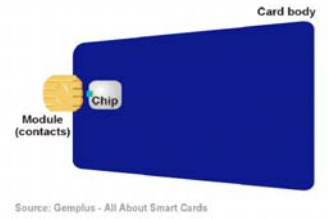
“Smart Card Evolution”



PG 6259 Fernando Ferreira
Universidade do Minho 31.1.2003

Outline of the evolution of the smart card

Year	Event
1968	2 German inventors patent combining plastic cards with micro chips
1970	Arimura invents and patents in Japan
1974	Roland Moreno invents and patents in France
1976	French DGT initiative, Bull (France) first licenses
1980	First trials in 3 Franch cities
1982	First U.S. trials in North Dakota and New Jersey
1996	First university campus deployment of chip cards

Smart Card Basics

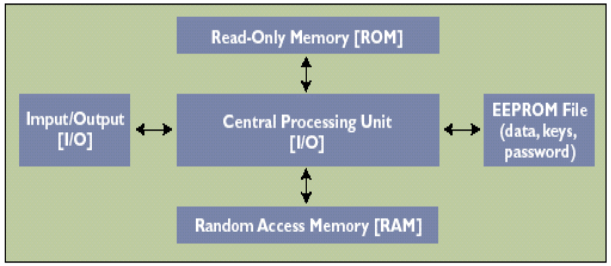
- One of the lastest additions of the IT
- Similar to today’s plastic payment card
- Microprocessor or Memory chip
- Reader
- Run their own OS
- API

Smart Card Basics

- Data portability
- Security
- Convenience

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

Architecture of a smart card



Memory

- Typically a smartcard will have the following amounts of memory: 6K to 20Kbytes of ROM (for the program), 1K to 16Kbytes of EEPROM (for transaction data that needs to be saved), and 128 to 1024 bytes of static RAM (for temporary storage).

Memory

- But, for example, we can have a smartcard with the following memory specification: 32 Kbytes of total ROM, 16 Kbytes of total EEPROM (up to 14.5 Kbytes are application memory – application code and application static data), 1280 Kbytes of total RAM (up to 400 bytes for DRAM - maximum session size is 400 bytes), 308 bytes of public memory

Comparison with PC CPU

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

The Processor

- Siemens SLE66 series chip with an 8051 CPU core
- Siemens SLE66C with a 16-bit core that will offer a bilingual instruction set for 8051
- ARM7TDM , a 32 bit RISC processor from TI, used in more recent Gemplus products
- Gemplus MPCOS-3DES
- one of the following, given as the most popular (manufacturers and processors) ones: SLE44C40S, SLE4436E, 44SLC80, SLE44C42 (from Siemens); SGS ST16601, 16SF48 (from Thomson); MC68HC05SC21, SC46 (from Motorola); 3102 (from Hitachi); H83102, P83C864 (from Philips).

8051 from Intel

- Most of these are slight variations of the standard types 8051, 6805 (Intel) and H8/300 (Hitachi). Having this in mind, only the 8051 will be described, as an example.
  - The 8051 has an 8-bit CPU, has not uniform and fixed length instruction fields (the instruction set consists of 49 single-byte, 45 two-byte and 17 three-byte instructions) and has not a large register bank (unlike RISC architecture). Also it is not a load-store architecture, because it has five addressing modes for source operands: Register, Direct, Register-Indirect, Immediate and Based-Register-plus Index-Register-Indirect Addressing.
  - The chosen microprocessor also has a Boolean processor that can be thought as a separate one-bit CPU: it has its own accumulator (the carry bit), instruction set for data moves, logic and control transfer, and bit addressable RAM and I/O; two 16-bit timer/counters and a full duplex UART, which allows the communications.

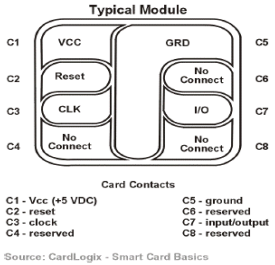
OS – Card standards

- Microsoft® Windows® for Smart Cards - uses common Microsoft Windows API calls
- Multi-Application Operating System (MULTOS) — developed by the MAOSCO consortium for financial transactions with emphasis on security
- Sun Microsystem Java Technology

Communication with the reader

- Contact cards
- Contactless cards
- Combination cards

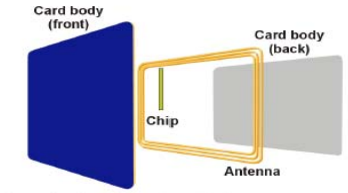
Contact Smart Cards



Source: CardLogix - Smart Card Basics

- 8 pin
  - Vcc
  - Reset
  - Clock
  - Ground
  - Input/Output

Contactless Smart Cards



Source: Gemplus - All About Smart Cards

- Antenna 10cm range
- Radio frequences

Smart Card Readers

- Interface
  - RS232 serial
  - USB
  - PCMCIA
  - IRDA
- Keyboard/CardReader

Standards

- ISO 7816-X — the dominant standard for contact smart cards consisting of ten sections that detail the physical, electrical, mechanical, and application programming interface. All other smart-card specifications are variations of this standard.

Specification	Definition
ISO 7816-1	Physical characteristic
ISO 7816-2	Dimension and location of contacts
ISO 7816-3	Electronic signal and transmission protocol
ISO 7816-4	Interindustry commands and responses
ISO 7816-5	Registration system for application identifiers
ISO 7816-6	Data elements for interchange
ISO 7816-7	Smart Card Query Language commands
ISO 7816-8	Security architecture
ISO 7816-9	Interindustry enhanced commands
ISO 7816-10	Synchronous cards

Standards

- ISO/IEC 14443-1 — the ISO and International Electrotechnical Commission (IEC) specification for contactless cards that changes the contact description to an antenna, and defines the protocol for communication over the air.
- ETSI — the European Telecommunications Standards Institute specification that defines a smallersized smart card to fit into GSM phones.
- EMV — the integrated circuit card specification for payment systems, which is managed, maintained, and enhanced by Europay International, Master Card International, and Visa International (EMV). This standard defines the way smart cards interchange in a payment terminal by disallowing the reader to be transparent. This increases security by preventing reading of the card for low-level information. This condition conflicts with Microsoft's Windows Hardware Quality Labs (WHQL) specification, which requires full ISO 7816 compliance.
- PC/SC — this PC/SC Workgroup specification builds on existing EMV and ISO 7816-X specifications by defining the smart-card reader/writer abstraction layer. This is a complementary specification that defines low-level device interfaces, device-independent application APIs, and resource management, which allows multiple applications to share smart-card devices attached to a system.
- JavaCard — this specification defines the way the Java Virtual Machine is implemented so that an end user can run any Java applet on the smart card.The Java Card Forum drives this specification.
- WHQL — the Microsoft WHQL facility defines the guidelines for products that are compliant with Microsoft OSs. The focus is to ensure that devices work in the Windows environment, and are compatible with other devices. WHQL requirements for smart cards require full ISO 7816 compliance.

Security

- Confidentiality
- User authentication
- Application authentication
- Transaction authentication
- Nonrepudiation
- PKI includes data encryption to ensure confidentiality, digital certificates to provide authentication, and digital signatures to prove the transaction was completed by the originator without intervention or error.

Biometric

Source: Frost & Sullivan

Biometric	Bytes Required
Finger-scan	300-1200
Finger geometry	14
Hand geometry	9
Iris recognition	512
Voice verification	1500
Face recognition	500-1000
Signature verification	500-1000
Retina recognition	96

Special Applications

- JavaCard and Personal Computer/Smart Card (PC/SC) allow programmers to write code for smart cards, much the same as the code written for PCs. The only limit for the code is the size of the EEPROM used in the smart card. Special applications that could be developed include:
  - Launching a web page on insertion of the card
  - Launching a support web page configured to the user's needs
  - Storing personal information
- The options for special smart-card applications are virtually unlimited depending on them creativity of the developer.

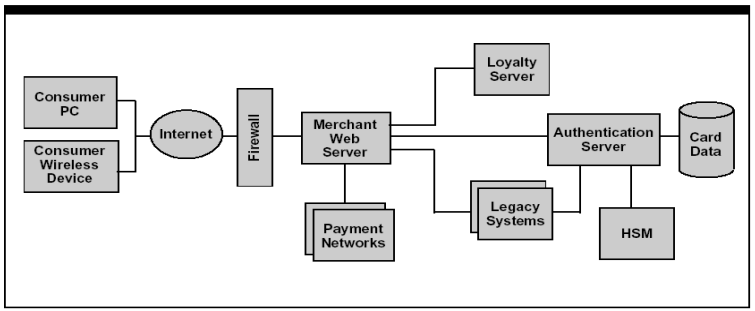
Support

- Windows XP Professional offers native support for smart cards. Other OSs require adding drivers supplied by the device manufacturer. Smart-card native support provided with Windows XP includes:
  - Reader drivers — supports several smart-card readers, and only requires that the reader is connected to the system, which allows Plug and Play to detect and configure the reader
  - PC/SC — supports the PC/SC card
  - Smart card ready — supports network PKI login

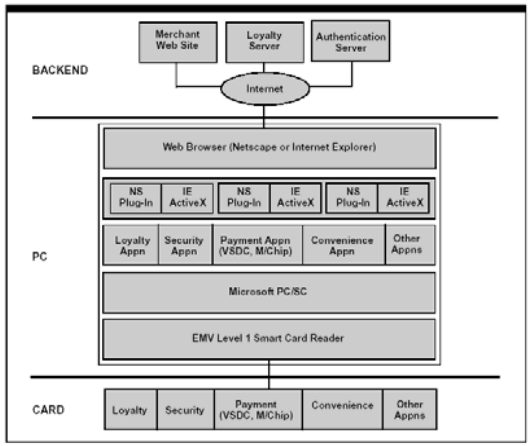
Internet Retail Payment

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

Smart card-enabled Internet System Architecture



Architecture of Smart-card support for the Internet Consumer



Emerging Markets and Applicattions

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

Comparison of alternative Technologies

	Card Features and Characteristics					Reader Features	
Card Type	Security [1]	Typical Memory Size [2]	Multi-Application Support	Standards	Upgrad-ability [3]	Reader Technology	Reader Portability
Smart Card	●	●	●	●	●	Solid state	●
Plastic	○	○	None	●	None	N/A	N/A
Magnetic Stripe	◐	○	○	●	◐	Solid state, moving parts	●
2D Barcode	◐	◐	○	●	◐	Solid state optics	●
Optical	◐	●	●	●	◐	Solid state, moving parts	○

Relative Position: Strong ● Medium ◐ Weak ○

Exemplos:Andante – Metro do Porto

“ Para validar basta aproximar o cartão ANDANTE do validador, a uma distância inferior a 10 cm e aguardar que acenda uma luz verde ”

Exemplos:VivoTech – uma “Start up”

Coleccionar empresas

Saiu da Gafanha para o Silicon Valley como aprendiz de electricista. Tirou o diploma em San Diego e começou a criar empresas tecnológicas em 1987

GESTÃO

JORGE FERNANDES, 38 ANOS

O leitor e o cartão com ‘chip’ criados pelo jovem português na América

(in Expresso 19.1.2003)

Exemplos: *Vital Card*

- *Vital Card* is a product developed in Portugal by Regimed but already used in other countries besides Portugal. The referred smartcard displays the bearer's digitised colour photograph and signature. The card contains the most important data about his or her medical history, such as blood group, whether he or she is an organ donor, wears a pacemaker or other prosthesis, any diseases or allergies currently suffered from, past surgery or transplants, personal and family history, what medication has been taken and stopped, current illnesses and factors that provide a risk of arteriosclerosis, congenital malformations and even the results of the latest laboratory tests [1]. Vital card carries the Siemens 8KB SLE44C80S microchip.
- [1] Solução Vital, <http://www.regimed.com>.

Policy, Ethics, Privacy, Legality

Policy	Recuirements	Solution
Voluntary vs. Mandatory	• Card is an alternative form factor to traditional ID forms, or • Card becomes a mandatory ID requirement for all citizens	• Solutions are designed to co-exist with traditional ID processes, or • Solutions are designed to replace the existing photo ID process.
Governance	• Requirements will specify responsibilities and roles for authorities involved in oversight, administration and enforcement of an ID program.	• Build solutions that can work with fragmented databases. • Design the IT architecture to ensure that cross-organization systems are integrated, communicate in near real time, and provide secure data storage.
Privacy	• Specify the amount of information stored for each individual. • Specify where this information should be stored and how it is protected from unauthorized access. • Specify who is entitled to have access to the identification information.	• Individual information can be stored in a secure centralized database, locally on a card or in both central and local locations. • Build a solution that allows the individual to control who has access to the identification information.
Degree of Authentication	• Issuing authorities or governments will specify the degree of authentication, based on the level of risk. • The general public will voice their opinions on the acceptability of the level of authentication and type of biometric scan.	• Design a solution that incorporates: (1) Something you have: Smart card or another type of ID. (2) Something you know: PIN or passcode. (3) Something you are: Biometric information (e.g., iris, hand geometry, fingerprint, voice print, facial scan).
Standards	• Specify which countries the solution should be compatible with and which standards it should support	• Build technology solutions based on industry standards to allow the widest compatibility and availability of components.
Profiling	• Specify the amount and type of information applied for risk profiling (e.g., age, gender, ethnicity, country of origin, traveler profile, criminal records, employment history)	• Design a technology solution that can interface with any number of databases. • Build risk profile algorithms based upon government specifications and needs and that can evolve and be upgraded over time.