TÉCNICO LISBOA

03
Human-Infrastructure Interaction

Alberto Ramos da Cunha
alberto.cunha@ist.utl.pt

Plan

- Basic requirements for personal identification
- Smart cards as security elements
- Standards and interoperability frameworks
- Smarphones vs smart cards

- People work, live and enjoy cities
- The seamless flow of people to/from workplaces, to access services, and to entertainment and leisure activities is a feature of dense urban spaces
- Most technological developments of personal devices target urban communities

Basic requirements

- Identification

  Identity check in public services or to reserve services and control accesses, login in IT services or communities

- Access rights validation

  Verification of the rigths to access or use a service

- Payment

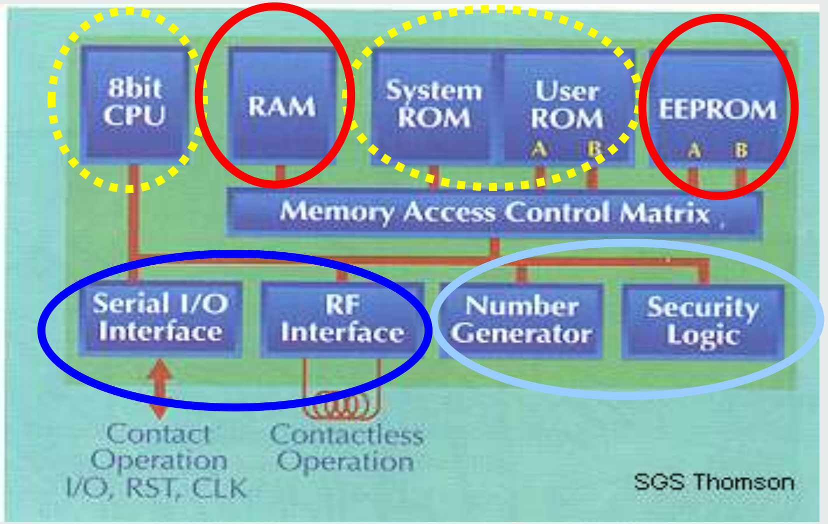
  Pay a service

- Non-functional requirements
  - Transaction speed
  - Security & Privacy
  - Autonomy

Main personal device technologies

- Smart cards and tags
- Smartphones

Main blocks of a chip card



▪ ▪ ▪ ▪ Functionality

━━ Memory

━━ Security

━━ Interface

Smart card interfaces

- Contact

  Mechanical connections

  Transaction time ≈ seconds

- Contacless

  Electromagnetic coupling

proximity	~ 60 cm	m
	magnetic induction	*radiofrequency*
passive cards	active cards	RF sensors
tags, stickers		

Transaction time ≈ mseconds

The smart card as a security element (1)

- The most important applications use smart cards as personal secure elements which are able to store reserved information and to check internally security keys
- The security properties are achieved by the electrical and logical construction of the card and by the deployment process
  - Electrical: Chip protection to reverse engineering
  - Logical: Memory hierarchy with strict access rules
  - Deployment process: Formal protocols to generate security keys involving the relevant organizations (manufacturer, managing organization, merchants, etc.)
- Small transaction time + strong security device ⇒ decentralized security

The smart card as a security element (2)

- Application examples
  - Government: ID card/citizen card, drivers license, passport
  - Banking: EMV for debit/credit cards
  - Telecommunications: SIM cards, pre-paid cards
  - Transportation: Calypso, Mifare cards with pre-paid and season tockets
  - Corporations: Identification and access control to premisses and facilities

Structure of commands

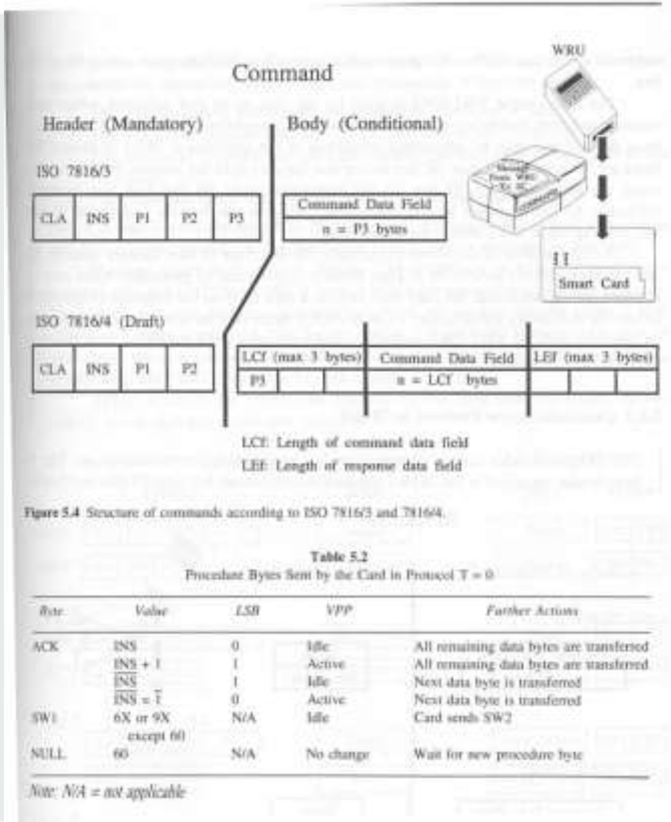


Figure 5.4 Structure of commands according to ISO 7816/3 and 7816/4.

Table 5.2
Procedure Bytes Sent by the Card in Protocol T = 0

Byte	*Value*	*LSB*	*VPP*	*Further Actions*
ACK	INS	0	Idle	All remaining data bytes are transferred
	INS + 1	1	Active	All remaining data bytes are transferred
	$\overline{\text{INS}}$	1	Idle	Next data byte is transferred
	$\overline{\text{INS}} = \overline{1}$	0	Active	Next data byte is transferred
SW1	6X or 9X except 60	N/A	Idle	Card sends SW2
NULL	60	N/A	No change	Wait for new procedure byte

Note: N/A = not applicable

© Smart Cards. José L. Zoreda, José M. Otón. Artech House, 1994.

Strict hierarchical memory structure (ISO 7816-4)

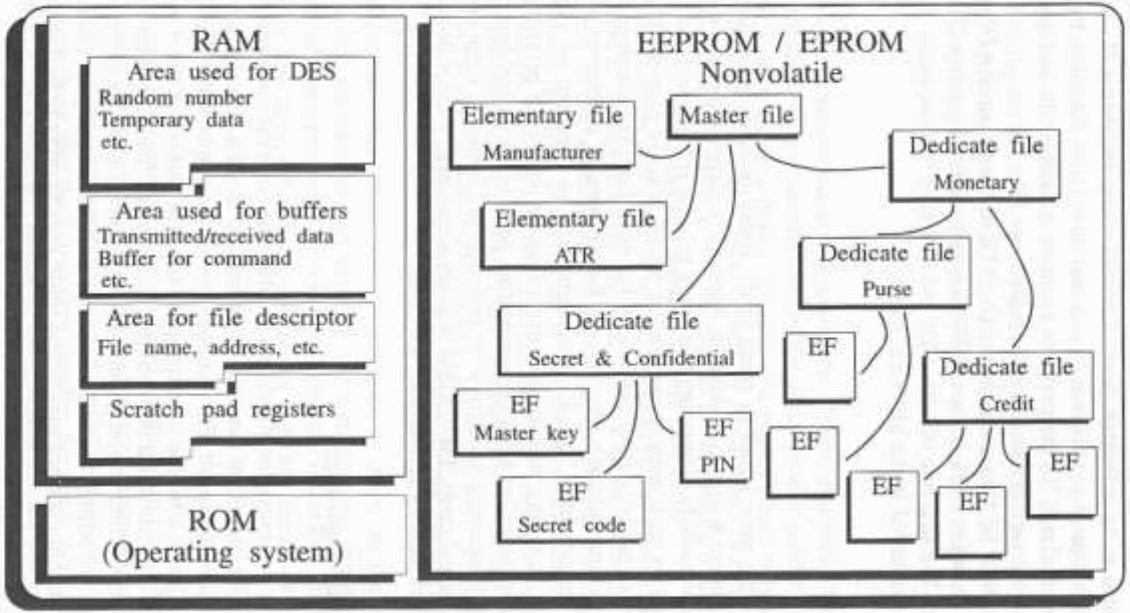
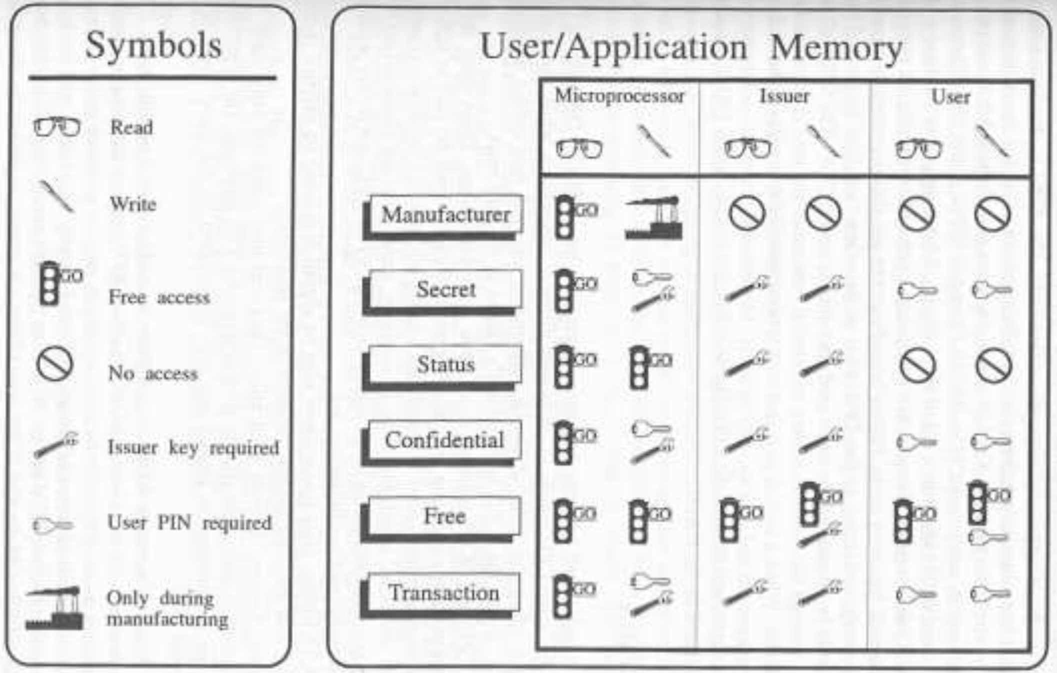


Figure 5.8 Hierarchical memory structure proposed by ISO 7816/4. ROM and RAM areas remain unmodified.

© Smart Cards. José L. Zoreda, José M. Otón. Artech House, 1994.

Mandatory access control to memory regions



Symbols

👓	Read
✎	Write
🚦	Free access
⊘	No access
⚷	Issuer key required
🔑	User PIN required
🏭	Only during manufacturing

User/Application Memory

	Microprocessor		Issuer		User	
	👓	✎	👓	✎	👓	✎
Manufacturer	🚦	🏭	⊘	⊘	⊘	⊘
Secret	🚦	🔑 ⚷	⚷	⚷	🔑	🔑
Status	🚦	🚦	⚷	⚷	⊘	⊘
Confidential	🚦	🔑 ⚷	⚷	⚷	🔑	🔑
Free	🚦	🚦	🚦	🚦 ⚷	🚦	🚦 🔑
Transaction	🚦	🔑 ⚷	⚷	⚷	🔑	🔑

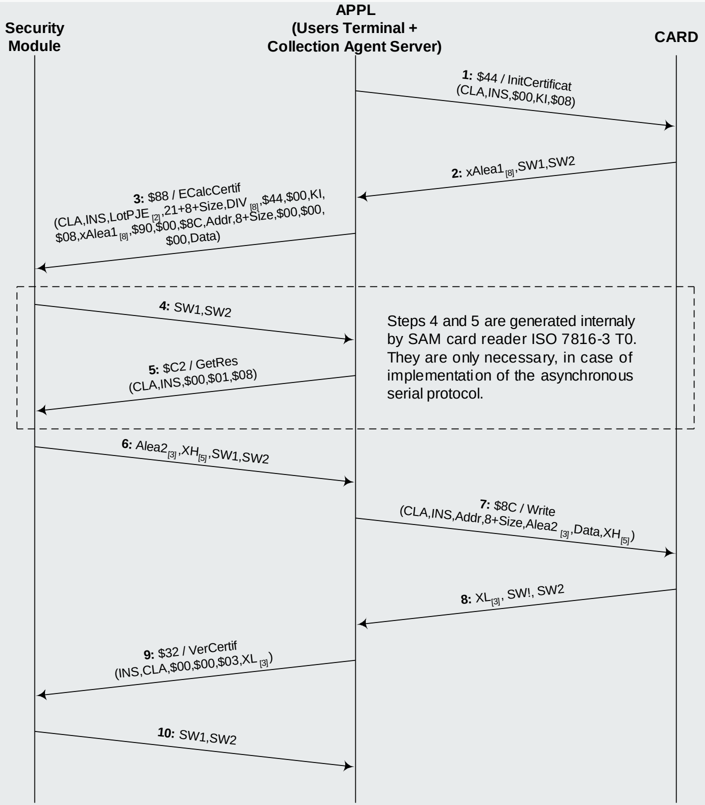
Figure 4.3 Typical zones of user/application memory.

© Smart Cards. José L. Zoreda, José M. Otón. Artech House, 1994.

Decentralised security
Mutual authentication

- Sometimes it is required the mutual authenticaton of the card and the terminal

- Terminal addresses the card
- Card replies and sends a piece of a certificate
- Terminal sends certificate to a Security Module (SAM – Security Application Module)
- SAM replies with the other part of the certificate
- Certificate is encapsulated in the message to write
- Mutual verification between card and terminal


Security Module
APPL (Users Terminal + Collection Agent Server)
CARD
1: $44 / InitCertificat (CLA,INS,$00,KI,$08)
2: xAlea1$_{[8]}$,SW1,SW2
3: $88 / ECalcCertif (CLA,INS,LotPJE$_{[2]}$,21+8+Size,DIV$_{[8]}$,$44,$00,KI, $08,xAlea1$_{[8]}$,$90,$00,$8C,Addr,8+Size,$00,$00, $00,Data)
4: SW1,SW2
5: $C2 / GetRes (CLA,INS,$00,$01,$08)
6: Alea2$_{[3]}$,XH$_{[5]}$,SW1,SW2
7: $8C / Write (CLA,INS,Addr,8+Size,Alea2$_{[3]}$,Data,XH$_{[5]}$)
8: XL$_{[3]}$, SW!, SW2
9: $32 / VerCertif (INS,CLA,$00,$00,$03,XL$_{[3]}$)
10: SW1,SW2

Steps 4 and 5 are generated internaly by SAM card reader ISO 7816-3 T0. They are only necessary, in case of implementation of the asynchronous serial protocol.

Smart card standards (1)

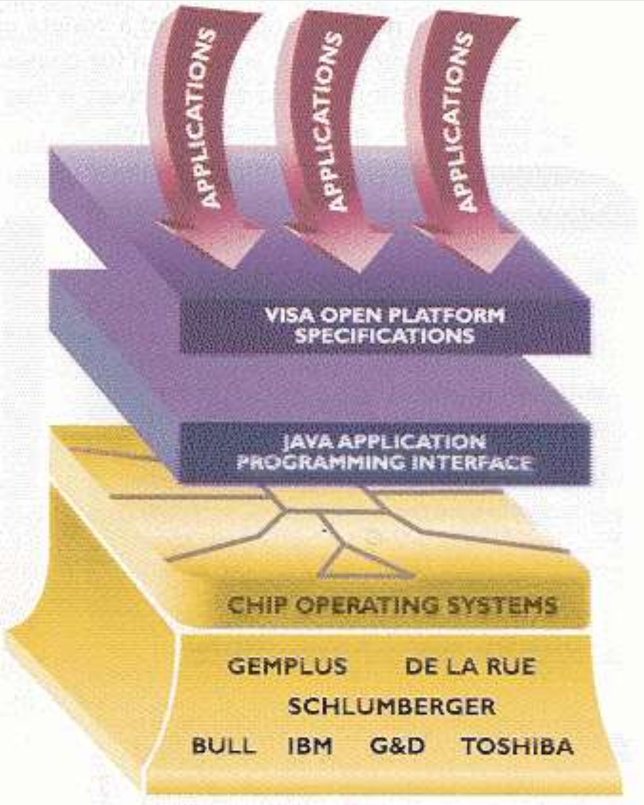
- Define levels of abstraction within the card

Application

Application interface (API)

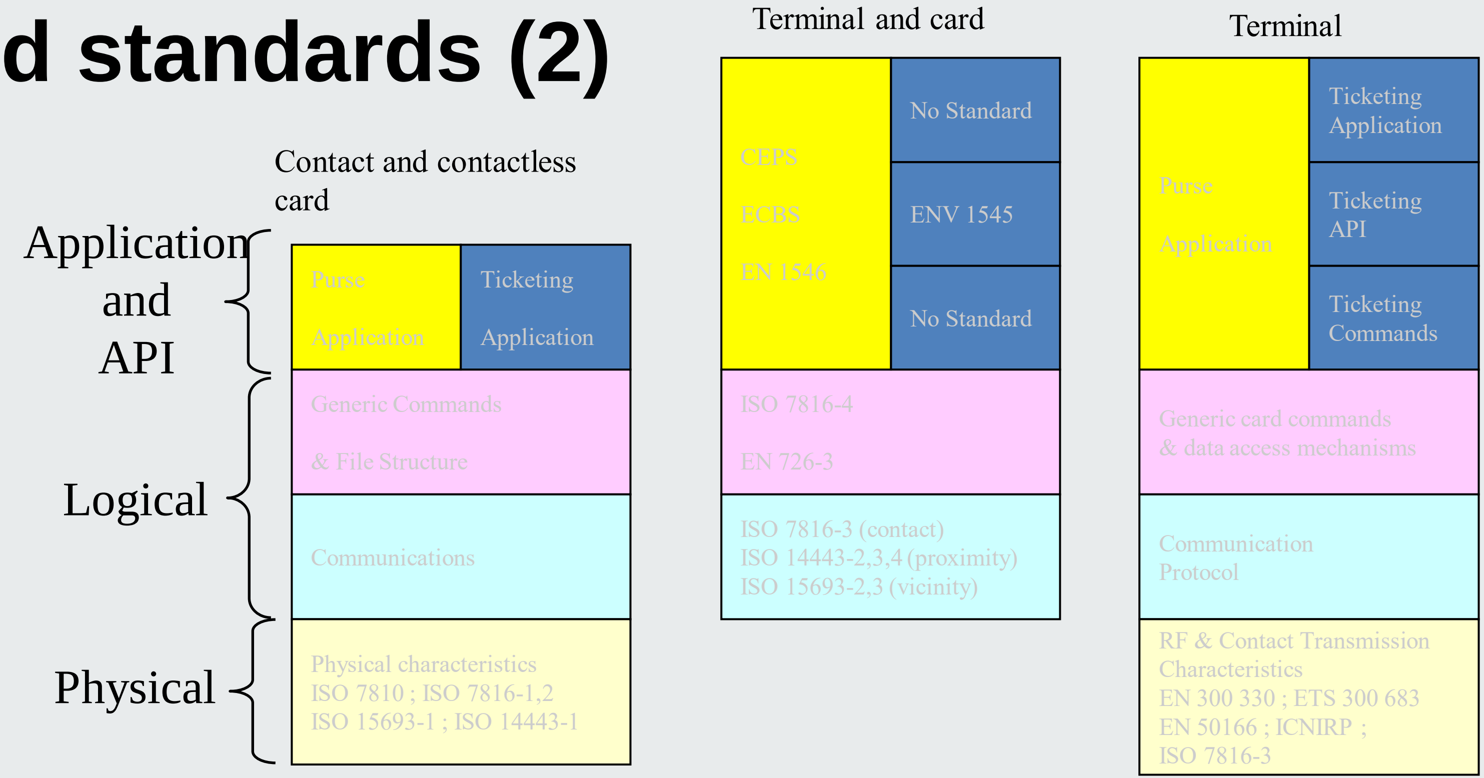
Logical

Physical



Smart card standards (2)

Define layers of abstration in the card and the terminals (e.g. Bank & Transports)



Application and API

Logical

Physical

Contact and contactless card

Purse Application

Ticketing Application

Generic Commands & File Structure

Communications

Physical characteristics
ISO 7810 ; ISO 7816-1,2
ISO 15693-1 ; ISO 14443-1

Terminal and card

CEPS
ECBS
EN 1546

No Standard

ENV 1545

No Standard

ISO 7816-4
EN 726-3

ISO 7816-3 (contact)
ISO 14443-2,3,4 (proximity)
ISO 15693-2,3 (vicinity)

Terminal

Purse Application

Ticketing Application

Ticketing API

Ticketing Commands

Generic card commands & data access mechanisms

Communication Protocol

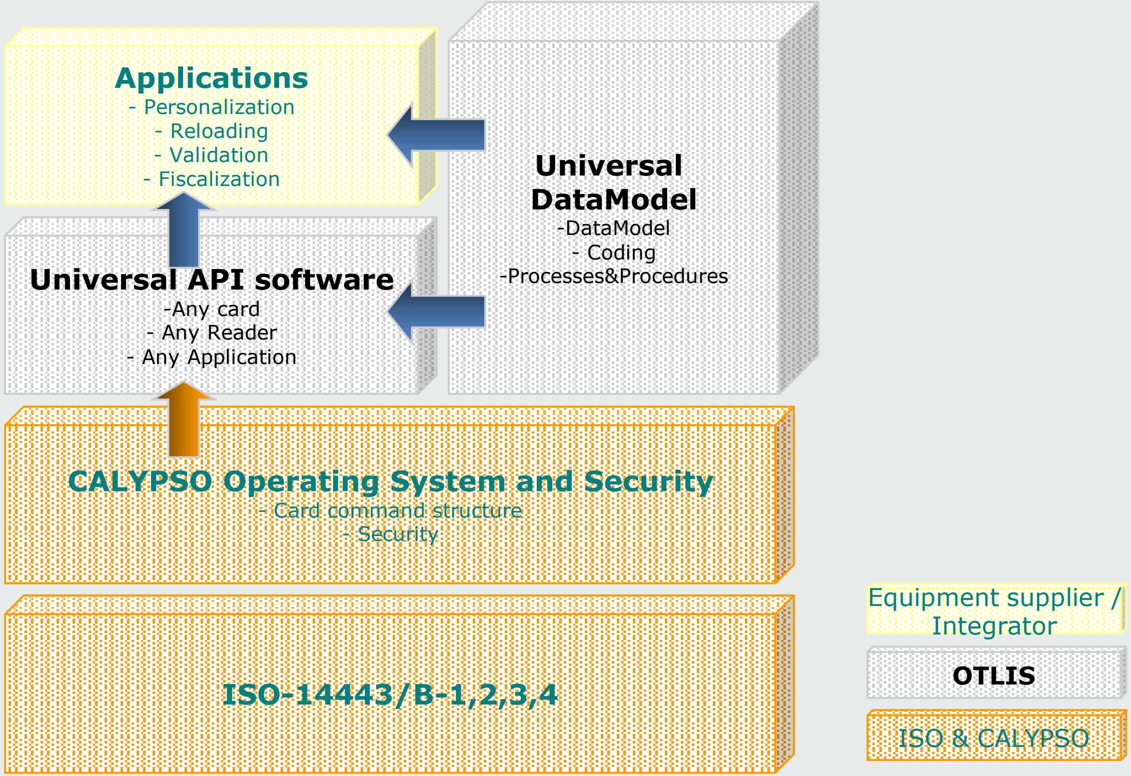
RF & Contact Transmission Characteristics
EN 300 330 ; ETS 300 683
EN 50166 ; ICNIRP ;
ISO 7816-3

Application level standards (Card and Terminal)

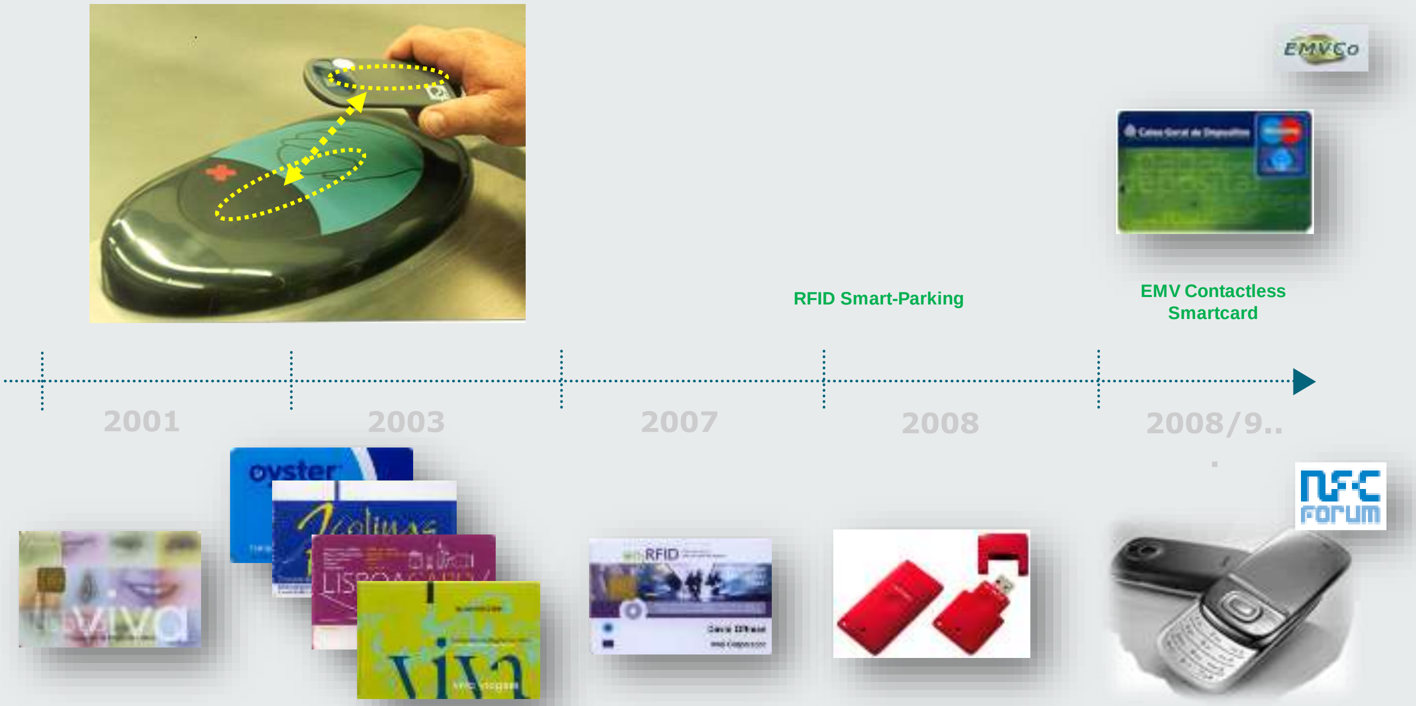
- Application
  - VisaCash, EN1546, ECBS-TCD, CEPS (e-purse)
  - Visa Smart Debit, Visa Smart Credit, EMV’96 (debit/credit)
- Terminal
  - OCF (OpenCard Framework) & PC/SC
  - Visa Open Platform (VisaCash, Visa Smart Credit, Visa Smart Debit, Java WORA™)

Interoperability frameworks

- Required to enable the smart card system to run across several service operators and with several technology providers
- Consider 3 layers
  - **Technology platform**: The card and its operating system standard (e. g. ISO & Calypso)
  - **Service level platform**: Common APIs and the data model of the federated service operators (e. g. OTLIS)
  - **Application level**



Evolution of RF/ID Portable Devices



2001

2003

2007

2008

2008/9..

RFID Smart-Parking

EMV Contactless Smartcard

Contactless Microprocessor Smartcard

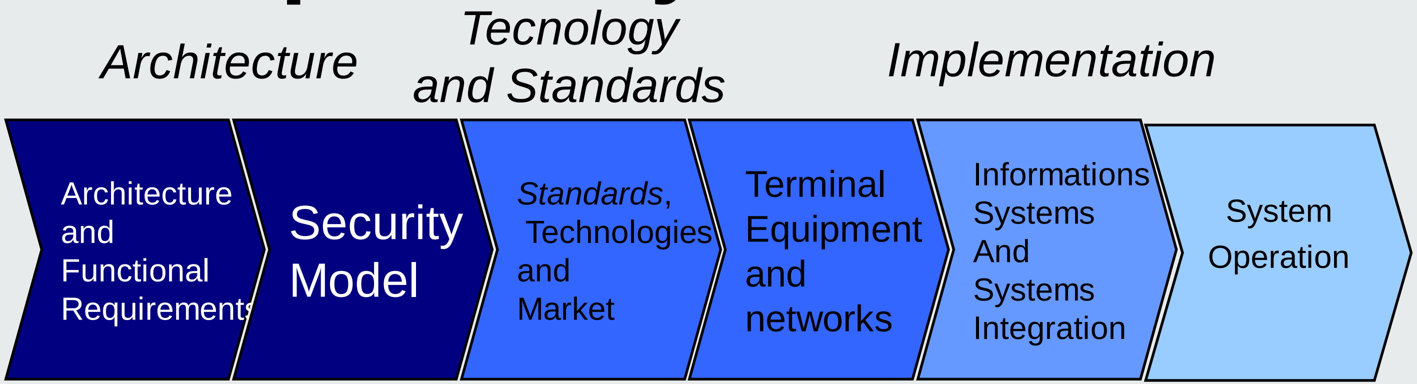
Contactless Paper Smart-ticket & Memory Card

Contactless Multi-application Smartcard

RFID USB Smart-Token

NFC Mobile Phone

Development cycle



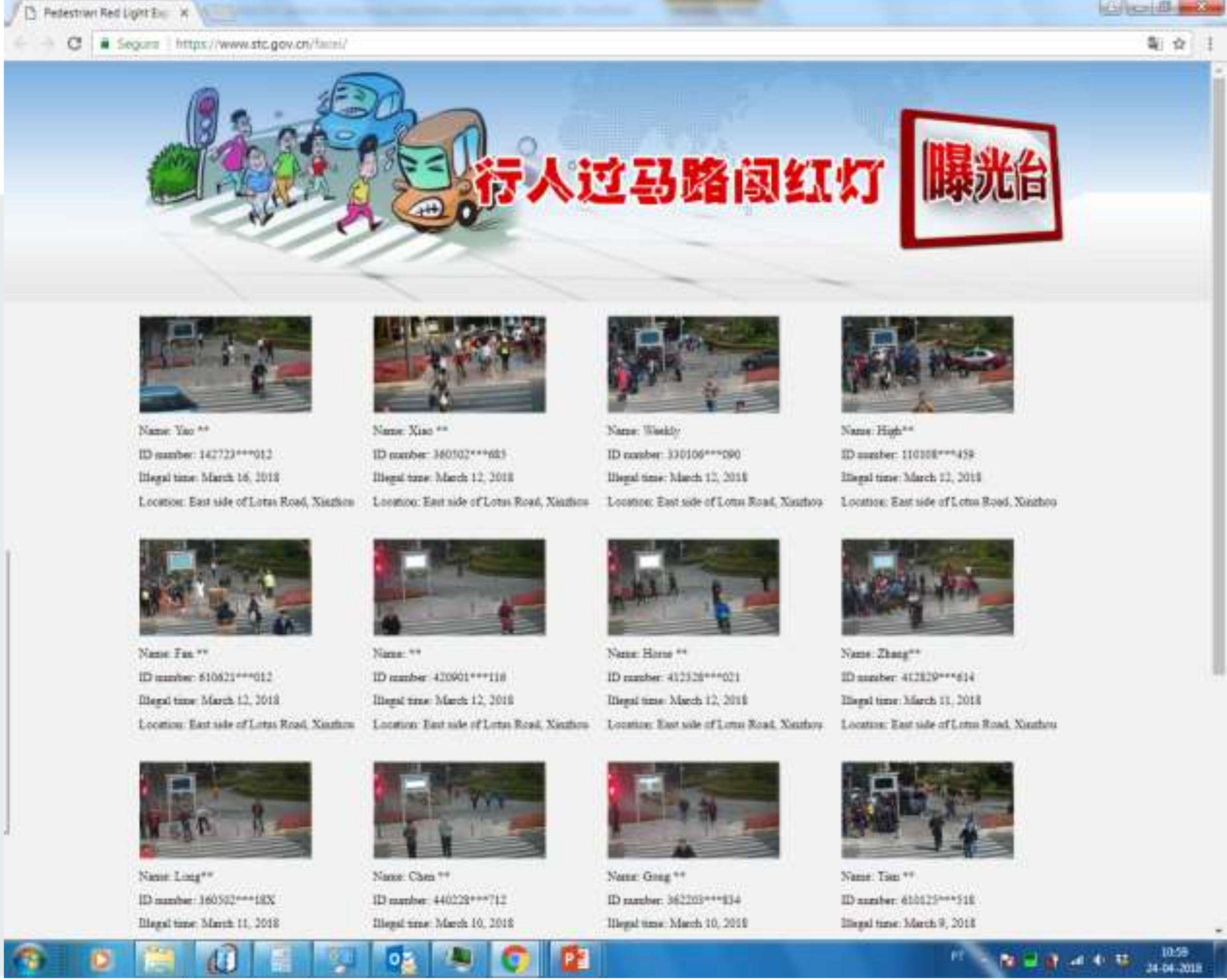
Architecture
Tecnology and Standards
Implementation
Architecture and Functional Requirements
Security Model
Standards, Technologies and Market
Terminal Equipment and networks
Informations Systems And Systems Integration
System Operation

Why smartphones are being slow to replace cards in these smart cities applications?

- Compared to smart cards smartphones are full fledged computers
- But they do not provide a security element comparable to the smart card
  - SIM card distribution is controlled by telecommunications operators which take advantage to control the provision of services over their networks
  - That is the same reason why there not so many cross sectorial application of cards (banks + telcos, telcos + transports, etc.)
- Perhaps wait for more devices with dual chip capability, or for service operators to value user convenience vs risk

Or no cards, no smartphones, just image processing

- Shenzhen traffic police webpage
  (24 April 2018, translated by Google, non accessible in 2021)



Name: Yao **
ID number: 142723***012
Illegal time: March 16, 2018
Location: East side of Lotus Road, Xinzhou

Name: Xiao **
ID number: 360502***683
Illegal time: March 12, 2018
Location: East side of Lotus Road, Xinzhou

Name: Weekly
ID number: 330106***090
Illegal time: March 12, 2018
Location: East side of Lotus Road, Xinzhou

Name: High**
ID number: 110108***459
Illegal time: March 12, 2018
Location: East side of Lotus Road, Xinzhou

Name: Fan **
ID number: 610621***012
Illegal time: March 12, 2018
Location: East side of Lotus Road, Xinzhou

Name: **
ID number: 420901***118
Illegal time: March 12, 2018
Location: East side of Lotus Road, Xinzhou

Name: Horse **
ID number: 412328***021
Illegal time: March 12, 2018
Location: East side of Lotus Road, Xinzhou

Name: Zhang**
ID number: 412829***614
Illegal time: March 11, 2018
Location: East side of Lotus Road, Xinzhou

Name: Long**
ID number: 360502***18X
Illegal time: March 11, 2018

Name: Chen **
ID number: 440228***712
Illegal time: March 10, 2018

Name: Gong **
ID number: 362203***834
Illegal time: March 10, 2018

Name: Tan **
ID number: 610125***518
Illegal time: March 9, 2018

For next lecture

- Imagine how traffic/mobility (vehicle and people flows) can/will be managed in the future