A11102 903092

NAT'L INST OF STANDARDS & TECH R.I.C.
A11102903092
Haykin, Martha E/Smart card technology :
QC100 .U57 NO.500-157 1988 V19 C.1 NIST-

U.S. Department of Commerce
National Institute of Standards and Technology
(formerly National Bureau of Standards)

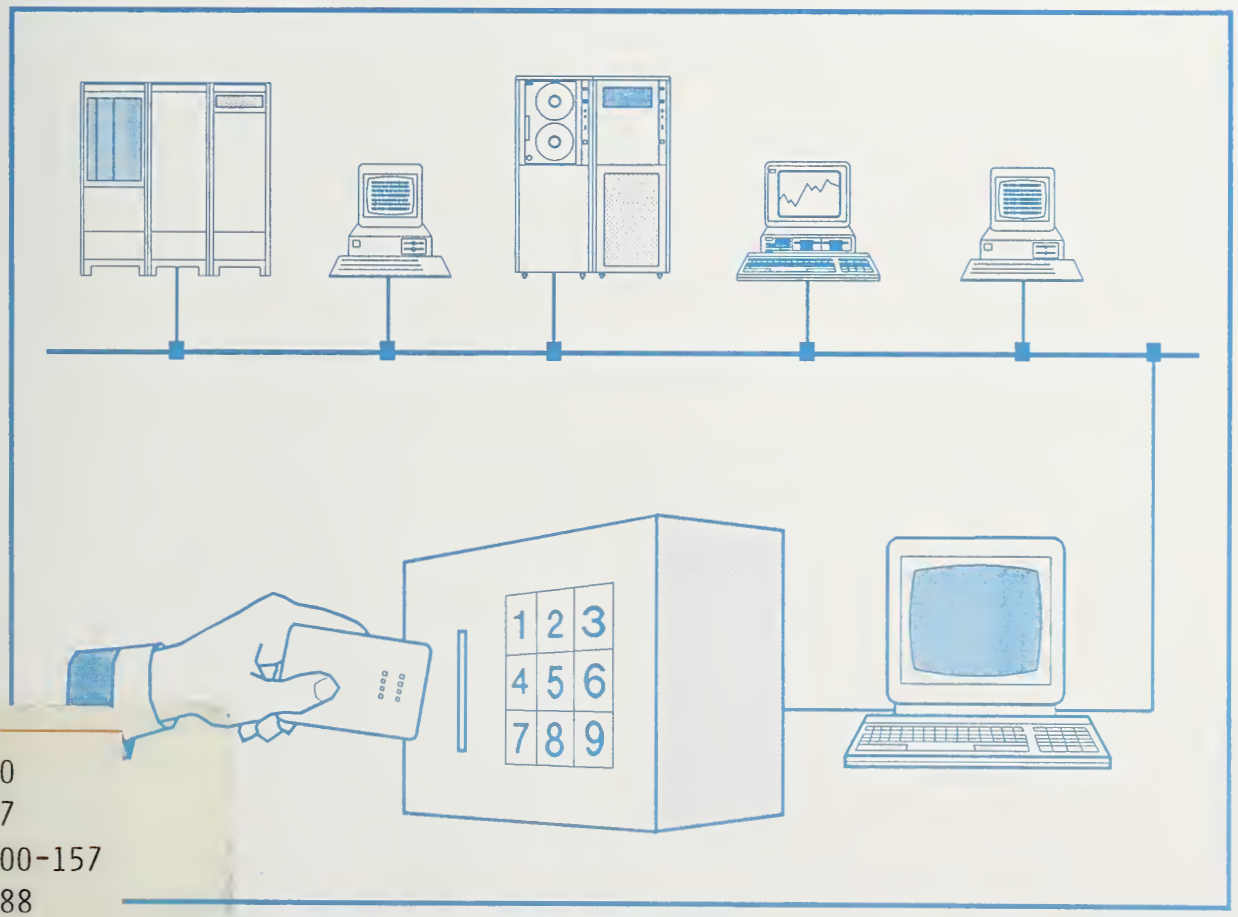
Computer Science and Technology

NBS
PUBLICATIONS

NIST Special Publication 500-157

Smart Card Technology: New Methods for Computer Access Control

Martha E. Haykin
Robert B. J. Warnar



QC
100
.U57
#500-157
1988
c.2

Computer Science and Technology

NIST Special Publication 500-157

Smart Card Technology: New Methods for Computer Access Control

Martha E. Haykin and Robert B. J. Warnar

Security Technology Group
Institute for Computer Sciences and Technology
National Institute of Standards and Technology
Gaithersburg, MD 20899

September 1988

NOTE: As of 23 August 1988, the National Bureau of Standards (NBS) became the National Institute of Standards and Technology (NIST) when President Reagan signed into law the Omnibus Trade and Competitiveness Act.

U.S. DEPARTMENT OF COMMERCE
C. William Verity, Secretary

National Institute of Standards and Technology
(formerly National Bureau of Standards)
Ernest Ambler, Director

IPR2025-01149
Apple EX1035 Page 3

Reports on Computer Science and Technology

The National Institute of Standards and Technology has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NIST Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NIST efforts to the Federal computer community as well as to interested specialists in the governmental, academic, and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

Library of Congress Catalog Card Number: 88-600577
National Institute of Standards and Technology
Special Publication 500-157, 52 pages (Sept. 1988)
CODEN: XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1988

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

CONTENTS

page

ABSTRACT 1

1.0 INTRODUCTION 1
1.1 Overview and Scope of this Document 1
1.2 The Definition of a Smart Card 2
1.3 Smart Cards and the International Organization for Standardization 2
1.4 Security in a Generalized Smart Card 4

2.0 SMART CARD INTEGRATED CIRCUIT TECHNOLOGIES . . . 5
2.1 Integrated Circuits (ICs) 5
2.2 Limitations of IC Technology 6

3.0 THE SMART CARD MICROCOMPUTER 6
3.1 Single-chip Versus Multiple-chip Smart Card Microcomputers . 7
3.2 The Smart Card Microprocessor 8
3.3 Smart Card Memories 8
3.4 Smart Card Input/Output (I/O) 10
3.4.1 Contact and Non-contact Smart Card Interfaces 10
3.4.2 The Smart Card Reader/Writer Device 13

4.0 OTHER CARD TECHNOLOGIES AND THE CURRENT ROLE OF THE SMART CARD 13
4.1 Storage Card Technologies—Machine- and Human- Readable . 13
4.2 Storage Card Technologies—Machine-Readable Only 14
4.2.1 Early Approaches 14
4.2.2 The Magnetic Stripe Card 15
4.2.3 The Laser-Written Optical Memory Card 15
4.2.4 The Integrated Circuit (IC) Storage Card 16
4.3 Current Constraints on the Role of the Smart Card 17
4.3.1 Factors in the Placement of the Smart Card IC Chip(s) 17
4.3.2 Cost Factors of the Smart Card 18

5.0 ACCESS CONTROL AND THE SMART CARD 18
5.1 Basic Access Control Concepts 18
5.1.1 Cryptographic Techniques: Encryption and Message Authentication 18
5.1.2 User Authentication 19
5.1.3 Device Authentication 20
5.2 The Smart Card and Authentication 21

IPR2025-01149
Apple EX1035 Page 5

5.3 Smart Card Encryption Capabilities 23
5.4 Secure Storage: Smart Card Memory Zones 24
5.5 Smart Card Life Cycle 26

6.0 NBS ACCESS CONTROL RESEARCH 28
6.1 NBS Plastic Memory Key Access Control Systems 28
6.1.1 Access Control System for "Dumb" Terminals 29
6.1.2 Access Control System for Cryptographic Workstations 29
6.2 The NBS Biometric Smart Card Access Control System . . . 31
6.3 Future NBS Investigations in Access Control 31

7.0 FUTURE SMART CARD FORECAST 33
7.1 Future Smart Card Costs 34
7.2 Future Changes in Smart Card Integrated Circuitry 34
7.2.1 The Role of EPROM in Future Smart Cards 35
7.2.2 The Role of EEPROM in Future Smart Cards 35
7.3 Expected Changes in the Appearance and Construction of the Smart Card 36
7.4 Expected Changes in Smart Card Operations and Applications 37
7.5 The Role of Standards in the Future of Smart Cards 40

APPENDIX: STANDARDS ACTIVITIES FOR INTEGRATED CIRCUIT CARDS 41

REFERENCES 43

IPR2025-01149
Apple EX1035 Page 6

LIST OF FIGURES

page

Figure 1: A Generalized Smart Card System 4

Figure 2: Expected ISO Specifications for Placement of Contact-Type I/O Connector 11

Figure 3: Expected ISO Specifications for Functions of Pins in Contact-Type I/O Interface 11

Figure 4: Contact-Type Smart Card Interface 12

Figure 5: Non-Contact-Type Smart Card Interface 12

Figure 6: A General System of Authentication 21

Figure 7: A System of Authentication Using Smart Cards 23

Figure 8: Possible Smart Card Memory Zones 25

Figure 9: Life Cycle of a Smart Card 27

Figure 10: Access Control System for Cryptographic Workstations 30

Figure 11: Biometric Smart Card Access Control System 32

Figure 12: Approximate Storage Capacity of Dedicated EPROM Chips 36

Figure 13: Current Smart Card Characteristics 38

Figure 14: Possible Features for Future Smart Cards 39

Figure A1: ISO IC Card Standards Groups 41

Figure A2: ANSI IC Card Standards Groups 42

IPR2025-01149
Apple EX1035 Page 7

LIST OF ACRONYMS

ALU . . . . . arithmetic logic unit
ANSI . . . . . American National Standards Institute
ATM . . . . . automated teller machine
CMOS . . . . . complementary metal-oxide semiconductor
DES . . . . . Data Encryption Standard
EEPROM . . . . . electrically erasable programmable read-only memory
EPROM . . . . . erasable programmable read-only memory
FTC . . . . . financial transaction card
IC . . . . . integrated circuit
ICC . . . . . integrated circuit card
I/O . . . . . input/output
ISO . . . . . International Organization for Standardization
LAN . . . . . local area network
MAC . . . . . message authentication code
NBS (now NIST) . . . . . National Bureau of Standards
(now National Institute of Standards and Technology)
NMOS . . . . . n-channel metal-oxide semiconductor
PIN . . . . . personal identification number
PC . . . . . personal computer
RAM . . . . . random access memory
ROM . . . . . read-only memory

ACKNOWLEDGMENTS

The authors would like to thank the following people for their assistance in the preparation of this document: Miles Smid, Dennis Gilbert, Dana Grubb, and especially Donna Fogle Dodson. Ms. Dodson's unfailing support in both the technical and editorial review of this document was extremely helpful.

IPR2025-01149
Apple EX1035 Page 8

ABSTRACT

A smart card is a credit-card-sized device containing one or more integrated circuit chips, which perform the functions of a microprocessor, memory, and an input/output interface. Smart cards, and other related devices, may be used to provide an increased level of security in applications requiring controlled access to sensitive information. This publication describes the basic components of a smart card, and the goals and obstacles of smart card application development. Possible roles for smart cards in modern computer security systems and research conducted at the National Bureau of Standards (NBS) in the area of smart card access control systems are discussed. A forecast is made for the characteristics and applications of future smart cards and related devices. An overview of current standards activities for smart cards is given in an appendix.

Key words: Access control; authentication; biometrics; computer security; cryptography; Data Encryption Standard (DES); electrically erasable programmable read only memory (EEPROM); erasable programmable read only memory (EPROM); integrated circuit card; microcomputer; reader/writer device; smart card; token.

1.0 INTRODUCTION

With microscopic electronic circuits placed inside credit-card-sized plastic carriers, smart cards offer the possibility that someday most individuals will carry their own computers in their pockets. Smart cards may greatly facilitate a wide range of information processing activities: Applied in banking, telephone services, medical records systems, and other areas, smart cards can provide users with both a secure medium for storing and carrying personal information and a means for accessing resources in a network of computers.

As the use of computers and computer networks has grown to encompass more and more of everyday life, the demand for effective computer security strategies has become more urgent. Smart cards, which are capable of both securely storing and *processing* data, may play a key role in improving the security of many computer systems.

1.1 Overview and Scope of this Document

This document describes the basic components of a smart card and provides background information on the underlying integrated circuit technologies. The capabilities of a smart card are discussed, with emphasis on the use of the smart card in computer security applications. Research conducted at the National Bureau of Standards (NBS) on smart card access control techniques is described. A forecast is made on expected developments in smart card technology. The appendix outlines the major U.S. and international groups involved in the development of standards for smart cards and related devices.

IPR2025-01149
Apple EX1035 Page 9

This document is intended to provide the reader with a general understanding of the use of smart card technology in computer access control. Several factors which must be considered in examining the security requirements of a computer system are discussed. It should be recognized, however, that smart cards and access control techniques are just one part of an overall computer security program. In accordance with the Brooks Act (P.L. 89-306) and the Computer Security Act of 1987 (P.L. 100-235), NBS develops guidelines, technology forecasts, and other documents to provide information on a wide range of computer security topics. Information about these documents is available in NBS Publications List 91, "Computer Security Publications." [NBS 88]

1.2 The Definition of a Smart Card

The term "smart card" has been used as a label for a wide variety of hand-held plastic devices containing mechanisms for storing and/or processing information. There is much debate over exactly what capabilities and characteristics a device must have in order to be considered a smart card. One source states that a smart card is implemented "in a piece of plastic the size of a credit card" and that "each smart card contains its own central processing unit [which is] essentially a small computer." [MCIV 85, p. 152] Another source, with a broader definition, suggests that a smart card "consists of an integrated circuit chip or chips packaged in a convenient form to be carried on one's person." [SVGL 85, p. 1] With the latter definition, the category of smart cards includes integrated circuit data storage cards and key-shaped devices, which may not have any computational powers. Magnetic stripe and optical laser storage cards have also sometimes been referred to as smart cards, because they have data storage capacity.

As researchers and manufacturers struggle to develop and distribute products in step with the latest technological advances, confusion over the terminology of new devices arises. For purposes of discussion, this document will use the following definition of a smart card:

> A smart card is a credit-card-sized device containing one or more integrated circuit chips, which perform the functions of a microprocessor, memory, and an input/output interface.

Devices which are not of standard credit card size (i.e., plastic keys and dogtags, or cards which are thicker than the standard credit card), but which otherwise conform to this definition, will be referred to in this document as "smart tokens."

1.3 Smart Cards and the International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) develops voluntary international standards in many scientific, technological, and economic fields. ISO has not defined or produced standards for any devices specifically labelled as "smart cards."

IPR2025-01149
Apple EX1035 Page 10

ISO is, however, actively involved in the development of standards for what ISO calls an integrated circuit card (ICC). Some of the fundamental characteristics of an ISO ICC are:

- The ICC contains one or more integrated circuits.
- The length (3.370 inches), width (2.125 inches), and thickness (0.030 inches) of an ICC are the same as the dimensions of a standard credit card.
- The ICC allows spaces on the surface of the card for magnetic stripe and embossed data storage, in order to allow compatibility with existing technologies.

(An outline of ISO integrated circuit card standards activities is given in the appendix.) Smart cards, as defined in this document, are similar to ISO IC cards except that 1) smart cards do not necessarily have magnetic stripe and embossing areas, and 2) smart cards must have processing capability. The ability of the smart card to *process* information, and not simply store it, is of vital importance in applications in which the security of sensitive information must be maintained. The following section presents a simple example of how a smart card system can be used to protect sensititive data.

1.4 Security in a Generalized Smart Card System

A generalized smart card system contains a smart card, a smart card reader/writer device, a terminal, a host computer, and the connections necessary to interface these components (see fig. 1).

On a superficial level, a smart card system resembles conventional data storage card systems, such as automated teller machine (ATM) systems which use magnetic stripe cards. However, because smart cards have computing powers and greater capacity for protected data storage, smart card systems can provide increased flexibility and security in many applications.

For example, a company that has proprietary information stored in its main computer could use a smart card system to maintain and protect this sensitive data in a scenario such as the following:

> A smart card is issued to each employee who has a need to access the computer system. Each employee's card is programmed with unique information, such as a personal identification number (PIN). The smart card's microcomputer performs a secret one-way transformation* on this PIN, to render it unreadable, and then stores the transformed PIN in a secret part of its memory.

---

* A one-way transformation is a mathematical function which is easy to perform but nearly impossible to reverse. That is, given the one-way transformation function f and the result of this function $R = f(D)$, it is extremely difficult to determine the input to the function D.

IPR2025-01149
Apple EX1035 Page 11

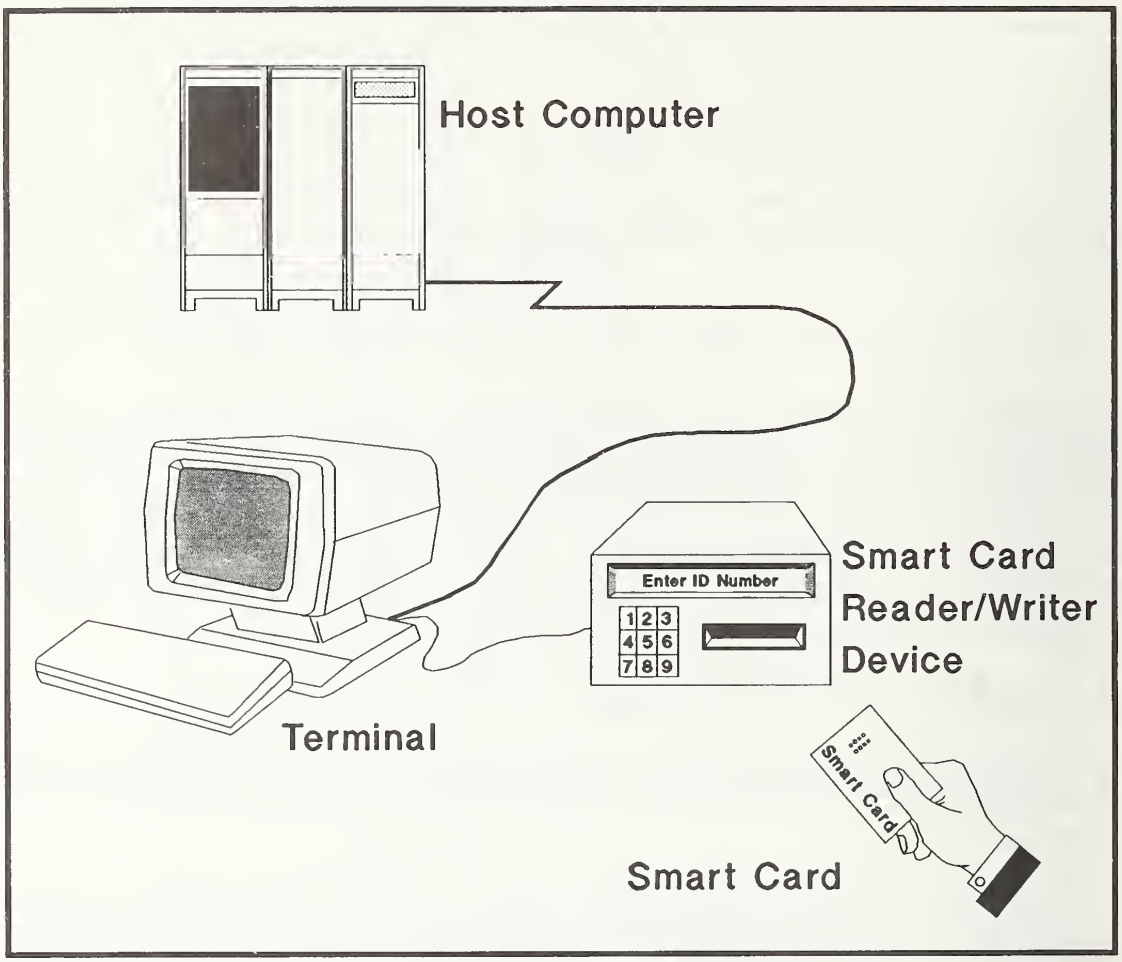


Figure 1. A Generalized Smart Card System

To access the computer system, an employee must insert his smart card into a reader/writer device and enter his unique PIN via the reader/writer's keyboard. The smart card's microcomputer chip then performs the same one-way transformation on the entered PIN and compares it with the stored PIN. Because this comparison is done completely inside the smart card's microcomputer chip, the employee's PIN is never written into the open working memory of the host computer, which might be exposed to modification or monitoring by an adversary.

If the smart card determines that the two PINs match, information is exchanged between the smart card and the host computer to determine the employee's identity and which files within the host the employee is entitled to access. The employee can then read and update only those files via a terminal connected to the host computer. A log of the employee's actions within the computer system can be maintained within the smart card's memories.

IPR2025-01149
Apple EX1035 Page 12

2.0 SMART CARD INTEGRATED CIRCUIT TECHNOLOGIES

The smart card's ability to perform the computations and other functions needed in security applications depends on the development of the smart card microcomputer, which, in turn, is inherently tied to the progress of integrated circuit technologies. This chapter discusses some of the concepts and considerations involved in the production of integrated circuits.

2.1 Integrated Circuits (ICs)

Integrated circuits (ICs) are electronic circuits, of varying complexity, which are formed on individual chips of silicon (or other semiconductor* material). Computers and digital instruments are filled with ICs, which are small and can be designed to quickly perform complicated functions.

The capability of an IC depends on the amount of circuitry it contains, a quantity often described in terms of transistor density. With current IC technology, close to 400 transistors can be formed in a space as small as the cross-section of a human hair, which is approximately 100 microns (millionths of a meter) in diameter. With this transistor density, ICs containing about 50,000 transistors can be produced; transistors are placed on an integrated circuit and interconnected with "wires" 1 micron in width. If this "wire" width were reduced to half a micron, 1500 transistors could be placed in a 100-micron cross-sectional area. Cutting the dimensions in half again would make each transistor the size of a large virus. With quarter micron "wire" widths, 4500 transistors could be placed in the cross-sectional area of a hair. It is predicted that the latter capability may be reached by 1995 . [WLSN 85, p. 83]

Some sources believe that with the increases in transistor density, the billion-transistor IC will become a definite reality by the year 2000. [COLE 87, p. 81] If an estimated 200,000 transistors are needed to store and handle one page of text, a billion-transistor IC could store several thousand printed pages. Any of these pages could be retrieved in a random fashion from such a supercircuit and transmitted between two computers in about a second.

It is important to realize, however, that as the density of transistors in ICs increases, so does the difficulty of producing ICs that function correctly. If a single transistor in any part of an IC fails, the operation of the entire IC chip may be impaired.

---

* Semiconductor is a material in which the conductivity ranges between that of a conductor and an insulator. The electrical characteristics of semiconductor material are dependent upon small amounts of added impurities, called dopants.

IPR2025-01149
Apple EX1035 Page 13

2.2 Limitations of IC Technology

Simply stated, the goal of IC technology is to produce reliable ICs which are reduced in size and yet increased in capability. The extent to which this goal can be attained is limited by the physical characteristics of the materials used for both the substrate (the foundation for the IC) and the actual circuitry to be placed on that substrate. All silicon materials used to produce IC substrates have a certain defect density. The IC fabrication engineer must work within the limitation that, in a given section of silicon substrate material, there will be a certain number of defects. If this section is cut into a small number of large chips, a high percentage of the chips produced will contain one or more defects. However, if the section is cut into a large number of small chips, a much lower percentage of the chips produced will contain defects. The chips produced must be both large enough to accomodate the circuitry to be placed on them and yet small enough that a reasonable yield of usable chips can be produced from each section of silicon substrate.

In order to increase the amount of circuitry which can be placed on a small silicon chip, the circuits themselves are made smaller. Much research is devoted to methods for reducing linewidth, the amount of space needed by an interconnecting "wire." Some sources predict that the conventional method (optical lithography) can be pushed to produce circuits with 0.1 micron linewidths. This would constitute a 5 to 10 times improvement over current capabilities. [COLE 87, p. 83] The smaller reliable circuitry can be made, the more functions each chip can support.

In addition to reducing linewidth, current research efforts are aiming towards the production of application-specific ICs (ASICs), partially customized ICs which are fabricated according to standard conventions. The increase in IC functionality, made possible by reduced linewidth and custom fabrication, will be of primary importance in the development of microcomputer chips such as those used in smart cards.

3.0 THE SMART CARD MICROCOMPUTER

The word microcomputer is typically used to mean simply a "small" computer. Within the category of "small" computers there is a very wide variety of devices, ranging from a personal computer (which may be equipped with such peripherals as a monitor, a keyboard, one or more floppy disk drives, a hard disk, a mouse, a modem, a printer, and/or others) down to an IC chip no larger than an eraser on the end of a pencil. Microcomputers may differ greatly in their costs, capabilities, and intended applications. In general, however, each microcomputer is comprised of three basic components: a microprocessor (for managing information), memory (for storing information), and an input/output (I/O) interface (for transmitting and receiving information).

The desktop personal computer is one of the most common types of microcomputer. A personal computer may contain dozens of integrated circuits; usually one IC forms

IPR2025-01149
Apple EX1035 Page 14

the microprocessor, a large number of ICs serve as memory, and a few ICs control the input/output interface. Because they are so small and because they are designed for different applications, smart cards do not contain all of the integrated circuitry that is housed within personal computers. Smart cards do, however, contain all three of the basic microcomputer components.

Researchers and manufacturers have developed many different designs for the tiny microcomputer to be placed in a smart card. A fundamental issue in smart card design is whether the microcomputer should be restricted to a single IC chip or distributed over several chips.

3.1 Single-Chip Versus Multiple-Chip Smart Card Microcomputers

There are advantages and disadvantages to both the muliple-chip and the single-chip smart card. A multiple-chip smart card may be less expensive to produce, since it can incorporate several easily-attainable, low-cost IC chips. A single-chip smart card, on the other hand, requires a more complex, specialized chip, carefully designed to accomodate all the required circuitry for the microprocessor, memory and I/O. [MCIV 85, p. 155] In addition, a multiple-chip smart card may be able to perform more functions and store more information than a single-chip smart card. However, including more than one chip in a smart card presents some difficult problems.

During the course of its use, a plastic credit-card-sized device is subject to a great deal of bending and twisting. To be reliable, a smart card IC chip must be placed in one of the few areas of a card where the effects of such stress are minimal. If several chips are to be contained in a smart card, some of them may have to be placed in the higher-stress areas of the card, where they may be more likely to break and cease to function. The connecting "wires" which are needed to link several chips together may be similarly susceptible to damage.

In addition to the increased chances of breakage, a multiple-chip smart card may present a risk in terms of the security of the information to be stored within the card. It may be possible for an adversary to "eavesdrop" on the chip-to-chip connections and extract secret data from a multiple-chip smart card. Since it contains no chip-to-chip connections, the single-chip smart card is generally considered more reliable and more secure than the multiple-chip card. For these reasons, the single-chip smart card is currently preferred for many applications.

Although it has some limitations, a single-chip smart card can perform all the functions of a microcomputer. The following sections describe the components of a microcomputer—microprocessor, memory, and input/output—as they may be implemented in a single smart card IC chip.

IPR2025-01149
Apple EX1035 Page 15

3.2 The Smart Card Microprocessor

The microprocessor is the component which makes a smart card "smart" and distinguishes it from cards designed to simply store data. The microprocessor and its associated operating system enables the smart card to "make its own decisions" concerning where it will store data in its memories and under what circumstances it will transfer information through its input/output interface. The microprocessor itself consists of three major components: the arithmetic logic unit (ALU), the control unit, and the bus.

- The ALU provides the basic logic and arithmetic functions for the microcomputer. It also contains small storage spaces, called registers, which are needed for performing computations, such as addition or multiplication. The ALU interacts with the memory and the input/output in order to coordinate the operations of the microcomputer.

- The control unit assures that the timing of events in the various parts of the microcomputer are coordinated.

- The bus provides a link between different parts of the smart card microcomputer. There are many possible configurations for the bus, which may be comprised of several segments. For example, one segment of the bus may link two registers in the ALU together, another may link the input/output interface to the microprocessor, and still another may link the microprocessor to the main memory of the smart card. In general, smart cards are designed such that the bus does not directly connect the input/output to the main memory. The microprocessor may be linked between the input/output and the main memory in order to "stand guard" over information entering and leaving the memory.

3.3 Smart Card Memories

A smart card may contain several kinds of memory for storing data and programs. Virtually all memories currently used in smart card microcomputers are manufactured from semiconductor materials. Semiconductor memories consist of matrices of cells formed by transistors to store information. By varying the composition and cell configurations of semiconductor materials, memories with differing characteristics can be produced. Four types of semiconductor memory used in smart cards are discussed below.

Random Access Memory (RAM) – Smart card RAM is generally manufactured from metal-oxide-semiconductor silicon. Any information stored in RAM can be accessed in a fixed amount of time regardless of the information's position within the memory. Access time to information in RAM is in the range of tens to hundreds of nanoseconds (billionths of a second). Smart card RAM is usually volatile in nature (that is, it will lose its stored information immediately if power to the memory is removed). RAM, the fastest type of memory, is often used as a "scratch pad," buffer, or other type of temporary storage.

IPR2025-01149
Apple EX1035 Page 16

Read Only Memory (ROM) – Smart card ROM is a semiconductor memory which is nonvolatile (i.e., its stored information is retained indefinitely without a continuous power supply to the memory). Smart card ROM is typically made from a section of semiconductor material in which a series of memory cells have been permanently burned or fused, in a particular pattern which forms the underlying structure for a program. In this programming process, which is completed at the ROM manufacturer's plant, the ROM is often masked in such a way that it cannot be read or altered by the user. Semiconductor ROM is typically used for storing the smart card's general operating system programs [MCIV 85, p. 154] (such as the program needed to start the smart card when its power is turned on).

Erasable Programmable Read Only Memory (EPROM) – Smart card EPROM is a nonvolatile semiconductor memory which can be initially programmed at the user's facility rather than at the ROM manufacturer's plant. Data and programs can be loaded into the smart card EPROM via a smart card reader/writer device; the transfer of information is controlled by the smart card's microprocessor. When it is used in other types of computers, EPROM can be erased (by exposure to ultraviolet light) and reprogrammed. However, EPROM that is used in smart cards is typically manufactured in such a way that it is permanently shielded and cannot be erased or altered. This shielding is intended to increase the security of the smart card, by preventing unauthorized modification of data stored in the EPROM.* EPROM may be used in a smart card to permanently store an audit trail, a complete history of the operation of the card. EPROM provides much greater storage density than other memories such as EEPROM (see below). However, because data can only be appended to and not erased from smart card EPROM, it may eventually become full, and thus the smart card will "expire."

Electrically Erasable Programmable Read Only Memory (EEPROM) – Smart card EEPROM is a nonvolatile semiconductor memory which can be electrically erased and reprogrammed via a reader/writer device at the user's facility. EEPROM can be used for storing programs and data which may need to be modified periodically. Since EEPROM can be erased, a smart card containing EEPROM will not "expire" because its memory is filled up. Currently, however, EEPROM memories have less storage capacity, require larger circuitry, and cost more than other types of memory. In addition, EEPROM may not be appropriate for storing an audit trail.

A smart card microcomputer chip usually contains both RAM and ROM, for the card's temporary working memory and for the operating system programs, and either EPROM or EEPROM as a large storage memory area. Using current techniques, EPROM and EEPROM cannot be placed together on the same IC chip. Thus, for single-chip smart cards, either EPROM or EEPROM must be chosen, depending on the intended

* While it may be possible to produce a smart card which contains erasable EPROM, it is generally not considered practical, due to packaging difficulties and other limitations of erasable EPROM.

IPR2025-01149
Apple EX1035 Page 17

application for the smart card. (Currently, few single-chip smart cards contain EEPROM.) In order to utilize both EPROM and EEPROM memories, some manufacturers place separate EEPROM chips in the smart card together with a microcomputer chip containing EPROM. It remains to be seen whether this endeavor is as reliable, secure, and cost-effective as the single-chip approach.

3.4 Smart Card Input/Output (I/O)

In order to communicate with the "outside world" of other computers, a smart card must have components to perform input/output (I/O) functions. Typically, a smart card has some logic circuitry which, in conjunction with the microprocessor, controls the timing and flow of data transferred into and out of the smart card's memories. A smart card must have some type of physical structure through which it can interface to a reader/writer device, which can be connected to other computers for the exchange of data. There are two general categories of physical interfaces for smart cards: the contact type and the non-contact (or contactless) type.

3.4.1 Contact and Non-contact Smart Card Interfaces

Many smart cards in production today are equipped with contact-type interfaces. Typically, this interface consists of an 8-contact connector, which looks like a small gold circle or series of squares on the surface of the card. The International Organization for Standardization (ISO) is currently developing an international standard for such an interface, which may be used in ISO integrated circuit cards (ICCs) or in smart cards. It is expected that the ISO standard will specify the size, placement, and functions of the pin contacts on the card, as well as certain protocols for transferring information through the contact interface. Figures 2 and 3 illustrate some of the features of a contact-type interface as they are expected to be specified in the ISO standard.

With a contact-type interface, the pins of the reader/writer's connector must physically touch the contacts on the smart card's connector during data transfer. In contrast, a smart card with a non-contact type interface can transmit information to and receive information from a reader/writer device without a physical connection. A non-contact type interface may be implemented using capacitive plates placed inside or on the surface of the card. When placed within a short distance from a reader/writer device containing corresponding capacitive plates, information can be exchanged. With a non-contact type interface, problems such as electrostatic discharge and contamination of physical contacts (with dirt, grease, etc.) may be avoided. [RSKI 87, p. 16] However, a smart card with a non-contact interface may require additional components which may increase the card's susceptibility to internal breakage. ISO is not currently working on standardizing any non-contact ICC interfaces. Figures 4 and 5 illustrate smart cards with contact and non-contact type interfaces, in their corresponding reader/writer devices.

IPR2025-01149
Apple EX1035 Page 18

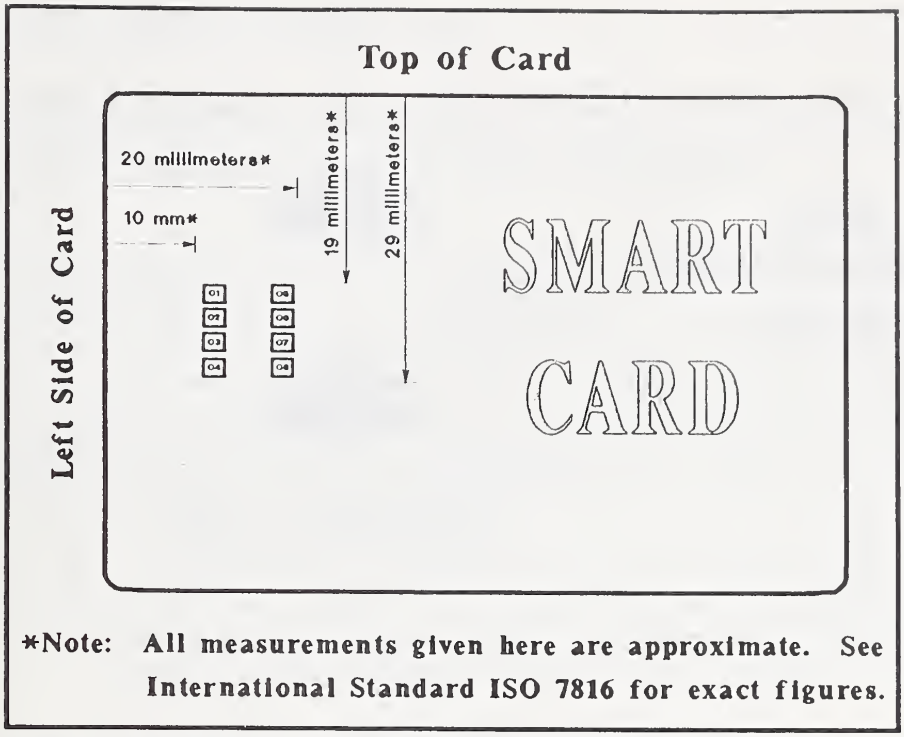


Figure 2. Expected ISO Specifications for Placement of Contact-Type I/O Connector

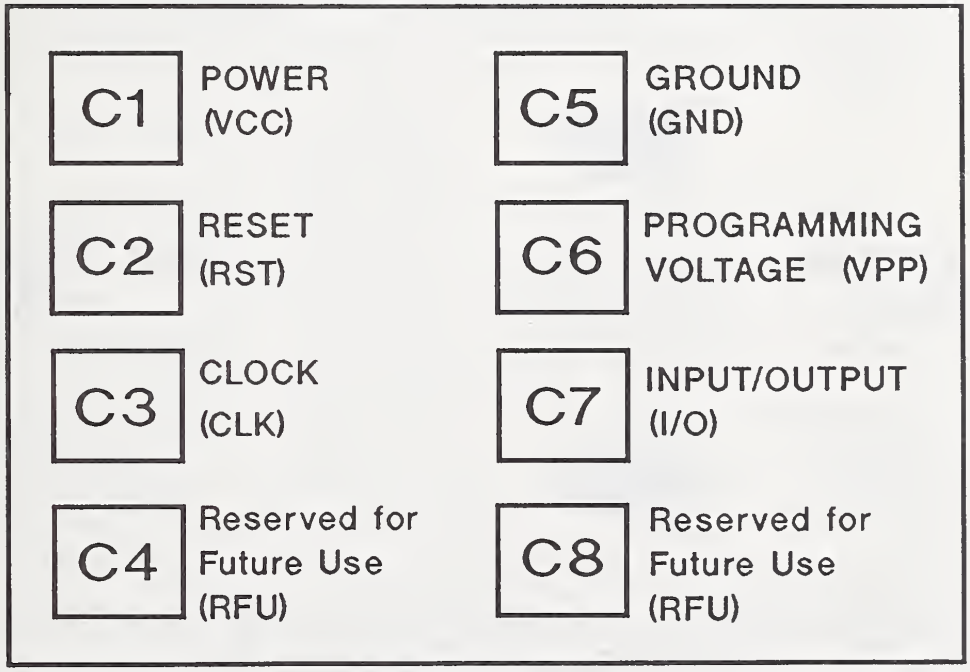


Figure 3. Expected ISO Specifications for Functions of Pins in Contact-Type I/O Interface

IPR2025-01149
Apple EX1035 Page 19

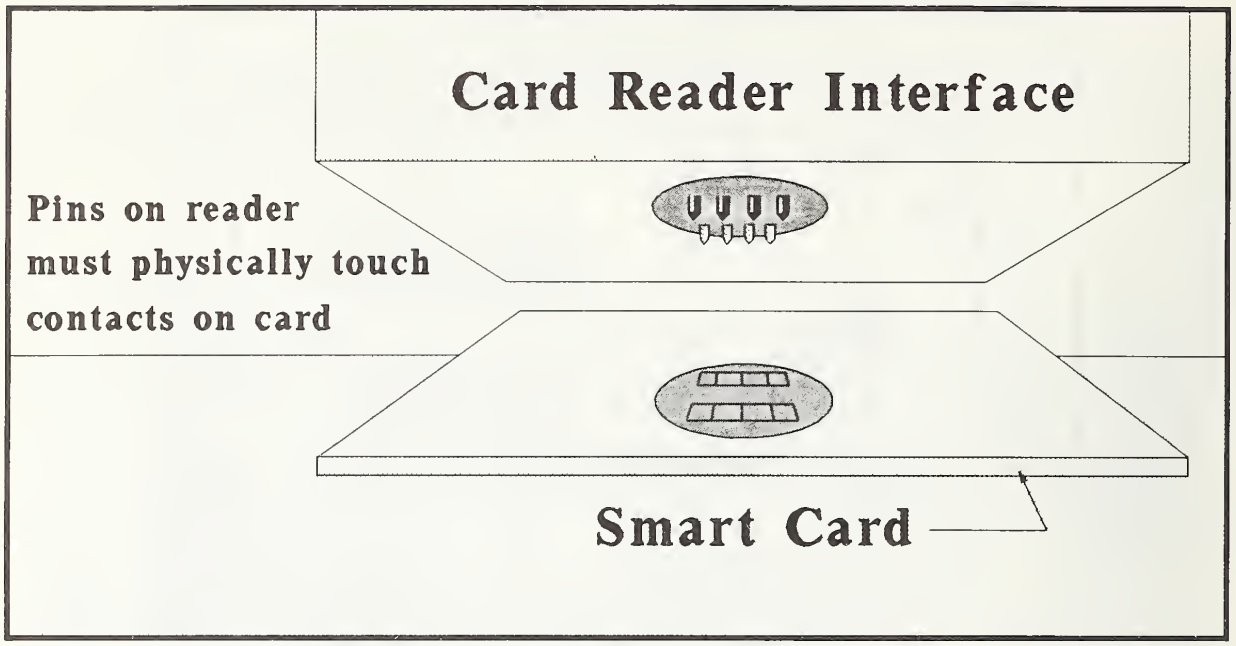


Figure 4. Contact-Type Smart Card Interface

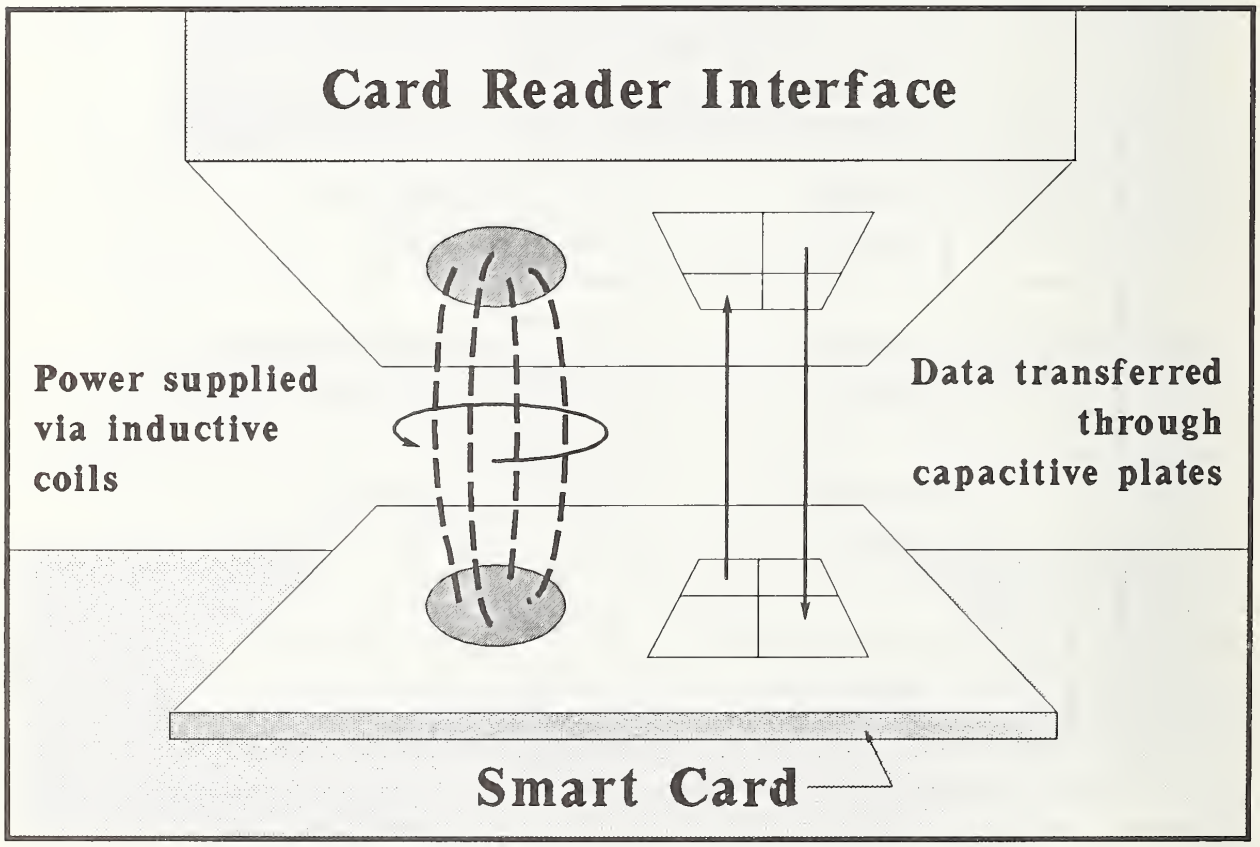


Figure 5. Non-Contact-Type Smart Card Interface

IPR2025-01149
Apple EX1035 Page 20

3.4.2 The Smart Card Reader/Writer Device

Although its importance is often underemphasized, the smart card reader/writer device is a major component of a smart card system. Nearly every smart card currently in production requires some type of specialized reader/writer device.

The main purpose of the reader/writer device is to provide a means for passing information from the smart card to a larger computer and for writing information from the larger computer into the smart card. The reader/writer device provides power to the smart card and physically links the card's hardware interface to the larger computer. Since the smart card's microprocessor can control the actual flow of information into and out of the card's memories, the reader/writer device may need only minimal processing capabilities for sending the information to other computers. As one source indicates, "Cards that include microprocessors are able to communicate with relatively inexpensive, 'dumb' reading and writing [devices]." [GLZR 86, p. 36] Some smart card systems incorporate reader/writer devices which perform calculations and other functions. However, it is generally the smart card itself that determines if and when data will be transferred into and out of the smart card's memories.

4.0 OTHER CARD TECHNOLOGIES AND THE CURRENT ROLE OF THE SMART CARD

Because it has active control over the information stored within its memory, the smart card is a very significant development in the long history of card-based data storage and management systems. While initially cards were designed without any effort to conceal the information which they held, secure data storage eventually became one of the most important goals of card system technology.

4.1 Storage Card Technologies—Machine- and Human-Readable

The concept of placing information on a card to be "read" by a machine originated in the early 1800's, when the French scientist Joseph-Marie Jacquard used punched cards to program an automatic loom. [AUGT 84, p. 63] Punched cards were a primary means for communicating with calculating machines and computers from the 1890's— when Herman Hollerith first used them in tallying the U.S. census— to the early 1970's. Punched cards were designed simply to automate data entry, thereby reducing the amount of switch-setting, typing, and other work that had to be done manually. As with other coded cards which were developed later, punched cards were designed so that their data could, if necessary, be read by humans as well as by machines.

The development of optical scanning devices in the early 1960's gave computers the ability to read letters, numbers, and patterns from printed materials. Optical character recognition (OCR) technology led to the development of two types of cards for storing machine- and human-readable data: the embossed card and the optical stripe card.

IPR2025-01149
Apple EX1035 Page 21

Embossing is a standard feature on most credit cards today. An embossed card enables a sales clerk or cashier to quickly make a carbon copy of the cardholder's credit account number, which can be read later by a computer. [SVGL 85, pp. 11-12] Since the cashier does not actually read or type the number, fewer errors are made and transactions are faster. However, the cashier can read the number directly from the card if for some reason this becomes necessary (for example, if the card number must be visually compared with a list of numbers of stolen cards.)

Optical bar code cards are also intended to store information to be read by both machines and humans. An optical bar code consists of a series of thin and thick parallel lines arranged in a pattern which is very easily readable by a computer. This pattern is difficult (though not impossible) for most humans to read; therefore the numbers that correspond with the code are typically printed on the card. Widely used in libraries, optical bar code cards enable a circulation librarian to quickly enter a book-borrower's card number without having to read it, unless some problem occurs (such as a computer breakdown or power failure).

4.2 Storage Card Technologies—Machine-Readable Only

Cards containing data which can be read both by humans and by machines are very useful in some applications. However, as the use of cards in financial and other sensitive information systems has increased, the demand for cards which can somehow conceal and protect stored information has also increased. During the past three decades, many types of hidden data storage cards have been developed.

4.2.1 Early Approaches

Many of the early approaches to cards with hidden data storage involved embedding various types of materials between opaque layers of plastic. Bits of magnetic or capacitive materials, small pieces of specially treated wire (i.e., Wiegand wires), or other particles with measurable physical characteristics were arranged in secret patterns and then sealed in plastic so they would not be visible on the exterior of the card. The pattern hidden within a card could be detected by a specialized reader which sensed the presence or absence of hidden materials in specific points on the card.

Though their development provided the impetus for further research in secure data storage cards, embedded materials cards are currently used only in limited applications. Some of them were too expensive for mass production, some did not effectively conceal the secret patterns, and most simply could not compete with the emerging technology of the higher capacity magnetic stripe card. [BWRS 86, p. 44]

IPR2025-01149
Apple EX1035 Page 22

4.2.2 The Magnetic Stripe Card

The magnetic stripe card, currently one of the most widely used storage cards, consists of a plastic card with a thin strip, or stripe, of magnetic material affixed to its surface. Small spots along the stripe are magnetized in varying degrees to form a code representing the stored data. With a capacity much greater than that of most earlier cards, a magnetic stripe card can store up to 240 characters of information.

Because it is inexpensive (about $.20 per card [SVGL 85, p. 148]), easy to produce, and high enough in storage capacity for many applications, the magnetic stripe card has been extremely popular throughout the world; millions of magnetic stripe cards are currently in circulation. Unfortunately, the widespread use and ease of production of the magnetic stripe card has made it a target for counterfeiting and fraud.*

Recently magnetic stripe manufacturers have developed techniques to increase the security of the magnetic stripe card. Some methods involve recording special markings or numbers in the magnetic stripe that cannot be duplicated by standard magnetic stripe production methods. A would-be counterfeiter, hopefully, will not be able to determine where the special markings are, nor how to reproduce them, and thus will not be able to produce a functional copy of a stolen card. Another technique is to store the information in the card in secret code form, so that anyone trying to illegally read the card will obtain only scrambled data.

In addition to possible forgery and illegal reading of stored data, the magnetic stripe card may be susceptible to erasure, if placed near other magnetic materials. [BRNS 86, p. 37]

4.2.3 The Laser-Written Optical Memory Card

In an attempt to increase on-card memory while circumventing some of the problems associated with the magnetic stripe card, a device known as the optical memory card was developed. Proponents of the optical memory card suggest that it is very difficult to copy and impossible to erase or illicitly alter. [BRNS 86, p. 37] Using technology similar to that of a compact disk, the optical memory card's stored information is written by a laser. A laser is used to burn millions of microscopic holes in a thin sheet of optical material (the optical stripe) on the surface of the card. At least 4 million bytes of information (several hundred printed pages) can be stored in an optical stripe with this technique. [BRNY 86, p. 58]

---

* Early in 1987, an $86,000 scam involving magnetic stripe financial transaction cards (FTCs) was discovered. It involved collecting discarded receipts and recording personal identification numbers by observing customers making transactions at automated teller machines (ATMs). The receipts were then used to produce counterfeit magnetic stripes on other FTCs. [SVGL 87, p. 4]

IPR2025-01149
Apple EX1035 Page 23

Though the information stored in an optical memory card is completely invisible to the naked eye, it may be readable if a microscope or other equipment is used. Therefore, data must be stored in secret code form in an optical stripe (as it is in a magnetic stripe) for high security applications. The optical memory card may become widely used for storing large medical, financial, and other records, if the cards and their associated optical reader devices are shown to be cost effective.

4.2.4 The Integrated Circuit (IC) Storage Card

Like a smart card, an integrated circuit storage card contains one or more integrated circuits. However, unlike a smart card, an IC storage card does not have processing capability; its ICs function only as memory. An IC storage card may have a memory capacity of 125 thousand bytes [CASA1 87, p. 24], which is considerably less than that of an optical stripe card, but considerably more than that of a magnetic stripe card.

Because they typically involve company-proprietary techniques, IC storage card production methods are largely unknown by and unavailable to the general public. A counterfeiter might find it very difficult to duplicate an IC storage card. Little or no information about the data stored in an IC card can be obtained by examining the IC's exterior.

The exact characteristics of an IC card, or of any of the other cards described above, may vary from manufacturer to manufacturer. Likewise, the usefulness of a particular card for a particular application may vary, depending on the amount of data storage required, the cost of the card and its associated reading and writing equipment, the level of security needed, and other application-specific factors.

Though data storage cards may differ in many aspects, all of them – the embedded materials cards, the optical memory card, the magnetic stripe card, and the IC storage card – are alike in that they are all *passive* devices. In this sense, the word passive indicates that the cards themselves cannot control the writing of information into an on-card storage area nor the subsequent retrieval of the information by an authorized, or an unauthorized, user. The smart card, on the other hand, is an *active* device, capable of independently performing calculations and controlling access to its own memory.

4.3 Current Constraints on the Role of the Smart Card

The processing and computational powers of the smart card may make possible a much higher level of security and flexibility in systems which currently incorporate passive storage cards. However, though the smart card may have technological advantages over passive devices, it faces several limiting factors which have kept it from supplanting other card technologies.

4.3.1 Factors in the Placement of the Smart Card IC Chip(s)

One difficulty in current implementations of the smart card is the placement of the IC chip(s). Ideally, the chip or chips should be placed in one of the four corners of the

IPR2025-01149
Apple EX1035 Page 24

smart card, since these areas are the least affected by bending of the card. However, due to constraints imposed by the conventions of the financial community, smart card chips typically are not placed in the cards' corners.

Over the course of time, the international banking community has established standards* for financial transaction cards (FTCs). Industry standard FTCs currently in circulation have a magnetic stripe, on the upper half of the back of the card, and embossing, on the lower half of the card. For compatibility with the existing FTC reading devices, smart cards often include embossing and magnetic stripes, placed according to the pre-existing standards. As long as magnetic stripes and embossing are widely used, the smart card IC chip(s) may be confined to the more damage-prone middle of the card. This may increase the difficulty of producing reliable smart card chips, which may, in turn, affect the prices of smart cards.

4.3.2 Cost Factors of the Smart Card

In addition to increasing the risks and costs associated with possible smart card chip breakage, including a magnetic stripe and embossing may increase the cost of the smart card in two other ways. First, it may raise the price of the card itself since more components must be added. Secondly, extra cost due to fraud may be encountered since a merchant may have the option to bill a card-holder by using the embossing, the magnetic stripe, or both, in addition to, or instead of, the smart card IC transaction. For these reasons, including embossing and/or a magnetic stripe on a smart card may be undesirable.

On the other hand, businesses currently using extensive embossing and magnetic stripe systems may be reluctant to make an overnight conversion to systems which use only the smart card's IC chip. Unless they are spread out over a period of time, the costs of replacing millions of embossed magnetic stripe cards and their corresponding readers may be prohibitive. Large-scale conversion to smart card systems with advanced security capabilities may be limited by "the enormous cost of gathering additional cardholder data not currently in the issuer's file, formatting it, encoding it in the [smart] card, and maintaining [such a] widely distributed database." [LNDN 86, p. 4]

Many foreign countries have succeeded in developing fairly wide-spread smart card systems for banking, telephone services, and other applications. In some cases (such as in France, for example, where smart cards are used in a telephone payment system), no card systems had been previously established; the smart card systems were set up "from scratch" without the need to replace existing technologies. In the U.S., the application of smart cards has been more limited, due in part to large corporate investments in embossed magnetic stripe cards. U.S. firms are, however, initiating pilot projects to "test [smart cards] as possible replacements for conventional credit cards." [GLZR 86, p. 34]

---

* The ISO standard for integrated circuit card contact-type interfaces (as described in sec. 3.4) is expected to specify an interface which will not interfere with embossing and/or a magnetic stripe to be placed on a card. (See fig. 2, page 10.)

IPR2025-01149
Apple EX1035 Page 25

Cost considerations and considerations involving existing embossed magnetic stripe card systems may somewhat delay the implementation of smart card systems for large-scale banking and credit applications. However, for smaller applications in which high security is imperative, viable smart card systems can already be implemented.

5.0 ACCESS CONTROL AND THE SMART CARD

A smart card can be used as part of an access control system to protect sensitive data. This chapter correlates the features of the smart card with general goals in computer access control.

5.1 Basic Access Control Concepts

As they are used more and more heavily, computer systems are greatly increasing in complexity, expanding to include combinations of large host computers, "dumb" terminals, personal computer workstations, and other devices, all linked together in extensive networks. The vast amounts of information contained in such computer systems can be made accessible to a widespread and diverse group of users. Ensuring the security of information in a computer system is an ever more difficult task.

In ever-widening information systems, there is no one comprehensive solution to the problem of providing computer security. Specific plans may, for example, need to be designed for the protection of

- information maintained within the system's large host computer(s),
- information maintained in personal computer workstations,
- information that is being transmitted between computers, and
- information kept in identification cards used for access (i.e., smart cards or passive storage cards).

Physical security measures, such as locks, gates, guards, badges, and other administrative methods, can provide some, although generally not all, of the necessary protection for a computer system. The use of cryptography is very often essential for computer security.

5.1.1 Cryptographic Techniques: Encryption and Message Authentication

Cryptography is the art or science of secret communications. It involves methods for converting information which is sensitive or secret from an intelligible *plain text* form to an unintelligible *cipher text* form. The process of converting plain text to cipher text is called encryption; the reverse process (converting cipher text to plain text) is called decryption. Most cryptographic algorithms make use of a secret value called a key. Encryption and

IPR2025-01149
Apple EX1035 Page 26

decryption are easy when the key is known, but decryption is intended to be virtually impossible without the key used for encryption.

Disguising and concealing secret messages via encryption has been the traditional purpose of cryptography. More recently however, the use of cryptography for *message (or data) authentication* has become widespread. Message authentication is a process for detecting unauthorized changes made to data which has been tranmitted between users and/or machines, or to data which has been retrieved from storage. Message authentication techniques can be used for plain text messages which do not necessarily have to be kept secret, as well as for encrypted messages.

The use of cryptography in message authentication is specifically aimed at protecting information from *intentional* modification by malicious intruders to the computer system. Simple accidental changes to data (e.g., those caused by problems in the transmission medium) can be pinpointed using ordinary error detecting codes. However, if the algorithm for the error detecting code is known, an adversary may be able to generate a modified code which corresponds with intentionally altered data. By using cryptography in message authentication, special "tamper-proof" checksums, often referred to as message authentication codes (MACs), can be generated. A cryptographic MAC is calculated using an encryption algorithm and a secret key. If the key is unknown, even a vary small change to a message will cause an unpredictable alteration of the MAC. Therefore, any intruder who intercepts authenticated messages and attempts to modify them will not know what the corresponding MAC for the altered message should be. [FP113 85]

Thus, cryptography can be used to ensure the safety of information, by making it unreadable and/or unalterable without detection, through encryption and message authentication. Physical security and cryptographic techniques combined can offer a great deal of security for a computer system. There is, however, yet another major component of computer security: user authentication for access control.

5.1.2 User Authentication

User authentication can be thought of simply as "making sure people are who they say they are" before allowing access to any element of a computer system. Unfortunately, because of the extensive use of electronic communications in modern computer applications, user authentication is not as easy as having a guard check photographs on ID badges. Some computer system users may never actually enter the computer facility, but instead access the system from remote workstations. A potential intruder may be able to pose as a legitimate remote user, and thus may never have to physically break into a computer room in order to abuse the system. Electronic authentication of all users attempting to log on to the system is necessary to address such threats.

User authentication typically involves verification of information which the user can be required to supply during a log on procedure. The information to be verified is drawn from at least one of the following categories:

IPR2025-01149
Apple EX1035 Page 27

(1) something the user KNOWS (e.g., passwords* or biographic information)

(2) something the user HAS (e.g., a magnetic stripe card or a smart card)

(3) some physical characteristic of the user (i.e., fingerprints, retina scans, or other biometric information)

In general, the more information each user must submit, the more time consuming and costly the user authentication process. However, requiring all users to submit information from each of the three categories provides the surest defense against intruders attempting to masquerade as legitimate users.

From an intruder's point of view, attempting to pose as an authorized computer user might seem a fairly straightforward attack. It might involve guessing passwords or forging magnetic stripe cards in order to elude the system's user authentication scheme. A more devious approach would be to masquerade not as a human user, but as a host computer or some other equipment in the system. An intruder could conceivably intercept communication lines between an unsuspecting user and a host computer and capture data which the user attempts to send to the host. The intruder could mimic messages which would have ordinarily been sent from the host to the user, and the user would have no reason to suspect an invasion of the system. The intruder could use such a technique to appropriate not only a few files which the user happens to transmit, but the user's password as well, for future masquerading endeavors.

5.1.3 Device Authentication

Because of such possible "spoofing" attacks, strategies for authenticating devices in a computer system may be necessary, in addition to user authentication procedures. For example, a cryptographic unit attached to a user's terminal might be required to authenticate itself to the host computer and vice versa. A cryptographic "challenge" procedure such as the following can be used to authenticate one device to another:

step 1: A secret cryptographic key is generated, and a copy is distributed to both of the devices which are to authenticate one another, e.g., the host computer and the cryptographic unit at the terminal. (Secure generation, distribution, and storage of the key are essential; methods for ensuring that the key is not compromised must be provided.)

step 2: One device initiates the authentication procedure by sending a message containing a random number or the current time and date to the other device.

---

* There are many criteria to be considered in the use of a password system for user authentication. For more information on this subject, the reader is refered to Federal Information Processing Standards Publication (FIPS PUB) 112, *Password Usage.* [FP112 85]

IPR2025-01149
Apple EX1035 Page 28

step 3: The device receiving the message uses the shared secret key to encrypt the message, and sends it back to the first device.

step 4: The first device encrypts the original plain text message (from step 2) and compares it to the encrypted message received from the second device. If the two encrypted messages are identical, then the identity of the second device is implicitly verified: an intruder attempting to masquerade as the second device would not have the correct secret key, and thus could not correctly encrypt the message. The use of a random number or the time and date in the message ensures that the message is not an intruder's replay of an earlier authentication message.

step 5: The roles of the two devices can be reversed and steps 2, 3, and 4 repeated so that both devices will be authenticated to one another.

Because no human can satisfactorily compute encryption algorithms by hand, some type of intermediary cryptographic device is necessary to perform authentication between the user and the host computer. To ensure that the cryptographic device has not been corrupted or replaced with a bogus device, the host may have to be authenticated to the cryptographic device (and vice versa), and the cryptographic device may have to be authenticated to the user (and vice versa). This would amount to four separate authentication procedures which would have to be performed in order to implicitly authenticate the user to the host, and vice versa. Figure 6 illustrates a general system in which a user and a host are authenticated to one another by means of an intermediary cryptographic device.

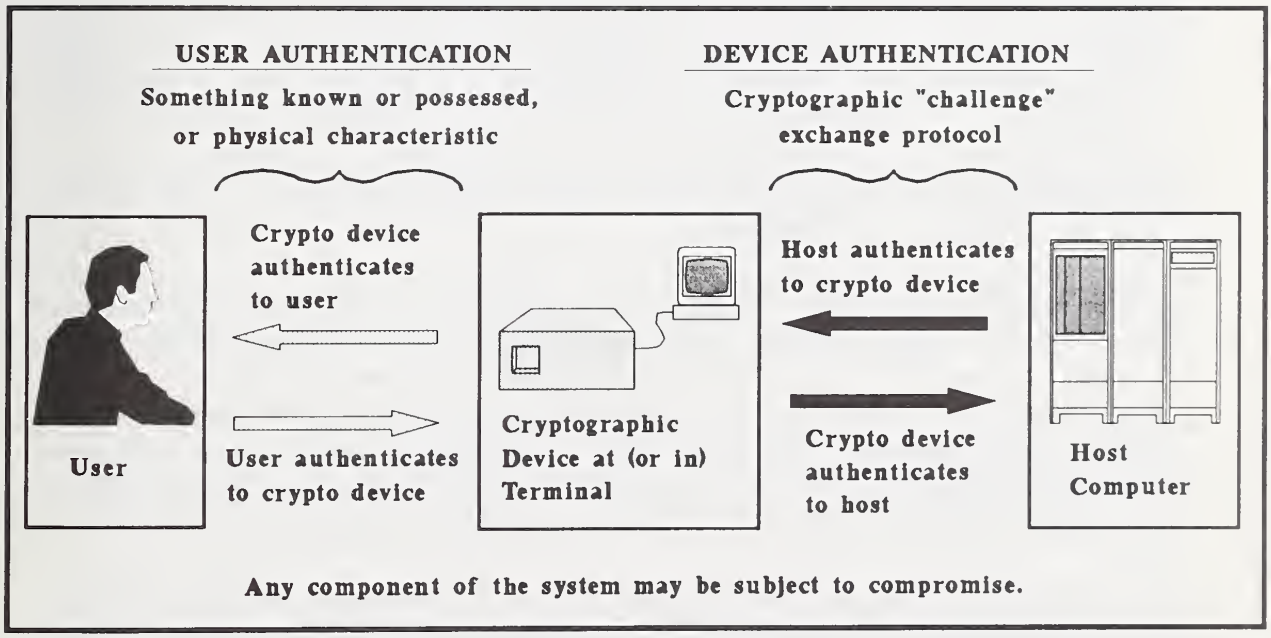


Figure 6. A General System of Authentication

IPR2025-01149
Apple EX1035 Page 29

5.2 The Smart Card and Authentication

Instead of a cryptographic device attached to (or inside) the terminal, a smart card could be used to perform the encryption operations needed for authentication. While a cryptographic device kept at the site of the terminal may be vulnerable to tampering, a smart card is intended to remain in the possession of its sole user, who is responsible for its protection. Cryptographic operations performed by a smart card thus have the potential to be more secure, because they are closer to the user.

Authentication procedures for a system using smart cards might proceed as follows:

1. *Authentication of the smart card to the user:* Authentication of the smart card to the user is intended to protect the user in the event that someone has secretly swapped a bogus card for the user's valid card. Since the user can keep a close watch on the smart card (by keeping it in his shirt pocket, for example), this type of threat should not be very great. Thus, the card-to-user authentication procedure is fairly simple: The user inserts the smart card into a "dumb" card-reader, the card reveals a predetermined password to the user (via the display on the card-reader), and the user verifies that the password is correct. If necessary, the user can specify a new password for the smart card to display during the next authentication procedure.

2. *Authentication of the user to the smart card:* To authenticate the user, the smart card sends a signal to prompt the user for a personal identification number (PIN). The card encrypts the PIN and compares it to an encrypted copy of the PIN stored in the card's memory. In addition to (or in place of) the PIN, the card may prompt the user to submit biometric information (such as a fingerprint, wristprint, or retina scan) via the appropriate reader or scanning device. The biometric information may be encrypted and compared to stored information in a manner similar to the PIN comparison. If the comparison fails for several consecutive tries, the card "locks up" and does not perform any further operations. (This prevents someone who has illegitimately acquired the card from obtaining any information.)

3. *Authentication of the host to the smart card:* Once the user has been authenticated, the smart card sends a random challenge value to the host. The host, which shares a secret cryptographic key with the smart card, encrypts the challenge and sends it back to the card. The smart card compares the host's response with its own encrypted version of the challenge. If the comparison is successful, the smart card prompts the host to begin smart card-to-host authentication. If the identity of the host cannot be verified, the smart card returns a warning/error message to the user.

4. *Authentication of the smart card to the host:* The host sends a random challenge to be encrypted by the smart card, and checks the smart card's response. If the smart card's response is correct, the authentication process terminates, and the user is allowed access to the host. (Steps 3 and 4 are often combined for efficiency.)

IPR2025-01149
Apple EX1035 Page 30

Figure 7 illustrates the use of a smart card in a process of authentication between a user and a host. Though a system of authentication using smart cards can be very intricate, it does not demand that the user perform any complicated operations. The commands needed to initiate and carry out the process are stored within the smart card. Thus, the user only needs to memorize one PIN and be able to recognize the smart card's password.

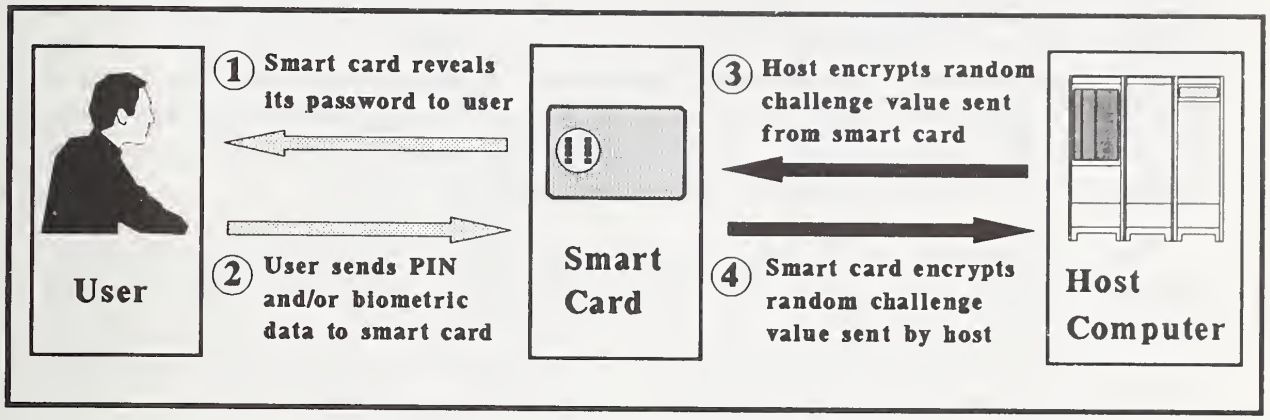


Figure 7. A System of Authentication Using Smart Cards

5.3 Smart Card Encryption Capabilities

As described above, the smart card is capable of encrypting short strings of data used in authentication procedures. Several encryption algorithms (some of which are company-proprietary) are currently available in smart cards. Implementations of the widely used Data Encryption Standard (DES)* algorithm are being developed for smart cards.

A smart card system of authentication provides a high degree of protection against unauthorized access and spoofing of computer system equipment by intruders. It is conceivable, however, that a particularly determined intruder could monitor a user-to-host connection and wait until all authentication procedures have been completed before attempting to intercept the communications. Encryption of all information passed between the user and the host is the most secure defense against such a threat.

The use of the smart card for extensive encryption operations is presently an open question. The processing speeds of most current smart card microcomputers are generally too slow for encryption of large files. If a large amount of bulk encryption is needed, it may be more cost- and time-efficient to use the host computer and/or a dedicated cryptographic

* The DES algorithm has been the U.S. government standard for cryptographic protection of unclassified data since 1977. For more information on this algorithm, the reader is referred to Federal Information Processing Standards Publication 46-1, *Data Encryption Standard.* [FP46-1 88]

IPR2025-01149
Apple EX1035 Page 31

devices for this task. However, it is likely that as smart card technology progresses, the use of the smart card itself for extensive cryptographic calculations will increase.

5.4 Secure Storage: Smart Card Memory Zones

Aside from its potential in cryptographic operations, the smart card can be made to perform a unique and important function: ensure the security of its own memory. The memory of a smart card may be divided into several zones, each with different levels of security, as required for an application. The smart card microprocessor and its associated operating system can keep track of which memory addresses belong to which zones and the circumstances under which each zone can be accessed.

Figure 8 illustrates a possible smart card memory divided into four zones: a secret zone, a confidential zone, a usage zone, and a public zone. A secret zone could be used for storage of information which can be used only by the microprocessor itself. Passwords, cryptographic keys, the card bearer's digitized fingerprint, or any other information which should never be readable outside of the smart card could be stored in this zone.

A confidential zone could be used to store an audit trail listing all transactions, or attempted transactions, made with the card. The confidential zone could have a password known only to the card issuer, who could examine the history of the card for evidence of misuse of the system. To prevent any attempts to modify the card's audit trail, the confidential zone could have a read-only access restriction.

A usage zone could be used for storage of information which is specific to the smart card application and which requires periodic updates and modifications. For example, the date of the card bearer's last access to the host computer, or the amount of computer time used, could be stored in the usage zone. Depending on the sensitivity of the data, a password could be required for this zone. The usage zone could have both read and write access protected by a password.

A public zone could be used for keeping nonsensitive information, such as the card issuer's name and address. The public zone could have read-only access, without a password.

The smart card's capacity for distinct memory zones presents several advantages. First and foremost is the smart card's ability to keep crucial secret information in a separate protected memory location. It may be possible to produce a smart card with features ensuring that the entire secret zone will be destroyed or "zero-ized" if any attempt is made to extract its secret data. Another advantage is the possibility of allotting separate memory zones for separate individuals (e.g., only the card bearer can access the usage zone, and only the card issuer can access the confidential zone). The actual allottment of memory zones depends on the application and the manufacturer's design.

IPR2025-01149
Apple EX1035 Page 32

At least one smart card manufacturer produces a card in which "lock bits" [MCT1 85, p. 18] can be set to prevent access to parts of the card's memory or to invalidate the card. For example, if a certain number of consecutive, unsuccessful attempts at accessing part of the card's memory are made, a lock bit might be set to permanently shut down the card. This would prevent someone who has illegitimately acquired the card from trying a long series of password guesses. Lock bits can be set during various stages in the life cycle of a smart card to ensure that important stored information cannot be tampered with.

SECRET ZONE

➡ **Unreadable**

For storage of passwords and cryptographic keys

CONFIDENTIAL ZONE

➡ **Read-Only, with Password**

For storage of an audit trail of card transactions

USAGE ZONE

➡ **Read/Write Access, with Password**

For storage of information actively used in applications

PUBLIC ZONE

➡ **Read-Only, without Password**

For storage of nonsensitive information, such as the issuer's name and address

Figure 8. Possible Smart Card Memory Zones

IPR2025-01149
Apple EX1035 Page 33

5.5 Smart Card Life Cycle*

As illustrated in figure 9, there are four general stages in the life cycle of a smart card: a manufacturing stage, an application preparation stage, an active use stage, and a retirement stage.

In the manufacturing stage, wafers of identical smart card ICs are produced at a chip manufacturer's plant. A general control program, suitable for several types of smart card applications, is burned in ROM for each IC. Programs for one-way tranformations or cryptographic algorithms may also be burned into ROM in this stage. A unique serial number and/or other identifying information is placed in the memory of each IC. A lock bit can be set once the serial number has been assigned to the chip to ensure that the memory location containing the serial number.cannot be overwritten or otherwise modified. The ICs are put into their plastic carriers, and any hardware input/output interfaces are attached. The smart cards are then shipped to various card-issuing organizations.

In the application preparation stage, the card-issuing organization tailors a shipment of generic smart cards for use in a specific application. Memory zones are allotted, as required in the application. Cryptographic keys and issuer passwords are written into each card's secret zone; lock bits may be set to prevent alteration of this information. Parameters may be established for the format of information to be later entered into the card. Once the card-issuer's specifications have been input, the individual who will actually carry and use the card may be called in to set card-bearer parameters. The card-bearer's password(s) and biometric information, such as a fingerprint or retina scan template (if required), are written into the card's secret zone. A lock bit may be set to protect this information also.

With all secret zone passwords and keys and all functional application parameters set, the smart card is ready for use and can be presented to the card-bearer. In the smart card's active use stage, information can be read from and written to the usage zone of the card's memory. (If the smart card contains EEPROM, information in the usage zone may also be erased, if necessary.) The card may be used to perform cryptographic algorithms or other functions, if it has been programmed to do so.

The smart card will remain in its active use stage until either 1) its memory is filled up (i.e., if the card has EPROM and not EEPROM), or 2) it has been invalidated. As described above, a smart card can be invalidated if several unsuccessful attempts at accessing a memory zone are made. Having entered its retirement stage, the card is no longer functional. The issuer may require that the card be returned or destroyed.

---

* The information for this subsection has been provided primarily by MicroCard Technologies, Incorporated, Dallas, Texas. [MCT2 85, pp. 5-6]

IPR2025-01149
Apple EX1035 Page 34

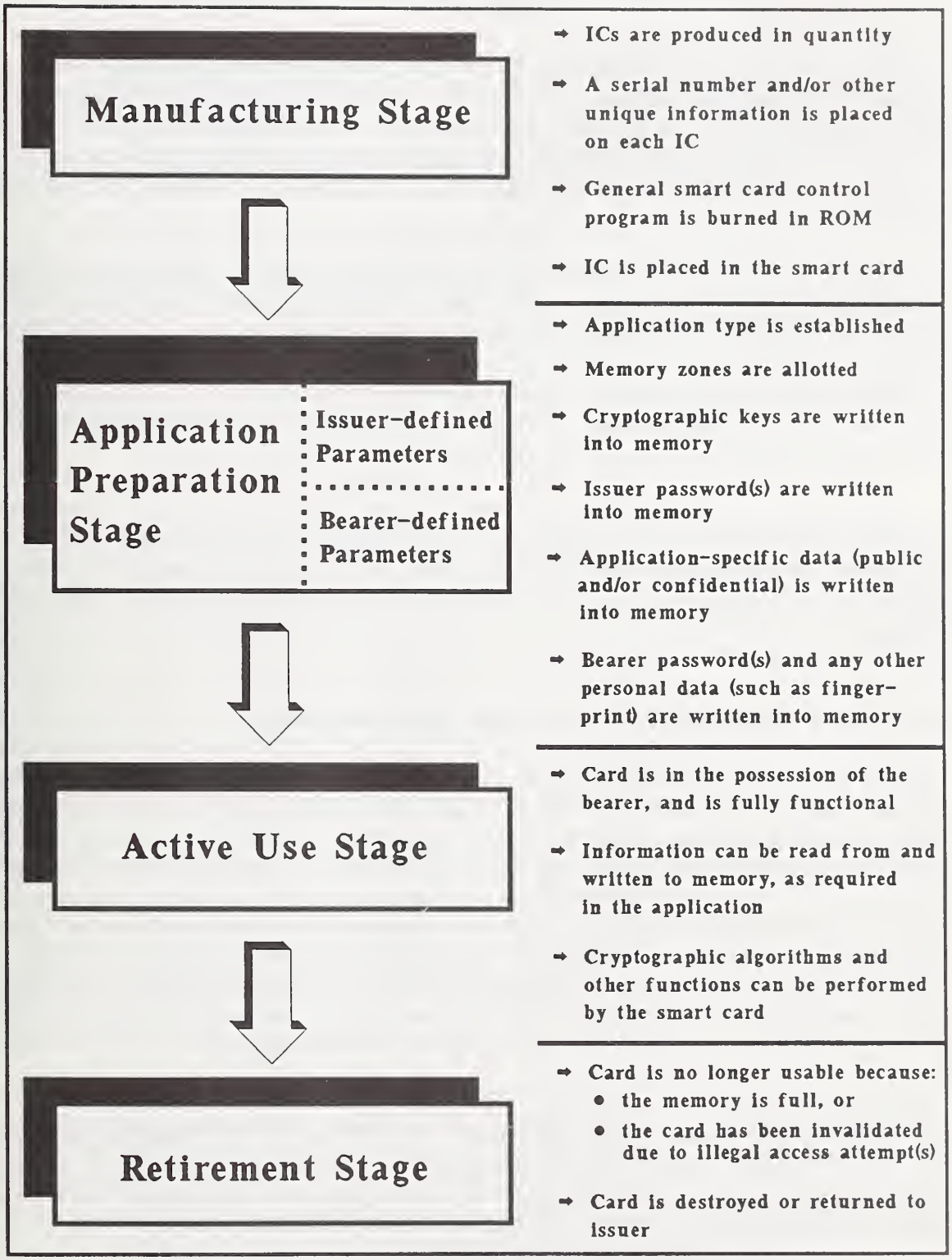


Figure 9. Life Cycle of a Smart Card

IPR2025-01149
Apple EX1035 Page 35

6.0 NBS ACCESS CONTROL RESEARCH

The National Bureau of Standards (NBS) has an ongoing goal of providing guideline documents and technical support to aid in the effective implementation of computer security measures. As part of this goal, NBS investigates authentication and access control methods, which may make use of passive storage tokens, smart cards, smart tokens, or hand-held cryptographic units. This chapter discusses planned and current NBS research in this area.

Passive devices, such as magnetic stripe and IC memory tokens (devices that contain only memory ICs and which may or may not be credit-card-sized), may be used in a user-to-host authentication process. A passive token can be used to store a password or cryptographic information which can aid in verification of a user's identity. In some systems, the host computer can send new information to be written into the passive token to be used for the next access attempt. Smart cards, which have computational capabilities, can be used in both user-to-host and host-to-user authentication processes.

NBS has been examining several authentication systems which employ either smart cards or passive storage tokens. Three access control systems have been implemented, using commercial products enhanced by NBS researchers, to illustrate how modern technology can be applied to improve access control between a host computer and a workstation or terminal.

6.1 NBS Plastic Memory Key Access Control Systems

The first two systems implemented at NBS make use of passive tokens, which may be read from and written to by a host computer, via a token reader device. Each plastic key-shaped token contains one or more IC memory chips, with a total capacity of 2000 bits (250 characters). [DTK 86, p. 5] Since their memory is EEPROM, the tokens can be repeatedly overwritten. The tokens are relatively low in cost, but they do not have any internal processing capabilities and cannot actively protect their stored information. If the information in the tokens is not stored in an encrypted form, then physical protection of the tokens is imperative for the security of the system. The token reader device has its own microcomputer and memory. It can be connected to a computer terminal with no internal processing capability or to a personal computer workstation.

NBS has implemented the plastic memory key system in two configurations: one for "dumb" terminals and one for workstations with cryptographic capabilities. In both configurations, the user is required to provide both a password and a token. This feature alone can prevent casual "hackers" from accessing many computer systems.

IPR2025-01149
Apple EX1035 Page 36

6.1.1 Access Control System for "Dumb" Terminals

In the first configuration, which was designed for "dumb" terminals, a user's plastic token is first initialized with a random (or pseudorandom) number generated by the host computer. During a subsequent log-on procedure, the user inserts the token into the token reader, and types a password into the terminal. The random value stored in the token is read by the host computer and compared with the value stored at the host.

If the two values are equal and the user-supplied password is correct, then access is granted. A new value is then generated and written into the token for the next access attempt. If this new value and the user's password were intercepted by a line tapper, the tapper could gain access to the host, but the valid user would be alerted on the next log-on attempt when access would be denied. In order to be reestablished in the system, the valid user would have to have the token reinitialized with a new value and password. Further unauthorized access would be prevented unless the line is again tapped.

6.1.2 Access Control System for Cryptographic Workstations

The second configuration (see fig. 10) was designed for personal computer workstations with cryptographic capabilities. Here cryptography is used to protect the transmitted data which is needed to authenticate the user to the host. A line tapper who intercepts this transmitted data will not find it useful, because it is in encrypted form. In this configuration, a user logs onto a host computer via a personal computer, rather than through a "dumb" terminal. Both the personal computer (PC) and the host are equipped to perform the DES encryption algorithm. The PC contains a master storage key (Key1) to be used with the DES algorithm. The host computer contains a second DES key (Key2), a random number (R), and a copy of the user's password, all of which are kept in protected storage. The user's token contains a copy of Key2 which has been encrypted using Key1 (abbreviated $E_{Key1}(Key2)$). The token is initialized with a copy of the random number R which has been encrypted by the host computer with Key2 (abbreviated $E_{Key2}(R)$.)

During a log-on procedure, the user inserts the token into the token reader attached to the PC. The PC reads the encrypted version of Key2 from the token and decrypts it using Key1. (This decryption operation is abbreviated $D_{Key1}(E_{Key1}(Key2)) = Key2$.) The PC reads the encrypted random number R from the token and decrypts it using Key2 (abbreviated $D_{Key2}(E_{Key2}(R)) = R$).

The user then enters a password via the PC's keyboard. The PC combines the password and the random number*, encrypts this combined value using Key2†, and sends the result to the host. The host performs the same combination and encryption operations on

---

* The password and the random number are combined by an "exclusive-OR" operation. The exclusive-OR operation (bit-by-bit addition modulo 2) is denoted by $\oplus$.

† Once it has finished encryption of the combined value, the PC destroys its copy of Key2. Key2 is never permanently stored in the PC.

IPR2025-01149
Apple EX1035 Page 37

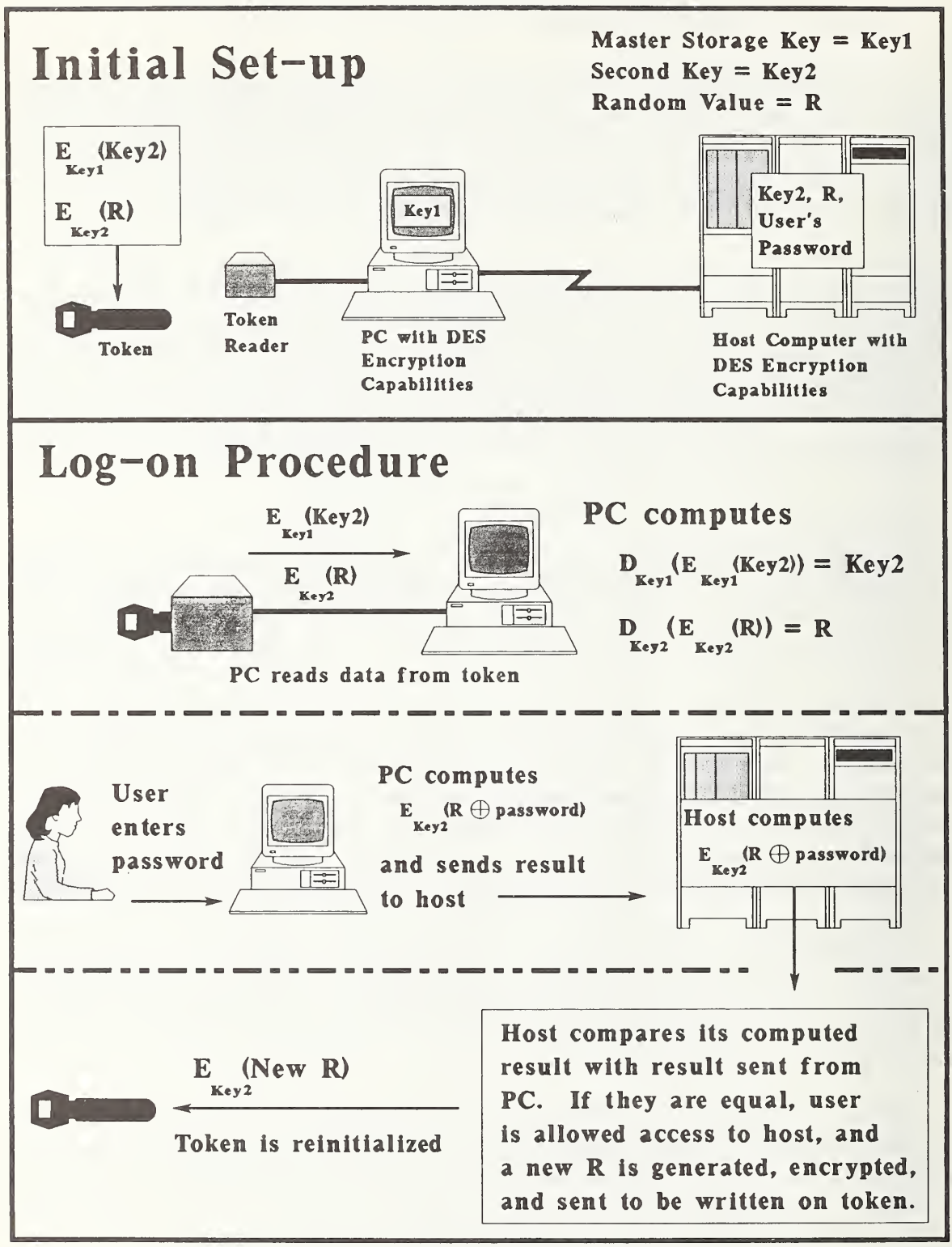


Figure 10. Access Control System for Cryptographic Workstations

IPR2025-01149
Apple EX1035 Page 38

the user's password and the random value stored at the host, and compares the result with the received result transmitted from the PC. If the comparison is successful, the user is allowed access to the host. A new random value is then generated by the host, encrypted under Key2, and sent back to the personal computer. The new encrypted random value is written into the user's token, for use in the next log-on procedure.

6.2 The NBS Biometric Smart Card Access Control System

The third access control system implemented at NBS uses a smart card designed to store a user's fingerprint template. In this system, the user must supply information from each of the three categories of user authentication data:

- something the user knows: a personal identification number (PIN)
- something the user has: a smart card
- some physical characteristic of the user: a fingerprint

As illustated in figure 11, this system consists of a fingerprint verification device, an NBS-designed switch, a dumb terminal, a printer, and a host computer. The fingerprint verification device includes a fingerprint scanner, a key pad, and a smart card reader/writer. The fingerprint verification device and the terminal are connected to the NBS-designed switch, which is in turn connected to the host. The switch permits both the fingerprint verification device and the terminal to communicate with the host over a single communications line. NBS enhanced the commercially available fingerprint verification device by giving it DES encryption capabilities.

In this system, the smart card is first initialized with the user's PIN and digitized fingerprint. During a subsequent log-on procedure, the user inserts the smart card containing the pre-recorded fingerprint information into the card-reader slot in the fingerprint verification device. The user then enters a PIN via the reader's key pad, and inserts the correct finger into the reader's print scanner. The fingerprint verification device compares the fingerprint and PIN entered by the user with the pre-recorded data read from the smart card. For each log-on attempt, the fingerprint verification device creates an access control record including the date, the time, the terminal number, the identification number of the smart card, and an indication of whether the user's identity is confirmed or rejected. This access control record is encrypted using DES and sent to the host.

The host decrypts the record and checks that it is not a playback of a previous record, and then grants or denies access, depending on the information in the record. Files of access control records can be maintained by the host computer as an audit trail for the system. At any time, the last user's fingerprint resident in the fingerprint verification device may be printed out upon request.

6.3 Future NBS Investigations in Access Control

NBS is now designing a smart card system for security in Local Area Networks (LANs). Because most LANs have very poor security features, any data sent on the network may

IPR2025-01149
Apple EX1035 Page 39

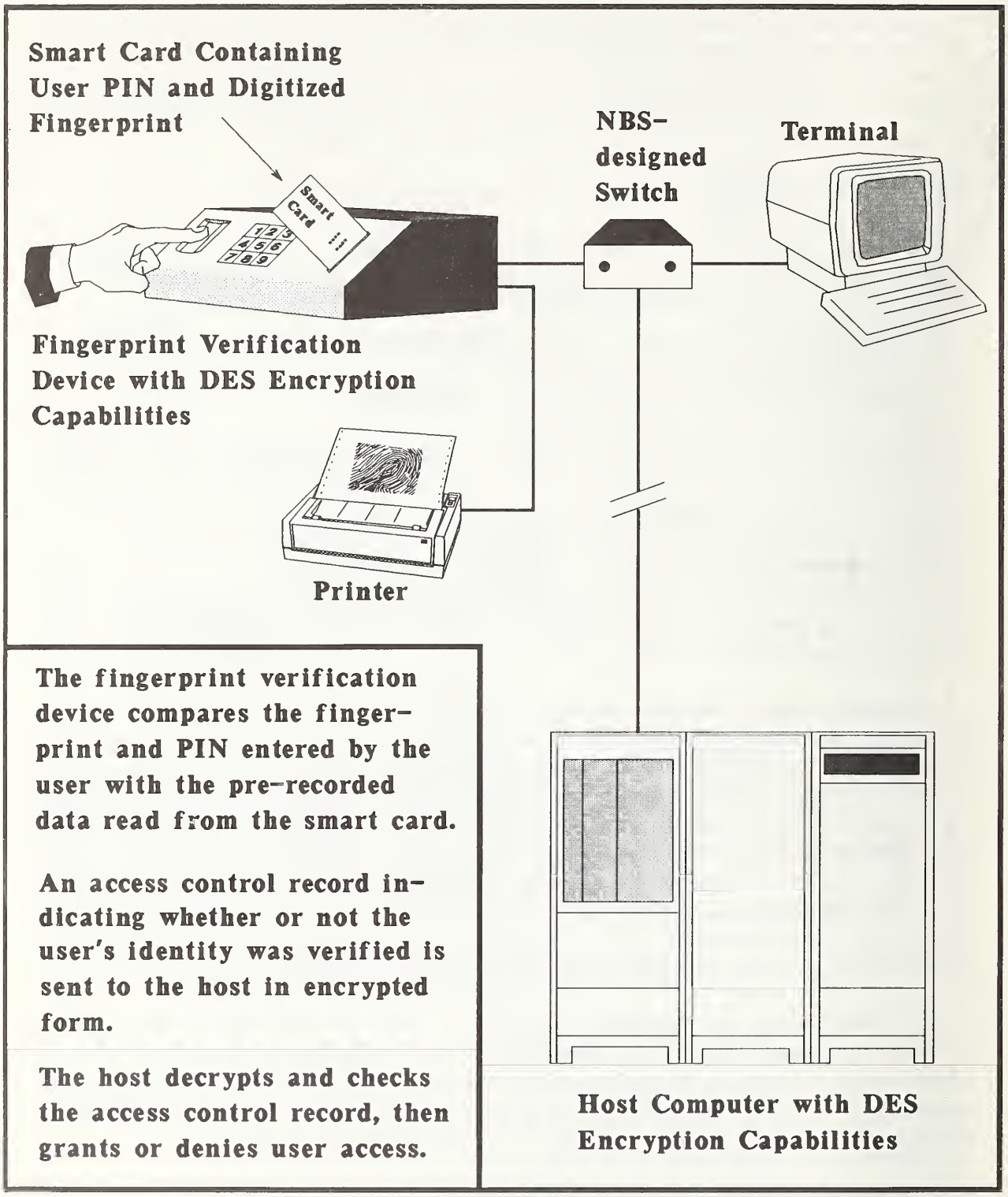


Figure 11. Biometric Smart Card Access Control System

IPR2025-01149
Apple EX1035 Page 40

be accessible to all users connected to the network. NBS plans to design a LAN security system whereby the LAN user is authenticated to an access control server by means of a smart card authentication system. The server will then check the user's request to communicate with another network user. If the request is allowed, the server will provide a cryptographic key to both users so that they may securely communicate with one another.

In addition, NBS is beginning investigations into smart tokens and hand-held cryptographic devices. Such products are often designed strictly as security mechanisms and are not necessarily intended to be used in everyday financial transactions for which devices must be restricted to credit-card size. NBS is considering the use of one smart token which is approximately 2" by 1" by 0.5" and contains approximately four times the nonvolatile programmable memory of current smart cards. [PRRY 88] Since it is much thicker than a smart card, such a smart token may be able to accomodate a larger, more powerful microprocessor, which could be used to perform more elaborate security procedures.

Another commercial product, a calculator-like hand-held cryptographic device, is also being examined at NBS for use in access control systems. This device can perform DES encryption of any seven digit number typed into its keypad. Using a DES key shared with the host computer, this device can be used to encrypt random challenge values sent from the host during a log-on procedure. The user types the challenge into the cryptographic device and then types the "answer" (the challenge value encrypted) into the terminal. If the "answer" is correct, the user can access the host. A system using this cryptographic device has the advantage that no specialized readers or hardware interfaces are necessary. It has the disadvantage, however, that the user may have to type at least two seven-digit numbers for each log-on procedure.

NBS will continue researching improved computer security methods as new products become available. The prototype systems already implemented at NBS illustrate some access control techniques which are now technologically possible. What will be possible in terms of cost, efficiency, ease of use, and other practical issues, is yet to be determined.

7.0 FUTURE SMART CARD FORECAST

The smart card is still in a relatively early stage of development, and its technological, economic, and social impact has not yet been realized. As researchers continue to explore smart card integrated circuit technologies, financial and government organizations are initiating test trials and limited prototype systems in order to examine the practical applications of the smart card. In 1985, MasterCard International began a test project in which 70,000 customers in Maryland and Florida were issued smart cards. [GLZR 86, p. 34] The Agricultural Stabilization and Conservation Service of the U.S. Department of Agriculture has implemented a smart card program to enhance record-keeping for 56,000 American peanut farmers. [CASA2 87, p.34] Results of such projects have generally been positive; however, further study will be required before smart cards can be put into wider use in the U.S. The acceptability of smart cards to a diverse group of users and the costs

IPR2025-01149
Apple EX1035 Page 41

associated with developing smart card systems are among the factors which still need to be considered.

7.1 Future Smart Card Costs

Smart cards have the potential for preventing tremendous financial losses due to weaknesses in current authentication and access control procedures. However, the initial costs of incorporating smart cards and their associated reader/writer devices into a security system is often an important concern. One source predicts that smart cards will undergo an immense growth in popularity and that manufacturers will "tap the economy of scale of mass production." [SVGL 85, p. 181] With an increase in public interest, smart card manufacturers may become more competitive, and smart card market prices may be driven down.

Underlying the market costs, of course, are the costs of the major components of smart cards: the integrated circuit chips. Long-term future costs of integrated circuits are difficult to predict, for several reasons. Some researchers believe that current methods for increasing the densities and capabilities of ICs will reach a limit, and greater circuit densities will be harder to obtain. "The point will come," one source suggests, "where it's no longer possible to shrink geometries any more without rendering the [conventional transistor] inoperable." [COLE 87, p. 81] New materials and production methods may have to be explored. With current technologies, chip prices, in terms of cost-per-bit of on-chip storage space, tend to decrease as circuit densities of the chips increase. [RANT 86, p. 2] It is unclear whether this trend will continue with new, and as yet undeveloped, IC production techniques. It has been suggested that as IC technology advances, ICs will have to be produced at completely automated construction facilities because, "the mere presence of a human being can contaminate the manufacturing process" of extremely complex chips. [WLSN 85, p. 83] Though it would require start-up investments, a changeover to completely automated construction might reduce labor costs, and thus help reduce or stabilize the costs of future ICs.

Some sources believe that the cost of an average smart card will decrease from the current range of $10 to $20 and stabilize in the $3 to $4 range within the next few years. It is unlikely that smart card costs will continue to fall indefinitely, however, because the demand for enhanced smart card capabilities will outweigh the demand for lower smart card prices. Very low cost smart cards may become technologically possible, but they may not be equipped with enough features to make them viable in the ever more demanding market.

7.2 Future Changes in Smart Card Integrated Circuitry

As smart card technology continues to develop, the circuitry used in smart card microcomputers will undergo many changes. One change which appears promising is the replacement of the conventional technology known as NMOS (n-channel Metal Oxide Semiconductor) with the newer CMOS (complementary MOS) technology. NMOS technology has

IPR2025-01149
Apple EX1035 Page 42

several qualities which have made it "the mainstay of present microprocessors." [HV&R 84, p. 393] NMOS circuits are fast and reliable, and can be densely packed onto small chips. Unfortunately, NMOS circuits are high in power consumption and tend to be susceptible to interference by "noise" from other devices. [MCIV 85, p. 157] CMOS circuitry uses much less power and has greater immunity to noise. The use of CMOS in smart cards may make on-card battery power supplies more feasible. Currently, CMOS circuits are more expensive and cannot be produced with densities as high as those of NMOS circuits. [MCIV 85, p. 158] However, CMOS technology is still relatively new; it is likely that these drawbacks in cost and circuit density will soon be overcome. Already several manufacturers have developed CMOS microcomputer chips suitable for smart cards.

7.2.1 The Role of EPROM in Future Smart Cards

Programmable memories will be of continued importance in the future of smart cards. For single-chip smart cards, EPROM is currently the most common type of programmable memory. The storage densities which can be attained using EPROM technology have been increasing continuously since EPROM was first introduced in the early 1970's. [RANT 86, p. 2] Figure 12 illustrates the general growth in capacity of dedicated EPROM chips.

Dedicated EPROM chips capable of storing as much as 1 million bits of information are currently being produced. However, current single-chip smart card microcomputers typically contain only 8,000 to 64,000 bits of EPROM, since much of the chip space must be used for other components (e.g., the microprocessor, RAM, and ROM). Because the general capabilities of EPROM have grown steadily and rapidly over many years, it is expected that the use of EPROM specifically for smart cards will also improve.

While EPROM is reliable and high in storage capacity, it is usually manufactured in such a way that it cannot be erased and reprogrammed when used in a smart card (see sec. 3.3). For this reason, EEPROM and other types of programmable memories will continue to attract the attention of smart card developers.

7.2.2 The Role of EEPROM in Future Smart Cards

Due to the complexity of EEPROM technology, current EEPROMs often suffer from reliability problems and have only one fourth of the storage density of EPROMs. However, EEPROM can be written and re-written thousands of times, and each write-to-EEPROM write operation takes considerably less power and less time than a write-to-EPROM operation. As manufacturers look towards making smart cards battery-powered, the reduced power consumption of EEPROM has particular appeal. Though few single-chip EEPROM smart cards are currently being marketed, several IC manufacturers have developed single-chip microcomputers containing EEPROM which may useable in smart cards. One expert predicts that, while advances in EEPROM will be made in the coming years, EEPROM and EPROM will eventually be replaced by new (and as yet un-named) nonvolatile read/write memories. [TASK 88]

IPR2025-01149
Apple EX1035 Page 43

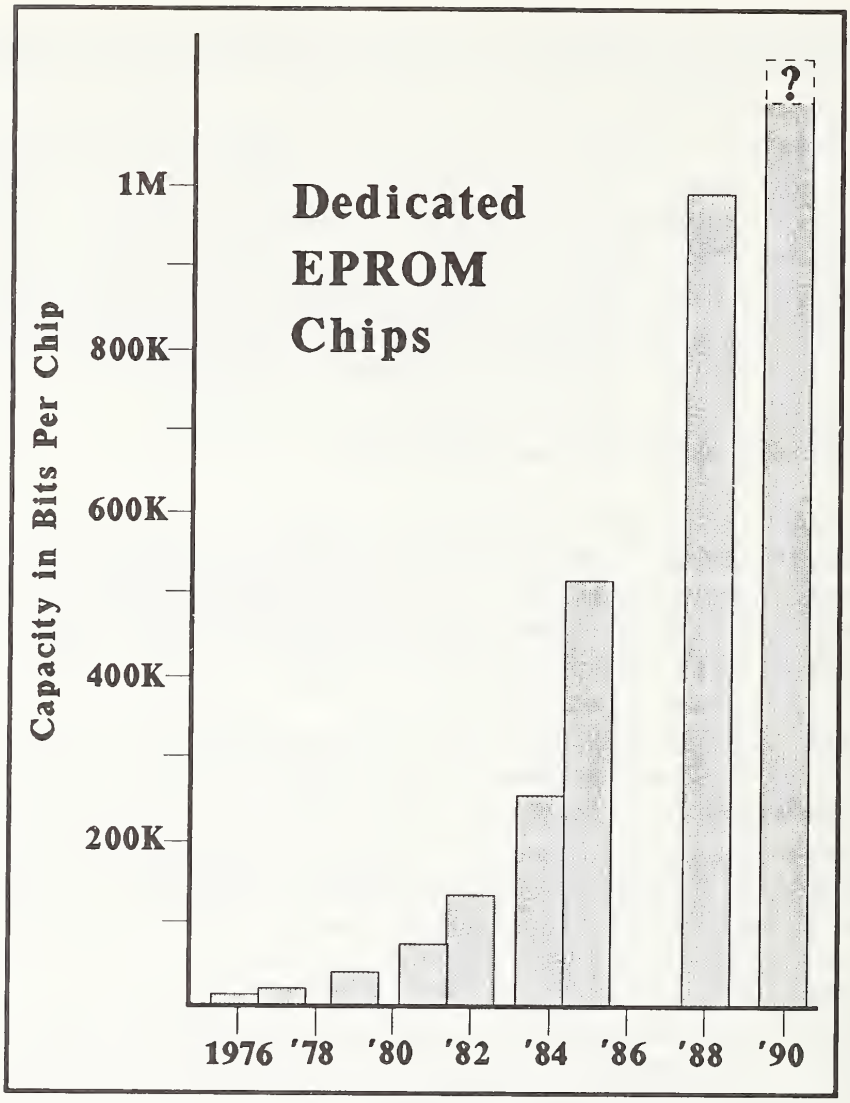


Figure 12. Approximate Storage Capacity of Dedicated EPROM Chips

7.3 Expected Changes in the Appearance and Construction of the Smart Card

In addition to changes in the circuitry hidden within the card, smart cards will undergo many noticeable transformations in appearance and contruction. As smart card reader/writer devices become more prevalent, smart cards may no longer have embossed regions or carry magnetic stripes. The written signature panel may also be dropped, since personal authentication will be carried out using electronic rather than visual means. Some sources suggest that smart cards will carry optical stripes for storage of extensive data files. However, since the optical stripe may not be addressable by the smart card microcomputer, the card reader/writer device may have to be equipped with an optical reader in addition to the integrated circuit interface.

IPR2025-01149
Apple EX1035 Page 44

Currently, many optical memory cards are made from fiberglass instead of the plastic traditionally used for credit cards. Fiberglass, which is more durable and less porous than plastic, may eventually be used for smart cards as well. However, while fiberglass provides better protection for electronic and optical components, it is currently much more expensive than plastic. Some sources predict that the smart card of the long-term future will consist of a shell of metal surrounding a sheet of fiberglass containing the electronic components.

It is likely that smart cards will retain the basic shape of a credit card in order to fit comfortably into wallets and pockets. However, smart cards will probably become thicker and less flexible as larger IC chips and/or more components are incorporated into the cards. The thicker smart cards may have touch-sensitive key pads and LCD displays which are flat and flush with the the card's surface. Future smart cards will probably have on-card power supplies, provided by solar cells, rechargeable batteries, or both. The thicker cards may be equipped with specialized interfaces which allow communication with peripheral IC memory cards, enhanced reader/writer devices, microprinters, personal computers, or other equipment. Figures 13 and 14 summarize some of the features of current smart cards and suggest several possibilities for smart cards of the future.

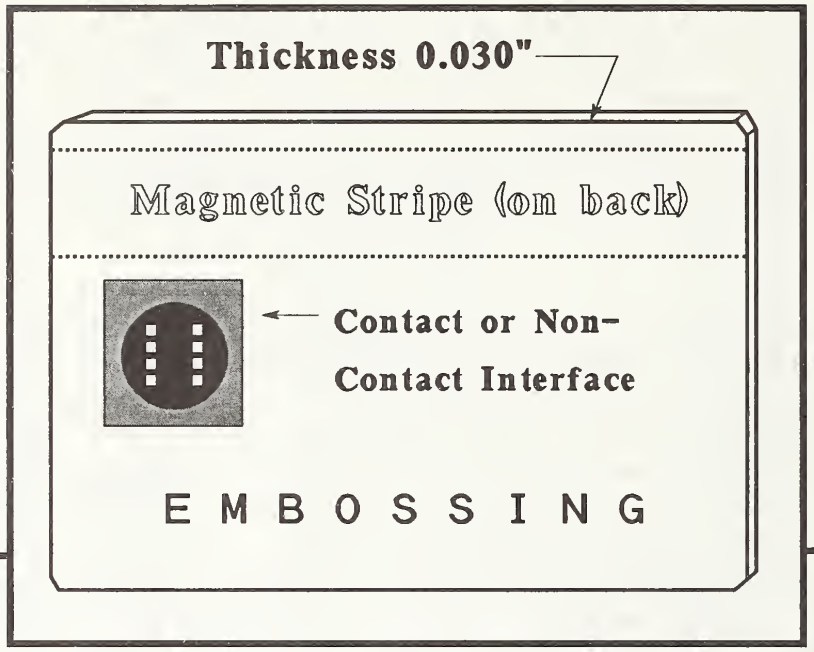
7.4 Expected Changes in Smart Card Operations and Applications

The enhanced features of the smart card will greatly affect the operations and applications of the card. The key pad and display will allow a direct user interface with the card; off-line operations will be possible, since the reader/writer device will no longer be the only means for communicating with the card. Smart cards will likely be programmed to perform cryptographic and arithmetic operations, and may incorporate the features of a pocket calculator in addition to their other processing capabilities.

As the smart card becomes a more independent unit, it will probably gain an increased capacity for testing and monitoring itself. The card may run tests each time it is turned on to verify that the battery (or solar cells), the key pad, the display, the reader/writer interface, and all other on-card devices are functioning properly. Any malfunctions could be reported directly to the user via the display. The card could also alert the user if any unauthorized access attempts have been made. A thorough self-test capability in future smart cards may provide means for detecting card-tampering and may increase user confidence in the card's reliability and security.

Security in the smart card will be of ever greater importance as the card is used for protecting larger and more diverse files of user data. It may eventually be possible to produce one smart card which will be used in several applications simultaneously. For example, one card could store a user's account balances from several different financial institutions. The card could be designed to allow the user access to any of this information while limiting access by a bank's reader/writer device to only the records on the card which pertain to that bank.

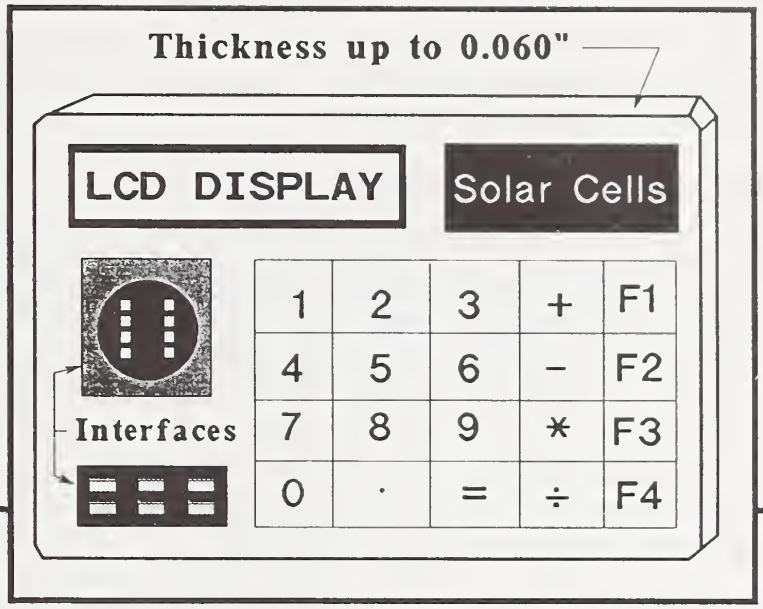
IPR2025-01149
Apple EX1035 Page 45



Size:	Standard Credit-Card Size: 2.125" by 3.370" by 0.030"
Appearance:	Contact or Non-contact Interface Embossing Magnetic Stripe
Construction:	Laminated Plastic
Integrated Circuitry:	(Approximation for Single-Chip Smart Card) 13 Kbits of ROM 300 Bits of RAM 8 Kbits of EPROM or 2 KBits of EEPROM NMOS Microprocessor
Power:	Supplied by Reader/Writer Device

Figure 13. Current Smart Card Characteristics

IPR2025-01149
Apple EX1035 Page 46



Size:	Somewhat Thicker Than Current Credit Card: 2.125" by 3.370" by 0.030" to 0.060"
Appearance:	Contact or Non-contact Interfaces to Reader/ Writer Devices and/or Other Equipment No Embossing; No Magnetic Stripe Touch-Sensitive Key Pad; LCD Display
Construction:	Laminated Plastic, Fiberglass, and/or Metal
Integrated Circuitry:	EPROM, EEPROM, and/or New Nonvolatile Memories, Increased Capacity ROM and RAM Higher Speed CMOS Microprocessor
Power:	Supplied by On-Card Battery and/or Solar Cells

Figure 14. Possible Features for Future Smart Cards

IPR2025-01149
Apple EX1035 Page 47

As the capabilities of the smart card increase, the variety of smart card applications will increase. In addition to expanding in the general access control functions for which they are particularly well suited, smart card systems may become the method of choice for managing medical records, educational records, passports, drivers' licenses, and many other extensive databases of personal information.

7.5 The Role of Standards in the Future of Smart Cards

Today there is a growing number of smart card and smart token manufacturers around the world, and there are already dozens, perhaps hundreds, of different smart card and token interfaces and interface protocols. While there may be a need for specialized cards or tokens in certain access control control systems, extensive use of smart cards in everyday activities depends on the interoperability of cards and card reader/writer devices produced by different companies. The current efforts of the International Organization for Standardization (ISO) and the American National Standards Institute (ANSI) may yield standards for contact-type smart cards (and their corresponding reader/writers) which will help steer the smart card industry toward interoperability.

While standardization of the contact-type smart card is a very significant first step, continued standards development will be crucial in the evolution of the smart card. One source suggests that, "All locations, time periods, industries, and applications are legitimate expectations for Smart Card realization. The Smart Card will be an important tool in the hands of mankind." [SVGL 85, p. 183] However, without adequate national and international standards, the usefulness of this tool will be severely limited.

IPR2025-01149
Apple EX1035 Page 48

APPENDIX: STANDARDS ACTIVITIES FOR INTEGRATED CIRCUIT CARDS

The International Organization for Standardization (ISO), which develops international standards for many fields, is comprised of numerous organizational units. Technical Committees, the largest ISO organizational units, are made up of Subcommittees, which in turn are made up of Working Groups. There are two Technical Committees currently supporting standards activities for integrated circuit cards: Technical Committee 68 and Joint Technical Committee 1. The newly-formed Joint Technical Committee 1 represents a combined effort between ISO and the International Electrotechnical Commission (IEC), an electronics and electrical engineering standards organization. Figure A1 outlines the organizational structure of the ISO groups involved with integrated circuit card standards.

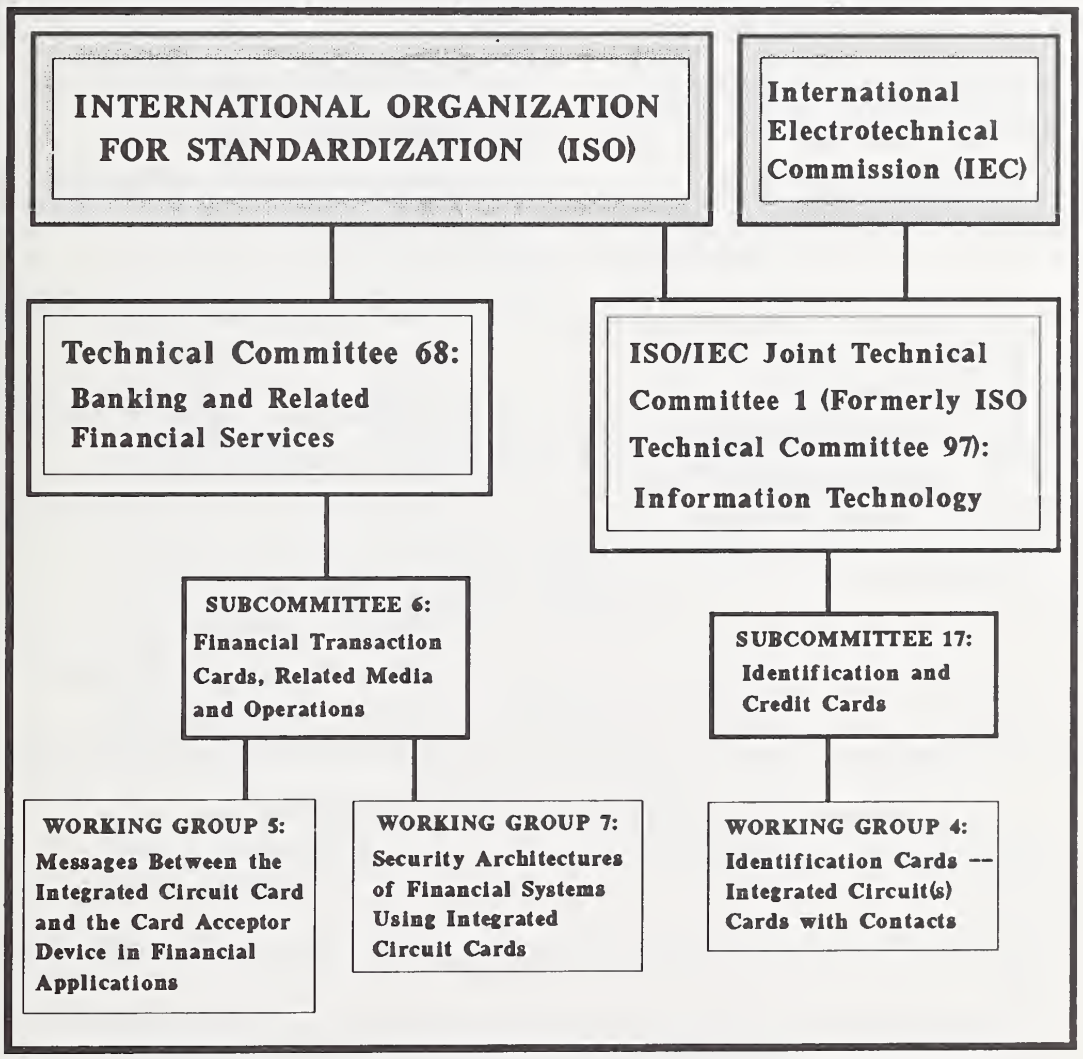


Figure A1. ISO IC Card Standards Groups

IPR2025-01149
Apple EX1035 Page 49

The American National Standards Institute (ANSI) does not, in itself, write or develop standards; rather, it accredits standards committees and supervises standards-making activities. Figure A2 outlines the organizational structure of the ANSI-accredited groups involved with integrated circuit card standards.

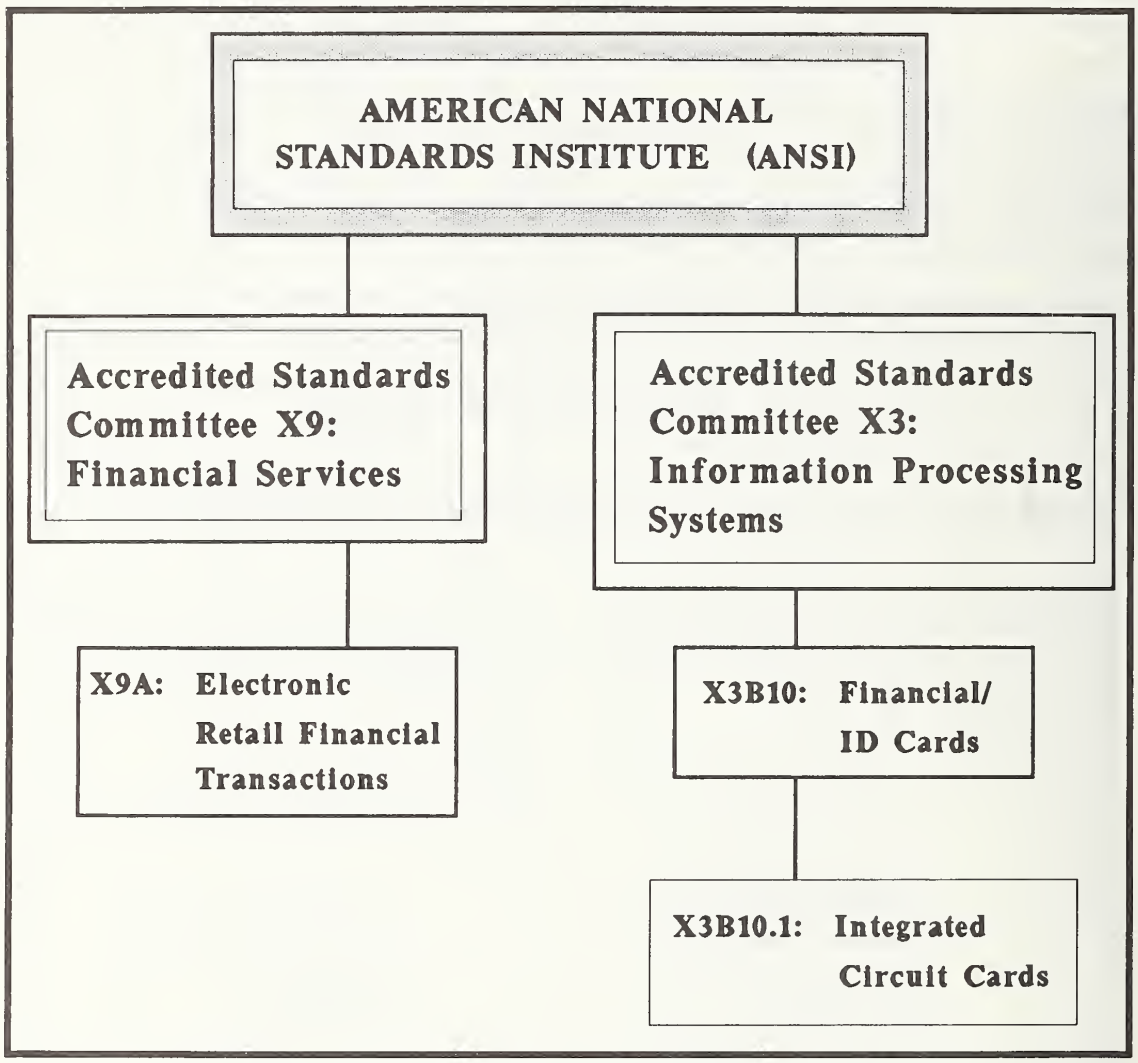


Figure A2. ANSI IC Card Standards Groups

IPR2025-01149
Apple EX1035 Page 50

REFERENCES

[AUGT 84] Augarten, Stan. *Bit by Bit: An Illustrated History of Computers.* Ticknor & Fields, New York, 1984.

[BRNS 86] Barnes, Robert, and Lawrence Kilty. "The Credit Card for the Nineties," *The Credit World*, May/June 1986, pages 36-40.

[BRNY 86] Barney, Clifford. "Smart Card: Will It Create a Billion Dollar IC Business?" *Electronics*, December 18, 1986, pages 55-58.

[BWRS 86] Bowers, Dan M. "Choosing the Right Card," *Security World*, June 1986, pages 42-47.

[CASA1 87] Casatelli, Christine. "All the Card You'll Ever Need," *Federal Computer Week*, June 1, 1987, pages 24-25.

[CASA2 87] Casatelli, Christine. "The Dawning of Smart Card Applications," *Federal Computer Week*, June 8, 1987, pages 34-35.

[COLE 87] Cole, Bernard C. "Here Comes the Billion-Transistor IC," *Electronics*, April 2, 1987, pages 81-85.

[DTK 86] Datakey, Incorporated, *Netlock Manual*, (Technical Specification for Models NL1400 and NL1400M Netlock Access Control Module), July, 1986.

[FP46-1 88] Federal Information Processing Standards Publication (FIPS PUB) 46-1, *Data Encryption Standard*, January 22, 1988. National Bureau of Standards, U.S. Department of Commerce.

[FP112 85] Federal Information Processing Standards Publication 113, *Password Usage*, May 30, 1985. National Bureau of Standards, U.S. Department of Commerce.

[FP113 85] Federal Information Processing Standards Publication 113, *Computer Data Authentication*, May 30, 1985. National Bureau of Standards, U.S. Department of Commerce.

[GLZR 86] Glazer, Sarah. "Smart Cards," *High Technology*, July 1986, pages 34-43.

[HV&Z 84] Hamacher, Carl V., Zvonko G. Vranesic, and Safwat G. Zaky. *Computer Organization*, Second Edition. McGraw-Hill, Incorporated, New York, 1984.

IPR2025-01149
Apple EX1035 Page 51

[LNDN 86] Linden, Larry F. "Taking the Media to Task," *Personal Identification News*, April 1986, page 4.

[MCT1 85] Micro Card Technologies, Incorporated, *Micro Card (Mask: M4) Designer's Guide*, Version 1.8, October 9, 1985.

[MCT2 85] Micro Card Technologies, Incorporated, *Micro Card (Mask: M4) Technical Overview*, Version 1.0, November 13, 1985.

[MCIV 85] McIvor, Robert. "Smart Cards," *Scientific American*, November 1985, pages 152-159.

[PRRY 88] Perry, John G., Technical Support Manager, Ultron Labs Corporation. Private Communication, April 19, 1988.

[RANT 86] Rant, Jon. "Intel's EPROMs: Lasting Memories for the Long Haul," *Solutions*, March/April 1986, pages 2-7.

[RSKI 87] Rosinski, John J. "Smart Card Puts a Database in Your Pocket," *AT&T Technology Products, Systems and Services*, Volume 2, #2, 1987.

[SVGL 85] Svigals, Jerome. *Smart Cards: The Ultimate Personal Computer*, MacMillan Publishing Company, New York, 1985.

[SVGL 87] Svigals, Jerome. "Wall Street Journal Offers How-To Course in ATM/PIN Fraud," *Smart Cards and Comments*, June 1987, page 4.

[TASK 88] Taskett, John, Customer Support Manager, Micro Card Technologies, Incorporated. Private Communication, June 8, 1988.

[WLSN 85] Wilson, John W. "Superchips: The New Frontier," *Business Week*, June 10, 1985, pages 82-85.

IPR2025-01149
Apple EX1035 Page 52

NBS-114A (REV. 2-80)

U.S. DEPT. OF COMM. **BIBLIOGRAPHIC DATA SHEET** *(See instructions)*	1. PUBLICATION OR REPORT NO. NIST/SP-500/157	2. Performing Organ. Report No.	3. Publication Date September 1988

4. TITLE AND SUBTITLE

Smart Card Technology: New Methods for Computer Access Control

5. AUTHOR(S)

Martha E. Haykin and Robert B.J. Warnar

6. PERFORMING ORGANIZATION *(If joint or other than NBS, see instructions)*

NATIONAL BUREAU OF STANDARDS
U.S. DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.

8. Type of Report & Period Covered
Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS *(Street, City, State, ZIP)*

Same as item 6

10. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number 88-600577

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)*

A smart card is a credit-card-sized device containing one or more integrated circuit chips, which perform the functions of a microprocessor, memory, and an input/output interface. Smart cards, and other related devices, may be used to provide an increased level of security in applications requiring controlled access to sensitive information. This publication describes the basic components of a smart card, and the goals and obstacles of smart card application development. Possible roles for smart cards in modern computer security systems and research conducted at the National Bureau of Standards (NBS) in the area of smart card access control systems are discussed. A forecast is made for the characteristics and applications of future smart cards and related devices. An overview of current standards activities for smart cards is given in an appendix.

12. KEY WORDS *(Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)*

access control; authentication; biometrics; computer security, cryptography; Data Encryption Standard (DES); electrically erasable programmable read-only memory (EEPROM); erasable programmable read-only memory (EPROM); integrated circuit card;microcomputer; reader/writer device; smart card; token

13. AVAILABILITY

☒ Unlimited
☐ For Official Distribution. Do Not Release to NTIS
☒ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.
☒ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES
52

15. Price

USCOMM-DC 6043-P80

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SCIENCE & TECHNOLOGY

Superintendent of Documents,
Government Printing Office,
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Bureau of Standards Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

☆U.S. Government Printing Office : 1988 - 201-597/92560

U.S. Department of Commerce
National Institute of Standards and Technology
(formerly National Bureau of Standards)
Gaithersburg, MD 20899

Official Business
Penalty for Private Use $300

Stimulating America's Progress
1913-1988