PERSONAL IDENTIFICATION AND AUTHENTICATION BY USING "THE WAY THE HEART BEATS"

Johan F. du Preez, Prof S.H. von Solms

University of Johannesburg (South-Africa)

e-mail : johan.dupreez@gmail.com

cell: +27823329434

Postal address : P.O. box 44935; Linden; Johannesburg; South-Africa; 2104

ABSTRACT

The use of current passwords and tokens (bank card) that's currently the most popular and well known mechanism for electronic identification can only identify the token or password but NOT the physical user using the token or password for identification.

Biometrics addresses exactly the above issue by being part of the physical user, for example: your fingerprint, retina or iris… BUT:

One of the biggest problem areas around Biometrics is the fact that most biometric tokens(fingerprints, hand geometry and even the human eye) can be used in some cases to identify the owner of the biometric token even after death as if the user were alive. The problem becomes apparent in the case of a person that passed away and the possibility of using the biometric tokens of the deceased to obtain access to his\her bank account.

This paper reports on the initial stages of a research project that addresses the above problem by proposing the use of biometric tokens that doesn't exist if the owner is not alive thus the paper coins the new term – Inherent Liveness Biometrics.

The way the human heart beats as a biometric token to identify or verify a person, might solve the issue of liveness testing, because "The way the human heart beats" might prove to be a natural biometric token that is only valid for a living person, it is an inherent liveness biometric.

KEY WORDS

Biometrics, Liveness-testing, Identification, Authentication, Inherent liveness

PREVENTING IDENTITY THEFT IN E-COMMERCE SYSTEMS THROUGH INHERENT LIVENESS BIOMETRICS

1 INTRODUCTION

The technology of biometrics, in many different forms, is currently being used very widely for individual identification and authentication of individuals.

One of the problems with many existing biometric solutions, is the fact that a specific biometric, belonging to a certain person, can be used, even if the person (owner) is not present or if the person (owner) passed away.

Several research projects report that, for example: a fingerprint of a person, "lifted" from almost any surface he/she touched were captured on a thin silicon film which deceived biometric readers, and was falsely accepted.

For this reason, many biometric hardware include liveness-testing, by measuring temperature, moisture, oxygen levels etc. Even these relatively sophisticated types of liveness testing is not foolproof.

This paper reports on the initial stages of a research project where, *The way the human heart beats* is investigated as a biometric. More specifically : *The way the human heart beats* doesn't exist if the owner is not alive and thus no explicit liveness testing is necessary, because of this phenomena this paper coins the term "Inherent Liveness Biometrics".

Inherent Liveness Biometrics is thus biometric features that stops to exist if its owner is not alive. Possible examples of Inherent Liveness Biometric features is *The way the human heart beats* (as stated before and being researched), Face-thermography, etc.

The research touches two uncharted domains, namely: The possibility of using *The way the human heart beats* as an Inherent Liveness Biometric, and the term/concept of Inherent Liveness Biometrics.

1.1 IDENTIFICATION and AUTHENTICATION in the electronic sense

Identification and authentication in the electronic sense ensures that systems have a way of making sure that you are who you say you are. Solutions to achieve this, range from traditional username/password regimes to the use of more complex devices such as tokens and biometric scanners.

A system can identify or verify who you say you are by examining three things: what you know, what you have, and what you are. Most solutions doesn't use all three, though. Tokens (what you have) can be paired with passwords (what you know) or biometric technology (what you are) to produce a stronger solution. This helps prevent the use of stolen tokens, but more on this later in the article.

Identity theft, whereby a person claim the identity of another person by mimicking and therefore pretending to the system to be someone else, is a major risk when considering identification and authentication systems. Just think about the implications of someone obtaining authorised access to another's bank account as someone he/she is not.

Technology will continue to play a vital role in overcoming identity theft by improving ways that individuals and organizations conduct financial transactions and by increasing authentication methods. Authentication can help verify the identity of the individual using the access device, credit card, debit card or personal check. Because account takeovers make up a large percentage of identity theft, several potential authentication techniques appear possible now or in the near future, but first an overview of some definitions.

Identification and authentication (also known as verification) are both used to declare the identity of a user, as in figure 1.1. Since the two terms identification and authentication are easily confused, we have the following definitions [1]:

Identification: In an identification system, an individual is recognized by comparing with an entire database of templates to find a match. The system conducts one-to-many comparisons to establish the identity of the individual. The individual to be identified does not have to claim an identity (Who am I?). [1]

Authentication (verification): In a verification system, the individual to be identified has to claim his/her identity (Am I whom I claim to be?) and this template is then compared to the individual's biometric characteristics. The system conducts one-to-one comparisons to establish the identity of the individual. [1]

Before a system is able to verify/identify the specific biometric of a person, the system requires something to compare it with. Therefore, a profile or template containing the biometric properties is stored in the system. Recording the characteristics of a person is called *enrolment* as in figure 1.1. [1]

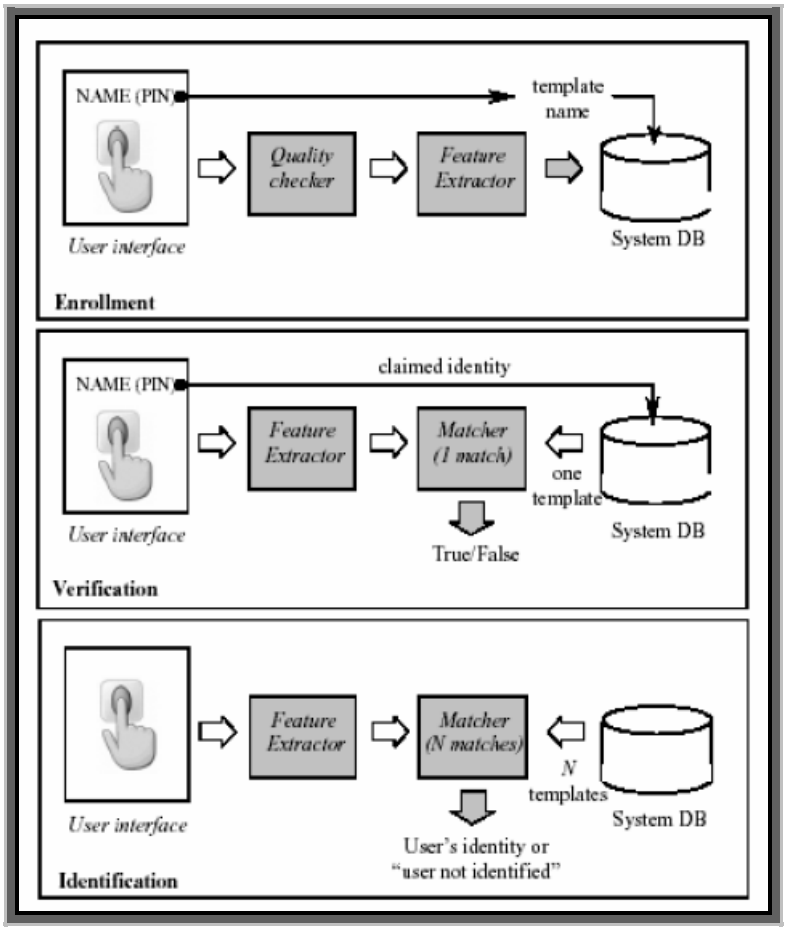

Figure 1.1. Enrolment, verification, and identification. [1]

In an effort to identify and/or verify a person the following “vehicles” are used:

- Something you KNOW
- Something you HAVE
- Something you ARE

It has to be noted that all three of the above “vehicles” are being used in the traditional-biological and electronic sense.

For example: in the traditional biological sense one may ask a person a question that you know only that person would KNOW in order to identify or verify the identity of that individual.

One might accept a certain object/token that only the person you are attempting to identify or verify is supposed to HAVE possession of.

And lastly, the “vehicle” that us as human beings and for that matter most mammals use most often as a means to identify, is who you ARE. We find an identity in who we are physically and by that we ARE part of our body and thus we identify other human beings mostly by looking at a face and identifying that individual.

The above three “vehicles” will be discussed with the focus on electronic identification and verification in the following three sections.

1.1.1 What you KNOW

‘What you know’ is for instance your PIN code. You need to learn the code and remember it. As a way of identification and verification, it is not very secure, the main reason is the fact that a password that is known by its owner can also be known by the possible intruder and thus there exists no direct connection between a password and its owner.

According to an article in SecurityProNews [2], a daily online and email publication focusing on internet security issues, the following were stated.

"The issue with password protection isn't just a number issue. Rather, from a cultural standpoint, many individuals do not believe the value of the password reflects the value of the assets it protects," said Earl Perkins, vice president with META Group's Security & Risk Strategies advisory service. "Time and again, the password is not afforded deserved protection. This renders passwords ineffective regardless of synchronization, best practices, or management efforts."

1.1.2 What you HAVE

‘What you have’ is for example a card (your Token), which you use to access a building. This is not directly connected to a specific person either. As a security level it is safer than the PIN code because you can’t duplicate it as easily, but there are still risks involved. If you give your card away, or lose it, someone else is able to authenticate himself as you.

Token-based security systems have been on the market for approximately a decade and have been proven in numerous environments. Token-based identification and verification solutions have been engineered to be an addition to a network perimeter. Meaning, primarily the remote connections to a system.

ATMs (Automatic teller machines) in South Africa and in most countries around the world is in essence a remote connection to a banks central account database, and thus acts as a perfect example of where token based-systems have been used extensively.

1.1.3 What you ARE

'What you are' is where biometrics comes into play. A Biometric feature is inherently connected to its owner, the owner IS the biometric, that is the biometric is a permanent part of the owner.

You 'are' your fingerprint for example, and it has a high security level. You can't lose it, you can't give it away, and you can't tell your friends about it either.

Casio Computer and Alps Electric [3] have developed a small fingerprint scanner (Figure 1.2.) built into a short, thin cylinder for use in cellular telephones and other portable devices for use in Fall 2003. The cylinder, 0.2 inches in diameter and 0.6 inches long, contains a sensor, light, and lens. When users roll their fingers over the device, it can produce an 8-level monochrome fingerprint image at 600 dots per inch resolution.

Figure 1.2. Casio Cellular Scanner

Figure 1.3. HP IPAQ H5450

Hewlett-Packard (Figure 1.3.) became the first manufacturer to add biometric identity checking to a mass-market consumer portable electronics device, when it built a small fingerprint scanner into its HP IPAQ H5450 PDA.

1.1.4 Authentication by means of a combination

A combination of these authentication Methods (What you KNOW, HAVE and ARE) will provide for more trusted authentication. If a system requires for example a token and a PIN, as in most ATM (Automatic teller machine) transactions, in order to authenticate a person then by having two authentication methods the intruder needs to provide both in order to authenticate himself as another.

2 LIVENESS OF A BIOMETRIC

Liveness checks are a technological countermeasure to spoofing using artifacts. They apply most obviously to biological biometrics such as finger, face, hand and iris, though they might also protect

behavioral biometrics in cases where mimicry might be performed by an artificial device (e.g. a signature signing machine).

Research by Putte and Keuning [4] that tested several fingerprint sensors to check whether they accept an artificially created (dummy) finger instead of a real finger, provides proof of just how crucial liveness testing is but also just how ineffective these liveness mechanisms currently is.

The authors[4] describe methods to create dummy fingers with and without the cooperation of the real owner of the biometric. When the owner cooperates (namely, he/she is helping the attackers) ,obviously, the quality of the produced dummy fingers can be higher than those produced without cooperation (namely, he/she is a victim of the attackers). In the scenario where the owner cooperates, a plaster cast of the finger is created, liquid silicon rubber is filled inside the cast to create a wafer-thin dummy that can be attached to a finger, without being noticed at all. This operation is said to take only a few hours.

In the second scenario where the owner doesn't cooperate, more time (nearly eight hours) and more skill are needed:

First, a fine powder is used to enhance the latent fingerprints left on a glass or scanner surface. Then, a photo of the print is taken which is used to transfer the print to a PCB (Printed Circuit Board). UV light exposure and acid etching leaves the profile of the print on the board, which is used for producing the silicon cement dummy. In both the cases, the authors used cheap and easily accessible material for the creation of the dummy finger.

Five out of six sensors (that included both optical and solid state sensors) tested by the authors[4] accepted a dummy finger created by the above methods as a real finger in the first attempt, the remaining sensor accepted the dummy finger in the second attempt. The authors argue that the properties (e.g. temperature, conductivity, heartbeat, dielectric constant, etc.) claimed to be used by the scanner manufacturers to distinguish a dummy finger from a real finger, may not perform well since the detection margins of the system need to be adjusted to operate in different environments (e.g., indoor vs. outdoor), different environmental conditions (e.g., hot summer vs. cold winter), etc. Wafer thin silicon dummy fingers may lead to changes that are still within the detection margins of the systems.

Liveness checks may detect physical properties of the live biometric, e.g. electrical measurement, thermal measurement, moisture, reflection or absorbance of light or other radiation, the presence of a natural spontaneous signal such as pulse, or the response to an external stimulus e.g. contraction of the pupil in response to light, muscular contraction in response to electrical signal etc. These Liveness checks in most cases simply doesn't measure up to the challenges of the technological advanced, twenty first century criminals of our modern age.

A better and more efficient way for a system to be sure that the live biometric of a user is presented at all times is needed.

3 A POSSIBLE SOLUTION: "THE WAY THE HEART BEATS" AS AN *INHERENT* LIVENESS BIOMETRIC

As stated before this paper coins the term "Inherent Liveness Biometrics", the following paragraph, again, highlights the definition of Inherent Liveness biometrics with the focus on the possibility of using *The way the heart beats* as an Inherent Liveness Biometric.

The way the heart beats is an exciting alternative inherent liveness biometric because of the small but very significant fact that *the way the heart beats* does not exist if the owner is not alive, therefore liveness testing and all the issues surrounding liveness testing are excluded in the scenario where an inherent liveness biometric is applied for identification and authentication. It is important to state at this point that because the heart is hidden, it is not possible to easily capture the

characteristics of an individuals heart without his\her consent, therefore, the recording of *The way the heart beats* is not as easy as other biometrics, for example: fingerprints and iris biometrics.

Documented research to my knowledge points to using the heart beat as a conformation of liveness [7] but not as a biometric trait in the sense of using the way the heart beats as a biometric.

The main concept of using the exciting possibility of *the way the heart beats* as an inherent liveness biometric revolves around using the electrical conductive properties inside the human heart as the unique biometric feature of the user to be identified/authenticated.

The electrical events occurring in the human heart are powerful enough to be detected by electrodes on the body surface. A recording of these events is an ECG (Electrocardiogram, figure 3.1) of the human heart.

Figure 3.1. A schematic of a typical ECG (Electrocardiogram).

Another more technologically advanced reading of the electrical flow inside the human heart is a Vectorcadiogram (VCG) figure 3.2.

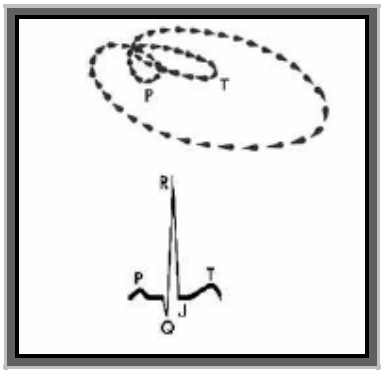

Figure 3.2. A schematic of a VCG graph (top) and a ECG graph (bottom).

3.1.1 Background to the Human heart

The heart is a four-chambered, muscular organ about the size of your fist. It lies within the chest, between the lungs, and just behind and to the left of the breastbone.

The heart's main job is to pump oxygen-rich blood throughout the body. It does this by contracting 60 to 90 times per minute. With each contraction, the heart chambers pump blood either into a ventricle or an artery. During the course of a day, your heart beats more than 100,000 times, pumping 7,000 liters of blood through thousands of miles of blood vessels.

The heart has an electrical conduction system that stimulates it to contract or beat. Each beat begins as an electrical impulse that arises from a specialized area of the right atrium called the

sinoatrial (SA) node. The SA node is the heart's natural pacemaker. It receives messages from the brain and other centres directing it to adjust the heart rate to meet the body's needs.

The above background information is important in the study of using *the way the heart beats* as a biometric because of the following:

- To use the heart as an inherent liveness biometric we are not referring to the pulse created by the heart beating.
- Also, We are not referring to the sounds that the heart makes (the heart contracting and the valves opening and closing)

When exploring to use *the way the heart beats* as a biometric we are considering the electrical activity inside the human heart, which bring us to the next section.

3.1.2 The Conduction system of the human heart

The heart has its own system to generate and spread electrical signals from one end of the heart to the other, making the muscle contract. The electrical impulse begins at a bundle of cells called the sinoatrial (SA) node. This node is a small pacemaker in the right atrium near the entrance of the superior vena cava. It is difficult to see this structure with the naked eye.

If one could look at the entrance of the superior vena cava into the heart, then follow along the front edge where it meets up with the atrium. This is where one will find a thickened area. This is the sulcus terminalis with the sinoatrial node inside.

The rest of the electrical conduction system cannot easily be seen without a microscope, figure 3.3.

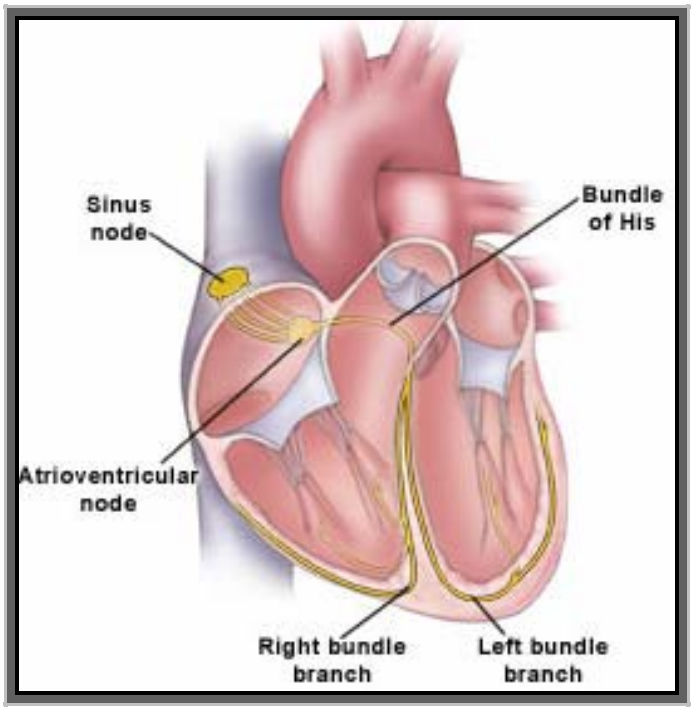

Figure 3.3. The conduction system of the human heart – [Source Unknown]

The electrocardiogram (ECG), as mentioned before in the beginning of chapter 3, is a way that we can “see” certain characteristics of the electrical signals in the heart.

There are three waves to the ECG, each of which corresponds to a stage of the heart's contraction.

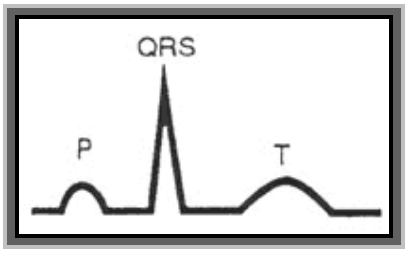

Figure 3.4. A Basic example of the three waves of an ECG.

These waves are called P, QRS, and T, figure 3.4. The stages of contraction for each wave are listed below:

- P: Atrial muscle contraction after the SA node fires
- QRS: Ventricular contraction
- T: Ventricular refilling and recharging after contraction

A real example of an ECG measurement of a human heart is depicted in figure 3.5 below.

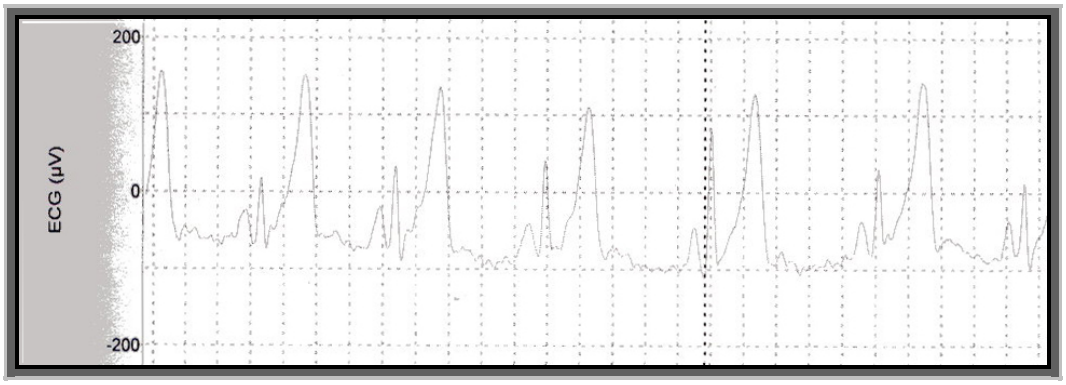

Figure 3.5. A Real example of a ECG measurement.

In an ECG graph, figure 3.5, electrical signals from the heart are presented as a graph of voltage against time. The voltages developed along the various axes of the heart are recorded using a set of lead configurations which are selected in turn.

However, more information can be derived from a vectorcardiogram (VCG) which can deliver a three-dimensional picture of the orientation and magnitude of the cardiac electrical vector throughout the cardiac cycle. In practice a two-dimensional image is displayed for each of the orthogonal planes, figure 3.6.

3.1.3 A possible more advanced sensor to use in order to read the electrical activity in the human heart, the Vectorcardiogram.

In discussions that we had with Professor A.L. van Gelder [5] it showed that the vectorcardiogram (VCG), figure 3.6., would provide more parameters than the electrocardiogram (ECG) to measure the electrical activity in the heart. We in conjunction with Ruben Hechter from TECMED [6] are in the process to obtain data from different age groups that the same vectorcardiogram reading of their heart more than once in the same year were taken. Data containing the above information will provide us with a platform to establish the possibility of using *the way the heart beats* as an inherent biometric.

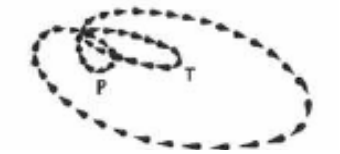

Figure 3.6. Vectorcardiogram (VCG)

The following is a definition of a vectorcardiogram, figure 3.6: the representation of the ECG as a three-dimensional signal, visualized as three two-dimensional Lissajous figures in three orthogonal planes.

3.1.4 Uniqueness of The way the heart beats.

There is no research, reference or information available regarding the application of using the electrical activity in the human heart as an inherent liveness biometric, and there is no information available regarding the uniqueness of the ECG or VCG measurement; this is because of the application of ECG and VCG measurements up to now:

ECG and VCG measurements have up-to now been used to diagnose a variety of heart diseases, this is done by interpreting the ECG or VCG reading and identifying characteristics that are ***similar*** to the characteristics of the different heart diseases.

To use the electrical conductance properties of the heart as a biometric one will have to interpret the ECG and VCG reading a lot differently, one will be looking for ***differences*** between different ECG readings and not similarities. For this reason the ECG and VCG readings of a human heart might not be the ideal sensing mechanism to use in capturing the needed characteristics of the conductivity of the heart, because of the fact that it was designed to identify ***similarities*** and not ***differences***.

Because of the above factors we will still need years of research to be able to capture the correct properties with a specifically designed sensor to prove this exiting possibility of using *the way the heart beats* as an inherent liveness biometric.

3.1.5 Benefits of using the way the heart beats as a Biometric

- *The way the heart beats* is a unique & private feature of an individual.
- Identical twins might have different and distinct electrical activities in their hearts.
- The Heart is hidden, it is not possible to easily capture the characteristics of an individuals heart without his\her consent.
- *The way the heart beat* are not easily observed.
- No liveness testing necessary, an Inherent liveness biometric. The nature of *the way the heart beats* as a biometric proves the liveness of the user in a natural way.
- In the possibility of using the way the heart beats as a biometric one might incorporate a stress level check that will ask a user in an ATM transaction to enter the bank if too

high stress levels are detected that might indicate a user being forced against his\her will to conduct a transaction.

- Everybody has a heart. Unlike a fingerprint, some individuals might be disabled and have no hands and thus no fingerprints. This is hindering systems where fingerprints are being used to identify and verify a large population.

3.1.6 Possible challenges and areas to look into.

- The way the heart beats will change if an individual suffers from a heart attack – even if it is still unique, re-enrolment will have to occur.
- If an artificial pacemaker is installed the way the heart beats will change –if it stays unique- re-enrolment will have to occur.
- To obtain a sufficient "noise free" electrical heart activity measurement the user must stay fairly still for 10 – 15 seconds.
- Sudden heart diseases will influence *the way the heart beats*.
- The way an individuals heart beats changes through time, thus the biometric system must have a way of adjusting small changes and adding those changes to the template in the database on a continuous bases.
- ECG and VCG instruments will still need some specific development in-terms-of the application as a biometric tool.
- People might be reluctant or find it too intrusive to have their heart activities recorded and used as a biometric.

3.2 Conclusion

To use *the way the heart beats* as a biometric has got it's benefits and drawbacks as is the case with all biometric features and technologies.

Maybe the most promising benefit regarding the possibility of using *the way the heart beats* as a biometric is the fact that the biometric feature, in its nature, solves one of the biggest concerns regarding biometrics today namely: Liveness testing.

One cannot measure the electrical activity of a human heart if the heart and thus the human are not alive, thus the term explained in the introduction and beginning of chapter 3, an Inherent liveness biometric trait.

And one of the most un-explored and un-researched fields in using *the way the heart beats* as an inherent liveness biometric is probably the ECG or VCG measuring readers, for that matter any to be developed reader, that will be best suited for the application of a sensor in a biometric system.

There is absolutely no information (to my knowledge) available at the time of writing this article, regarding the use of *the way the heart beats* as an inherent liveness biometric. Thus there is still a long way to go regarding research into this exiting possibility.

4 REFERENCES

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar (2003). Handbook of Fingerprint, Springer, New York.

[2] Available from http://www.securitypronews.com/news/securitynews/spn-45-20040915MostCustomerPasswordImplementationsandPoliciesIneffectiveAccordingtoMETAGroup.html - Staff Writer (Accessed 12 January 2005).

[3] Available from http://www.mobileinfo.com/News_2003/Issue15/Casio_Scanner.htm (Accessed 24 March 2005).

[4] T. Putte and J. Keuning (2000). Biometrical fingerprint recognition: don't get your fingers burned, *Fourth Working Conf. Smart Card Research and Adv. App.*, pp. 289-303.

[5] Professor A.L. van Gelder - FRCP(London) Head, Dept of Internal Medicine, University of Pretoria and the Pretoria Academic Hospital

[6] Ruben Hechter (rubenh@tecmed.co.za) – Sales Representative, Electro Medical, Techmed (Pty) Ltd

[7] Available from http://www.ttivanguard.com/phoenixreconn, Proof-of-Life Biometric – RichardBennett,TarianTechnology (Accessed 2June 2005)