Delhi Business Review ✍ Vol. 3, No. 1, January - June 2002

RE-ENGINEERING EDUCATIONAL INSTITUTIONS THROUGH SMART CARDS

Lavanya Rastogi
Pranabjyoti Das

BACKGROUND

Most of us would agree that Information Technology has been evolving at an amazing pace, giving us more innovations in the past one decade than it did in an entire century before. No aspect of human life today has been left untouched by this revolution.

Personal computers, fax machines, pagers, and cell phones in the hands of millions of people worldwide have led to the evolution of a completely "*Connected or Wired Society*" realizing the metaphor *Vasudhaiv Kutumbakam*. With the advent of wireless internet, smart homes, refrigerators that talk to the internet, pace makers that contact the emergency services in case of a stroke, one can't but opt for the hyperbole to describe these seemingly magical innovations that have left precious little to our imagination.

In a subtler vein however, almost as an ode to Charles Darwin, this journey has not always been a story of evolution. It is replete with instances where the De Novo of yesterdays have failed to find even a fleeting mention in the daily diaries of today. This has increasingly saddled us with generations of hardware and software systems that are completely incompatible with each other. It is almost paradoxical that larger the capital investment required for these systems faster is the obliteration rate. This problem assumes added dimensions for organizations that are preparing for their first serious round of computerization or planning to integrate their hitherto isolated systems. As the average lifetime of a system has shrunk to even lesser than a complete calendar year, scalability and open-endedness for systems has become more important than ever before.

As a part of all computing infrastructure modernization projects, for long developers and system administrators alike have been looking for ways and means to seamlessly integrate the distributed and somewhat disjoint systems that have traditionally existed in organizations. However such systems almost always evolve from one stage to another with most of the development being undertaken by in-house functional experts on diverse range for software and hardware platforms, making data or information exchange between them an uphill task. This literally means that any upgradation or integration will inherently entail redevelopment. Therefore till recently it had been virtually impossible to build coherent, robust, reliable, scalable and effective information systems in such cases.

Much to the relief of all stakeholders, in the recent years certain breakthroughs in the domain traditionally know as IC cards have led to the birth of a truly mobile computing platform known as the SMART CARD, which on one hand allows us to integrate the widely distributed and, hitherto, disjoint systems, making scalability inherent into the information system, and on the other hand it gives us an open window to seamlessly plugin any vendor specific, technology specific, platforms specific addons into the system without necessarily having to modify the existing ones. This not only improves the quality of information sharing between different applications,but in most cases it makes the need for them to be physically on the same network almost redundant, this inturn significantly cuts down networking costs and maintenance overheads.

Introduction

This paper has been written with the aim of introducing the reader to the history and basics of smart cards technology and its potential areas of application with a specific focus to the Re-engineering of educational campuses.

This paper also introduces the reader to **S-Card** A Smart Card based campus card product developed by the SHTR Consulting Group which serves as all in one photo identity card, library card, report card, attendance card, health card, parking lot pass, canteen card etc. along with a brief technical overview of the **S-Card SMART Solutions Framework** for third party applications integration or custom development of S-Card applications. The non-technical readers may want to skip over the Technology Overview section and straightaway move on from Evolution of Smart cards to Applications of Smart cards.

The paper further list 100 possible applications for Smart Campus Card in **Annexure I,** whereas, **Annexure II** carries the list of universities that have already introduced smart cards in their campuses. The paper briefly addresses some common problems of campus computerization and explores how the same may be overcome with the use of Smart Cards.

What is a Smart Card

Imagine the power of a computer, the speed and security of electronic data, and the freedom to carry that information, anywhere, on earth. Imagine a computer so small - it fits inside a plastic card like the credit card you carry in your wallet.

And you imagine the Smart Card

A smart card is a card with a microchip embedded in it. The card is similar in size and shape to a plastic credit card. These cards take the form of either “contact” cards that require a card reader or “contactless” cards which use radio frequency signals to operate. The embedded chip, however, empowers the card to be useful in a variety of environments.

The driving factors of the growing interest in smart cards include the declining cost of smart cards and the growing concern that magnetic stripe cards cannot provide the protections necessary to thwart fraud and security breaches. This security issue alone may propel smart card technology to the forefront of business transactions.

The Evolution of Smart Cards

“First appearance deceives many”, Roy Bright (1988)

A number of parallel trends occurring in computing, microelectronics, cryptography and financial services in the early 1960s acted as the catalysts to the emergence of Smart Cards toward the late sixties and early seventies.

Roy Bright's book (Bright Roy, 1988) gives credit to Arimura in Japan in the beginning of the 1970s and Roland Moreno of France in the period 1973-74 for introduction of smart cards. This is echoed in the paper by Philip le Clech at the Smart Card Europe conference (Moreno Roland and Clech Philippe Le, 1995). However, at the same conference Jurgen Dethloff tabled details of his own work in the late 1960s (Dethloff Jurgen, 1995).

When some leading corporations became involved in a Smart Card project in 1981 they investigated prior patents that had been published. It was found that Ellingboe (Ellingboe Jules K, 1967) had filed a patent application in October 1967 which was abandoned and refiled in 1970. It covered not merely the contact Smart Card essentially as we know it now, but also a contactless card with inductive or capacitive coupling to a reader.

The first cards originated as embossed and magnetic stripe cards suitable for both eyeball reading and magnetic readers. The standard dimensions originated with IATA and led to the ISO standard on magnetic stripe cards for identification. Before very long a wide variety of card shaped products using other technologies than magnetic recording began to appear. In the late 1960s there were products available which contained coded conductor

tracks. Some came from the British company Counting Instruments Ltd of Borehamwood and were utilized by the Post Office and other organizations with large fleets of vans and lorries. The system enabled authorized drivers to collect petrol and other fuel for their vehicles.

> There was also talk from Sweden at this time of cards containing radio-active phosphorus with data recorded as different emissions from the radio activity! Even in those days there was some concern about the radiation hazards, so we no longer hear anymore of this product proposal.

Other trends in the 1960s that helped make Smart Cards feasible were the miniaturization of electronic calculators and the reduction in the size and complexity of integrated circuit semiconductor memory to the point where it was small enough and cheap enough to be incorporated in a bank card.

Having set the scene as a nascent technology the stage was ripe to move from the invention phase to overcome the perceived barriers to introduce true Smart Card products. These barriers were perceived as:

1. Agreement on international standards for Smart Cards

2. Reduced card cost

3. The establishment of competitive advantage over existing and other new card storage media, e.g. optical recording.

IC contact cards, an original French invention, though still pretty much a cutting edge technology have been with us for well over 20 years. Since the 1970s, the history of smart cards has reflected steady advances in chip capabilities and capacity, as well as increases in the number and variety of applications.

Key Milestones in the growth of Smart Cards

1970*	Dr. Kunitaka Arimura of Japan filed the first and only patent on the smart card concept.
1974	Roland Moreno of France filed the original patent for the IC card, later dubbed the “smart card”.
1977	Three commercial manufacturers, Bull CP8, SGS Thomson, and Schlumberger began developing the IC card product.
1979	Motorola developed the first secure single chip microcontroller for use in French banking.
1982	Field testing of serial memory phone cards took place in France—the world’s first major IC card test.
1984	Field trials of ATM bank cards with chips were successfully conducted.
1986	In March, 14,000 cards equipped with the Bull CP8 were distributed to clients of the Bank of Virginia and the Maryland National Bank. Also, 50,000 Casio cards were distributed to clients of the First National Palm Beach Bank and the Mall bank.
1987	First large-scale smart card application implemented in the United States with the U.S. Department of Agriculture’s nationwide Peanut Marketing Card.
1991	First Electronic Benefits Transfer (EBT) smart card project launched for the Wyoming Special Supplemental Nutrition Program for Women, Infants, and Children (WIC).
1992	A nationwide prepaid (electronic purse) card project (DANMONT) was started in Denmark.
1993	Field test of multi-function smart card applications in Rennes, France, where the Telecarte function (for public phones) was enabled in a Smart Bank Card.

** http://egov.gov/smartgov/tutorial/tutorial_text.doc*

1994 Europay, MasterCard, and Visa (EMV) published joint specifications for global microchip-based bank cards (smart cards).

Germany began issuance of 80 million serial memory chip cards as citizen health cards.

1995 Over 3 million digital mobile phone subscribers worldwide begin initiating and billing calls with smart cards.

First of 40,000 multi-functional, multi-technology MARC cards with chips were issued to U.S. Marines in Hawaii.

1996 Over 1.5 million VISACash stored value cards were issued at the Atlanta Olympics. MasterCard and Visa began sponsorship of competing consortia to work on solving the problems of smart card interoperability; two different card solutions were developed: the JavaCard backed by Visa, and the Multi-application Operating System (MULTOS) backed by MasterCard.

1998 In September 1998, the U.S. Government's General Services Administration and the United States Navy joined forces and implemented a nine-application smart card system and card management solution at the Smart Card Technology Center in Washington, DC. The Technology Center's primary purpose is to demonstrate and evaluate the integration of multi-application smart cards with other types of technology, showcasing systems available for use in the Federal Government. Microsoft announced its new Windows smart card operating system.

France began piloting a smart health card for its 50 million citizens.

1999 The U.S. Government's General Services Administration has been involved in the Smart Access Common identity Project for the past year. The Smart Access Common identity Card program will establish a contract vehicle for use by all Federal agencies to acquire a standard, interoperable employee identification card, from one or more vendors, capable of providing both physical and logical (system/network) access to all Federal employees. The United States Government (General Services Administration) began a true multi-application Java card pilot in the Washington, DC, metropolitan area.

2000 onwards Smart cards are used by millions of cardholders worldwide and are at work in more than 90 countries, primarily in Europe and the Far East, processing point-of-sale transactions, managing records, and protecting computers and secure facilities. Another revolution will probably occur when users are able to buy and configure their own cards. That will make the 'universal card' a reality, and it's technically possible today.

Smart Cards and Technological Convergence

In the world around us today we are seeing the convergence of technologies and communications methods: banking services are available over the mobile phone, internet services are available via a host of different media such as digital television, mobile phones and public payphones, and e-purse developments are seeing the integration of transport, retail, parking and other public services. Though this revolution is yet to really take off in India in a big way but with the pilot projects of similar type succeeding, on all accounts, the reverse counting has already begun.

Smart cards have already been accepted as the most portable and secure system. With the introduction of biometrics and additional cryptographic capabilities to ensure even higher levels of security, individuals can carry their own personalized digital identity around with them

"The 21st century will usher in the digital age and smart cards will provide the key to access its benefits" says Olivier Piou. "The way that commerce has functioned for the last two millennia, via face-to-face contact, written signatures, handshakes and cash, will be fundamentally changed with electronic transactions. Smart cards are the solution and in the next twenty years every person on the planet will use the technology." *(Press Release, "Smart Cards Maketh Digital Man", 1999)*

Smart cards maketh digital man – Enter your smart card into your mobile phone, banking terminal or computer, present it to your doctor or at the airport security counter, and it will enable secure access to all the appropriate information in order to allow you to communicate, execute financial transactions, be reimbursed for medical expenses and travel freely.

All these developments require a single portable identity system that can easily and securely recognize the individual user of the service. For example hypothetically speaking why can we not have the same card as our Voter identity card, Ration Card, Driving License, Passport, Birth and Marriage Certificates, Health Card, and all the while using the same as our Credit Card, Debit Card, prepaid calling card and even the Cell phone SIM cards.

So no discussion about convergence can ever be complete without Smart Cards finding a mention. One basic reason for the same is that before we can talk about the higher order convergence of technologies we must first address the question at the grassroot level of applications, processes and access points, for which the most viable medium currently seems to be that of smart cards. Smart Cards are no longer *De Novo* but the De Corsica of modern lifestyles, for all developing societies there may soon be no choice but to embrace the same as they cross the line from being a necessity today to a criticality in the foreseeable future.

Future of the Smart Cards: The Indian Perspective

The industry analysts and the specialized press forecast a brilliant future for the smart cards in India with Millions of cards predicted to be circulating in a few years. There are several reasons for the same, some of them may be summarized as, hereunder:

- In India the government usage of smart cards for health care, voter identity, ration, driver's license and other similar programs will be a decisive factor in expanding the smart card market. Owing to the large population any of the above may turn out to be the killer application for smart cards. This may just turn out to be a killer application for smart card in India but is bound to have long gestation period.
- India has a large student population and most of the Universities in India have not yet woken up to the call of computerization, this puts Indian Universities in the unique position to be able to leverage Smart Card enabled campus information systems to their maximum potential.
- Other high growth areas could be, access control applications and the telecommunication industry which is slated to be a high growth domain for the next few years.
- Since the credit card industry is still in its nascent stage in India it may well turn out to be a major driver for cutting edge technology adoption in this sector.

Driving License Project in Gujrat, India *(Panel on Security of the Legislative Council ,2001)*

The smart card will store the driver's fingerprint as well as demographic information. An estimated 10 million licenses will be issued. The cards will be read by traffic police at mobile terminals, which will read and verify personal details and previous offences. Fresh traffic offences will be written direct to the cards. Details of on-the-road transactions will be uploaded to terminals at police stations.

Smart Card Technology: An Overview

There are three main categories of smart card technologies: contact, contact less, and hybrid smart cards — also known as combination cards.

Contact Cards

A contact card has a gold chip embedded in the card; the dimensions and location of the chip are standard and are defined in ISO 7816-2. This kind of card requires insertion into a smart card reader and a direct connection with the physical contact points on the card to transmit data. Contact cards are used frequently in banking, communications, and loyalty programs.

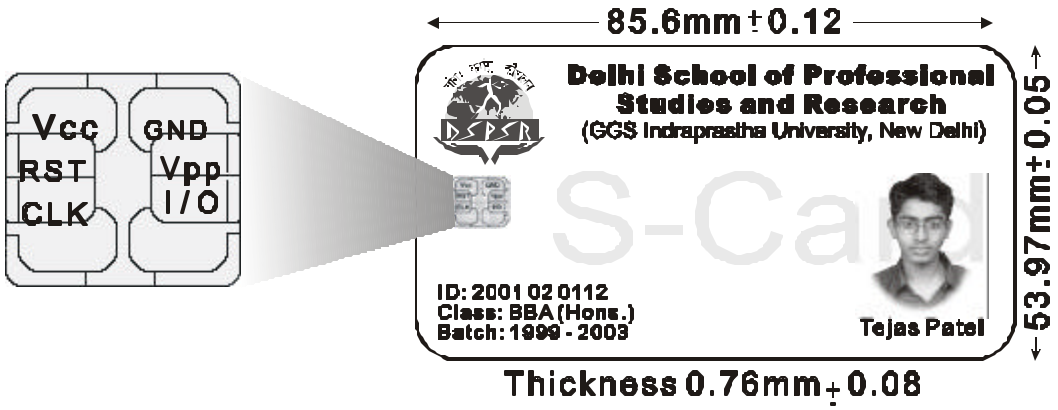

Figure 1: ISO 7816-2 Dimensions and Contact Locations

Contactless Cards

Although the reliability of smart cards is much higher than magnetic stripe cards, careless handling and very frequent use can take its toll on the gold contact surface, leading to eventual failure of the chip contacts. Contactless cards manage to avoid this pitfall, as they do not require insertion into a card reader and can work up to several centimeters away from the reading device. Contactless cards are ideal for people who are moving in vehicles or on foot. It would be ideal to wave at scanning machines collecting payment for motorway tolls, on buses or at train stations, for parking, admission fees or ferry crossings.

Hybrid Cards

There is some overlap where different card types are implemented in one card leading to the so-called hybrid cards. A smart card can also have a magnetic stripe and this can provide a convenient path for migration. But the term hybrid card generally refers to cards that have both a contact and a contactless interface. The contact interface is used by the microprocessor chip module and the contactless interface is used by the memory chip module. There is no physical connection between the two chips and therefore no shared memory is available.

Combi Cards/Dual Interface Cards

Combi cards also have a contact and contactless surface but the two interfaces are connected and have access to one shared data area via a microprocessor or logic module. The contact surface is always controlled by a microprocessor. The shared data area may be controlled by a microprocessor or a logic module.

The disadvantage of a contactless/combi card over a contact card is the increased cost required to implement the antenna into the plastic card, and more expensive readers that need to have radio frequency (RF) transmitter/receivers. Combi card performance is likely to be slower than a contactless card because the RF unit has to get the data via the CPU. Another disadvantage with this type of card is that communication can be interrupted by removing the card from the RF field, or it can be possibly traced or disturbed.

Optical Cards

Optical memory cards are for applications where a very large amount of storage capacity is required. It can store for instance X-ray images of a patient. These cards usually have a microprocessor chip embedded and use the smart card security to protect the optical data from unauthorized access.

The optical card provides some megabytes of write-once/read-many (WORM) storage. Data can be read by appropriate devices and is not protected, unless it is encrypted.

The Application Capability of SMART CARDS

At the application capability level the smart cards fall into two categories: memory and microprocessor.

Memory Cards

Memory cards communicate through a process that is controlled by the terminal. This type of card primarily stores information, access control, or a value that can be "spent." These cards can hold from 103 to 16,000 bits of data. They are considerably less expensive than microcontroller cards. But, memory cards also offer minimum security to the consumer, making them ideal for use in low- to medium-security applications. Memory cards can be divided into two categories.

The first type of memory card is the *Storage-Only Memory Card*. This type of card has rewriteable memory. It is often used in loyalty applications to store a buyer profile. The buyer earns points as they spend money and these points are later redeemed for various rewards.

The second kind of memory card is the *Memory Card with Register*. This card starts with a set value that decreases with use. It is not rewriteable; once the value is exhausted, the card is discarded. The most common applications for the Memory Card with Register are prepaid telephone and vending cards

Microprocessor Cards

A microprocessor card is truly "smart." It contains a microprocessor chip that can add and delete information. This type of smart card is basically a miniature computer. The microprocessor card has an input/output port, an operating system, a security structure, and a hard disk. Microprocessor chips come in 8-bit, 16-bit, and 32-bit formats with data storage capacities ranging from 300 to 32,000 bytes.

Microprocessor cards offer a high degree of security to the user, offering the ability to verify the cardholder; a PIN (or other secret code) is entered a for verification. Banking, identification, healthcare, and other industries that require high security are currently utilizing microprocessor cards.

Smart Card Standards

Standards are key to ensuring interoperability and compatibility in an environment of multiple card and terminal vendors. Integrated circuit card standards have been underway since the early 1980's on both national and international levels.

Standardization efforts for SMART CARDS

Standards are key to ensuring interoperability and compatibility in an environment of multiple card and terminal vendors. Integrated circuit card standards have been underway since the early 1980's on both national and international levels.

There are many standards, specifications and recommendations for smart cards. Some of them come from recognized international bodies such as ISO. Some come from industry organizations such as financial institutions; some come from companies that want their products set the norms; some are de facto standards.

The standards can be categorized in the following groups based on the standard organizations:

- The International Organization for Standardization (ISO) standards: eg. ISO 7816 Parts 1-8: contact integrated circuit (IC) cards.
- The country and/or industry standards. Some of them are not smart card standards, but are used by applications running in smart cards.eg ANSI (US Standard body) X9 series: for digital signature, secure hash, RSA, and data encryption algorithms.
- There are many standards, specifications and recommendations for smart cards. Some of them come from recognized international bodies such as ISO. Some come from industry organizations such as financial institutions; some come from companies that want their products set the norms; some are de facto standards.

Major Application areas

A logical extrapolation useful to organizations considering the incorporation of smart card technology into their operations may best be defined as:

If

- A portable record of one or more applications is necessary or desirable.
- The records are likely to require updating over time.
- The records will interface with more than one automated system.
- Security and confidentiality of the records are important.

Then

The smart card is a feasible automation solution for making data processing and data transfer more efficient and secure.

Else

The only other option is expensive and difficult to maintain Computer Networks and Real time systems.

Where they are being used today ?

Financial Applications

- Electronic Purse to replace coins for small purchases in vending machines and over-the-counter transactions.
- Credit and/or Debit Accounts, replicating what is currently on the magnetic stripe bank card, but in a more secure environment.
- Securing payment across the internet as part of Electronic Commerce.

Communications Applications

The secure initiation of calls and identification of caller (for billing purposes) on any Global System for Mobile Communications (GSM) phone.

Government Programs

- Electronic Benefits Transfer using smart cards to carry Food Stamp and WIC food benefits in lieu of paper coupons and vouchers.
- Agricultural producer smart marketing card to track quotas.

Information Security

- Employee access card with secured passwords and the potential to employ biometrics to protect access to computer systems.

Physical Access

- Employee access card with secured identity and the potential to employ biometrics to protect physical access to facilities.

Transportation

- Driving Licenses.
- Mass Transit Fare Collection Systems.
- Electronic Toll Collection Systems.

Retail and Loyalty

- Consumer reward/redemption tracking on a smart loyalty card, that is marketed to specific consumer profiles and linked to one or more specific retailers serving that profile set.

Health Card

- Consumer health card containing insurance eligibility and emergency medical data.

University Identification

All-purpose student identity card, containing a variety of applications such as electronic purse (for vending and laundry machines), examination card, fee card, health card, attendance card, library card, and meal card.

German Health Card*: A Case Study

These Cards mostly contain administrative data, insurance related data, past and current medication, and disease specific data set, as well as, data related to specific devices related to the disease. Data contained in small RAM, and every health professional can access it (hence security issues was not maintained).

Later, a statutory Health Insurance Card HIC, was introduced to all 16 German states, over 80 million of 256 Byte RAM card was issued. Health Professional Card (HPC) introduced as a means for authenticating access to the various patients cards e.g. in BayerCard (for pregnant women), Quasi-Niere (as quality assurance for patients with chronic kidney disease). BayerCard used 4Mbyte laser field on the reverse side of the card for the storage and transmission of original baseline medical data, in addition to administrative data and information about the gravidity together with actual ultrasound pictures and emergency related data. However this was not very successful since reading and writing the laser portion was too expensive to place in the necessary user settings.

In December 1999, an Electronic Physicians identity became the first health professional card in Germany with an application neutral design adaptable to most other professions in the German health community. The basic functions of this identification chip card are generic and not specific to any certain application or profession. This card functions as: visual identity i.e. general proof of identity (e.g. name, picture); digital identity i.e. base certificate identifies the holder's name electronically (including digitized picture), signed by the issuing Medical Association; and three private keys (PIN protected), each with different functions:

- for client/server authentication towards a medical application system using encryption
- for transport encryption using a hybrid symmetric/asymmetric encoding scheme
- for generation of personal electronic signature.

**Karweni Titis, 2001*

Why Smart Cards*

The reasons why smart cards are destined to become a part of our life are many. Here are just a few obvious arguments:

- They offer a quick, easy and personal way to verify the identity of a user.
- They are more secure and durable than magnetic stripe cards and more difficult to tamper with than bar code cards.
- They can store more data and physically separate the data into a multipartition file system, so that many applications can safely run on a single card.
- They can control who has access to files on the card as well as in a computer network.

- They can carry unlimited monetary value. The electronic manipulation of the card can add or subtract value.
- They can store biometrics for complete security.
- They can be designed with their own levels of cryptographic algorithms.
- They offer the flexibility of inexpensive read-only capabilities to the elaborate mini-laptop re-programmability of a chip.
- They can accommodate and upgrade all current technologies in piggy back fashion instead of replacing the standard 39 bar code or the three-track, high energy stripe systems.
- They can carry a photo, text, mag stripe, bar code and embedded computer chip all on one standard-sized card.

* http://www.identicard.com/ididеas/smartcardart.htm

Smart Card Applications for Educational Campuses: A Case in Perspective -

Managing the optimal utilization of campus resources has always been a challenge for administrators but this is extra true in case of technological resources because of their high cost of acquisition and commissioning coupled with very fast obsolescence rate. This has achieved, hitherto, unheard of dimensions as the resource pool has extended and evolved beyond merely computers terminals and printers in the yesteryears to more recently the public labs, internet access, document management on the campus intranet, electronic learning resources, ATMs and personnel access points for all faculty and students in the modern day. Also with breakthroughs taking place at an unprecedented pace in the areas of wireless networks and mobile computing these resources are no longer limited to the controlled environs of computer labs but are rather scattered and distributed as far and wide as the campuses extend and more often than not the world beyond. Furthermore these diverse and distributed resources, increasing enrollment, and decreasing funding all in the same package contribute to the resource management challenge.

Today, campuses no longer have the choice of shutting their eyes on the technological revolutions taking place all around them. They must fast adapt to these changes and embrace the new technologies with anticipation, learning to harness them to maximum potential, because even the last of the optimists will accede that these are no longer only technological marvels to be showcased and admired but innovation that add a lot beyond the wow value, delivering key functionalities and enabling services that make life easier for the administrators, faculty and students alike.

One of the proactive way how the campuses can build in scalability into their on campus technology initiatives and investments is with a smart card enabled campus, a group of applications seamlessly integrated and significantly facilitating campus automation and resource management.

Current Scenario

Traditionally on campus the students are required to carry a number of cards. Most of these cards are required for authorizations and identification purposes owing its roots in the policies of the administration. They not only lead to an over head of the student and the administration having to keep track of all of them but it's a challenge in itself to manage the validity of the same.

Also as the level of computerization in the campus increases these cards are either produced after repeated data punching into independent systems or will need to interface with various computers systems operationally adding only confusion value.

As long as they continue to be run of the mill paper or plastic cards they make no value addition to the computerization initiative. If replaced by magnetic swipe cards they are a greater menace as they have proprietary applications running the systems that they interface with. This on one hand compounds the

problem of issuing and life cycle tracking. On the other hand this neither reduces the number of cards a student has to carry nor does it ease the complexity of the computerization. However, what it ensures is a significant vendor lock in and huge migration costs for these systems. Also for these disjoint systems to come anywhere close to working with each other, one needs huge investments in campus wide networks, which in itself, is not in any way bereft of maintenance woes.

This forces us to wonder - Is there any SMART way of achieving end-to-end campus computerization all the while ensuring scalability, security and economy ?

Implementing S-Card – Campus Re-engineering the SMART Way

Common Problems in Campus Computerization

"Problems arise from management of Information Systems built from disjoint systems of ever increasing complexities. All Information systems therefore with time degrade into merely record keeping systems. This adversely effects both the Quality of software systems as well as efficient administration and record keeping"

In the absence of a campus wide network, highly fragmented and disjoint applications emerge as the information system. This leads to duplication of information and, whenever, a part of the information on one system is needed by another system, data inconsistency problems have more often than not been seen.

This problem of data redundancy and inconsistency can be done away with the use of smart card to integrate all the disjoint systems. This ensures an open and SCALABLE solution rather than the literally and figuratively a STRETCHED solution via the campus area network.

BPR and Smart Cards

"Don't Blindly automate - obliterate" – Hammer and Champy (1993)

Most people often confuse computerization with blind automation. No computerization initiative can ever be successful if it involves only a blind automation of existing processes, because if the processes being followed currently are inefficient and making a mess, then if we undertake mere blind automation then in effect what we are doing is simply replacing human hand with the power of the microprocessor allowing us to make more mess and at a faster pace. Should we then be surprised if soon we find only mess all around?

Therefore, before an organization jumps headlong into deploying a plethora of software applications it must realize that computerization can be used only as a tool to help in transformation of organizations from being traditionally closed systems into truly world class. This shall in effect involve a complete rediscovery of the atman (soul) of the organization. The rediscovery may involve the need to consciously undertake the exercise of introducing a Quality Management System to help the organization rethink, re-discover, re-invent and re-engineer their processes. A model has been developed by SCG (Singh et.al., 2000) after conducting an international survey by creating a resource site on the internet for 12 months from September 1998 to August 1999 based on structured questionnaire on 696 managers from India, USA, China, Russia, Ukraine, Canada, Australia, Japan, Brazil, West Indies and Nigeria. The model (*The Wheel of Transformation*) provides a detailed guideline for transforming the organizations towards world class.

The SMART solutionsframework ensures that each placation can be understood as a part of a big system that uses smart card for both transferring the data and also enable remote and mobile computing. In addition to the same, it also helps in obliterating the redundancies of workflow increasing both efficiency and effectiveness of the systems.

The S-Card helps in creating a convenient environment for students and staff – by developing a suite of automated, cost-saving efficient applications for schools, colleges or universities.

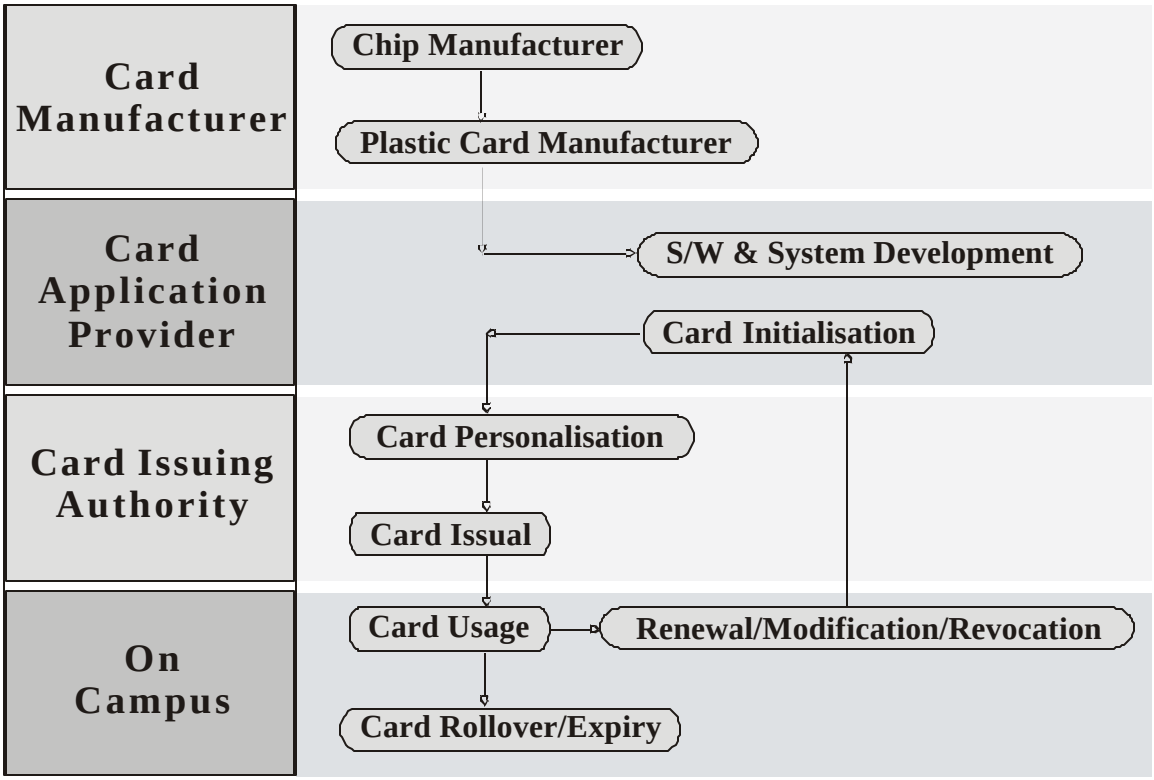

Figure 2: S-Card Life Cycle: An Overview

Instead of carrying many cards on the campus one can carry a single multi-application smart card, which serves better as a bearer of all the information of a student.

With a single identity card, cardholders can identify themselves, check out books, buy food, attend sports activities and access services and facilities across campus.

One card does it all !

Objectives:
The objectives of the S-Card program are to:

- Make access to campus services more convenient for the students, faculty, staff, and campus visitors;
- Increase administrative efficiency;
- Provide building access that will enhance safety and security.

Component of S-Card Smart Solution Framework
1. Smart Cards

2. Card Readers

3. Software Systems

Basic S-Card Applications for Educational Campuses
The Smart Campus Card may be planned to eventually integrate with or replace all existing campus identity and other card applications like photo identity card, attendance card, library card, health card,

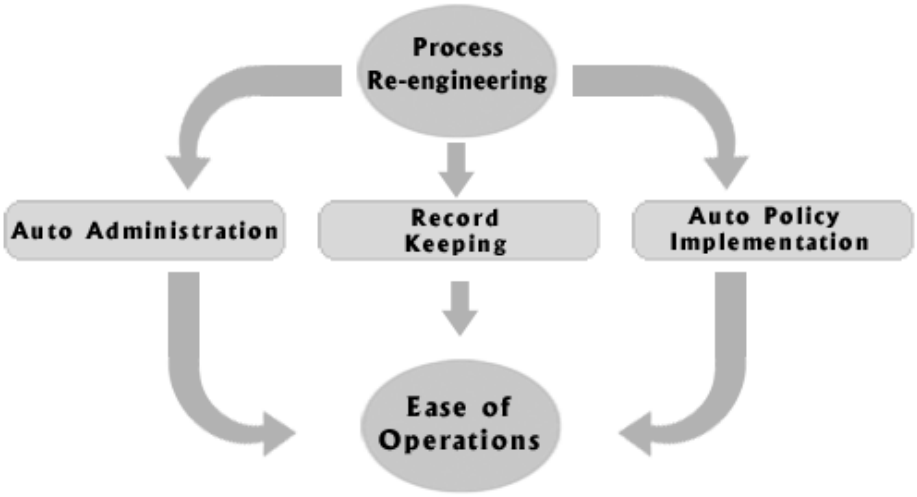

Figure 3: S-Card Smart Solutions Framework – A Conceptual Overview

Administration	***End User***
Process Acceptance	User Delight
Efficiency	Loyalty
Cost Saving	Brand Building

academic record card, fee record card, canteen card, access card (physical access, computer access, network access etc.), temporary debit card (stationary store, cloths store, tuck shop etc.), an affiliate card for alumni, parents of students, etc.

The card may access any off the following computer database and transaction processing systems:

- ✍ Photo identification and Access control systems
- ✍ Human Resource System (Employee Database System)
- ✍ Student Information System (SIS)
- ✍ Library Information System
- ✍ Point of Sale (POS) system and
- ✍ The Student Billing and Receivables System for payment of small balances.

S-Card Security Features

Security may be built into a smart card enable system at various levels

- ✍ Human-readable security features
- ✍ At the Application Level
- ✍ Network
- ✍ Operating System
- ✍ Smart Card Chip

Human-readable security features

There is often a need to include human-readable security identifiers on smart cards; these features try to prevent smart card falsification. These features, of course, do not protect the data in the card. They prevent the misuse of the card as a badge identificator.

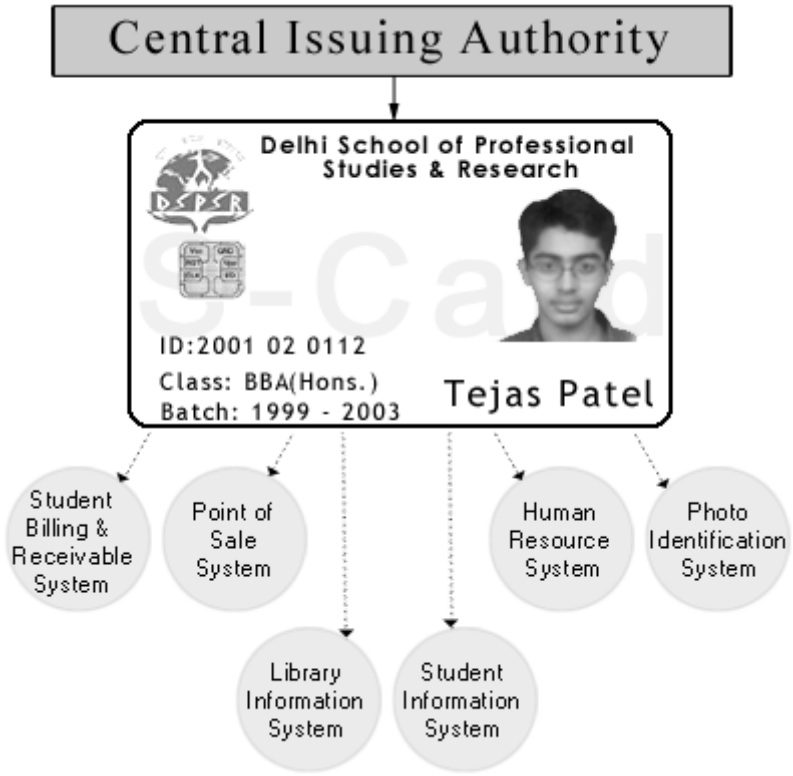

Figure 4: S-Card Smart Solution Framework – The Application Integration Perspective

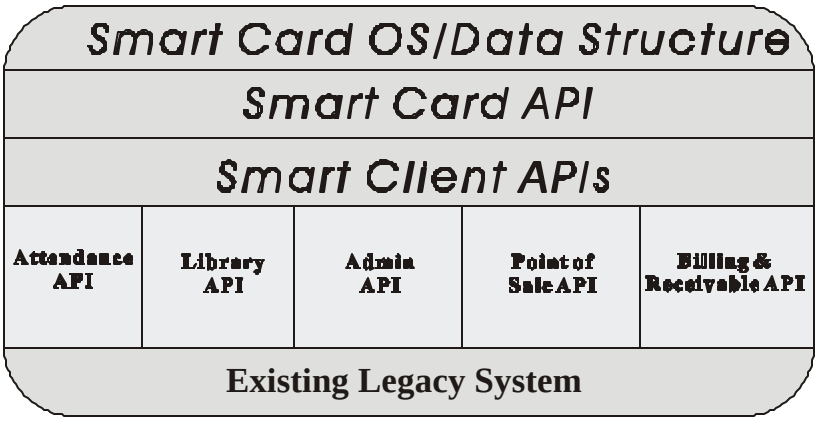

Figure 5: S-Card Smart Solution Framework – A Technical Overview

Photo lamination : The smart card is personalized when issued to the cardholder with a passport-sized photograph of the cardholder. The photo would be laminated to the card. The security is embodied in the procedure followed before the photo is laminated. The cardholder must present the photo in person to a certified representative so that the cardholder's identity can be confirmed before the smart card is issued.

Signature strip : This is a very familiar feature on credit cards. A signature strip is bonded onto the card at manufacture. The cardholder must sign the strip using indelible ink when the smart card is issued. The signature cannot be modified nor the strip be replaced, without being obvious to the naked eye.

Holograms : This is another common feature found on credit cards. The holograms are bonded to the card

Florida State University, Multi application student card for on and off campus services (http://www.gemplus.com/app/closedsys/cybermark.htm)

In 1997, CyberMark, high education card systems specialist, acquired the FSU program (started 94) and took the responsibility for the management of the existing card system and its evolutions. CyberMark is more specifically focus on developing and enhancing the chip card applications.

- **Personalization and subscription:** The personalization and issuance of the card is done in less than 2 minutes with the photo directly taken at Florida State. The card contains a color ID picture of the bearer, his/her signature, personal information and university status.
- **Identification:** The magnetic card is used for nearly every identification on campus.
- **Access control:** Each time a student enters a restricted area where he has to be identified, his card is a " key " to that service. It is used for dormitories, classrooms, buildings and administrative offices, computer labs, university libraries.
- **Library:** The card contains the book borrowing rights and they can be checked on-line any time it is needed.

Financial transactions:

- **Personal account:** Agreement between FSU and a partner banking institution: Suntrust. Every student has the opportunity to open a personal account at Suntrust bank.
- **Withdraw from ATMs:** possibility to make a deposit, withdraw money, or obtain information from Automated Teller Machines on campus, around town and even worldwide (Cirrus).
- **Payments:** Possible use to purchase a variety of goods and services at both on and off campus locations to: buy books, meals, supplies, merchandise, personal computers, pay university related fees, pay housing... and more.
- **Tuition fees:** Automatic debit from FSUCard account to pay tuition fees.
- **Electronic purses:** The chip contains several distinct e-purses, among them some are limited to specific goods like books and meals.
- **Pre-paid value:** Pre-paid value is stored in the chip for small purchases such as beverages and snacks at vending machines, photocopies, laundry, and laser printing around the campus.
- **Associated merchants and loyalty program:** Many merchants, both on and off campus, participate to the program. The cardholder can purchase goods and services under US$ 100, and accumulate points to be redeemed in other merchandises and discounts.
- **Internet & secure access to University records:** Through an encrypted internet session, the student may access personal university data such as transcripts, course schedules, and other research materials from any computer with its personal FSUCard.
- **Telecommunications:** Local and long-distance calls from on-campus payphones.
- **Voice messaging:** The university's official means of communicating with its students via the telephone.

by manufacturer and cannot be separated from the card without destroying the substrate. The security feature of the hologram is based on:

- The difficulty in reproducing the hologram
- The limited number of firms who can manufacture the hologram itself

Microprinting This feature is ultra-fine printing that appears as a line to the naked eye but is visible under magnification. The printing itself is difficult to reproduce.

Embossing : This is another familiar feature of credit cards. The card number is pressed into the card, sometimes over the hologram for additional security, so that the numbers are raised above the surface of the card. An impression of the number can be transferred to paper using a machine.

Security patterns : It is the printing of very fine, interwoven lines onto the card substrate. This is a typical security feature on paper currency. The security feature is similar to holograms; they are difficult to reproduce and only a limited number of companies can perform this procedure.

Laser gravure : Using a laser, it is possible to burn images into the card substrate. The burning is indelible because it can be done when the smart card is issued to the cardholder

Biometrics – The Emerging Dimension

Biometrics is the science and technology of measuring human biological features to unambiguously identify an individual within a group of people.

Some of the biological features that are both unique to an individual and that can be measured are:

- Signature
- Fingerprint
- Voiceprint
- Hand geometry
- Eye retina
- Facial recognition

At the Application Level

This security feature is absolutely dependent on the application developer. One can apply any encryption level of data.

Security Features of the Network

The system design should take into account the accessibility of data in transit and protect it accordingly or design the transport protocol such that tampering will not affect the overall system security.

Modern card terminals are just a part of a larger, more complex network of communications links between computers. These communications links must be physically protected from tampering if data integrity is to be maintained. The smart card reader and any communications links can be physically protected by placing them in a secured environment where personnel or monitoring equipment continuously observe the use of the smart card reader and prevent tampering.

Security Features of the Card Operating System

One of the enormous strengths of smart cards is the card operating system. All memory accesses must flow through the CPU so the design of the card operating system is critical for implementing security at a logical level. The logical organization of the dedicated files in EEPROM memory forms a security barrier.

Security Features of the Smart Card Chip

It is necessary during production for the smart card chip to test the microcircuit. After the chip has been tested, the chip must be irreversibly converted to a mode where it is impossible to access the internal chip circuit.

Smart cards have circuits to detect external tampering with the chip. There are circuits to detect too high or too low supply voltage, as well as, external clock frequency or sometimes too low an operating temperature.

To prevent electrical signals emitted by the memory cells from being monitored externally, the area of the chip around the EEPROM is coated in a metal shield. Removing this shield will destroy the chip and it will no longer function. The chip is also coated with a passivation layer to stop ultraviolet light from erasing the memory on the chip.

The Road Ahead

"The woods are lovely, dark and deep; But I have promises to keep,
And miles to go before I sleep; And miles to go before I sleep"

– Frost Robert, 1923

The smart card programs around the world are growing fast. More and more applications are being handled by smart cards. There is a progressive shift from the magnetic stripe to the chip. Despite problems ahead the following quote seems to capture the spirit of it all *"When all the dust is settled, it is expected that smart cards will be accepted and as ubiquitous as magnetic stripe cards are today, but with vastly greater capabilities" (Seidman, 1996).*

Smart cards are poised to go well beyond the typical applications of identity verification, security access, authentication for network security, loyalty programs and transactions such as on-line banking with debit and credit features, but all this will not happen on its own as the late Carl Sagan observed several years ago, *"We live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology."*

Consequently, a continuous awareness program and discussion is necessary to properly investigate all the possibilities that a smart card program for campuses can deliver. This will of course require an ongoing investment of time, effort and resources by the campuses opting for a card program, but as Derek Bok said, "If you think education is expensive, try ignorance."

Smart Card Initiative at SHTR Consulting Group:

The team at SHTR Consulting Group has set up an applications and technology incubation center to develop cutting edge smart card applications headed by the first author, (www.shtrconsulting.com/S-Card/) which is also actively engaged in research, on campus card applications for educational institutions in the country. A pilot project for the same is already being rolled out at Delhi School of Professional Studies and Research, affiliated to GGSIP University, New Delhi, D.CIT, accredited to DOEACC, Ministery of Information Technology, Government of India and DSEL affiliated to Karnataka State Open University and INDELTA under the stewardship of the second author and soon to follow suit is an internationally renowned school.

SCG proposes to conduct a series of training programs for the universities and other educational institutions to help create an awareness about campus computerization, this shall all related aspects like Internet and Broadband for educational institutions, re-engineering of capmus using smart cards, e-learning and virtual class rooms, developing Quality Management Systems for educational Institutions using ISO 9000, Security on Campus Area Networks, etc., One such program is scheduled to be organized in the first week of February, 2002 at New Delhi. The calender of training programs of SCG is available at www.shtr.org/edp/edp2002.html.

SCG is currently also developing a suite of software products (in a limited sense like an ERP for educational institutions) that will enable integration of all systems on the campus possible, making the seeming distant dream of a SMART CAMPUS a reality.

Reference

Bright, Roy (1988) "Smart Cards Principles, Practice, Applications", Published by LS Horward Books, Chichester, ISBN 0 7458 0374 1.

Dethloff, Jurgen "Intellectual Property Rights and Smart Card Patents" by Smart Card Europe, London, 12 December.

Ellingboe, Jules K. (1967)"Active Electrical Card Device", (TRW Inc.), US Patent 3637994, first filed as continuation in part of an application of 29.10.67 (abandoned).

Experience of Using Smart Identity Cards in Other Countries, Panel on Security of the Legislative Council, 2001 (http://www.legco.gov.hk/yr00-01/english/panels/se/papers/b695e01.pdf)

http://www.gemplus.com/app/closedsys/cybermark.htm

Hammer, M. and J. Champy, (1993) Reengineering the Corporation, London: Nicholas Brearley Publishing.

NACCU, October 31, 2001 (http://www.naccu.org/memlinks.htm)

Moreno, Roland and Clech, Philippe Le (1995) "IPR and Smart Card Patents – France", (Innovatron), Smart Card Europe, London, 12 December.

Press Release (1999) "Smart Cards Maketh Digital Man", (www.1.slb.com/smartcards/news/pr99/first/sct_20anniv0623.html)

http://www.identicard.com/ididеas/smartcardart.htm

http://egov.gov/smartgov/tutorial/tutorial_text.doc

Robert Huber Associates (2001) (http://www.allcampuscard.com/potential.htm)

Seidman, S. (1996) Emerging markets, persistent problems: Smart cards have come a long way, but still have a long way to go, Report on Smart Cards, December.

Singh, Ajay Kr., Maheshwari, Suneel, Rastogi Lavanaya and Chatterjee, Kumardev (2000) The Wheel of Transformation: A Model for Developing World Class Organizations, Delhi Business Review, Vol.1, No.1, p.1-11.

Titis, Karweni (2001) Authentication Techniques & Some Case Studies, (http://www.nhsia.nhs.uk/erdip/archive/erd_030401/dg5_030401.pdf.)

Bibliography

Cordonnier & Cordoonier, V. and Watson, A. (1996) The concept of suspicion: A new security tool.

Daview, D.W. "Cryptography and the Smart Card", Chapter 8 of Reference 1.

Dinnissen, Paul (1995)"Electronic Cash – What is it and What it Means", DigiCash bv, Smart Card'95, London, Feb. p.14-16.

Everett, David (1994) Smart Card Tutorial "Contactless Cards", Smart Cards News, Sept., p.175-178.

George, H. Martin (1995) "A New Strategy for Low Power, High Discrimination Voice Biometrics", Domain Dynamics, Smart Card'95, London, Feb.,14-16.

(1996) "Guglielmo Marconi and Early Systems of Wireless Communication" by R W Simons (formerly of Marconi Radar Systems), GEC Review, Vol. 11, No. 1, p.37-55.

http://www.1.slb.com/smartcards/news/pr99/first/sct_20anniv0623.html

http://www.fargo.com/ID_Info_Center/white_pages_pdf/SMART.PDF

http://www.smartcard.co.uk/articles/cardstokens.html

http://www.datacard.com/solutions_for/schools/school_integrated_campus.shtm

http://home.hkstar.com/~alanchan/papers/multiApplicationSmartCard/

Hawkes, Peter, Some Aspects of the History of Smart Cards and Tokens - Ancient and Modern, BTG Limited.

Hawkes, P., Davies, D. and Price, W. (1990) "Integrated Circuit Cards, Tags and Tokens", BSP Professional Books, London.

Hawkes, P. (1996) "Contactless Integrated Circuit Cards, and Radio Frequency Identification Tags - An Introduction", BTG, Smart Card'96, London, Feb., p.12-15.

Heggenbath, M. (1995) "Overview of IC Cards Standards", CardTech'95, Washington D.C., Apr., p.10-13.

Higgs, M. (1995) "The Case for the Contactless Card" by M Higgs (AES Prodata UK Ltd), Smart Card Europe, London, Dec., p.12-13.

Koo, Roland (1994)"ASIC's for Chip Cards", Mikron, Smart Card '94, London, 15-17 February.

Koo, Roland (1995) "Contactless Smart Cards in Public Transit Installations", Mikron, CardTech'95, Washington D.C., Apr., p.10-13.

Kreft, H.D. (1995) "Latest Developments on the Card Scene", ADE, Smart Card Europe, London, Dec., p.12-13.

Lessin, Arlen (1995) "A US Pioneer's snapshot views of the early years through today", Smart Card International Inc., Smart Card Europe, London, 12 December.

Looi, M.H. (1995) Authentication for applications in computer network environments using intelligent tokens, School of Data Communications. Queensland University of Technology.

Matilla, P. (1992) Setec Oy Supplying Multiservice Application and Medical Trial, Report on Smart Card, April 1992, p.7.

Morgan, Gwyn (1991) "Smart Cards for Subscription Television Videocrypt - A Secure Solution", (News Datacom International Ltd), Smart Card '91, London, Feb. p.12-14.

Price, W.L. and Chorley, B.J. "Secure Transactions with an Intelligent Token", Chapter 6 of Reference 1.

Smart Card Tutorial (1995) "Review of Contactless Cards", Smart Card News, June, p.105-109.

(1998) Smart Cards: A Case Study, International Technical Support Organization, October, IBML (http://www.redbooks.ibm.com)

Stanford C.J. (1995) "Contactless Card Standards are Here", CJS Consultants, Smart Card'95, London, February, p.83-89 of Technology and Markets Volume.

Ugon, Michel (1995) "The Future of Smart Card Operating Systems", Bull CP8, Smart Card'95, London, Feb., p.14-16.

Ugon, Michel (1995) "Security in Cash Card Systems", (CP8 Transac), CardTech '95, Washington D.C., Apr., p.10-13.

Annexure I

Potential Campus Card Applications (Robert Huber Associates, 2001)

1. Admissions Office
2. Airport
3. Alumni Office
4. Amusement Area (Contracted)
5. Amusement Area (Self-Operated)
6. Arena (Contracted)
7. Arena (Self-Operated)
8. Athletic Complex
9. Athletics Office
10. Bakery
11. Bank
12. Barber Shop
13. Beauty Salon
14. Beverage Machines
15. Billiards Center
16. Bookstore (Contracted)
17. Bookstore (Self-Operated)
18. Bowling Center
19. Bursar's Office
20. Business Office
21. Cable TV Station
22. Campus Safety Office
23. Candy Shop
24. Card Shop
25. Cinema
26. Computer Center
27. Computer Labs
28. Computer Repair Shop
29. Computer Store
30. Concessions (Food)
31. Concessions (Novelty)
32. Conferences (Business)
33. Conferences (Summer)
34. Continuing Education Office
35. Convenience Store
36. Convocation Center
37. Cookie Stand
38. Copiers
39. Copy Center (Contracted)
40. Copy Center (Self-Operated)
41. Day Care Center (Contracted)
42. Day Care Center (Self-Operated)
43. Deli
44. Donut Shop
45. Equestrian Center
46. Financial Aid Office
47. Florist
48. Food Mall
49. Food Service (Board)
50. Food Service (Cash)
51. Food Service (Contracted)
52. Food Service (Self-Operated)
53. Golf Course (Contracted)
54. Golf Course (Self-Operated)
55. Health Center
56. Hospital
57. Infirmary
58. Information Desk
59. Laundry (Coin)
60. Laundry (Contracted)
61. Laundry (Self-Operated)
62. Library
63. Married Housing (Contracted)
64. Married Housing (Self-Operated)
65. Medical Center
66. Parking Garage (Contracted)
67. Parking Garage (Self-Operated)
68. Parking Lot (Contracted)
69. Parking Lot (Self-Operated)
70. Parking Office
71. Print Shop
72. Pub (Alcohol)
73. Pub (Non-Alcohol)
74. Radio Station
75. Recreation Center
76. Registrar's Office
77. Residence Halls (Contracted)
78. Residence Halls (Self-Operated)
79. Security Office
80. Shuttle Service (Contracted)
81. Shuttle Service (Self-Operated)
82. Skating Rink (Ice)
83. Skating Rink (Roller)
84. Ski Lodge
85. Snack Bar
86. Snack Machines
87. Sports Complex
88. Student Association
89. Student Organizations
90. Student Union
91. Swimming Pool
92. Theater (Movie)
93. Theater (Stage)
94. Ticket Office (Contracted)
95. Ticket Office (Self-Operated)
96. Travel Agency
97. TV Station / Studio
98. VCR Rental Store
99. Video Game Room
100. Voting

Annexure II

Worldwide Campus Card initiatives (NACCU, 2001)

Abraham Baldwin Agricultural College	Florida Institute of Technology
Angelo State University	Florida State University Card Program
Arizona State University Card Program	Frostburg State University Card Program
Arkansas Tech University	Gannon University Card Program
Auburn University	George Mason University Card Program
Bates College	Georgetown University Card Program
Baylor University Card Program	Georgia Institute of Technology Card Program
Bishop's University	Goucher College
Black Hills State University Card Program	Grinnell College Card Program
Bloomsburg University of Pennsylvania	Hampton University
Boston University	Harper College
Bowdoin College	Harvard University Card Program
Brandeis University Card Program	Hofstra University Card Program
Brigham Young University – Hawaii Campus	Holy Cross Card Program
British Columbia Institute of Technology Card Program	Idaho State University Card Program
Brown University Card Program	Illinois Institute of Technology Card Program
Bryant College	Illinois State University Card Program
California Polytechnic State University Card Program	Indiana University Card Program
California State University – Bakersfield	Indiana University of Pennsylvania Card Program
California State University – Chico	Indiana University Purdue Indianapolis Card Program
California State University – Fullerton Card Program	Iowa State University Card Program
California State University – Sacramento Card Program	James Madison University Card Program
California University of Pennsylvania Card Program	Kansas State University Card Program
Carleton University Card Program	Kent State University Card Program
Central Connecticut State University Card Program	Lansing Community College Card Program
Central Michigan University Card Program	Lock Haven University of Pennsylvania
Claremont University Consortium	Logan College of Chiropractic
Clemson University Card Program	Louisiana State University
Cleveland State University Card Program	Loyola Marymount University
College of Mount St. Joseph	Marquette University Card Program
Colorado College	Mary Washington College
Concordia College Card Program	Massachusetts Institute of Technology Card Program
Concordia Theological Seminary	Medical College of Georgia Card Program
Concordia University	Memorial University of Newfoundland
Deakin University Card Program	Mercer University Card Program
Drexel University Card Program	Mesa State College Card Program
Duke University Card Program	Michigan Technological University Card Program
East Tennessee State University Card Program	Middlebury College Card Program
Eastern Illinois University Card Program	Minnesota State University, Mankato MavCard
Eastern Michigan University Card Program	Morgan State University Card Program
Elon University	Mount Holyoke College Card Program
Embry-Riddle Aeronautical University Card Program	Mount Royal College Card Program
Endicott College	New Jersey City University
Fairfield University	New York University Card Program
Florida Gulf Coast University	North Georgia College and State University
	North Idaho College
	Northeastern University Card Program
	Northern Arizona University Card Program
	Northern Illinois University
	Northern Kentucky University Card Program

Northwest Missouri State University Card Program
Northwestern University Card Program
Nova Southeastern University
Ohio State University Card Program
Oklahoma State University
Oral Roberts University
Park Point College
Pennsylvania State University Card Program
Pepperdine University
Pikeville College Card Program
Pittsburg State University Card Program
Providence College
Quinnipiac University
Randolph – Macon College
Red Deer College
Rensselaer Polytechnic Institute
Robert Morris College
Rutgers – The State University of NJ Card Program
Ryerson Polytechnic University Card Program
Saint Michael's College
Salisbury State University Card Program
Santa Clara University Card Program
Seattle University Card Program
Shepherd College
Shorter College
South Dakota State University Card Program
Southern Adventist University
Southern Methodist University Card Program
Southwest Missouri State University Card Program
Southwest Texas State University
St. Cloud State University
St. Norbert's College Card Program
State University of West Georgia
SUNY – Campus Card Program
SUNY – Oneonta Card Program
Stevens Institute of Technology
Tennessee Technological University
Texas A & M University Card Program
The George Washington University Card Program
Trinity University – San Antonio
Trinity Western University
Tri-State University
Troy State University Card Program
Tulane University Card Program
University of Alabama – Birmingham
University of Alaska Fairbanks
University of Alberta Card Program
University of Arizona Card Program
University of California – Berkeley Card Program
University of California – Riverside Card Program
University of Colorado at Boulder Card Program
University of Dayton Card Program
University of Delaware
University of Florida Card Program
University of Houston Card Program
University of Illinois – Springfield
University of Iowa Card Program
University of Kansas Card Program
University of Louisville
University of Maine Card Program
University of Maryland – Baltimore County
University of Michigan Card Program
University of Minnesota Card Program
University of Missouri – Columbia Card Program
University of Nevada – Las Vegas Card Program
University of New Mexico
University of North Alabama
University of North Carolina – Chapel Hill Card Program
University of North Carolina – Greensboro Card Program
University of North Carolina – Pembroke Card Program
University of Northern British Columbia
University of Northern Colorado Card Program
University of Pittsburgh
University of Richmond Card Program
University of San Diego
University of Science & Arts of Oklahoma
University of South Carolina
University of South Florida Card Program
University of Southern Indiana Card Program
University of Southern Maine Card Program
University of Texas – Austin Card Program
University of Texas – El Paso
University of Toledo Card Program
University of Virginia Card Program
University of Waterloo Card Program
University of West Florida Card Program
University of Winnipeg
University of Wisconsin – Green Bay Card Program
University of Wisconsin – Milwaukee
University of Wisconsin – Oshkosh Card Program
University of Wisconsin – Stevens Point Card Program
University of Wisconsin – Stout Card Program
Utah State University Card Program
Valdosta State University
Vanderbilt University
Virginia Commonwealth University Card Program
Washburn University Card Program
Washington and Jefferson College
Waterford Institute of Technology
Western Kentucky University Card Program
Wichita State University Card Office
Wilfred Laurier University
Willamette University
William Paterson University
Wright State University Card Program
Xavier University Card Program

Annexure III

Key Features and Characteristics *(http://egov.gov/smartgov/tutorial/tutorial_text.doc)*

Mentioned below are some of the key features and characteristics of smart cards.	
Cost	Typical costs range from $1.00 to $10.00. Per card cost increases with chips providing higher capacity and more complex capabilities; per card cost decreases as higher volume of cards are ordered.
Reliability	Vendors guarantee 10,000 read/write cycles. Cards claiming to meet International Standards Organization (ISO) specifications must achieve set test results covering drop, flexing, abrasion, concentrated load, temperature, humidity, static electricity, chemical attack, ultra-violet, X-ray, and magnetic field tests.
Error Correction	Current Chip Operating Systems (COS) perform their own error checking. The terminal operating system must check the two-byte status codes returned by the COS (as defined by both ISO 7816 Part 4 and the proprietary commands) after the command issued by the terminal to the card. The terminal then takes any necessary corrective action.
Storage Capacity	EEPROM: 8K – 128K bit. (Note that in smart card terminology, 1K means one thousand bits, not one thousand 8-bit characters. One thousand bits will normally store 128 characters, the rough equivalent of one sentence of text. However, with modern data compression techniques, the amount of data stored on the smart card can be significantly expanded beyond this base data translation.)
Ease of Use	Smart cards are user-friendly for easy interface with the intended application; handled like the familiar magnetic stripe bank card.
Susceptibility	Susceptible to chip damage from physical abuse, but more difficult to disrupt or damage than the magnetic stripe card.
Security	Smart cards are highly secure. Information stored on the chip is difficult to duplicate or disrupt, unlike the outside storage used on magnetic stripe cards that can be easily copied. Chip microprocessor and Co-processor supports DES, 3-DES, RSA or ECC standards for encryption, authentication, and digital signature for non-repudiation.
First Time Read Rate	ISO 7816 limits contact cards to 9600 baud transmission rate; some Chip Operating Systems do allow a change in the baud rate after chip power up; a well designed application can often complete a card transaction in one or two seconds.
Speed of Recognition	Smart cards are fast. Speed is only limited by the current ISO Input/ Output speed standards.
Proprietary Features	These include Chip Operating System and System Development Kits.
Processing Power	Older version cards use an 8-bit micro-controller clockable up to 16 MHz with or without co-processor for high-speed encryption. Current trend is toward customized controllers with a 32-bit RISC processor running at 25 to 32 MHz.
Power Source	Mostly 5 volt DC power source.
Support Equipment Required	For most host-based operations, only a simple Card Acceptance Device (that is, a card reader/writer terminal) with an asynchronous clock, a serial interface, and a 5-volt power source is required. For low volume orders, the per unit cost of such terminals runs between $100 and $250, the cost decreasing significantly with higher volumes. More costly Card Acceptance Devices are hand-held, battery-operated terminals and EFT/ POS desktop terminals.