SMART CARD SECURITY

Abstract

Now-a days Chip card technology (smart cards) is fast becoming commonplace in our culture and daily lives. A **smart card** is a card that is embedded with either a microprocessor and a memory chip or only a memory chip with non-programmable logic. The microprocessor card can add, delete, and otherwise manipulate information on the card, while a memory-chip card (for example, pre-paid phone cards) can only undertake a pre-defined operation. Smart cards, unlike magnetic stripe cards, can carry all necessary functions and information on the card. Therefore, they do not require access to remote databases at the time of the transaction. This paper deals with what is a smart card, why smart cards are used, what are the different types of chip cards, multi application card systems, and their security.This paper mainly concentrates on smart cards security. Lastly this paper discuss on applications and on future scope.

Introduction

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.

Why Smart Cards

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:

- Loyalty and Stored Value
- Securing Information and Physical Assets
- E-Commerce
- Health Care
- Network Security
- Loyalty and Stored Value

A primary use of smart cards is stored value, particularly loyalty programs

that track and incentives repeat customers. Stored value is more convenient and safer than cash. 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.

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.

E-Commerce

Smart cards make it easy for consumers to securely store information and cash for purchasing. The advantages they offer consumers are:

- The card can carry personal account, credit and buying preference information that can be accessed with a mouse click instead of filling out forms.
- Cards can manage and control expenditures with automatic limits and reporting.
- 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.
- Micro Payments - paying nominal costs without transaction fees associated with credit cards or for amounts too small for cash, like reprint charges.

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.

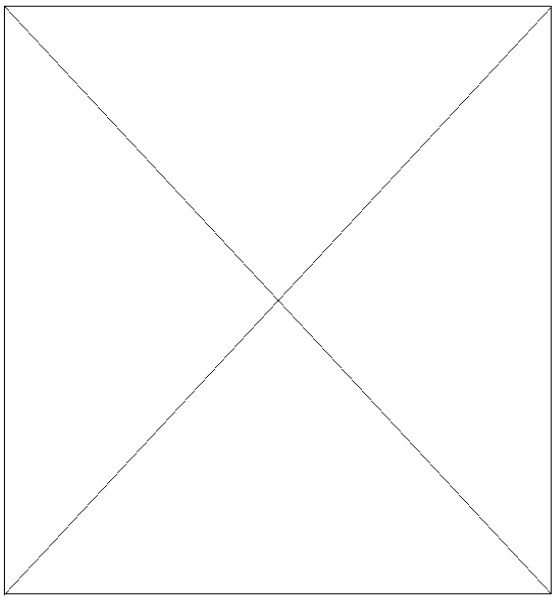
- Rapid identification of patients; improved treatment
- A convenient way to carry data between systems or to sites without systems
- Reduction of records maintenance costs

Network Security

Business to business Intranets and Virtual Private Networks “Vans” 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.

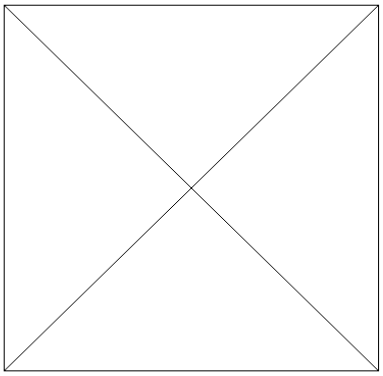
Types of Chip Cards

Smart cards are defined according to 1). How the card data is read and written and 2). The type of chip implanted within the card and its capabilities. There is a wide range of options to choose from when designing your system.



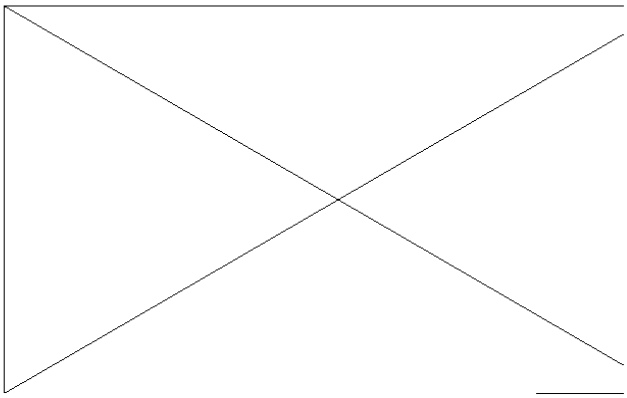
Contact Cards

The most common type of smart card. Electrical contacts located on the outside of the card connect to a card reader when the card is inserted.



Increased levels of processing power, flexibility and memory add cost. Single function cards are often the most cost-effective solution. Choose the right type of smart card for your application by evaluating cost versus functionality and determine your required level of security. All of these variables should be weighted against the expected lifecycle of the card. On average the cards typically comprise only 10 to 15 percent of the total system cost with the infrastructure, issuance, training and advertising making up the other 85 percent. The following chart demonstrates some general rules of thumb;

Card Function Trade-Offs



Memory Cards

Memory cards have no sophisticated processing power and cannot manage files dynamically. All memory cards communicate to readers through synchronous protocols. In all memory cards you read and write to a fixed address on the card. There are three primary types of memory cards: 1). Straight, 2). Protected, and 3). Stored Value.

1. 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. These cards are easily duplicated and cannot be tracked by on-card identifiers.

2. 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 the entire 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. These cards are not easily duplicated but can possibly be impersonated by hackers. They typically can be tracked by an on-card identifier.

3. 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.

Contactless Cards

These are smart cards that employ a radio frequency (RFID) between card and reader without physical

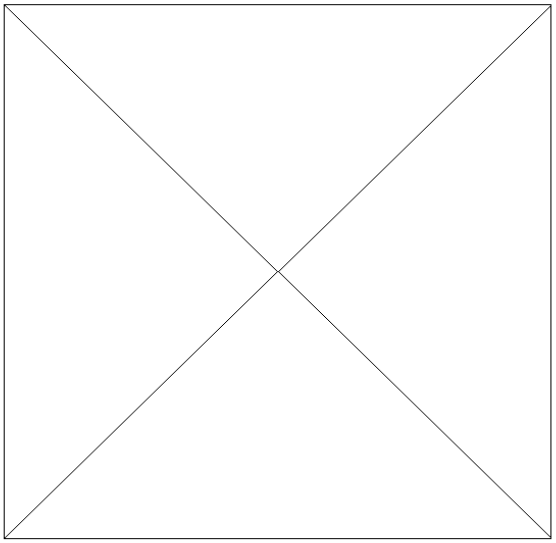
insertion of the card. Instead the card is passed along the exterior of the reader and read. Types include proximity cards which are implemented as a read-only technology for building access. These cards function with a limited memory and communicate at 125 MHz. True read & write contactless cards were first used in transportation for quick decrementing and re-loading of fare values where their lower security was not an issue. They communicate at 13.56 MHz, and conform to the ISO14443 standard. These cards are often straight memory types. They are also gaining popularity in retail stored value, since they can speed-up transactions and not lower transaction processing revenues (i.e. VISA and Mastercard), like traditional smart cards. Variations of the ISO14443 specification include A, B, and C, which specify chips from either specific or various manufacturers. A=Philips B=Everybody else and C=Sony chips. Contactless card drawbacks include the limits of cryptographic functions and user memory versus microprocessor cards and the limited distance between card and reader required for operation.

Combination Cards

These are hybrids that employ both contact and contactless technology in one card. Combi-cards can also contain two different types of chips in contrast to a Dual-Interface card where a single chip manages both functions.

Multi-Application Card Systems

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



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

As the minimum steps in deploying a stored value or multi-application system, establish clear achievable program objectives;

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

Smart Card Security 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

Type Of Data	Security Concern	Type Of Access
Drug Formula	Basis of business income. Competitor spying	Highly selective list of executives
Accounting, Regulatory	Required by law	Relevant 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 such as customers, visitors, or vendors
Building safety, emergency response	All employees	Outside emergency response

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:

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 eventual 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 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

Smart Card Security (Section 2)

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 or value. In authentication systems, authentication is measured by assessing the mechanisms strength and how many factors are used to confirm the identity. In a PKI system 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. Card management also requires the management of card issuance, replacement and retirement as well as polices that govern a system.

Cryptography/Confidentiality

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.

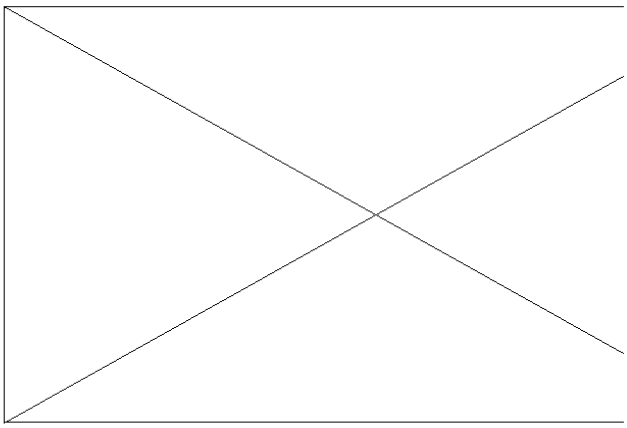
Cryptography is the method of converting data from a human readable form to a modified form, and then back to its original readable form, to make unauthorized access difficult. Cryptography is used in the following ways:

- 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.

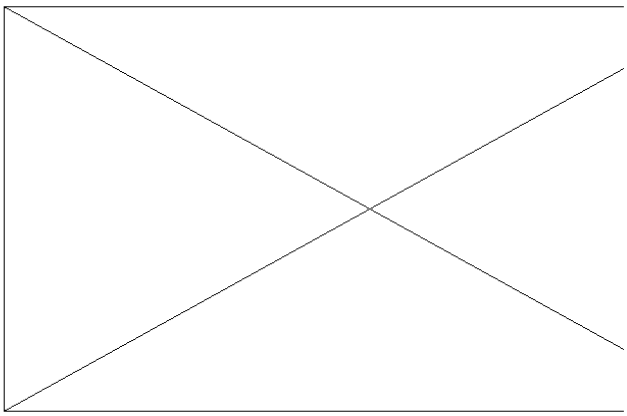
Data Security Mechanisms and their Respective Algorithms

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).

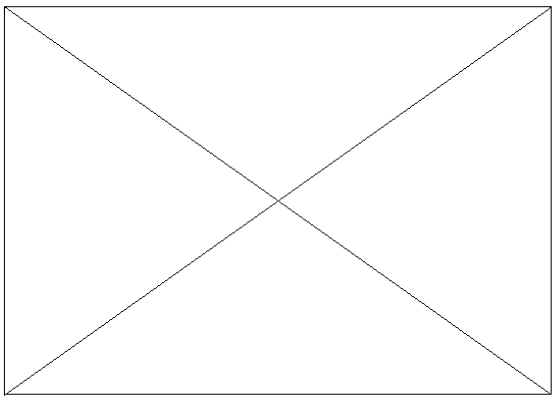


The Data Encryption Standard (DES) was invented by the IBM Corporation in the 1970's. During the process of becoming a standard algorithm, it was modified according to recommendations from the National Security Agency (NSA). The algorithm has been studied by cryptographers for nearly 20 years. During 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 256 or 7 x 1016 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.

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.



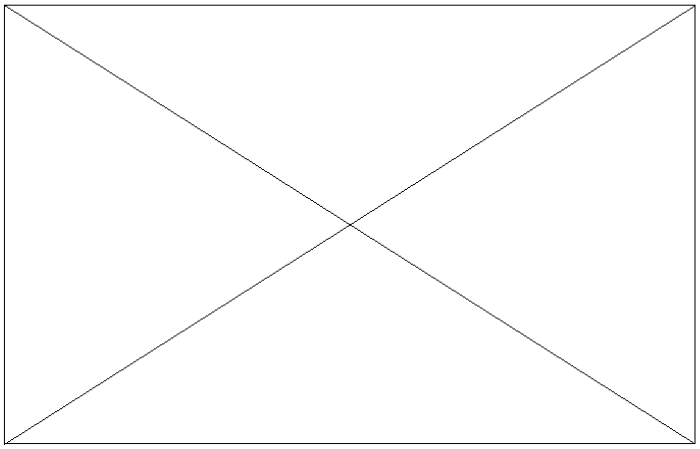
If different keys are used for encryption and decryption, the algorithm is called an asymmetric algorithm. The most well-known asymmetric algorithm is RSA, named after its three inventors (Rivest, Shamir, and Adleman). This algorithm uses two keys, called the private key. These keys are mathematically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



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.

Smart Card Security (Section 3)

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. The card can be in a standard CR80 form factor or be in a USB dongle or it could be a GSM SIM Card.

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: Types 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.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.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.

The most common **smart card applications** are:

- Credit cards
- Electronic cash
- Computer security systems
- Wireless communication
- Loyalty systems (like frequent flyer points)
- Banking
- Satellite TV
- Government identification

. Future of Smart Cards:

Given the advantages of smart cards over magnetic stripe cards, there can be no doubt that the future of smart cards is very bright. If the current trends are anything to go by, the smart card market is set for exponential growth in the next few years. Future for smart cards depends mainly on the introduction of multi-application cards and overcoming the simplistic mindset that smart cards are just a method of making a payment.

Conclusion:

Smart cards can add convenience and safety to any transaction of value and data; but the choices facing today's managers can be daunting. We hope this paper has adequately presented the options and given you enough information to make informed evaluations of performance, cost and security that will produce a smart card system that fits today's needs and those of tomorrow. It is our sincere belief that informed users make better choices, which leads to better business for everybody.