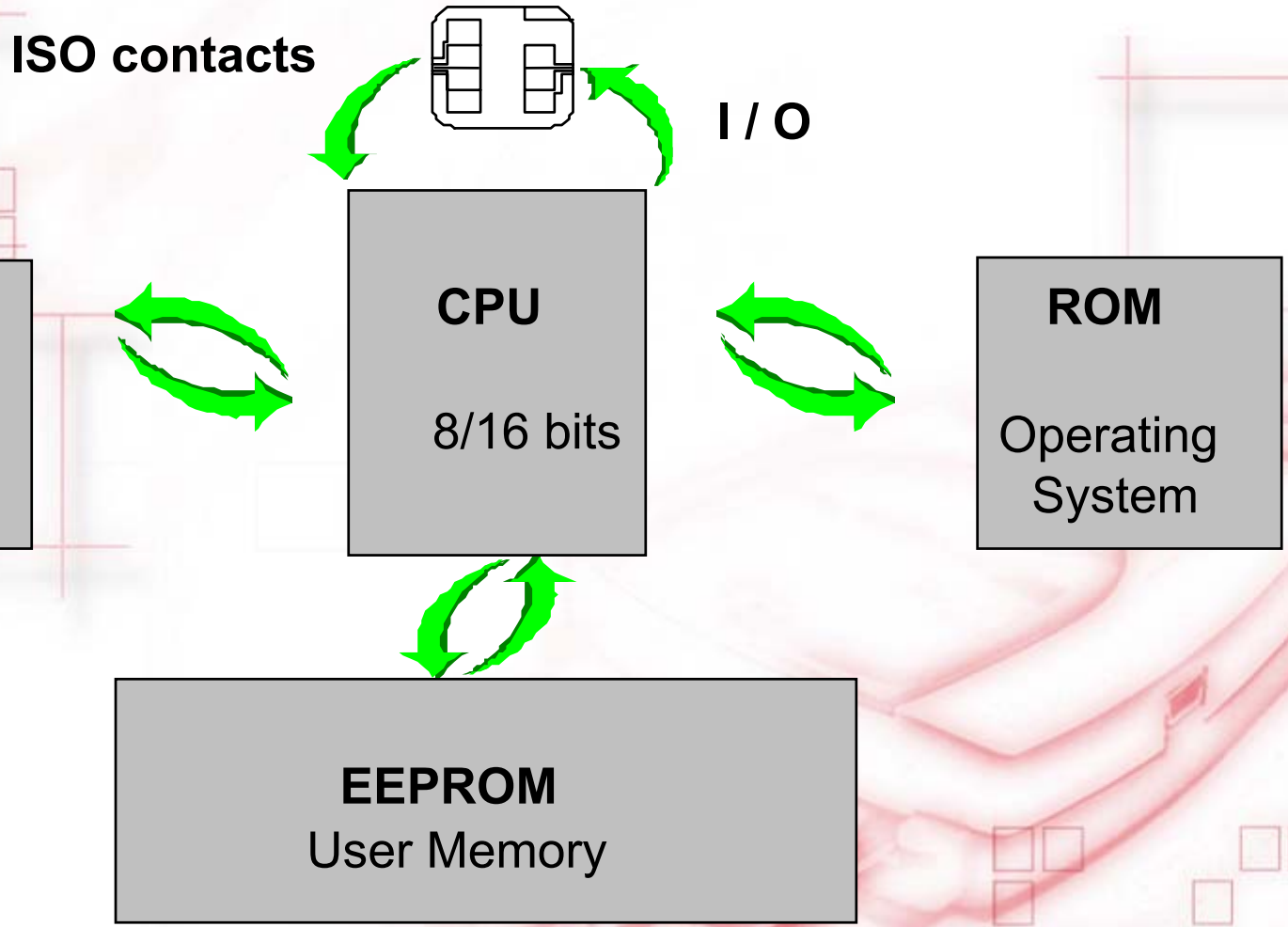
CPU Card Architecture



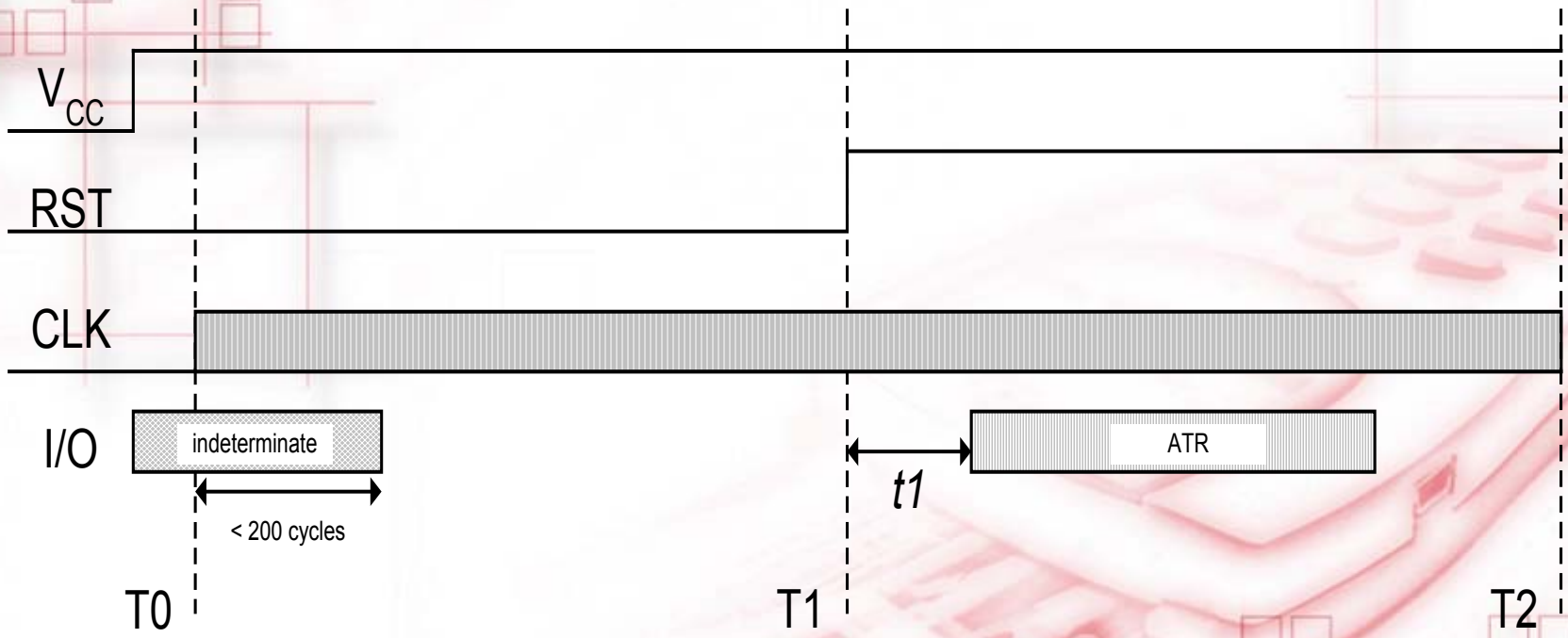
Smart Card

- 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 3Kbytes to 32 Kbytes
  - RAM ~100 bytes to 1 Kbytes
  - EEPROM 512 bytes to 32 Kbytes

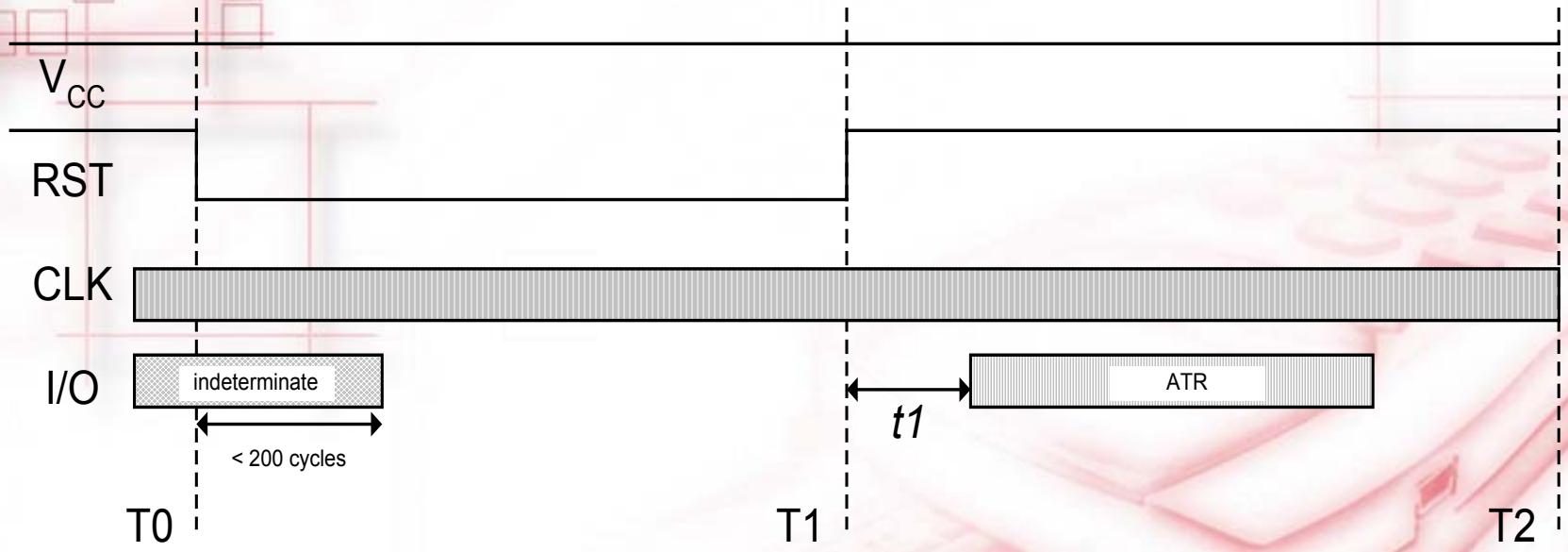
Smart Card Standard ISO-7816

- Part 1 - Physical Characteristics
- Part 2 - Dimensions & Locations of Contacts
- Part 3 - Electronic Signals & Transmission Protocol
- Part 4 - Inter-industry Command For Interchange

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

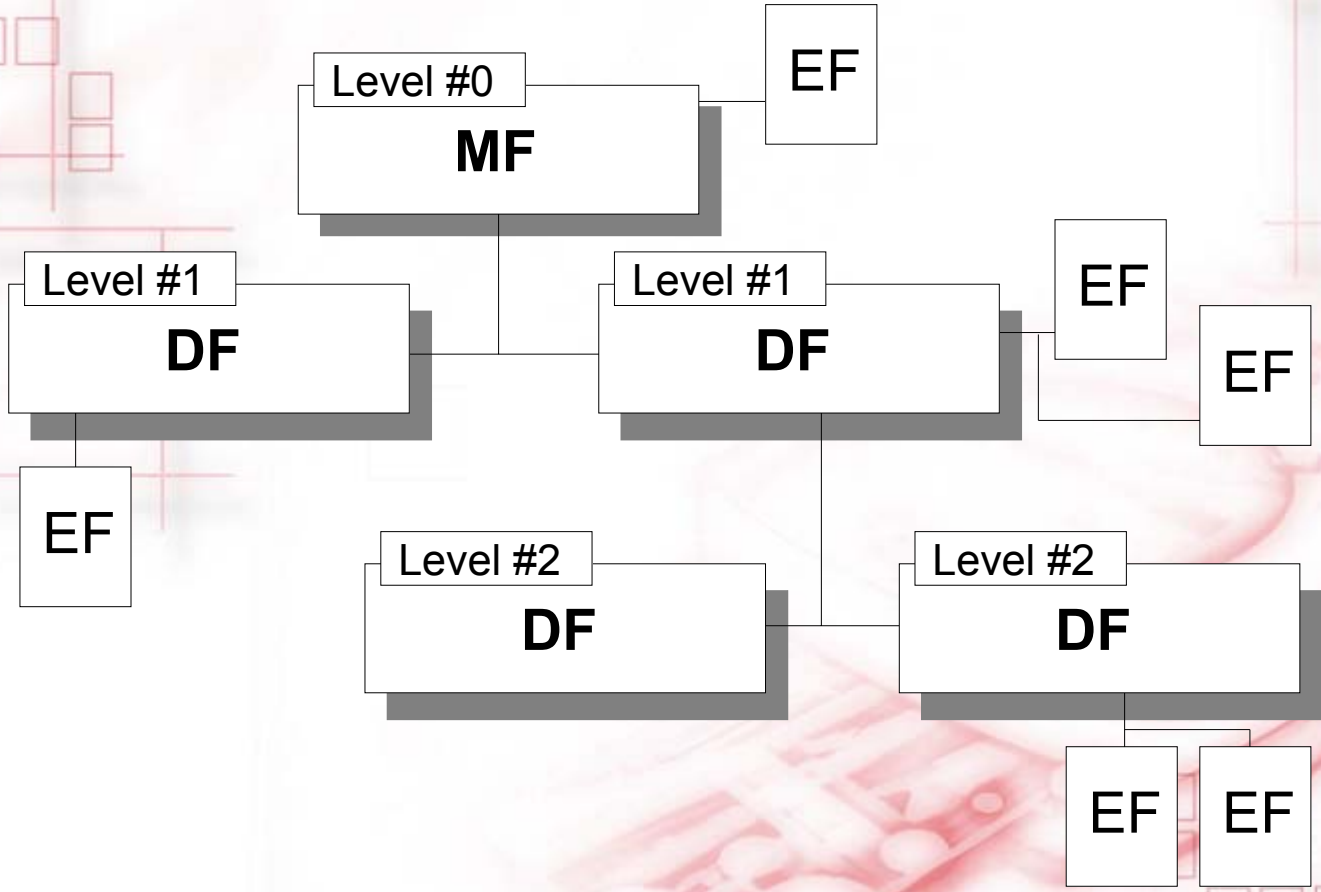
TA2 = specific mode
TB2 = PI2
TC2 = specific
TD2 = Y3, T
TD2 = Y3,T
T1..Tk = historical characters

ISO-7816 Part 3 -- TPDU FORMAT

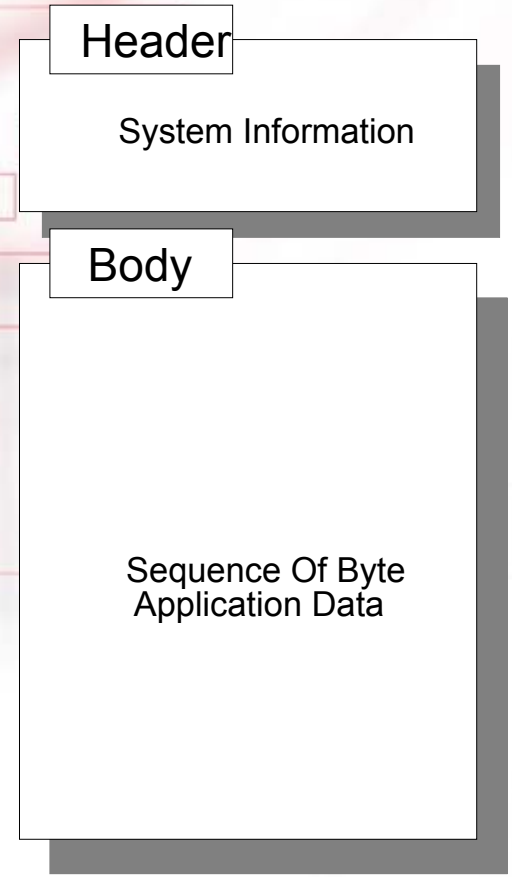
ISO-IN Command

ISO-Out Command

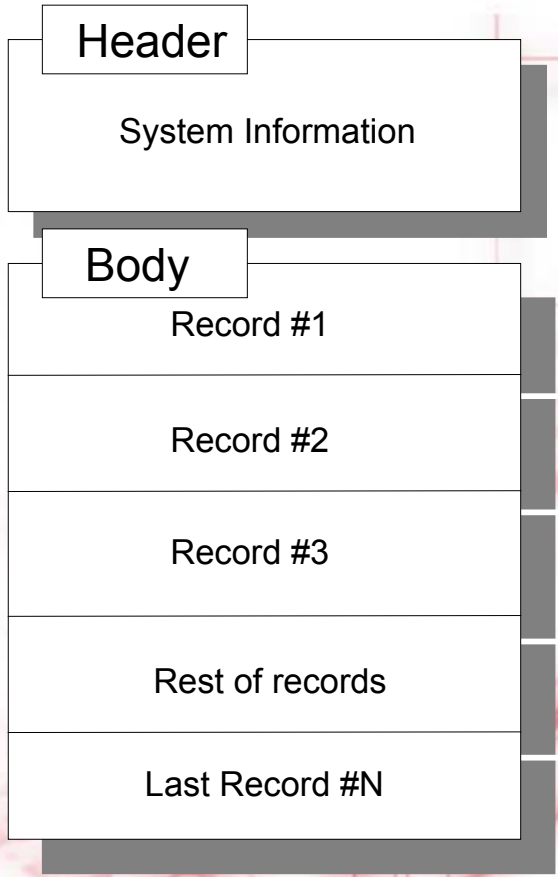
ISO-7816 Part 4 -- File Organizations



ISO-7816 Part 4 -- File Structures

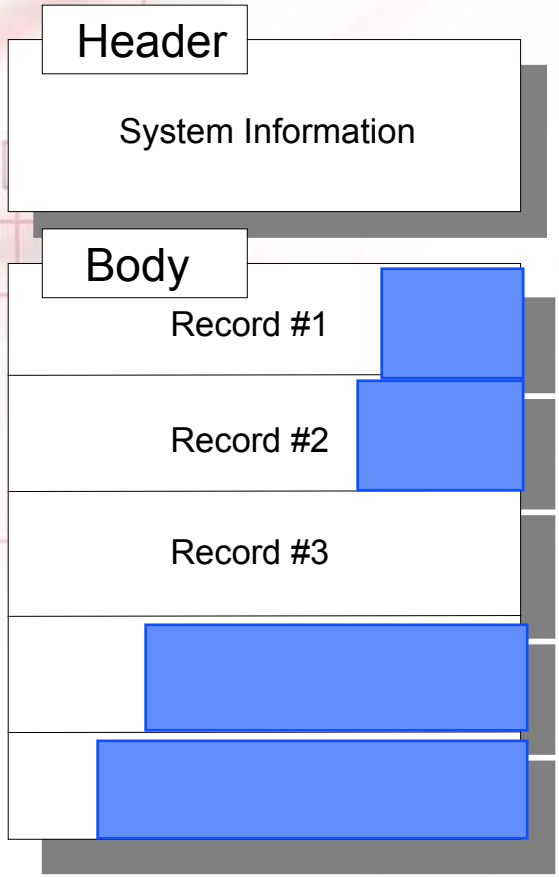


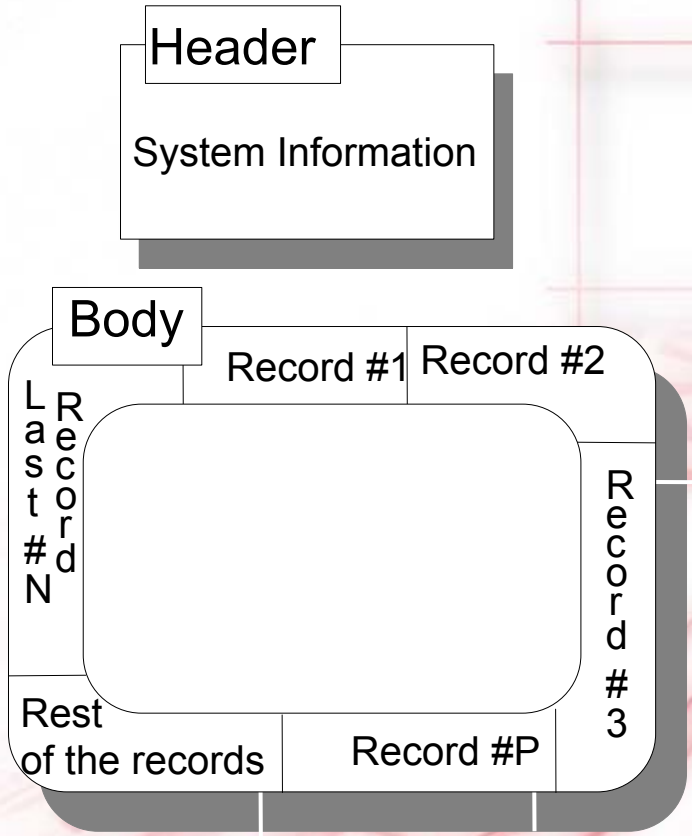
TRANSPARENT FILE



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
- GET RESPONSE
- ENVELOPE
- GET DATA
- WRITE BINARY
- WRITE RECORD
- UPDATE BINARY
- PUT DATA
- UPDATE RECORD
- APPEND RECORD

Payment Commands

- Get Balance
- Debit / Purchase
  - Initialize For Purchase
  - Purchase
  - Get Transaction Proof
- Credit
  - Initialize For Credit
  - Credit

Payment Commands

- Unload
  - Initialize For Unload
  - Debit For Unload
  - Get Transaction Proof
- Update Parameter
  - Update Overdraw Limit

Administrative Commands

- Create File
- Delete File
- Create Record
- Set Lock
- PIN Unblock
- Reload PIN
- Application Block
- Application Unblock

Smart Card Security Attributes

- File access
  - Read, write, update/erase
  - Access locks
  - Access in plain or ciphered
  - Secured messaging
  - Invalidate, rehabilitate
- 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

COS Techniques

- Security
  - At implementation level
  - At command definition level
- Flexibility
  - COS development process
  - Security policy
- Reliability
  - Stress reduction of EEPROM cell
  - Anti-tearing

File Header – MF / DF Header

The MF/DF header has the following structure:

Byte 0	File descriptor byte
Byte 1-2	File ID
Byte 3-4	File size allocated
Byte 5	DF State AND mask
Byte 6	DF body size
Byte 7-8	Create / Delete Access
Byte 9-10	File size remaining
Byte 11	Current DF headers checksum

File Header – Transparent / TLV / Variable Record File

The transparent header has the following structure:

Byte 0	File descriptor byte
Byte 1-2	File ID
Byte 3-4	File size allocated
Byte 5-6	Read Access
Byte 7-8	Update Access

File Header Linear / Cyclic Record File

The file header has the following structure:

Byte 0	File descriptor byte
Byte 1-2	File ID
Byte 3-4	Number of record; Record length
Byte 5-6	Read access
Byte 7-8	Update access

Security Policy

- Access Condition is defined by
  - Active Logic
  - Active State
- DF Access Condition
  - CREATE / DELETE
- EF Access Condition
  - READ
  - UPDATE

File Access

B7	B6	B5	B4	B3	B2	B1	B0	Description
1	-	-	-	-	-	-	-	1 = Ciphered
-	1	-	-	-	-	-	-	1 = MAC
-	-	Level	-	-	-	-	-	0 = key in current DF, 1 = parent DF
-	-	-	x	x	x	x	x	11111 indicates that the key is session key else indicates key number in the key file

B7	B6	B5	B4	B3	B2	B1	B0	Description
X	X	X	-	-	-	-	-	Access Logic
-	-	-	X	X	X	X	X	Access State

Key File – Key Record Descriptor

Each key record contains the following fields:

Byte 0, bit 7-5	ACTIVE_LOGIC
Byte 0, bit 4-0	ACTIVE_STATE
Byte 1, bit 4-0	NEXT_STATE
Byte 1, bit 7-5	RFU
Byte 2-3	Key capability
Byte 4,5	max error/ usage counter
Byte 6,7	error / usage counter
Byte 8 – XX	key content

Active Logic

000 – Always

001 – Less Than (<)

010 – Less Or Equal (<=)

011 – Equal (==)

100 – Greater Or Equal (>==)

101 – Greater (>)

110 – Not Equal (!=)

111 – Never

State

- COS has a state {0,1,2..31}
- State is defined by a 5 bits field
- State = 0 is the power-on default state (ALWAYS)
- State = 31 is the NEVER (LOCKED) state
- State is changed by a secret code presentation or key authentication
- Active Logic, Active State set the pre-condition to use a secret code / key
- Next State of secret code / key change to state machine
- If the state machine matches the Access, access is authorized