Advanced Card Systems Ltd.
Card & Reader Technologies

Smart Card Technical Introduction

CARD & READER TECHNOLOGIES

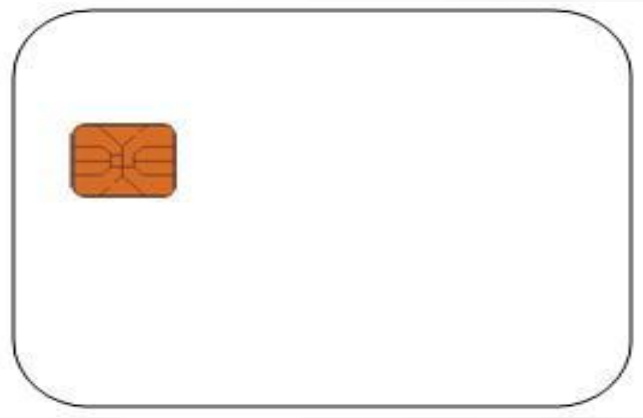
Contents

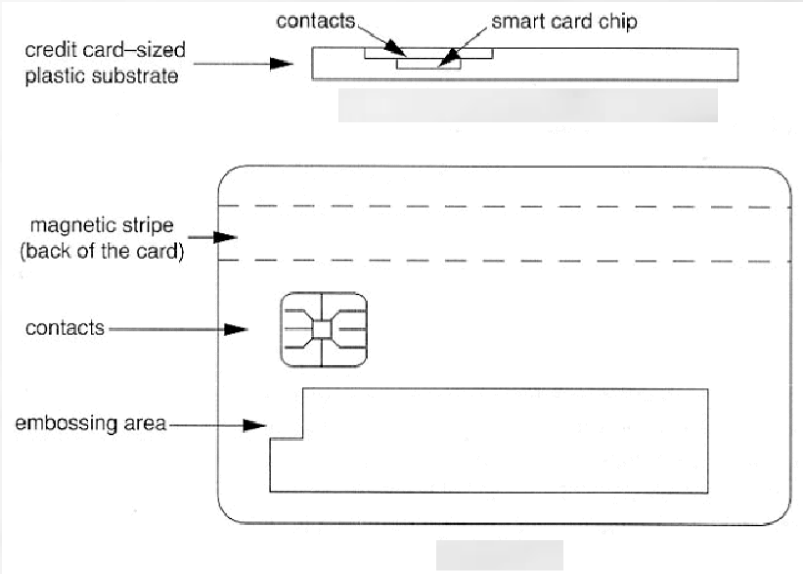
Advanced Card Systems Ltd.
Card & Reader Technologies

Contact Smart Card

CARD & READER TECHNOLOGIES

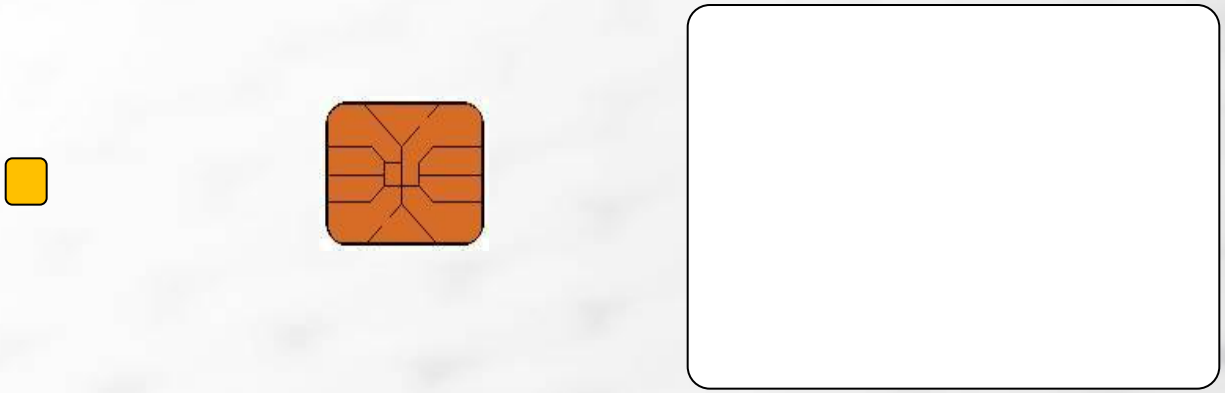
What is a Smart Card?





- A credit card sized (ID-1) plastic card with an IC chip on board
- Conforms to ISO-7816

Components of a Contact Smart Card

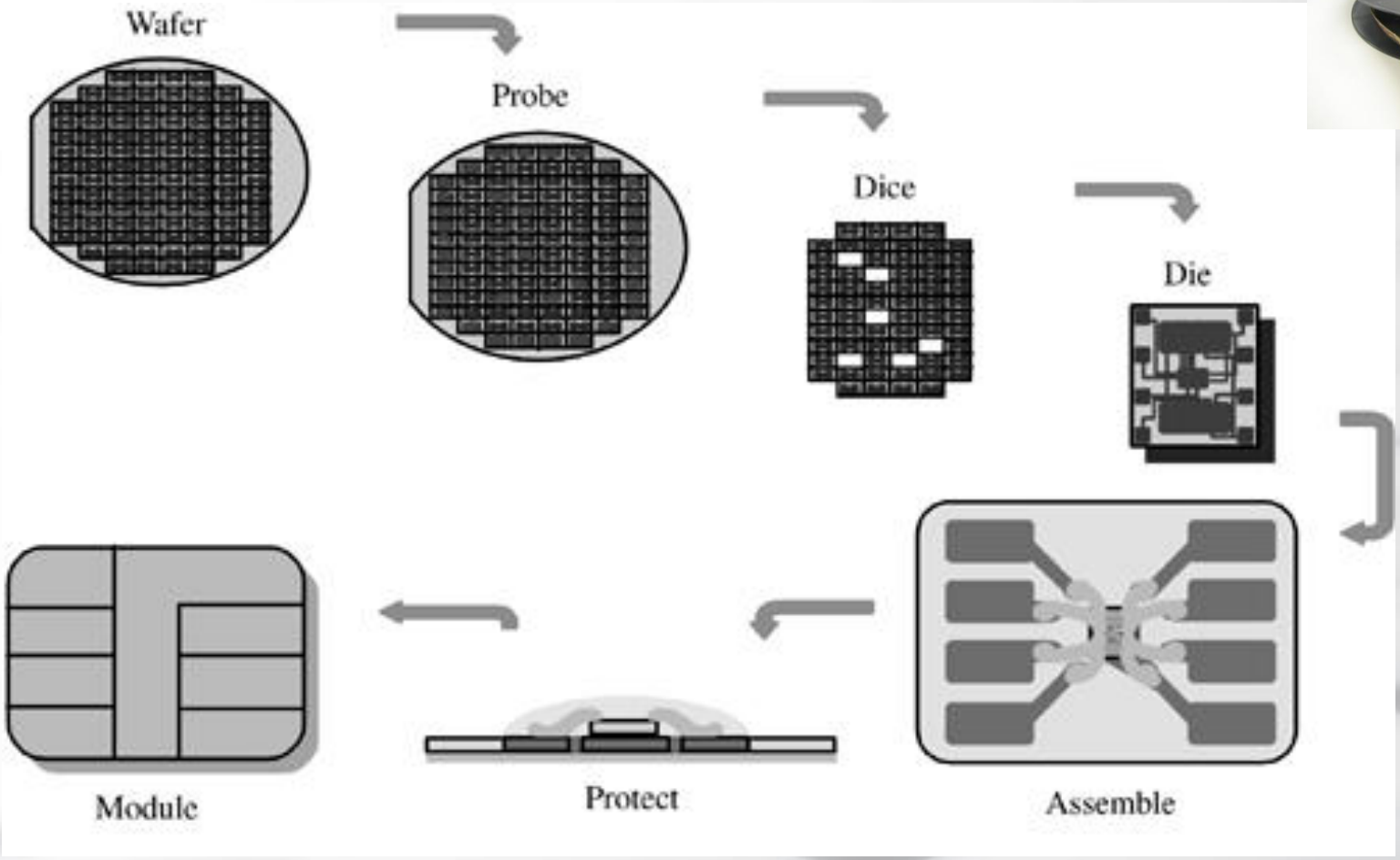


- **A smart card comprises 3 parts**
  - Contact Disc
  - Chip
  - Plastic Body with Cavity

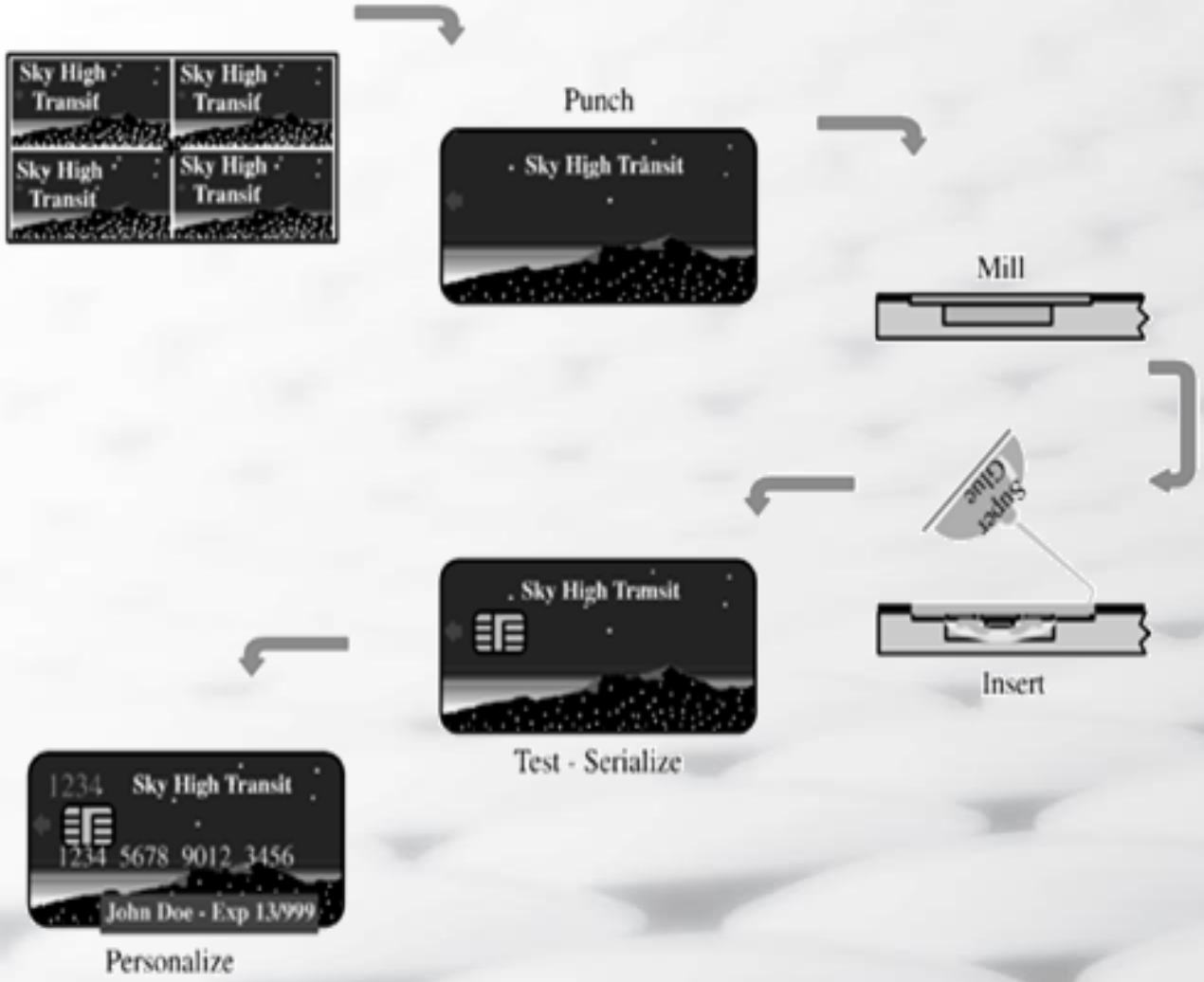
Contact Disc

- A contact disc with a chip is called a **micro-module**
  - Usually composed of 6 or 8 contacts
    - 6 contacts – usually for memory cards & low end CPU cards
- Module
  - Usually square or oval
  - Can have different patterns defining the contacts
  - Contact position complies with **ISO-7816-2**
- The Answer-To-Reset value will indicate if it is a CPU card
  - Cannot visually tell the card type based on the contact disc

Micro-Module Manufacturing



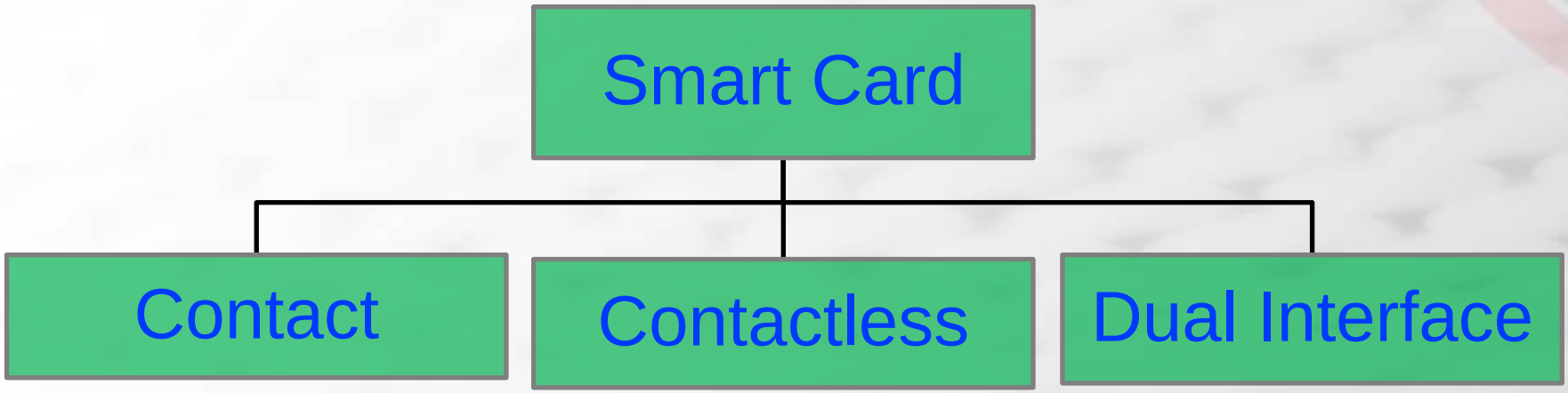
Card Manufacturing



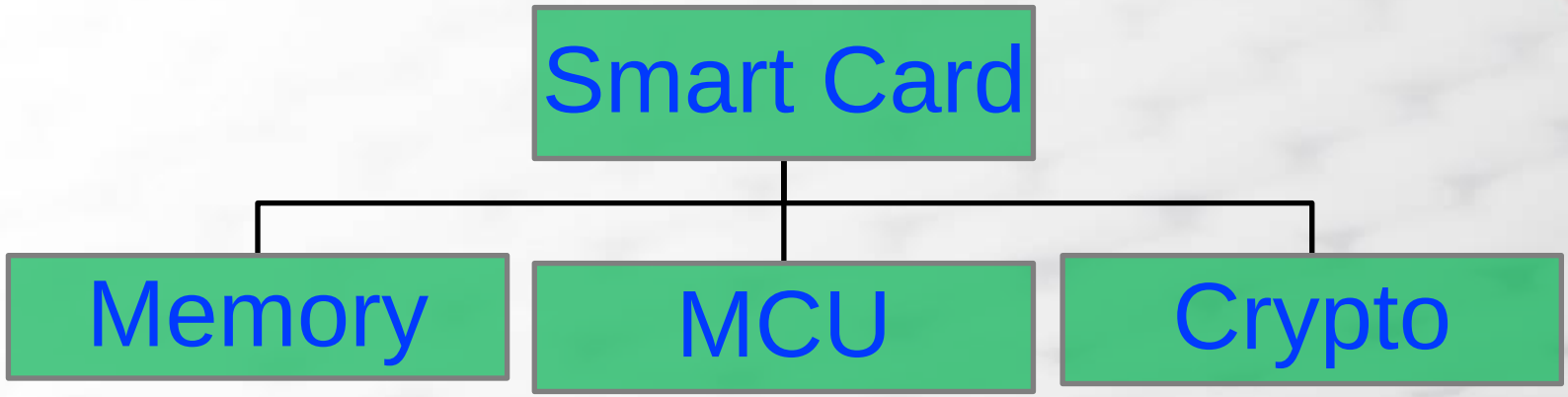
Smart Card IC Family

- Contact Memory Card
  - Infineon, Atmel, ISSI (Infineon/Atmel compatibles)
- Contact CPU Card
  - GSM SIM, Smart Debit/Credit EMV Card
  - National smart card (banking / ID card)
- Dual Interface CPU Card

Category by Technology



Category by Security

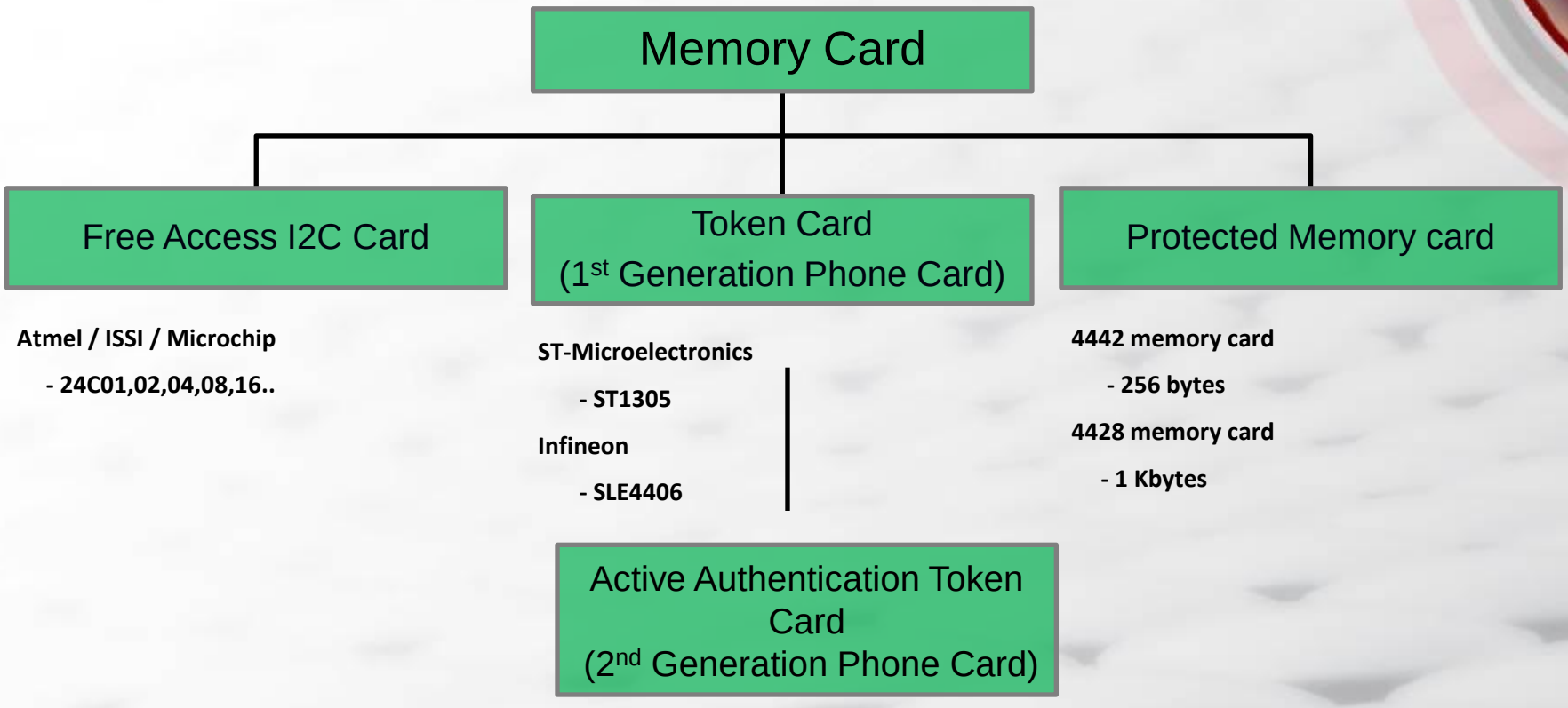


- Payphone
- Proprietary applications

- GSM-GSM11.11
- Banking - EMV
- Proprietary applications

- E-Identification
- E-commerce
- M-commerce
- GSM11.11,11.14

Types of Contact Memory Cards



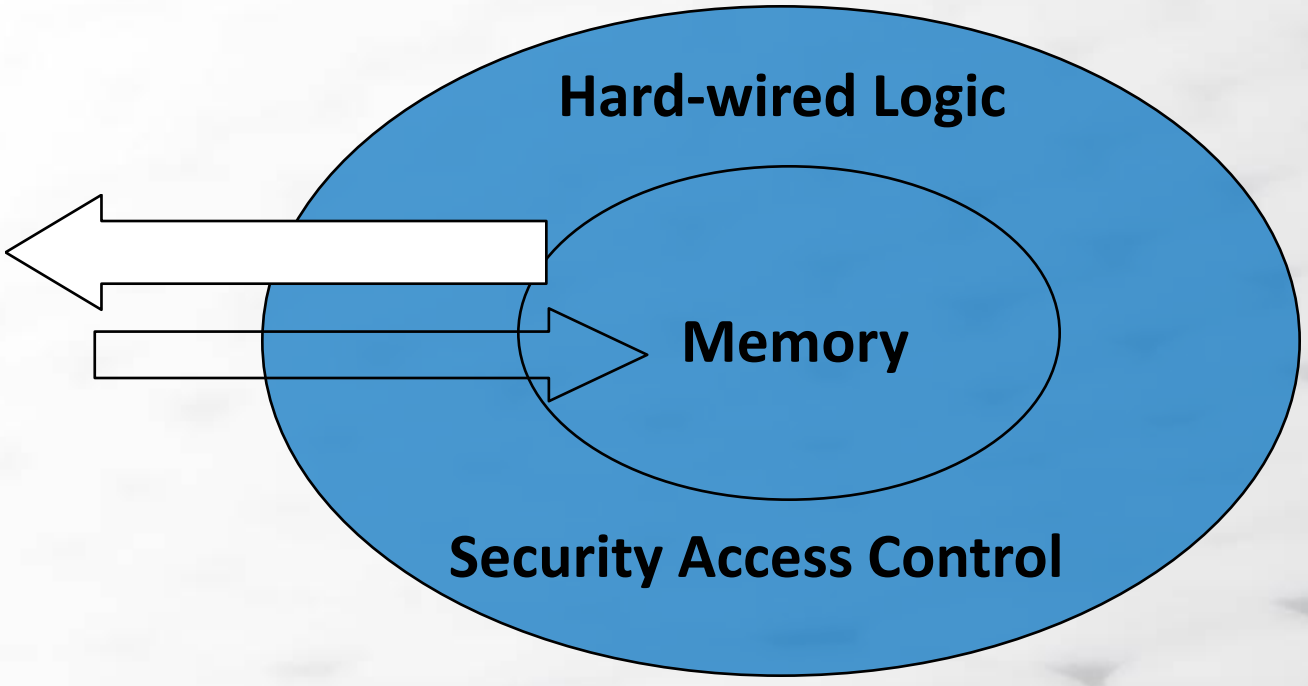
Contact Card Chip

Memory	MCU
Chip Manufacturers • Atmel • Infineon • Infineon compatibles	Chip Manufacturers • ST Microelectronics • Atmel • Renesas • Infineon • NXP • Samsung
Card Manufacturers embed the chip in card	Card manufacturers must design the chip operating system There are also COS vendors

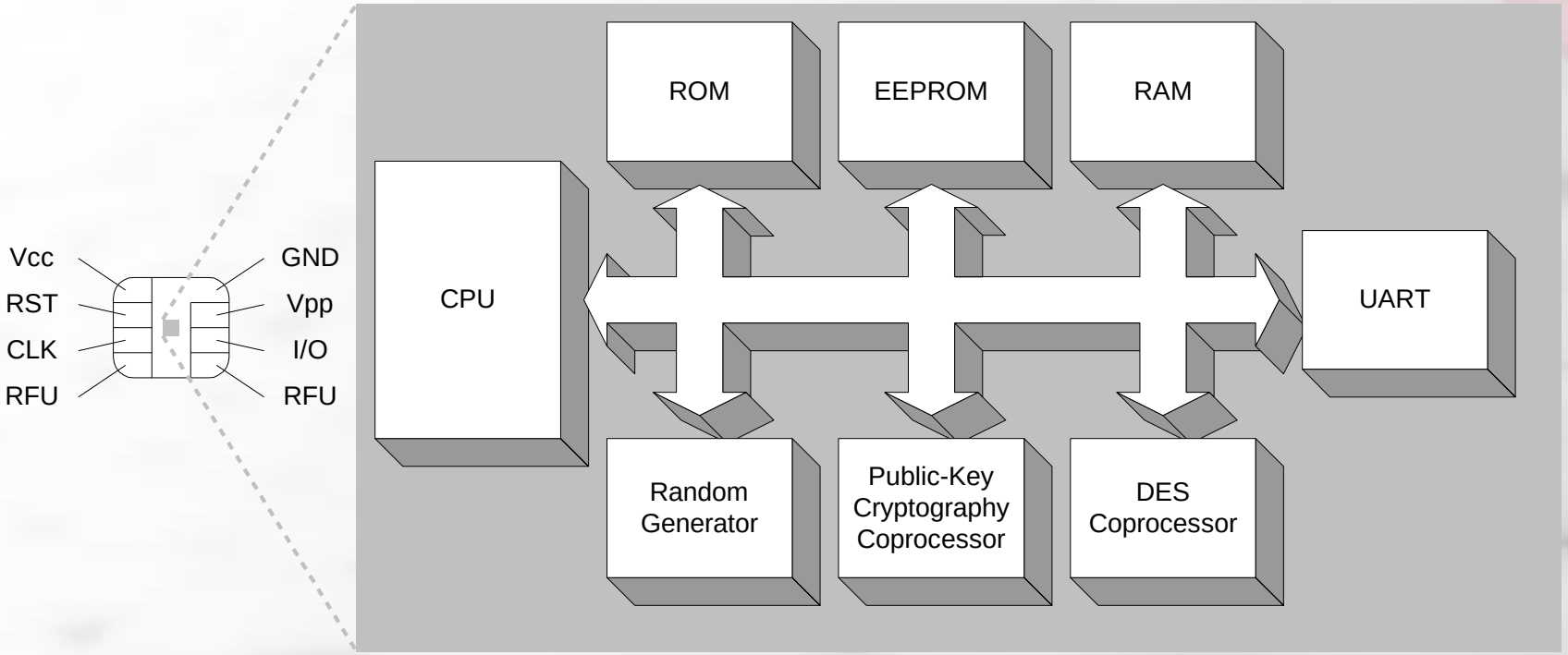
Plastic Card Body

Material	Advantage	Disadvantage	Usage
PVC	- Allows metallic color printing, hot stamping, embossing and adding magnetic stripe	- Cannot withstand high temperature (e.g. temperature inside a car), hence not suitable for parking & tolling applications	- Banking card - Loyalty card
High temp. PVC	- Can withstand high temperature		- GSM SIM card *(requires the card to be able to withstand up to 85℃)*
ABS	- Commonly used for GSM SIM cards & telephone prepaid cards.	- Cannot allow addition of magnetic stripe, hot stamping, metallic color printing and embossing	- GSM SIM card -Telephone prepaid card
PET	- Can withstand high temperature	- More expensive than PVC (about $0.05 to $0.10)	- Parking and tolling card, National ID card, Passport, Driver's license
PC	- Can withstand high temperature - Highly durable and light weight - Stronger than PVC cards	- Expensive	- National ID card, Passport, Driver's license

Memory Card Security Architecture



CPU Card Architecture



Smart Card Memory Capacity

- Memory size is described in bits / bytes
- Memory size refers to the application memory
  - **EEPROM** - erasable, if authorized
- Memory card storage: 104 bits to 16 Kbits
- CPU card - 8bits/16 bits, 8051 or 6805 core
  - **ROM** - 6Kbytes to a few hundred Kbytes
  - **RAM** - 100 bytes to a few Kbytes
  - **EEPROM** - 512 bytes to 1 Mbyte
  - **Flash CPU card is also available**

Smart Card Standard – ISO 7816

- **Part 1: Physical Characteristics**
- **Part 2: Dimensions & Locations of Contacts**
- **Part 3: Electronic Signals & Transmission Protocol**
- **Part 4: Inter-industry Command for Interchange**
- Part 5: Numbering System & Registration Procedure for Application Identifiers
- Part 6: Inter-industry Data Elements
- Part 7: Inter-industry Structured Card SQL
- Part 8: Security Related Security Commands

Smart Card Standard – ISO 7816

- Part 9: Additional Inter-industry Commands & Security Attributes
- Part 10: Electronic Signals & ATR for Synchronous Card
- Part 11: Personal Verification through Biometrics Method
- Part 12: USB Electrical Interface and Operating Procedure
- Part 13: Cards for Application Management in a multi-application environment
- Part 15: Cryptographic Information Application

ISO-7816 Part 1: Physical Characteristics

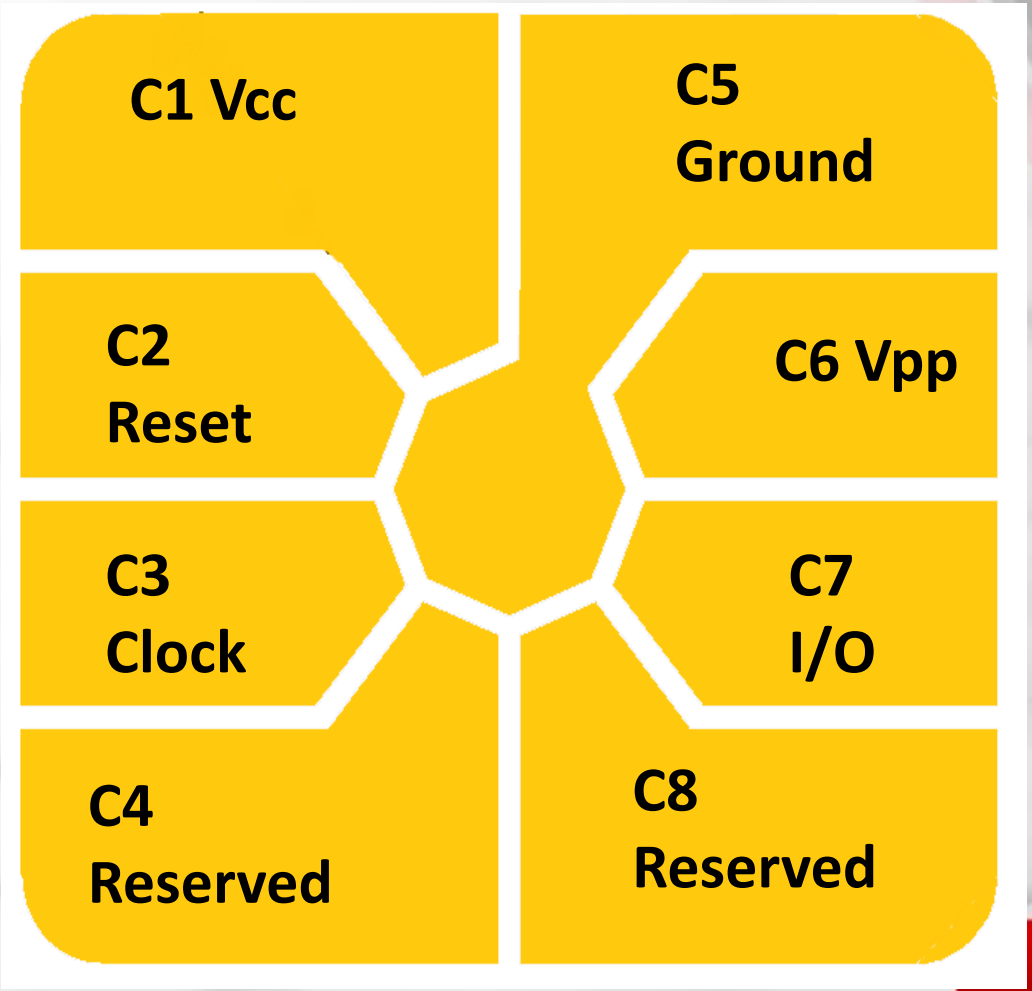
- UV light
- X-ray
- Contacts Surface Profile
- ESD
- Torsion
- Heat dissipation
- Bending
- Mechanical strength of card, contacts
- EMI

ISO-7816 Part 2

Class A = 5V

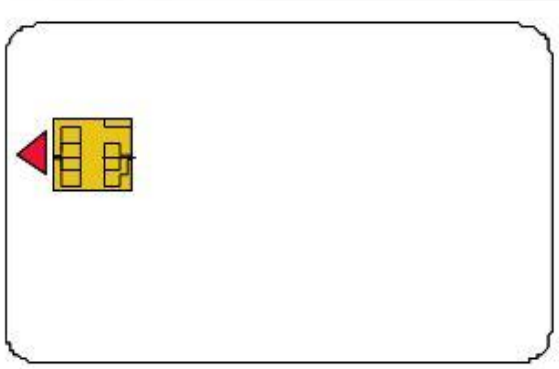
Class B = 3V

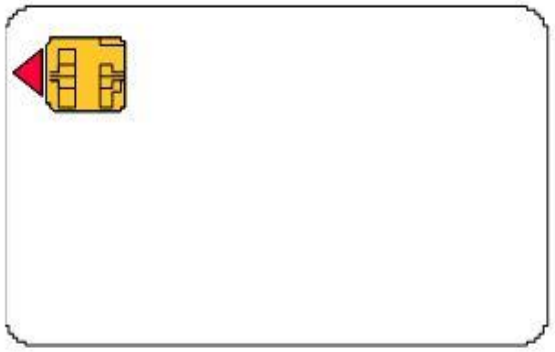
Class C = 1.8V



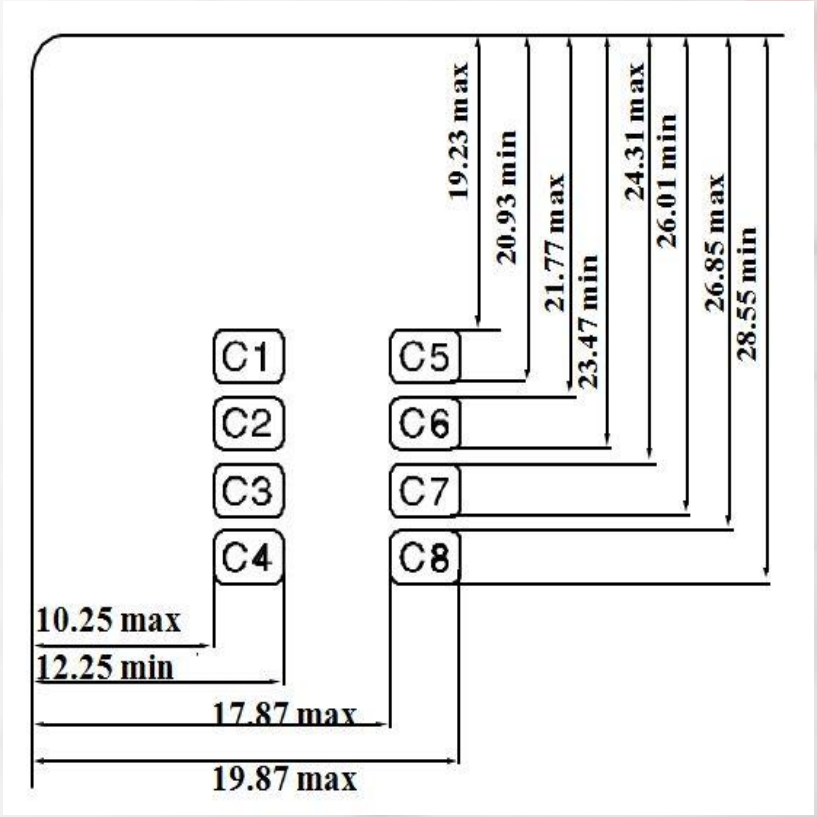
ISO-7816 Part 2: Location & Assignment of Contacts

ISO POSITION

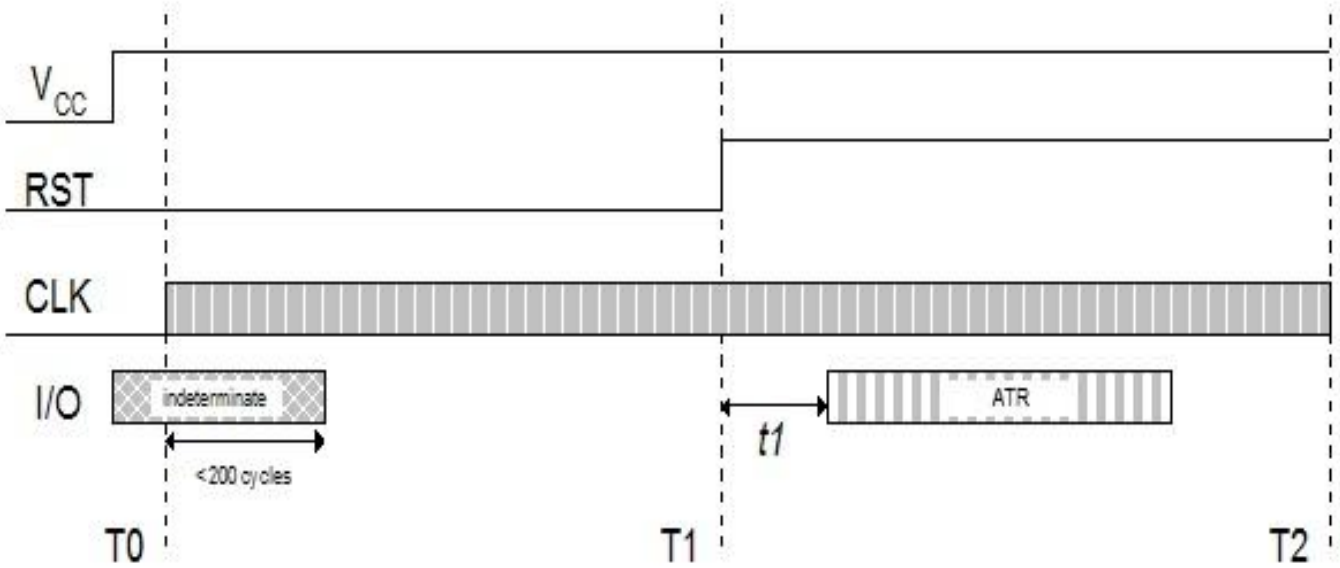




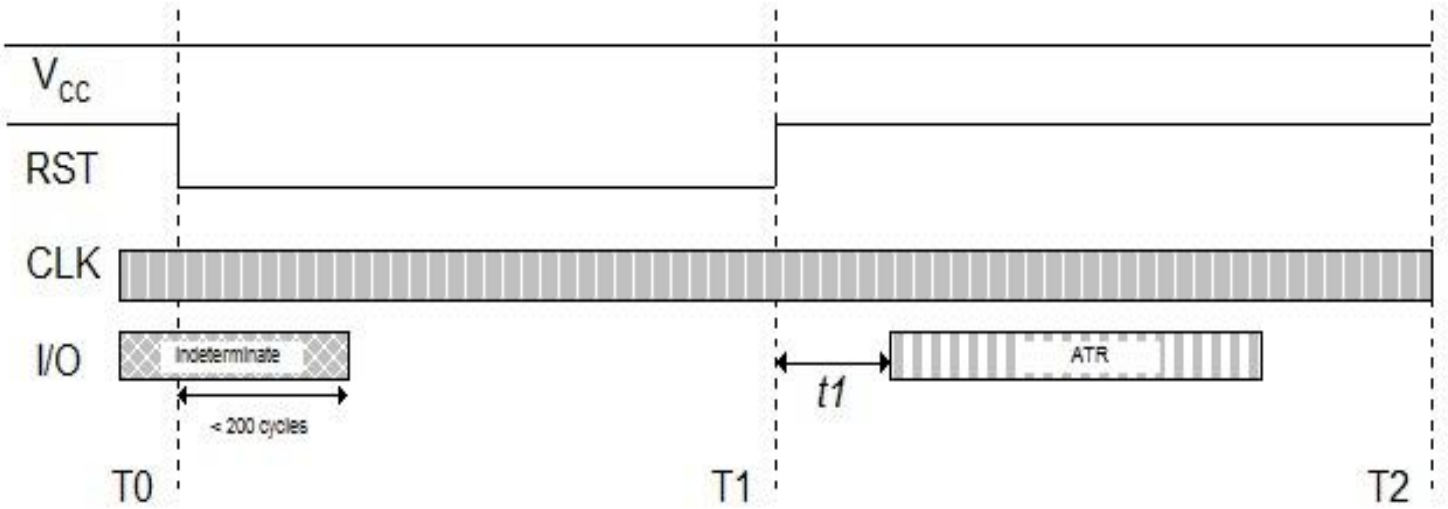
AFNOR POSITION



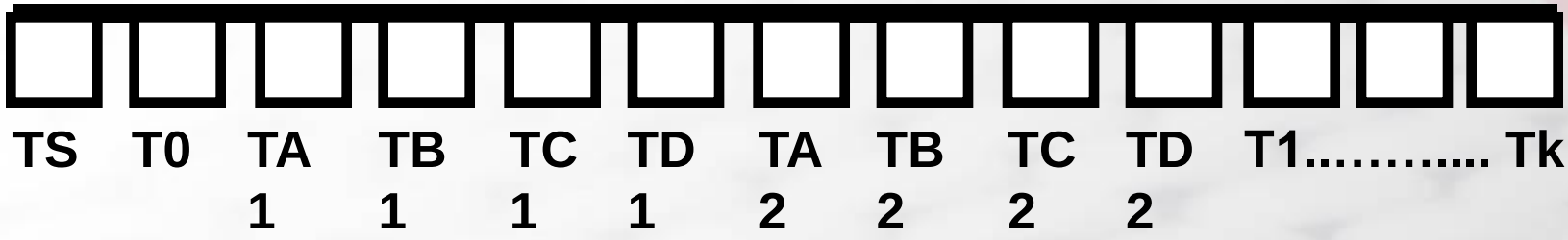
ISO-7816 Part 3: Cold Reset



ISO-7816 Part 3: Warm Reset



ISO-7816 Part 3: Answer to Reset



TS = Initial Character
T0 = Format Character Y1,K
TA1 = FI,DI
TB1 = II,PI1
TC1 = N
TD1 = Y2, T

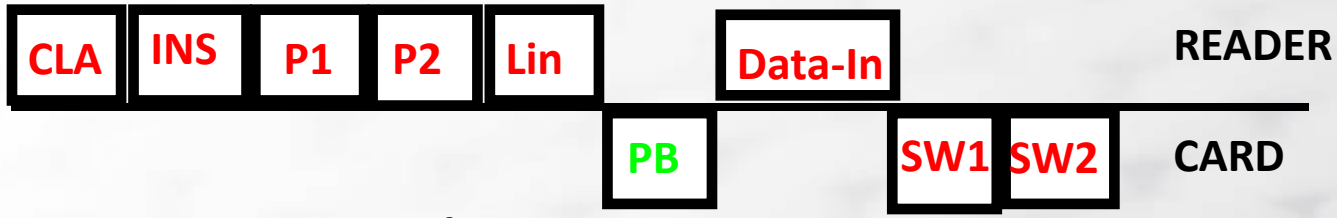
TA2 = Specific Mode
TB2 = PI2
TC2 = Specific
TD2 = Y3, T
TD2 = Y3,T
T1..Tk = Historical Characters

ISO-7816 Part 3

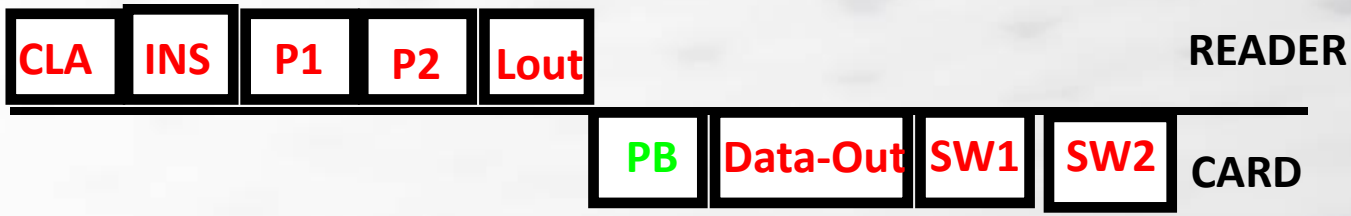
- **T=1(Block Protocol)**
  - TBi(i>2) BWI,CWI
  - BWI = Block Waiting Integer
  - CWI = Character Waiting Integer
- **T=15 (Additional Global Interface Bytes)**
  - TAi(i>2) = SI,CI
  - SI = Sleep Mode Indicator
  - CI = Class A (5V), Class B (3V), Class AB

ISO-7816 Part 3: T=0 TPDU

ISO-IN Command



ISO-OUT Command

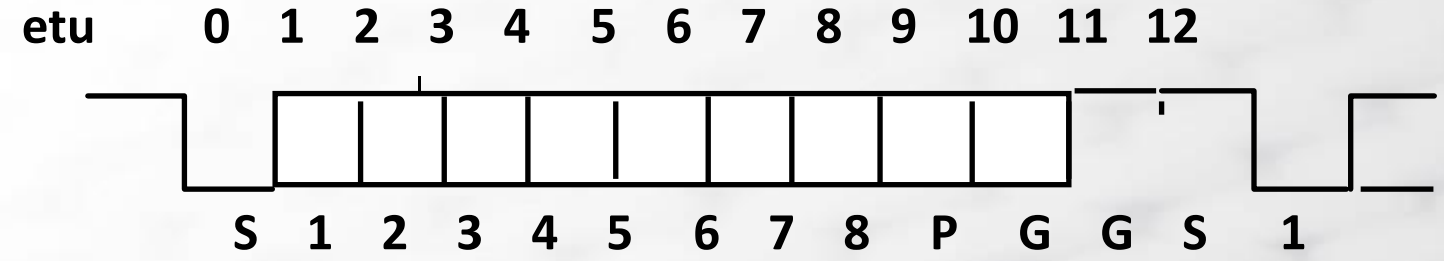


PB = INS : Send me next byte

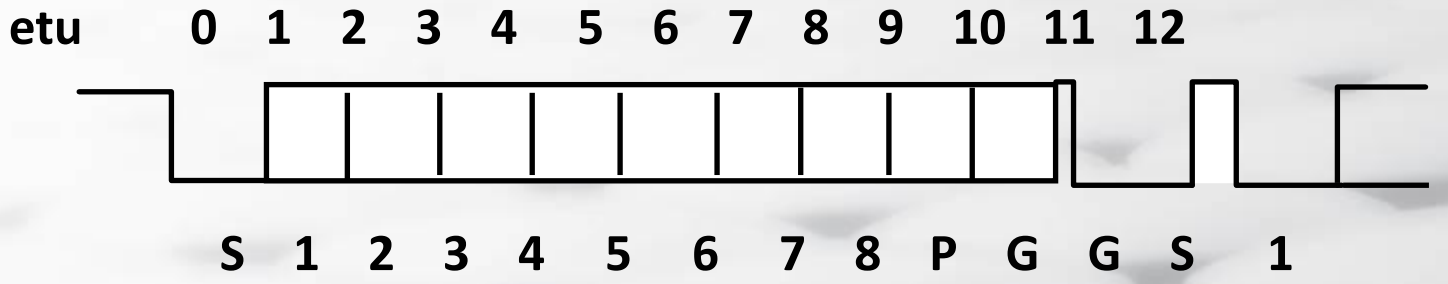
PB = INS : Send me all bytes

ISO-7816 Part 3: Transmitting a Byte

No transmission error



Transmission error



ISO-7816 Part 3: T=1 TPDU

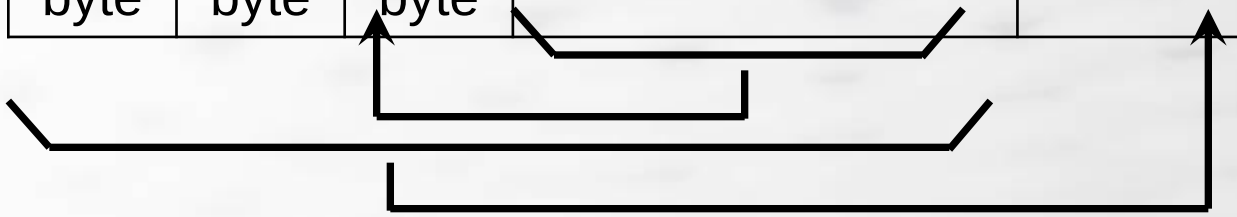
ISO-IN Command

ISO-OUT Command

ISO-IN & OUT Command

ISO-7816 Part 3: T=1 TPDU Frame

PROLOGUE			INFORMATION	EPILOGUE
NAD	PCB	LEN	INFORMATION FIELD	EDC
1 byte	1 byte	1 byte	0 to 254 bytes	1 or 2 bytes

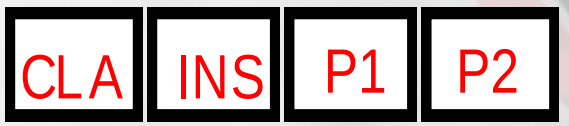


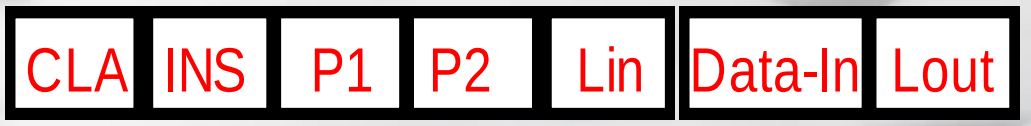
PCB conveys the type of frame

I-BLOCK (Information Block)
R-BLOCK (Receive Ready Block)
S-BLOCK (Supervisory Block)

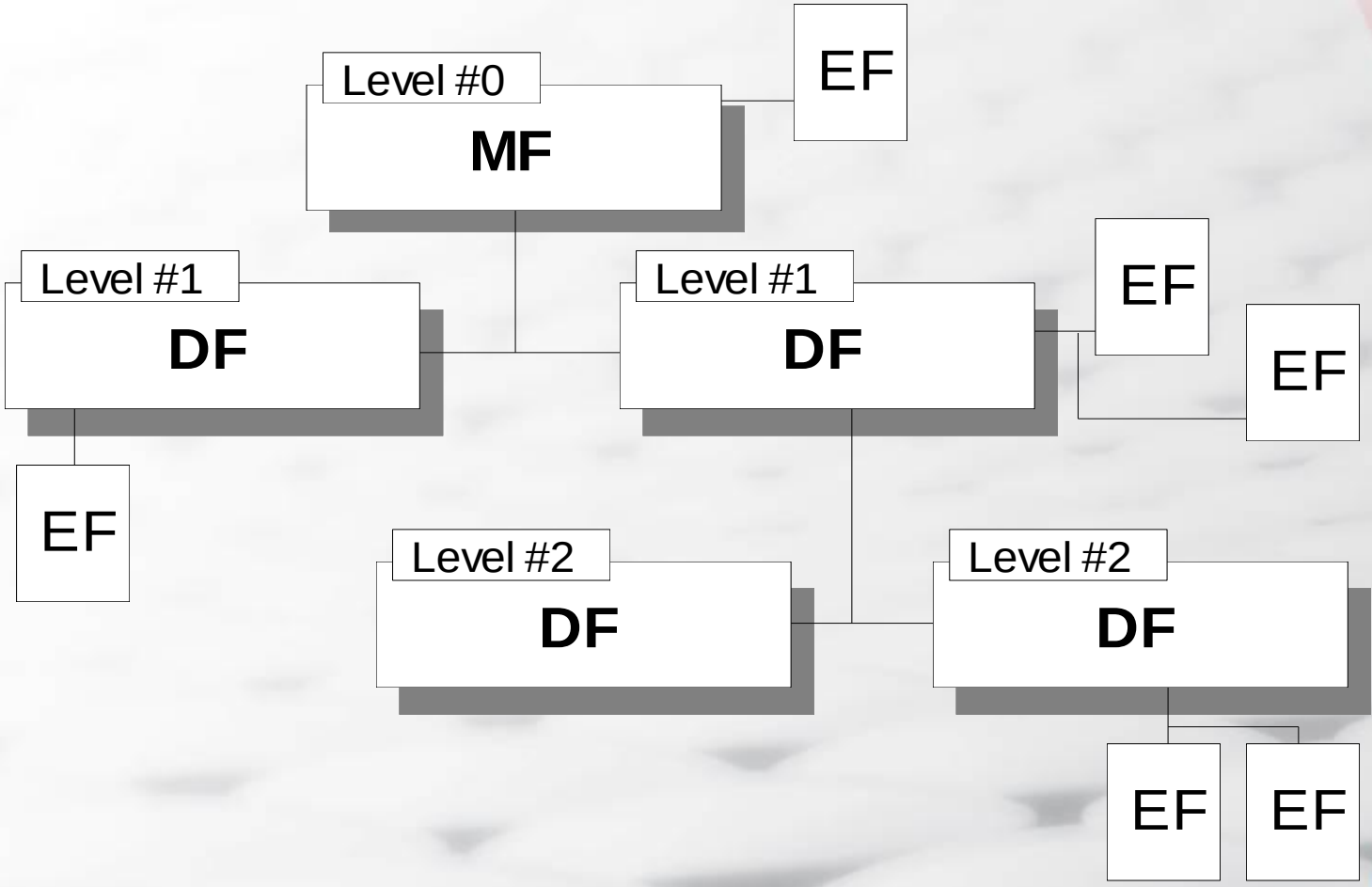
ISO-7816 Part 4: APDU FORMAT

Case	Command	Response
	data	data
1	no data	no data
2	no data	data
3	data	no data
4	data	data

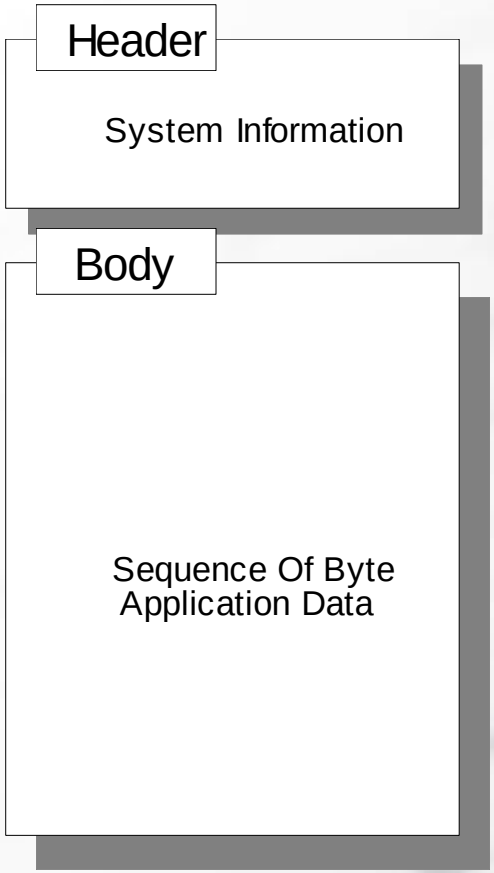




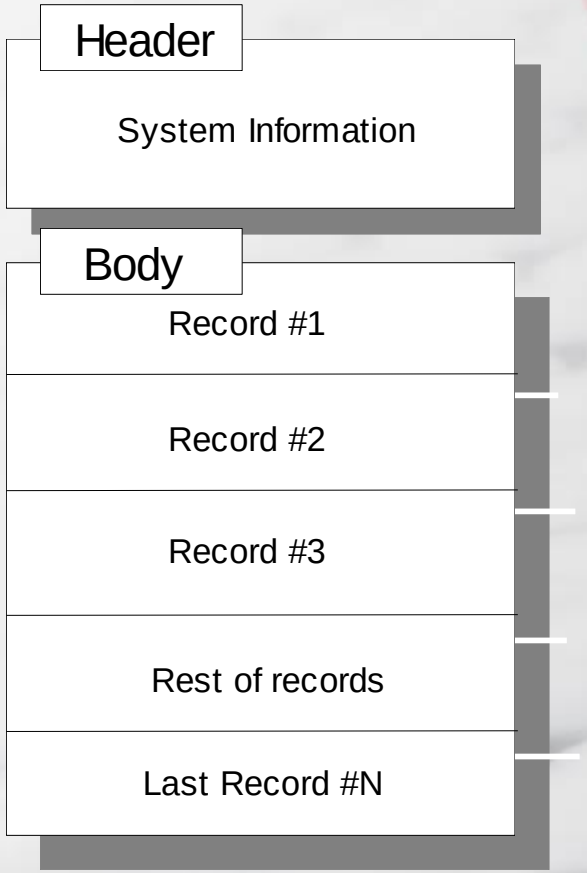
ISO-7816 Part 4: File Organization



ISO-7816 Part 4: File Structures

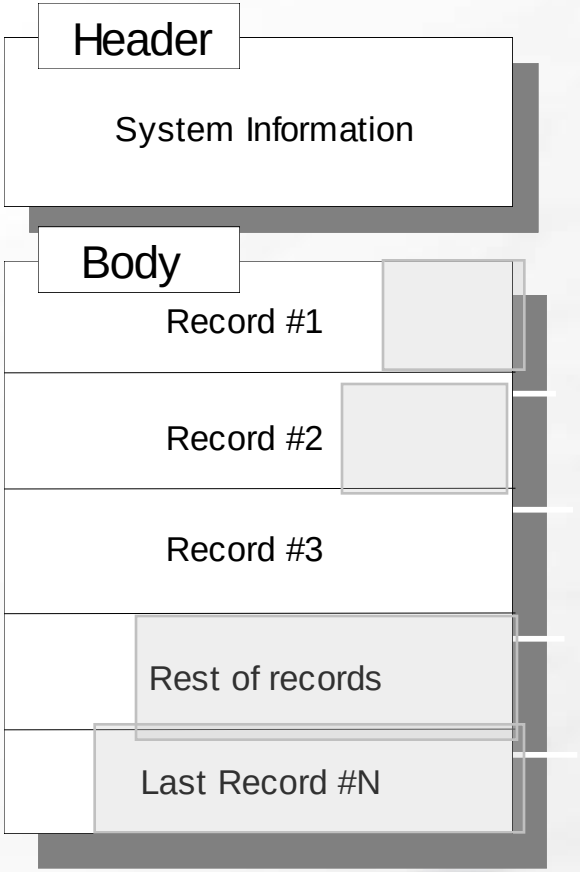


TRANSPARENT FILE

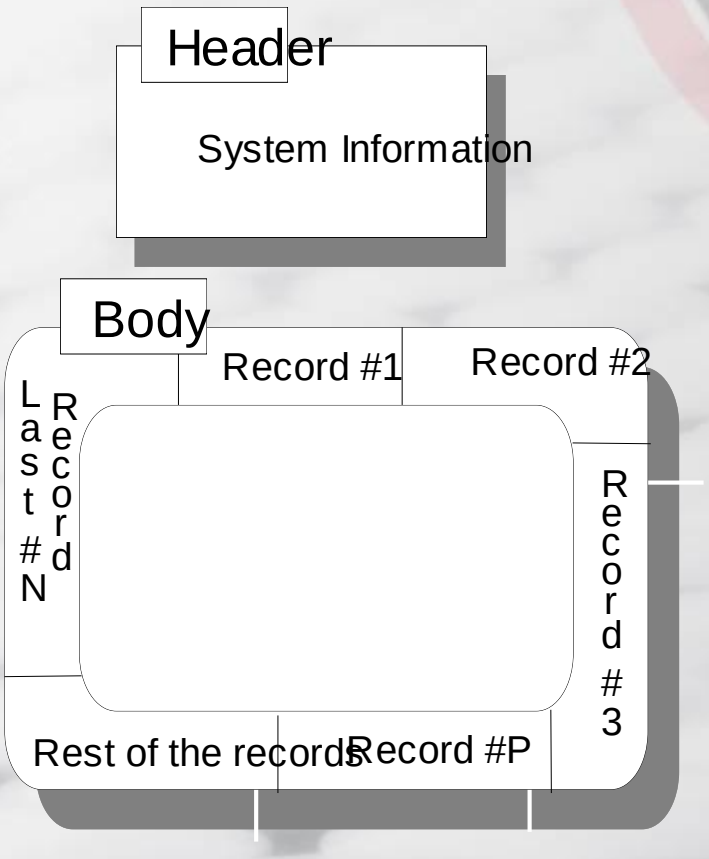


LINEAR FIXED FILE

ISO-7816 Part 4: File Structures



LINEAR VARIABLE FILE



CYCLIC FILE

ISO-7816 Part 4: Inter-industry Commands

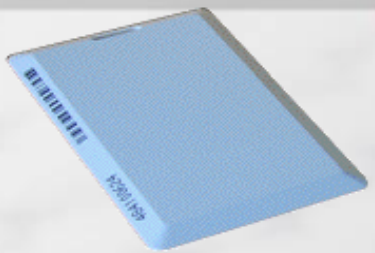
- ERASE BINARY
- VERIFY
- MANAGE CHANNEL
- EXTERNAL AUTHENTICATE
- READ RECORD(S)
- READ BINARY
- SELECT FILE
- INTERNAL AUTHENTICATE
- GET CHALLENGE
- GET RESPONSE
- ENVELOPE
- GET DATA
- WRITE BINARY
- WRITE RECORD
- UPDATE BINARY
- PUT DATA
- UPDATE RECORD
- APPEND RECORD

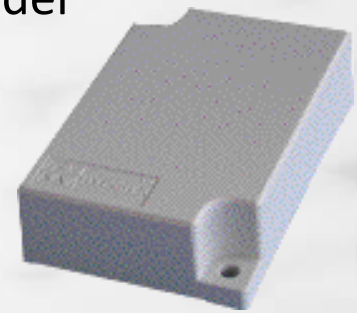
And many more commands with the new ISO-7816 part 4!!!

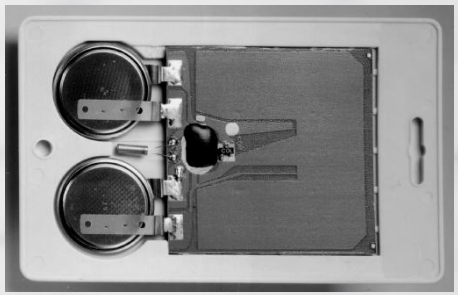
Contactless Technology

Types Of RFID

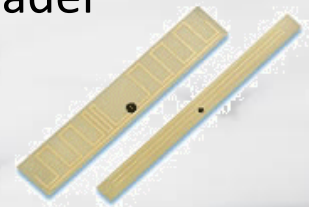
- Active Tag
  - On-board power source
  - Requires less power from the reader
  - Longer read/write range
  - Limited operating life
  - More expensive

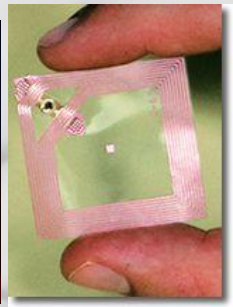






- Passive Tag
  - Obtains operating power from the reader
  - Higher-powered reader
  - Shorter read range
  - Unlimited life time
  - Smaller, lighter, and less expensive

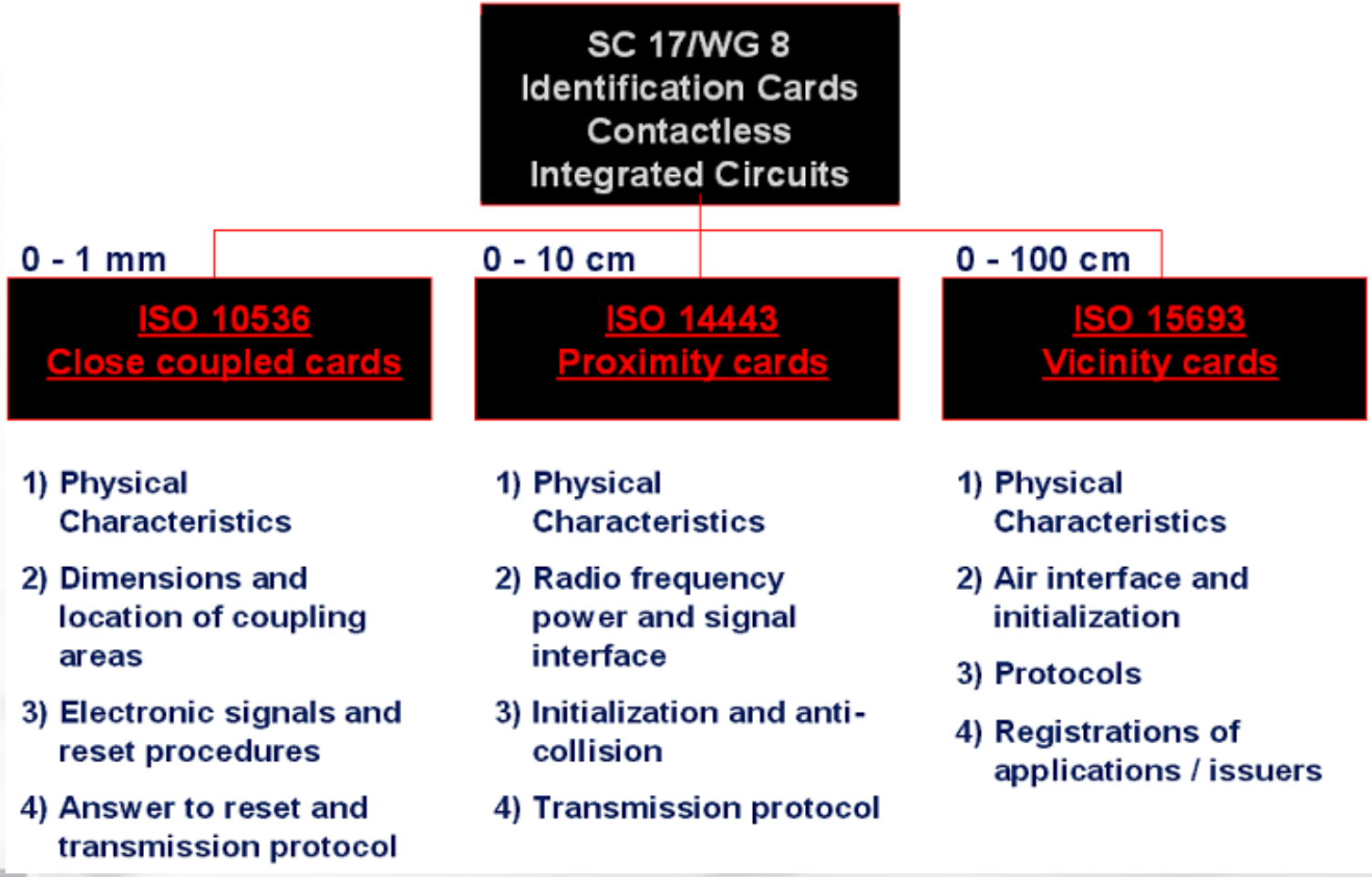




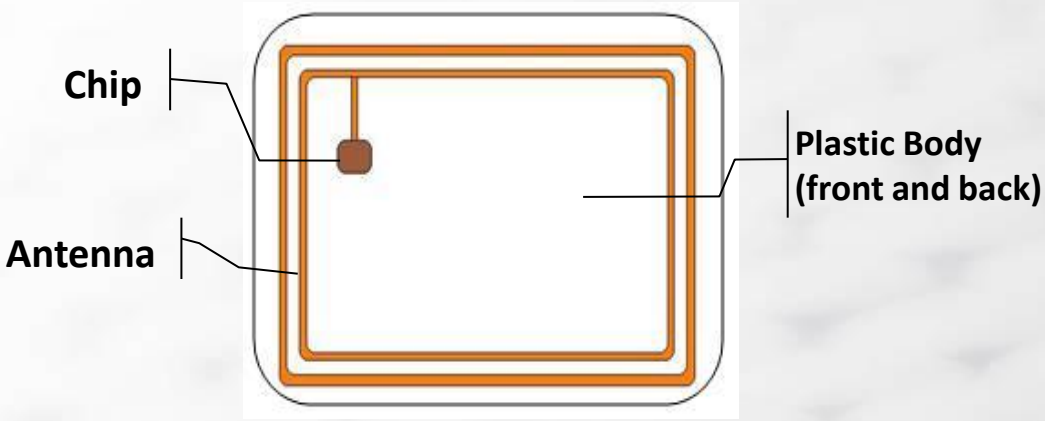
RFID Operating Frequencies

Frequency Band	Characteristics	Typical Applications
Low: 100-500 kHz 125kHz : Low Frequency	➢Short to medium read range ➢ Inexpensive ➢ low reading speed	➢ Access control ➢ Animal identification ➢ Inventory control ➢ Car immobilizer
Intermediate: 10-15 MHz 13.56MHz: High Frequency	➢ Short to medium read range ➢ potentially inexpensive ➢ medium reading speed	➢ Access control ➢ Smart cards
High: 850-950 MHz (UHF) 2.4-5.8 GHz (SHF)	➢ Long read range ➢ High reading speed ➢ Line of sight required ➢ Expensive	➢ Railroad car monitoring ➢ Toll collection systems

ISO Standards of RFID in 13.56 MHz



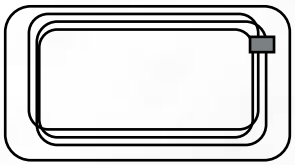
Components of a Contactless Smart Card



- A contactless smart card comprises of 3 parts
  - Chip
  - Antenna
  - Plastic body (front and back)

Types of Contactless Cards

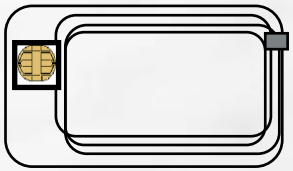
Contactless Card



Memory or µprocessor chip connected to an antenna. Antenna and module embedded into the plastic card body.

Low cost solution
Full contactless

Hybrid Card



Contactless card with an added contact chip. There is **no link** between the 2 chips.

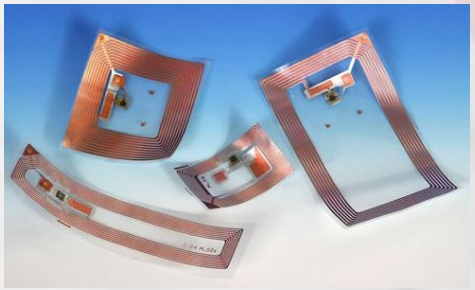
Fast time to market
High price

Combi Card

Microprocessor chip with the **2 interfaces**. Single OS managing transactions in both modes.

One single chip
Applications and data sharing between contact & contactless

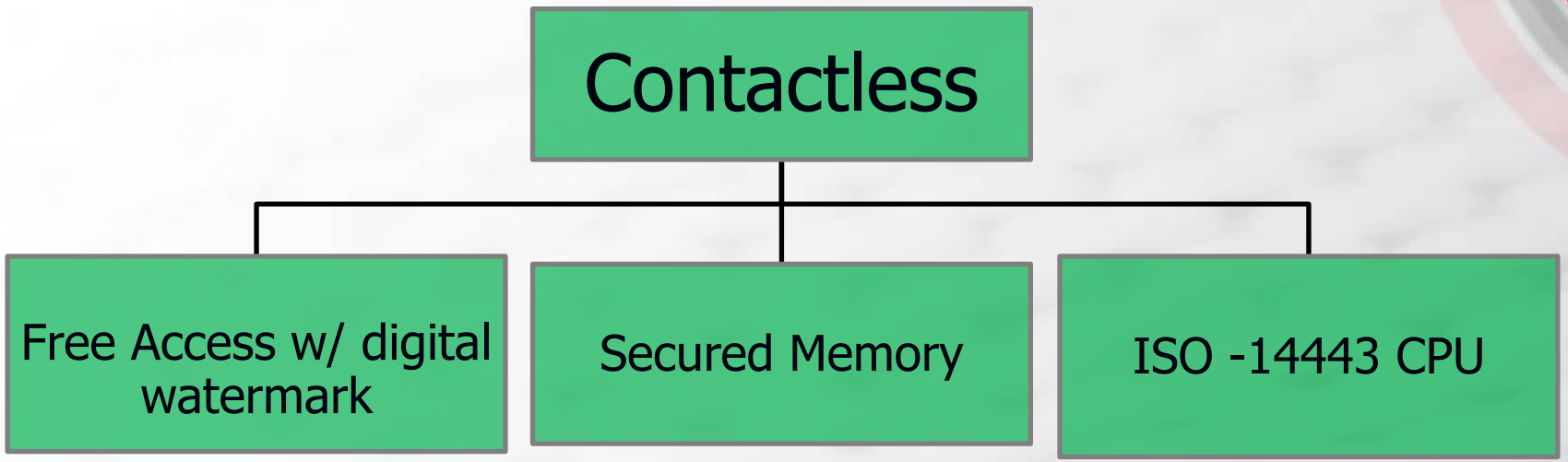
Different Forms of RFID Tags



Contactless for Security Applications

- **Contactless Memory - Mifare**
  - NXP, Infineon, Atmel
  - Prepaid, transportation, physical access
- **Contactless CPU Card - Readily available types**
  - Desfire (for e-purse)
- **Contactless CPU – National standard**
  - China transportation
  - Singapore CEPAS e-purse
- **Contactless CPU – Application standard**
  - EMV – Paypass, Visa-wave
  - ICAO Biometrics Passport

Types of Contactless Cards



-MiFare Ultralight

- ISO -15693 I-code

- Mifare Classics

- DESFire

- Paypass

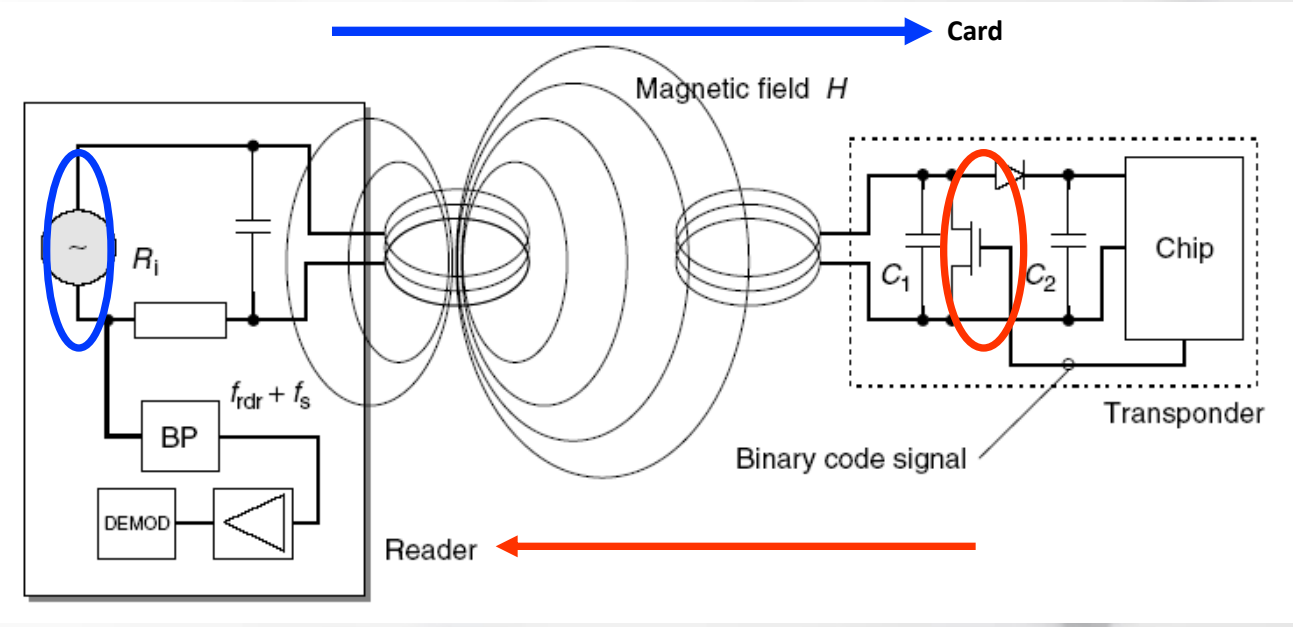
- Visa-wave

- ICAO passport

How Tag is Powered & How it Communicates

Inductive Coupling

ASK (Amplified Shifted Keying)



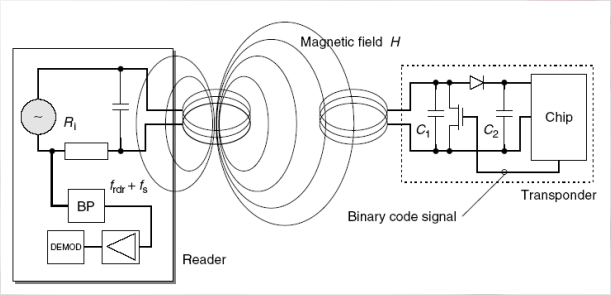
Card Reader: Load Modulation

ISO 14443 Part 1:Physical Characteristics

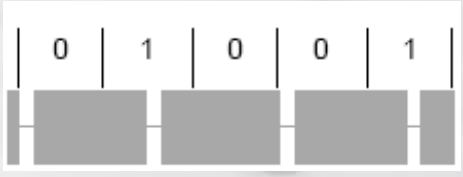
- This standard defines
  - Card dimensions (refer to ISO 7810 for ID-1 cards)
  - Surface quality for printing
  - Mechanical resistance
  - UV and X-ray resistance
  - Sensitivity to surrounding magnetic fields
- The standard introduces the specific terms:
  - PICC: Proximity Integrated Circuit Card
  - PCD: Proximity Coupling Device (the card reader or terminal)

ISO 14443 Part 2: RF Power & Signal Interface

- This standard defines:
  - Characteristics of power transfer (inductive coupling & communication between PICC & PCD at 13.56 MHz)



- It has 2 different types:
  - Type A Card
    - 100% modulation ASK
  - Type B Card
    - 10% modulation ASK



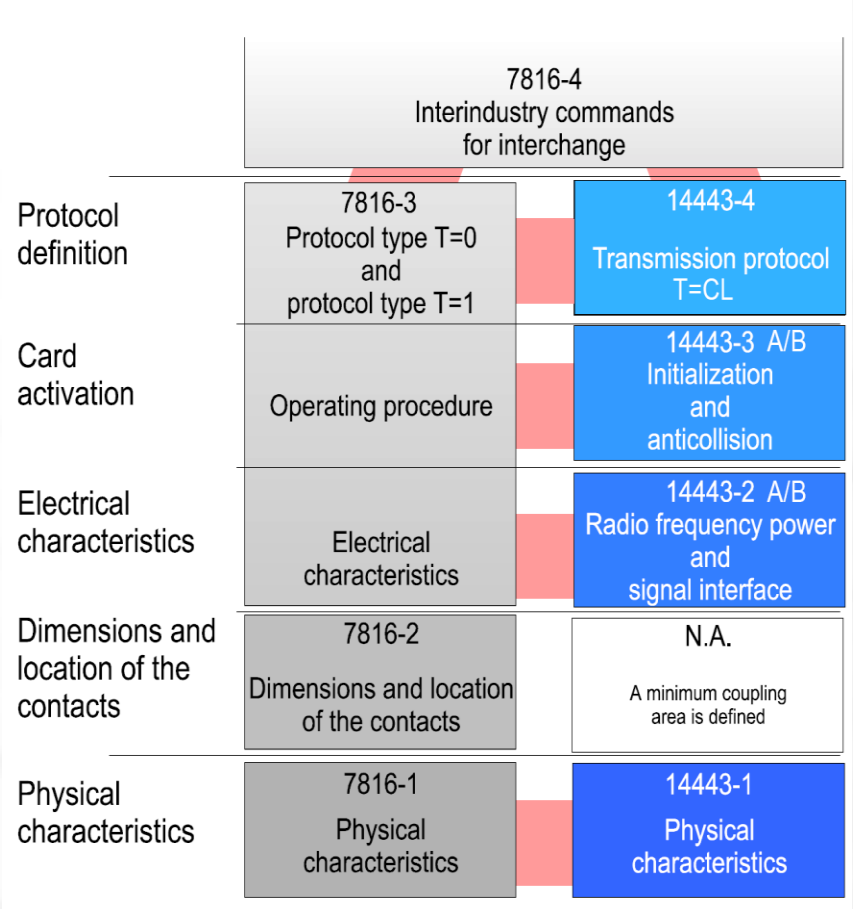
ISO 14443 Part 3: Initialization & Anti-collision

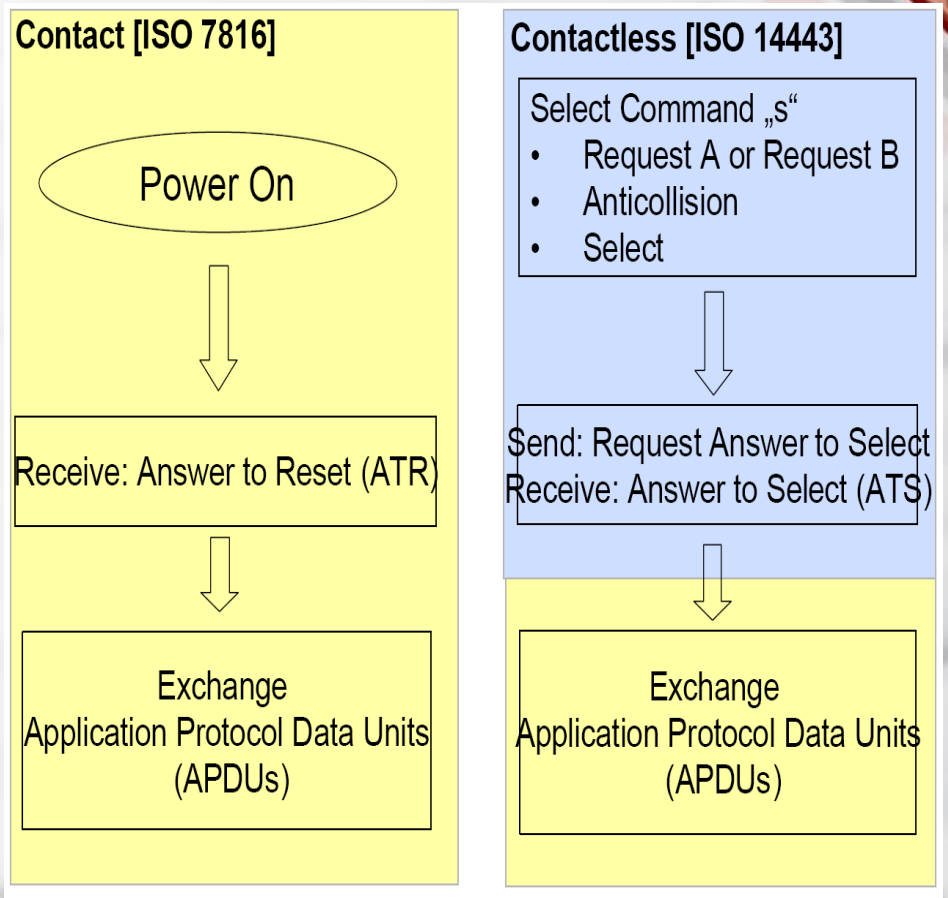
- This standard defines :
  - Poll for PICCs entering the field of a PCD
  - Format, command frames and timing
  - Request(REQ) and Answer To Request(ATQ) commands
  - Anti-collision methods for A & B cards:
    - Detects & communicates with 1 out of n cards
    - Relies on a unique ID per card
- It has 2 different types:
  - Type A: Binary search referring to the card UID
  - Type B: Slotted Aloha method

ISO 14443 Part 4: Transmission Protocol

- This standard defines:
  - A half duplex block transmission protocol, T=CL
  - Similar to T=1
  - Independent of lower layers

ISO-7816 vs ISO-14443





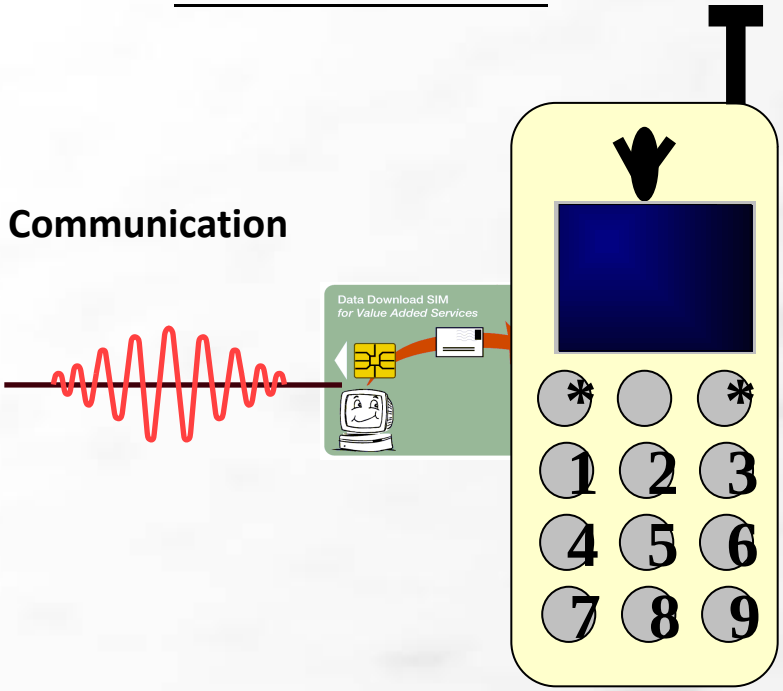
Advanced Card Systems Ltd.
Card & Reader Technologies

NFC Technology

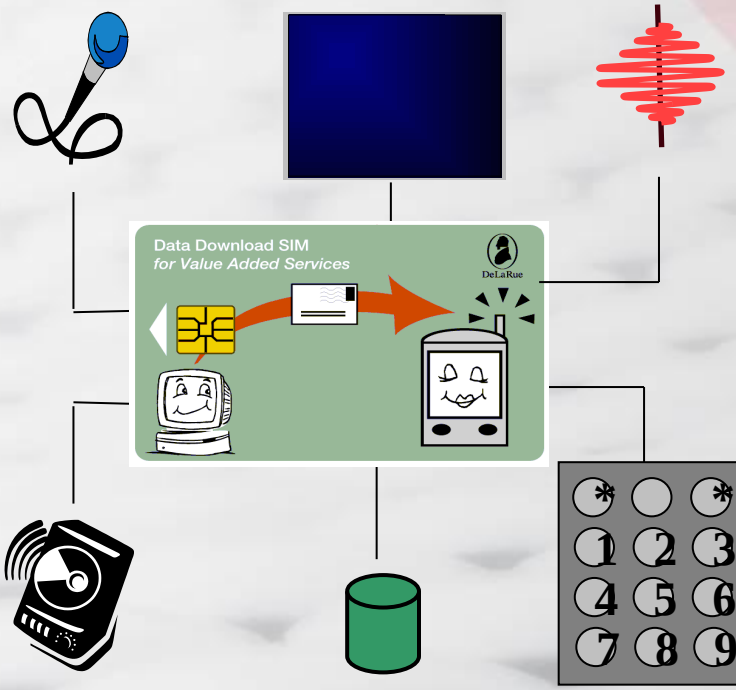
CARD & READER TECHNOLOGIES

What is NFC?

GSM SIM card



NFC-based GSM SIM card



*Note: NFC application can be in the SIM or in the phone with a Java Smart Card chip in the handset.

NFC Handset Architecture

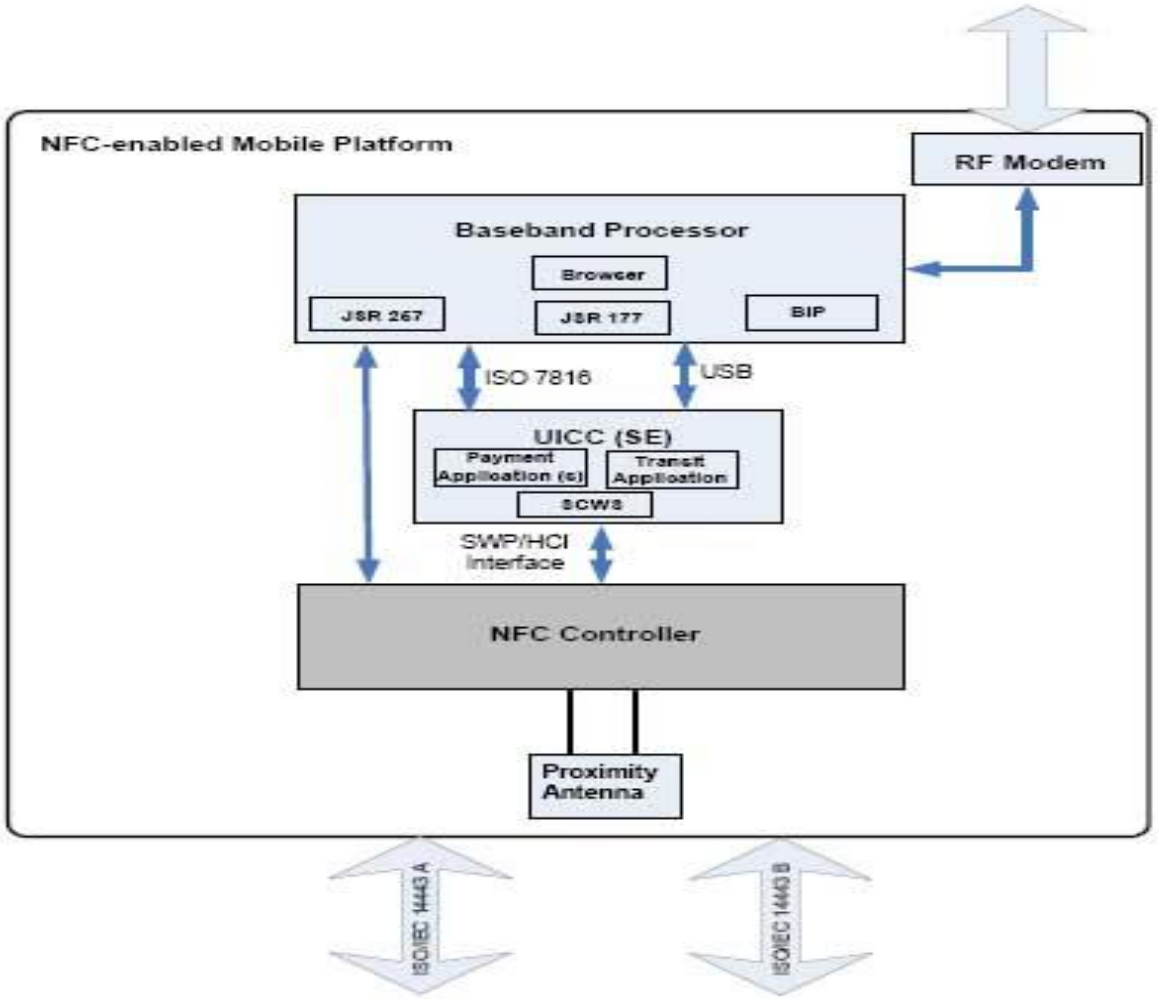
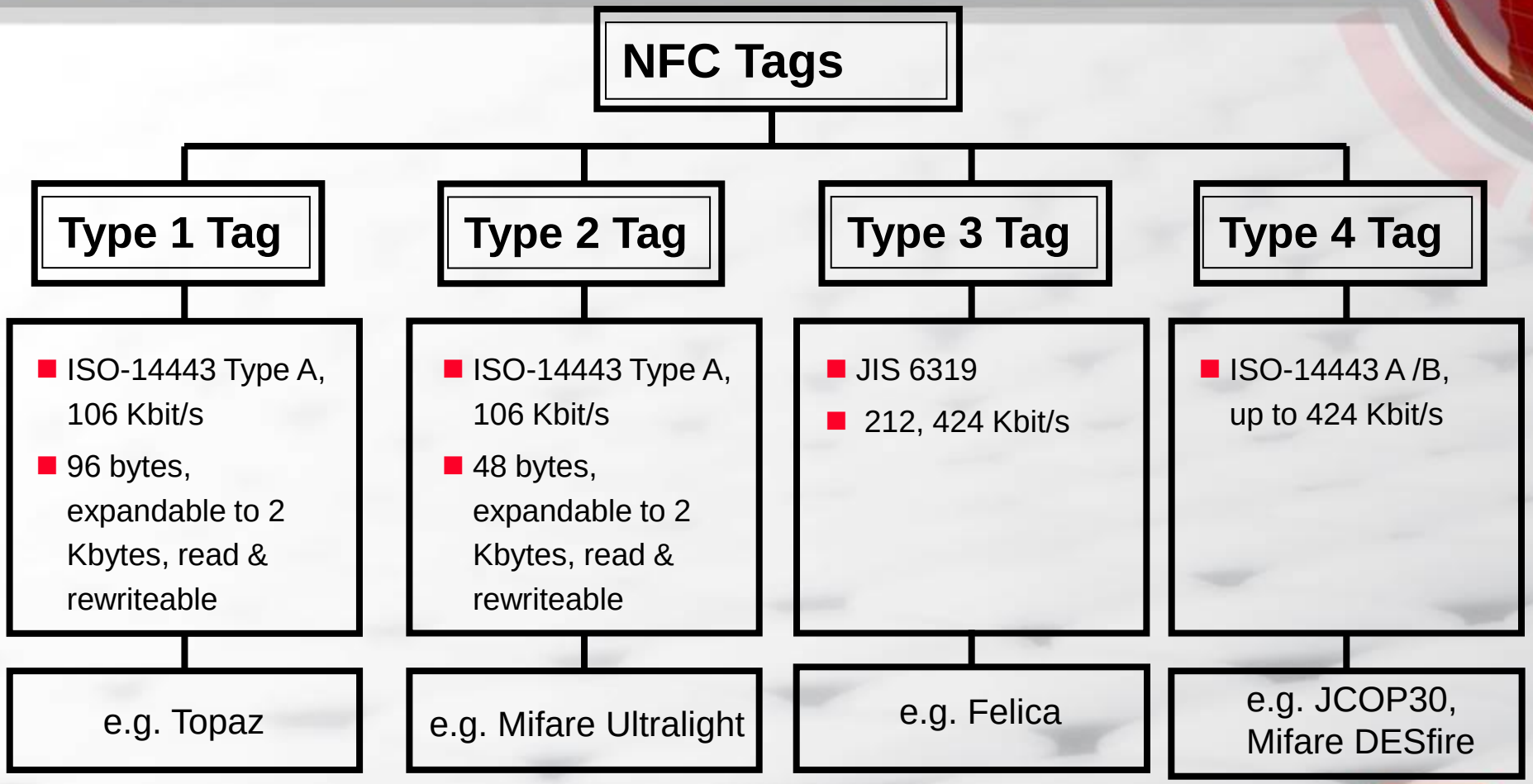


Figure 3-1: NFC Handset Functional Architecture.

What are NFC Tags?



Typical NFC Applications

- **Contactless card and Personal contactless terminal**
  - Automatic Fare Collection
  - Loyalty
  - Credit Card
- **Smart Poster**
- **Blue-tooth pairing**

Advanced Card Systems Ltd.
Card & Reader Technologies

Secured Smart Card Printing

CARD & READER TECHNOLOGIES

Secure Printing

- Main Goal of Secure/Security Printing
  - Prevent forgery or counterfeiting
- Typical Application
  - National ID cards, Passport, Banking cards
- Typical Examples
  - UV Printing
  - Microtext
  - Guilloche
  - Multiple laser image (MLI)
  - Watermark
  - Hologram, etc…

Secure Printing

Secure Printing

(Source: HK Immigration Department)

Secure Printing (more examples)

HOLOGRAM

More about hologram

Setup charge for molding may cost US $2,000!

Secure Printing (more examples)

Microtext

Secure Printing (more examples)

UV Printing

UV light

Secure Printing (more examples)

Watermark

Glossary for Secure Printing

- **Guilloche:** printed security lines- the layout of intersections and geometry are unique. Guilloches are created from two or more indicated and overlapping lines.
- **Hologram:** a unique form of photographic printing that appears as flat optical image to the naked eye and provides a three-dimensional effect on a flat surface. Holograms cannot be easily copied and are used for security and aesthetic purposes on cards.
- **Microtext:** involves extremely small texts that are small enough to be indiscernible to the naked eye.
- **MLI(Multiple Laser Image**): image that can be viewed at different angles.
- **OVI (Optical Variable Ink):** a high security feature showing different colors as the angle of view changes.

Glossary for Secure Printing

- **UV (Ultraviolet) Printing:** is invisible under regular illumination. By viewing the text/graphic under UV light, they become visible with a yellow colour.
- **Offset printing:** a method of printing that transfers the paint from the printing platform under pressure onto an intermediate elastic rubber surface, and then to the product surface.
- **CMYK (Cyan-Magenta-Yellow-Black):** a system of color separation for printing.

http://www.smartcardalliance.org/pages/smart-cards-intro-glossary

Why Use Smart Card Technology?

What Can Go Wrong with Existing Systems

- Magnetic ATM Card
  - Cloning of card at POS for fund transfer
  - Cloning of card by fake ATM
- Magnetic Credit Card
  - Card duplicated during usage
  - Fake card
  - Fake transaction

Installing a magnetic card reader attachment

Magnetic reader attachment installed

RF transmission Camera to capture PIN entry

Transmission to a receiver 200 meters away


Panasonic
PV-BP50
Camera
Battery
Antenna

What Can Go Wrong with Existing Systems

- Magnetic Payphone Card
  - Buying 5 fake cards for the price of one authentic card
  - Tampering with the value
  - Frequent cleaning of read/write head
  - Local power supply required

- Mobile Phone System
  - Eavesdropping on conversation
  - Cloning of mobile phone during usage or repair

What Can Go Wrong with Existing Systems

- Pay TV
  - Cloning of decoder after establishing customer base
- Logon to Computer System
  - Unauthorized access to computer network

Advanced Card Systems Ltd.
Card & Reader Technologies

Smart Card Security Features

CARD & READER TECHNOLOGIES

Smart Card Security Capabilities

- Card Authentication
- Terminal Authentication
- Cardholder Authentication
- Transaction Certification
- Data Confidentiality

Card Authentication

- The terminal ensures that the card is authentic before continuing with the transaction.
- The issuer loads into each card & terminal a secret key before issuance.
- The card must prove to the terminal that the card knows the secret key.
- The card must not expose the secret key during the authentication process.
- Since the card knows the secret key, it must be an authentic card.

Terminal Authentication

- The card ensures that the terminal trying to access the card is a genuine terminal.
- The issuer loads into each card & each terminal a secret key before issuance.
- A genuine terminal must be able to prove that it knows the secret key by presenting the secret key to the card.
- Since the terminal can prove its authenticity, the card grants the terminal the required access rights.

Card Holder Authentication

- The card ensures that only the genuine cardholder can use the card.
- The issuer loads into each card a cardholder PIN.
- The cardholder must prove to the card that he knows the PIN.
- The card grants the cardholder the required access rights since the cardholder is able to present the correct PIN.
- The card can automatically block successive wrong PIN presentation
- Incorporating biometrics (thumb print, retina/vein pattern, voice, signature dynamics) is also possible.

Transaction Certification

- The issuer loads a unique certification key into the card before issuance.
- The terminal sends transaction into the card after successful card, terminal and card-holder authentication.
- The card generates an electronic signature of the transaction with the certification key.
- The fact that the signature is verified to be correct indicates that the transaction actually took place.
- The transaction certificate can be used for non-repudiation and data integrity.

Data Confidentiality

- The issuer loads a unique encryption key into each card before issuance.
- This key is used to encrypt the data between the terminal and the remote host.

Conclusion

- The smart card is only one component in a smart card based system implementation.
- **What you want is a solution.**
- Using a smart card does not automatically imply security; the system design, together with the smart card, is what makes for security.
- A smart card is not always the best solution if the smart card's capabilities are not fully utilized.

Smart Card Market

MCU Cards Shipment (Millions of Units)

	2004	2005	2006	2007	2008	2009
Telecom	1,050	1390	2,040	2,650	3,200	3,300
Financial Services/ Retail/ Loyalty	280	336	410	510	650	730
Government/ Healthcare	45	60	90	105	140	160
Transport	15	20	20	30	30	40
Pay TV	55	55	65	85	100	100
Others (including Corp. ID	24	27	30	65	65	70
Total	**1,469**	**1,888**	**2,665**	**3,445**	**4,185**	**4,400**

Source: Eurosmart (http://www.eurosmart.com)

MCU Cards Shipment (Millions of Units)

	2004	2005	2006	2007	2008	2009
Financial Services/ Retail/ Loyalty	280	336	410	510	650	730
Government/ Healthcare	45	60	90	105	140	160
Transport	15	20	20	30	30	40
Others (including Corp. ID	24	27	30	65	65	70
Total	**349**	**443**	**550**	**710**	**885**	**1,000**

Source: Eurosmart (http://www.eurosmart.com)

Memory Card Shipment (Millions of Units)

	2004	2005	2006	2007	2008	2009
Telecom	710	580	480	440	380	300
Financial Services/ Retail/ Loyalty	35	30	30	30	30	30
Government/ Healthcare	20	25	250*	300*	250	170
Transport	60	73	140	160	160	160
Others (including Corp. ID	20	30	35	80	80	80
Total	**845**	**738**	**1,020**	**970**	**900**	**740**

*included the Chinese ID at 200 Mu (2006), 250 Mu (2007)

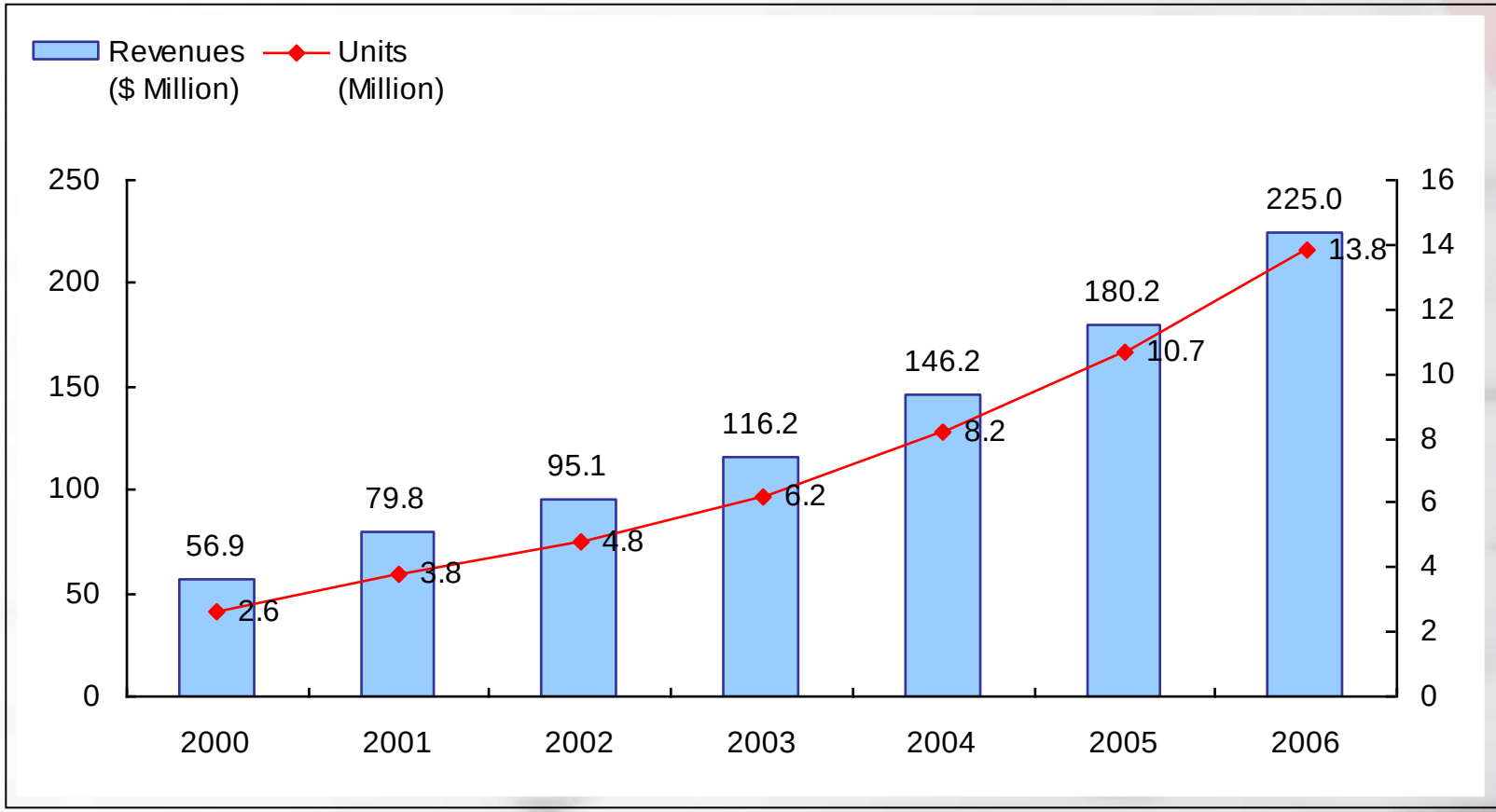
Source: Eurosmart (http://www.eurosmart.com)

Contactless Cards Shipment (Millions of Units)

	2007	2008	2009	2010 (Forecast)
	MCU	MCU	MCU	MCU
Financial Services/ Retail/ Loyalty	60	100	110	140
Government/ Healthcare	50	60	75	90
Transport	30	30	40	50
Others (including Corp. ID	30	30	30	30
Total	**170**	**220**	**255**	**310**

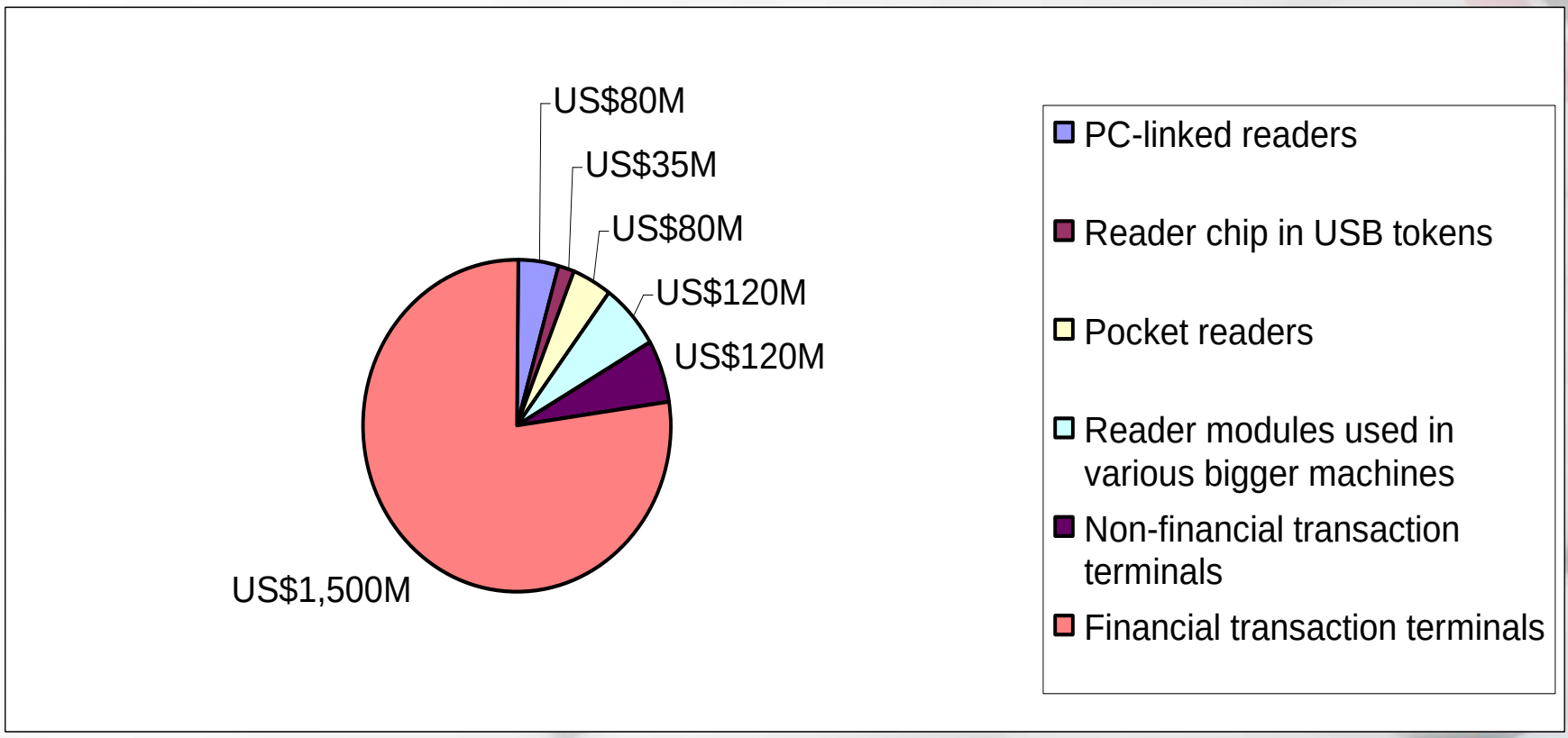
Source: Eurosmart (http://www.eurosmart.com)

Total Smart Card Reader Market



Source: Frost & Sullivan

Smart Card Reader Market Size



Smart Card Applications

Telecommunications Prepaid Card

- Lower infrastructure cost
- Lower maintenance cost
- Cash in advance
  - Unspent money
- Opportunity for new service – Card Roaming
- Opportunity for new markets
- Electronic Purse

Mobile Communications - GSM / PCN

- No eavesdropping on conversation
- No cloning of handsets
- Regional roaming
- Lower cost of handsets
- More value-added services
  - Fixed dialing
  - Advice of charge
  - Short Message Service (SMS)
  - SIM Tool kit
  - And more…

Financial Sector

- **Smart Debit / Credit Card - Europay Master Visa**
  - Online and Offline Transactions
  - No card cloning
  - Value-added services
    - Loyalty
- **Debit Card / Electronic Passbook / Electronic Purse**
  - Security
  - Off-line transaction
  - High availability, speed of service
  - Low cost per transaction
  - Low cost system infrastructure maintenance

Retail

- **Loyalty Card**
  - Collect & analyze customer needs
  - Increase market share
  - Increase profit
  - Provide value-added services
  - Retain customer loyalty
- **Gift Voucher / Prepaid Card**
  - Increase market share
  - Increase profit

Healthcare

- **Health & Insurance**
  - Administrative cost saving through automation
  - Fraud control
  - Waste control
  - Prevention of abuses
  - Medical records

Identification

- Identification card
- Physical access
- Logical access
- Clocking
- Resource booking
- Library card
- Vending
- Staff canteen

Questions?