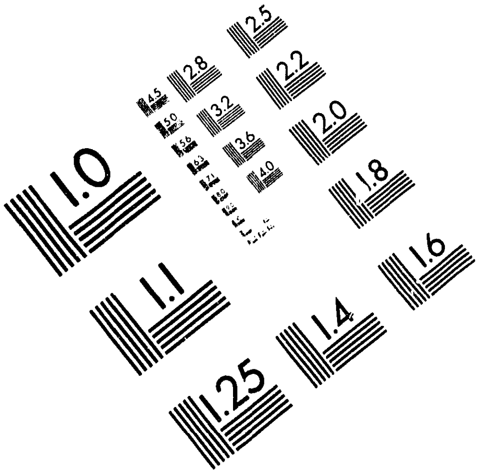
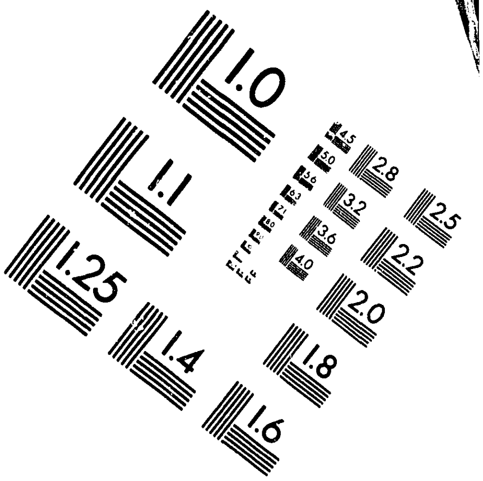
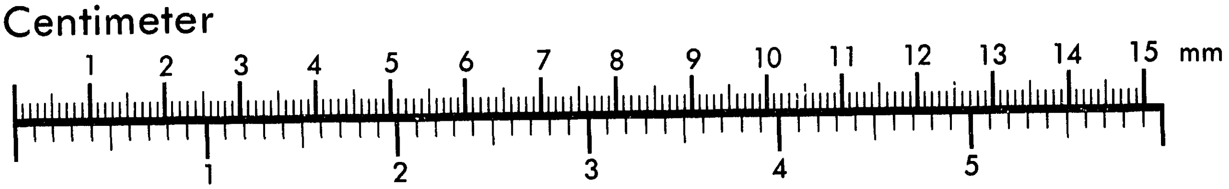


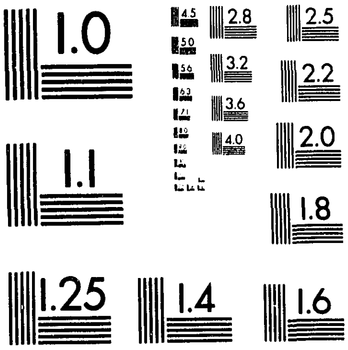


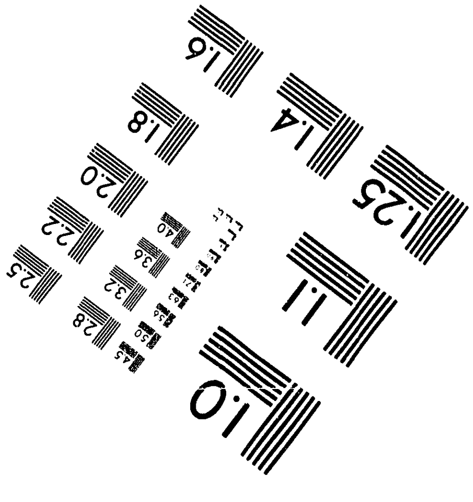
Association for Information and Image Management

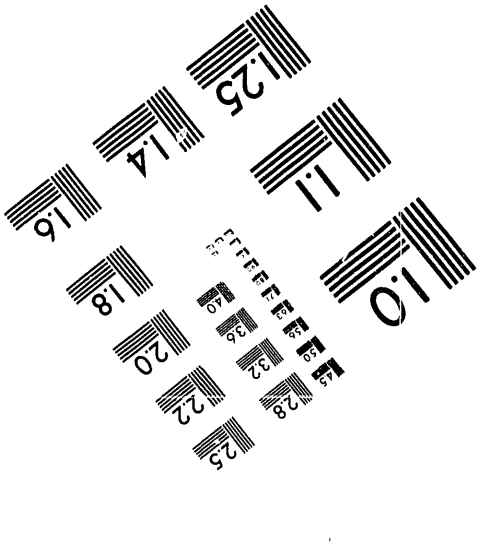
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

301/587-8202









MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

WHC-SA-1956-FP

Smart Card Multiple Function Badge

R. A. Nelson

Date Published
June 1993

To Be Presented at
Industry Symposium on
Security Technology
Virginia Beach, Virginia
June 21-24, 1993

Prepared for the U.S. Department of Energy
Office of Environmental Restoration and
Waste Management

Westinghouse
Hanford Company
P.O. Box 1970
Richland, Washington 99352

Hanford Operations and Engineering Contractor for the
U.S. Department of Energy under Contract DE-AC06-87RL10930

rb

Smart Card Multiple Function Badge

R.A. Nelson

ABSTRACT

Smart cards are credit card-sized computers with integrated data storage, an operating system to manage the data, and built-in security features that protect the data. They are used to distribute information to remote sites, providing the same or greater reliability, data integrity, and information security than a network system. However, smart cards may provide greater functionality at a lower cost than network systems.

The U.S. Department of Energy Hanford Site is developing the smart card to be used as a multiple function identification badge that will service various data management requirements on the Site. This paper discusses smart card technology and the proposed Hanford Site applications.

CONTENTS

FIGURES

LIST OF TERMS

APDU	application protocol data unit
CAD	card-acceptor device
EEPROM	electrically erasable programmable read-only memory
EPROM	electrically programmable read-only memory
IC	integrated circuit
ISO	International Organization for Standardization
PIN	personal identification number
RAM	random access memory
ROM	read-only memory
SPOM	self-programmable one-chip microcomputer

1.0 INTRODUCTION

Machine readable computer cards carry information that is available for computer transactions. Computers equipped with card readers can read or transfer this information from the card directly into their system memory, where they process the information. Common techniques used to carry information on computer cards are optical, magnetic, or integrated circuit (IC). Figure 1 shows the relationship of computer card technologies.

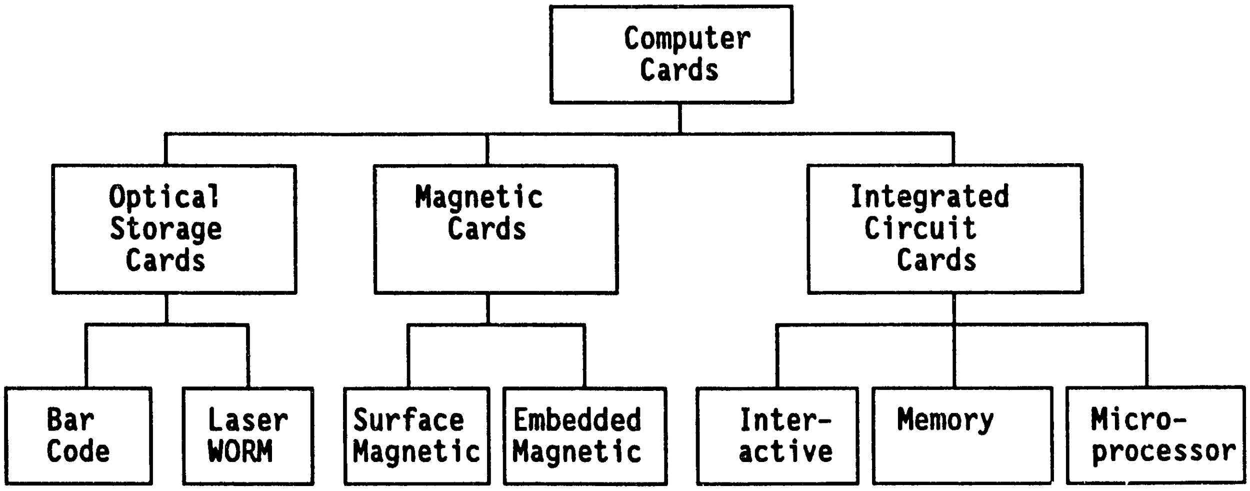


Figure 1. Computer Card Topology.

Smart cards are IC cards with the distinction that the IC card is a fully functioning microprocessor.

2.0 SMART CARDS

A smart card is really three components: a plastic card, a microprocessor, and a signal/communication interface. The plastic card is a convenient package for the microprocessor and provides a place to print text and graphics. Smart cards are generally produced in credit card format, but have also been packaged in plastic keys, dog tags, and other forms.

The microprocessor is the functional component in smart cards. It is a self-programmable one-chip microcomputer (SPOM) that incorporates the central processing unit, memory, communication port, and control logic on a single chip. The IC engineers optimize the microprocessor for security, communication, and the physical demands of the smart card environment.

The microprocessor stores programs and data in read-only memory (ROM), random access memory (RAM), electrically programmable read-only memory (EPROM), and electrically erasable programmable read-only memory (EEPROM). The manufacturer programs the operating system into ROM during microprocessor manufacturing. The RAM provides storage for temporary data, microprocessor state conditions, and input/output buffers. Write-once EPROM memory provides programmable, permanent information storage for serial numbers and other fixed information. The EEPROM is nonvolatile read/write memory and compares to a computer disk drive. It is the storage location for data and application program files with common capacities of 2,000 to 8,000 bytes[1].

The physical demands placed on smart cards through their use limits the practical size of the microprocessor. The microprocessor must resist damage caused by card bending, and it must fit into the standard credit card thickness. These two physical constraints limit microprocessor size to a 25-mm^2 (0.04-in^2) area and a 0.076-mm (0.030-in.) thickness. The size determines the number of transistors in the microprocessor and, consequently, the memory size and microprocessor's capabilities.

Data compression techniques may be used to increase the effective EEPROM storage in the smart card. Data compression techniques remove redundant and nonessential data, maximizing the capacity of the memory. Decompression restores the information to its original content. The size reduction or savings depends on the information type (e.g., photograph and text) and the compression technique used.

The smart card is not a self-contained computer, it requires power and timing signals from an external source to communicate with other computers and devices. The signal interface provides a mechanism for the microprocessor to communicate with external devices and a way for power and timing signals to reach the microprocessor. The signal interface, either a set of metal pads on the card surface or subsurface plates, determines how the smart card interfaces to other systems.

3.0 SMART-CARD-TO-SYSTEM INTERFACE

Card-acceptor devices (CADs) provide the physical interface between the smart card and other devices. The CAD holds the smart card in place and includes a set of leads that correspond to the interface pads on the smart card. The CAD provides power and timing signals plus a lead for serial communication between the smart card and other devices.

The most widely used smart cards have metal surface pads and are called "contact smart cards." The CAD physically couples with the smart card contacts and passes signals through conductance. Standards published by the International Organization for Standardization (ISO) define the physical location, name, and functions of the individual contacts as power (V_{cc}, ground, and V_{pp}), clock, input/output, and reset. The CADs designed for ISO contact smart cards use leads that couple with the smart card contacts in standard positions, meaning they can couple with ISO cards from different manufacturers.

Smart cards with subsurface leads are called "contactless smart cards." These cards receive power through inductive coils and exchange signals through capacitive plates. The term contactless does not mean a proximity-type smart card, the effective range is only about 2 mm (0.08 in.). Immaturity of ISO standards for contactless cards make them a less attractive alternative for multiple function applications.

[1] Smart cards with 16,000 to 128,000 bytes have been developed, they but are not standard products.

While standards define contact arrangement, smart cards from different manufacturers are not necessarily interchangeable. This is due to the difference in the manufacturers' electrical signals and software protocol requirements. The solution to incompatibility is a CAD with a processor module. This processor module detects the smart card manufacturer and provides information that allows the terminal controller to determine the correct communication protocol. A CAD processor module provides a system interface to smart cards from different manufacturers and also may support multiple technologies (e.g., magnetic stripe and bar code).

The terminal controller (connected to a CAD) uses a software protocol as a data interface between itself and smart cards. This protocol is the application protocol data unit (APDU) and is implemented in software that executes in the terminal controller. The APDU translates service requests from application programs running in the terminal controller into commands for the smart card. These commands are formatted with a message code and a data field and used to pass command requests and data between the terminal controller and smart card. The smart card services or refuses each command by returning a response (i.e., return value, error code) and acting appropriately depending on the current smart card security status.

4.0 INFORMATION AND PHYSICAL SECURITY

Computer card transactions generally require a card, a remote reader, and a centralized host computer. The role of the centralized host computer is to verify the authenticity of the card and control and record the transaction. The capabilities of smart cards allow them to authenticate themselves and record the transaction, effectively eliminating the need for a centralized host computer and online network. Authentication and transaction recording are handled at the remote site by the smart card and transaction terminal.

Large amounts of information stored in a portable package requires a security design that prevents data compromise and counterfeit cards. This is achieved by using logical and physical protection measures and card authentication to maintain information security.

4.1 LOGICAL SECURITY FEATURES

The logical architecture, which includes the operating system and file access control, manages access to information stored in the microprocessor. The logical architecture protects information using the following techniques.

- Data is not written or read directly by a reader; rather it is written or retrieved using command requests from a host system, with the microprocessor controlling access to the data.

- Data file access authorizations (e.g., read and write) are protected with password-type data access control.

- Algorithms proving data encryption are available for information communicated between the card and terminal controller.

- The operating system protects internal security information in hidden data areas.

- The personal identification numbers (PINs) and cryptographic keys never leave the card, so that they cannot be captured and analyzed.

- Cards "lock up" after successive invalid PIN entries.

- Authority access matrices determine whether an instruction executed in one memory area can access data stored in another area.

4.2 PHYSICAL SECURITY

The physical design of the smart card helps prevent information compromise by providing tamper detection and tamper resistance. Techniques that may be manufactured into the smart card microprocessor are as follows.

- Memory, CPU, and logic are integrated onto a single IC with no external bus that can be monitored.

- Tamper detection devices disable the microprocessor when card tampering is detected.

- Isolated circuits and supply-current scrambling prevent current load monitoring that could be used to determine number of bits set in a ROM or EEPROM byte.

- Tamper protection by card layering, microprocessor embedding, protective coatings, and epoxy technologies prevent compromise through layer and IC removal.

- Encoded address information and small transistor size in ROM prevents information from being read by a microscope.

- Leads used for IC testing are fuse connected, then blown before the cards are issued.

- The smart cards and ICs are manufactured in secure facilities where the chip wafers are accounted for, tested, and assigned a unique serial number.

4.3 CARD AUTHENTICATION

Smart card authentication is the cornerstone of smart card system security. Card authentication proves that a smart card is valid and belongs to the system. The same function is performed in traditional card system using a physical connection from a central computer to remote terminals in network systems. Smart card systems use smart cards' processing capabilities for authentication. Ignoring authentication of either the terminal or the card, even when the data is protected by a PIN, severely compromises the system's integrity.

Smart card and terminal authentication are accomplished using cryptographic techniques with secret keys stored in both the card and terminal. Through a series of interactions between the smart card and terminal both are able to verify authenticity of the other, without sharing secret information (i.e., passwords).

This approach requires that the terminal generate a random number, encrypt the number with a secret key, then send it to the smart card. The smart card decrypts the number with its secret key and returns the number to the terminal. The premise of the proof is that only a card with the proper secret key can return the original random number. The terminal compares the returned number against the original number to verify the card. The reverse of the process accomplishes terminal authentication.

Counterfeiters and emulator builders do not know the secret key and cannot generate a valid signature for the card. Secret information is not exchanged between the card and terminal, so it is not possible to record or capture the information. The secret key is 64 bits long, so it is extremely difficult to guess the secret information. These features help ensure the effectiveness of smart card authentication and system integrity.

4.4 SECURITY LEVEL

Determining the security of smart cards requires a basic understanding of smart cards, their goals, methods, capabilities and limitations. Independent testing has shown that smart cards protect against an adversary with bounded time and resources and no knowledge of secret codes (practical security). They are not invincible; an adversary with unlimited time and manpower or knowledge of secret codes can extract information and counterfeit cards. However, smart cards provide a sophisticated security device with information security and anticounterfeit protection that is not available in other card technologies.

5.0 CARD LIFE AND COSTS

The ISO identification card standards specify card protection requirements from static electricity, bending, ultraviolet light, and other hazards encountered in normal use. Cards that meet the ISO standards are generally immune to all but the most severe abuse.

Field-related experience shows that ISO cards have lasted five years in a laboratory environment and have survived over three years in normal use.

These results are in line with independent testing that was performed to determine smart card durability.

Smart card costs are dependent on quantity, memory size, built-in security, and complex function features. Costs for 10,000 cards with 2,000 bytes of EEPROM and cryptographic module range from $5 to $12 each, depending mostly on the built-in security features.

6.0 CARD PERSONALIZATION

Smart card personalization assigns the smart card to a person and places it into the system. During personalization, the authentication code, PINs, and encryption keys are written to the secret data area. Then application data and personal information are written to the application area. A printer may print graphics onto the card, including name, identifying number, and photograph. Proper personalization of all cards is required before the card can be used in the system. This provides the assurance that cards used successfully in the system are authorized.

7.0 SMART CARD APPLICATIONS

Smart cards have been used as medical record, dosimetry, cryptography, and access control cards in which the user carries a secure, distributed database of information. Smart cards provide information at the point of the transaction and can be updated and actions recorded without direct communication to a central database. The card carries all information necessary for transactions, so there is no requirement for enrollment and authorization information to be distributed to remote locations.

7.1 SECURITY APPLICATIONS

A smart card stores information, including cryptographic keys, PINs, and biometrics, which are available for holder identification and card authentication. With the addition of photographs and graphics to the face of the card, smart cards are appropriate for use as "smart badges."

The smart badge as a security device provides automated access control and audit trail recording at remote sites, without door-by-door enrollment or a full-time network. The smart badge provides the information necessary for the remote terminal to grant or deny access.

Remote terminals grant access based on two criteria, authenticated badge and positive identity verification (biometric) of the holder. Concern over lost or stolen badges is diminished because it is nearly impossible to fake the holder's identity. The physical security features of smart cards make it extremely difficult to counterfeit cards. Self-invalidating badges and "blacklists" control the authorized user's list. Badges can be programmed to disable themselves on a given date or under certain conditions. Blacklists[2] are stored at the remote terminals and used to stop the use of certain badges. Once disabled, a badge cannot be authenticated until enabled by a system administrator.

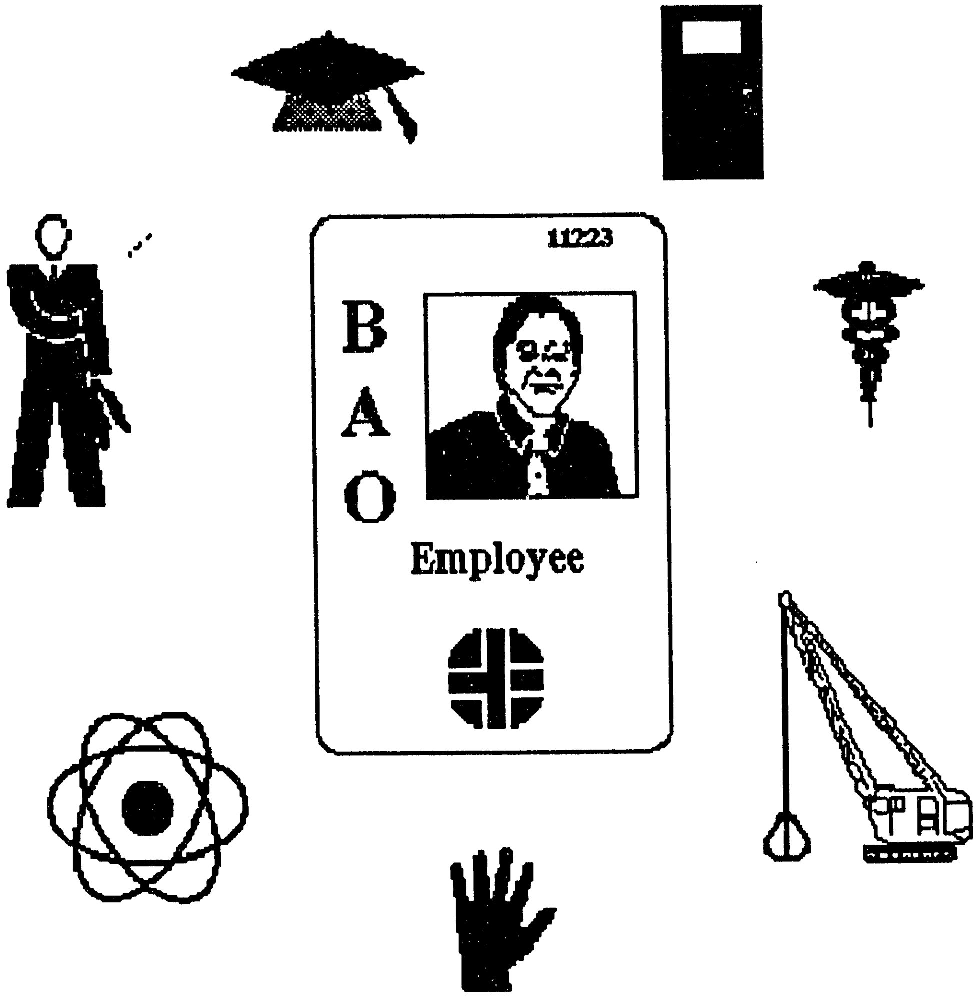


Figure 2. Multiple Application Badge.

7.2 MULTIPURPOSE APPLICATIONS

The smart badge provides the most cost benefits when used as a multiple application device. The smart badge is a data carrier for medical, training, health, safety, and payroll information. It is an active component in a data management system that may prove personnel qualifications or update itself to provide running totals of cost or exposure information. It will improve database management, data distribution, and information timeliness at a cost advantage over centralized, highly integrated database management systems. The cost effectiveness results in the savings incurred by replacing a physical network with the smart card. Each person using the system carries current

[2] A blacklist is a list of badge numbers held by people whose access rights have been revoked but whose badges have not been recovered.

information on their person. This information is used at remote terminals for transactions.

There are many other applications that a smart card system can service. These include electronic signature for a document authentication in a paperless office, time distribution reporting for automated payroll, coinless systems for vending machines, and bus passes for site bus services.

The smart badge can provide multiple technologies (e.g., magnetic stripe, bar code, optical storage) so that a single badge can meet different needs or can be phased into existing systems. The smart badge meets strict security requirements and also provides a platform for carrying information that is useful for nonsecurity applications.

8.0 CONCLUSION

Many security and systems professionals perceive smart cards as enhanced magnetic stripe cards that can store large amounts of data with a high level of information security. Smart cards are more than an enhanced magnetic stripe card. They act as active components in data management systems in a credit card format. These features enable smart cards to solve application requirements with distributed processing, which would be expensive and complicated using a card network system. Realizing the full potential of smart cards will bring unique, cost-effective security and information management solutions in the future.

DISTRIBUTION

Number of copies

OFFSITE

1 U.S. Department of Energy-Headquarters
SA-121, Room E-378
19901 Germantown Road
Germantown, MD 20874

R. J. Sentell
Westinghouse Hanford Company
Security Applications Center

ONSITE

5 U.S. Department of Energy-
Richland Operations Office

L. A. Marzetti (5)	A6-35

12 Westinghouse Hanford Company

M. R. Duncan	L6-10
R. A. Nelson	L6-09
D. E. Palmer (5)	L6-09
C. J. Udell	L6-12
C. W. Walton	L6-11
Information Release Administration (3)	L8-07

DATE

FILMED

9/16/93

END