Engineering and Scientific International Journal (ESIJ)
Volume 3, Issue 1, January – March 2016
ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

A Study on E-Smart Card System

A.Jegan

Lecturer, School of ICT, DMI-St.Eugene University, Lusaka, Zambia
jgnantony@yahoo.co.in

Abstract— Smart card provides detection, verification, data storage space and application processing. Smart cards are openly connected to the volume of information and applications that are automatically used on a card. A single smart card could be planned with multiple banking purposes, medical privilege, and driver's authorization. Multi-factor and immediacy validation has been fixed into smart cards to raise the protection of all services on the card. For example, a smart card can be able to programmed to only allow a contactless transaction like exclusively paired smart phones. This can be extensively increasing the security of the smart card.

A Smart card is fully a mechanical one.

- Peoples can update the information easily.
- It provides online purchasing facility.
- Peoples can easily find the Status of processing can be verified and identified at any stage of process
- Well-organized allocation of resources.
- It provides Time-management.

Keywords— detection, verification, privilege, immediacy, extensively

1. Introduction

A smart card or sometimes it is called as chip card, or sometimes it is called as integrated circuit card (ICC). These cards are any pocket-sized cards with entrenched integrated circuits. It contains unstable memory and microchip components. This card made-up of synthetic, polyvinyl chloride (PVC), and sometimes it is made-up of acrylonitrile butadiene styrene (ABS) or polycarbonate (PC). This smart card also provides strong protection, verification, Validation for single sign-on (SSO) within large organizations.

A. Smart card characteristics

- Dimensions:- ID-1 of the ISO/IEC 7810 standard defines cards as nominally 85.60 by 53.98 millimeters (3.370 × 2.125 in).
- One more size is ID-000 which is nominally 15 by 25 millimeters. (0.59 inch × 0.98 inch). Both are 0.76 millimeters (0.030 inch) thickness. (Example: SIM card)
- It contains a tamper-resistant security system (Example: a secure crypto processor and a secure file system) and provides security services (Example: protects in-memory information).
- It managed by an administration system which strongly interchanges information and settings with the card and also it is scheming with card blacklisting and application-data updates.
- It communicates with external services via card-reading devices. Example: ticket readers, ATMs, etc.

B. Properties

Fig.1: Smart Card

- A smart card has two properties (that is credit card and debit card).
- The 3/5 millimeter security chip entrenched in the card is shown enlarged in the inset.
- The contact pads of the card will be facilitating electronic contact with the chip.

C. History of Smart card

- In 2001, Honeywell Bull invented the first microchip card and he patented the self programmable one-chip micro card(SPOM) and it defines the essential structural design to program with the microchip.
- After 3 years, Motorola Company used this same patent in their "CP-8" model chip.
- In 2006, Axalto and Gemplus, the world's top two micro chip smart card manufacturers.
- In 2008 Dexa Systems, which includs the smart card solutions division responsible for binding the first huge level public key infrastructure (PKI) based on smart card management systems.
- The major boom in smart card use came in the 1990s, with the introduction of smart-card-based SIMs used in

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

GSM smart phones equipment in Europe. With the ubiquity of smart phones in Europe.

- Nowadays smart card becomes more popular for people use.

2. EMV (EuroPay MasterCard and Visa)

The global payment popular brands are MasterCard, Visa card, and Euro pay. These cards are agreed in 1993. The first version of the EMV smart card system has been released in 1994. In 1998, a standard version of EMV smart card has been released in the name of EMVco. The company responsible for the enduring maintained of the system upgraded the specification in 2000 and in 2004. EMVco purpose is to assure the various economic institutions and protect toward the back compatibility with the 1998 version.

There are two types of cards. Contactless cards and contact cards.

A. Contactless cards

For contactless smart cards, do not have need of physical contact between card and card reader. This contactless smart cards becomes more popular for payment and e-ticketing applications such as shipment and motorway tolls. Visa card and Master card have agreed to an easy-to-implement version. It was worked in the year of 2004–2006 at USA. Most of the contactless cards are fare collection implementations, custom and unsuited though the MIFARE Standard card has a significant market share in the US and Europe.

Smart cards are also being introduced in personal recognition and privilege schemes at regional, national, and international levels like Citizenship cards, driving licenses, and patient admission card. For example, In Malaysia, the required national ID scheme called as “MyKad” includes 8 different applications and has 18 million users. Contactless smart cards are part of ICAO which is working in the biometric passports to improve the security for international travel.

B. Contact cards

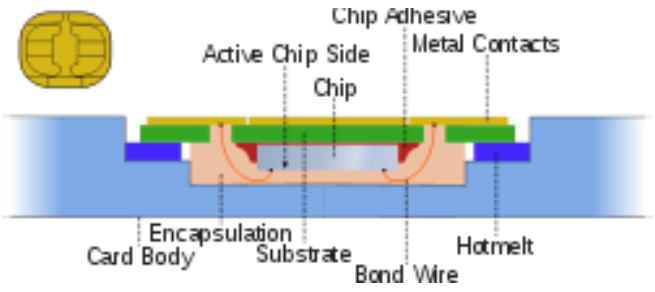

Fig.2: Structural Design of Contact cards

This type of smart card has makes contact with area of 1 sqre centimetre (0.16 square inch) approx, comprising several gold-plated contact pads. This contact pad provides electrical connectivity when inserted into a card reader machine.

The ISO/IEC 7810 and ISO/IEC 7816 series of characteristics:

- Physical outline and individuality.
- electrical connector positions and shapes
- Electrical characteristics.
- Communications protocols, including instructions has been sent to that card and responses getting from the card.
- Basic functionality.
- Card does not hold batteries; but power is supplied by the card reader.

C. Communication Protocols

Table 1: List of Communication protocols

Communication protocols	
Name	**Explanation**
T=0	Character level transmission protocol, defined in ISO/IEC 7816-3
T=1	Block level transmission protocol, defined in ISO/IEC 7816-3

Fig.3: Pin diagram of the Smart Card

- VCC - Power supply; RST - Reset signal, which is used to reset the card’s communications.
- CLK – which means the card with clock signal, from which data communications timing is derived;
- GND – This means Ground connection.
- VPP - Designated this as a programming voltage - an input for a higher
- Voltage to program persistent memory (Example: EEPROM).
- ISO/IEC 7816-3:2006 designates it SPU, as input and/or Output;
- I/O - Serial input and output (half-duplex);
- C4, C8 - The two types of contacts are AUX1 and AUX2 respectively and which is used for USB interfaces.

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

D. Smartcard Reader works on a Laptop

- Smart card readers are used as connections between the smart card and a computer (Example: a computer with a point of sale terminal).
- The chip in financial cards are the same as those used in subscriber identity modules (SIMs) in mobile phones, automatic differently and entrenched in a different part of PVC.
- The Chip manufacturers are building to the more challenging on GSM/3G standards.

E. Functionality of Smart Card -Smart Card Web Server

In 2007, the Open Mobile Alliance (OMA) estimated a new standard significant V1.0 of the Smart Card Web Server (SCWS).

HTTP server embedded in a SIM card intended for a smart phone User. The non-profit trade organization of SIMalliance organization has been promoting the growth and implementation of SCWS. The SIMalliance organization states that SCWS offers "OS-independent" platform for end-user. As of mid-2010, SIMalliance organization had not reported extensive industry acceptance of SCWS. The OMA has been maintaining the Standard version V1.1 in May 2009, and another version V1.2 is expected to be approved in October 2012.

3. Applications

A. Computer security

The Mozilla Firefox web browser may use the smart cards to store certificates for secure web browsing. Some disk encryption algorithms are to be followed such as True Crypt. Microsoft Windows 7 Bit Locker, which is used to smart cards for securely hold encryption keys.
It also adds another layer of encryption to critical parts of the secured disk.

The mechanism called as "On-the-fly encryption (OTFE)", also known as "real-time encryption", mechanism which is used by some encryption programs. Smart cards are also used for single sign-on(SSO) to log on with computers. Smart card functionality has been added to Windows Live passports.

B. Credit cards

These are the popular payment cards (classic plastic card):

- Visa card
- MasterCard
- American Express
- Discover

Credit card usage started in the year of 2005 at USA and it has been followed in the countries namely, Asia and Europe at the year of 2006. Contactless (non PIN) transactions cover a payment range of ~$5–50. There is an ISO/IEC 14443 Pay Pass implementation.

Non-EMV cards work like magnetic stripe cards. This is a classic USA card technology. The cards do not hold/maintain the account balance. All payment method passes without a PIN number, and also used in off-line internet mode. EMV cards have contact and contactless interfaces.

C. Cryptographic smart cards

Cryptographic algorithms to be followed by two different ways;

- RSA
- DSA.

Today Cryptographic smart cards produce key pairs and which is used to avoid the risk from having more than one copy of the key. Smart cards are mainly used for digital signature and secure detection, The most common way to access cryptographic smart card functions is Vendor-provided PKCS#11 library. The most commonly used cryptographic algorithms in smart cards are;

- Triple DES
- RSA.

The key set will be loaded in DES or generated by RSA on the card. Some of these smart cards are also made to support the NIST standard for Personal Identity Verification, FIPS 201.

D. Financial

Smart cards used as in the format of credit card, debit cards, ATM cards, fuel cards, mobile SIM cards, authorization cards for pay television. Household utility pre-payment cards, high security identification and access control cards, and public transport and public phone payment cards. Smart cards may also be used as electronic wallets.

E. Health care (medical)

Smart health cards can improve the security and privacy of patient information. It also provides a secure carrier for portable medical records. It reduces health care fraud, and support new processes for portable. Medical records also gives all the information about emergency medical information, facilitate compliance with government initiatives (Example, organ donation) and mandates. It provides the platform to implement other applications as needed by the health care organization.

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

F. Identification

Recently, a quickly growing application is called as "digital identification". In this application, the cards can be holds authenticate identity. Example, public key infrastructure (PKI). The card stores an encrypted digital certificate issued from the PKI provider along with other related information. Examples: In U.S.A, the Department of Defense (DoD), Common Access Card (CAC), and various identification cards used by many governments for their citizens. This card has been combined with biometrics systems and also it can provide 2 or 3 factor authentication.
The first smart card driver's license system was implemented in the year of 1987 at Turkey. Turkey had a high level of road accidents and it has decided to develop. It uses digital macrograph devices on heavy vehicles, instead of the existing motorized ones for reducing speed violations.

Later, a smart card driver's license system was issued in 1995 at Mendoza province of Argentina. Mendoza had a high level of road accidents, driving offenses. It had a poor record of recovering outstanding fines. Smart card license system holds the latest records of driving offenses and unpaid fines.

In 1999, Gujarat was the first Indian state to introduce a smart card license system. Till now, it has issued 5 million smart card driving licenses to its people. In 2002, the Estonian government started to issue smart cards, named as "ID Kaart", the primary identification for citizens to replace the usual passport in domestic and EU use. By the start of 2009, the entire population of Spain and Belgium will have an "eID card" which is used for identification. This card contain two certificates: first certificate provides authentication and second certificate provides signature.

In 2010, about 1 million smart cards have been issued (total population is about 1.3 million) and they are widely used in internet banking, buying public transport tickets, authorization on various websites etc.

G. Schools

- Tracking student attendance.
- As an electronic purse, to pay for items at canteens, transaction machines etc.
- Tracking and monitoring food choices at the canteen and also it helps the student to maintain a healthy diet.
- Tracking loans from the school library

H. Public Transit

Smart cards with integrated ticketing have become commonly used by public transit operators around the world.

I. Concessionary travel

A highly successful use for smart cards within the UK is in concessionary travel schemes. Mandated by Transport department for travel entitlements and disabled residents are administered by local authorities.

J. Security

Smart cards have been advertised as suitable for personal identification tasks, since they are engineered to be interfering resistant. The chip usually implements some cryptographic algorithm. There are several methods for recovering some of the algorithm's internal state.

4. Problems

The plastic card with embedded chip is fairly flexible, and it is larger than chip, the likelihood that normal use could damage it. Cards are often carried in wallets or pocket a harsh situation for a chip. However, for large banking systems, failure-management costs can be more than offset by fraud reduction.

A. Drawbacks of the Existing System

- It requires many departments to handle variety of tasks.
- It involves lot of paper work.
- No proper assignment of responsibilities would be there.
- No electronic workflow, processing and approvals.
- No automation and centralization of records.
- Low and dragging access to records and details on employees, clients, dealers.
- New changes cannot be easily implemented.
- Loss of records is possible to occur.

B. Proposed system

The proposed System is fully an automated one. As the proposed system is a centralized one, redundancy can be avoided; furthermore the coordination of various departments becomes much easier. Improve business practices and streamline operations.

- Reduce the departmental system requirement.
- Provide a single point of entry for information.
- Provide electronic workflow, processing's and
- approvals.
- Automate audits and edits, and centralize rules
- administration.
- Improve information access at the Suppliers,

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Employee, Customers and Administrative levels.

- Provides new functionality.

5. Conclusion

The fundamental problem is managing and maintaining the work by the administrator. Prior to this it was a bit cumbersome for maintaining the library and also track keeping of the users who were using it. The amount of time consumption is abridged and also the manual calculations are omitted, the reports and bills can be obtained regularly. The storage facilities will easiness the work of the operator. Thus the system developed will be helpful to the administrator by easing his/her task.

References

[1] Rankl, W.; W. Effing (1997). Smart Card Handbook. John Wiley & Sons. ISBN 0-471-96720-3.

[2] Guthery, Scott B.; Timothy M. Jurgensen (1998). Smart Card Developer's Kit. Macmillan Technical Publishing. ISBN 1-57870-027-2.

[3] "Monticello Memoirs Program". Computerworld honors. http://www.cwhonors.org. February 2012.

[4] "Emergency Response Official Credentials: An Approach to Attain Trust in Credentials across Multiple Jurisdictions for Disaster Response and Recovery". January 3, 2011. "OMA Newsletter 2007 Volume 2". http://www.openmobilealliance.org/com.

[5] K.Mala andT.Lavanya (2015), Image Enhancement using Adaptive and Gaussian Filters, DWT for Face Recognition, Special Issue of Engineering and Scientific International Journal (ESIJ) , (TSRW-MCA-SAEC) – May 2015

A. Jegan is working as a Lecturer in DMI – St. Eugene University, Lusaka, Zambia. He did his M.Phil in Prist Universty, Thanjavur, India in the year of 2012. He had his MCA in Bishop Heber college, Trichy, India in the year of 2010. He completed his B.Sc at Arul Anandar College, Madurai, India. His Research interest is Web designing, soft Computing, Data Mining.