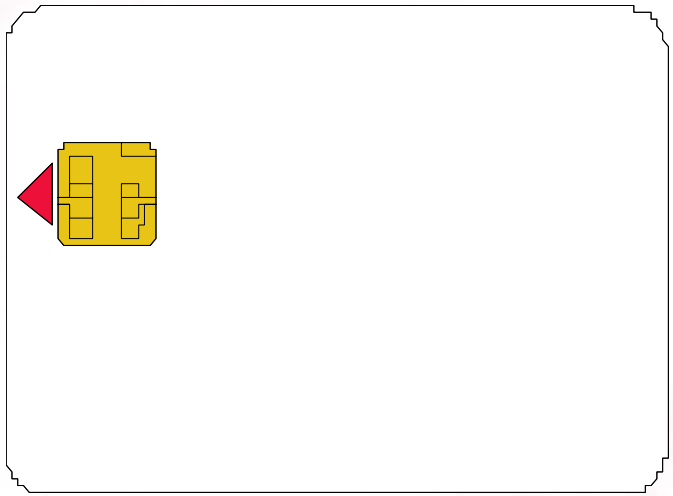
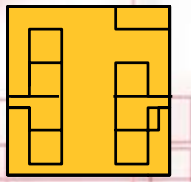
What is a Smart Card



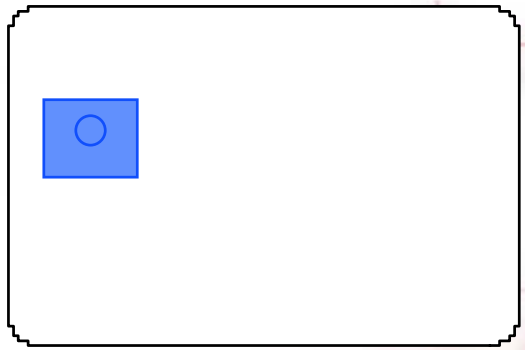
- A credit card-sized plastic with a single IC chip on board conforming to ISO-7816

Components of a Smart Card



Contact disc

Chip



Plastic body

- A smart card comprises of 3 parts
  - Contact disc
  - Chip
  - Plastic body with cavity

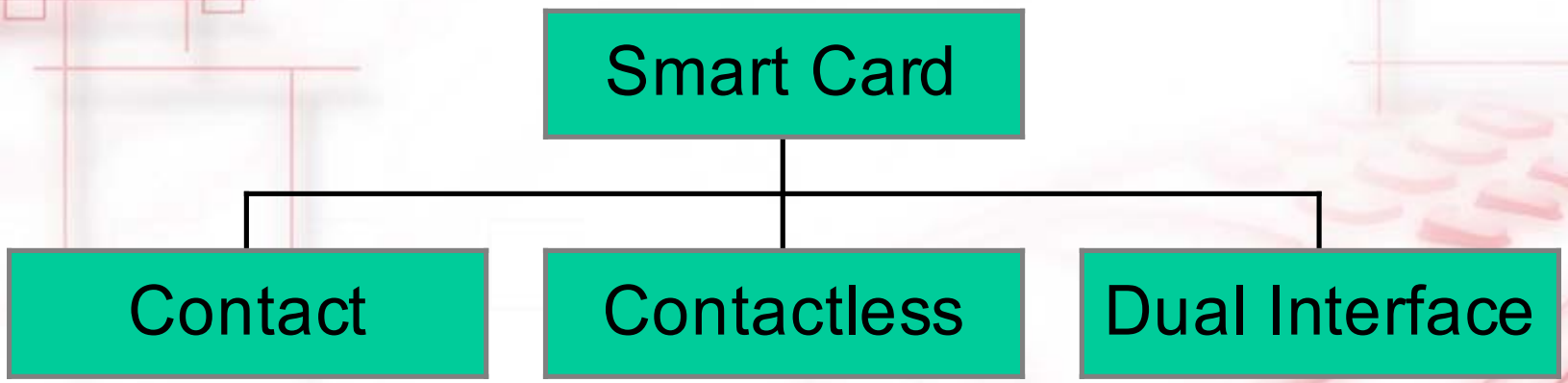
Contact Disc

- 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 card from the contact disc

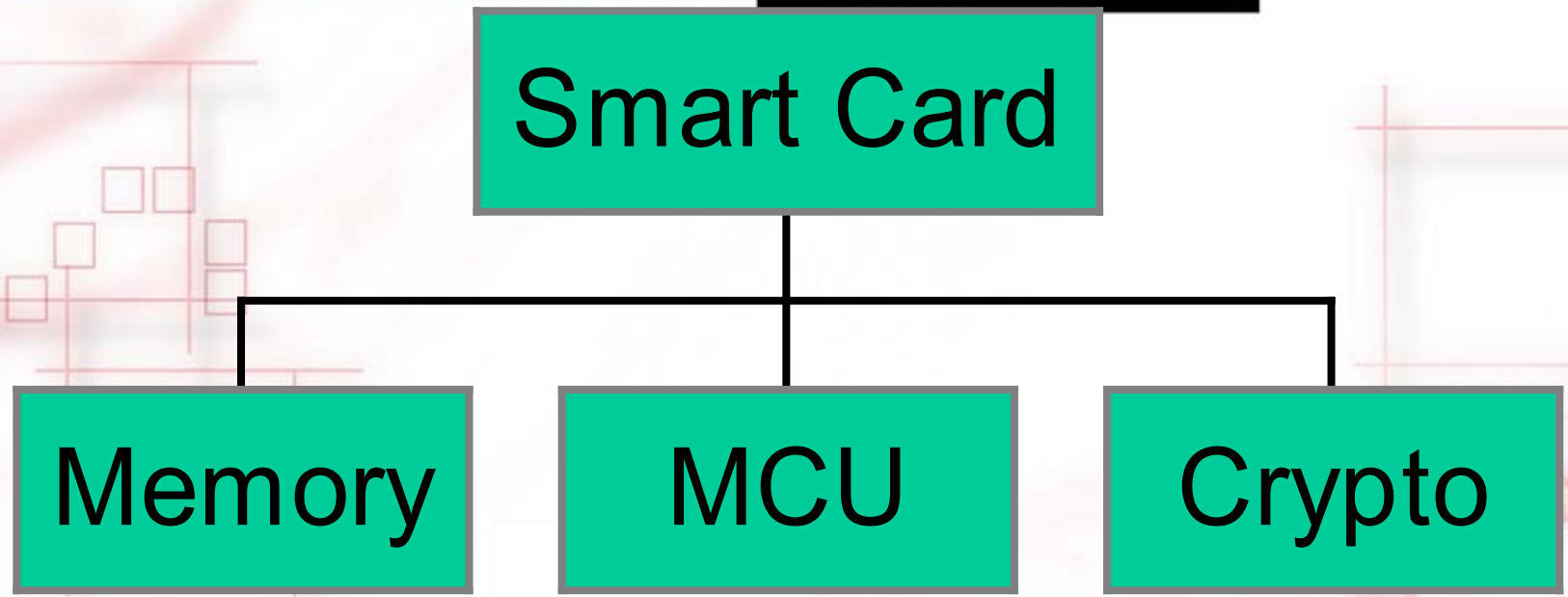
Smart Card / IC Card Family

- Contact Memory Card
  - Infineon, Atmel
- Contact CPU Card
  - GSM SIM, Smart Debit/Credit
  - National smart card (banking / ID card)
- Contactless Memory Card
  - Philips / Infineon, Sony, Legic
- Dual Interface CPU Card

Categorization By Technology



Categorization By Security

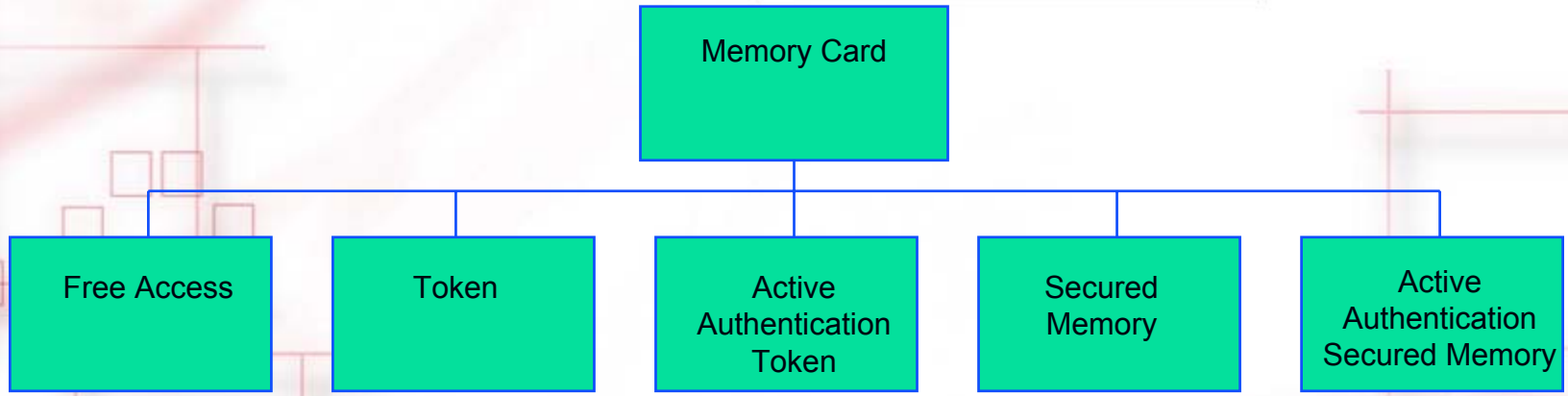


- Payphone
- Proprietary applications

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

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

Type Of Contact Memory Card



Atmel

AT24SC01,02,04,08,16

Infineon

SLE4432

SLE4418

STMicroelectronics

ST1305

Infineon

SLE4406

STMicroelectronics

ST1333,ST1335

Infineon

SLE4436,SLE5536

Atmel

AT88SC101,102

AT88SC1003

Infineon

SLE4442

SLE4428

Atmel

AT88SC153

AT88SC1601,04,08,16

Infineon

SLE4463

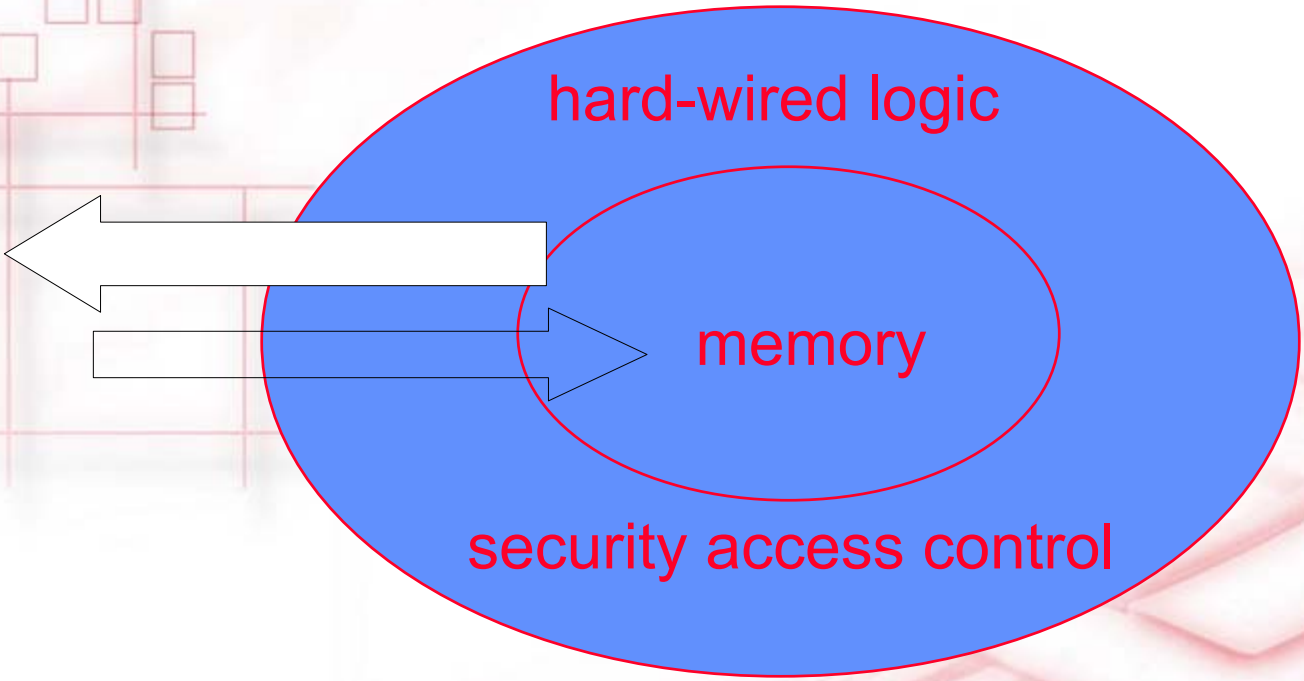
Chip

- Memory
  - Infineon
  - Atmel
- Embedding by card manufacturers
- CPU
  - STMicroelectronics
  - Atmel
  - Hitachi
  - Infineon
  - Philips
- Card manufacturers must design the chip operating system

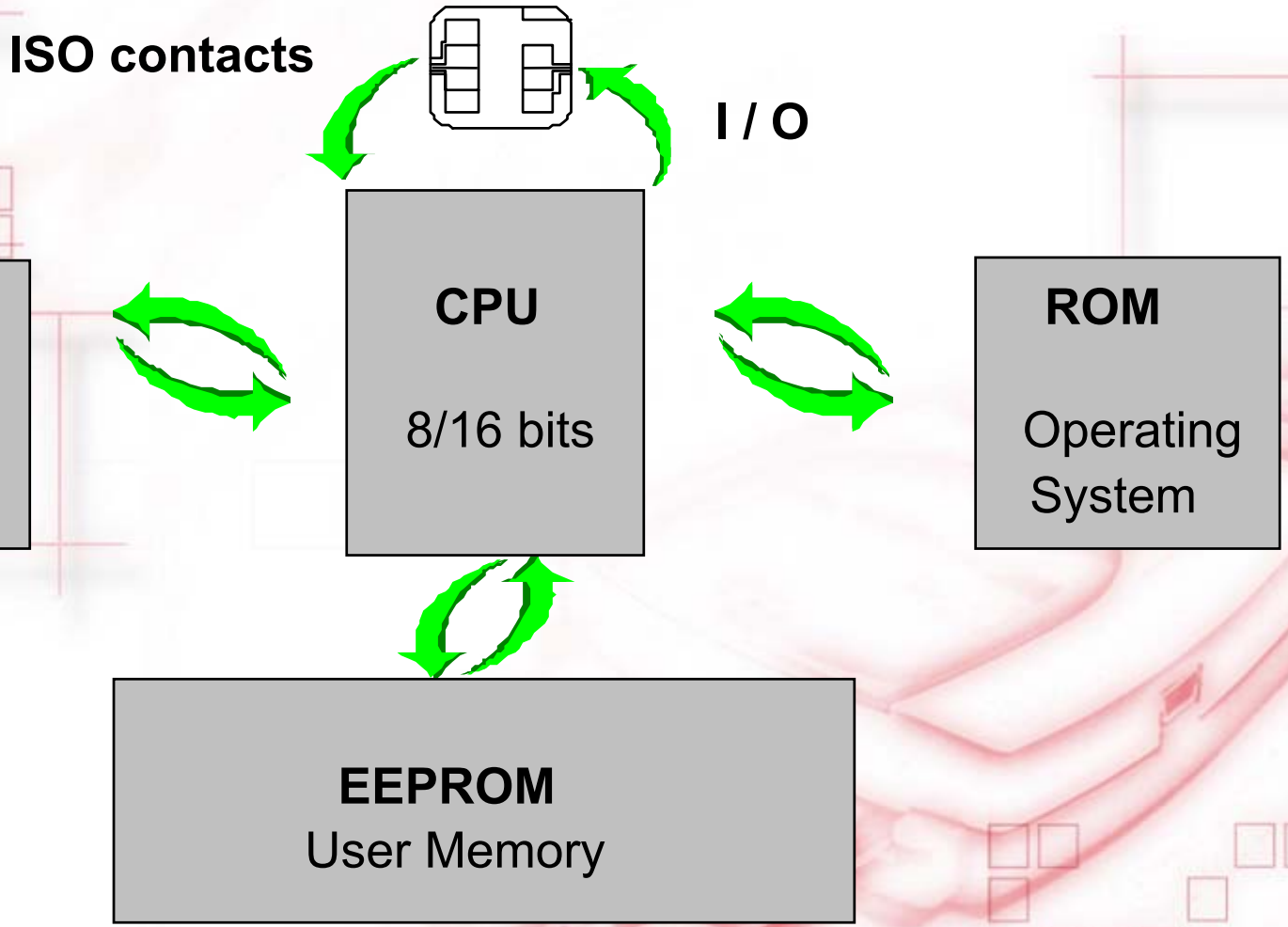
Plastic Body

- ABS
  - Difficulty in embossing, thermal transfer printing, hot stamping, metallic colours, magnetic stripe
  - Injection mould (cheaper)
- PVC
- PETG
- Polycarbonate (PC)

Memory Card Security Architecture



CPU Card Architecture



Smart Card

- Memory size is described in bits / bytes
- Memory size is referring 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 128 Kbytes
  - RAM ~100 bytes to a few Kbytes
  - EEPROM 512 bytes to 64 Kbytes

Smart Card CPU – In Early 90s

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

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

Smart Card CPU

Infineon	ROM (bytes)	RAM (bytes)	E2PROM (bytes)
44C80	15K	256	8K
66C40P	30K	1024	4K
66C80P	30K	1024	8K
66CX160S	32K	1980	16K
66C160S	32K	1280	16K
66C320S	32K	1280	32K
66C324P	134K	4352	32K
66C644P	134K	5052	64K

Smart Card CPU – In 2002

Philips	ROM (Kbytes)	RAM (bytes)	E2PROM (Kbytes)	
P8WE6004	32	768	4	
P8WE6008	32	1280	8	
P8WE6017	48	1280	16	
P8WE6032	32	1280	32	
P8WE6033	96	2304	32	
P8WE5008	32	2304	8	crypto
P8WE5016	32	2304	16	crypto
P8WE5017	64	2304	16	crypto
P8WE5032	32	2304	32	crypto
P8WE5033	96	2304	32	crypto

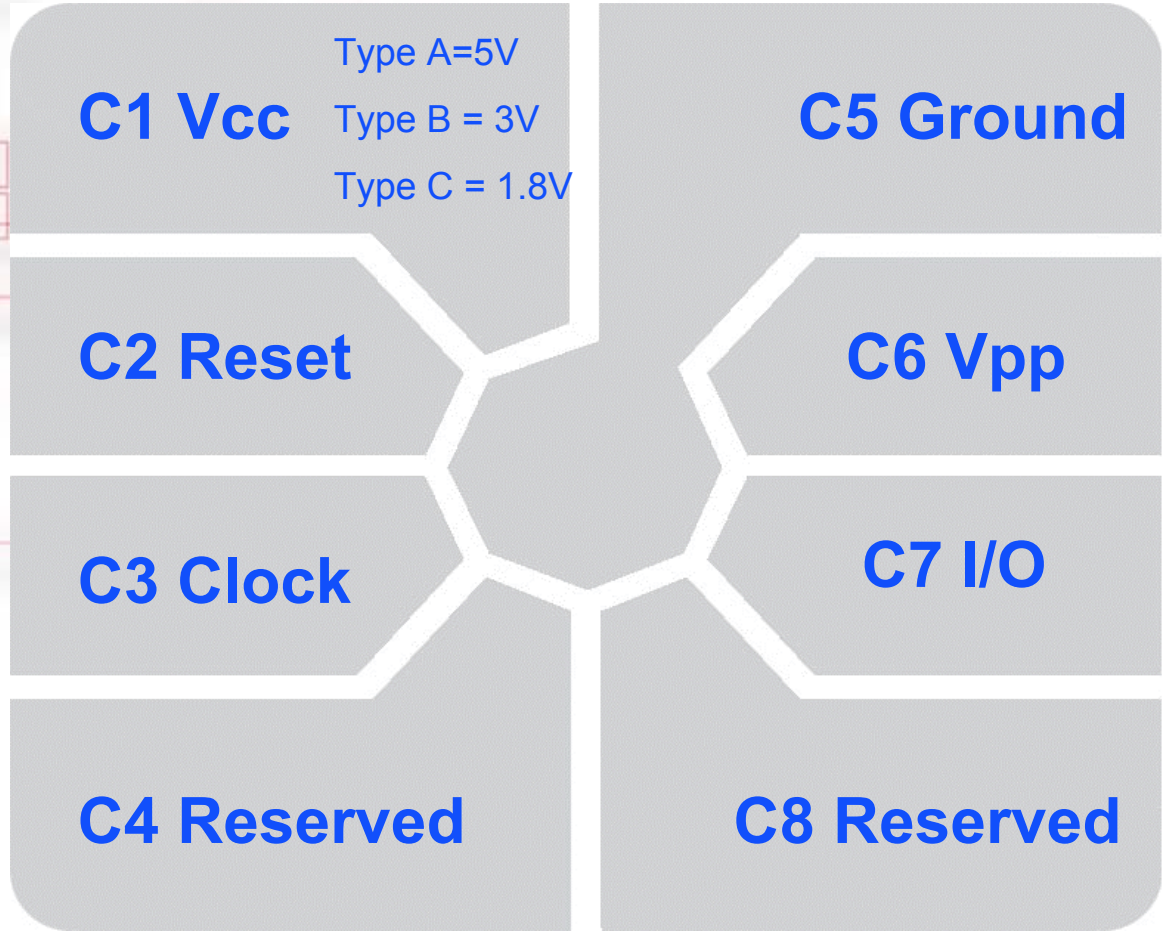
Smart Card Standard ISO-7816

- Part 1: Physical Characteristics
- Part 2: Dimensions & Location of Contacts
- Part 3: Electronic Signals & Transmission Protocols
- 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
- Part 9: Additional Inter-industry Commands & Security Attributes
- Part 10: Electronic Signals & ATR for Synchronous Card
- Part 11: Personal Verification Through Biometric Method
- Part 12: USB Electrical Interface And Operating Procedure
- Part 13: Registration Of IC Card Manufacturer
- Part 15: Cryptographic Information Application

ISO-7816 Part 1 Physical Characteristics

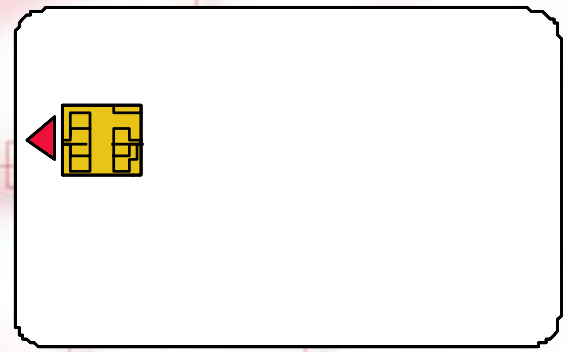
- UV light
- X-ray
- contacts surface profile
- ESD
- torsion
- heat dissipation
- bending
- mechanical strength of card, contacts
- EMI
- bending

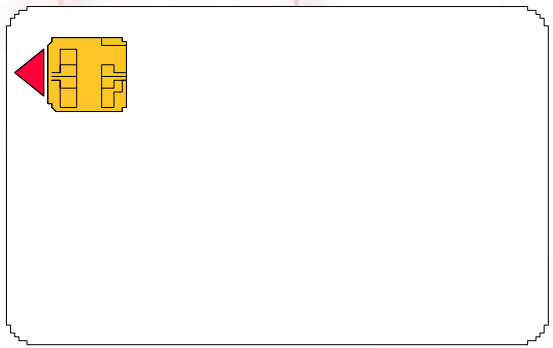
ISO-7816 Part 2

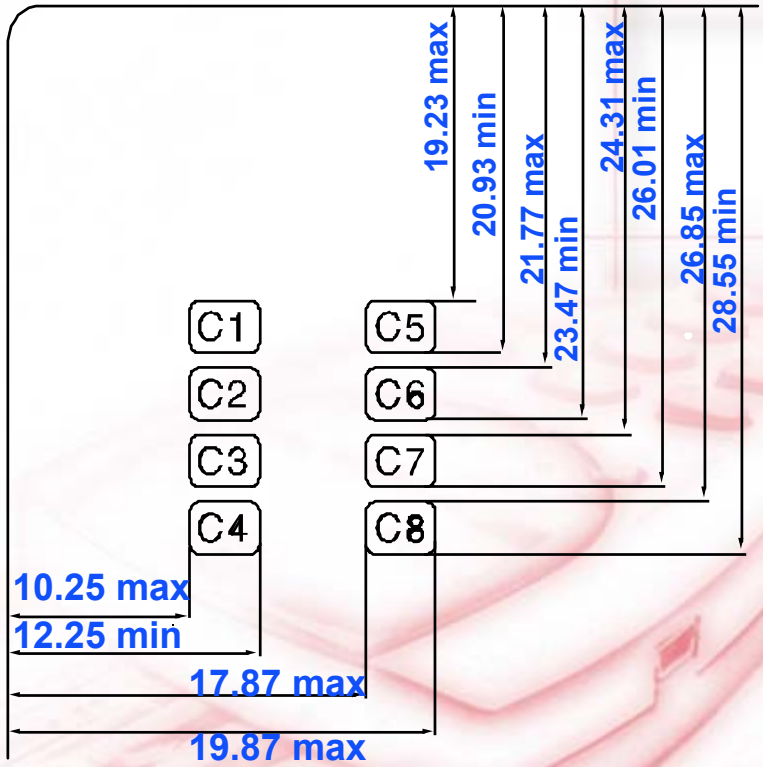


ISO-7816 Part 2 -- Location & Assignment If Contacts

ISO POSITION

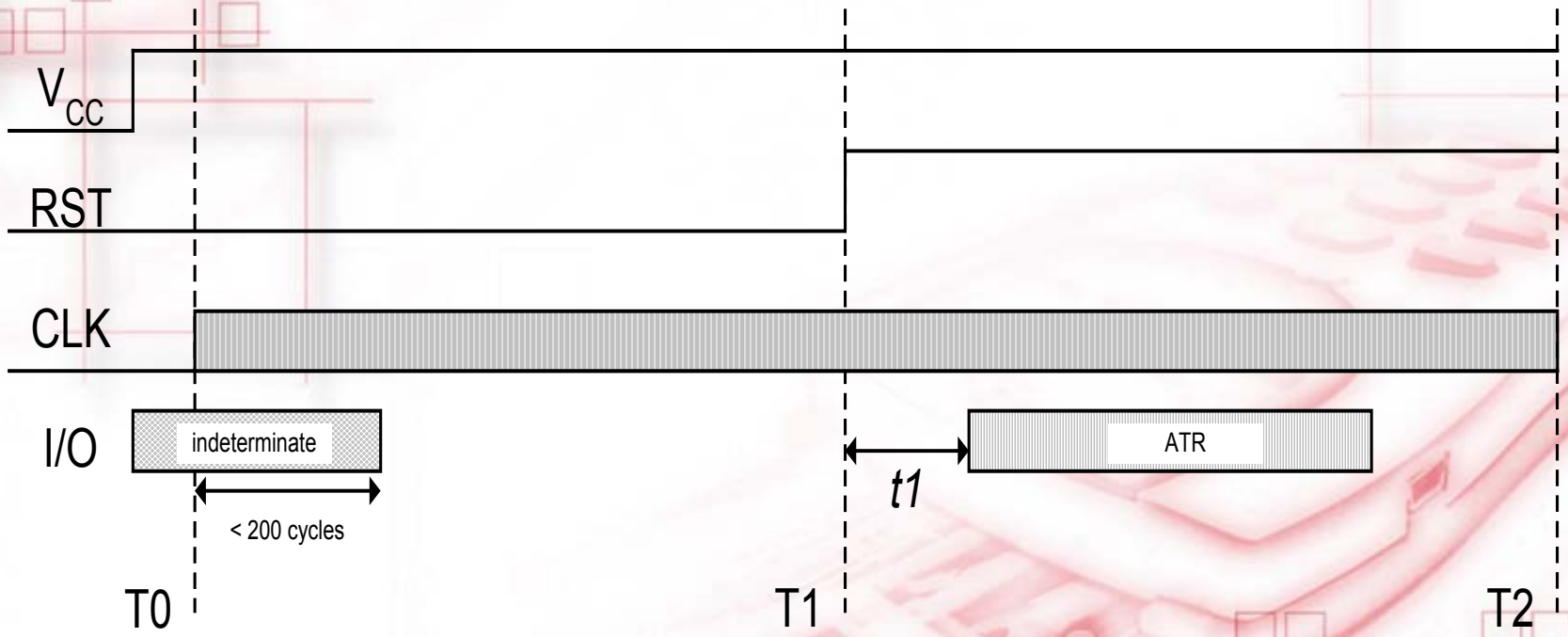




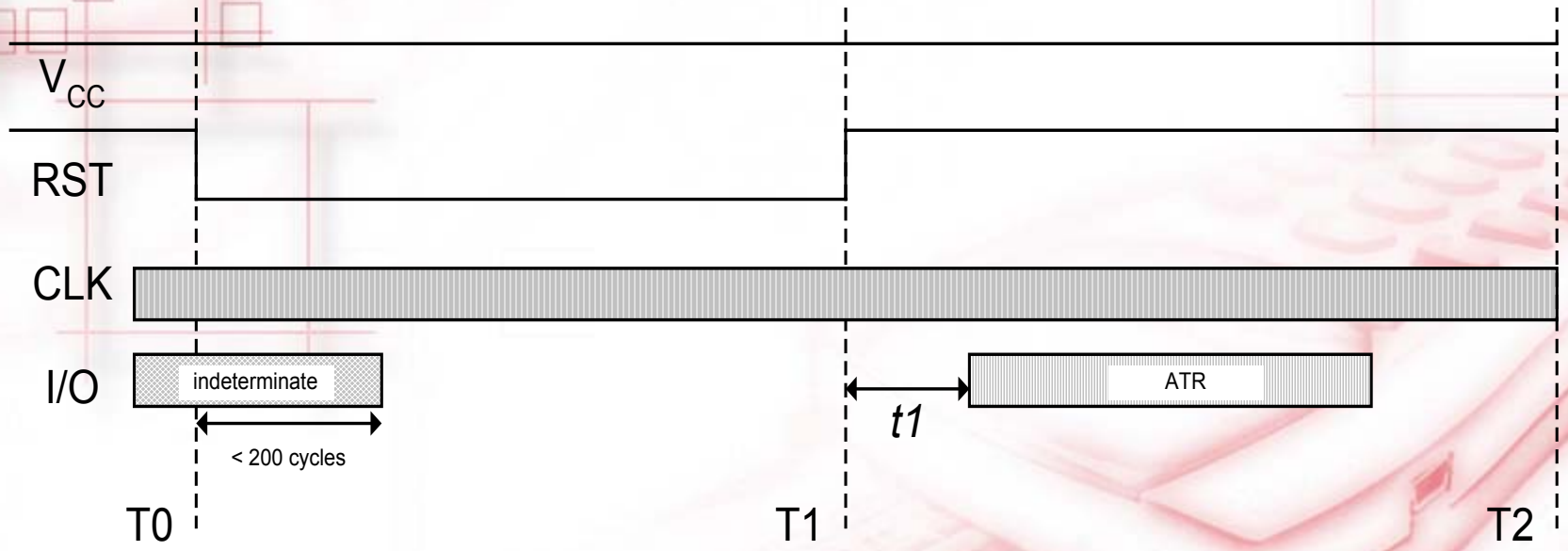


AFNOR POSITION

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

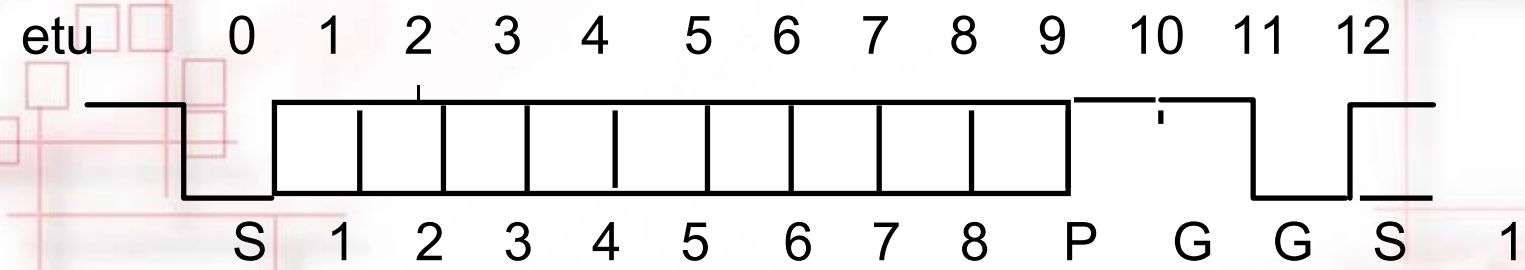
TA2 = specific mode
TB2 = PI2
TC2 = specific
TD2 = Y3, T
TD2 = Y3,T
T1..Tk = historical characters

ISO-7816 Part 3

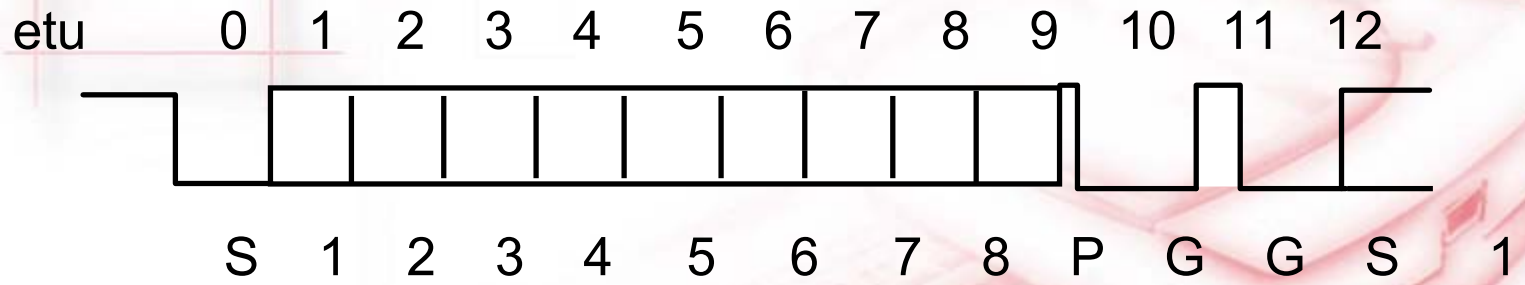
- T=1 (block protocol)
  - TBi(i>2) BWI,CWI
  - BWI = Block Waiting Integer
  - CWI = Character Waiting Integer
- T=15 (Additional global interface bytes)
  - TAi(i>2) = SI,CI
  - SI = Sleep mode Indicator
  - CI = class A (5V), class B (3V), class AB

ISO-7816 Part 3 -- Transmitting a Byte

no transmission error

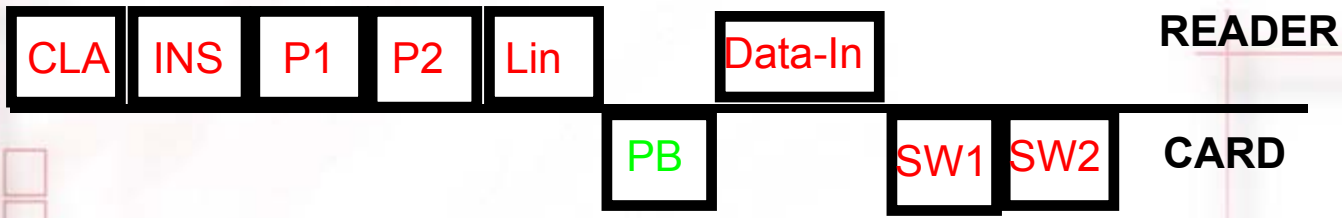


transmission error

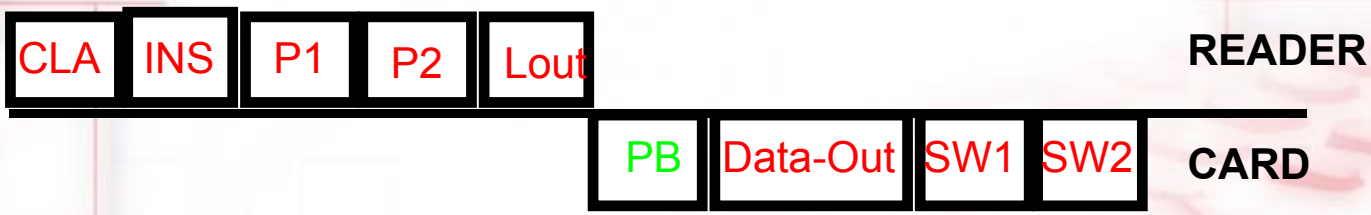


ISO-7816 Part 3 T=0 TPDU

ISO-IN Command



ISO-OUT Command



PB = INS : send me next byte

PB = INS : send me all bytes

ISO-7816 Part 3 -- T=1 TPDU

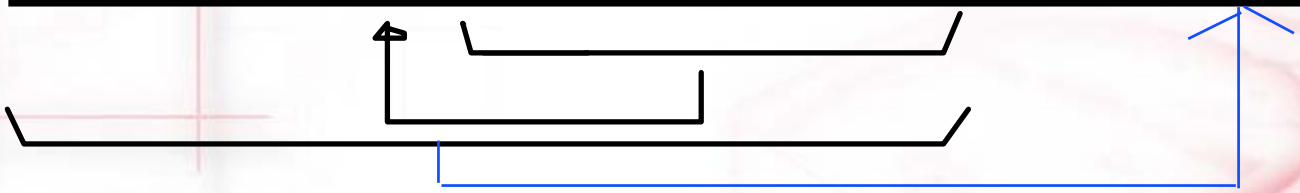
ISO-IN Command

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



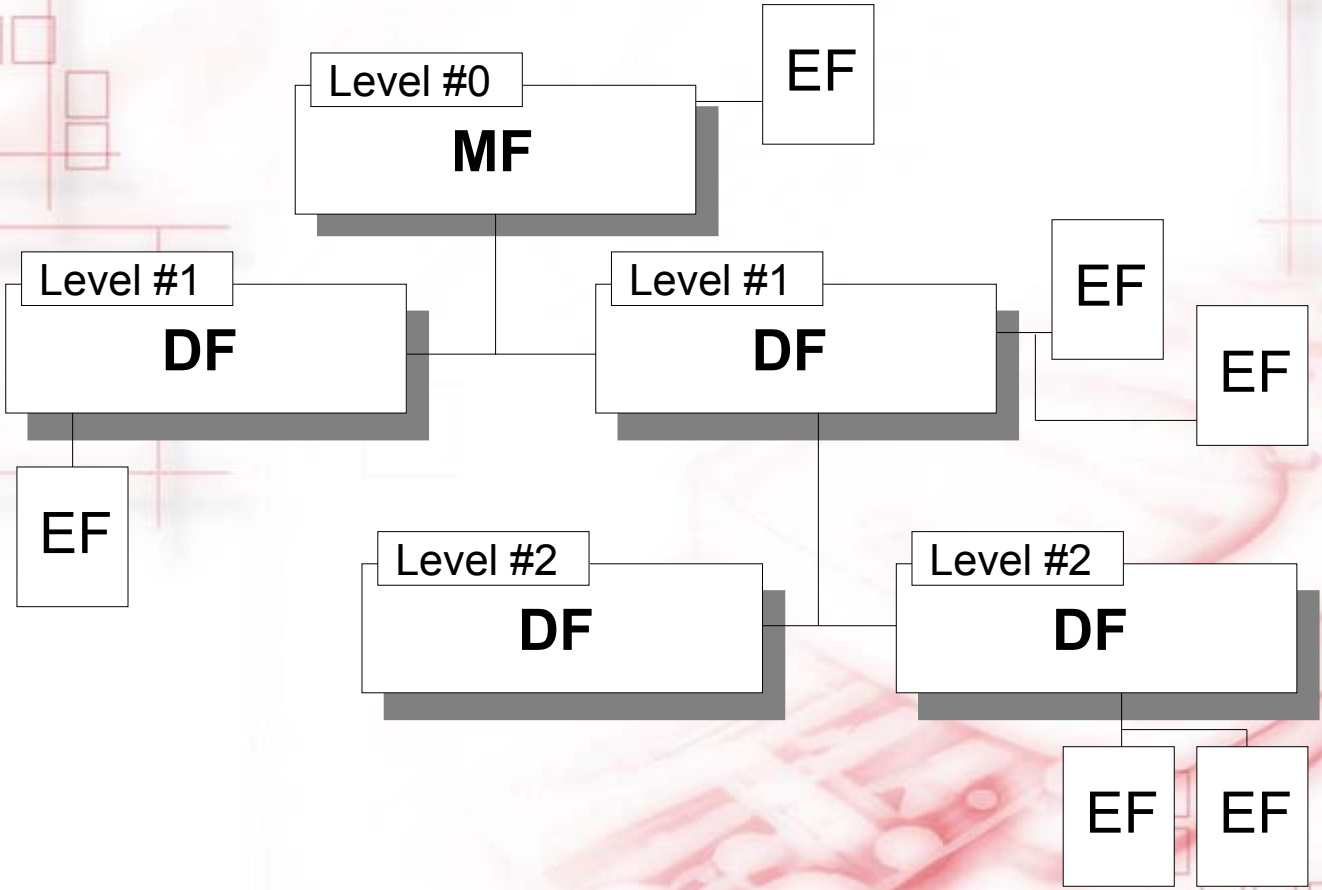
PCB conveys the type of frame

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

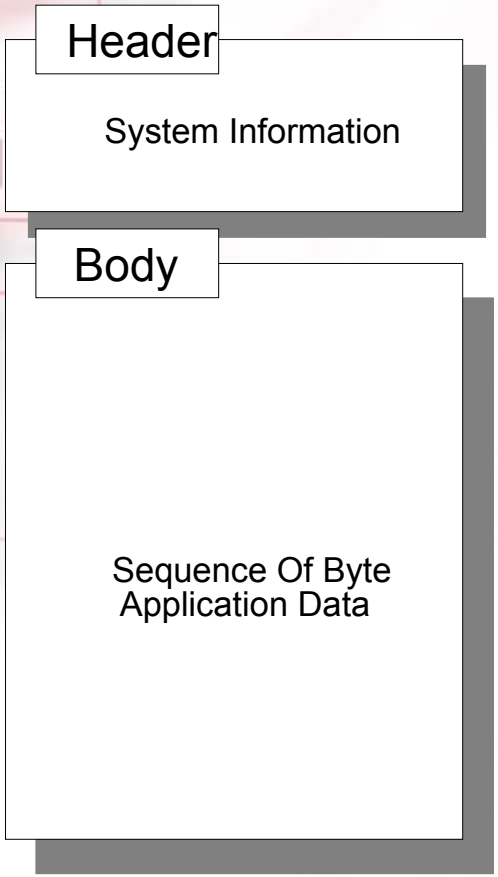
ISO-7816 Part 4 -- APDU FORMAT

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

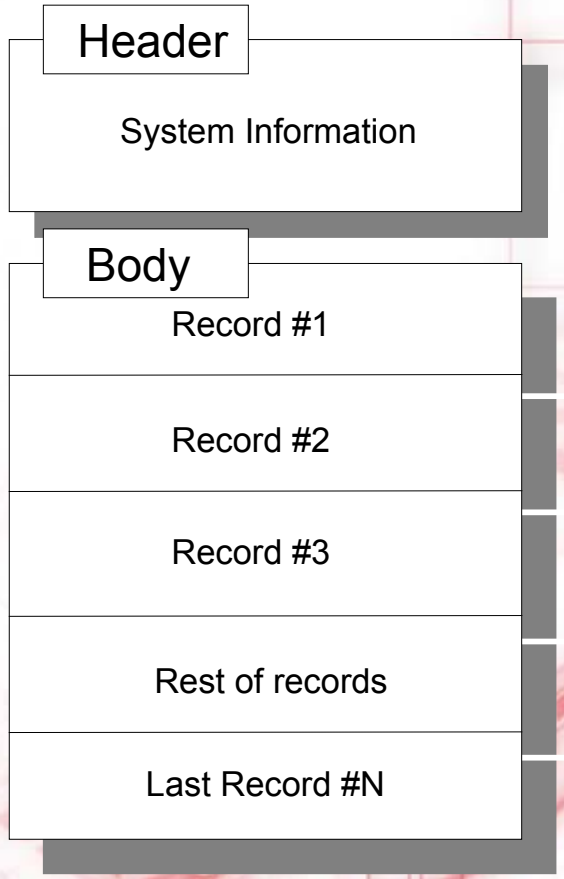
ISO-7816 Part 4 -- File Organizations



ISO-7816 Part 4 -- File Structures

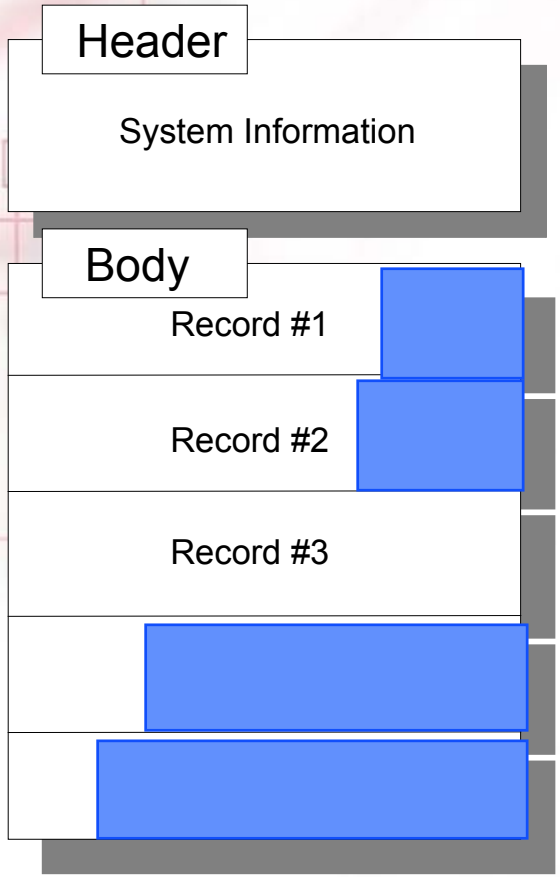


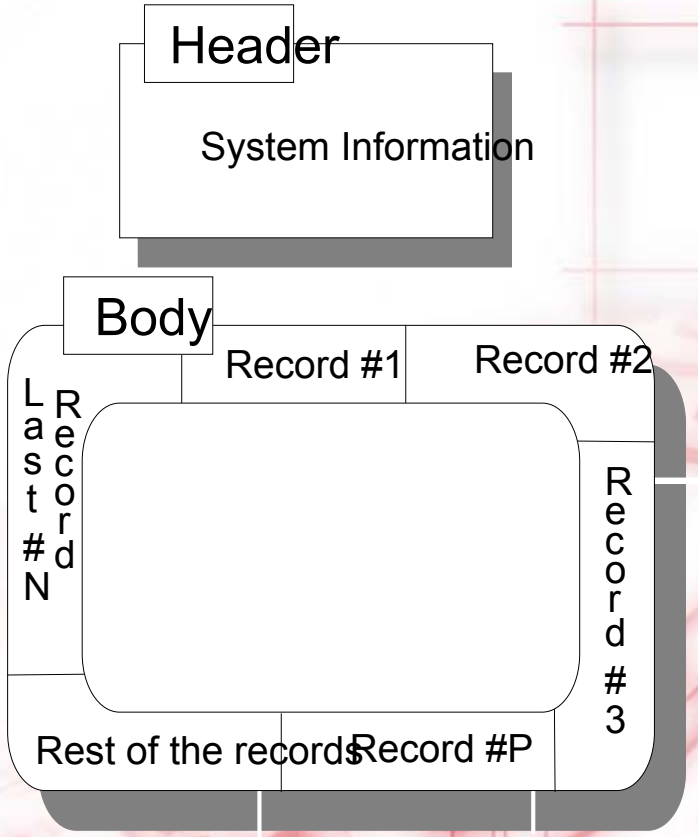
TRANSPARENT FILE



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
- 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

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
  - Unauthorized access to computer network

Smart Card Security Capabilities

- Card authentication
- Terminal authentication
- Cardholder authentication
- Transaction certification
- Data confidentiality

Card Authentication

- Terminal ensures that the card is authentic 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 cardholder PIN
- The cardholder must prove to the card that he knows the PIN
- Card grants the cardholder the required access rights since he knows the PIN
- Card can commit suicide if there is successive wrong PIN presentations
- Biometric methods (fingerprint, retina/vein pattern, voice, signature dynamics) are also possible

Transaction Certification

- Issuer loads a unique certification key into the card before issuance
- Terminal sends transaction into the card after successful card, terminal and cardholder 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 has actually taken place
- Can be used for non-repudiation and data integrity

Data Confidentiality

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

Smart Card Market, History and Forecast

Market (Million pieces)	1997	2003	CAGR
Public telephone	684	3270	30%
Wireless telephone	69	760	49%
Banking	49	690	55%
Loyalty	22	320	56%
Health	16	210	54%
Pay TV	12	150	52%
Transport	8	240	77%
Gaming	2	70	78%
Access Control	10	260	72%
Identification	2	50	71%
E-Security	1	120	142%
Others	24	170	38%
TOTAL	899	6310	36%

Smart Card Chips Usage

Company	'01 units	'00 units	'01 CPU	'00 CPU	'01 memory	'00 memory
Infineon	1142	955	281	249	861	706
ST	652	668	220	280	432	387
Philips	207	80	105	50	102	25
Hitachi	130	135	128	133	2	2
Atmel	83	77	62	54	21	23
Samsung	50	30	50	30	0	0
Others	54	44.5	36	36.5	18	8
Total	2318	1989.5	882	832.5	1436	1151

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 eavesdropping of conversation
- No cloning of handset
- Regional roaming
- Lower cost of handset
- Value-added services
  - Fixed dialing
  - Advice of charge
  - Short messages service
  - SIM ToolKit
  - Etc.

Smart Card Applications - Banking

- **Smart Debit / Credit Card - Europay Master Visa**
  - Offline & semi online transaction
  - No cloning of card
  - Value added services e.g. loyalty
- **Debit Card / Electronic Passbook / Electronic Purse**
  - Security
  - Offline transaction
  - High availability, speed of service
  - Low cost per transaction
  - Low system infrastructure

Smart Card Applications - 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

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

Organization 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 utilized