Module 1: Smart Card Fundamentals

Smart Card Alliance
Certified Smart Card Industry Professional
Accreditation Program

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

Important note: *The CSCIP training modules are only available to LEAP members who have applied and paid for CSCIP certification. The modules are for CSCIP applicants ONLY for use in preparing for the CSCIP exam. These documents may be downloaded and printed by the CSCIP applicant. Further reproduction or distribution of these modules in any form is forbidden.*

TABLE OF CONTENTS

1 Introduction

This module describes the fundamentals of smart card technology and uses. After reviewing this module, CSCIP applicants should be able to answer the following questions:

- What are common smart card-based applications?
- What are the different types of integrated circuits (ICs) used in smart cards?
- What are the different smart card communications interfaces and what standards are used to govern those interfaces?
- What are the components of a microcontroller-based smart card?
- What form factors is smart card technology available in?
- What operating systems are available for smart cards? What are the functions performed by the operating system? How do operating systems differ?
- How are smart cards manufactured?
- What types of smart card readers are available?
- What are the relevant industry standards and specifications and how are they used in different applications?

2 Smart Card Overview

This section provides an overview of the history of smart card technology, the current market size, the types of smart cards available and example smart card functions and applications.

2.1 Smart Card History and Market

A smart card (also called an "integrated circuit card") is a device in which an integrated circuit, or chip, is embedded. Systems using smart cards have multiple point-of-service terminals (or readers) which communicate with the card and with a central host computer system. The development of smart cards dates back to the 1970s, when patents were filed in France, Germany, and Japan.

The first practical smart card implementation was developed in France, to combat the rising cost of fraud in telecommunications and banking applications. Motorola produced the first secure single-chip microcontroller (MCU)[1] in 1979 for use in French bank cards. Two types of smart card products were introduced in the early 1980s. One, for telephone cards, used a serial-memory integrated circuit (IC)[2]. The other, for banking applications, used the more secure MCU.

The first mass rollout of smart cards took place in 1992, when the cards were adopted by all French banks. More than 10 million cards were issued that year. Smart card shipments have grown dramatically, with Eurosmart forecasting a growth for the worldwide shipments of smart cards and secure elements of 9% to 8.79 billion units to be shipped in 2015, with an estimate of 8.04 billion secure elements shipped in 2014.[3] This rapid growth is due to the increasing use of smart cards for many financial, telecommunications, transit, healthcare, access and secure identification applications. An area of high growth is secure contactless devices, with 23% growth forecast from 2013 to 2014; this growth is driven by increasing use of contactless smart cards for financial, government, access control and transit applications.

Table 1, Table 2 and Table 3 show Eurosmart estimates of worldwide smart card shipments for 2014 and 2015.[4]

The name, "smart card," is something of misnomer. While the plastic card was the initial smart card form factor, smart card technology is now available in wide variety of form factors, including plastic cards, key fobs, subscriber identification modules (SIMs) used in GSM mobile phones, watches, electronic passports and USB-based tokens. Devices that incorporate smart card technology may be called smart cards, secure elements or smart secure devices by different industry sources.

What started as an electronic device to store bank account information securely has evolved into a sophisticated computing device capable of supporting many different applications on a single card or token. These applications include bank cards, mobile phone subscriber identity modules (SIM), healthcare cards, government and enterprise ID cards, benefits and social welfare cards, driver's licenses, physical and logical access cards, mass transit (ticketing) cards, and even cards that combine multiple applications on a single card.

---

[1] An MCU is a computer chip that contains the components of a controller. Typically, these include a central processing unit (CPU), random access memory (RAM), some form of read-only memory (ROM), electrically erasable programmable read-only memory (EEPROM), input/output (I/O) ports, and timers. Unlike a general purpose computer, a microcontroller is designed to control only a particular system

[2] A memory-only smart card chip contains a memory array with hard-wired security logic to control access to the memory and to prevent unauthorized writing and erasing of the data. It has neither a microprocessor nor MCU, so its functionality and security capabilities are limited.

[3] Eurosmart forecast, "Providing Trust and Security is Key for a Successful Mobile Lifestyle in the Hyperconnected World of 2020," November 2014, http://www.eurosmart.com/publications/market-overview

[4] Note: Eurosmart refers to "smart secure devices" and "secure elements." These are other names for devices that use smart card technology. These modules refer to all such devices as "smart cards."

Table 1. Worldwide Smart Secure Device Shipments – 2014 and 2015 Forecasts (Millions of Units, Source: Eurosmart - November 2014)

Worldwide Shipments*	2013	2014 (Forecast)	2015 (Forecast)	2014 vs 2013 % growth	2015 vs 2014 % growth
Telecom	4,850	5,100	5,250	5%	3%
Banking	1,550	1,950	2,350	26%	21%
Government	350	390	440	11%	13%
Device Manufacturers	190	190	310	0%	63%
Others	390	410	440	5%	7%
Total	7,330	8,040	8,790	10%	9%

**Shipments of secure elements are reported by issuing entity:*

- *Telecom represents mobile network operators; banking represents banks; government represent public authorities as well as private healthcare organizations*
- *Device manufacturers represent original equipment manufacturers of mobile phones, tablets, navigation devices and other connected devices*
- *Others include shipments from entities issuing transport, pay TV and physical and logical access cards*

Table 2. Worldwide Smart Secure Contactless Shipments– 2014 and 2015 Forecasts (Millions of Units, Source: Eurosmart - November 2014)

Worldwide Contactless**	2013	2014 (Forecast)	2015 (Forecast)	2014 vs 2013 % growth	2015 vs 2014 % growth
Banking	590	800	1,000	36%	25%
Government	200	230	260	15%	13%
Others**	250	250	280	0%	12%
Total	1,040	1,280	1,540	23%	20%

***Others include transport and physical and logical access cards.*

Table 3. Worldwide NFC Secure Element Shipments– 2014 and 2015 Forecasts (Millions of Units, Source: Eurosmart - November 2014)

Worldwide NFC Secure Elements***	2013	2014 (Forecast)	2015 (Forecast)	2014 vs 2013 % growth	2015 vs 2014 % growth
NFC Secure Elements	270	350	600	30%	71%

**** NFC secure elements include NFC enabled UICCs and embedded secure elements and other form factors of NFC enabled secure elements.*

2.2 Types of Smart Cards[5]

Three different types of chips can be associated with smart cards: memory only, which includes serial-protected memory, wired logic and microcontroller. The terms "memory only," "wired logic" and "microcontroller" refer to the functionality that the chip provides. The following further discusses the types of chip cards.[6, 7]

- **Memory-Only Integrated Circuit Cards (including Serial Protected Memory Cards).** Memory-only cards are "electronic magnetic stripes," and provide little more security than a magnetic stripe card. The two advantages they have over magnetic stripe cards are: a) they have a higher data capacity (up to 1024 kilobits (Kbits) compared with 80 bytes per track), and b) the read/write device is much less expensive. The memory-only chip cards do not contain logic or perform calculations; they simply store data. Serial-protected memory chip cards have a security feature not found in the memory-only chip card; they can contain a hardwired memory that cannot be overwritten.

  Early versions of memory-only cards were read-only, low capacity (maximum of 160 units of value), prepaid disposable cards with little security. New versions include prepaid disposable cards that use read/write memory and binary counting schemes that allow the cards to carry more than 20,000 units of value. Many of these cards also have advanced logic-based authentication schemes built into the chip. Other memory-only cards have been developed for re-loadable stored value applications. The cards contain a purse, which can be protected through the use of a personal identification number (PIN) and counters, which limit the number of times the purse can be reloaded.

- **Wired Logic Integrated Circuit Smart Cards**. A wired logic chip card contains a logic-based state machine that provides encryption and authenticated access to the memory and its contents. Wired logic cards provide a static file system supporting multiple applications, with optional encrypted access to memory contents. Their file systems and command set can only be changed by redesigning the logic of the IC. Wired logic-integrated chip cards include contactless variations such as I-Class™ or MIFARE™.

- **Secure Microcontroller Integrated Circuit Smart Cards**. Microcontroller cards contain a microcontroller, an operating system, and read/write memory that can be updated many times. The secure microcontroller chip card contains and executes logic and calculations and stores data in accordance with its operating system. The microcontroller card is like a miniature PC one can carry in a wallet. All it needs to operate is power and a communication terminal. Contact, contactless and dual-interface microcontroller ICs are available. Unlike memory-only products, these microcontroller ICs have been designed (and can be verified) to meet security targets, such as Common Criteria (for example, the Department of Defense Common Access Card).

There are two primary types of smart card interfaces—contact and RF-enabled contactless. The terms "contact" and "contactless" describe the means by which electrical power is supplied to the chip and by which data is transferred from the chip to an interface (or card acceptance) device (reader).

- **Contact Smart Cards.** A contact smart card must be inserted into a smart card reader that directly touches the conductive contact plate on the surface of the card. Transmission of commands, data, and card status takes place over these physical contact points.

---

[5] Source: *Government Smart Card Handbook*, U.S. General Services Administration, 2004 (with updates)

[6] Jack M. Kaplan, Smart Cards: The Global Information Passport, (New York: International Thomson Computer Press, 1996), 69-75.

[7] Jose Luis Zoreda and Jose Manuel Oton, Smart Cards (Boston: Artech House, Inc., 1994), 5-6.

- **RF-Enabled Contactless Smart Cards.** RF-enabled contactless smart cards must only be in near proximity to the reader (generally within 4-10 centimeters or 2-4 inches) for data exchange to take place. The contactless data exchange takes place over radio frequency (RF) waves. The device that facilitates communication between the card and the reader are RF antennae internal to both the card and the reader.
- **Hybrid Smart Cards.** A hybrid card contains two chips on the card, one supporting a contact interface and one supporting a contactless interface. The chips contained on the card are generally not connected to and cannot communicate with each other.
- **Dual-Interface Smart Cards.** A dual-interface smart card contains a single chip that supports both contact and contactless interfaces. These dual-interface cards provide the functionality of both contact and contactless cards in a single form factor, with designs able to allow the same information to be accessed via contact or contactless readers. Dual interface cards can apply different security protocols to the same data, depending on which interface is used to access it.

Contact, contactless and dual-interface smart cards support the same high levels of security that are needed for protecting sensitive information and enabling secure transactions.

2.3 Smart Card Functions and Applications

Smart card technology is used provide data portability, security and convenience for many different applications. Smart cards allow data and applications to be securely stored and accessed on the chip and enable secure data exchange with a reader and host system. Smart card technology provides high levels of security and privacy protection, making it ideal for handling sensitive information such as payment account and identity information. Since smart cards can store virtually any type of information, they can be combined with other technologies such as biometrics in systems requiring the highest levels of assurance.

Smart cards are now used worldwide in many payment, identity and access applications. Table 4 shows examples of smart card applications; these applications are discuss in more detail in CSCIP Modules 4, 5 and 6.

Table 4. Example Smart Card Applications[8]

Physical access	• Environment: port facility, campus, single building, parking lot • Interior: entrances, lobbies, offices, computer rooms, vaults • Transportation: buses, planes, trains, ships, subways
Logical Access	• Network and computer system login • Signed and encrypted e-mail, secure transactions requiring higher levels of assurance • Common files: shared/working documents, employee handbook, newsletters • Confidential files: payroll, trade secrets, human resource files
Data Storage	• Property management • Clearance information • Personnel rosters • Medical information • Training/certifications • Personal information for electronic forms submission
Financial	• Electronic purse: cafeteria, transit, parking • ATM, credit, debit and prepaid payment (contact and contactless)

[8] Smart Card Alliance, *Secure Identification Systems: Building a Chain of Trust*, March 2004

Privilege Management	• Healthcare • Voting • Driver's license • Travel/border crossing • Electronic benefits
Law Enforcement	• Criminal records • Citizenship • Immigration status • User/document authenticity confirmation • Identification at time of death

3 Integrated Circuit Types[9]

Integrated circuits go by many names: IC, microcircuit, microchip, silicon chip, or just plain chip. An IC is simply a miniaturized electronic circuit that is manufactured in the surface of a thin substrate semiconductor material. In a smart card, the IC provides the computing platform for executing applications specific to that card. The ICs used in smart cards are "secure" ICs – meaning that they have been designed and manufactured with features that are used to protect the data and enable secure transactions with smart card applications. Applications contained on smart cards vary in complexity, memory requirements, and the security required to protect the information stored and processed in the IC. Depending on the requirements, the ICs used for smart card programs are either secure memory ICs or secure microcontrollers.

3.1 Memory and Secure Memory

Memory ICs are used for smart card applications that need data storage, but that have minimal requirements for data protection. The data can be any information required by the specific smart card application. For example, the following information can be stored on a memory IC to support an identification application:

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

Memory smart cards use non-volatile memory (NVM) which allows the card to hold data even after its power source is removed. The NVM in a memory smart card can incorporate different memory technologies but typically uses erasable programmable read-only memory (EPROM) or electrically erasable programmable read-only memory (EEPROM). EPROM can only be changed once and is often used in prepaid service cards such as telephone calling cards that count off the minutes used and are then discarded. EEPROM can be changed up to 500,000 times. Logic that can be used to update a counter in prepaid service cards is built in.

Every secure memory IC is identified by a unique serial number. Optional fields on the memory IC include authentication logic, counter logic, error counter, data, and secret codes or keys. Application developers have options for several different memory card structures to meet design requirements. Figure 1 shows the block diagram of a typical secure memory IC.

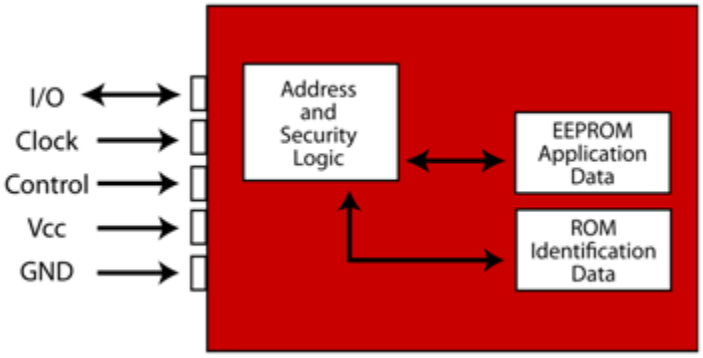


Figure 1. Secure Memory IC Block Diagram

Of the two types of secure ICs – memory and microcontroller – used in smart cards, the secure memory IC is the less secure. In the simplest designs, secure memory ICs have logic that prevents writing or erasing data. More complex designs also restrict memory read access. Security for the memory card is managed by static logic that allows for the execution of symmetric cryptographic algorithms, which are

[9] Smart Card Alliance, *What Makes a Smart Card Secure?*, October 2008

used to encrypt the data to be transmitted from the card. Currently, secure memory cards support symmetric algorithms with key lengths of up to 128 bits.

3.2 Microcontroller

The secure microcontroller is a more sophisticated smart card IC. A secure microcontroller chip has[10]:

- An 8-bit to 32-bit central processing unit (CPU);
- Read Only Memory (ROM) or flash memory that contains the chip's operating system and, optionally, application software;
- Random Access Memory (RAM) that serves as a temporary register for data;
- Other non-volatile memory (NVM) that is used for storage of user data (e.g., Electrically Erasable Programmable Read Only Memory (EEPROM), ferroelectric RAM, flash memory);
- Features that integrate countermeasures against known and foreseen security threats to achieve Common Criteria or FIPS 140-2 certification;
- Environmental sensors (e.g., voltage, frequency, temperature);
- At least one serial communication port;
- A random number generator;
- Timers;
- Optional cryptography engine(s) (e.g., hardware accelerators for commonly used cryptographic algorithms such as 3DES, AES, RSA, and ECC);
- Optional other dedicated peripherals (e.g., checksum accelerator, Serial Peripheral Interface (SPI) communication port).

Figure 2 shows a block diagram of a typical secure microcontroller IC. Secure microcontroller ICs are programmed to execute applications, and functionality can be performed dynamically. Depending on what security functions the microcontroller is required to perform in a particular application, the controller may also have a cryptographic engine to more quickly and securely process asymmetric and/or symmetric algorithms.

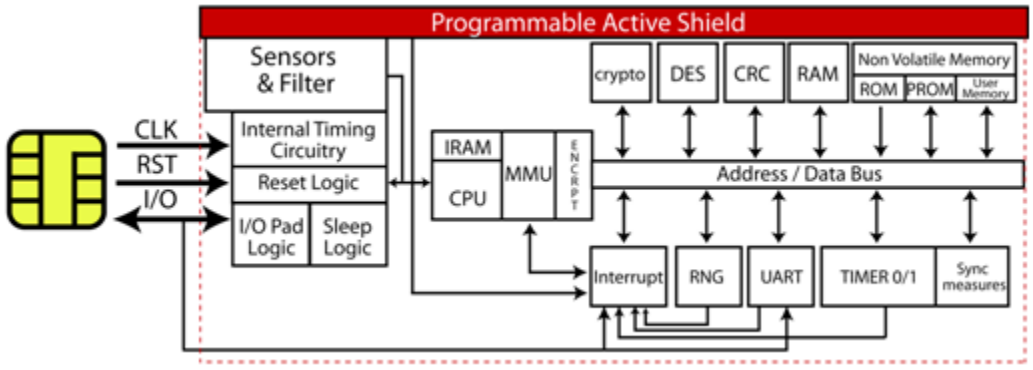
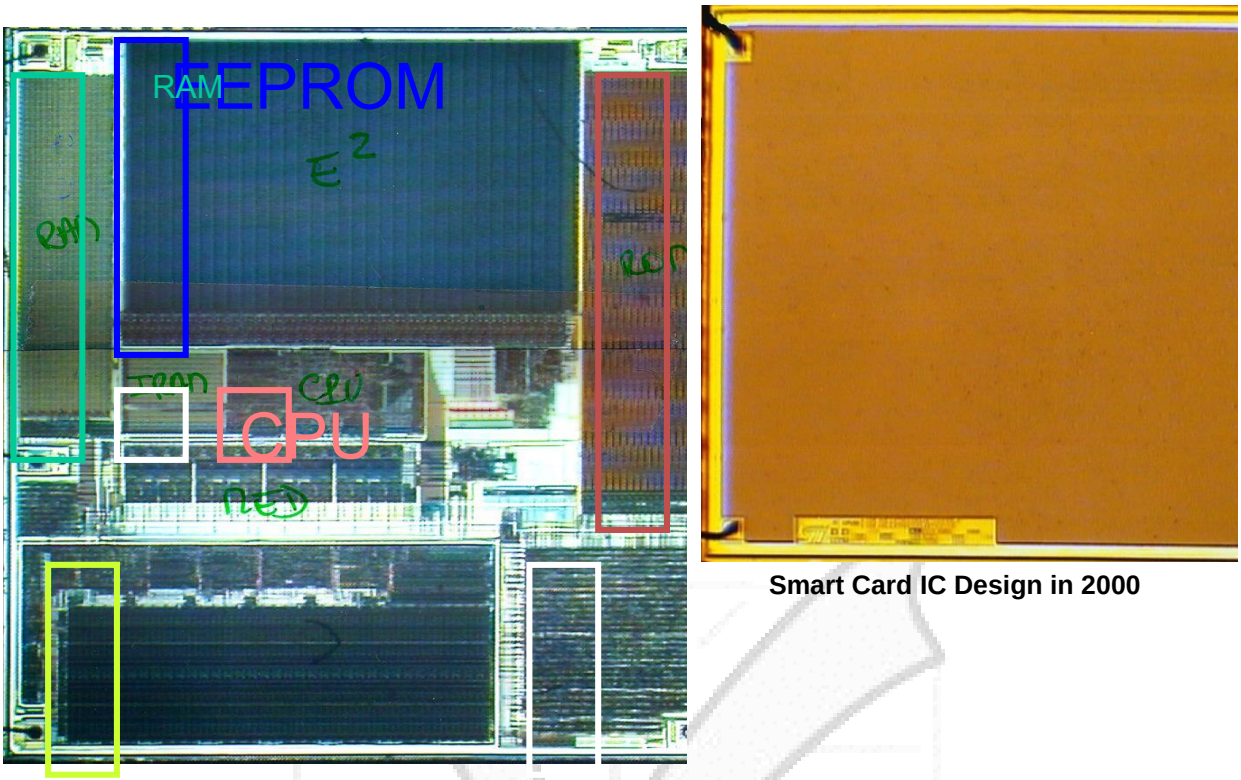


Figure 2. Components of a Typical Secure Smart Card Microcontroller

[10] Source: *Government Smart Card Handbook*.



Smart Card IC Design in 2000

Smart Card IC Design in 1996

Figure 3. Example Smart Card IC Designs[11]

Figure 3 shows the layout of an example smart card IC design in 1996 and in 2000. In earlier smart card designs, the IC's blocks can be easily identified, with no shield or glue logic and bus lines clearly visible. Current smart card ICs provide additional security protections, with 0.18µm designs, an active shield, glue logic and no visible bus lines.

Program code is written into the microcontroller's ROM during the IC manufacturing process. This program code, which is often referred to as the IC's operating system (OS), supports the execution of the applications that the microcontroller is intended to perform. Data and application program code are stored in NVM, which can be modified under the control of the OS after the IC has been manufactured and embedded into the smart card. The NVM in a secure microcontroller IC can be one or a combination of memory technologies: EPROM, EEPROM, flash memory and ferroelectric random access memory (FRAM). Flash memory is a specific type of EEPROM that is erased and programmed in large blocks. FRAM is a fast and low power technology that uses the material to hold and change polarity for data storage over 100 trillion times.

One of the primary features of a secure microcontroller is dynamic active security. Microcontrollers have been adopted in smart cards mainly for secure data transactions. If a user or system cannot successfully authenticate to the microcontroller, the data stored on the card cannot be retrieved. Therefore, even if a smart card is lost, the data stored on the card will not be exposed. In addition, as a portable computer, a microcontroller smart card can process internal data securely and output the calculated result to a terminal for further processing. The integrity of the stored data is protected by a suite of countermeasures that are invoked when the microcontroller senses an attempted attack. These countermeasures are discussed in CSCIP Module 2.

[11] CSCIP Exam Preparatory Course, Module 2, Gilles Lisimaque, July 2010

Secure microcontrollers offer on-chip security features that protect against physical and logical attacks. External clock frequency and voltages are monitored. Memory access rights are controlled by the memory management and protection unit. An active shield layer can detect attempts to probe or force internal components or signal lines. Random generation of current noise on idle buses (bus confusion) protects against attackers who analyze the bus. When someone tries to analyze the IC with various techniques, the built-in sensors are activated and trigger a special security reset, which immediately overwrites the RAM area. A functional current scrambling engine, in conjunction with the true random number generator and random wait state feature, protect against power and timing analyses.

Secure microcontrollers have begun to replace secure memory ICs as semiconductor technology has evolved to offer more functionality on less silicon area (i.e., lower cost). At the low-end, secure microcontrollers are available with 8KB or less NVM and provide basic file system card capabilities or traditional paged/banked storage space structured similarly to the NVM of secure memory ICs. Such low cost and fixed ROM devices provide the security features of secure microcontrollers presented in this paper, but can be confused or mis-identified as secure memory ICs.

4 Form Factors for Smart Card Technology

The name, "smart card," is something of misnomer. The term "smart card" now refers to any form factor that incorporates a smart card integrated circuit. While the ID-1 format plastic card was the initial smart card form factor, smart card technology is now available in wide variety of form factors, including plastic cards, key fobs, subscriber identification modules (SIMs) used in GSM mobile phones, watches, electronic passports and USB-based tokens.

4.1 Card Form Factor

ISO/IEC 7816 Parts 1 and 2 and ISO/IEC 7810 describe the specifications for the physical characteristics of integrated circuit cards with contacts and the dimensions and location of coupling areas for contact smart cards. Figure 4 shows the dimensions of the contact card form factor. The card form factor is the widely used for access, identity, healthcare and payment applications and is available with both contact and contactless interfaces. (See Section 5 for a detailed discussion of smart card interfaces.)

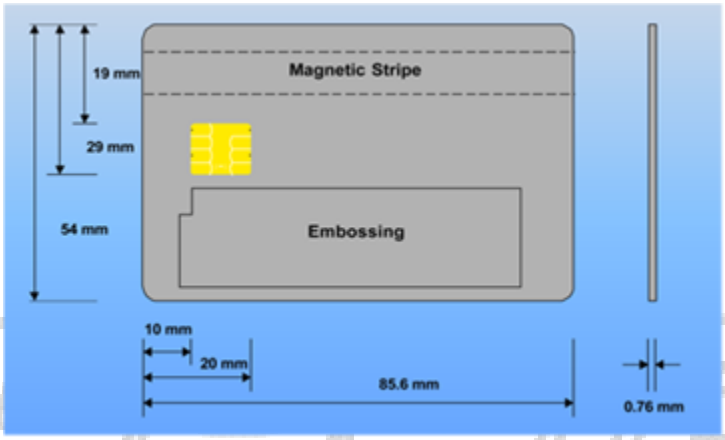


Figure 4. Dimensions of the ID-1 contact smart card form factor[12]

4.2 USB Tokens

Smart card technology is built into USB-based tokens that provide a portable authentication device that can be used with any computer with a USB port – i.e., without a dedicated smart card reader. USB-based tokens can be used for any logical access applications that a smart card can be used for – secure data, password and PKI credential storage, encryption/decryption and multi-factor access to computers and networks. Smart card-based USB tokens may be designed to incorporate a SIM to provide field-serviceability.

Figure 5 shows examples of smart-card-based USB tokens.

[12] Won J. Jun, "Smart Card Technology Capabilities," presentation, July 8, 2003

Figure 5. Examples of Smart Card USB Tokens[13]

4.3 Subscriber Identity Module/Universal Integrated Circuit Card Form Factor

The European Telecommunications Standards Institute (ETSI) defined the dimensions of the plug-in SIM/UICC that is used in mobile phones and is now also used in conjunction with USB tokens. The SIM/UICC has the same thickness as the ID-1 form factor[14] and is available in two form factors, both standardized in ETSI TS 102 221:

- Plug-in UICC (2FF, or second form factor), which is 25 mm x 15 mm.
- Mini UICC (3FF, or third form factor), which is 15 mm x 12 mm.

Plug-in SIM cards are typically supplied as a full-sized card with the smaller card held in place by a few plastic links that are broken to remove the smaller SIM (see Figure 6).

Figure 6. Examples of SIM cards/UICCs[15]

4.4 Secure Element and Embedded Card Form Factors

Smart card technology is also available in surface mount device (SMD) form factors to be used as the secure element in mobile devices or as an embedded secure device in machine-to-machine applications. These form factors are available as:

- A solderable small SIM (MFF1 or MFF2), which is 5 mm x 6 mm and is standardized in ETSI TS 102 671.

[13] Images provided courtesy of ActivIdentity, Gemalto, HID Global and SCM Microsystems.
[14] ETSI, *Digital Cellular Telecommunications System (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) Interface, GSM 11.11*, December 1995
[15] Images provided courtesy of Oberthur Technologies and Giesecke & Devrient.

- A SIM component in surface mount device packaging to allow the component to soldered onto printed circuit boards.

Figure 7 shows examples of these form factors.

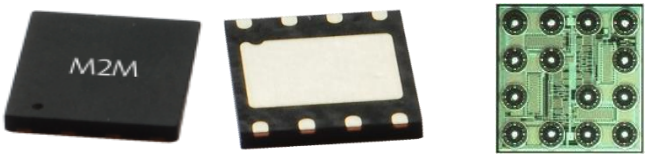


Figure 7. SMD Form Factors for Secure Elements and Embedded Cards[16]

4.5 Other Form Factors

Contactless smart card technology has enabled a wide range of new form factors, including key fobs, wrist watches, mini cards, contactless USB devices and ePassports. Near Field Communication (NFC) technology is also enabling mobile phones to be used for proximity mobile payments at point-of-sale terminals that accept contactless payments. With these new form factors, contactless smart card technology enables convenient and secure identity and payment transactions. Figure 8 shows examples of different contactless form factors to illustrate the variety of form factors now available.

Figure 8. Examples of Form Factors Using Contactless Smart Card Technology[17]

[16] Images provided courtesy of Oberthur Technologies.
[17] Images provided courtesy of Oberthur Technologies, First Data, MasterCard and Visa. Visa image and logo are copyright Visa 2008.

5 Communications Interfaces[18]

In general, smart cards currently cannot display information or directly accept input from the user.[19] For the user to access the information a smart card contains, the card needs an interface to communicate with a reader or terminal, such as a merchant point-of-sale terminal, a bank ATM or a computer smart card reader.

Four elements are required for a smart card to communicate with the outside world:

- A power source
- Clock signal transmission
- Data transfer to the secure IC
- Data transfer from the secure IC

Data can be transferred either by physical contact, using electrical connections with the contact pads on the surface of the smart card, or without contact (i.e., contactless), using radio frequency (RF) transmission.

The two methods of data transfer give rise to three types of smart cards: contact cards with a contact interface, contactless cards with a contactless interface, and dual-interface cards, with both a contact interface and a contactless interface. The choice of interface depends on both application and business requirements, which must also include security considerations. Contact and contactless smart cards may use either secure memory or a secure microcontroller as the underlying IC.

5.1 Contact Interface

A typical smart card is assembled with an IC delivered as a sawn wafer, packaged in a module, and embedded into a plastic card.[20] The component elements are shown in Figure 9.

Interfacing with the outside world requires the card to be inserted into a smart card reader or terminal in such a way that the smart card module makes a physical connection with the contact wiper pads within the reader device. Two primary types of contact readers are used: landing contact and friction contact (also known as sliding or wiping). In card readers featuring friction contact, the contact part is fixed. The contact wipes on the card surface and the chip when a card is inserted. In card readers using the landing type, the contact part is movable. The contact "lands" on the chip after a card is wholly inserted. In general, card readers of the landing type provide better protection to the card than that of the friction type. Landing type readers typically have longer lives in terms of the number of insert/remove cycles before failure.

Contact smart cards are used for many applications, including EMV credit/debit cards, healthcare cards, national ID cards and government and corporate employee ID cards that are used for accessing computers and networks.

[18] Smart Card Alliance, *What Makes a Smart Card Secure?*, October 2008

[19] Smart cards are emerging with numeric LED displays that can display (for example) an internally generated authorization code or with an activation button that controls whether a particular function (e.g., contactless mode) is on or off. However, these cards are currently complex and costly and have yet to reach mass deployment with proven reliability. They usually contain additional circuitry, such as additional ICs, and require a battery to power any display.

[20] Secure IC-based devices (i.e., smart cards) can come in a variety of form factors, including plastic cards, key fobs, wristbands, wristwatches, PDAs, and mobile phones.

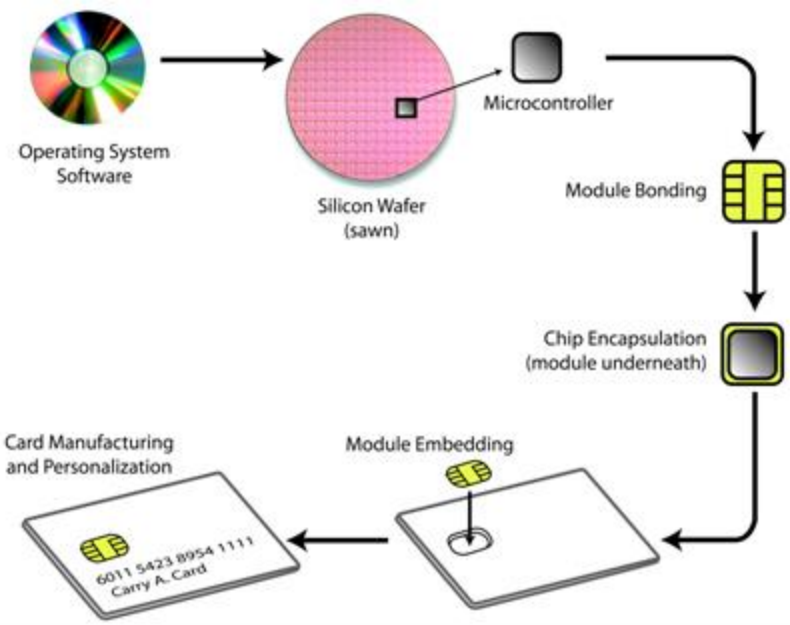


Figure 9. Component Elements of a Contact Smart Card

5.1.1 Contact Interface Standards

A contact smart card's protocol interface for data communication is standardized in ISO/IEC 7816-3, while its physical connections are standardized in ISO/IEC 7816-2.

ISO/IEC 7816-3 specifies the power and signal structures, and information exchange between an integrated circuit card and an interface device such as a terminal. It also covers signal rates, voltage levels, current values, parity convention, operating procedure, transmission mechanisms and communication with the card.

ISO/IEC 7816-3 supports the following contacts.

C1: supply power input (VCC)
C2: reset signal input (RST)
C3: clock signal input (CLK)
C5: ground (GND)
C7: input/output for serial data (I/O)

ISO/IEC 7816-3 standard defines the various bytes contained in the technical bytes of the Answer-to-Reset (ATR) as well as the various transmissions protocols (T=0 or T=1) available to contact smart cards. A section also defines how a card and the interface device can negotiate the transmission protocol of the various parameters (e.g., speed, block size) of the transmission. This procedure, which happens just after the answer-to-reset, is called Parameter Protocol Selection (PPS).

5.1.2 Data Transmission Protocols

Two data transmission protocols, T=0 and T=1, defined in ISO/IEC 7816-3 are primarily used with contact smart card implementations. Both T=0 and T=1 protocols are master/slave oriented, with the terminal always initiating the command to the card.

The **protocol T=0** is a half-duplex byte-oriented protocol. The interface device initiates every command by transmitting a five-byte header that tells the card what to do. The command processing continues with the transfer of a variable number of data bytes in one direction under the control of procedure bytes

transmitted by the card. It is assumed that the card and the interface device know *a priori* the direction of transfer, in order to distinguish:

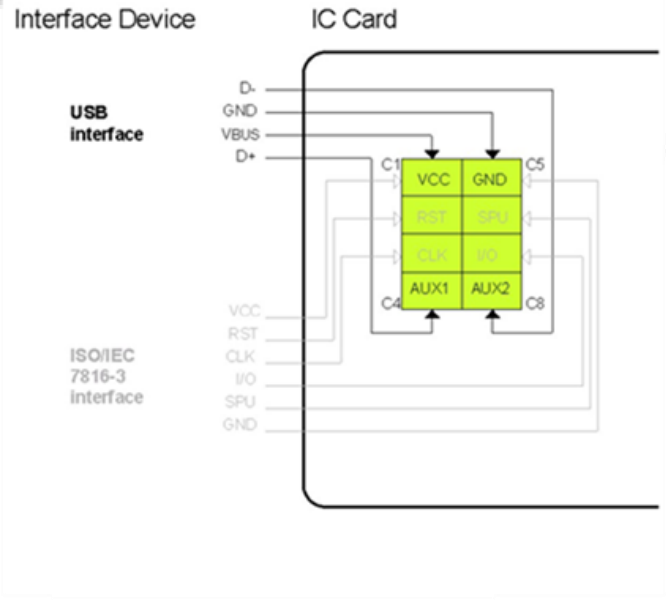
- Commands for incoming data transfer where the data bytes enter the card while processing, and
- Commands for outgoing data transfer where the data bytes leave the card while processing.

The **protocol T=1** is a half duplex block transmission protocol. A block is a byte string conveyed in asynchronous characters. The interface device and the card may initiate these commands. The main characteristics of the T=1 transmission protocol are the following.

- The transmission protocol starts with a first block transmitted by the interface device; it continues with alternating the right to transmit a block.
- A block is the smallest data unit that can be exchanged. A block may be used to convey application data transparent to the transmission protocol and transmission control data (including transmission error handling).
- The block structure allows checking the received block before processing the conveyed data. The T=1 transmission protocol applies the principle of the OSI reference model. Three layers are defined:
  - The physical layer transmits moments organized in asynchronous characters.
  - The data link layer includes a character component and a block component. The character component recognizes the beginning and the end of a block. The block component exchanges blocks.
  - The application layer processes commands, which involves the exchange of at least one block or chain of blocks in each direction.

In addition to the protocols defined in ISO 7816-3, **ISO 7816-12** defines a USB electrical interface and operating procedures for data transmission. Figure 10 shows the assignment of the contact fields for a USB interface and – to illustrate interoperability – the assignment used in ISO/IEC 7816-3.

Figure 10. Assignment of Contacts for USB-ICC



Two other transmission protocols used with smart cards are:

- The **MultiMediaCard (MMC) interface**. The MMC interface specification, published by the MultiMediaCard Association, was designed for data transfer with a memory card.

- The **Single Wire Protocol (SWP)**. The SWP is a specification for communication between a GSM phone's Subscriber Identity Module (SIM) and the Near Field Communication (NFC) controller, providing another channel for SIM communication. The specification is published by the European Telecommunications Standards Institute (ETSI).[21]

5.2 Contactless Interface

Contactless smart card technology is used increasingly in applications that must protect personal information and deliver fast, secure transactions. Leveraging many years of smart card security developments, contactless smart cards have the ability to store, protect, manage, and provide access to secure data and to support the security protocols and algorithms required by an application. In addition, contactless smart card technology delivers the convenience, durability, and reliability required by applications that must support fast transaction throughput in demanding environments. Contactless cards and readers can be used in hostile environments (e.g., outdoor use) that might cause contact card or reader failure due to exposure to moisture.

A contactless smart card-based device includes an embedded secure microcontroller or equivalent intelligence, internal memory, and a small antenna, and communicates with a reader through a contactless radio frequency (RF) interface. The contactless interface provides users with the convenience of allowing the contactless device to be read at short distances with fast transfer of data.

Contactless smart chip technology is available in a variety of forms–plastic cards, watches, key fobs, documents, and other handheld devices such as mobile phones. Contactless technology is used for applications such as mass transit tickets, physical access control, and debit and credit payment cards. Contactless mobile payment applications[22] are also now being implemented using Near Field Communication (NFC) technology, which follows universally implemented standards from ISO, Ecma International, and the European Telecommunications Standards Institute (ETSI) and is compliant with ISO/IEC 14443.

There are two main differences between a contact and contactless smart card. First, there are no physical connections between the contactless card and the reader. Second, a contactless card's power to drive the secure IC is derived from energy transferred from an RF field generated by the reader that induces an electrical current in the IC's antenna coil when it enters the reader's RF field (Figure 11).

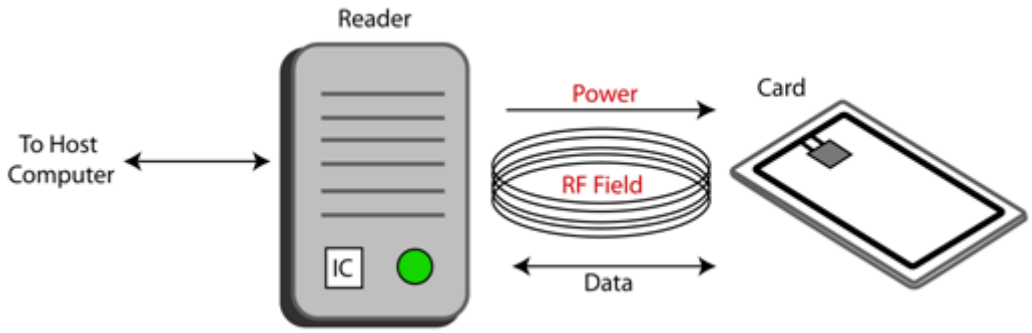


Figure 11. Contactless Smart Card in RF Field

The secure IC module is embedded in the card with no exposure to the card surface. The module has only two external contacts (whereas a contact smart card normally has five), which connect to an antenna coil that is also embedded in the card (Figure 12).

[21] http://en.wikipedia.org/wiki/Single_Wire_Protocol
[22] Contactless mobile payment is also called proximity mobile payment.

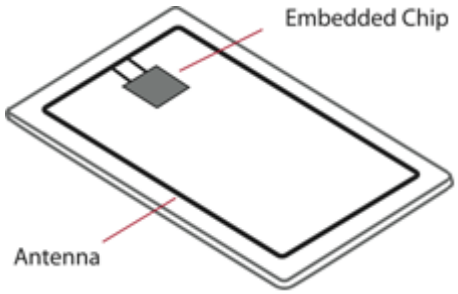


Figure 12. Contactless Card

5.2.1 Contactless Technology Standards

The International Organization for Standards (ISO) has created standards for three contactless technologies that are relevant for smart card interfaces and applications:[23]

- ISO/IEC 10536 close coupling cards
- ISO/IEC 14443 proximity cards
- ISO/IEC 15693 vicinity cards

ISO/IEC 10536 has not been widely deployed. In addition, advances in the ISO/IEC 14443 and ISO/IEC 15693 technologies have made the ISO/IEC 10536 contactless standard increasingly less appealing.

ISO/IEC 10536, ISO/IEC 14443 and ISO/IEC 15693 contactless technologies make use of the application-level standards defined in ISO/IEC 7816, part 4 and above. These standards define the structure of commands sent to the card, data and file structures, security mechanisms, identification of applications, inter-industry data elements and card life cycle management.

While not a smart card standard, the Near Field Communication (NFC) standard, ISO/IEC 18092, is an important contactless technology standard that is expected to be integrated into mobile phones and other devices.

5.2.1.1 ISO/IEC 14443

ISO/IEC 14443 is an international standard that defines the interfaces to a "proximity" contactless smart card, including the radio frequency (RF) interface, the electrical interface, and the communications and anti-collision protocols. ISO/IEC 14443 compliant cards operate at 13.56 MHz and typically have an operational range of up to 4-10 centimeters (2-4 inches).

ISO/IEC 14443 is the primary contactless smart card standard being used for transit, financial, and access control applications. It is also used in electronic passports and in the FIPS 201 PIV card.

Type A and Type B are two communication methods defined by the standard. Differences include the modulation of the magnetic field used for coupling, the coding format and the anticollision method (i.e., how the cards and readers respond when more than one card responds at the same time to a reader's request for data). In 1994, when standardization began, Type A and Type B had slightly different application focus. Today's technological advances have removed this application differentiation. By including both in the final version of the ISO/IEC 14443 standard, the widest base of vendors are able to offer standardized contactless technology.

- **ISO/IEC 14443 Part 1 - Physical characteristics.** The standard defines the following:
  - Card dimensions (referring to 7810 for ID-1 cards)
  - Surface quality for printing
  - Mechanical resistance
  - UV and X-ray resistance

[23] Smart Card Alliance, *Contactless Technology for Physical Access: Technology and Standards Choices*, October 2002

- Sensitivity to surrounding magnetic fields

The standard also introduces the following specific terms:
- PICC: Proximity integrated circuit(s) card
- PCD: Proximity coupling device (the card reader or terminal)

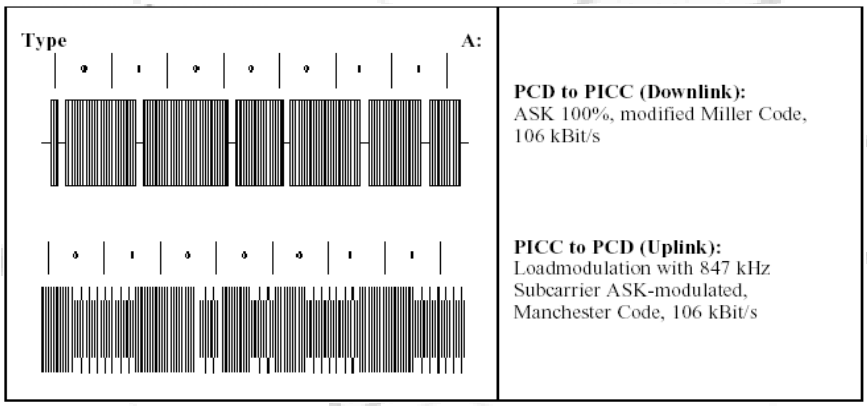
- **ISO/IEC 14443 Part 2 - Radio frequency power and signal interface**. This standard describes the characteristics of power transfer (based on inductive coupling) and communication between the PICC and PCD. Power is transferred to the card using a frequency-modulated field at 13.56 MHz +/- 7 kHz.

  Two different types of communication signal interfaces (bit coding) are specified: Type A and Type B. The bit protocol timings are defined and the standard (default) data transmission rate is defined at 106 kBaud.

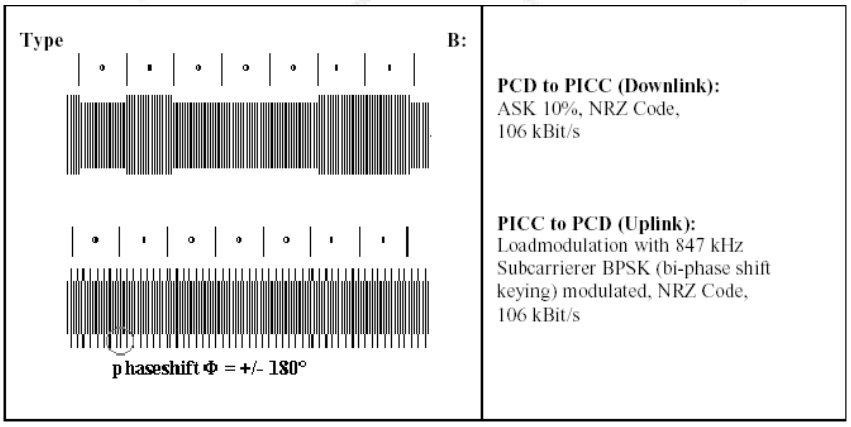
  Figure 13 shows the communications interface signals with Type A and Type B methods. The protocol as defined in the standard (Type A or Type B) does not imply the nature of the chip in the card. Since many current MCUs are able to generate their clock internally, even when the external modulation is 100% (Type A), MCU-based smart cards can be fully compatible with ISO/IEC 14443 Type A protocol.

Figure 13. Type A and Type B Communication Interface Signals[24]

Type A communication interface signal



Type B communication interface signal



[24] *eEurope Smart Cards document: TB6 WP1 Interoperability Draft May 2002*

- **ISO/IEC 14443 Part 3 Initialization and anticollision.** This part of ISO/IEC 14443 describes:
  - Polling for PICCs entering the field of a PCD (i.e., the terminal talks first).
  - Byte format, command frames and timing.
  - Request (REQ) and Answer To Request (ATQ) commands
  - Anti-collision methods to detect and communicate with one particular card when several cards are presented to the same reader. Anti-collision methods rely on a unique ID per card; however, depending on the communication type (A or B), the anti-collision method is different.
    - Type A: Binary search method referring to the unique identifier (UID) of the card.
    - Type B: Slotted Aloha method.
- **ISO/IEC 14443 Part 4 Transmission protocol.** This standard specifies a half-duplex block transmission protocol (T = CL). Several protocol scenarios are included in Appendix B of the standard, showing how this common transmission protocol can be used. The standard also defines the transparent exchange of data, independent of the lower layers. The commands in this set are all mandatory, providing interoperability with fully compliant products.

5.2.1.2 ISO/IEC 15693

ISO/IEC 15693 describes standards for "vicinity" cards. Specifically, it establishes standards for the physical characteristics, radio frequency power and signal interface, and anti-collision and transmission protocol for vicinity cards that typically operate within 1.5 meters (approximately 5 feet). ISO/IEC 15693-based smart cards are typically used in physical access control applications.

- **ISO/IEC 15693-1 Physical characteristics. T**his standard refers to ISO/IEC 7810 for dimensions and introduces specific terms:
  - VICC: Vicinity integrated circuit(s) card
  - VCD: Vicinity coupling device

ISO/IEC 15693-1 also includes definitions for the behavior of the card when exposed to mechanical stress, static and alternating electric fields, and magnetic fields.

- **ISO/IEC 15693-2 Air interface and initialization**. This part of ISO/IEC 15693 describes the characteristics of power transfer (based on inductive coupling) and communication between the VICC (card) and VCD (reader device). The power is transferred to the card using a frequency-modulated field at 13.56 MHz +/- 7 kHz. The standard requires that several different modes be supported by the VICC.
- **ISO/IEC 15693-3 Anti-collision and transmission protocol**. This part of ISO/IEC 15693 describes:
  - Protocols and commands.
  - Other parameters required to initialize communication between a VICC and a VCD.
  - Methods to detect and communicate with one card among several cards presented (anti-collision).
  - Data elements – for example, UID and Application Family Identifier (AFI).
  - Memory organization.
  - Behavior of VICCs described in state machine diagrams.
  - Set of commands (mandatory, optional, custom and proprietary).

5.2.1.3 Near Field Communication Standards and Specifications

Near Field Communication (NFC) is a short-range wireless connectivity technology that provides intuitive, simple, and safe communication between electronic devices. Communication occurs when two NFC-compatible devices are brought within four centimeters of one another. NFC operates at 13.56 MHz and transfers data at up to 424 Kbits/second.

NFC-enabled devices are specified by standards in ISO/IEC (ISO/IEC 18092), ETSI (ETSI TS 102 10 V1.1.1 (2003-03)) and Ecma International (ECMA-340) and by specifications published by the NFC Forum.

ISO/IEC 18092[25] (also ECMA-340) defines communication modes for Near Field Communication Interface and Protocol (NFCIP-1) using inductive coupled devices operating at the center frequency of 13.56 MHz for interconnection of computer peripherals. The standard defines:

- Both active and the passive communication modes of NFCIP-1 to realize a communication network using Near Field Communication devices for networked products and also for consumer equipment.
- Modulation schemes, codings, transfer speeds and frame format of the RF interface, as well as initialization schemes and conditions required for data collision control during initialization.
- Transport protocol including protocol activation and data exchange methods.

ISO/IEC 18092 allows backward compatibility with existing contactless devices by supporting ISO/IEC 14443 Type A, and the Japanese Industrial Standard (JIS) X 6319-4 (also known as FeliCa, see Section 5.2.1.4) contactless interface protocols.

An NFC-enabled device can operate in reader/writer and peer-to-peer mode, and may operate in card emulation mode. An NFC tag is typically a passive device (for example, integrated in a smart poster) that stores data that can be read by an NFC-enabled device. NFC Forum-certified devices in NFC Forum Reader/Writer mode must support the RF requirements for ISO/IEC 14443 Part A, ISO/IEC 14443 Part B and FeliCa (see Section 5.2.1.4) and as outlined in the relevant parts in the ISO/IEC 18092.[26]

ISO/IEC 21481 (also ECMA-352) specifies the communication mode selection mechanism for devices implementing ISO/IEC 18092, ISO/IEC 14443 or ISO/IEC 15693; the standard was designed to not disturb any ongoing communication at 13.56 MHz.

Additional information about the application and implementation of NFC is covered in detail in CSCIP Module 4, *Smart Card Usage Models: Mobile and NFC*.

5.2.1.4 Other Contactless Smart Card Technology Implementations

Vendors also offer contactless smart card technology based on proprietary specifications. In general, most smart card applications today use one of the contactless technology standards discussed above.

Two of the prominent proprietary specifications that are now included in industry standards are the NXP Semiconductor MIFARE™ protocol and the Sony FeliCA protocol.

5.2.1.4.1 NXP Semiconductors MIFARE[27]

NXP Semiconductors MIFARE Classic™ contactless memory IC uses a protocol complying with ISO/IEC 14443 Type A up to Part 3 and ISO/IEC 18092. The protocol for this IC does not implement ISO/IEC 14443 Part 4 and uses a proprietary cryptographic algorithm. NXP Semiconductors' MIFARE Classic is one of the most widespread contactless technologies used in contactless e-ticketing systems.

In addition, NXP Semiconductors offers MIFARE-branded products that are fully compliant with ISO/IEC 14443 Type A up to Part 4. Furthermore, the trend towards open cryptography is reflected in the MIFARE DESFire EV1, MIFARE Plus and MIFARE Ultralight C products, which are based on the Advanced Encryption Standard AES-128 and/or on DES/Triple DES. The MIFARE Plus and MIFARE DESFire EV1 products feature a fixed operating system on a contactless microcontroller IC and are certified according to Common Criteria EAL 4+.

[25] Source: ISO/IEC
[26] NFC Forum, NFC Forum Frequently Asked Questions, http://www.nfc-forum.org/resources/faqs/
[27] Source: NXP Semiconductors

According to NXP, more than 1 billion MIFARE-based contactless and dual-interface smart card chips and 10 million reader components have been sold.[28]

5.2.1.4.2 Sony FeliCa

FeliCa is a contactless smart card technology developed by Sony and widely used in Asia for electronic purse systems, mobile payment and public transport payment and ticketing. Prominent implementations include: the East Japan Railway's Suica card (ticket and e-money); bitWallet, Inc.'s Edy e-money in Japan; and the Hong Kong Octopus Card (ticket and e-money).

FeliCa complies with Japanese Industrial Standard (JIS) X 6319-4, Specification of Implementation for Integrated Circuit(s) Cards - Part 4: High Speed Proximity Cards, and in ISO/IEC 18092.

FeliCa is similar to ISO/IEC 14443. FeliCa operates at 13.56 MHz, uses Manchester coding at up to 424 Kbit/sec, and has on operating range of 10 centimeters or less.

5.2.1.5 Comparison of Contactless Technology: ISO/IEC 14443 and ISO/IEC 15693

ISO/IEC 14443 and ISO/IEC 15693 technologies, the primary contactless technology standards, have evolved with their own set of features and specifications. Both solve specific market requirements and each is now expanding into application areas originally addressed by the other technology. The key differentiators between the technologies are their operational ranges, speed (data transfer rates) and extent and maturity of features and applications using the technologies.

ISO/IEC 14443 and ISO/IEC 15693 technologies share the following important features and benefits:

- 13.56 MHz frequency of operation. This frequency is able to be used throughout the world for contactless applications.
- Read/write capability to the card. This allows user information to be stored and updated on the card (for example, a PIN or biometric template) and helps eliminate the need to access a host computer or database during use.
- Ability for manufacturers to implement security features. Although neither standard specifies security, features such as DES, Triple DES and AES, are commonly available.
- Support for card-to-reader authentication.
- Support for multiple interface readers, allowing a single reader to work with multiple technologies. This approach offers businesses a migration path into contactless smart card technology that does not require them to abandon their currently installed access control solution.
- Hybrid card capability, allowing incorporation of multiple contactless technologies on a single card.

The various RF standards specify the minimum and maximum field strength but do not define any minimum or maximum operational range. The distance at which a contactless smart card can be read is subject to multiple factors, including size and gain of the antenna (for receiving and transmitting data), magnetic field strength, frequency used, and power required by the chip to operate. Operational ranges specifying the maximum distance at which the different RF technologies work can be expected to vary based on these factors. For example, ISO/IEC 10373 tests ISO/IEC 14443-compliant smart cards from 0 to 4 centimeters, but some chips/cards could operate to 10 centimeters under favorable conditions. ISO/IEC 15693-based smart cards have three different modes of operation which support varying operational ranges (based on different power requirements for the chip):

- To read a device unique number, the range can be up to 5 feet (approximately 1.5 meters);
- To both read and write, operations are possible from 1- 2 feet;
- To support a cryptographic authenticated mode (if available in the chip), the range is approximately 4 inches (10 centimeters).

[28] http://www.nxp.com/#/pip/pip=[pfp=53422]|pp=[t=pfp,i=53422]

Table 5 compares technical features for contactless smart card technology and Section 10.3 includes additional information about contact and contactless smart card standards. ISO/IEC 14443-based contactless smart card technology is now being used in credit/debit payment, transit payment and physical access applications. ISO/IEC 15693-based contactless smart card technology is primarily used for physical access applications.

Table 5. Comparison of Contactless Technology Technical Features

Features	ISO/IEC 14443	ISO/IEC 15693
Standards	ISO/IEC 14443 ISO/IEC 7810	ISO/IEC 15693 ISO/IEC 7810
Frequency	13.56 MHz	13.56 MHz
Operational range	Up to 4-10 centimeters (~2-4 inches)	Up to 1-1.5 meter (~5 feet)
Chip types supported	Memory Wired logic Microcontroller[29]	Memory Wired logic
Encryption and authentication functions[30]	MIFARE, 3DES, AES, RSA[31], ECC	Supplier specific, 3DES
Memory capacity range	64 to 64K bytes	256 and 2K bytes
Read/write ability	Read/write	Read/write
Data transfer rate (Kb/sec)	Up to 106 (ISO) Up to 848 (available)	Up to 26.6
Anti-collision	Yes	Yes
Card-to-reader authentication	Challenge/Response	Challenge/Response
Hybrid card capability	Yes	Yes
Contact interface support	Yes	Yes

In addition to the standards-based contactless technology, proprietary contactless smart card technologies are also in use[32], primarily for transit applications.

5.2.1.6 Comparison of Contactless Technology: ISO/IEC 14443 and ISO 18092/NFC

ISO/IEC 18092 was defined to allow backward compatibility with existing contactless devices by supporting ISO/IEC 14443 Type A and the Japanese Industrial Standard (JIS) X 6319-4 (also known as FeliCa, see Section 5.2.1.4) contactless interface protocols.

[29] ISO/IEC 14443 uses the standard ISO/IEC 7816 for common application-level functions.
[30] The ISO standard does not specify security functions.
[31] RSA-based encryption and authentication may not be available on all cards due to power consumption, execution time or key length constraints.
[32] Examples are Sony FeliCa, Cubic GO Card and Calypso.

Table 6 shows a comparison of NFC devices with contactless smart card systems. Two primary differences from an architectural perspective are:

- An NFC-enabled device can be either an Initiator (i.e., initiating and controlling the data exchange) or a Target (i.e., a device that responds to commands from the Initiator). A contactless smart card operates only as a Target, with the reader/writer the Initiator.
- The NFC protocol supports active and passive communication modes. In active mode, both the Initiator and the Target generate an RF field for transmitting data; in passive mode, only the Initiator generates an RF field.

Table 6. Comparison of NFC Devices and Contactless Smart Card Systems[33]

	NFC Devices		Contactless Smart Card Systems	
	Initiator	**Target**	**Reader/writer**	**Contactless smart card**
Communication Principle	Active communication mode: Both Initiator and Target generate RF field		Reader generates RF field and card answers using load modulation	
	Passive communication mode: Initiator generates RF field and Target answers using load modulation			
Initialization	Active communication mode: RF collision avoidance		Initialization and anti-collision	
	Passive communication mode: Initialization and anti-collision			
Speed at initialization (Kbit/s)	106, 212, 424		106 for ISO/IEC 14443 Type A 212, 424 for FeliCa	
Communication protocol	NFC IP-1 data exchange protocol		ISO/IEC 14443 transmission protocol MIFARE: fixed command set FeliCa: fixed command set	
Speed at communication protocol (Kbit/s)	106, 212, 424		106, 212, 424, 848 for ISO/IEC Type A (including amendments) 106 for MIFARE 212, 424 for FeliCa	

Table 7 and Table 8 show how ISO/IEC 18092 accommodates compatibility among the existing standards and proprietary specifications that make up the majority of the installed base of contactless smart cards.

Table 7. Comparison of ISO/IEC 18092 Initiator Passive Mode, ISO/IEC 14443 and FeliCa[34]

Initiator (Reader)	NFC (Passive)	MIFARE Classic	ISO/IEC 14443 Type A	ISO/IEC 14443 Type B	FeliCa
Protocol	Data Exchange Protocol	MIFARE Classic	ISO Protocol (T=CL)	ISO Protocol (T=CL)	FeliCa
Anti-collision procedure	Bitwise (106 Kbit/s); Time Slot (212, 424 Kbit/s)	Bitwise	Bitwise	Slot Marker	Time Slot

[33] NFC vs. ISO 14443 vs. Felica, Bob Jiang, Philips presentation, Feb. 23, 2006, http://blogs.forum.nokia.com//data/blogs/resources/300066/Philips-NFC-vs-ISO14443-vs-Felica-SLIDES.pdf, , with updates from the NFC Forum

[34] Ibid.

Initiator (Reader)	NFC (Passive)	MIFARE Classic	ISO/IEC 14443 Type A	ISO/IEC 14443 Type B	FeliCa
RF Interface	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz
	106 - 424 Kbit/s	106 Kbit/s	106 - 848 Kbit/s	106 - 848 Kbit/s	212 Kbit/s
	106: 100% ASK 212/424: 8-30% ASK	100% ASK	106: 100% ASK >212: 60% ASK	10% ASK	8-30% ASK
	106: Modified Miller 212/424: 8-30% Manchester	Modified Miller	Modified Miller	NRZ	Manchester

Table 8. Comparison of ISO/IEC 18092 Target (Card/Tag) Passive Mode, ISO/IEC 14443 and FeliCa[35]

Target (Tag)	NFC (Passive)	MIFARE Classic	ISO/IEC 14443 Type A	ISO/IEC 14443 Type B	FeliCa
Protocol	Data Exchange Protocol	MIFARE	ISO Protocol (T=CL)	ISO Protocol (T=CL)	FeliCa
Anti-collision procedure	Bitwise (106 Kbit/s); Time Slot (212, 424 Kbit/s)	Bitwise	Bitwise	Slot Marker	Time Slot
RF Interface	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz
	106 - 424 Kbit/s	106 Kbit/s	106 - 848 Kbit/s	106 - 848 Kbit/s	212-424 Kbit/s
	Load Modulation	Load Modulation	Load Modulation	Load Modulation	Load Modulation
	106: Manchester (with subcarrier) 212/424: Manchester	Manchester (with subcarrier)	Manchester (with subcarrier)	BPSK	Manchester

5.3 Dual Interface

The dual-interface smart card, as the name implies, has both a contact interface and a contactless interface. Physically the card looks like a contact card, but the IC module has two additional contact points for the antenna coil. The IC can use either ISO/IEC 7816 or ISO/IEC 14443 protocols to communicate with a reader. Figure 14 shows an illustration of a dual-interface card.

[35] Ibid.

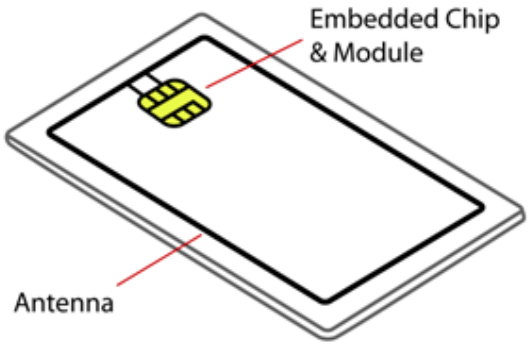


Figure 14. Dual-Interface Smart Card

A dual-interface card may be required, for example, for a transit card, which requires the contactless mode for fast transaction times and throughput at turnstiles and the contact mode to allow funds to be reloaded at an ATM or merchant POS terminal.

A hybrid smart card can be considered a type of dual-interface card. Hybrid cards operate in both contact and contactless modes by using separate secure ICs for each mode. Hybrid cards, while still in use, do not represent current technology; they were an earlier solution to allow smart cards to operate in both contact and contactless modes, which is now readily available with today's dual-interface products. Hybrid cards differ from dual-interface cards in that the two interfaces of a hybrid card typically provide access to different memories, while the single memory of a dual-interface can be accessed via either interface.

6 Memory Sizes and Types

6.1 Memory-Based Smart Cards[36]

Memory smart cards are used for applications that need data storage, but that have minimal requirements for data protection. The data can be any information required by the specific application.

Memory smart cards use non-volatile memory (NVM) which allows the card to hold data even after its power source is removed. The NVM in a memory smart card can incorporate different memory technologies but typically uses erasable programmable read-only memory (EPROM) or electrically erasable programmable read-only memory (EEPROM). EPROM can only be changed once and is often used in prepaid service cards such as telephone calling cards that count off the minutes used and are then discarded. When the device is used at room temperature, EEPROM can be changed up to one million times. Logic that can be used to update a counter in prepaid service cards is built in.

Memory smart cards can have different levels of security, from no security to moderate security implemented with logic in conjunction with the memory IC. Security mechanisms provided include: unique serial numbers, authentication logic, counter logic, error counters, personal identification number (PIN), secret codes or keys, and other security logic.

6.2 Secure Microcontroller-Based Smart Cards[37]

Secure microcontroller-based smart cards use a number of types of memory.

- **Read-Only Memory (ROM)** contains the chip's operating system. The operating system or command set controls all communication between the chip and the outside world. The operating system controls the access to the file system or applets. The ROM is masked or written during production by the semiconductor manufacturer and, once written, cannot be altered. Applications may also be stored in ROM. Some implementations make provisions for patching the ROM by redirecting execution to EPROM.
- **Electrically Erasable Programmable Read-Only Memory (EEPROM)** is non-volatile memory (i.e., it does not lose its data if power is shut off) and is read/write memory for the storage of data. Access to the EEPROM memory is controlled by the chip's operating system. EEPROM can currently contain 128 kilobytes (Kbytes) of memory with the potential for more than 256 Kbytes. EEPROM may contain data such as a PIN that can only be accessed by the card operating system. Other data, for example, a card's serial number, can be written to EEPROM during card manufacture. EEPROM is typically used for application data and for certain filtered functions. Most of the EEPROM memory is used to store user data such as a biometric, purse balance, special use authorization or payment tokens, loyalty tokens, demographic information, and transaction records, but it may also be used to store software such as a Java Virtual Machine and Java applets. EEPROM can be rewritten from tens to hundreds of thousands of times and can be programmed or erased in either blocks or bytes.
- **Flash Memory** (sometimes called "flash RAM") is a type of constantly-powered, non-volatile memory that must be erased and reprogrammed in units of memory called *blocks*. Flash memory is often used to hold control code such as the basic input/output system (BIOS) in a personal computer. When the BIOS needs to be changed (rewritten), the flash memory can be written to in block (rather than byte) sizes, making it easy to update. Since flash products are generic and applications can be downloaded at the last step of the production flow, they add flexibility and can provide faster time-to-market. While features vary among different products, flash memory is usually lower cost than byte-addressable EEPROM but current products generally can't be programmed and erased as many times and can't program or erase single bytes of memory.

[36] Smart Card Alliance, *What Makes a Smart Card Secure?, October 2008*.
[37] Source: *Government Smart Card Handbook*

Flash memory gets its name because the chip is organized so that a section of memory cells are erased in a single action or "flash." The erasure is caused by Fowler-Nordheim tunneling in which electrons pierce through a thin dielectric material to remove an electronic charge from a *floating gate* associated with each memory cell. A form of flash memory is available today that holds two bits (rather than one) in each memory cell, thus doubling the capacity of memory without a corresponding increase in price.

Some chip manufacturers provide components with a combination of ROM, flash memory and EEPROM.

- **Random Access Memory (RAM)**, which is volatile, is used as a temporary storage register by the chip's microcontroller. For example, when a PIN is being verified, the PIN sent by the terminal or PIN pad is temporarily stored in RAM. RAM is also used as 'scratch-pad' memory for cryptographic, biometric and other complex algorithms.

The following example will further explain the functions of the memory types listed above. A commonly used microcontroller smart card would have its operating system stored in ROM. The operating system or command set would respond to commands, such as "read a record," "write a record," and "verify PIN," sent to the card by a terminal or reader. Information such as fund balances, card serial number, and demographic information are stored in EEPROM. The CPU performs all processing functions, such as encryption, while RAM serves as a temporary register for information. During PIN verification, the PIN is temporarily stored in RAM. Since RAM memory is volatile, as soon as a card is powered off, all information stored in RAM is lost.

When evaluating card types for a particular application, the amount of memory in various components is important. The EEPROM capacity of a card is critical because a larger capacity EEPROM can store a greater number of application records and transaction files. The amount of ROM is also important because a larger capacity ROM can contain a more sophisticated operating system, which facilitates complex card and system operations. There is also a relationship between ROM and EEPROM in some cards because several vendors allow custom code extending the ROM's operating system to EEPROM. While this technique increases the card's functionality, it decreases the amount of EEPROM available for application and transaction storage. Conversely, more established and accepted applications can be included in ROM in future chip versions, freeing up EEPROM space for additional applications and expansion.

Recently the U.S. National Institute of Standards and Technology (NIST) has been working to standardize implementation of "match on card" fingerprint algorithms. These algorithms perform fingerprint template comparisons for the purpose of identity verification, and tend to demand larger than average RAM capacities. Porting such an algorithm to a smart card lacking sufficient RAM may require significant algorithm rework.

7 Smart Card Operating Systems

Smart cards are based on a secure computer architecture (with processor, storage memory, working memory and input/output communication lines) and contain embedded software which allows the device to operate. This embedded software, or operating system, manages:

- Memory access and access to the various logical structures the smart card contains;
- Program loading into the smart card;
- Program (or function) execution;
- Communication lines.

The operating system also enforces all of the security rules that are attached to various data structures or pieces of executable code.

A smart card chip is a single, monolithic piece of silicon with no possibility of adding, removing or changing anything in the chip without the operating system being involved. As specified in the ISO/IEC 7816 standard, the outside world only sees the smart card's behavior at the card interface.

Two different types of smart card operating systems are used:

- Native operating systems, also called "file-oriented systems"
- Object-oriented operating systems, also called "interpreted operating systems"

7.1 Native Operating Systems

In a traditional, "native" smart card operating system, the executable code is shared by the entire card and cannot be modified once the smart card is manufactured. A list of possible commands (also called Application Protocol Data Units or APDUs) is published by the manufacturer as part of the card product specification. These commands are typically a subset of the possible commands defined by the ISO/IEC 7816 Parts 4, 8, or 9 standard. These commands allow the card issuer to create and manage application data structures in the card's protected memory. The commands also allow the issuer to create separate application-specific directories, to which access will be protected by separate access conditions; this allows application independence (delegating management of the application from the card issuer to the application provider).

In this type of smart card, the operating system would manage two types of file: Dedicated Files (DFs) and Elementary Files (EFs). The DFs are similar to directories since they can contain other DFs or EFs. EFs can contain only data.

Both types of file can contain application data stored as simple binary strings, records or data objects. Data objects are identified by a tag and have a length and a value. They are also called BER-TLV data objects since they are encoded according to the ISO/IEC 8825 Section Basic Encoding Rules for Tag, Length, Value data objects. Access conditions are attached to these data structures at the time of their creation. In these operating systems, the access conditions (also called security attributes and stored in access control rules) cannot be changed after the data structure is created. The access conditions use various secrets protected by the card operating system to authenticate the process that is external to the card and that is asking to process a given command at the card interface. The secrets can be passwords or biometric templates, in applications which require the legitimate user to be identified, or cryptographic keys, in applications where a process needs to be identified or a communication line needs to be secure.

Table 9 shows an example of a possible set of commands for a smart card with a native operating system. Figure 15 illustrates an example of a native operating system smart card running multiple applications.

Data Structure Management	Security Management
SELECT	VERIFY
ACTIVATE FILE	EXTERNAL (/ MUTUAL) AUTHENTICATE
CREATE FILE	GENERATE ASYMMETRIC KEY PAIR
DEACTIVATE FILE	GET CHALLENGE
DELETE FILE	INTERNAL AUTHENTICATE
GET DATA	MANAGE SECURITY ENVIRONMENT
PUT DATA	CHANGE REFERENCE DATA
TERMINATE DF	RESET RETRY COUNTER
TERMINATE EF	

Table 9. Example Set of Commands for a Smart Card with Native Operating System

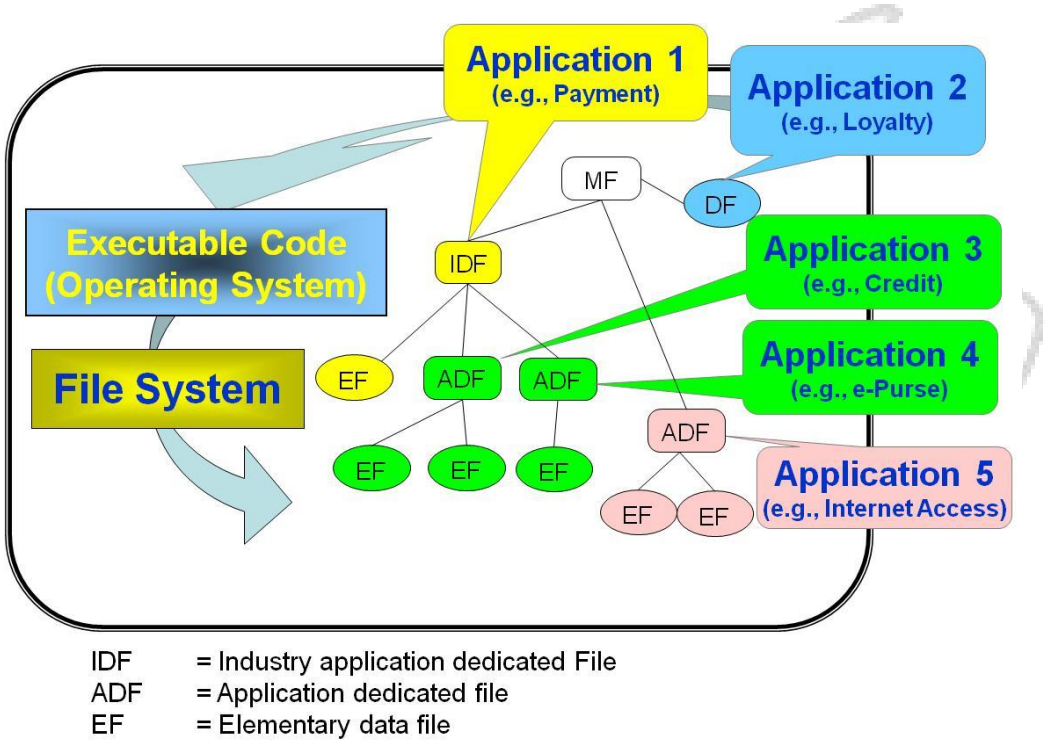


Figure 15. Native Operating System Smart Card with Multiple Applications

7.2 Object-Oriented Operating Systems

In the late 1990s, when smart cards started to be popular, card and application issuers discovered that the long development cycle required for a new smart card operating system was not compatible with their processes. A complete operating system requires about two years to develop and issuers wanted to deploy trials of new application functions at a much faster pace. The late 1990's development of electronic purse applications and custom applications using the mobile phone SIM card also drove the need for more application commands than the ISO specification covered. Various solutions were proposed by the industry to provide the smart card with core functionality (the smart card operating system) to manage application code and data objects instead of just data structures.

The following solutions emerged:

- Java Card, supported by Sun Microsystems and Visa, using a subset of the Java interpreted code as the development language for smart card applications.
- MULTOS, supported by MasterCard as well as a consortium of UK and Asian companies, using a proprietary interpreted language (MULTOS Executable Language (MEL)) as the development language for smart card applications.
- BasicCard, developed by a German company, allowing the creation of an application which automatically splits between the client and the card.

Object-oriented operating systems deliver the following benefits:

- Allowing new applications (including new commands) to be added to a smart card even after the card has been delivered to the customer (i.e., cardholder).
- Reducing the development time between new application requirements and deployment.
- Providing electronic component independence to enable multiple silicon suppliers to provide the same application support.
- Providing clean and simple isolation and separation of multiple applications in the same card environment. (Functions can be specific to an application.)
- Providing a good solution for rapidly evolving environments, where the cost of issuing a new card to an end user would be prohibitive. They are also a good technical solution for web developers who are willing to use cards already provided by other issuers.
- Providing a solution for systems where one issuer controls the card environment and offers multiple services that can be downloaded dynamically to the card without needing to change the silicon component (e.g., mobile phones, some government ID cards such as the Department of Defense Common Access Card).

Object-oriented operating systems, however, have the following drawbacks:

- The interpreted language is slower than native code. To address this, as many of the subroutines supporting frequently-used application functions as possible are loaded in the native operating system.
- They require a large and powerful integrated circuit (IC), since they have additional functions in the operating system that interprets the application requests. As a consequence, they require the most powerful silicon chips available, which also are the most expensive.
- Multi-application cards often use an object-oriented operating system platform for the initial deployment (i.e., test phase). The cost of the chip typically limits its use to applications that issue 10 million cards when the card needs to be renewed every three years. Multi-application cards have also had limited use in the financial market, since the branding on the card body surface is important and cannot be updated.
- In many systems, it has been found that the cost of a remote secure update infrastructure to manage post-issuance applications on a multi-application smart card is higher than issuing a new card. The main exception is with smart cards used in systems which are nearly always connected to an active network. This is the case for GSM mobile phones, pay TV applications and some corporate identification cards.

The main technical difference between a native smart card operating system and the object-oriented operating systems is the ability to attach specific application code to any structure defined by the application. This enables application-specific commands as well as application-specific functions that are loaded in the application domain along with the data structures that the functions are able to work with.

Figure 16 illustrates the object-oriented operating system blocks in a smart card chip.

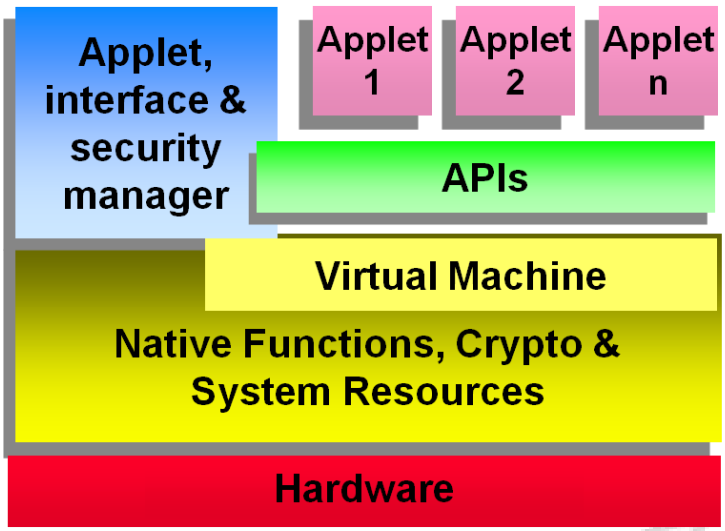


Figure 16. Object-Oriented OS Blocks in the Smart Card Chip

The applet, interface and security manager component has a very important role in this architecture. Some operating systems have this functionality built in (e.g., MULTOS); some others have it as an independent component (e.g., Java Card). This component uses a card registry to perform four very important roles:

1. **Command dispatcher**. The command dispatcher filters the commands which are relevant to the security manager or to the applications themselves.
2. **Security manager**. The security manager enforces the security rules for all applications and the firewalls between them. The security manager also allows the card to have global functions such as a user verification method (e.g., card PIN) which could be used by all applications.
3. **Secure installer**. The secure installer controls the loading and instantiation of any new application into a card. The secure installer requires and manages the required authentications, as well as the amount of memory that can be allocated and used by applications.
4. **Life cycle manager**. The life cycle manager turns on (enables) or turns off (disables) applications, functions, or the card itself. The life cycle manager also reports what is installed and active in a given card to the outside world.

7.2.1 MULTOS

MULTOS relies heavily on a public key infrastructure (PKI) architecture to provide security for the various application components. MULTOS comes complete with a certification authority, its own language (MULTOS Executable Language (MEL), but now also Java and C), and a complete personalization process. MULTOS consists of an operating system that contains a security manager on top of which is built a virtual machine that is able to handle the MEL application codes. MULTOS maintains very strict independence among applications, forcing them to communicate (if they need to) using internal APDU formats as if the applications were held in independent physical cards. MULTOS relies heavily on public key cryptography for all authentication between applications and their issuers, and allows dynamic loading and managing of applications in smart cards that have already been issued to end users.

The latest versions of MULTOS are now compatible with GlobalPlatform application management principles, allowing an application issuer to use either MULTOS or Java Card in the same application deployment.

7.2.2 Java Card: A Tool for Smart Card Applet Developers

Based on the Sun motto, "write once, run everywhere," the Java Card specification addresses what happens in the card, but does not address the terminal application. Java Card is primarily an on-card application programming interface (API) for application developers. The application in the terminal may not even know that the card is a Java Card-based device, since it sees only APDUs at the interface and no code.

The Java Card API needed the ability to securely manage the code to be loaded in the card, as well as the development of a standard interface. This capability was developed initially by Visa under the name of Visa Open Platform. The open industry consortium, Global Platform, standardized the concepts of a card manager and application domains in a Java Card.

The Java Card operating system provides a set of native functions and system resources, which can be called by application code written in Java through API calls that are interpreted by a virtual machine interface embedded in the card. Java Card alone is not enough to address the security and independence of all applications to be loaded on a given card, and is always used along with GlobalPlatform. GlobalPlatform is now considered a natural part of Java Card, even though its external mechanisms can also be used by other object-oriented operating systems.

7.2.3 Basic Card: Proprietary Solution for Easy Card Development

Some proprietary card operating systems are still commercially available. However, they are not used in large deployments, are primarily used for demonstrations or closed applications, and do not really qualify as object-oriented operating systems. For example, the BasicCard is a system developed by a German company, where the application is developed using the BASIC programming language. The application is automatically split between the card and the client it works with, and does not use the standard APDU commands defined by ISO/IEC 7816. The development kit allows the development of functions (basic subroutine calls with parameters and return values) which will be hosted in the BasicCard and called by the BASIC program in the client using a proprietary communication protocol. Each command (subroutine call) is identified using two bytes (defined by the developer). The BasicCard can be used as a cryptographic engine since most of the cryptographic protocols are available on the cards offered by the company. Nevertheless, since the approach doesn't use the standard tools defined by ISO/IEC 7816 for the various layers, BasicCard is very dependent on the client, which must have the "other half" of the application to work with a given card.

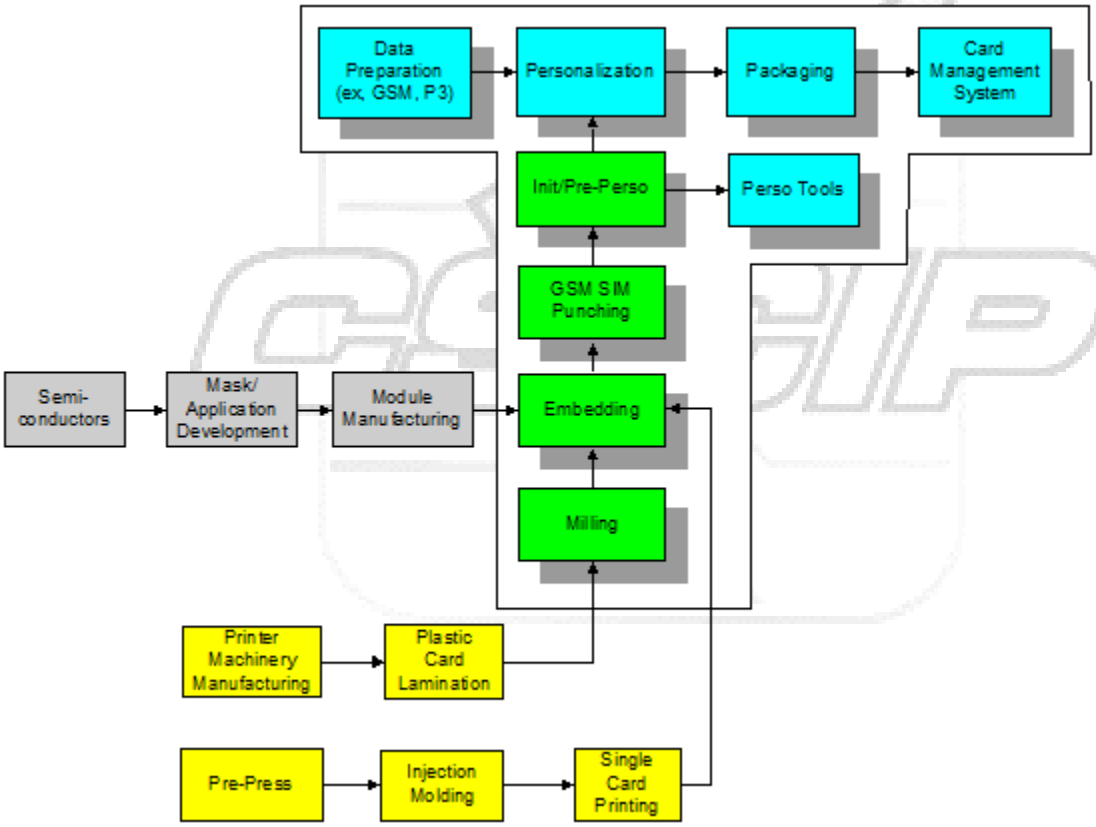
8 Smart Card Manufacturing Process[38]

This section provides an overview of a general smart card manufacturing process, illustrated in Figure 17. Inputs into the process are the smart chip micro-module, provided by semiconductor manufacturers (process shown in gray), and the card itself, provided by manufacturers who produce the card body (process shown in yellow). The card manufacturer will create specifications for both the card body and chip module to be used that are specific to the issuer's smart card application.

The smart card manufacturer performs the steps shown in green, milling the card body, embedding the module, punching the SIM (if a GSM application), and initializing the smart card in a pre-personalization step. Either the smart card manufacturer or a personalization bureau performs the steps shown in blue, preparing the data, electrically and graphically personalizing the card, packaging the card for shipment and providing card management services.

The manufacturing process will differ by supplier and by end customer. For example, some smart card manufacturers also produce modules and offer printing services, and some large banks operate their own personalization bureaus.

Figure 17. Smart Card Manufacturing Steps and Process



[38] Source: The content in this section was provided by CPI Card Group.

8.1 Card Body Material and Production

The card body material is selected based on the application for which the smart card will be used. The primary types of card body materials are acrylonitrile-butadiene-styrene (ABS), pre-molded ABS and polyvinyl chloride (PVC). PVC is primarily used by the financial market for payment cards since the cards can be embossed. ABS is a less expensive card body material, used primarily in the telecommunications market. With a pre-molded ABS card body, the milling stage in the smart card manufacturing process is not needed since the module cavity is pre-molded into the card.

Identity cards tend to use higher stability material. If laser engraving is required, polycarbonate card body material would be used to provide support for high resolution printing.

Table 10 shows the different types of card body materials, with key properties and applications that the card body technology is used for.

Table 10. Card Body Materials: Properties and Typical Applications

	PVC	ABS	PC	PETF	PETG	PET
Chemical Name	Polyvinyl chloride	Acrylonitrile-butadiene-styrene	Polycarbonate	Polyethylene terephthalate film	Polyethylene terephthalate glycol	Polyethylene terephthalate (polyester)
Manufacturing Form	Co-extruded and laminated	Molding	Co-extruded	Co-extruded and laminated	Co-extruded and laminated	Molding
Temperature Stability	80 degrees C, maximum	100 degrees C, maximum	160 degrees C, maximum	200 degrees C, maximum	70 degrees C, maximum	75 degrees C, maximum
Mechanical Properties	Ages very quickly	Mechanically strong	High stability	Very high stability	High stability	Ages very quickly and becomes brittle with age
Typical Applications	Bank cards, GSM SIMs, pay TV modules	Telephone cards, GSM SIMs	GSM SIMs, identity cards	Health identity cards, identity cards, transit fare cards	Bank cards, health identity cards, identity cards	Health identity cards, identity cards, transit fare cards

Card body production includes a number of processes and steps that will depend on the application that the card is used for, including:

- Printing non-personalized images and/or data on the card
- Laminating the card with magnetic stripe and optical variable device layers.
- Laminating the card with an inlay that includes the smart card chip and/or antenna (for a contactless smart card)

8.2 Smart Chip Micro-Modules

Semiconductor manufacturers produce the smart card silicon chips in wafer form. Wafers are then sawed into individual chips and micro-modules are manufactured. Micromodules protect the silicon chip in the card and provide the electrical contacts to the outside world. Thousands of different types of smart chip micro-modules are available from semiconductor manufacturers.

Microcontroller modules are used for GSM SIMs, EMV bank cards and identity cards. An example memory module application is a prepaid phone card.

Figure 18 illustrates the construction of a contact smart card micro-module. The bond wire is connected directly from the silicon chip to the contact.

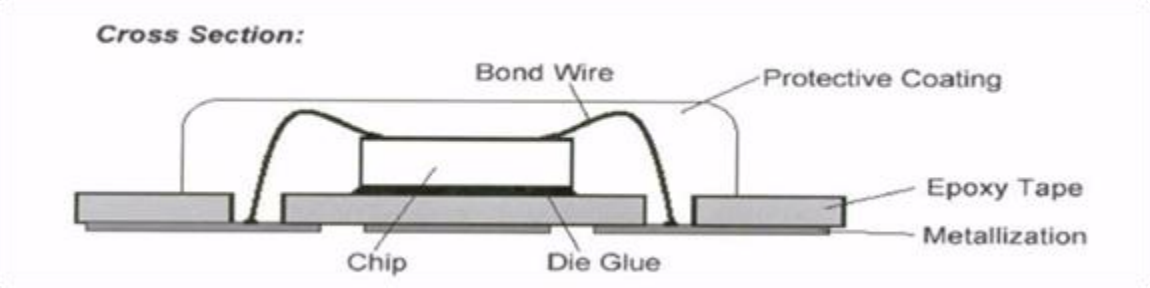


Figure 18. Contact Smart Card Micro-Module Construction

Figure 19 shows the construction of a dual interface smart card micro-module. As with the contact smart card module, the silicon chip contacts are connected to the contact plates. The smart card manufacturing process has an extra step to link the chip electrically to the antenna.

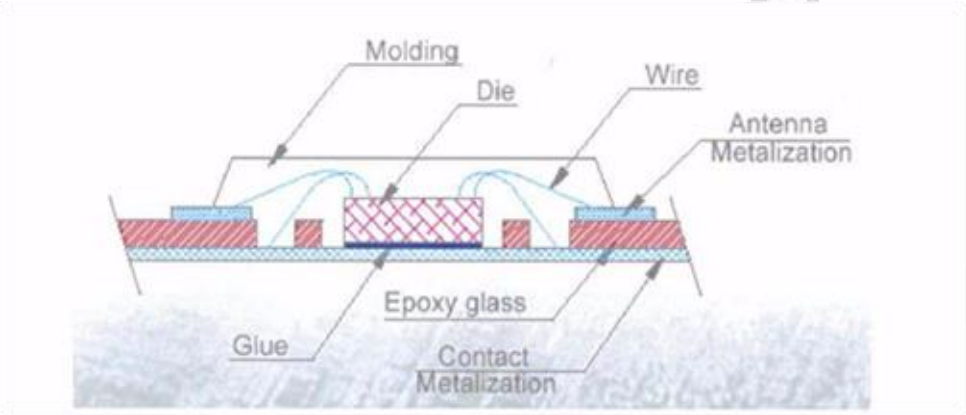


Figure 19. Dual Interface Smart Card Micro-Module Construction

In the case of a contactless smart card, the chip and antenna are laminated into the card body and the card would go directly to the pre-personalization or personalization step.

Modules are typically delivered to the smart card manufacturer on film (shown in Figure 20). The production of the module and the placement of the module on film may be done by the same or different companies.

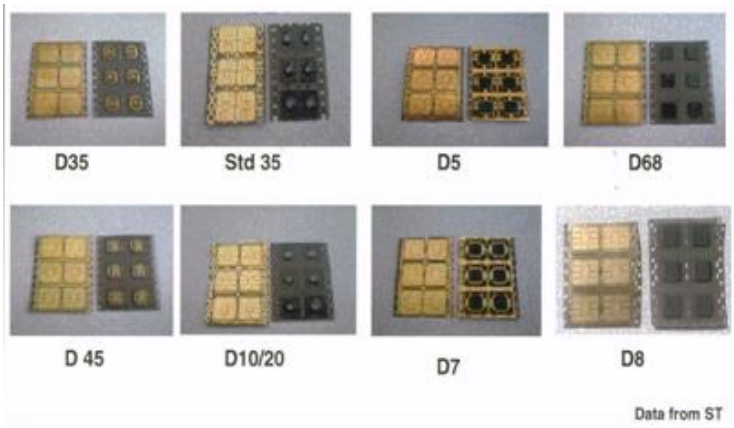


Figure 20. Examples of Modules and Film Types

8.3 Smart Card Manufacturing

The first step in manufacturing the smart card is milling the cavity for the micro-module into the card body (shown in Figure 21). This is a straightforward mechanical step, where a milling tool removes the P1 and P2 material. P1 provides the support for the adhesive or potting material used to embed the micro-module and P2 is sized to accept the micro-module. Different micro-modules require different cavity shapes, with the dimensions programmed into the milling machine.

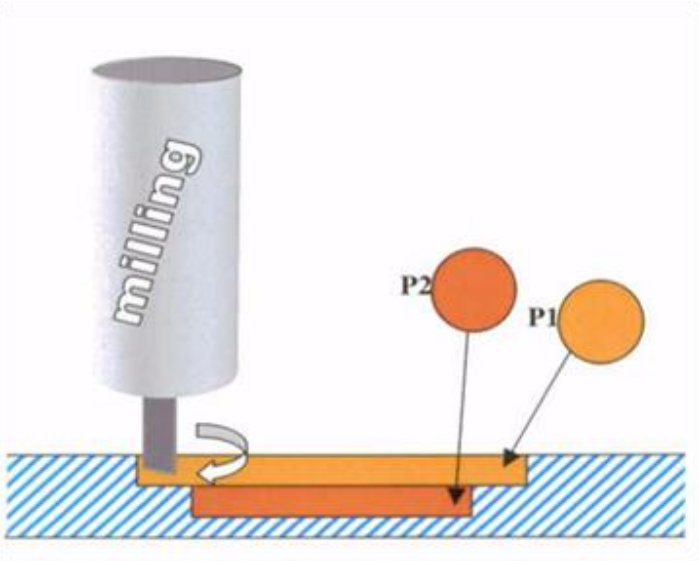


Figure 21. Milling the Micro-Module Cavity

Two processes are used to adhere the micro-module to the card. The original smart manufacturing method used cyanoacrylate (or "super glue"). With this process, the punched micro-module is attached to the milled card body with a drop of cyanoacrylate liquid glue in the bottom of the cavity. This process is rarely used now since the glue is too rigid and the process needs a clean room environment.

Most commonly used now is the hot melt process. In this process, hot melt adhesive tape is punched and laminated beneath the micro-module film (see Figure 22).

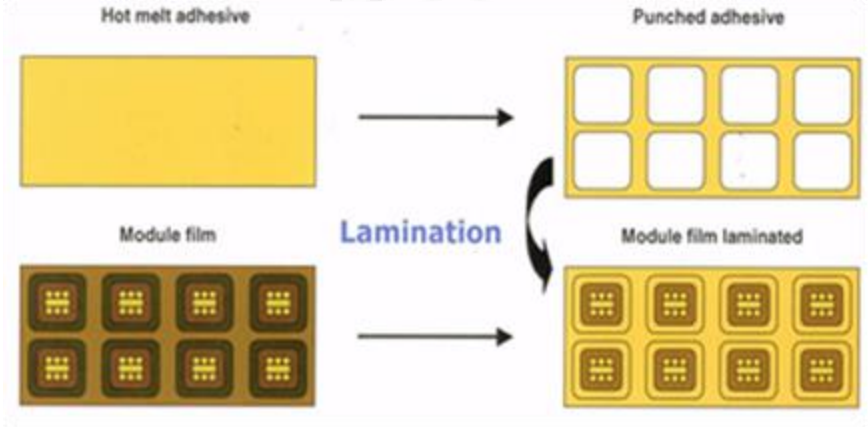


Figure 22. Hot Melt Adhesive Lamination

Once the module has the tape laminated and the card body is milled, the embedding machine punches the module out of the film and attaches it to the smart card body (Figure 23). When using the hot melt process, both the module and the card body must be heated prior to embedding. The module and card body are then pressed together with the module heated to activate the glue. In high volume production,

the module and card must also be cooled prior to the next step. Smart card manufacturers create this process in collaboration with the glue, module and plastic manufacturers.

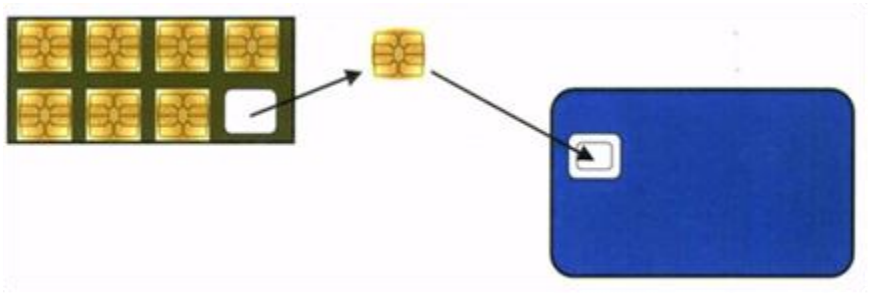


Figure 23. Embedding the Smart Card Module

For SIMs, there is one more step in the process after embedding the micro-module. A punch tool pre-cuts around the module to create the SIM "plug" (see Figure 24).

Figure 24. SIM Plug Punch

The last step of the manufacturing process is initializing or pre-personalizing the smart card chip. All semiconductor manufacturers ship micro-modules locked with a transport key. The smart card manufacturer unlocks the module as part of the production process. At this point, the smart card is ready to be personalized.

8.4 Smart Card Personalization

Personalization may be done by the smart card manufacturer or by a personalization bureau. This process both electrically personalizes the card (writing data to the chip and on the magnetic stripe) and graphically personalizes the card (printing and/or embossing information on the card body).

Three types of printing methods can be used during personalization: ink jet, thermal and laser. Laser printing is becoming more important in the market since it is fast and secure and uses no consumables. Laser marking is now used to print high resolution photos on identity cards and to burn the ID onto a SIM. Recently, certain financial institutions have started to use laser printing and to eliminate card embossing.

Personalization is discussed in more detail in CSCIP Module 3.

9 Smart Card Readers[39]

Smart card read/write devices provide the link between the smart card and the host system or application. The host system can be a PC, a network device, a stand-alone access control device such as a turnstile controller, a merchant's POS system or other type of computer system. The read/write device delivers power, initializes the card, and acts as the mediator between the smart card and the host. Power is delivered to the smart card by making a physical contact on the contact smart card micro-module or by inducing current through the antenna of contactless designs. Initialization is a specified protocol that must be performed on all smart cards and is supported by compatible readers.

Smart card read/write devices can be either transparent, requiring a host device to function, or they can be standalone devices functioning independently. Transparent read/write devices require a host for all signaling functions, including initialization and application delivery. This type of hardware has no internal logic except for a line driver to condition the signal between the card and the host. A transparent reader is similar to a PC soft modem; a host drives the reader and the card. This requires more support from the software, which must understand the design of the reader and the card communication requirements.

A standalone read/write device has all of the logic required to initialize a card and to act as a mediator between a smart card and the host. For example, the host may deliver a large packet of information to the reader to pass on to the card. The reader checks the packet and sometimes breaks it into smaller packets before sending the information to the smart card. This means that the host is only concerned with communication to the reader and not to the smart card. Standalone readers may have application-specific code or an operating system (often Linux or an embedded OS). Some standalone readers have integral hardware security modules (HSMs) for cryptographic key storage and are capable of authenticating with the smart card without host intervention.

Transparent readers require more drivers than standalone types, but are cheaper to manufacture and easier to change. Standalone readers, although more expensive than transparent devices, have generic driver sets that define the communication between a reader and a host. This is an important distinction because the design of a system's architecture will determine the ease of adding future applications and performing software upgrades.

A variety of smart card readers are available to support different applications and their host systems. Smart card readers are also available that support multi-factor authentication, including the card reader, keypad for secure personal identification number (PIN), and/or biometric readers.

9.1 Smart Card Readers for Secure Computer Access[40]

Smart cards are widely used to allow employees and users to securely login to computers and networks. Smart card readers are now easily integrated with applications and desktop operating systems through two standards: the Personal Computer/Smart Card (PC/SC) standard and the Chip Card Interface Device (CCID) specification.

The PC/SC standard allows smart card readers to be integrated easily with middleware or other applications, regardless of manufacturer or command set. Although this standard was developed for use in a Microsoft environment, it is now considered the de facto standard for many other platforms as well.

The CCID specification was developed for USB smart card readers. The specification was defined by the USB Implementer's Forum (USB-IF)[41] in conjunction with the smart card industry. CCID defines a command set and transport protocol over the USB so that a host system can communicate with a smart card reader. A specific USB class is now defined for smart card readers.

A wide variety of solutions are available for connecting a smart card to a computer, including readers that connect through the USB, RS-232 PCMCIA and Expresscard interfaces, as well as those that are

[39] Source: *Government Smart Card Handbook*
[40] Smart Card Alliance, *Logical Access Security: The Role of Smart Cards for Strong Authentication*, October 2004
[41] Additional information about CCID can be found at the USB Implementer's Forum web site, http://www.usb.org.

integrated into laptops and computer keyboards. In addition, smart phones and pocket PCs can include a separate smart card reader to allow users to authenticate themselves to the smart device with a separate smart card; for example, Research In Motion offers a reader to support smart card-enabled access to BlackBerry® smart phones[42].

Figure 25 shows examples of different reader solutions used for computer access. Additional information about the use of smart cards for secure computer and network access can be found in CSCIP Module 5.

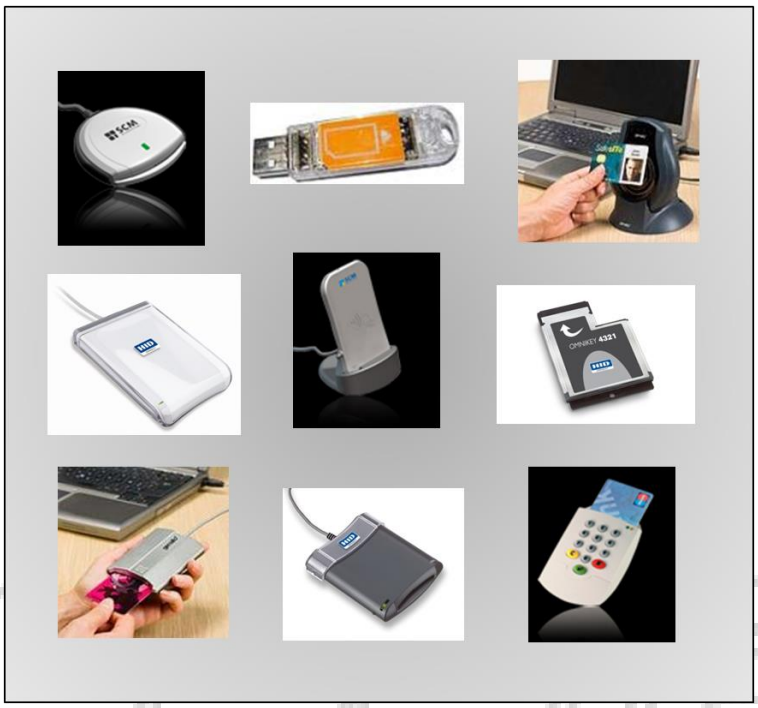


Figure 25. Examples of Smart Card Readers for Computer Access[43]

9.2 Smart Card Readers at the Point-of-Sale

Smart card technology is being used worldwide at the retail point-of-sale (POS). Vendors offer a wide variety of POS terminals supporting contact and contactless payments. POS terminals interface with the merchant POS system to accept and authorize payment transactions. Figure 26 shows examples of POS terminals that accept smart card-based payment. Additional information about the use of smart cards for secure payment can be found in CSCIP Module 6.

[42] Additional information is available at: http://na.blackberry.com/eng/ataglance/security/products/smartcardreader/

[43] Photos provided by Gemalto, HID Global and SCM Microsystems. Additional information about smart card readers can be found in the Smart Card Alliance smart card reader catalog at http://www.smartcardalliance.org.

Figure 26. Examples of Smart Card POS Terminals[44]

9.3 Smart Card Readers and Physical Access Control

Physical access control readers are typically self-contained units that interface to the access control card (e.g., an employee ID badge) and communicate to the physical access control system. Readers designed for secure physical access control applications are usually mounted at a convenient height on a door or turnstile with wiring hidden from view to prevent tampering. The physical access control reader can have one or more interfaces, accommodating a combination of contactless or contact smart card, PIN pad, biometric reader and sometimes turnstile control relays. Multi-technology readers are also available that accommodate more than one card technology in the same reader (e.g., both ISO/IEC 14443 and ISO/IEC 15693 contactless smart card technologies, both 13.56 MHz and 125 kHz contactless technologies or both contactless smart card and magnetic stripe technology). Multi-technology readers are often used to assist with migration from an installed physical access control system.

Figure 27 shows examples of smart card-based physical access control readers. Additional information about the use of smart cards for physical access can be found in CSCIP Module 5.

[44] Photos provided by VeriFone and ViVOtech.

Figure 27. Examples of Physical Access Control Readers[45]

[45] Photos provided by HID Global, Bridgepoint and Morpho.

10 Relevant Standards and Specifications

Numerous standards are relevant to smart card applications and more are created every year. They have various impacts at different levels of a smart card based-system and may deal with physical characteristics, security certifications, transmission protocols, and application loading or design. There are also industry "specifications," which are not "standards," but which play a very important role in smart card applications. Not all application specifications are listed in this section, though some of the important industry-focused applications are included.

Standards are voluntary, but are generally adhered to in the interest of achieving conformity and interoperability. A brief synopsis of the various smart card standards and specifications is included in this section. Additional information can be found in the body of work referenced with each smart card standard or specification.

ISO/IEC is the worldwide standard-setting body for technology, including plastic cards. These standards set minimums, but also include many options and tend to leave some issues unaddressed. As a result, conformance to ISO standards alone does not necessarily ensure interoperability – nor does it ensure that cards and terminals built to the specifications will interoperate. The main standards that pertain to smart cards are ISO/IEC 7810, ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 15693, ISO/IEC 24727 and ISO/IEC 7501.

The following should be noted:

1. Some standards listed below are available free of charge, but many must be purchased.
2. Some standards may not be listed in this section, but could be relevant to a specific application or a specific technique required by an implementation (e.g., standardized format of biometric information).

All standards and specifications covered in the CSCIP course and exam are included in this section. Other CSCIP modules include a list of standards and specifications relevant to the module topic, but do not include the details included in this section.

10.1 Standards Relevant to Smart Card Physical Characteristics

10.1.1 ISO/IEC 7810 – Identification Cards – Physical Characteristics

ISO/IEC 7810 was published in 1985 and describes major characteristics for four different sizes of cards with nominal thickness of 0.76 mm:

- ID-000 25 mm x 15 mm
- ID-1 85.60 mm x 53.98 mm
- ID-2 105 mm x 74 mm
- ID-3 125 mm x 88 mm

ID-1 is the standard size for contact as well as contactless smart cards. Standard card dimensions are: 54 mm x 85.6 mm x 0.76 mm (2.125 in x 3.370 in x 0.03 in).

The standard also specifies:

- The conditions for conformance
- The dimensions and tolerances of identification cards
- The construction and materials of identification cards
- The physical characteristics of the cards, such as bending stiffness, flammability, toxicity, resistance to chemicals, dimensional stability, adhesion or blocking, warpage, resistance to heat, surface distortions, and contamination.

10.1.2 ISO/IEC 7816 – Identification Cards – Integrated Circuit Cards[46]

ISO/IEC 7816 is a multi-part international standard broken into fourteen parts. ISO/IEC 7816 Parts 1, 2, 3 and 12 deal only with contact smart cards and define the various aspects of the card and its interfaces, including the card's physical dimensions, the electrical interface and the communications protocols. ISO/IEC 7816 Parts 4, 5, 6, 7, 8, 9, 11, 13 and 15 are relevant to all types of smart cards (contact as well as contactless).

ISO/IEC 7816, Part 1 describes the specifications for the physical characteristics of integrated circuit cards with contacts.

10.1.3 ISO/IEC 10373 – Identification Cards – Test Methods

- Part 1: General characteristics tests
- Part 2: Cards with magnetic stripes
- Part 3: Integrated circuit cards with contacts and related interface devices
- Part 5: Optical memory cards
- Part 6: Proximity cards
- Part 7: Vicinity card
- Part 8: USB-ICC (to be published)

10.1.4 ISO/IEC 24789 – Identification Cards – Card Service Life

- Part 1: Application profiles
- Part 2: Methods of evaluation

10.2 Standards Relevant to Technologies Which Could Be Found on a Smart Card

Smart cards often include other technologies in the card body. The following standards apply to common technologies:

- Magnetic stripes: ISO/IEC 7811 series, Identification cards – Recording technique
- Linear bar codes: ISO/IEC 15416 Information technology – Automatic identification and data capture techniques – Bar code print quality test specification – Linear symbols
- PDF417 bar code: ISO/IEC 15438 Information technology – Automatic identification and data capture techniques – PDF417 bar code symbology specification
- Optical memory cards: ISO/IEC 11693 Identification cards – Optical memory cards; ISO/IEC 11694 Identification cards – Optical memory cards - linear recording method

10.3 Standards and Specifications Relevant to Technologies Related to the Card Interface

10.3.1 ISO/IEC 7816 Series – Identification Cards – Integrated Circuit(s) Cards with Contacts

- **Part 2: Cards with contacts: Dimensions and location of the contacts**. This part of ISO/IEC 7816 specifies the dimensions and locations for each of the contacts on an integrated circuit card of an ID-1 card type. This part also provides information on the way to identify which standards define the use of the contacts.

[46] Source: http://www.iso.org

- **Part 3: Cards with contacts: Electrical interface and transmission protocols**. This part of ISO/IEC 7816 specifies the power and signal structures, and information exchange between an integrated circuit card and an interface device such as a terminal. It also covers signal rates, voltage levels, current values, parity convention, operating procedure, transmission mechanisms and communication with the card.
- **Part 12: Cards with contacts: USB electrical interface and operating procedures**. This document describes the operating conditions of an integrated circuit card that provides a USB interface.

10.3.2 ISO/IEC 14443 Series – Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards

ISO/IEC 14443 is an international standard that defines the interfaces to a "proximity" contactless smart card, including the radio frequency (RF) interface, the electrical interface, and the communications and anti-collision protocols. ISO/IEC 14443 compliant cards operate at 13.56 MHz and typically have an operational range of up to 4-10 centimeters (2-4 inches). ISO/IEC 14443 is the primary contactless smart card standard being used for transit, financial, and access control applications. It is also used in electronic passports and in the FIPS 201 PIV card.

Type A and Type B are two communication methods defined by the standard. Differences include the modulation of the magnetic field used for coupling, the coding format and the anticollision method (i.e., how the cards and readers respond when more than one card responds at the same time to a reader's request for data). In 1994, when standardization began, Type A and Type B had slightly different application focus. Today's technological advances have removed this application differentiation. By including both in the final version of the ISO/IEC 14443 standard, the widest base of vendors are able to offer standardized contactless technology.

10.3.3 ISO/IEC 15693 – Contactless Integrated Circuit Cards – Vicinity Cards

ISO/IEC 15693 describes standards for "vicinity" cards. Specifically, it establishes standards for the physical characteristics, radio frequency power and signal interface, and anticollision and transmission protocol for vicinity cards that typically operate within 1.5 meters (approximately 5 feet).

10.3.4 ISO/IEC 18092 – Information technology – Telecommunications and Information Exchange between Systems – Near Field Communication – Interface and Protocol

ISO/IEC 18092:2004 defines communication modes for Near Field Communication (NFC) interface and protocol (NFCIP-1) using inductive coupled devices operating at the center frequency of 13.56 MHz for interconnection of computer peripherals.

10.3.5 Personal Computer/Smart Card (PC/SC) Specifications

The PC/SC Workgroup was formed in 1996 and included Schlumberger Electronic Transactions, Bull CP8, Hewlett-Packard, Microsoft, and other leading vendors. This group has developed open specifications for integrating smart cards with personal computers. The specifications are platform-independent and based on existing industry standards. They are designed to enable application developers to create smart card-based secure network applications for banking, health care, corporate security, and electronic commerce. The specifications include cryptographic functionality and secure storage, programming interfaces for smart card readers and PCs, and a high-level application interface for application development. The specifications are based on the ISO/IEC 7816 standard and support EMV and GSM application standards.

10.3.6 Circuit(s) Card Interface Device (CCID) Specification[47]

The CCID specification defines requirements and specifications for Universal Serial Bus (USB) devices that interface with integrated circuit(s) cards or act as interfaces with integrated circuit(s) cards. The document specifies the USB-related characteristics of the integrated circuit(s) cards interface devices (CCID). The specification applies to smart cards and similar devices conforming to ISO/IEC 7816 specifications.

When a CCID is connected to a USB host, it may or may not have an ICC "inserted." The CCID identifies to the host its capabilities and requirements, and the host prepares to communicate with it. The CCID may then, at any time, detect the presence of an ICC, at which time it communicates that information to the host. As soon as the host receives information about the "attached" ICC, further communications may then take place between the host and the ICC through the CCID.

The CCID model assumes that an ICC is or can be inserted into the device. This is the purpose for the "slot change" interrupt message.

The specification was defined by the USB Implementer's Forum (USB-IF)[50] in conjunction with the smart card industry.

10.4 Standards and Specifications Relevant to the Card Commands and Application Data Structures

10.4.1 ISO/IEC 7816 Series – Identification Cards – Integrated Circuit(s) Cards

The following ISO/IEC 7816 parts apply to both contact and contactless smart cards.

- Part 4: Organization, security and commands for interchange
- Part 6: Interindustry data elements for interchange
- Part 7: Commands for Structured Card Query Language (SCQL)
- Part 8: Commands for security operations
- Part 9: Commands for card management
- Part 11: Personal verification through biometric methods
- Part 13: Commands for application management in a multi-application environment
- Part 15: Cryptographic information application

10.4.2 ISO/IEC 8825-1

ISO/IEC 8825-1 defines a set of Basic Encoding Rules (BER) that may be applied to values of types defined using the ASN.1 notation. Application of these encoding rules produces a transfer syntax for such values. It is implicit in the specification of these encoding rules that they are also used for decoding.

Information technology – ASN.1 encoding rules:

- Specification of Basic Encoding Rules (BER),
- Canonical Encoding Rules (CER)
- Distinguished Encoding Rules (DER)

[47] http://www.usb.org/developers/docs/devclass_docs/DWG_Smart-Card_CCID_Rev110.pdf

10.4.3 GlobalPlatform[48]

GlobalPlatform (GP) is an international, non-profit association. Its mission is to establish, maintain and drive adoption of standards to enable an open and interoperable infrastructure for smart cards, devices and systems that simplifies and accelerates development, deployment and management of applications across industries. According to GlobalPlatform, as of October 2008, an estimated 305.7 million GlobalPlatform-based smart cards had been deployed across the world, with an additional 2 billion GSM cards using GlobalPlatform technology for over-the-air (OTA) application download.

The applicable GlobalPlatform specification is: *GPD/STIP 2.2 Common Open Software Platform Technology for Smart Card Accepting Devices.*

10.4.4 Java Card[49]

Java Card provides a smart card operating system for running multiple applications. The applicable Java Card specification is: *Java Card 3.0.1 Platform Specification*.

10.5 Standards and Specifications Relevant to Security or Cryptography

10.5.1 ISO/IEC 9798 - Information Technology – Security Techniques – Entity Authentication

- Part 1: General
- Part 2: Mechanisms using symmetric encipherment algorithms
- Part 3: Mechanisms using digital signature techniques
- Part 4: Mechanisms using a cryptographic check function
- Part 5: Mechanisms using zero-knowledge techniques
- Part 6: Mechanisms using manual data transfer

10.6 Standards and Specifications Relevant to Security or Cryptography

10.6.1 ISO/IEC 9798 - Information Technology – Security Techniques – Entity Authentication

- Part 1: General
- Part 2: Mechanisms using symmetric encipherment algorithms
- Part 3: Mechanisms using digital signature techniques
- Part 4: Mechanisms using a cryptographic check function
- Part 5: Mechanisms using zero-knowledge techniques
- Part 6: Mechanisms using manual data transfer

10.6.2 ISO/IEC 11770 - Information Technology – Security Techniques – Key Management

- Part 1: Framework
- Part 2: Mechanisms using symmetric techniques
- Part 3: Mechanisms using asymmetric techniques
- Part 4: Mechanisms based on weak secrets

[48] GlobalPlatform specifications are available at http://www.globalplatform.org/specifications.asp
[49] Java Card specifications are available at http://java.sun.com/javacard/3.0.1/specs.jsp

10.6.3 ISO/IEC 18033 - Information Technology – Security Techniques – Encryption Algorithms

ISO/IEC 18033 specifies encryption systems (ciphers) for the purpose of data confidentiality and has 4 parts:

- Part 1 specifies the terms and definitions used throughout ISO/IEC 18033; the purpose of encryption, the differences between symmetric and asymmetric ciphers, and the key management problems associated with the use of ciphers; the uses and properties of encryption; the criteria for the inclusion of encryption algorithms in ISO/IEC 18033.
- Part 2 specifies asymmetric encryption systems (ciphers) for the purpose of data confidentiality.
- Part 3 specifies block cipher algorithms. A block cipher is a symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e., a string of bits of a defined length, to yield a block of ciphertext.
- Part 4 specifies stream cipher algorithms.

10.6.4 ISO/IEC 24727 - Information Technology – Identification cards – On-Card Biometric Comparison

ISO/IEC 24727 is a multipart standard aimed at achieving interoperability among various smart card systems. The standard for on-card biometric comparison is currently under development.

10.6.5 Common Criteria

Common Criteria (CC) is an internationally approved security evaluation framework providing a clear and reliable evaluation of the security capabilities of IT products, including secure ICs, smart card operating systems, and application software. CC provides an independent assessment of a product's ability to meet security standards, with the goal of giving customers confidence in the security of IT products and leading to better decisions about security. Security-conscious customers, such as national governments, are increasingly requiring CC certification in making purchasing decisions. Since the requirements for certification are clearly established, vendors can target very specific security needs while providing broad product offerings. CC has been adopted and is recognized by 26 countries.[50]

10.6.6 NIST Federal Information Processing Standards

FIPS standards are developed by NIST Computer Security Division. FIPS standards are designed to protect federal computer and telecommunications systems. The following FIPS standards apply to security or cryptography.

10.6.6.1 FIPS Standards for Digital Signatures

- **FIPS 186-2 Digital Security Standard** specifies a set of algorithms used to generate and verify digital signatures. This specification relates to three algorithms specifically, the Digital Signature Algorithm (DSA), the RSA digital signature algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA).
- **ANSI X9.31-1998** contains specifications for the RSA signature algorithm. The standard specifically covers both the manual and automated management of keying material using both asymmetric and symmetric key cryptography for the wholesale financial services industry.
- **ANSI X9.62-1998** contains specifications for the ECDSA signature algorithm.

[50] https://www.commoncriteriaportal.org/

10.6.6.2 FIPS Standards for Secure Hash Algorithms

- **FIPS 180-3, Secure Hash Standard,** defines five hashing algorithms that can be used within Federal applications : SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 (SHA: Secure Hash Algorithm).

10.6.6.3 FIPS Standards for Digital Encryption

- **FIPS 197 Advanced Encryption Standard** (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information.

10.6.6.4 FIPS 140 Security Requirements for Cryptographic Modules Standard

The security requirements contained in FIPS 140 pertain to areas related to the secure design and implementation of a cryptographic module, specifically: cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks. The current version is FIPS 140-2. NIST has a current draft of FIPS 140-3 available for public comments.

10.6.6.5 NIST Special Publications

NIST has issued a number of special publications with additional specifications for cryptography use within the U.S. Federal government.

- NIST SP800-21-1, "Guideline for Implementing Cryptography In the Federal Government," Second Edition, December 2005
- NIST SP800-57, "Recommendation for Key Management," Parts 1 and 2, August, 2005

10.7 Standards and Specifications Relevant to Issuers or Specific Industry Sectors

10.7.1 ISO/IEC 7501 Series, Identification Cards – Machine Readable Travel Documents

This international standard specifies the form and provides guidance on the construction of machine readable travel documents for both visible and machine readable features.

It is based on a standard established by the International Civil Aviation Organization, Doc 9303, which is maintained by a Technical Advisory Group on Machine Readable Travel Documents.

- Part 1: Machine readable passport
- Part 2: Machine readable visa
- Part 3: Machine readable official travel documents

10.7.2 ISO/IEC 7812 Series, Identification Cards – Identification of Issuers

- ISO/IEC 7812-1 specifies a numbering system for the identification of issuers of cards that require an International Identification Number (IIN) to operate within an interchange environment.
- ISO/IEC 7812-2 specifies the application and registration procedures for Issuer Identification Numbers (IINs) issued in accordance with ISO/IEC 7812-1.

10.7.3 ISO/IEC 7813, Identification Cards – Financial Transaction Cards

This document specifies the data structure and data content of magnetic track data used to initiate financial transactions. It takes into consideration both human and physical aspects and states minimum requirements of conformity. It references layout, recording techniques, numbering systems, registration procedures, but not security requirements.

10.7.4 ISO/IEC 7816 Series, Identification Cards – Integrated Circuit(s) Cards with Contacts

- Part 5: Registration of application providers

10.7.5 ISO/IEC 8583 – Financial Transaction Card Originated Messages – Interchange Message Specifications

ISO/IEC 8583 is a multi-part standard that specifies interchange messages for financial transaction card originated messages.

- Part 1 specifies a common interface by which financial transaction card originated messages may be interchanged between acquirers and card issuers. It specifies message structure, format and content, data elements and values for data elements. The method by which settlement takes place is not within the scope of this part of ISO 8583.
- Part 2 specifies the application and registration procedures for Institution Identification Codes.
- Part 3 establishes the role of the maintenance agency (MA) and specifies the procedures for adding messages and data elements to ISO 8583-1 and to codes listed in Annex A of ISO 8583-1.

10.7.6 ISO/IEC 9992 – Financial Transaction Cards – Messages between the Integrated Circuit Card and the Card Accepting Device

- Part 1: Concepts and structures
- Part 2: Functions, messages (commands and responses), data elements and structures

10.7.7 ISO/IEC 18013 – Personal Identification – ISO-Compliant Driving License

- Part 1: Physical Characteristics and Basic Data Set. Part 1 describes the basic terms for this Standard including physical characteristics, basic data element set, visual layout, and physical security features.
- Part 2: Machine-Readable Technologies. Part 2 describes the technologies that may be used for this Standard, including the logical data structure and data mapping for each technology.
- Part 3: Access Control, Authentication and Integrity Validation. Part 3 describes the electronic security features that may be incorporated under this Standard, including mechanisms for controlling access to data, verifying the origin of an IDL, and confirming data integrity.

10.7.8 ISO/IEC 21549 – Health Informatics – Patient Health Card Data

- Part 1: General structure
- Part 2: Common objects
- Part 3: Limited clinical data
- Part 4: Extended clinical data
- Part 5: Identification data
- Part 6: Administrative data
- Part 7: Medication data
- Part 8: Links

10.7.9 ISO/IEC 24014-1 – Public Transport – Interoperable Fare Management System – Architecture

ISO/IEC 24014-1 identifies a system architecture and delineates public transport fare collection use cases and some high-level business rules with the goal of providing a sort of reference architecture that allows various national transit standards to fit within it without prescribing a specification for those national standards to meet.

10.7.10 Doc 9303, ICAO Machine Readable Travel Documents

The International Civil Aviation Organization (ICAO) is responsible for issuing guidance on the standardization and specifications for Machine Readable Travel Documents (MRTD) – i.e., passports, visas, and travel documents. ICAO published the specification for electronic passports that uses a contactless smart chip in the passport to securely store information on the passport holder's data page

- Part 1 - Machine Readable Passport - Volume 1 Passports with Machine Readable Data Stored in Optical Character Recognition Format
- Part 1 - Machine Readable Passport - Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capabilities
- Part 2 - Machine Readable Visas
- Part 3 - Machine Readable Official Travel Documents - Volume 1 MRtds with Machine Readable Data Stored in Optical Character Recognition Format
- Part 3 - Machine Readable Official Travel Documents - Volume 2 Specifications for Electronically Enabled MRTDs with Biometric Identification Capability

10.7.11 European Telecommunications Standards Institute (ETSI)

The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for information and communications technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies. ETSI standards areas that are relevant to smart cards are:

- **GSM**. ETSI TS 100 977: "Digital cellular telecommunications system (Phase 2+) (GSM)." The mobile phone industry has several telecommunication standards, but the predominant one globally is GSM. The GSM standard uses smart cards called Subscriber Identity Modules (SIMs) that are configured with information essential to authenticating a GSM-compliant mobile phone, thus allowing a phone to receive service whenever the phone is within coverage of a suitable network. According to the GSMA, GSM is used in 218 countries and territories serving more than three billion people. (See GSM statistics at http://www.gsmworld.com.) This standard is managed by the European Telecommunications Standards Institute (ETSI). ETSI TS 100 977: "Digital cellular telecommunications system (Phase 2+) (GSM)" is the specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface.

- **NFC**. ETSI TS 102 10 V1.1.1 (2003-03)) "Near Field Communication (NFC) IP-1; Interface and Protocol (NFCIP-1)"
- ETSI TS 102 221 V9.2.0 (2010-10), “Smart Cards; UICC-Terminal interface; physical and logical characteristics”
- ETSI TS 102 484 V10.0.0 (2011-01), “Smart Cards; Secure channel between a UICC and an end-point terminal”
- ETSI TS 102 600 V10.0.0 (2010-10), “UICC-Terminal interface; Characteristics of the USB interface”
- ETSI TS 102 613 V9.2.0 (2011-03), “UICC – Contactless Front-end (CLF) Inteface; Part 1: physical and data link layer characteristics”
- ETSI TS 102 671 V9.1.0 (2011-09), “Smart Cards; Machine to Machine UICC; Physical and logical characteristics”

Additional information about ETSI can be found at http://www.etsi.org.

10.7.12 Comité Européen de Normalisation Technical Committee TC 224

The Comité de Européen Normalisation (CEN) technical committee TC 224 on "personal identification, electronic signature and cards and their related systems operations" defines the necessary standards to be used to perform the desired level of commercial interoperability in Europe for bank, transport, telecommunication and e-Government applications.

Additional information can be found at: http://www.cen.eu.

CEN/TS 15480 Identification card systems - European Citizen Card is the standard for the European Citizen Card, a smart card issued under the authority of a government institution which carries credentials in order to provide all or part of the following services: verify the identity; act as an Inter-European Union travel document; facilitate logical access to e-Government or local administration services. The standard includes four parts:

- Part 1: Physical, electrical properties and transport protocols (physical card interface);
- Part 2: Logical data structures and card services (logical card interface);
- Part 3 (under development): Interoperability using and application interface (middleware);
- Part 4 (under development): Recommendations for issuance, operation and use (card profiles)

Parts 1 and 2 were published in 2007, parts 3 and 4 are currently under development in CEN TC 224 WG 15.

Additional information on the European Citizen Card can be found in CSCIP Module 5.

10.7.13 ECMA International

ECMA International is an industry association founded in 1961 and dedicated to the standardization of Information and Communication Technology (ICT) and Consumer Electronics (CE). ECMA is active in defining standards for Near Field Communication (NFC), including:

- ECMA-340: NFCIP-1 Interface and Protocol (now ISO/IEC 18092)
- ECMA-352: NFCIP-2 Interface and Protocol (now ISO/IEC 21481)
- ECMA-356: NFCIP-1 RF Interface Test Methods (now ISO/IEC 22536)
- ECMA-362: NFCIP-1 Protocol Test Methods (now ISO/IEC 23917)

10.7.14 NFC Forum

Near Field Communication technology evolved from a combination of contactless identification and interconnection technologies. In June 2006, the NFC Forum took a significant step to enable manufacturers and applications developers to create powerful new consumer-driven products when it unveiled NFC technology architecture and announced the first Forum-approved specifications at a Web news conference.

The NFC Forum supports four initial tag formats based on ISO 14443 Type A and 14443 Type B standards (ISO 14443 is a four-part international standard for contactless smart cards operating at 13.56 MHz in close proximity with a reader antenna), and on the NFC standard ISO 18092. NFC Forum-compliant devices must support these formats.

The NFC Forum has released 16 specifications, as of September 2010:

- *NFC Logical Link Control Protocol (LLCP) Technical Specification*
- *Digital Protocol Technical Specification*
- *NFC Activity Technical Specification*
- *NFC Data Exchange Format (NDEF)*
- *NFC Simple NDEF Exchange Protocol*
- *NFC Tag Types 1-4*
- *NFC Record Type Definition (RTD)*
- *NFC Text Record Type Description*
- *NFC Uniform Resource Identifier (URI) Service Record Type Description*
- *NFC Smart Poster Record Type Description*
- *NFC Generic Control RTD Technical Specification*
- *Signature RTD Technical Specification*
- *NFC Forum Connection Handover 1.2 Technical Specification*

Additional information can be found at http://www.nfc-forum.org

10.7.15 EMV: Integrated Circuit Card Specifications for Payment Systems[51]

To expedite the issuance of globally interoperable financial smart cards, Europay, MasterCard, and Visa (EMV) published the first version of standard card and transaction terminal specifications in 1995. The specifications are built on the ISO/IEC 7816 standard and serve as an expansion to accommodate debit and credit transactions. Version 4.3 was published in November 2011.

- Book 1, Application-Independent Integrated Circuit Card (ICC) to Terminal Interface Requirements, describes the minimum functionality required for integrated circuit cards and terminals to ensure correct operation and interoperability independent of the application to be used.
- Book 2, Security and Key Management, describes the minimum security functionality required for integrated circuit cards and terminals to ensure correct operation and interoperability. Additional requirements and recommendations are provided on online communication between ICC and issuer and the management of cryptographic keys at terminal, issuer and payment system level.
- Book 3, Application Specification, defines the terminal and integrated circuit card procedures necessary to effect a payment system transaction in an international interchange environment.
- Book 4, Cardholder, Attendant, and Acquirer Interface Requirements, defines the mandatory, recommended, and optional terminal requirements necessary to support the acceptance of integrated circuit cards in accordance with Books 1, 2 and 3.

[51] EMV specifications can be found at http://www.emvco.com.

10.7.16 Common Electronic Purse Specification

The Common Electronic Purse Specification (CEPS) was developed by Visa in the early 2000s, but the specification had little adoption around the world as a universal e-purse. The CEPS specifications can be found at http://www.irisa.fr/vertecs/Equipe/Rusu/FME02/functionalrequirements6-3.pdf.

10.7.17 Comité Européen de Normalisation

The Comité de Européen Normalisation (CEN) produced a European standard, EN 1546, for inter-sector electronic purse systems.

10.7.18 Contactless Fare Media Standard

The American Public Transportation Association (APTA) has published the Contactless Fare Media System (CFMS) Standard that provides a manual of standards and recommended practices for universal transit farecards. Additional information is available at http://www.aptastandards.com.

10.7.19 Integrated Transport Smartcard Organization

The Integrated Transport Smartcard Organization (ITSO) was formed in 1988 as a membership organization with the mission to create a common specification at both the card and application level, to enable the use of interoperable smart cards in transport. The specification – current version 2.1.3 dated April 2008 – includes ten parts covering customer media data and architecture, terminals, host operator or processing system, customer media data record, message data, security and communications. The specification is available at http://www.itso.org.uk.

10.7.20 Verband Deutscher Verkehrsunternehmen

The Verband Deutscher Verkehrsunternehmen (Association of German Transport Undertakings – VDV) in Germany has defined the Electronic Fare Management (EFM) standard. Additional information is available at http://www.vdv.de/en/index.html.

10.7.21 Open Standard for Public Transport

The Open Standard for Public Transit (OSPT™) Alliance is an international association chartered to define a new open standard for secure transit fare collection solutions, CIPURSE™. OSPT provides industry education, creates work group opportunities and catalyzes the development and adoption of innovative fare collection technologies, applications and services. Additional information is available at: http://www.osptalliance.org/.

10.7.22 ANSI INCITS 410-2006 – Identification Cards – Limited Use (LU), Proximity Integrated Circuit Card (PICC)

ANSI INCITS 410-2006 is a physical specification with similar electronic characteristics of a Proximity Integrated Circuit Cards (PICCs) such as those specified within ISO/IEC 14443 Part-2 and 3 but in thinner ID-1 (card body) formats as defined within the selected card thickness of ISO/IEC 15457 for thin flexible cards. Construction attributes, pertaining to the materials, functionality and environmental requirements and targeted use are also specified. This type of PICC is to be classified as a Limited Use - Proximity Integrated Circuit Card (LU-PICC). Limited use cards are used in the transit industry.

10.8 Other Standards Related to Smart Cards or their Software Clients

10.8.1 ISO/IEC 24727 Identification Cards – Integrated Circuit Card Programming Interfaces

ISO/IEC 24727 is a multi-part standard aimed at achieving interoperability among various smart card systems. The goal is to provide the necessary interfaces and services to enable interoperability among divergent systems, with a particular focus on identification, authentication, and signature services, and removing the dependence on vendor specific implementations.[52]

ISO/IEC 24727 is a set of programming interfaces for interactions between integrated circuit cards and external applications, including generic services for multi-sector use. The organization and the operation of the ICC conform to ISO/IEC 7816-4.

- Part 1: Architecture
- Part 2: Generic Card Interface
- Part 3: Application Interface
- Part 4: API Administration
- Part 5: Test Procedures
- Part 6: Registration authority procedures for the authentication protocols for interoperability

10.9 Primary U.S. Standards and Specifications Related to Smart Cards – Federal Information Processing Standards (FIPS)

FIPS standards are developed by NIST Computer Security Division. FIPS standards are designed to protect federal computer and telecommunications systems. The following FIPS standards apply to smart card technology and pertain to digital signature standards, advanced encryption standards, security requirements for cryptographic modules and personal identity verification cards.

10.9.1 FIPS Standards for Digital Signatures

- **FIPS 186-2 Digital Security Standard** specifies a set of algorithms used to generate and verify digital signatures. This specification relates to three algorithms specifically, the Digital Signature Algorithm (DSA), the RSA digital signature algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA).
- **ANSI X9.31-1998** contains specifications for the RSA signature algorithm. The standard specifically covers both the manual and automated management of keying material using both asymmetric and symmetric key cryptography for the wholesale financial services industry.
- **ANSI X9.62-1998** contains specifications for the ECDSA signature algorithm.

10.9.2 FIPS Standards for Digital Encryption

- **FIPS 197 Advanced Encryption Standard** (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information.

10.9.3 FIPS 140 Security Requirements for Cryptographic Modules Standard

The security requirements contained in FIPS 140 pertain to areas related to the secure design and implementation of a cryptographic module, specifically: cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security;

[52] Source: NIST, http://www.itl.nist.gov/ITLPrograms/IDMS/external/standards_metrics.html

operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks. The current version is FIPS 140-2. NIST has a current draft of FIPS 140-3 available for public comments.

10.9.4 FIPS 201 Personal Identity Verification of Federal Employees and Contractors

Homeland Security Presidential Directive 12 (HSPD-12) was issued by President George W. Bush on August 27, 2004 and mandated the need "to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification." HSPD-12 specifically calls for the use of a common identification credential for "gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems."

As a result of this directive, the National Institute of Standards and Technology (NIST) published *FIPS 201 Personal Identity Verification of Federal Employees and Contractors*. FIPS 201 defines the identity vetting, enrollment, and issuance requirements for a common identity credential and the technical specifications for a government employee and contractor ID card—the PIV card. The FIPS 201 PIV card is a smart card with both contact and contactless interfaces that is now being issued to all Federal employees and contractors. The PIV card is being used for both physical and logical access and can be used for other applications as determined by individual agencies.

On August 2, 2013 FIPS 201-2 replaced the FIPS 201-1 specification. FIPS 201-2 is available at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

10.9.4.1 NIST Special Publications and Interagency Reports

NIST has issued a number of special publications with additional specifications for PIV card implementations, available at http://csrc.nist.gov/groups/SNS/piv/index.html. FIPS 201 also references a number of other NIST special publications and interagency reports as part of the specification.

- NIST Special Publication 800-53 (SP 800-53 Rev 4), "Recommended Security Controls for Federal Information Systems," April 2013
- NIST Special Publication 800-57 (SP 800-57), "Recommendation for Key Management, Part 1 Draft," May 5, 2014
- NIST Special Publication 800-57 (SP 800-57), "Recommendation for Key Management, Part 3," December 2009
- NIST Special Publication 800-63-2 (SP 800-63-2), "Electronic Authentication Guideline," August 2013
- NIST Special Publication 800-73-3 (SP 800-73-3): "Interfaces for Personal Identity Verification" (4 parts) – 1- End-Point PIV Card Application Namespace, Data Model and Representation; 2- End-Point PIV Card Application Interface; 3- End-Point PIV Client Application Programming Interface; 4- The PIV Transitional Data Model and Interfaces
- NIST Special Publication 800-76-2, "Biometric Data Specification for Personal Identity Verification," (SP 800-76-2), July 2013
- NIST Special Publication 800-78-2 (SP 800-78-2), "Cryptographic Algorithms and Key Sizes for Personal Identity Verification," (SP 800-78), February 2010; SP 800-78-4 Draft, May 19, 2014
- NIST Special Publication 800-79-1 (SP800-79-1): "Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)," June 2008; SP 800-79-2 Draft, June 2, 2014
- NIST Special Publication 800-85 A-1 (SP 800-85 A-1), "PIV Card Application and Middleware Test Guidelines," March 2009

- NIST Special Publication 800-85 A-1 (SP 800-85 A-1), "PIV Card Application and Middleware Test Guidelines, (SP 800-73-3 Compliance)," July 2010
- NIST Special Publication 800-85 A-1 (SP 800-85 B), "PIV Data Model Test Guidelines," July 2006
- NIST Special Publication 800-87 (SP 800-87), "Codes for Identification of Federal and Federally-Assisted Organizations," April 2008
- NIST Special Publication 800-96 (SP800-96): PIV Card / Reader Interoperability Guidelines, Sept. 2006
- NIST Special Publication 800-104 (SP 800-104): "A Scheme for PIV Visual Card Topography," June 2007
- NIST Special Publication 800-116 (SP 800-116), "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)," November 2008
- NIST Interagency Report 6887 (NISTIR 6887), "Government Smart Card Interoperability Specification," Version 2.1, July 2003
- NIST Interagency Report 7123 (NISTIR 7123), "Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report, NIST, June 2004,
- NIST Interagency Report 7452, (NISTIR 7452), "Secure Biometric Match-on-Card Feasibility Report," November 2007
- NIST Interagency Report 7477 (NISTIR 7477), "Performance of Fingerprint Match-on-Card Algorithms Phase II/III Report," updated January 30, 2013

10.9.4.2 ANSI INCITS Standards Referenced by FIPS 201

- ANSI INCITS 322 Information Technology, Card Durability Test Methods, ANSI, 2002
- ANSI INCITS 378-2004, "Information technology - Finger Minutiae Format for Data Interchange," ANSI, 2004

10.9.4.3 ISO/IEC Standards Referenced by FIPS 201

- ISO/IEC 7810, Identification Cards – Physical Characteristics
- ISO/IEC 7816, Identification Cards – Integrated Circuit Cards
- ISO/IEC 10373, Identification Cards – Test Methods
- ISO/IEC 14443, Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards

10.9.4.4 Other Standards Referenced by FIPS 201

- Personal Computer/Smart Card (PC/SC) Specification, http://www.pcscworkgroup.com/
- "PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version 1.1, published by the authority of the Secretary General, International Civil Aviation Organization, October 1, 2004
- RFC 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)," Internet Engineering Task Force (IETF)
- RFC 4122, "A Universally Unique Identifier (UUID) URN Namespace," Internet Engineering Task Force, July 2005

10.10 Biometrics Standards

Many new secure ID system implementations are using both biometrics and smart cards to improve the security and privacy of the ID system. The following standards apply to biometric applications in general, and may apply to portions of a smart card-based system.

- **ANSI-INCITS 358-2002, BioAPI Specification - (ISO/IEC 19784-1).** BioAPI is intended to provide a high-level generic biometric authentication model–one suited for any form of biometric technology. It covers the basic functions of enrollment, verification, and identification, and includes a database interface to allow a biometric service provider (BSP) to manage the technology device and identification population for optimum performance. It also provides primitives that allow the application to separately manage the capture of samples on a client workstation, and the enrollment, verification, and identification functions on a server. The BioAPI framework has been ported to Win32, Linux, UNIX, and WinCE. Note that BioAPI is not optimum for a microcontroller environment such as might be embedded within a door access control reader unit or within a smart card processor. BioAPI is more suitable when there is a general-purpose computer available.
- **ANSI-INCITS 398, Common Biometric Exchange Formats Framework (CBEFF) - (ISO/IEC 19785-1).** The Common Biometric Exchange Formats Framework (CBEFF) describes a set of data elements necessary to support biometric technologies and exchange data in a common way. These data can be placed in a single file used to exchange biometric information between different system components or between systems. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange. This specification is a revised (and augmented) version of the original CBEFF, the Common Biometric Exchange File Format, originally published as NISTIR 6529.
- **ANSI-INCITS Biometric Data Format Interchange Standards.** ANSI-INCITS has created a series of standards specifying the interchange format for the exchange of biometric data. These standards specify a data record interchange format for storing, recording, and transmitting the information from a biometric sample within a CBEFF data structure. The ANSI-INCITS published data interchange standards are shown below. The ISO equivalent standards for each are in process but not yet finalized.
- **ANSI-INCITS 377-2004 - Finger Pattern Based Interchange Format**
- **ANSI-INCITS 378-2004 - Finger Minutiae Format for Data Interchange**
- **ANSI-INCITS 379-2004 - Iris Interchange Format**
- **ANSI-INCITS 381-2004 - Finger Image Based Interchange Format**
- **ANSI-INCITS 385-2004 - Face Recognition Format for Data Interchange**
- **ANSI-INCITS 395-2005 - Signature/Sign Image Based Interchange Format**
- **ANSI-INCITS 396-2004 - Hand Geometry Interchange Format**
- **ISO/IEC 19794** series on biometric data interchange formats. Part 1 is the framework. Part 2 defines the finger minutiae data. Part 3 defines the finger pattern spectral data. Part 4 defines the finger image data. Part 5 defines the face image data. Part 6 defines the iris image data, and still in development. Part 7 defines the signature/sign time series data. Part 8 defines the finger pattern skeletal data. Part 9 defines the vascular image data. Part 10 defines hand geometry silhouette data.

10.11 Other Standards and Specifications that Relate to Smart Card-Based Applications

10.11.1 G-8 Health Standards

The G-8 countries have come together to develop a standard format for populating data on a health card. This standard attempts to create interoperability across health cards from the G-8 countries. It addresses file formats, data placement on the card, and use of digital certificates in health care

10.11.2 ISO/IEC Standards for Healthcare Informatics

- ISO/IEC 13606, which specifies the communication of part or all of the electronic health record (EHR) of a single identified subject of care between EHR systems, or between EHR systems and a centralized EHR data repository.
- ISO/IEC 18307, which specifies interoperability and compatibility in messaging and communication standards for health informatics.
- ISO/IEC 21549, which specifies patient health card data.

10.11.3 The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191)

This law states that the Secretary of Health and Human Services (HHS) is to adopt national standards for implementing a secure electronic health transaction system. Examples of these transactions include: claims, enrollment, eligibility, payment, and coordination of benefits. The goal of HIPAA is to create a secure, cost-effective means for individuals to efficiently accomplish electronic health care transactions. HHS has designated the Centers for Medicare and Medicaid Services the responsible entity for enforcing HIPAA.

10.11.4 The Health Information Technology for Economic and Clinical Health (HITECH) Act

The American Recovery and Reinvestment Act of 2009 (ARRA) HITECH Act provides incentives for the U.S. healthcare industry to move to electronic health records and a national healthcare infrastructure. The HITECH Act widens the scope of privacy and security protections available under HIPAA, increases potential legal liability for non-compliance and provides for more enforcement.

10.11.5 American National Standards Institute

INCITS 284 Identification cards – Health Care Identification Cards

This American National Standards Institute specifies directly or by reference the requirements for cards used in healthcare transactions. It takes into consideration both human and machine aspects and states minimum requirements for conformity. It contains physical characteristics, layout, data access techniques, data storage techniques, numbering system, registration procedures, but not security requirements. Security measures are at the discretion of the card issuer.

10.11.6 USB Implementers Forum

The CCID Specification for Integrated Circuit(s) Cards Interface Devices was developed for USB smart card readers. It was designed to support easy integration of smart card readers with desktop operating systems, thereby removing the need to install additional reader driver software onto the user's

desktop. The specification was defined by the USB Implementer's Forum (USB-IF)[53] in conjunction with the smart card industry. CCID defines a command set and transport protocol over the USB so that a host system can communicate with a smart card reader. A specific USB class is now defined for smart card readers.

10.11.7 Initiative for Open Authentication (OATH)[54]

OATH is an industry-wide collaboration to develop an open reference architecture by leveraging existing open standards for the universal adoption of strong authentication. OATH has developed reference architecture specifications and standards for OTP algorithms that are now being managed by the Internet Engineering Task Force (IETF). Key standards and draft specifications are:

- *HOTP: An HMAC-Based OTP Algorithm* (IETF RFC 4226) standard
- *OCRA: OATH Challenge/Response Algorithms Specification* - draft IETF specification
- *TOTP: Time-based One-Time Password Algorithm* - draft IETF specification
- *OATH Token Identifier Specification*

10.11.8 SD Association[55]

The SD Association is a global ecosystem of companies setting industry-leading memory card standards that simplify the use and extend the life of consumer electronics, including mobile phones, for millions of people every day.

- The Advanced Security Secure Digital (ASSD) standard was defined by the SD Association to enable memory card devices to support ISO/IEC 7816 functions.
- The smartSD standard was defined by the SD Association enable memory card devices to support ISO/IEC 14443 functions.

[53] Additional information about CCID can be found at the USB Implementer's Forum web site, http://www.usb.org.
[54] Source: http://www.openauthentication.org/
[55] https://www.sdcard.org/home/

11 References

American Public Transportation Association web site (APTA), http://www.apta.com/

American National Standards Institute (ANSI), http://www.ansi.org

BasicCard web site, http://www.basiccard.com

Common Criteria web site, http://www.commoncriteriaportal.org/

Contactless Technology for Secure Physical Access: Technology and Standards Choices, Smart Card Alliance white paper, October 2002, http://www.smartcardalliance.org

ECMA International web site, http://www.ecma-international.org/

EMVCO web site, http://www.emvco.com

GlobalPlatform web site, http://www.globalplatform.org/

Government Smart Card Handbook, General Services Administration, February 2004

GSMA web site, http://www.gsmworld.com

HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements, Smart Card Alliance white paper, September 2003, http://www.smartcardalliance.org

IATA web site, http://www.iata.org/

ICAO web site, http://www.icao.int/mrtd

ISO/IEC web site, http://www.iso.org

Java Card specifications, available at http://java.sun.com/javacard/specs.html

MULTOS specifications, available at http://www.multos.com

NIST Computer Security Division web site, http://csrc.nist.gov

NIST FIPS publications web site, http://csrc.nist.gov/publications/PubsFIPS.html

NIST PIV web site, http://csrc.nist.gov/groups/SNS/piv/index.html

PC/SC Work Group web site, http://www.pcscworkgroup.com/

Secure Identification Systems: Building a Chain of Trust, Smart Card Alliance white paper, March 2004, http://www.smartcardalliance.org

Smart Cards, by Jose Luis Zoreda and Jose Manuel Oton (Boston: Artech House, Inc., 1994)

Smart Cards: The Global Information Passport, by Jack M. Kaplan (New York: International Thomson Computer Press, 1996)

Smart Cards & Payments: Technology, Standards and Transactions, by Gilles Lisimaque, Smart Card Alliance webinar presentation, November 18, 2008

USB Implementer's Forum web site, http://www.usb.org

Using Smart Cards for Secure Physical Access, Smart Card Alliance white paper, July 2003, http://www.smartcardalliance.org

What Makes a Smart Card Secure?, Smart Card Alliance white paper, October 2008, http://www.smartcardalliance.org

12 Acknowledgements

This document was developed by the Smart Card Alliance for the Certified Smart Card Industry Professional (CSCIP) program. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance thanks the following organizations for their review of this CSCIP module:

- **NXP Semiconductors**
- **Identification Technology Partners**
- **Oberthur Technologies**
- **Deloitte**
- **NFC Forum**

The Smart Card Alliance thanks the organizations for contributing content to this CSCIP module:

- **NXP Semiconductors**, Section 5.2, *Contactless Interface*.
- **CPI Card Group**, Section 8, *Smart Card Manufacturing*
- **Identification Technology Partners**, Section 7, *Smart Card Operating Systems*, and Section 10, *Relevant Standards and Specifications*,

The Smart Card Alliance thanks **ActivIdentity, CPI Card Group, Gemalto, Giesecke & Devrient, HID Global, Hirsch Electronics, Identification Technology Partners, Oberthur Technologies, SCM Microsystems, VeriFone, Visa, Inc.,** and **ViVOtech** for providing images and graphics for this module.

The Smart Card Alliance wishes to acknowledge the **GSA** for the content from the *Government Smart Card Handbook* used in several sections in the module.

The Smart Card Alliance thanks the many current and past members of the Smart Card Alliance Councils and Task Forces who contributed to the development of the white papers and reference material that was used to create this module, including:

ActivIdentity	IfD Consulting	Security Sciences International
Alegra Technologies	Infineon Technologies	Sun Microsystems
AOS Hagenuk	INSIDE Contactless	Taiwan Bureau of National Health Insurance
Assa Abloy ITG	JCB	TecSec
Atmel Corporation	LaserCard Systems	Texas Instruments
Bank of America	Litronic/SAFLink	Thales
CardLogix	Lockheed Martin	Turtle Mountain Systems
Datakey	MartSoft Corporation	Unisys
Datatrac Information Services, Inc.	MasterCard Worldwide	University of Pittsburgh Medical Center
Deloitte	Mississippi Baptist Health Systems	U.S. Department of Defense
Discover Financial Services	NBS Technologies	U.S. General Services Administration
EDS	Northrop Grumman	Venyon
*e*ID Security	NTRU	VeriFone
First Data Corporation	NXP Semiconductors	VeriSign
Gemalto	OTI America	Visa Inc.
Giesecke & Devrient	Privamed, Inc.	ViVOtech
Honeywell Access Systems	Raak Technologies	Wave Systems
IBM	SCM Microsystems	XTec, Incorporated
Identix	Smart Commerce Inc.	

Special thanks go to all of the individuals who worked on the development of the white papers and reference material used for this CSCIP module, including:

David Asay	Henk Dannenberg	Diana Knox	Cathy Medich	Bruce Ross
David Berman	Michael Davis	Kevin Kozlowski	Yahya Mehdizadeh	Denis Scheller
Troy Bernard	Sunil Dewan	Julie Krueger	Bob Merkert	Rajesh Sharma
Ralph Billeri	Gwynneth Dido	Colleen Kulhanek	John Moore	Ron Stephenson
Iana Bohmer	Ian Duthie	Michael Laezza	Fred Namdar	Nick Stoner
Dovell Bonnett	Patrice Erickson	Philip Lee	Tim Ostrem	Jan van der Sluis
Kirk Brafford	Shrinath Eswarahally	Paul Legacki	Neville Pattinson	Michael Vermillion
Linda Brown	Neal Goman	Albert Leung	Joseph Pearson	Jay Wack

John Butterworth	John Harrison	Vince Ley	Dwayne Pfeiffer	Charles Walton
Jim Canfield	Nick Hislop	Gilles Lisimaque	Joe Pilozzi	Bob Wilberger
Jean-Paul Caruana	Wendy Humphrey	Louis Liu	Ron Pinkus	Shawn Willden
Yuh-Ning Chen	Mansour Karimzadeh	Don Malloy	Tate Preston	Erik Wilson
Patrick Comiskey	Jeff Katz	Mark McGovern	Neil Ringwood	Jeremy Wyant
Jay Cornish	Mohammad Khan	John McKeon	Herve Roche	

About LEAP and the CSCIP Program

The Smart Card Alliance Leadership, Education and Advancement Program (LEAP) was formed to offer a new individual members-only organization for smart card professional; advance education and professional development for individuals working in the smart card industry; and manage and confer, based on a standardized body-of-knowledge examination, the Certified Smart Card Industry Professional (CSCIP) designation.

LEAP members who wish to achieve certification as experts in smart card technology may do so at any time. Certification requires that LEAP members meet specific educational and professional criteria prior to acceptance into the certification program.

A series of educational modules forming the CSCIP certification body of knowledge has been developed by leading smart card industry professionals and is updated regularly. These educational modules prepare applicants for the multi-part CSCIP exam administered by the Smart Card Alliance. The exam requires demonstrated proficiency in a broad body of industry knowledge, as opposed to expertise in specialized smart card disciplines. Applicants must receive a passing grade on all parts of the exam to receive the CSCIP certification.

LEAP membership in good standing is required to sustain the certification, and documentation of a required level of continuing education activities must be submitted every three years for CSCIP re-certification.

Additional information on LEAP and the CSCIP accreditation program can be found at http://www.smartcardalliance.org.

Trademark Notice