Smart Card Technology: Past, Present, and Future

L. A Mohammed, Abdul Rahman Ramli, V. Prakash,
*and **Mohamed B. Daud****

Department of Computer and Communication Systems Engineering
*Department of Biology and Agricultural Engineering
43400, UPM Serdang Selangor, Malaysia
e-mail: auwala@hotmail.com

Abstract

Smart Cards are secure portable storage devices used for several applications especially security related ones involving access to system's database either online or offline. For the future of smart card to be bright, it is important to look into several aspects and factors especially those resulted due to the rapid advancement in information and communication technology. This paper looks into current trends in smart card technology and highlights what is likely to happen in the future. Moreover, the paper addresses other aspects in order to identify the core concepts that are of interest to smart card developers and researchers. More emphasis is given to four key characteristics of smart cards: portability, security, open platform, and memory management, as they are believed to be at the heart of many smart card applications.

1. Introduction

Smart card is one of the greatest achievements in the world of information technology. Similar in size to today's plastic payment card, the smart card has a microprocessor or memory chip embedded in it that, when coupled with a reader, has the processing power to serve many different applications. As an access-control device, smart cards can be used to access server remotely over the Internet and they can make personal and business data available only to the appropriate users. Smart cards provide data portability, security, convenience and the like. According to Gemplus (ref. [19]), smart cards can be categorized into the following:

Memory and microprocessor- Memory cards simply store data and can be viewed as a small floppy disk with optional security. A microprocessor card, on the other hand, can add, delete and manipulate information in its memory on the card.

Contact and contactless - Contact smart cards are inserted into a smart card reader, making physical contact with the reader. However, contactless smart cards have an antenna embedded inside the card that enables communication with the reader without physical contact. A combi card combines the two features with a very high level of security.

Smart cards help businesses evolve and expand their products and services in a changing global marketplace. The scope of uses for a smart card has expanded each year to include applications in a variety of markets and disciplines. In recent years, the information age has introduced an array of security and privacy issues that have called for advanced smart card security applications.

The rest of the paper is organized as follows; the next section briefly discusses the history of smart card development and the current and future market analysis. Section three looks into some application areas, their limitations and strengths. This section addresses the future directions of smart card technology giving more emphasis to security consideration and memory management among others. The section also discusses some areas that need further studies in order to improve the current state of smart cards so that they can fit into the future needs. Like smart cards, biometric is also an approach used in identification protocol. Section four deals with comparison between the two schemes. Finally, the paper concludes in section five.

2. Historical Perspective

Smart card was invented at the end of the seventies by Michel Ugon (Guillou, 1992). The French group of bankcards CB (Carte Bancaire) was created in 1985 and has allowed the diffusion of 24 million devices (Fancher, 1997). For the physical characteristics the first draft proposal was registered in 1983. A long discussion resulted in the standardization of the contact location. Next was the standardization of signals and protocols which resulted in standards ISO/IEC 7816/1-4. Logical security came next, as it was clear from the beginning that there was a need for cryptographic capabilities, though this was a bit difficult due to the limited computing power and the few bytes of RAM available at that time (Quisquater, 1997). Nowadays, smart cards are used in several applications.

A survey completed by Card Technology Magazine (http://www.cardtechnology.com) indicated that the industry had shipped more than 1.5 billion smart cards worldwide in 1999. Over the next five years, the industry will experience steady growth, particularly in cards and devices to conduct electronic commerce and to enable secure access to computer networks. A study by Dataquest in March, 2000, predicts almost 28 million smart card shipments (microprocessor and memory) in the U.S. According to this study, an annual growth rate of 60% is expected for U.S. smart card shipments between 1998 and 2003. Smart Card Forum Consumer Research, published in early 1999, provides additional insights into consumer attitudes towards application and use of smart cards. The market of smart card is growing rapidly due to its wide range of applications. The worldwide smart cards market forecast in millions of dollars and millions of units as shown in figure 1:

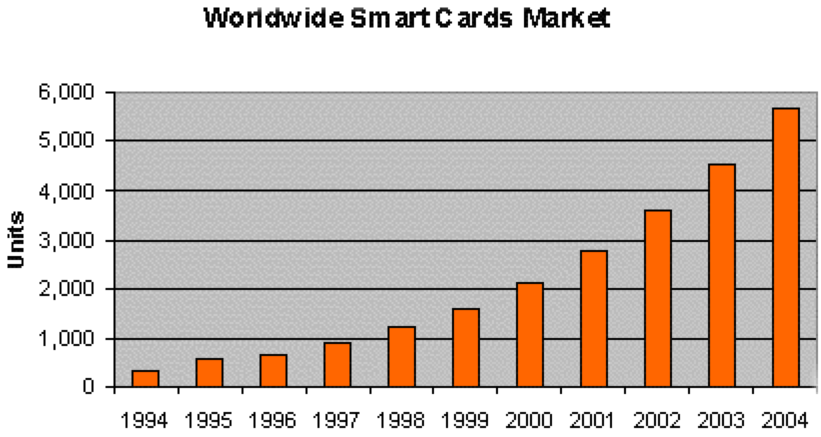

Figure 1. Smart card Market (Source: www.smartcardcentral.com)

3.1 Memory Management

Smart card is a device with major hardware constraints: low-power CPU, low data rate serial I/O, little memory etc. Today, card technology utilizes 8 bit processors (mainly of the 6805 or 8051 family) whose memory sizes are about a few tens of kilobytes (Urien, 2000), typically 1-4 kb RAM (Random Access Memory), 32-128 kb ROM (Read Only memory) and 32-64 kb EEPROM (Electrically Erasable Programmable Read Only Memory) at least, with options on FLASH and FRAM (Ferroelectric Random Access Memory) as well. As the demand for smart cards matures, the standard memory of 32 or 64 KBytes can prove a serious limitation. A solution to this is to look at some of the design issues and techniques to incorporate multiple memory chips in a single smart card. Gemplus had already produced a twin card, incorporating two unconnected chips in a single card. Other approaches include the use of PC in conjunction with smartcard. For instance, Blaze (1996) proposes the use of a powerful PC with a smart card for symmetric key encryption because the PC provides higher encryption bandwidth. Table 1 below shows storage capacity needed for various communication rates.

Table 1: Communication rate and storage capacity

	Communication rate	**Storage capacity**
P C (Pentium IV)	120 Mbps	10 GBytes
Standard smart card	9600 bps	64 Kbytes
Multiple chip card	20 Mbps	224 Mbytes

According to Junko (2002), the EEPROM used in current smart cards is reaching its scalability limits, particularly for smart card devices built in 0.13-micron technology and beyond. For this reason, companies like Philips agree on the need for alternative non-volatile memory for future smart cards. Currently Philips is leaning toward magnetic RAM as an alternative to EEPROM.

Another important application that requires memory management is the application of biometrics. The use of biometrics within the card itself will mean that biometric features (fingerprint, retina, voice etc) can reliably identify a person. With enhancement in memory system, it will soon be possible to authorize the use of electronic information in smart card using a spoken word. The use of some of these features has already been implemented in many applications. Malaysia's national ID, for instance, is a multipurpose smart card with a fingerprint biometric. The card is first of its kind in the world as it combines many applications such as driving licence, passport, healthcare, and non-government applications such as an e-purse. (See http://www.jpn.gov.my/ or www.iris.com.my for details). Table 2 below gives the required bytes for various biometrics. Additional information about biometric technology and standards can be found from the following organisations: The Biometric Consortium (www.biometrics.org), International Biometric Industry Association (www.ibia.rg), or BioAPI Consortium (www.iapi com).

Table 2. Required Bytes for Biometrics

Biometric	Bytes Required
Finger scan	300-1200
Finger geometry	14
Hand geometry	9
Iris recognition	512
Voice verification	1500
Face recognition	500-1000
Signature verification	500-1000
Retina recognition	96

Source: Smart Card Alliance

3.2 Security Issues

Security is always a big concern for smart cards applications. This naturally gives rise to the need for reliable, efficient cryptographic algorithms. We need to be able to provide authentication and identification in online-systems such as bank machine and computer networks, access control, and the like. Currently, such facilities allow access using a token; however, it is vital that the holder of the token be the legitimate owner or user of the token.

As smart card is handicapped or highly restricted in their input/output (unable to interact with the world without outside peripherals), this leads to the involvement of many parties in its applications. Some of the parties involve: Cardholder, Data Owner, Card Issuer, Card Manufacturer, Software Manufacturer, and Terminal Owner as mentioned in (Schneier, 1999). It is therefore essential to ensure that none of the above mentioned parties is threat to one another. To achieve this, there is need for further investigation in the design and analysis of smart card authentication and identification protocols. For this reason, Gobioff (1996) proposes that smart cards be equipped with "additional I/O channels" such as buttons to alleviate these shortcomings. Further, there are numerous intrusion techniques able to tamper with smart cards and other similar temper-resistant devices as presented in (Anderson, 1997). This also indicates the need for effective intrusion detection/prevention techniques.

3.3 Open Architecture

Existing smart card standards leave vendors too much room for interpretation. To achieve wider implementation, there is need for an open standard that provides for inter-operable smart cards solutions across many hardware and software platforms. *Open Platform*, as defined by GlobalPlatform (www.GlobalPlatform.org) is a comprehensive system architecture that enables the fast and easy development of globally interoperable smart card systems. It comprises three elements; card, terminal and systems, each of which may include specifications, software and/or chip card technology. Together these components define a secure, flexible, easy to use smart card environment. Development environment in use today include; Java, Visual C, Visual Basic, C++, and the like.

The development of standards like GSM, EMV, CEPS, PC/SC, OCF, ITSO and IATA 791 represents an opportunity for manufacturers to produce products on an economic scale and give stability to systems designers. According to a report by DatacardGroup (White paper version 1.0), True 'open' smart cards will have the following characteristics:

- They will run a non-proprietary operating system widely implemented and supported.
- No single vendor will specify the standards for the operating system and the card's use.
- The cards will support a high-level application programming language (e.g., Java, C++) so issuers can supply and support their own applications as well as applications from many other vendors.
- Applications can be written and will operate on different vendor's multi-application smart cards with the same API (Application Programming Interface).

To overcome the problem of lack of standardization, U.S. organizations have developed an add-on piece of smart card software meant to overcome communication problems between chip cards and readers from different vendors. They would like to see this technology, which they call a "card capabilities container," used worldwide, making it an industry standard that would allow U.S. agencies to buy cards and readers from many vendors, sure that they would work together (Cathy, 2002). Another move is the development of a new organization called Smart Card Alliance, formed by Smart Card Industry Association (SCIA) and Smart Card Forum (SCF) to act as a single voice for the US smart card industries.

Even in biometrics, each vendor has its own methods for enrolling individuals and later checking someone's identity against the stored image. However, there are efforts underway to create biometric standards, largely driven by the U.S. government. In a major step, the American National Standards Institute approved BioAPI as a standard way for biometric devices to exchange data with ID applications. ANSI now is preparing to propose BioAPI to ISO for adoption as an international standard (Donald, 2002).

3.3.1 Operating Systems

Today's smart card operating systems and application frameworks are intrinsically local and monoapplication. Moreover, smart card communicates with the outside world through a serial link. As the chip has a single bi-directional I/O pin, this link can only support half-duplex protocol. The majority of chips work at the speed of 9600 baud, although the ISO standard 7816 has defined a maximum data rate of 230400 baud. A new type of SPOM (Self-Programmable One-Chip Microcomputer), named ISO/USB has been introduced in 1999; it provides a direct connection between a SPOM and the terminal via an USB port (Urien, 2000). According to USB specifications, a data throughput from 1.2 to 12 Mbit/s may be obtained between the chip and the terminal.

The vision of smart card as an application platform rather than a simple security token is a paradigm shift for smart card operating systems. According to Jurgensen (2002), the current operating system model cannot completely support the needs or the vision of Universal Integrated Circuit Card (UICC). The move is now towards the development of Next Generation Smart Card Operating Systems (COSng), which will able to handle multi-applications and support future requirements.

3.4 Performance

Performance and speed are very important factors that need to be considered in most smart card application. To achieve this, transistor scaling or the reduction of the gate length (the size of the switch that turns transistors on and off), must be taken into consideration. This idea not only improves the performances of chips but also lowers their manufacturing cost and power consumption per switching event. Recently, IBM have built a working transistor at 6 nanometres in length which is per beyond the projection of The Consortium of International Semiconductor Companies that transistors have to be smaller than 9 nanometres by 2016 in order to continue the performance trend.

The ability to build working transistors at these dimensions could allow developers to put 100 times more transistors into a computer chip than is currently possible. The IBM results will lead to further research into small, high-density silicon devices and allow scientists to introduce new structures and new materials. Details are available from IBM Research News 9th December 2002, available online: http://www.research.ibm.com/.

3.5 Reader Requirements

As the needs and uses of smart card increases, the need for a Smart Card reader that is not portable, small or light, but also easy to connect and access has arrived. However, some developers like "Browns" (http://www.brownsbox.com/) believe that the need for a reader is a problem, meaning extra expenditure, and, when working with a laptop, is a waste of a port. In view of this, an approach toward a device that can be attached to a PC (internally or externally) has arrived. To solve this problem, Browns developed a method that turns a floppy disk drive into a smart card reader. Another popular approach in Europe is the smarty smart card reader/writer the size of a 3.5-inch diskette by SmartDisk Corp. The device does not require a serial, parallel, or USB port, instead it works directly from a diskette drive. Smarty supports all smart card protocols, including ISO 7816, and it works under different operating systems. Details are available from:

http://www.smartcomputing.com/. This idea of smart diskette was initially proposed by Paul (1989) as shown in figure 3. A similar approach involves the development of keyboard with integrated card reader, and/or keyboard with integrated fingerprint sensor and card reader by "Cherry" (http://www.accesskeyboards.co.uk/cherry.htm).

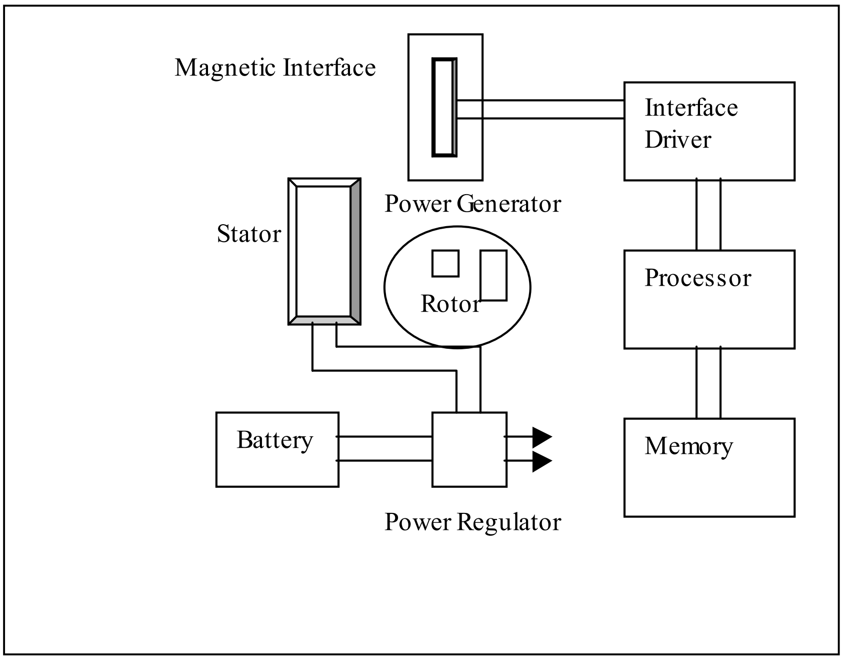

Figure 3. Architecture of Smart Diskette

3.6 Portability

As mentioned earlier, portability or convenience of handling is one of the most important characteristics of smart cards. Since the smartness of smart card relies on the integrated circuit embedded in the plastic card, it is possible that the future smart cards might look like other everyday objects such as rings, watches, badges, glasses or earring because that same electronic function could be performed by embedding it in these objects. What remains is for developers and researchers to look into the best way of implementing it if the need arises.

3.7 Mobile Services

Over the years, continued developments in GSM SIM smart card standards have produced innovations such as SIM Toolkit, which defines how to deliver value-added services to the handset menu system. The latest Javacard SIM Toolkit cards allow the operator to offer handset services including customized stock, weather and traffic information, banking, email, and airline reservations. In Malaysia, companies like Celcom (www.celcom.com.my) are making move towards these services. A new generation of GSM phones are enabled for two card slots and Wireless Access Protocol (WAP) connection to the Internet. The SIM smart card handles identification and handset features, while a second slot can support a multi-application smart card that delivers payment and loyalty application functions.

Going beyond current GSM mobile-phone and banking markets, the smart-card industry is now casting an eye on the home entertainment market: “digital rights management, home entertainment, multimedia applications, 3G mobile messaging, Wi-Fi with smart card security, electronic legal signature and digital authentication" as logical places to extend the reach of smart cards.

4. Smart card Vs Biometric

One of the primary reasons that smart cards exist is for security. The card itself provides a computing platform on which information can be stored securely and computations can be performed securely. Consequently, the smart card is ideally suited to function as a token through which the security of other systems can be enhanced. Most of today’s systems need proper user authentication/identification as it is a crucial part of the access control that makes the major building block of any system’s security. Three methods are currently in use: what the user has (e.g. smart card), what the user knows (e.g. password), and what the user is (biometrics). Each of these methods has it’s own merits and demerits especially when used alone. When a single method is used, we believe smartcard is the best choice. Passwords can easily be forgotten, attacked, and guessed. Similarly, biometric schemes alone are not good enough to ensure user authentication, as they are also vulnerable to attacks. First, we look into some of the benefits in using biometric schemes and then analyze some of their limitations.

The primary advantage of biometric authentication methods over other methods of user authentication is that they use real human physiological or behavioural characteristics to authenticate users. These biometric characteristics are (more or less) permanent and not changeable. It is also not easy (although in some cases not principally impossible) to change one’s fingerprint, iris or other biometric characteristics. Further, most biometric techniques are based on something that cannot be lost or forgotten. This is an advantage for users as well as for system administrators because the problems and costs associated with lost, reissued or temporarily issued tokens/cards/passwords can be avoided, thus saving some costs of the system management.

However, as reported in (Luca 2002), the major risk posed by the use of biometric systems in an authentication process is that a malicious subject may interfere with the communication and intercept the biometric template and use it later to obtain access. Likewise, an attack may be committed by generating a template from a fingerprint obtained from some surface. Further, performance of biometric systems is not ideal. Biometric systems still need to be improved in terms of accuracy and speed. Biometric systems with the false rejection rate under 1% (together with a reasonably low false acceptance rate) are still rare today. Although few biometric systems are fast and accurate (in terms of low false acceptance rate) enough to allow identification (automatically recognizing the user identity), most of current systems are suitable for the verification only, as the false acceptance rate is too high.

Moreover, not all users can use any given biometric system. People without hands cannot use fingerprint or hand-based systems. Visually impaired people have difficulties using iris or retina based techniques. Some biometric sensors (particularly those having contact with users) also have a limited lifetime. While a magnetic card reader may be used for years (or even decades), the optical fingerprint reader (if heavily used) must be regularly cleaned and even then the lifetime need not exceed one year.

Biometric data are not considered to be secret and security of a biometric system cannot be based on the secrecy of user's biometric characteristics. The server cannot authenticate the user just after receiving his/her correct biometric characteristics. The user authentication can be successful only when user's characteristics are fresh and have been collected from the user being authenticated. This implies that the biometric input device must be trusted. Its authenticity should be verified (unless the device and the link are physically secure) and user's likeness would be checked. The input device also should be under human supervision or tamper-resistant. The fact that biometric characteristics are not secret brings some issues that traditional authentication systems need not deal with. Many of the current biometric systems are not aware of this fact and therefore the security level they offer is limited.

User's privacy may be violated by biometric schemes. Biometric characteristics are sensitive data that may contain a lot of personal information. The DNA (being the typical example) contains (among others) the user's preposition to diseases. This may be a very interesting piece of information for an insurance company. The body odour can provide information about user's recent activities. It is also mentioned in (Jain, 1999) that people with asymmetric fingerprints are more likely to be homosexually oriented, etc. Use of biometric systems may also imply loss of anonymity. While one can have multiple identities when authentication methods are based on something the user knows or has, biometric systems can sometimes link all user actions to a single identity.

Furthermore, biometric systems can potentially be quite troublesome for some users. These users find some biometric systems intrusive or personally invasive. In some countries people do not like to touch something that has already been touched many times (e.g., biometric sensor), while in some countries people do not like to be photographed or their faces are completely covered. Lack of standards may also poses a serious problem. Two similar biometric systems from two different vendors are not likely to interoperate at present.

Although good for user authentication, biometrics cannot be used to authenticate computers or messages. Biometric characteristics are not secret and therefore they cannot be used to sign messages or encrypt documents and the like. On the other hand, smart cards provide tamper-resistant storage for protecting private keys, account numbers, passwords, and other forms of personal information. Smart cards can also serve to isolate security-critical computations involving authentication, digital signatures, and key exchange from other parts of the system that do not have a "need to know." In addition, smart cards provide a level of portability for securely moving private information between systems at work, home, or on the road.

A better approach for the usage of biometrics is to combine biometrics with smartcards. The advantages of this may include: all attributes of the smartcards will be maintained, counterfeiting attempts are reduced due to enrolment process that verifies identity and captures biometrics. It will be extremely secure and provide excellent user-to-card authentication.

Conclusion

Most of the smart card systems in use today serve one purpose and are related to just one process or is hardwired to only one application. A smart card cannot justify its existence in this respect. The approach of future smart card is therefore towards designing multi-application card with own operating system based on open standard that can perform a variety of functions. It must be configurable and programmable and it must be able to adapt to new situations and new requirements especially in areas such as security, memory management, and operating system. Most of smart card application methods today rely on the fact that the code of functions to be performed should be imported by card operating system from an outside server. This approach is quite weak with regards to security. It is, therefore, important to find ways of relaxing this requirement so that the card on its own can support all functions and operations. Further, we notice that one of the drawbacks of smart card has been the small amount of non-volatile memory. Since this memory will be used to store keys, cryptographic certificates etc, only applications that require a minimal amount of memory have been implemented. Hence, there is need to do a more thorough investigation of suitable means (such as data compression) of managing the available memory.

Security is very crucial issue in smart card especially due to the various independent parties involve throughout the card's life cycle leading to what is now called "splits" in trust. There is need to develop a method in which even without trust none of the parties can cheat one another. Further, to overcome the lack of security provided by passwords or PINs for authentication and access control, some researchers believe that biometric is the best genuine means of authentication. However, due to the significant amount of processing and memory capacity required by this approach, implementing it in smart card remains difficult. Hence, this area needs to be further evaluated to make it suitable for built-in smart card applications. Other important security issues involve further investigation of elliptic curve and quantum cryptography on smart cards.

In the future, smart cards could handle multiple tasks for their owners, from providing access to company networks, enabling electronic commerce, storing health care information, providing ticketless airline travel and car rentals, and offering electronic identification for accessing government services such as benefit payments and drivers licenses etc. Smart cards of the future may even stop resembling "cards" as smart card technology is embedded into rings, watches, badges, and other forms and factors that will make them remarkably convenient to use. In the near future, we believe all PC's and Network Computers will be integrated with smart card readers. These can be implemented either as part of the keyboard or occupying one of drives or perhaps as an external units. It is hoped that the smart card of the future will be a PC in pocket size with sensors for biometric features and a human interface.

Reference

1. Anderson R., and M. Kuhn, (1997) Low Cost Attacks on Tamper Resistant Devices, *Security Protocol*.

2. Blaze M. (1996), High-bandwidth encryption with low-bandwidth smart cards. In *Proceedings of the Fast Software Encryption Worksho*p, volume 1039 of *Lecture Notes in Computer Scienc*e, pp. 33 – 40. Springer Verlag .

3. **"Breaking the byte barrier", www.gemplus.com/smart/enews/st3/sumo.html Oct-15-2002 14:19, [6/12/02]**

4. Cathy Bowen (2002), Government Smart Card IDs: Lessons Learned**,** *Card Technology Magazine*, November.

5. DatacardGroup, The Transition to Multi-application Smart Cards with Post Issuance Personalization Capabilities, *Datacard White Paper Version 1.0*, May 2001, available online: (www.datacard.com).

6. Donald Davis (2002), Early Steps Toward Biometric Standards**,** *Card Technology Magazine*, November.

7. Fancher C. H. (1997), In your Pocket: Smartcards, *IEEE Spectrum* (February), pp. 47-53.

8. Gobioff et al. (1996), Smart cards in hostile environments. In *Proceedings of The Second USENIX Workshop on Electronic Commerc*e, Oakland, CA.

9. Guillou L. C., et al. (1992), The smart Card: A Standardized Security Device Dedicated to Public cryptology, in G.J. Simmons (Ed.), *Contemporary Cryptology. The Science of Information Integrity,* IEEE Press, pp. 561-613.

10. Jain A, Bolle R. and Pankanti S. BIOMETRICS: Personal Identification in Networked Society. Kluwer Academic Publishers, 1999.

11. Jurgensen T., and Scott Guthery, Smart Cards: The developer's toolkit, Prentice Hall PTR Upper Saddle River, NJ. 2002.

12. Junko Yoshida (2002), Smart-card chips advance as market stalls, *EE Times*, 11 Nov., available online at www.eetimes.com

13. Luca B., et al, (2002), Biometrics authentication with smartcard, IIT TR-08/2002, Online [15/12/02] http://www.iat.cnr.it/attivita/progetti/parametri biomedici.html

14. Paul B., and Raymund E. (1989), The Smart Diskette – A universal token and personal crypto-engine, *Advances in Cryptology-CRYPTO'89*, Lecture Note in Comp. Sc. pp. 74-79, G.Goos and J. Hartmanis (Eds).

15. Quisquater J-J. (1997), The adolescence of smart card, *Future Generation Computer Systems*, pp.13 - 37.

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

17. Secure Personal Identification System: Policy, Process and Technology Choices for a privacy – Sensitive Solution, available online www.smartcardalliance.org [8/9/02]

18. Urien P.(2000), Internet Card, a Smart card as a true Internet node, *Computer Communication,* 23, pp. 1655-1666.

19. What's so smart about smart cards? Available at www.gemplus.com [2/12/02]