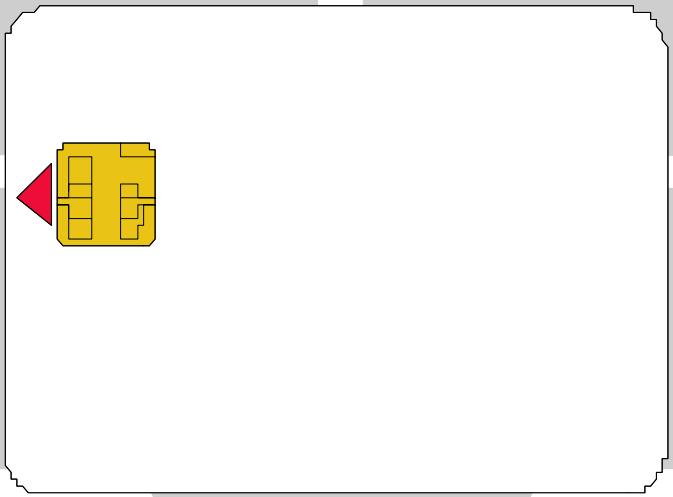
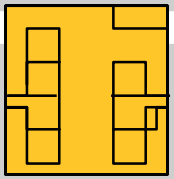
What is a smart card



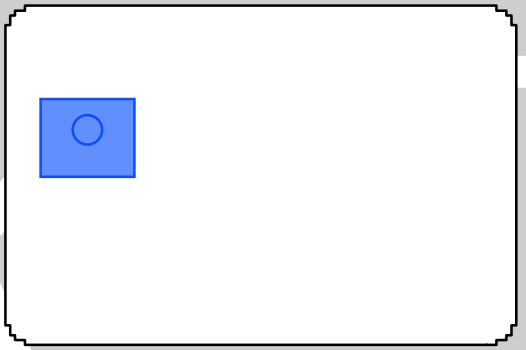
- a credit card size plastic with a single IC chip on board and conforms with ISO-7816

Components Of A Smart Card



contact disc

chip



plastic body

- a smart card comprises of 3 parts
  - contact disc
  - chip
  - plastic body with cavity

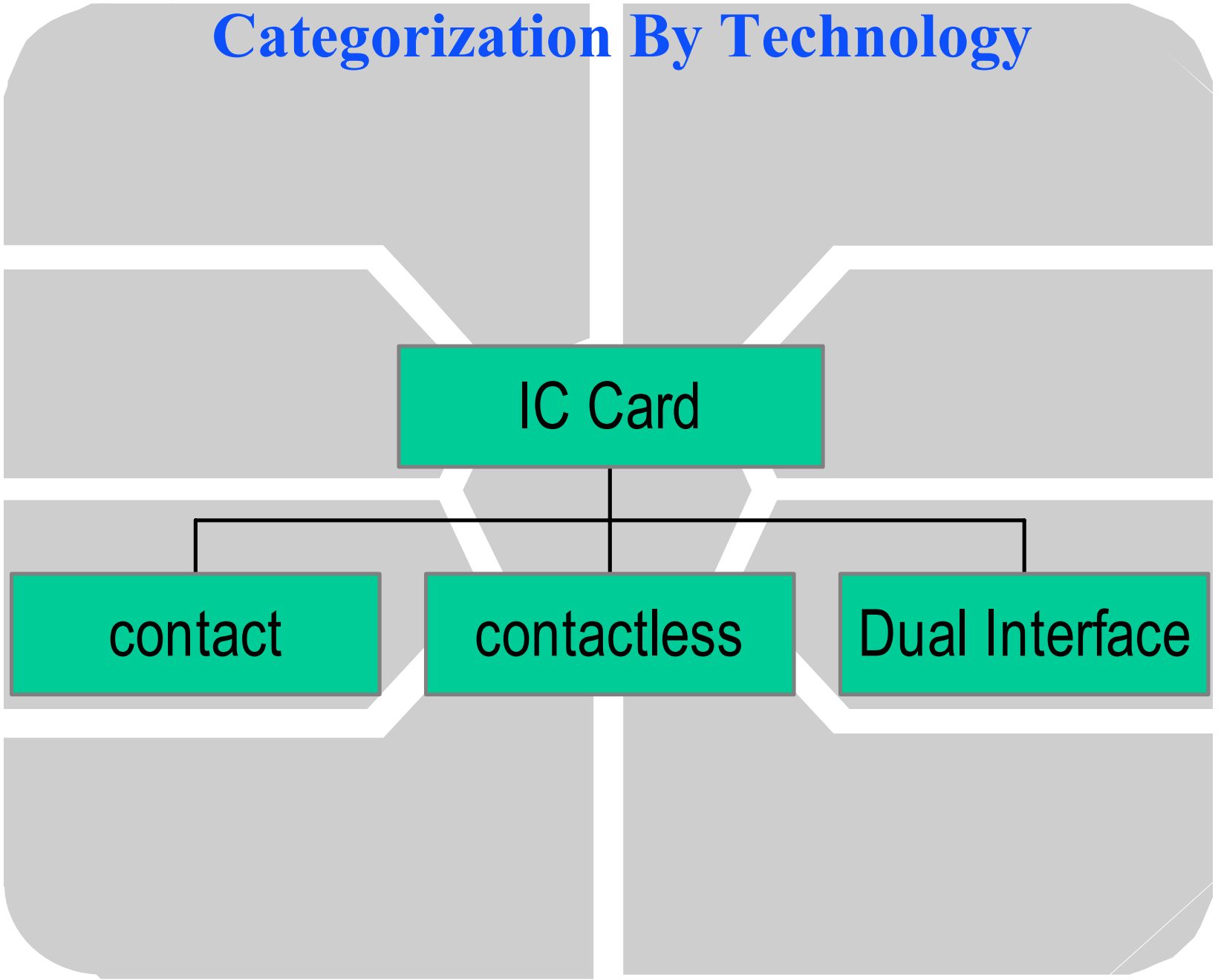
Contact Disc

- 6 or 8 contacts
- square or oval shape
- can have different patterns defining the contacts
- contact position complies with ISO-7816-2
- cannot tell the type of cards from the contact disc

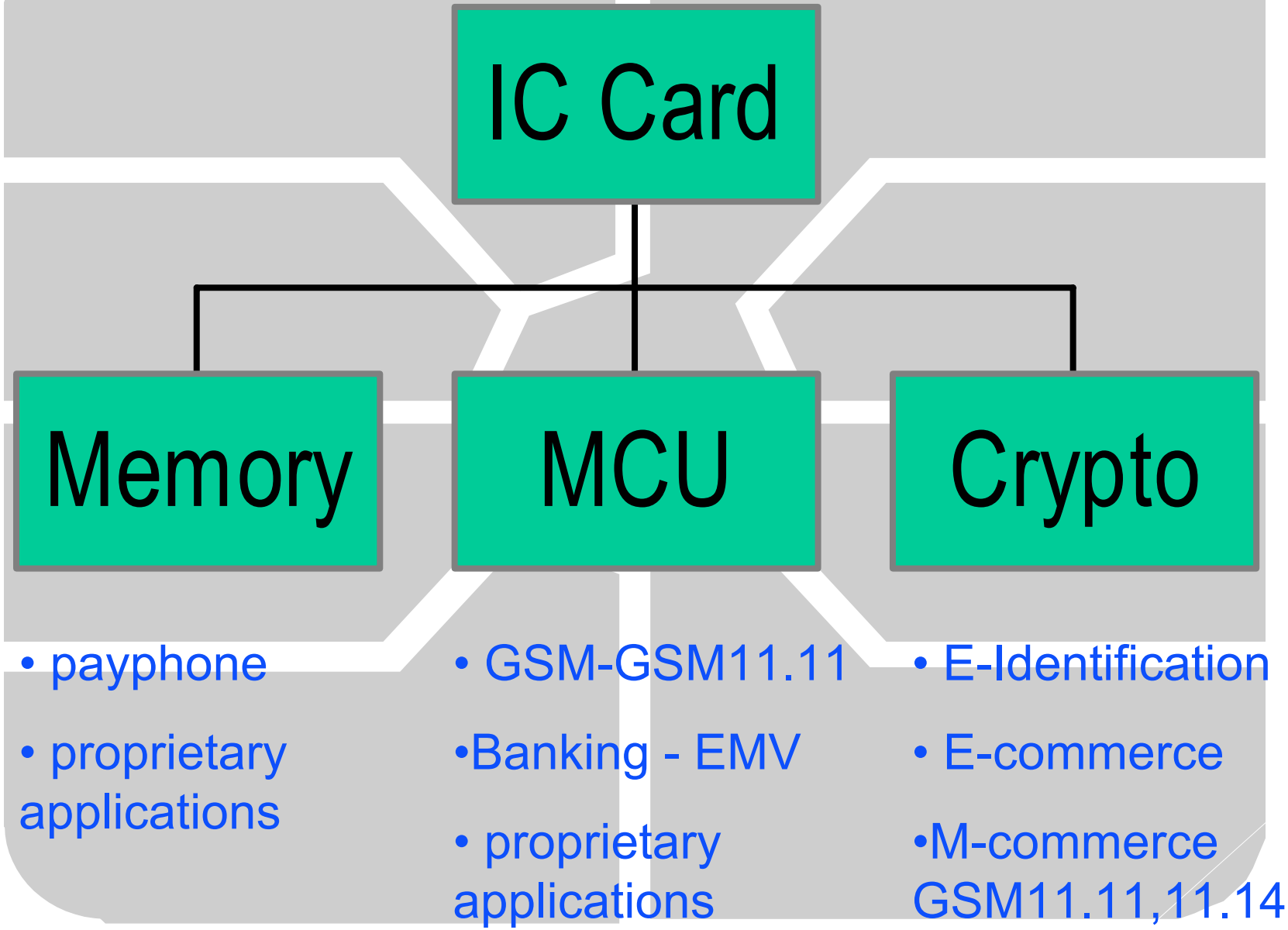
Smart Card / IC Card Family

- Contact Memory Card
  - Siemens, Atmel, Xicor
- Contact CPU Card
  - GSM SIM, Visa Smart Debit/Credit
  - national banking card
- Contactless Memory Card
  - Philips / Siemens; Sony
- Dual Interface CPU Card

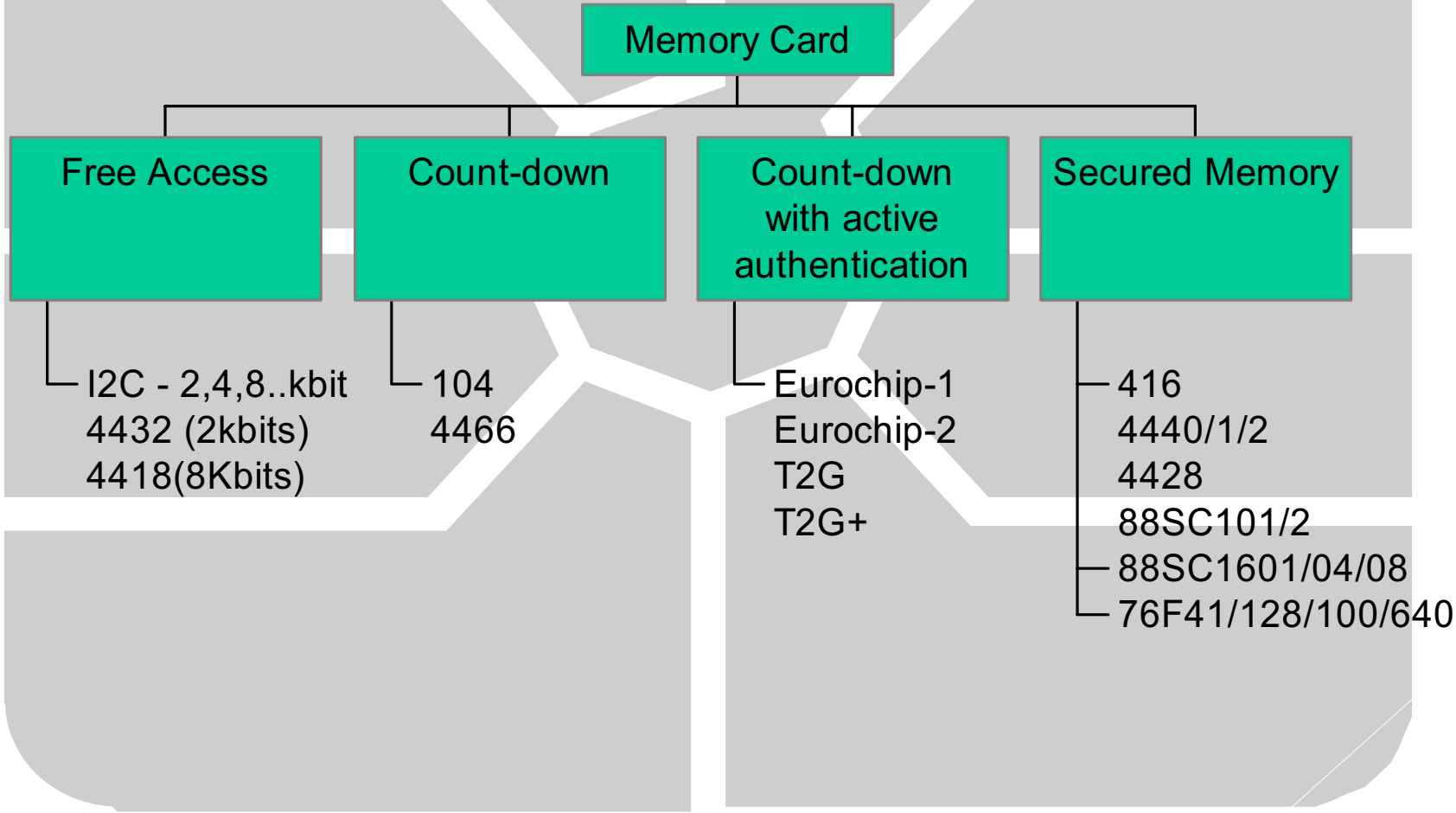
Categorization By Technology

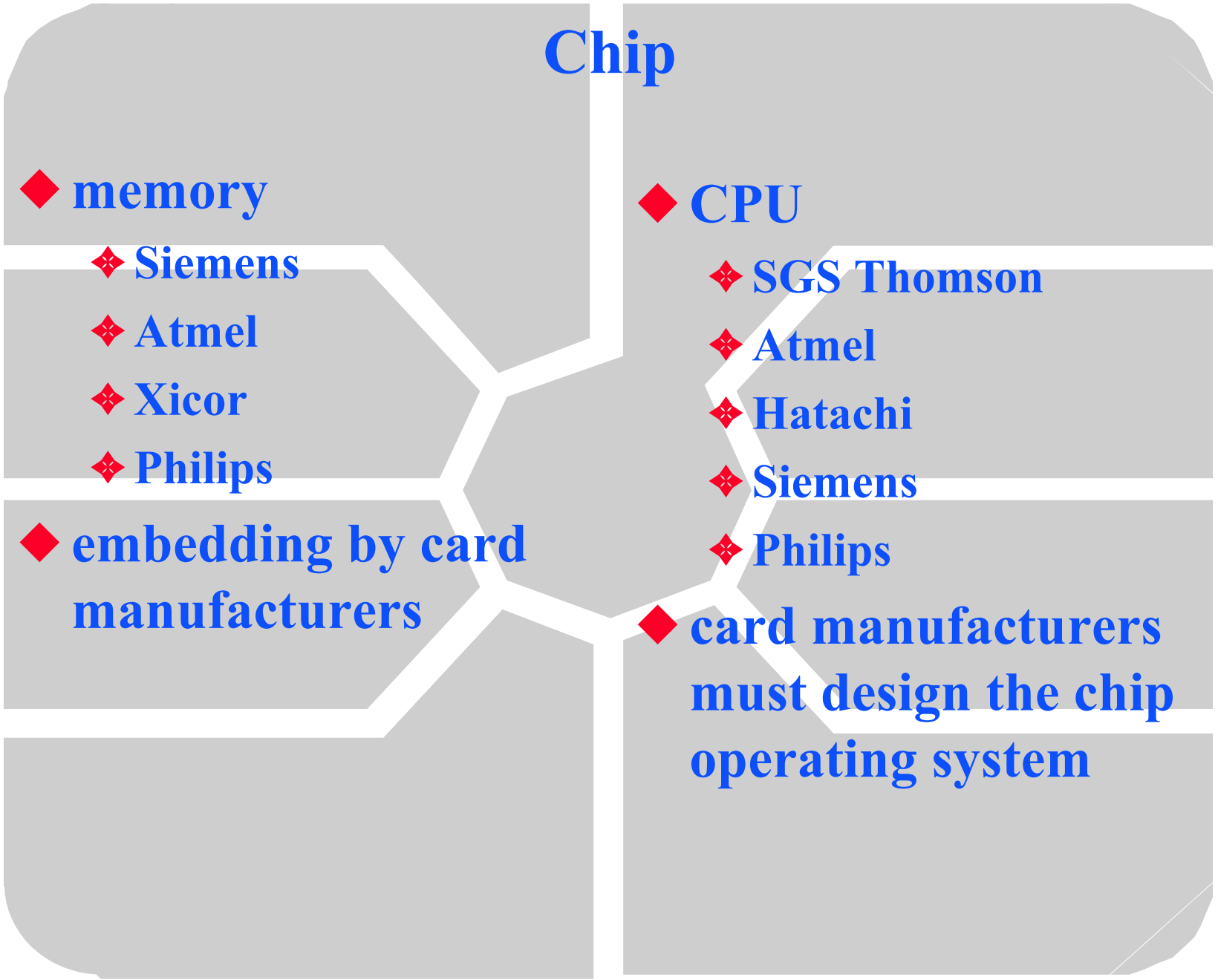


Categorization By Security



Types Of Memory Cards




Chip
memory
Siemens
Atmel
Xicor
Philips
embedding by card manufacturers
CPU
SGS Thomson
Atmel
Hatachi
Siemens
Philips
card manufacturers must design the chip operating system

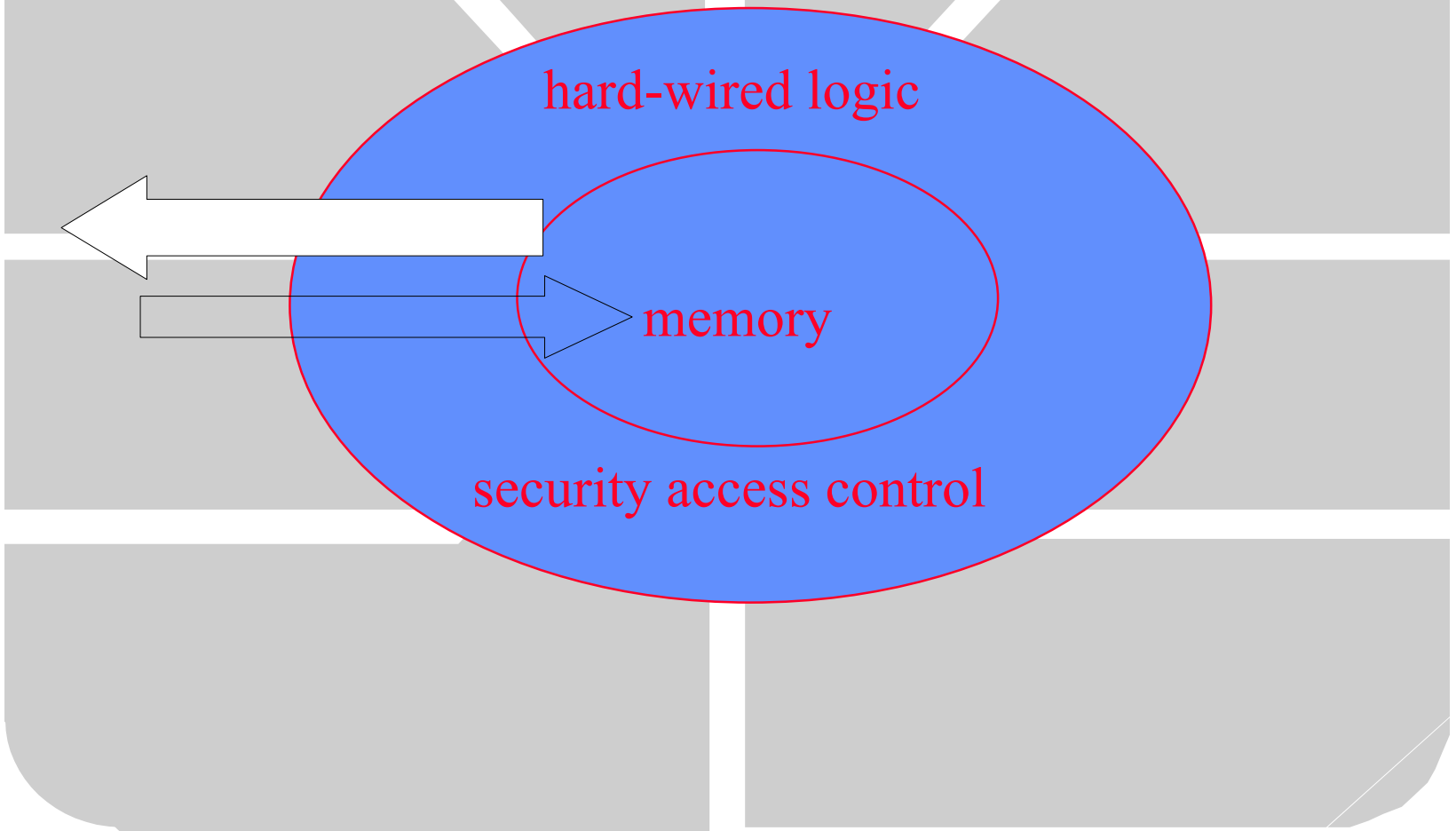
Memory Cards Manufacturer

Philips	Siemens	Atmel	ST-Micro	Xicor
			ST1333	
PCF2006 PCF2036	SLE4406 SLE4436 SLE5536	AT88SC06	ST1305	
		AT24C01 AT24C02 AT24C04 AT24C08 AT24C16	ST14C02C ST14C04C	
	SLE4404	AT88SC101 AT88SC102 AT88SC1601 AT88SC1604		
	SLE4463			
	SLE4418 SLE4428			
PCF2042	SLE4432 SLE4442			
				24C65
				93CS06/46
				93CS56/66
				X76F041
				X76F128/640
				X76F100

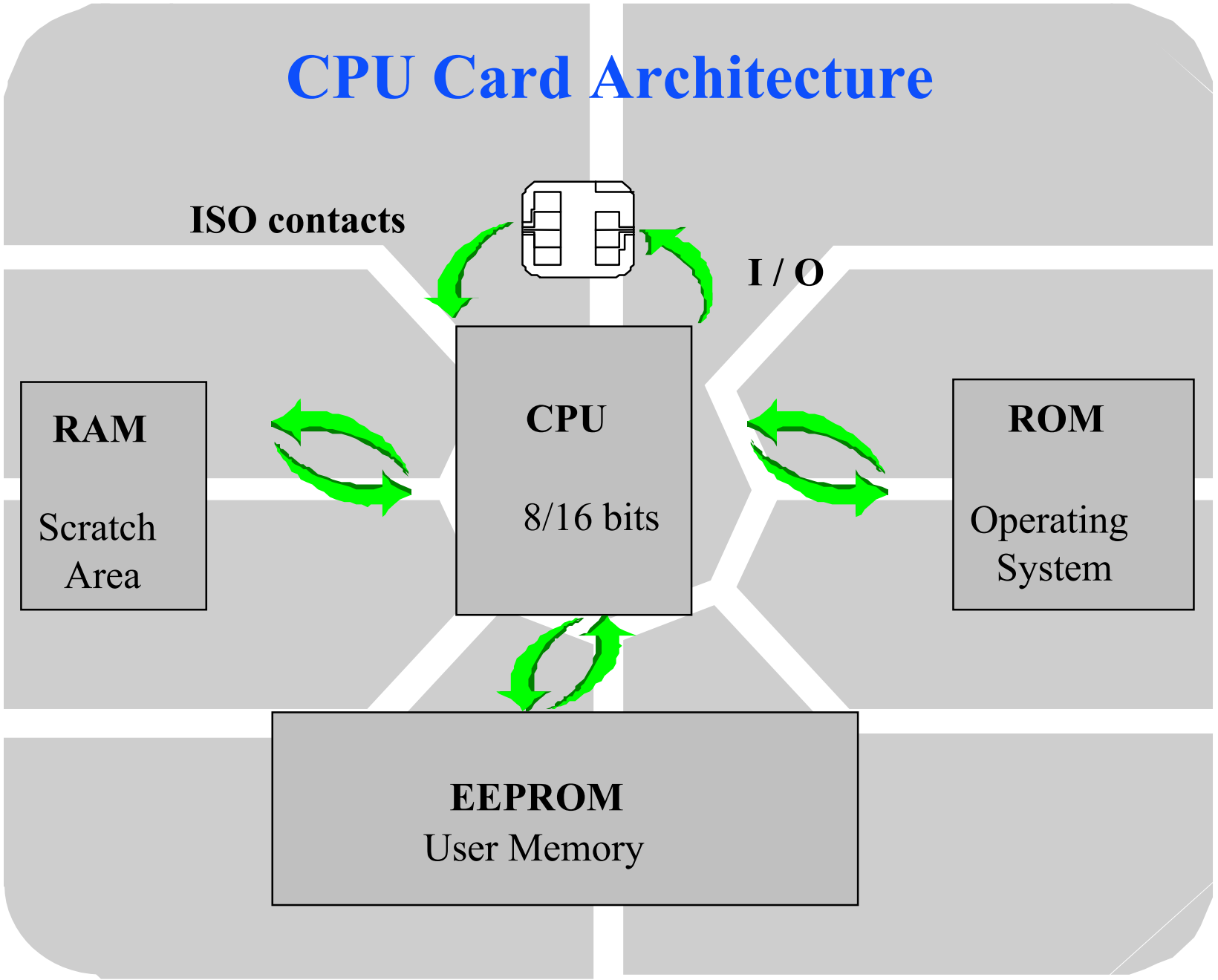
Plastic Body

- ABS
  - difficulty in embossing, thermal transfer printing, hot stamping, metallic colours
  - injection moulded (cheaper)
- PVC
- Polycarbonate (PC)

Memory Card Security Architecture



CPU Card Architecture



Smart Card

- memory size is described in bits / bytes
- memory size is refering to the application memory
  - EEPROM - erasable, if authorised
- memory card storage, 104 bits to 16 Kbits
- CPU card - 8bits/16 bits, 8051 or 6805 core
  - ROM 3Kbytes to 32 Kbytes
  - RAM ~100 bytes to 1 Kbytes
  - EEPROM 512 bytes to 32 Kbytes

Smart Card CPU

SGS-Thomson	ROM (bytes)	RAM (bytes)	E2PROM (bytes)	SIZE (sq.mm)
16301	3K	128	1K	18
16612	6K	160	2K	21.48
16623	6K	224	3K	24.19
16601	6K	128	1K	10.10
16F44	16K	288	8K	18.60
16F48	16K	288	8K	23.30
16SF48	16K	384	8K	23.30
16CF54	16K	480	8K	23.80
Hatachi				
H8/310	10K	256	8K	27.56
H8/3102	16K	512	8K	19.08

Smart Card CPU

Motorola	ROM (bytes)	RAM (bytes)	E2PROM (bytes)	SIZE (sq.mm)
SC21	6K	128	3K	14.58
SC24	3K	128	1K	10.36
SC26	6K	160	1K	13.40
SC27	16K	240	3K	20.58
SC28	13K	240	8K	25.97
SC29	13K	512	4K	26.00
Siemens				
44C10	4K	128	1K	13.00
44C40	8K	256	4K	18.39
44C42S	16K	256	4K	
44C80	16K	256	8K	21.70
44C160S	16K	256	16K	
44CCR80	16K	256	8K	

Smart Card CPU

Philips	ROM (Kbytes)	RAM (bytes)	E2PROM (Kbytes)	SIZE
83C852	6	256	2	
83C855	20	512	2	
83C852	20	640	8	
83C864	16	256	4	
83W86xx	20-28	256-512	2,4,8,16	

Smart Card Standard ISO-7816

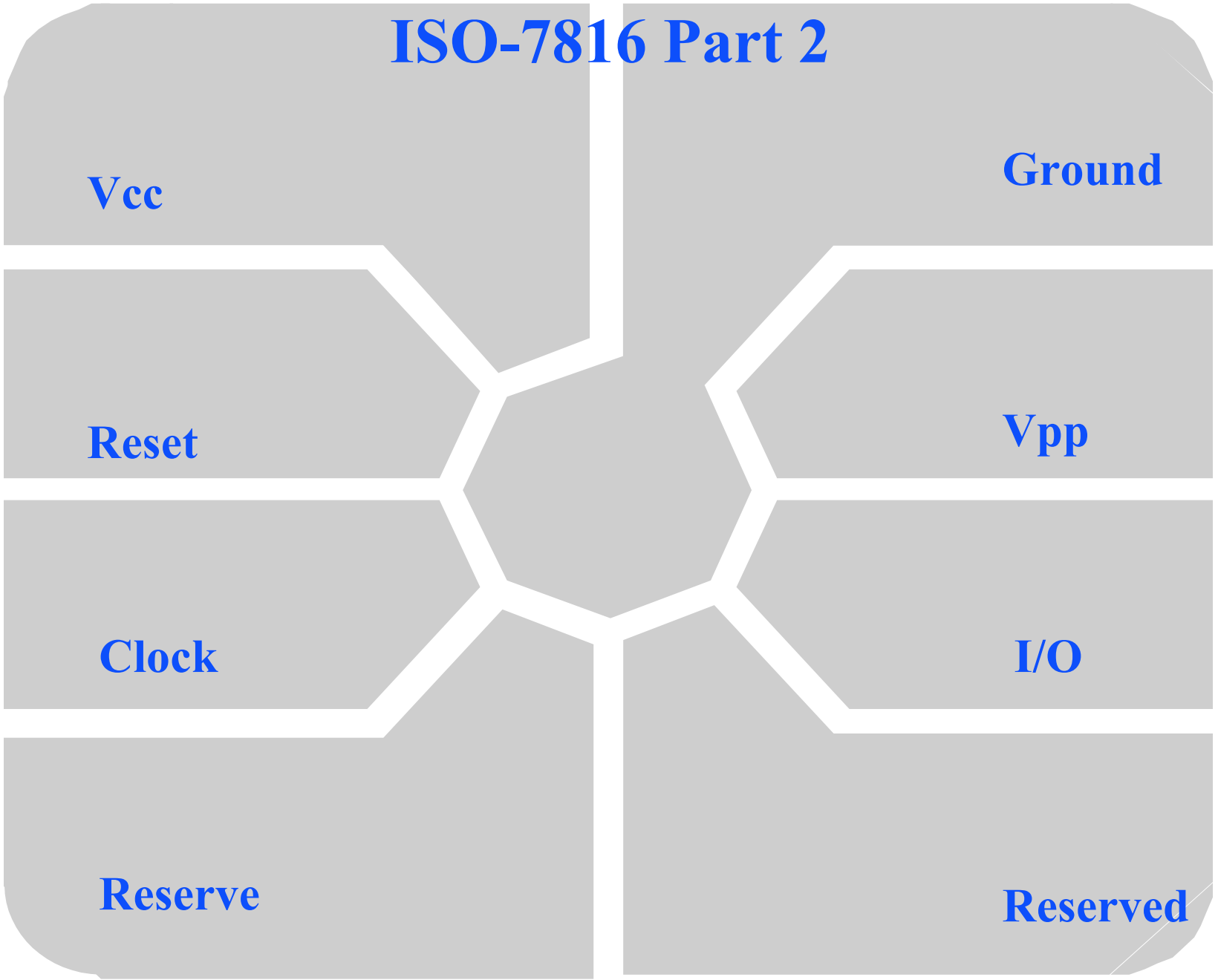
- Part 1 - Physical Characteristics
- Part 2 - Dimensions & Locations of Contacts
- Part 3 - Electronic Signals & Transmission Protocol
- Part 4 - Inter-industrry Command For Interchange
- Part 5 - Numbering System & Registration Procedure for Application Identifiers
- Part 6 : Inter-industry Data Elements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

ISO-7816 Part 1 Physical Characteristics

- UV light
- X-ray
- contacts surface profile
- ESD
- torsion

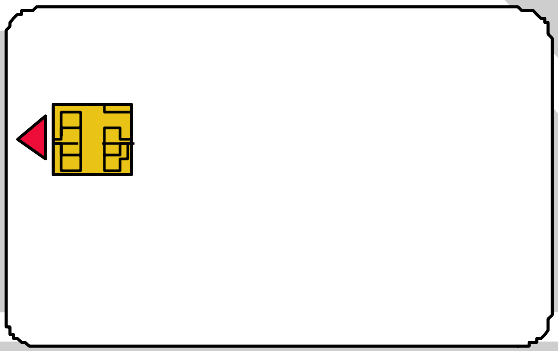
- heat dissipation
- bending
- mechanical strength of card, contacts
- EMI
- bending

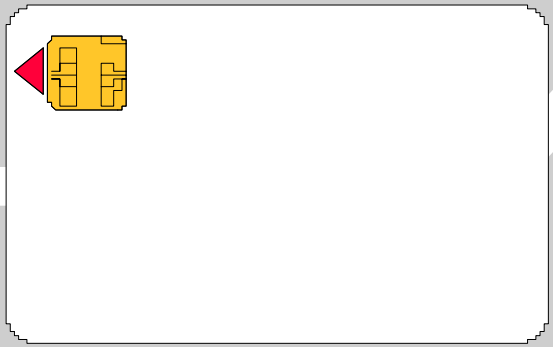
ISO-7816 Part 2



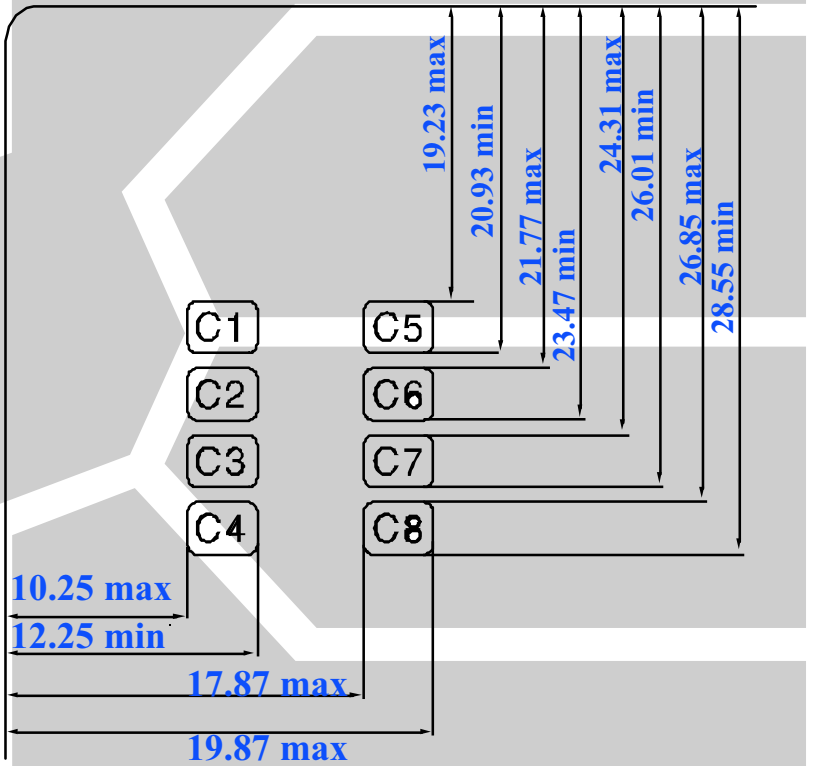
ISO-7816 Part 2
Location & Assignment If Contacts

ISO POSITION

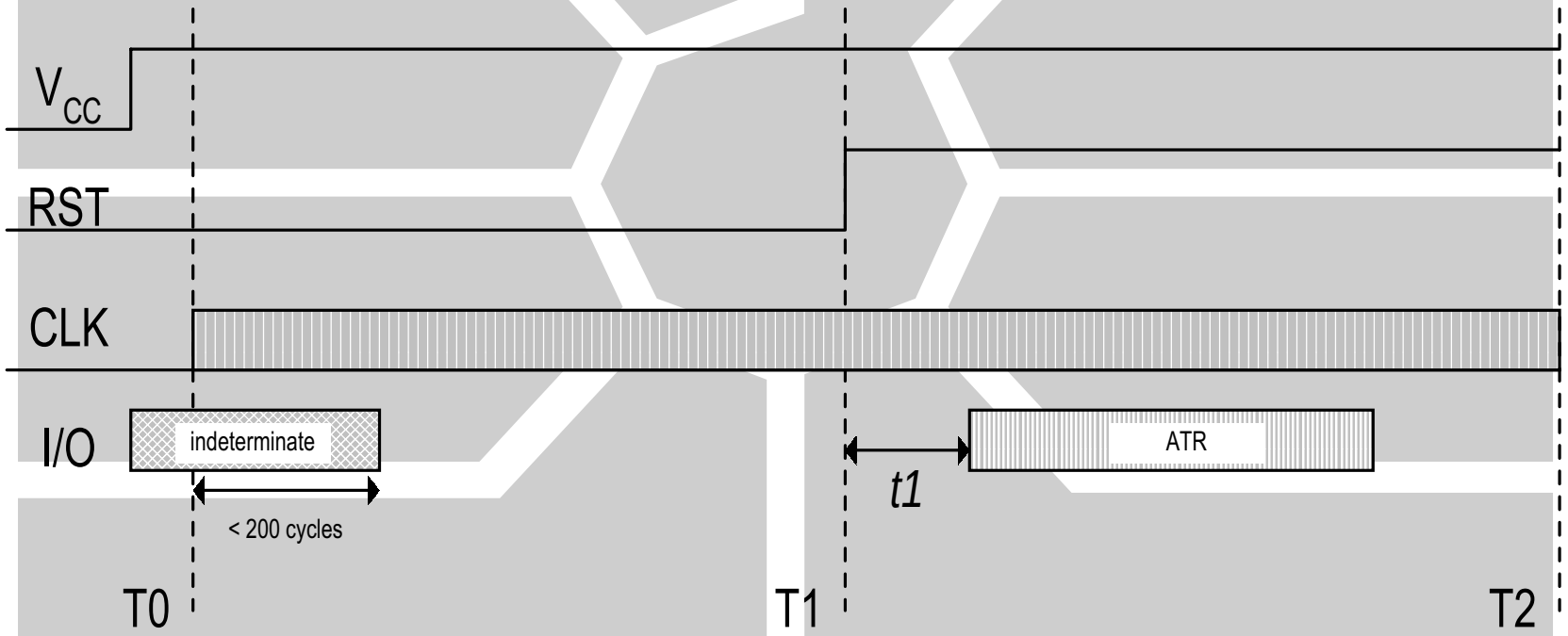




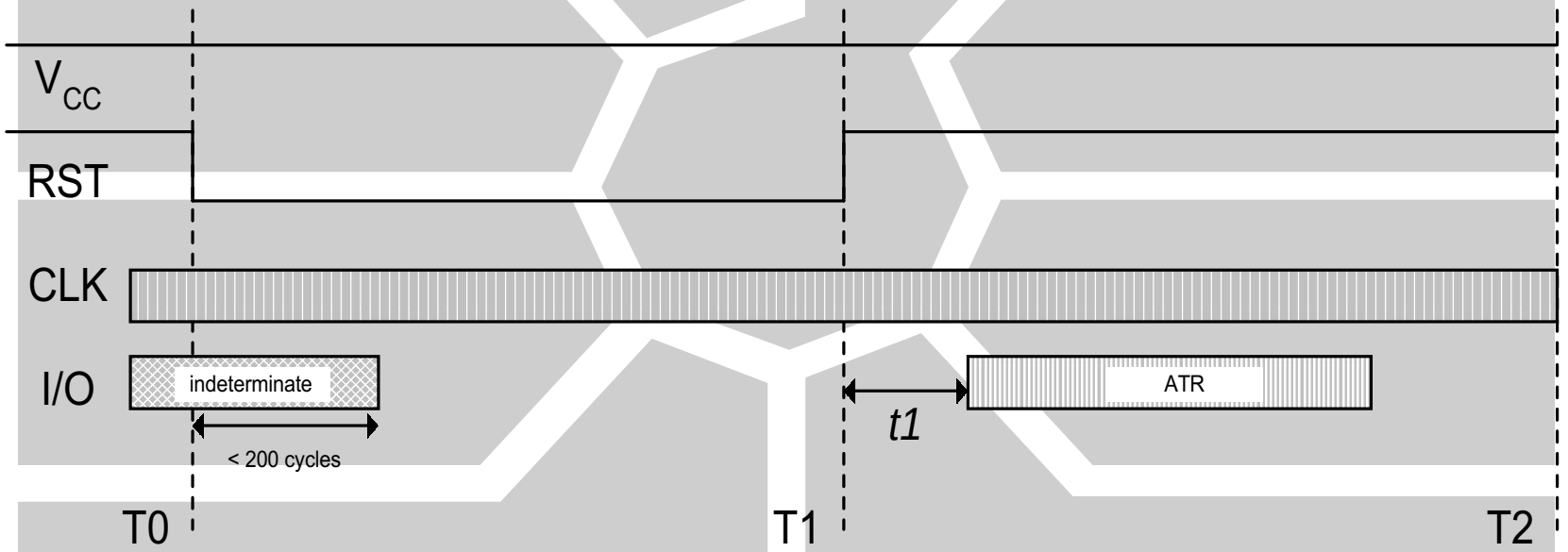
AFNOR POSITION



ISO-7816 Part 3 - Cold Reset



ISO-7816 Part 3 - Warm Reset



ISO-7816 Part 3
Answer To Reset

TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 .T1..Tk Tck

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

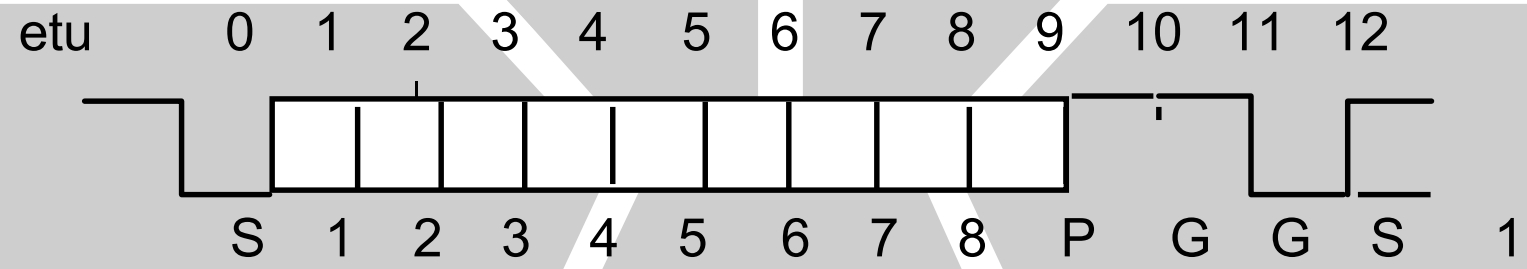
TA2 = specific mode
TB2 = PI2
TC2 = specific
TD2 = Y3, T
TD2 = Y3,T
T1..Tk = historical characters

ISO-7816 Part 3

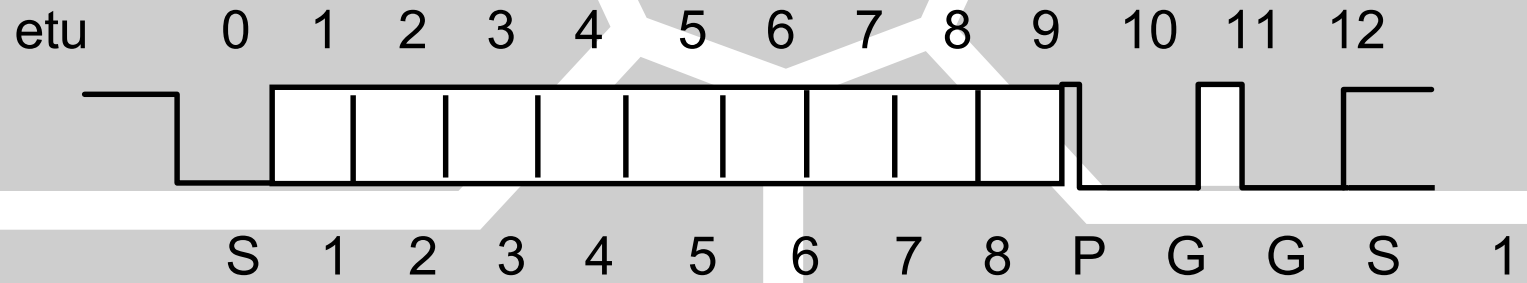
- T=1(block protocol)
  - TBi(i>2) BWI,CWI
  - BWI = block waiting integer
  - CWI = character waiting integer
- T=15 (additional global interface bytes)
  - TAi(i>2) = SI,CI
  - SI = sleep mode indicator
  - CI = class A (5V), class B (3V), class AB

ISO-7816 Part 3
transmitting a byte

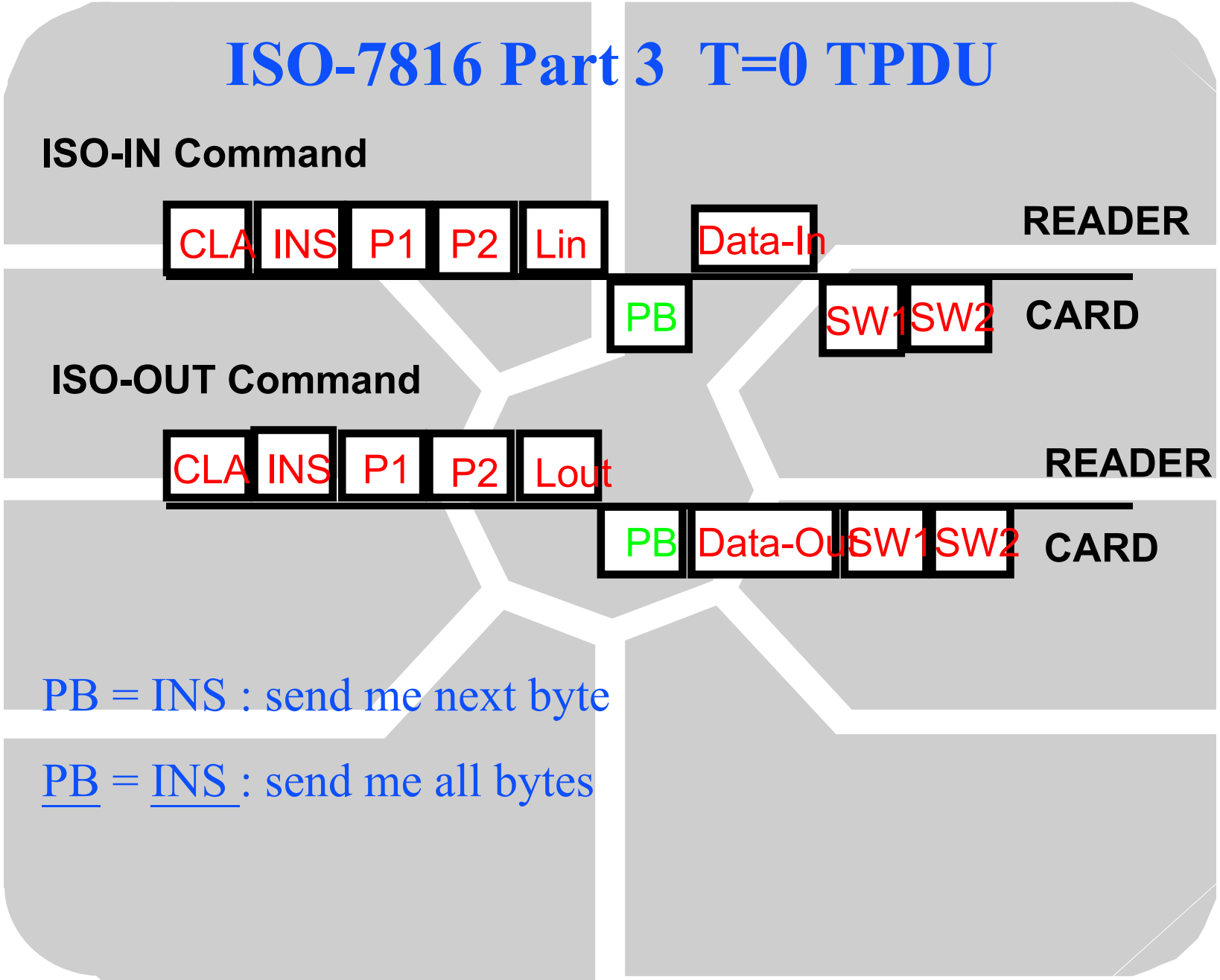
no transmission error



transmission error



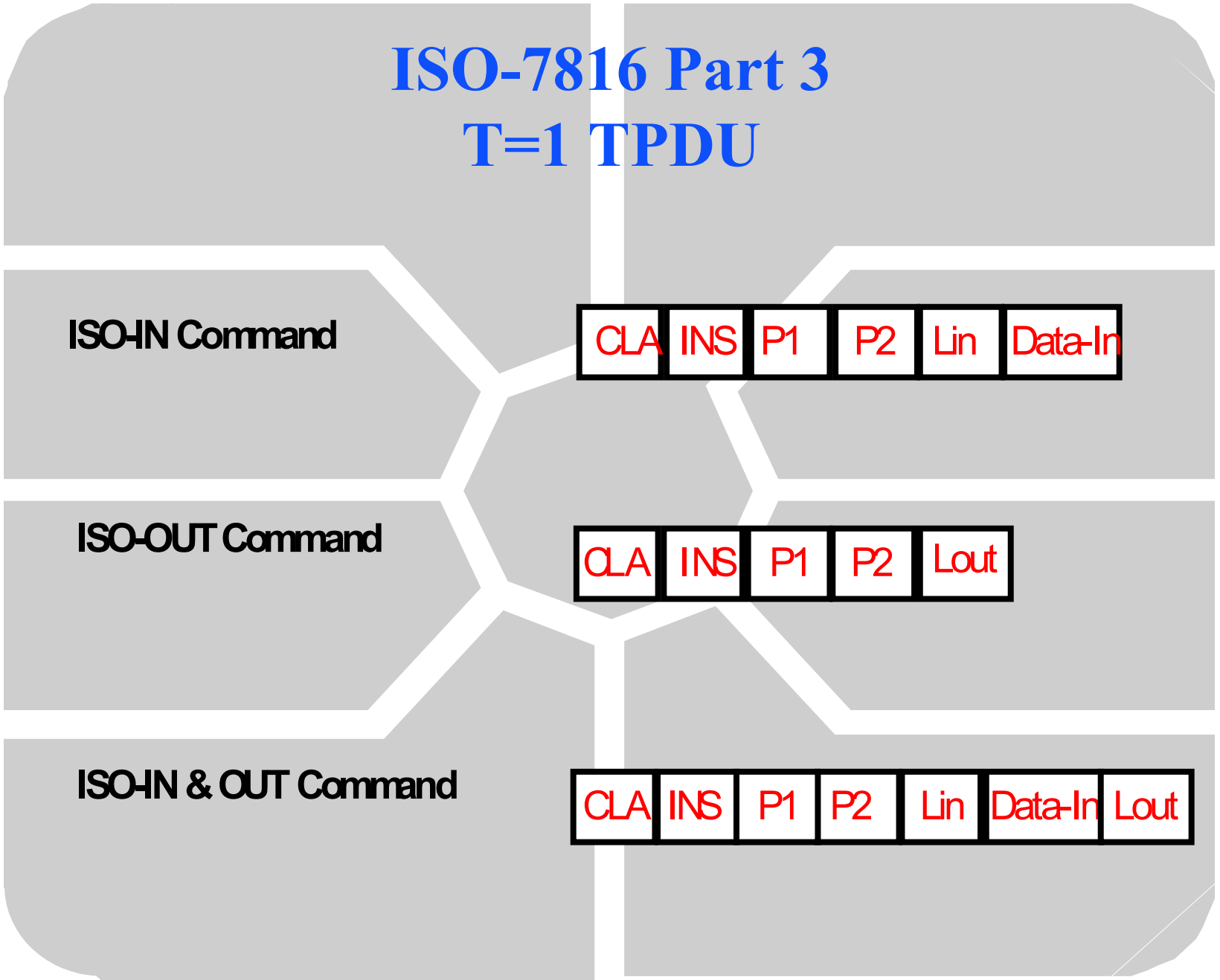
ISO-7816 Part 3 T=0 TPDU



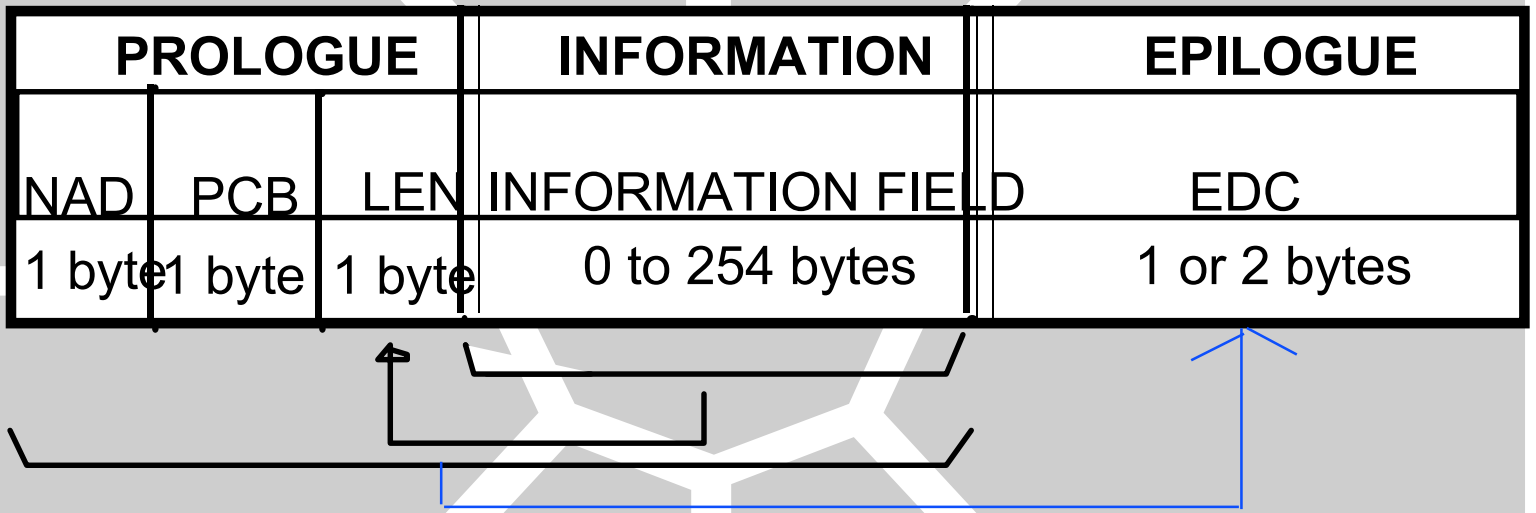
PB = INS : send me next byte

PB = INS : send me all bytes

ISO-7816 Part 3
T=1 TPDU



ISO-7816 Part 3
T=1 TPDU Frame



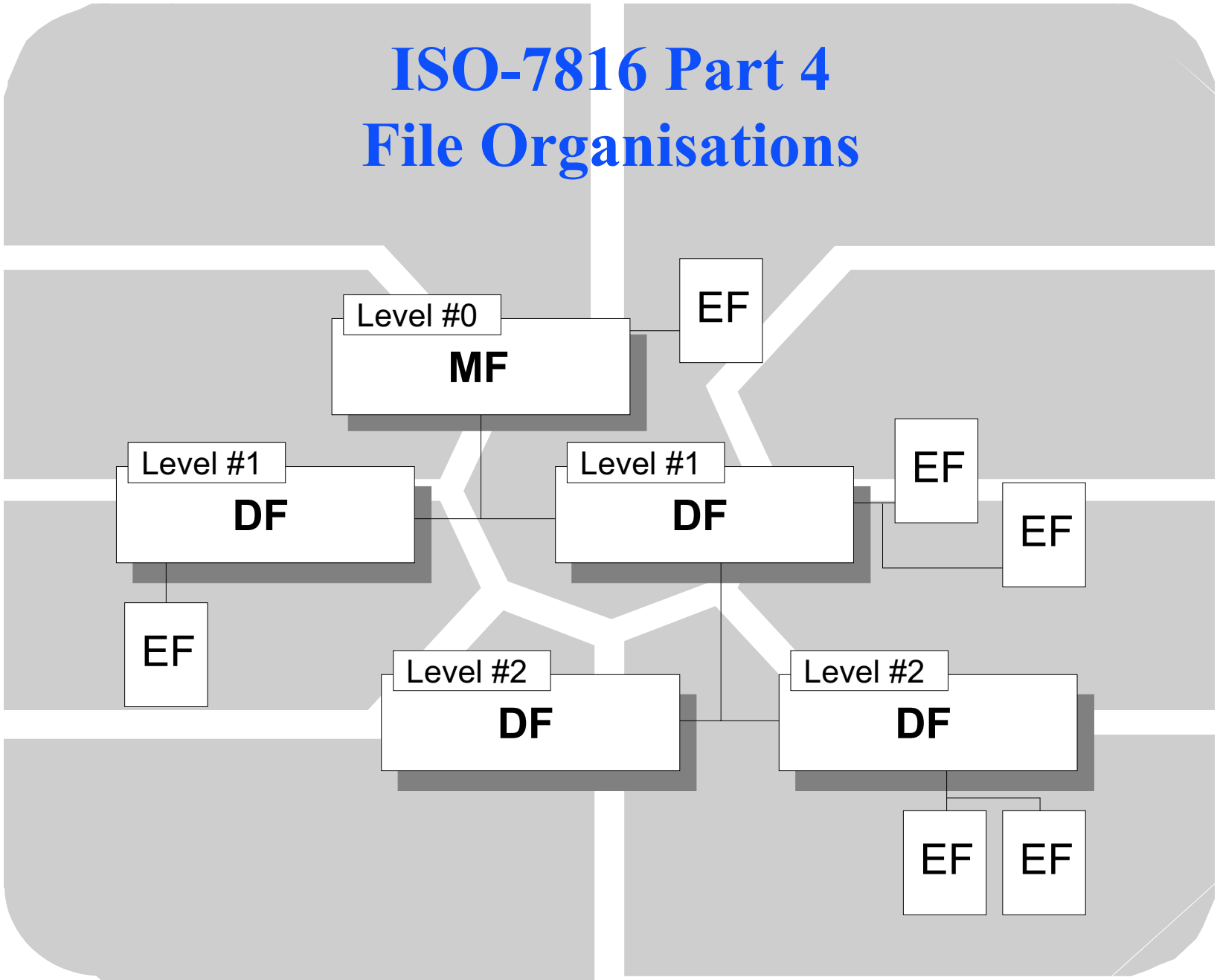
PCB conveys the type of frame

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

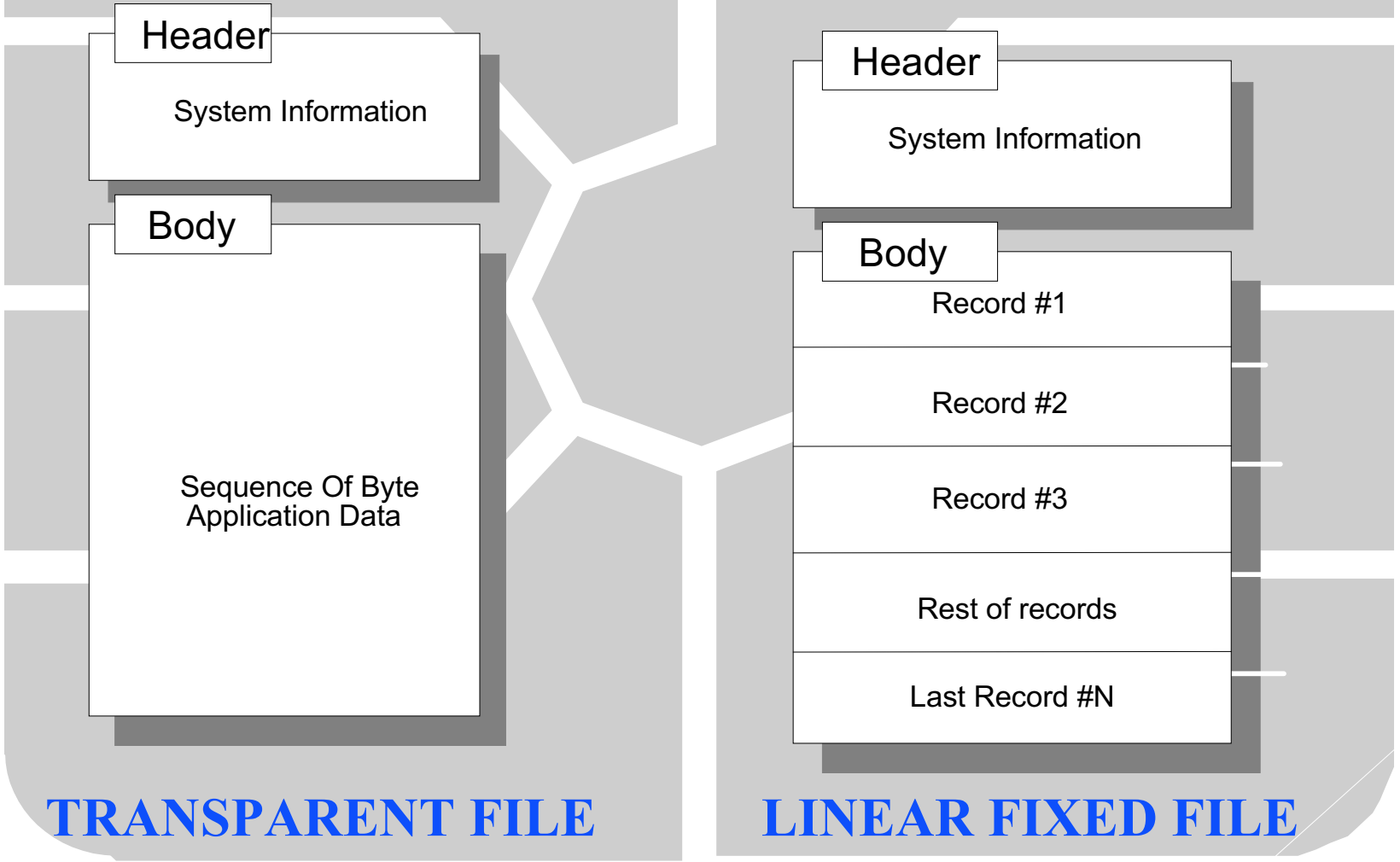
ISO-7816 Part 4
APDU FORMAT

case	command data	response data
1	no data	no data
2	no data	data
3	data	no data
4	data	data

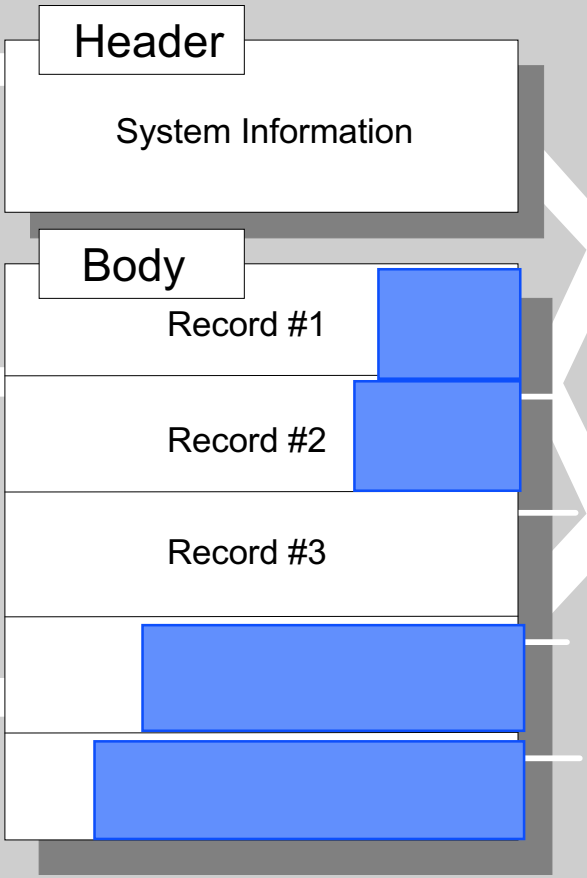
ISO-7816 Part 4
File Organisations

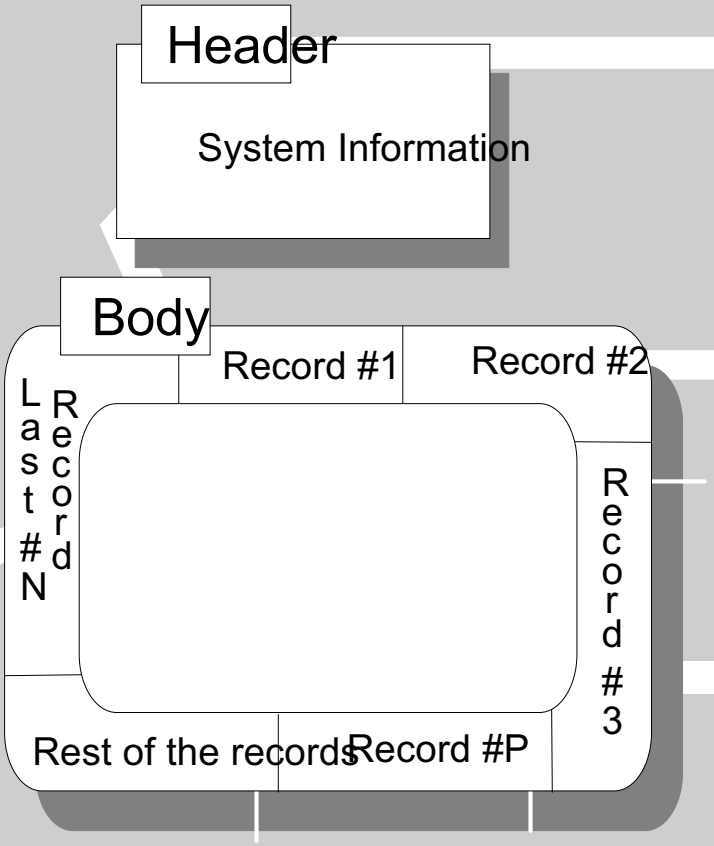


ISO-7816 Part 4
File Structures



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
- GET CHALLENGE
- INTERNAL AUTHENTICATION
- SELECT FILE
- READ BINARY
- READ RECORD(S)
- GET RESPONSE
- ENVELOPE
- GET DATA
- WRITE BINARY
- WRITE RECORD
- UPDATE BINARY
- PUT DATA
- UPDATE RECORD
- APPEND RECORD

Smart Card Security Attributes

- file access
  - read, write, update/erase
  - access locks
  - access in plain or ciphered
  - secured messaging
  - invalidate, rehabitate
- command execution
  - file selection
  - read command
  - write command
  - erase command
  - authentication command
  - credit command
  - debit command

Security Mechanism

- passive authentication
  - VERIFY command with PIN / password
- active authentication
  - INTERNAL AUTHENTICATION with challenge
  - EXTERNAL AUTHENTICATION with response to challenge

Security Mechanism

- data authentication
  - READ, WRITE, UPDATE command with secured messaging
  - protecting access channel
- data encipherment
  - READ, WRITE, UPDATE command with ciphered data

Why Use Smart Card

- What can go wrong with existing systems
- Smart card capabilities
- Some smart card applications
- What problems can smart card solve
- what new services can it provide

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

What Can Go Wrong With Existing Systems

- Magnetic Payphone Card
  - buy 5 fake cards for the price of one
  - tampering with the value
  - frequent cleaning of read/write head
  - local power supply required
- Mobile Phone System
  - eavesdropping of conversation
  - cloning of mobile phone during usage or repair

What Can Go Wrong With Existing Systems

- Pay TV
  - cloning of decoder after customer base established
- Logon To Computer System
  - un-authorised access to computer network

Smart Card Security Capabilities

- card authentication
- terminal authentication
- card-holder authentication
- transaction certification
- data confidentiality

Card Authentication

- terminal ensures that the card is authenticatic before continuation of transaction
- issuer loads into each card & terminal a secret before issuance
- card must prove to the terminal that the card knows the secret
- card must not expose the secret during the authentication process
- since the card knows the secret, it must be an authentic card

Terminal Authentication

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

Card Holder Authentication

- card ensures that only the genuine card holder can use the card
- issuer loads into each card a card-holder PIN
- the card-holder must prove to the card that he knows the PIN
- card grants the card-holder the required access rights since he knows the PIN
- card can commit suicide if there is successive wrong PIN presentation
- biometrics (thumb print, retina / vein pattern, voice, signature dynamics) is also possible

Transaction Certification

- issuer loads an unique certification key into the card before issuance
- terminal sends transaction into the card after successful card, terminal and card-holder authentication
- 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 take place
- can be used for non-repudiation and data integrity

Data Confidentiality

- issuer loads an unique encryption key into each card before issuance
- this key is used to encrypt data between the terminal and the remote host

Smart Card Applications
Telecommunication Prepaid Card

- lower infra-structure cost
  - local supply not required
- lower maintenance cost
  - less frequent R/W head cleaning
  - no moving mechanism
- cash in advance
  - unspent money
- opportunity for new service - card roaming
- opportunity for new markets
- electronic purse

Smart Card Applications
Mobile Communication - GSM / PCN

- no evasdropping of conversation
- no cloning of handset
- regional roaming
- lower cost of handset
- more value-added services
  - ★fixed dialing
  - ★advice of charge
  - ★short messages service
  - ★SIM ToolKit
  - ★etc

Smart Card Applications - Banking

- Credit Card - Europay Master Visa
  - off-line & semi on-line transaction
  - no cloning of card
  - value added services eg loyalty
- Debit Card / Electronic Passbook / Electronic Purse
  - security
  - off-line transaction
  - high availablility, speed of service
  - low cost per transaction
  - low system infra-structure

Smart Card Applications - Retail

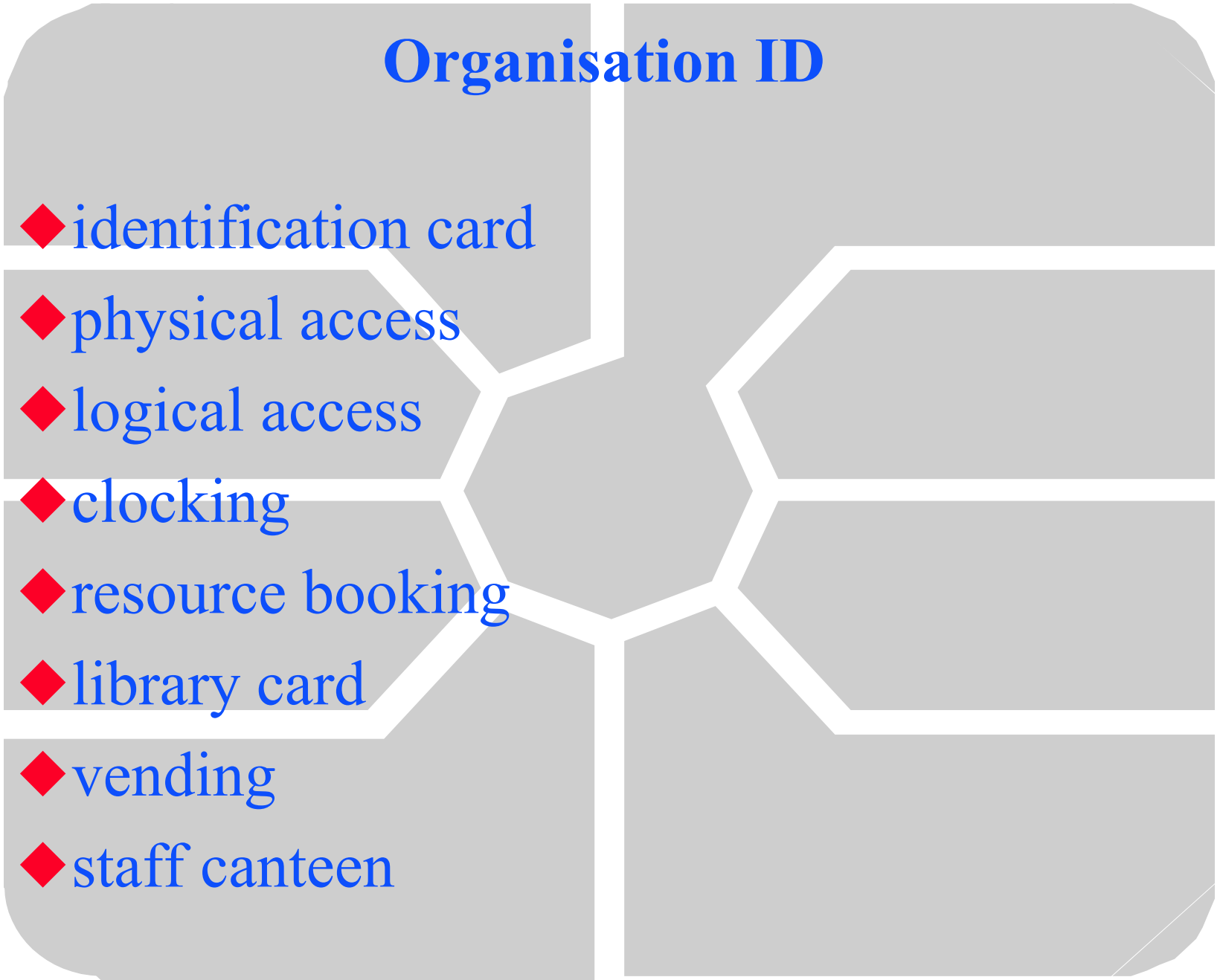
- Loyalty Card
  - collect & analyse customer needs
  - increase market share
  - increase profit
  - provide value-added services
  - retain customer loyalty
- Gift Voucher / Prepaid Card
  - increase market share
  - increase profit

Smart Card Applications - Portable File

- Health & Insurance
  - administrative cost saving thru' automation
  - fraud control
  - wastage control
  - prevent abuses
  - medical records

Smart Card Applications - Gaming

- profit depends on how fast one can play
- money no longer idling in the machines but earning interest in the bank
- easy management and control
- reduce fraud


Organisation ID
identification card
physical access
logical access
clocking
resource booking
library card
vending
staff canteen

Smart Card Applications

- smart card is just a very small part in a system, but affecting the entire system
- it is analogous to an intelligent diskette
- what you want is a solution
- using smart card does not automatically imply security, the system design together with smart card makes it secure
- smart card is not always the best solution if smart card capabilities not utilised