Biometric Solutions to Personal Identification

A White Paper Describing Technologies Available for Establishing and Maintaining Your Identity in Cyberspace

For More Information Contact

DigitalPersona™
Providers of U.are.U®
Fingerprint Recognition System
805 Veterans Blvd.
Redwood City, CA 94063 USA
650/261-6070
www.digitalpersona.com

Contents

Executive Summary

With the proliferation of electronic devices that each of us has incorporated into our everyday lives, including desktop and notebook computers, ATM machines, cellular phones, physical access devices and many others, the need for secure and convenient personal digital identification is becoming increasingly urgent. We are depending more and more on security devices including smart cards, PIN numbers, and passwords. However, even with such devices in place, losses in revenue due to fraudulent identification are skyrocketing, and affecting the cost of all types of goods and services.

We all need our interactions and transactions with digital systems and devices to be *both* convenient and secure. That is, we need to be able to use these systems quickly and easily with little or no chance of fraud. However, with current access devices, based on smart cards, PIN numbers and passwords, there is an inverse relationship between security and convenience. Full security is never achieved and even *better/good* security comes at the price of less convenience. To achieve better security we must use more complex - and less convenient --passwords. If we use the same password across a number of systems we have a better chance of remembering the password and therefore increase convenience but we seriously compromise security.

At the Gartner Group's ITxpo in October, 1997 Bill Gates made the statement that biometrics technologies - those that use human characteristics such as fingerprint - will be the most important IT innovations of the next several years.[1] The reason for Gates' statement is that increasingly individual consumers, companies and government agencies are admitting that current identification systems based on cards, PINs and passwords, are woefully inadequate. Identification systems based on biometrics offer a potential solution.

A biometric is *both* the most convenient *and* the most secure identification device available. It is not based on something you remember like a PIN code, nor is it based on something you have in your possession like a smart card. A biometric is something you ARE. Nothing is more convenient to use or more secure.

This white paper, prepared by DigitalPersona, the leader in mass-market solutions to personal identification based on biometrics, provides an overview of the field of biometrics, explores the different biometric identification systems currently available, and describes how they can be used for system and network access, physical access, Internet access, and electronic transactions.

[1] Maria Seminerio, "Experts See a New PC Revolution," The ZDNN News Channel (October 8, 1997)

History of Biometrics

Biometrics dates back to the ancient Egyptians who measured people to identify them. Such rudimentary means of identification based on measurements of parts of bodies or aspects of behavior have continued to be used ever since throughout the centuries. Fingerprint identification dates back to ancient China. Identification based on fingerprints has been in effect in the United States and Western Europe for over 100 years.

Commercial advancements for biometric devices began in earnest in the 1970s when a system called Identimat which measured the shape of the hand and length of the fingers was used as part of a time clock at Shearson Hamill, a Wall Street investment firm. Subsequently, hundreds of Identimat devices were used to establish identity for physical access at secure facilities run by Western Electric, U.S. Naval Intelligence, the Department of Energy, U.S. Naval Intelligence and like organizations.[2] Identimat went out of business in the 1980s, but it set the stage for future biometric identification systems based on hand measurement.

Progress was made on fingerprint biometric devices during the 1960s and 1970s when a number of companies developed products to automate the identification of fingerprints for use in law enforcement. In the late 1960s, the FBI began to automatically check fingerprints, and by the mid 1970s, it had installed a number of automatic fingerprint systems across the U.S. Automated Fingerprint Identification Systems (AFIS) are now used by police forces all around the globe. This widespread use of fingerprint data for law enforcement lends a 'Big Brother' feel to the use of fingerprint biometrics for identification, making it important for current fingerprint identification system providers to reassure consumers that their identity is 'safe,' their privacy maintained, and that their fingerprint will not be entered into a law enforcement database. Consumers must understand that current fingerprint recognition systems used for digital transactions differ widely from traditional AFIS systems.

Automated systems for measuring other biometrics developed similarly to those used with fingerprints. The first systems to measure the retina were introduced in the 1980s. The work of Dr. John Daughman at Cambridge University led to the first iris measurement technology. Identification based on signature and face biometrics is relatively new.

Biometrics has been widely researched inside certain universities for the past two to three decades, and most commercial products emerging today have strong roots inside institutions of advanced education. Caltech and MIT are two

[2] Benjamin Miller, "Vital Signs of Identity," IEEE Spectrum (February, 1994): p.22

leaders in the study of biometrics and the related fields of pattern recognition, learning theory and artificial intelligence. Because of its inherent complexity and because of their longer history with biometrics, individuals inside universities are closely involved with the most important product innovations involving biometrics.

Growing Need for Convenient, Secure Identification Schemas

All of us have experienced the proliferation of electronic devices and systems in our everyday lives. Many of us have devised special ways to keep track of the passwords, PIN codes and access devices we are required to remember. The need for more convenient, secure systems has become imperative:

Network Security - A separate study of 533 IT managers reported that unauthorized use of computer systems in their companies grew to 49% in 1997 from 42% in 1996, and losses to the companies involved totaled more than $100 million each year.[3]

Credit Card Fraud - Credit card fraud is currently at a level of four to six billion dollars a year, and it grows every year.

Physical Entry Fraud - The inconvenience to employees is matched by the lack of security to building owners as users share cards, use temporary cards because of failure to bring their regular card, and otherwise 'fool' a pass card system that is annoying to use.

Internet Fraud - All companies that deliver content over the Internet are looking for ways to make that content more secure, from try-and-buy software sites to high end content providers, to push technology sites, to retail sites which depend on credit cards.

Intranet Fraud - Companies are increasingly depending on their corporate Intranet as a means of handling electronic transactions with employees, from sending contracts to filling out forms for health benefits. It is imperative that the Intranet be secure and that different users have selective, secure access to specific company information. Yet systems based on passwords and PIN codes are inherently insecure.

[3] Lawrence Aragon, "Facing Up to Security Technology," PC Week (January 12, 1988): p.88.

Identification System Fraud -- The State of Connecticut, which has been a leader in adopting a fingerprint identification system, estimates that it has saved over $7.5 million in fraudulent welfare claims with this system each year. Los Angeles County saw savings of almost $100 million in a biometric test it ran for public aid recipients.[4]

Electronic Transaction Fraud -- Increasing numbers of people are purchasing goods and services electronically with no physical contact between buyer and seller. BCC, Inc. in Norwalk, CT indicates that during 1996 consumer electronic commerce expenditures were $254 billion and that this number is expected to grow to $1 trillion in 2001.[5] The potential for increased fraud in such a setting with increased transactions, no physical contact and security systems based on password and PIN numbers, is obvious. Virtually all companies involved in electronic commerce are investigating new ways to identify and verify the identity of their customers

Biometrics to the Rescue?

With huge growth already occurring in electronic commerce it is essential that we institute better systems of identification before the current system implodes. By elimination, as more primitive systems fail, biometrics is becoming the means of identification with the most promise.

There are levels of security from the most basic to the most robust with biometrics being the most secure:

1. Something that you *have* - such as an ID badge with a photograph on it.

2. Something that you *know* - such as a password or PIN number.

3. Something which you *are* - such as biometric data – fingerprints, iris, voice or face scans.

A biometric is a unique, measurable characteristic or trait for automatically recognizing or verifying the identity of a human being. Biometrics at its most basic level is the statistical analysis of these traits or characteristics. At a basic level biometric devices, which are technologies for analyzing human characteristics, all work in the same way using a four-step process *of capture, extraction, comparison and matching*.

[4] "Smart Cards Meet Biometrics," Card Technology (September/October, 1996): p.30
[5] "Electronic Commerce: How Soon? How? How Much?," Business Communications Company (April, 1997): p.1.

A system captures a sample of the biometric characteristic. Unique features are then extracted and converted to a mathematical code and this code is stored as the biometric template for that person. The template may reside in the biometric system itself, or in any other form of memory storage, such as a computer database, a smart card or a barcode. The individual then interacts with the biometric system to verify his or her identity and obtain matching or non-matching.

Technology Overview

There are a number of different biometrics that can be used for identification. DigitalPersona believes that the fingerprint biometric is the most convenient, proven, non-invasive and inexpensive to implement. It has the best potential for mass-market application. DigitalPersona technologies and proprietary algorithms can be applied to other biometrics based on pattern recognition should it make sense to do so. Here we describe how the most popular biometric systems work, and review their ability to capture, extract, compare and match data.

Iris Scan Identification Systems

The iris is the colored ring of textured tissue that surrounds the pupil of the eye. Each iris contains a unique structure based on characteristics known as corona, crypts, filaments, freckles, pits, radial furrows and striations. It is claimed that no two irises are alike. Iris scanning security systems include a robotic camera that seeks out your eye and zooms in once it finds the iris. To guard against fraud the system checks for Rapid Eye Movements (REMs).

Iris Scan Strengths

- Convenient for the user.
- Might prove to be a reliable biometric, though it is presently untested.
- The subject places him/herself in front of the scanning device but does not interact with it physically.

Iris Scan Weaknesses

- One major weakness of iris scanning is that it is relatively untested. Current iris identification systems use the statistical theory of small samples rather than real-world data to back their claims of unique identification capabilities.
- Potential for miniaturization of the image acquisition device is low.
- An expensive camera is required because of the zoom requirement. The lowest cost iris scan system costs around $4,000.
- Glasses can distort the image and should not be worn for complete reliability.

- Dark eyes are difficult to read.
- Requires good lighting to be effective.
- There are diseases that adversely affect the iris biometric.

Retina Scan Identification systems

The retina is also used for biometric data identification and some feel that the retina is a more unique biometric than the iris. Retina scanning requires that a laser is shined onto the back of the eye and the unique characteristics of the retina are measured.

Retina Scan Strengths

- The retina is an extremely stable biometric because it is “hidden” and not subject to wear, other than aging and disease.
- The user does not have to interact physically with the scanning device.
- Might be a hard system to fool because the retina is not visible and cannot be faked easily.

Retina Scan Weaknesses

- Retina scanning is almost completely untested.
- There are obvious potential risks to health that require further study.
- The invasive nature of retina scanning is unattractive to consumers.
- Potential for low cost, miniaturized devices is low.

Face Identification

Face scanning identification systems measure the unique characteristics of the face and their relationships. Identification based on these unique characteristics is a complex process usually requiring artificial intelligence and machine learning techniques. The two technologies used for capturing face data are standard video and thermal imaging technologies. With video capture, a standard video camera captures an image or a series of images of the face. After the face is captured a number of core data points are mapped out. For instance, the position of the eyes, nose and mouth relative to one another is established and used to create a template. With a thermal imaging approach, a thermal imaging camera analyzes heat caused by the flow of blood under the face. Unlike video capture, thermal imaging cameras do not depend on good lighting conditions and can therefore be used in dark environments. A proprietary algorithm or neural network within the capture engine converts the face to a unique pattern and a mathematical code for match or non-match.

Face Scan Strengths

- Face scanning is non-invasive and the user does not need to physically interact with the sensor.
- Although desktop video cameras are available, currently only high end versions of these cameras are fast and reliable for face scanning.

Face Scan Weaknesses

- The precise position of the user's face and surrounding lighting may affect the system's accuracy.
- Among those who study biometrics and pattern recognition, face recognition is considered the least accurate and the easiest identification system to fool.
- Face recognition technologies are dependent on the extraction and comparison engine that is used, and the capture of the data can be more costly than other biometric data capture.
- Artificial intelligence is needed to compensate for the many changes that occur in the face including facial hair, makeup, aging and other changes. Machine learning is used to continuously compare new samples to previous ones and to update the core data to compensate for the flow of changes.
- Potential for miniaturization is low. Cost for high quality devices is high.

Signature Identification

Signatures have been used for hundreds of years to establish identity, and we are all familiar with having a signature card on file at the bank to be used as a basis of comparison for verifying our signature. Digital capture of the signature is a measurement of the image itself as well as the dynamics -- the speed, order and pressure used to create each of the letters in relation to the other letters in the signature. Signature, like voice, is a behavioral biometric.

Signature Strengths

- Use of signatures is familiar to consumers and trusted as a means of verifying identity.

Signature Weaknesses

- Our signature changes dramatically with changes in experience, mood, and life style.
- The tolerances need to be so great to deal with the inevitable natural changes in signature that security is compromised.
- Writing your signature is not quick. You would not use a signature to log onto the Internet.

- The pad used to capture signature is complex and expensive. Incorporating signature capture into the touch pad on a laptop, for instance is not possible because the touch pad would need to be far higher in resolution than the standard touch pad.
- Potential for miniaturization is low.

Voice Identification

Like signature identification, voice is a behavioral biometric. Voice identification devices measure the imaged spectrum of the voice over time. Changes in sound frequency are measured. Voice identification is based on precise matching of voice picked up by the sensor with the voice that has been registered as a template. Unlike voice recognition technology, which is based on creating the widest tolerances possible to be able to match many voices with a particular computer command, voice identification needs to create extremely small/no tolerances. This makes it difficult to apply one technology to both purposes.

Voice Identification Strengths

- Voice scanning is non-invasive and natural for consumers.

Voice Identification Weaknesses

- Like other behavioral biometrics, voice is subject to wide variations and is therefore harder to apply to the exacting requirements of identification verification.
- Changes in volume, speed and quality of voice (as when you have a cold) affect the scan that is obtained and the outcome that results.
- As technology improves you will be able to detect and reject a recorded voice. However, currently it is possible to fool voice recognition devices with a recorded voice.
- Cost for high-resolution microphone is high.

Fingerprint Recognition Systems

Fingerprints have been used for centuries for establishing identity. DigitalPersona regards the fingerprint as the most viable biometric for mass-market identification schemas. In a general sense, fingerprint recognition technologies analyze global pattern schemas along with small unique marks on the fingerprint known as minutiae, which are the ridge endings and bifurcations or branches in the fingerprint ridges. The data that is extracted from fingerprints is extremely dense which explains why fingerprints are an extremely reliable means of personal identification. There are on average seventy unique, measurable minutiae points in each fingerprint, and each point has seven unique characteristics - more than enough to establish identity. Should we desire an

even more foolproof identification schema, because each of our fingerprints is unique, we can use as many as ten fingerprints which yield at least 4900 independent measurable characteristics. Here we give an overview of fingerprint capture, extraction and verification.

Optical and Capacitive Technologies for Fingerprint Capture

The two main technologies used to capture fingerprints are optical and capacitive. Optical technologies require a light source that is refracted through a prism. The fingerprint is placed on a surface known as a platen. Light shines on the print and an impression is captured. DigitalPersona has created a proprietary approach to this technology, which eliminates the need for a large, costly prism, replacing it with a thin proprietary component that acts as a prism would.

With capacitive-based semiconductor technologies, the finger is placed on the sensor chip and the ridges and valleys create capacitance variations between the skin and the chip. The chip captures the fingerprint by measuring the spatial variations in the field voltages.

Weaknesses of Capacitive Solutions

Capacitive sensors call for a chip as large as the fingerprint and this chip is expensive. Several companies attempt to get around this problem by offering smaller chips, which measure a part of the fingerprint. With these sensors the user must place a precise portion of his fingerprint on the small sensor in order to get a proper reading. This requirement for precise positioning of the fingerprint makes the sensor harder to use in unattended installations. A further problem with smaller chips is that the amount of data used for matching part of a fingerprint is less than for a full print, making the security that the system provides less robust overall.

Capacitive sensors are also susceptible to noise, including noise from the 60Hz power line noise picked up by the user and electrical noise from within the sensor. And a final problem with capacitive sensors is reliability. Electrostatic discharge, salt from sweat and other contaminants, and physical wear are hard on a semiconductor-sensing chip. Capacitive sensors have difficulty reading dry fingerprints. DigitalPersona believes that the optical sensor currently provides a more reliable solution. DigitalPersona's U.are.U product provides the superior performance of an optical solution with the small size and low cost of the chip-based or capacitive solution.

Fingerprint Identification Strengths

- Fingerprints are unique, and they are complex enough to provide a robust template for identification verification.
- Should we want increased levels of security we can easily register and require verification of one, two, or more fingerprints, up to ten prints. Each of our fingerprints is unique.
- Scanning a fingerprint is quick and extremely convenient for consumers.
- Users must interact with the fingerprint scanner, placing their finger on the scanner to obtain a biometric reading. Direct interaction between the user and the sensor is the most accurate way to obtain a biometric reading, and it is one of the main reasons why fingerprint scanning can be applied to mass markets.
- Fingerprint scanners can be easily miniaturized and they can be mass-produced at low cost.

Fingerprint Identification Weaknesses

- Some people and groups have relatively poor quality fingerprints that are difficult to image. DigitalPersona's software has been optimized to deal with poor quality fingerprints.
- The use of fingerprints in law enforcement leads some consumers to fear "having their fingerprint on file." DigitalPersona reassures consumers that it never stores an image of their fingerprint. Rather the information from the print is stored as a small, encrypted numeric file.
- Latent prints are afterimages that are left on the sensor after each use. Potentially such latent fingerprints could be used to recreate a fingerprint for identification. DigitalPersona has proprietary technology that removes latent fingerprints.

The Importance of Software and Firmware in Fingerprint Identification

Although the cost, size and design of the hardware sensor is important in fingerprint identification, it is only one determiner of whether a biometric system is completely robust or not. The firmware and the recognition algorithms are at least as important as hardware in creating a total solution, especially one that is ready for mass-market employment.

The firmware resides in the hardware sensor and coordinates the capture of the image and its connection to the PC. In most fingerprint systems the firmware is simple and relatively ineffective. It dumps a continuous stream of image data to the host computer. However, in doing so it creates a number of problems. One major problem with this overly simple firmware is that the image data stream, either digital or analog, can be recorded and played back later. This opens the entire identification system to a "replay attack," and compromises security. A

further problem is that the sensor's power must always be on full, and the computer must be continuously capturing and processing the image stream to determine whether there is a fingerprint present. If there is, it must capture a single fingerprint image at the optimal time. Lastly, simple firmware cannot dynamically adjust the system to deal with a dirty sensor surface or "latent" fingerprint images resulting from the last use.

DigitalPersona has addressed these issues in developing the firmware for its U.are.U Fingerprint Sensor, and this makes a difference in the overall effectiveness of the system. The DigitalPersona proprietary firmware handles the USB connection, which provides the power, bandwidth, and plug and play ease of use. It continuously processes within the Sensor to determine when the environment has changed, such as when there is dirt on the Sensor surface, when a fingerprint is present on the Sensor, and when to grab the optimal image. The firmware cannot be too quick to grab the image or the entire fingerprint area will not have been placed on the Sensor, nor can it be too late and risk the user pressing too hard.

Once the image is captured the firmware sets up a 128-bit challenge-response encryption link with the host PC or server, which it uses to transmit the image in a secure manner. In doing so it also alerts the PC or server with an interrupt that a fingerprint has been captured. Afterward, the Sensor reverts back to a low-power mode to await the next finger tap -- an important feature for laptops.

Once the host computer has securely obtained the fingerprint image from the Sensor, the recognition algorithm must take over to perform the verification or identification. Fingerprints are a very robust biometric. They contain so much unique information that only a small portion of the total print is needed for accurate identification. This fact is not apparent with most fingerprint recognition systems. Most systems require that users place their full finger on the sensor, and that they do so carefully so that the fingerprint is aligned with crosshairs that are visible on the screen. If the finger placement is wrong, or if the print quality is not good, the user must retry until correct. Such a requirement makes these sensors less effective for mass-market adoption.

From the beginning, DigitalPersona's commitment to ease of use and reliability has grown from the robustness of the company’s core recognition algorithm. The user does not need to worry about finger placement when using the U.are.U system. The algorithm is completely rotation and distortion invariant. The user taps the finger on the Sensor, without having to worry about precisely placing it on the platen. Finger rotation and pressure, fingerprint quality, and the presence or absence of dirt and moisture has no adverse effect on the system.

Attended and Non-Attended Fingerprint Capture - One-to-One and One-to-Many Verification

With fingerprint identification it is important to understand the difference between technologies that are based on attended or supervised capture of the print versus unattended capture, as well as one-to-one identification versus one-to-many verification schemas. In traditional law enforcement a fingerprint is given under supervision and a match is established by comparing that print to a database of many prints.

For fingerprint recognition to be applied to a mass-market, the capture of the print must be an unattended process in which an individual gives a print quickly without an attendant lining up the print and ensuring a perfect capture of the data. Further, in the case of identification for entry or electronic transaction, the data that is captured is compared to a template that has previously been registered as the valid print. In most instances, the matching is a one-to-one match rather than a one-to-many match.

Unattended fingerprint capture and one-to-one or one-to-many matching place different constraints on the DigitalPersona fingerprint recognition system than exist for the traditional law enforcement fingerprint capture and matching technologies. The unattended model requires that the sensor be much more tolerant of poor quality prints and that the software algorithms be much more robust than those used with attended models.

Conclusion

Identification systems based on biometrics are important building blocks in simplifying our interaction with the myriad digital systems and devices that we are all using in increasing numbers. Important, transformative systems such as electronic banking will not flourish without these devices. This is why computer industry leaders like Microsoft's Gates have gone on record saying that biometrics technologies are the most important technologies to watch over the next three years. DigitalPersona has been formed to bring such technologies to mass, consumer markets based on the research of the world's leading biometrics experts from Caltech and MIT. Should you need more in-depth information about DigitalPersona's technologies please call the company's Marketing or Sales departments.