PHILIPS

mifare® *DESFire & ISO14443*

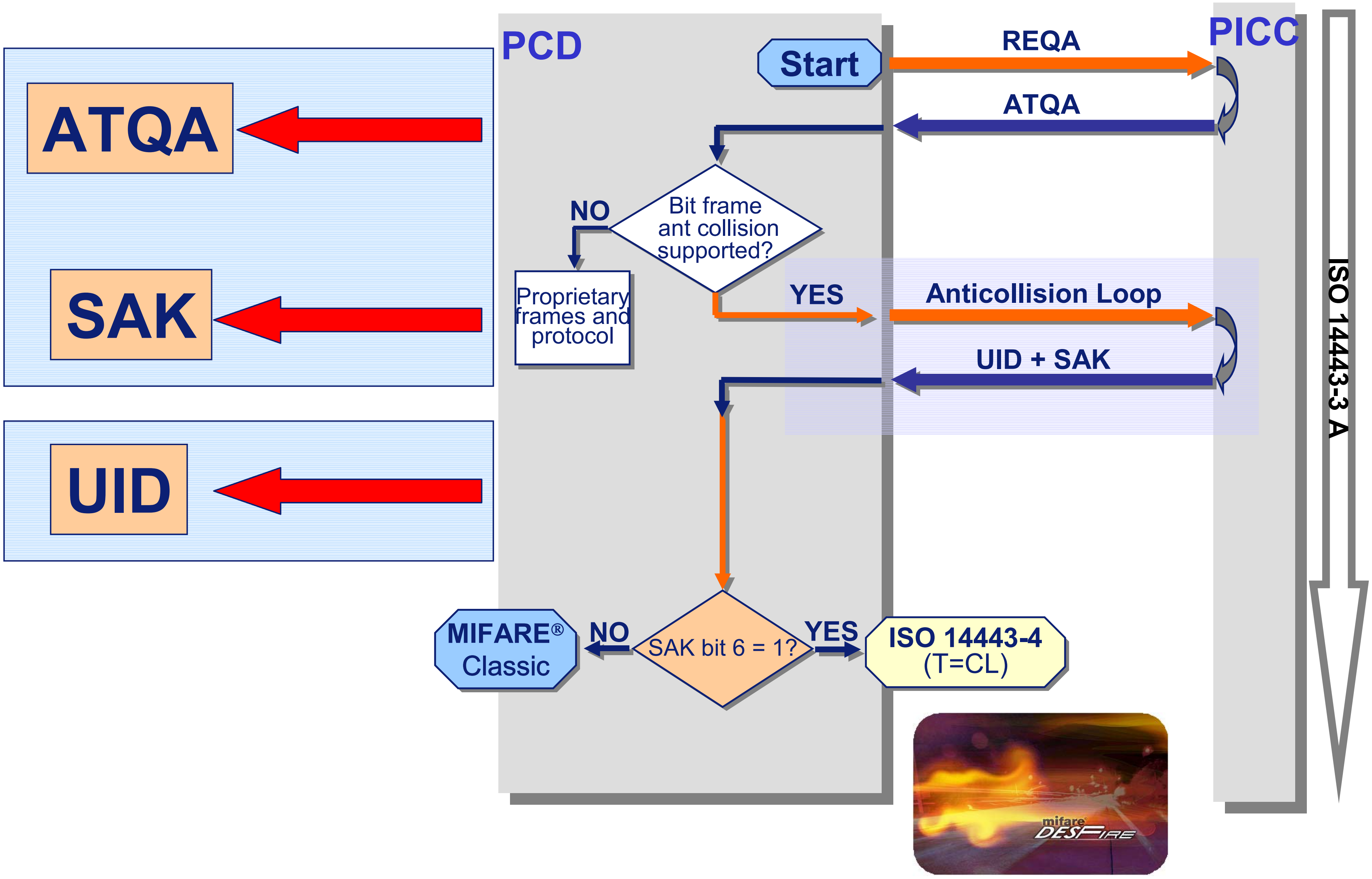
CAS - 2006

mifare® DESFire & ISO14443 Agenda

- mifare® *DESFire* Type ID
- mifare® *DESFire* ATQA
- mifare® *DESFire SAK*
- mifare® *DESFire UID*
- *ISO14443A RATS & PPS*
- mifare® *DESFire (R)ATS*
- mifare® *DESFire PPS (Request)*
- *Block Exchange via „T=CL“*

PHILIPS

mifare® *DESFire* Type ID



PCD

PICC

Start

REQA

ATQA

Bit frame ant collision supported?

NO

Proprietary frames and protocol

YES

Anticollision Loop

UID + SAK

ATQA

SAK

UID

ISO 14443-3 A

MIFARE® Classic

NO

SAK bit 6 = 1?

YES

ISO 14443-4 (T=CL)

PHILIPS

mifare® *DESFire* ATQA Coding

	MSB ATQA								LSB ATQA							
Bit no.	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ISO/IEC 14443A-3	RFU[1]				Proprietary coding				UID size		RFU[1]	Bit frame anticollision				
212 kbit/s								1								
424 kbit/s							1									
848 kbit/s						1										
Single UID									0	0						
Double UID									0	1						
Triple UID									1	0						
RFU									1	1						
Bit Frame Anticollision												1	0	0	0	0
Bit Frame Anticollision												0	1	0	0	0
Bit Frame Anticollision												0	0	1	0	0
Bit Frame Anticollision												0	0	0	1	0
Bit Frame Anticollision												0	0	0	0	1

ATQA of mifare® ICs

MIFARE® UL (0x0044)	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0
MIFARE® 1K (0x0004)	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
MIFARE® 4K (0x0002)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
MIFARE® DESFire (0x0344)	0	0	0	0	0	0	1	1	0	1	0	0	0	1	0	0
MIFARE® ProX	0	0	0	0	0	X[2]	X[2]	X[2]	0	0	0	0	X[2]	X[2]	X[2]	X[2]

[1] All RFU bits shall be set to ‘0’

[2] Depends on OS

mifare® *DESFire* SAK Coding

SAK bit values as defined in the ISO/IEC 14443A-3	**SAK**							
Bit no.	8	7	6	5	4	3	2	1
Cascade bit set: UID not complete			x			1		
UID complete, PICC compliant with ISO/IEC 14443-4			1			0		
UID complete, PICC not compliant with ISO/IEC 14443-4			0			0		

SAK of mifare® ICs

MIFARE® ultralight (0x04) – cascade level 1	0	0	0	0	0	1	0	0
MIFARE® ultralight (0x00) – cascade level 2	0	0	0	0	0	0	0	0
MIFARE® 1K (0x08)	0	0	0	0	1	0	0	0
MIFARE® 4K (0x18)	0	0	0	1	1	0	0	0
MIFARE® DESFire (0x24) – cascade level 1	0	0	1	0	0	1	0	0
MIFARE® DESFire (0x20) – cascade level 2	0	0	1	0	0	0	0	0
MIFARE® ProX	0	0	x[1]	x[1]	x[1]	x[1]	0	0

[1] Depends on OS

PHILIPS

mifare® *DESFire* UID Coding

UID size

ISO/IEC 14443A3

Single

PCD	93					
PICC		UID0	UID1	UID2	UID3	BCC

Double

PCD	93							95					
PICC		CT	UID0	UID1	UID2	BCC			UID3	UID4	UID5	UID6	BCC

Triple

PCD	93							95							97					
PICC		CT	UID0	UID1	UID2	BCC			CT	UID3	UID4	UID5	BCC			UID6	UID7	UID8	UID9	BCC

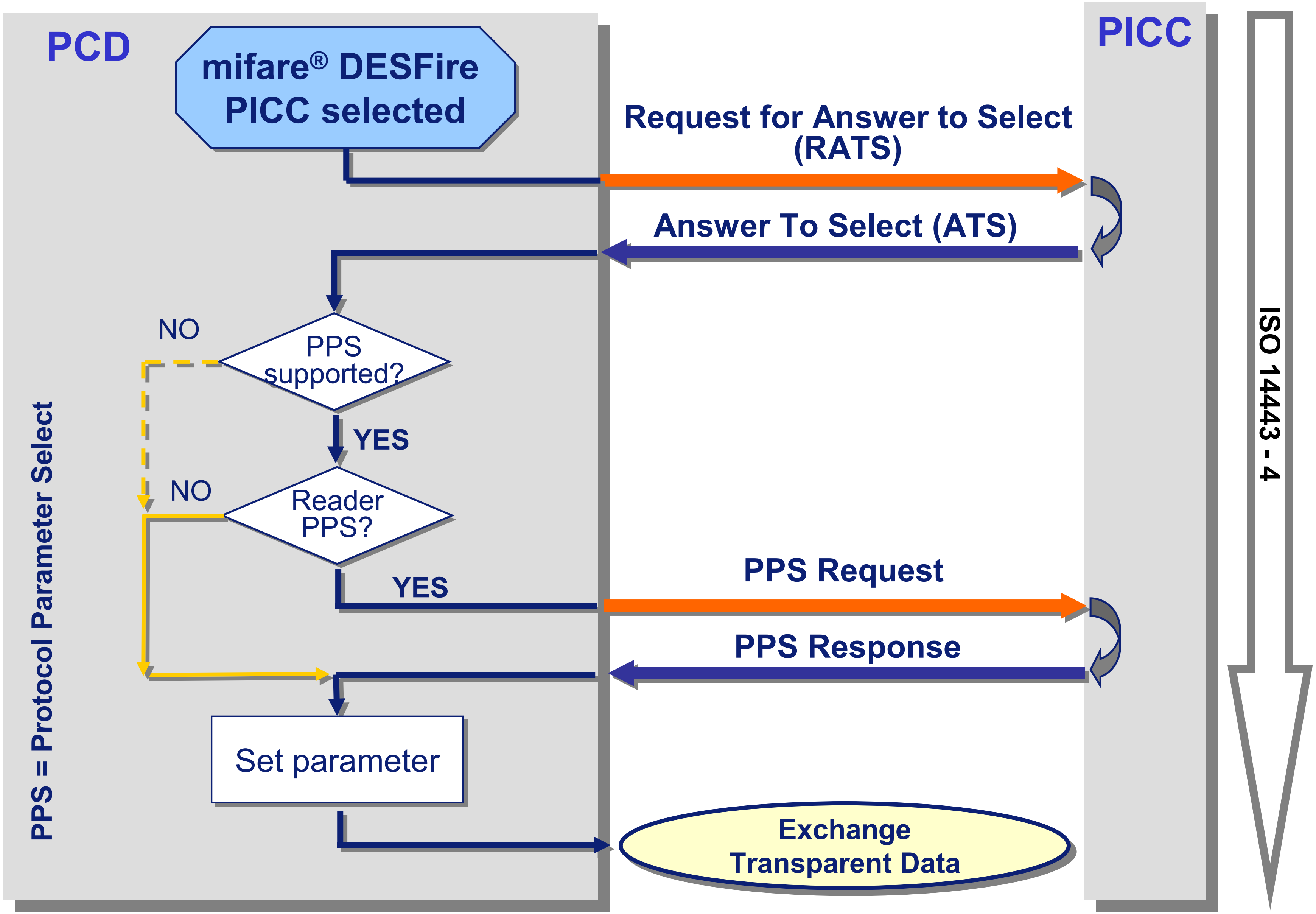
Double or Triple Size UIDs:

ISO 14443	UID0	UID1 – UID6 (resp. UID1 - UID9)
	Manufacturer ID according to the ISO/IEC 7816-6/AM1	Each manufacturer is responsible for the uniqueness of the value of the other bytes of the unique number.
Philips	0x04	x

PCD	93							95					
DESFire PICC		0x88	0x04	xx	xx	xx			xx	xx	xx	xx	xx

mifare® *DESFire*

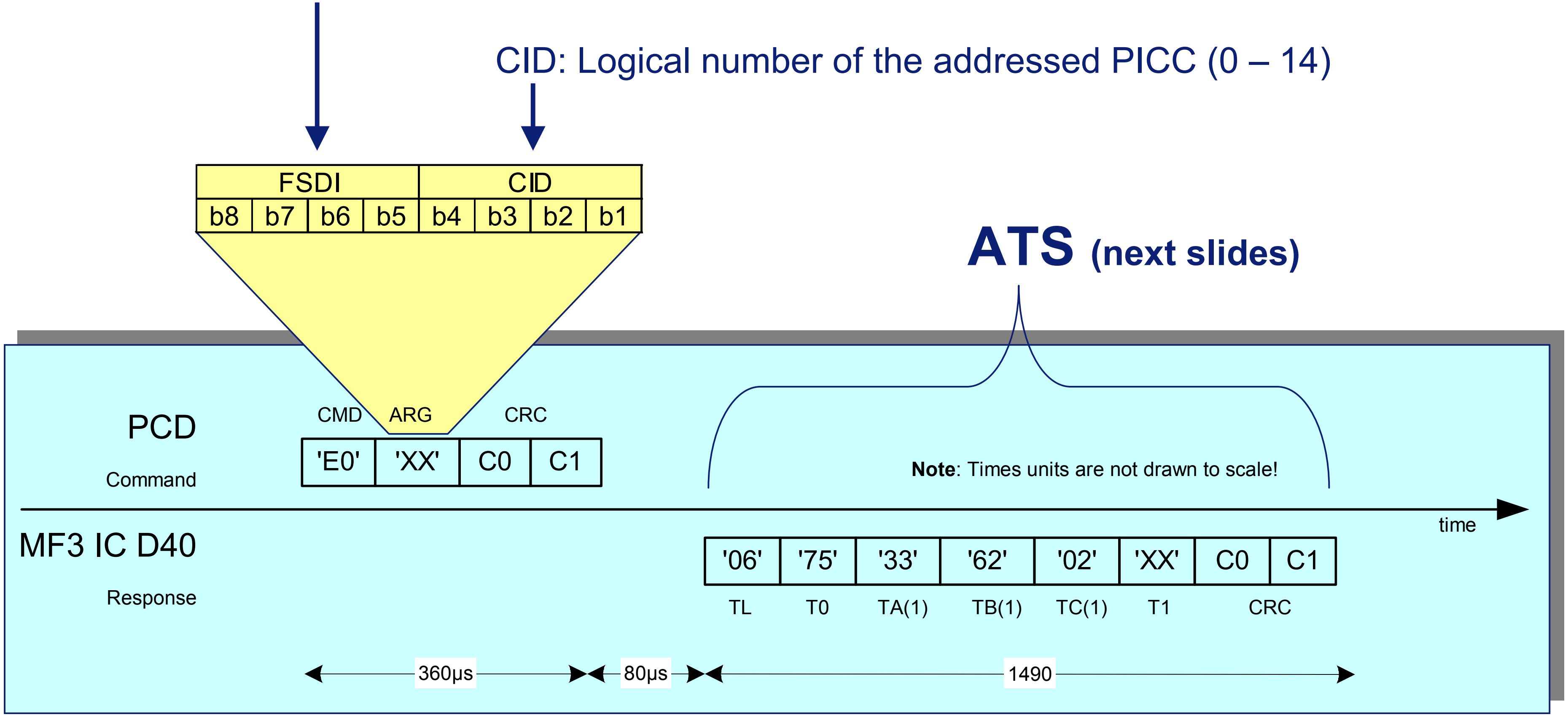
ISO14443A RATS & PPS


PCD
mifare® DESFire PICC selected
PICC
Request for Answer to Select (RATS)
Answer To Select (ATS)
NO
PPS supported?
YES
NO
Reader PPS?
YES
PPS Request
PPS Response
Set parameter
Exchange Transparent Data
PPS = Protocol Parameter Select
ISO 14443 - 4

Request for Answer To Select (RATS)

FSD: Maximum frame size supported by the PCD:

FSDI	0	1	2	3	4	5	6	7	8	9-F
FSD	16	24	32	40	48	64	96	128	256	RFU

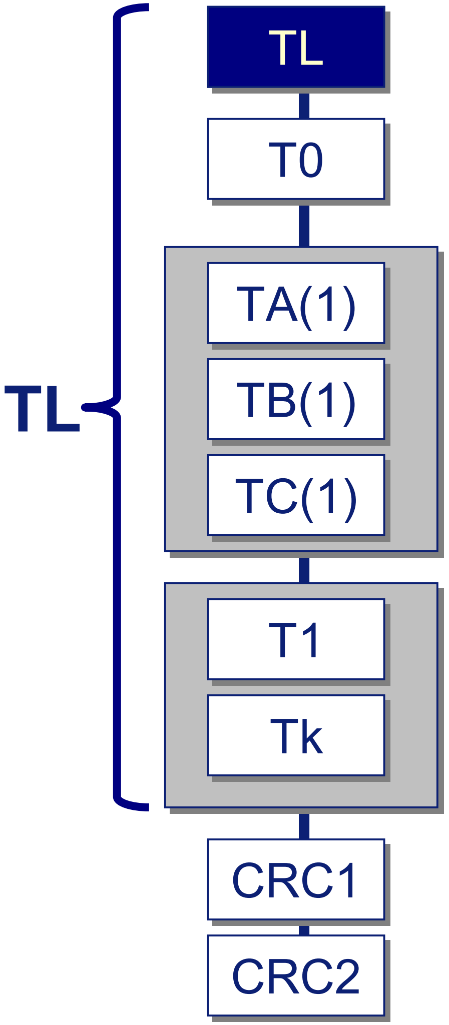


CID: Logical number of the addressed PICC (0 – 14)

FSDI				CID			
b8	b7	b6	b5	b4	b3	b2	b1

ATS (next slides)

ATS 1: Length Byte



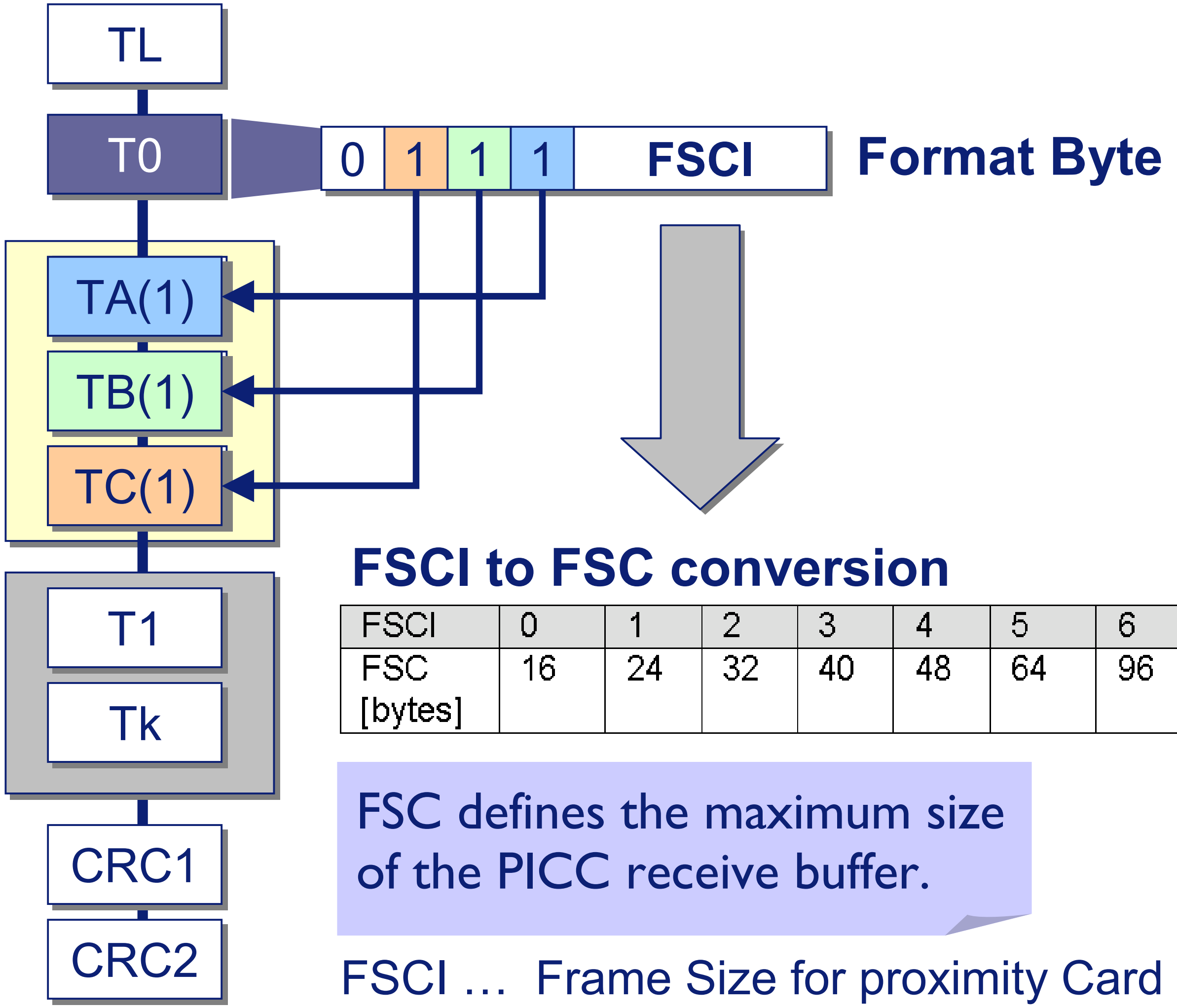
Length Byte

Format Byte

Interface Bytes
Optional

Historical Bytes
Optional
ISO/IEC 7816- 4
specifies the content

ATS 2: Format Byte T0



FSCI to FSC conversion

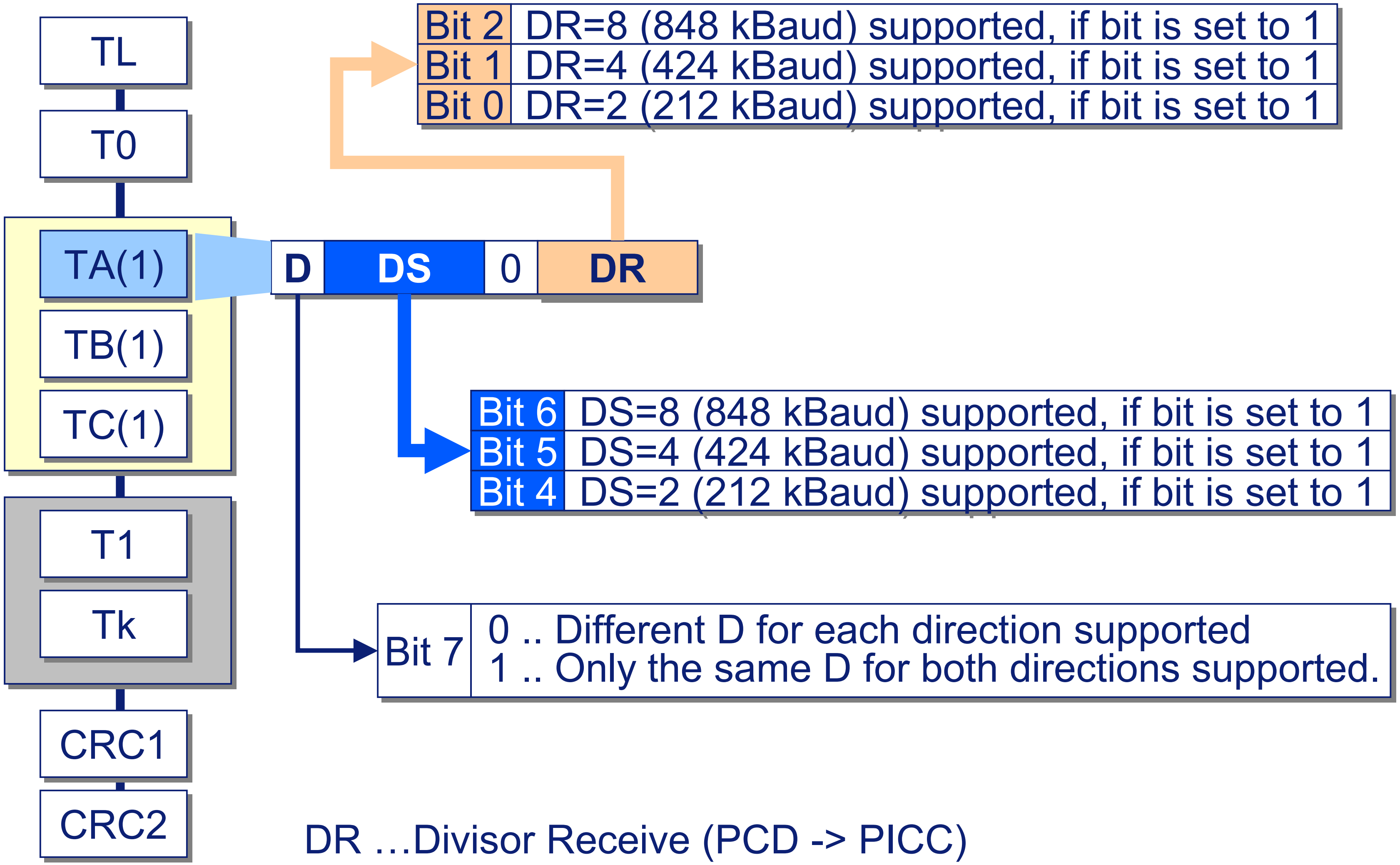
FSCI	0	1	2	3	4	5	6	7	8	9 – F
FSC [bytes]	16	24	32	40	48	64	96	128	256	RFU >256

FSC defines the maximum size of the PICC receive buffer.

FSCI … Frame Size for proximity Card Integer

FSC … Frame Size for proximity Card

ATS 3: Interface Byte TA(1)



Bit 2	DR=8 (848 kBaud) supported, if bit is set to 1
Bit 1	DR=4 (424 kBaud) supported, if bit is set to 1
Bit 0	DR=2 (212 kBaud) supported, if bit is set to 1

Bit 6	DS=8 (848 kBaud) supported, if bit is set to 1
Bit 5	DS=4 (424 kBaud) supported, if bit is set to 1
Bit 4	DS=2 (212 kBaud) supported, if bit is set to 1

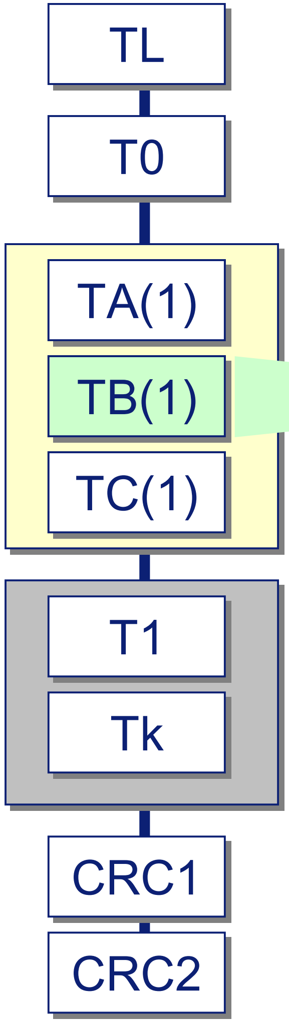
Bit 7	0 .. Different D for each direction supported 1 .. Only the same D for both directions supported.

DR …Divisor Receive (PCD -> PICC)

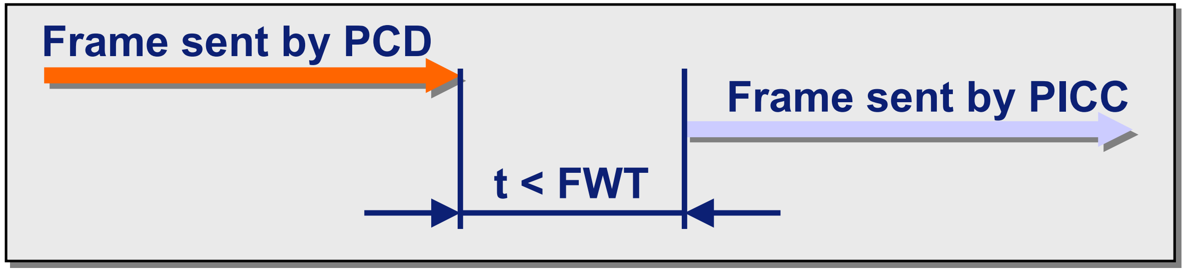
DS …Divisor Send (PICC -> PCD)

PHILIPS

ATS 4: Interface Byte TB(1)



Frame Waiting Time:



FWI	SFGI

$$FWT = (256 \times 16 / fc) \times 2^{FWI}$$

Example:

$FWT_{MIN} =$ 0: $(256 \times 16 / 13{,}56 * 10^6) \times 1 \approx 302\ \mu s$

$FWT =$ 4: $(256 \times 16 / 13{,}56 * 10^6) \times 2^4 \approx 4833\ \mu s$

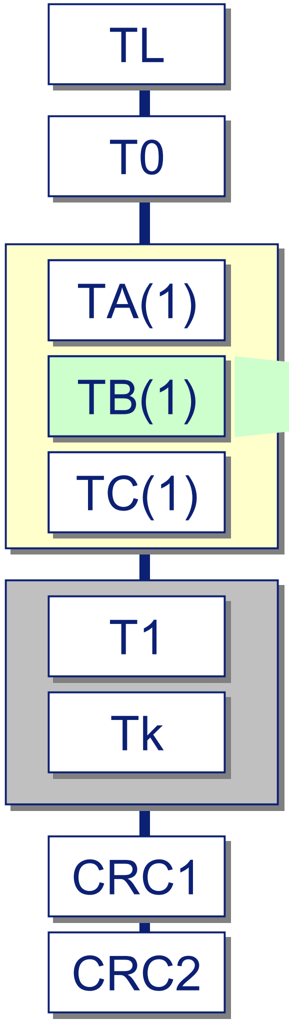
$FWT =$ 9: $(256 \times 16 / 13{,}56 * 10^6) \times 2^9 \approx 154\ ms$

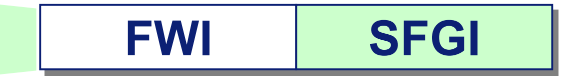
$FWT_{MAX} =$14: $(256 \times 16 / 13{,}56 * 10^6) \times 2^{14} \approx 4949\ ms$

FWI … Frame Waiting Time Integer

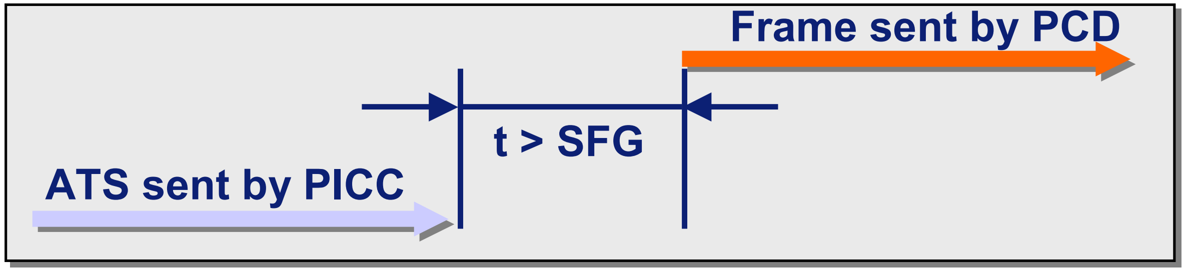
FWT … Frame Waiting Time

ATS 5: Interface Byte TA(1)





Start-up Frame Guard Time:

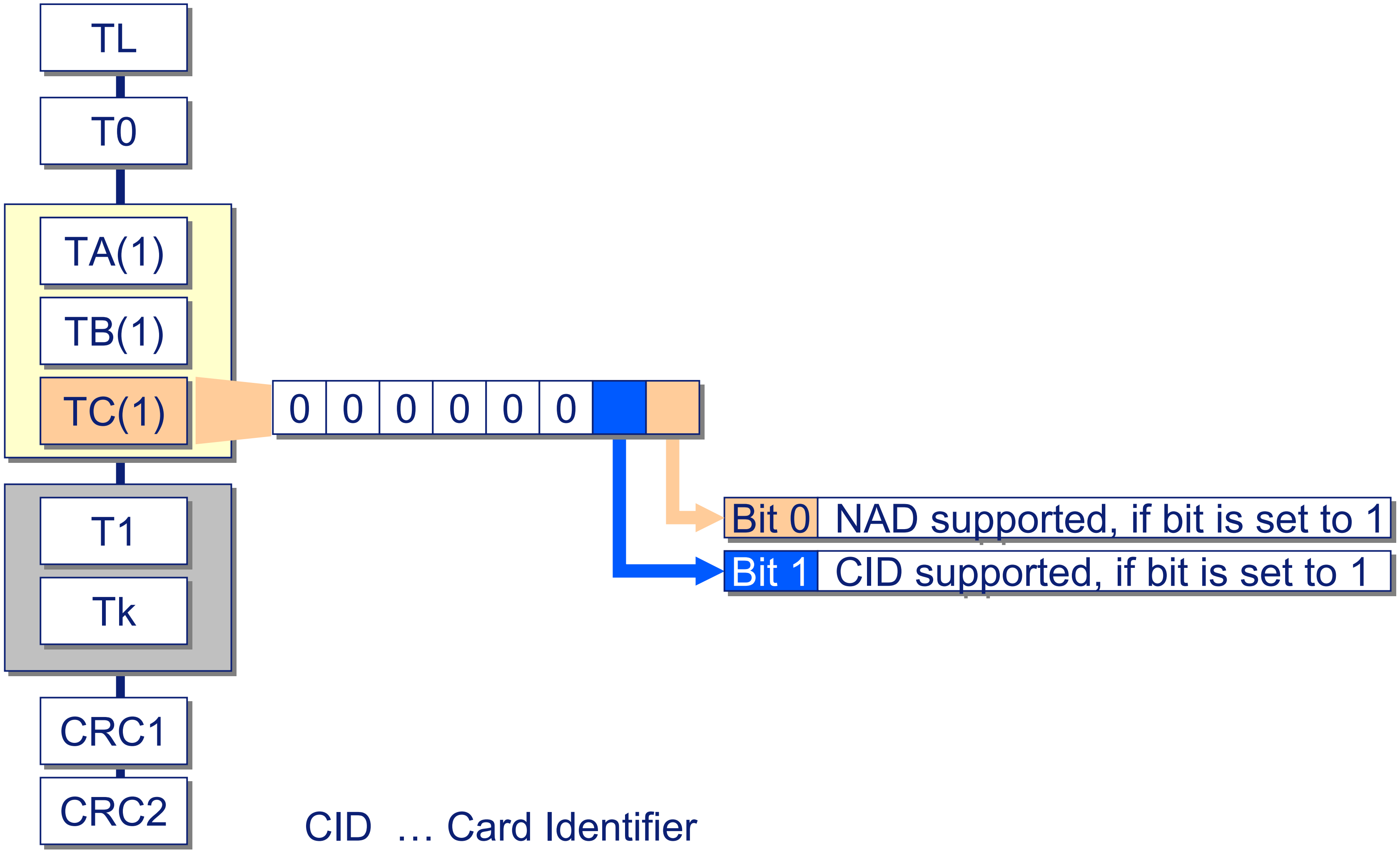


$$SFG = (256 \times 16 / fc) \times 2^{SFGI}$$

SFGI …Start-up Frame Guard Time Integer

SFG …Start-up Frame Guard Time

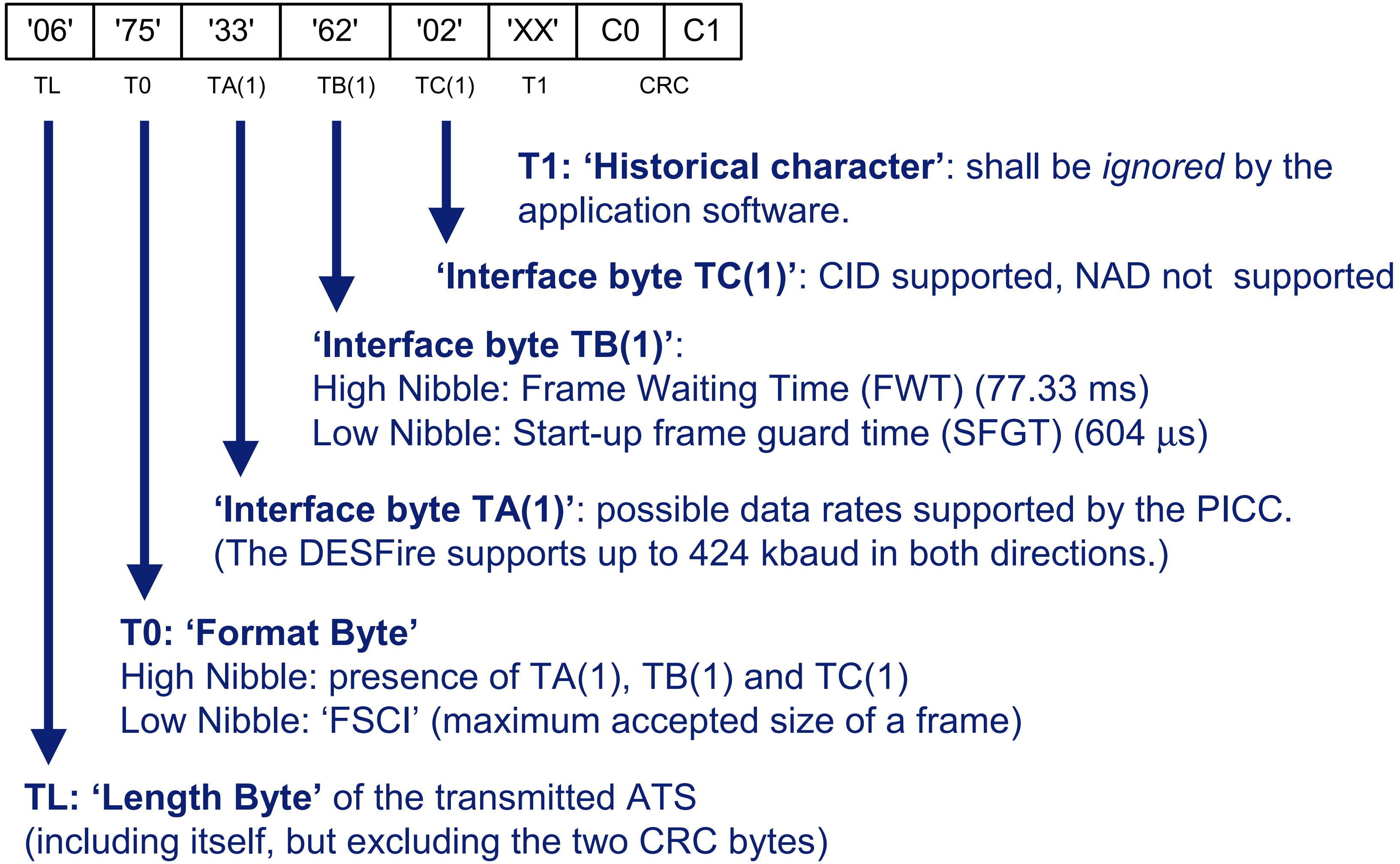
ATS 6: Interface Byte TC(1)


TL
T0
TA(1)
TB(1)
TC(1)
T1
Tk
CRC1
CRC2
0 0 0 0 0 0
Bit 0 NAD supported, if bit is set to 1
Bit 1 CID supported, if bit is set to 1

CID … Card Identifier

NAD … Node Address

Answer To Select (ATS)



'06'	'75'	'33'	'62'	'02'	'XX'	C0	C1
TL	T0	TA(1)	TB(1)	TC(1)	T1	CRC	

T1: 'Historical character': shall be *ignored* by the application software.

'Interface byte TC(1)': CID supported, NAD not supported

'Interface byte TB(1)':
High Nibble: Frame Waiting Time (FWT) (77.33 ms)
Low Nibble: Start-up frame guard time (SFGT) (604 µs)

'Interface byte TA(1)': possible data rates supported by the PICC.
(The DESFire supports up to 424 kbaud in both directions.)

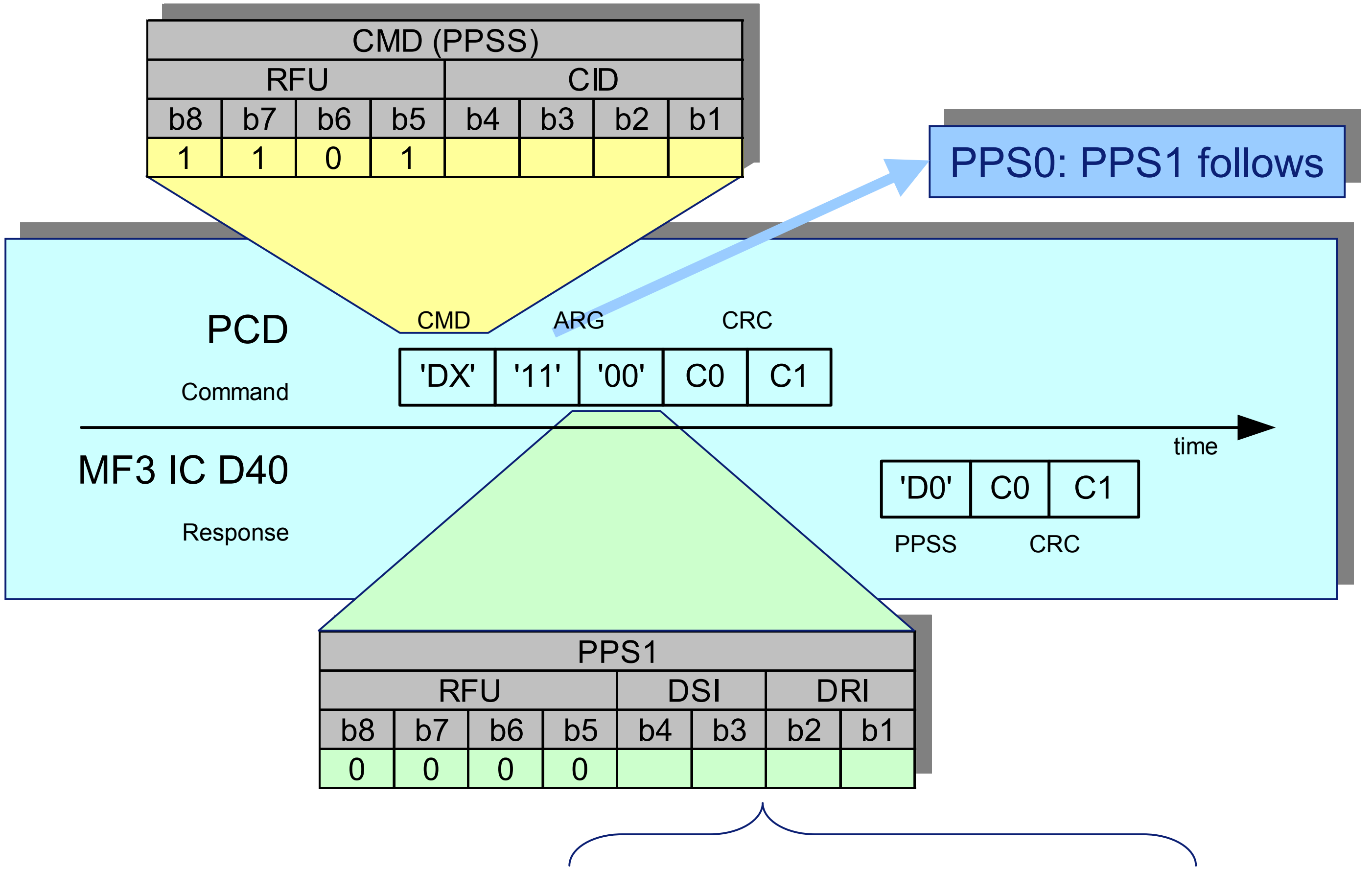
T0: 'Format Byte'
High Nibble: presence of TA(1), TB(1) and TC(1)
Low Nibble: 'FSCI' (maximum accepted size of a frame)

TL: 'Length Byte' of the transmitted ATS
(including itself, but excluding the two CRC bytes)

PHILIPS

mifare® *DESFire* PPS (Request)

Protocol Parameter Selection Request



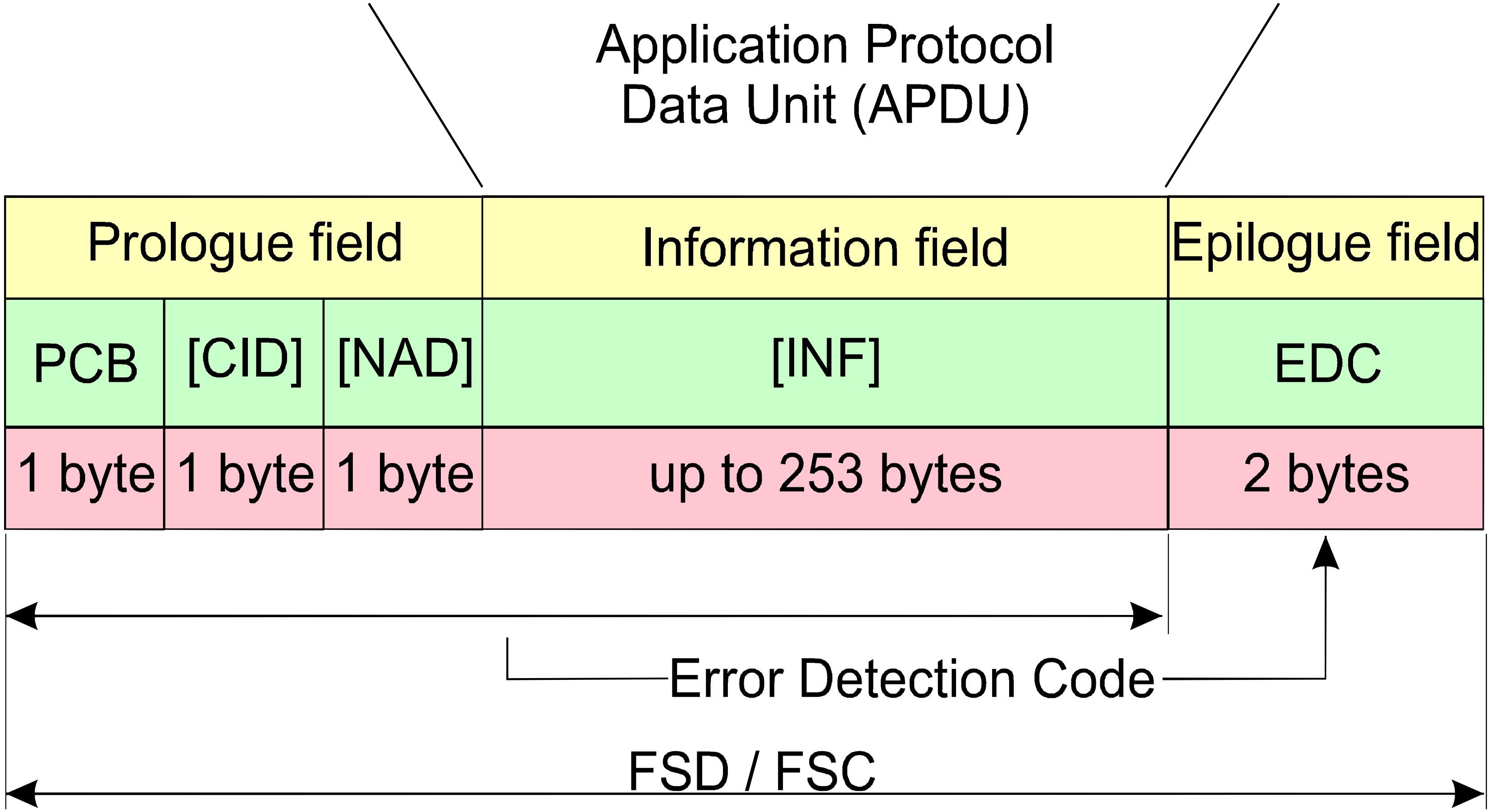
CMD (PPSS)							
RFU				CID			
b8	b7	b6	b5	b4	b3	b2	b1
1	1	0	1				

PPS1							
RFU				DSI		DRI	
b8	b7	b6	b5	b4	b3	b2	b1
0	0	0	0				

DSI, DRI	00*	01	10
Divisor	1	2	4
Baudrate	106kBd	212kBd	424kBd

* ’00’ (106 kbaud in both directions) is the default if no PPS command is sent

Block Structure of T=CL



Application Protocol
Data Unit (APDU)

Prologue field			Information field	Epilogue field
PCB	[CID]	[NAD]	[INF]	EDC
1 byte	1 byte	1 byte	up to 253 bytes	2 bytes

Error Detection Code

FSD / FSC

FSD ... Frame Size for PCD
FSC ... Frame Size for PICC

Protocol Control Byte 1

b8	b7	b6	b5	b4	b3	b2	b1

0 0

- Information Block (I-Block)
  - Exchange of Application Data Units (APDUs)

1 0

- Receive Ready Block (R-Block)
  - ACK or NACK (containing no INF Field)

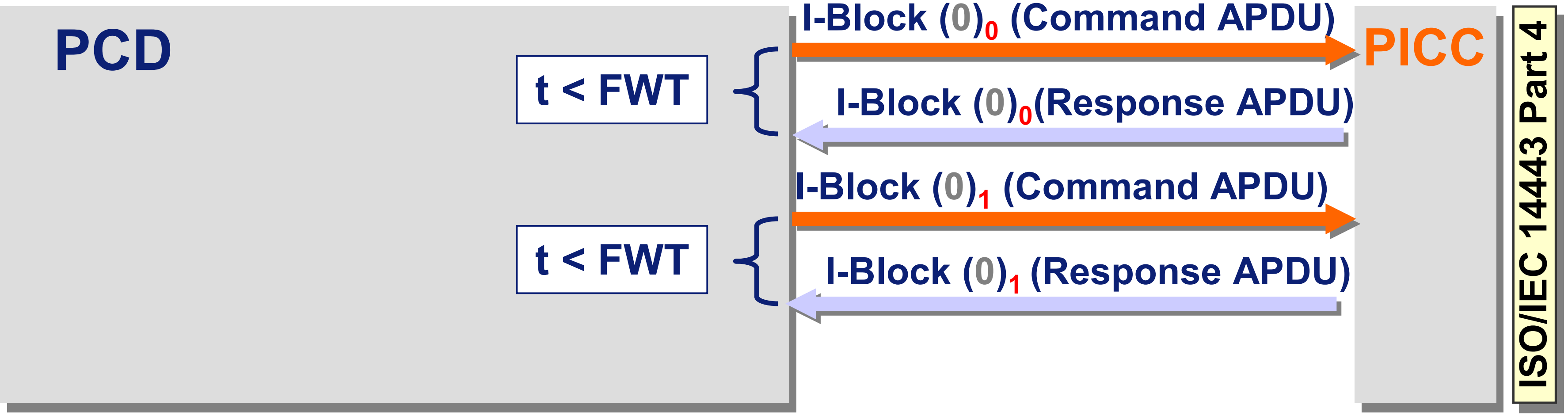
1 1

- Supervisor Block (S-Block)
  - Waiting Time Extension (contains 1 INF Field)
  - Deselect (containing no INF Field)

Protocol Control Byte 2

b8	b7	b6	b5	b4	b3	b2	b1
0	0	0				1	

Bit 1	Block Number
Bit 3	NAD following, if bit is set to 1
Bit 4	CID following, if bit is set to 1
Bit 4	Chaining, if bit is set to 1



PCD

PICC

ISO/IEC 14443 Part 4

t < FWT

I-Block (0)$_{0}$ (Command APDU)

I-Block (0)$_{0}$(Response APDU)

t < FWT

I-Block (0)$_{1}$ (Command APDU)

I-Block (0)$_{1}$ (Response APDU)

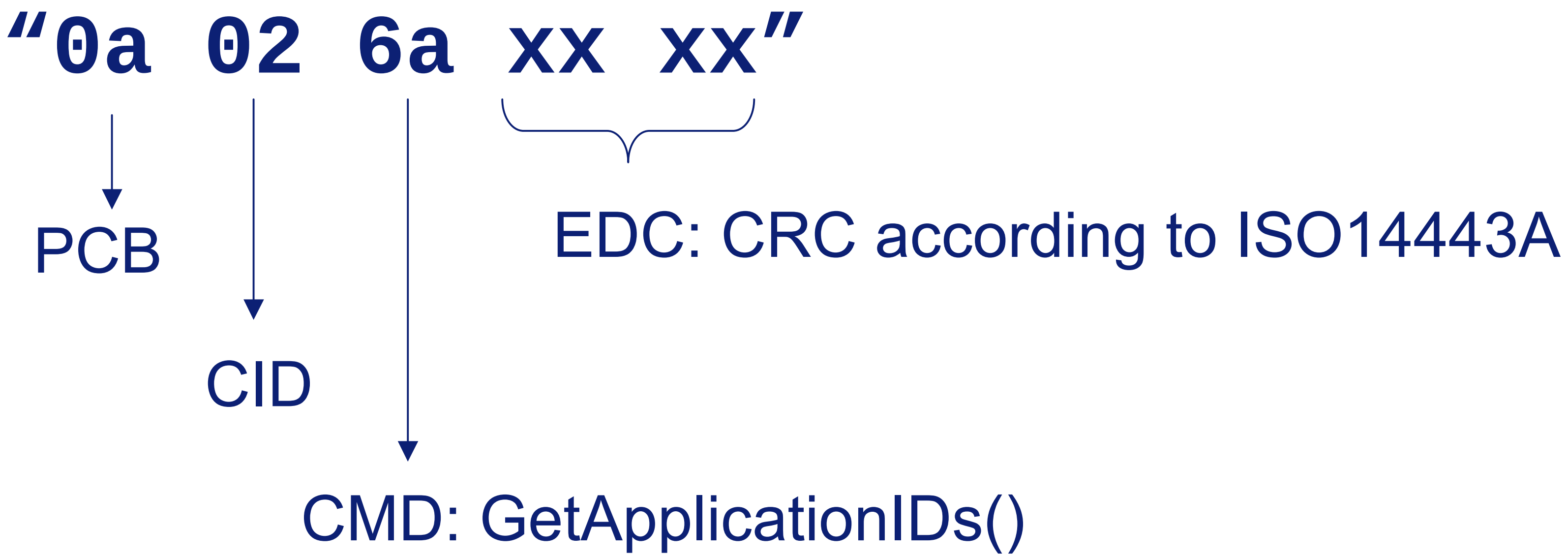
I-Block (0)$_{X}$ … I-Block with chaining bit not set and block number X

I-Block (1)$_{X}$ … I-Block with chaining bit set and block number X

Example of Block Exchange

	Prologue Field			Information Field	Epilogue Field
	PCB	[CID]	[NAD]	[INF]	EDC
no of bytes:	1	1	0	max. 60	2
no of bytes:	1	0[1]	0	max. 61	2

[1] If CID = 0, no CID byte is sent



“0a 02 6a xx xx”

PCB

CID

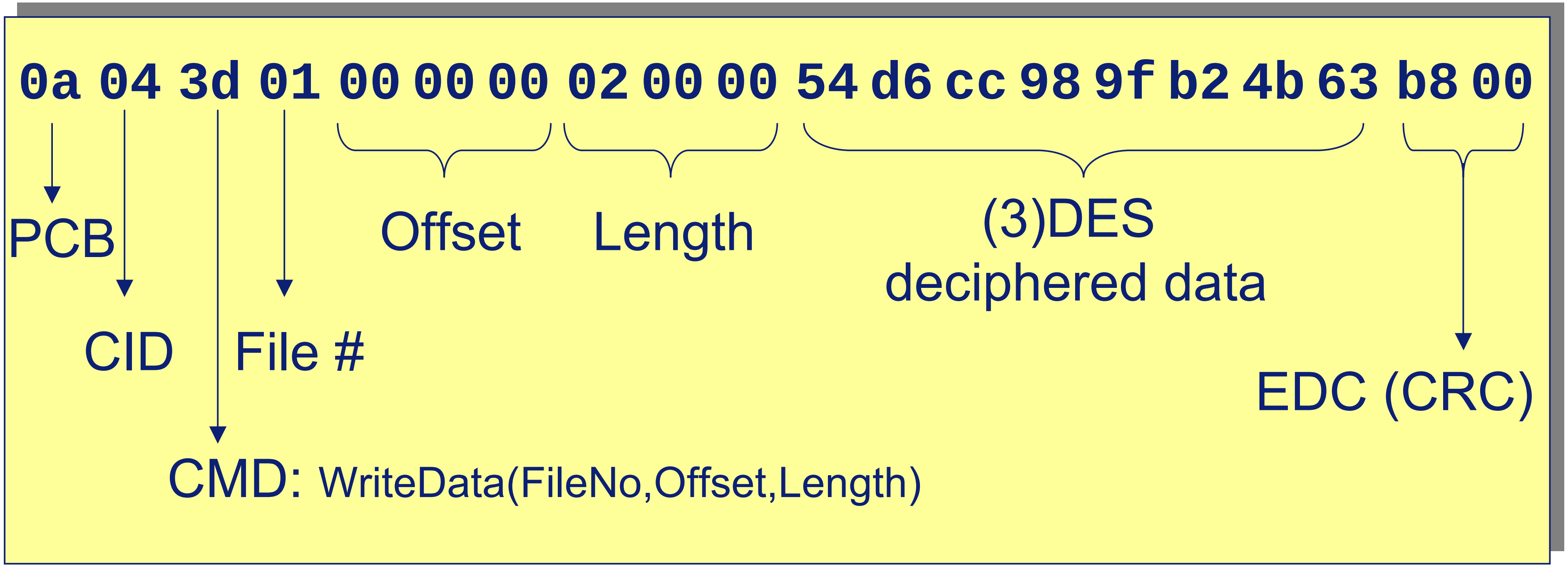
CMD: GetApplicationIDs()

EDC: CRC according to ISO14443A

mifare® DESFire command example

Example: - **Write** 2 Bytes of „0x ff ff“ into a
- DES encrypted DataFile with
- File number 1
- CID 4

Assumption:
The DESFire PICC is selected, RATS is performed with CID = 4. The according application (whatever number) ist selected, and the authentication with the according key is performed.



```
0a 04 3d 01 00 00 00 02 00 00 54 d6 cc 98 9f b2 4b 63 b8 00
```

PCB

CID

File #

Offset

Length

(3)DES deciphered data

EDC (CRC)

CMD: WriteData(FileNo,Offset,Length)

PHILIPS