

The future of identity:

Biometrics solutions to  
enhance the performance of  
businesses and governments



**accenture**

*High performance. Delivered.*

Point of View

• Consulting • Technology • Outsourcing

A knock at the door, followed by “Who’s there?” This most basic question of identity is older than the tale of Little Red Riding Hood. But with new virtual doors opening online—and as a growing number of clever cyberwolves hide their identities—the answer has become more complex and costly.

The stakes are rising dramatically as far as identity fraud is concerned. Identity theft is the fastest-growing crime problem in the United States, according to the Federal Bureau of Investigation. In the United Kingdom, the Home Office estimates 100,000 citizens are affected each year. A report from the Aberdeen Group forecasts the global cost of identity theft will reach \$2 trillion by the end of 2005, and “traditional access and integrity controls will do nothing to stem the tide.”<sup>1</sup>

People whose identities have been stolen can spend months—and sizable sums of money—clearing their names and cleansing their muddied credit histories. Also, consider the knock-on effect on costs and image for businesses and governments alike.

Identity also looms large on the radar screens of governments concerned about illegal immigration and terrorism. But there is a delicate balance to maintain. Lax controls

may appear to roll out a “welcome mat” for international criminals. But border controls that are too tight can slow international trade and tourism to an irritating crawl.

Increasing globalization, terrorist threats and online fraud are prompting governments and businesses to search for more intelligent identity solutions. Technology developments and scientific progress are paving the way for new solutions with biometrics. Biometrics help strengthen identity systems by adding in physical or behavioral characteristics (e.g., fingerprints, facial structure, iris structure, signature, gait) to the identity information. Accenture Technology Labs, the technology research and development organization of Accenture, has been researching this technology to understand the impact of biometrics-based systems that deliver greater accuracy, speed and convenience for enhanced performance of governments and businesses.

“Phishing” lures Internet users to what appear to be trusted bank or government sites through spam and pop-up messages. At the fake sites, unsuspecting users enter in bank account information, credit-card numbers, passwords and other confidential data. Thousands of people have been hoodwinked in such scams, and their revealed data can be used to apply for credit, obtain cell phones, print fraudulent checks on personal computers, or apply for government benefits.

1. Aberdeen Group: “Identity Theft: A \$2 Trillion Criminal Industry in 2005”, May 2003.

# What is identity?

Our sense of identity is assumed so that many of us take it for granted. We expect people to know us and trust what we tell them. But what exactly is identity, and how do we go about determining if the stranger seeking access to our offices or website is truly who he or she says she is?

"Simply keying in some personal data—which can be stolen in a phishing scam or fishing through garbage and finding old credit-card and bank statements—is no longer enough to assure identity and deter fraud."

Identity can be thought of as a set of characteristics uniquely associated to a person. There are three attribute types: primary (e.g., name, date of birth), biographical (e.g., schools attended, marriage) and more recent biometric methods (e.g., voice, hand geometry, iris, ear shape).

Businesses and governments employ systems, usually electronic, to store data to establish whom to include or exclude. In these systems, a process of enrollment records characteristics of individuals in a data store. Once an individual is enrolled, he or she receives a token—a passport, driver's license or smart card with printed or embedded information—as proof of identity.

Because Internet transactions continue to increase, organizations are upgrading their online ID systems. Simply keying in some personal data—which can be stolen in a phishing scam or fishing through garbage and finding old credit-card and bank statements—is no longer enough to assure identity and deter fraud. Consequently, organizations should look to biometrics to add another layer of assurance to establish and confirm identity.

# Increasing complexity, fragmentation and frustration

Whether by accident or design, identity schemes have grown in complexity and diversity. Efforts for standardization are under way by various organizations—including the BioAPI consortium and International Standards Organization—but guidelines are not yet ready or being widely followed.

Local and regional government agencies (e.g., health, motor vehicle, voting) follow protocols and require different tokens to national identification schemes (e.g., passports, visas, residence permits). Consequently, people's wallets and purses bulge with a growing number of cards and identity papers.

Accenture has identified four broad models among national governments to establish identity:

**Common law** (US, UK, Australia, Canada), with no national ID card or identifier, and people relying instead on drivers' licenses and passports.

**Civil law** (most of the original European Union countries), with a mostly compulsory national ID card.

**Nordic model** (Denmark, Sweden, Norway and Finland), with a centralized unique identifier, and optional digital certificates on private-sector cards (e.g., banks).

**Asian model** (Malaysia, Hong Kong and Singapore), with compulsory multipurpose electronic ID cards.

Several South American countries use the civil law identity scheme, as do many African nations, where biometric ID techniques are growing in acceptance. Mauritania and Nigeria require fingerprints for citizen identification, and Uganda uses face recognition for voting purposes. In South America, Peru stores fingerprint information in bar codes.

The weakest link of current systems is enrollment. In other words, if an individual can easily be entered into an identity system by submitting false documentation, the system has serious flaws. Ahmed Rassam, who confessed participation in a plan to bomb the Los Angeles airport during New Year's 2000, obtained a valid Canadian passport after having obtained a blank, stolen baptismal certificate. (An historical note, by the way: birth certificates were introduced to record life-expectancy statistics and were not intended to form the basis for strong personal identification.) In addition, seven of the 19 hijackers in the 2001 terrorist attacks in the United States held valid drivers' licenses that were obtained with phony documents. Once a criminal acquires one convincing false token of identity, it is increasingly easier to solidify the illusion with additional papers and supporting documents. Lax enrollment processes can pave the way for serious crime and catastrophe.

# We need security, but what about privacy?

Identification is not always required nor wanted. People expect anonymity at certain times: walking down a city street, seeing a movie, telephoning for quotes to compare prices, participating in surveys or clinical trials. At other times, establishing identity may be required initially (to determine voting eligibility, for example) but not later on so as to keep private the choices made by an individual.

As with other technologies, biometrics are not intrinsically good or bad. Their application needs to be judged by intent and usage. In the futuristic movie "Minority Report," the law-enforcement officer played by Tom Cruise has his retinas scanned to gain access to high-security areas. This seems to be a worthwhile and convenient application of biometrics for work-related security. But the film also depicts a "Big Brother" environment as sensors scan the hero's eyes in public spaces to establish his identity and personalize holographic advertising messages. Since he seems unable to escape being bombarded by promotional messages, this application of biometrics seems invasive and offensive.

Privacy issues are not exclusive to biometrics, and businesses and governments have recently tightened procedures and regulations to keep personal data from being misused or falling into the wrong hands. In Accenture's view, it is in the best interests of organizations to regulate themselves through the systematic development of trust.<sup>2</sup> A company that is known to violate the privacy of customers is likely to lose business to competitors as word of ethical lapses spreads. The Organization for Economic Co-operation and Development has an Information and Privacy group working to promote a "global, coordination approach to policymaking ... and to help build trust online".<sup>3</sup> In addition, the BioPrivacy Initiative of the International Biometric Group seeks "to increase the likelihood that biometric technologies, when deployed, will be as protective of personal and informational privacy as possible".<sup>4</sup> Biometrics, for example, can strengthen privacy by denying access or release of confidential information to the wrong people.

2. For more information, visit [www.accenture.com/privacyandtrust](http://www.accenture.com/privacyandtrust).

3. The OECD ([www.oecd.org](http://www.oecd.org)) issued a report in April 2004 on "Biometric-Based Technologies," including privacy and information security issues.

4. For more information, see [www.bioprivacy.org](http://www.bioprivacy.org).

# Best practice relies on multiple factors

How will organizations deliver a stronger, more reliable ID infrastructure? Amid the increasing volume and speed of international travel and commerce, governments must perform a balancing act. They must weigh security concerns with the needs of business people and the desire of tourists not to spend half of their trips abroad clearing security. Similarly, when venturing online, some users have so many passwords and user names to keep track of that secret-access codes end up written on Post-It notes stuck to computer terminals—so much for network security.

The emerging wave of new systems aims for triple strength. In simple, non-technical language, they require something you **have**, such as an ID card or token; something you **know**—a PIN or password, or a shared secret; and something you **are**, supplied by biometric applications.

When it comes to biometrics, no one system is best in all cases, and acceptability is an obvious concern. Fingerprinting, for example, is often associated with criminal behavior, although the development of inkless fingerprinting removes some of this muddy taint. Members of some religious groups might not consent to a photograph of an unveiled face. Other people might wonder if there are health risks to iris scans (more accurate than fingerprints), and people with eye diseases might be excluded from being enrolled with this metric.

Consequently, Accenture believes the future lies in multimodal biometrics, which consists in using a combination of several biometrics, depending on the application, individual and interaction channel. More in-depth study needs to be conducted to identify the most suitable biometrics for specific applications. No technology is 100% foolproof, which is why multimodal solutions are advisable, and why human intervention will be required in exceptional cases.

For speed and efficiency, identity needs to be recorded in electronic format for automation and network-based validation. Fortunately, content technologies enable the storage of biometrics data in digital format. In addition, Moore's law is still valid, and storage capacity and speed continue to race ahead at a remarkable pace. While the costs are relatively high now, they will come down with time and large-scale deployment.

As businesses and governments head toward electronic solutions, it is important to keep in mind there needs to be a transition (i.e., backward compatibility) with paper. This can be achieved in the near term, for example, by travelers carrying a smartcard version of a passport along with a traditional paper version.

A likely success factor in biometric solutions is giving people a choice to opt-in for more advanced technologies and convenience. In Spain, the Baja Beach Club in Barcelona offers patrons a choice between a standard access card and a radio frequency identification (RFID) chip, about the size of a grain of rice, implanted under the skin of the triceps. A scanner reads the microchip and sends out a radio frequency signal. The chip enables patrons to jump the queue for club entrance and to have drink purchases tracked and paid for without carrying cash.

# Innovative biometrics applications in government and industry

Another example can be seen at Galp Energia, an oil and gas company formerly owned by the Portuguese government. Galp Energia set out to become the world's first petrol-station operator to install a thumbprint biometrics payment system. Accenture was part of the team that helped develop this solution. Within four months, customers who elected to join the scheme conducted transactions 75 percent faster and company performance has improved, as have customer satisfaction ratings.

Additional biometric applications can be found in fleet management. International attacks on fuel-laden tankers have prompted security officials to include trucks on their lists of potential terrorist targets. To help prevent dangerous and costly incidents, Accenture has developed Transport Security Services, a prototype to provide security throughout a truck's journey from manufacturing plant to delivery point. Biometrics, in the form of fingerprint technology, are used to identify the driver before the truck door can be opened, thus ensuring that only authorized personnel can drive the truck.

A large number of biometric trials and full-scale deployments are under way for national identity and specific government functions. They are proving that electronic ID schemes are feasible and deliver tangible benefits. For instance, the US-VISIT program, which is taking digital photographs and index-finger scans of visitors at a number of US ports of entry, processed nearly 4 million foreign national applicants for

admission in the first year. Since inception, US-VISIT has prevented 372 known criminals and visa violators from entering the country.<sup>5</sup>

While people tend to think first of public safety, identity systems with biometrics will provide a wide range of advantages for individuals, businesses and governments. Citizens and businesses stand to face a reduced risk of identity theft. They will also benefit from greater convenience in access to services and benefits, which will be made easier for honest citizens and more difficult for those who aren't. In terms of government operations, citizens can expect to see more efficient use of tax money, with better detection of fraud and more accurate control of service and benefits.

The future of identity, after all, is not only to keep the wolves from the door, but to deliver innovative, high-performance solutions that efficiently speed the delivery of products and services to trusted individuals.

"International attacks on fuel-laden tankers have prompted security officials to include trucks on their lists of potential terrorist targets. To help prevent dangerous and costly incidents, Accenture has developed Transport Security Services, a prototype to provide security throughout a truck's journey from manufacturing plant to delivery point. "

5. [www.dhs.gov/us-visit](http://www.dhs.gov/us-visit); Fact Sheet: Year One of US-VISIT: A Historical Year of Successes and Accomplishments, January 2005

"The future of identity, after all, is not only to keep the wolves from the door, but to deliver innovative, high-performance solutions that efficiently speed the delivery of products and services to trusted individuals."

Copyright © 2005 Accenture  
All rights reserved.

Accenture, its logo, and  
High Performance Delivered are  
trademarks of Accenture.

## About Accenture Technology Labs

Accenture Technology Labs, the dedicated technology research and development (R&D) organization within Accenture, has been turning technology innovation into business results for almost 20 years. The Labs create a vision of how technology will shape the future and invent the next wave of cutting-edge business solutions. Working closely with Accenture's global network of specialists, Accenture Technology Labs helps clients innovate to achieve high business performance. The Labs are located in Chicago, Illinois; Palo Alto, California; and Sophia Antipolis, France. For more information, please visit our website at [www.accenture.com/accenturetechlabs](http://www.accenture.com/accenturetechlabs).

## About Accenture

Accenture is a global management consulting, technology services and outsourcing company. Committed to delivering innovation, Accenture collaborates with its clients to help them become high-performance businesses and governments. With deep industry and business process expertise, broad global resources and a proven track record, Accenture can mobilize the right people, skills, and technologies to help clients improve their performance. With more than 100,000 people in 48 countries, the company generated net revenues of US\$13.67 billion for the fiscal year ended Aug. 31, 2004. Its home page is [www.accenture.com](http://www.accenture.com).