Smart Cards Structure and Applications: Emerging and Evolution

Ass. Prof. Magdy Elhennawy
Department of Computer Science
Computers & Information Technology
Institute – ElShourouk Academy
Dr.magdy.ezzat@sha.edu.eg

Dr. M. Amer
Department of Computer Science
Computers & Information Technology
Institute – Future Academy
Mo_amer2002@gmail.com

Abstract. *Information technology plays a vital role for the development of smart cards. Smart cards can change the form of the delivery of services and goods, through the automated identification and verification of customers, resulting in significant efficiency gains and ultimately lower costs for consumers. Smart cards have the potential of providing privacy's benefits to its users and guaranteeing confidence in the trustworthiness of commercial organizations and institutions who provides services to such users.*

The diversity of modern networks, the Internet in particular, introduces a lot of facilities. Currently, all commercial services and applications are tended to be done through the Internet, such as electronic commerce, electronic funds transfer, electronic payment, and so forth. Even the office network environment is now extending to employee's home. Other applications can be banking, accounting, auditing, distant learning, and electronic voting. The management and accessing of such services and applications can be facilitated using smart objects like the smart cards. Accordingly, the employment of such smart cards has increased, and their applications have spread widely, covering all domains. In the near future, it is expected that the cash-less society is being dominating due to heavily provision of the portable secured enough object like the smart cards.

Meanwhile, smart cards are, further employed to support commercial and industrial applications by providing security services such as authentication and authorization.

In this paper we have introduced smart cards as an efficient smart object. A wide band of smart card services and applications are introduced, while it is still expected that such services and applications are spreading.

Key Words: Smart cards, Security via smart cards, Chip cards, ICC.

1. Introduction

A smart card is any standard-sized plastic card with embedded one or more integrated circuits within its thickness. It is often called chip cards or integrated circuit (IC) cards **[1]** which gives the card the ability to store and/or process data **[2]**. The application of smart cards has become more common and visible in our society due to its easy access and usage. Smart cards have revolutionized the types of physical interaction between different agents. Smart cards can be used for a variety of general purposes applications, e.g., authentication, data storage and data processing **[2]**. Other specific applications within particular industry sectors can be financial services and

health insurance, such applications should expand as the cards become smaller, cheaper, and more powerful. The data stored on a smart card can be protected by active data encryption schemes along with biometric identification (fingerprints, for example), which can be used to uniquely identify and authenticate the authorized and claimed user **[3].**

Biometric technology is a method of authentication. It measures human characteristics such as voice, fingerprint, and iris pattern and thus eliminates the problems associated with password management. It provides an additional security layer to the smart card system. Biometric module capabilities are embedded in the smart card chip to verify user's authenticity for a secure access control system by comparing the presented identity with a template, stored on a database in smart card, or optical card **[4].**

Today's, smart cards and their related technologies are an emerging component of electronic commerce worldwide. In some countries, they are revolutionizing aspects of commerce, health care, and others.

Smart cards appeared on the horizon when two German inventors, Jurgen Dethloff and Helmut Grotrupp, patented the idea of having plastic cards hold microchips in 1968. The Japanese patented another version of the smart cards in 1970. France was an early smart card proponent, and its investment in smart card research in the 1970's reflected a national effort to modernize its technological infrastructure. French financial institutions replaced magnetic stripe cards with smart cards in 1992. This resulted in a 75% reduction in credit card fraud over a five-year period **[3] [4].**

In this paper we present in section 2, the multi-application smart cards have been introduced. In section 3 the main uses of smart cards has been introduced. In section 4 an overview about smart card construction and organization covering: HW chip cards organization, SW chip cards architecture card file system, and chip cards Command and Response Format are presented. Security of Smart Cards has been surveyed in section 5, including; privacy, integrity, non-Repudiation, authentication, and verification. Authentication/Authorization Oriented Smart Cards Application is presented in section 6. The Smart Cards Standards is presented in section 7, then the conclusion is stated in section 8.

2. Multi-Application Smart Card

Multi-application smart cards are getting more and more attractive for numerous good reasons. Users are willing to reduce the number of cards in their wallets, issuers want to decrease the time-to-market, the development, the infrastructure and deployment costs. In addition multi-application smart cards allow commercial synergies between partners and can lead to new business opportunities **[5].**

A multiple application card is a smart card that can support different types of applications on the card itself **[6]**

The Malaysian Smart Card, MyKad, is a multipurpose or multiplication smart card, incorporates a set of applications including NIC, ID (Identification), DL (Driving License), passport information, health information, electronic purse, automated teller

machine (ATM) access, transit application, public key infrastructure (PKI), and frequent traveler card **[7]**.

On multi-application platform, we usually find an operating system managing the card resources (like I/O, memory, random number generator, crypto engine …) and some applications, possibly loaded after the OS ensures application segregation and provides mechanisms to allow controlled data sharing between applications **[5].**

One big issue when employing a multi-application smart card is the isolation between applications installed on the card and control the data and information flow to prevent the interference between applications installed on the card.

Meanwhile, to support on-board data processing and sophisticated applications, processor-enabled smart cards carry significantly more memory. This beefed-up memory capacity allows a processor-enabled smart card to function as a multi-application card, combining functions of: credit card, debit card, stored value card, information management card, and loyalty card.

Meanwhile, Visa's multiple application card strategies are based on providing applications that add value to Visa's core credit and debit payment products.
A key component of Visa's multi-application offering is the flexible Open Platform technology. In addition to providing added application security through the use of 'firewalls' on the chip, the Open Platform allows for downloading new applications to the chip without reissuing the card.

Another multi-application program was conducted at Florida State University, where 40,000 smart cards were deployed, which featured students' identification, dormitory security, banking, and a wide range of stored value functions for food, payphone, photocopying, transportation, and vending service **[6].**

For example, the chip on Blue from American Express currently offers two applications: extra security when shopping online using a PC smart card reader and an online wallet, and a ticketing application that verifies a Cardmember's ticket order. Blue uses a multiple application operating system, and American Express plans to add other applications to the card's smart chip **[6].**

We can find other examples with the Estonian ID card (Identity, transport, voting...), the Malaysian ID card (Identity, micro-payment, transportation, driving license, health care, welfare...), the Portuguese ID card (identity, welfare, tax, healthcare, voting), the Belgian and Finnish ID (ID and health) **[6].**

3. Main Uses of Smart Cards

We have identified three widely used categories of smart card applications: authentication, authorization, and transaction processing **[3]**.

Authentication. Smart cards provide personal identification information to authenticate an individual’s claim using either token-based or knowledge-based authentication approaches. Token-based systems use an item such as a passport, driver’s license, credit card, or key for identification, whereas knowledge-based

systems tend to rely on memorized information such as PIN numbers or passwords. High-tech smart card-based drivers' licenses not only serve as a means of identification, but can also contain driving records and unpaid traffic fines. Potentially, new traffic offenses could be updated to a person's smart card within minutes of the offense, although such an application could present some interesting legal issues, depending on which country or state issued the license **[3]**.

Authorization. As mentioned previously, smart cards offer data encryption and the ability to store biometric information for the purpose of authenticating the cardholder. Smart cards have potential to facilitate storage of demographic information for voting purposes, and they are playing a growing role in healthcare industry, which is experiencing a technological overhaul as electronic data management becomes more widespread and sophisticated. The Smart Card Industry Association reports that over 80 million smart cards are currently used in Germany's healthcare system. France's Sésam-Vitale program includes 10 million cards in its family plan and about 35 million individual cards. Smart cards could help automate and standardize patient demographic information on medical records, including those of insurance carriers. Smart cards with optical storage could store and transfer both text and image-based medical records between patient and healthcare providers. These cards can also assist patients whose care depends on complicated equipment, such as kidney dialysis machines. Configuration for dialysis equipment, as well as medication information, could be stored on smart cards and inserted into a smart card-enabled dialysis chine anywhere in the world. Of course, privacy, technology, legal, and cost issues must be addressed before such health-related applications become widespread. Smart cards could also facilitate drug prescription fulfillment. Prescription's information could be loaded onto a smart card at the physician's office, and read by the pharmacist's reader for patient and physician information, and dosage and refill specifications. With proper encryption, prescriptions could also send electronically from the physician's office. Again, patients could have their card swept at the pharmacy for fulfillment. Payment terms could also be arranged through the card **[3].**

Transaction processing. There are also numerous ways smart cards have potential to assist in goods and service transactions, both in Web-based and traditional "bricks and mortar" establishments. The cards could be reloaded with cash value in ATM machines and used as a credit card. The currency carried on a smart card could be utilized in different countries, as an electronic, multinational traveler's check. Smart card technology also provides a secure Internet-based payment mechanism through data encryption. The contact-less version of a smart card is now used in situations requiring short transaction times, including issuing driving tickets and paying toll fares. Smart cards are helping to expand the application of Global System for Mobile Communications (GSM) phones in regions such as Asia, Europe, and South America. Using a smart card equipped with a Subscriber Identity Modules (SIM) chip, an individual subscriber can be identified and charged for services by his or her telecommunication system. The card can facilitate this identification through any GSM phone. The SIM chip can also store a subscriber's personalized electronic phonebook. Such an application represents a rapidly expanding segment of the smart card industry. Some GSM phones have two smart card slots, with the second slot allocated for an electronic wallet, thereby permitting the mobile terminal to also serve as a "pocket ATM machine". Voting is another type of transaction, but instead of having a basis in commerce, it is based in authorization and information exchange.

Smart cards have the capability of biometric-based voter registration, using fingerprints, for example, which can help prevent voter fraud **[3].**

The use of smart cards has expanded each year to include applications in various markets and disciplines. In recent years, the information age has introduced various security and privacy issues that have called for advanced smart card security applications **[6].**

For online banking payments, new display cards are available. They come with an LCD and optionally with a keypad. The cards store information, money, and/or applications that can be used for: banking/payment, loyalty and promotions, access control, identification, ticketing, parking and toll collection **[6].**

An electronic ID (e-ID) card fulfills various roles: it acts as a traditional means of identification, as a travel document, and finally, as a passkey to citizen's data.
Many international regulations and standards have been established on e-ID, most of which are applied by States **[6].**

National ID cards are now also being used to access an array of services that were previously difficult to synchronize. Health cards, including a microprocessor, also act as a **significant component of an IT system.** They identify the holder and his/her affiliation to an organization and verify his/her rights. These cards are widely used. Every French and German citizen has a smart card for health insurance. Unlike paper documents, which can easily be forged, these tamper-proof devices are challenging to reproduce or unlawfully manipulate **[6].**

Migration to electronic passports has been in progress since 2005. Over 1 billion e-passports are now in circulation, and more than 150 states have started issuing this new type of travel document in mid-2019. The electronic passport integrates smart card technology with a microprocessor that stores a digital version of the ID photo and all of the ID data found on the paper passport's first page. The ICAO International Civil Agency Organization) 9303 standards have been vital for the international deployment of biometric identification and electronic data storage in so-called machine-readable travel documents (MRTDs) **[6].**

4. Chip Cards Construction and Organization

A smart card can be categorized as either memory card or a processing-enabled card. A memory card is the simplest form of a smart card. Such a card provides limited capability to securely store personal information. (According to a smart card manufacturer, the currently available memory for memory cards ranges from eight bytes to 2KB, while traditional magnetic stripe-based cards can store approximately 220 bytes of information.) The storage on a memory card is nonvolatile memory. Such cards are sometimes referred to as “asynchronous cards,” since they are used offline and their associated flow of data is essentially one-directional: value on the card is moved to the reader (and/or the vendor’s computer system). These are simple prepaid cards, which transfer the electronic equivalent of cash to a vendor’s digital cash register. Transactions can then be directed to traditional bank account. Europe’s phone card was the predecessor of this type of smart card. More sophisticated cards

are the processor-enabled smart cards, some refer to as “true” smart cards, which are based on semiconductor technology **[3].**

4.1 Hardware Structure of Chip Cards

A smart card is a piece of plastic, similar to the size of a credit card, in which a single chip microcontroller is embedded. Usually, microcontrollers for cards contain a microprocessor and different kinds of memories: RAM (for run-time data), ROM (in which the operating system and the basic applications are stored), and EEPROM in which the persistent data are stored). Since there are strong size constraints on the chip, the amounts of memory are small. The ROM is masked in the chip and can not be changed during the whole lifetime of the chip card. The EEPROM permanently stores data that can be read but also modified during the lifetime of the card. The RAM is volatile memory that keeps data needed for processing performed by the chip's microprocessor during one card session **[8].** The memory management unit MMU controls the access to these memories **[9].**

The chip is connected to outside world through five contacts, which are assigned as follows: the chip input/output serial line for communicating with the outside world (I/O), the electrical power for the chip two contacts (V_{CC} and GND), the synchronization clock (CLK), and the reset signal from the terminal, which brings the chip on an initial status (RST). The single-chip computer is a slave depending on the terminal, which can be regarded as a master. The chip does not take initiative, but simply driven by the terminal.

4.2 Software Architecture of Chip Cards

At the beginning, in the mid of the 1980’s, a typical smart card had 6 Kbytes ROM, 128 Byte RAM and 3 Kbytes EEPROM. Thus, program written in assembler were developed directly upon the physical layer of the card. Particularly the development of I/O routines for communicating to the terminal is a rather time intensive task. For that reason, these functions were typically included into libraries to prevent programmers from writing every application from scratch. Because of the known advantages of reusing code during the years, more functions were added to these libraries that were of course optimized to the properties of a special micro-controller. This library-oriented approach is known as the first generation of smart card operating system **[10].**

The second generation of smart card operating systems were monolithic which provide an interface to hardware and I/O having more general functionality than library-based system. Monolithic operating system did not have the property of modularity. Thus, although it was easier to run application on different cards, porting operating systems remained a serious problem. During the 1990’s smart cards became a widespread digital device and the portability became an important issue. The wish for open standards and higher compatibility and modularity led to the development of smart card operating system of third generation, which overcome the mentioned problems **[10].** However, SW architectures of smart cards can be classified as: proprietary SW organization and non-proprietary SW organization.

The proprietary SW organization does not allow for the portability of card applications. It can be seen that the card application makes direct call to either a proprietary application programming interface API or to card's native operating system. Since each ICC producer has its own operating system and its proprietary API, the card application is not portable from one chip card to another. Every time an issuer changes the chip card producer, the card application has to be rewritten. The operating system and proprietary API are masked in the ROM, whereas the card application can reside either in the ROM or in the EEPROM. In the majority of the proprietary card implementation, however, the card application physically resides in the ROM and logically integrated in the operating system instead of being on top of OS. The card file system that contains the data structures needed during the processing performed by the card application is always kept in the EEPROM, since both read and write operations must be available on the permanently stored data **[9].**

Non-proprietary SW organization can, further, classified as Java card, Multos, or more recently smart card for windows **[5].**

In the Java card SW organization, the code of the card application is isolated from OS libraries through the Java Virtual Machine JVM. The JVM interprets the byte code corresponding to the java source of the card application and translates it into instructions that are executable by the HW and native OS. Each chip HW platform has its own JVM, which allows the card application to be independent of the HW and the native OS of the card. Thus this SW organization guarantees the interoperability of the card applications written for different chip card platform **[9].**

The actual competitor of the Java card is the MULTOS OS for chip cards, in which the card applications are coded using the MULTOS executable language, MEL, which is an interpreted language that is hardware-independent. The MULTOS architecture bases its functionality on a MEL interpreter, which can be regarded as a virtual machine, and an application loader. Generally there is a distinction between off-card and on-card virtual machines. In contrast to the Java card, the MULTOS virtual machine is completely realized on-card. This allows implementing firewalls between the applications, which provides a suitable security level for multi application environments. The application loader ensures the possibility of secure loading and deletion of card applications to and from the EEPROM, even during the utilization life stage of the card **[9].**

4.3 Card File system [9]

The operating system of the chip card manages a file system that stores the data needed by each card application. Two categories of files are supported: dedicated files DFs and elementary files EFs. They are organized in a hierarchical tree, with DF as branches and EF as leafs.

The highest DF in the hierarchy, which is the root of the tree, also called the master file MF, is the only mandatory DF in the file system organization. A dedicated file can be seen as a container for data belonging to one card application. Application control information and cardholder financial data are stored in the elementary files composed in the same DF. Each DF may contain cryptographic keys for

implementing various security services, and each may have its own application PIN, which can be used to refine the access mechanism of multi-application card.

The referencing of a DF in the card's file system, which corresponds to the possibility of selecting card application from the terminal's side can be performed in two distinct ways: with a fixed file identifier FID or Referencing with an application identifier AID.

The data elements of a card application are encoded in elementary files EF, which can be further subdivided into working and internal EF. Cryptographic parameters used for security services provided by the card as well as the cardholder's PIN or other cardholder verification codes CHVs are stored in internal EF.

Two referencing methods for elementary files are used: with an FID or with a short File Identifier SFI, which consists of a number between 1 and 30 that can be encoded on 5 bits.

The structure of an EF depends on its intended use. An EF can have one of four types: Transparent files which consists of a sequence of bytes. Linear fixed file which consists of a number of fixed length records. Linear variable files which consists of a number of variable length records. Cyclic files, which contains records of fixed length organized in a ring structure.

The file header of each EF stores information about the type of EF file structure, the size of the file, the possible actions to be performed on the file and the access conditions under which the terminal application can perform that action.

4.4 Command and Response Format

In accordance with the ISO 7-layer model, the transactions exchanged between the card and the terminal can be divided into three protocol sections. *The physical layer protocol (layer 1),* corresponds to the electrical signals on the I/O contact of the card. *The data transmission protocols (layer 2)*, corresponds to T=0 and T=1 protocols. They are both asynchronous, half-duplex protocols. T=0 is a byte-oriented transmission protocol of the first-generation chip, while card T=1 is a block-oriented protocol, which better respects the OSI reference model and allows transmission of data both in the command and in the response. *Application protocols for command and response data (layer 7)*. A step in an application protocol consists of sending a command application protocol data unit C-APDU from the application to the card application. The later processes it and sends back the response application protocol data unit R-APDU to the terminal application. Figure 4-1 shows the formats of C-APDU and R-APDU **[9].**

4.5 Card Application and Terminal Application Interactions

The terminal at the point of service is a card acceptor device equipped with a chip card reader, which is often referred to as the Interface Device IFD. The terminal interacts with an ICC according to the client server model, in which a client application runs in the terminal, referred to as the terminal application and a server application runs in the ICC, referred to as the card application

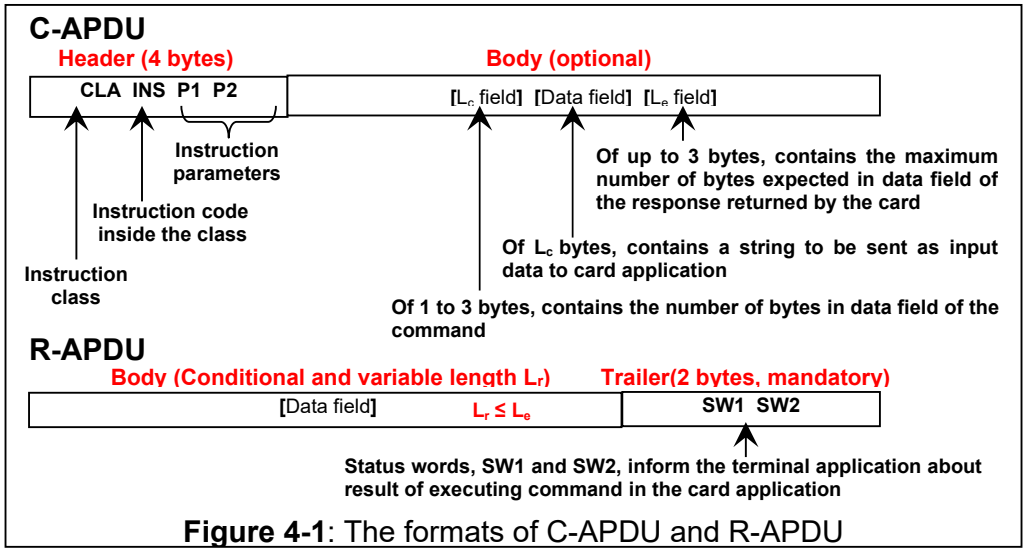

Figure 4-1: The formats of C-APDU and R-APDU

5. Security of Smart Cards [11]

Smart card is characterized by its high security applications, so it is often used to prove identity, control access to protected areas, or guarantee payments. The reason for its high security is due to the fact that the users of the system are given access to the smart card. Some components that play a role in smart card security: human-readable security features, security features of the smart card chip, security features of the operating system, and security features of the network.

Human Readable Security Features of Smart Cards

Smart card includes human readable security identifiers. Smartcard falsification is prevented by features. The data in the card do not protected by this features, but abuse of the card as badge identification are prevented by features**.** Some of such features can be: Photo lamination, Signature strip, Hologram, Micro Printing, Embossing, Security Patterns, and Laser Graver.

Security Features of the Smart Card Chip

The microcircuit of the smart card is tested during the production for the security features of the chip. After testing the chip, it is converted to a specific mode. Accessing the internal chip circuit is impossible for this mode. For example outsiders can't access the memory directly. For example with interchange the conductor; deducing the function is impossible for firms. The connections between on-chip elements are encrypted. There are circuits in smart card which can detect external tampering. The circuit detects too high and too low supply, too high or too low external clock frequency and too low an operation temperature.

Security Features of the Card Operating System

Access to smart card files can be protected with a Personal Identification Number (PIN) or with cryptographic keys. PIN protected card access to different areas of memory, functions in the card multi-programmable smartcards to help safeguard lost and stolen smartcards against potential abuse. When a pin isn't entered correctly then after number of attempts, which is setting by issuer of smartcard, the smart card is deactivated**.**

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. Placing the smart card reader and communications link in a secured environment can physically protect them.

There are several reasons one requires security in a smart card system. The principles being enforced are namely; Privacy, Non-repudiation, Authentication, Integrity, Verification. Smart cards use different encryption algorithms to implement these principles. In some cases a single mechanism can provide a number of security services.

5.1 Privacy

It is the act of ensuring the nondisclosure of data between two parties to a third party. [18]. Symmetrical cryptography and asymmetrical cryptography are used to assure privacy. Single, standard, algorithm will be used. For symmetric key cryptography this will almost certainly mean DES (FIPS 46-3**)** or maybe triple DES (ANSI X9.17**)** and for asymmetric cryptography the typical algorithm of choice will be RSA**.** In the future there might be moves towards using the AES (FIPS 196**)** as a replacement for DES, but this is not likely any time soon.

In symmetric-key cryptography, encrypting plain text into enciphered text and decrypting enciphered text back into plain text, an encryption key (referred to, also, as secret key or single key) is used. It means to encrypt and decrypt the message the same key is used. DES is utilizable on smart card software and it is fast algorithm (FIPS 46-3**).** The only disadvantage is the encryption key exchange. To overcome such disadvantage, the DES key is stored on the card at personalization time.

Asymmetric-key cryptography appeared in 1976, to overcome the above disadvantage in symmetric-key. The idea is to replace the single encryption key in symmetric-key into two different keys, one is the inverse of the other; one public known to everyone and another private kept secret. It was first proposed in an article by W. Diffie and M.E. Hellman entitled “New Directions in Cryptography”. This idea has since become known as asymmetrical cryptography. The public-key is used to encrypt the plain text and the private to decrypt the enciphered text. The keys are mathematically related. The best-known asymmetrical cryptographic algorithm is RSA**.**

The credit card companies use asymmetrical cryptography for authentication purpose. It uses rarely to perform the data encryption .also the symmetrical cryptography is used to this aim. For send the des key securely from one partner to another the asymmetrical encryptions is often used. If the Des key is known by both partners transmission of data is symmetrically encrypted. This act improves the performance.

5.2 Integrity

Integrity assures that only those authorized can access or modify the information. Cryptographic techniques insures the correctness of message transmitted from the sender to the receiver. It is referred to as data integrity. A data integrity service guarantees the correctness of content of message which we sent**.**

One-way cryptographic algorithm is used to uniquely define the sent message, since it cannot be reversed and guarantee the uniqueness of the enciphered message. It is referred to as the message Mac. DES using a key calculates the Mac in smart cards. Both the smartcard and smart card reader share it.

Before the message being sent, the Mac is attached at the end of plain text message. When message is received, the Mac value is calculated and compared by recipient. The Mac changed in an unforeseen way if even one character in the message is changed. That way Mac ensures the recipient that massage hasn't been tampered.

5.3 Non-Repudiation

Non-repudiation confirms that the origin of data is exchanged in transaction. Like that, transaction never could be denied by the sender or by the receiver. Non-repudiation of the transaction is ensured by cryptography. This can be achieved by the application of digital signature**.**

5.4 Authentication

Authentication is the process which specifying identity of the sender. In fact it specifies that someone or something is who or what it is claims to be. This service protect against a lot of threats such as impersonation and man-in-middle.

5.5 Verification

Confirming the identity of cardholder is the useful act before using a card. If two parties want to start business, they must be assured of identify of another party. For recognizing other parties visual and verbal clues can help us. Encryption technology is used to verify that another person is who to pretend to be. This can be insured by means of the PIN codes and the biometrics.

PIN consists of four- or five-digit numbers this number attaches to smart card. Cardholder memorizes this number. PIN is saved safely. Until accessing from the external world is allowed, data and functions on the smartcard can be protected. Biometric is the technology of measuring personal features. Users are reluctant to memorize passwords and pin numbers. This reluctance is one of the driving forces behind the development of biometric. Also, many people can share pin numbers then it is not uniquely but biometrics can specify the real person because it is unique. Some of the biological features that can be measured are: signature, fingerprint, voiceprint, hand geometry, eye retina, and facial recognition.

One of the important services, in smart cards, is Mutual Authentication. When smart card put into smartcard reader, they verify to identify each other automatically**.** For example, Bob sends a number to Alice. Alice needs to use DES key to encrypt the number then Alice returns back the enciphered text to Bob. Enciphered text is decrypted by Bob and Bob compares this number with the number that he sent. If they be the same then Bob understands that the same key is shared by Alice**.**

6. Authentication/Authorization Oriented Smart Cards Application

The rapid progress of networks facilitates and connecting huge number of computers together allows the exchange of great information and share system resources, leading

to the need to protect such computer networks. Recently, based on various techniques, many password authentication schemes using smart cards have been proposed by some researchers. These schemes can allow a legal user to login to remote server and access its facilities **[12].** Accordingly, entity authentication is one of the most important security services that can be applied by smart cards. It is necessary to verify the identities of the communicating parties when they start a connection **[13].**

As the authentication and authorization are two essential functions of access control in computer networks, authorization plays an important role in securing computing system resources from unauthorized access. Authentication is the means of verifying the identity of a user or entity. Authorization is the means of determining whether a user or entity is permitted to perform a particular operation. An authorization service has been introduced **[14]** that include a method for allocating privileges to an entity, and also provide an access enforcement function to ensure access is provided only if the privileges satisfy the access decision rules. Authorization schemes can employ smart cards that can allow users to access resources directly with the preloaded authorization credentials and eliminate the repeat of user authentication in every access as in the traditional mechanism.

7. Smart Cards Standards

Standards help ensure smart cards can be read by any retailer equipped with a smart card reader **[3].** Smart objects, in general, need to fulfill a set of standard requirements such as controllability, maintainability, scalability, Interoperability, Security and privacy, and reliability **[15].**

Primarily, smart card standards govern physical properties, communication characteristics, and application identifiers of the embedded chip and data, whereas, application-specific properties are being debated with many large organizations and groups proposing their standards. Open system card interoperability should apply at several levels: the card itself, the card's access terminals (readers), the networks and the card issuers' own systems. Open system card interoperability will only be achieved by conformance to international standards **[16][17].**

Several organizations have participated in issuing smart card standards, such as: ISO, FIPS, EMV, CEN/ETSI, HIPAA, and PC/SC.

ISO - International Standards Organization facilitates the creation of voluntary standards through a process that is open to all parties. The ISO/IEC 7810 ID-1 standard defines, in particular, the usual size of an ID card **[6].**
ISO 7816 is the international standard for integrated-circuit cards that use electrical contacts on the card, as well as cards that communicate with readers and terminals without contacts, as with radio frequency (RF/Contact less) technology. ISO/IEC 7816 is an international standard related to electronic identification cards with contacts, especially smart cards, managed jointly by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC**[6])**

ISO/IEC 14443 defines the standard for contactless cards **[6].**

Other sort of standards has been issued by FIPS. FIPS, the abbreviation of Federal Information Processing Standards, are designed to protect federal assets including computer and telecommunications systems. The FIPS standards apply to smart card technology and pertain to digital signature standards, advanced encryption standards, and security requirements for cryptographic modules.

Meanwhile, Europay, MasterCard and Visa formed EMV Company, created the "Integrated Circuit Card Specifications for Payment Systems". These specifications are related to ISO7816 and create a common technical basis for card and system implementation of a stored value system.

On the other hand, Microsoft proposed and implemented standard for cards and readers, called the PC/SC specification. They have also built into their CryptoAPI a framework that supports many security mechanisms for cards and systems. PC/SC is now a fairly common middleware interface for PC logon applications. The standard is a highly abstracted set of middleware components that allow for the most common reader card interactions.

The Health Insurance Portability and Accountability Act, abbreviated as HIPAA, adopts national standards for implementing a secure electronic health transaction system in the U.S.

8. Conclusions

The rapid diversion of networks facilitates the more and more need to a portable, secure, and efficient smart object, like smart cards, that can be used to facilitate the efficient utilization of the wealth of information stored and distributed over the various applications.

The smart card has a microprocessor or memory chip embedded in it that has the processing power to serve many different applications when coupled with a smart card reader **[6].**

On the other hand, smart cards as a portable, efficient, small computer can be employed to evolve such applications and services. The introduction, on the other hand, of the biometrics as a part of the smart card increases its capabilities and expands the range of applications and services that can be utilized. Meanwhile, existing applications and services can be enhanced through the utilization of the progressive smart card introduced new capabilities.

In the form of **credit cards** and **SIM cards, smart cards** are the most common form of IT processing power on the planet. It's is estimated that between 30 to 50B smart cards are in circulation today **[6].**

Smart credit cards mediate daily transactions worth trillions of dollars, while, SIM cards facilitate billions of conversations that bind together our social and economic worlds **[6].**

As a **National eID card**, **residence permit,** or **electronic passport**, smart card technology offers more robust identification and authentication tools for both authorities' and citizens' benefits. As a driver's license or a tachograph card, the technology contributes to road safety **[6].**

2020-2021 market share [2021 Thales Group] shows that Telecom (SIM cards) accounts for 52% of the total market, Payment and banking cards for 34%, Government (eIDs and e-passports) and healthcare for 4%, Device manufacturers for 5%: mobile phones, tablets, navigation devices, and other connected devices, including an embedded secure element without SIM application, and Others for 5%: cards issued by operators, for transport, toll or car park services; cards for pay-TV; physical and logical access cards [6].

In this paper we have introduced smart cards as an efficient smart object. A wide band of smart card services and applications are introduced, while it is still expected that such services and applications are spreading.

References

[1] **Hendry, Mike (2007).** Multi-application Smart Cards: Technology and Applications. 2nd ed. UK: Cambridge University Press.

[2] **Mitra, Arami, Monika, Koller, & Robert, Krimmer (2004).** User acceptance of multifunctional smart cards. In proceeding of: Proceedings of the 13th European Conference on Information Systems, The European IS Profession in the Global Networking Environment, ECIS 2004 Proceedings, 80-88.

[3] **[2]** Katherine M. Shelfer and J. Drew Procaccino, “Smart Card Evolution”, Communications of ACM, Volume 45, Issue 7, ACM Press, July **2002**.

[4] **[3]** Jarunee Wonglimpiyarat, "Strategies of Competition in the Bank Card Business, Innovation Management in a Complex Environment", Sussex Academic Press, **2003**.

[5] **[7]** Pierre Girard, “Which Security Policy for Multi-application Smart Cards?”, Proceeding of USENIX Workshop on Smartcard Technology, pp. 21-28, Usnix Association, **1999**.

[6] https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/smart-cards-basics Last updated: 04 June 2021, Thales Group

[7] **Loo, W.H., Yellow, Paul, H.P. & Chong, S.C. (2009**). User Acceptance of Malaysian Government Multipurpose Smart Card Applications. Government Information Quarterly, 26 (2), 358-367.

[8] **[5]** Gilles Grimaud, Jean-Louis Lanet, and Jean-Jacques Vandewalle, @ACM SIGSOFT Software Engineering Notes, Proceedings of the 17th European Software Engineering Conference held jointly with the 17th ACM SIGSOFT International Symposium on Foundations of Software Engineering

ESEC/FSE-7, Volume 24, Issue 6, Springer-Verlage, ACM Press, October, **1999**.

[9] **[4]** Cristian Radu, "Implementing Electronic Card Payment Systems", Artech House, Inc., **2004**.

[10] **[6]** Felix Pletzer, "Architecture of a Portable Smart Card Operating System", 17th May **2004**

[11] **[HSN 2011]** Hamed Taherdoost, Shamsul Sahibuddin & Neda Jalaliyoon International Journal of Security (IJS), Volume (5) : Issue (2) : 2011

[12] **[11]** Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Peng Yang, "A Flexible Remote User Authentication Scheme Using Smart Cards", ACM SIGOPS Operating Systems Review, Volume 36, Issue 3, ACM Press, July **2002**.

[13] **[12]** B . Schneier, Applied cryptography, John Wiley & Sons, Inc., **1996**.

[14] **[14]** Richard Au, Mark Looi, and Paul Ashley, "Cross-Domain One-Shot Authorization using Smart Cards" , Proceedings of the 7th ACM Conference on Computer and Communications Security, ACM Press, November **2000**.

[15] **[8]** Craig W. Thompson, "Smart Devices and Softcontrollers", IEEE Internet Computing Journal, P.P. 82-85, January/February **2005**.

[16] **[9]** EMVCO, EMV2000 Integrated Circuit Card Specification for Payment Systems, BOOK 1 - Application Independent ICC to Terminal Interface Requirements, Version 4.0, December, **2000**, http://www.emvco.com/Specifications.cfm.

[17] **[10]** EMVCO , EMV2000 Integrated Circuit Card Specifications for Payment Systems, Book 4 - Cardholder, Attendant, and Acquirer Interface Requirements, Version 4.0, December, **2000**, http://www.emvco.com/Specifications.cfm.