Research Paper Engineering

A Study on E-Smart Card System

Dr.P.Anandraj | Assistant professor, Infant jesus College of Engineering, Keelaval-lanadu,

ABSTRACT

Smart cards can provide identification, authentication, data storage and application processing. Smart cards are directly related to the volume of information and applications that are programmed for use on a card. A single contact/contactless smart card can be programmed with multiple banking credentials, medical entitlement, driver's license/public transport entitlement, loyalty programs and club memberships to name just a few. Multi-factor and proximity authentication can and has been embedded into smart cards to increase the security of all services on the card. For example, a smart card can be programmed to only allow a contactless transaction if it is also within range of another device like a uniquely paired mobile phone. This can significantly increase the security of the smart card. Transformation of smart-card-based single-purpose e-micropayment scheme to multi-purpose scheme.

E Smart System is fully an automated one.

- Easy updating of information
- Provides online resource sharing facility
- Status of processing can be verified and identified at any stage of process
- Efficient allocation of resources
- Ensures timeline management

KEYWORDS

INTRODUCTION:

A **smart card**, **chip card**, or **integrated circuit card** (**ICC**), is any pocket-sized card with embedded integrated circuits. A smart card or microprocessor cards contain volatile memory and microprocessor components. The card is made of plastic, generally polyvinyl chloride, but sometimes acrylonitrile butadiene styrene or polycarbonate. Smart cards may also provide strong security authentication for single sign-on (SSO) within large organizations.

A smart card may have the following generic characteristics:

- Dimensions similar to those of a credit card. ID-1 of the ISO/IEC 7810 standard defines cards as nominally 85.60 by 53.98 millimeters (3.370 × 2.125 in).
- Another popular size is ID-000 which is nominally 25 by 15 millimeters (0.984 × 0.591 in) (commonly used in SIM cards). Both are 0.76 millimeters (0.030 in) thick.
- Contains a tamper-resistant security system (for example a secure crypto processor and a secure file system) and provides security services (e.g., protects in-memory information).
- Managed by an administration system which securely interchanges information and configuration settings with the card, controlling card blacklisting and application-data updates.
- Communicates with external services via card-reading devices, such as ticket readers, ATMs, etc.

Benefits

Smart cards can provide identification, authentication, data storage and application processing.

The benefits of smart cards are directly related to the volume of information and applications that are programmed for use on a card. A single contact/contactless smart card can be programmed with multiple banking credentials, medical entitlement, driver's license/public transport entitlement, loyalty programs and club memberships to name just a few. Multi-factor and proximity authentication can and has been embedded into smart cards to increase the security of all services on the card.

A smart card, combining credit card and debit card properties. The 3 by 5 mm security chip embedded in the card is shown enlarged in the inset. The contact pads on the card enable electronic access to the chip.

History:

In 2001, Bull sold its CP8 division together with its patents to Schlumberger, who subsequently combined its own internal smart card department and CP8 to create Axalto.

In 2006, Axalto and Gemplus, at the time the world's top two smart card manufacturers, merged and became Gemalto.

In 2008 Dexa Systems spun off from Schlumberger and acquired Enterprise Security Services business, which included the smart card solutions division responsible for deploying the first large scale public key infrastructure (PKI) based 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 GSM mobile phone equipment in Europe. With the ubiquity of mobile phones in Europe, smart cards have become very common.

EMV (EuroPay MasterCard and Visa)
The international payment brands MasterCard, Visa, and Euro pay agreed in 1993 to work together to develop the specifications for smart cards as either a debit or a credit card. The first version of the EMV system was released in 1994. In 1998 a stable release of the specifications became available. EMVco, the company responsible for the long-term maintenance of the system, upgraded the specification in 2000 and in 2004. EMVco's purpose is to assure the various financial institutions and retailers that the specifications retain backward compatibility with the 1998 version.

Contactless
Contactless smart cards that do not require physical contact between card and reader are becoming increasingly popular for payment and ticketing applications such as mass transit and motorway tolls. Visa and MasterCard have agreed to an easy-to-implement version that was deployed in 2004–2006 in the USA. Most contactless fare collection implementations are custom and incompatible, though the MIFARE Standard card from Philips has a considerable market share in the US and Europe.

Smart cards are also being introduced in personal identification and entitlement schemes at regional, national, and international levels. Citizen cards, drivers' licenses, and patient card schemes are appearing. In Malaysia, the compulsory national ID scheme MyKad includes eight different applications and has 18 million users. Contactless smart cards are part of ICAO biometric passports to enhance security for international travel.

Contact

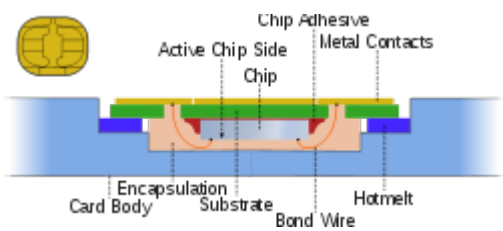

Illustration of smart card structure and packaging

Contact smart cards have a contact area of approximately 1 square centimeter (0.16 sq in), comprising several gold-plated contact pads. These pads provide electrical connectivity when inserted into a reader.

The ISO/IEC 7810 and ISO/IEC 7816 series of standards define:

- physical shape and characteristics
- electrical connector positions and shapes
- electrical characteristics
- communications protocols, including commands sent to and responses from the card
- basic functionality
- Cards do not contain batteries; power is supplied by the card reader.

Communication protocols:

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

Signals

A smart card pinout
- VCC - Power supply; RST - Reset signal, used to reset the card's communications.
- CLK - Provides the card with a clock signal, from which data communications timing is derived;
- GND - Ground (reference voltage).
- VPP - ISO/IEC 7816-3:1997 designated this as a programming voltage - an input for a higher
- Voltage to program persistent memory (e.g., EEPROM).
- ISO/IEC 7816-3:2006 designates it SPU, for either standard or proprietary use, as input and/or
- Output; I/O - Serial input and output (half-duplex); C4, C8 - The two remaining contacts are AUX1 and AUX2 respectively, and used for USB interfaces and other uses.

Reader:
Smartcard Reader on a Laptop
Contact smart card readers are used as a communications medium between the smart card and a Host (e.g., a computer, a point of sale terminal) or a mobile telephone.

Because the chips in financial cards are the same as those used in subscriber identity modules

(SIMs) in mobile phones, programmed differently and embedded in a different piece of PVC,

Chip manufacturers are building to the more demanding GSM/3G standards.

Functionality
Smart Card Web Server
In 2007, the Open Mobile Alliance (OMA) proposed a new standard defining V1.0 of the Smart Card Web Server (SCWS), an HTTP server embedded in a SIM card intended for a smart phone User. The non-profit trade association SIMalliance has been promoting the development and Adoption of SCWS. SIMalliance states that SCWS offers end-users a familiar, OS-independent, Browser-based interface to secure, personal SIM data. As of mid-2010, SIMalliance had not reported widespread industry acceptance of SCWS. The OMA has been maintaining the Standard, approving V1.1 of the standard in May 2009, and V1.2 is expected to be approved in October 2012.

APPLICATIONS
Computer security
The Mozilla Firefox web browser can use smart cards to store certificates for use in secure web browsing. Some disk encryption systems, such as Free OTFE, True Crypt and Microsoft Windows 7 Bit Locker, can use smart cards to securely hold encryption keys, and also to add another layer of encryption to critical parts of the secured disk.

Smart cards are also used for single sign-on to log on to computers.

Smart card support functionality has been added to Windows Live passports.

Credit cards
These are the best known payment cards (classic plastic card):
- Visa: Visa Contactless, Quick VSDC—"qVSDC", Visa Wave, MSD, pay Wave
- MasterCard: Pay Pass Magistrate, Pay Pass Mchip
- American Express: Express Pay

- Discover: Zip

Roll-outs started in 2005 in USA. Asia and Europe followed in 2006. Contactless (non PIN) transactions cover a payment range of ~$5–50. There is an ISO/IEC 14443 Pay Pass implementation. Some, but not all Pay Pass implementations conform to EMV.

Non-EMV cards work like magnetic stripe cards. This is a typical USA card technology (Pay Pass Magistrate and VISA MSD). The cards do not hold/maintain the account balance. All payment passes without a PIN, usually in off-line mode. The security of such a transaction is no greater than with a magnetic stripe card transaction.EMV cards have contact and contactless interfaces.

Cryptographic smart cards

Cryptographic smart cards are often used for single sign-on. Most advanced smart cards include:

Specialized cryptographic hardware that uses algorithms such as RSA and DSA. Today

Cryptographic smart cards generate key pairs on board, to avoid the risk from having more than one copy of the key (since by design there usually isn't a way to extract private keys from a smart card). Such smart cards are mainly used for digital signature and secure identification, The most common way to access cryptographic smart card functions on a computer is to use a Vendor-provided PKCS#11 library.[] On Microsoft Windows the CSP API is also supported.

The most widely used cryptographic algorithms in smart cards (excluding the GSM so-called

"Crypto algorithm") are Triple DES and RSA. The key set is usually loaded (DES) or generated (RSA) on the card at the personalization stage.

Some of these smart cards are also made to support the NIST standard for Personal Identity Verification, FIPS 201.

Financial

Smart cards serve as credit or ATM cards, fuel cards, mobile phone SIMs, 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.

Health care (medical)

Smart health cards can improve the security and privacy of patient information, provide a secure carrier for portable medical records, reduce health care fraud, and support new processes for portable. Medical records provide secure access to emergency medical information, enable compliance with government initiatives (e.g., organ donation) and mandates, and provide the platform to implement other applications as needed by the health care organization.

Identification

A quickly growing application is in digital identification. In this application, the cards authenticate identity. The most common example employs public key infrastructure (PKI). The card stores an encrypted digital certificate issued from the PKI provider along with other relevant information. Examples include the U.S. Department of Defense (DoD) Common Access Card (CAC), and various identification cards used by many governments for their citizens. Combined with biometrics, cards can provide two- or three-factor authentication.

The first smart card driver's license system in the world was implemented in 1987 in Turkey. Turkey had a high level of road accidents and decided to develop and use digital macrograph devices on heavy vehicles, instead of the existing mechanical ones, to reduce speed violations.

A smart card driver's license system was later issued in 1995 in Mendoza province of Argentina. Mendoza had a high level of road accidents, driving offenses, and a poor record of recovering outstanding fines. Smart licenses hold up-to-date records of driving offenses and unpaid fines.

In 1999 Gujarat was the first Indian state to introduce a smart card license system. To date it has issued 5 million smart card driving licenses to its people.

In 2002, the Estonian government started to issue smart cards named ID Kaart as 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 that is used for identification. These cards contain two certificates: one for authentication and one for signature.

As of 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.

Schools

Smart cards are being provided to students at schools and colleges. Usage includes:

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

Public transit

Smart cards and integrated ticketing have become widely used by public transit operators around the world.

Concessionary travel

A highly successful use for smart cards within the UK is in concessionary travel schemes. Mandated by the Department for Transport, travel entitlements for elderly and disabled residents are administered by local authorities and passenger transport executives.

Security

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

Problems

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

Existing System

The Existing system for E-smart is a manual process. Taking existing system in to consideration, we can find that the manager has to interact with the dealer, clients in person, brief on the requirements they expect and so on. All these require more time and labor. The data collected may be inconsistent, redundant and getting in touch with a remote candidate will become impossible.

Drawbacks of the Existing System:

The existing system has the following disadvantages:

- Requires many departments to handle variety of tasks.
- 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 probable to occur, as it is paper works.

Proposed system:
The proposed E-Smart System is fully an automated one. In the proposed system, the clients online can view the company details and requirements put forward by them. As the proposed system is a centralized one, redundancy can be avoided; moreover the coordination of different departments becomes much easier. Above all the system provides high security for all its data. The proposed system is mainly required to be listed as:

- Easy updating of information
- Provides online resource sharing facility
- Status of processing can be verified and identified at any stage of process
- Efficient allocation of resources
- Ensures timeline management
- Improve business practices and streamline operations.
- Reduce the need for departmental system.
- 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 employee, Suppliers, Customers and Administrative levels.
- Provides new functionality.

CONCLUSION
The fundamental problem in managing and maintaining the work by the administrator is hence overcome. Prior to this it was a bit cumbersome for maintaining the library and also keeping track of the users who were using it. But by developing this web-based application the administrator can enjoy the task, doing it ease and also by saving the valuable time. The amount of time consumption is reduced and also the manual calculations are omitted, the reports and bills can be obtained regularly and also whenever on demand by the user. The effective utilization of the work, by proper sharing it and by providing the accurate results. The storage facility will ease the job of the operator. Thus the system developed will be helpful to the administrator by easing his/her task.

REFERENCES

Rankl, W.; W. Effing (1997). Smart Card Handbook. John Wiley & Sons. ISBN 0-471-96720-3. Guthery, Scott B.; Timothy M. Jurgensen (1998). Smart Card Developer's Kit. Macmillan Technical Publishing. ISBN 1-57870-027-2. "Monticello Memoirs Program". Computerworld honors. http://www.cwhonors.org. February 2012. "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/comms/pages/OMA_quarterly_2007_v2.htm#news1.