Smart Card Evolution

Fernando Ferreira

Departamento de Informática, Universidade do Minho
4710 - 057 Braga, Portugal
fernando.ferreira4@mail.telepac.pt

Abstract. This comunnication describes the state of art in smart-card technology and explores some of the consumer applications currently in use. Smart cards are powerful devices that can be programmed to perform a number of security-related tasks, ranging from user identification to secured network transmissions. New Java and PC/SC smart cards coupled to biometrics provide almost unlimited potential for embedded applications. With operating systems providing native support, smart-card technology will be positioned in a mainstream computer industry tool.

1 Introduction

Smart cards appeared on the horizon when two German inventors, Jürgen Dethloff and Helmut Grötrupp, patented the idea of having plastic cards hold microchips in 1968. The Japanese patented another version of the smart card in 1970 and former French journalist Roland Moreno filed for a patent on the IC card, later dubbed the "smart card," in 1974, and received a first (that is, priority) patent in France in 1975 and a U.S. Patent in 1978.

2 Smart Card Basics

The smart card is one of the latest additions to 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 make personal and business data available only to the appropriate users. Another application provides users with the ability to make a purchase or exchange value. Smart cards provide data portability, security and convenience.

Smart cards offer virtually unlimited application possibilities. Storage capacity is a maximum of 32 kilobytes (KB) per card, but this is more than adequate for storing:

- Personal information
- Electronic purse transactions
- Prepaid telephone transactions
- Personal authentication information
- Personal finance transactions
- Health-care data
- Loyalty program information

Some applications require more powerful smart cards containing memory and logic for handling more complex tasks. Microprocessor smart cards run their own operating system (OS). Programmers can develop complex programs in common programming languages and a known application program interface (API). Special smart-card microprocessor applications can target specific tasks, such as launching a support website configured to a specific user's needs.

3 Smart-Card Variations

Smart cards are composed of an IC, an interface between the IC and card reader, and a body. The IC type, size, and the method of communication differentiate smart cards with the reader. Integrated circuits in a smart card, ICs, provide the logic for specific card applications. The ICs are memory chips or microprocessor chips.

3.1 Memory Chips

Smart-card memory chips are used for data storage and identification applications. Data can consist of any information required for transmitting to a specific application. The main use for memory smart cards is to store keys and certificates for cryptography. Keys function as passwords to secure environments, and certificates verify the authenticity of keys. Memory smart cards are built with EPROM or electrically erasable EPROM chips (see Figure 1). EPROM, which can only be changed once, is often used in prepaid service cards such as telephone calling cards that count off minutes used and then are discarded. EEPROM, which can be changed up to 100,000 times, includes built-in logic that can be used to update a counter in prepaid service cards.

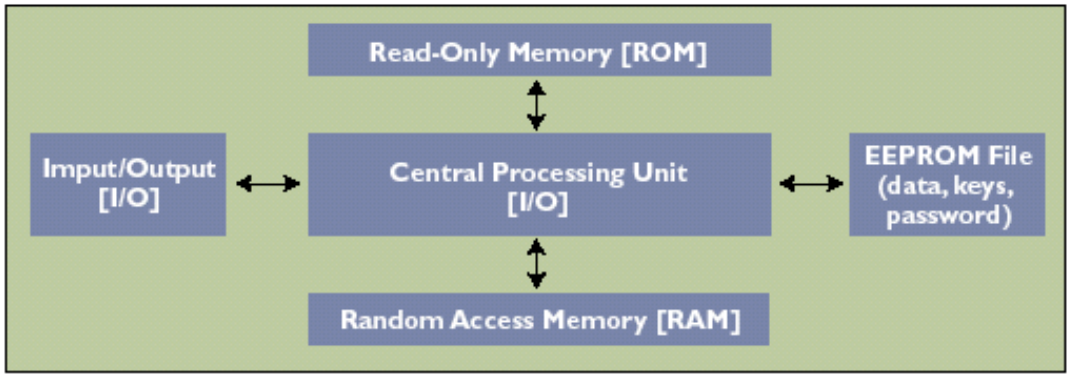

Figure 1. Architecture of a smart card electronic module

The architecture of a memory chip varies (and thus, cost), depending on the application. However, the manufacturer identification (ID) and the application ID fields in the architecture are the same for all memory card chips. The smart-card reader uses these fields to communicate with the card. The application ID includes:

- Card issuer
- Card serial number
- Other user information (depending on the card application)

The serial number is unique for each card. Optional fields on memory chips include counter logic, data, and secret codes or keys. Application developers have options for several memory-card structures to meet design requirements.

3.2 Microprocessor Chips

Smart-card microprocessor chips are smaller, slower versions of the central processing units (CPUs) used in PCs (see Table 1).

Table 1. Smart-Card Microprocessor/PC CPU Comparison

Smart-card microprocessor	PC CPU
8-bit machine	32-bit machine
3.57 MHz speed	Up to 1-GHz speed

Their programming capability provides for many uses. Different applications can even be combined on a single card. Microprocessor smart cards are required for applications that manipulate or compare data, such as public key infrastructure (PKI) data encryption, Java applets, and electronic purses.

Every microprocessor smart card has an OS on the chip to operate the internal functions of the application. The OS loads off of the read-only memory (ROM), much like a basic input/output system (BIOS) on a modern PC.

The primary function of the card OS is to enable memory access. The OS also manages the security functions that these cards typically perform. A microprocessor card, using an OS, has a predefined behavior that allows the card and application to communicate using predefined commands. Smart-card microprocessors use either open-OS or Oslike programs. Open-OS applications are easier to write because software developers use programming interfaces that they already know. The development code is the same code used to write a program for an Intel or PowerPC machine; thus, the learning curve is eliminated.

Three of the open-OS card standards include:

- Microsoft® Windows® for Smart Cards - uses common Microsoft Windows API calls
- Multi-Application Operating System (MULTOS) — developed by the MAOSCO consortium for financial transactions with emphasis on security
- Sun Microsystem Java Technology — provides for dowloading and running Java applets OS-like programs use proprietary software solutions for specific applications that are usually developed by the smart-card manufacturer. Because a developer must learn a proprietary code, the software is initially more difficult to write, but can provide additional security from hackers.

3.3 Smart-Card Dimensions

Two physical dimensions are specified for smart cards. The most popular form is approximately the size of a credit card. Small enough to be conveniently portable, the card is large enough to display graphics and advertising on its side.

The second, smaller smart-card size, specified by the European Telecommunications Standards Institute (ETSI), is used specifically for Global System for Mobile Communications (GSM) phones.

4 Communication with a Reader

A smart-card chip communicates with a reader by direct physical contact or by a radio frequency (RF) signal, depending on the system design. Three smart-card designs for chip-to-reader communications are:

- Contact cards
- Contactless cards
- Combination cards

4.1 Contact Smart Cards

Contact smart cards are the most popular card-connection design, and are used for both card sizes and chip types.

Contact cards use an eight-pin contact, micromodule to physically connect to the card reader. Five pins are defined as Vcc (+5 VDC), reset, clock, ground, and input/output (I/O). Figure 2 shows an example of a typical contact card module.

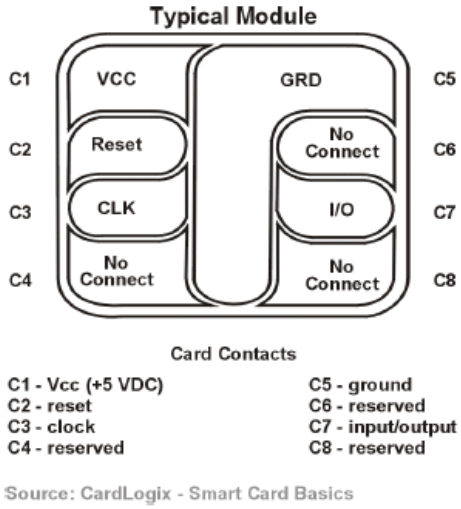

Figure 2. Eight-Pin Micromodule

4.2 Contactless Smart Cards

Contactless smart cards as shown in Figure 3 use an antenna with approximately a 10-centimeter (cm) range to communicate with the reader. These credit-card sized memory-chip devices derive their power from an RF field generated by the card reader. The RF field also transfers information to and from the card and card reader. Employee identification badges issued by large companies for building access are typically contactless smart cards.

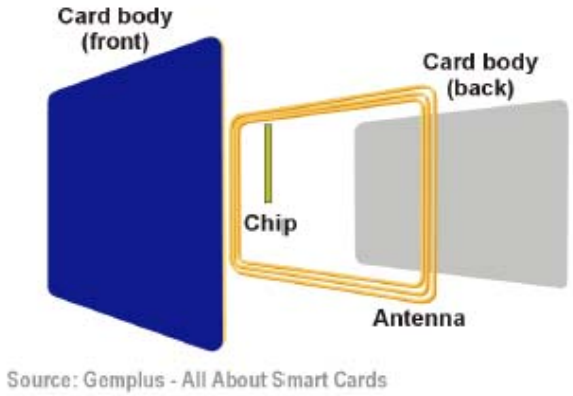

Figure 3. Contactless Smart Card

4.3 Combination Smart Cards

Multipurpose combination smart cards are a hybrid mix of the contact and contactless designs. They include the eight-pin contact for communication with a contacttype reader, and also include an antenna for communication with an RF-type reader.

5 Smart-Card Readers

For the sake of clearly defining all of the different hardware devices that smart cards can be plugged into the industry has adopted the following definitions:

The term "reader" is used to describe a unit that interfaces with a PC for the majority of its processing requirements. In contrast a "terminal" is a self-contained processing device.

Both terminals and readers read and write to smart cards. Readers come in many form factors and in a wide variety of capabilities. The easiest way to describe a reader is by the method of its interface to a PC. Smart Card Readers are available that interface to RS232 serial ports, USB ports, PCMCIA slots, floppy disk slots, parallel ports, infrared IRDA ports and Keyboards and keyboard wedge readers. Another difference in reader types is the on board intelligence and capabilities or lack thereof. Extensive price and performance differences exist between an industrial strength intelligent reader that supports a wide variety of card protocols and a home style win-card reader that only works with microprocessor cards and performs all processing of the data in the PC.

The options in terminal choice are just as wide. Most units have their own operating systems and development tools. They typically support other functions such as magstripe reading, modem functions and transaction printing.

Card readers provide the physical link between the smart card and the host. Figure 4 shows a combination keyboard/card reader. The host can be a PC or a standalone device. The reader delivers power, initializes the card, and acts as the mediator between the smart card and the host. Power is delivered to the smart card through a contact on the micromodule of contact smart cards or by inducing current through the antenna of contactless designs. Initialization is a specified protocol that all cards must perform. All smart-card readers support the initialization of any smart card, but they may not support the card after it switches to its specific application.

Figure 4. Smart-Card Reader

6 Smart-Card Standards

Smart-card standards define the operation of the technology, and promote product interoperability between smart-card manufacturers. Because there are a variety of smart-card applications requiring different solutions, several standards were needed to define smart-card technology. The International Organization for Standardization (ISO) 7816-X specification defines the complete characteristics of smart-card technology.

7 Special Applications

JavaCard and Personal Computer/Smart Card (PC/SC) allow programmers to write code for smart cards, much the same as the code written for PCs. The only limit for the code is the size of the EEPROM used in the smart card. Special applications that could be developed include:

- Launching a web page on insertion of the card
- Launching a support web page configured to the user's needs
- Storing personal information

The options for special smart-card applications are virtually unlimited depending on them creativity of the developer.

8 Smart-Card Security

One major use for smart cards is to protect data as information is exchanged between the card and reader. Companies using smart-card systems often require security for: confidentiality, user authentication, application authentication, transaction authentication, non-repudiation.

Most of these security needs can be met by PKI, which provides the policies and procedures required to establish secured information exchange. PKI includes data encryption to ensure confidentiality, digital certificates to provide authentication, and digital signatures to prove the originator without intervention or error completed the transaction.

Smart cards are used to store the public and private keys, the algorithm, and the digital certificates. The keys never leave the card, and the algorithm is used on the card to decrypt the message. This means that no third party can "listen" to the communication between the card and the reader to intercept the private key. PINs also provide protection for keys stored on a smart card. If the card is stolen and the thief attempts to guess the PIN to access the keys, the system can lock out the card after a few wrong guesses, thus preventing any further use of the card.

Biometrics can be used with the card technologies (e.g. smart cards), where biometric information is stored on the card and then verified with the received biometric at the point of interaction. By securely recording and then checking an individual's unique biometric information (e.g., fingerprints, hand geometry, retinal or iris patterns, facial patterns or voiceprints), the system can validate the individual's identity. The verification process may be done by the smart card or by a biometric-specific reader. Alternatively, a central database of biometric information can be used, with an online screening device.

Table 3. Biometric Template Size
Source: Frost & Sullivan

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

10 Smart-Card Support

Windows XP Professional offers native support for smart cards. Other OSs require adding drivers supplied by the device manufacturer. Smart-card native support provided with Windows XP includes:

- Reader drivers — supports several smart-card readers, and only requires that the reader is connected to the system, which allows Plug and Play to detect and configure the reader.
- PC/SC — supports the PC/SC card.
- Smart card ready — supports network PKI login.

Although Windows XP supports smart cards used for network PKI logins, a user needs a certificate server and a smart card configured with a certificate before this function can be used. The certificate server acts as the certifying authority by issuing and verifying certificates in use on the network. After the network is set up and configured, the user is required to use the smart card to log on to the network. Microsoft Outlook and Internet Explorer also provide smart-card support. Smart cards can be used with Outlook to digitally sign e-mail, and to send PKI secure transmissions. They can be used with Internet Explorer to control access to secured websites.

11 Internet Retail Payment and Smart Cards

The Internet retailer smart card infrastructure includes the following components:

- Consumer smart cards and smart card applications.
- A smart card reader for the consumer's personal computer (PC).
- PC client software to support smart card applications.
- Internet retailer server support for smart card applications.
- Acquirer/processor infrastructure for authorization and settlement of smart card transactions.
- Issuer systems supporting the authentication and transaction process and managing the issuer card base.

12 Emerging Smart Card Markets and Applications

Athough it is the smart card payment application that attracts media attention in the financial world, emerging non-payment applications are expected to create the business case for issuers to introduce smart card products, retailers to accept them and consumers to demand them. The smart cards currently being issued by American Express and by MasterCard and Visa issuers support multiple applications. Many new POS terminals also have expanded memory and increased power, enabling them to be multifunctional and support multiple applications.

Seven key markets, each with a specific set of application drivers, are adding momentum to the movement toward smart card implementation today. Each market application is concerned about security, speed, convenience and customer gratification. The markets are:

- Internet commerce
- General retail
- Mobile commerce
- Transit
- Contactless payment
- Campuses
- Government

New smart card applications are setting the stage for additional penetration by card issuers, adoption by merchants and usage by consumers. Integrating non-payment applications with new and traditional payment applications creates a compelling business case for implementing smart card technology.

13 Conclusions

Smart cards have to the potential to contribute greatly to the "integration of commercial transactions, data warehousing and data mining". These cards support an impressive variety of applications presently, and this variety should expand as the cards become smaller, cheaper, and more powerful. We know of one senior scientist with extensive expertise in smart card technology who has indicated his serious reservations about combining varied information, such as financial, health, and employment information on a single card.

As with other technologies that facilitate electronic information exchange, including the Web, email, and organizational network-based communications, issues involving privacy, legality, and ethics must be fully addressed before smart cards can truly take off.

References

[1] Smart Card Alliance: Secure Personal Identification Systems: Policy, Process and Technology Choices for a Privacy-Sensitive Solution A Smart Card Alliance White Paper, www.smartcardalliance.org (February 2002)

[2] Dustin Sorenson, Peripheral Development Group I/O Engineer: Smart-Card Devices and Applications White Paper, www.dell.com (January 2001)

[3] W. Rankl, W. Effing: Smart Card Handbook. 2nd edn. John Wiley & Sons.(2000)

[4] Scott B. Guthery, Timothy M. Jurgensen: Smart Card Developer's Kit. Macmillian Technical Publishing. (1998)

[5] Mike Hendry: Smart Card Security and Applications. Artech House. (1997)

[6] Henry Dreifus, J. Thomas Monk: Smart Cards – A guide to building and managing smart card applications. John Wiley & Sons.Inc. (1997)

[7] Smart Card Alliance: Smart Cards and the Retail Payments Infrastructure: Status, Drivers, and Directions. A Smart Card Alliance White Paper, www.smartcardalliance.org (October 2002)