Updated November, 2007

W.A.R.N. Passive Biometric ID Card Solution

Biometric technology has advanced so quickly in the last decade that questions and facts about its cost, use, and accuracy are often confused or intermingled with facts about older versions of the technology.

Once exotic, biometric identification is rapidly becoming a commodity.

The new issues of biometric identification today are not about its potential for accuracy, but about current solutions commercially available "off the shelf" and the ***costs, ease of use, and security and management*** of the collected data and card output..

The W.A.R.N. offering into this arena --- an affordable and rugged system of "passive biometric" fingerprint identification, represents a new, more secure generation of biometric ID.

It will, over time, make commonly-used older technologies and methods obsolete.

First Generation ID Systems

Biometrics is the science behind positively recognizing a person using unique and individually distinguishing traits such as **fingerprint, facial, retina or iris eye scans, voice prints, or and geometry**.

For our purpose here, the **fingerprint biometric** will be the focus, because only fingerprint (and DNA) is currently allowable evidence in court.

There are about one billion possible minutiae combinations on a fingerprint. Estimating there are about 6 billion alive today, and that each has ten fingers, this means that statistically only about sixty people on Earth can share a fingerprint.

These are the points that have traditionally defined the accepted modes of identification:

1. Something You **Have** (an identity card or driver's license)
2. Something You **Know** (a password)
3. Something You **Are** (a fingerprint)

Most security systems still depend entirely on **having or knowing something**, and never even attempt to further verify that the person who "knows or possesses something" is in fact the actual person. **Biometric verification accomplishes this.**

The first biometric systems were predicated on computer networks, using standard file server methods. That meant the **biometric identifier for an individual was stored on a server somewhere**, and a request had to be sent to that server from an ID checkpoint to provide the identifier file so the checkpoint could match it to a fingerprint scan.

If the network was down, the system did not work. Efforts to improve the reliability of the network system included storing identifier files on local computers, but this didn't allow someone who was not on the local system to be identified. For large organizations, this was not satisfactory.

The Biometric "Smart Card" Compromise: Convenience vs. Security

To try and overcome the problems of reliability and convenience, **the electronic "Smart Card" was adapted to biometric identification tasks**. Original electronic smart cards had been developed for purchasing, acting to store and calculate how much money a card represented.

In the role of biometric identification card, a biometric identifier was stored on the card in memory, and could be retrieved at a checkpoint station and compared to a fingerprint scan of the individual. The encumbering dependence on a network was lessened.

The weaknesses of the electronic smart card were vulnerability to hacking, and alteration of the data in the card. A sophisticated underground of electronic card hackers already existed, stealing money by copying bank credit and debit cards, and phone and cable TV cards. Press announcements are not uncommon each year about successful "hack and crack" attempts.

The **vulnerability of the electronic smart card was, and is, basic and inherent in the solution itself.** It has to be programmable in some fashion, to be useful, and hackers are able to consistently exploit this necessity.

A serious problem with ALL card-based ID systems is security of the card. "Mag-striped" cards (the common credit card or driver's license configuration with a magnetic stripe on the back) are easily demagnetized or preprogrammed by hackers.

Communications technology, military, and commercial workers who are in the presence of intense magnetic fields caused by radio broadcast of power generation equipment, often have mag-stripe cards demagnetized or "blanked out".

The "Passive Card" Breakthrough: The "Security Card"

With the introduction of an industry standard high-density printed barcode (the PDF417), the possibility emerged for **more secure, less expensive biometric identification system that was not dependent on networks.**

Because the electronic smartcard is electronic, it is an “active” system as opposed to the non-electronic, non-magnetic “passive” printed barcode.

Early attempts to harness the PDF417 barcode to biometric identification held promise. One variation was to simply put the file location into the barcode, so the matching biometric identifier could be retrieved from a server. Another was to store the individual’s biometric data within the barcode (if it could be compressed enough), where card machine results and data are compared to a scan of the individuals enrolled finger.

This “stored biometric” approach showed great possibilities. **The problems encountered were in data security implementation.** Security methods, reliable card reader units, and scalable systems to distribute and manage the data existed only in elementary form.

Printed cards were static, and unchanging. Often, **cracking one card issued by an organization allowed all its cards to be compromised.** The ability to protect each card with individual security without use of passwords or PIN codes was very, very rare.

The W.A.R.N. Passive Biometric Security Solution

Scalability & Security: and the “One-Time Pad” *en masse.*

The original thinking was that *one-to-one* systems were limited, and that *one-to-many* systems were the only way to serve large numbers of people. This was before the inexpensive, secure, passive W.A.R.N. SOLUTION card had emerged as a contender.

The W.A.R.N. SOLUTION encrypted PDF417 printed barcode is exactly like the “one-time codebook pad”, **the only unbreakable code ever devised and proven when its simple rules are followed.**

The coding of every message sent by a “one-time pad” was unique and never repeated. In this case, **the “code sender” is the enrolled person, and the “code receiver” is the biometric in the barcode**. Altering the barcode renders it useless --- because it no longer matches the individual. No other person can use the barcode, because it will not biometrically match.

Each read and verification of the fingerprint to barcode is as secure as a single use of the one-time pad. The primary privacy and security issue that an “identity” can be stolen is solved because each check of the identity is verified only to the enrolled person.

Non-magnetic, printed W.A.R.N. SOLUTION ID cards **can't be blanked or reprogrammed, and they contain expiration dates, use restrictions, and data management and handling commands.**

Even counterfeited cards made with genuine but stolen W.A.R.N. SOLUTION enrollment software may look good to the eye, but **will not pass scanning checks that look for secret enrollment verification data within the card.**

The Cost Consideration

Printed W.A.R.N. SOLUTION barcodes on ID cards, labels, and other documents are inexpensive and can be made by common laser and inkjet printers.

Electronic smart cards and optical cards are significantly more expensive to issue, support, and replace. **A replacement PDF417 ID card image can be e-mailed to a site for printing and verification against the receiving individual, or a printed card may be used physically mailed to a cardholder without any worry that if it is lost or stolen, that someone else could use it.**

Advanced Security Card Passive Technology

Memory or micro chip cards are considered an "active" technology with vulnerabilities not present in **the more advanced "passive" technology** of the optically read card.

The term "active technology", and "chip card", cover smart cards (featuring embedded microcontroller silicon), memory cards (featuring embedded EEPROM silicon), and contact and contact-less technologies. Contact chip cards conform to ISO 7816, and are easily identified by their metallic contact pads.

Contact-less smart cards conform to ISO 14443 (Type A,B or C), do not have power cells, communicate by radio frequency (RF) modulation, and are energized by movement within the electromagnetic field produced by the card-reader antenna.

1. Passive optically read cards are not subject to the magnetic damage or reprogramming of active technology cards.

2. Passive technology cards may operate securely without dependence on databases.

3. Passive cards hold unchanging data about an individual, including a biometric identifier (fingerprint or retinal scan), biographical information, and layered security concealing key medical information, special police or military classifications, or other.

Actual PDF417 optical card creation costs are approximately $2 to $3 US at the point of output and distribution, or less, per card. The remaining systems costs are:

1. **Card reading scanners.**
2. **Fingerprint scanners.**
3. **Computer system installation and maintenance.**
4. **Card issue database maintenance.**

(See Cost Reduction and Management Key Below)

Key to Cost Reduction Issues:

1 & 2 (above): Significant cost reductions are achieved immediately, with commercially available Symbol Technologies PDF417 optical scanners, and fingerprint scanners already produced by a variety of international manufacturers.

3 (above): Computer system installation is simplified by requiring only IBM compatible "personal computer" hardware, and the level of commodity cost and maintenance associated with such hardware. The only special costs are for the construction of kiosk type cabinetry and housings at border authorization points to protect and conceal the hardware. Further cost reductions are allowed by the use of reliable Linux operating system for the reader stations.

4 (above): While the normal use of an optical card requires no access to a remote database for verification, a database record of cardholder traffic is maintained, and a provision to post and update a "watch-list" or "stop-list" at each kiosk is provided. This special list is typically very small and requires that each station check passage approval against just it, without the time penalty searching a large database would impose.