Smart card

A smartcard is a specific type of plastic card generally made of polyvinyl chloride based on polyesters or polycarbonate. It is the size of credit card. There is a 3by 5 mm imbedded chip in the card. Smart card contains either memory card or microprocessor that holds data and information. The microprocessor card can add, delete, and manipulate information on the card, while a memory-chip card (for example, pre-paid phone cards) can only undertake a pre-defined operation.

Smart cards, unlike magnetic stripe cards, can carry all necessary functions and information on the card. Therefore, they do not require access to remote databases at the time of the transaction. A typical smartcard consists of an 8-bit microprocessor running at approximately 5 MHz with ROM, EEPROM and RAM, together with serial input and output, all in a single chip that is mounted on a plastic carrier. The operating system is typically stored in ROM, the CPU uses RAM as its working memory, and most of the data is stored in EEPROM. Fig:-1 shows smart card. History

In 1968 and 1969 German electrical engineers Helmut and Jurgen jointly developed automated chip card. Then after in 1974 French inventor Roland Moreno gives memory card concept called smart card. An important patent for smart cards with a microprocessor and memory as used today was filed by Jurgen Dethloff in 1976 and granted as USP 4105156 in 1978. The first mass use of the cards was as a telephone card for payment in French pay phones starting in 1983. Carte Bleue After the Telecarte microchips were integrated into all French Carte Bleue debit cards in 1992.

Customers inserted the card into the merchant's POS terminal, then typed the PIN, before the transaction was accepted. Only very limited transactions

(such as paying small highway tolls) are processed without a PIN. Smart-card-based electronic purse systems store funds on the card so that readers do not need network connectivity and entered service throughout Europe in the mid-1990s. 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. Development of contactless systems 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 .

Smart cards are also being introduced in personal identification at national and international levels. Citizen cards, drivers' licenses, and patient card schemes are appearing. A smart card is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use. Currently or soon, you may be able to use a smart card to: Dial a connection on a mobile telephone and be charged on a per-call basis

* Establish your identity when logging on to an Internet access provider or to an online bank * Pay for parking at parking meters or to get on subways, trains, or buses * Give hospitals or doctors personal data without filling out a

form * Make small purchases at electronic stores on the Web (a kind of cybercash) * Buy gasoline at a gasoline station Over a billion smart cards are already in use. Currently, Europe is the region where they are most used. Ovum, a research firm, predicts that 2. billion smart cards will be shipped annually by 2003. Another study forecasts a $26. 5 billion market for recharging smart cards by 2005. Compaq and Hewlett-Packard are reportedly working on keyboards that include smart card slots that can be read like bank credit cards. The hardware for making the cards and the devices that can read them is currently made principally by Bull, Gemplus, and Schlumberger. How Smart Cards Work A smart card contains more information than a magnetic stripe card and it can be programmed for different applications.

Some cards can contain programming and data to support multiple applications and some can be updated to add new applications after they are issued. Smart cards can be designed to be inserted into a slot and read by a special reader.. An industry standard interface between programming and PC hardware in a smart card has been defined by the PC Working Group, representing Microsoft, IBM and other interested companies. Like smart cards with contacts, contactless cards do not have an internal power source.

Instead, they use an inductor to capture some of the incident radio-frequency interrogation signal, rectify it, and use it to power the card's electronics. Hybrids A hybrid smart card which clearly shows the antenna connected to the main chip Dual-interface cards implement contactless and contact interfaces on a single card with some shared storage and processing. An example is Porto's multi-application transport card, called Andante, which

uses a chip with both contact and contactless interfaces . Applications First introduced in Europe nearly three decades ago, smart cards debuted as a stored value tool for payphones to reduce theft.

As smart cards and other chip-based cards advanced, people found new ways to use them, including charge cards for credit purchases and for record keeping in place of paper. In the U. S. , consumers have been using chip cards for everything from visiting libraries to buying groceries to attending movies, firmly integrating them into our everyday lives. Several U. S. states have chip card programs in progress for government applications ranging from the Department of Motor Vehicles to Electronic Benefit Transfers (EBTs).

Many industries have implemented the power of smart cards in their products, such as the GSM digital cellular phones as well as TV-satellite decoders. Why Smart Cards Smart cards improve the convenience and security of any transaction. They provide tamper-proof storage of user and account identity. Smart card systems have proven to be more reliable than other machine-readable cards, like magnetic stripe and barcode, with many studies showing card read life and reader life improvements demonstrating much lower cost of system maintenance. Smart cards also provide vital components of system security or the exchange of data throughout virtually any type of network.

They protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. The costs to manage password resets for an organization or enterprise are very high, thus making smart cards a cost-effective solution in these environments. Multifunction

cards can also be used to manage network system access and store value and other data. Worldwide, people are now using smart cards for a wide variety of daily tasks, which include: 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. Non-EMV cards work like magnetic stripe cards. This is a typical USA cardtechnology(PayPass Magstripe 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. They work as a normal EMV card via contact interface. Via contactless interface they work somewhat differently in that the card command sequence adopts contactless features such as low power and short transaction time. 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.

Contactless smart cards that can be read from within a wallet or even a garment simplify authentication; however, there is concern over criminals accessing data from these 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's 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

The first smart card river's license system in the world was implemented in 1987 in Turkey. Turkey had a high level ofroad accidentsand decided to develop and use digital tachograph devices on heavy vehicles, instead of the existing mechanical ones, to reduce speed violations. Since 1987, the professional driver's licenses in Turkey are issued as smart cards and the driver is required to insert his driver's license into the digital tachograph before starting to drive. The tachograph unit records speed violations for each driver and gives a printed report. The driving hours for each driver is also being monitored and reported.

In 1990 the European Union conducted a feasibility study through BEVAC Consulting Engineers, titled " Feasibility study withrespectto a European electronic driver's license (based on a smart-card) on behalf of Directorate General VII". In this study, chapter seven is dedicated to the experience in Turkey, stating that the electronic driver's license application, in the form of smart cards, was first implemented in Turkey in 1987. Public transit Smart cards and integrated ticketing have become widely used by public transit operators around the world. Card users may use their cards for other purposes than for transit, such as small purchases.

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 TrueCrypt and Microsoft Windows 7 BitLocker, 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. Schools Smart cards are being provided to students at schools and colleges. Tracking student attendance * As an electronic purse, to pay for items at canteens, vending machines etc. * Tracking and monitoringfoodchoices at the canteen, to help the student maintain a healthy diet

* Tracking loans from the school library Healthcare Smarthealthcards can improve the security and privacy of patient information, provide a secure carrier for portable medical records, reduce health care fraud, 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. Advantages 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, loyaltyprograms 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. Individuals gain increased security and convenience when using smart cards designed for interoperability between services. For example, consumers only

need to replace one card if their wallet is lost or stolen. Additionally, the data storage available on a card could contain medical information that is critical in an emergency should the card holder allow access to this.

The first main advantage of smart cards is their flexibility. There is no need, for example, to carry several cards: one card can simultaneously be an ID, a credit card, a stored-value cash card, and a repository of personal information such as telephone numbers or medical history. Such a card can be easily replaced if lost, and, because a PIN number (or other form of security) must be used to access information, is totally useless to people other than its legal bearer. At the first attempt to use it illegally, the card would be deactivated by the card reader itself. The second main advantage is security.

Smart cards can be electronic key rings, giving the bearer ability to access information and physical places without need for online connections. They are encryption devices, so that the user can encrypt and decrypt information without relying on unknown, and therefore potentially untrustworthy, appliances such as ATMs. Smart cards are very flexible in providing authentication at different level of the bearer and the counterpart. Finally, with the information about the user that smart cards can provide to the other parties, they are useful devices for customizing products andservices.

Other general benefits of smart cards are: * Portability * Increasing data storage capacity * Reliability that is virtually unaffected by electrical and magnetic fields. Smart Cards andElectroniccommerce Smart cards are turning out to be a fundamental piece of the transformation of retailing into electronic commerce. The impressive growth of the Internet is making

electronic shopping at least a real possibility, if not a habit, among computer users. However, the business model used in current electronic commerce applications still cannot enjoy the full potential of the electronic medium.

Moreover, concerns about the reliability of an invisible counterpart and about the safety of the Internet for credit card information increase the wariness and thereby limit the use of the electronic shopping on the part of customers. Of the estimated 360 billion payments that took place in the United States in 1995, approximately 300 billion could not have taken place using the existing electronic media. Such transactions involved micro-payments p; i. e. payments for less than $10 p; which are virtually outside of the electronic arena for lack of a payment method compatible with such low amounts.

Credit cards or checks are simply too expensive to use for micro-payments, and the e-cash currently being experimented on the World Wide Web does not seem to have the characteristics to appeal to shoppers. For this reason, smart cards could be a fundamental building block of widespread use of electronic commerce, since they are an instrument to pay at a low cost for transactions involving small amountsofmoney. Another big advantage of smart cards for electronic commerce is their use for the customization of services.

It is already possible to purchase tailored services on the World Wide Web p; MyYahoo and FireFly are well known examples. However, in order for the service supplier to deliver the customized service, the user has to provide each supplier with her profile p; a boring and time consuming activity. A smart card can contain a non-encrypted profile of the bearer, so that the

user can get customized services even without previous contacts with the supplier. Finally, smart cards are a key technology enabler for financial institutions.

The processing power, the portability and the interactive properties of smart cards will constitute the basis for a revolution in the relationship between consumers and banks. PC-based home banking and phone banking will give way to card banking: a phone equipped with a smart card reader will be all that is needed for any kind of transaction. A smart card is a plastic card with a small, built in microcomputer chip and integrated circuit that can store and process a lot of data. It is considered to be a secure, time saving device that can access information without use of a PC or the Internet.

However, smart cards have both Flexibility * Smart cards have a lot of flexibility. They can store multiple types of information including identification, credit cards, business andfamilycontacts. Cost and Availability * Smart card readers are expensive to produce. These readers are not available in all locations and may have compatibility issues due to the differences of each smart card brand. Adafruit Raspberry Pi Starter Kit Now available in India ProtoCentral Security * Smart cards are individually encrypted and can only be accessed by pin number.

However, there is concern about privacy and whether or not information on the card could be accessed or used illegally by the government or other third-party sources. Data Integrity * Information on a smart card cannot be erased or removed accidentally by any electrical or magnetic means. Smart Card Uses * Smart cards are useful for setting limits on expenses, customizing customer loyalty programs and accessing critical health care

information. Smart cards save users from having to remember multiple usernames and passwords. Disadvantages

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 pockets, a harshenvironmentfor a chip. However, for large banking systems, failure-management costs can be more than offset by fraud reduction. Client-side identification and authentication cards are the most secure way for e. g. , internet banking applications, but security is never 100% sure. If the account holder's computer hosts malware, the security model may be broken.

Malware can override thecommunication(both input via keyboard and output via application screen) between the user and the application. Rabobank (" random reader") in the Netherlands combine a smart card with an unconnected card reader to avoid this problem. The customer enters a challenge received from the bank's website, a PIN and the transaction amount into the reader, The reader returns an 8-digit signature. This signature is manually entered into the personal computer and verified by the bank, preventing malware from changing the transaction amount. Another problem is the lack of standards for functionality and security.