Overview of Biometrics:

The word Biometrics comes from the Greeks. The combination of the words *bio* meaning life and *metry* meaning to measure makes biometry. It refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. They are of interest in any area where it is important to verify the true identity of an individual. This method of identification is preferred over traditional methods involving passwords and personal identification numbers (PIN) numbers. Initially, these techniques were employed primarily in specialist high security applications; however we are now seeing their use and proposed use in a much broader range of public facing situations. With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports and driver's licenses may be forged, stolen, or lost.

Thus biometric systems of identification are enjoying a renewed interest. Various types of biometric systems are being used for real-time identification, the most popular are based on face recognition and fingerprint matching. However, there are other biometric systems that utilize iris and retinal scan, speech, facial thermo grams, and hand geometry.

Evolution of Biometrics:

Biometrics is becoming a buzzword in regards to computer and network security. However the ideas of biometrics have been around for many years. Possibly the first known example of biometrics in practice was a form of finger printing being used in China in the 14th century, as reported by explorer Joao de Barros. According to him, the Chinese merchants were stamping children's palm prints and footprints on paper with ink to distinguish the young children from one another. This is one of the earliest known cases of biometrics in use and is still being used today.

In the 1890s, an anthropologist named Alphonse Bertillion wanted to fix the problem of identifying convicted criminals and turned biometrics into a distinct field of study. He developed 'Bertillonage', a method of bodily measurement which got named after him. The problem with identifying repeated offenders was that the criminals often gave different aliases each time they were arrested. Bertillion realized that even if names changed, even if a person cut his hair or put on weight, certain elements of the body remained fixed, such as the size of the skull or the length of their fingers. His system was used by police authorities throughout the world, until it quickly

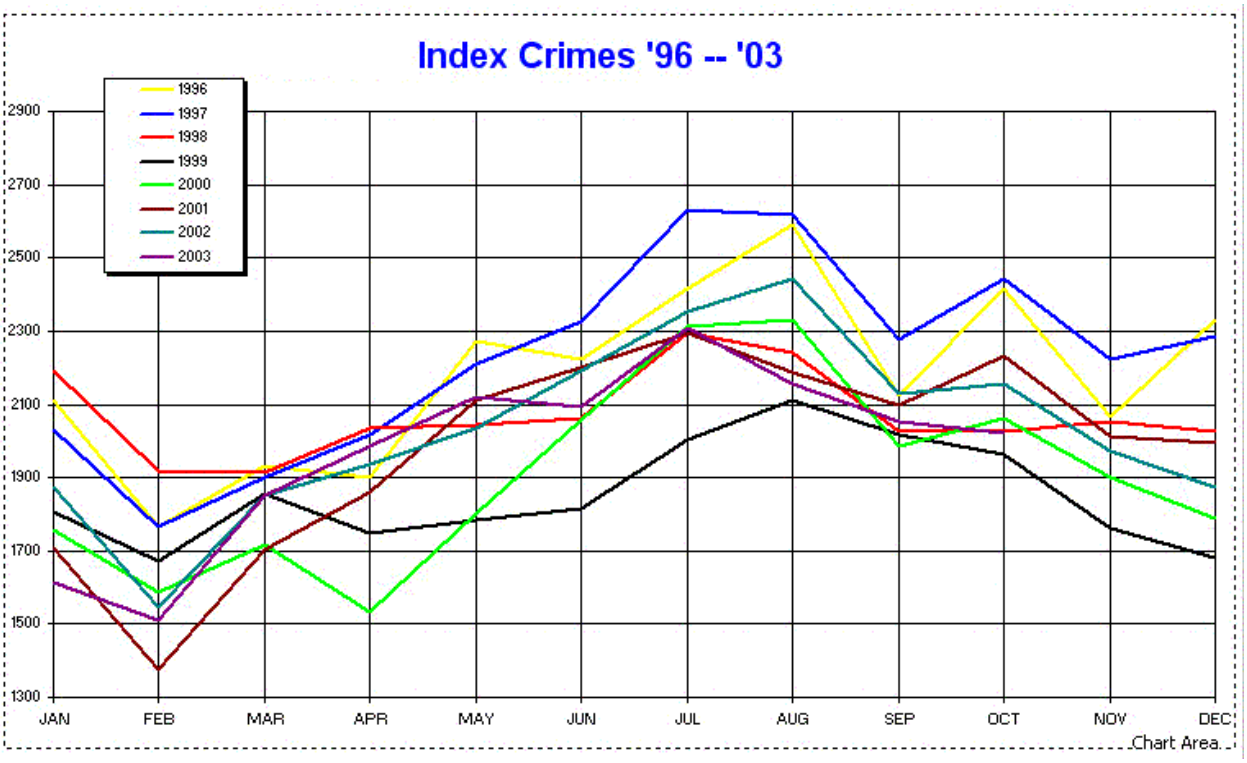
faded when it was discovered that some people shared the same measurements and based on the measurements alone, two people could get treated as one.

This system was a huge breakthrough and was adopted by prisons and police stations across the country and world, though it did have some drawbacks. For instance, some large cities had huge databases of cards, and sorting and searching for a particular card could take days. Another drawback was that anthropometrical signalment was found not to be a totally unique biometric. This was discovered when they found that some people shared the same measurements

After this, the police used finger printing, which was developed by Richard Edward Henry of Scotland Yard, instead. Essentially reverting to the same methods used by the Chinese for years. However the idea of biometrics as a field of study with useful identification applications was there and interest in it has grown. Today we have the technology to realize the aims, and to refine the accuracy of biometric identification, and therefore the possibility of making it a viable field.

Need of Biometrics:

Pin's (personal identification numbers) were one of the first identifiers to offer automated recognition. However, it should be understood that this means recognition of the PIN, not necessarily recognition of the person who has provided it. The same applies with cards and other tokens. We may easily recognize the token, but it could be presented by anybody. Using the two together provides a slightly higher confidence level, but this is still easily compromised if one is determined to do so.



A biometric however cannot be easily transferred between individuals (replacement part surgery is outside the scope of this paper) and represents as unique an identifier as we are likely to see. If

we can automate the verification procedure in a user friendly manner, there is considerable scope for integrating biometrics into a variety of processes.

Identification and Authentication:

You will often come across the terms '*verification*' and '*authentication*' which are sometimes confused when people are discussing biometrics.

This is perhaps the most important aspect of the definition of biometrics, because the products associated with each category are vastly different.

Authentication

The majority of available devices operate in authentication mode. Authentication occurs when an individual makes a claim of identity by

Presenting a code or a card. Called a "one-to-one" search, the question put to the machine is "Are you who you claim to be?" In this sense, the individual's characteristics are being measured against an enrolled image that is stored on a token or in a local database with the

image presented. These types of products costs between $100 and $3,000 and are used in applications including physical access control and logical access control. Because the person presenting him or herself for authentication presents a PIN or password as an index, the search time and subsequent authentication are much faster than its counterpart where 100,000 matches are made in a second; an authentication occurs in a millisecond.

Identification:

Identification occurs when an individual's characteristics are being selected from a group of stored images. Called a "one-to-many" search, the question put to the machine is "Do I know you?" The search algorithm will search a database and return a likely list of candidates in a matter of minutes. A more complex one to many match which may generate a multiple result according to the number and similarity of stored templates. These types of products can cost between $40,000 and $1 million depending on the configuration. The most popular application for identification devices is law enforcement. These AFIS (automated fingerprint identification system) systems can perform over 100,000 fingerprint match attempts in a second.

For various reasons, one should exercise extreme caution when considering biometric 'identification' systems. Even as one can readily understand the attraction of this mode of operation, it has to date rarely been successful in practice, except in small scale carefully controlled

situations. Verification systems on the other hand are straightforward in operation and may easily be deployed within a broad cross section of applications, as indeed has been the case.

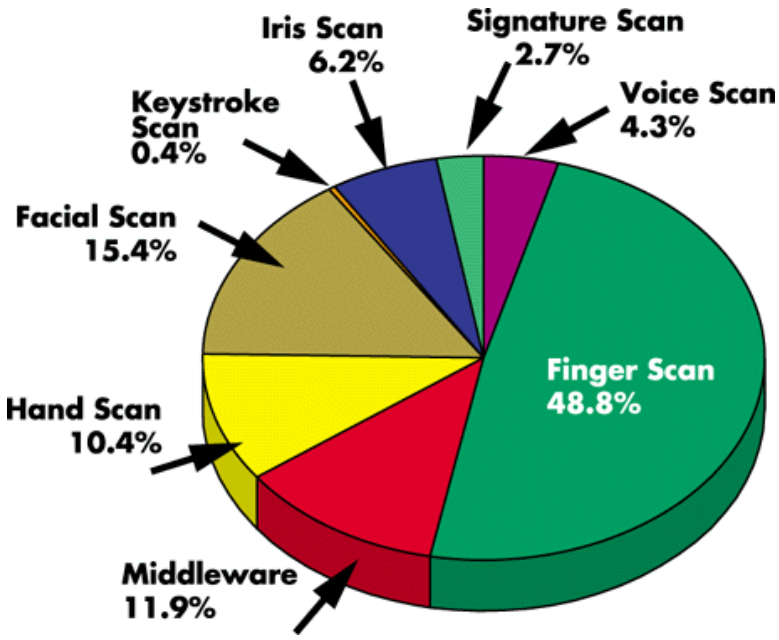
Popular Biometric Methodologies ~ what are they?

You will see reference to a number of biometrics, some of which are rather impractical even if technically interesting. The 'popular' biometrics seems to gravitate at present around the following methodologies.

Fingerprint verification:

Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. The stability and uniqueness of the fingerprint are well established. Upon careful examination, it is estimated that the chance of two people, including twins, having the same print is less than one in a billion. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

There are a variety of approaches to fingerprint verification. Some of them try to emulate the traditional police method of matching minutiae, others are straight pattern matching devices, and some adopt a unique approach all of their own, including moiré fringe patterns and ultrasonic. .



Some of them can detect when a live finger is presented, some cannot. There is a greater variety of fingerprint devices available than any other biometric at presentPotentially capable of good accuracy (low instances of false acceptance) fingerprint devices can also suffer from usage errors among insufficiently disciplined users (higher instances of false rejection) such as might be the case with large user bases. One must also consider the transducer / user interface and how this would be affected by large scale usage in a variety of environments. Fingerprint verification may be a good choice for in house systems where adequate explanation and training can be provided to users and where the system is operated within a controlled environment. It is not surprising that the workstation access application area seems to be based almost exclusively around fingerprints, due to the relatively low cost, small size (easily integrated into keyboards) and ease of integration.

Hand geometry:

As the name suggests, hand geometry is concerned with measuring the physical characteristics of the users hand and fingers, from a three dimensional perspective in the case of the leading product. One of the most established methodologies, hand geometry offers a good balance of performance characteristics and is relatively easy to use. This methodology may be suitable where we have larger user bases or users 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. Hand geometry readers are deployed in a wide range of scenarios, including time and attendance recording where they have proved extremely popular. Ease of integration into other systems and processes, coupled to ease of use makes hand geometry an obvious first step for many biometric projects.

Hand geometry is employed at over 8,000 locations, including the Colombian legislature, San Francisco International Airport, day care centers, a sperm bank, welfare agencies, hospitals and immigration facilities for the INSPASS frequent international traveler system.

Voice verification:

A potentially interesting technique bearing in mind how much voice communication takes place with regard to everyday business transactions. Voice verification is a very attractive biometric approach because of its acceptability to users. There are several approaches to analyzing the voice, although all systems are rooted in broader based speech processing technology. Some designs have concentrated on wall mounted readers whilst others have sought to integrate voice verification into conventional telephone handsets. Even if there have been a number of voice verification products introduced to the market, many of them have suffered in practice due to the variability of both transducers and local acoustics. In addition, the enrolment procedure has often been more complicated than with other biometrics leading to the perception of voice verification as unfriendly in some quarters. However, much work has been and continues to be undertaken in this context and it will be interesting to monitor progress accordingly.

Several large organizations, including AT&T, ITT, France Telecom, Bellcore, Texas Instruments, and Siemens, have developed verification algorithms for communications applications. A common question about voice systems is impersonations. This is not a serious problem, because the devices purposely focus on different characteristics of speech than people do.

Retinal scanning:

An established technology where the unique patterns of the retina are scanned by a low intensity light source via an optical coupler. Retinal scanning has proved to be quite accurate in use but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient if you are a spectacle wearer or have concerns about intimate contact with the reading device. For these reasons retinal scanning has a few user acceptance problems although the technology itself can work well. The leading product underwent a redesign in the mid nineties, providing enhanced connectivity and an improved user interface; however this is still a relatively marginal biometric technology.

Iris recognition:

Iris scanning is undoubtedly the less intrusive of the eye related biometrics. It utilizes a fairly conventional ccd camera element and requires no intimate contact between user and reader. In addition it has the potential for higher than average template matching performance. As a technology it has attracted the attention of various third party integrators and one would expect to see additional products launched in due course as a result. It has been demonstrated to work with spectacles in place and with a variety of ethnic groups and is one of the few devices which can work well in identification mode. Ease of use and system integration have not traditionally been strong points with the iris scanning devices, but we can expect to see improvements in these areas as new products are introduced.

Signature verification:

Signature verification enjoys a synergy with existing processes that other biometrics do not. People are used to signatures as a means of transaction related identity verification and would mostly see nothing unusual in extending this to encompass biometrics. Signature verification devices have proved to be reasonably accurate in operation and obviously lend themselves to applications where the signature is an accepted identifier. Curiously, there have been relatively few significant applications to date in comparison with other biometric methodologies. If your application fits, it is a technology worth considering, although signature verification vendors have tended to have a somewhat chequered history.

Facial recognition:

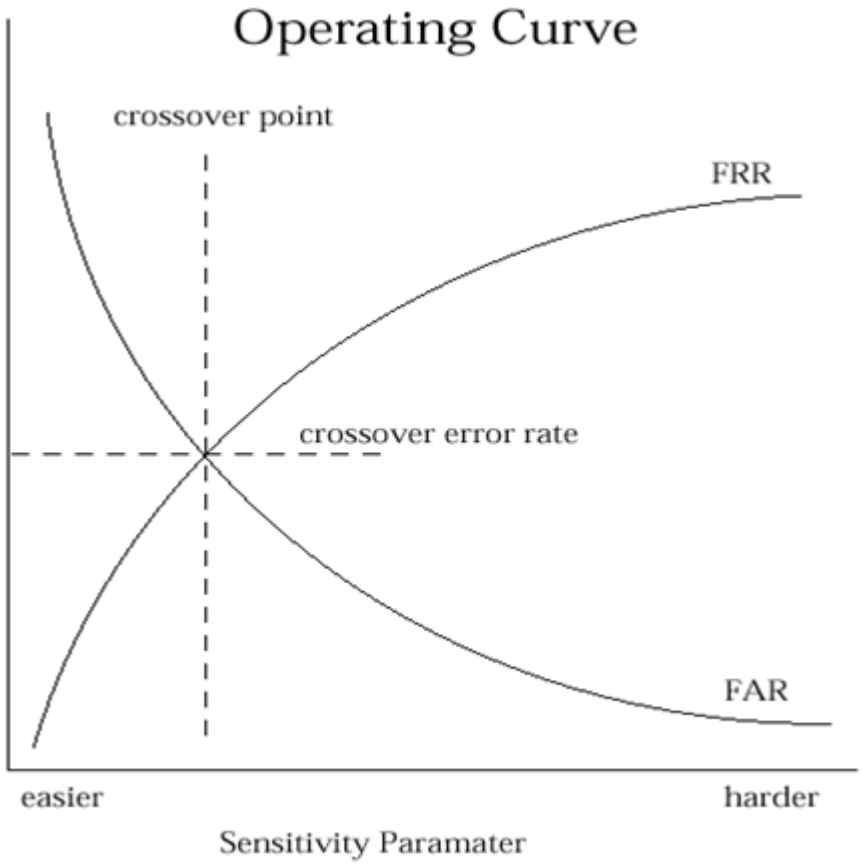
A technique which has attracted considerable interest and whose capabilities have often been misunderstood. Extravagant claims have sometimes been made for facial recognition devices which have been difficult if not impossible to substantiate in practice. It is one thing to match two static images (all that some systems actually do - not in fact biometrics at all), it is quite another to unobtrusively detect and verify the identity of an individual within a group (as some systems claim). It is easy to understand the attractiveness of facial recognition from the user perspective, but one needs to be realistic in ones expectations of the technology. To date, facial recognition systems have had limited success in practical applications. However, progress continues to be made in this area and it will be interesting to see how future implementations perform. If technical obstacles can be overcome, we may eventually see facial recognition become a primary biometric methodology.

There are other biometric methodologies including the use of scent, sear 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. Those listed above represent the majority interest and would be a good starting place for you to consider within your biometric project. The sections of this paper dealing with performance issues and user psychology offer a further insight into the application of these devices.

Performance Measures: What do they really mean?

False accepts, false rejects, equal error rates, enrolment and verification times - these are the typical performance measures quoted by device vendors. But what do they really mean? Are these performance statistics actually realized in real systems implementations? Can we accept them with any degree of confidence?

The terms that define ID Power are a slippery pair known as False Rejection Rate (FRR), or Type I Error, and False Acceptance Rate (FAR), or Type II Error. False accept rates (FAR) indicate the likelihood that an impostor may be falsely accepted by the system. False reject rates (FRR) indicate the likelihood that the genuine user may be rejected by the system. This measure of template matching can often be manipulated by the setting of a threshold which will bias the device towards one situation or the other. Hence one may bias the device towards a larger number of false accepts but a smaller number of false rejects (user friendly) or a larger number of false rejects but a smaller number of false accepts (user unfriendly), the two parameters being mutually exclusive.



Advantages of biometrics:

Biometrics is the only way to automatically confirm the presence of the correct person! As such, biometrics is the essential tool for use whenever it is necessary to accurately recognize the individual. A tool that provides an automatic audit of *WHO* did *WHAT*, *WHERE* and *WHEN*!

There are many business benefits to be gained from using Biometric technology. We believe that an assessment of your organization's specific situation with regard to the use of biometric technology is the best way to realize the business benefits of installing such technology.

- Provide a convenient and low-cost additional tier of security.
- Reduce password administration costs.
- Prevent unauthorized use of lost, stolen or “borrowed” ID cards.
- Unequivocally link an individual to a transaction or event.
- Replace hard-to-remember passwords which may be shared or observed.
- Minimize the opportunity for ID fraud.
- Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN!

Implementing biometrics:

There are a very large number of relatively small security related applications undertaken by specialist security systems suppliers. These systems account for the majority of unit sales as far as the device manufacturers are concerned and are often supplied via a third party distribution chain.

The most applications of biometrics are those in the public domain. These include:

- Prison visitor systems, where visitors to inmates are subject to verification procedures in order that identities may not be swapped during the visit - a familiar occurrence among prisons worldwide.
- Drivers licenses, whereby some authorities found that drivers (particularly truck drivers) had multiple licenses or swapped licenses among themselves when crossing state lines or national borders.
- Canteen administration, particularly on campus where subsidized meals are available to bona fide students, a system which was being heavily abused in some areas.
- Benefit payment systems. In America, several states have saved significant amounts of money by implementing biometric verification procedures. Not surprisingly, the numbers of individuals claiming benefit has dropped dramatically in the process, validating the systems as an effective deterrent against multiple claims.

- Border control. A notable example being the INSPASS trial in America where travelers were issued with a card enabling them to use the strategically based biometric terminals and bypass long immigration queues. There are other pilot systems operating in S.E. Asia and elsewhere in this respect.

Case study:

Biometrics: Critical tool for Comsat Max's growth

As a company that hosts, protects and manages servers of the corporate sector, Comsat Max has to ensure that its own server rooms are completely secure.

Comsat Max, traditionally a VSAT service provider, introduced a solution called HPDM (host, protect, deliver and manage) to offer cost-effective IT infrastructure management services to its customers. Positioning itself to become the No. 1 outsourced IT and communication infrastructure Internet solutions provider, Comsat decided to set up a facility which could help deliver the HPDM model in a secure manner.

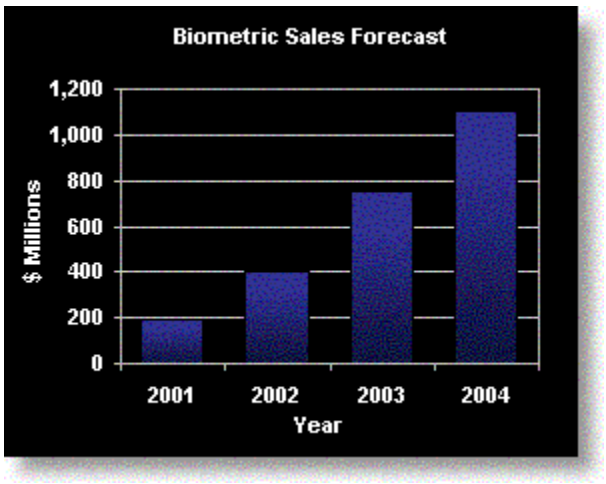
To ensure complete protection of its client data, Comsat designed multiple security layers, resulting in a narrowed access. These layers varied from physical security checks, access control to biometricsThe entry to the server room and the surveillance room is through smart cards, with each card allowing entry to only certain authorized areas. The two server rooms—one consisting of the Comsat Max/non-militarized zone, and the other the co-location/militarissszed zone—are further secured through a biometrics solution.

The co-location is totally barred for other employees. The entry in the militarised zone is restricted to only two individuals, who also have to take permission from the company before entering the area. And whatever communication happens is through the Comsat server in the non-militarised zone. In the militarised zone unless and until the first door closes the other doors do not open. In case an individual leaves the door open, his card gets blocked. All this is to ensure a perfect secured environment for our customer. For both the zones the entry is through swipe cards and fingerprint recognition solutions. Employees are given a card that stores their fingerprint template in a two-dimensional bar code, or on the single track of a magnetic strip. Whenever a person's identity needs to be verified, the card is presented and the barcode scanned. The fingerprint is automatically loaded into a verification unit and compared to the one on the template. While the standard access control and identification could be hampered with through defrauding the identification cards, or by using other person's PIN number or by simply borrowing a card, biometrics provides a solution which is almost full-proof, since people cannot replicate fingerprints. The company has opted for a fingerprint evaluation solution called Verid, offered by TSSI.

The biometrics solution is platform independent, and the PIN and door controls run on Windows 2000 workstation.

According to Joyjit Chatterjee, general manager, marketing and sales, Comsat Max, this solution provides a very cost-effective way of controlling entry to premises. According to him, the reason why Comsat Max has gone for multiple layers of security, is not only to provide a comfort level for the customer, but also to ensure maximum precaution on its part. The company is extremely satisfied with the solution, and is planning on deploying it for its upcoming facility in other centers.

What does future hold for biometrics?



Like the perennial bridesmaid hoping to find her perfect match, makers of biometrics technology continue to search for easier and more cost-effective means to secure user implementation. Biometric technology is just completing its "proof of concept" stage, and will find greater use by governments and in the private sector in the coming years. Despite some big strides made in last few year's by physical recognition devices and software in building relationships with industry heavyweights such as Microsoft, IBM, Visa, and Wells Fargo, questions still linger as to the proper use and placement of biometrics. Ultimately, the technology could find its strongest role as an intertwined and complementary piece of a multifactor authentication system, rather than a stand-alone single point of defense. Companies turning to biometrics to enhance their e-business systems hope to enhance user verification while maintaining customer satisfaction and accuracy. Many of those customers are discovering that biometrics products are becoming more flexible, capable of serving different purposes, or being used in tandem, accomplishing more than authentication.

- The future applications of biometrics may include: Most of the leading banks have been experimenting with biometrics for ATM machine use and as a general means of combating card fraud.
- Travel and tourism**:** There are many in this industry that have the vision of a multi application card for travelers which, incorporating a biometric, would enable them to participate in various frequent flyer and border control systems as well as paying for their air ticket, hotel room, hire care etc., all with one convenient token.
- Public identity cards: A biometric incorporated into a multi purpose public ID card would be useful in a number of scenarios.

Conclusion:

Bibliography:

Websites:

1. www.avanti.1to1.org
2. www.biometricgroup.com
3. www.findbiometrics.com
4. www.cfo.com

5. www.biometrics.cse.msu.edu
6. www.fcw.com
7. www.school-for-champions.com
8. www.aamva.org