# Global Information Assurance Certification Paper

# Biometrics: Has its time come?

Dani Gustafson
October 31, 2000

**Introduction:**

The word biometrics basically means "bio" or life and "metrics" or measurement. So the literal translation is "life measurement". Biometrics measures the life traits of a person, this can be anything from physical measurements such as fingerprints, irises, retinas, or facial and hand measurements, to more behavioral traits of someone such as voice patterns, keystroke rhythms or even heat patterns. These can then be used to uniquely identify an individual from millions of others. This can then be incorporated into a network in many different ways and combinations to create an extremely secure system that cannot be easily circumvented.
In the beginning of the introduction of biometrics into the marketplace around 1996 or so there was much confusion and the different companies did not want to work together and share their proprietary information. Since the development of the Biometrics Consortium or BioAPI, the different companies have come together in a common goal and have really made significant strides in making biometrics a viable and reliable answer to security.
It is not only being used for the basic login, replacing the need for passwords and pin numbers, but more and more uses are being discovered to stop the flood of identity theft and fraud.
But since the time of sci-fi fantasy is now upon us, we have to look seriously at biometrics and realize that it does have some definite issues associated with the technology that need to be addressed.

**Key issues and concerns with biometrics:**

The main issues that need to be dealt with when biometrics is discussed are:

- False Rejection Rate and False Acceptance Rate
- Durability
- Ease of use
- Physical Privacy
- Information Privacy
- Religious objections

The first three issues are mainly issues with equipment and software options while the last three are social/cultural issues. Let's take at them individually.
Getting a false rejection, which is a valid user being denied access, is just as bad as getting a false acceptance, where an unauthorized person is allowed in. When you try to balance between the two, one must suffer to get a good rate in the other. As processors and technology are increasing in speed this area has been improving dramatically. In most systems now you can usually get a reliable match in less than 2 seconds, with an average

company's size database.
If the system is going to be exposed to elements or left unattended, it must be able to withstand both normal weather and temperature changes, but also the damage that can be inflicted by the general public. It must be protected in such a way that it will still function under the needed conditions. Iris scans and facial recognition are being looked at closely by the Military because of the special conditions that are needed while soldiers are in the field. This type of system can be used even when a soldier is in full biohazard gear.
Over the last decade with research in biometrics and computer technology greatly advancing the equipment issues are becoming less and less of an issue. One of the main problems in the industry as a whole was the incompatibility issue. At the end of this year the BioAPI are releasing a standard application programming interface that can be incorporated into individual companies operating systems, software and hardware so that interoperability between systems can be achieved. For example, when one banks smart card with the users fingerprint imbedded into a chip is used in another banks ATM machine with a different type of biometric reader, the fingerprint file on the original card can still be read and the users id can be securely verified.
The general consensus of the industry is the only way this technology will grow is how comfortable the user is with using the system. Not only must the device be simple to understand with no physical discomforts but also the databases created must be protected so that there is no unauthorized use.
While the user must not be compromised in any way that makes the user uncomfortable physically, such as having them hold still for a long period of time for scanning, or shining lasers in their eyes, they must also feel that data will not be misused.
This is one of the most important areas that implementers are concerned with. Government agencies, including Congress, and BioAPI (the biometrics consortium) are very aware of just how important this issue is. Just like when the issue came up for the first time over 70 years ago with wire tapping, the public is very concerned with how the government can monitor their citizens.
With biometrics, people are even more nervous with the large number of biometric databases being created and how they can be misused. Fingerprint databases are being created not only by government agencies but also by a growing number of public and private companies. People are afraid that their fingerprint can be taken from the file and be used to take their identity. But the file is actually not a fingerprint but a compressed file of minutia points from their print. A fingerprint cannot be reconstructed from these points. These concerns are being seriously addressed, but public education is the key. How and where this data is being stored and used needs to be explained in ways that anyone can understand.
One of the major ways the industry wants to store the biometric file is with the user, thus do away with the need for a database at all. Using a smart card the user can be in possession of their own information at all times. Should the card be lost the information is encoded and cannot be reproduced. Then the biometric device just compares the live image with the file given for verification. This has shown to work well, especially in Europe. This way the fear over vast shared databases is eliminated. Also it is very important that database information is not shared or compared with each other to ensure privacy. This is one specific area that can be addressed through legislature.

Also biometric devices do require live submissions, so the common scene in movies where they eyeball or finger is cut from the victim and used to bypass security can't be done. Also latent prints can't be feed into nonforensic systems. Encryption is used not only between the peripheral and the PC, but the template can be encrypted when stored. This is one of the shared protections with all biometric technologies.
Besides "Big Brother" people are also concerned with "the Mark of the Beast". Many in the religious community are concerned with prophecies in the book of Revelation coming true. But with true biometrics nothing is added to or put on anyone, but rather God given identifiers are measured.

**Conclusion: Has its time come?**

But again perception is reality; so public acceptance is the biggest hurdle that the industry faces. In Europe, this technology is being strongly embraced. It is being used by government agencies, the financial industry and many businesses. There it is looked at as providing identity security rather than an invasion of privacy. Are people in the U.S. ready to embrace biometric technology to help stop identity theft? With more and more login passwords and pin numbers needed, will people tire of trying to come up with new, different and more secure passwords that can't be cracked in less than 30 seconds? As the computer industry and the biometrics industry grows hopefully more of the concerns addressed here will be solved. Legislation and controls need to be implemented, but in a nationwide survey by Network World on 5/8/00 while only 4% of responding companies are currently using biometrics within the next 18 months 11% said they plan to add biometric authentication to their networks. So this is a rapidly growing alternative to traditional security measures.

**Reference:**

[1] Garfinkel, Simson – The Measure of Man, Discover, September, 2000
URL: http://www.findarticles.com/cf_0/m1511/9_21/64698192/print.jhtml

[2] Nickell, Joe – Biometrics Standards in Works, Wired News, April 28, 1998
URL: http://www.wired.com/news/topstories/0,1287,11937,00.html

[3] Willing, Richard – Pentagon turns to body-based ID systems, USA TODAY 6/21/00
URL: http://www.usatoday.com/news/washdc/ncswed20.htm

[4] Verton, Dan – Senate shores up DOD security, Federal Computer Week 6/5/00
URL: http://www.fcw.com/fcw/articles/2000/0605/pol-dod-06-05-00.asp

[5] Harreld, Heather – Biometrics points to greater security- Agencies eye the latest devices to verify ID's, Federal Computer Week 7/19/99
URL: http://www.fcw.com/fcw/articles/1999/FCW_071999_799.asp

[6] Weinberg, Neal – Security Survey, Network World 05/08/00

[7] Steinhardt, Barry and Nanavati, Samir, Face-off: Is the use of Biometrics and invasion of privacy? Network World, 05/08/00
URL: http://www.nwfusion.com/columnists/2000/0508faceno.html
URL: http://www.nwfusion.com/columnists/2000/0508faceyes.html