Smart Cards

The ISO 7816 Smart Card is a conventional plastic financial transaction card into which an integrated circuit chip is embedded. The chip is reached electronically through surface contacts, by radio frequency signals, or both with combination smart cards.

The PC Card is a thick bank card with capacity for multiple and larger IC chips. It is used in laptop and mobile computers to add features and functions.

The microprocessor and memory of the ISO 7816 Smart Card embedded chip make it a pocket and portable computer system. This introduces application functions and capabilities into the conventional plastic transaction card.

What is the Smart Card?

A Smart Card is a hand-held package with one or more IC chips and a communications interface. There are many versions. Several types have been or are in the process of being standardized. This material discusses two versions. First, the Personal Computer Memory Card International Association (*PCMCIA*) has standardized the PC Card. Second, the International Standards Organization (*ISO*) 7816 IC or Smart Card.

The PC Card

The PC Card is used in laptop and mobile computers. It offers memory extensions, communications interfaces, and input/output devices interface. Use of the PC Cards reduces the size and entry cost of the basic laptop or mobile computer. The PC Card is a physical package of 54.0 mm by 85.6 mm with a 64 pin connector. The PC Card comes in three thicknesses. Type I is 3.3 mm thick and is used primarily for memory devices. Type II is 5.0 mm thick and is typically used for input/output devices. Type III is 10.5 mm thick and is used for external functions, such as an antenna or for thicker parts, such as a rotating mass storage device. The PC Card is being used in other devices, such as personal Computers, electronic cameras, cellular phones, and security access systems. An effort is underway to define a smaller PC Card for pocket devices.

PC Card standards are controlled by the PCMCIA in San Jose, California, (www.pc-card.com, 2635 North First St (suite 218), San Jose CA 95134 USA. www.pcmcia.org, tel 408-433-2273, fax 408-433-9558). The organization also provides for and supports software. It is needed to enable the devices to operate, to interface, and to maintain security controls. PC Card technology features include the following:

Card and Socket Services Card services software manages system resource allocation. Socket services recognize card insertion.

Cardbus Allows 32 bit bus mastering at speeds to 132 Mbytes per second, at a clock frequency of 32 MHz.

Card Information Structure Software that describes the card characteristics to enable the host to configure its interface automatically.

Execute in Place (XIP) Allows host operation directly from PC Card content.

Low Voltage Operation Enables 3.3 V or 5 V operation.

Multifunction Cards Allows mixing functions in one PC Card.

Hot Swappabilities Enabling card changing with power on in the host.

Zoomed Video Enables writing video directly to a host without a buffer.

The physical PC Card has the following elements:

Physical card package
Card interface, electrical and mechanical
Card metaformat, hardware and data attributes
Fat File system, operating system interface
Execute in place, application software execution

The PC card uses a 68-pin format, as follows:

28—address bus
16—data bus
6—power and ground
2—programming
7—control bus
5—status indicators
4—future use

PC Card Security Application

Several applications show the need for the chip capacity of the PC Card. The security application is a good example. A high security access card has these parts within the PC Card:

32 bit microprocessor

Impenetrable storage areas:

Nonvolatile—to more than 20 M Bytes Flash technology. Nonvolatile memory keeps its content when power is removed.

User IDs, application data, certificates, block decryption keys, transaction recording.

Proprietary software: for security management, C language library, and application program interfaces.

One or more encryption engines for DES (private keys), RSA (public key), and proprietary security algorithms. Larger chips are used to provide a coprocessor to improve performance of some security algorithms, such as RSA.

Possibly a biometric template for biometric entry or personal identification evaluation.

Digital signatures and certificates: Version, serial, validity period, subject, public key, issuer ID, signature to 1,000 digits, to 100 certificates.

J. Webster (ed.), *Wiley Encyclopedia of Electrical and Electronics Engineering*. Copyright © 2007 John Wiley & Sons, Inc.

There are other functions available in the PC Card including key exchange mechanisms, message digest (Hash) algorithms, and personal digital assistant (*PDA*)/personal computer (*PC*) interfaces.

There are several active PCMCIA committees considering new features, such as a physically smaller card and further security functions.

PC Card Applications

The PC Card offers parallel input and output to several IC chips. The enlarged physical capacity offers chip capacities that range from very large IC memories (more than 100 MBytes) to rotating mass storage devices (more than 500 MBytes). The added physical space allows use of stronger packaging. One vendor offers a bulletproof case for a security application PC Card. The security applications require PC Card physical capacity. Extensive memories are needed to store digital signatures and certificates. Some are as large as 4,000 bytes each, and one PC Card may need to contain more than 100 such certificates. In addition, the PC Card also carries a variety of encryption engines to encrypt and decrypt information in a secure message environment.

PC Cards for use as input or output devices also require added memory. For example, use of a PC Card as a modem interface for facsimile messages also requires memory capacity to store the facsimile message as received. This is required because the added memory card is removed to allow inserting the facsimile PC Card. More recent mobile computers have two PC Card insertion slots to provide for this added capacity. It is not unusual to find a small library of PC Cards supporting a laptop or mobile computer.

The PCMCIA

PCMCIA has more than 300 members. They represent hardware, software, and using organizations. Contact them for further specifications and membership. They also offer marketing services for promotion and education about the PC Card. There is a large library of supporting documentation and software available. There are several vendors offering design tools and services. (www.pcmcia.org).

The ISO 7816 Smart Card

The ISO 7816 Smart Card is a conventional plastic transaction card into which an integrated circuit (*IC*) chip is embedded. It has an eight-part surface electrical contact for card-to-card-acceptor communications. The ISO 7816 standards describe the interfacial characteristics between the contacts on the card and the card acceptor devices. It does NOT specify chip location or internal chip operating characteristics. That is left to the market forces between the buyer and seller of the IC chips. The ISO 7816 standards include the following:

7816-1: Physical card characteristics
7816-2: Dimension and location of the contacts
7816-3: Electronic signals and transmission protocols
7816-4: Interindustry commands for interchange
7816-5: Application and registration procedures (a common numbering system)
7816-6: Interindustry data elements
7816-7: Interindustry enhanced commands for interchange
7816-8: Interindustry security architecture and functions
7816-9: Commands for card management
7816-10: Electronic signals and answer to Reset
7816-11: Biometric functions
7816-12: Mobile use
7816-13: Banking card specifications
7816-14: Public Key based security
7816-15: Cryptographic applications

There are other standards for specific applications, such as cellular telephones, banking card transactional messages and also for advance versions, such as contactless (via radio frequency signals) and application and security architecture for banking. Contact your national standards organization for standards copies and status. In the United States contact the American National Standards Institute (*ANSI*) at 25 West 43 St (4th floor) New York, NY 10036, tel 212 642 4980, fax 212 392 1286, info@ansi.org

The ISO 7816 Contacts and Chip Interface

There are eight contact segments. Two are reserved for future use. Two are used to distinguish voltage levels (3.3 V or 5 V). The remaining four are input/output (serial), clock frequency, reset, and ground. Most chips are made from CMOS. The multiprocessor is 8 bits wide. There may be additional coprocessors on the chip for specialized computing functions, such as encryption and decryption. Each chip has several security features provided by the chip fabricator beyond those required by industry standards. These include, among others, voltage and frequency change detectors, and electronic fuses. The nonvolatile memory may vary up to 8,000 bytes. However, vendors are now offering memories to 16,000 and 32,000 bytes.

Combination cards with both contact and contactless (radio frequency transmission) interface are now entering use. The contactless cards speed passenger use in mass transit, reduce the complexity of the card acceptor, and decrease transaction times. There are also some applications in which the chip and a small amount of the surrounding plastic card are removed from a full card and then are used in other devices, such as cellular phones, pocket terminals, and point-of-sale terminals. These are called Secure Application Modules (*SAMs*).

Smart Card Types and Use

The 7816 Smart Card is a conventional, magnetic-striped, plastic transaction card containing an embedded integrated circuit chip and a communications interface. These cards are called integrated circuit chip cards, memory cards, chip cards, PC cards, cash cards, calling cards, electronic purses, stored value cards or Smart Cards.

One type of ISO 7816 Smart Card is used for coin replacement, such as in coinless telephones. This Smart Card has a chip with a small memory of under 1,000 bits. The second type of Smart Card has an IC chip which includes a combined microprocessor and a non-volatile memory of up to 64,000 bits or 8,000 characters. Both card types look the same externally. There is a set of eight electrical contacts in the same location on the face of the card. The small memory card, however, lacks a magnetic stripe and is not embossed. Both card types are used in the same telephones.

This discussion focuses on the microprocessor version. The Smart Card chip has a computer as the data entry point. It is an eight-bit-wide microprocessor with its own operating system and its own control program. Behind the computer are two memories. One is read only for computer programs (*ROM*) storage. The second is a read/write working memory, usually EEPROM. This memory is nonvolatile, that is, it retains its stored content when power is removed from the card as it is taken out of the card acceptor or terminal. The card has no power of its own. Programs are also executed from the read/write, nonvolatile EEPROM memory.

The chip is small, about 22 mm square. This is about one-tenth of usual chip size. Chips are not flexible. The plastic transaction card is flexible. The standards for the Smart Card include an expected maximum bending specification. Cards are carried in flexible wallets, pockets, and purses. The card with an embedded rigid chip, however, must survive moderate bending and they do. Failure rates from all failure types are less than 250 per million cards with the smaller chip.

Smart cards are used extensively in Europe (primarily France) and in Asia (primarily SE Asia). North America has used these Smart Cards for secure network access, portable data bases in multiple application cards for supermarkets, and secure identifiers for government (civilian and military) programs. The cards are physically compatible with today's magnetic-striped, embossed cards for transitional purposes. The magnetic-striped portions of the Smart Cards are usable in current magnetic-striped card acceptor units.

The memory of the microprocessor is divided, logically, into several areas.

Free Access Memory This portion of memory is access by anyone with a suitable card acceptor. It does not require a secure access code. This area duplicates the data carried on a magnetic stripe and is freely accessible. Another function of this area is storing medical information needed in an emergency medical facility. The absence of a security access code is for the occasion when the card holder is not conscious and, hence, cannot provide an access code to most important emergency medical facts.

Confidential Access Memory This area of the Smart Card memory is the location of application data. Access to each of a dozen or two applications is controlled by security provisions specified for each. The individual application content and its access rules are specified by the application provider. When the Smart Card is inserted into the card acceptor, application access is limited to those acceptors which are entitled to access. Access between application sections is prevented. For example, removing funds from a checking account to be placed into a telephone calling card area must pass through an intermediate process between two application providers. This prevents one application provider from gaining access to confidential data, such as account balances or credit limits of a second application provider.

Secret Memory This segment of memory contains information never accessible from outside the card. For example, it is the segment of memory where the expected Personal Identification Number (PIN) value is stored. That value is used internally only to make a PIN validation decision. The circuits through which an expected PIN value is inserted into the Smart Card memory are destroyed after the data loading. This is done with fusible segments controlled externally as part of the card personalization process.

Nonvolatile memory area is also allocated by applications. Each application has a specified memory area, specified access code, and specified content format. The format is needed to address memory segments required for application processing. This is similar to addressing segments of the memory in a large computer. The applications share memory segments, as in a transaction register or journal. All applications share the Operating System. This is a program which control input/output and data flow with the card logic functions.

Smart Card Application Attributes

The microprocessor Smart Card offers a new set of application attributes, compared with the conventional magnetic-striped cards:

Information Capacity. Information content is 12 to 400 times larger than the current magnetic-stripe track (39 digits) used by the financial transaction card industry. This allows extended customer data, multiple relationship accounts data, a transaction journal, application/account control information (control values, telephone numbers and business rules), and stored programs, as needed.

Dynamic Application Update. The content update is achieved by rewriting under secure controls, when the card is on-line to its control facility. Updatable account information, names and address, dynamic account limits, business rules for each application/account, and the addition of new account relationships and applications take place electronically. This results in extended card life and reduced losses by more timely limit controls.

In-Card Decisions:. The in-card logic and control values make "local on-line" transaction decisions for most routine transactions (to 90%). The in-card logic recognizes when to require a "central" on-line authorization to central site data.

Application Security Controls. Improved security is achieved through several features. Transaction access is direct or through a PIN or biometric entry. The Smart card also keeps a transaction journal for inquiry and audit trail purposes. Initial card use is preceded by an exchange of algorithmic values to determine if the Smart Card and its acceptor are mutually valid and acceptable units.

Communications Management. Communications management provides direct terminal dialing to application-oriented, remote control points. This is used when central on-line transaction control is required. This includes access protocols or procedures, telephone numbers, and communications billing numbers. These internal data reduce the card acceptors need for sign-on training and the time to enter data for transaction initiation.

Messages between the Smart Card and the Accepting Device

This standard (ISO 9992), applies to Smart Cards issued by financial institutions in retail financial applications for interchange. It describes the prescribed message types and content, as follows:

Part 1: Concepts and structures

Part 2: Functions

Part 3: Messages (commands and responses)

Part 4: Common data for interchange

Part 5: Organization of data elements

Smart Card Software. Smart Cards require the following three types of software:

Operating System This program operates the input/output and internal chip flow of information. Until recently, each Smart Card vendor provided its own operating system and related interfacial programs. Recently, several leading Smart Card providers have started a common operating system called MULTOS. The development effort is controlled by MAOSCO (MULTOS CONSORTIUM, 16-18 Monument St, London EC3R 8AJ, UK, tel +44(0)207 868 5073, www.multos.com). This nonproprietary "Open System" is expect to be a multiple industry tool. It permits products from different industries, such as GSM Smart Card cellular phones and EMV (Europay-MasterCard-Visa) credit/debit products.

MULTOS Multiple Application Control Program This program allows downloading new products or services into the Smart Card. It allows issuers to update, add, or change applications in an issued Smart Card. It allows adding application and security upgrades to issued cards when placed in a card acceptor. Card applications are kept separate in a multiple application smart card credit card by a highly secured firewall. That is a program designed to prevent one application from searching another.

Application Development MULTOS provides developers with an application programming language called MULTOS Executable Language (*MEL*). They also provide an Application Programming Interface (*API*) to develop high security, high integrity applications. APIs may be developed with "C" programming language. A member of the consortium, is working with Sun Microsystems to develop JavaCard V2.2.2. Java has been selected as the application interchange language by Smart Card vendors.

Security Software The Smart Cards have a built-in card-to-card security system. Other Smart Cards need a security solution for use in open systems, such as phones or Internet. The security software generates a digital signature. It is an encrypted identification to replace signatures and secure transactions.

Smart Card Terminals

Conventional terminals will be upgraded to read both magnetic-striped cards and Smart Cards. This includes point-of-sale units, automatic teller machines, cash registers, display PIN pads, and similar units. There are new terminal types appearing. These are associated with new communication services now coming to market. These units use Smart Cards as security entry devices, digital signature and certificate carriers, multiple application access devices and devices to interface with new services.

These new devices will expand further in the market. A number of TV set top units use Smart Cards to control TV signal descrambling, provide TV shopping, and expand the use of Internet financial transaction services. Card interfacing to these units cannot be handled by the conventional magnetic-striped transaction cards. The secure smart card operation in these new areas is described in subsequent sections.

The Prepaid Smart Card

A prepaid card is a machine-readable medium on which information is recorded representing an earlier deposit of funds. One of the common forms of the prepaid card is the mass transit ticket. Another replaces coins for pay phones. More than 80 countries use Smart Cards in pay phones. More than one hundred mass transit systems (trains and busses) use prepaid Smart Cards for fare payments. The approach decreases the remaining units of value by an electronic re-recording or card updating method. This continues until there is no value left and the card is discarded. The stored value ticket is like a pocket full of change which is purely machine-readable. If the ticket is lost, the coin value can be used by someone else. Use of prepaid cards is also migrating into other low-value transaction areas, such as fast food outlets, low-price restaurants, and vending machines. Noncoin machines cost less and are cheaper to maintain and service. The need for low-value but costly coins is reduced. Also, price increases need not be limited to the face value of the coins in issue in a particular country. Changes in price as small as three decimal places are easily accommodated by prepaid cards.

Prepaid cards made of paper have been used for many years. They were used for access to lectures in the 1870s. Their use to pay for telephone calls in France dates back to the central telephone offices in the 1880s. The mass transit use of the cards shifted from paper to plastic cards between the 1950s and 1970s. In the 1990s the focus has expanded to include the telephone. The major telephone companies in Europe are in the next phase of development in this area, smart card coin value cards.

The acceptor of a prepaid card makes important savings. Removing a coin receiver from a telephone reduces its cost. Servicing costs are reduced by a similar amount. Removal of cash also means less vandalism, less loss through counterfeit coins, and reduced out-of-service periods. Tariffs are set to increase in increments of as little as a third decimal digit.

The user has the convenience of not carrying, counting, and inserting coins, especially in a time of mainly paper currency. Security departments have to deal with a reduced number of devices containing coins of value. Prepaid card issuers enjoy the funds on deposit before the user spends them and a merchant claims the funds. The card acceptor saves the cost of handling cash, estimated at up to 6 percent of its face value. The prepaid card removes coins and currency notes from the payment process, with significant gains in productivity and reduced merchant shrinkage (the unexplained disappearance of cash). There are significant productivity advantages for all participants with prepaid cash cards.

From an economic point of view, the stored value card is a productivity device. Not one of several hundred Smart Card prepaid card systems has reported a profit. It does improve speed, reduce service complexities, and reduces losses. In a multiple application Smart Card, the economics improve by sharing card costs. However, profit is realized from credit cards and revenues from other application providers in a multiple application Smart Card.

Smart Card System Improvements and Options

The use of the Smart Card application attributes enables a new series of systems enhancements when compared with past goals of fully on-line systems architecture and functions.

Local Decisions and Control for Routine Transactions. Local decisions and control allows handling routine transactions locally in the Smart Card microprocessor chip. This reduces the network and central processing load for formerly “central on-line only” transactions. The “local online” mode is under control of issuer-specified Smart Card internally carried logic, control values, and business rules. Often this will be with a large reduction in losses because the current central on-line system cannot be reached for all transactions with conventional striped cards.

The Smart Card offers distributed access control, local proprietary access software protection, and direct communications routing. This is done with issuer-entered protocols from the Smart Card application content. This is of high value in locations with PC work stations or microprocessor-based terminals. It avoids expensive education of accepting personnel to start the PC facilities.

Communications Productivity. The large reduction of transactions requiring central on-line handling allows existing networks to support transactions systems with larger activity volumes. Local on-line decisions reduce unnecessary line usage and reduce chances for security penetration in pure central on-line systems.

Multiple Application-Systems-Oriented Database. Each of up to 20 Smart Card applications contains their own instructions and protocols for application control and security and also for communication with independent application provider control points and the communications protocols necessary to reach them. The card acceptor device dials directly to an insurance, telephone, travel and other central online control/product locations without loading up the card issuer dedicated network.

Issuer-Controlled Distributed Logic and Controls. Distributed application rules and controlling database allow for local on-line decisions. These rules may be tailored to individual card holder accounts and services. An adaptive learning program in the Smart Card allows direct experience gathering, no matter how the transactions are authorized. This experience is reported during each central on-line transaction. Thus, the Smart Card content is dynamically updated during central on-line transactions.

Secure Portable Data Base Access Device. Marketing, servicing, and remote operations often require the use of data which is proprietary, valuable, or damaging if it is obtained by competitors. The Smart Card offers a protected carrier which uses the data available remotely but does not allow casual access to the data. For example, a valuable entry communications algorithm or piece of security enabling data is executed within the Smart Card and only the result is available externally. This is an effective way of protecting software distributed to remote personal computers.

Portable and Mobile Encryption and Security Device. The Smart Cards are available with internally carried and executable algorithms.

Bridge Between Incompatible Systems. Several industries require transaction handling between departments or between businesses units which are not interconnected by communications. Frequent shopper points need to be easy to use between grocery chains which are not on-line with each other. Vocational training programs need access to multiple departments which do not share a common network or database. The Smart Card offers a bridge to noncompatible or stand-alone network locations. Each system provides a common interface to the Smart Card. This also allows carrying data between different application systems.

Nonstop (Fault Tolerant) Transaction Control. Major systems are faced with communications outages for which there may not be an adequate fallback or failure alternative. The Smart Card internally based decision process and database offers local on-line decisions and data capture for routine transactions with recovery after the outage. This offers lower cost and higher availability of solutions in geographically distributed environments where duplicate networks are expensive or unavailable.

Application Controls. The Smart Card is electronically updated with *EVERY* transaction, central on-line, local on-line, or off-line. The transaction amounts, transaction frequency and the transaction mode (central on-line versus local on-line) are captured and assessed in the Smart Card. The new business rules include the following:

Number of consecutive local transactions on-line.
Maximum cumulative local transaction value on-line.
Available funds for card use in the specified period.
Available credit line based on current payment record.

Technical Support for the Smart Card. The adaptation of a Smart Card for a particular application requires preparatory steps. It covers the following areas:

Application Requirements.

data content, format, and location (card, card acceptor, local client/server support, distributed or regional center, central repository);
business rules, control logic, authentication, and authorization processes;
card personalization processes; and
transaction records and journals.

Operational Requirements. These are dictated by peak-load responses, network loading capacities, and required capacity levels.

Control Requirements. The business rules and control logic dictate each business decision made during transaction processing. These controls include the following:

general sensitivity test (such as the number of transactions in a specific period) to detect attempted violations of the system; and
the reconciliation data and logic required for the local on-line mode.

During local on-line operation, the central site account details are compared with the data captured in the card acceptor. The captured data is sent in a batch daily from acceptors. After reconciliation, appropriate data is loaded into the user card. This updates the control values, the business rules, and implements changes to the applications, including additions and deletions. This ability to update the smart card is an important difference compared with conventional card systems. The conventional card has a passive minimum data recording which is not updatable.

Multiple-Application Management. Successful introduction of the multiple-application Smart Card requires proper management of the elements that make the card possible. Some of these are described in the following sections.

Memory Allocation. The card's memory carries the logic for the overall management of the card's applications. This includes the business rules for interapplication activity and the rules controlling access to each application. Security rules, guidelines, and control values are also carried in the card memory.

Communications. Each application has its own communication rules and data. These include telephone numbers, charge numbers, information protocols and formats, and security requirements. The card issuer needs to be kept up-to-date on individual application changes.

Human Factors. Field tests show that users and acceptors of the multiple-application card have little difficulty in understanding the range of applications available. Trouble arises only when there are changes in individual application relationships, limits, and features. These need to be communicated to the card user, and there are opportunities to do this by the following:

monthly statements;
direct mail fliers;
transaction receipts and displays;
advertisements;
card acceptor statements and bulletins; and
exception transaction handling messages.

Application Changes. Application changes include alterations to application specifics, such as terms and conditions, prices, availability, and marketing incentives. There may also be changes in the actual applications offered. These come and go depending on business criteria. Details that may need to be communicated to users if a change include the following:

Application title, provider, account number, feature or option designation.
New account limits or prices.
Law conformity requirements.
Qualification status.
Reassignment to a different application provider. Reassignment may involve changes to rules, limits, conditions, acceptor locations and incentives.
Monthly billing or statement arrangements.
Payment terms, options and locations.

System Attachment Options. System attachment is either central site on-line or local on-line. Central on-line is where a transaction requires communication with a central control point as a part of each transaction. Local on-line occurs when there are enough logical controls and local account data to complete a transaction independently. In either case, data is captured to allow updating the central account records, customer status, and reissue of a card, if required.

The use of the Smart Card makes possible a new systems mode, called local on-line. In this mode, routine transactions are handled on-line to the Smart Card, but the detection of exception conditions interrupts the operation and forces a central on-line transaction. This interruption is not noticeable by the card user or card acceptor if the system is properly designed.

The local on-line mode of operation means improved system and operational productivity. In the credit card and banking card area, local on-line activity may be reduced to as little as 10% to 15% of the transactions requiring central online. This compares with the 85% to 90% of transactions requiring central on-line communication with a magnetic-striped conventional card system.

The local on-line mode reduces network load and expense and speeds up transactions. It also reduces losses, because all transactions are subject to better control. Bad cards/accounts have their application turned off within the card until the account is under control. That is not possible with conventional cards. The absence of a turn-off function in conventional magnetic-stripe cards is responsible for more than 20% of annual credit card losses.

Smart Card Support Rules. A basic rule with the Smart Card is that all data must be 100% redundant, that is, the central control point for each application must have enough current data to replace the Smart Card content at any time. This means that periodic central on-line reconciliations must be supplemented with batch entry of local on-line or off-line transactions. The data redundancy is required for the following:

to replace lost cards;

to issue of next generation cards;

to evaluate changes to account limits;

to provide a decision base at the issuer to deal with customer requests or inquiries;

to react to missed payments;

to react to sudden changes in credit demand or to dynamically redistribute credit capacity among multiple relationships;

to react to requests for additional applications or changes to applications;

to prepare monthly statements and assess charges; and

to capture market data.

If there is a requirement to replace a Smart Card, it is necessary to do the following:

turn off the lost card on return or at its next central on-line presentation; and

maintain full security management at all times. This includes insuring that nothing in one card application is used to gain access to information in another card application.

Other support measures include the following:

In-card controls must not allow designated account activity limits to be exceeded.

The cardholder must be fully informed of changes to his or her account or application status.

Card acceptors must be told of responses to transactions and the reasons.

The card acceptor unit must not indicate central or local on-line operation.

The electronic resetting of all card acceptor controls must be possible at any time.

The Need for Central Databases. The Smart Card requires that a set of databases be maintained at a designated central site. These are used in communications with the Smart Card. The areas covered by the databases include the following:

Application controls for each user
- business rules
- control values and limits
- control dates

Personalization data, definitions, and limits
- credit levels
- required payment periods and amounts
- missed payment cycle, controls, and amounts

The reconciliation record for the next central on-line session
- changes in logic and business rules
- changes to applications
- revisions to control values and time cycles

Transaction journal
- transaction journal capacity
- merchants and locations
- transaction type and amount

Frequency of use/incentive points record
- special offer periods
- redemption record

Physical card record
- card manufacturer, model, and serial number
- technology and capacities
- card life-cycle dates and access controls
- assigned storage areas for free, confidential, and secret memory
- operating system type
- operating system changes

Security management for each card
- card security features, including personal identification number (PIN) and biometric comparison values
- contact telephones

Communications management for each application
- application control point
- billing codes
- access formats
- customer behavioral model
- demographics data
- store/department visit records

Credit scoring model and status

"Budget" Credit Card Operation. The Smart Card makes tight credit control possible and this introduces a major new marketing opportunity by expanding the number of potential credit card users. The "budget credit card" allows extending credit to bank customers with low conventional credit capabilities or needs. It also allows segmenting credit and assigning it to specific purposes: a child's school expenses, vacations, hobbies or house maintenance, for example.

The tight control comes from several new features in the Smart Card including the following:

better logic and business controls
central and local on-line operating options
a portable database allowing better account usage
better security, inhibiting card misuse and abuse
quick and easy control of cardholder eligibility

Take the example of a budget card with a $100 per month spending limit subject to timely installment payments. In-card data and controls would include the following:

a central on-line reconciliation cycle (for example, at least every two weeks)
a specified maximum number of transactions between central on-line reconciliations
A specified cumulative transaction value between central on-line reconciliations.

A special procedure is required to handle negative approvals. As the available funds are depleted, the frequency of nonapprovals increases. To prevent system overloading when funds are not available, a transaction receipt is printed showing the number of days to the next cycle start date. That instructs the cardholder to conduct the next transaction when funds are available so as to avoid unnecessary rejections.

Another situation arises when there are only enough funds for a partial payment for a transaction. The cardholder should be encouraged to make part of the payment in cash, and the printed receipt should then give the date of the next credit-cycle start time. When a payment is missed, the available credit line should be reduced until payment is received.

Security of Financial Transaction Systems Using IC Cards. These standards are to be used during the full life cycle of the financial transaction card, from initial manufacture to final use and disposal. Following are the major ISO standard components:

10202-1: describes the life cycle
10202-2: describes the transaction process
10202-3: discusses cryptographic key relations
10202-4: describes Secure Application Modules (*SAMs*)
10202-5: discusses the use of algorithms
10202-6: describes cardholder verification
10202-7: suggests key management steps
10202-8: gives a general overview of the security recommendations

The multiple application Smart Card is issued by the card issuer. It supports applications from different application providers. Transactions are processed in the Smart Card processor with the self-contained database. It is also referred to different control points using the communications management functions in the application logic and data. The card function allows activating or deactivating individual applications. A common data file contains identification data common to all of the applications. The card issuer is responsible for the security of the Smart Card and its contained applications. The application provider is responsible for security within the individual application and its operation.

The ISO 10202 security standard specifically states that it is NOT intended to protect against a bogus card acceptor unit. However, the standard does cover the security associated with matching something a card holder possesses, the Smart Card, and something the cardholder knows, namely, a PIN.

The Contactless Smart Card. Contactless describes cards and tags. The card is the conventional ISO 7816 Smart Card. A radio frequency (RF) generator and receiving antenna has been added to the card. The antenna may receive power to operate the chip. It also receives signals with data to communicate with the chip logic. In turn, the RF generator produces a signal with data for the accepting equipment. For example, a fare collection device receives value through the signals to pay the required fare.

RF Tags are small devices appended to articles for the purpose of providing identification via an exchange of RF signals. RF tags may be imbedded in plastic cards to create a contactless card. There are a variety of RF tags from passive (receive power to operate), to active (contain their own power). See Google: Wikipedia - RF Tags for a complete description.

There are a number of operational environments where the requirement of inserting a card into an acceptor causes delay or difficulty. An example is the collection of fares from passengers passing through transit entry gates. Areas of use include the following:

10526-1: *Moving Environments* tolls and mass transit systems
10536-2: *Entry and Exit Detection* parking lots, taxable congested road areas and ski lifts
10536-3: *Physical Area Access/Security* with adverse environmental conditions
10536-4: *Logistics Management* loading manifests and container or rail car inventory management
Medical Environments monitoring of mobile patients

The contactless Smart Card uses radio frequency signals to be read at a distance of up to 10 cm or 4 inches from the reader/writer. It is intended for application in which speed of travel is desirable, such as a customer entering a mass transit system. The Smart Card may remain in a purse or wallet. The cards will be produced with combined contact and contactless features in one card. The contacts might be used in a telephone whereas the contactless portion is used in an entry gate. It is expected that the combined card will cost the same as a single functional card within the next five years.

The International Standards for contactless Smart Cards, ISO 14443, covers the following:

1. Physical characteristics
2. Dimensions and locations of coupling areas
3. Electronic signals and reset procedures
4. Answers to reset and transmission protocols

The following will be required:

transmitter/modulators and receivers/antennas

an algorithmic means of distinguishing between multiple-simultaneous presenters

adequate human factors designed to guide users

appropriate lighting and markers for successful use

a means of replenishing value content

Radio Frequencies. Transmission to distances of hundreds of meters requires a basic radio frequency signal or carrier. The signal is measured in hertz per second. The carriers used have characteristics which depend on their frequencies:

Low frequency: under 500 kHz. Lower frequencies have slower data rates, but are adequate for short to moderate distances. They need less costly equipment and have lower sensitivity to card orientation.

Mid frequencies: 1.7 MHz to 10.0 MHz, with medium range and equipment costs.

High frequencies: 2.6 MHz to 50 MHz. These offer faster data transfer rates and medium to long transmission distances, but require more expensive equipment and perhaps greater sensitivity to card orientation.

Some frequency ranges may require regulatory permission.

Contactless Smart Cards offer several economic and operational advantages over conventional Smart Card systems. As experience with the cards grows, the cost differential will quickly be overshadowed by these functional and operational gains. The key advantages are faster response, less operational interference, and use for remote input/output.

The Economics of Smart Cards. Consider the economics of the Smart Card:

Card Purchase:	$1.00 (A multiple application card)
Card Issue:	$1.50 (Personalization, account data)
Total	$2.50
Per month (36):	0.07

Consider the magnetic striped card:

Card Purchase:	$0.40
Card Issue:	0.75
Total:	$1.15
Per month (16):	0.07

The Smart Card economics benefit from a longer useful life, and the Smart Card content can be updated. By industry agreement the magnetic stripe content cannot be updated or rewritten. Conversely, the Smart Card can be updated with a set of controls and checks. The useful lives are set by industry standards agreement.

There are large additional revenues earned from other application providers on the multiple application Smart Card. With ten coresident applications, the revenues for the Smart Card may be more than five times that of a magnetic-striped conventional credit card.

The Smart Card Alliance is a multi-industry association. It has four priorities:

Standards for Smart Card adoption and implementation.

Serve as a voice in public policy to support Smart Cards.

Serve as an educational resource.

Provide a forum for education and discussion.

The principal activities are:

Work groups.

Annual meeting.

Educational Institute.

Get more information at www.smartcardalliance.org.

Summary

The conventional magnetic-striped card and the Smart Card are as different as a passive piece of magnetic tape and a full functional microprocessor chip. The passive piece of tape is a storage medium. All of its use is controlled remotely, usually through a large network connected to large central computers. As with any chain, the weakest link sets the lowest level of performance. The weakest link is the stripe. It has shortcomings in security, reliability, data content, and performance. It is severely restricted in application content, function, security, and it is not updatable in any manner.

The Smart Card creates a fully transportable application performing unit with the same logical capabilities as the central site computer. The one element not available to the Smart Card is the collective market activity for the accounts carried on the card. These are substituted for by the following:

in-card logic, business rules and controls;
specific limits for local on-line, card-only activity;
specific conditions requiring central on-line control; and
periodic reconciliation between the Smart Card and consolidated central site records.

Experience in national banking systems in Europe employing the Smart Card confirms a large reduction (to 90%) in central on-line activity to supervise properly application activity controlled by the local on-line Smart Card.

These application attributes represent the significant emerging capabilities of Smart Card. The Smart Card provides a new set of system alternatives. These attributes offer direct system and economic benefits. They allow the Smart Card to achieve a lower cost per transaction than the conventional magnetic striped plastic transaction card and interfacing system.

BIBLIOGRAPHY

Books

J. Svigals, *Smart Cards 2010*, Lafferty Press, 1998.

M. Hendry, *Smart Card Security and Applications*, Artech House, 2001.

D. Paret, *RFID and Contactless Applications*, Wiley, 2001.

U. Hannsmann, *Smart Card Application Development using Java*, Wiley, 2002.

Monthly Newsletters

Card Technology, USA, custserv@tfn.com

Card technology Today, England, eatsales@elsevier.com

Card Management, USA, custserv@thomsonmedia.com

European Card Review, kaye@europeancardreview.com

CardsNow, Asia, subscription@cardsnowasia.com

Internet

A Compinfo Directory: compinfo.co.uk/tpsmrt.html

Wikipedia-Smart Cards: wikipedia.org/wiki/Smart_Cards

Links to Smart Card Sites: members.aol.com/pjsmart/page4

Lists SC Products: timberlinetechnologies.com/smart.html

JEROME SVIGALS
Jerome Svigals, Inc.