Smart Cards

José Costa

Software for Embedded Systems

Departamento de Engenharia Informática (DEI)
Instituto Superior Técnico

2015-11-09

Outline

- Application Domains:
- Smart Cards

Smart Card

Motivations for Using Smart Cards

- How do I avoid having to handle changes and coins? - Payphones
- How do I identify a user in order to bill him? - Mobile communications
- How do I protect users, merchants and banks from fraudulent use in banking transactions? - Banking and Retail
- How do I get rid of all the cash I'm handling? - Electronic purse
- How do I safely and realibly store patient health information? - Health care
- How do I store personal information about a user in order to reliable identify him? - ID verification and access control

History of Smart Cards

		Business cards
1950	Diners Club	Plastic card
1960	Bank of America credit card	Magnetic card
	IATA card	
1970, 74-76	K. Arimura and R. Moreno patents	
1976, 79	Chip card and intelligent card (Bull)	Chip card
1981	LaserCard (Drexler)	Optical card
1982-84	Large field experience with electronic cards (Carte Bancaire)	
1986	First standard for electronic cards (ISO7816/1)	
1986	Telephone card (French Telecom)	

Market of Smart Cards

Smart cards with microprocessor

	2000	2002	2004	2006	2007	2008	2009	2010	2011	2012	(F) 2013	(F) 2014
Telecoms	370	430	1050	2040	2650	3200	3400	4200	4700	5100	5000	5200
Financial Services	120	175	280	410	510	650	750	880	1050	1200	1480	1730
Government/ Healthcare	30	32	45	90	105	140	160	190	240	310	360	410
Transport	3	15	15	20	30	30	40	65	100	160		
Pay TV	25	42	55	65	85	100	100	110	125	145	390	415
Others	3	7	24	30	65	65	70	75	80	100		
Total	551	701	1469	2655	3445	4185	4520	5520	6135	6970	7230	7755

in millions of units

Source: Eurosmart

Market of Smart Cards

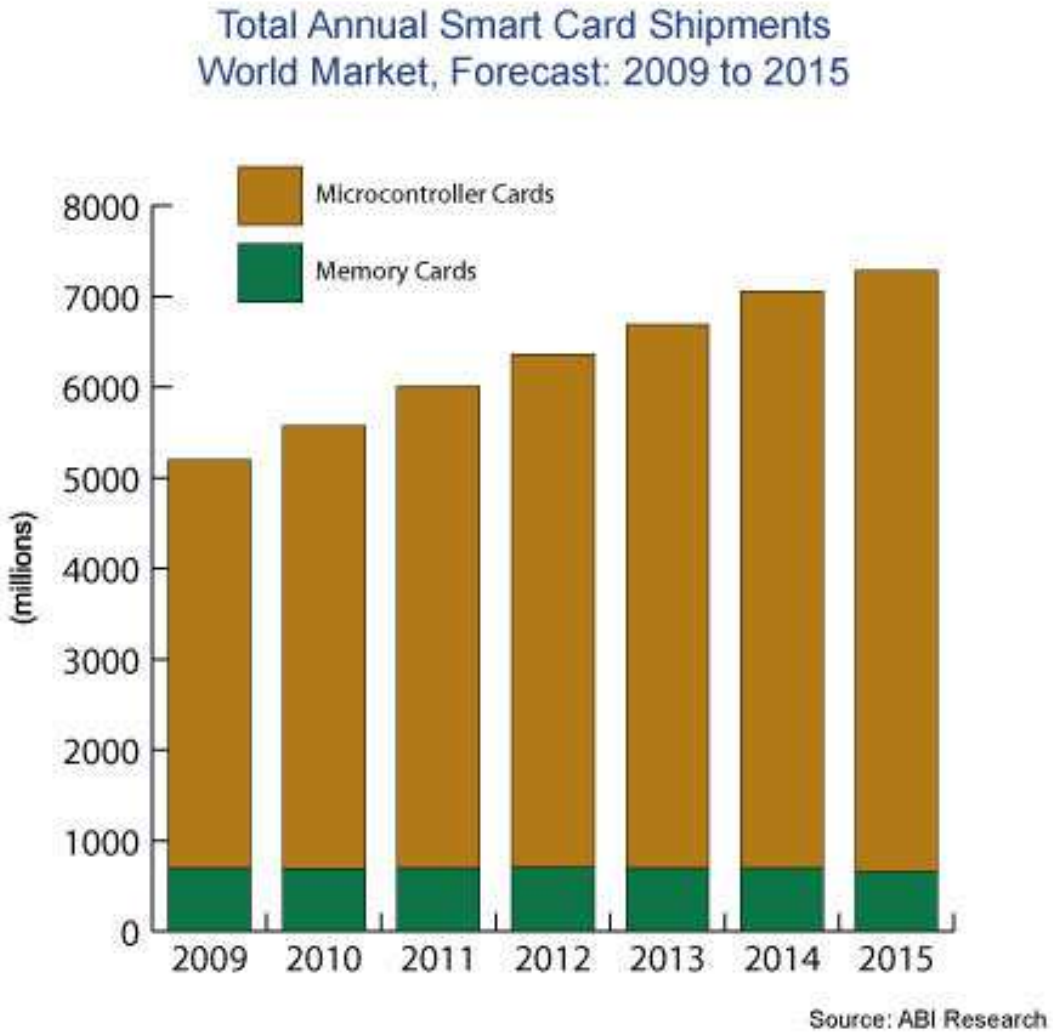
Contactless smart cards with microprocessor

	2007	2008	2009	2010	2011	2012	(F) 2013	(F) 2014
Financial Services	60	100	120	175	200	295	500	650
Government/50 Healthcare		60	75	100	130	170	200	240
Transport	30	30	40	65	100	135	160	180
Others	30	30	30	30	50	60	70	70
Total	170	220	265	370	480	660	930	1140

in millions of units

Source: Eurosmart

Market of Smart Cards



Smart Cards and Security

- Smart cards are especially well suited for applications in which security-sensitive or personal data is involved
- A smart card provides both the data and the means to process it, then information can be processed to and from a network in cyphered format
- Smart cards are mobile devices, enabling users to carry critical data in the card rather than entrusting information coming from network storage devices or backend server (where it could be sold or accessed by unknown persons)

Smart Card Types

Memory cards

- simply store data and can be viewed as small floppy disks with optional security
- depend on the security of a card reader for their processing

Microprocessor cards

- can add, delete, and manipulate information in their internal memory
- it's like a mini-computer with input and output port, operating system, and hard disk with built-in security features

Memory Cards

- Cannot manage files and have no processing power for data management
- Communicate to readers through synchronous protocols
- You read and write to a fixed address on the card

Three primary types

- Straight
- Protected/Segmented
- Stored Value

Straight Memory Cards

- Just store data and have no data processing capabilities
- Traditionally the lowest cost per bit for user memory
  - This has now changed with the larger quantities of processors being built for the GSM market
- These cards cannot identify themselves to the reader
  - your host system has to know what type of card is being inserted into a reader
- Easily duplicated

Protected / Segmented Memory Cards

- Have built-in logic to control the access to the memory of the card
  - can be set to write-protect some or the entire memory array
- Can be configured to restrict access to both reading and writing
  - usually done through a password or system key
- Segmented memory cards can be divided into logical sections for planned multi-functionality
- Are not easily duplicated but can possibly be impersonated by hackers

Stored Value Memory Cards

- Designed for the specific purpose of storing value or tokens
- Are either disposable or rechargeable
- Incorporate permanent security measures at the point of manufacture
  - e.g., password keys and logic that are hard-coded into the chip by the manufacturer
- The memory arrays on these devices are set-up as decrements or counters
- There is little or no memory left for any other function

Microprocessor Cards

- On-card dynamic data processing capabilities
- Allocate card memory into independent sections or files assigned to a specific function or application
- Microprocessor or microcontroller chip manages this memory allocation and file access
- Microprocessor manages data in organized file structures, via a card operating system (COS)
- Can have different and multiple functions and/or different applications on the card

Smart Card Interfaces

Two different smart cards interfaces are available

- Contact smart cards
- Contactless smart cards

New cards are now available offering a dual interface enabling both contact and contactless data exchanges with a high level of security.

Smart Card Interfaces - Contact

- Mechanical connection
- Must be inserted into a smart-card reader
- The reader makes contact with the card module's electrical connectors
- Connectors used to transfer data to and from the chip
- Transaction time $\approx$ seconds

Smart Card Interfaces - Contactless

- Use electromagnetic coupling
- Have embedded electronic microchip and antenna
- These allow data exchange with a reader without physical contact
- Are an ideal solution when transactions must be processed quickly
- Transaction time $\approx$ mseconds

Other Cards

- Multi-mode Communication Cards
  - multiple methods of communications, including ISO7816, ISO14443 and UHF gen 2
- Hybrid Cards
  - multiple chips in the same card - typically attached to each interface separately
- Dual Interface Cards
  - one chip controlling the communication interfaces
- Multi-component Cards
  - used in specific market solution - e.g. cards where the fingerprint sensor is built on the card

Integrated Circuit

- Device is designed to securely store data withstanding outside electrical tampering or hacking
- Aditional security features include a long list of mechanisms
  - e.g., no test points, special protection metal masks and irregular layouts of the silicon gate structures

Trusted silicon semiconductor vendors (2010)

Atmel EM systems Felicia Infineon Microchip NXP
Renasas Samsung Sharp Sony ST Microelectronics

Card Operating Systems

The two primary types of smart card operating systems

- fixed file structure
- dynamic application system

Selection of COS depends

- application
- encryption capabilities (Symetric or Asymetric key)

Fixed File Structure Card Operating System

- Treats the card as a secure computing and storage device
- Files and permissions are set in advance by the issuer
- Are ideal and economical for a fixed type of card structure and functions that will not change in the near future

Are the most common microprocessor cards.

Dynamic Application Card Operating Syster

- JavaCard and MULTOS card
- Enables developers to build, test, and deploy different card applications securely
- Software updates can be made

Types of Memory

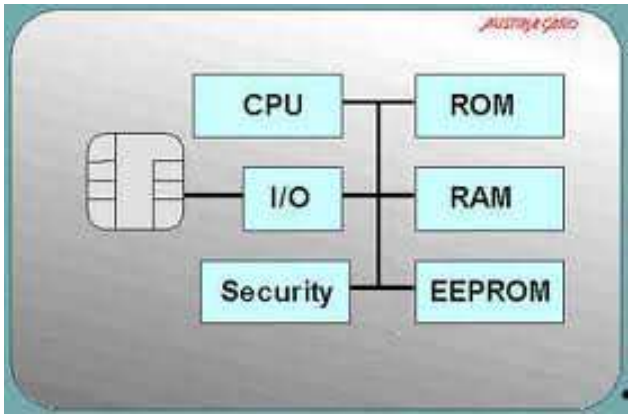
- Persistent non-mutable memory - ROM
- Persistent mutable memory - EEPROM
- Non-persistent mutable memory - RAM

File Structure

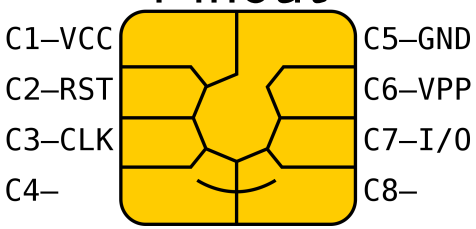
- MF (Master File): the root of the file structure
  - Equivalent to a root directory
- DF (Dedicated File): a file containing other data files
  - Equivalent to a directory
  - Each DF behaves like a separate card
- EF (Elementary File): a file containing data
  - Equivalent to a file

Contact Cards with Microprocessor

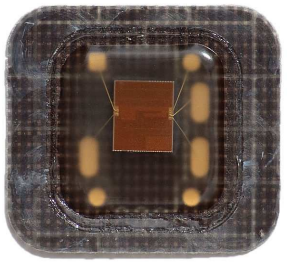
Architecture



Pinout

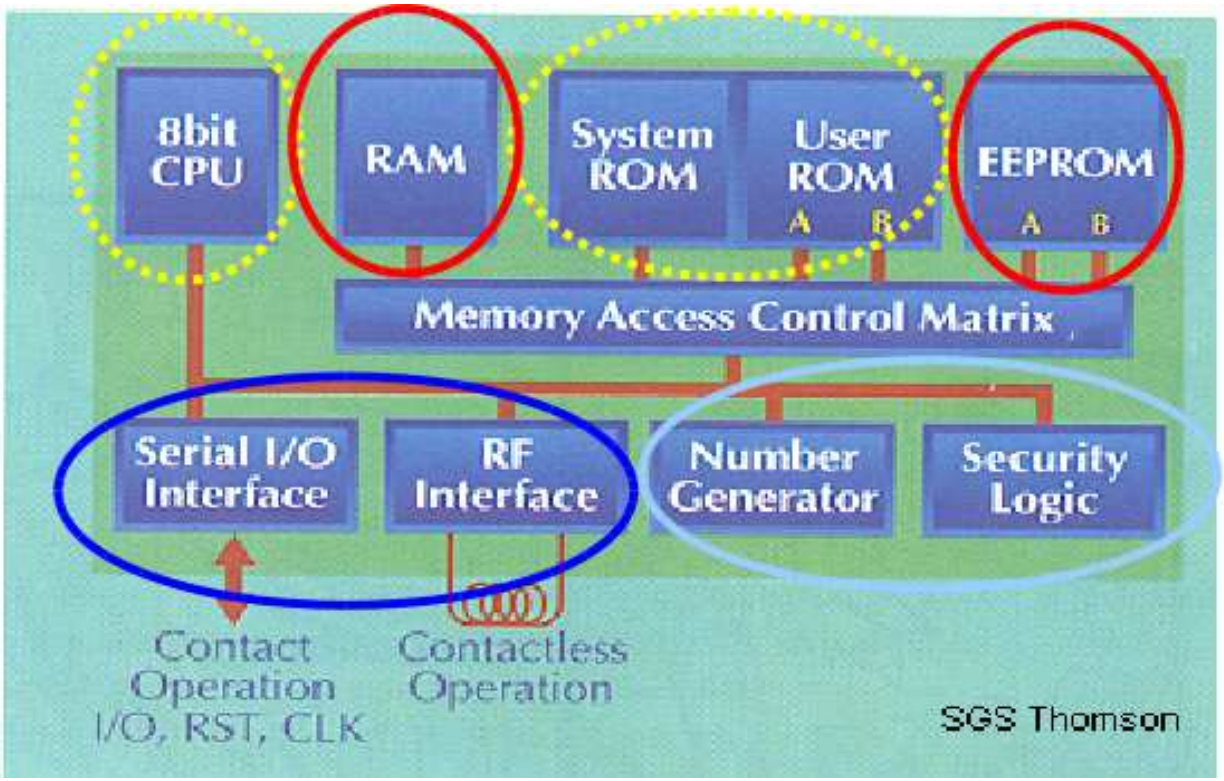


Chip



from wikipedia

Main Blocks of a Chip Card



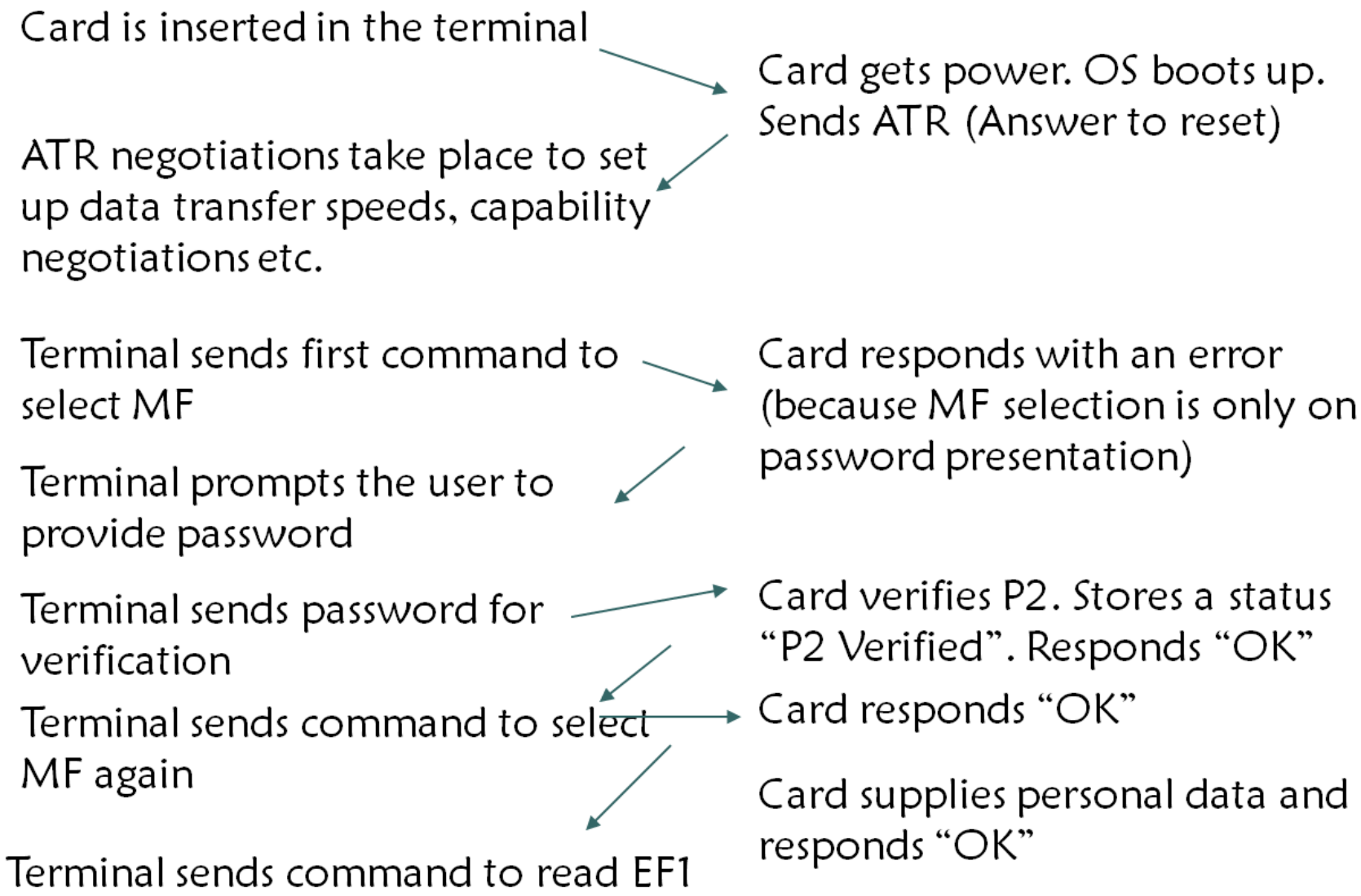
Functionality

Memory

Security

Interface

Card Interfacing



Access Control to Memory Regions

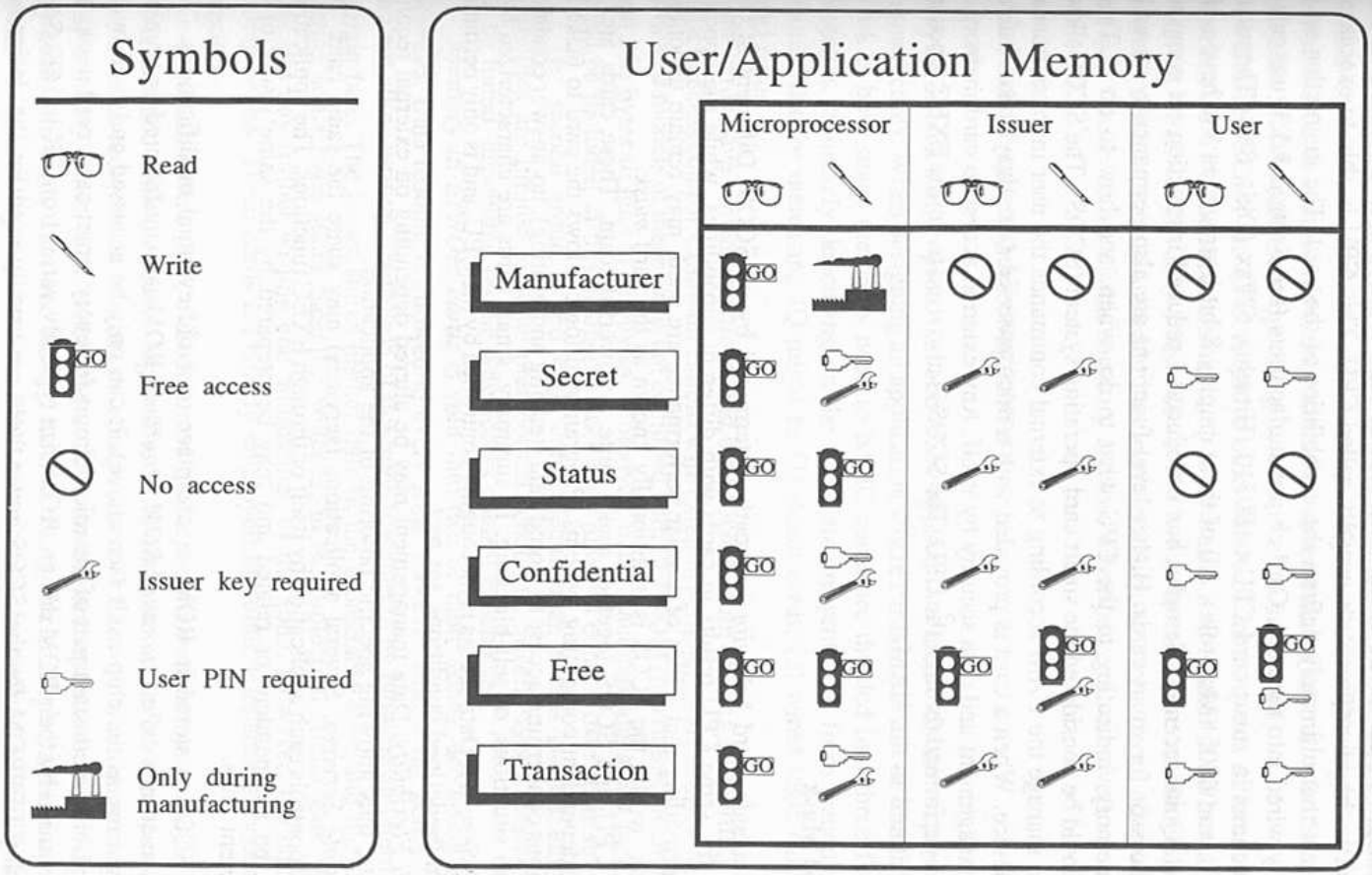


Figure 4.3 Typical zones of user/application memory.

Standard ISO 7816

- Physical characteristics (part 1)
- Dimensions and location of the contacts (part 2)
- Electronic signals and Transmission protocols (part 3)
- Inter-industry commands for interchange (part 4)
- Application identifiers (Part 5)
- Inter-industry data elements (Part 6)
- Inter-industry commands for SCQL (Part 7)

ISO 7816-4 Hierarchical Memory Structure

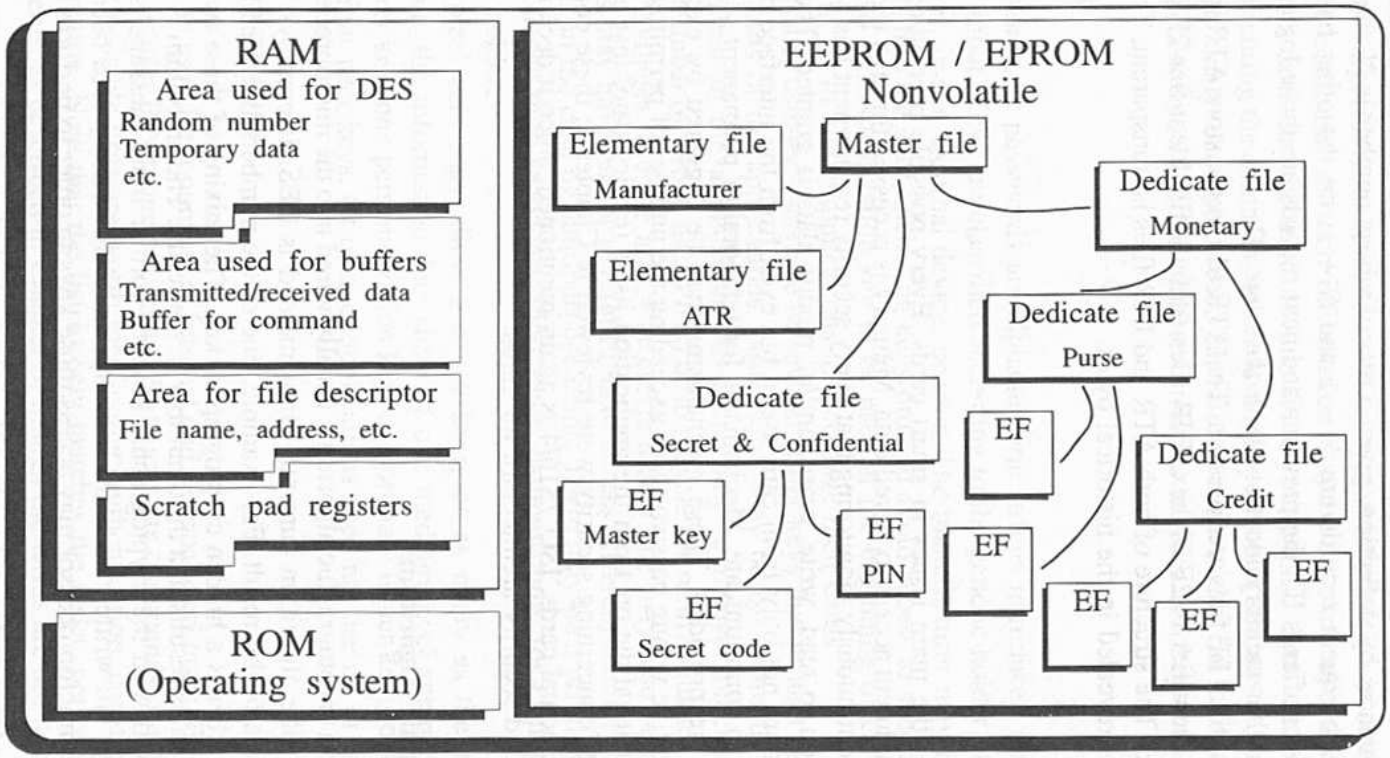
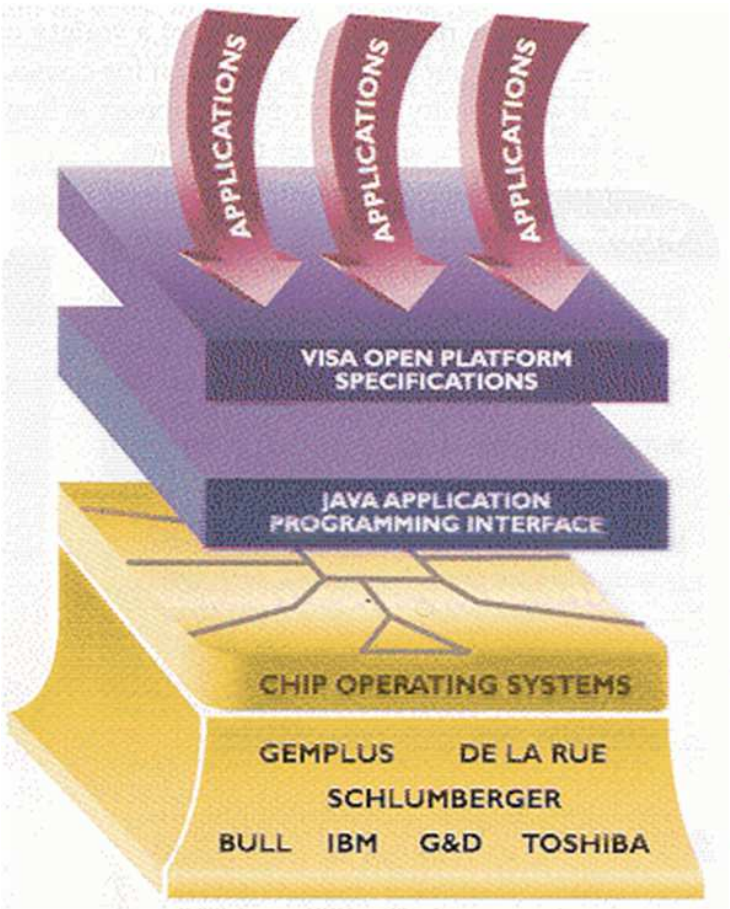


Figure 5.8 Hierarchical memory structure proposed by ISO 7816/4. ROM and RAM areas remain unmodified.

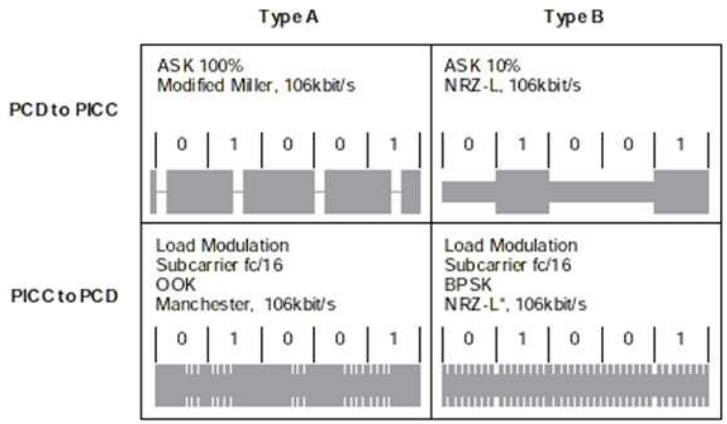
Standards – Levels of Abstraction

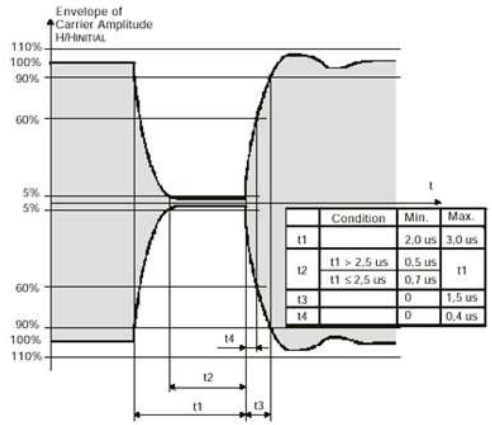


- Application
- Application interface (API)
- Logical
- Physical

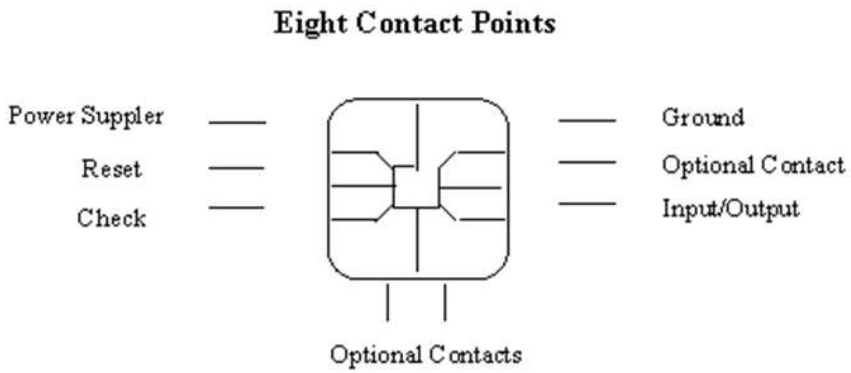
Standards – Physical and Logical Levels

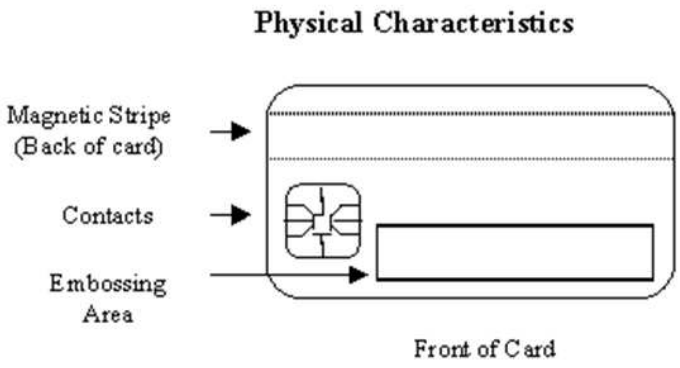
Logical (14443-2/B)





Physical (7816-1)





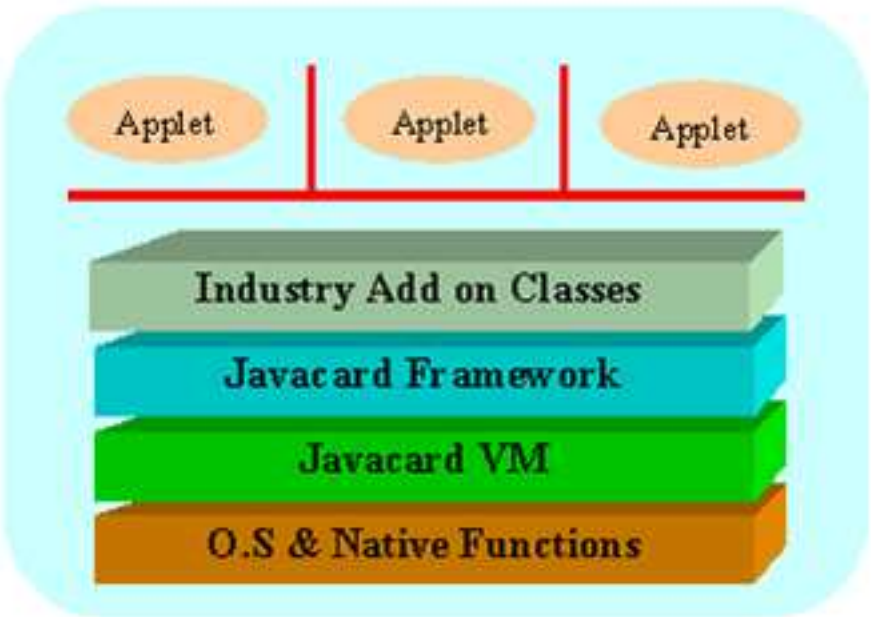
Extensions to ISO 7816

- ISO 7816 not enough to most advanced segments of the market
- EMV (Eurocard, MasterCard, VISA)
- GSM SIM (Subscriber Information Module)

Application level - JavaCardTM 2.1

Secure, multi-application smartcard platform (Sun JavaSoft division)

- Platform Independent (Java Card API)
- Multi-Application Capable
- Post-Issuance of Applications
- Flexible (Object-Oriented methodology of the Java Card)
- Compatible with existing Smart Card Standards (ISO7816, EMV)



Java Card 2.0 Language Subset

- Java Card programs are, of course, written in Java.
- They are compiled using common Java compilers
- Due to limited memory resources and computing power, not all the language features defined in the Java Language Specification are supported on the Java Card
- Specifically, the Java Card does not support:
  - Dynamic class loading
  - Security manager
  - Threads and synchronization
  - Object cloning
  - Finalization
  - Large primitive data types (float, double, long, and char)

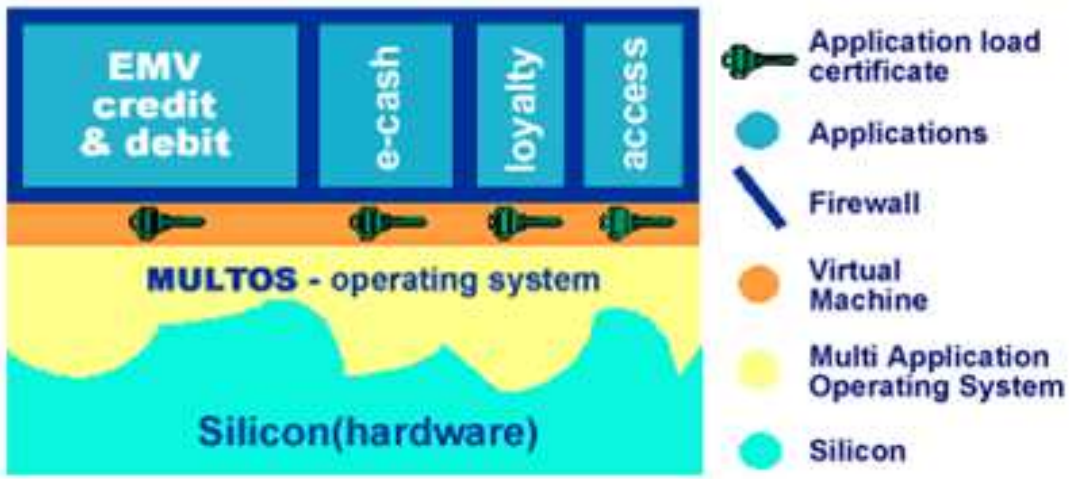
Java Card Security

- Java applets are subject to Java security restrictions
  - however, the security model of Java Card systems differs from standard Java in many ways
- Language security policies are implemented by the virtual machine
- Java applets create objects that store and manipulate data
  - an object is owned by the applet that creates it
  - an applet can share any of its objects with a particular applet or with all applets
- An applet is an independent entity within a Java Card
  - its selection, execution, and functionality are not affected by other applets residing on the same card.

Application Level - MULTOS

Secure, multi-application smartcard platform (MAOSCO)

- For multi-application smart card issuers
- A platform for interoperability
- An open, royalty free standard
- A complete scheme for managing smart card applications



MULTOS - Code Execution

- Code is developed in the C / Java / VB language and compiled into MULTOS bytecodes
- Code is interpreted every time it is executed
- The virtual machine performs code validity and memory access checks during execution of the code

Application level - Smart Card for Windows

Included in Cards for Windows are:

- A multipartition file system that physically separates data files so that multiple applications can safely run on a single card
- Access control rules that allow only certain people to access files on the card
- Pluggable algorithms that allow developers to specify their own levels of cryptographic support
- Support for existing smart card standards such as ISO 7816-4 commands

WFSM Virtual Machine & Security

Virtual Machine is Optional

Security

- Depends on how the application is written
- If application is compiled with OS function
  - then security by code inspection
  - else VM will take care of security

Which card to choose?

- Increased levels of processing power, flexibility and memory will add cost
- Single function cards are usually the most cost-effective solution
- Choose the right type of smart card for your application by determining your required level of security and evaluating cost versus functionality in relation to the cost of the other hardware elements found in a typical workflow
- All of these variables should be weighted against the expected lifecycle of the card
- On average the cards typically comprise only 10 to 15 percent of the total system cost
  - the infrastructure, issuance, software, readers, training and advertising making up the other 85 percent.

Application Domains (1/3)

- Banking and Finance
  - Debit/Credit cards
  - Prepaid cards
  - Multipurpose
- Health care
  - Patient cards
  - Health insurance cards

Application Domains (2/3)

- Telecommunications
  - Prepaid cards (telephone, TV)
  - Follow-me cards
  - SIM cards
- Transports
  - Prepaid and season tickets
- Government
  - Identity card, Passport
  - Drivers license, Social security

Application Domains (3/3)

- Corporations
  - Identification and access control to premisses and infrastucture
  - Prepaid cards
- Education
  - Identification
  - Prepayment

Future Trends

- Multi-services
- Biometric identification
- Contactless interface
- Multi-function personal assistants
- More structured system architectures

Outline

- Application Domains:
- Smart Cards

Next Class

- Mobile phones