



Our Bodies, Our Passwords

BIOMETRICS HAVE THE POTENTIAL TO MAKE LIFE EASIER — AND MORE SECURE

“Everybody’s an individual,” begins an old joke. “Not me,” goes the response, proving that indeed we’re all different. Biometrics capitalizes on this fact. Biometrics is the analysis of human physiological features, such as fingerprints, iris and retina patterns, facial characteristics, and handwriting and speech patterns, to verify individual identities, explains Glover Ferguson, chief scientist at **Accenture Ltd.** (ACN).

Biometrics can help airports automatically identify a person amid a database of thousands; it can also help banks quickly verify a customer’s identity before authorizing a withdrawal, says Darrin Reilly, vice president and general manager of **Motorola Inc.’s** (MOT) biometrics business unit. He notes that biometrics can replace or augment passwords and other security techniques used in everything from cell phones to computer networks.

Indeed, the flexibility of biometrics makes it ideal for even the most daunting tasks, such as national security, says Eric Stange, managing partner for defense and homeland security at Accenture. In June the U.S. Department of Homeland Security (USDHS) reported it had selected the Accenture-led Smart Border Alliance team, which includes **Raytheon Co.** (RTN), **SRA International Inc.** (SRX) and **Titan Corp.** (TTN) to design and implement a multibillion-dollar biometrics-based program that uses digital finger scans and digital photos. The system, called the United States Visitor and Immigrant Status Indicator

Technology (US-VISIT), will be deployed at more than 400 ports of entry during the next five years, reports the USDHS, to verify the identities of the 300 million-plus annual visitors and confirm their compliance with visa and immigration policies.

Although consumer acceptance of biometric devices has been slow, **Gartner Inc.** (IT) reports, events such as 9/11 and the rapid rise in identity theft have heightened customer awareness, as well as the acceptance of, biometrics. A recent Gartner study showed at least 2 million bank accounts were compromised by fraud in 2003, resulting in banks and consumers losing a total of \$2.4 billion.

Biometrics makes it possible to reduce such theft because users become their passwords, according to Motorola’s Reilly. Beyond preventing loss due to theft, adds Larry Goldstein, director of the knowledge systems laboratory at **Honeywell International Inc.** (HON), biometric systems can also improve customer relations by making services easier to use and boost business efficiencies by reducing the number of employees needed for security operations.

“Biometrics generally works very well as a convenience factor for users,” explains Raymond Wagner, Gartner vice president and research director of information security strategies. He says he envisions Websites where “biometrics could be used in place of passwords or tokens to streamline lengthy processes or provide ‘forget-proof’ credentials.” [CONTINUED ON NEXT PAGE]

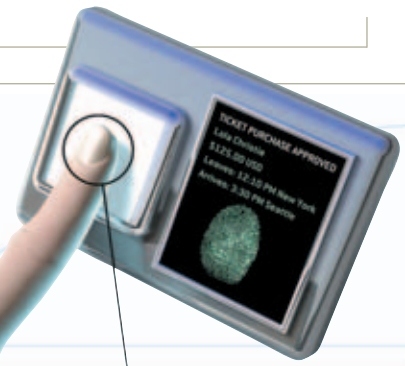
POINT OF CONNECTION

APPLICATION: Fingerprint-recognition technology compares prints against a database of thousands.

Fingerprint technology accounts for 48 percent of the biometrics market, analysts say. The growing use of commercial fingerprint-identification systems is opening up new opportunities for manufacturers, reports Motorola, whose Omnitrak-branded fingerprint and database software is used in law enforcement. Eventually, fingerprints will be stored on smart cards, says Motorola, so a biometric reader at a cash register can confirm that the customer is the authorized user of a credit card.

Titan Corp. says it makes fingerprint card scanners that will be used as part of the US-VISIT project. **Siemens Co.** (SI) reports that it is testing fingerprint-recognition technology in desktop computers to improve network security.

The owner of an **NTT DoCoMo Inc.** (DCM) Foma F900iC phone in Japan can swipe a finger on the reader to unlock it. The company says that by year-end it plans to offer finger-swipe devices that will wirelessly authenticate train-pass purchases and credit-card transactions. Some handsets available this year will employ **Sony Corp.**'s (SNE) Edy e-money system for making wireless purchases at 9,000 participating shops in Japan. Users will even be able to view current balances and payment records on their phones, the company explains.



A FAMILIAR FACE

APPLICATION: Facial-recognition biometrics integrates existing technology, such as video cameras, to take digital photos or scans and create an individual facial template.

Hotels and casinos such as **MGM MIRAGE** (MGG) report using facial-recognition software sophisticated enough to spot known criminals, even if they are disguised or wearing body padding, saving the company estimated millions from theft losses in Las Vegas each year, according to the company. **Computer Sciences Corp.** (CSC), which says it integrates facial-recognition technology into the security systems it develops for businesses and computer networks, explains that the intelligence and defense industries can use the technology to control access to sensitive facilities and identify subjects on watch lists. CSC says next-generation systems, which construct three-dimensional face models, offer improved accuracy in varying lighting conditions and environments. Such advances make it possible to use facial recognition to enhance surveillance capabilities in locations where illumination is inconsistent, such as some airport security areas.

By combining radio-frequency identification (RFID) cards with biometrics technology, Honeywell says that facilities such as hospitals can improve security and efficiency while reducing personnel. RFID cards containing biometric information can wirelessly confirm identity for access control; an automated computer can then track a card-carrying person's location, which, in addition to improving security, the company says could help reduce energy costs by showing which portions of a building are unoccupied.

PLEASE SIGN HERE

APPLICATION: Electronic-signature verification seeks to be more accurate than manual-signature comparison.

Saying it is too easy for determined counterfeiters to fool human cashiers, **General Electric Co.**'s (GE) GE Capital Corp. division reports funding work in the area of automatic signature verification. So-called fuzzy logic software, says the company, takes into account not only the size and shape of a signature but also factors such as writing speed and pen pressure. According to the GE Capital-backed SOFTPRO, which makes the software, more than 200 financial institutions, including **Bank of America Corp.** (BAC) and **Citigroup Inc.** (C), use the technology.

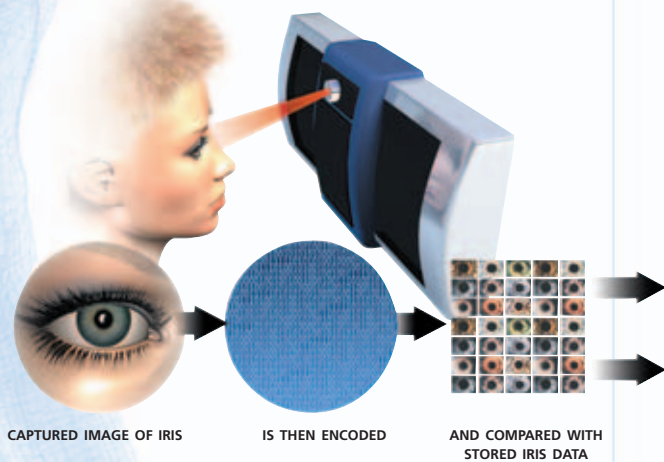
NCR Corp. (NCR) says its point-of-sale signature-capture terminals are equipped to read smart cards and will enable future interfaces with other technologies, including fingerprint-recognition systems. **The Home Depot Inc.** (HD) says its self-checkout touch-screen systems may reduce customer queue time by 40 percent.



TALK TO THE HAND

APPLICATION: Hand-geometry systems match hand parameters with building-access system databases for speed and one-to-one comparisons.

Hand-geometry systems made by **Ingersoll-Rand Co. Ltd.**'s (IR) Recognition Systems division measure as many as 96 hand parameters and then check identity against those in an existing database, according to **Electronic Data Systems Corp.** (EDS), which installed the hand scanners at airport kiosks as part of its support of the Immigration and Naturalization Service Passenger Accelerated Service System, a voluntary system designed to reduce security-checkpoint delays. After passing a background check, frequent fliers can scan their hands at unmanned security kiosks. The airport in San Francisco, among others, reports using the readers for convenience and to restrict tarmac access. **Unisys Corp.** (UIS), which says it integrates hand-geometry systems, indicates the technology works in dirty or cold conditions, and the digital information fits on a standard credit card's magnetic strip, rather than requiring pricey smart cards.



FOR YOUR EYES ONLY

APPLICATION: Iris-recognition technology scans retina patterns.

Matsushita Electric Industrial Co. (MC) says businesses as varied as financial institutions, power plants and hospitals currently use its Panasonic-branded Iris Reader products for security applications. In addition, the U.S. Transportation Security Administration has integrated the product into its Registered Traveler Program, according to Matsushita, in the first public application of the product. Matsushita reports that the Iris Reader is also being considered for rollout in the US-VISIT Program. Analysts say future public eye-recognition systems could be used at ATMs to help eliminate concerns about stolen passwords and bank cards.

ONE VOICE

APPLICATION: Voice-recognition applications allow customers to conduct secure transactions, such as transmitting financial data, via the phone.

AT&T Corp. (T) says it has been researching speaker-verification technology since the 1970s. Typically, a caller is prompted to repeat a phrase, which the system compares against examples of the caller's voice. For added security, the company says, it expects to integrate voice biometrics into voice-controlled services already in place.

Unisys, which says its systems are used to clear about half of the world's checks, points out that using biometric voice-verification for financial transactions could obviate the need to reset customer passwords, which takes up to 60 percent of a typical call-center support staff's time. Unisys is currently conducting a pilot speech-biometrics program at **Lloyds TSB Group plc** (LYG) in Florida for customer-account services over the phone.

IBM Corp. (IBM) reports that it continues research on conversational biometrics, which it says is an even more advanced version of speaker verification. By examining a combination of individual vocal, cognitive and behavioral characteristics based on a speaker's dialogue rather than on a single spoken phrase, researchers say they can identify a person. The system can also be used without initial training on the part of the customer (who generally has to repeat certain phrases to make other systems work), because the IBM system automatically performs its verification while the customer is engaged in conversation. IBM hopes to see the system used in areas such as banking, allowing customers to access accounts from anywhere in the world without worrying about stolen passwords or Social Security numbers.

