The Future of Identification Card Technology

By Joel Hershkowitz, Idesco Corporation

It was time for the renewal of my library membership. So I entered the administrative office area where I promptly filled out a new application form. Then an instant photo camera captured my image. It was developed immediately, placed on a preprinted card with the organization's preprinted logo. Then a clerk typed in my name on the card and had the card laminated. It was then handed to me. The clerk told me I was ready for another year at the library. "Show the card at the front desk and you can enter the facility," he said. I looked at him and I said, "Wait just one second. Is this what you are giving me? This isn't the year 2000. It is 2005. Shouldn't my card have a magnetic stripe on the back to track my movements. Where's the DNA embedded hologram? How about the smart card chip containing my billing information and all my vital health information? Shouldn't you have a digital photo of me? Or maybe this library shouldn't be the one issuing me an ID card. Maybe it should come from a government agency as part of a Universal National ID Card.. And where is the special customized corresponding ID cards for my kids? Then again, do I need to carry around an ID card at all? After all, you can use a reader to check my hand, or perhaps my eyes, and be able to confirm my identification in seconds."

At one time an ID card was used for some very simple purposes. To show you were a member of some type of a closed organization that probably charged a fee to join, or at the very least a group that had something valuable to protect. The fact that you were issued a card was proof enough that your membership was valid. After all, why would someone falsify a card? To get in for free? To steal something? To get a drink when they are under age? To drive a car when under age? To purposely inflict damage to people or equipment? Well, as we all know, I am sorry to report, the answer to all of those questions today is YES. Today, we have to spend a lot of money to save a lot more money. And to possibly save our life! So the more you spend on making the ID card secure, the more technology you will have built into it. However, that doesn't mean you have to go into "overkill" when developing a suitable ID card. Build in enough security for your situation and then maybe just a little bit more. Here are the newer types of ID cards you already see and additional cards you most certainly will see in the future.

A "magstripe" card can be quite effective. It is designed with three "tracks" to store information. Track 1, which was designed by the International Air Transportation Association, contains alphanumeric information, i.e., a person's name. Track 2 was designed by the American Bankers Association. It contains numeric information, i.e., numeric information. Track 3, designed by the Thrift industry, contains information that can be updated. It is the "active" part of the card. Magstripe cards are available in two types: High-coercivity-(Hi-Co). This type is hard to erase and is ideal for cards used over and over, such as an ID card used to get into a facility, then through card readers and various locations within a facility, then back out again. Low-coercivity magstripe cards use a lower amount of energy to record, are cheaper, but shouldn't be used for day-in, day-out operations. The information is "coded" onto the tracks using "AAMVA" and "ISO 7811" standard type coding. and can only be "decoded" by a corresponding Magnetic Card Reader.

Instead of a magstripe, an ID card may contain a "bar code." It may have a one-dimensional barcode or a two-dimensional barcode. A typical Code 39 symbology encodes numeric and alphanumeric information. A typical "interleaved 2 from Five" barcode symbology uses only numerics. A major advantage of a one-dimensional barcode is that its information is carried throughout the height of the barcode. If part of that height is cut off, the barcode can still be read.

A major advantage of a two-dimensional barcode is that it can make use of the entire vertical dimension of the code and thus contain much more information. The problem, however, with a two-dimensional code is that if part of the code is cut off, the barcode becomes unreadable. Both have their important place in ID cards. One-dimensional are ideal for numbering applications, two-dimensional where a great deal of information is required. Another advantage of all barcodes is that the cost is low to have them printed on a card. The real expense is limited to the equipment needed to read the barcode.

These cards may also contain a "debit stripe." Typically, small cash values are maintained via this stripe, used for such things as vending machines. This is an offline system where all the value is on the ID card. Money can be added to the card at any time. However, if you lose this card, all of the money value will be lost as well.

Weigand ID badges add extra security. They are very hard to reproduce. Each badge contains strips of wire that are embedded into the bade. The strips send electric pulses in the form of 0 or 1. The placement of the wires determines its encoded number.

Proximity (prox for short) ID cards are becoming increasingly popular. As they do not have to be read by having them "swiped" through a card reader, they have very little wear. A tiny antenna embedded in the cards becomes "activated" when it is approximately 2 1/2" to 24" from the reader, depending on the particular system being used. Prox cards can store quite a bit of information and are ideal for use by government workers, military personnel and students, to name a few. As the card passes through the "reader," information stored on a microchip on the card is received, verified in the main database and a detailed record maintained. As companies' technologies change over time, "multi-technology" prox cards can play an important role. This type of a card can combine prox card technology with another technology, for example, a magstripe. So a company that has been using magstripe cards in one building and now wants to use prox card technology in another facility they are updating or recently purchased can use one ID card.

Introducing the Smart Card

When considering one ID card for many different uses, the way to go is with a "smart card." Designed to be the size of a credit card, a smart card contains an embedded 32-bit microprocessor, unlike a magstripe, barcoded or prox card, which all operate with information stored on a computer. And the

computer in turn reads a code on the card to allow or disallow access. With a smart card, the information is stored right on the card.

Smart cards can store up to 400 kilobytes of ROM. Talk about changing technologies: it wasn't that long ago that the smart card had a 16-bit microprocessor and 346 kilobytes of ROM. We have to see what the "future" brings. We might not have to wait too long.

Should you desire, there are companies offering a multifunctional card (just about everything on one card). They are a combination smart card and proximity card with a magstripe or barcode and hologram design.

How a Smart Card Operates

The smart card contains the microprocessor which contains the data, and it communicates with the card reader known as a Card Accepting Device or CAD. Packets of data are transmitted at 9,600 bits per second through a serial bidirectional transmission line.

The data sent back and forth between the card and the CAD are encrypted using a mutually active authentication protocol. Security is obtained by setting up the data in a logical "tree" order. There is a master file standing alone at the top, followed by a row of elementary files (or subsets to the master file) and dedicated files. The dedicated files act as a functional group of files with a group of elementary files under it. It sounds complicated, but in effect it acts in a similar manner to how one sets up directories and files on a computer. Each part of the "tree" is given security "rights." An application searching for data from an elementary file or a complete dedicated file must have the appropriate rights to the file to enter. There are at least five levels of security with a smart card: 1. Always (ALW): Access of a particular file will be able to be performed without any restrictions at all. 2. Card Holder Verification 1 (CHV1): Access can only be performed when the Card Holder Verification has been validated. 3. Card Holder Verification 2 (CHV2): Access can only be performed when the next level Card Holder Verification has been validated. 4. Administrative (ADM): The Administrative Authority is responsible for this level of access and security. 5 Never (NEV): Access to the file is forbidden.

The Future Is Now

If you aren't using a smart card today, get ready. The future is now. Smart cards are and will be used for military identification, national, state and local identification, electronic money, transit cards, airplane tickets, stored medical data, driver's licenses, telephone cards, just to name a few. Government agencies, both large and small companies, utilities, medical facilities, etc., will be switching to these cards (if they haven't already because they offer many advantages. These cards are very cost-effective. They are paperless! They are easy to encrypt and hard to "hack," making them very secure. It will be easier to confirm one's identity at an airline terminal, making it safer for us all. And they just might reduce the long lines at the ticket counter and security gate. Emergency and personal medical information can be stored on them, hastening the possibility of getting the correct medical care administered to the owner of the card. Your wallet will become thinner, too, with just one card handling all of your transactions.

So with all the advantages mentioned and the technology in place today, why haven't governments and corporations gotten together to get this single card working in as many areas as possible? Well, it turns out there are probably as many reasons that question the use of such a card as there are advantages. If a card is used by so many different organizations, then whose card is it? That is, from whom does one purchase the card? And who provides the technical support if there is a problem? What happens if the card is stolen? If we think that having a Social Security number stolen from us is a problem, imagine the problems people would have with a card that contains virtually every piece of important information about them.

Time for the Government to Step In?

If our federal government were to decide that smart cards would be ideal as a means of security identification, then they might also solve all of the disadvantages of the card. They would be the one and only issuers of the card. They would provide technical support. They could foot the bill for additional security features if the card was lost or stolen. Or should we say, we would foot the bill with our tax money? But, in return we could have a card that could contain very positive ID for us.

One of the biggest problems with smart cards at the moment is that they are not interoperable. So a smart card that has been purchased from a particular vendor will not work with applications designed to work with a different vendor's smart card. Therefore, regardless of who would ultimately be responsible for controlling the overall distribution of smart cards, all the cards produced must be interchangeable. The National Institute For Standards And Technology (NIST), working with the Government Services Administration (GSA), developed a smart card interoperability specification and testing program. This program has also been introduced to the International Standards Organization (ISO), and this problem has been for the most part solved, but there is not yet a worldwide standard.

However, the United States Government is implementing a smart card under a program sponsored by the Department of Homeland Security. FIPS 201 is the Federal Information Processing Standard of the United States Government. It describes the type of personal identity verification that is required for both federal employees and contractors who use federal facilities.

The goal of FIPS is to have, for the first time, a kind of "universal" ID Card that can be used by employees and contractors at ALL federal facilities. For example, a federal employee in a federal agency in Atlanta, Georgia, can use his or her ID Card in a different federal agency in another state if for any reason it was necessary for that person to do so.

The intent of Homeland Security was that in the case of an emergency such as a terrorist attack or possibly a severe hurricane, i.e., Hurricane Katrina, or any other type of catastrophic event, all federal agencies that will be required to respond to the emergency will not be held up by the identification process required for one to have access to the affected area(s). It can also be an effective tool for monitoring the location of the individuals working in those areas. And it can be used to muster those individuals at the end of a work period of any length.

FIPS is simply an effective access control system. An individual has his or her ID (smart card) scanned and read in a card reader. The information is registered. The person is given access. The person's movements are updated as the individual moves through different access points. Information is then updated upon departure from the area. The management software of the ac-

cess control system is used to control and evaluate the movement of the individuals working within the designated area. FIPS is not only used for emergency situations. It is an effective method for any interaction required between federal agencies. The National Institute of Standards and Technology (NIST) created the FIPS 201 Standard. The General Services Administration (GSA) evaluates and approves the equipment required for FIPS programs. But this government card does not have the personal information that can allow it to be used when these government personnel are not at their jobs and are then ordinary citizens.

What Would Be Some of the Features of a Virtually Secure Smart Card for the General Public?

It includes a series of biometric features: fingerprints, iris scans, facial recognition, voice recognition, DNA information, signatures. A ***virtually secure*** card could actually mean the end of the need for Social Security numbers-and thus put a big dent in identity theft.

So, based on that information, it would seem that all U.S. citizens would jump on the bandwagon and vote to get the cards into circulation immediately. Right? Wrong. According to the Consumer Sentinel which collects information from the Federal Trade Commission and 150 other organizations, there were over 635,173 consumer fraud and identity theft complaints in 2004, 542,378 complaints in 2003 and 403,688 complaints in 2002. Those are frightening statistics. Here's another one: since 1997, there have been over two million complaints.

In addition, George Orwell knew the reason back in 1948. YOUR PRIVACY. If you knew that all of your personal information was in just one database, and that it was located in a card in your wallet, would you trust the security you have been told it had? Many believe that a national identification card of any type will allow the federal government to monitor the financial transactions and the movements of all of us. And there is the possibility that your card may be confiscated by a government agency in a legal case against you and, in a sense, used to testify against you. You may take the Fifth Amendment and not testify against yourself. But what about your card? Would it be totally protected by the Fifth Amendment? Should we leave the answer up to the Supreme Court? In addition, would you be concerned that perhaps a medical facility in adding additional personal information about you on the card would be able to access how much money you had in your savings and/or checking account? Or how about going on a job interview and having your card used as a means of checking your complete background. Furthermore, we have seen how hackers have been able to get into the most secure credit card databases. With many of us having more than one credit card and debit card, can you imagine someone getting all of that information in one quick keystroke? And what if the hacker was a terrorist? One of the things we fear most, a terrorist being able to compromise an airplane or get into a building, etc., and here in his very hands could be the key to destruction. So then the future may not hold such a national ID Card after all. Right?

Well, a congressional vote has recently endorsed standardizing driver's licenses made in this smart card manner. Known as "The Real ID Act," it "requests" all states to design driver's licenses by the year 2008 that would comply with U.S. standards. The goal-to combat terrorism. Those states that do not comply will find that their residents will NOT be able to board a plane. What do individual states think of this plan? The National Conference of State Legislators (NCSL) estimates the national Real ID Act would cost states as much as $13 billion to put into place. However, one very good aspect of the Real ID Act is that it gives authority to the Department of Homeland Security to specify machine-readable technology. So all states would be on the same page when it comes to scanning not only this type of ID, but biometrics such as fingerprints and retina scans as well. That could really interfere with terrorist plans.

Moreover, the federal "Help America Vote Act" of 2002 requires people to show a current and valid photo ID when voting for the first time in a federal election. With 2008 being the target date for standardized driver's licenses, most likely a type of smart card will become the "acceptable" ID for first-time voters. This Voter Act, though, is a way to show that ID cards, smart or otherwise, as well meaning as they may appear on the surface, can in fact turn out to be detrimental. For example, as the American Association of Retired People (AARP) points out, the poor and the elderly (whom, of course, they represent) may not own cars. They may not have driver's licenses to show. Nor are they likely to have other acceptable IDs, such as U.S. passports, U.S. Government employee ID cards, or U.S. military photo ID cards. Although this law is now in effect, it should be tossed back to the drawing board for refinement. How about having the U.S. Government issue a universal smart card, for instance? If the idea is to prevent terrorism (i.e., prevent illegal immigration), these are federal, not state, problems. Nevertheless, this looks like the future of ID cards.

Facial recognition technology is beginning to be used in a number of airports around the world. Here a reader captures a 3D biometric image using optical technology, structured light, algorithms, a projector and a digital camera. As a person nears an entrance, a reader captures the facial image and determines to accept or reject it. The facial images that are captured are so exact that the reader can distinguish even between identical twins. At an airport the facial image can be captured and linked to the barcode or magnetic stripe on the boarding pass. This insures the right person enters the aircraft. Baggage stickers can also be scanned. The same technology is and will be used for airport personnel as well. Trusted traveler programs have and will be set up to allow people who meet certain criteria to have their biometrics stored on a card. Those people can then have their card information matched at the airport gate to a live image for easy access to the plane. These programs have already gone into effect in the entire group of New York City metropolitan airports as well as in major airports throughout the country. Within just a few years, they will likely be in every airport in the country. Similar card/live image matching will soon become popular at hospitals and labs, ATMs, time and attendance systems, as well as government agencies.

How about no ID cards at all? YOU can be your own ID card! With your own blood as the authentication. We all have our own individual blood vessel patterns. And they are extremely hard, if not impossible, to recreate. Instead of a reader checking a fingerprint, it would look at the image of a blood vessel pattern. If that pattern has been entered into a security system, it will make an instant identification. Watch for this to be used to gain access to a facility,

check on work attendance, pay for purchases and borrow money. And you won't ever lose it!

Then there is the botanical DNA encrypted hologram. Here plant DNA is extracted and used as an encrypted molecule that is embedded into materials such as inks, papers, holograms and microchips. These are then integrated into products such as currency, textiles, passports, ID cards and access control devices

These are just a few of the things we will be seeing very shortly. We won't be needing a time machine to view them. They are in production right now.

The Future of Our Future-Our Children

Each day in the United States, up to 2,000 children are reported either missing or kidnapped. Many companies have produced, or are in the process of making, child-specific ID cards. Copies of the cards are given to the parents, grandparents, other close friends and relatives and to law enforcement agencies. Similar to a driver's license, the cards contain a picture, a fingerprint and general information that can help police when looking for the child, or when the child has been recovered.

Joel Hershkowitz is Director of Marketing at Idesco Corporation. He has 26 years experience in the security industry and holds a degree in Business Management from Fairleigh Dickinson University. For more information please visit www.idesco.com.

SOME TYPICAL SMART CARD USES

Security
- Store credentials
- Encryption
- Decryption
- Store fingerprints
- Store biometrics
- Store DNA

Transportation
- Commuter passes
- Plane tickets and boarding passes
- Baggage claim
- Subway and bus passes (mass transit)
- Employee (pilot, etc.) authorization

Banking
- Credit cards
- Debit cards
- Checking
- Savings
- Loans

Schools
- Attendance
- Lunch programs
- Snacks
- Library use
- Tuition
- Grades

Retail
- Gift cards
- Promotional cards
- Loyalty cards
- Store credit
- Parking meters
- Parking garages
- Communications
- Client authorization
- Digital signatures
- Client-to-server authorization
- GSM (Global System for Mobile Phones)
- Phone cards
- Online services

Health Care
- Personal medical records
- Insurance information
- Billing
- Donor information

Military/Government/Industry
- Identification access control
- Computer use
- Personal records
- Purchasing

Personal
- Password alternatives
- Driver's licenses
- Visas and passports
- Immigration cards
- National ID
- Voter registration
- Library cards
- Health clubs
- Child watch