

# Biometrics - A Perspective and a Case Study

Michael A Pepper MSc CPP PSP

(First Published in New Zealand Security, April/May 2002)

*The views expressed in this article are those of the author and do not necessarily represent the views of the Northern Ireland Prison Service or the UK Government Biometrics Working Group.*

## Introduction

I was delighted to be asked to write an article on the subject of biometrics. Having migrated from the UK less than a year ago, I cannot really comment on the use of biometrics in New Zealand so all I can do is confine my comments to personal experience elsewhere.

I have, of course, asked around. I have been met with responses ranging from the "Sorry, don't know anything about it" to "Yes, I have come across biometrics, but they don't work very well." If the responses I have received are typical, then there would seem to be a dearth of information around the security industry. This is not a unique phenomenon or a criticism. I have met with such responses in the UK as well. All sorts of claims are made about the capabilities of the different systems in the marketplace and the end user has a really difficult time deciding which system is the best for a particular application. Organisations such as banks and government security agencies have a need for complete assurance about a person's identity and very often find themselves wrestling with the question, "What is the best system?" Even after scientific testing, no independent organisation is likely to commit itself to a definitive answer. I have come across a range of products that have shown great promise, and, whilst I have seen real success with a particular system in one environment, attempts to use the same system elsewhere has been doomed to failure. Some of the reasons why will be explored later. Before moving on to discuss my experience with biometrics, I need to offer a definition so that the uninitiated can gain some understanding of what the subject matter is about.

## What's it all about ? (The tekky bit)

Biometrics is not a new subject. The nineteenth and early twentieth centuries saw a range of efforts to classify people through measurements of the skull, limbs and extremities so that those with criminal tendencies might be identified from their physical characteristics. Such ideas became generally discredited, however, it was recognised that some measurements could be used to distinguish one person from another. For example, fingerprints have for decades been the primary method of identification accepted by courts of law. So what is biometrics? The Association for Biometrics (UK) (see <http://www.afb.org.uk/>) defines it as " A measurable, physical characteristic or personal behavioural trait used to recognise the identity, or verify the claimed identity, of an enrollee". The Biometrics Consortium (USA) (see <http://www.biometrics.org/>) offers a narrow definition, "Automatically recognizing a person using distinguishing traits". I prefer the AfB definition as it more accurately describes the two main applications of biometrics today, namely identification and

identity verification. I will deal with the difference between the two later. What has changed things dramatically is the technology that has become available in recent years that makes the use of biometrics, in whatever form, a speedy and often highly reliable means of confirming identity.

The systems around today cover measurement of just about anything. Each claims that no two people have exactly the same characteristics, whether these be ears, iris, retina, hand geometry, finger geometry, fingerprint, handwriting, face, voice, hand veins or even keyboard typing rhythm. Some systems actually rely on more than one feature. The manufacturer of each system is well able to demonstrate that theirs has a False Accept Rate (FAR) or a False Reject Rate (FRR) of whatever figure. What they don't often admit to is the size of the test population, whether they were all of the same ethnic background and just what was the recognition threshold (adjustable on most systems). Furthermore, because of the plethora of systems, and the fact that even similar systems employ different algorithms and software, there is as yet no standard test methodology that allows true comparison of one against another. The systems with which I am most familiar are hand geometry, fingerprint, dynamic signature, iris pattern and facial recognition. I am loath to suggest that any one is better than another; it all depends on one's definition of "better". Each has its own characteristics and as I have suggested already, a system may perform perfectly well in one environment but fail abysmally in another. The security manager of a government installation may well be quite happy with the odd false reject as long as there are no false accepts. Banks on the other hand, are likely to be very concerned if their system annoys customers by incorrectly rejecting their access attempts.

Now to clarify the difference between identification and identity verification. Identification is often referred to as a 'one to many' comparison or a 'cold search'. The subject's characteristic, for example a fingerprint or face, will be examined against the contents of a database without the need for presentation of a token, such as an access card or PIN. Identification systems can be either positive or negative. In some applications it is necessary to prove that the subject is not contained in the database, for example, to ensure that a person has not already been enrolled or is not included in a database of known criminals. With identity verification or 'one to one' comparison, the subject will present a token that says, "This is who I say I am". The system will call up the relevant template for that token and compare it with the 'live' characteristic presented, for example, a hand or a signature. Generally, identity verification systems operate much faster than identification systems because of the reduced search times.

### **Hey, I want one of those! (But wait just a minute!)**

There are a number of points to bear in mind before proceeding down the road of acquiring a biometrics system. Always ask, "Why do I need a biometrics system at all?" It may seem an odd question, however it should be borne in mind that such systems do not come cheap, although prices are considerably less than they were a few years ago. Also, the high levels of administration and maintenance sometimes required are not obvious at the outset. The answer really depends upon the level of security that is needed. If your existing access control system is well managed and the risk to business through compromise of an access card or PIN is low, then

biometrics is not for you. It has to be accepted that access cards can be stolen (or given away) and a PIN or password is only as good as the piece of paper its not supposed to be written on. If, however, the risk to business through unauthorised access is truly high and you **really** need to know that the person gaining access is your trusted employee and not some impostor, then either employ static guards to check identity or invest in a biometrics system.

Never be blinded by the sexiness of the technology. A vendor may give a perfectly good demonstration in a specific environment with a very small number of people enrolled on the system. Suddenly, when you purchase and install your new toy, you find it doesn't deliver what you expected. It operates too slowly for your hundreds of employees who need to enter your premises by 8am every day or your intended users cannot or will not use the system properly. For example, it might just be a little imprudent to install a voice recognition system in a steel mill or facial recognition in a location that is subject to variable lighting levels.

Also, it is vital to consider the legality of the intended purpose and whether you are likely to fall foul of privacy legislation. Can you legitimately maintain a database containing biometric templates of members of the public? What about cultural issues? Some cultures may have an aversion to touching a reader that has been handled by others, whilst facial recognition is unlikely to find universal success in societies accustomed to wearing veils.

I could go on and on, but I want to provide some detail about a successful use of biometrics in a high security environment. For those interested in exploring the types of issue to be considered prior to procurement, really good advice is available from the UK Government's Biometrics Working Group (BWG) web site located at <http://www.cesg.gov.uk/technology/biometrics>.

### **The Case Study (the bit you have been waiting for!)**

I achieved real success with the installation of a system in a maximum security prison, although I did not choose the product as a result of some scientific research methodology. The simple reason for this is that a small field trial over a period of a few months produced a highly enthusiastic response from the target user group (prison officers). Following the advice of BWG about knowing your users led me to conclude that there was little point in moving away from a product that had gained instant respect and affection. The system used was the ID3D HandKey manufactured by Recognition Systems Inc., now a subsidiary of the Ingersoll-Rand Corporation. Other products including Facelt (facial recognition), Countermatch (dynamic signature verification), IrisScan (iris pattern recognition) and Veriprox (fingerprint) had been evaluated, but not deployed on field trials for a host of reasons. It was known that attempts by the Prison Service of England and Wales to use the ID3D HandKey as a means of verifying the identity of visitors to inmates had met with limited success. Visitors just did not like using it. By contrast, and quite surprisingly, they actually preferred to use fingerprint readers, which have now become the standard means of visitor identity verification in several prisons across the UK. Different strokes as they say.

In the case of the Northern Ireland Prison Service, the trial consisted of the use of a stand-alone unit utilised by prison staff in a low security environment. That initial success led to deployment of more stand-alone units in both low and medium security areas over a period of two to three years. It was at about that time I had a rather novel idea. What was novel, from the point of view of a prison service long used to placing static guards at key access points, was the suggestion that a network of hand geometry readers could replace prison officers in a maximum security prison, improving security and reducing costs at the same time. To say that there were a few raised eyebrows is something of an understatement. I had some convincing to do. In an environment where reducing costs always featured as part of a manager's life, it was simple arithmetic. A prison officer cost at least £25,000 per year. Two hand readers and a control panel on each access point cost around £6,000. No hard sell there, I thought. All I had to do was prove that the system would work. At the same time, I was given the task of coming up with a new staff identity card production system. The challenge for me was to combine the two systems.

A working prototype was built which comprised of two hand readers, Wiegand card readers and a full height turnstile (purchased second hand from a local electricity generating company). The system was demonstrated to senior managers who were suitably impressed, not only with the operation of the system, but also with the fact that it could potentially pay for itself in two years through staff efficiencies. Additional benefits included highly visual evidence of enhanced security, reducing the number of keys in circulation, helping prevent the unauthorised removal of keys from a prison and actually speeding up the entry of staff at peak periods. It was vital to test the reactions of users, because if they proved to be negative, the project was guaranteed to fail. Several members of staff including civilians and their respective trade union representatives were invited to try the system for themselves and raise any concerns they might have. The feedback was very positive. OK, maybe I was lucky, but do bear in mind that if the people using the system have no input, you are not going anywhere.

The locations where the hand readers were to be installed had already been identified. These included the main staff entry points and a number of other gates and doors that led to the prisoner accommodation areas. Tailgating was only an issue at the main entry points and full height turnstiles were deployed to deal with this. Additionally, to ensure that only members of staff left the prison, the hand reader key pads at these locations were disabled, forcing users to swipe their new identity cards. A single enrolment point was established at the main entry gate. This required not a little ingenuity, as the prison officer enrolling a new person had to do so from behind several millimetres of bullet resistant glass in a secure area. Wiegand swipe cards were chosen instead of proximity cards, partly due to the fact that staff preferred them and partly because there was a considerable amount of metal adjacent to the card readers. I learned from experience that proximity card readers tended not to like that sort of environment. The network was run from a stand-alone PC in the prison control room using a Windows 98 platform with a range of security measures added. I could have opted for bespoke operating software but was deterred by the excessive cost. I could spend around £20,000 and have all my needs met or spend around US\$1000 and meet 95% of the requirement by running RSI's own HandNet for Windows software. It was an easy choice to make - besides I was on a budget.

Commissioning of the new system was a breeze compared to the nightmare of photographing every member of staff, issuing a new identity card and enrolling each person on a hand reader in preparation for going 'live'. That is a job that should never be underestimated, even though it only took about 5 minutes per person. Be prepared for serious delays at this point. At 9pm on a Sunday evening the system was switched on. If it failed, the start-up would be delayed for at least a week. Immediately, there was a communication problem with one of the hand readers, an old model. It would not accept the new data it was being fed. I have always been a firm believer in Murphy's Law ("if it can go wrong it will" - and it did!) and made sure there was a spare of just about everything available. All worked properly once the faulty unit was swapped out. By midnight, all the testing was complete and I had a green light for the following morning. Of course, that meant being back on site at 5.30am for the first of around 350 staff coming on duty.

It should be noted that prison officers (at least in the UK) are not exactly renowned for being terribly sympathetic when a new system fails to work, so there was a certain amount of trepidation (never mind the amount of credibility that was on the line). I need not have worried. I was truly excited at watching staff use their access cards and operate the hand readers for the first time. Only three members of staff had problems gaining access and they were asked to stand aside so that others would not be delayed. I was nearly disappointed, but all three succeeded at the second attempt. That made me happy, not exactly ecstatic, but really pleased that it all worked in the way it was intended.

In conclusion, the real message of this article is that biometrics systems can work extremely well. There are caveats of course. Know who will use the system and take account of their cultural and ethical values. Know what is likely to work in your environment by getting the vendor to tell you who, in your line of business, uses biometrics, and then go talk to them. Alternatively, be prepared to experiment - some companies are actually prepared to lend demonstration versions of the equipment for evaluation. It really is an exciting security innovation. Go for it, but only if you need to.