Smart Card Data Transmission Protocols

連元宏

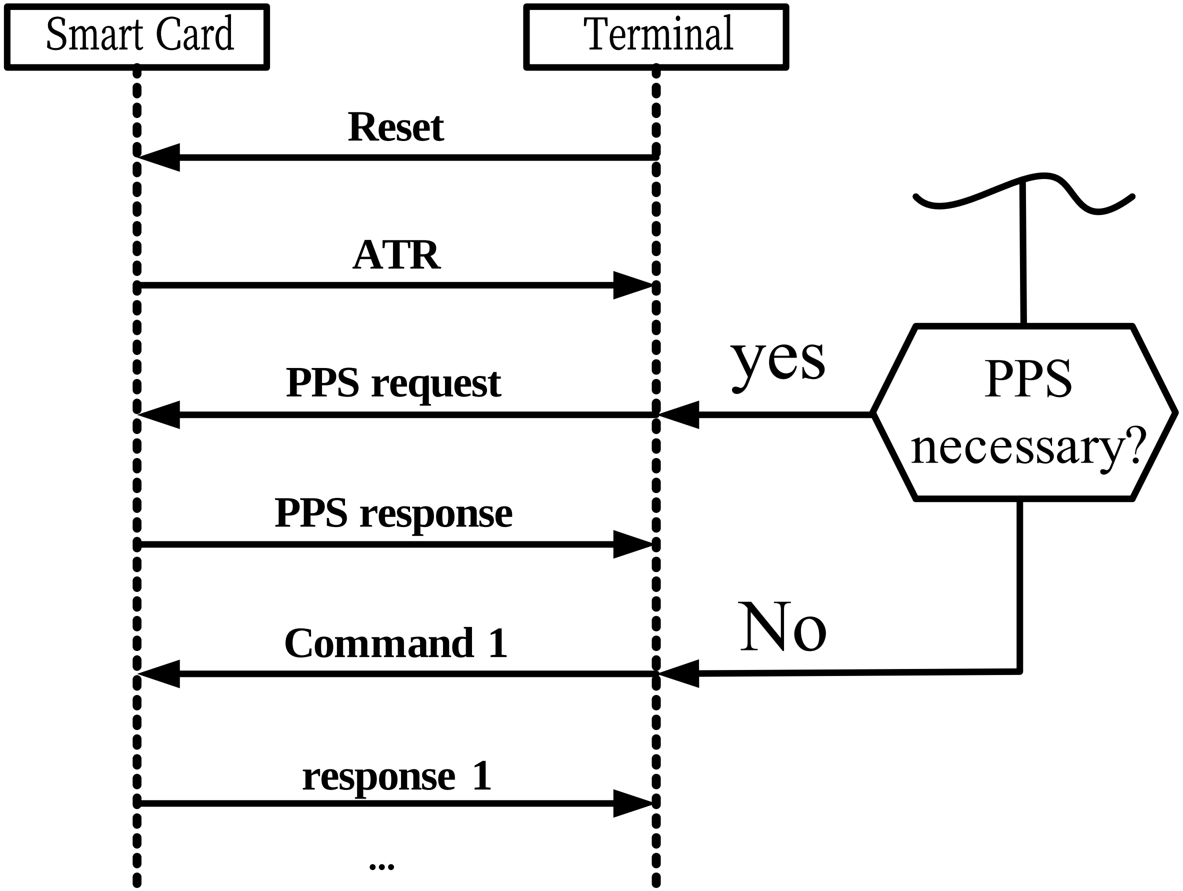
Lien Yuan-hung

E-mail: d9102401@mail.ntust.edu.tw

Outline

- Card operating procedure
- Answer to reset (ATR)
- Protocol parameter selection (PPS)
- Asynchronous transmission protocol (T=0& T=1)

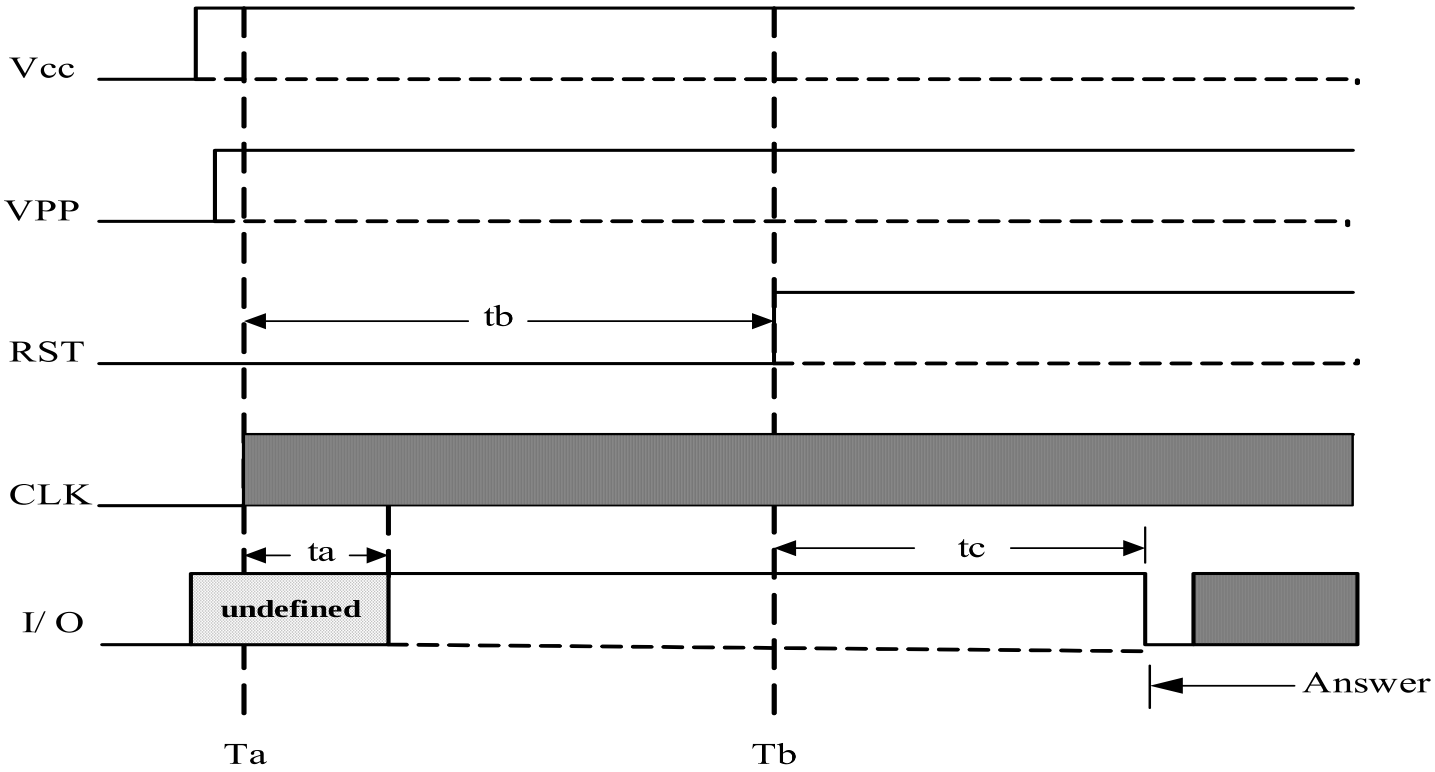
Initial data transfer



Card operating procedure

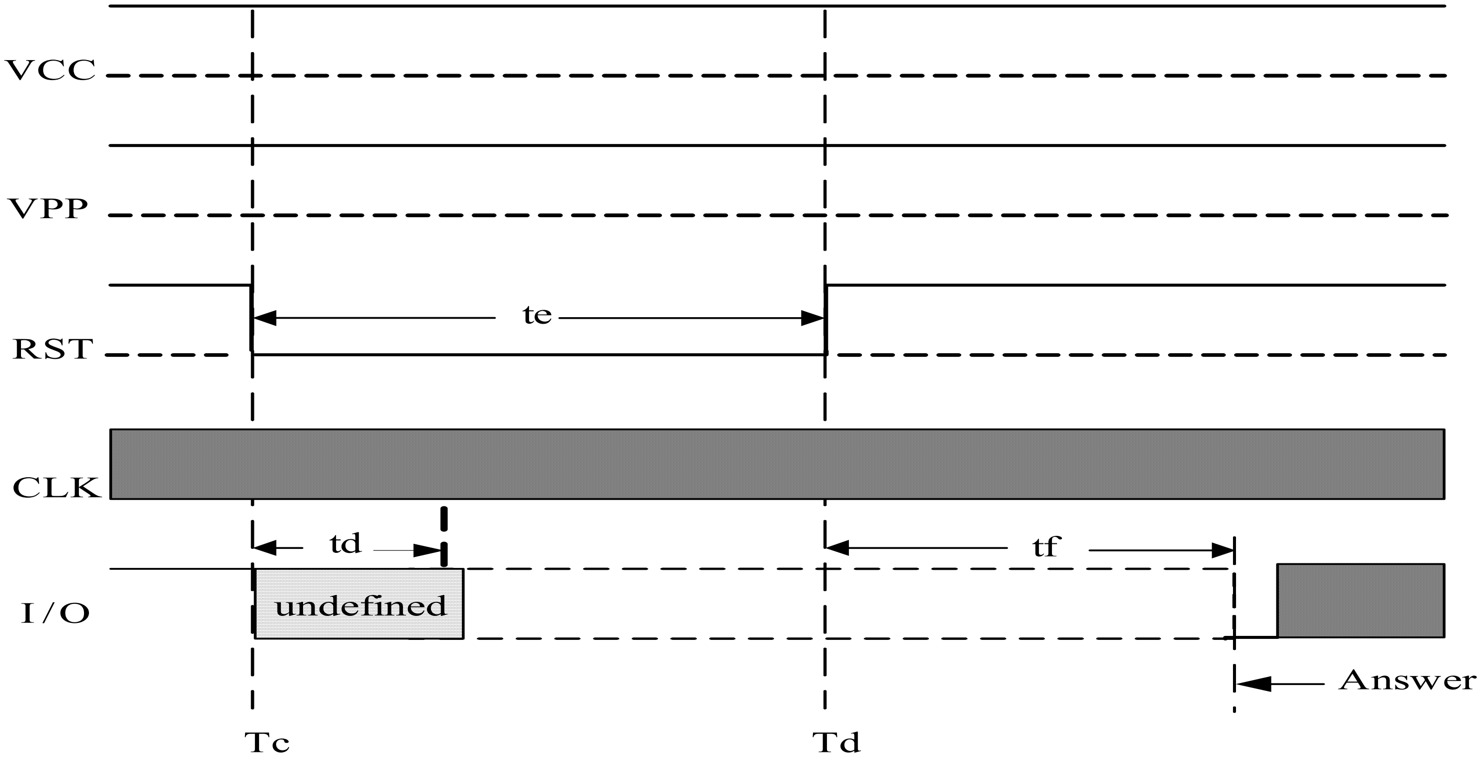
- ISO 7816 – 3 / CNS 12971-3
- Selection of the operating class
  - class A : 5V Vcc
  - class B : 3V Vcc
- The interacted operations
  - Activation of the electrical circuits by the interface device.
  - Information exchange between card and interface device always initiated by the card answering to the cold reset.
  - Deactivation of the electrical circuits by the interface device.

Activation and Cold Reset



$ta \leq \frac{200}{f}$ $\frac{400}{f} \leq tb$ $\frac{400}{f} \leq tc \leq \frac{40000}{f}$

Warm Reset

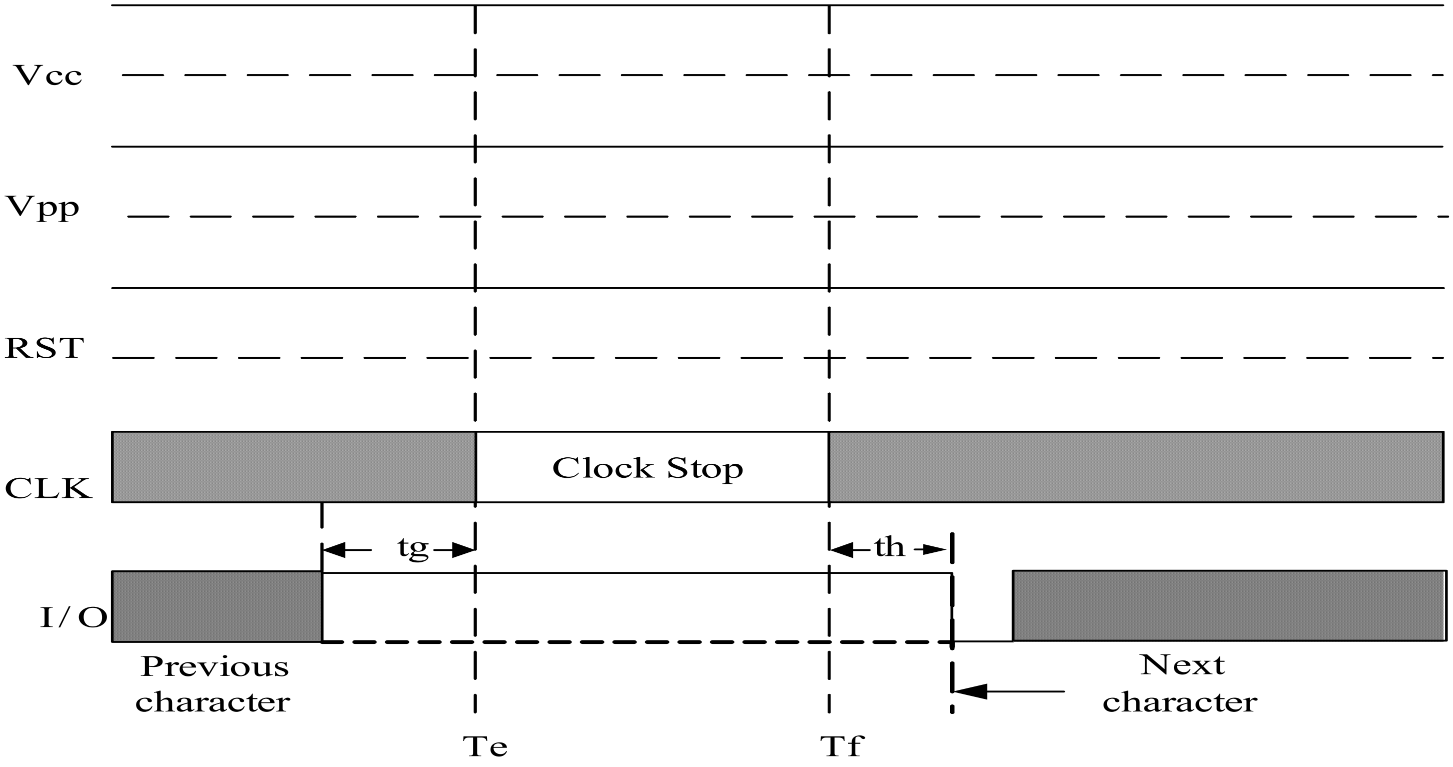


$td \leq \frac{200}{f}$

$\frac{400}{f} \leq te$

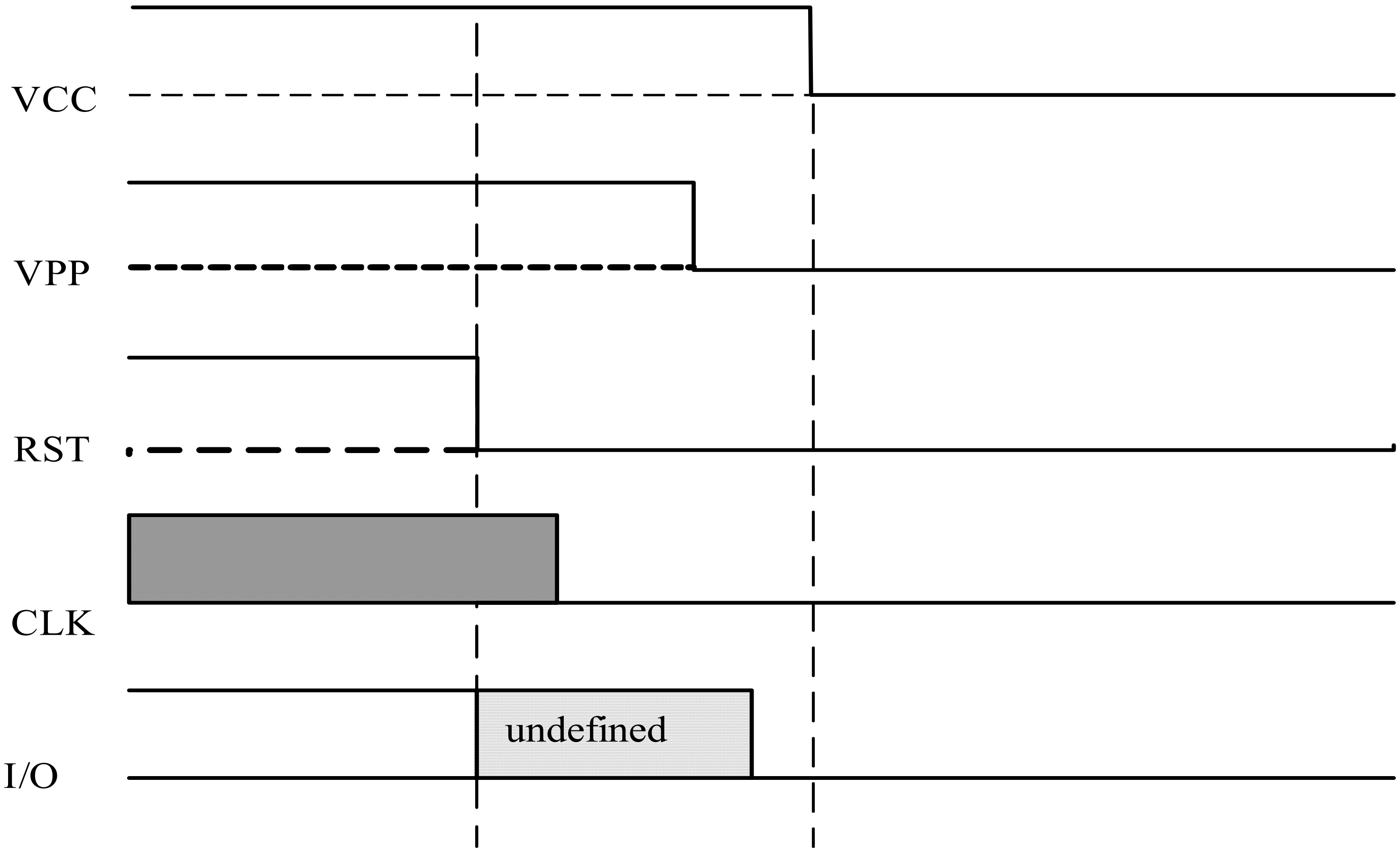
$\frac{400}{f} \leq tf \leq \frac{40000}{f}$

Clock Stop



$$\frac{1860}{f} \leq tg \qquad \frac{700}{f} \leq th$$

Deactivation



Answer to reset (ATR)

- Definition : Answer to Reset is the value of the sequence of bytes sent by the card to the interface device as the answer to a reset.
- Communication with the card is always initiated by the terminal.
- The data transmission process always follows the master-slave principle, with the terminal as master and the card as slave.

Answer to reset (cont.)

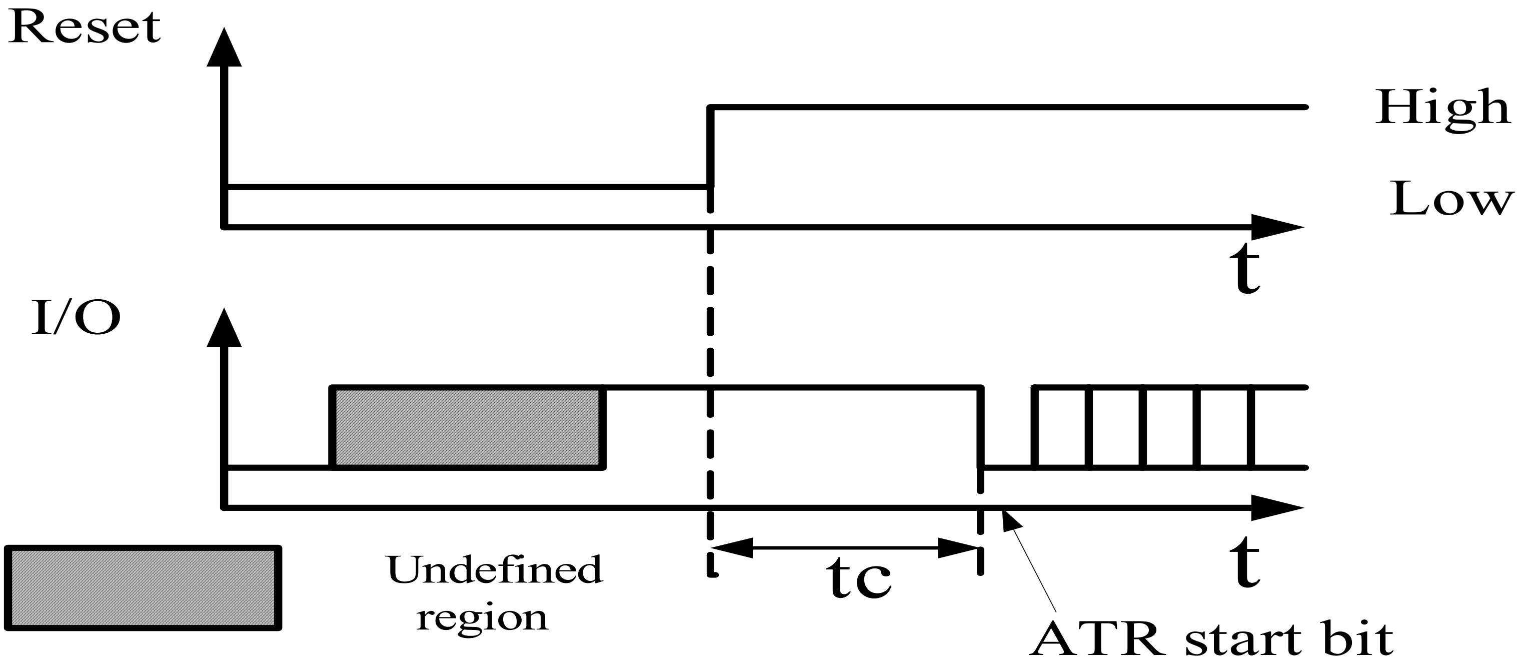
- The card executes a power-on reset and then sends an ATR to the terminal.
- The ATR data string, which contains at most 33 bytes, most often consists of only a few bytes.
- Initial waiting time (9600 etu maximum):

  The time between the leading edges of two successive byte (character) during the ATR.

Elementary time unit (etu): It is the duration of one bit.

Answer to reset (cont.)

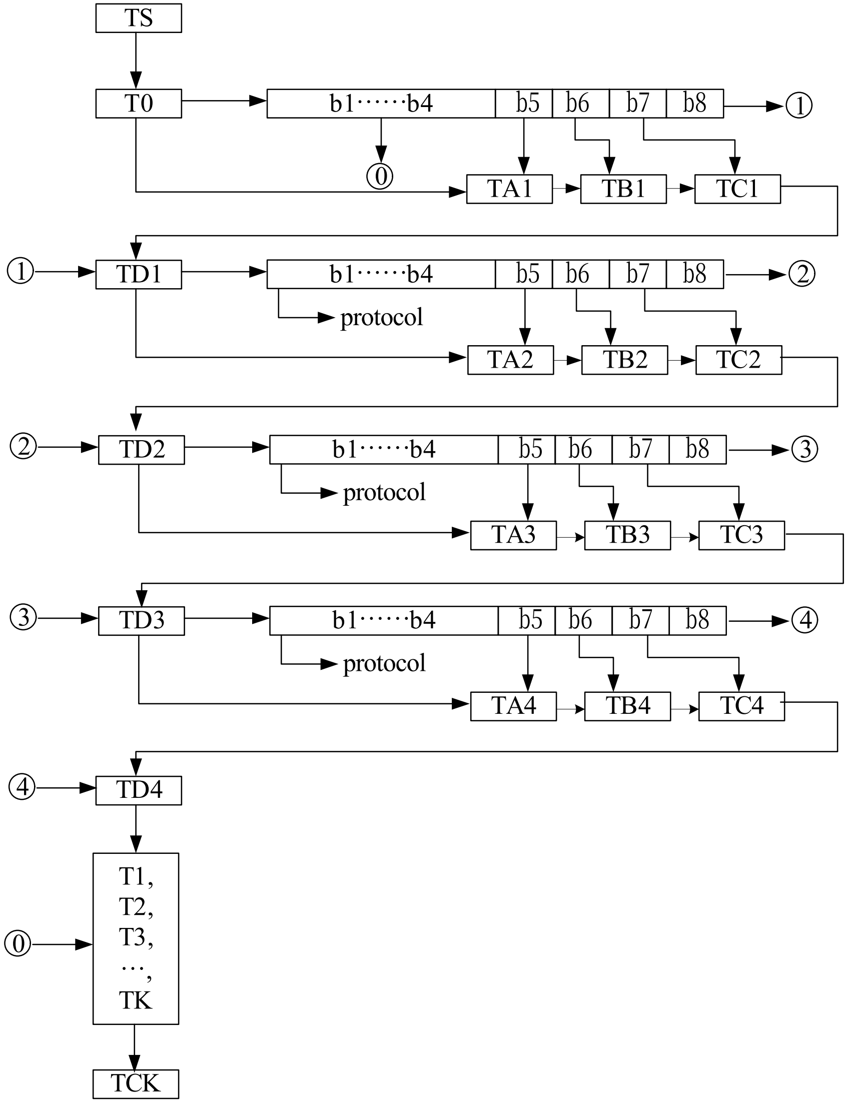
- The start of the ATR transmission must occur between 400 and 40,000 clock cycles (tc) after the terminal issues the reset signal.



Answer to Reset (Cont.)

- Successful reset includes follow asynchronous characters:
  - Ts: Initial character (1 byte)
  - T0: Format character (1 Byte)
  - Interface characters: TA(1), TB(1), TC(1), TD(1), and TA(2) etc.
  - The Historical characters:T1…Tk, maximum number is 15.
  - The Check character: TCK

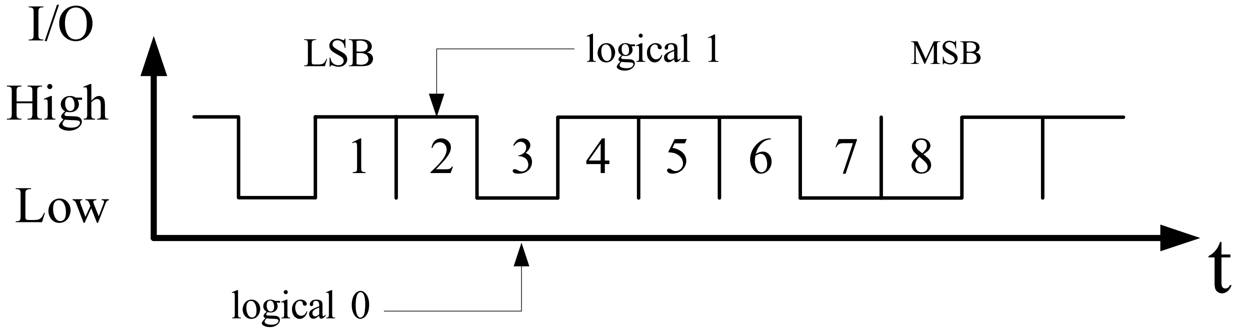
Basic structure and data elements of ATR



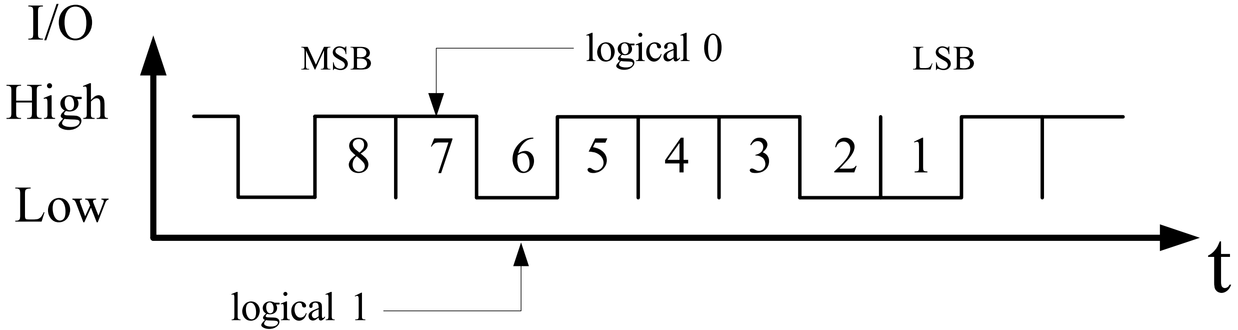
ATR characters

Data element	Description
TS	Initial character, mandatory
T0	Format character, mandatory
TA1, TB1, TC1, TD1	Interface characters, optional
T1, T2, ……, TK	Historical characters, optional
TCK	Check character, conditional

Data transmission convention

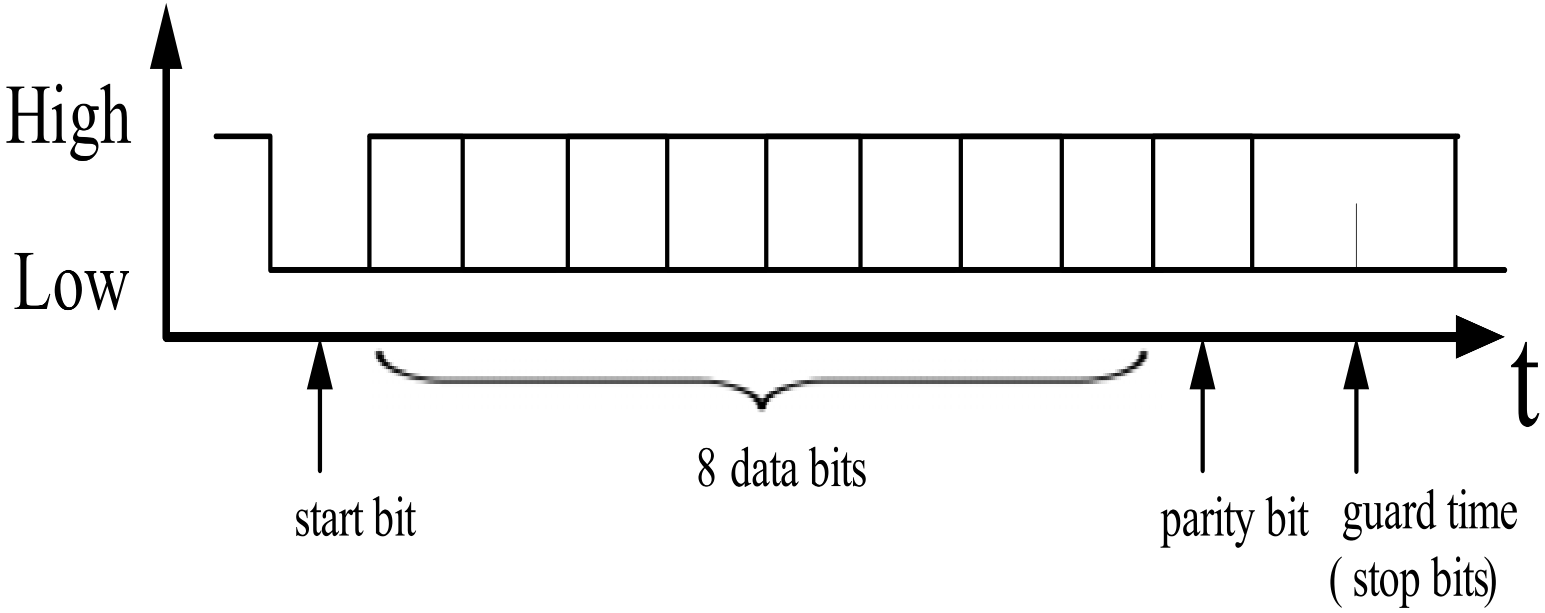


Direct convention

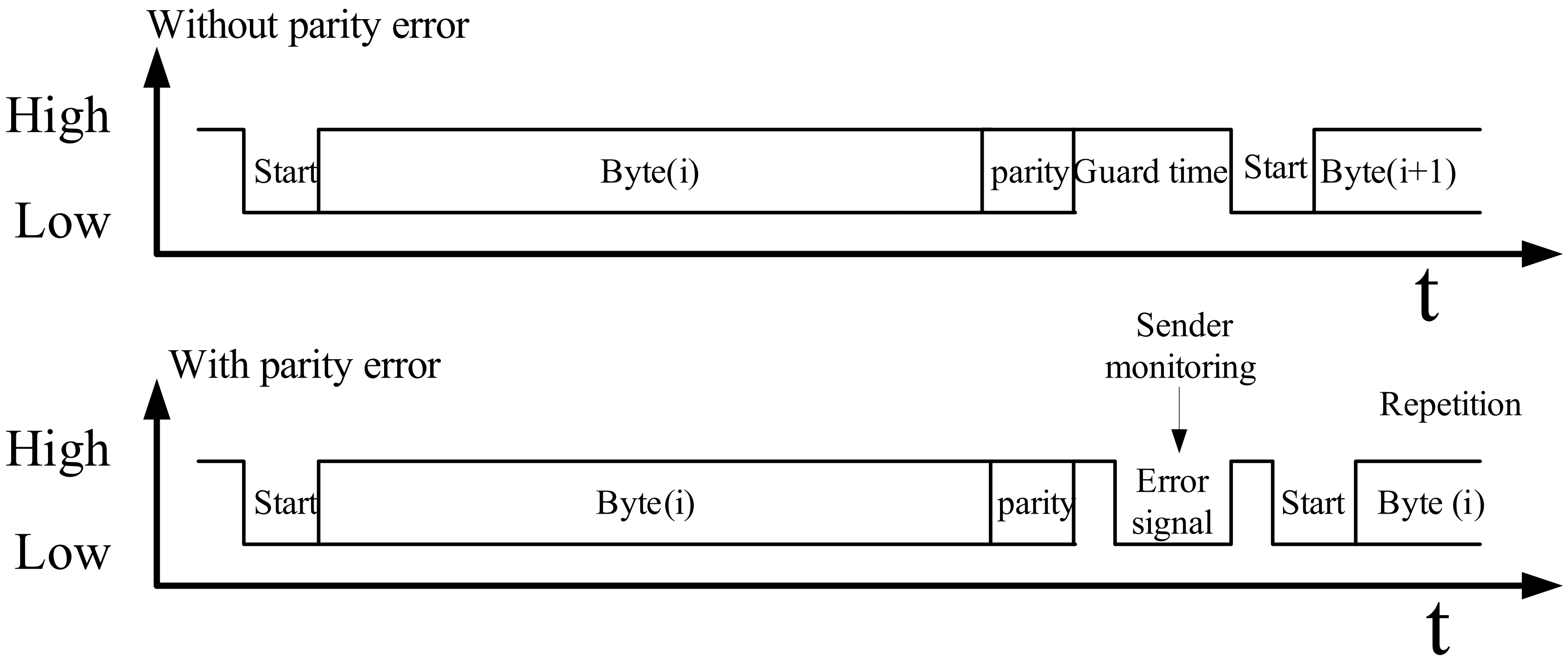


Inverse convention

Character structure



Character transmission and repetition diagram

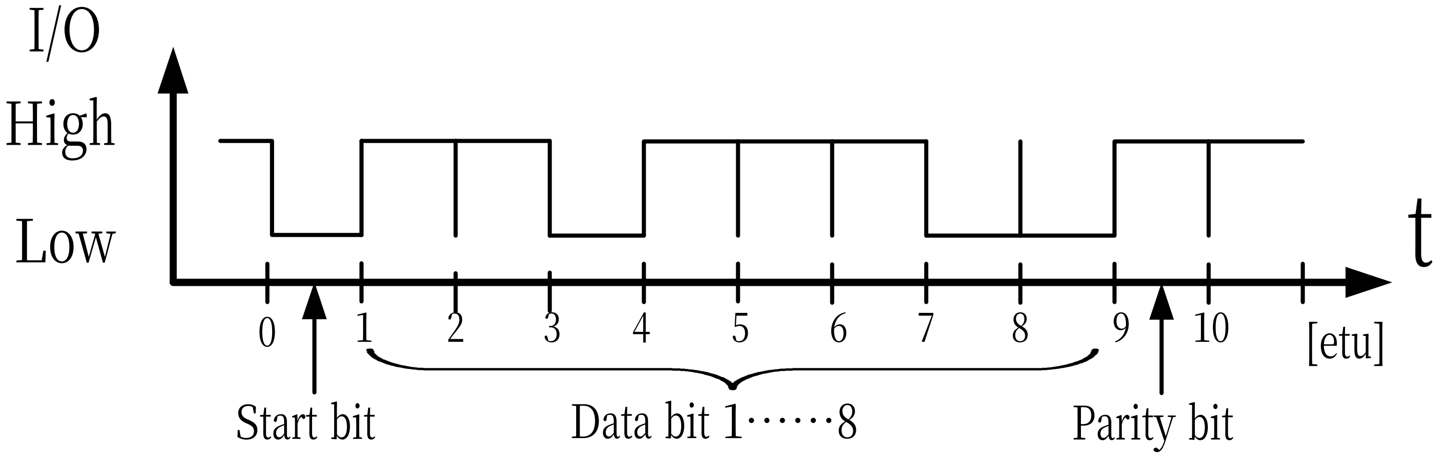


The repetition procedure is mandatory for T=0 and the others are optional.

Initial character TS

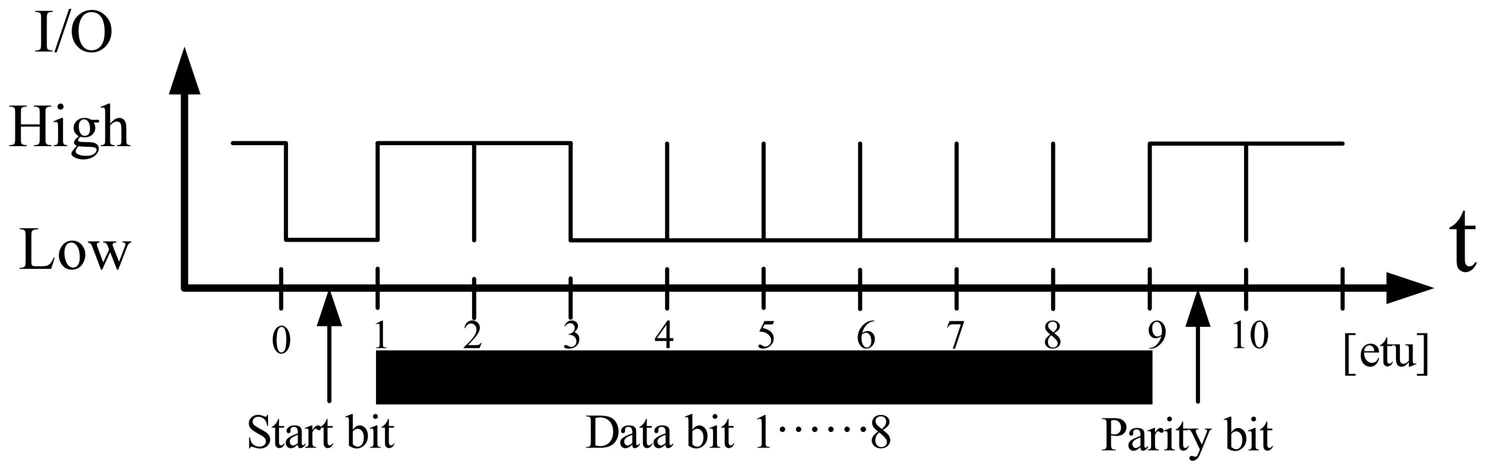
b8 b7 b6 b5 b4 b3 b2 b1	Meaning
‘3B’	Direction convention
‘3F’	Inverse convention

Initial character TS (cont.)



Direct convention (’3B’= 0011 1011)

Initial character TS (cont.)



Inverse convention (‘3F= 0011 1111)

Format character T0

b8 b7 b6 b5	b4 b3 b2 b1	Meaning
… … … …	‘0’ ‘F’	Number of historical characters (K=0 to 15)
… … … 1	… … … …	TA1 sent
… … 1 …	… … … …	TB1 sent
… 1 … …	… … … …	TC1 sent
1 … … …	… … … …	TD1 sent
← Y1 →	← K →	

Interface character TDi
i = 1,2,…

b8 b7 b6 b5	b4 b3 b2 b1	Meaning
… … … …	‘0’ ‘F’	Transmission protocol number (T=0 to 15)
… … … 1	… … … …	TA(i+1) sent
… … 1 …	… … … …	TB(i+1) sent
… 1 … …	… … … …	TC(i+1) sent
1 … … …	… … … …	TD(i+1) sent

If TDi is absent, the interface characters TA(i+1),TB(i+1), TC(i+1) and TD(i+1) are absent.

Global and specific interface characters

- The interface characters TAi, TBi, TCi, for i = 1, 2, 3,…are either global or specific.

Global interface characters refer to parameters of the integrated circuits within the card.

Specific interface characters refer to parameters of a transmission protocol offer by the card.

Global and specific interface characters (cont.)

- The interface characters TA1, TB1, TC1, TA2, TB2 are global.
- The interface character TC2 is specific.
- The interface characters TAi, TBi, TCi for i＞2 depends on the value of parameter T (i.e. b4 b1) in TD(i-1). If T ≠ 15 the characters are specific. If T = 15,the characters are global.

Global interface character TA1

b8 b7 b6 b5	b4 b3 b2 b1	Meaning
‘0’ ’F’ …	… ‘0’ ’F’	FI DI

Bit interval

- The bit interval for the ATR and PPS are called

  initial etu =372 / f (sec), f: clock frequency
- The bit interval after the ATR and PPS are called

  work etu = F / (D . f) (sec), f: clock frequency
- The transmission rate (i.e., 1/etu) to be modified and adapted to individual circumstances by F and D.

Global interface character TA1 (cont.)

FI	0000	0001	0010	0011	0100	0101	0110	0111
F	372	372	558	744	1116	1488	1860	RFU
f_{max}	4 MHz	5 MHz	6 MHz	8 MHz	12 MHz	16 MHz	20 MHz	…
FI	1000	1001	1010	1011	1100	1101	1110	1111
F	RFU	512	768	1024	1536	2048	RFU	RFU
f_{max}	…	5 MHz	7.5 MHz	10 MHz	15 MHz	20 MHz	…	…

F: Clock rate conversion factor

f_{max} : maximum allowable clock rate

Global interface character TA1 (cont.)

DI	0000	0001	0010	0011	0100	0101	0110	0111
D	RFU	1	2	4	8	16	32	RFU
DI	1000	1001	1010	1011	1100	1101	1110	1111
D	12	20	RFU	RFU	RFU	RFU	RFU	RFU

D : bit rate adjustment factor

Global interface character TAi

The value of TAi is interpreted as XI // UI if i＞2 and T = 15 in TD(i-1).

b8 b7	b6 b5 b4 b3 b2 b1	Meaning
00 11	…	XI
…	’00’ ’FF’	UI

Global interface character TAi (cont.)

XI	00	01	10	11
Meaning	Not support	Low state	High state	No preferred state
UI	000001	000010	000011	All other values
Meaning	Voltage class A 4.5—5.5 V	Voltage class B 2.7—3.3 V	Voltage classes A & B	RFU

XI : the clock stop indicator

UI : the class indicator

Global interface character TB1

- b8 = 0
- b7 b6 (II), the reference to the maximum programming current
- b5 b1(PII), the value of the programming voltage
- These parameters were only need for the first generation (used EPROM) of smart cards. It is normally no longer used in the ATR now.

Global interface character TC1

b8 b7 b6 b5 b4 b3 b2 b1	IFSC
’00’ ‘FE’	Extra guard time, with a range of N= 0--254

‘FF’	N=255 and T=0: guard time =2 etu
	N=255 and T=1: guard time =1 etu

Global interface character TC1 (cont.)

- The extra guard time:

  -- It is defined as an extension to the duration of stop bit.

  -- The card requires the extra time delay from the leading edge of the previous character.

  -- The extra guard time = 12 + (Q.   N/f)   (etu),

  Q = F/D

Global interface character TB2

- b8 b1(PI2) : the external programming voltage in tenths of a volt.
- It is normally no longer used in the ATR, for same reason as TB1.

Specific interface character TC2

(for the T=0 transmission protocol)

b8 b7 b6 b5 b4 b3 b2 b1	Meaning
’XX’	WI

- TC2 is the final parameter for the T=0 protocol.
- If the TC2 character is not present in the ATR, the default value of WI=10.

Specific interface character TC2 (cont.)

(for the T=0 transmission protocol)

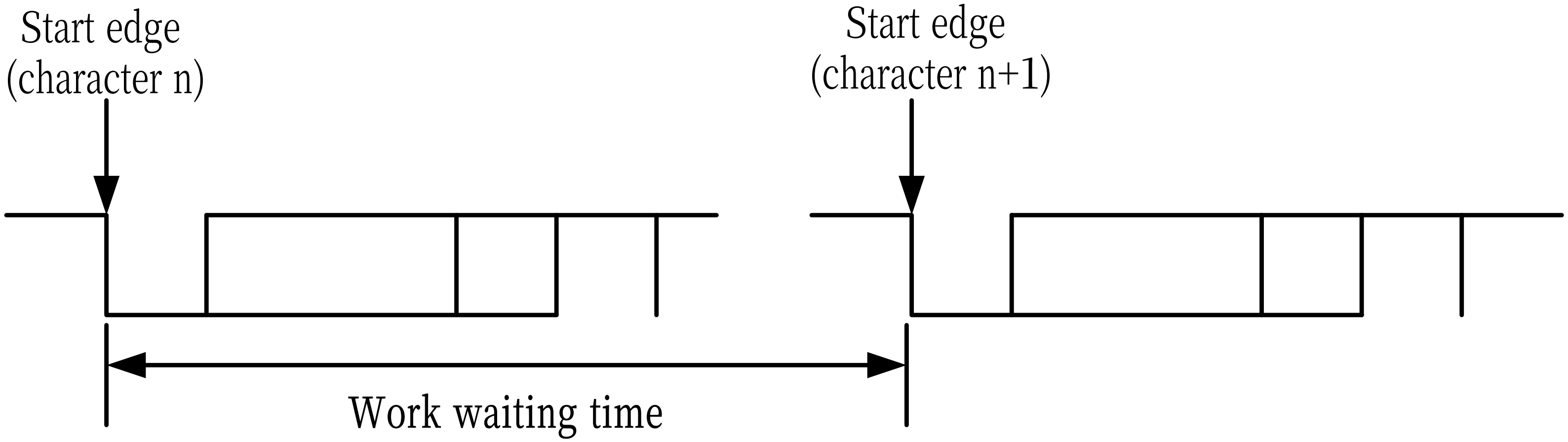
- **Work waiting time (WWT)**

  It is defined the maximum interval between the leading edges of two consecutive bytes .

working waiting time = (960. D. WI) (etu)

Specific interface character TC2 (cont.)

(for the T=0 transmission protocol)



Specific interface character TAi

(for i＞2 and the T=1 transmission protocol)

b8 b7 b6 b5 b4 b3 b2 b1	Meaning
’XX’	The maximum length of the information field size that can be received by the card (IFSC)

The default value of IFSC (information field size for the card) is 32 bytes.

Specific interface character TBi

(for i＞2 and the T=1 transmission protocol)

b8 b7 b6 b5	b4 b3 b2 b1	Meaning
…	‘X’	CWI
‘X’	…	BWI

Specific interface character TBi (cont.)

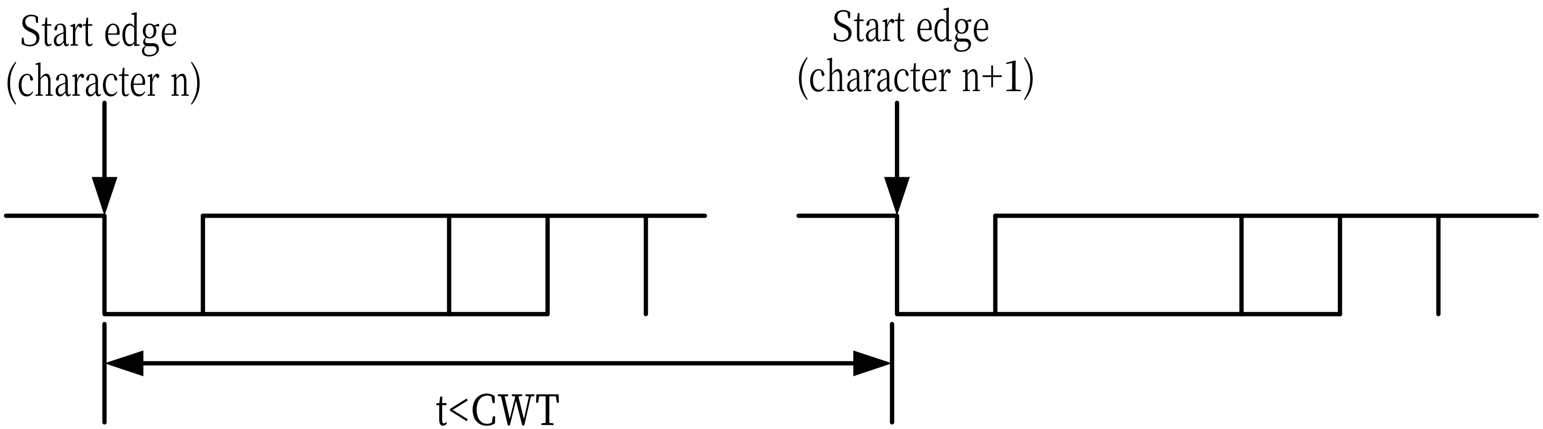
(for i＞2 and the T=1 transmission protocol)

- **Character waiting time (CWT)**
  It is defined as a maximum interval between the leading edges of two consecutive characters within a block.

Character waiting time (CWT) $= 2^{\mathrm{CWI}} + 11$ (etu)

Specific interface character TBi (cont.)

(for i＞2 and the T=1 transmission protocol)



Specific interface character TBi (cont.)

(for i＞2 and the T=1 transmission protocol)

- **Block waiting time (BWT)**

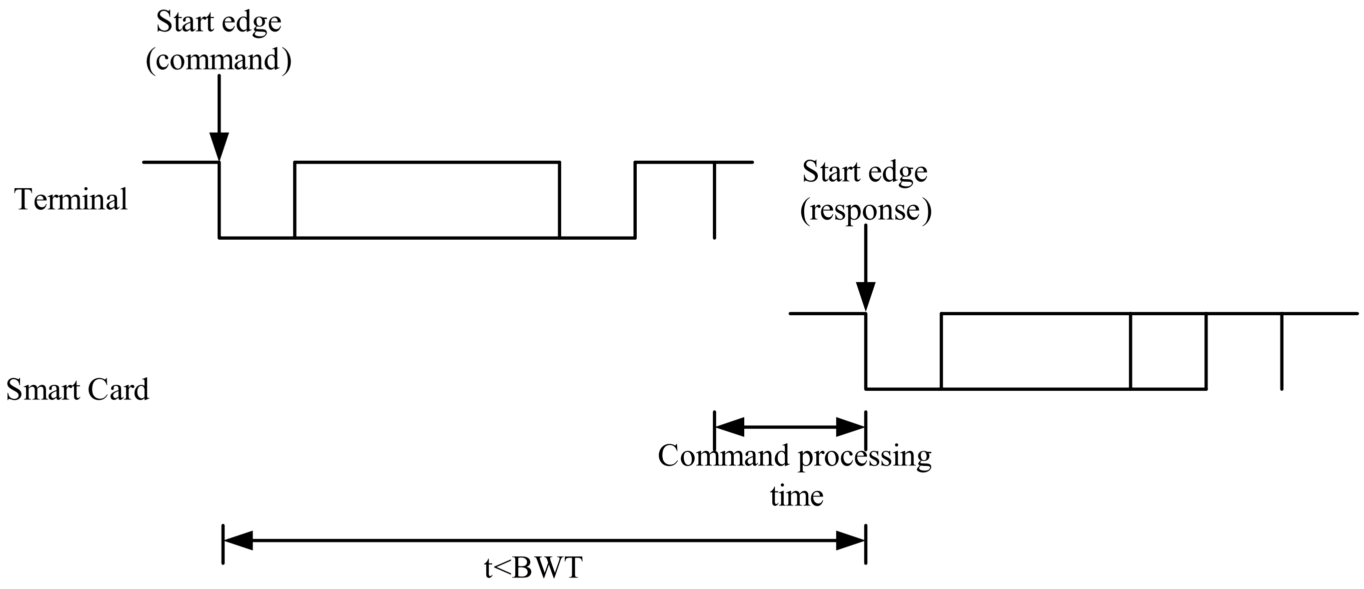
  It is the maximum allowed interval between the leading edge of the last byte of a block sent to the card and the leading edge of the first byte returned by the card.

Block waiting time (BWT) = 2^{BWI}. 960. 372/f + 11 (etu)

Specific interface character TBi (cont.)

(for i＞2 and the T=1 transmission protocol)

Last character of the block (command) First character of the block (response)



Specific interface character TC(i)

(for i＞2 and the T=1 transmission protocol)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
…	…	…	…	…	…	…	0	LRC is used
…	…	…	…	…	…	…	1	CRC is used
0	0	0	0	0	0	0	…	RFU

Historical characters T1, T2, …, Tk

- The historical characters designate general information, for example, the card manufacture, the chip inserted in the card, the masked ROM in the chip, the state of the life of the card.

Check character TCK

- The check character TCK contains the XOR checksum of the bytes from T0 through the last byte before the check character.

Practical example of ATR

(W. Rankle and W. Effing, “smart Card Handbook”, John Wiley &Sons, third edition,2003)

Designation	Value	Meaning	Remark
TS	‘3B’	direct convention	
T0	‘B5’	Y0=‘B’=1011	TA1,TB1 and TD1
		K=‘5’	follow 5 historical characters
TA1	’11’	FI=‘1’=0001	F=372
		DI=‘1’=0001	D=1
TB1	’00’	II=0	I=0
		PII=0	Vpp contact not used
TD1	’81’	Y1=‘8’=1000	TD2 follows
		T=1	Transmission protocol T=1
TD2	’31’	Y2=‘3’=0011	TA3 and TB3 follow
		T=1	Transmission protocol T=1

Practical example of ATR (cont.)

Designation	Value	Meaning	Remark
TA3	‘46’	buffer size=70 bytes	IC card I/O buffer size
TB3	‘15’	BWI=‘1’	BWT=2011 etu
		CWI=‘5’	CWT=43 etu
T1	‘56’	“V”	V 1.0, ASCII code
T2	‘20’	“ “	
T3	’31’	“1”	
T4	‘2E’	“. “	
T5	‘30’	“0”	
TCK	‘1E’	check character	XOR checksum of T0 through T5

Protocol parameter selection (PPS) procedure

- PPS request:

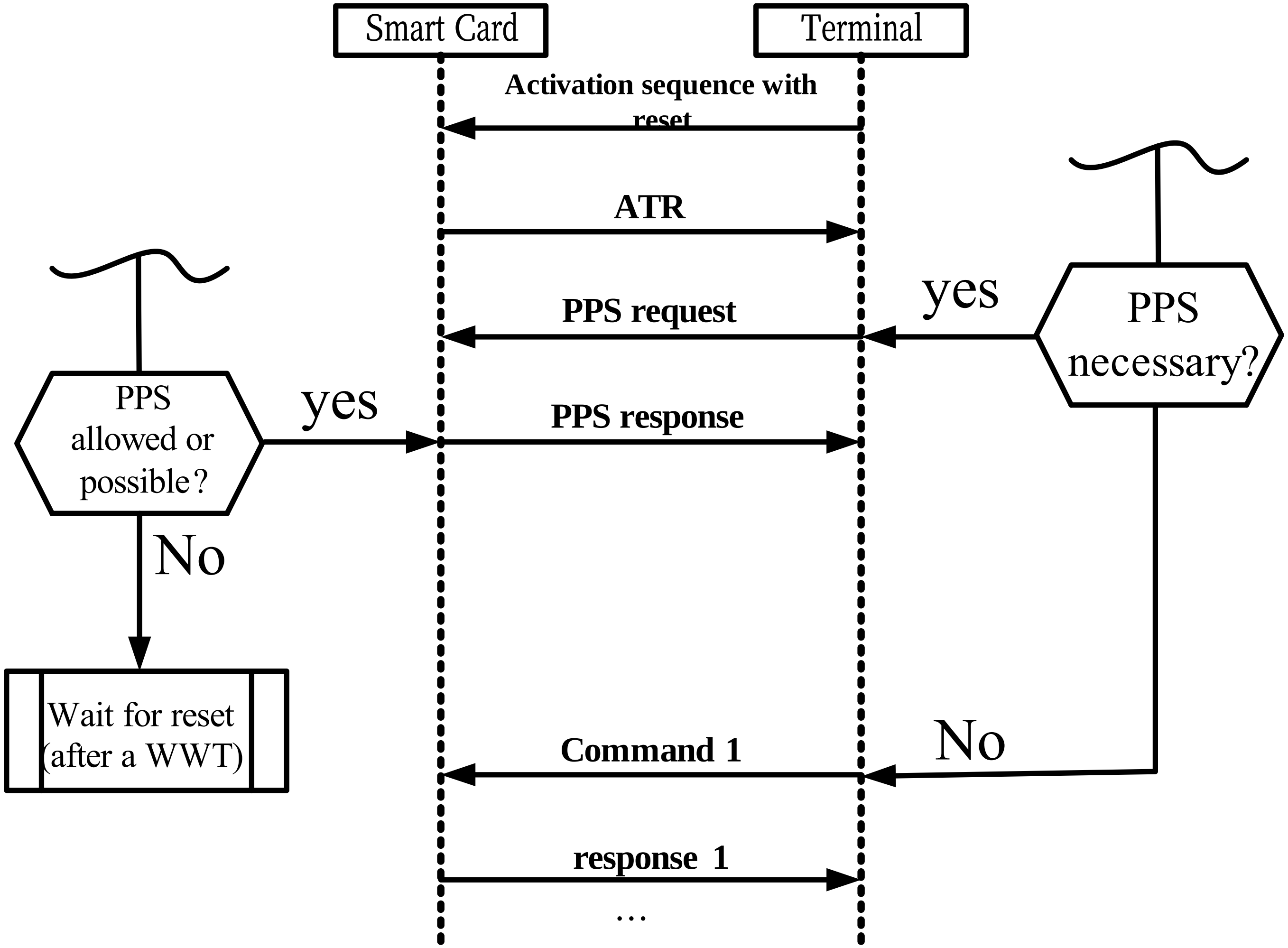
  - If a terminal wants to modify one or more data transmission parameters, which were specified by ATR, it must perform a PPS procedure before the transmission protocol is actually used.

Protocol parameter selection (PPS) procedure (cont.)

- PPS response:

  - If the card allows the requested changes to the protocol parameters, it sends the received PPS bytes back to the terminal (an echo of the received data).

Protocol parameter selection (PPS) procedure (cont.)



Protocol parameter selection (PPS) procedure (cont.)

- **PPS can be performed in two mode:**

-**Negotiable mode**: (TA2 is absent)

The standard values of the divider F and the bit rate adjustment factor D remain unchanged until a PPS is successfully executed.

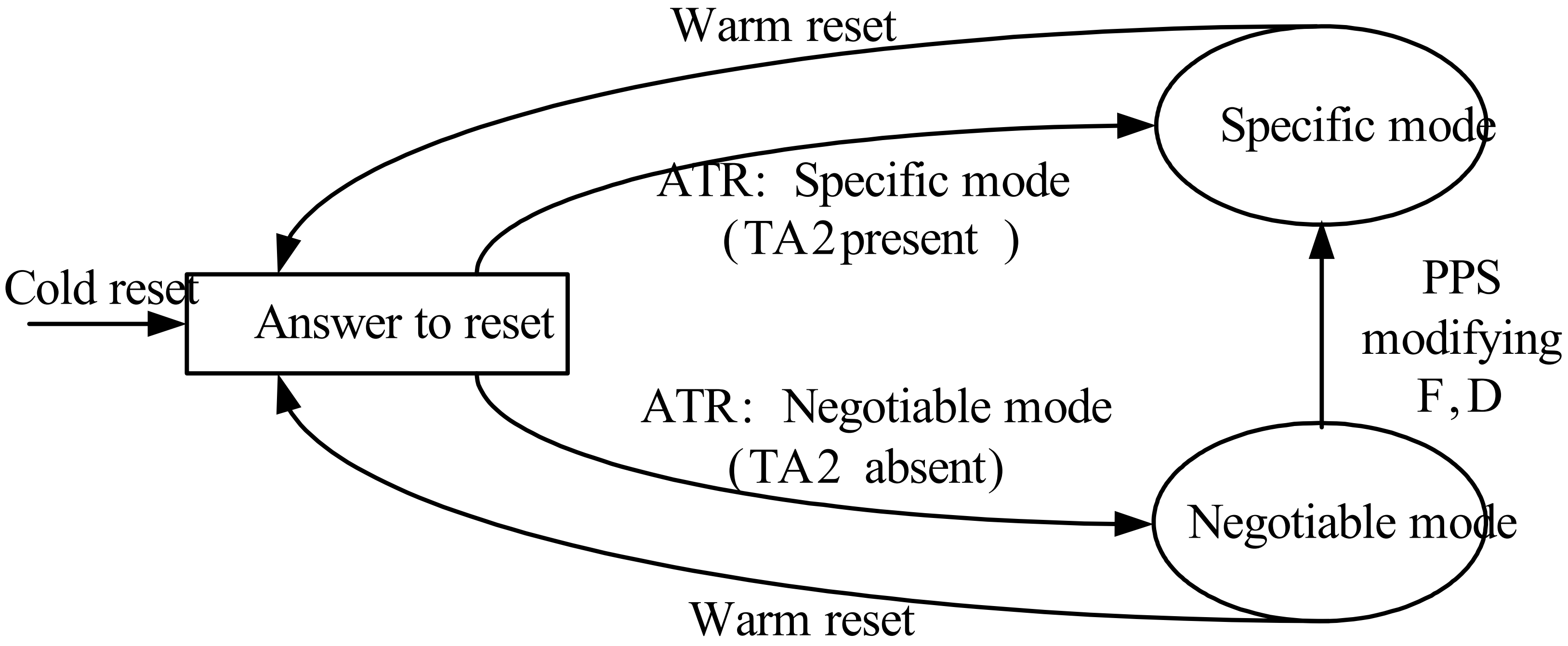
-**Specific mode**: (TA2 is present)

The value of D and F specified by the ATR must be used for transmitting the PPS.

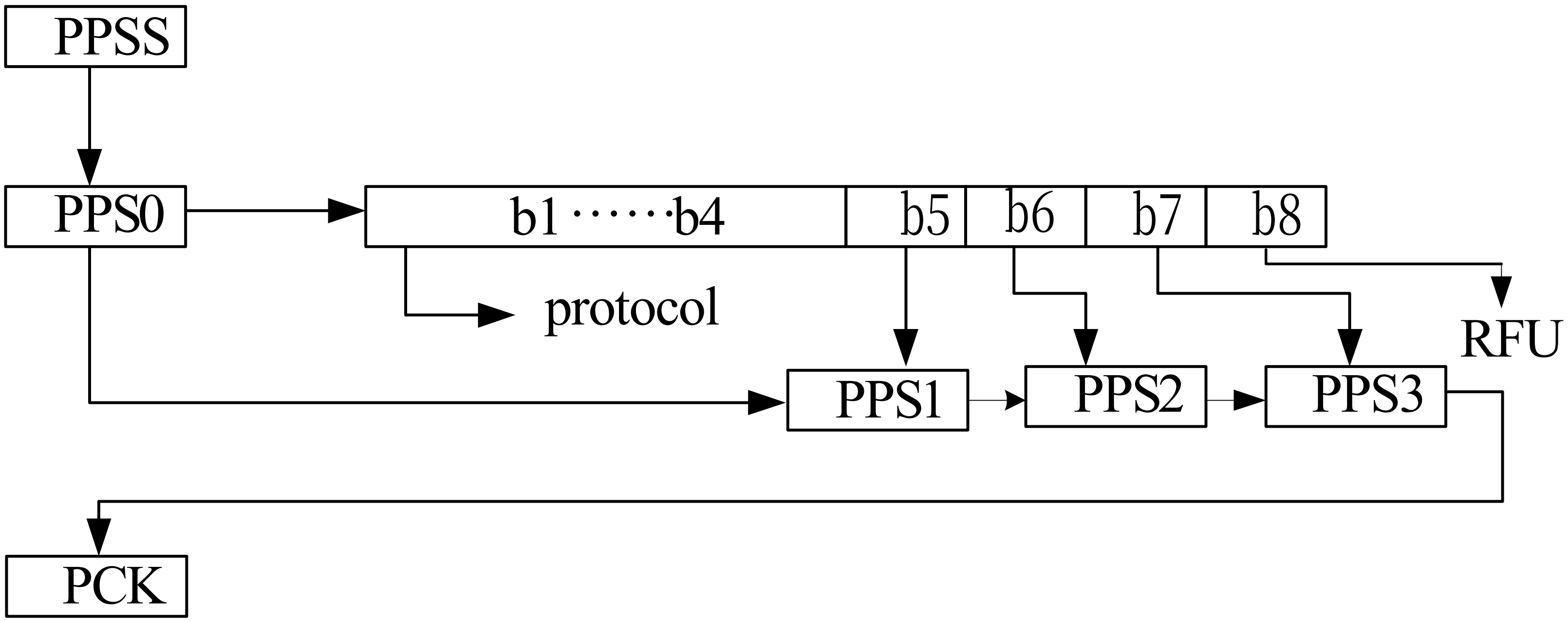
Global interface character TA2

b8 b7 b6 b5	b4 b3 b2 b1	Meaning
0 … … …	…	Switching between negotiable mode and specified mode is possible.
1 … … …	…	Switching between negotiable mode and specified mode is not possible.
… 0 0 …	…	Reserved for future use.
… … … 0	…	Transmission parameters Fi and Di defined by the interface characters.
… … … 1	…	Transmission parameters (use default value) did not define by the interface characters.
… … … …	X	Protocol T=X is to be used in the specific mode

Negotiable and specific mode



The structure and data elements of PPS



The structure and data elements of PPS (cont.)

Data element	Designation
PPSS = ‘FF’	Initial character, mandatory
PPS0	Format character, mandatory
PPS1, PPS2, PPS3	Parameter characters, optional
PCK	Check character, mandatory

Format character PPS0

b8	b7	b6	b5	b4 b3 b2 b1	Meaning
…	…	…	…	X	Transmission protocol to be used
…	…	…	1	…	PPS1 is present
…	…	1	…	…	PPS2 is present
…	1	…	…	…	PPS3 is present
0	…	…	…	…	Reserved for future use

Parameter character PPS1

b8	b7 b6 b5 b4 b3 b2 b1	Meaning
X	…	FI
…	X	DI

PPS2 and PPS3 are reserved for future use.

Check character PCK

- It contains the XOR checksum of all previous bytes, starting with PPSS.

Successful PPS exchange

- If PPS response echoes exactly the PPS request.
- The PPS response is in the following conditions

 1. PPSS-Response = PPSS-Request
 2. PPS0-Response:
    - -- The b1 to b4 shall be echoed.
    - -- If b5=1, PPS1-Response = PPS1-Request.
      If b5=0, PPS1-Response is not present, meaning that Fd= 372 and Dd=1 shall be used.
    - -- If b6=1, PPS2-Response = PPS2-Request.
      If b6=0, PPS2-Response and PPS2-Request are both absent.
    - -- If b7=1, PPS3-Response = PPS3-Request.
      If b7=0, PPS3-Response and PPS3-Request are both absent.

Data transmission protocols

- Synchronous data transmission protocol

  -- memory chips card
- Asynchronous data transmission protocol

  -- processor chips card

Asynchronous data transmission protocol

Protocol	Meaning
T=0	•Asynchronous, half-duplex, byte oriented, specified in ISO/IEC 7816-3
T=1	•Asynchronous, half-duplex, block oriented specified in ISO/IEC 7816-3 Amd. 1
T=2	•Asynchronous, full duplex, block oriented specified in ISO/IEC 10536-4

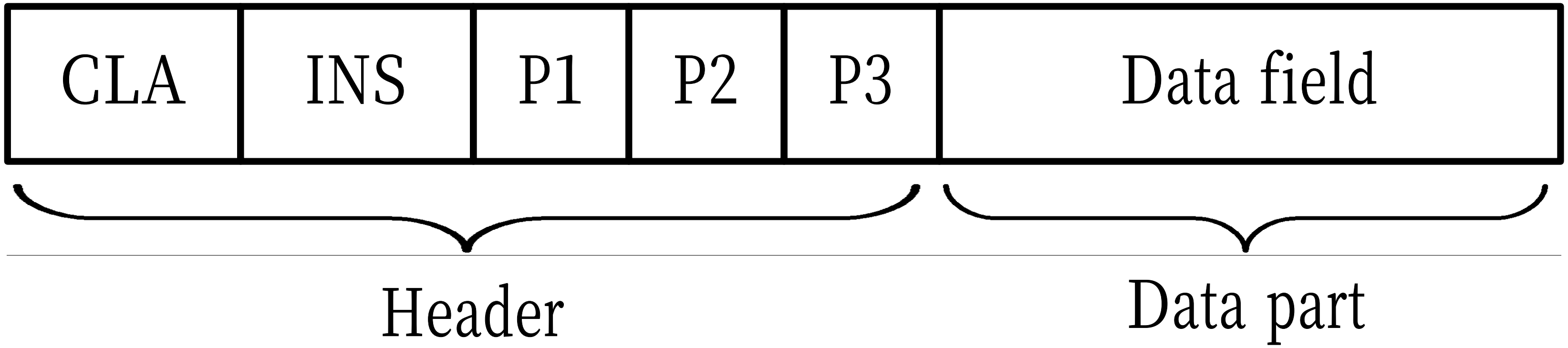
Asynchronous data transmission protocol (cont.)

Protocol	Meaning
T=3	•Full duplex, not yet specified
T=4	•Asynchronous, half-duplex, byte oriented extension of T=0, not yet specified
T=5..13	•Reserved for future use
T=14	•For national use, not standardized by ISO
T=15	•Reserved for future use

T=0 transmission protocol

- The first internationally standardized of smart card protocols
- Designed for minimum memory usage and maximum simplicity
- Asynchronous and half-duplex
- Byte oriented with parity bit error detecting
- Allows an external programming voltage for EEPROM/EPROM

Structure of a command with the T=0 protocol



CLA | INS | P1 | P2 | P3 | Data field

Header

Data part

CLA: Class byte INS: Instruction/Command byte

P1 P3: Parameter bytes Data field: Optional

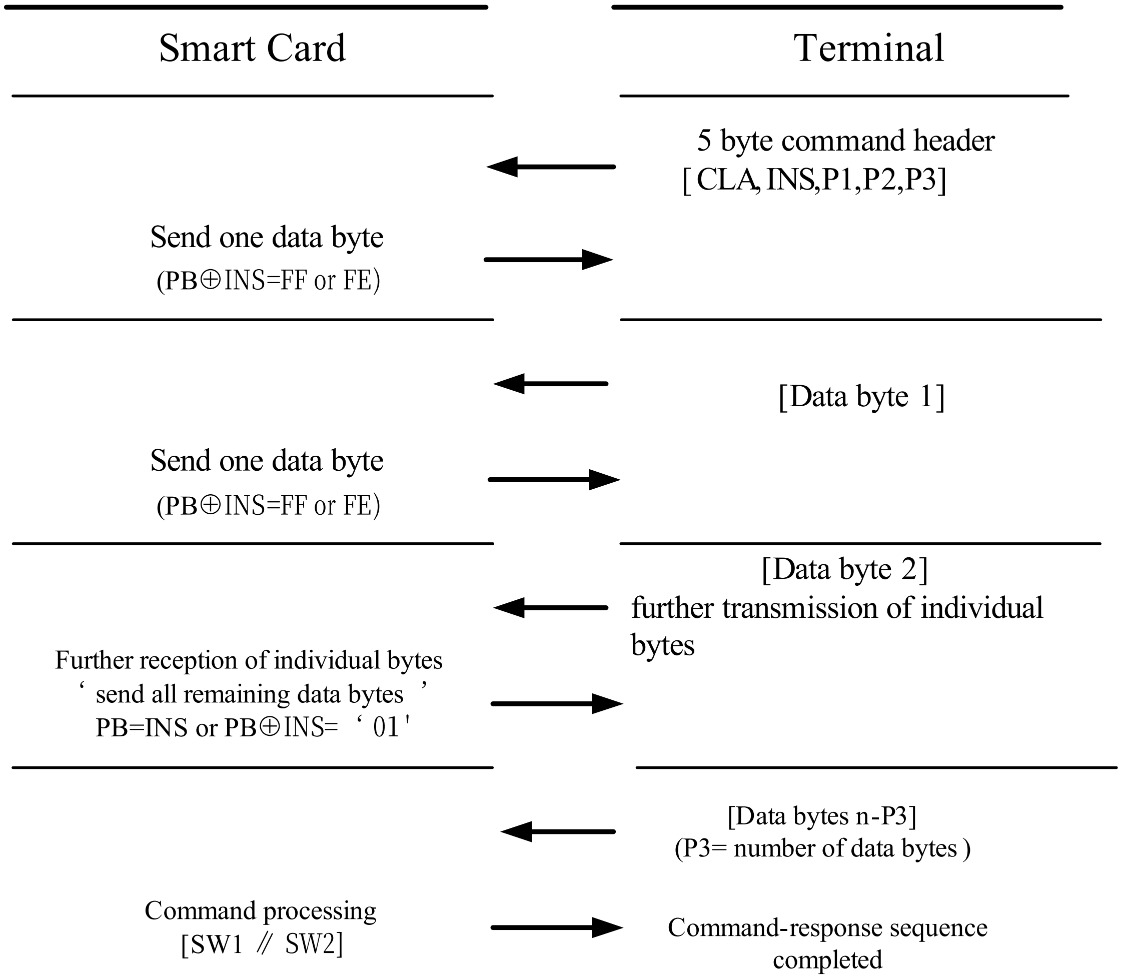
Procedure byte

The card returns a procedure byte (PB) after it received a command byte (INS byte).

Byte (PB)	**Value**	**Result on Vpp**	**Result on data transfer**	**Then reception of**
NULL	’60’	No action	No action	A procedure byte
ACK	INS	Pause state	All remaining data byte	A procedure byte
	INS⊕’01’	Programming state	All remaining data byte	A procedure byte
	INS⊕’FF’	Pause state	The next data byte	A procedure byte
	INS⊕’FE’	Programming state	The next data byte	A procedure byte
SW1	‘6X’(≠’60’), ‘9X’	Pause state	No action	A SW2 byte

Example:

(W. Rankle and W. Effing, “smart Card Handbook”, John Wiley &Sons, third edition,2003)



Smart Card

Terminal

5 byte command header
[CLA, INS,P1,P2,P3]

Send one data byte
(PB⊕INS=FF or FE)

[Data byte 1]

Send one data byte
(PB⊕INS=FF or FE)

[Data byte 2]
further transmission of individual bytes

Further reception of individual bytes
‘ send all remaining data bytes ’
PB=INS or PB⊕INS= ‘ 01'

[Data bytes n-P3]
(P3= number of data bytes)

Command processing
[SW1 // SW2]

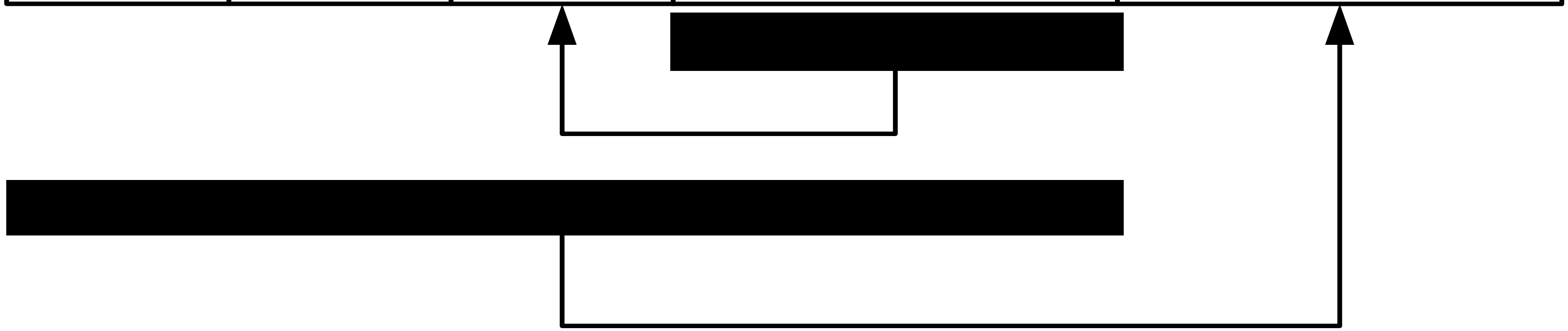
Command-response sequence completed

T=1 transmission protocol

- Asynchronous and half-duplex
- Block oriented with LRC/CRC error detecting
- Block chaining function
- Permits secure data transmission

The structure of a T=1 transmission block

Prologue field			information field	epilogue field
NAD	PCB	LEN	APDU	EDC
1 byte	1 byte	1 byte	0-254 bytes	1-2 bytes



[redacted]

[redacted]

Block types

contents of PCB byte	**Block type**	**Meaning**
b8 = 0	Information block (I-block)	The data of application layer
b8 b7 = 10	Receive ready block (R-block)	A positive or negative acknowledgement
b8 b7 = 11	Supervisory block (S-block)	The control information

Node address (NAD) field

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	…	…	…	X	…	…	…	Vpp control
…	X	X	X	…	…	…	…	DAD (destination address)
…	…	…	…	…	X	X	X	SAD (source address)

Protocol control byte (PCB) for an I-block

b8 b7 b6 b5 b4 b3 b2 b1	Meaning
0 … … … … … … …	I block identifier
… N(S) … … … … … …	Send sequence number
… … X … … … … …	Sequence data bit M
… … … X X X X X	Reserved

Protocol control byte (PCB) for a R-block

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	0	…	…	…	…	…	…	R block identifier
…	…	0	N(R)	0	0	0	0	No error
…	…	0	N(R)	0	0	0	1	EDC or parity error
…	…	0	N(R)	0	0	1	0	Other error

Protocol control byte (PCB) for a S-block

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	1	…	…	…	…	…	…	S block identifier
…	…	0	0	0	0	0	0	Resync request (only from terminal)
…	…	1	0	0	0	0	0	Resync response (only from smart card)
…	…	0	0	0	0	0	1	Request change to IFS
…	…	1	0	0	0	0	1	Response to request change to IFS
…	…	0	0	0	0	1	0	Request abort
…	…	1	0	0	0	1	0	Response to abort request
…	…	0	0	0	0	1	1	Request waiting time extension (only from smart card)
…	…	1	0	0	0	1	1	Response to waiting time extension (only from terminal)
…	…	1	0	0	1	0	0	Vpp error response (only from smart card)

Length (LEN) field

- from ’00’ to ‘FE’; ‘FF’ is reserved for future use

Information field

- In an I block, the information field serves as a container for application layer data.
- In a S block, the information field transfers data for the transmission protocol.
- In a R block, the information field is not necessary.

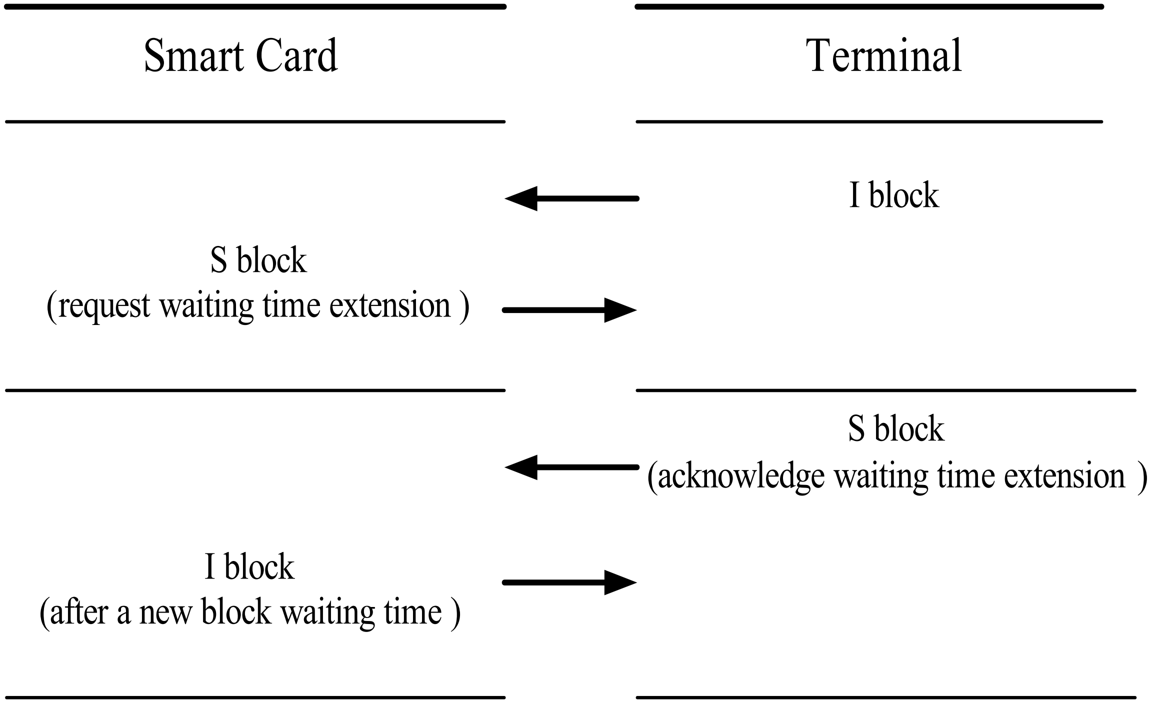
Epilogue field

- The single byte longitudinal redundancy check (LRC) is computed using XOR concatenation of all previous bytes in the block.
- The cyclic redundancy check (CRC) consists of two byte that is carried out according ISO 3309 ($x^{16}+x^{12}+x^{5}+1$).

Waiting time extension

- If the smart card needs more time to generate a response than the maximum time allowed by the BWT , it can request a waiting time extension from the terminal.
- The terminal is not allowed to refuse this request.
- This extension is only valid for the most recently send I-block.

Waiting time extension (cont.)



Smart Card

Terminal

I block

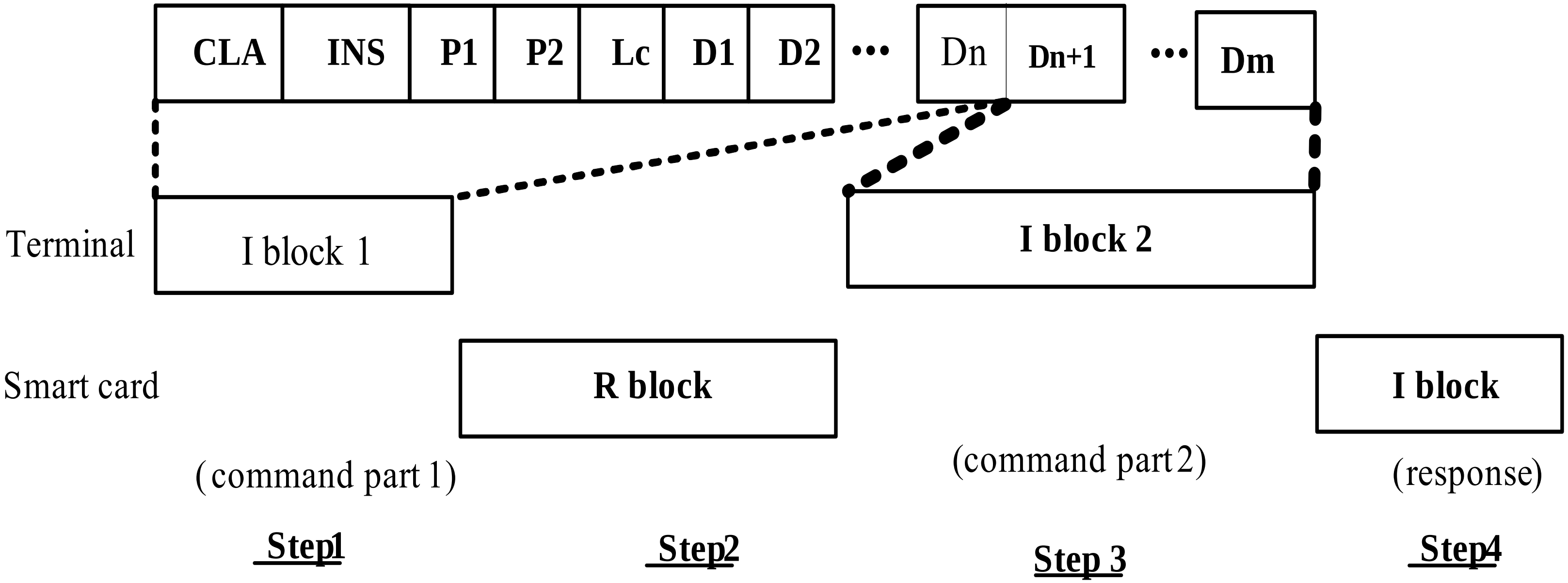
S block
(request waiting time extension)

S block
(acknowledge waiting time extension)

I block
(after a new block waiting time)

Block chaining

- It allows either party to send data blocks that are large than the size of its transmit or receive buffer.

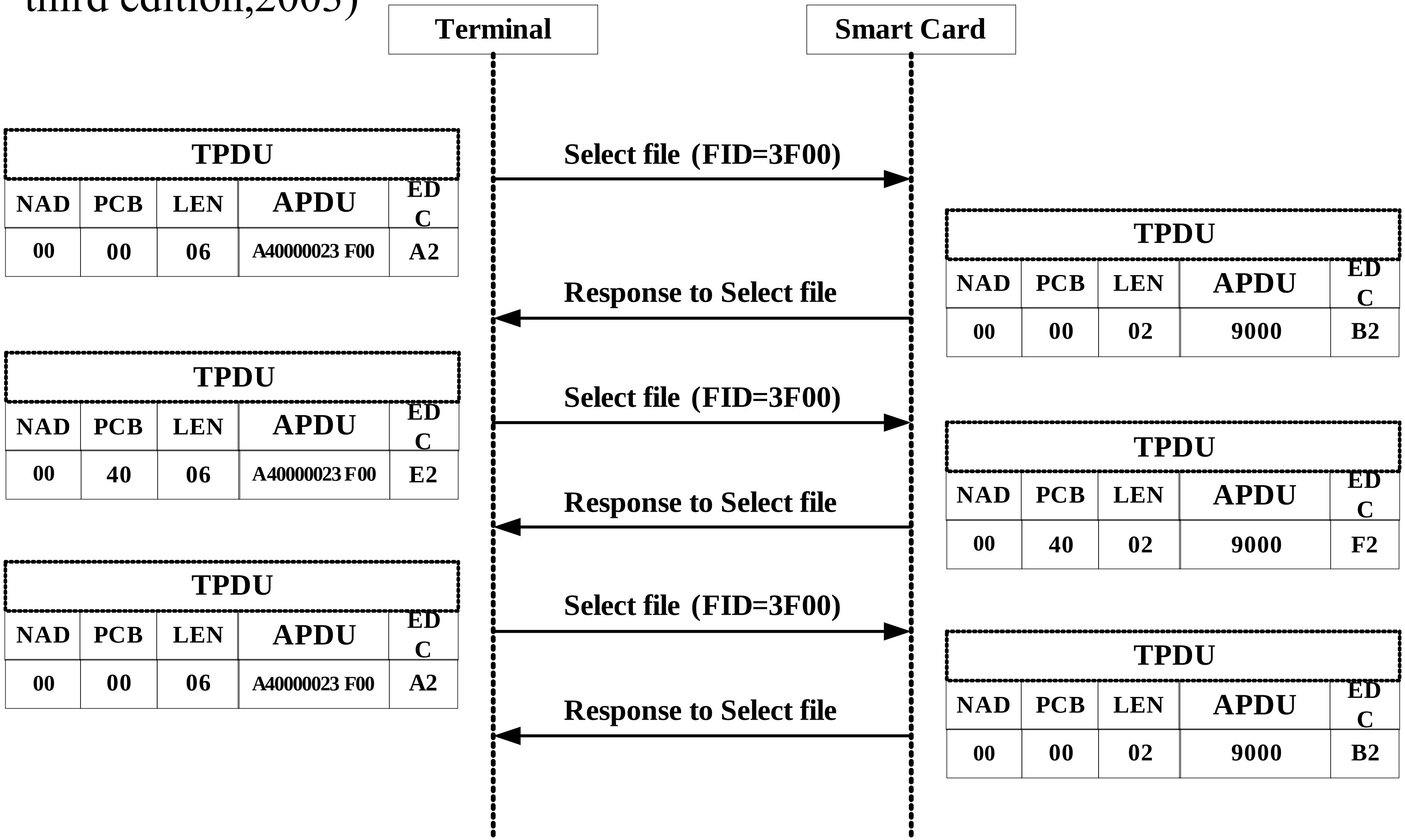


Error handling

Synchronization stage	Mechanism
Stage1	Repeat the erroneous block
Stage2	Resynchronize and then repeat the erroneous block
Stage3	Reset the smart card and establish the connection anew

Example :

(W. Rankle and W. Effing, “smart Card Handbook”, John Wiley &Sons, third edition,2003)



TPDU				
NAD	PCB	LEN	APDU	EDC
00	00	06	A40000023 F00	A2

TPDU				
NAD	PCB	LEN	APDU	EDC
00	00	02	9000	B2

TPDU				
NAD	PCB	LEN	APDU	EDC
00	40	06	A40000023 F00	E2

TPDU				
NAD	PCB	LEN	APDU	EDC
00	40	02	9000	F2

TPDU				
NAD	PCB	LEN	APDU	EDC
00	00	06	A40000023 F00	A2

TPDU				
NAD	PCB	LEN	APDU	EDC
00	00	02	9000	B2

Comparison of asynchronous transmission protocols

Criterion	T = 0	T = 1
Data transmission	asynchronous, half duplex, byte-oriented	asynchronous, half duplex, block-oriented
Standard	ISO/IEC 7816-3, GSM 11.11, EMV	ISO/IEC 7816-3, EMV
Divider	Freely definable, usually 372	Freely definable, usually 372
Block chaining	Not possible	possible
Error detection	Parity bit	Parity bit and EDC at end of block
Memory required for implementation	300 bytes	1100 bytes

Q & A

Thank you ！