Secure Smart Objects: Issues and Research trends

Samia Bouzefrane

SEMpIA team

CEDRIC Lab

March 19th, 2013

samia.bouzefrane@cnam.fr

Agenda

- What is SSO ?
- Characteristics of the platforms
- Security issues
- Actions to promote SSO domain

Context

Secure Devices

- Smart cards exist since 1979/1980
  - Research work for 30 years
- Evolution from contact to contactless devices
- New technologies : wireless networks, RFID
- Needs in terms of Security leading to trust systems

Characteristics

- Light-weight resources
  - Memory
  - Computation
  - Energy
- Strong security constraints

Properties

- Communicating Objects
  - Interaction with remote resources
- Secure Objects
  - Secure interaction with the environment
- Interface Objects
  - To access services
- Trust Objects
  - The user trusts these objects
- Domestic Objects
  - Human-Centered Design

Hard/Soft Platforms

- Smart cards (contact/contactless)
- Crypto-keys
- RFID sensors
- NFC chips
- TPM (Trusted Platform Module)
- TEE (*Trusted Execution Environment*)
- Mobile Trusted Modules for Mobile phones
- etc.

Research communities

- Smart Cards
- RFID / Sensor Security and Privacy
- Trusted computing
- Internet of things

Smart cards as secure devices

According to eurosmart

Worldwide Smart Secure Device shipment - 2012 and 2013 forecasts (Source: Eurosmart, November 2012)

WW shipments forecast millions of units	2012f	2013f	2013 vs 2012 % growth
Telecom	5 200	5 450	5%
Banking	1260	1480	17%
Government	290	350	21%
Transport	120	140	17%
PayTV	135	145	7%
Others	90	100	11%
Total	7 095	7 665	8%

Included in the above forecasts are the following contactless shipments (including dual interface contact and contactless):

Worldwide Smart Secure Contactless market figures – 2012 and 2013 forecasts (Source: Eurosmart, November 2012)

of which contactless millions of units	2012f	2013f	2013 vs 2012 % growth
Banking	270	360	33%
Government	150	180	20%
Transport	120	140	17%
Others	60	70	17%
Total	600	750	25%

Source Eurosmart: http://www.eurosmart.com/index.php/publications/market-overview.html

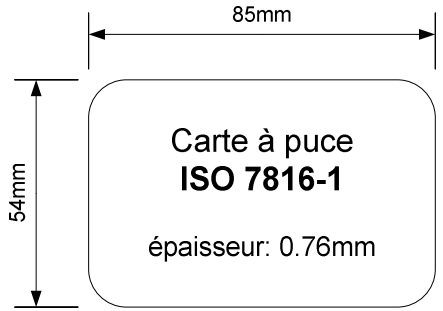
Evolution of smart cards

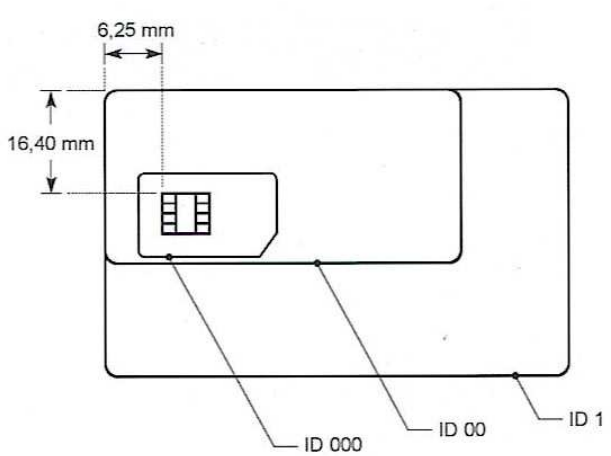
- Inventor: Roland Moreno (1974-1979), 47 patents in 11 countries

- Involvement of industrials like Bull and Schlumberger
- Used in many domains: transport, telecom, banking, check access, passport
- From mono-application to multi-application
- From proprietary OS to open OS (Java Card, .NET)

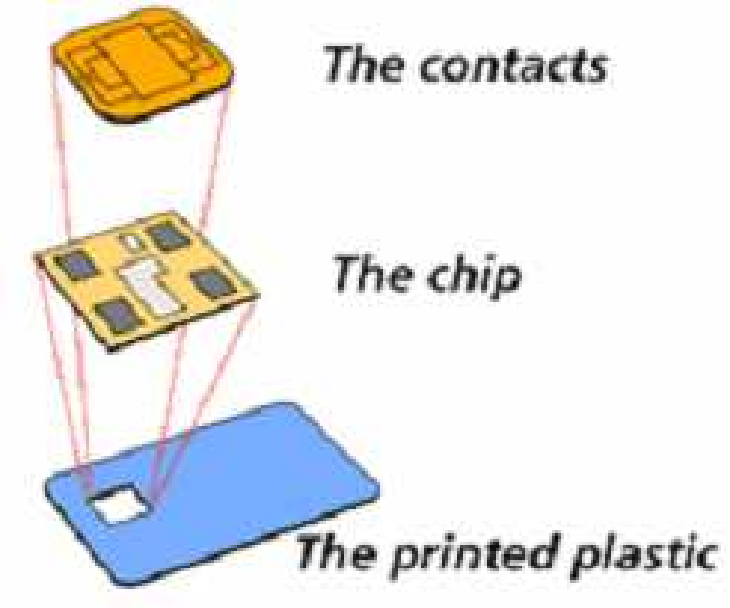
ISO7816 Standard

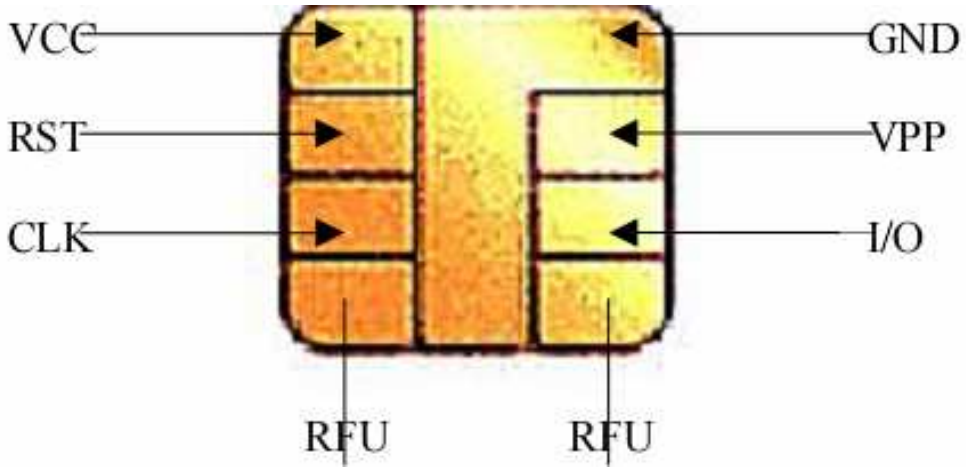
- The standard ISO 7816-1 defines the physical characteristics of the card
- The standard ISO 7816-2 defines the position of the contacts within the card
- The standard ISO 7816-3 defines the electric signals used to communicate with the card
- The standard ISO 7816-4 defines the basic commands to interact with the smart cards





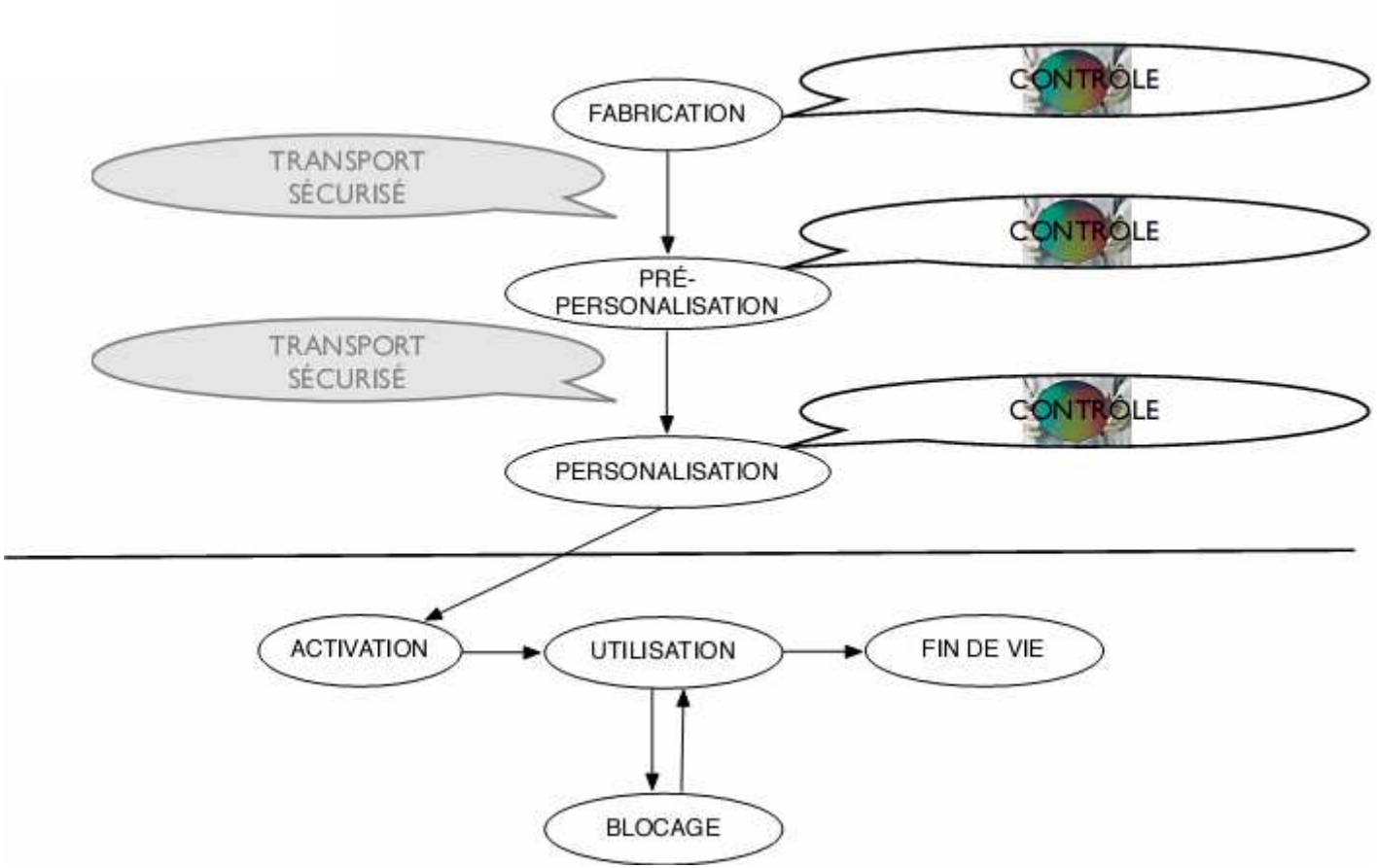
Card Contacts in ISO7816-2





APDU protocol for communication

Card life cycle



Physical characteristics

- Monolithic component :
  - CPU (8, 16, 32 bits)
  - PROM (32 to 64 KB) contains OS (JVM)
  - RAM (1 to 4 KB)
  - EEPROM/Flash 1KB to 128 KB (256 KB for Java Card) contains data and applications
  - I/O interface
  - crypto processor

Physical security

- Sensors to detect:
  - a loss of electrical power,
  - overheating of the components,
  - light sensor.

A safety box

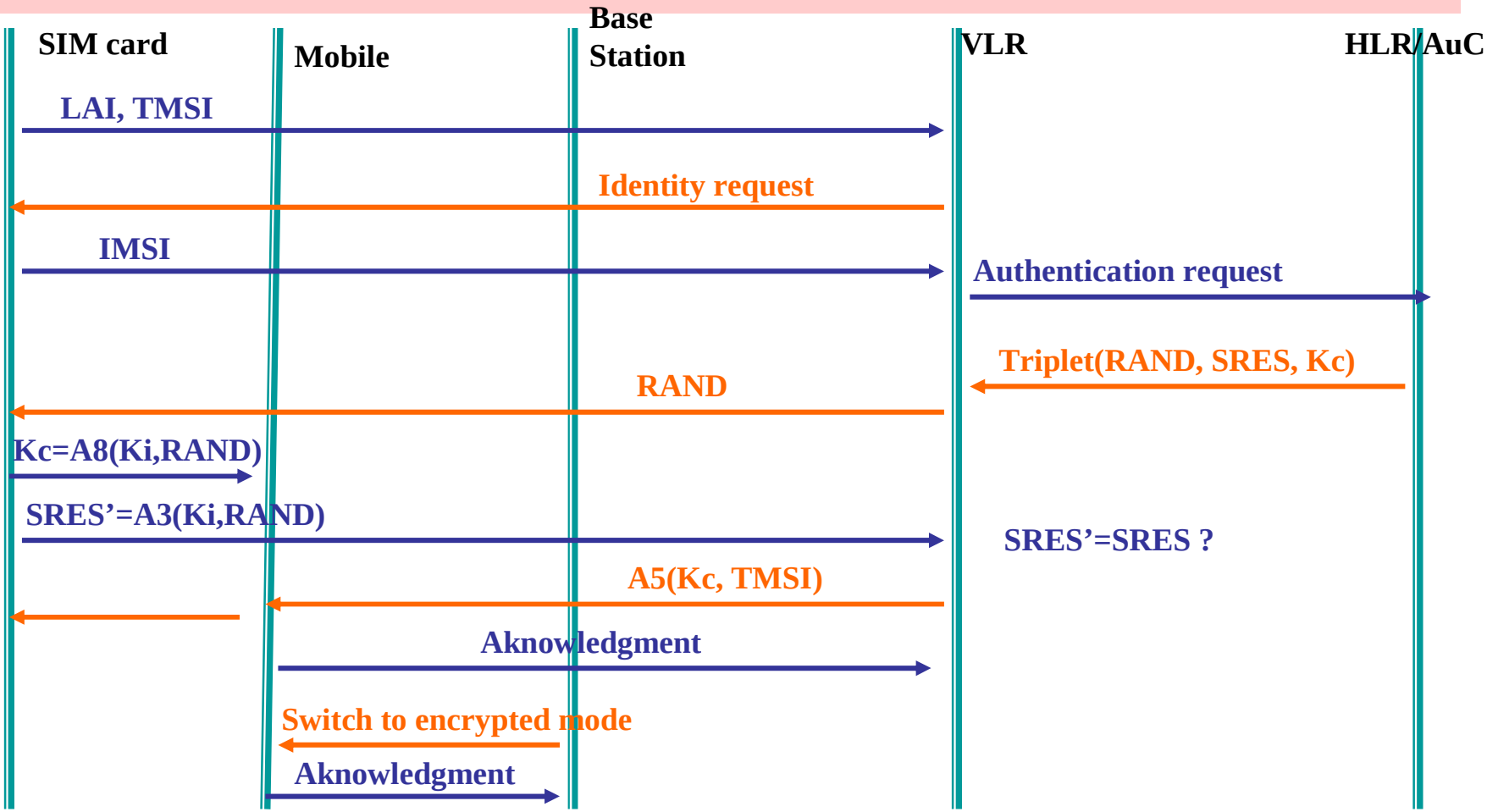
- Stores security keys and sensitive data
- Implements cryptographic algorithms
- Crypto-processor
- Used for authentication and encryption
  - SIM card authentication with the cell networks
  - Banking card authentication with payment terminals

Security protocols

Standards

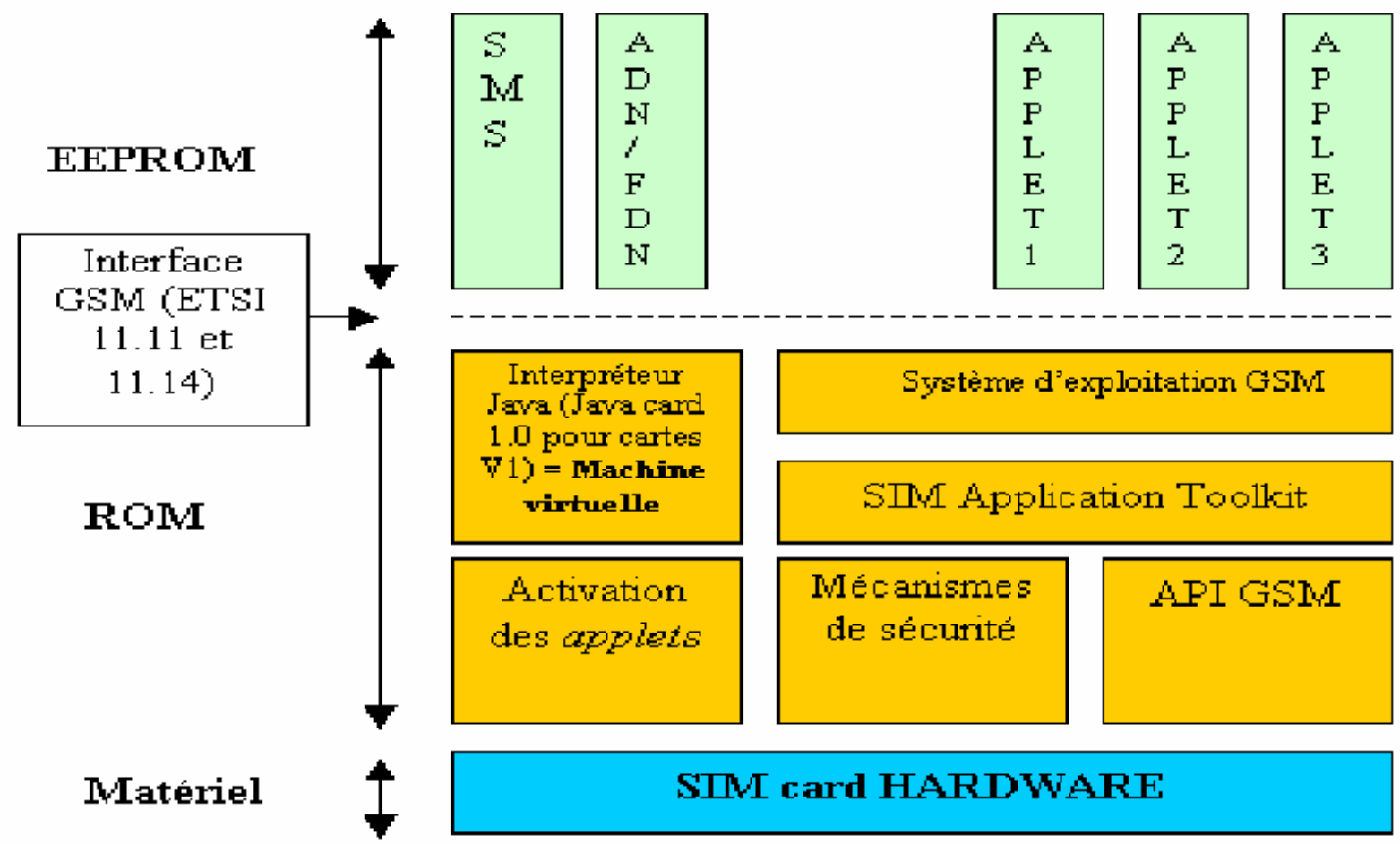
- ISO 7816 (basic standard)
- ETSI (for SIM/USIM cards)
- EMV (*Europay Mastercard Visa*, for banking cards)
- ICAO (*International Civil Aviation Organization*, ONU agency, for biometry, passport)
- Health

SIM card Authentication with GSM



ETSI Standard

SIM card architecture

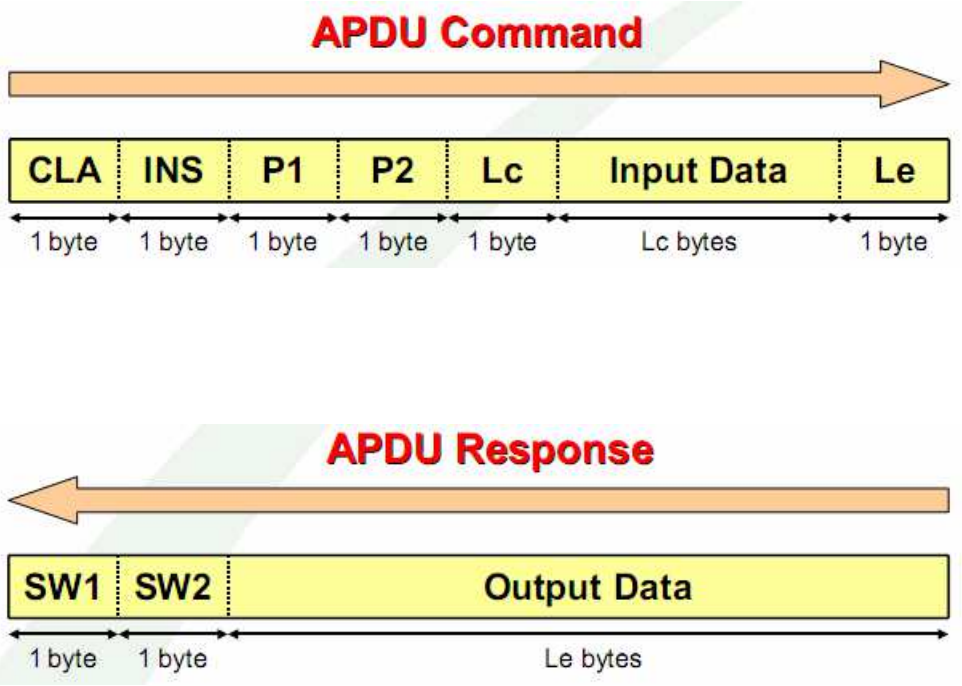


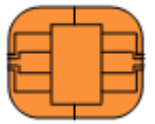
SIM card services

- Data Storage
  - For network configuration (IMSI, lang. pref.)
  - For the user (agenda, SMS file, MSISDN)
  - Dynamic information: session key (Kc), geo-localization (LAI, TMSI)
- Service Storage
  - Applications
  - Remote updates
  - Proactive behaviour

APDU communication

Mobile

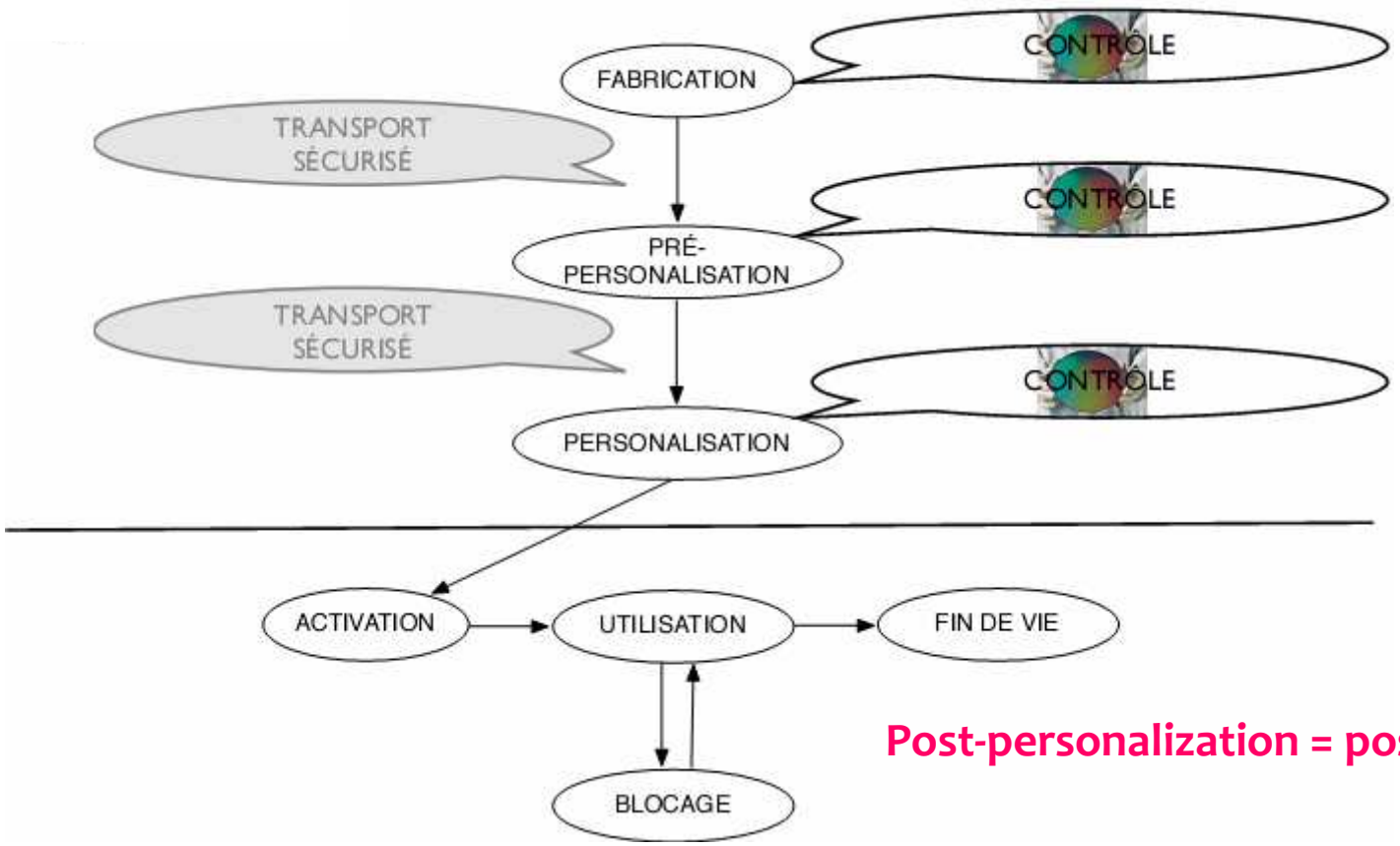




SIM

Pro-active mode

Post-issuance

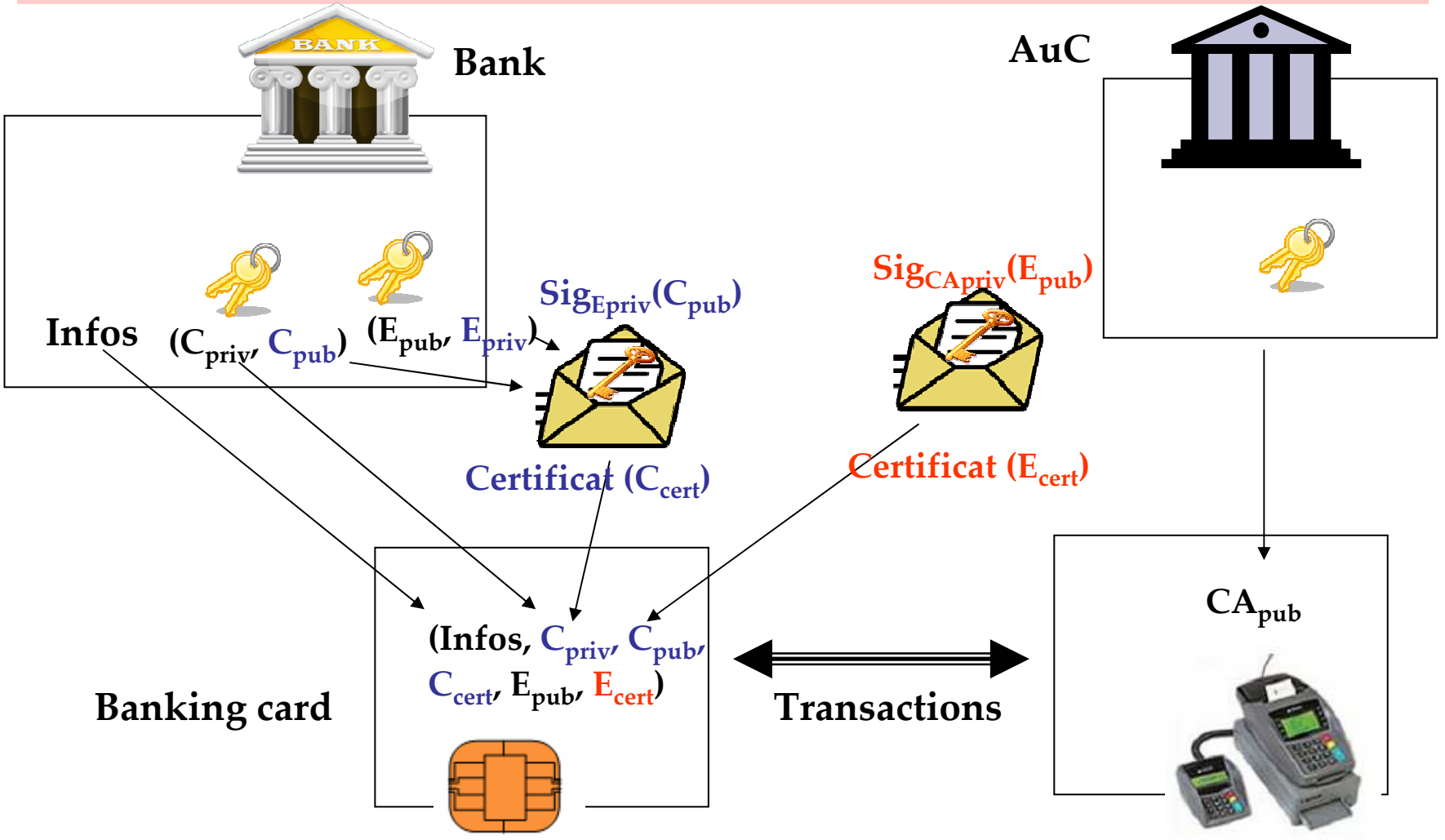


Post-personalization = post-issuance

Over The Air management

- 3GPP TS 23.048 Standard (ETSI)
- SMS of type "SIM Data Download"
- Security mechanisms
  - Authentication: DES signature (Hash message) added to the message
  - Confidentiality: DES encryption of messages
  - Integrity: add a checksum to the message
  - Againts replay: add a seq no for each message

EMV payment
Personalization with DDA



Dynamic Data Authentication

$C_{cert} = Sig_{Epriv}(C_{pub})$

$E_{cert} = Sig_{CApriv}(E_{pub})$

(Infos, C_{cert}, E_{cert})

(Infos, C_{cert}, E_{cert})

T_{alea}

(Infos, C_{pub}, C_{priv}, C_{cert}, E_{pub}, E_{cert})
PIN code

$Res=Sig_{Cpriv}(C_{alea}, T_{alea}), C_{alea}$

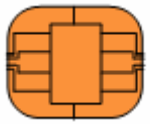
CA_{pub}

$RSA(E_{cert}, CA_{pub})=E_{pub}$

$RSA(C_{cert}, E_{pub})=C_{pub}$

$Decrypt(Res, C_{pub}) ?= C_{alea}, T_{alea}$

Ask to PIN code



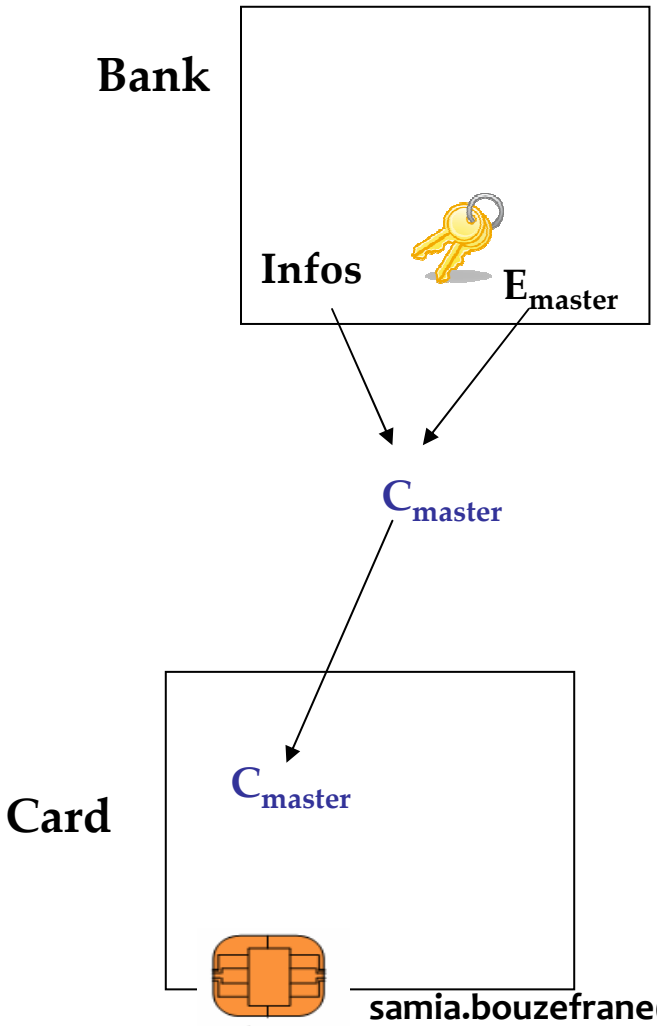
Banking card

$Crypt_{Cpub}$(PIN code, alea1, alea2)

Merchant

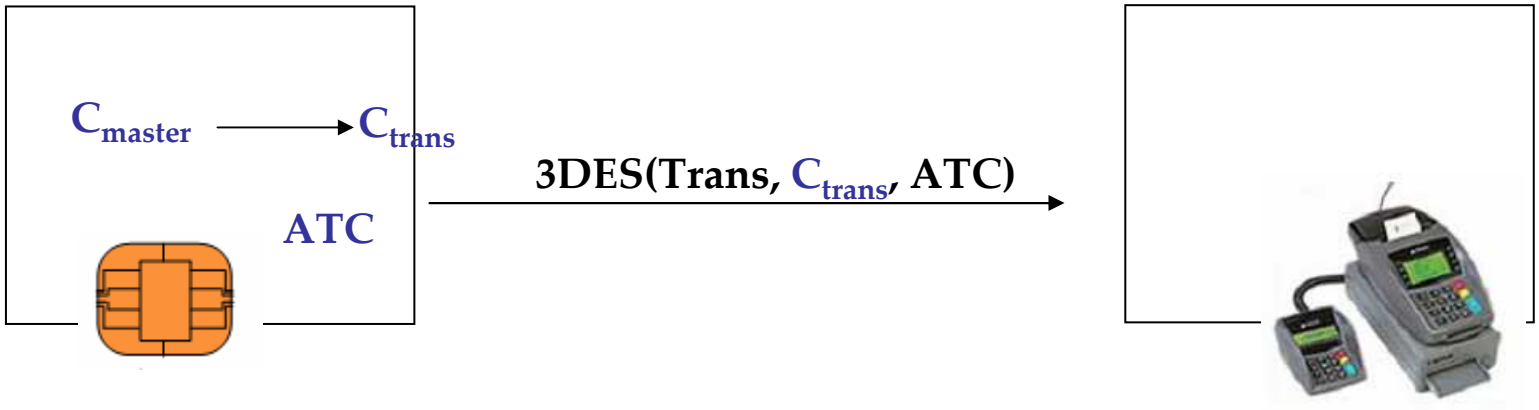
samia.bouzefrane@cnam.fr

Personalisation for payment



Off line payment

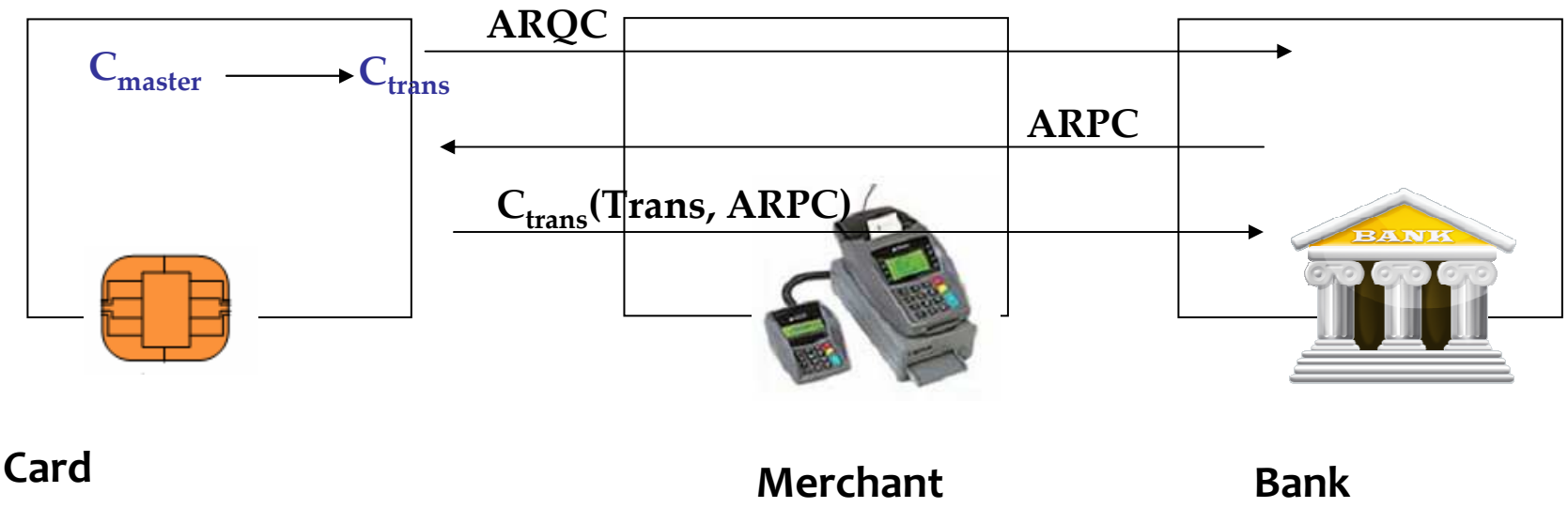
Derivation of a unique key for each transaction:



Card

Merchant

On line payment

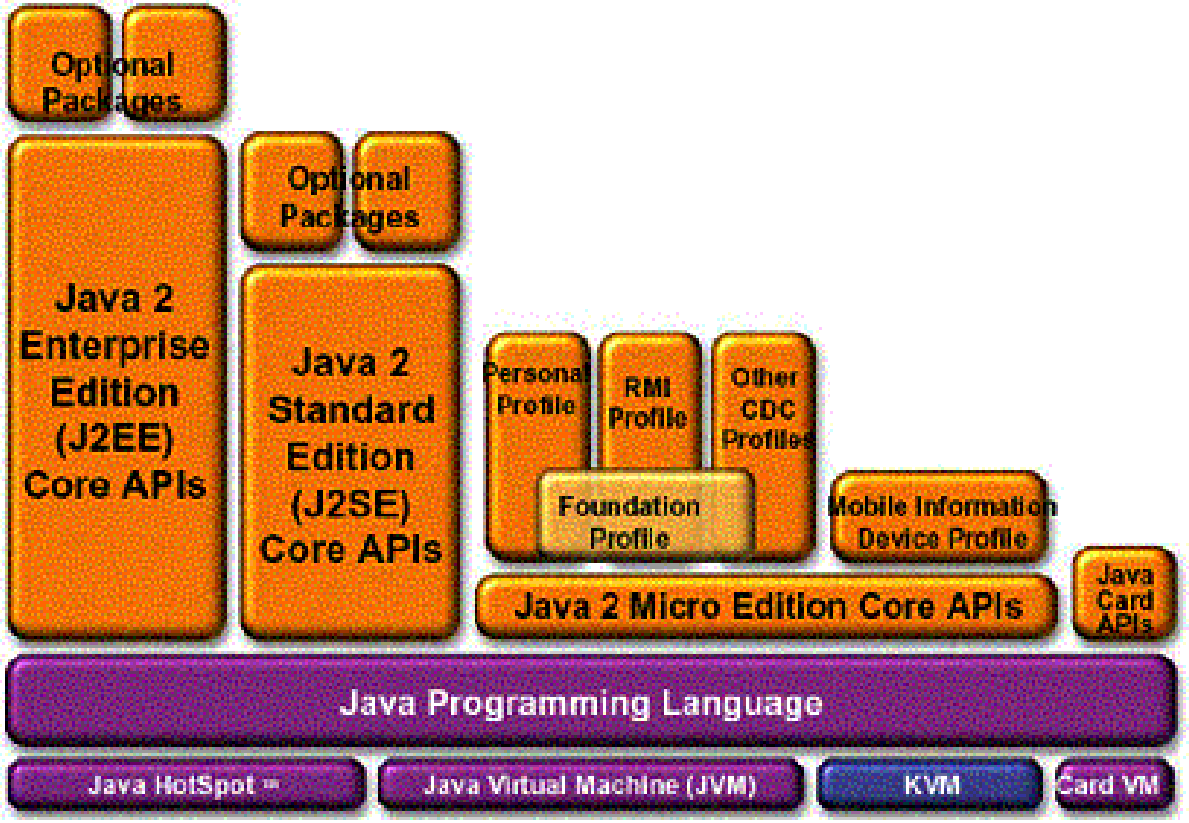


Trusted Execution Environment

Industry development

- The pioneers (1975-1985): first foundation
- 1985-1995: the technology is improved
  - Markets and large deployments: CB, GSM
  - Limits: need more flexibility
- 1995-2005 : explosion of the market, cards based on Scalable Java Card
- 2013: 90% SIM cards are Java Card platforms
    - With 5 billions in 2012
- 2005-???: the card becomes an element of the network
  - SCWS (Smart Card Web Server), .Net, Java Card 3.0

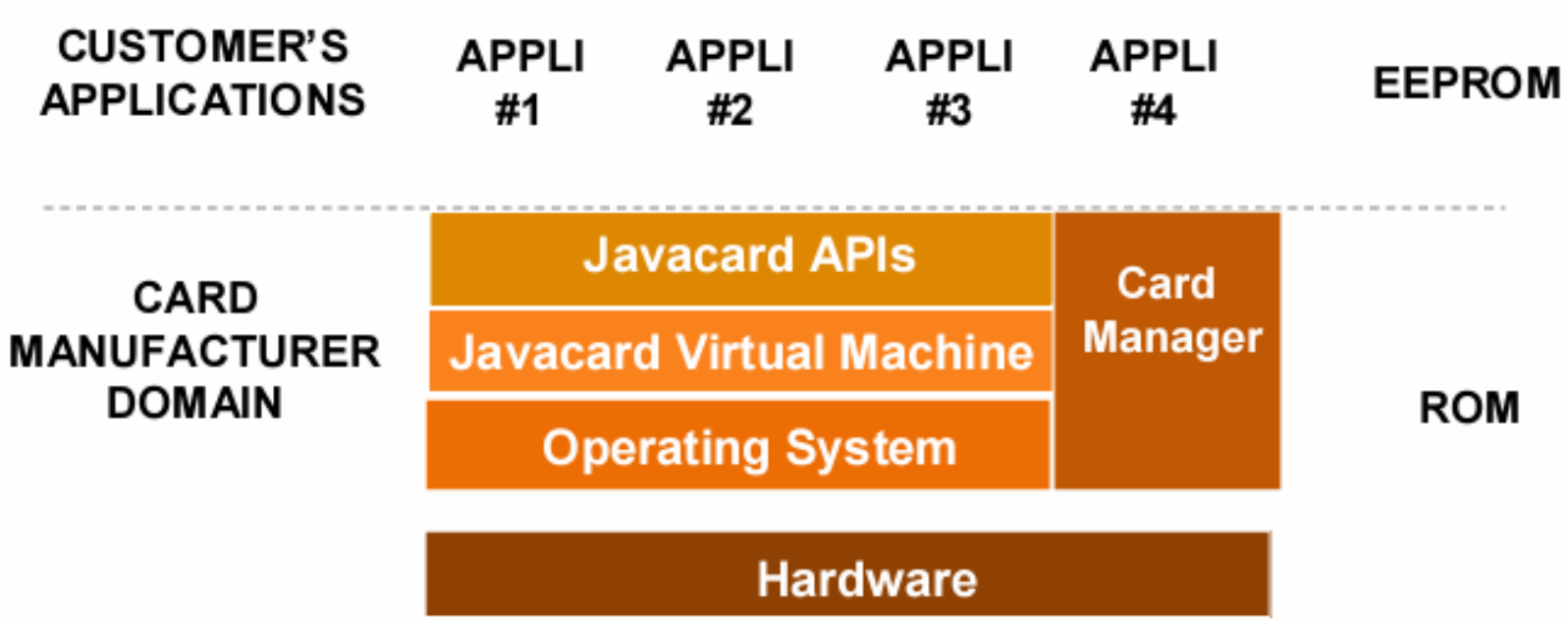
Java Card technology



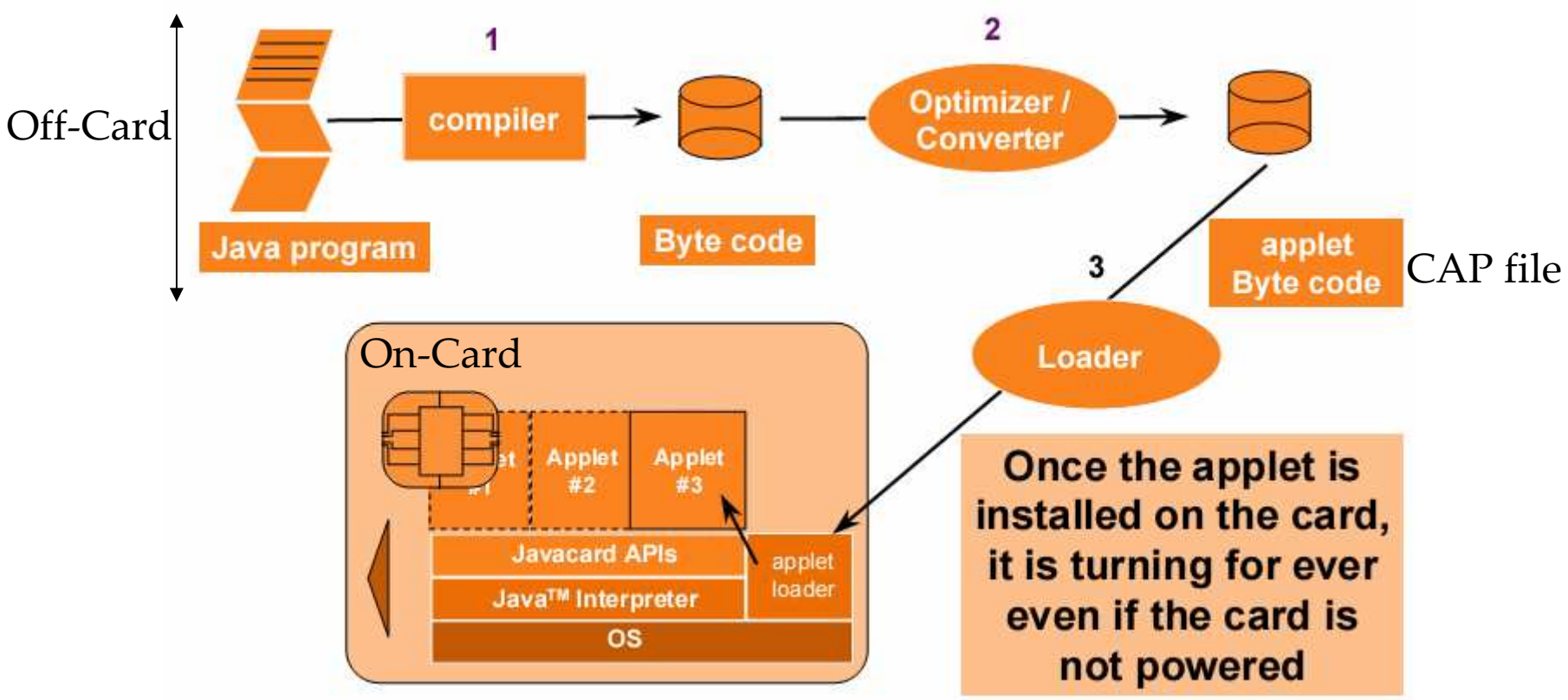
Java Card Specification

- Java Card 3 Specification by Oracle
  - Classic edition (extension of Java Card 2.2)
    - Java Card API Specification
    - Java Card Runtime Environment Specification
    - Java Card Virtual Machine Specification
  - Connected edition (Web oriented, not deployed)
- Java Card forum promotes Java Card Tech.
- Global Platform defines a trust environment in a multi-application cards (as for Java Card)

Java Card platform



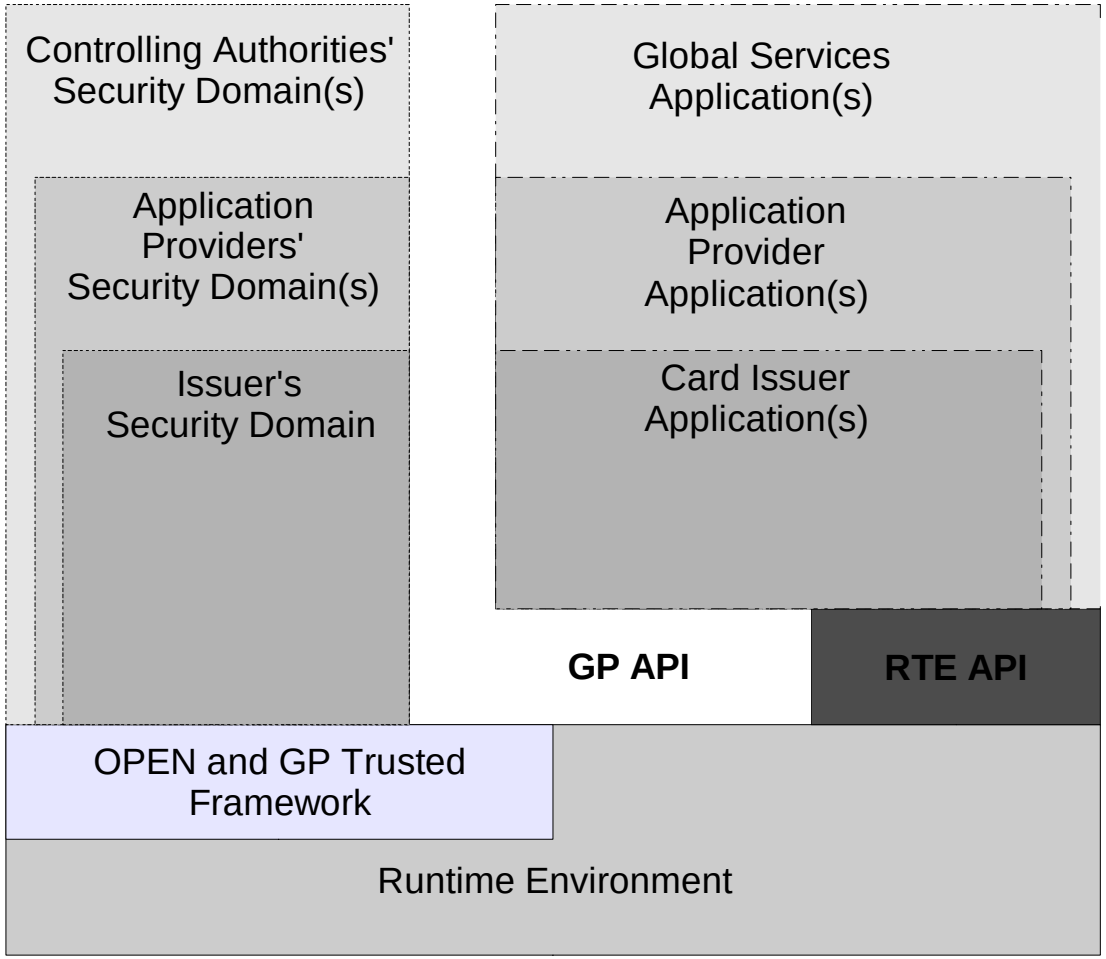
Development process



Global Platform standard

- CAP file signed before conversion
- Checks the integrity of the installed applications
  - Checks if the CAP file is signed
- Secure communication from the terminal
  - Package authentication before applet installing
  - Secure channels

GlobalPlatform Card Specification v2.2.1



GP RunTime Environment

- RTE dedicated to multi-applications card
- Provides to the applications
  - A secure execution environment
- The code/data of applications are isolated from each other
  - In Java Card, this is achieved thanks to the firewall applet

Security domains in Java Card

- In Java Card platforms
  - Each application (package) in a Security Domain
  - Many applications from distinct providers may co-exist in the same card
  - A firewall applet checks the isolation
  - Each application has its own trusted execution environment
  - The applications may share objects

Attacks

Motivation

- Objective
  - Find/modify confidential information
- Benefits
  - Make a financial order, impersonation, invasion of privacy

Physical attacks

- Inspection of the circuit
  - using the microscope (examples of results http://www.flylogic.net/)
- Observation
  - Measure the response time of a query, measure the current consumption or electromagnetic circuit
  - Micro-probing (to examine the data exchange of a bus)
- Disruption
  - Change the clock rate (which is external)
  - Vary the voltage
  - Generate a strong magnetic field
  - Light the silicon using a laser or a camera

Logical attacks

- Attacks taking advantage of bugs in the implementation of the JCVM.
- Weakness in the bytecode verifier
- Injection of code
- Laser attack to modify data values

Towards the contactless

RFID

- **R**adio **F**requency **Id**entification
  - Identification of persons, objects, services
  - Contactless technology: transmission by radio

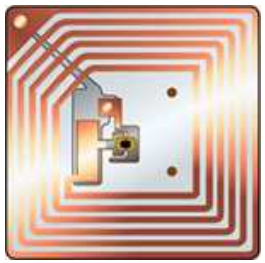
RFID components

❑ **RFID architecture :**

- ***base station***: a reader, a terminal, cell phone, etc. that identifies and processes the information read by radio waves

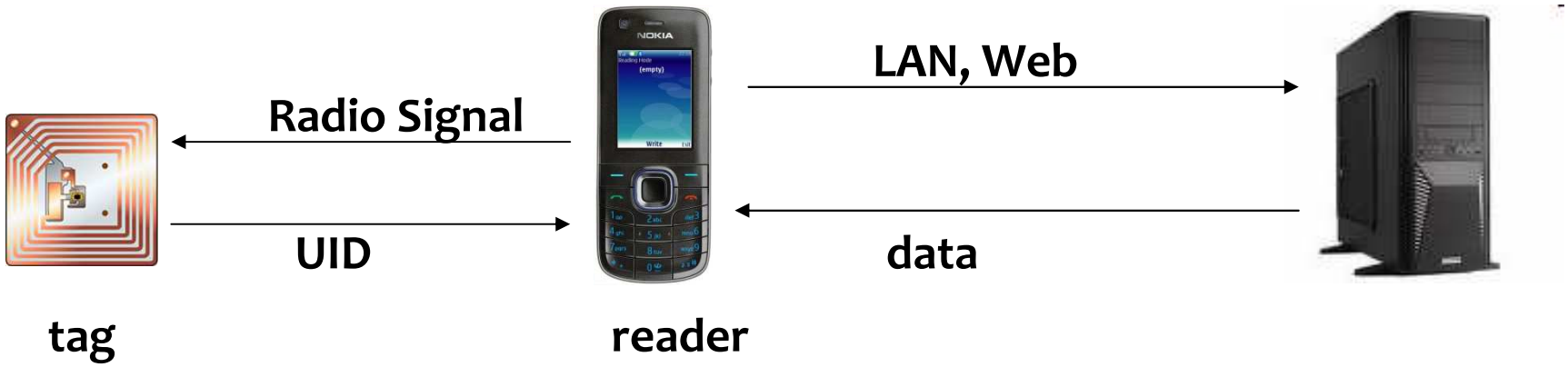


▪ A **transponder** or "**tag**" **:** electronic label, contactless card.

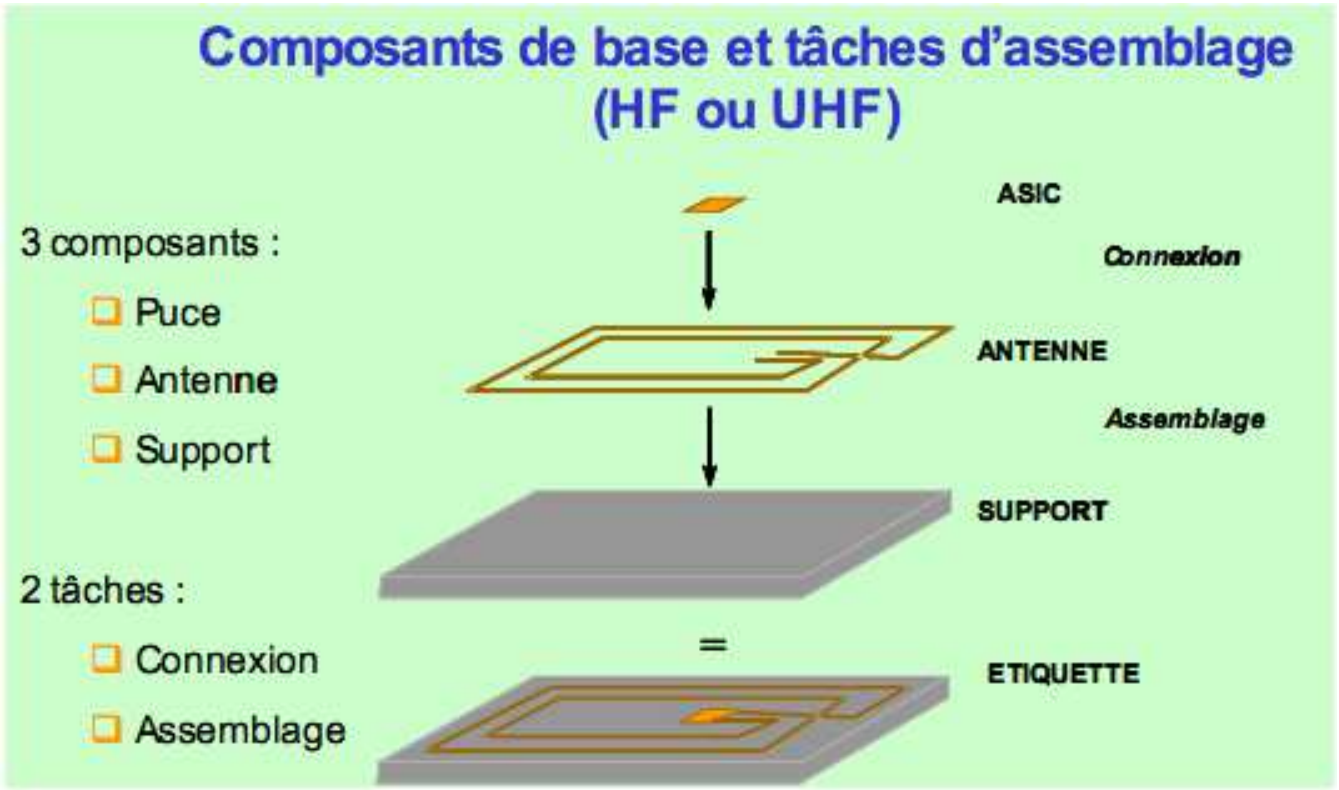



▪A **system**: web service, information systems, middleware processes the data for analysis, archiving, traceability.

RFID system architecture



Tag components



RFID Tags/Frequencies

- Tags
  - Memory/Microprocessor tags
  - Passive/Active
- Frequencies
  - Low frequency LF (<= 135KHz)
  - High frequencey HF (around 13.56 MHz)
  - Ultra-high frequency UHF (~ 434 MHz, 869-915 MHz, 2.45 GHz)
  - Micro-waves (~ 2.45 GHz)

ISO 14443 standards

- ISO 14443 (Part 1 to 4)
  - Part 1 : contacless integrated circuit cards: physical characteristics
  - Part 2: contacless integrated circuit cards: radio frequency power and signal inteface
  - Part 3: contacless integrated circuit cards: initialization and anti-collision
  - Part 4: contacless integrated circuit cards: transmission protocol

- ISO 14443
  - Standards for contactless
  - Distance : 10 cm
  - rate: some hundreds of kilobits/s

ISO 10536 Standards

- ISO 10536 (1 to 4) : contacless integrated circuit cards
  - Part 1: Physical characteristics
  - Part 2: Dimension and location of coupling areas
  - Part 3: Electronic signals and reset procedures
  - Part 4: Answer to reset and transmission protocols.

- ISO 10536
  - Distance : 10 mm

ISO 15693 Standards

- ISO 15693 (1 to 3) : contacless integrated circuit cards
  - Part 1 : vicinity cards: physical characteristics
  - Part 2: vicinity cards: air interface and initialization
  - Part 3: vicinity cards: anti-collision and transmission protocol

- ISO 15693
  - Distance : 1m

Electronic passport

- According to ICAO DOC 9303 standard
- The electronic passport
  - is a passive tag
  - compatible with ISO/IEC 14443 standard
  - has a cryptoprocessor (RSA-1024, elliptic curves)
  - EEPROM: 30KB to 70KB

Security problems

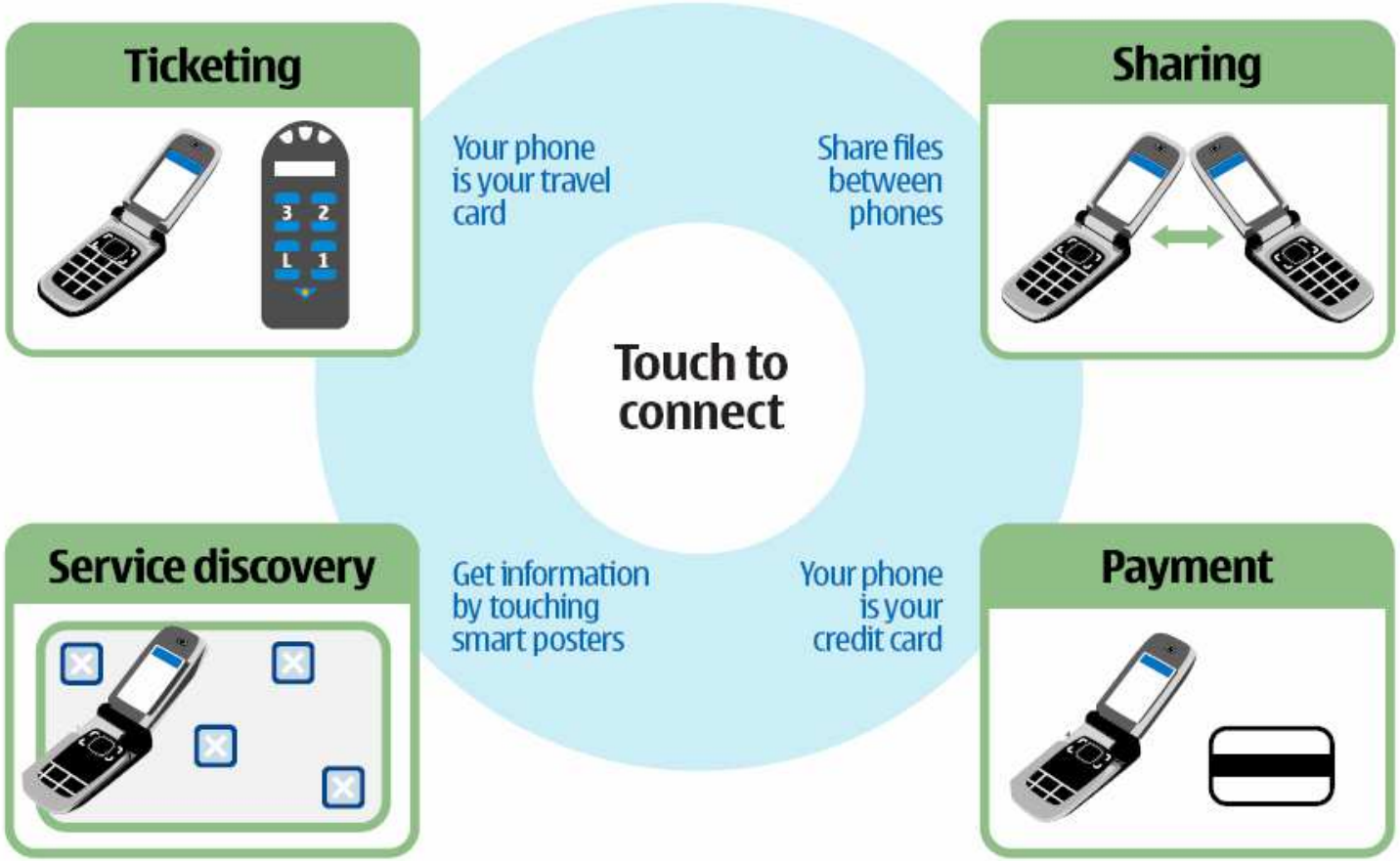
- Basic tags used for identification with no authentication
  - Resolved on the server: as in EPCglobal
  - Centralized solution: implementation of cryptographical solutions for tags with resource capabilities (like smart cards)
- Privacy
  - Ex: biometric passeport includes an authentication mechanism (faraday cup)
- Geo-localization of objects
- Standardization in the field: too many different solutions
- Respect of the environnement: Biodegradable tags

Near Field Communication

NFC over the world

- Japan with Sony FeliCa, NTT DoCoMo
- Cingular Wireless, Citigroup, New York subway, MasterCard Worldwide, Nokia, Venyon
- StoLPaN « Store Logistics and Payment with NFC » is a european consortium : http://www.stolpan.com
- Touch&Travel: Vodafone, Deutsche Bahn, Motorola, Giesecke&Devrient, ATRON electronic, Germany
- Manchester City Football Club, Orange, Barclays, TfL Oyster card
- Transportation in London, smart poster
- Cityzi at Nice, mobile payment at Caen and Strasbourg.

NFC modes


Ticketing
Your phone is your travel card
Share files between phones
Sharing
Touch to connect
Service discovery
Get information by touching smart posters
Your phone is your credit card
Payment

NFC Forum specifications/1

- NFC Forum gathers a great number of industry: Samsung, Sony, Nokia, Nec, Panasonic, Visa …
- Goal of standardization of RFID market like EPCglobal
  - Modular architecture and interoperable
  - targets the mobile market.

- **Frequency 13.56MHz (HF)**
- **Rate of 424 Kb/s**
- Standardized by
  - ISO 18092
  - ISO 21481
  - l'ECMA (European Computer Manufacturer Association)
  - ECMA 340 NFC IP-1
  - ECMA 352 NFC IP-2+
- Compatible ISO 14443-A, Felica (Sony), Mifare (Philips)

NFC Forum specifications/2

- NFC allows a phone to read / write a tag, to act as a smart card or to communicate with another phone.
- 3 modes :
  - Read/write of tags (MIFARE …)
  - Peer to peer (initiator & target)
  - Card emulation
- Distance : 0 - 20 cm
- Rate: 424 kbits/s
- NFC Forum : NDEF specs

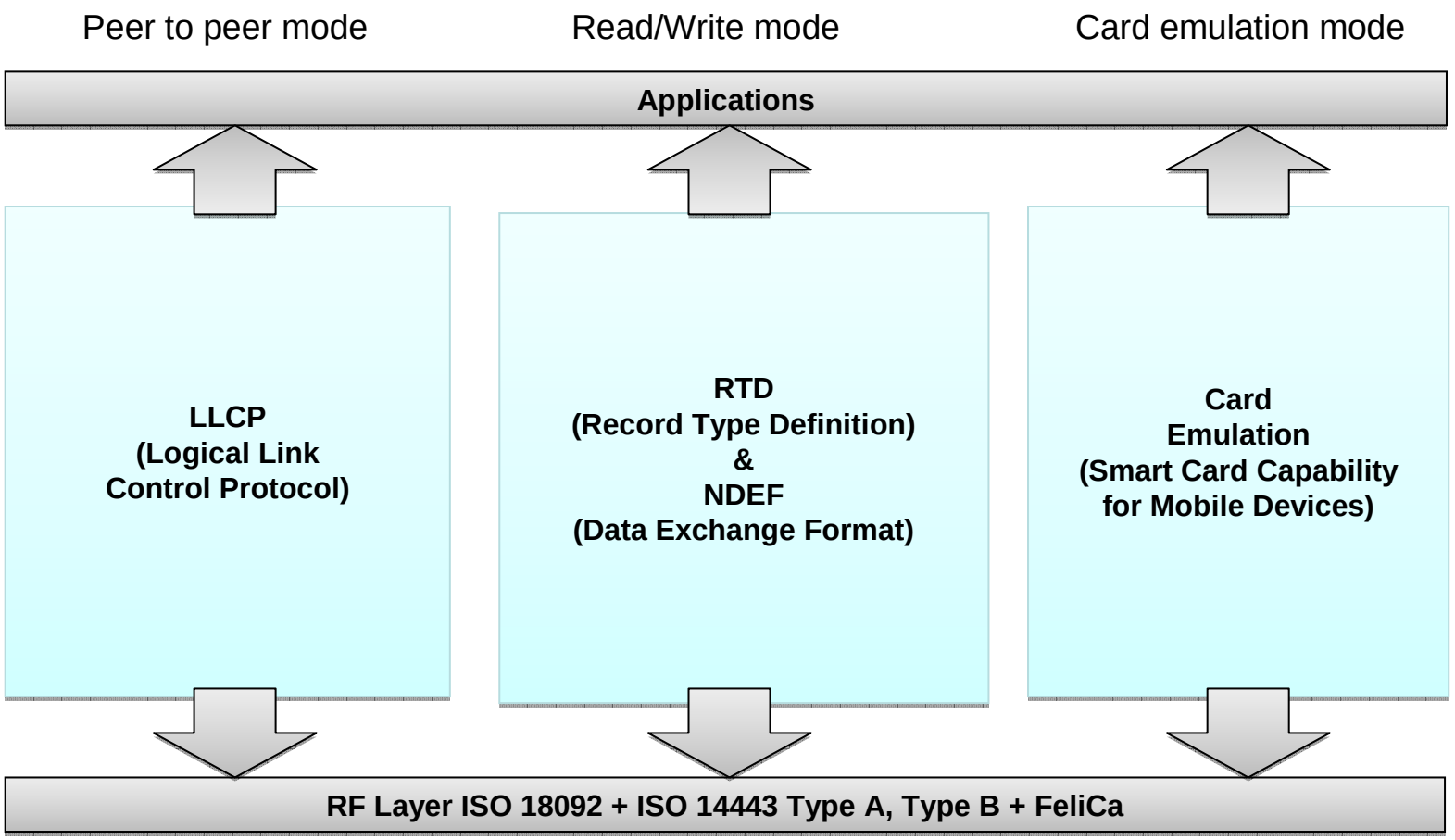
Other standards

- 

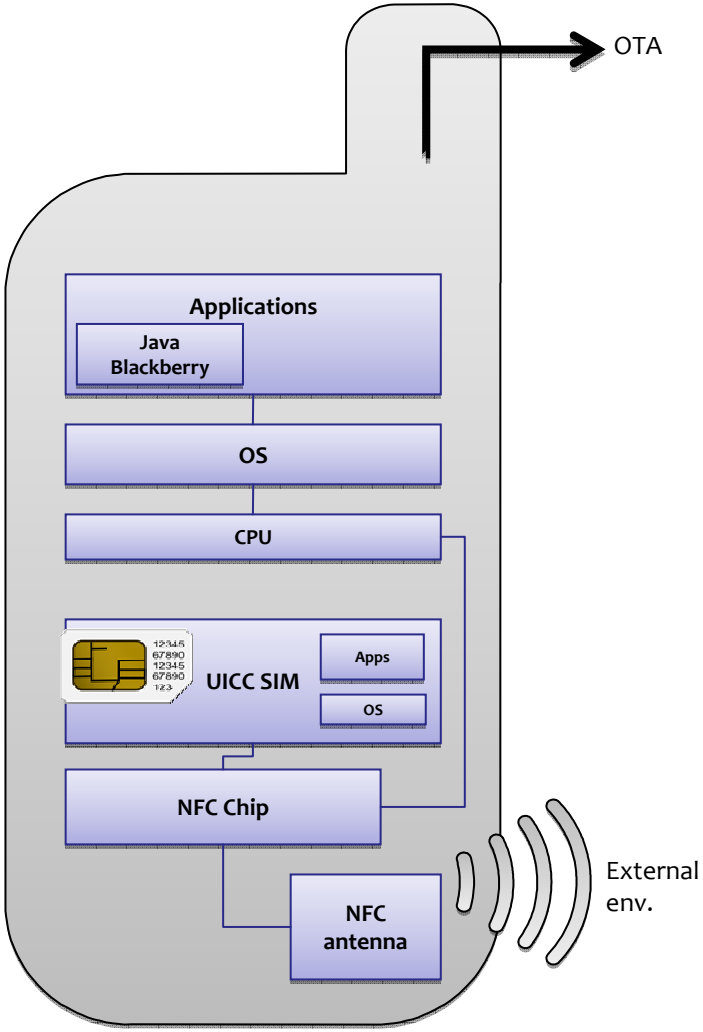
/ SCP (Smart Card Platform) to specify the interface between the SIM card and the chip NFC.
- GLOBALPLATFORM to specify the multi-application architecture of the *secure element*.
- 

for the impact on the EMV payment applications.

NFC Forum specifications



Mobile Payment



- Single Wire Protocol (SWP) : the SIM card is linked to the Secure Element (SE) building a same Java Card.
- GlobalPlatform is used for isolation & security.

Threats

- Denial of service by using a jammer to disrupt the communications
- Identity Theft:
  - Solution:
    - use a challenge-response protocol instead of a simple identification protocol
- Data recovery: data leakage, traceability, etc.
- Relay attacks:
  - Solution
    - distance bounding protocol that evaluates the distance by measuring the time elapsed

Trusted Platform Module

Trusted Platform Module

- Manufacturers: HP, Infineon, Intel Dell, FUJITSU, etc.
- Sensors: Over/Under voltage detection, low frequency sensor, high frequency filter, reset filter
- More than 500 millions of PCs with TPMs

http://trusted-computing.wikispaces.com/M+-+TPM+Chip+can+be+turned+off+Entirely

Trusted Computing Group

- Called Trusted Computing Platform Alliance until 2003
- Consortium of companies: Compaq, HP, IBM, Intel, Microsoft, AMD, etc.
- Designed a specification "for computing platforms that creates a foundation of trust for software processes, based on a small amount of hardware within such platforms".
- The cheapest way to enhance security in an ordinary, non-secure computing platform.
- PCs, servers, personal digital assistant (PDA), printer, or mobile phone can be converted to Trusted Platforms.

First trusted platforms : PCs

- to store secret keys to encrypt data files/messages, to sign data, etc.
- implement mechanisms and protocols to ensure that a platform has loaded its software properly.
- Have their own hardware and are independent from the operating system of the PC.

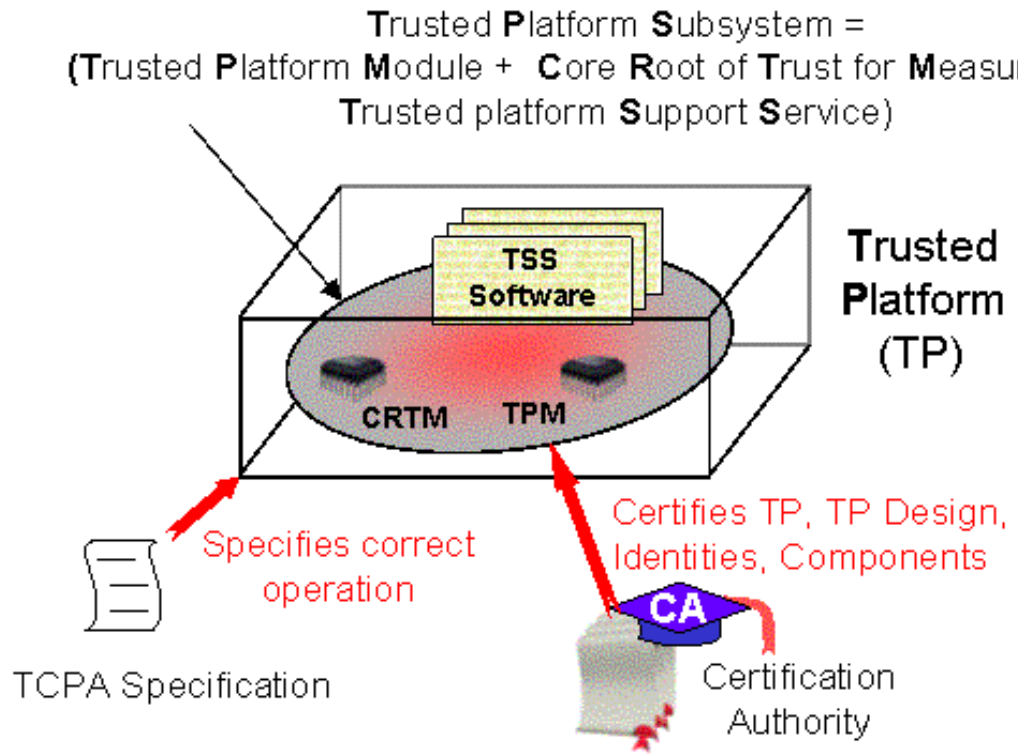
TPMs of Microsoft for PCs, Tablets

- Encryption of data files : Windows EFS (Encrypting File System), Virtual Encrypted Drive (Personal Secure Drive)
- Electronic mails with Outlook, Outlook Express that take into account digital signature, encryption/decryption of emails.
- VPN (Virtual Private Network), client authentication

Benefits

- Existing applications may benefit from enhanced security of the platforms
- Development of new applications that require higher security levels
- New applications: electronic cash, email, single sign-on, virtual private networks, Web access, and digital content delivery.

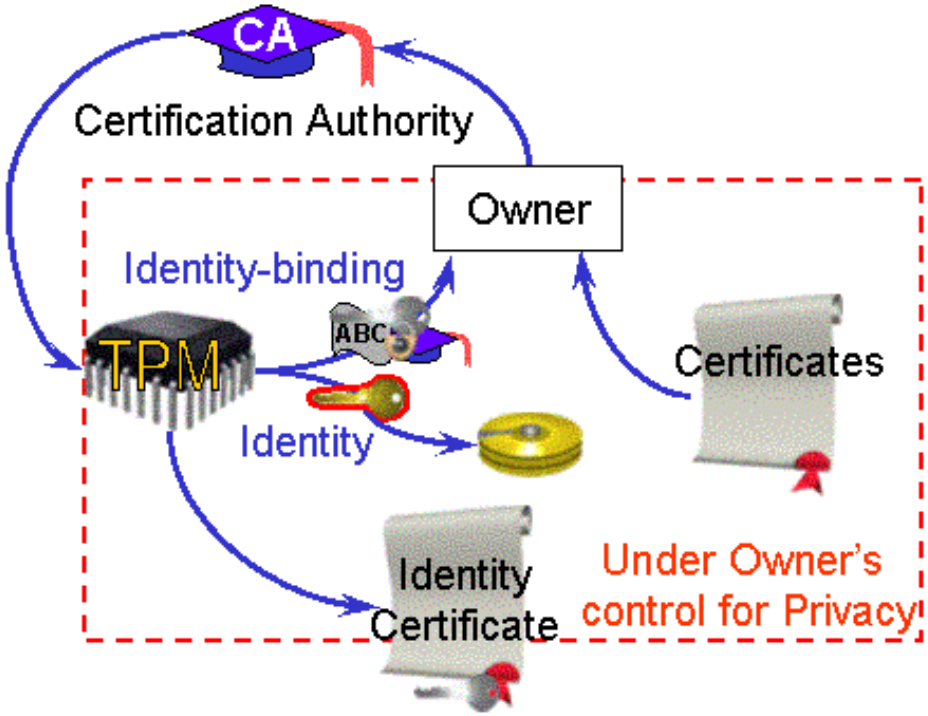
Trusted Platform Subsystem



TPM: chip
CRTM: boot process
TSS: services for
the platform and others

http://www.hpl.hp.com/techreports/2002/HPL-2002-221.pdf

Attestation Identity to prove TP authenticity

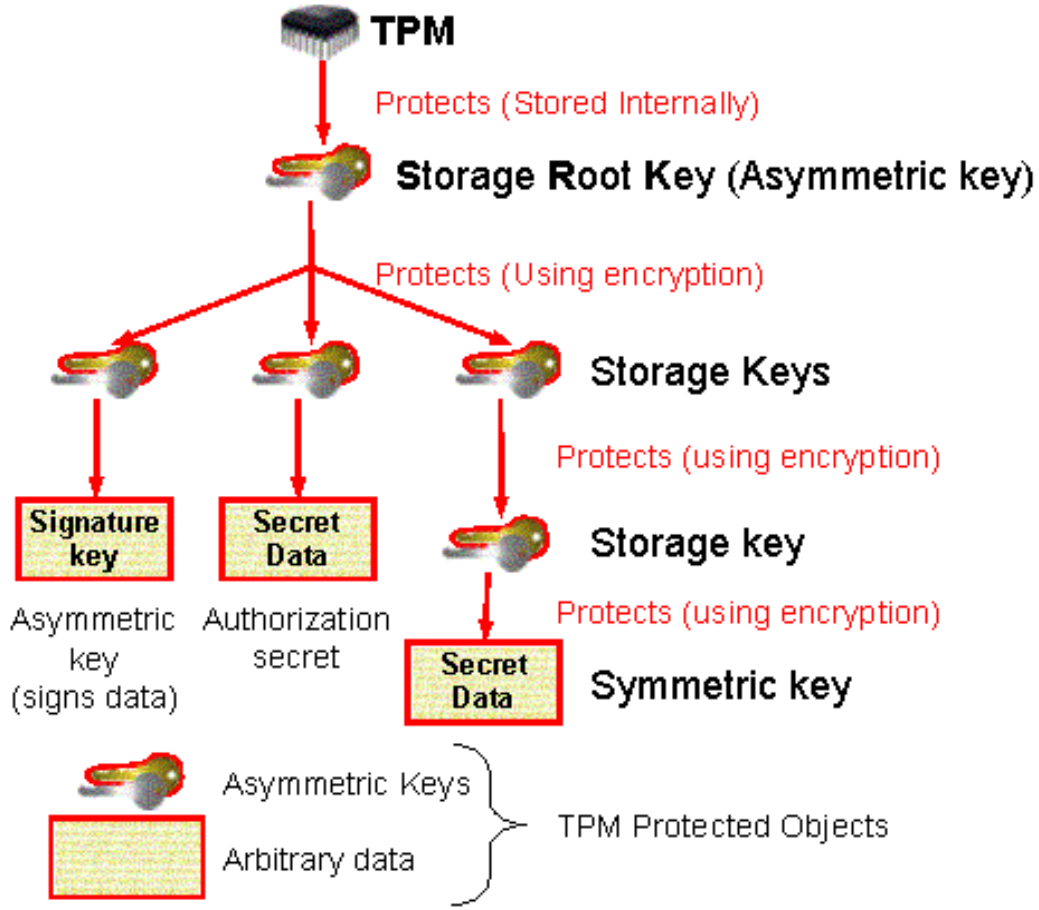


Identity created by the TP

Identity Attestation from the CA

http://www.hpl.hp.com/techreports/2002/HPL-2002-221.pdf

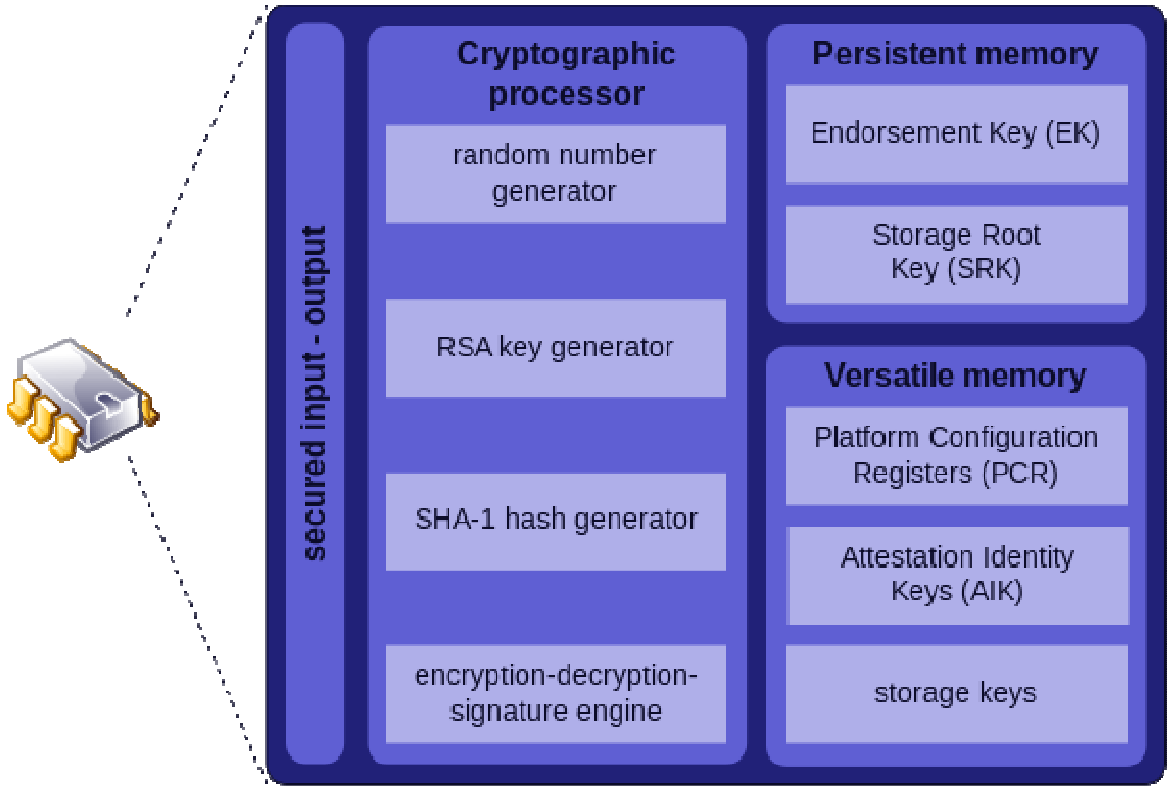
TPM protected objects



http://www.hpl.hp.com/techreports/2002/HPL-2002-221.pdf

Trusted Platform Module

"TPM chip" or "TPM Security Device"



http://en.wikipedia.org/wiki/Trusted_Platform_Module

Issues

- Privacy issue: security is delegated to the TPM, the user has no control on his data
- Each object is signed (what about the free software?)
- The TPM is a trust root that needs to interact with trust Cloud if any.

Mobile Trusted Module

- Mobile Phone Work Group has proposed a MTM
- Generally not implemented in mobile platforms
- Software trusted domains are proposed
  - As security domains of Global Platform
  - Attestation techniques to verify the integrity of the mobile

Our activities

- What is a Cloud of trust ?
- How to define a trust mobile using a piece of software and the SIM card instead of MTM?
- How to build a trust environment including mobile platforms and a cloud (mobiCloud computing) ?
- How to manage privay in this context ?

References

- ETSI Standard: http://www.etsi.org/
- EMV Standard: http://www.emvco.com/
- Trusted Computing Platforms, the Next Security Solution, http://www.hpl.hp.com/techreports/2002/HPL-2002-221.pdf
- Lecture notes of Samia Bouzefrane http://cedric.cnam.fr/~bouzefra/
- NFC forum: http://www.nfc-forum.org/home/
- Java Card forum: http://www.javacardforum.org/
- Global Platform: http://www.globalplatform.org/
- Oracle: www.oracle.com/
- TCG: http://www.trustedcomputinggroup.org/

Actions to promote SSO

Communauté SSO

- À l'échelle nationale:
  - créer une action CNRS
- A l'échelle internationale:
  - Un workshop international co-localisé avec IEEE iThings'2013

Action CNRS SSO

GDR ASR 2013-2016

- Pôle **Architectures Embarquées** dirigé par Claire Pagetti (ONERA) et Pierre Boulet (Université de Lille 1, LIFL)
- Pôle **Systèmes** dirigé par Jean-Marc Menaud (Ecole des Mines de Nantes) et Jean-Louis Pazat (IRISA)
- Pôle **Réseaux de Communication** dirigé par Eric Fleury (ENS Lyon) et André-Luc Beylot (IRIT/ENSEEIHT)
- Action **Cloud Computing** dirigée par Pierre Sens (LIP6) et Samir Tata (Institut Mines Telecom)
- Action **Secure Smart Objects** dirigée par Samia Bouzefrane (CNAM) et Maryline Laurent (Institut Mines Telecom)

Action CNRS “SSO”

- Objectifs
  - regrouper la communauté française travaillant sur cette thématique
  - renforcer et faire connaître ses activités
  - organiser des événements scientifiques comme des Conférences, des Écoles d’été, etc.
  - impliquer les entreprises

Journée NFC/SSO le 29 Mars

- Lien: http://www.sigops-france.fr/Main/Journee-NFC-SSO
- Organisateurs:
  - S. Bouzefrane & P. Paradinas (CNAM)
  - M. Laurent (Télécom SudParis)
  - P. Métivier (Forum des Services mobiles sans contact)
- Programme
  - Matin dédié au NFC:
    - 4 intervenants (Forum du Sans contact, Inside Secure, Orange Labs, Visa Europe)
  - Après-midi dédié au SSO:
    - Présentations par les entreprises et les universités

International Workshop on SSO

International Workshop SSO

- Lien: http://www.china-iot.net/Workshops/SSO.htm
- Workshop international sur SSO
  - Associé à la Conférence IEEE iThings
  - 19-23 Août 2013 à Beijing
  - Organisateurs:
    - S. Bouzefrane (CNAM), Jean-Louis Lanet (univ. Limoges), M. Laurent (Telecom SudParis), Li Li (Wuhan univ.)

Traités Hermès

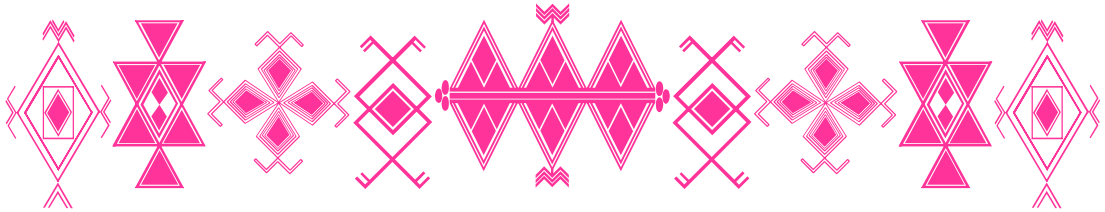
Traité Hermès “Carte à puce”

- Initié et coordonné par S. Bouzefrane & P. Paradinas
- Dédié à la carte à puce
- 12 chapitres
- 24 participants
- Parution en Avril 2013

Traité Hermès “gestion d’identités numériques”

- Initié et coordonné par S. Bouzefrane & M. Laurent
- Différents aspects de la gestion d’identités
- Ouverture vers le Cloud computing
- Parution en fin 2013

Thank you



samia.bouzefrane@cnam.fr