**SMART CARD TECHNOLOGY**

**BY**

**DANIEL MUSA**

**ST/CS/ND/19/204**

**BEING A SEMINAR PAPER**

**PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE**

**SCHOOL OF SCIENCE AND TECHNOLOGY**

**FEDERAL POLYTECHNIC, MUBI ADAMAWA STATE**

**DECEMBER, 2021**

# ABSTRACT

*Smart Cards are handy bits of plastic with embedded microprocessor or memory chips that are used for identification. Smart cards look like a credit card in size but have a computer chip embedded in them. The chip has a certain amount of memory capable of storing data, with a Card Operating System (COS), which is protected with advanced security features. Smart cards when coupled with a reader have the processing power to serve several different applications. Smart cards can be considered as the world’s smallest computers. It’s quite possible that smart cards will follow the same trend of rapid increases in processing power that computers have, following "Moore’s Law" and doubling in performance while halving in cost every eighteen months. As their capabilities grow, they could become the ultimate thin client, eventually replacing all of the things we carry around in our wallets, including credit cards, licenses, cash, and even family photographs. Smart cards have tremendous applications starting from the simple driving license to biometrics.*

**INTRODUCTION**

Smart cards have proven to be quite useful as a transaction or authorization or identification medium in European countries. As their capabilities grow, they could become the ultimate thin client, eventually replacing all of the things we carry around in our wallets, including credit cards, licenses, cash, and even family photographs (Blaze, 1996). By containing various identification certificates, smart cards could be used to voluntarily identify attributes of ourselves no matter where we are or to which computer network we are attached. According to Dataquest, the worldwide smart card market has grown 4.7 Billion units and $6.8 Billion by 2002 (Blaze, 1996).

We live in a world of fast-moving technical change. This is perhaps particularly relevant and challenging when related to smart cards, where hundreds of thousands of card-reading terminals need to be available, and tens of millions of smart cards need to be deployed, all with a potential life of several years. Forwards compatibility, and cross border and cross scheme interoperability is increasingly difficult to maintain against the background of rapid chip technology development. EEPROM may give way to faster and longer-lived Flash memory. Voltages for powering smart cards are reducing almost annually. Security technologies demand ever-faster processing power (Gobioff, 1996).

**DEFINITION OF A SMART CARD**

The smart card is one of the latest additions to the world of information technology. Similar in size to today's plastic payment card, the smart card has a microprocessor or memory chip embedded in it that, when coupled with a reader, has the processing power to serve many different applications. This chip is the engine room of the smart card, and indeed is what makes it ‘smart’. The information or data stored on the IC chip is transferred through an electronic module that interconnects with a terminal or a card reader (Guillou, 1992). This union between a conventional PVC card and a microprocessor allows an immense amount of information to be stored, accessed and processed either off-line or on-line. According to Paul and Raymund (1989) a smart card carries more information than can be accommodated on a magnetic stripe card. It can make a decision, as it has relatively powerful processing capabilities that allow it to do more than a magnetic stripe card (e.g., data encryption).

**CLASSIFICATION OF SMART CARDS**

1. **MEMORY CARDS**

Memory cards simply store data. They do not have any processing capability and can be viewed as a small floppy disk with optional security. The main storage area in such cards is normally EEPROM (Electrically Erasable Programmable Read-Only Memory), which - subject to defined security constraints - can have its content updated, and which retains current contents when external power is removed (Blaze, 1996). Memory cards can be either memory only or can have security logic using passwords and pin codes. Memory cards are further divided into 2:

1. IC Memory Cards: Can store data, but do not have a processor on the card.
2. Optical Memory Cards: Can only store data, but has a larger memory capacity than IC memory cards.
3. **MICROPROCESSOR/INTELLIGENT SMART CARDS**

A microprocessor card, on the other hand, can add, delete and manipulate information in its memory on the card. Similar to a miniature computer, a microprocessor card has an input/output port, card operating system (COS) and hard disk with built-in security features (Gobioff, 1996). These cards have on-card dynamic data processing capabilities. Within the card is a microprocessor or microcontroller chip that manages this memory allocation and file access this type of chip is similar to those found inside all personal computers and when implanted in a smart card, manages data in organized file structures, via a card operating system. Unlike other operating systems, this software controls access to the on-card user memory. This capability permits different and multiple functions and/or different applications to reside on the card, allowing businesses to issue and maintain a diversity of ‘products’ through the card (Guillou, 1992).

# APPLICATIONS OF SMART CARDS

1. **Financial Applications**

Electronic Purse: Electronic Purse is designed to replace coins for small purchases in vending machines and over-the-counter transactions. VISACash Card issued during Olympics 1996 were the best example for this and Singapore’s Net Cash Card system is a Smart card which acts like electronic purse and holds the money. The money can be spent for Payment in Parking Lots, museums, telephones, fast food joints, vending machines, transportations and many more places. Such electronic money can take many forms, and has been endowed with a wide and misleading vocabulary including stored value and e-purse.

Telephone Payment Cards:These are the most widely used cards in the world. They have replaced coin-operated public phones, and have become advertising devices as well as collector’s items (Paul & Raymund, 1989).

1. **Government Applications**

National ID card:Smart Card based National ID’s project have started to take off in many countries among which Sultanate of Oman is first middle east country to deploy 1.2 million National ID cards to its residents. Gem plus, one of the leading providers of smart cards is behind this project with their solution called Resident for this purpose. Smart Card is one of the most secure mechanism today compared to any other type of ID cards, but when applications start to be deployed in such large scales it must take care to make sure the whole system of such a project is secure rather than just the information on the smart card, failing to do so will result for high threats and failure of such systems.

Driving License:The citizens of Argentina, El Salvador don’t need to carry dumb cards/ license booklets as a proof of eligibility to drive; they are allotted smart cards with their complete information on it. This almost reduces the license fraud to none with a secure mechanism which is difficult to be faked.

1. **HEALTH APPLICATIONS**

Patient Data Card (PDC): A Patient data Card is a mobile data card held by the patient. It stores current, accurate health information. Data typically stored on a PDC includes patient ID, insurance information, emergency record, disease history and electronic prescriptions (Schneier & Shostack, 1999).

Health Professional Card (HPC): An HPC is an individually programmed access authorization card held by the health professional. It gives him/her the right to read or write specific data fields on a PDC and it can also carry a digital signature for secure communication. This solution is popular and can be found available for citizens of countries like France, Germany, Slovenia, and Belgium.

1. **CAMPUS SOLUTIONS**
   1. Student Identification
   2. Library Card
   3. Meal Card
   4. Transportation Card

Student ID card, containing a variety of applications such as electronic purse (for vending and laundry machines), library card, meal card and transportation are used and University of Nottingham is one of them.

1. **EMPLOYEE CARDS**

Employee Identification Cards:These are used as identification cards at offices.

Employee Access Cards:Employee access card are used in most of the organizations today and millions of cards are being distributed every year catering this market, this mechanism replaces the conventional lock and key security, employees today don’t need to carry different keys to different locks for the secure office areas and access can be given or terminated at given point with just a click on the access software without any management of conventional keys , with the older mechanism of lock and key any disgruntled employee could make a fake key of the original while it was in his possession and misuse it later but in the case of smart cards this is almost impossible and if higher security is needed then biometrics can be combined to protect physical access to facilities (Blaze, 1996).

Time Attendance System:It monitors staff attendance and streamlines the input of data into the payroll system eliminating re-keying time sheets of time cards. These systems interact with existing automated Payroll systems, reducing administrative work, maximizing resources and optimizing performance. It customizes company data and it’s GUI Interface of point and click processing now automates this process and eliminates manual data entry. Its unique working timetable with varying schedules and work rules help ensuring company policies, accurate pay and uniformly administers benefits (Urien, 2000).It’s searching capabilities for employee records or date intervals produce detailed reports according to the searching criteria. The security features enable only the authorized person or administrator to view and modify data records as permitted to.

1. **COMMUNICATIONS AND ENTERTAINMENT**

SIM (Subscriber Identity Module):Subscriber Identification Module (SIM) providing secure initiation of calls and identification of caller (for billing purposes) on any Global System Mobile Communications (GSM) Mobile Phones. According to the survey don’t by GSM Worldaround 763 million cards used worldwide; this is one of the biggest applications of smart cards in the world after payphone cards.

Subscriber Activation Card for Pay-Tv:Subscriber activation for various programmes on Pay-Tv like Showtime and others is a big market for smart cards.

1. **INFORMATION SECURITY**

PC Security Cards:Chip cards are used today by majority of the corporations like Microsoft, Oracle to access their networks, chip cards can be incorporated with technologies like Active Directory to store the PKI certificates for authentications makes it dual factor (Digital Certificate + User password) and the it also allows the users to encrypt the files and digitally sign the emails. The advantage of this mechanism is that in case of any damage to smart card due to tampering/usage the user data is still secure to be decrypted by issuing a new card with the same original Digital Certificate. In case the smart card is lost or if company decided not to reissue the same digital certificate to avoid any kind security breach, they can reissue the smart card with a new private key (Digital Certificate) and the data can be decrypted for the user by an special key (Gobioff, 1996).

Digital Signature:Web based HTML forms can be digitally signed by your private key. This could prove to be a very important technology for internet based business because it allows for digital documents to be hosted by web servers and accessed by web browsers in a paperless fashion. Online expense reports, W-4 forms, purchase requests, and group insurance forms are some examples. For form signing, smart cards provide portability of the private key and certificate as well as hardware strength non repudiation. If an organization writes code that can be downloaded over the web and then executed on client computers, it is best to sign that code so the clients can be sure it indeed came from a reputable source. Smart cards can be used by the signing organization so the private key can’t be compromised by a rogue organization in order to impersonate the valid one.

Encryption:Smart cards can cipher into billions and billions of foreign languages, and choose a different language at random every time they communicate. This authentication process ensures only genuine cards and computers are used and makes eaves-dropping virtually impossible.

Telecommuting and Corporate Network Security:Business to business Intranets and Virtual Private Networks “VPNs” are enhanced by the use of smart cards. Users can be authenticated and authorized to have access to specific information based on preset privileges. Additional applications range from secure email to electronic commerce. A smart card as an interoperable computing device has become the ultimate utility of processor cards. Today's networked societies revolve around accessing the worldwide information superhighways. As more people log-on to the network and more and more activities take place through networks, online security is of utmost importance (Blaze, 1996).

# ADVANTAGES OF SMART CARDS

1. **CONVENIENCE**
   1. Light and easy
   2. Easy to use
   3. Portable
   4. Can be used independent of terminal devices.
   5. Secret place for storing information.
2. **INTELLIGENCE**
   1. Capable of processing, not just storing information.
   2. Communicating with computing devices.
   3. Information and applications on a card can be updated without having to issue new cards
3. **MULTIFUNCTIONALITY**

The processing power of a smart card makes it ideal to mix multiple functions. For example, government benefit cards will also allow users access to other benefit programs such as health care clinics and job training programs. A college identification card can be used to pay for food, phone calls and photocopies, to access campus networks and to register classes. By integrating many functions, governments and colleges can manage and improve their operations at lower costs and offer innovative services (Guillou, 1992).

1. **ECONOMIC BENEFITS**

Smart cards reduce transaction costs by eliminating paper and paper handling costs in hospitals and government benefit payment programs. Contact and contactless toll payment cards streamline toll collection procedures, reducing labor costs as well as delays caused by manual systems. Maintenance costs for vending machines, petroleum dispensers, parking meters and public phones are lowered while revenues could increase, about 30% in some estimates, due to the convenience of the smart card payment systems in these machines (Blaze, 1996).

1. **CUSTOMIZATION**

A smart card contains all the data needed to personalize networking, Web connection, payments and other applications. Using a smart card, one can establish a personalized network connection anywhere in the world using a phone center or an information kiosk. Web servers will verify the user's identity and present a customized Web page, an e-mail connection and other authorized services based on the data read from a smart card. Personal settings for electronic appliances, including computers, will be stored in smart cards rather than in the appliances themselves. Phone numbers are stored in smart cards instead of phones. While appliances become generic tools, users only carry a smart card as the ultimate networking and personal computing device.

1. **SECURITY**
   1. Information stored on the card can be PIN code and/or read-write protected. The most common method used for cardholder verification at present is to give the cardholder a PIN (Personal Identification Number) which he or she has to remember.
   2. Who can access the information?
      1. Everybody**:** Some smart cards require no password. Anyone holding the card can have access (e.g. the patient's name and blood type on a Medi Card can be read without the use of a password).
      2. Card Holder Only: The most common form of password for card holders is a PIN (Personal Identification Number), a 4 or 5 digit number which is typed in on a key pad. Therefore, if an unauthorized individual tries to use the card, it will lock-up after 3 unsuccessful attempts to present the PIN code. More advanced types of passwords are being developed.
2. **PESONALISATION**

There are two types of personalization. The first one is the ElectronicPersonalization, which means writing the data (particular data, fingerprint minutiae, variable data, etc.) into the chip.

The second is the GraphicalPersonalization, which means printing the required optical layout on the card surface (Text, Photos, Signature, and Graphics).

**DISADVANTAGES OF SMART CARDS**

1. The first issue with security involves public perception of the technology. People must believe that the cards are secure. This depends to a great extent upon actual security, but people must also be convinced of it. (Schneier & Shostack, 1999).
2. The second issue concerns the individual that holds responsibility for the card. If the cash balance is wiped clean by a memory failure, who is liable, the person or the bank.
3. Furthermore, another problem which smart cards will face in their move to diffuse extensively involves product complements.
4. **Easily Lost:** Like a credit card, smart cards are small, lightweight and can be easily lost if the person is irresponsible. Unlike credit cards, smart cards can have multiple uses and so the loss may be much more inconvenient.
5. **Security:** A second disadvantage of the using smart cards is their level of security. They are more secure than swipe cards. However, they are not as secure as some in the general public would believe.
6. **Slow Adoption:** If used as a payment card, not every store or restaurant will have the hardware necessary to use these cards. Therefore, some stores may charge a basic minimum fee for using smart cards for payment, rather than cash (Urien, 2000).
7. **Possible Risk of Identify Theft:** When used correctly for identification purposes, they make the jobs of law enforcement and healthcare professionals easier. However, for criminals seeking a new identity, they are like gold, based on the amount of information it can contain on an individual.

**CONCLUSION**

Smart cards can add convenience and safety to any transaction of value and data; but the choices facing today's managers can be daunting. We hope this site has adequately presented the options and give you enough information to make informed evaluations of performance, cost and security that will produce a smart card system that fits today's needs and those of tomorrow. Security is very crucial issue in smart card especially due to the various independent parties involve throughout the card’s life cycle leading to what is now called “splits” in trust. There is need to develop a method in which even without trust none of the parties can cheat one another.

**RECOMMENDATION**

Smart card is an excellent technology to secure storage and authentication. If an organization can deploy this technology selecting the right type of solutions which is cross platform compatible and supports the standards required, it would be economical as well as secure. This technology has to be standardized and used in various applications in an organization not just for physical access or information access. Various developments are happening in the smart card industry with respect to higher memory capacities and stronger encryption algorithms which could provide us with much tougher security. But we need to understand that we will achieve better security only if we have users educated to use this technology with at most care. A smart world is the future.

**REFERENCES**

Blaze, M. (1996). *High-bandwidth encryption with low-bandwidth smart cards. International Journal of Computer science, 4 (3),* 33-40.

Gobioff, D. (1996). *Smart cards in hostile environments,* Oakland publishers, CA.

Guillou, L. (1992). The smart Card: A Standardized Security Device Dedicated to Public cryptology, in G.J. Simmons (Ed.). *Contemporary Crypto-logy. The Science Journal of Information Integrity, 2(3),* 561-613.

Paul, B. & Raymund, E. (1989). The Smart Diskette – A universal token and personal crypto-engine. *International Journal of Advances in Cryptology, 1 (4),* 74-79.

Schneier, B. & Shostack, A. (1999). *Breaking Up Is Hard to Do:* Modeling Security Threats for Smart Cards, USENIX Workshop on Smart Card Technology, USENIX Press, pp. 175-185.

Urien, P. (2000). Internet Card, a Smart card as a true Internet node, Computer Communication. *International Journal of Sciences,* *2* (23), pp. 1655-1666.