **Signature**

Signatures are not universally accepted as a biometric because of their individual variability and the thought that they can easily be forged. In the paper world only the static image is ever checked and such checking has difficulty in distinguishing from an individual's variability in signing and a forger's attempt to impersonate.

A handwriting expert with closer analysis is able to deduce an individual's manner of signing and therefore eliminate attempted forgery.

By capturing an individual's signature electronically the manner of an individual signing (the dynamics) can be exploited and signatures used as a true biometric.

Signatures are a natural choice that is already used in the paper world and can be exploited electronically to provide the correct level of performance for a significant number of purposes and processes. This is especially true where the biometric signature is to be used where devices themselves are built around their electronic inking capability (i.e. PDAs, Tablet PCs, or electronic scribble pads) and the biometric is replacing the wet ink signature.

Users see the process remaining the same, yet the digital authentication and electronic capture of associated data provides the organisation improved efficiencies.

## **KeCrypt Biometric Signature**

KeCrypt Signature verification analyses a handwritten signature produced on a touch screen or pad as a conventional waveform, extracting certain parameters of this waveform and assigning them numeric values in order to build a set of software filters. These filters then provide the first stage in authenticating any subsequent specimens of the signature.

KeCrypt does not convert the signature itself to any time, frequency, or spatial-normalised template for use in techniques such as DTW (Dynamic Time Warping) or HMM (Hidden Markov Model) analysis. The filters record data which state how much a given part of a given signature is allowed to vary. The variability of any particular signature heuristic is based upon standard deviation around the mean of the calibration samples. Thus filters for each signature variable measured are set.

The filter data, therefore, may not be used to reconstitute any part of the signature. Unlike competitive biometric products, KeCrypt does not store a template, and therefore the signature **cannot** be replicated.

The KeCrypt biometric signature solution provides significant advantages:

- Nothing is stored that can reveal a user's signature
- The authentication process cannot be reversed
- It is not dependent on the user's written language.
- Registration of signatures are automatically optimised to obtain the best balance between security and usability

## **KeCrypt User Trial in the NHS**

To assess the viability of the KeCrypt signature verification in a working environment a trial was carried out in the pharmacy departments of a number of London hospitals. Within a pharmacy and prescribing environment a signature is used to authorise a wide range of activities. The trial confirmed that the KeCrypt biometric signature has a high level of user acceptance. The trial also showed that KeCrypt signature verification was as successful as fingerprint recognition when compared with results from the Government's recent National ID trial. More importantly, all attempted forgeries were rejected by the KeCrypt system.

### **Comparison of KeCrypt Performance with National ID Trial**

	<b>Success Rate</b>	<b>Comment</b>
KeCrypt Signature	81.7%	No forgeries accepted
Fingerprints	82.3%	-
Iris Scans	98.8%	12% failed to register
Facial Scans	69.2%	-

The trial results show that **KeCrypt verification of signatures** can deliver a similar level of performance to fingerprints and is readily accepted by

users. Given this comparable performance, the KeCrypt signature biometric has the following advantages over the fingerprint:

- The signature is the most natural method of authentication and authorisation
- A signature demonstrates intention to authorise. Fingerprints can be taken from a latent and replicated
- The KeCrypt signature biometric works entirely on the dynamics of the way that the signature is written, making it extremely difficult to forge
- The KeCrypt signature biometric means that template images do not have to be encrypted and managed, making personal biometric data secure from compromise.

## **Conclusions**

Overall there is no one biometric suitable for all applications and the wider the user group the more difficult the problem becomes. This is born out by the early trials of the UK identity card where three types of biometric were tested.

Although the commercial adoption of biometrics is relatively new there are already a range of successful biometric projects. Trials clearly test the performance of the biometric against the original objectives, and most importantly establish user acceptance. If the right biometric is used and introduced properly then users respond well to the benefits. When fingerprint scanners were introduced at a border crossing where workers had to cross on a daily basis users enjoyed the benefit of reduced lost time travelling to and from work.

Electronic ID cards are being introduced in the UK and examined in many other countries for a variety of reasons – aid against terrorism, entitlement to benefits, access to government (local and central) services. These may or may not achieve their objectives, but once introduced they will contain electronic biometric information coupled with other identity information that could enhance a range of commercial processes thus bring everyday benefits to the users.

User acceptability is essential to the wide adoption of commercial (and governmental) use of electronic biometric identification. Signatures are a natural choice that is already familiar to the general public. Signatures unlike many of the other biometrics show intent and are therefore very applicable for transaction authorisation. The KeCrypt biometric signature solution provides the following advantages:

- Nothing is stored that can reveal a user's signature
- The authentication process cannot be reversed
- It is not dependent on the user's written language.
- Registration of signatures are automatically optimised to obtain the best balance between security and usability

## **About KeCrypt Systems**

KeCrypt Systems is the UK's leading biometric signature security company focusing on Identity Management. The KeCrypt Solution is unique in identity management in providing a user verification process that's impossible to fake, fool or forge.

KeCrypt Signature is available to Developers as a simple plug-in. If you would like more information on a Partnership with KeCrypt, please email us on [sales@kecrypt.com](mailto:sales@kecrypt.com)

### **KeCrypt Systems Limited**

Business & Technology Centre

Bessemer Drive

Stevenage

Hertfordshire SG1 2DX

UK

Tel: +44 (0)1438 791026

Fax: +44(0)1438 791086

Website: [www.kecrypt.com](http://www.kecrypt.com)