IDRBT's Working Paper No. 6

A Framework for Smart Card Payment Systems

Ashutosh Saxena and Aditya Gaiha

ABSTRACT

This work is a compilation of current knowledge relating to a new technology known as Smart Card. We begin by understanding the various physical and technical characteristic features of Smart Cards and then move on to various operational issues involved in setting up of a Smart Card-based Payment System. We present a foundation for understanding Smart Cards and follow it up by specific application software that is required for understanding the technology -- and challenges -- associated with the uses of Smart Cards for banking applications. Java Card and Windows for Smart Cards (WfSC) have also been separately discussed. The paper concludes with an overview of Smart Cards for payment systems in the country (SMARS) along with emerging scenarios, and also focuses on the prevailing multi-application on Smart Card.

1.0 What is a Smart Card?

Smart Card is a fully functioning computer system built on a single chip (integrated circuit). This computer system has important similarities and differences from other kinds of traditional computers. Like others, it has a central processing unit (CPU) and various kinds of memory. Unlike others, since cost is a major constraint, these computers are sold for a few hundred of Rupees. The chips must also be as small as possible to meet the form-factor requirements of bank card applications (ATMs, Point of Sale devices, etc.).

1.1 Smart Card Memory

Smart Cards use several types of memory, all implemented within a single chip. These are:

- Permanent memory
- Programmable nonvolatile memory
- Volatile memory

January, 2001

Permanent memory is generally ROM (Read Only Memory), placed in the chip hardware during manufacturing. It cannot be changed, although its operation can be blocked through logical operations. Programmable nonvolatile memory is generally EEPROM (Electrically Erasable Programmable Read Only Memory). It can be programmed after the chip is manufactured, exposing both its strength and its weakness. E-squared PROM permits making changes to programs, increasing the Smart Card's flexibility but also exposes it to various types of nasty security attacks. Volatile memory is generally RAM (Random Access Memory), used as a temporary storage area for interim operations. It loses its contents when power is removed from the chip. Smart Card programming requires special skills since programs must be written using the smallest amount of memory possible. One major factor in understanding Smart Cards is realizing the implications of when a program is added to what type of memo ry. If a program is added in ROM, it must be added when the basic chip is manufactured, and no changes can be made to it. If programs are added to EEPROM, they can be added both prior to issuance of the card or afterwards.

1.2 Smart Card Processing Power

Most Smart Cards today use 8-bit microprocessors. Although more powerful 16- and even 32-bit chips will be available soon, none have multi-threading and other powerful features that are common in standard computers. Memory sizes range from as little as 1K of programmable non-volatile memory to as much as 24K, with larger memory chips coming soon and ROM size is similarly limited. However large memory may become, the total amount will always be relatively limited compared to normal computer capabilities. That imposes the requirement of strict discipline in coding and limits the defensive measures that can be implemented.

1.3 Chip Family

A chip family has a single CPU with many different memory configurations. This is to accommodate programs of varying sizes and states of maturity. The smallest chip in the family may have 4 K of ROM, 256 bits of RAM, and 1 K of EEPROM. The next size may have the same ROM and RAM, but varying amounts of EEPROM - 2K or 4 K, for example. The next members of the family may have 6 K of ROM, 256 bits of RAM, and 6, 8, or 10 K of EEPROM. Another possibility is 8 K ROM and 4 or 6 K of EEPROM. A cryptographic co-processor may also be added for those applications that require faster execution of cryptographic algorithms, sometimes with some additional dedicated RAM.

1.4 Soft Mask and Hard Mask Cards

Smart Card industry experts refer to Smart Cards as being either soft mask or hard mask. Masking refers to where an application program is placed. If the application is placed in EEPROM, it is termed a soft mask card. If most of the application is placed in ROM, it is called a hard mask card, though variable features and personalization data is still placed in EEPROM.

Banks commonly use a soft mask card for pilot testing new applications and then move on to hard mask cards for larger deployments. However, some applications have limited deployments that are never taken to hard mask, as hard masking is expensive in terms of both time and money. Hard masks may also not be justified for some applications, such as an employee identification card for small companies.

Differentiating cards into soft or hard masks works well for single application cards, but is often confusing when there are multiple applications on the same chip. That is, a single card may have one application in ROM and thus be considered a hard mask card with respect to that application, but also have another application placed in EEPROM, and so it may be a soft mask card with respect to that application.

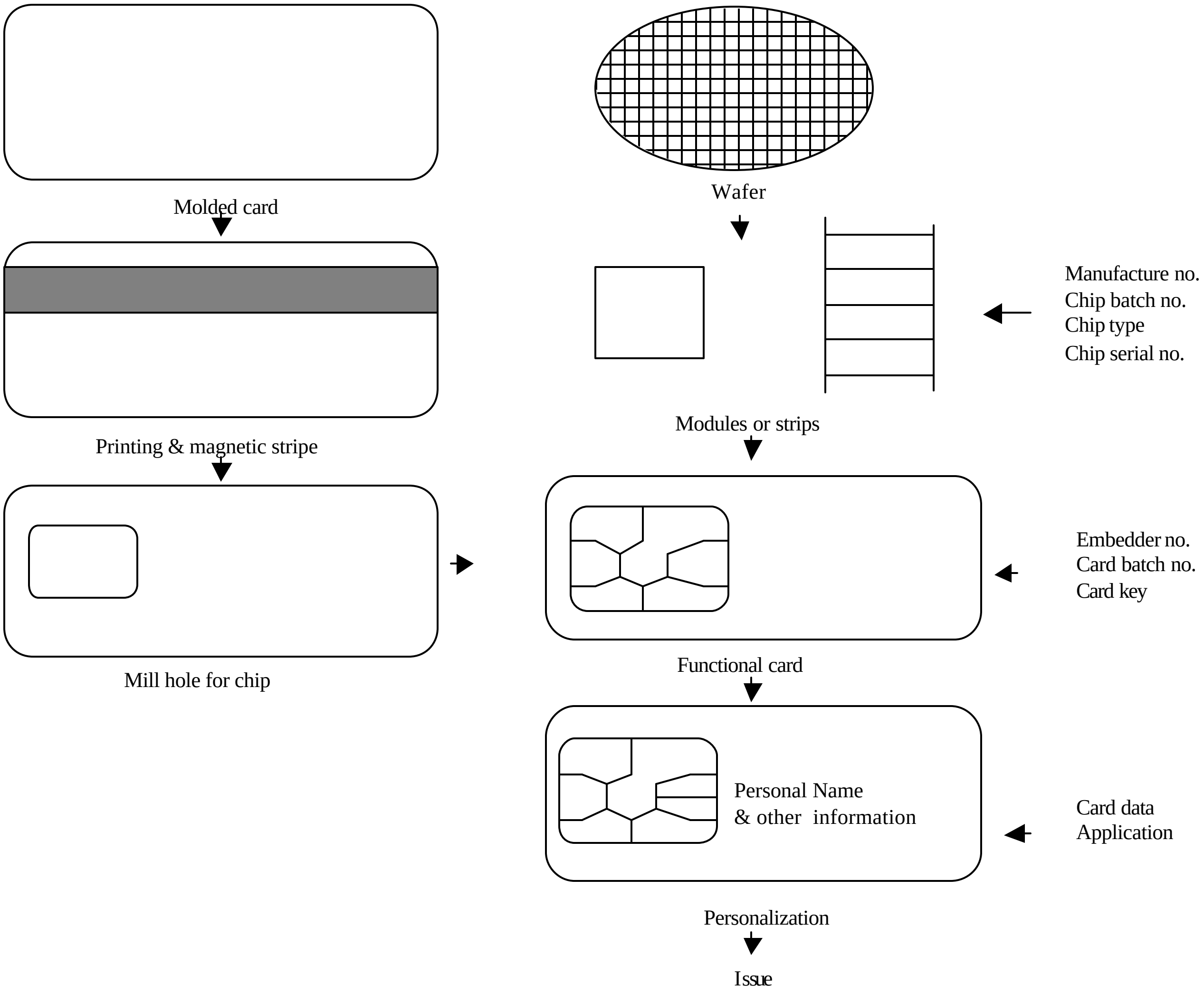

Figure – 1 : Smart Card Production Cycle

1.5 Programming Languages

Most Smart Cards are currently programmed in low-level languages based on proprietary Smart Card operating systems. Some of the programming has been done in the chip's native instruction set (generally Motorola 6805, Intel 8051, or Hitachi H8). Though this results in highly efficient code, it is much more difficult to program than higher-level languages. The number of programmers who could do this type of programming is quite limited.

In 2000, a new type of card has shown up, sometimes called a re-configurable card. These re-configurable Smart Cards have a more robust operating system that permits the addition or deletion of application code after the card is issued. Such cards are generally programmed in Java, Windows for Smart Cards, or MEL (the Multos programming language). These cards may have a card operating system and additional layers, which offer industry or application specific features. The operating system must ensure that only authorized applications can be added after the card is issued to the cardholder and that deletions of applications are only done under proper authorization. These re-configurable cards use programming languages that are very well known in the software community, which is one of their advantages. Many programmers will be able to write Smart Card programs that will run on these operating systems, although the special skill of being able to write very memory efficient programs will be needed.

In the next section we present Smart Cards from the perspective of their life cycle -- from pre-personalization to disposal -- where functionality and security concerns constantly mutate.

2.0 Smart Card Life Cycles

Smart Card life cycles are often very complex; development of a new card usually requires the involvement of multiple developers, progressing over several years, with multiple paths, and follows evolutionary growth -- each new version of a specific card product is an improvement over the earlier version.

In the context of this working paper, the life cycle represents the process of developing silicon, software, and systems to perform useful functions. There is no single typical Smart Card life cycle, rather, there are several cycles and several unique routes through them. Application life cycles -- which often intersect with several card life cycles -- are unique to each application and no single standard model exists for all of them. When dealing with applications, the card issuer (bank in case of payment system, etc.) normally determines the application life cycle.

There are also many uses for Smart Cards and the chips that are used in them. The security needs of Smart Cards, and Smart Card chips, range from nonexistent to high. Security generally has a cost, in money, time to market, and Smart Card markets are very price sensitive. Building a Smart Card typically involves a constant concern for cost containment and often means a trade-off of cost against other desirable things. Various decisions are possible and are often driven by conflicting and quickly changing technological, security, and market needs. Minimally, a Smart Card must meet some user requirements, without which there will be no market. It must be designed, manufactured, issued, used, and taken out of use. Each of these steps requires discussion.

2.1 User Requirements

All Smart Cards begin with user requirements. These requirements drive the rest of the process. The user requirements may be well known and have high security needs, such as those for the Secure Application Module (SAM) implemented on a Smart Card in some stored value systems. Alternatively, the user requirements may be generally stated and only partially known, both to the users and the developers involved. They also may be incomplete, in the sense that additional details must be specified in order to build a functioning card. This can either be because the user is unfamiliar with the technology or because the user is familiar enough with the technology to want to use several different suppliers in order to be independent of any one of them. In the case of the EMV specifications, this desire was coupled with the fact that there were three different international organizations involved, each of which wanted scope to tailor the application to specific regional, national, and market needs, and also wanted international interoperability. This kind of application typically goes through a series of different cards, refining the user requirements as time progresses.

2.2 Design

Smart Cards put applications and operating systems into integrated circuits that are embedded in a printed card. Each of these (application, operating system, integrated circuit, and card) is generally designed and manufactured by a different compan y, although the application and the operating system are sometimes done by the card integrator company. The design stage may occur sequentially or simultaneously.

2.3 Manufacturing

Manufacturing involves several developers: application, operating system, chip, and card manufacturing may all be done by separate companies. The chip is manufactured in a semiconductor foundry, the operating system and application are software, and the card is manufactured in a factory dedicated to that purpose. All must have appropriate security arrangements, but these are different depending on the kind of product and company involved. Integrated circuits are tested after the wafer is manufactured. Application(s) may be added during the chip manufacturing stage, when the card is manufactured, or after the card has been issued. The chip manufacturer may not know what application(s) will be added to the chip if the applications are added during card manufacture (personalization) or after the card has been issued (post-issuance downloads to the chip).

2.4 Issuance

A banking application is issued by a financial institution, which has a contract with the end user that governs use of the application. Debit and credit applications typically are used to access an account at the issuing bank. The application developer may or may not be the card issuer. The card issuer may authorize which applications may be placed on the card, each with its own life cycles and requirements.

2.5 Use

The application is used in a transaction, which requires supporting software in a Card Acceptance Device (CAD) or Point of Interaction (POI).

2.6 End of Card Life

Typically, cards have a useful life and an expiration date. The terminal will not accept a transaction from a card that has expired. SAMs are issued in relatively limited numbers and are usually under strict inventory control. They are returned to the issuer upon the end of card life. The end user card is seldom returned to the issuer; they are usually simply discarded.

3.0 Re-configurable Card Life Cycle Overview

Since modern versions of Smart Cards, based on dynamic card operating system features (e.g. MULTOS, JavaCard, Windows for Smart Cards), are becoming more pervasive in the marketplace, we will also focus here on the life cycle for these re-configurable cards.

3.1 User Requirements

One principal user requirement enables the changing or adding of applications during the useful life of the card. This requires appropriate security on the program management functions, as the card will now be subject to virus-like attacks. A complete operating system is needed, and applications desired in the future may not yet be known.

3.2 Design

The operating systems to support these cards are Java, Windows for Smart Cards, or MEL (the MULTOS programming language). These systems will be covered in the later part of the paper, prior to application reviews.

One of the advantages of these cards is that the programming languages used within them are well known and many programmers can create applications for them. This means that the applications will be designed independent of the chip, operating system, and card designs.

3.3 Manufacturing

As stated earlier, chips, operating systems, cards and applications are manufactured separately. Operating systems are generally added to the chip at the chip manufacturing stage. Chips are embedded in modules and modules embedded in cards in the same way as with other cards.

3.4 Issuance

Re-configurable cards are personalized for the end user and issued in the same way as other types of cards are issued. Instruction must be given to the end user on the proper loading and deletion of applications, which is not needed with the other types of cards. The end user has more options available than with the other types of cards, and hence more opportunity to make mistakes.

3.5 Use

As with the other types of cards, these are also used to conduct transactions. Applications must be properly loaded in order to work, and each application will have its own usage instructions and requirements.

3.6 End of Life

These cards are just beginning to come to market and many of the issues regarding the end of card life remain unknown.

4.0 Multi-application Smart Card

Today's Smart Cards are delivered to card issuers and personalization bureaus that operate on the behalf of card issuers with an operating system (OS) already embedded on the chip. These cards are then ready for personalization activities that enable the card's use at the point of sale or with an attached reader on a PC. Until the cards undergo personalization and application loading activities, their abilities are limited to what the primitive card OS permits. The microprocessor chips that support these card OSs are designed and optimized for a specific OS, providing the basic platform for those functions and programs the issuer wishes to support.

One can think of the card OS as a layer of abstraction above the microprocessor and cryptographic co-processor (if present) on the card to insulate developers from the details about the chip's instruction set. This layer of insulation permits a wide variety of developers to create Smart Card applications, and helps to drive down the costs of development and maintenance while helping to assure high degrees of security and flexibility.

The early versions of Smart Cards had no real conception of an operating system. Rather they had application programs 'burned in' at the time of manufacture to support a single purpose (stored value, hold credentials, etc.). Today's multi-application Smart Cards use the card operating system (OS) to create a dynamic usage environment that permits a variety of applications and associated data storage.

Multi-application card OSs are designed to meet the needs of today's business requirements, which include the following:

- Running of applications on a variety of chip and card types
- Isolation of applications from the operating systems
- Common card acceptance device interfaces
- Issuer control over application loading and deleting
- Support for dynamic updates in the field
- Common protection of data and applications
- Multiple sources of applications and card suppliers
- Standardized Application Program Interfaces (APIs)
- Common runtime environments
- Firewalls between applications and data

4.1 MULTOS

MULTOS was originally developed by Natwest Bank in the UK to support the MONDEX e-purse application. MONDEX has since spun off from Natwest into a subsidiary of Mastercard International. Banks and other volume issuers can license MULTOS royalty-free for use with their own branded Smart Card products. Developers build MULTOS applications using the MULTOS Executable Language (MEL) development kit for card issuers or to license common applications to any bank or issuer who wants to place them on their cards. Some of the applications already developed or being developed for MULTOS include:

- Loyalty
- Health
- EMV debit, credit, and charge card
- E-purse
- Global System for Mobile communications (GSM)
- Pay TV
- Mass transit ticketing
- Access controls
- Digital signatures
- Biometrics
- Travel and Entertainment

MULTOS is enjoying wide industry support from a variety of issuers, including:

- Mastercard International
- American Express
- Europay International
- Discover Financial Services
- JCB (Japan)
- MONDEX International

Dozens of individual banks around the world have committed to MULTOS, and today over 14 million cards are on their way, intended for a variety of new pilot and production uses. The MAOSCO Consortium, established to promote MULTOS, provides a central point of coordination for all parties interested in MULTOS implementations.

4.2 Open Platform

Open Platform was developed by Visa International to support banking applications. It is now managed by GlobalPlatform, a new consortium intended to promote Open Platform beyond banking uses. Open Platform is an architecture and sets standards to define and manage dynamic multi-application Smart Cards. Open Platform is an added layer of abstraction atop other card operating systems, including Java Card from Sun

Microsystems and Windows for Smart Cards from Microsoft, described later in the paper, Open Platform includes:

- Card specifications
- Card implementation specifications
- Terminal specifications
- Support infrastructure specifications

Open Platform operates with standard underlying card OSs and POS terminal technologies, adding additional security and functionality to the process. Some of the technology benefits of Open Platform include:

- A wide selection in card types, terminals, operating systems, software providers, and back office support systems for issuers, acquirers, and merchants
- Secure and controlled support of multiple applications on a single card
- Support for existing standards, such as EMV and ISO7816, to assure backward compatibility with existing Smart Card implementations
- Robust security mechanism to aid issuers in risk management of applications and the card itself.

The Open Platform Card Architecture Specification defines an operating system component (Java Card or Windows for Smart Cards), a virtual machine, an API, the Open Platform API, and a set of Open Platform applications. Open Platform maintains the security and risk management aspects of the applications loaded on the card using a resource called Card Manager (CM). CM represents the issuer's interests on the card by preventing and reporting any unauthorized uses of the card. CM supports these four major functions:

- Command dispatch to receive incoming commands and dispatch them to the appropriate on-card application
- Content management to control what gets written to the card, according to issuer requirements
- Security management using a Global PIN that any application can use to control access and to prove user identity
- Security domains that contain issuer-specific cryptographic keys in key-sets that provide for secure communications and privileged operations such as application loading, removal, initialization, and personalization activities.

Open Platform has been extended to support all types of new uses and applications, including set-top boxes, PDAs, smart phones, etc. Although the Visa Open Platform (VOP) version is intended to support the issuance of Smart Cards by banks and other financial services companies for their customers, Open Platform is being promoted by Global Platform to industries outside the purview of financial services.

4.3 Java Card

The Java Card platform enables Java technology to run on Smart Cards and other devices that possess limited memory. The Java Card API permits applications written for one Smart Card platform using Java Card to run on any other such platform. The Java Card Application Environment (JCAE) is licensed on an OEM-basis to Smart Card manufacturers, who produce cards and then sell them as products that support Open Platform or are used as it is.

The Java Card API defines the calling conventions by which an applet accesses the Java Card Runtime Environment (JCRE) and native services. It also allows applications written for one Java Card-enabled platform to run on any other Java Card-enabled platform.

Some of the benefits of Java Card technology are:

- Platform Independence - Java Card applets that comply with the Java Card API specification will run on cards developed using the JCAE, enabling developers to use the same Java Card applet on different vendors' cards.
- Multi-Application Capable - Multiple applications can run on a single card. In the Java programming language, the inherent design around small, downloadable code elements enables secure running of multiple applications on a single card.
- Post-Issuance of Applications - The installation of applications after the card has been issued lets card issuers to dynamically respond to their customer's changing needs.
- Flexible - The Object-Oriented methodology of Java Card technology provides flexibility in programming Smart Cards.
- Compatible with Existing Smart Card Standards - The Java Card API is compatible with formal international standards, such as ISO7816, and industry-specific standards, such as EMV and Open Platform.

Java Card technology was developed to preserve many of the benefits of the Java programming language while enabling Java technology for use on Smart Cards. The Virtual Machine (VM), the language definition, and the core packages are compact and optimized for the resource-constrained environment of Smart Cards. Several of the off-the-shelf development tools for Java can be used to develop applets for the Java Card platform.

4.4 Windows for Smart Cards

Windows for Smart Cards (WfSC) is touted by Microsoft as a means of turning a Smart Card into a near-traditional microprocessor environment without a Graphical User Interface (GUI). It's intended to enhance the uses of existing networks based on Windows95/98, Windows NT, and Windows 2000. Microsoft describes WfSC as the key to a lock that protects business data. The keys are customized to each user and may serve as a replacement to user ID and password logons. WfSC, in conjunction with one or more of the Windows OSs, bring about what Microsoft calls the 4Ps:

- Protection

- Improved Productivity
- Increased Profit
- Facilitates Promotion

Protection
WfSC can help prevent multiple log-ons from occurring on different computers to reduce the problems associated with stolen passwords and stolen identities.

Productivity
Because WfSC is an extension of Windows, developers and users gain consistent experience when dealing with application development tools and application program uses. With standard Windows APIs, issuers of WfSC cards can customize how they are deployed to best meet business and security requirements.

Profit
Reduced credit card fraud, reduced identity theft, and fewer problems with repudiated transactions helps banks and other financial services issuers to realize higher profits and reduced computer security incidents.

Promotion
WfSC products can be used to promote a business to their customers and partners through advertisements and offers on the card, as well as loyalty programs that reward customers to shop and spend.

With a Smart Card framework, payments systems are enhanced and made more impervious to fraud and security problems by providing both new applications and a second factor for user authentication. Converging Smart Card technology with Internet technology yields a synergy, and entirely new possibilities emerge.

5.0 SMARS

The Smart Card based payment scheme developed for banks is essentially due to the co-operative efforts of a group comprising of Reserve Bank of India, I.I.T (Mumbai) and IDRBT. Finally, the group has expanded to 17 partners, each actively involved in developing a smart card based payment system for banks using open standards and ensuring interoperability among the participating banks.

Project SMARS began in 1996. The primary aim of the project was to establish interoperability between different technologies and standards of cards, card readers and the clearing and settlement system. Amongst the other important aims were, the making of technical standards for cards, card readers and the clearing and settlement system, operational standards for operating smart cards and preparation of a business model for smart card deployment.

The project was started as a pilot project in December, 1998, at IIT, Mumbai campus. The main aim was to practically establish an interoperable system using different products of different technology vendors. Two bank branches, Canara Bank and State Bank of India, in IIT, Mumbai, issued cards to all their savings bank account holders. Card reader machines of different vendors were deployed at merchant establishments in the IIT campus. The pilot project worked very efficiently at the IIT campus.

The preparation of technical standards was carried out simultaneously along with the SMARS pilot project. This was a Herculean task and involved concerted effort by all the partners. The standards were made as open as possible and in order to follow the internationally emerging standards. The members of SMARS team also studied the various experiences of similar experiments in different countries around the world. The aim was to incorporate the best international practices in the formulation of standards for Smart Cards as payment instruments in India. The standards were also prepared keeping in mind the future technological roadmap in Smart Card technology. As a result of the effort, the SMARS team came up with a set of standards, which were forwarded to the Reserve Bank of India for consideration. These technical standards pertained to the use of Smart Cards for a pre-loaded debit functionality. However, the flexibility of loading additional applications like credit card application was possible on the same card.

In addition to the technical specifications, the SMARS team also formulated a business model for implementation and a set of operational guidelines for smart card implementation.

The Reserve Bank of India formed a committee to look into the SMARS recommendations. Based on the recommendations of the committee, the Reserve Bank of India issued operational guidelines for Smart Card deployment in banks on 16th November, 1999. Further, the Reserve Bank of India submitted the technical specifications to the Bureau of Indian Standards for consideration to be adopted as national standards for Smart Cards in the banking and financial sector. The Bureau of Indian Stan dards is now seized of the matter.

Meanwhile, various banks and financial institutions wanted to move ahead and deploy smart cards for payment purposes. Therefore a historic meeting of SMARS was held in May, 2000. It was decided that IDRBT, Hyderabad, would be the single key management agency for the debit functionality for smart card deployment in the country. The set of five common keys were defined jointly by the Reserve Bank of India, IIT, Mumbai and IDRBT, Hyderabad, and kept in the custody of IDRBT, Hyderabad. Further, it was decided that IDRBT, Hyderabad would devise the various policies and procedures in close consultation and coordination with banks, financial institutions, SMARS partners and industry partners.

The set of master keys was released for the first time to IDBI Bank in June, 2000. In furtherance of the mandate given to IDRBT, Hyderabad, a workshop was held at IDRBT, Hyderabad, wherein representatives of banks, SMARS partners and various industry partners were invited. Discussions were held about the policies and procedures to be followed for key management.

Based on the discussions held and after a study of the best international practices in the area of key management, a set of operational policies, guidelines and procedures were formulated by IDRBT, Hyderabad. The SMARS technical specifications, being under the consideration of BIS, are available only for banks and financial institutions that are in the process of implementing Smart Cards as payment instruments in India.

The setting up of a smart cards clearing and settlement system, for settlement of inter bank transactions, is also required once multiple banks start using smart cards with interoperability, for debit functionality (individual banks having the freedom to load multiple applications like credit functionality etc. on the same card), having being induced into the system with the common set of master keys and single key management agency having being already put in place.

There is still much to be done on the smart card payments system front for it to become a vibrant means of retail payment mode in the country.

The need to introduce internationally acclaimed 'best practices' in the Key Management System (KMS) has to be adopted, so that the essential elements of secured transactions such as message integrity, card authenticity, data confidentiality and non-repudiation of transaction are met. The various 'forces that act as barriers to entry' for the setting up of an interoperable Smart Card based payment system can be due to the lax regulatory framework, poor existing infrastructure and limited geographical spread, which has to be minimized during the actual commercialization of the Smart Card.

6.0 Applications of Smart Cards

Typical applications of Smart Cards today include:

- Financial - Payment schemes may include credit, debit, stored value purse, stored token, or mass transit (generally dedicated to a single transport system and typically having low value).
- Telephony - The primary use is the Subscriber Identification Module (SIM) for digital mobile telephones.
- Identification - Various public and private schemes provide identification credentials to participants. These may be government, corporate, university, or other entities. The identification credentials are typically associated with various rights and duties, defined by the identification provider. These can include membership, driver's licenses, benefit access, passports, national identification, etc. Typically, the identification credentials have great value because the credential holder cannot alter them easily, and assets in the credential must be protected against alteration by the cardholder. Digital certificates used in public key systems fit in to this category.
- Secure information storage - Information that is useful and is stored in a secure fashion include health records, health insurance, and other medical information.
- Loyalty - These are programs like the frequent flyer points awarded by airlines. Points are added and deleted from the card memory in accordance with program rules. The total value of these points may be quite high and they must be protected against improper alteration in much the same way that currency value is protected.

- Networked applications - Smart Cards can hold access credentials such as passwords that authenticate a user to a computer network.

Each of these applications may have somewhat differing security requirements, security features, roles, and environmental considerations (e.g., whether they are used always on-line, always used off-line, usually off-line with the capability of going on-line, etc.). The security requirements for the operating software, applications, and the procedures for adding or deleting those applications must therefore clearly be identified and the security functions that are present must be appropriate to the type and intended use of the card.

Applications may range from very simple to very complex. For example, a loyalty application may be no more than an identifying code, such as a hotel or airline frequent user account code. Most of the information (preferences, total points, etc.) is stored on a mainframe computer somewhere; the card is only used to access the account accurately. The application becomes more complex as more of the information and processing is moved from the computer(s) on the network to the card, which may be desired so that activity can take place off line.

Payment applications are often complex, since one of the main reasons for moving from magnetic stripe only uses to Smart Cards permits off line transactions to be conducted more securely.

With the concept of e-Governance emerging as a prime measure for the performance and efficiency of governmental agencies Smart cards and their multifarious applications provide ready solution for a secure, efficient, effective form of governance. There are many potential advantages of e-signatures. A significant amount of time could be saved in complex negotiations by exchanging documents electronically instead of passing physical documents back and forth. Storing documents electronically instead of in paper form could save tremendous amounts of space. Today’s technology presents many options, including credit-card-sized smart cards that can be scanned into a computer through various encryption methods.

Various functions of an e-Government envisage the extensive usage of workflow emails and database applications which in turn can be securely and efficiently implemented with the use of Digital Certificate on Smart cards. For example, digital signatures that use encrypted algorithms, in combination with passwords, can be employed to identify an individual. Public-key infrastructure (PKI) is one such technology. With PKI, both senders and receivers have two "keys," each, one public and one private. Passwords and specialized software encrypt and "lock" the document and signature, and a second set of passwords act as the "key" to open the "lock." PKI technology ensures that a document came from a particular computer.

7.0 Conclusion

In some countries, it is common to demand a toll for using certain roads. In contrast to blanket fees that are paid for stickers, tolls are usage dependent and have usually been paid in cash at tollbooths. A few isolated electronic systems using various types of cards, have been used over the past few years in toll systems. The control stations were installed along with motorway on flyovers and sign bridges as necessary. No modifications to the roadway construction were necessary. The smart cards used did not contain sophisticated e-purse but only very simple and fast debiting commands. Another example of notable mention is of a Smart University where a student at the time of taking an admission is being provided with a Smart Card for multiple purposes in the university, which he can use in the lab, the library, access to swimming pool paying, his hostel/college fees and above all marking his attendance in various classes.

The possible applications for Smart Cards are extremely diverse and are being constantly extended with the increasing arithmetic power and storage capacity of integrated circuits. Smart Cards are not only devices for various applications like, electronic payments, authorization, identification etc., but are in fact, the powerful agents for unshackling the individuality and spontaneity amongst citizens of the 21st century. It will not be long before Smart Cards prove to be catalyst in a society that is changing at a breath-taking pace due to the technological innovations of a gigantic scale never seen before in the history of mankind.

References:

"Smart Card Hand Book", Second Edition, W. Rankl & W. Effing, John Wiley & Sons, Ltd.

Web sites of manufacturers, solution providers, integrators

1. **Advanced Card Systems Ltd., Hong Kong**
   Smart Cards, terminals
   http://www.acs.com/hk/
2. **Aladdin Knowledge Systems Ltd., USA**
   Terminals, software, Smart Cards
   http://www.aks.com/
   http://www.aladdin.de/
3. **American Magnetics, USA**
   terminals
   http://www.magstripe.com/
4. **Amazing Controls Inc., USA**
   Smart Cards, terminals
   http://www.amazingcontrols.com/
5. **American Express, USA**
   card user
   http://www.americanexpress.com/
6. **Ross Anderson's Home Page, Great Britain**
   information about attacks on Smart Cards
   http://www.cl.cam.ac.uk/users/rja14/
7. **Aspects Software Ltd., Scotland**
   software and hardware for testing Smart Card terminals
   http://www.aspects-sw.com/

8. **AU-System Ego AB, Sweden**
   security modules; Smart Cards; personalization equipment
   http://www.ego.ausys.com/
9. **Bull CP8 Smart Card and Terminals, France**
   Smart Cards, terminals
   http://www.cp8.bull.net/
10. **Chaos Computer Club e.V., Germany**
    attacks on Smart Cards; cryptographic algorithms
    http://www.ccc.de/
11. **Dai Nippon Printing Co. Ltd., Japan**
    Smart Card manufacturer
    http://www.dnp.co.jp/
12. **Da La Rue Card Systems, Great Britain**
    Smart Card manufacturer
    http://www.delarue.com/
13. **Giesecke & Devrient GmbH, Germany**
    Smart Cards; operating systems; terminals
    http://www.gdm.de/
    http://gdasia.com/
14. **Gemplus S.C.A., France**
    Smart Cards, operating systems, terminals
    http://www.gemplus.com/
15. **General Information Systems Ltd., Great Britain**
    electronic payments; terminals
    http://www.gis.co.uk/
16. **IBM**
    Smart Card manufacturer; terminals
    http://www.ibm.zurich.ch/
    http://www.chipcard.ibm.com/
    http://www.research.ibm.com/
    http://zurich.ibm.ch/Technology/Security/publications/1995/rap.html/
17. **Javasoft, USA**
    Java, Java for Smart Cards
    http://www.javasoft.com/
18. **Java Card Forum, USA**
    Java, specifications for Java on Smart Cards
    http://www.javacardforum.org/
19. **Java Operating System, USA**
    Java operating system
    http://www.jos.org/
20. **Kaba Holding AG, Germany**
    contactless Smart Cards; Legic
    http://www.kaba.com/
21. **Maosco Ltd., Great Britain**
    Smart Card operating system
    http://www.multos.com/

22. **Microsoft Corporation**
    http://www.microsoft.com/windowsce/smatdcard/
23. **Mondex International Ltd., Great Britain**
    electronic purse, Smart Card operating system
    http://www.mondex.com/
24. **Smart Card Developer Association, USA**
    attacks, software
    http://www.scard.org/
25. **Schlumberger Ltd., France**
    Smart Card manufacturer; terminals; operating systems
    http://www.slb.com/
26. **The Smart Card Club**
    http://www.smartcardclub.co.uk/
27. **The Smart Card Forum**
    http://www.smartcardforum.org/
28. **Visa International**
    http://www.visa.com/openplatform
29. **Verifone Inc., USA**
    terminals
    http://www.verifone.com/