Spelunking credit cards with Ruby

Chang Sau Sheong
8 Jan 2013

About me

About me

About me

About me

About me

hp

Garena

Y! YAHOO!

WELCOME

About me

hp

Garena

YAHOO!

WELCOME

About me

About me

hp

Garena

YAHOO!

WELCOME

Ruby on Rails
Web Mashup Projects
A step-by-step tutorial to building web mashups
Chang Sau Sheong
PACKT

About me

hp
Garena
YAHOO!
WELCOME

Cloning Internet Applications with Ruby
Rails
up Projects
PACKT

About me

Garena

YAHOO!

WELCOME

Discover the World Around You Through Programming
Exploring Everyday Things with R and Ruby
Sau Sheong Chang
O'REILLY
...ernet ...s with Ruby
PACKT open source
Rails ...up Projects
PACKT

What computers are you carrying with you?

BRITISH AIRWAYS
4417 1234 5678 9112
CARDMEMBER SINCE 1999
GOOD THRU 00/00
D. WALDEN
EXECUTIVE CLUB # 12345678
VISA
SIGNATURE

BRITISH AIRWAYS
4417 1234 5678 9112
CARDMEMBER SINCE 1999
GOOD THRU 00/00
D. WALDEN
EXECUTIVE CLUB # 12345678
VISA
SIGNATURE

The new at&t
3G

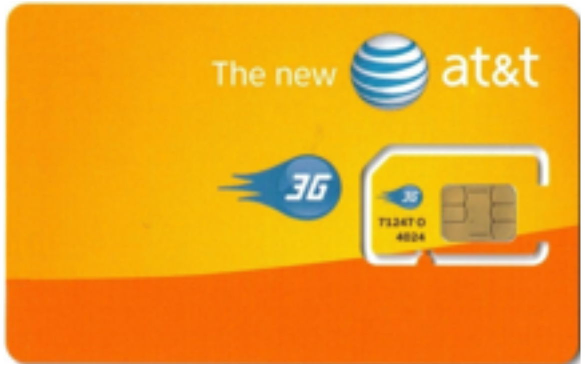
BRITISH AIRWAYS
4417 1234 5678 9112
CARDMEMBER SINCE 1999
GOOD THRU 00/00
D. WALDEN
EXECUTIVE CLUB # 12345678
VISA
SIGNATURE

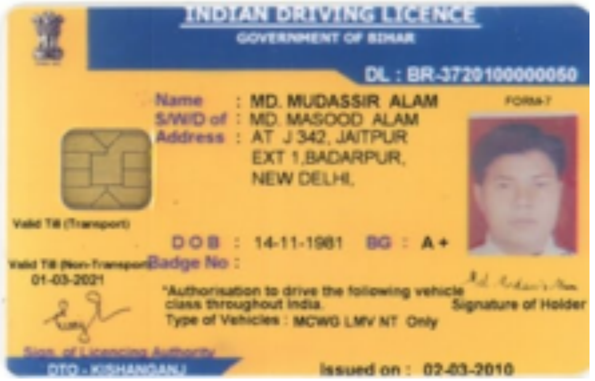
The new at&t
3G

O:K
OMNIKEY

Smart card

A card with an embedded integrated circuit which has components for transmitting, storing and processing data


The new at&t
3G


INDIAN DRIVING LICENCE
GOVERNMENT OF BIHAR
DL : BR-3720100000050
Name : MD. MUDASSIR ALAM
S/W/D of : MD. MASOOD ALAM
Address : AT J 342, JAITPUR
EXT 1,BADARPUR,
NEW DELHI.
DOB : 14-11-1981 BG : A+
Badge No :
Valid Till (Transport)
Valid Till (Non-Transport) 01-03-2021
"Authorisation to drive the following vehicle class throughout India.
Type of Vehicles : MCWG LMV NT Only
Signature of Holder
DTO - KISHANGANJ
Issued on : 02-03-2010

TRANSLINK

CashCard

BRITISH AIRWAYS
4417 1234 5678 9112
CARDMEMBER SINCE 1999
GOOD THRU 00/00
D. WALDEN
EXECUTIVE CLUB # 12345678
VISA
SIGNATURE

香港永久性居民身份證
HONG KONG PERMANENT IDENTITY CARD
李智能
LEE, Chi Nan
2621 2535 5174
樣本 SAMPLE
出生日期 Date of Birth
01-01-1968
女 F
***AZ
簽發日期 Date of Issue
(01-79)
15-09-03
C668668(E)

Mount Sinai
Mount Sinai Medical Center
Health Card
MARIA ANNA LUGO
002345345
SIEMENS

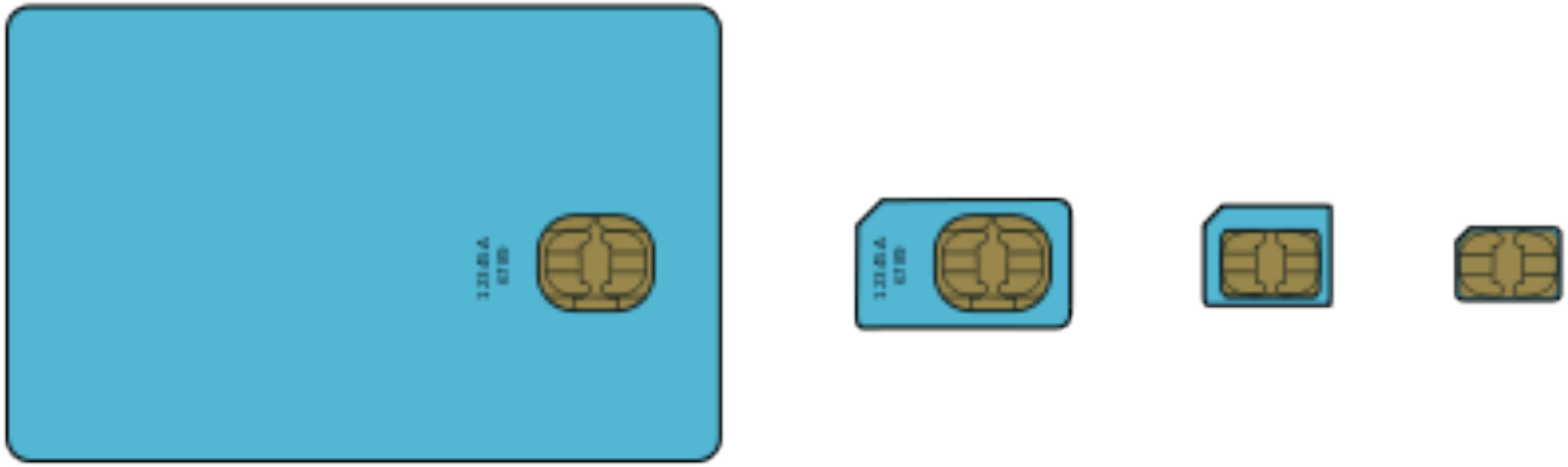
NDS
KabelBW
02 6922 5787 02

NETS
FlashPay

oyster™
Issued subject to conditions – see over

BARCLAYS
4659 0000 0000 0000
4659
VALID FROM 00/00
EXPIRES END 00/00
G TURNER
00-00-00 00000000
VISA
DEBIT

KAD PENGENALAN
MALAYSIA
MyKad
710804-06-5472
NORLELA BINTI
IBRAHIM
NO 16
JALAN ANGGERIK DORITIS 31/138
KOTA KEMUNING
40460 SHAH ALAM
SELANGOR DARUL EHSAN
WARGANEGARA
ISLAM PEREMPUAN



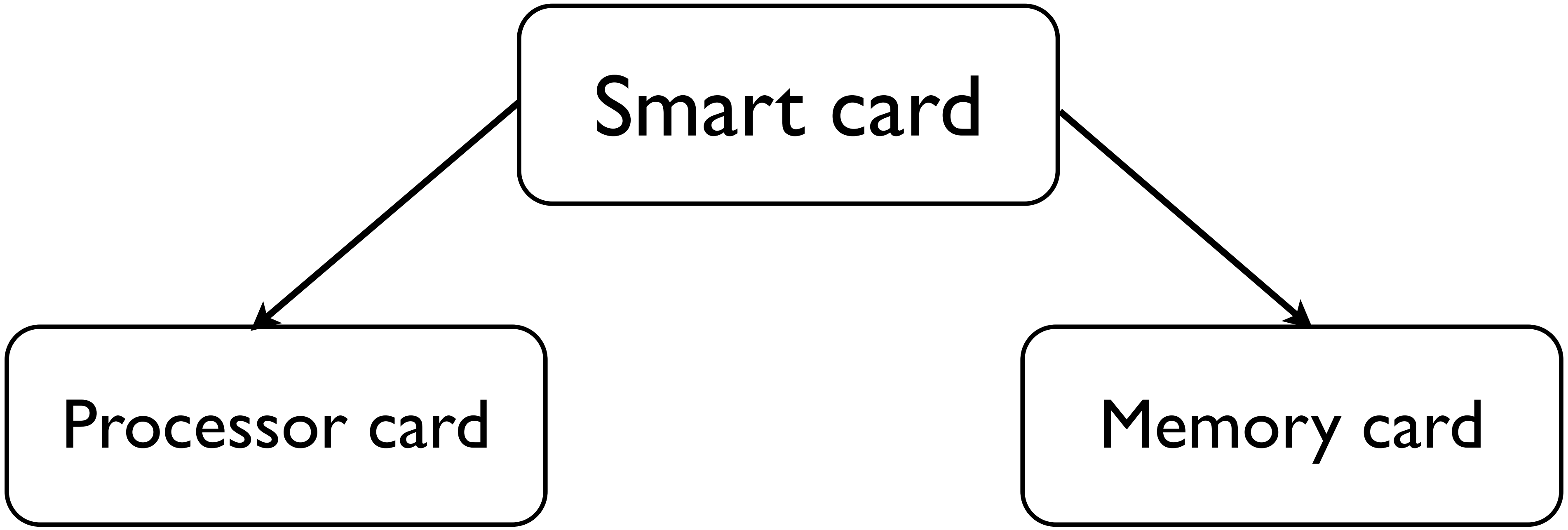
ID-1

ID-000
(mini SIM)

Mini-UICC
(micro SIM)

nano SIM

Smart cards



- Can process data on card
- More memory storage
- More secured data
- 8 - 32-bit processors
- More expensive

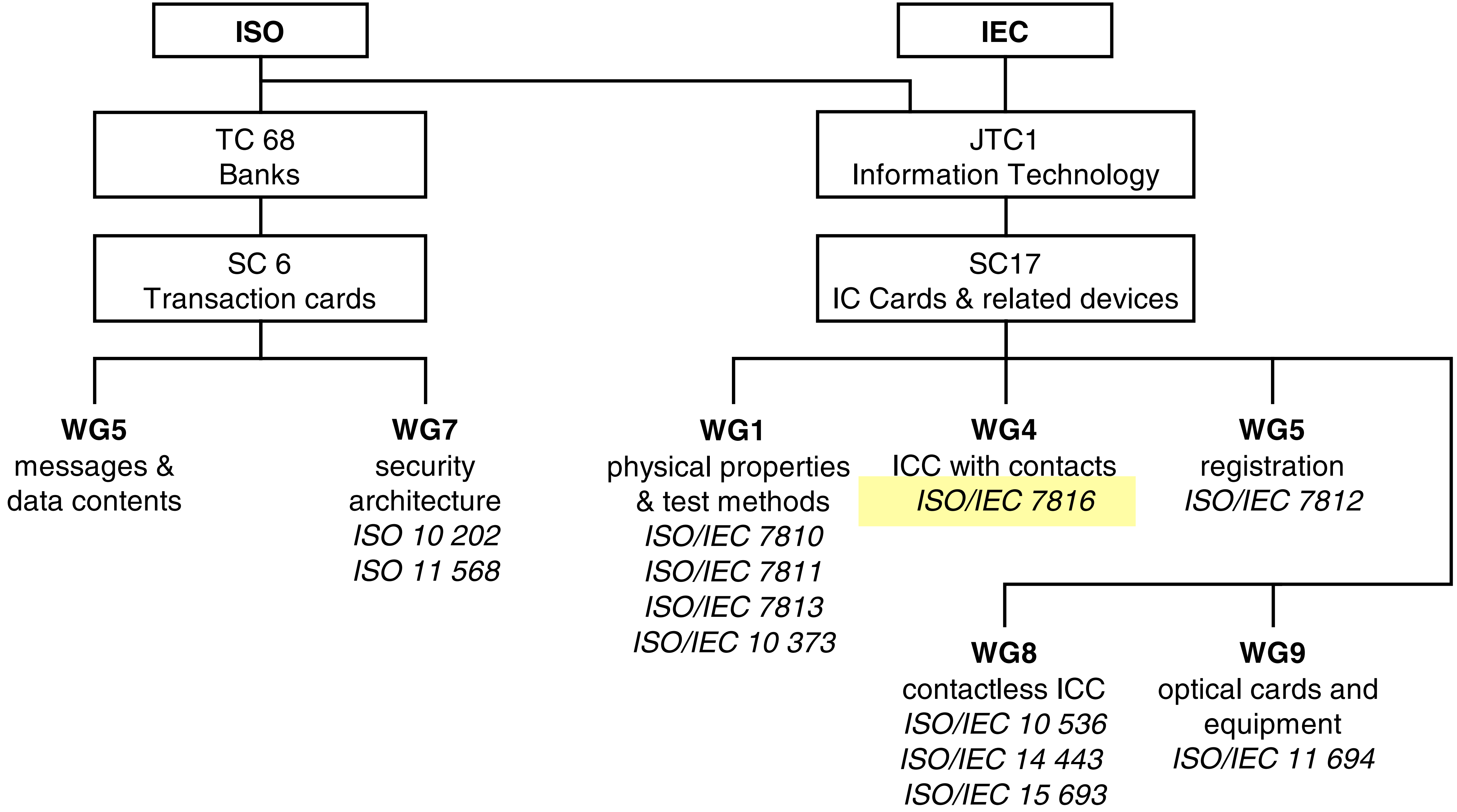
- Stores data only
- Performs fixed data manipulation
- Smaller memory storage
- Cheaper

History of smart cards

- 1968/69 - 2 German engineers Helmut Gröttrup and Jürgen Dethloff filed for patent for a chip on an ID card
- 1970 - similar patent filed by Kunitaka Arimura in Japan
- 1974 - Roland Moreno filed smart card patents in 11 countries
- 1977 - Michel Ugon from Honeywell Bull invented the first microprocessor smart card
- 1983/84 - First mass use of smart cards as telephone cards by French PTT
- 1991 - First SIM cards created by German smart card manufacturer G&D
- 1992 - smart cards used in Carte Bleue debit cards
- 1996 - EMV specification first published, version 3.1.1
- As of Q2 2012, there were 1.55 billion EMV compliant cards in use worldwide
- As end of 2011, there are about 6 billion GSM subscribers in the world

Standards

- Development and functionality of smart cards strongly driven by international standards
    - Interchangeability and interoperability very important
    - No particular vendor has dominant position



ISO

IEC

TC 68
Banks

JTC1
Information Technology

SC 6
Transaction cards

SC17
IC Cards & related devices

WG5
messages &
data contents

WG7
security
architecture
ISO 10 202
ISO 11 568

WG1
physical properties
& test methods
ISO/IEC 7810
ISO/IEC 7811
ISO/IEC 7813
ISO/IEC 10 373

WG4
ICC with contacts
ISO/IEC 7816

WG5
registration
ISO/IEC 7812

WG8
contactless ICC
ISO/IEC 10 536
ISO/IEC 14 443
ISO/IEC 15 693

WG9
optical cards and
equipment
ISO/IEC 11 694

ISO/IEC 7816

- 7816-1
  - Physical characteristics of a card
  - For card manufacturers
- 7816-2
  - Dimension, location, functions of contacts
  - For card manufacturers
- 7816-3
  - Electronic signals, transmission protocols
  - For reader manufacturers
- 7816-4
  - Commands, messages, responses, files and data
  - For application developers
- 7816-5
  - Registration for application identifiers (AID)
- 7816-6
  - Inter industry data elements

Smart card OS

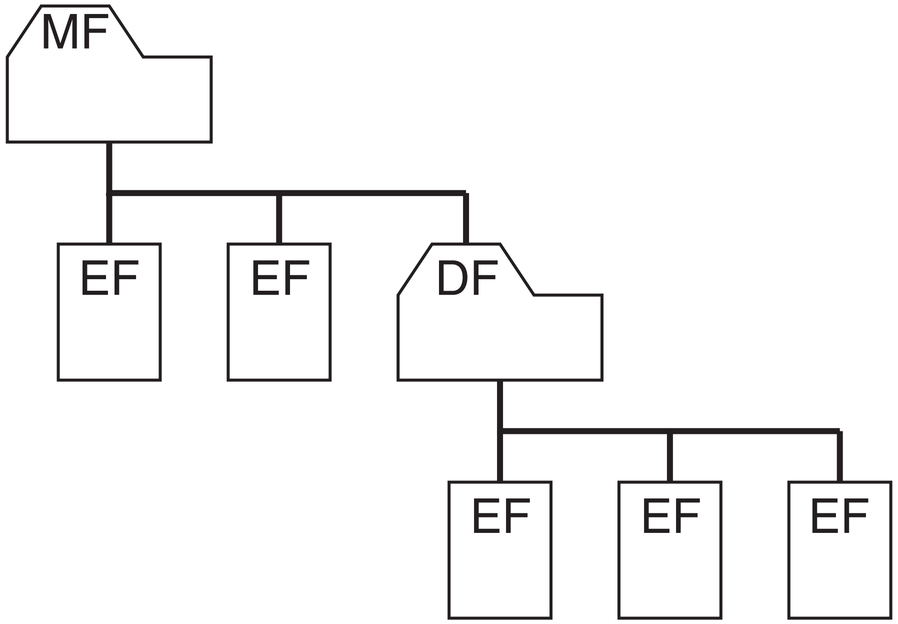
- Stored in the ROM of the microcontroller in unalterable form
- Classified into:
  - Native operating systems
    - OS and applications execute in machine language
  - Interpreter-based operating systems
    - OS in machine language, applications can be written in another language
    - Most popular include Java Card, MultOS and BasicCard

Application types

- Memory-based applications
  - The terminal accesses the entire memory for read and write operations
  - Can require certain conditions such as a PIN verification
  - Limited in terms of their complexity, typical use include transit cards
- File-based applications
  - Require processor cards and a smart card OS
  - A set of data files (EFs) located in a directory file (DF)
  - The smart card OS provides a large number of commands for data access, authentication and other operations
- Code-based applications
  - Also use data files, but includes application-specific program code that can be executed in the smart card
  - Examples include Java Card, BasicCard, Multos

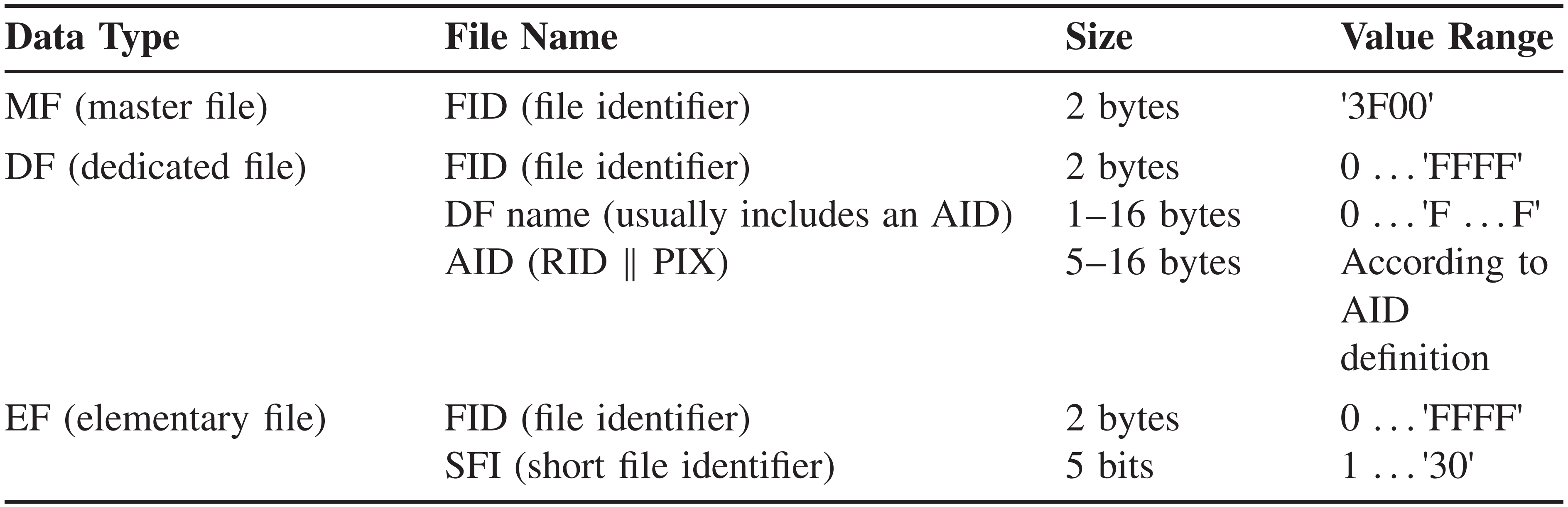
File management

- Smart card file structures based on a tree structure with a root directory called MF (master file)
- The directories of a smart card are called DFs (dedicated files)
- The actual application data and operating system data are stored in EFs (elementary file)



Identifying files

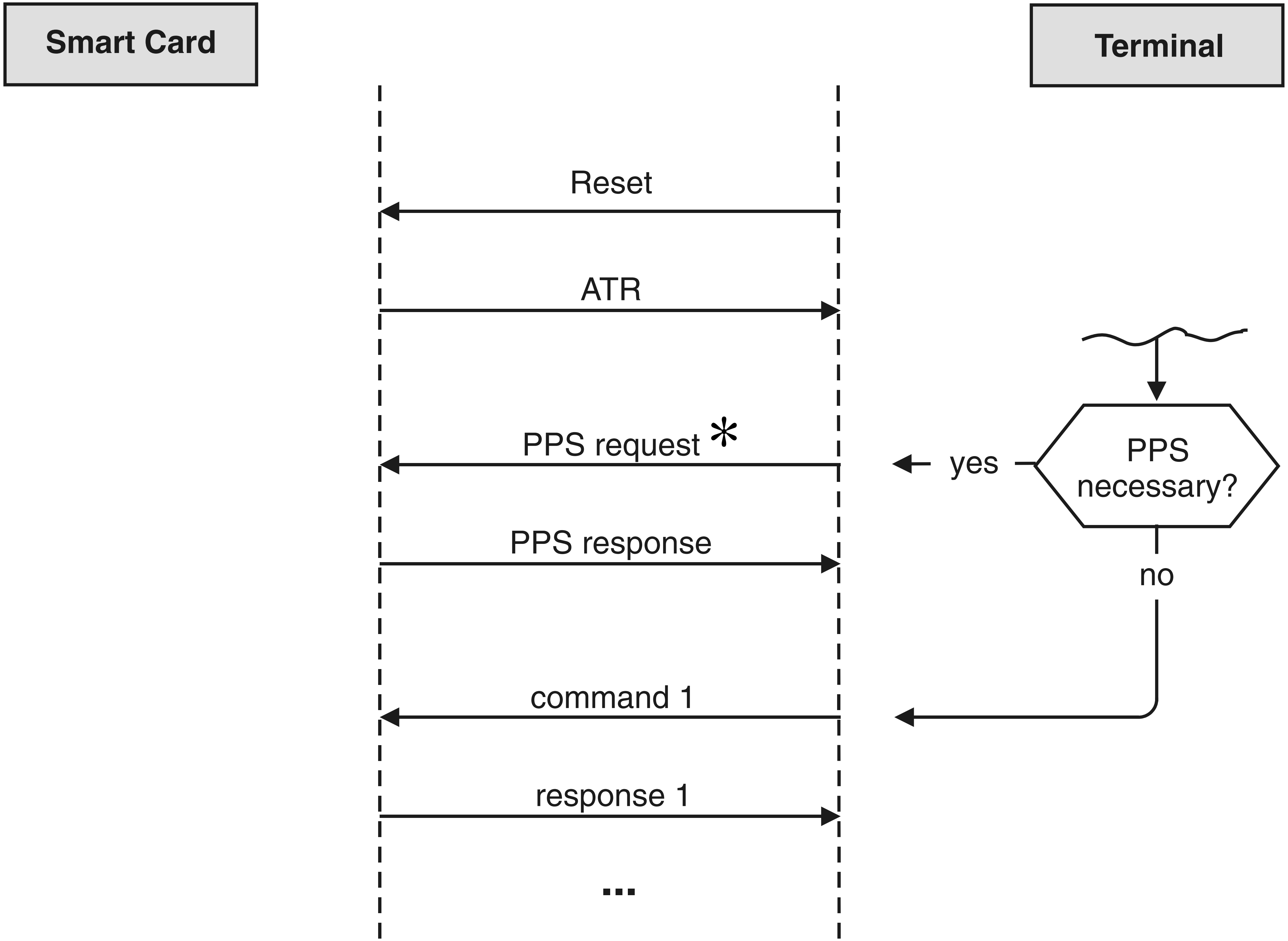
- Standard filename consists of a 2-byte data element called the FID (file identifier). The FID of the MF is '3F00'
- Each DF has a DF name in addition to its FID and includes an AID (application identifier)
  - The AID consists of an RID (registered application provider identifier) and a PIX (proprietary application identifier extension). RIDs can be registered officially to ensure that they are unique throughout the world.
- Each EF has has an SFI (short file identifier) which can be provided as a parameter of a read or write command to select the EF directly



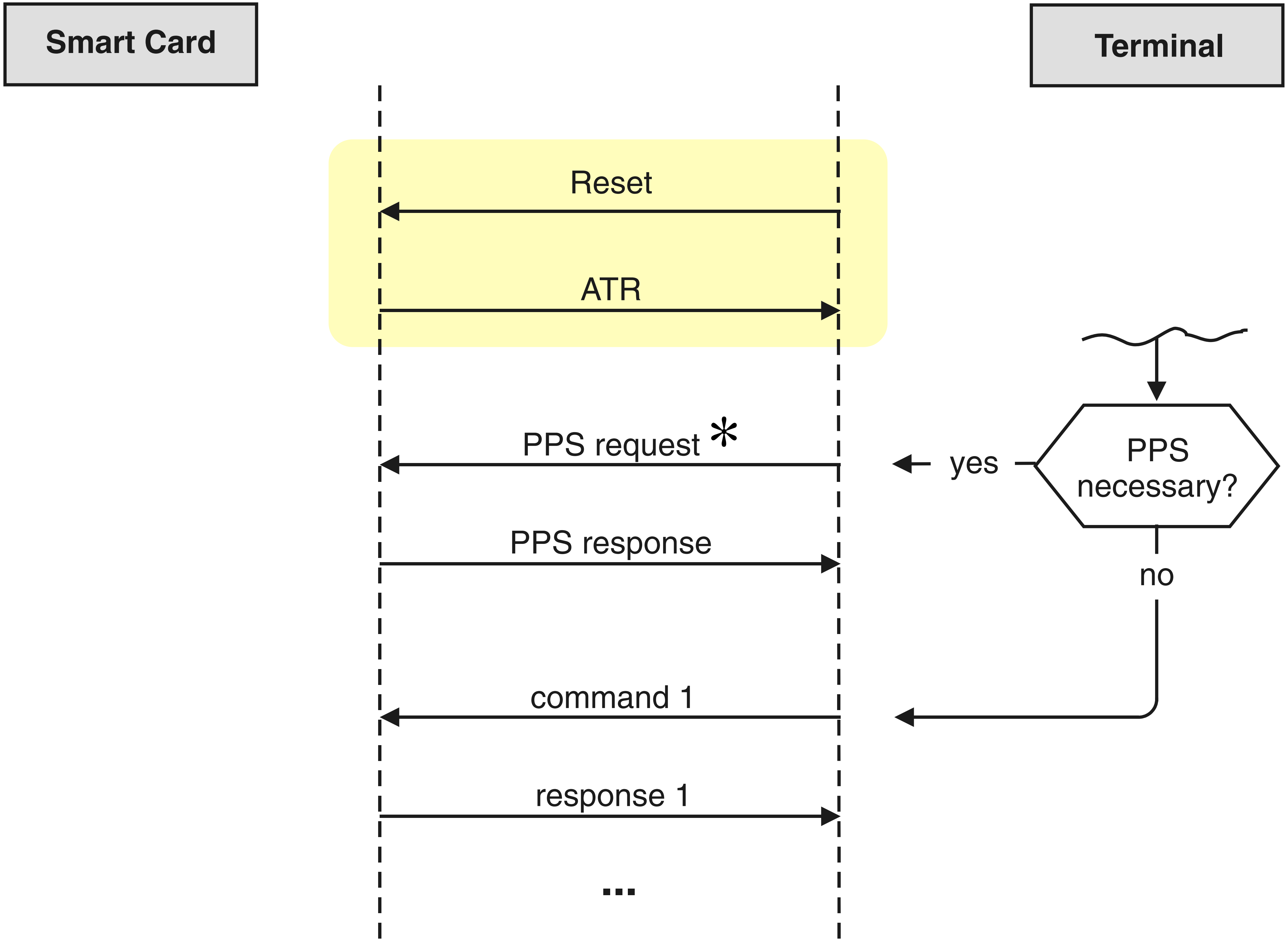
Data Type	File Name	Size	Value Range
MF (master file)	FID (file identifier)	2 bytes	'3F00'
DF (dedicated file)	FID (file identifier)	2 bytes	0 . . . 'FFFF'
	DF name (usually includes an AID)	1–16 bytes	0 . . . 'F . . . F'
	AID (RID ‖ PIX)	5–16 bytes	According to AID definition
EF (elementary file)	FID (file identifier)	2 bytes	0 . . . 'FFFF'
	SFI (short file identifier)	5 bits	1 . . . '30'

Interfacing with smart cards

- Communication with contact smart cards takes place via a half-duplex, bit-serial link
- This means that only one of the communicating parties can transmit at any given time
- To prevent collisions, it is necessary to fix which party initiates communication
- For smart cards, the terminal always initiates communications, which means it is the master and the smart card is the slave
- This means the smart card transmits data only in response to a request from the terminal.
- This master–slave principle pervades all communications with smart cards



*Protocol Parameter Selection



Smart Card

Terminal

Reset

ATR

PPS request *

yes

PPS necessary?

PPS response

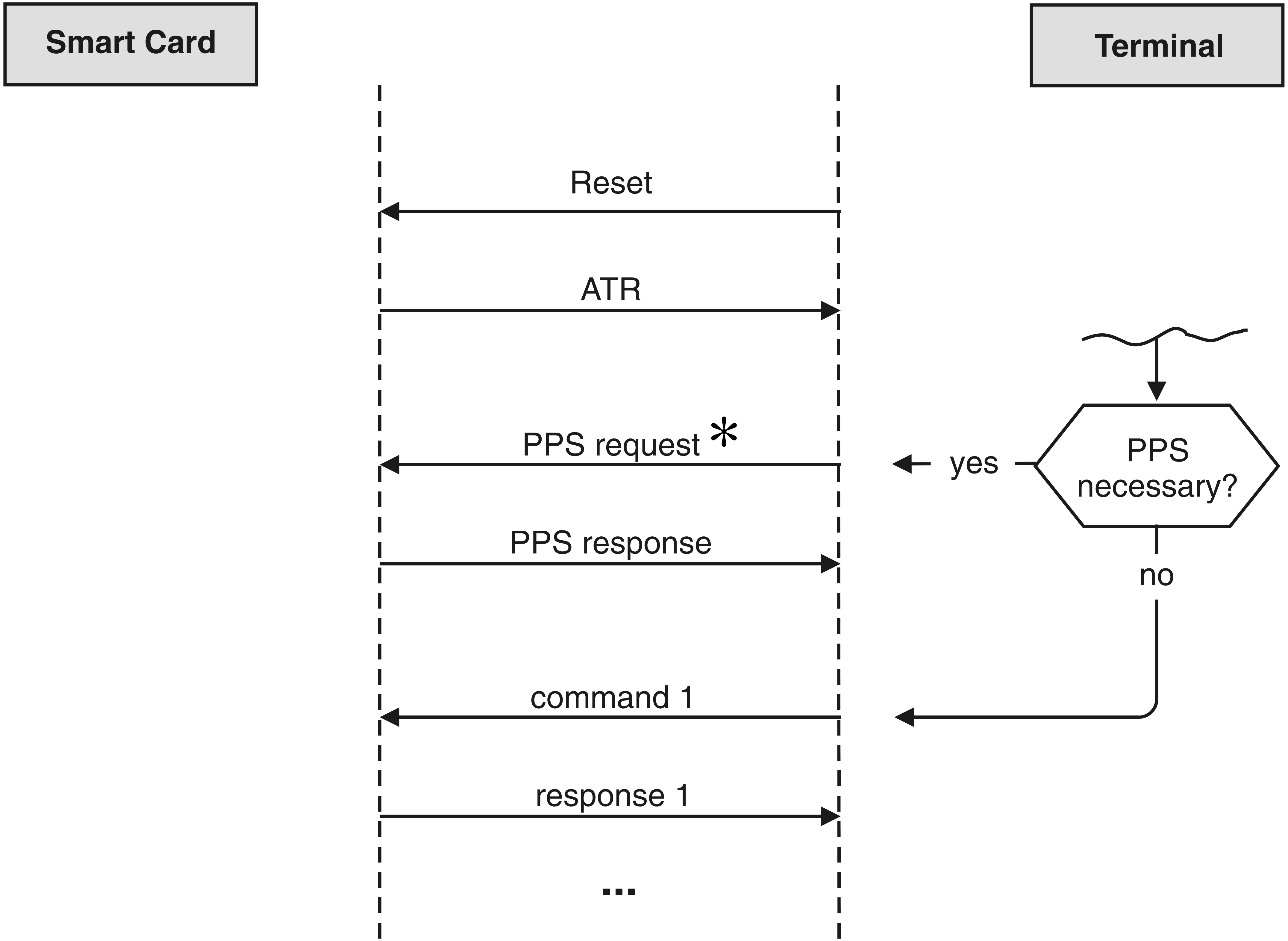
no

command 1

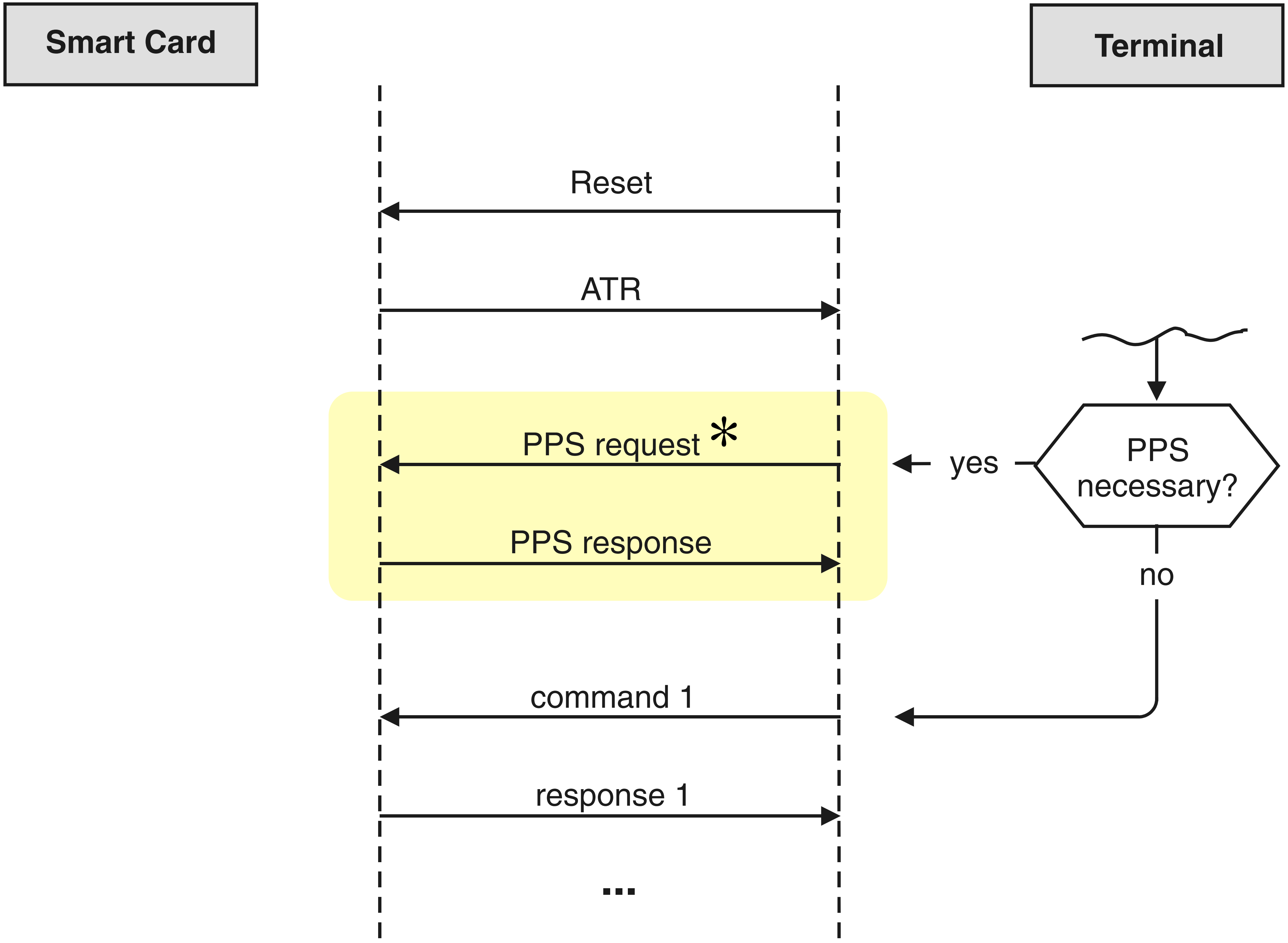
response 1

...

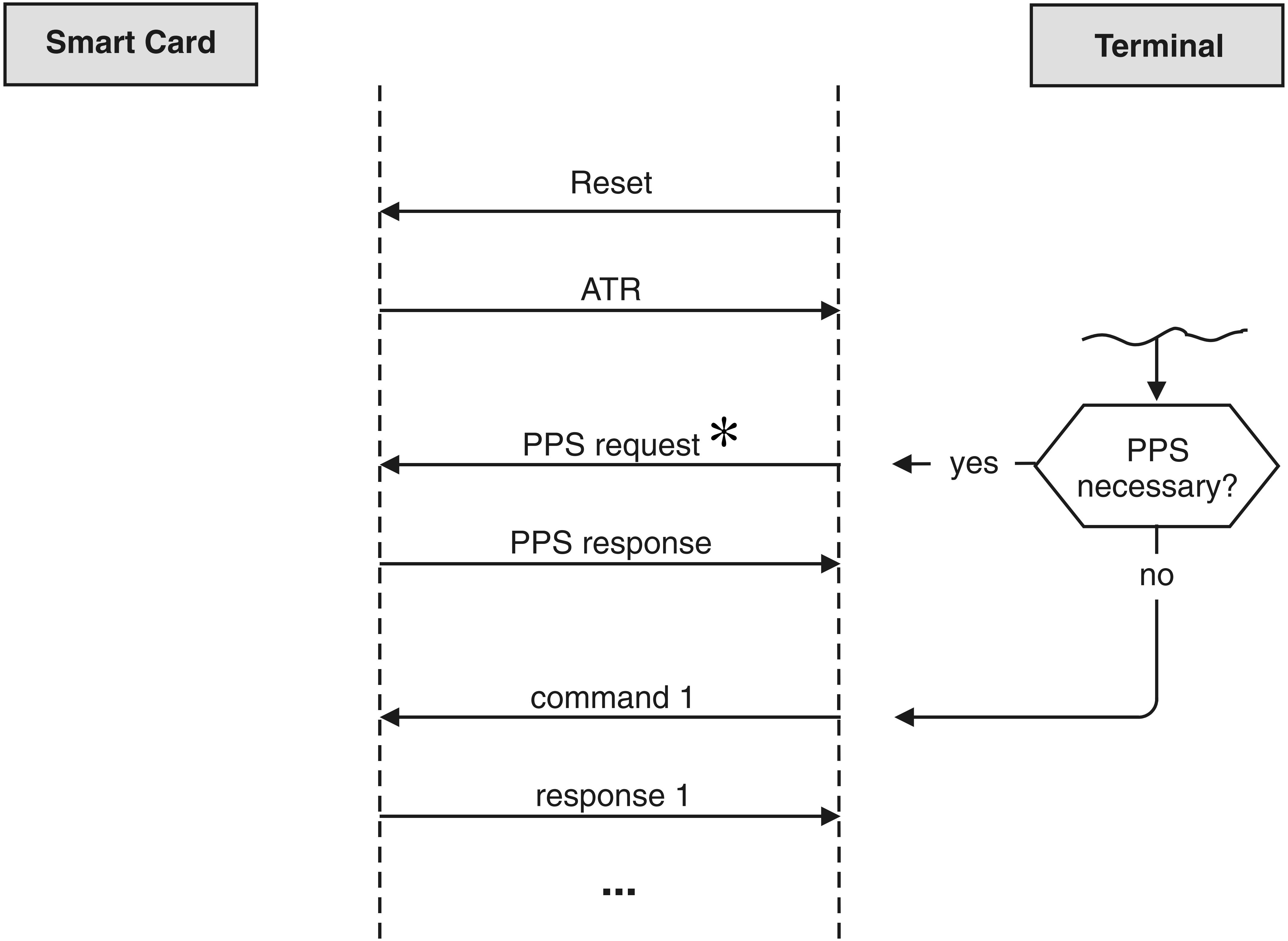
*Protocol Parameter Selection



*Protocol Parameter Selection



*Protocol Parameter Selection



Smart Card

Terminal

Reset

ATR

PPS request *

PPS response

command 1

response 1

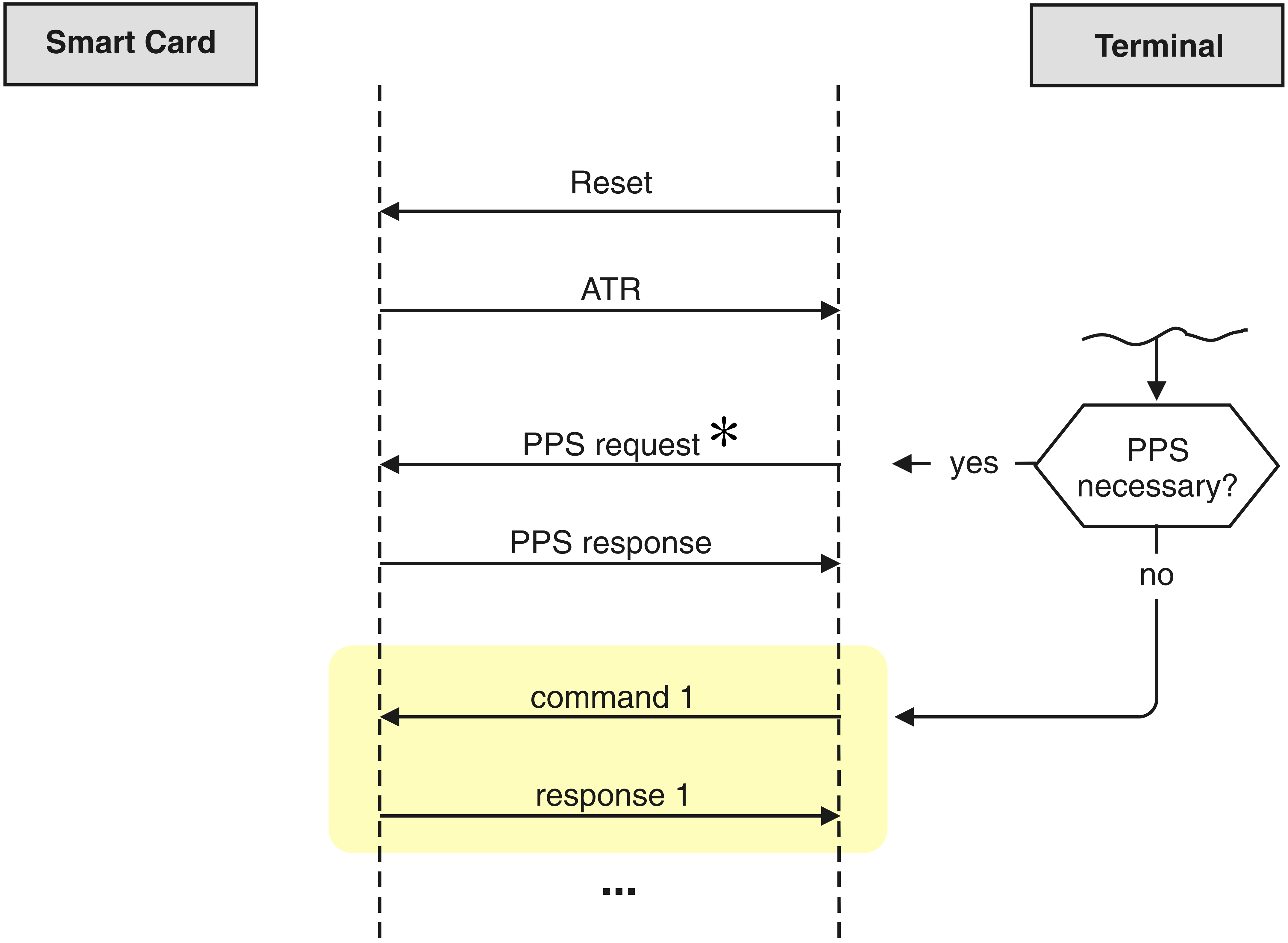
...

yes

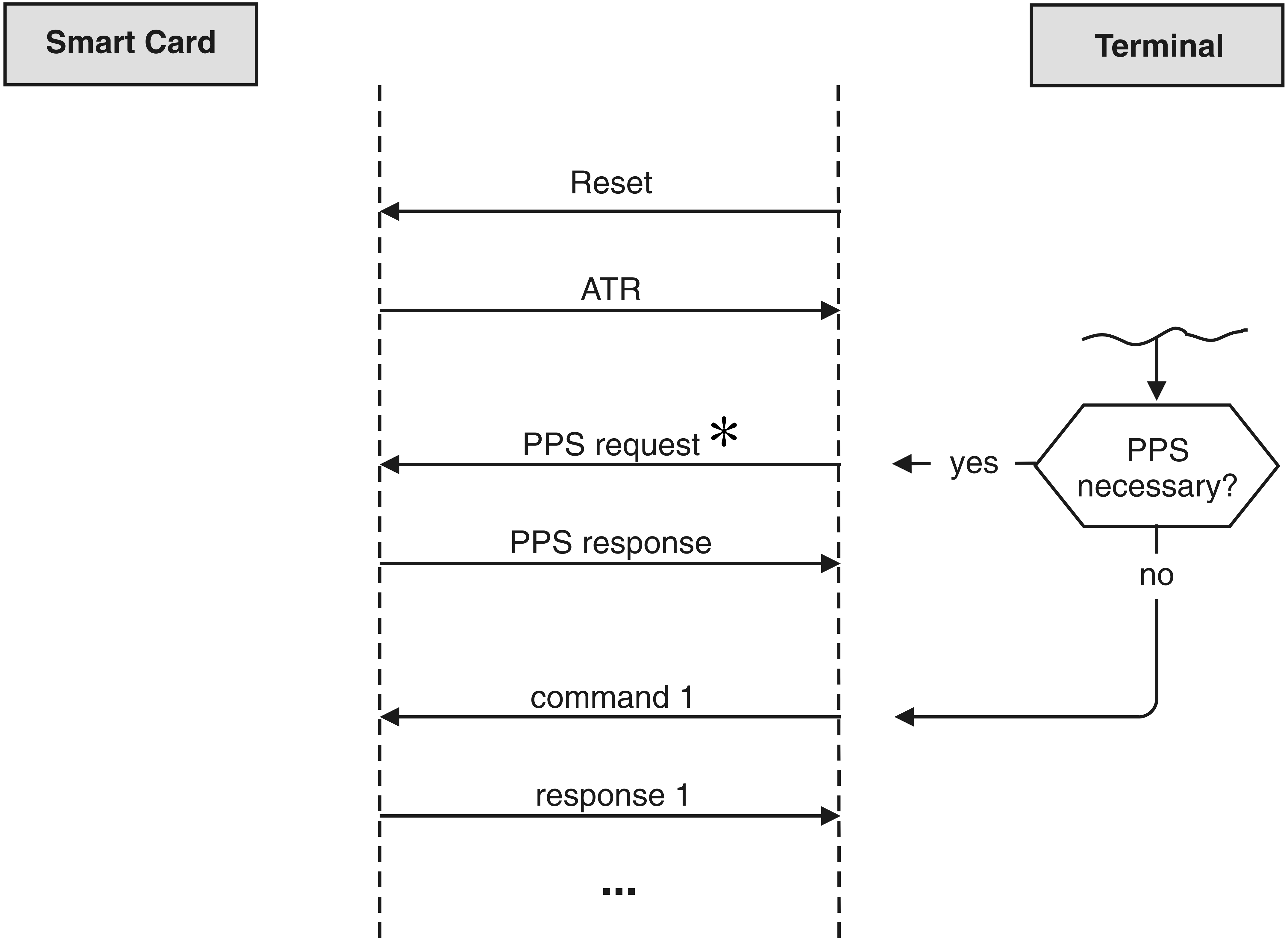
PPS necessary?

no

*Protocol Parameter Selection



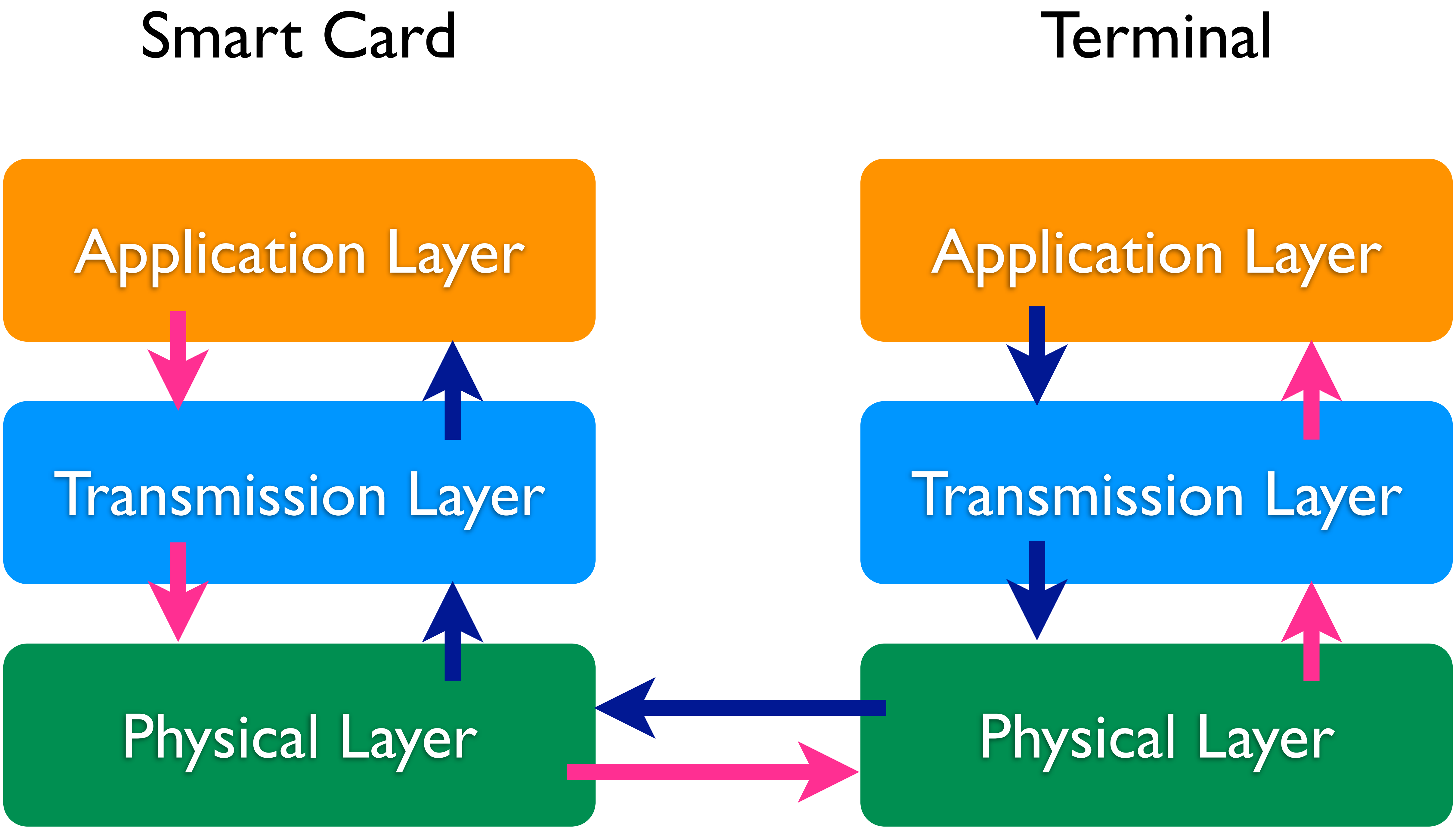
*Protocol Parameter Selection



*Protocol Parameter Selection

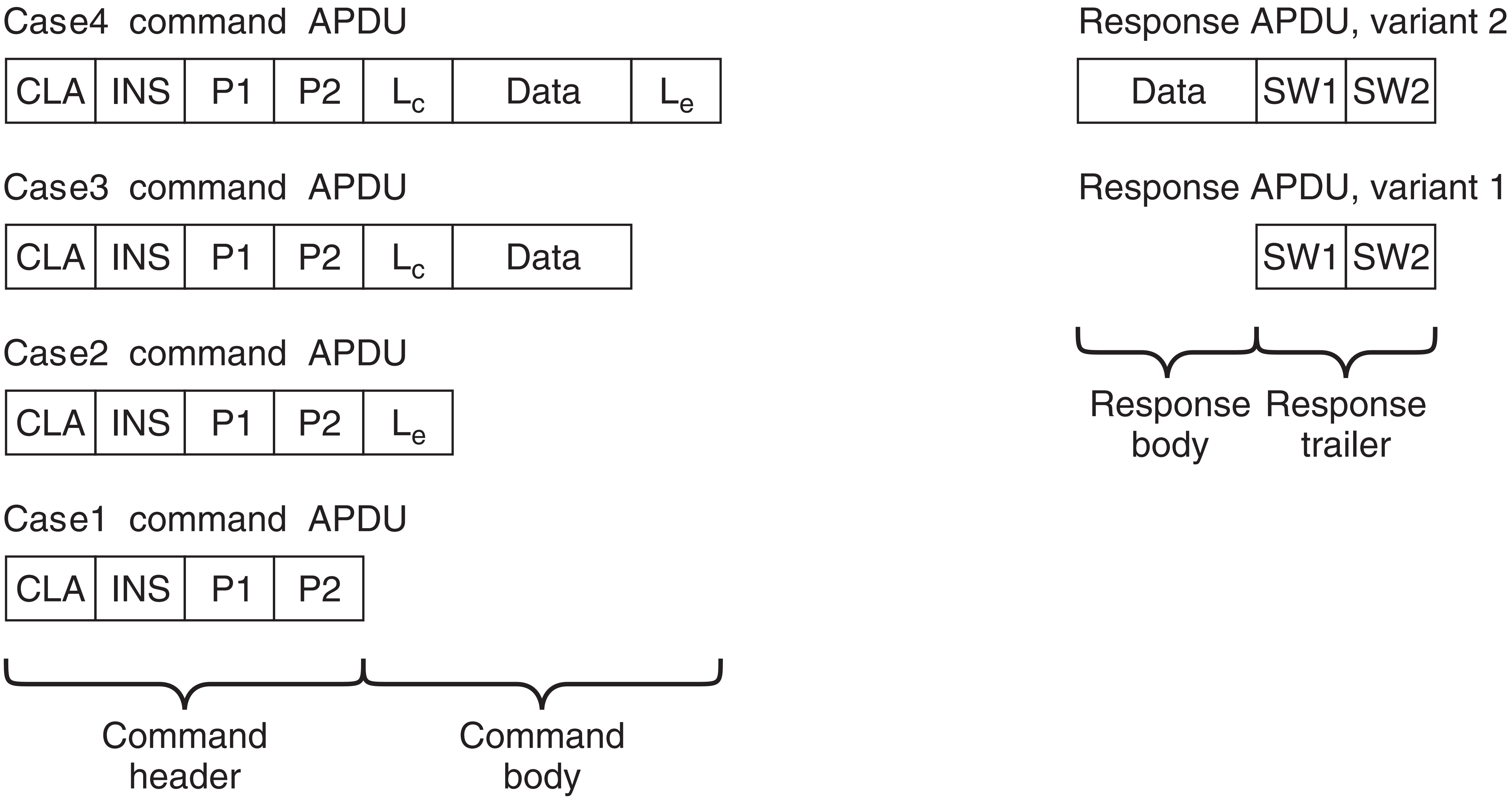
Communicating with smart cards

- The T=0 transmission protocol
  - The oldest and most widely used protocol for smart cards including SIM cards
  - Byte-oriented transmission protocol with relatively poor layer separation so Case 4 commands are not possible
  - Terminal must use the GET RESPONSE command to retrieve data to be provided
- The T=0 transmission protocol
  - Block-oriented T=1 protocol has distinct layer separation, so all four cases of command APDUs can be used
  - Has a significantly more complicated structure than T=0, but it is also more robust
  - Often used with payment cards and ID cards


Smart Card
Terminal
Application Layer
Application Layer
Transmission Layer
Transmission Layer
Physical Layer
Physical Layer

Message structure

- Applications protocol data units (APDUs) are used to exchange all data that passes between the smart card and the terminal
- Holds a complete command to the card or a complete response from the card
- APDU commands sent to card are called command APDUs
- APDU response sent to terminal are called response APDUs



Case4 command APDU

CLA	INS	P1	P2	L_c	Data	L_e

Case3 command APDU

CLA	INS	P1	P2	L_c	Data

Case2 command APDU

CLA	INS	P1	P2	L_e

Case1 command APDU

CLA	INS	P1	P2

Command header

Command body

Response APDU, variant 2

Data	SW1	SW2

Response APDU, variant 1

SW1	SW2

Response body

Response trailer

Command APDUs

- CLA - class byte
- INS - instruction byte
- P1, P2 - parameter bytes
- Lc - length of command data
- Le - length of expected response data
- Example command APDUs
  - SELECT FILE
  - READ RECORD
  - GET RESPONSE

Response APDUs

- SW1, SW2 - status word 1 and 2
- Example SW1, SW2:
- Normal response
    - 90 00 - Ok
    - 61 xx - Has more data, length of data is SW2
- Warning response
    - 62 81 - return data corrupted
    - 63 00 - authentication failed
- Error response
    - 68 00 - request not supported
    - 6A 82 - File not found

PC communications

- PC/SC (Personal Computer/Smart Card)
  - De facto specification for smart card integration with PCs
  - Default in Windows, ported to Linux with PC/SC Lite, forked version in OS X
- CT-API (Card Terminal API)
  - Alternative, older specification
  - Single application, single user
- OpenCT
  - Alternative open source driver
  - Not standard

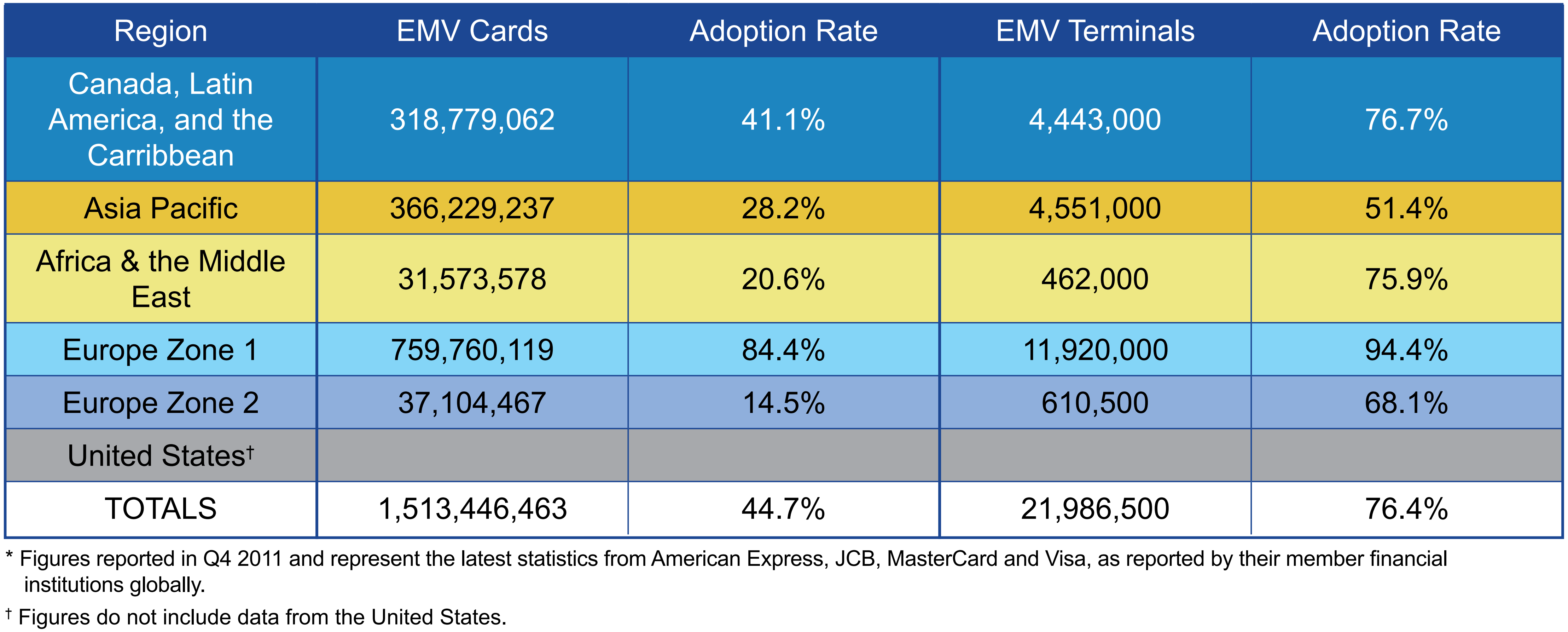
EMV

- EMV (Europay, Mastercard, Visa) is a global standard for credit and debit payment cards based on chip card technology
- First published 1996 version 3.1.1
- Current version 4.3 November 2011
- JCB joined 2004, American Express joined 2009
- Controlled by EMVCo, with 25% shareholdings amongst Visa, Mastercard, American Express and JCB
- Defines interaction at physical, electrical, data and application layers between smart card and terminals for financial transactions

EMV

- Standards based on ISO/IEC 7816 for contact cards, ISO/IEC 14443 for contactless cards
- As of Q2 2012, there were 1.5 billion EMV compliant cards in use worldwide
- Main purposes for increased security (reducing fraud) and finer control of offline transactions
- Multiple implementations of EMV -
  - VSDC - Visa
  - M/Chip - Mastercard
  - AEIPS - American Express
  - J Smart - JCB
  - D-PAS - Discover/Diners Club International

EMV Adoption



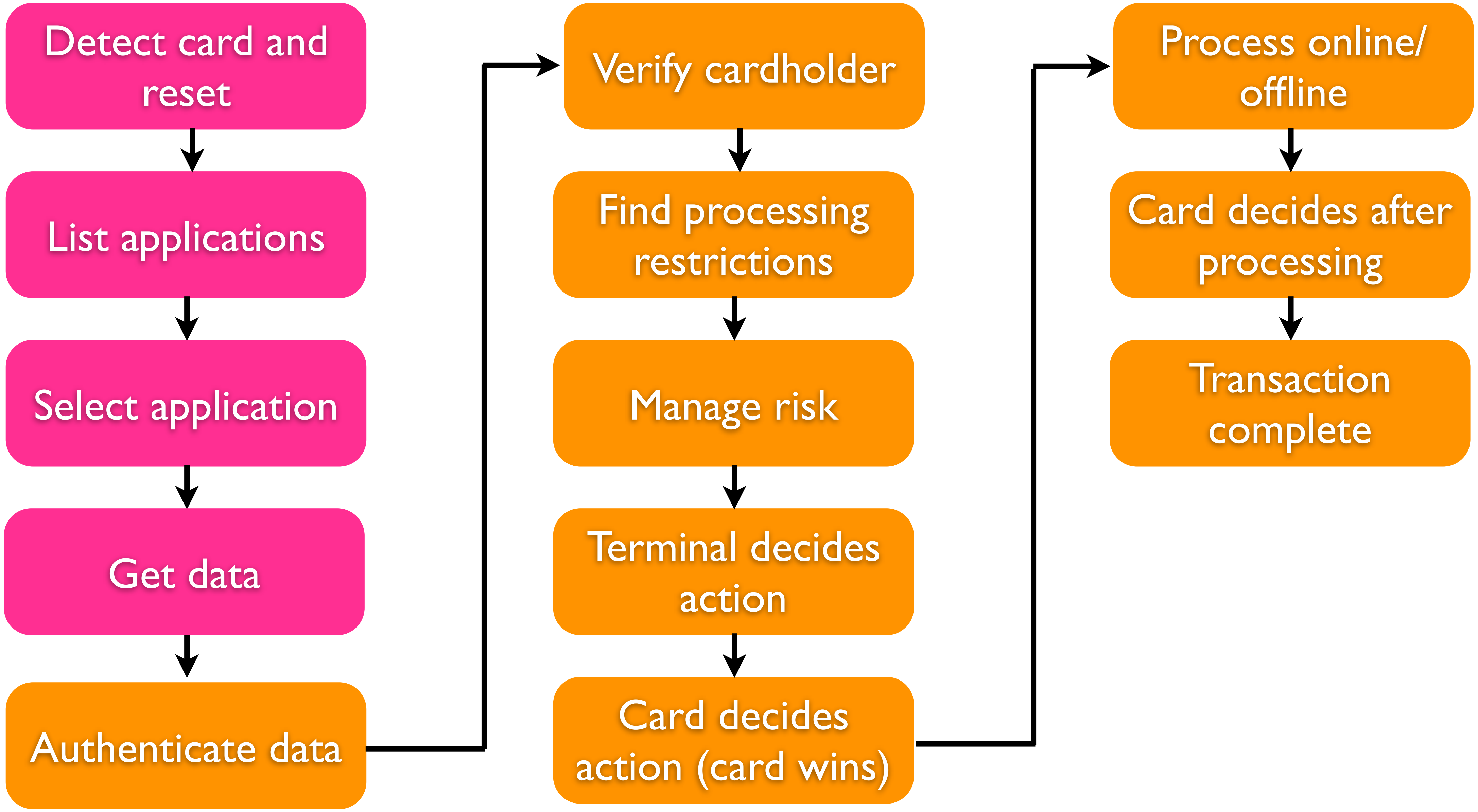
Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America, and the Carribbean	318,779,062	41.1%	4,443,000	76.7%
Asia Pacific	366,229,237	28.2%	4,551,000	51.4%
Africa & the Middle East	31,573,578	20.6%	462,000	75.9%
Europe Zone 1	759,760,119	84.4%	11,920,000	94.4%
Europe Zone 2	37,104,467	14.5%	610,500	68.1%
United States[†]				
TOTALS	1,513,446,463	44.7%	21,986,500	76.4%

* Figures reported in Q4 2011 and represent the latest statistics from American Express, JCB, MasterCard and Visa, as reported by their member financial institutions globally.

[†] Figures do not include data from the United States.

- Figures as of end 2011
- Does not include US (slow adoption - cost, weak justification, large number of banks)
- Liability shift to acquirers over next 3 (Visa) - 5 (Mastercard) years in US

(typical) EMV flow



Detect card and reset

List applications

Select application

Get data

Authenticate data

Verify cardholder

Find processing restrictions

Manage risk

Terminal decides action

Card decides action (card wins)

Process online/ offline

Card decides after processing

Transaction complete

TLV

- Tag-Length-Value
- Tag - 1 or 2 bytes
- Length - length of the value (in bytes)
- Value - actual data
- Can be nested or in sequence

Let's dive in.

Detect card and reset

- Insert card
- Wait for ATR
- Show ATR

Payment System Environment

- PSE is a DDF with the name 1.PAY.SYS.DDF01
- Contains one or more EMV applications
- Doesn't always exist

List applications

- SELECT the PSE
- If PSE doesn't exist, go through list of AIDs that the terminal supports to get the list of EMV applications
- If PSE exists, use GET_RESPONSE to get the PSE FCI
- PSE FCI has the SFI to the PSE record
- Use GET_RECORD with SFI to get the PSE record
- PSE record has ADFs of the EMV applications

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x				SFI
					1	0	0	P1 is a record number

Select application

- ADF represents 1 EMV application
- SELECT the ADF to get the ADF FCI
- ADF FCI has information on application including the PDOL (Processing Options Data Object List)
    - PDOL tells the terminal what the card needs
    - PDOL doesn't always exist, if there is no PDOL use 83 00
- use GET_PROCESSING_OPTIONS with the PDOL to initiate the EMV transaction

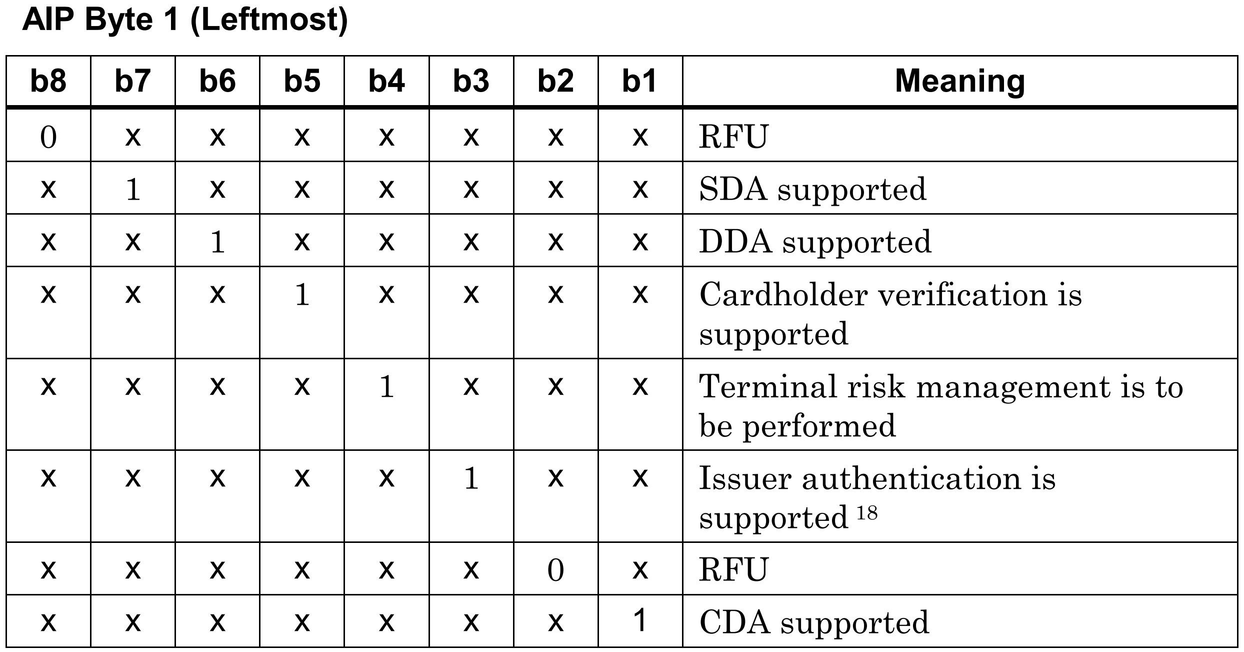
Get data from card

- GPO returns the AIP (Application Interchange Profile) and AFL (Application File Locator)
- AIP tells the terminal which features are supported
- AFL tells the terminal while files and records can be read

AIP

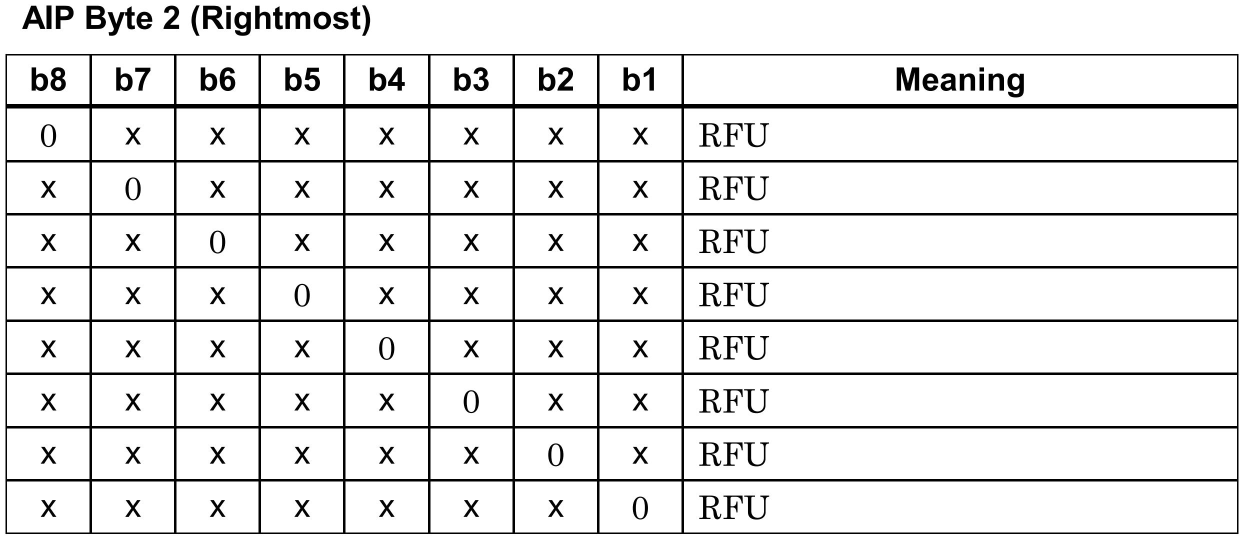
AIP tells the terminal:

- What features are supported by the application
- Whether terminal risk management should be performed



AIP Byte 1 (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	RFU
x	1	x	x	x	x	x	x	SDA supported
x	x	1	x	x	x	x	x	DDA supported
x	x	x	1	x	x	x	x	Cardholder verification is supported
x	x	x	x	1	x	x	x	Terminal risk management is to be performed
x	x	x	x	x	1	x	x	Issuer authentication is supported [18]
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	1	CDA supported



AIP Byte 2 (Rightmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	RFU
x	0	x	x	x	x	x	x	RFU
x	x	0	x	x	x	x	x	RFU
x	x	x	0	x	x	x	x	RFU
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

That’s it folks
(for now)