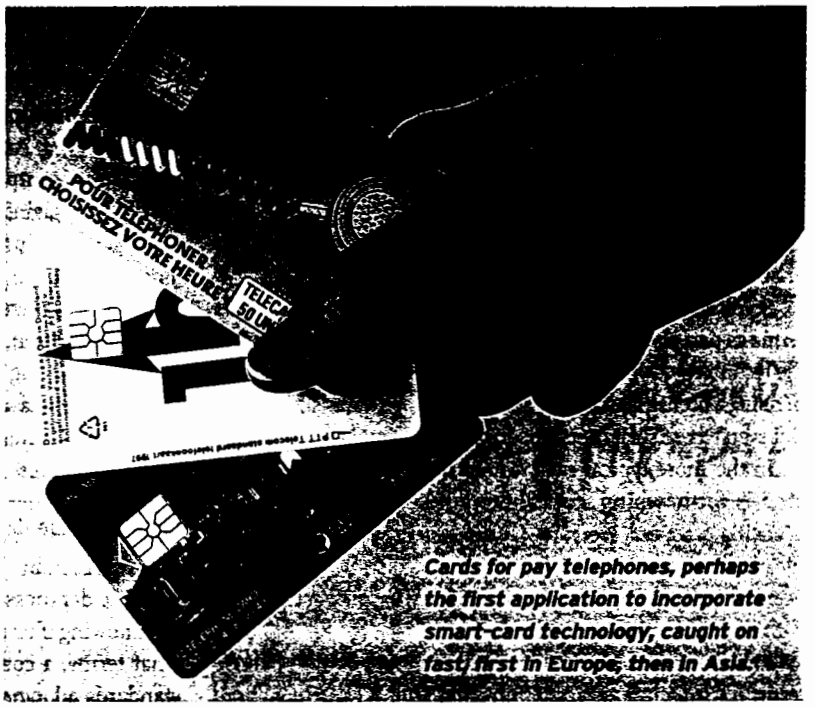
Smart Cards, Widely Used In Europe, Migrate to United States

They're getting an extra boost from 11 September security concerns

SECURITY • In mid-January, the American Association of Motor Vehicle Administrators, Arlington, Va., representing all 50 U.S. states, agreed to develop a common approach and common standards for upgrading drivers' licenses. They want to embed biometric information, such as a finger or palm print, iris or facial scans, or even DNA data, into the licenses to turn them in effect into a national ID firmly linked to the holder. The methods of data encoding under consideration include magnetic stripes, bar codes, optical scanning, and smart cards incorporating chips—a technology well-entrenched overseas in banking, healthcare, and telephony, but with barely a foothold in the United States.



Cards for pay telephones, perhaps the first application to incorporate smart-card technology, caught on fast, first in Europe, then in Asia.

Though U.S. natives like to think they lead the global pack in technology, in the case of smart cards, the country has lagged steadily behind Europe—France especially—and Asia. Until recently, just about the only U.S. application to be invaded by smart cards was the public laundromat, where moisture made magnetic swipe cards unreliable. Now the cards are beginning to make inroads in other areas, notably personal identification, which has loomed larger amid security concerns after the 11 September terrorist attacks.

They may still be an unpromising candidate for use in U.S. identification cards, but quite a few other countries have adopted them as national IDs. In Sweden, Finland, and Malaysia, for instance, they do double duty as authentication cards for government services and financial transactions.

Smart cards took off in Europe about a dozen years ago, when national telephone companies outfitted their awkward pay-phone systems with them. Previously, special tokens were required in some countries, while in others, the pay phone itself was overly complicated. Plastic smart cards, embedded with microprocessor chips and ample memory, caught on fast, and then invaded other areas, such as national healthcare.

Europe's edge

Relatively small markets and government-controlled businesses aided Europe's adoption of smart cards in many sectors. "In Europe, you meet with a few ministers, and 80 million health ID cards get ordered; in the United States, you have to navigate local, state, and federal bureaucracies," observed Charles Cagliostro, executive director of the Digital Security Initiative of the Smart Card Alliance Inc., a trade association in New York City. "It's the same situation in banking: European countries are dominated by four or five banks, while the United States has 9000."

In banking, because European data networks were not as reliable as those in the United States for transferring funds, the need was for a card capable of authorizing payment. And money could be held in the smart card itself.

Of course, the magnetic stored-value cards of some U.S. transit systems also contain a sum of money or number of units, with money or units subtracted from the card's balance with each use. In this respect they resemble smart cards. But the latter can hold much more infor-

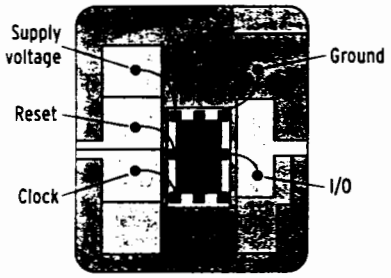
NICHOLAS EVELEIGH

PEIDONG YANG

mation—up to 64 kB, versus 200 bytes—and can do more elaborate processing. Plus, in certain operating environments, the smart cards have a distinct edge.

But now, as smart-card technology has advanced further, and the cards have continued to catch on elsewhere, potential U.S. users are paying them more serious attention.

Of special appeal are applications that consolidate functions performed at several locations within a locality or region, involve tougher methods of identification, and offer wireless transmission. Already Royal Dutch/Shell, the U.S. Department of Defense, and others have combined company ID badges and computer passwords into one smart card. And



The gold square on a smart card [visible on the pay phone cards on the page opposite] consists of contacts with leads going to an IC buried under the center of the square. The arrangement of contacts varies among applications, but is standard for each individual application.

computer systems such as Microsoft Windows 2000 and XP are now equipped with a built-in smart-card reader interface.

In October, Cubic Transportation Systems Inc., in San Diego, Calif., conducted a successful test of the smart card with the Washington, D.C., transit system. Participants used a single wireless card that stores a sum of money for paying for local public transportation and parking plus information for workplace access, speeding up transit times and burdening them with fewer cards.

In another recent demonstration, Netsmart Technologies Inc., in Islip, N.Y., is working with California's San Joaquin County to facilitate a county law, in effect since July, mandating treatment for nonviolent drug offenders. An offender is issued a card that tracks every class, medical appointment, counseling session, and probation officer meeting, and deposits the information in a central databank. The card is inserted into a computer plug-in and can communicate with several platforms, including many

Two companies selling this technology are Electronic Data Systems Corp., in Plano, Texas, and Precise Biometrics, in Lund, Sweden. Both make machines that read a person's palm or fingerprint and compare it to information stored on a smart card. The units are already in use at some airports to expedite travel through customs or to block trespassing into secure areas and IT systems.

"The debate now is if this type of security could have prevented the events of 11 September," said Cubic Transportation's chief technical officer, Walt Bonneau, whose firm opened a new security division last October to address the issue. "We believe this technology has many of the attributes that could have moved the industry toward 9/11 prevention. But no one security system is without fault. A totally integrated security system using smart cards, database, biometrics, electronic gating, X-ray, and skilled human intervention would have provided significant security."

–Susan Karlin

PEIDONG YANG

NICHOLAS EVELEIGH

BRIEFS

NANOWIRES GET NANOLAYERED. In the first seven days of February, three research groups announced that they have independently developed nanowires—shafts of semiconductor with diameters measured in nanometers—which for the first time consist of regularly alternating types of materials rather than just a single material. The researchers, from the University of California at Berkeley, Lund University in Sweden, and Harvard University, Cambridge, Mass., created nanowires that alternate between silicon and silicon germanium, indium phosphide and indium arsenide [see photo], and gallium arsenide and gallium phosphide, respectively. The Harvard team also developed n- and p-type silicon and indium phosphide. Experts say the breakthrough will lead to pn junctions, coupled quantum dots, even heterojunction bipolar transistors on single nanowires, and could be the building blocks of nanoelectronic circuits.

HP'S DATE WITH DESTINY. On 19 March, Hewlett-Packard Co. shareholders will vote on the proposed merger with Compaq Computer Corp. The vote will bring to a close the battle between HP executives and Walter Hewlett, a dissident board member and son of the company's co-founder, who opposes the merger. Both sides claim to be gaining support among institutional investors, who own a majority of the company.

DOUBLE CROSSING? As investigators examine the finances of Global Crossing Ltd., Bermuda, the failed optical-fiber network capacity marketer, there's a sense of déjà vu. On 6 February came disclosures reminiscent of Enron: of an internal auditor's warning, well before the collapse; of irregularities in the company's guidance to investors; of the chief executive officer unloading huge stock holdings; and of the firm's accountant, Arthur Andersen, turning a blind eye.