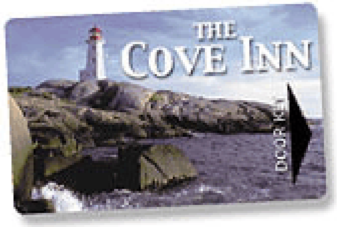
INTRODUCTION

The world of IT is establishing its base in every facet of life. From software programming to netbanking to controlling appliances to managing databases etc. The list is endless. One of the rapidly developing fields of IT is of ‘ Smart Cards’. A smart card, simply speaking, is a credit card-sized plastic card with an embedded computer chip and some memory. One can put it to a wide variety of uses to help simplify our daily life. Access Control , Shopping, identification, telephone services, and licenses are just a couple of them. ISO 7816 defines the smart card standard—it details the physical, electrical, mechanical, and application programming interface for it. From driving licenses to SIM cards, this credit card-sized device seems to have found diverse applications . Smart cards greatly improve the convenience and security of any transaction. They provide tamper-proof storage of user and account identity. Smart cards also provide vital components of system security for the exchange of data throughout virtually any type of network. They protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Multifunction cards can also serve as network system access and store value and other data. People worldwide are now using smart cards for a wide variety of daily tasks.

In Indian Army the most important use for Smart Cards is in the field of access control in order to allow a limited access to personal inside classified areas like Labs, Control rooms , Ops Room etc .This is primarly in order to exercise control and security.

AIM

2. To work out the Essential Requisites for Establishing a SMART CARD Lab in MCEME.



Why Smart Cards :An Oveview

3. Smart cards greatly improve the convenience and security of any transaction. They provide tamper-proof storage of user and account identity. Smart cards also provide vital components of system security for the exchange of data throughout virtually any type of network. They protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Multifunction cards can also serve as network system access and store value and other data. People worldwide are now using smart cards for a wide variety of daily tasks, these include:

(a) Loyalty and Stored Value. A primary use of smart cards is stored value, particularly loyalty programs that track and incentivize repeat customers. Stored value is more convenient and safer than cash. For issuers, float is realized on unspent balances and residuals on balances that are never used.

For multi-chain retailers that administer loyalty programs across many different businesses and Point of sale systems, smart cards can centrally locate and track all data. The applications are numerous, from parking and laundry to gaming, as well as all retail and entertainment uses.

(b) Securing Information and Physical Assets. In addition to information security, smart cards achieve greater physical security of services and equipment, because the card restricts access to all but the authorized user(s). E-mail and PCs are being locked-down with smart cards. Information and entertainment is being delivered via to the home or PC. Home delivery of service is encrypted and decrypted per subscriber access. Digital video broadcasts accept smart cards as electronic keys for protection. Smart cards can also act as keys to machine settings for sensitive laboratory equipment and dispensers for drugs, tools, library cards, health club equipment etc.

(c) E-Commerce .Smart cards make it easy for consumers to securely store information and cash for purchasing. The advantages they offer consumers are:

(i) The card can carry personal account, credit and buying preference information that can be accessed with a mouse click instead of filling out forms.

(ii) Cards can manage and control expenditures with automatic limits and reporting.

(iii) Internet loyalty programs can be deployed across multiple vendors with disparate POS systems and the card acts as a secure central depository for points or rewards.

(iv) ”Micro Payments” - paying nominal costs without transaction fees associated with credit cards or for amounts too small for cash ,like reprint charges.

(d) Personal Finance. As banks enter competition in newly opened markets such as investment brokerages, they are securing transactions via smart cards at an increased rate. This means:

(i) This will improve customer service. Customers can use secure smart cards for fast, 24-hour electronic funds transfers over the Internet.

(ii) Costs are reduced: transactions that normally would require a bank employee's time and paperwork can be managed electronically by the customer with a smart card.

(e) Health Care. The explosion of health care data brings up new challenges to the efficiency of patient care and privacy safeguards. Smart cards solve both challenges with secure storage and distribution of everything from emergency data to benefits status.

(i) Rapid identification of patients; improved treatment

(ii) A convenient way to carry data between systems or to sites without systems.

(iii) Reduction of records maintenance costs.

(f) Telecommuting And Corporate Network Security. Business to business Intranets and Virtual Private Networks “VPNs” are enhanced by the use of smart cards. Users can be authenticated and authorized to have access to specific information based on preset privileges. Additional applications range from secure email to electronic commerce

(g) Campus Badging and Access. Businesses and universities of all types need simple identity cards for all employees and students. Most of these people are also granted access to certain data, equipment and departments according to their status. Multifunction, microprocessor-based smart cards incorporate identity with access privileges and also store value for use in various locations, such as cafeterias and stores.

Types and Range of Smart Cards

4. **Types** . There are two types of smart cards—contact or contactless.

(a) Contact smart Card . A contact smart card has to be inserted into a smart card reader for access .A smart card involves much more than just sticking a chip on plastic. The plastic used is usually PVC (poly vinyl chloride), but other substitutes like ABS (acryl nitrile butadiene styrene), PC (polycarbonate), and PET are also used. The chip, also known as micromodule, is very thin and is embedded into the plastic substrate or card. To do this, a cavity is formed or milled into the plastic card. Then, either a cold or hot glue process bonds the micromodule to the card. The micromodule has connectors that are accessed by the reader for data transfer. These are typically gold plated.

(b) Contactless . Smart Card A contactless card doesn’t need physical contact with a reader. Both sides have antennae that are used for communication. The antenna is typically three to five turns of very thin wire connected to the chip. You have to place the card about 2"-3" from the reader for data access. Here, the card doesn’t need an additional power source for data transfer. The electromagnetic signal emitted by the reader is enough to power the chip as well. Because they’re fast to use, these cards can be used where a lot of people need to access the reader, for example, at a railway subway system.

Two additional categories, derived from the contact and contactless cards are: Combi cards and Hybrid cards. A Hybrid card has two chips, each with its respective contact and contactless interface. The Combi card is an emerging technology, which has a single chip with a contact and contactless interface.

5. **Range**. Range of Smart Cards vary according to the type of chip implanted in the card and its capabilities. There is a wide range of options to choose from when designing system

(a) Memory Cards . Memory cards have no sophisticated processing power and cannot manage files dynamically. All memories communicate to readers through synchronous protocols. There are three primary types memory cards:

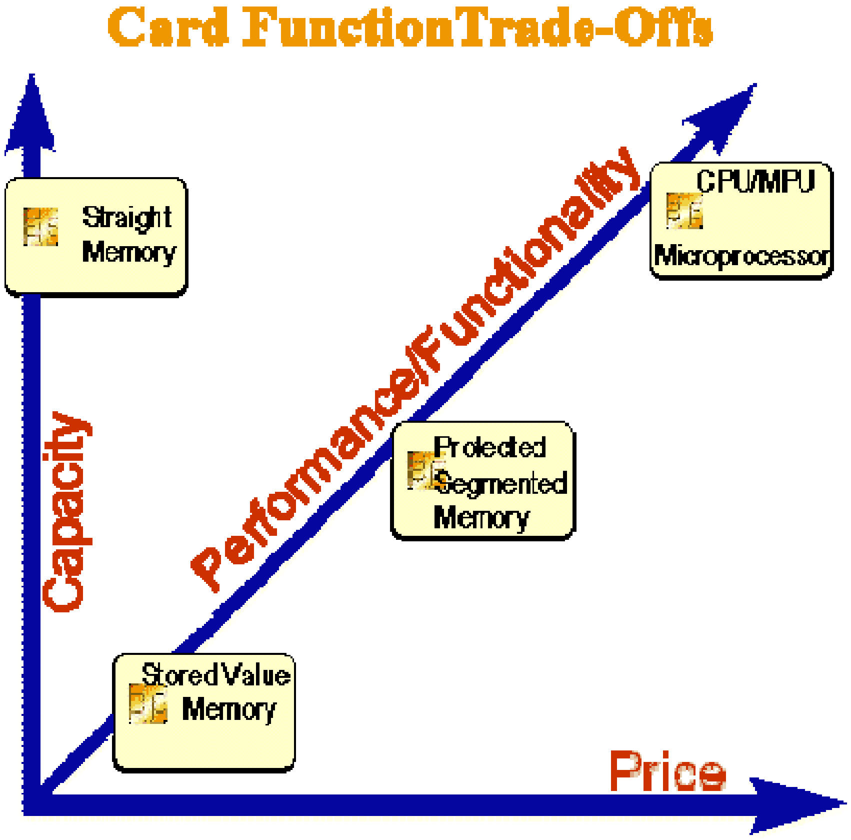
(b) Straight Memory Cards These cards just store data and have no data processing capabilities. These cards are the lowest cost per bit for user memory. They should be regarded as floppy disks of varying sizes without the lock mechanism. These cards cannot identify themselves to the reader, so your host system has to know what type of card is being inserted into a reader

(c) Protected / Segmented Memory Cards. These cards have built-in logic to control the access to the memory of the card. Sometimes referred to as Intelligent Memory cards these devices can be set to write protect some or all of the memory array . Some of these cards can be configured to restrict access to both reading and writing. This is usually done through a password or system key. Segmented memory cards can be divided into logical sections for planned multi-functionality

(d) Stored Value Memory Cards These cards are designed for the specific purpose of storing value or tokens. The cards are either disposable or rechargeable. Most cards of this type incorporate permanent security measures at the point of manufacture. These measures can include password keys and logic that are hard-coded into the chip by the manufacturer. The memory arrays on these devices are set-up as decrements or counters. There is little or no memory left for any other function. For simple applications such as a telephone card the chip has 60 or 12 memory cells, one for each telephone unit. A memory cell is cleared each time a telephone unit is used. Once all the memory units are used, the card becomes useless and is thrown away. This process can be reversed in the case of rechargeable cards.

6. Increased levels of processing power, flexibility and memory add cost. Single function cards are often the most cost-effective solution.

One must choose the right type of smart card for application by evaluating cost versus functionality and determine required level of security. While installing the facility of Smart Card Lab the type and range of the Smart Card has to kept in mind. The following chart demonstrates the general rules of thumb.

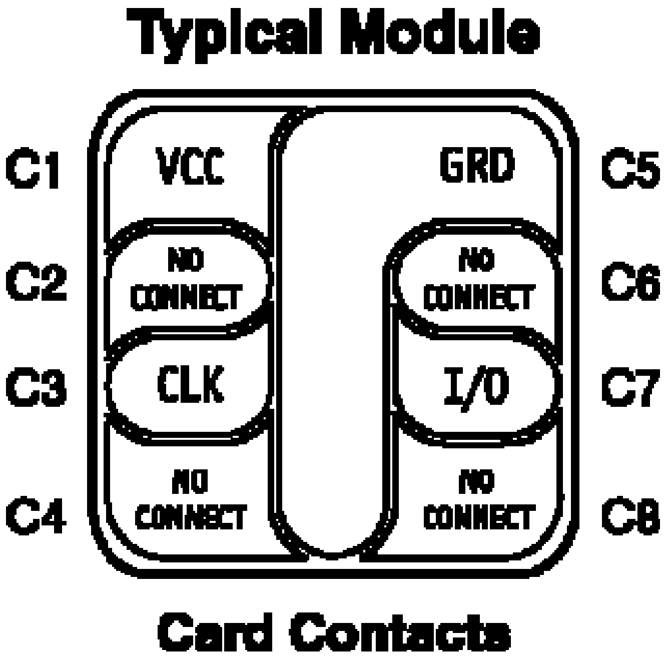


Graphic Courtesy of CardLogix Corporation

(Fig 1)

Technology and Standards

7. Smart cards can be fabricated with just memory, or can have a microprocessor with memory. Memory-based smart cards simply have memory to store information, such as personal identification details. These can be used as identity cards, or phone cards—debit cards which can be used as a payment mechanism to make calls from phone booths. Processor-based smart cards are more complicated. They contain a ROM to store an operating system, a main memory (RAM), and a memory sector for application data (EEPROM). So, they're more expensive too. These cards can be used where heavy calculations or more security is required. For example, it can be used as an ATM card to determine how much money is there in the account. This information will then be stored on smart card. Processor-based cards can also be used to encrypt data.



(Fig 2)

8. CPU/MPU Microprocessor Multifunction Cards . These cards have on-card dynamic data processing capabilities. Multifunction smart cards allocate card memory into independent sections assigned to a specific function or application. Within the card is a microprocessor or microcontroller chip that manages this memory allocation and file access. This type of chip is similar to those found inside all personal computers and when implanted in a smart card, manages data in organized file structures, via a card operating system (COS). Unlike other operating systems, this software controls access to the on-card user memory. This capability permits different and multiple functions and/or different applications to reside on the card, allowing businesses to issue and maintain a diversity of 'products' through the card. One example of this is a debit card that also enables building access on a college campus. Multifunction cards benefit issuers by enabling them to market their products and services via state-of-the-art transaction technology. Specifically, the technology permits information updates without replacement of the installed base of cards, greatly simplifying program changes and reducing costs. For the card user, multifunction means greater convenience and security, and ultimately, consolidation of multiple cards down to a select few that serve many purposes.

9. Standards. Primarily, Smart Card standards govern physical properties and communication characteristics of the embedded chip and are covered through the ISO 7816-1,2,3.

Application-specific proprieties are being debated with many large organizations and groups proposing their standards. Open system card interoperability should apply at several levels -1) to the card itself, it's access terminals (readers), the networks and the card issuers' own systems. This will only be achieved by conformance to international standards. This Site's sponsors are committed to compliance with ISO and CEN standards as well as industry initiatives such as EMV, the Open Card Framework and PC/SC specifications.

Following organizations are active in smart card standardization:

(a) The International Standards Organization (ISO) facilitates the creation of voluntary standards through a process that is open to all parties. ISO 7816 is the international standard for integrated-circuit cards (commonly known as smart cards) that use electrical contacts. Anyone interested in obtaining a technical understanding of smart cards needs to become familiar with what ISO 7816 does NOT cover as well as what it does. Copies of these documents can be purchased through ANSI American National Standards Institute. ANSI's address and phone is: 11 West 42nd Street, New York, NY 10036 - (212) 642-4900.

(b) National Institute of Standards and Technology (NIST) publishes a document known as FIPS 140-1, "Security Requirements for Cryptographic Modules". This concerns physical security of a smart card chip, defined as a type of cryptographic module.

(c) Europay, MasterCard and Visa have created their "Integrated Circuit Card Specifications for Payment Systems". The specification is intended to create common technical basis for card and system implementation of a stored value system. Integrated Circuit Card Specifications for Payment Systems can be obtained from a Visa, MasterCard or Europay member bank. It may also be posted on the VISA web site.

(d) Microsoft has proposed a standard for cards and readers, called the PC/SC specification. This proposal only applies to CPU cards.

(e) CEN or the (Comite' Europe'en de Normalisation) and ETSI (European Telecommunications Standards Institute is focused on telecommunications, as with the GSM SIM for cellular telephones. GSM 11.11 and ETSI300045. CEN can be contacted at Rue de Stassart,36 B-1050 Brussels, Belgium, attention to the Central Secretariat.

(f) ISO 7816 Summary This is a quick overview of what the 7816 specifications cover. Some of these are frozen and some are in revision; please check with ANSI for the most current revision. ISO 7816 has six parts. Some have been completed; others are currently in draft stage.

Part 1: Physical characteristics-ISO 7816-1:1987 defines the physical dimensions of contact smart cards and their resistance to static electricity, electromagnetic radiation and mechanical stress. It also describes the physical location of an IC card's magnetic stripe and embossing area.

Part 2: Dimensions and Location of Contacts- ISO7816-2:1988 Defines the location, purpose and electrical characteristics of the card’s metallic contacts (see above illustration).

Part 3: Electronic Signals and Transmission Protocols- ISO 7816-3:1989 defines the voltage and current requirements for the electrical contacts as defined in Part 2 and asynchronous half-duplex character transmission protocol (T=0). Amendment 1:1992 Protocol type T=1, asynchronous half duplex block transmission protocol. Smart cards that use a proprietary transmission protocol carry the designation, T=14. Amendment 2:1994 Revision of protocol type selection.

Part 4: Inter-industry Commands for Interchange- ISO 7816-4Establishes a set of commands for CPU cards across all industries to provide access, security and transmission of card data. Within this basic kernel, for example, are commands to read, write and update records.

Part 5: Numbering System and Registration Procedure for Application Identifiers- ISO 7816-5:1994 establishes standards for Application Identifiers (AIDs). An AID has two parts. The first is a Registered Application Provider Identifier (RID) of five bytes that is unique to the vendor. The second part is a variable length field of up to 11 bytes that RIDs can use to identify specific applications.

Part 6: Inter-industry data elements- ISO 7816-6 Details the physical transportation of device and transaction data, answer to reset and transmission protocols. The specifications permit two transmission protocols: character protocol (T=0) or block protocol (T=1). A card may support either but not both. (Note: Some card manufacturers adhere to neither of these protocols. The transmission protocols for such cards are described as T=14).

Genesis for Establishing Smart Card Lab

10. MCEME imparts technical training to Offrs and men from the Corps of EME. As a result there is always a presence of large strength in the campus. To manage such a large strength in terms of looking after their professional and administrative needs a sizable amount of manpower ,stationary and time is required. The problem is further supplemented due to various resource crunch.

11. In order to overcome this heavy demand of manpower time and stationary it is proposed to establish a Smart Card Lab which will act as nerve center for various Smart Card Applications The Smart Card applications will be installed at various locations like Central Library, Main CSD Canteen, Offrs Mess ,System Lab in FEL etc

Hardware Requirements for Establishing Smart Card Lab in MCEME

12. The Smart Card Lab which is proposed to be formulated and brought up from the infancy stage will work as hub center to various Smart Card Applications proposed to be implemented in

MCEME Campus .These are enlisted in subsequent paragraphs. The requirement of various hardwares for establishuing the Smart Card Lab are :

(a) Smart Cards. It is required for the basic end user. These are proposed to be multifunctional , microprocessor and memory based . The memory is required to store vital information an example of which is given below :

(i) Personal No.

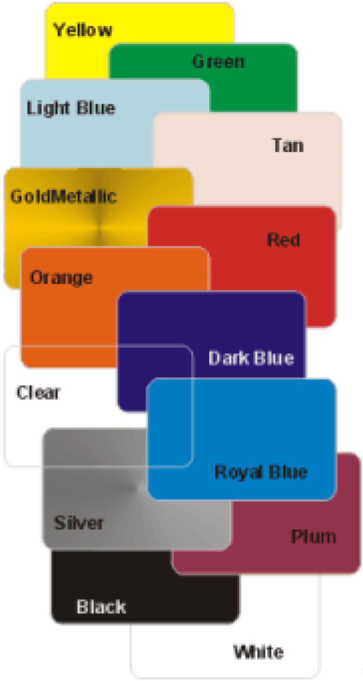
(ii) Name.

(iii) Course.

(iv) Valid Upto.

(v) Balance Amount.

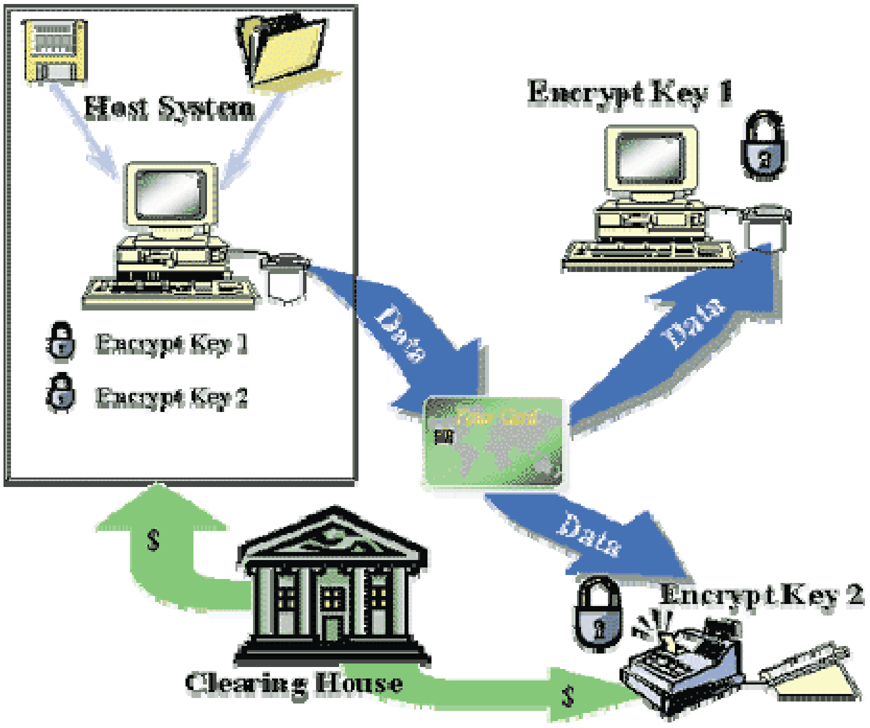
Intelligence is required to carry out dynamic data processing, memory allocation etc.



(Fig 3)

(b) Reader . The term "reader" is used to describe a unit that interfaces with a PC for the majority of its processing requirements. Readers can read and write to smart cards. Readers come in many form factors and in a wide variety of capabilities. The easiest way to describe a reader is by the method of it’s interface to a PC. Smart Card Readers are available that interface to RS232 serial ports, USB ports, PCMCIA slots, floppy disk slots, parallel ports. Another difference in reader types is the on board intelligence and capabilities or lack thereof. Extensive price and performance differences exist between an industrial strength intelligent reader that supports a wide variety of card protocols and a home style win-card reader that only works with microprocessor cards and performs all processing of the data in the PC.

(c) PC. It is required to store the data .It will act as a main databank and also to write on to the Smart Card, if there is a requirement to reprogram the Smart Card. This need may arise when an individual proceeds on posting from MCEME. It may also arise when it is required to add or delete certain facilities available to the user of the card.



(Fig 4)

Applications of Smart Card in MCEME

13. Access Control. Many a times it is required to restrict the movement of the personal into a particular room or enclosed area due to the security reasons. In MCEME this application can be used for :

(a) Restricting the entry of personal in the Systems Lab in Computer Science Dept in Faculty of Electronics.

(i) Hardware Requirements

(aa) Smart Card – Contact Type. Memory based.

(ab) Reader.

(ac) PC to control the Opening and closing of the door and storage of the data.

(ad) Solenoid Operated Lock.

(ae) UPS backup for power failure.

(ii) Cost Analysis

(aa) Smart Card - Rs 100/- each.

(ab) Reader - Rs 20,000/-.

(ac) Solenoid operated lock - Rs 1500/-.

(ad) PC and UPS - Inhouse.

(iii) Advantages.

(aa) Entry to auth personals only.

(ab) Data bank of personals entering the lab on a specific day is available.

(ac) Enhanced Security .

(b) Restricting the entry of personals in the strong room in Quarter Guard where wpns are kept.

(i) Hardware Requirements

(aa) Smart Card – Contact Type. Memory based.

(ab) Reader.

(ac) An embedded Control Circuit in lieu of PC to control the Opening and closing of the door and storage of the data.

(ad) Solenoid Operated Lock.

(ae) UPS/Bty backup for power failure.

(ii) Cost Analysis

(aa) Smart Card - Rs 100/- each.

(ab) Reader - Rs 20,000/-.

(ac) Solenoid operated lock - Rs 1500/-.

(ad) Embedded Control Circuit – Rs 5000/-

(iii) Advantages.

(aa) Entry to auth personals only.

(ab) Better Security.

14. Financial Transactions. A Smart Card loaded with electronic money can reduce cash handling costs and fraud and provide an easy payment thus providing consumers the convenience and ease of electronic payment. In MCEME this application can be used for

(a) Transactions done at the CSD ,Offr Mess ,Kerb side pump and the Liquor Counter.

(i) Hardware Requirements

(aa) Smart Card – Contact Type. Memory and microprocessor based.

(ab) Reader.

(ac) PC for storing and maintenance of the data .

(ii) Cost Analysis

(aa) Smart Card - Rs 250/- each.

(ab) Reader - Rs 20,000/-.

(ac) PC - Inhouse.

(iii) Advantages.

(aa) No cash transaction .

(ab) Easy handling of accounts.

(ac) Payment mode made simpler. It can be arranged to give the payment to a central agency like Offr Mess which in turn will distrubute to CSD canteen and Liquor counter.

(ad) Reduction in manpower in CSD Canteen

15. Data Updation. A Smart Card can be used to access data of different nature and helps in its updation.

(a) To maintain the record of the various books issued to an indl in the MCEME Library.

(i) Hardware Requirements

(aa) Smart Card – Contact Type. Memory and microprocessor based.

(ab) Reader.

(ac) PC to store and update the data

(ii) Cost Analysis

(aa) Smart Card - Rs 250/- each.

(ab) Reader - Rs 20,000/-.

(ac) PC - Inhouse.

(iii) Advantages.

(aa) Easy maintenance of data.

(ab) No library card required.

(ac) Quick transaction.

16. Health Care Services. A Smart Card can store data in respect to the medical history of an indl.

(a) An indl reporting at the MI Room is required to carry the Smart Card only.

(i) Hardware Requirements

(aa) Smart Card – Contact Type. Memory based.

(ab) Reader.

(ac) PC to store and update the data

(ii) Cost Analysis

(aa) Smart Card - Rs 100/- each.

(ab) Reader - Rs 20,000/-.

(ac) PC - Inhouse.

(iii) Advantages.

(aa) Easy maintenance of data.

(ab) No Health card required.

(ac) Data centrally available for drawing various inferences.

(ad) Less requirement of stationary and manpower.

17. Identity Verification . There are a no of places where an indl is required to prove his identity .There fore instead of carrying the Identity Card a Smart Card can be carried.

(a) Entries to movie hall can be permitted only after verification of the identity.

(i) Hardware Requirements

(aa) Smart Card – Contact Type. Memory based.

(ab) Reader.

(ii) Cost Analysis

(aa) Smart Card - Rs 100/- each.

(ab) Reader - Rs 20,000/-.

(ac) PC - Inhouse.

(iii) Advantages.

(aa) Easy maintenance of data.

(ab) No cinema card required.

(ac) No requirement of carrying I-Card everywhere.

18. The applications of Smart Card discussed above can be carried out using only one Smart Card having multifunction facility. Also the Card should be microprocessor and memory based card.

19. During the market survey following points came to the limelight :

(a) Not all the companies are ready to give the exact cost of the Smart Cards and other necessary hardware.

(b) Very few companies are ready to provide after sales services.

(c) The software required to program the Smart Card will be provided along with the full package i.e second time onwards we can program the Smart Card in the Smart Card Lab.

(d) The availability of various micro controllers and readers is at times thin. Hence sufficient time should be catered for the procurement of the same.

CONCLUSION

Smart cards can add convenience and safety to any transaction of value and data .Because smart cards are indeed tiny computers, it’s difficult to predict the variety of applications that will be possible with them in the future. It’s quite possible that smart cards will follow the same trend of rapid increases in processing power that computers have, following "Moore’s Law" and doubling in performance while halving in cost every eighteen months. Smart Cards have proven to be quite useful as a transaction/authorization/identification medium in European countries. As their capabilities grow, they could become the ultimate thin client, eventually replacing all of the things we carry around in our wallets, including credit cards, licenses, cash, and even family photographs. Establishing the Smart Card Based Lab in MCEME can earmark the beginning of a new era which will be a step forward in the right direction. For one thing is sure –Smart Cards are here to stay

(a) Data bank of personals entering the lab on a specific day is available.

Enhanced Security

Welcome to Smart Card Basics.com. This is a sponsored site brought to you by a number of companies in the smart card industry. We have tried to make this site informative with out a single perspective or marketing fluff. It is our belief that informed users make better choices.

Chip card technology is fast becoming commonplace in our culture and daily lives. We hope that this site will bring you a little closer in your understanding of this exciting technology and the benefits it can bring to your applications.

If you have specific questions regarding a specific technology discussed below feel free to send us an e-mail and the appropriate sponsor will respond.

SMART CARDS AND SECURITY OVERVIEW

1. Overview

A smart card – a type of chip card – is a plastic card embedded with a computer chip that stores and transacts data between users. This data is associated with either value or information or both and is stored and processed within the card's chip, either a memory or microprocessor. The card data is transacted via a reader that is part of a computing system. Smart card-enhanced systems are in use today throughout several key applications, including healthcare, banking, entertainment and transportation. To various degrees, all applications can benefit from the added features and security that smart cards provide. According to Dataquest, the worldwide smart card market will grow to 4.7 Billion units and $6.8 Billion by 2002.

Applications

First introduced in Europe over a decade ago, smart cards debuted as a stored value tool for pay phones to reduce theft. As smart cards and other chip-based cards advanced, people found new ways to use them, including charge cards for credit purchases and for record keeping in place of paper.

In the U.S., consumers have been using chip cards for everything from visiting libraries to buying groceries to attending movies, firmly integrating them into our everyday lives. Several states have chip card programs in progress for government applications ranging from the Department of Motor Vehicles to Electronic Benefit Transfer (EBT). Many industries have implemented the power of smart cards into their products such as the new GSM digital cellular phones to TV-satellite decoders.

3.

5. System Planning and Deployment

Smart card system design requires advance planning to be successful and to avoid problems. It is highly recommended that you graphically diagram the flow of information for your new system. The first question is always: Will the card and system transact information, or value, or both? If it stores keys or value i.e. gift certificates or sports tickets, greater design detail is required than in data-only systems. When you combine information types on a single card, other issues arise. The key to success is not to overrun the system with features that can confuse users and cause problems in management. We recommend that you phase-in each feature set as each one is working. To properly implement a functional smart card system you should be able to answer the following questions. **NOTE:** These are only general guidelines, provided as a basis for your individual planning. Many other steps may be involved and are not mentioned here.

Basic Set-Up

1. Is there a clear business case? Including financial and consumer behavior factors?
2. Will the system be single or multi-application?
3. What information do I want to store in the cards?
4. How much memory is required for each application?
5. If multi-application, how will I separate different types of data?
6. Will card data be obtained from a database? Or loaded every time?
7. Will this data concurrently reside on a database?
8. How many cards will be needed?
9. Are card/infrastructure vendors identified? What are the lead times?

Security

1. What are the security requirements?
2. Does all, or only some of the data need to be secure?
3. Who will have access to this information?
4. Who will be allowed to change this information?
5. In what manner shall I secure this data i.e. encryption, Host passwords, card passwords/PINs or all of these?
6. Should the keys/PINs be customer or system-activated?

7. What form of version control do I want?

Value Applications

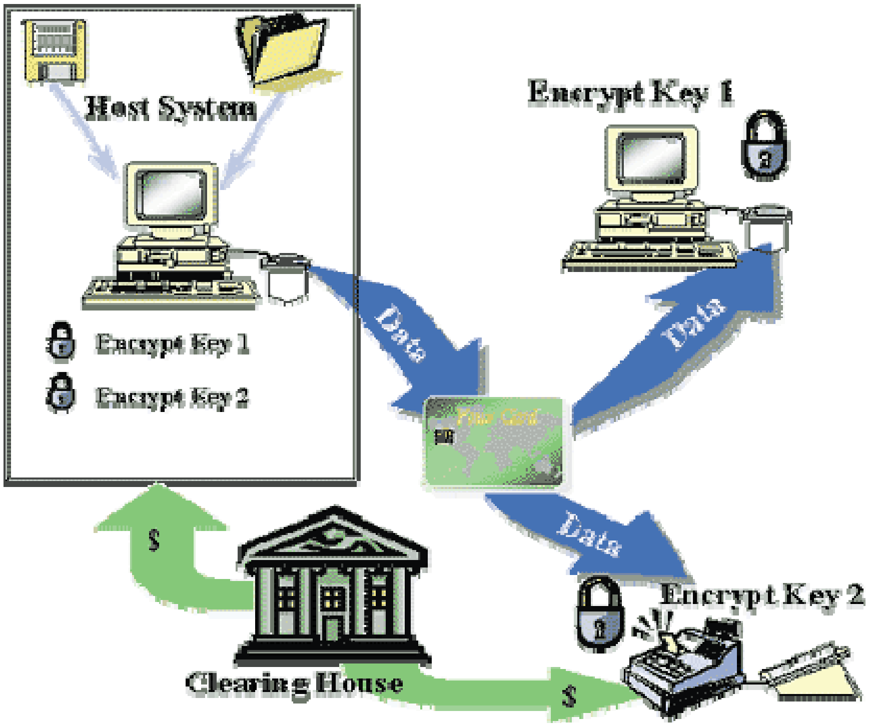
1. Should the value in the cards be reloadable or will the cards be disposable?
2. How will I distribute the cards?
3. How will cards be activated and loaded with value?
4. What type of card traceability should I implement?
5. What is the minimum and maximum value to store on each card?
6. Will there be a refund policy?

General

1. How many types of artwork will be included in the issuance?
2. Who will do the artwork?
3. What is needed on the card? For example signature panels, Mag-Stripe, Embossing etc.

It is highly recommended that you graphically diagram the flow of information.

Multi-Application Card System



Building a smart card system that stores value i.e. gift certificates, show tickets, redemption points or cash equivalents requires an attention to detail not necessary in other information management systems. The key to success is not to overrun the system with features that can confuse users and cause problems in management. We recommend that you phase-in each feature set after the first one is working. Here is a list of some questions that are pertinent to these systems in addition to the above questions.

Deployment

We recommend as the minimum steps in deploying a Stored Value or Multi-Application System.

A. Establish clear achievable program objectives

B. Make sure the organization has a stake in the project's success and that management buys into the project.
C. Set a budget.
D. Name a project manager.
E. Assemble a project team and create a team vision.
F. Graphically create an information - card and funds-flow diagram.
G. Assess the card and reader options.
H. Write a detailed specification for the system.
I. Set a realistic schedule with inch-stones and mile-stones.
J. Establish the security parameters for both people and the system.
K. Phase-in each system element, testing as you deploy.
L. Reassess for security leaks.
M. Deploy the first phase of cards and test, test.
N. Train the key employees responsible for each area.
O. Set-up a system user manual.
P. Check the reporting structures.
Q. Have contingency plans should problems arise.
R. Deploy and announce.
S. Advertise and market your system.

6. Security

Smart cards provide computing and business systems the enormous benefit of portable and secure storage of data and value. At the same time, the integration of smart cards into your system introduces its own security management issues, as people access card data far and wide in a variety of applications.

The following is a basic discussion of system security and smart cards, designed to familiarize you with the terminology and concepts you need in order to start your security planning.

What Is Security?

Security is basically the protection of something valuable to ensure that it is not stolen, lost, or altered. The term "data security" governs an extremely wide range of applications and touches everyone’s daily life. Concerns over data security are at an all-time high, due to the rapid advancement of technology into virtually every transaction, from parking meters to national defense.

Data is created, updated, exchanged and stored via networks. A network is any computing system where users are highly interactive and interdependent and by definition, not all in the same physical place. In any network, diversity abounds, certainly in terms of types of data, but also types of users. For that reason, a system of security is essential to maintain computing and network functions, keep sensitive data secret, or simply maintain worker safety. Any one company might provide an example of these multiple security concerns: Take, for instance, a pharmaceutical manufacturer:

Type Of Data	**Security Concern**	**Type Of Access**
Drug Formula	Basis of business income. Competitor spying	Highly selective list of executives
Accounting,	Required by law	Relevant

Regulatory		executives and departments
Personnel Files	Employee privacy	Relevant executives and departments
Employee ID	Non-employee access. Inaccurate payroll, benefits assignment	Relevant executives and departments
Facilities	Access authorization	Individuals per function and clearance
Building safety, emergency response	All employees	

What Is Information Security?

Information security is the application of measures to ensure the safety and privacy of data by managing it’s storage and distribution. Information security has both technical and social implications. The first simply deals with the ‘how’ and ‘how much’ question of applying secure measures at a reasonable cost. The second grapples with issues of individual freedom, public concerns, legal standards and how the need for privacy intersects them. This discussion covers a range of options open to business managers, system planners and programmers that will contribute to your ultimate security strategy. The ultimate choice rests with the system designer and issuer.

The Elements Of Data Security

In implementing a security system, all data networks deal with the following main elements:

1. **Hardware,** including a servers, redundant mass storage devices, communication channels and lines, hardware tokens (smart cards) and remotely located devices (e.g., thin clients or Internet appliances) serving as interfaces between users and computers
2. **Software**, including operating systems, database management systems, communication and security application programs.
3. **Data**, including databases containing customer - related information.
4. **Personnel**, to act as originators and/or users of the data; professional personnel, clerical staff, administrative personnel, and computer staff.

The Mechanisms Of Data Security

Working with the above elements, an effective data security system works with the following key mechanisms to answer:

1. **Has My Data Arrived Intact? (Data Integrity)** This mechanism ensures that data was not lost or corrupted when it was sent to you.
2. **Is The Data Correct And Does It Come From The Right Person? (Authentication)** This proves user or system identities.

3. **Can I Confirm Receipt Of The Data And Sender Identity Back To The Sender?** (Non-Repudiation)
4. **Can I Keep This Data Private?**(Confidentiality) – Ensures only senders and receivers access the data. This is typically done by employing one or more encryption techniques to secure your data.
5. **Can I Safely Share This Data If I Choose? (Authorization and Delegation)** You can set and manage access privileges for additional users and groups.
6. **Can I Verify The That The System Is Working?** (Auditing and Logging) Provides a constant monitor and troubleshooting of security system function.
7. **Can I Actively Manage The System? (Management)** Allows administration of your security system.

Data Integrity

This is the function that verifies the characteristics of a document and a transaction. Characteristics of both are inspected and confirmed for content and correct authorization. Data Integrity is achieved with electronic cryptography that assigns a unique identity to data like a fingerprint. Any attempt to change this identity signals the change and flags any tampering.

Authentication

This inspects, then confirms, the proper identity of people involved in a transaction of data. In Authentication, a Digital Signature verifies data at its origination by producing an identity that can be mutually verified by all parties involved in the transaction. A cryptographic hash algorithm produces a Digital Signature.

Non-Repudiation

This eliminates the possibility of a transaction being repudiated, or invalidated by incorporating a Digital Signature that a third party can verify as correct. Similar in concept to registered mail, the recipient of data re-hashes it, verifies the Digital Signature, and compares the two to see that they match.

Authorization and Delegation

Authorization is the processes of allowing access to specific data within a system. Delegation is the utilization of a third party to manage and certify each of the users of your system. (Certificate Authorities)

Auditing and Logging

This is the independent examination and recording of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Management

Is the oversight and design of the elements and mechanisms discussed above and below.

Confidentiality/Cryptography

Confidentiality is the use of encryption to protect information from unauthorized disclosure. Plain text is turned into cipher text via an algorithm, then decrypted back into plain text using the same method.

Cryptography is the method of converting data from a human readable form to a modified form, and then back to its original readable form, to make unauthorized access difficult. Cryptography is used in the following ways:

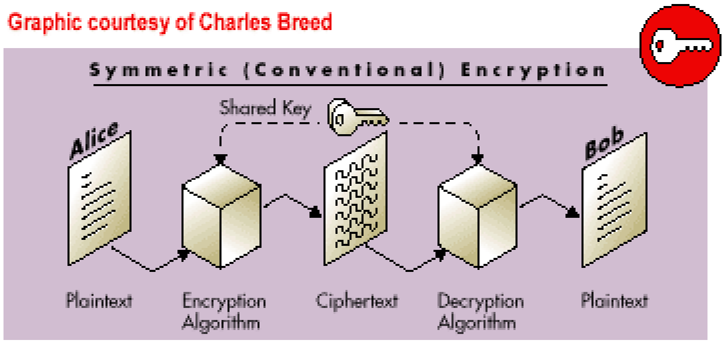
- Ensure data privacy, by encrypting data
- Ensures data integrity, by recognizing if data has been manipulated in an unauthorized way
- Ensures data uniqueness by checking that data is “original”, and not a “copy” of the “original”. The sender attaches a unique identifier to the “original” data. This unique identifier is then checked by the receiver of the data.

The original data may be in a human-readable form, such as a text file, or it may be in a computer-readable form, such as a database, spreadsheet or graphics file. The original data is called **unencrypted data** or **plain text**.The modified data is called **encrypted data** or **cipher text**. The process of converting the unencrypted data is called **encryption**. The process of converting encrypted data to unencrypted data is called **decryption**

In order to convert the data, you need to have an encryption algorithm and a key. If the same key is used for both encryption and decryption that key is called a **secret key** and the algorithm is called a **symmetric**

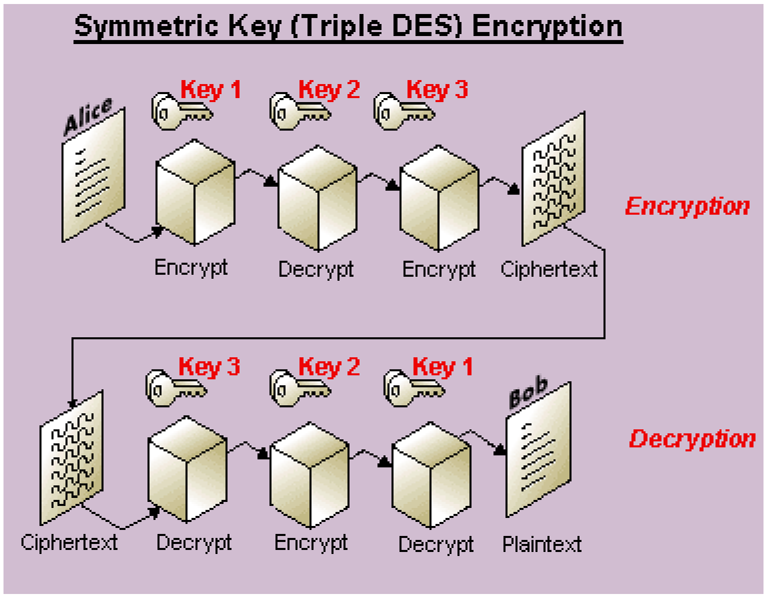
algorithm. The most well-known symmetric algorithm is DES (Data Encryption Standard).

Graphic courtesy of Charles Breed



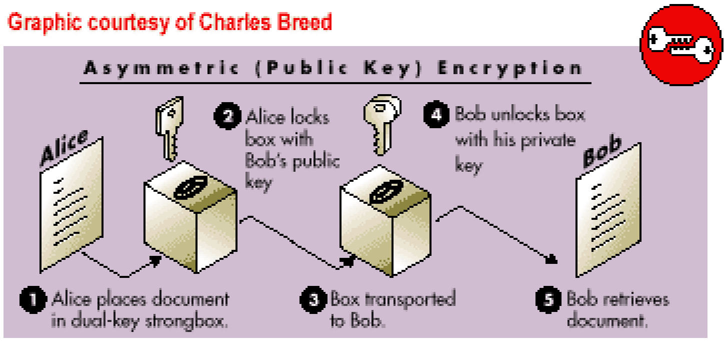
The Data Encryption Standard (DES) was invented by the IBM Corporation in the 1970's. During the process of becoming a standard algorithm, it was modified according to recommendations from the National Security Agency (NSA). The algorithm has been studied by cryptographers for nearly 20 years. During this time, no methods have been published that describe a way to break the algorithm, except for brute-force techniques. DES has a 56-bit key, which offers 2^{56}or 7 x 10^{16} possible variations. There are a very small numbers of weak keys, but it is easy to test for these keys and they are easy to avoid. Please contact CardLogix directly for more details.

Triple-DES is a method of using DES to provide additional security. Triple-DES can be done with two or with three keys. Since the algorithm performs an encrypt-decrypt-encrypt sequence, this is sometimes called the EDE mode. This diagram shows Triple-DES three-key mode used for encryption:



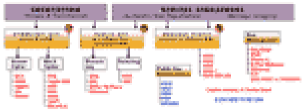
If different keys are used for encryption and decryption, the algorithm is called an **asymmetric algorithm**. The most well-known asymmetric algorithm is RSA, named after its three inventors (Rivest, Shamir, and Adleman). This algorithm uses two keys, called the **private key**. These keys are mathematically linked. Here is a diagram that illustrates an asymmetric algorithm:

Graphic courtesy of Charles Breed


Asymmetric (Public Key) Encryption
Alice
❷ Alice locks box with Bob's public key
❹ Bob unlocks box with his private key
Bob
❶ Alice places document in dual-key strongbox.
❸ Box transported to Bob.
❺ Bob retrieves document.

Asymmetric algorithms involve extremely complex mathematics typically involving the factoring of large prime numbers. Asymmetric algorithms are typically stronger than a short key length symmetric algorithm. But because of their complexity they are used in signing a message or a certificate. They not ordinarily used for data transmission encryption.

Data Security Mechanisms And Their Respective Algorithms



CLICK TO ZOOM

Smart Cards For Data Security

As the card issuer, you must define all of the parameters for card and data security. There are two methods of using cards for data system security, host-based and card-based. The safest systems employ both methodologies.

Host-Based System Security

A host-based system treats a card as a simple data carrier. Because of this, straight memory cards can be used very cost-effectively for many systems. All protection of the data is done from the host computer. The card data may be encrypted but the transmission to the host can be vulnerable to attack. A common method of increasing the security is to write in the clear (not encrypted) a key that usually contains a date and/or time along with a secret reference to a set of keys on the host. Each time the card is re-written the host can write a reference to the keys. This way each transmission is different. But parts of the keys are in the clear for hackers to analyze. This security can be increased by the use of smart memory cards that employ a password mechanism to prevent unauthorized reading of the data. Unfortunately the passwords can be sniffed in the clear. Access is then possible to the main memory. These methodologies are often used when a network can batch up the data regularly and compare values and card usage and generate a problem card list.

Card-Based System Security

These systems are typically microprocessor card-based. A card, or token-based system treats a card as an active computing device. The Interaction between the host and the card can be a series of steps to determine if the card is authorized to be used in the system. The process also checks if the user can be identified, authenticated and if the card will present the appropriate credentials to conduct a transaction. The card itself can also demand the same from the host before proceeding with a transaction. The access to specific information in the card is controlled by A) the card's internal Operating System and B) the preset permissions set by the card issuer regarding the files conditions.

There are predominately two types of card operating systems. One type of card OS is the most cost- effective in many businesses because you only pay for the size and functions that you specify. This ***Classic*** approach treats each card as a secure computing and storage device. Files and permissions to these files are all set by the issuer in advance. The only access to the cards is through the operating system. There are no back doors, no reconfiguration of file structures on the card. Data is read or written to the card through permissions set only by the issuers. The operating system performs a set of "applications" such as authentication and encryption as requested through commands sent to the card. The CardLogix M.O.S.T. OS is one example of this type.

The second methodology is the ***Disk Drive*** approach to card operating systems. The card is a computing device with an active memory manager this allows you to load onto the card specific “applications” and files. The card operating system allows for active file allocation and management. It is designed for card programs that have a long expected user life (4 years +). Java Cards and the Microsoft Windows Card OS are examples of this approach. These cards have a much higher risk of tampering due to the ability to introduce active applets and or viruses into the card. You could conceivably replace a purse or file with a low value with a new purse that has the same name with a higher value.

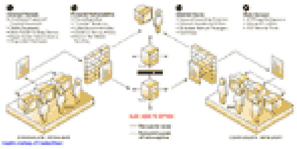
Initial issuance of these cards is costly, due to the sophistication of the OS. The advantage of this approach is that card replacement costs can possibly go down through the use of in field upgrades. These card architectures need a larger memory for future unplanned upgrades and a larger program memory to upload applets. This translates to larger semiconductors at a higher cost. These approaches also come with a licensing burden that is ultimately paid by the card issuer. Also, the security infrastructure costs are much higher to manage due to the multiple points of entry to card system functions.

Threats To Cards and Data Security

Effective security system planning takes into account the need for authorized users to access data reasonably easily, while considering the many threats that this access presents to the integrity and safety of the information. There are basic steps to follow to secure all smart card systems, regardless of type or size.

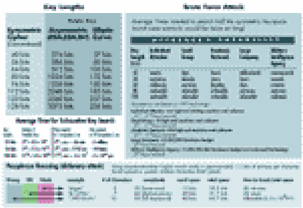
- **Analysis:** Type(s) of data to secure; users, points of contact, transmission. Relative risk/impact of data loss
- **Deployment of your proposed system**
- **Road Test:** Attempt to hack your system; learn about weak spots, etc.
- **Synthesis:** Incorporate road test data, re-deploy
- **Auditing:** Periodic security monitoring, checks of system, fine-tuning

When analyzing the threats to your data an organization should look closely at two specific areas: Internal attacks and external attacks. The first and most common compromise of data comes from disgruntled employees. Knowing this, a good system manager separates all back-up data and back-up systems into a separately partitioned and secured space. The introduction of viruses and the attempted formatting of network drives is a typical internal attack behavior. By deploying employee cards that log an employee into the system and record the time, date and machine that the employee is on, a company automatically discourages these type of attacks.



CLICK TO ZOOM

External attacks are typically aimed at the weakest link in a company's security armor. The first place an external hacker looks at is where they can intercept the transmission of your data. In a smart card enhanced system this starts with the card.



CLICK TO ZOOM

The following sets of questions are relevant to your analysis. Is the data on the card transmitted in the clear or is it encrypted? If the transmission is sniffed, is each session secured with a different key? Does the data move from the reader to the PC in the clear? Does the PC or client transmit the data in the clear? If the packet is sniffed, is each session secured with a different key? Does the operating system have a back door? Is there a mechanism to upload and down load functioning code? How secure is this system? Does the OS provider have a good security track record? Does the card manufacturer have precautions in place to secure your data? Do they understand the liabilities? Can they provide other security measures that can be implemented on the card and or module? When the card is subjected to *Differential Power* attacks and *Differential Thermal* attacks does the OS reveal any secrets? Will the semiconductor utilized meet this scrutiny? Do your suppliers understand these questions?

Other types of problems that can be a threat to your assets include:

- Improperly secured passwords (writing them down, sharing)

- Assigned PINs and the replacement mechanisms
- Delegated Authentication Services
- Poor data segmentation
- Physical Security (the physical removal or destruction of your computing hardware)

Security Architectures

When designing a system a planner should look at the total cost of ownership this includes:

- Analysis
- Installation and Deployment
- Delegated Services
- Training
- Management
- Audits and Upgrades
- Infrastructure Costs (Software and Hardware)

Over 99% of all U.S.- based financial networks are secured with a Private Key Infrastructure. This is changing over time, based on the sheer volume of transactions managed daily and the hassles that come with private key management. Private Key-based systems make good sense if your expected user base is less than 500,000 participants.

Public Key Systems are typically cost effective only in large volumes or where the value of data is so high that its worth the higher costs associated with this type of deployment. What most people don’t realize is that Public Key systems still rely heavily on Private Key encryption for all transmission of data. The Public Key encryption algorithms are only used for non-repudiation and to secure data integrity. Public Key infrastructures as a rule employ every mechanism of data security in a nested and coordinated fashion to insure the highest level of security available today.

CONCLUSION

Applications

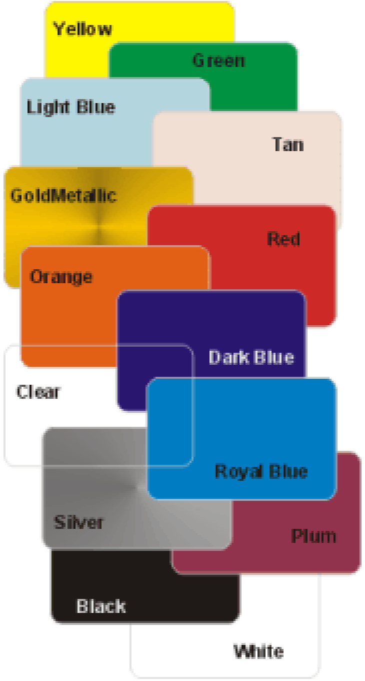
The SIM (Subscriber Identification Module) cards in cellphones are smart cards, and act as a repository for information like owner ID, cash balance, etc. More than 300 million of these cards are being used worldwide today.

Small dish TV satellite receivers also use smart cards for storing subscription information. There are over four million in the US alone and millions more in Europe and Asia.

There are tons of other applications that smart cards can be used for. For example, they could be used for computer or Internet user authentication, or for simply giving physical access through a gate. You could have resort membership cards, or tickets for mass transport such as metro rail and buses. Smart cards can be extremely useful in Government departments such as in collecting toll tax on highways, or as identity cards, passports, etc.

INDEX

INDEX


Yellow
Green
Light Blue
Tan
GoldMetallic
Red
Orange
Dark Blue
Clear
Royal Blue
Silver
Plum
Black
White

State of affairs in India

In India, the Gujarat government has recently switched completely to smart cards for all new driving licenses. Each card carries its owner’s photograph and fingerprint, and traffic offenses are recorded on the spot using hand-held terminals. One indirect advantage is that making fake licenses has become almost impossible.

Welcome to Smart Card Basics.com. This is a sponsored site brought to you by a number of companies in the smart card industry. We have tried to make this site informative with out a single perspective or marketing fluff. It is our belief that informed users make better choices.

Chip card technology is fast becoming commonplace in our culture and daily lives. We hope that this site will bring you a little closer in your understanding of this exciting technology and the benefits it can bring to your applications.

If you have specific questions regarding a specific technology discussed below feel free to send us an e-mail and the appropriate sponsor will respond.

SMART CARDS AND SECURITY OVERVIEW

1. Overview

A smart card – a type of chip card – is a plastic card embedded with a computer chip that stores and transacts data between users. This data is associated with either value or information or both and is stored and processed within the card's chip, either a memory or microprocessor. The card data is transacted via a reader that is part of a computing system. Smart card-enhanced systems are in use today throughout several key applications, including healthcare, banking, entertainment and transportation. To various degrees, all applications can benefit from the added features and security that smart cards provide. According to Dataquest, the worldwide smart card market will grow to 4.7 Billion units and $6.8 Billion by 2002.

Applications

First introduced in Europe over a decade ago, smart cards debuted as a stored value tool for pay phones to reduce theft. As smart cards and other chip-based cards advanced, people found new ways to use them, including charge cards for credit purchases and for record keeping in place of paper.

In the U.S., consumers have been using chip cards for everything from visiting libraries to buying groceries to attending movies, firmly integrating them into our everyday lives. Several states have chip card programs in progress for government applications ranging from the Department of Motor Vehicles to Electronic Benefit Transfer (EBT). Many industries have implemented the power of smart cards into their products such as the new GSM digital cellular phones to TV-satellite decoders.

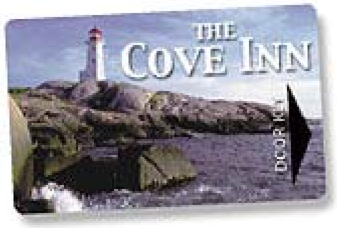
3. Reader and Terminal Basics

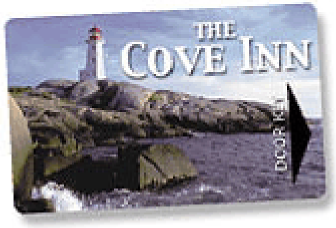
For the sake of clearly defining all of the different hardware devices that smart cards can be plugged into. The industry has adopted the following definitions:

The term "reader" is used to describe a unit that interfaces with a PC for the majority of its processing requirements. In contrast a "terminal" is a self-contained processing device.

Both terminals and readers read and write to smart cards. Readers come in many form factors and in a wide variety of capabilities. The easiest way to describe a reader is by the method of it's interface to a PC. Smart Card Readers are available that interface to RS232 serial ports, USB ports, PCMCIA slots, floppy disk slots, parallel ports, infrared IRDA ports and Keyboards and keyboard wedge readers. Another difference in reader types is the on board intelligence and capabilities or lack thereof. Extensive price and performance differences exist between an industrial strength intelligent reader that supports a wide variety of card protocols and a home style win-card reader that only works with microprocessor cards and performs all processing of the data in the PC.

The options in terminal choice are just as wide. Most units have their own operating systems and development tools. They typically support other functions such as magstripe reading, modem functions and transaction printing.




THE
COVE INN
DOOR KEY