

Biometrics Get Real

By Lynn Koller

Are biometrics catching on? The question is important for card issuers because technologies that identify individuals by the whorls on their fingers, the spacing of facial features or the timbre of someone's voice, can provide a strong reason to introduce smart cards. That is because the chip on a smart card can securely hold the digitized biometric data used to identify individuals, whereas a magnetic stripe cannot.

The question also is important because biometrics could eliminate the need for cards altogether. If biometrics ever become accurate and inexpensive enough, someone could simply place a finger on a scanner at an automated teller machine and be identified as surely as cardholders are today with cards and passwords.

Biometrics do not seem likely to replace cards in consumer applications soon, although that already is a reality in some corporate settings. But biometrics certainly are being used more widely. "It's becoming more of a realistic business solution than it was a few years ago," says Raj Nanavati, a partner at the New York-based International Biometric Group consulting firm.

More accurate and reliable biometric devices, lower prices, easier integration into popular networking software from such companies as Microsoft Corp. and Novell Inc., and a broader awareness of biometrics are speeding adoption, Nanavati says. What is more, the growing experience with biometrics is providing lessons in how to work around the problems that do crop up, including how to convince an individual enrolling in a biometric program that the technology will not track their every move. While still a small industry, biometrics is growing. Nanavati's firm estimates biometrics revenue worldwide will grow from \$58.4 million in 1999 to \$594 million in 2003. Those estimates do not include the much larger market for fingerprint registration and retrieval for police agencies.

Biometrics vendors are quick to point out that while their systems may scan a finger or other part of the body, the technology uses mathematical formulas to convert images of those body parts into long numbers that are stored for comparison. Those numbers cannot be reconverted to produce an image of a fingerprint or any other body part, they say.

Of all the biometric methods, finger-imaging is the most commonly used, representing about a third of the market, according to International Biometric Group. Other popular biometrics are based on handprints, facial makeup, iris, voice, retina and signature.

Government projects traditionally have made up the bulk of biometric activity, and that figures to continue as several countries roll out large-scale chip card programs that incorporate biometrics. For instance, the Indian state of Gujarat has issued more than 1 million driver's licenses on smart cards that carry a digitized version of the motorist's fingerprint. Italy also has begun issuing new chip-based national ID cards with a fingerprint biometric, a card that could ultimately be carried by 50 million Italians (Card Technology, July 2001.)

Hong Kong's ID Card

Hong Kong is moving forward with a US\$360 million project to give chip-based ID cards with two biometrics—finger and face—to citizens over 11 years old in the district of 6 million. Government officials say the chip cards will cut down on forgeries, noting that there have been 4,000 cases of counterfeit ID cards in the past five years.

The first batch of 1.2 million smart cards is to be issued in 2003. Meanwhile, the government will study the feasibility of using chip cards for more than just physical identification. Possible applications include digital credentials so that cardholders can identify themselves online to government agencies and private companies.

Nigeria is planning a national ID card that will register each citizen's finger image on the card, Nanavati says. And Mexico has decided on a voter registration card that will carry a biometric based on analyzing the voter's face. The system measures such characteristics as the distance between eyes and the width of the mouth. "Facial recognition is good in large-scale applications where you have to do fast matching and you already have to take a picture," Nanavati says.

Relatively low cost is one of the reasons fingerprint is the most popular biometric. Nanavati says the cost of a hardware scanner and finger-recognition software for a personal computer is only about \$100. That is down dramatically from a few years ago, when fingerprint scanners alone could cost thousands of dollars. However, he says, an organization wanting to use fingerprints to authenticate employees logging onto a network can expect to pay anywhere from \$500 to \$10,000 for network software upgrades.

Other biometric technologies have seen similar price declines. Hand recognition costs from \$200 to \$1,000 per individual and iris-recognition from \$1,500 to \$9,000 per seat, says Bill Rogers, publisher of the Biometric Digest newsletter.

Network Security

Securing computer networks is a growth area for biometrics. Several organizations are installing fingerprint scanners on personal computers so employees or business partners can authenticate themselves more securely or conveniently than with user IDs and passwords.

The City of Glendale, near Los Angeles, has enrolled about 200 of its employees in a program that ultimately will include all of the city's 2,100 workers. The finger-imaging technology from Redwood City, Calif.-based DigitalPersona installs easily on most desktops in about 20 minutes, says Steve Richmond, a security analyst for Glendale.

There has been little resistance from employees, he says. "One or two said something like, 'OK, you're going to take my fingerprint?' But we're not the FBI, and it's just an encrypted algorithm. It's not like we're storing the fingerprint."

Employees typically do not have to remember their user ID code, since each PC stores the last five IDs entered. As most PCs are used by only one employee, most days a worker will turn on the PC, see their user ID pop up and scan their finger. The system then compares the scanned image to the stored template for that user.

"For the most part the response has been positive," Richmond says. "People are tired of forgetting passwords or having them expire. The help desk appreciates getting less phone calls on passwords."

Glendale officials estimate 45% of computer-related calls for assistance are for lost or forgotten passwords, and expect help desk savings will partly defray the undisclosed cost of the biometric system.

The Vancouver-based Credit Union of British Columbia has enrolled 1,200 individuals in a system that identifies them by their thumbprints, and aims to reach 2,000 enrollees this year, says Oscar van der Meer, associate vice president of technology services. The system allows workers at hundreds of credit unions across Canada to access CUBC, which offers credit unions such services as check processing and bill payment.

CUBC considered issuing smart cards for online authentication, but decided they would not provide enough security, van der Meer says. He says CUBC would have to conduct continual audits to make sure that no cardholder had given their card and personal identification number to an unauthorized individual. Biometrics eliminate that threat.

CUBC also considered authenticating individuals solely with the biometric, eliminating user IDs. But van der Meer says that would have opened up security holes.

Each time someone logged on, the system would have to search a database of 1,200 registered fingerprint templates to see if one matched. Because there might be a few finger images that were close, and since a biometric system does not produce precisely the same result each time, CUBC would have to require a very precise match or set the matching threshold low. The former could result in log-in failures, while the latter could permit unauthorized individuals to log in.

Instead, individuals first put in a user ID and then scan their thumbprint. That way the system only has to determine that the scanned image is close to the stored template for that user ID. "We want to have both high accuracy and security, that's why we did a combination with user ID," van der Meer says.

He adds only a handful of individuals have had trouble logging on with their thumbprints, mostly because they did not press hard enough. He says there was some resistance from labor unions that died down after CUBC explained that the biometric was being used only for authentication to a security portal and that the system was no more intrusive than the signatures CUBC keeps on file. CUBC uses finger-recognition technology from Milpitas, Calif.-based SecuGen Corp.

While CUBC and Glendale say they are satisfied with their biometric systems, analyst Frank Prince of Cambridge, Mass.-based Forrester Research believes widespread use of biometrics for network security is still two years off.

He says biometrics remains a new technology and costs are still high. Besides, he says, many companies wind up using biometrics in addition to passwords, so the \$200-a-year average cost for password maintenance does not go away.

A Forrester survey of large global companies last year found 4% were using biometrics to authenticate employees, with 34% planning to do so by 2002. But he says companies often introduce such new technologies more slowly than they expect, as they see early adopters having more problems than expected. However, by 2003, he predicts, biometrics will be widely used for network security.

While governments and employers can demand acceptance of biometrics, many organizations that serve consumers do not have that luxury. However, there are times when consumers will accept biometrics if they benefit as a result.

Continued...

Dutch Nightclubs

For instance, 15 nightclubs in the Netherlands began last year a program aimed at weeding out troublemakers by encouraging customers to enroll a facial image and fingerprint. The digitized versions of those characteristics are stored on a smart card that the customer shows when entering the club. The clubs keep a database of individuals who have made trouble, and the system is aimed at keeping them out.

The combination of smart cards and biometrics has provoked little customer resistance, says Ruud Wouters, manager of the Xanadu club in Bergeek. The club, which caters to teenagers and is among the few clubs to require smart cards for entry, has enrolled 600 customers. "There are some who don't like it," he says. "Others say, 'It's for our own safety. We like this.'"

He says the main resistance has been to the 25 guilder (\$10) charge for the card, which allows a cardholder to enter the club free for a year. He says the cost has been a barrier to attracting new customers.

Operationally, Wouters says, the system has worked pretty well. It takes a few minutes to enroll a customer, and no more than 4 seconds for the cardholder to authenticate themselves when entering the club.

Some 40,000 clubgoers have enrolled in such programs across Holland, says Ron Velders, president of Interstrat BV, a systems integrator based in Enchede, the Netherlands, that implemented the system. The biometrics come from Keyware Technologies, which has headquarters in Brussels and Woburn, Mass.

Voluntary use of biometrics is also growing in financial services in the United States. The Purdue Employees Federal Credit Union has installed nine unattended kiosks at six locations since 1997 that allow customers to authenticate themselves with a fingerprint to apply for loans, print out checks with funds drawn from their accounts and access other services.

Of 62,000 customers, 16,276 have signed up, with few objections, says Gail J. Koehler vice president of technology and retail delivery. "It's not something our members felt uncomfortable with," Koehler says. In fact, the credit union threw out the brochures it had printed to address privacy concerns when it moved offices in 1998.

High Accuracy

A few customers have had trouble enrolling because of dry fingertips, but the credit union came up with a solution. "We have them rub their fingertip behind their ear, because there's oil there," Koehler says. Koehler says improved scanners largely resolved the issue.

In April 2001, for example, the bank enrolled 480 users with no problem. She says .08% of individuals were unable to enroll, generally older individuals. They are allowed to sign in with a PIN.

The accuracy of the system is good, with only 184 credit union members rejected falsely in over 200,000 transactions, an error rate of .092%. The kiosks, along with ATMs and other electronic delivery channels, allow the Purdue credit union to deliver 82% of its services electronically. Kiosks, says Koehler, "are cheaper to run than people."

And biometric components are getting cheaper, as Purdue is paying about \$150 today for finger scanners that cost \$500 in 1997, Koehler says. More credit unions are following Purdue's lead, says Rick Scali, kiosk division director for Norfolk, Va.-based Real-Time Kiosks, which supplies the Purdue kiosks. Scali says the company has sold credit unions some 55 kiosks with biometrics, 25 of the sales in the first half of this year. "People were waiting for validation, and I think they're getting it now," he says.

In an initiative aimed at individuals without bank accounts, San Francisco-based InnoVentry Corp. has deployed 1,300 kiosks across the United States that allow registered users to cash checks. The kiosks use facial-recognition technology to identify the customer, and 1.1 million individuals have signed up for the service, InnoVentry officials say.

Travelers, too, will freely participate in a biometric system if it gets them through airports quicker. There are biometric-based programs in place at both Canadian and U.S. airports to speed entry by frequent travelers, and Canada announced this spring a plan to expand its program to eight major airports (Card Technology, May 2001.)

But what about typical consumers? In a trial this summer sure to be closely watched, Oakland, Calif.-based VeriStar Corp. is testing a biometric payment system with Schnucks, a St. Louis-based grocery store chain. To participate in the voluntary program, consumers have their fingers scanned at the store and provide payment card or bank account information.

To pay, instead of swiping a card, a shopper places a finger on the scanner, enters their PIN and a VeriStar server compares the image to the digitized version stored in its database. If they match, the transaction is approved and the purchase amount billed to the card account or debited from the bank account.

Nanavati says focus groups organized by International Biometric Group show many consumers can be convinced to use biometrics if they understand it—and especially if they try it. "When we explain biometrics, favorable responses go up to 50% to 60%; when people enroll and use it, it shoots up to 90%," he says.

If those focus groups are representative, acceptance of biometrics should grow. Because it appears many more people will have a chance to try out biometric technologies over the next few years.