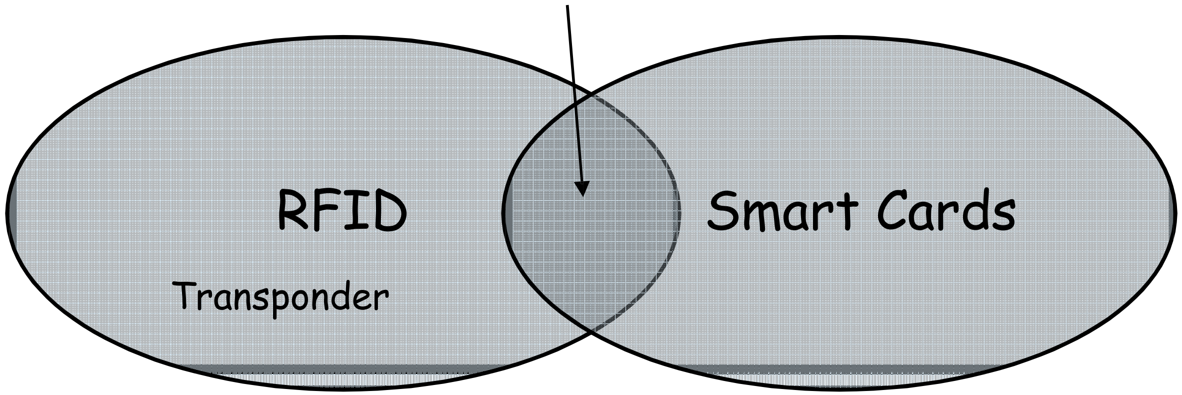
RFID, Smart card systems and authentication

CEN 464 – Cyber Security
Assoc.Prof.Dr. Fatih ABUT

RFID (Radio Frequency Identification)

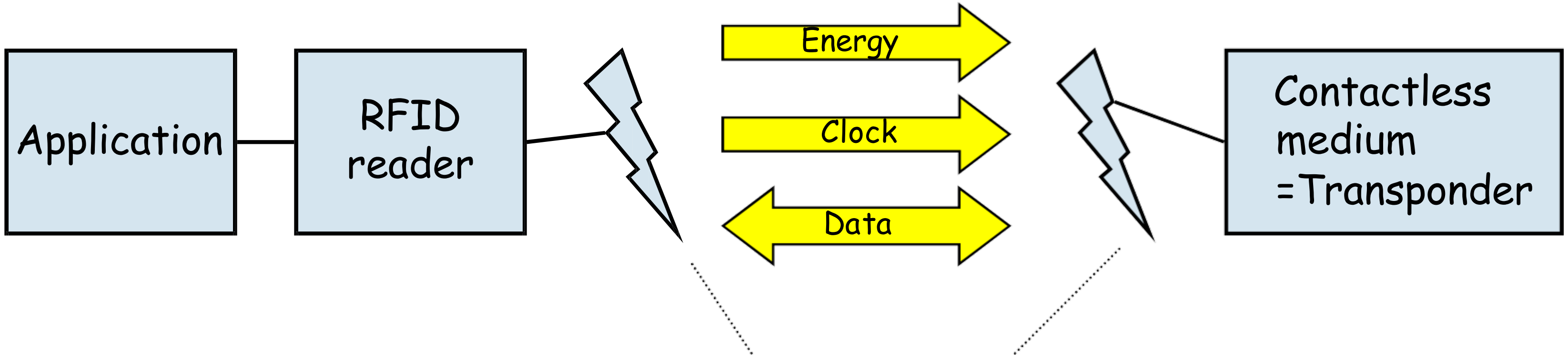
contactless smart cards



RFID

Transponder

Smart Cards



Application

RFID reader

Energy

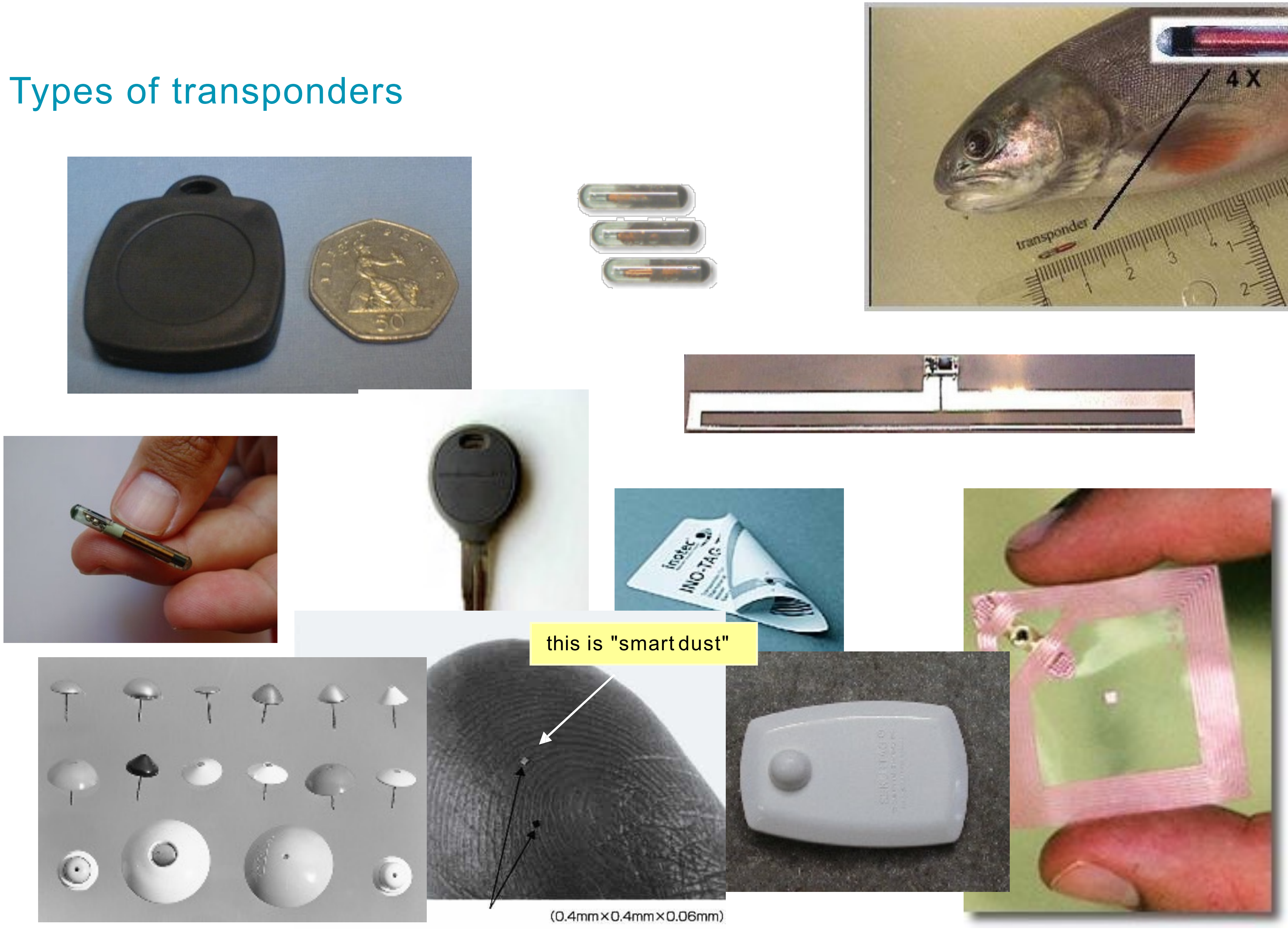
Clock

Data

Contactless medium =Transponder

coupling element

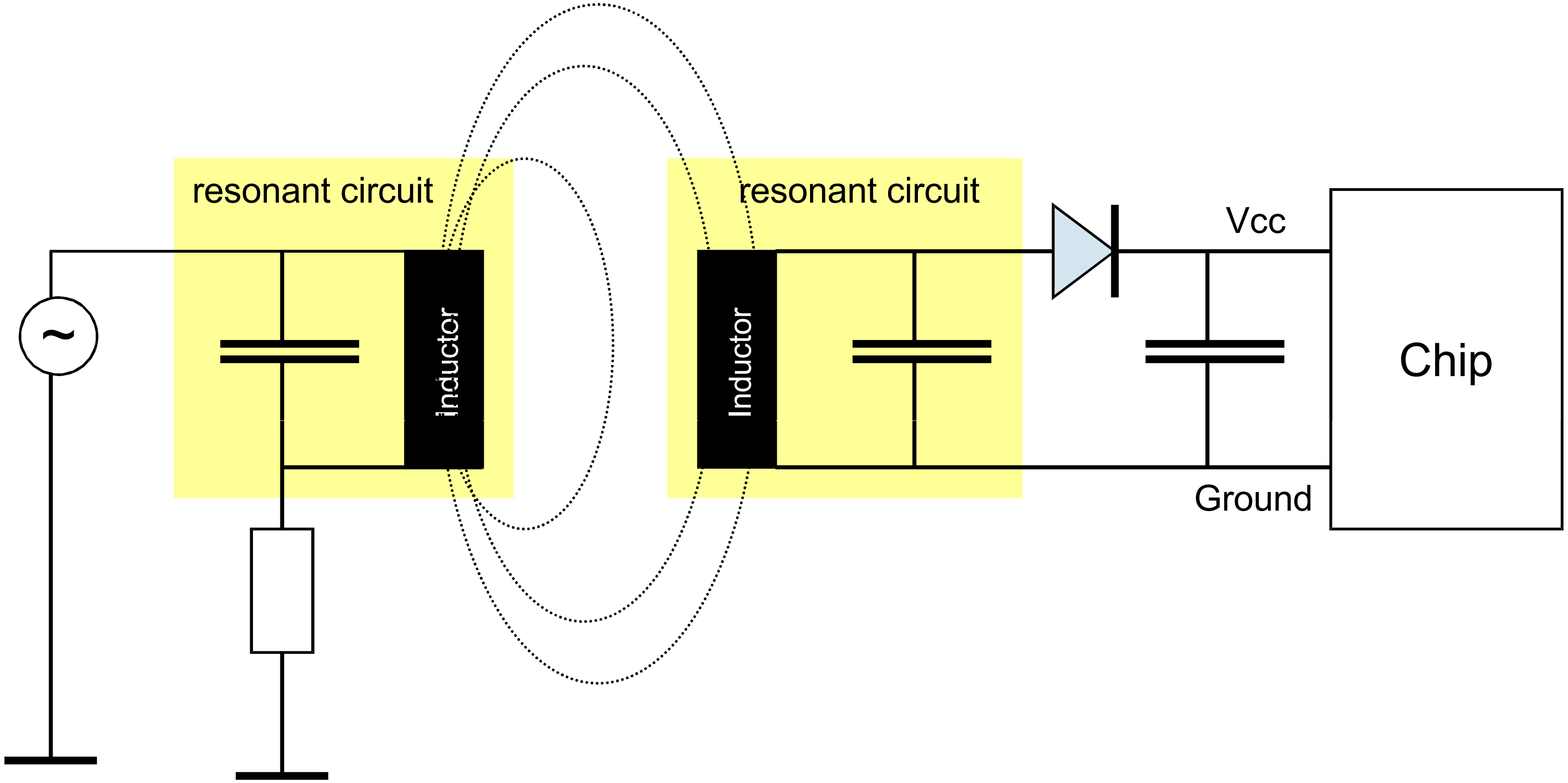
Types of transponders



this is "smart dust"

(0.4mm×0.4mm×0.06mm)

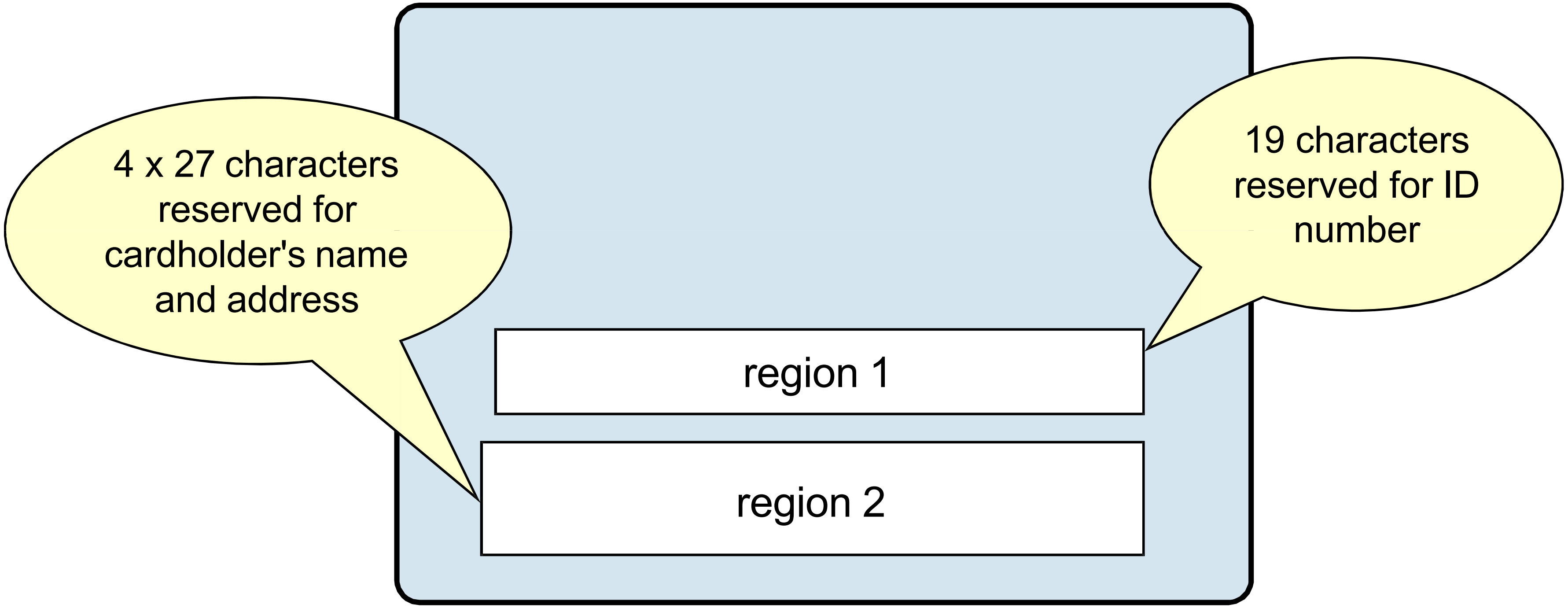
Inductively coupled transponder



Reader

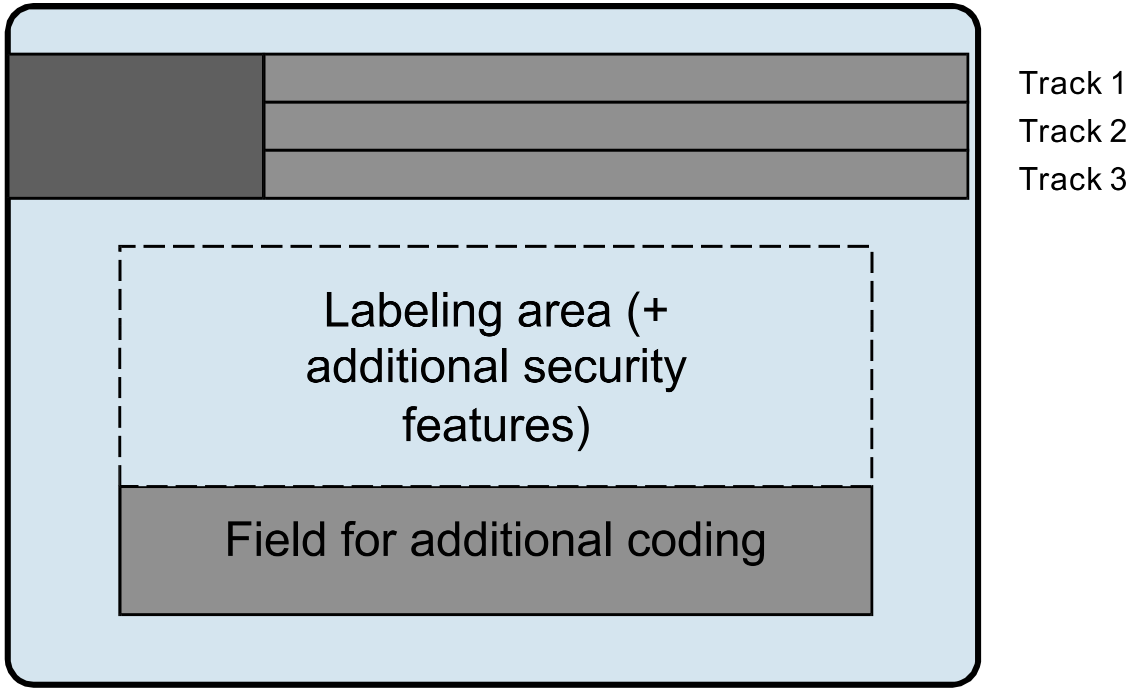
Transponder

Card Types: Embossed Cards



4 x 27 characters reserved for cardholder's name and address
19 characters reserved for ID number
region 1
region 2

Card Types: Swipe Card


Track 1
Track 2
Track 3
Labeling area (+ additional security features)
Field for additional coding

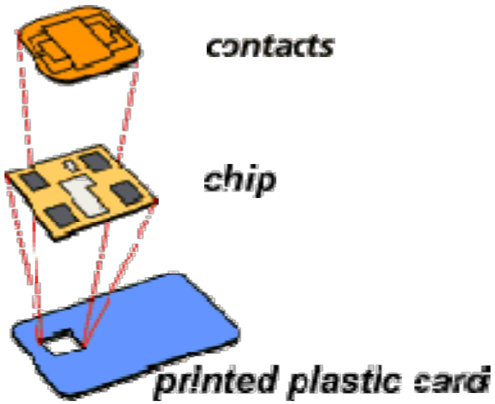
What is a Smart Card ?

Definition

A smart card is a (mostly) credit card-sized device embedded with

- either a memory chip or
- a memory chip and a microprocessor.

Think of microprocessor smart card as a tiny, portable database and computer that you can carry in your pocket.



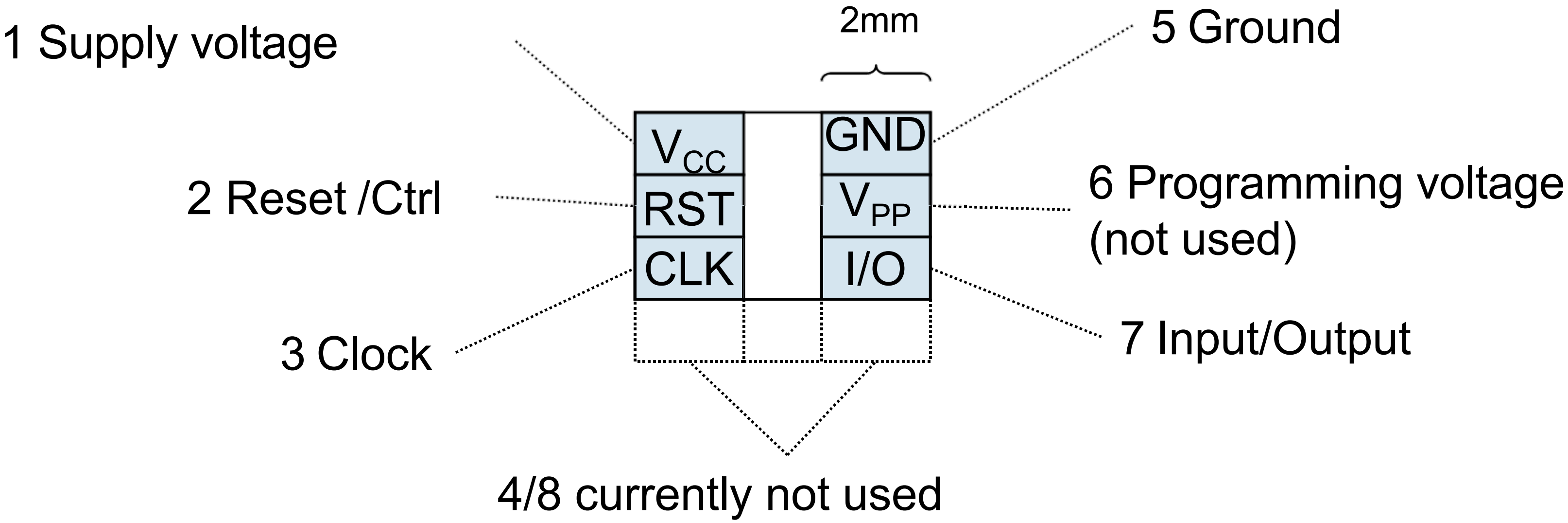
25 March 1974:

Roland Moreno, a French journalist, filed the first patent for the Smart Card

Types of smart card storage

- ROM
- PROM
- EPROM
- EEPROM
- Flash-EEPROM
- FeRAM
- RAM

Contact fields of a chip card (ISO 7816-2)



1 Supply voltage

2 Reset /Ctrl

3 Clock

2mm

5 Ground

6 Programming voltage
(not used)

7 Input/Output

V_{CC}

RST

CLK

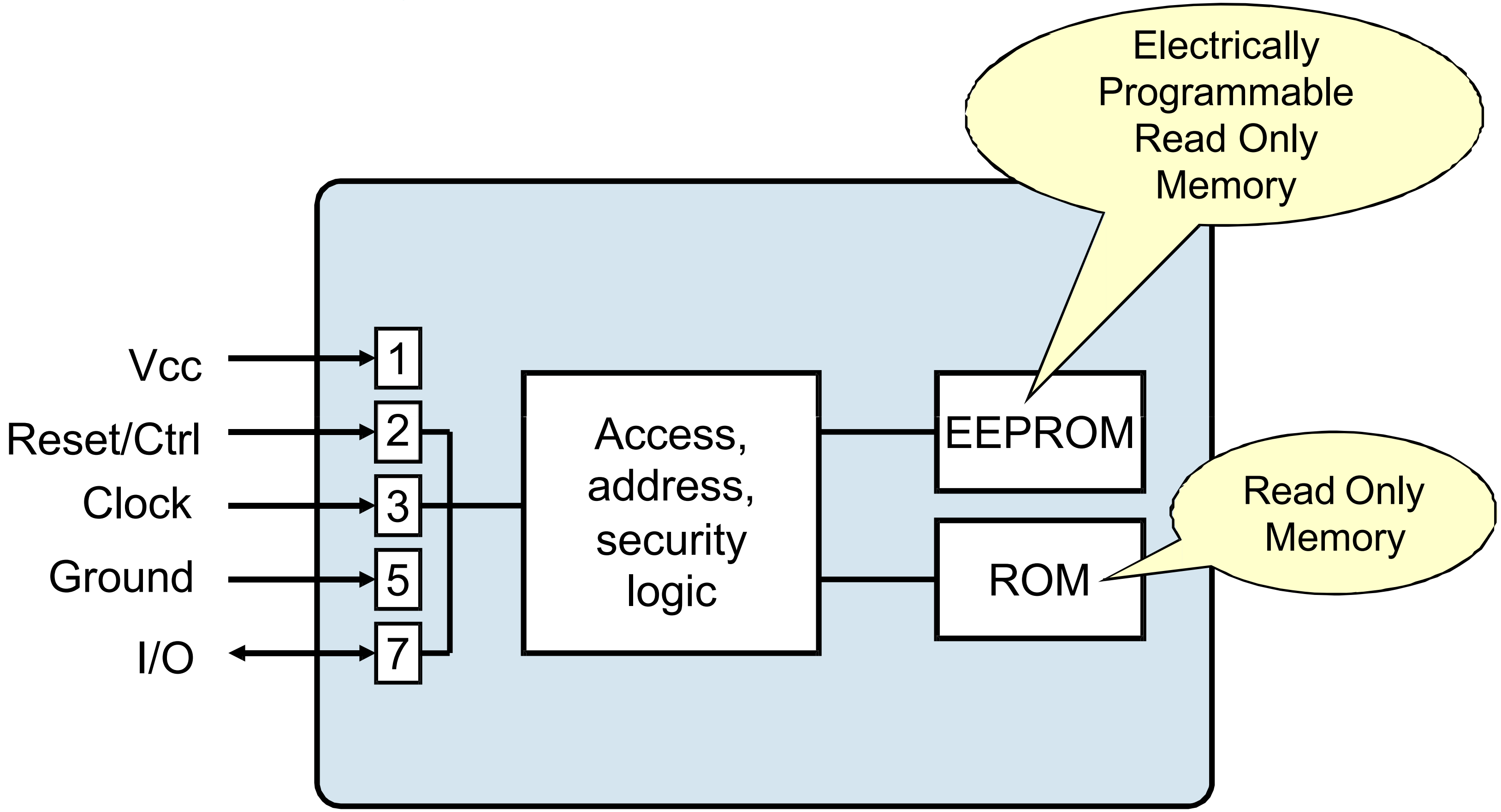
GND

V_{PP}

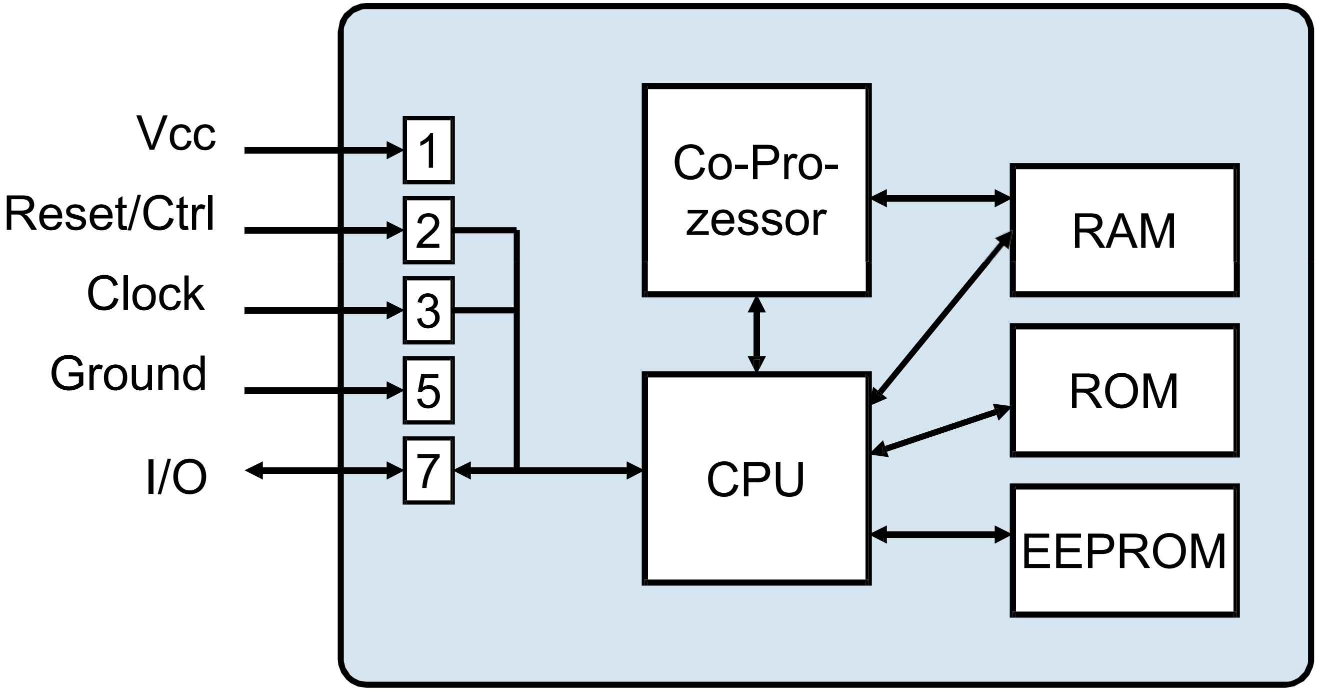
I/O

4/8 currently not used

Structure of a memory chip card

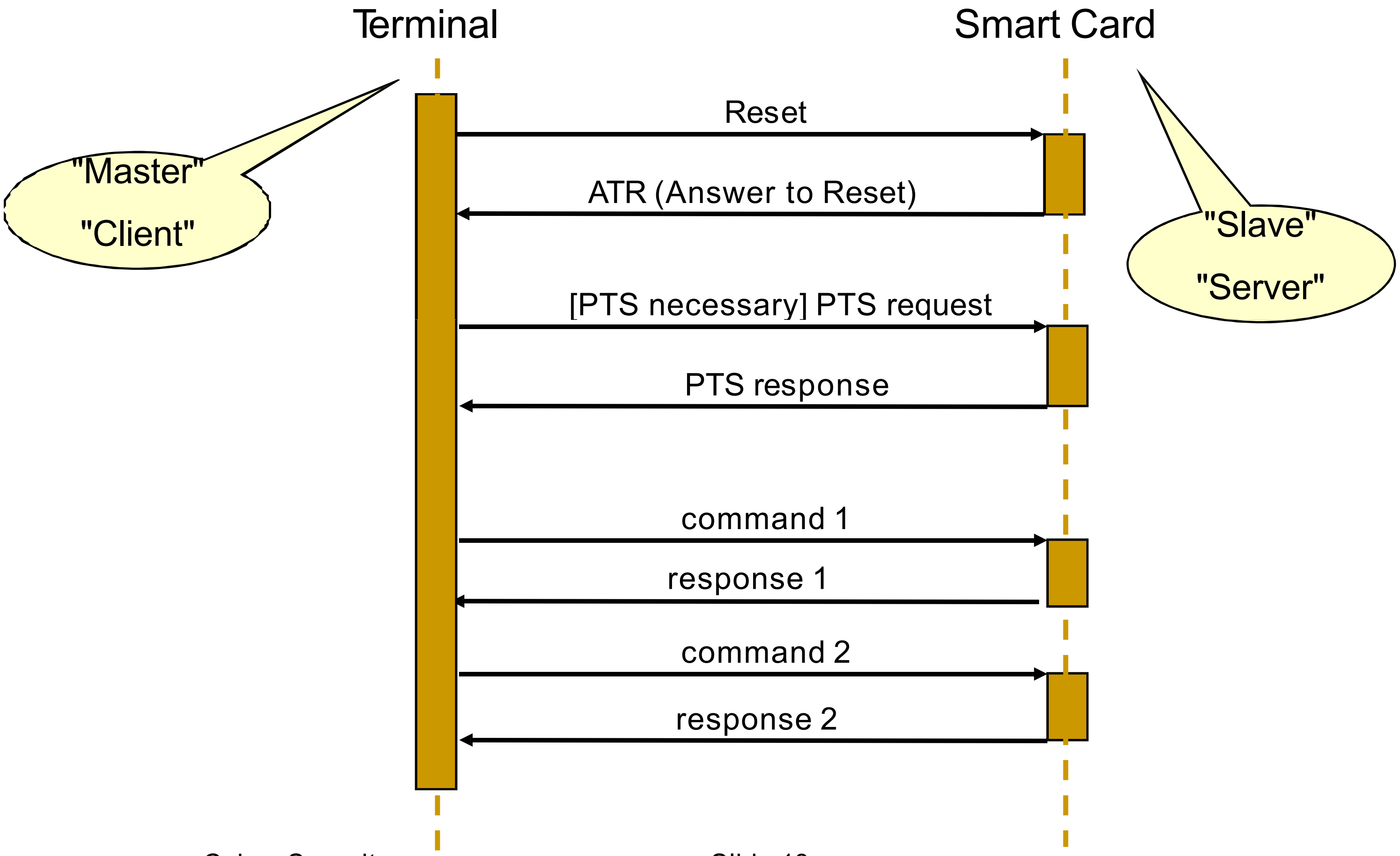

Electrically Programmable Read Only Memory
Vcc
1
Reset/Ctrl
2
Clock
3
Ground
5
I/O
7
Access, address, security logic
EEPROM
ROM
Read Only Memory

Structure of a processor chip card



Communication card / terminal

Basic scheme of chip card protocol



Activation Sequence and Reset

Activation sequence (driven by the terminal):

1)Ground

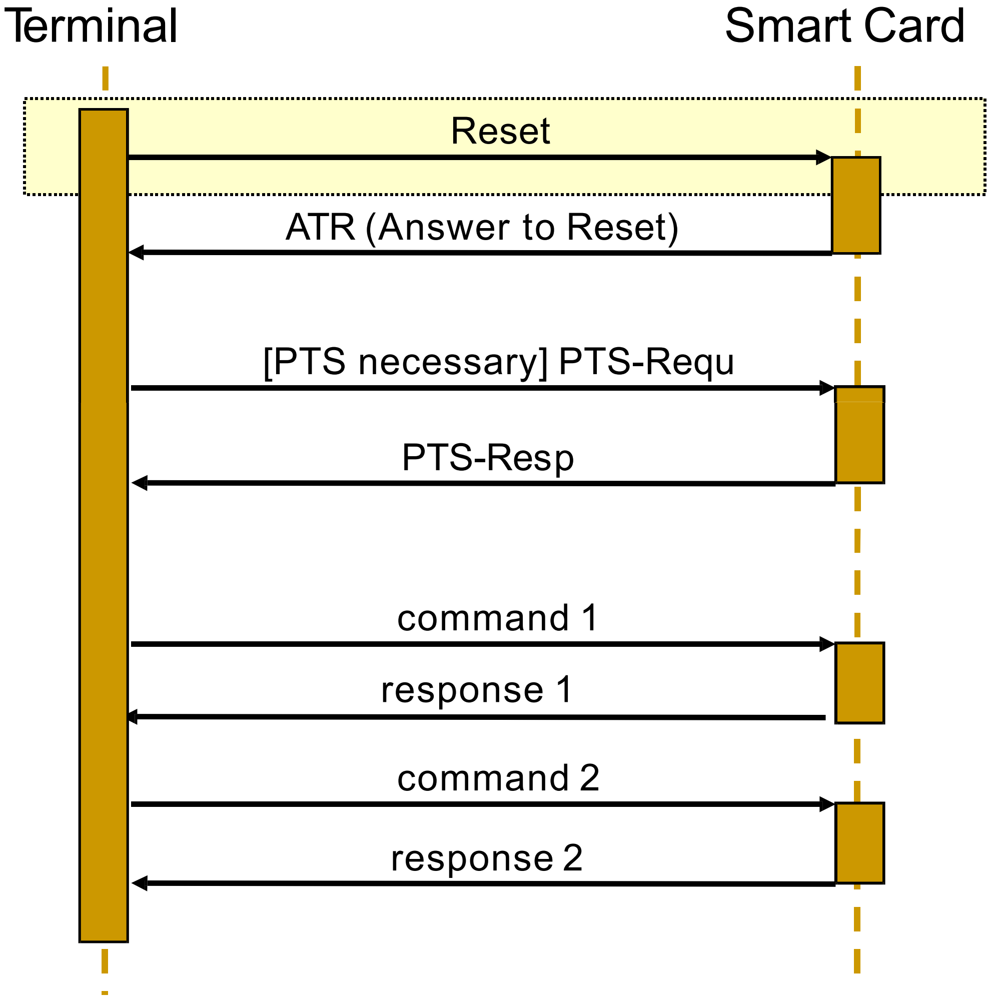
2)Power supply

3)(external) Clock

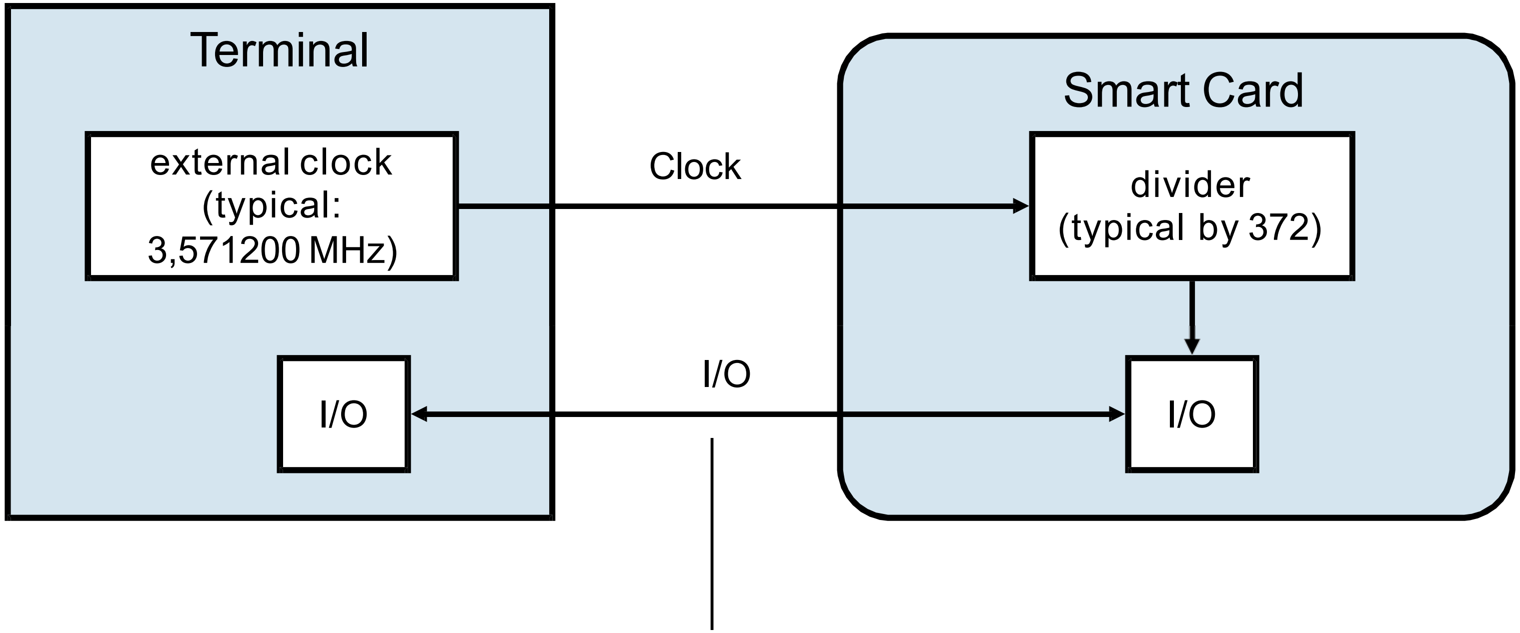
4)Reset

5) ....

V_{CC}		GND
RST		V_{PP}
CLK		I/O



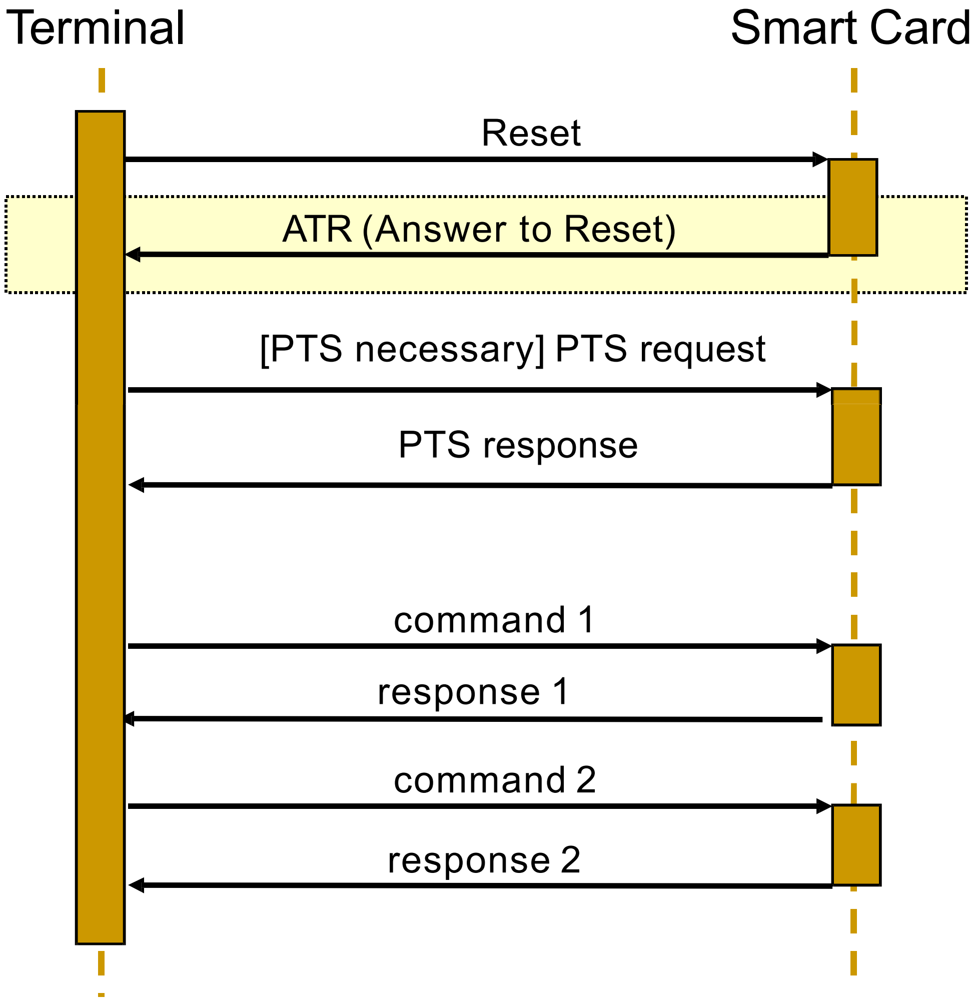
Physical Layer - Transmitting a Bit



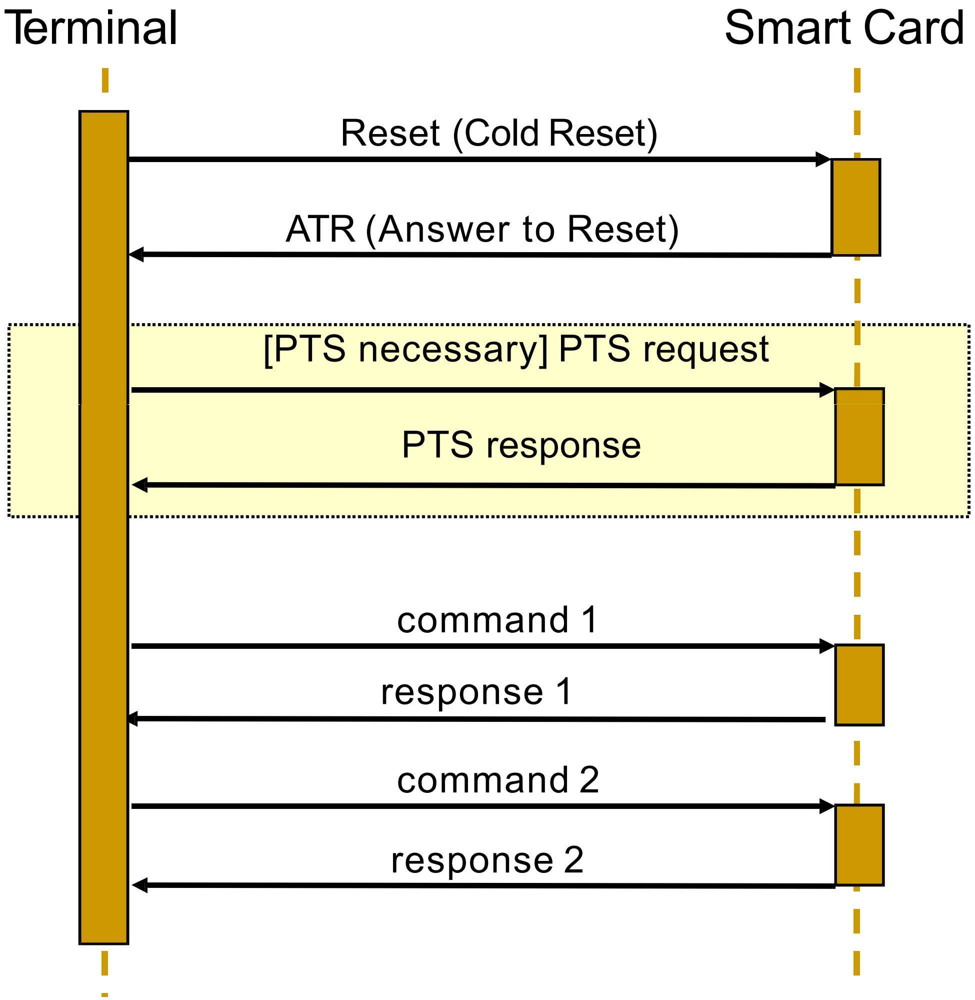
data transmission rate = 3571200 / 372 = 9600 bit/s

etu (elementary time unit) = length of a bit
= 372 / 3571200 = 104 µs

Answer to Reset



Protocol Type Selection



Terminal

Smart Card

Reset (Cold Reset)

ATR (Answer to Reset)

[PTS necessary] PTS request

PTS response

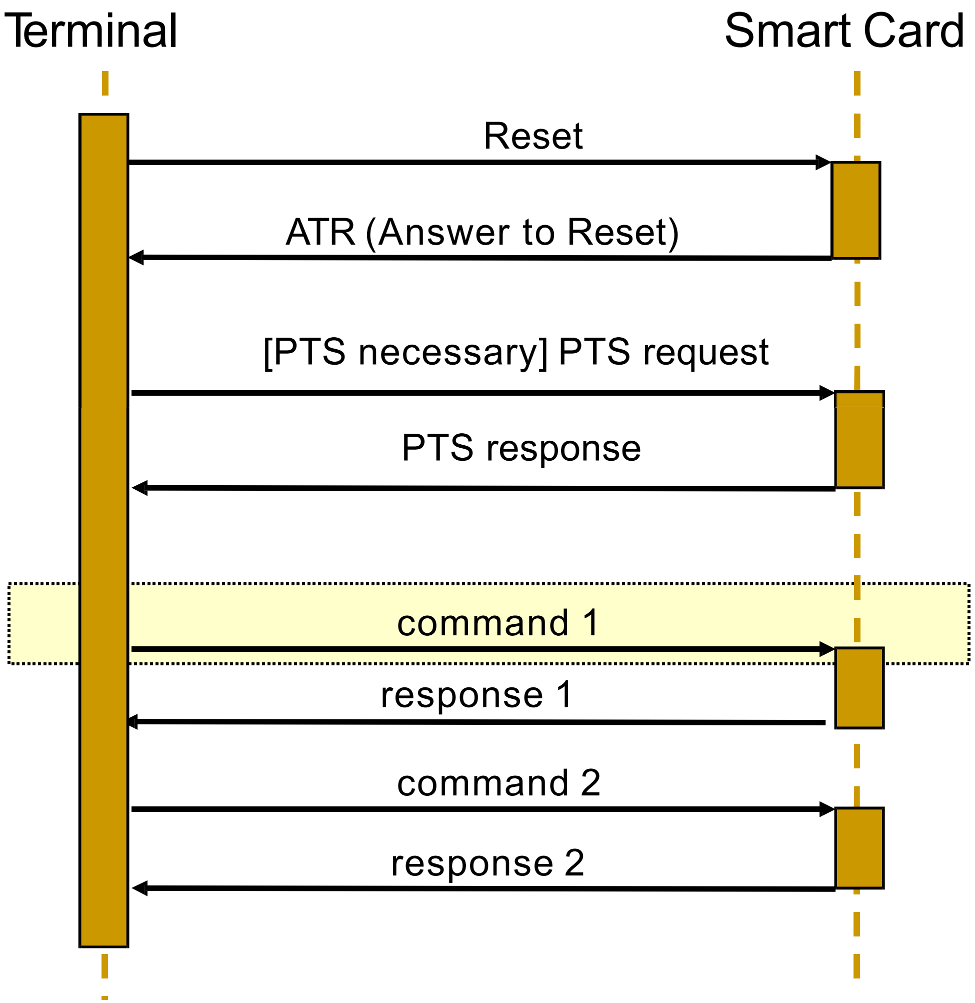
command 1

response 1

command 2

response 2

Sending a Command



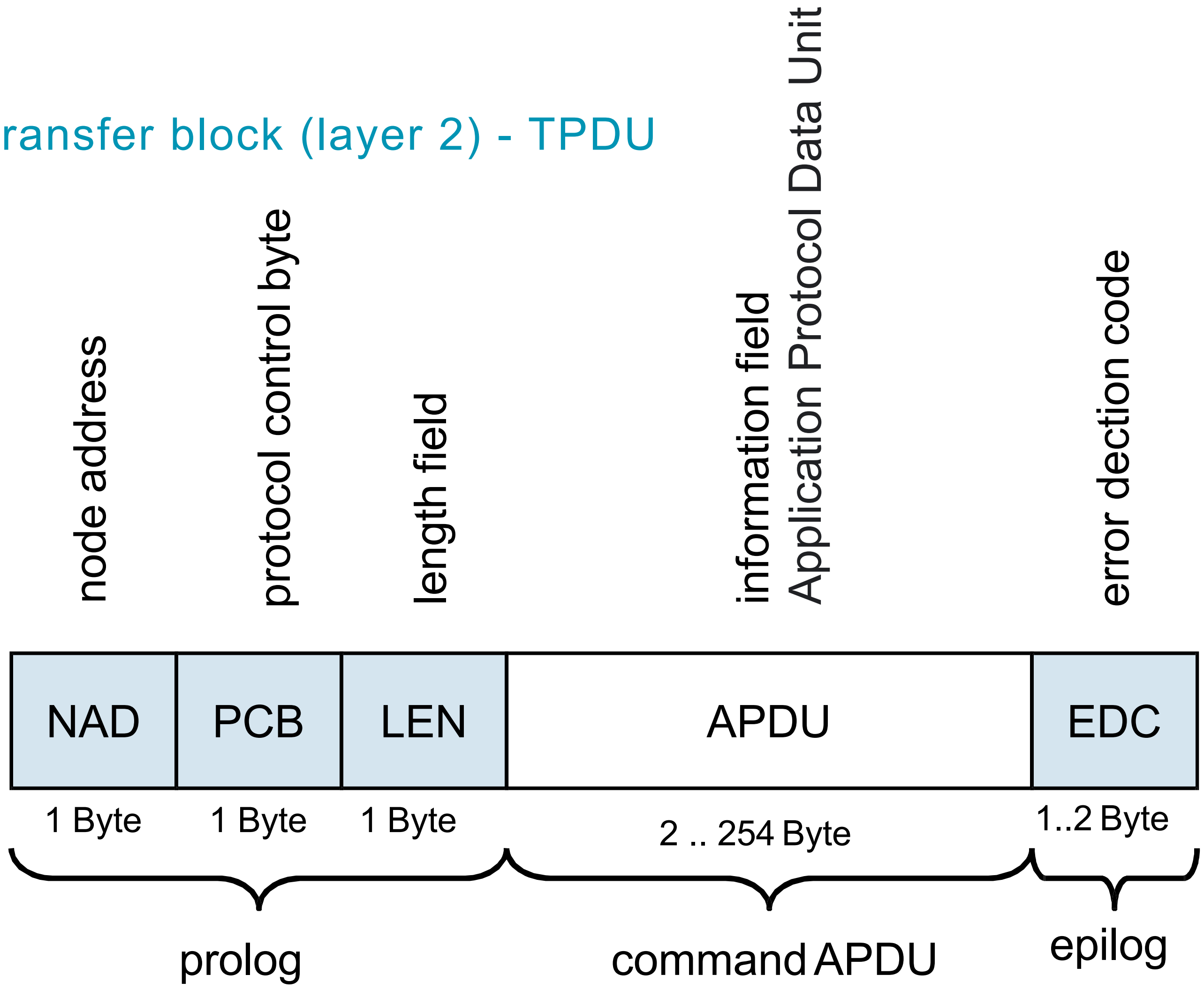
Layered Communication Model for Smart Card DataTransfer

OSI	*layer*	*specification*
OSI layer 7 transfer of application data	application layer	ISO/IEC 7816-4 EMV GSM **1 .1** , ...
OSI layer 2 transfer of data frames	data link layer	ISO/IEC 7816-3 (T=0 / T=1) ISO/IEC 10536-4 (T=2)
OSI layer 1 transfer of bits	physical layer	ISO/IEC 7816-3

Transmission Layer (Data Link Layer, Übertragungsschicht)

Protocol	Norm	Meaning
T=0	ISO/IEC 7816-3	half-duplex, asynchronous block-oriented
T=1	ISO/IEC 7816-3	half-duplex, asynchronous block-oriented
T=2		full duplex, asynchronous block oriented (in normalization)
T=3		full duplex,
T=4		half-duplex, asynchronous byte-oriented extension of T = 0
T=14		

Structure of a T1 transfer block (layer 2) - TPDU



node address	protocol control byte	length field	information field Application Protocol Data Unit	error dection code
NAD	PCB	LEN	APDU	EDC
1 Byte	1 Byte	1 Byte	2 .. 254 Byte	1..2 Byte
prolog			command APDU	epilog

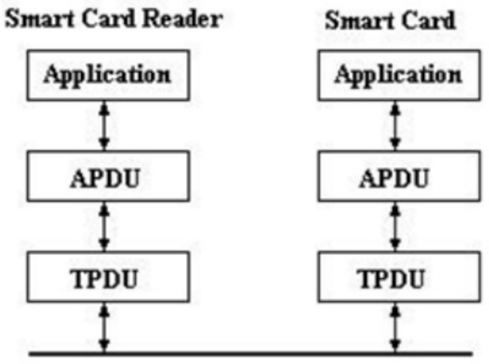
T1 is a transparent, block-oriented, asynchronous half-duplex protocol with error handling

Structure of command APDU

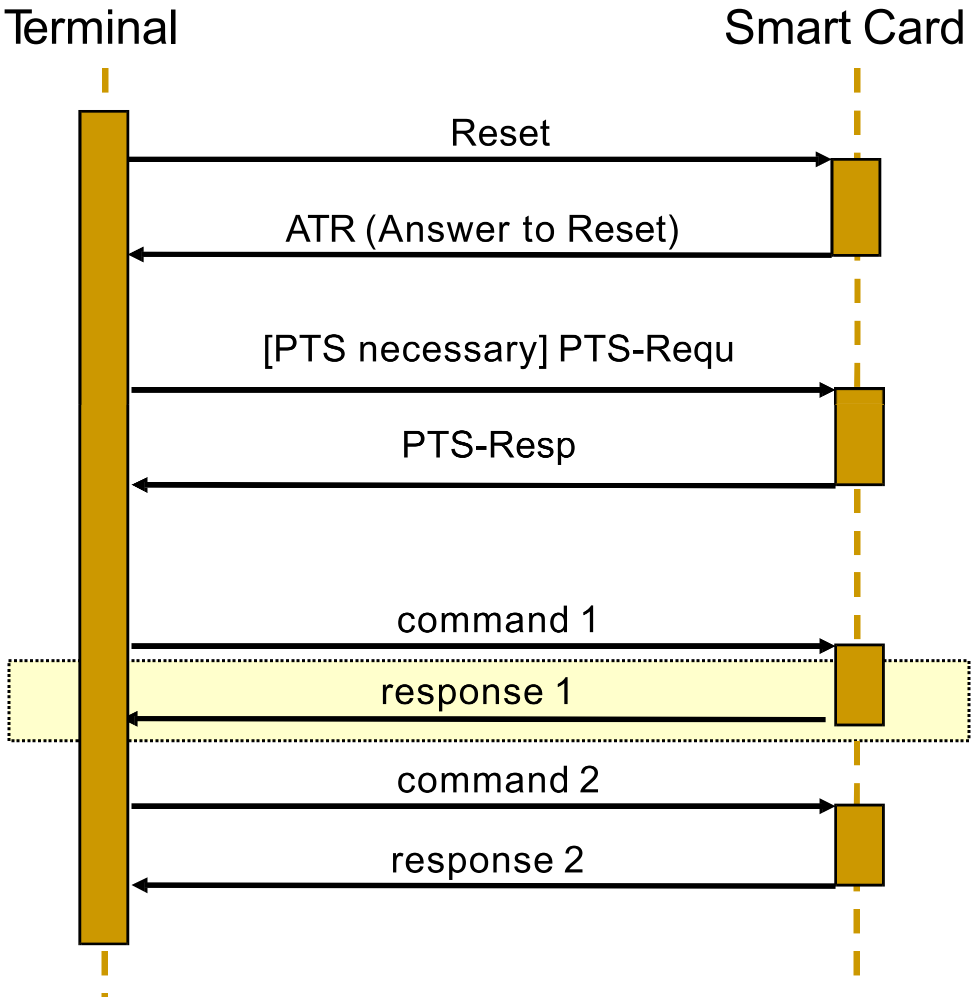
Class	Instruction	Parameter 1	Parameter 2	Length of data for command		Length of data expected for response
CLA	INS	P1	P2	Lc-Feld	Data	Le-Feld

Header

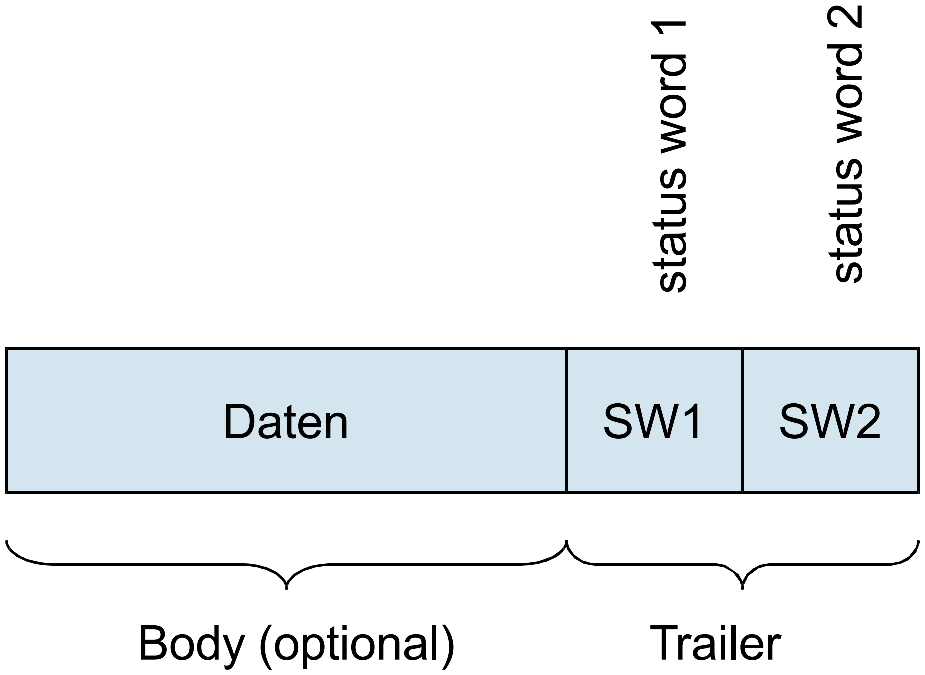
Body



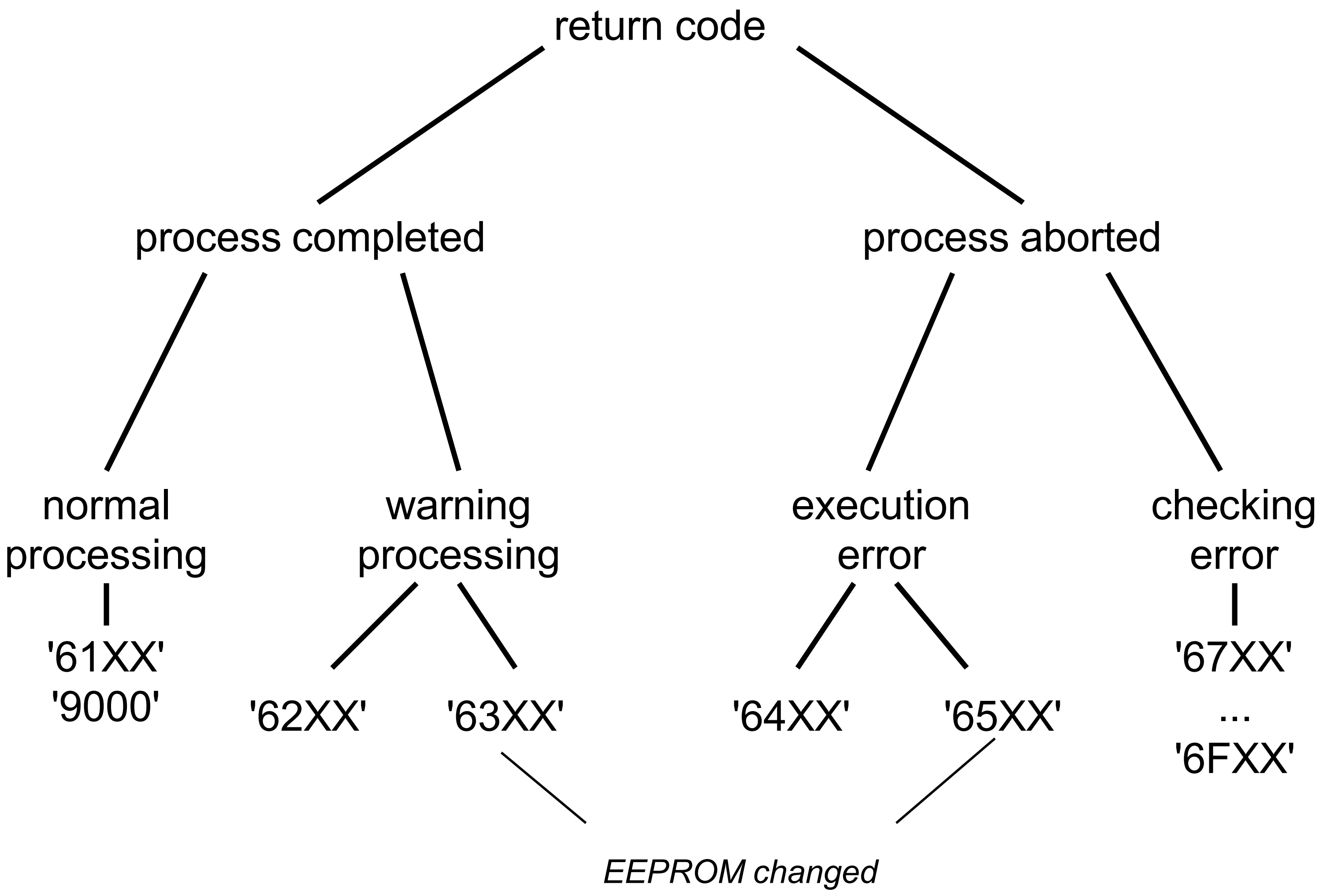
Sending a Response



Aufbau Response-APDU



Classification Scheme for the Return Code (SW1, SW2)



Resource requirements of a chip card

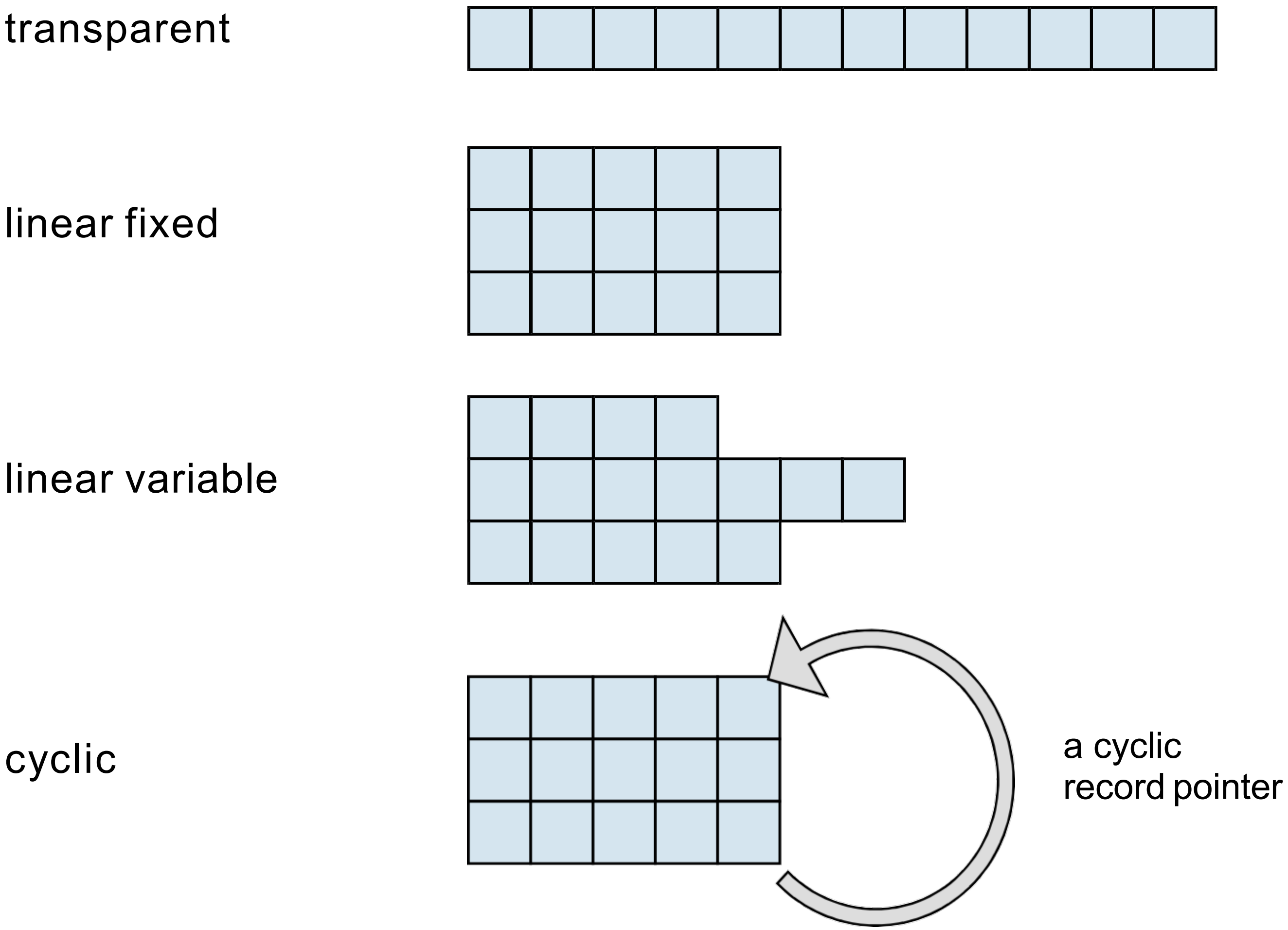
	ROM	RAM	EEPROM
Basic Card	min. 8 KB	256 Byte	8 KB
Java Card / MultOS	min. 16 KB	1 KB	8 KB

- Chip card file system is organized in directories and elementary files.

- There are four types of elementaryfiles
  - Transparent
  - Linear fixed
  - Linear variable
  - Cyclic

Four Types of Elementary Files

File structure:



transparent

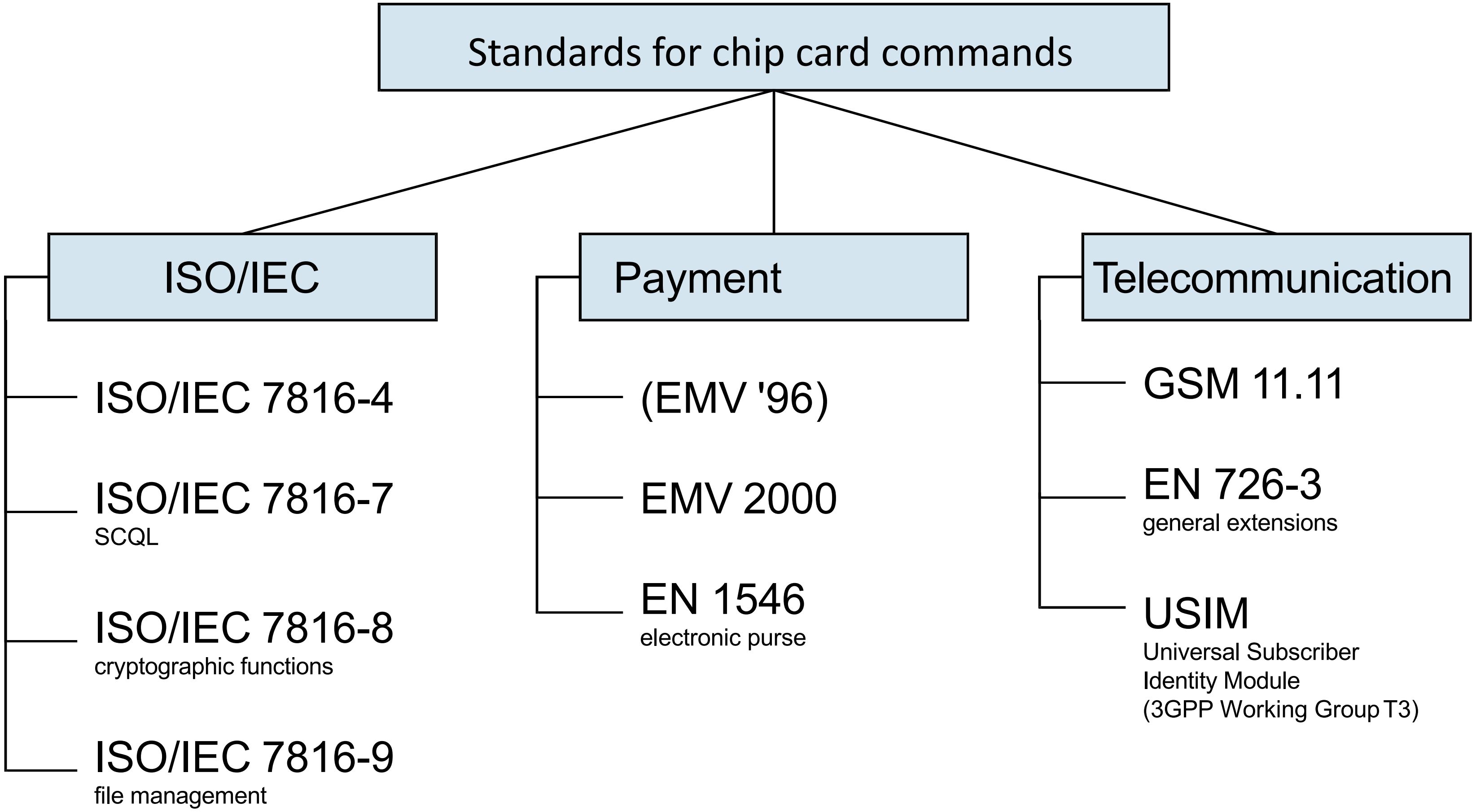
linear fixed

linear variable

cyclic

a cyclic
record pointer

Standards for chip card commands



Standards for chip card commands

ISO/IEC

- ISO/IEC 7816-4
- ISO/IEC 7816-7 SCQL
- ISO/IEC 7816-8 cryptographic functions
- ISO/IEC 7816-9 file management

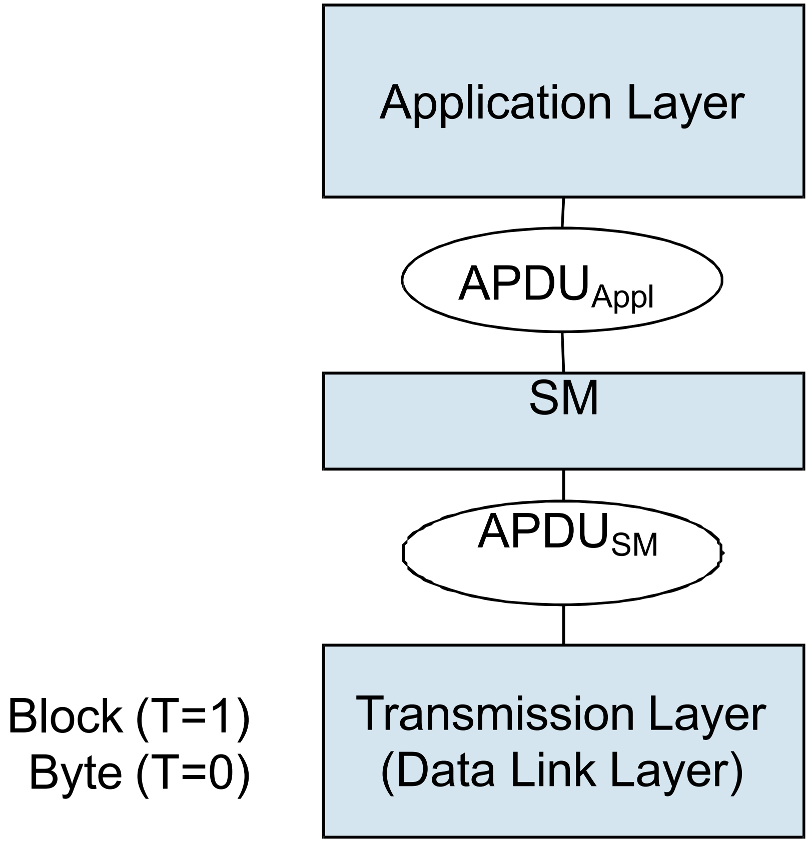
Payment

- (EMV '96)
- EMV 2000
- EN 1546 electronic purse

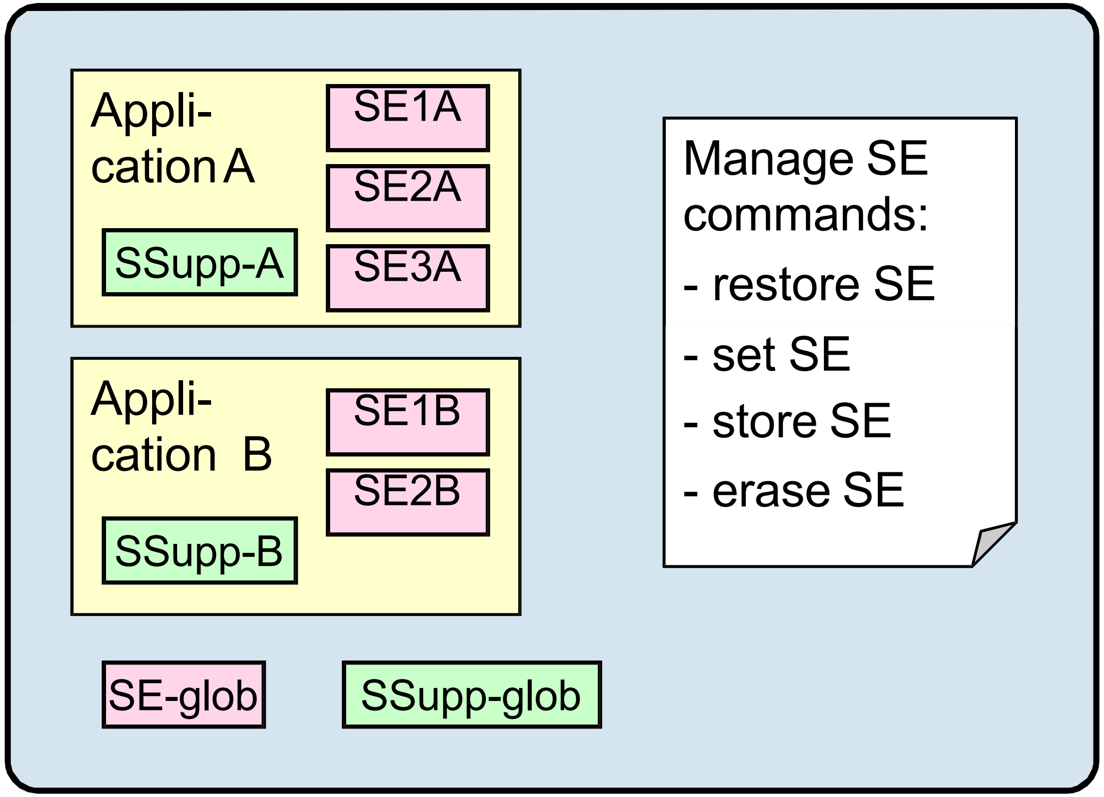
Telecommunication

- GSM 11.11
- EN 726-3 general extensions
- USIM Universal Subscriber Identity Module (3GPP Working Group T3)

Secure messaging as an intermediate layer



Secure Environment Concept



Manage SE commands:

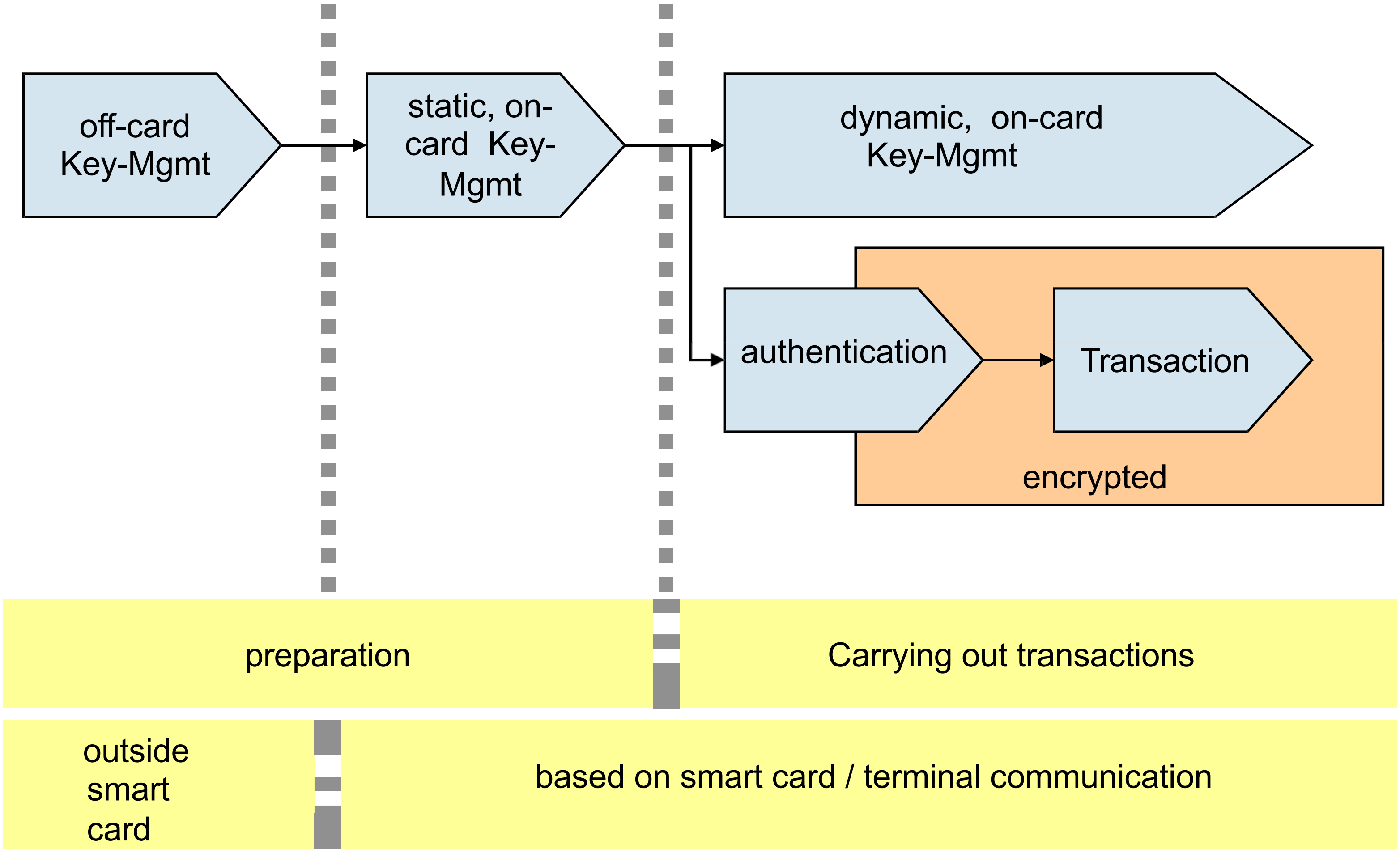
- restore SE
- set SE
- store SE
- erase SE

Layer architecture of smart card communication

OSI	*Layer*	*Specification*
OSI Layer 7 APDU	application layer	ISO/IEC 7816-4 EMV GSM 11.11, ...
	secure messaging	ISO/IEC 7816-4 und -8
OSI Layer 2 Frames	data link layer	ISO/IEC 7816-3 (T=0 / T=1) ISO/IEC 10536-4 (T=2)
OSI Layer 1 Bits	physical layer	ISO/IEC 7816-3

Authentication with smart cards

Key Management, Authentication and Encryption



Different definitions 'Authentication’

- American National Standard for Telecommunications (http://www.its.bldrdoc.gov):
  - A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator.
- OASIS, the Organization for the Advancement of Structured Information Standards (http://www.oasis-open.org/committees/security)
  - Authentication is the process of confirming a system entity’s (=an active element of a system - e.g., an automated process or set of processes, a subsystem, a person or group of persons--that incorporates a specific set of capabilities) asserted principal identity (= AAA Service clients) with a specified, or understood, level of confidence.
- Center for Democracy and Technology (http://www.cdt.org/)
  - Authentication - the process of verifying that a file or message has not been altered in route from the distributor to the recipient(s).

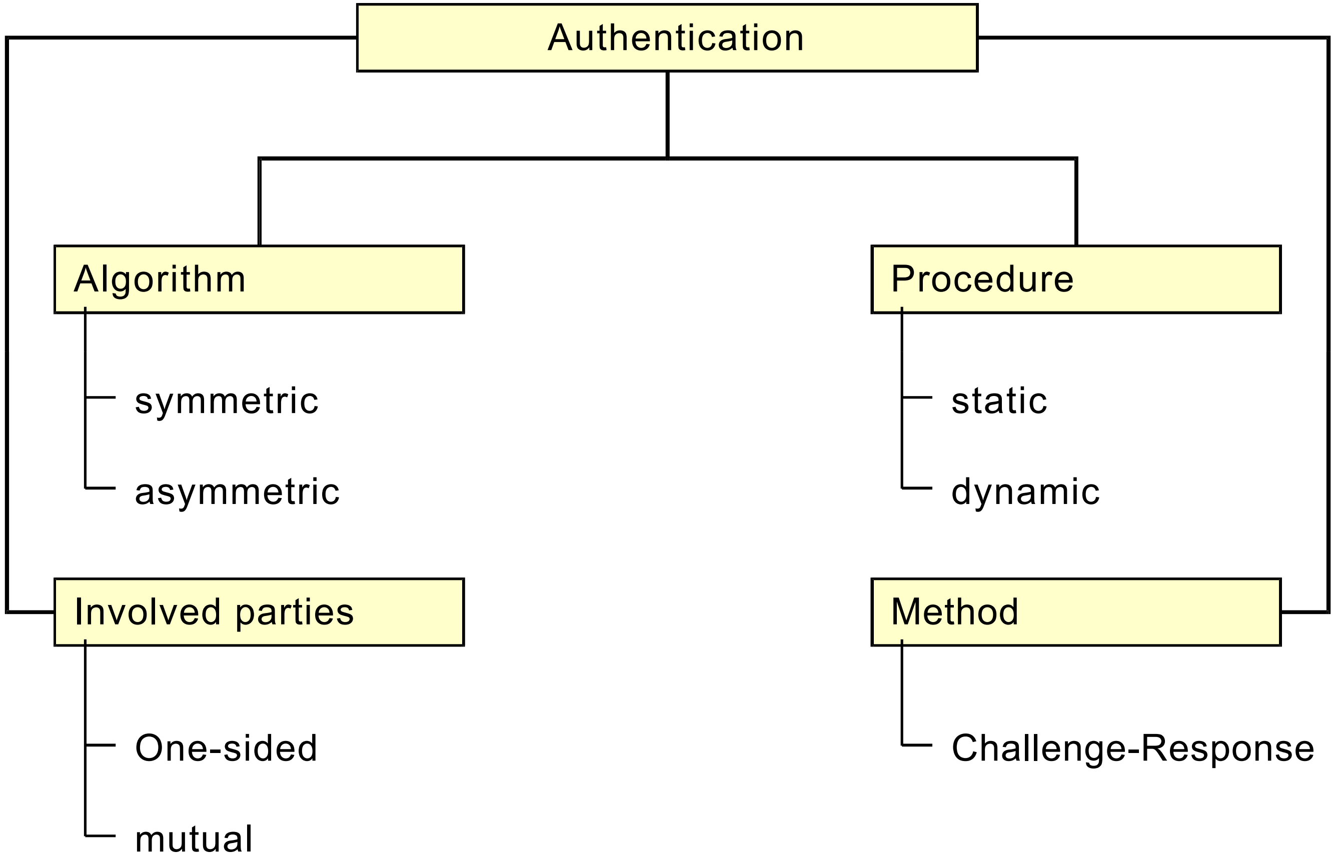
Definitionen 'Authentisierung' nach Clifford Lynch

- Authentication is the process where a network user establishes a right to an identity - in essence, the right to use a name.
- Validating authenticity entails verifying claims that are associated with an object - in effect, verifying that an object is indeed what it claims to be, or what it is claimed to be (by external metadata).

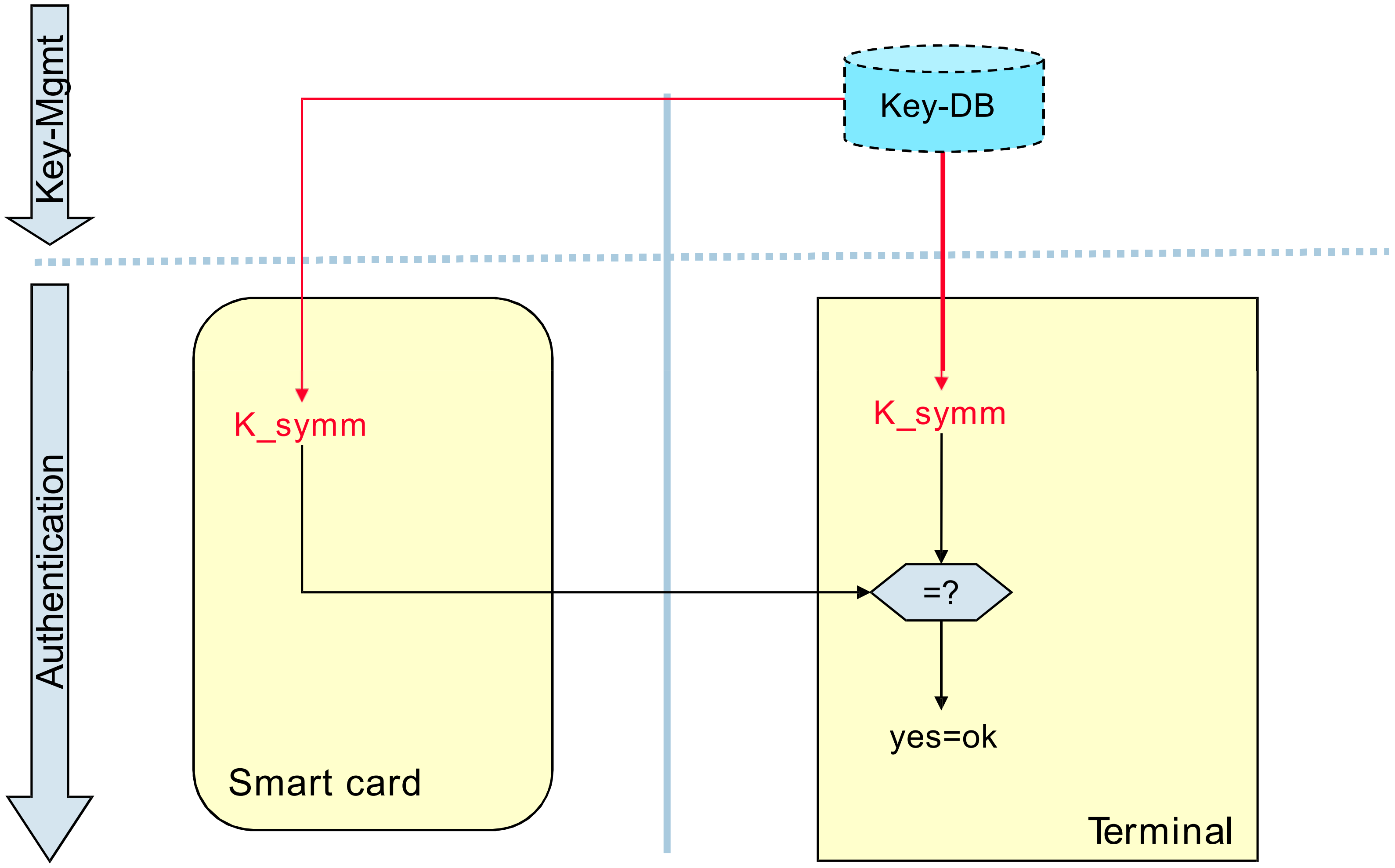
Clifford Lynch (ed.): A White Paper on Authentication and Access Management Issues in Cross-Organizational Use of Networked Information Resources, Coalition for Networked Information, Spring 1998. (Revised discussion draft – April 14).
Available at http://www.cni.org/projects/authentication/authentication-wp.html, accessed: November 20, 2001.

Lynch Clifford A.: Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust," Authenticity in a Digital Environment. Washington, DC, Council on Library and Information Resources, pp 32-50, 2000. Available at http://www.clir.org/pubs/reports/pub92/lynch.html, accessed: November 20, 2001.

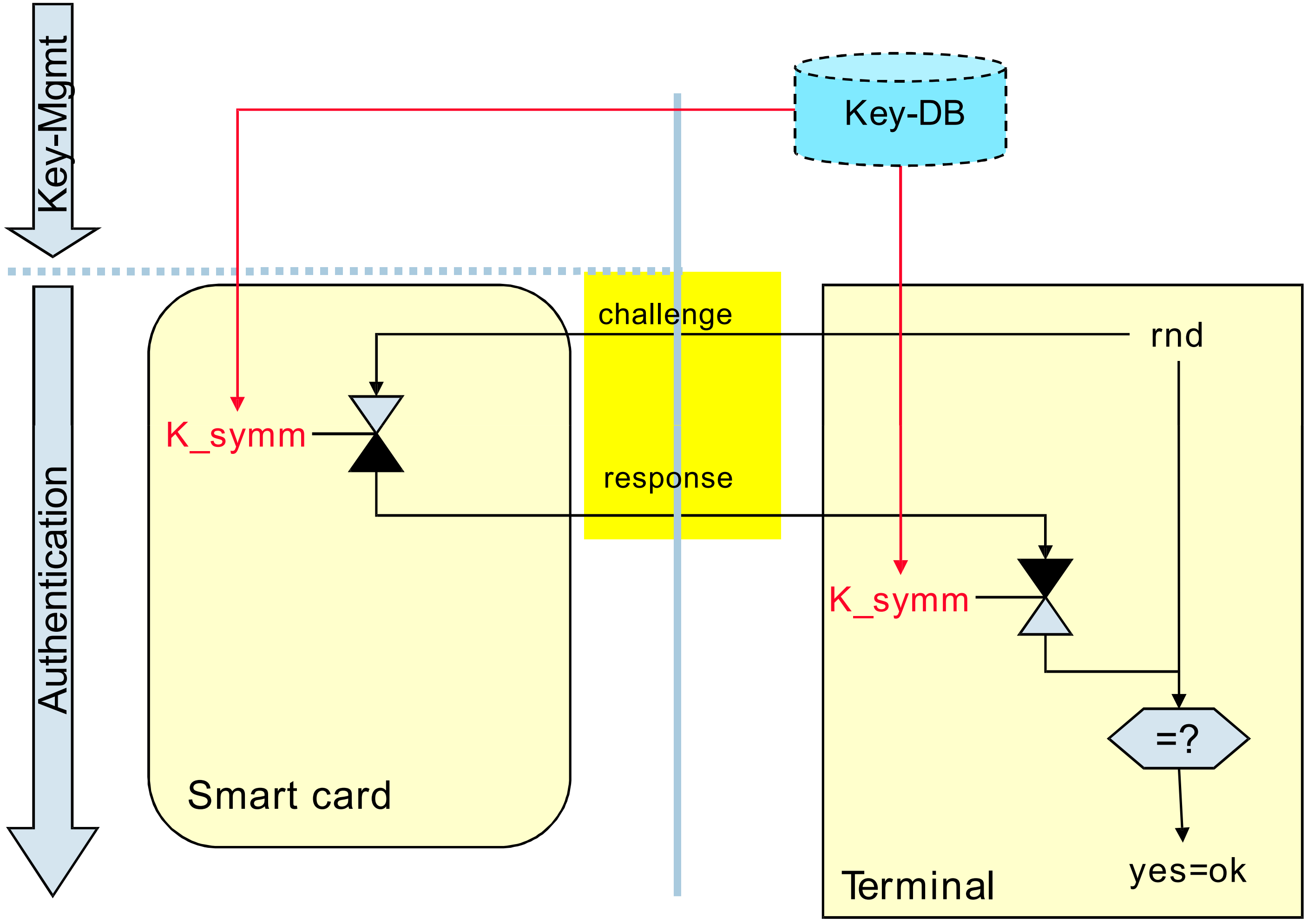
Classification scheme Authentication (according to Rankl / Effing)



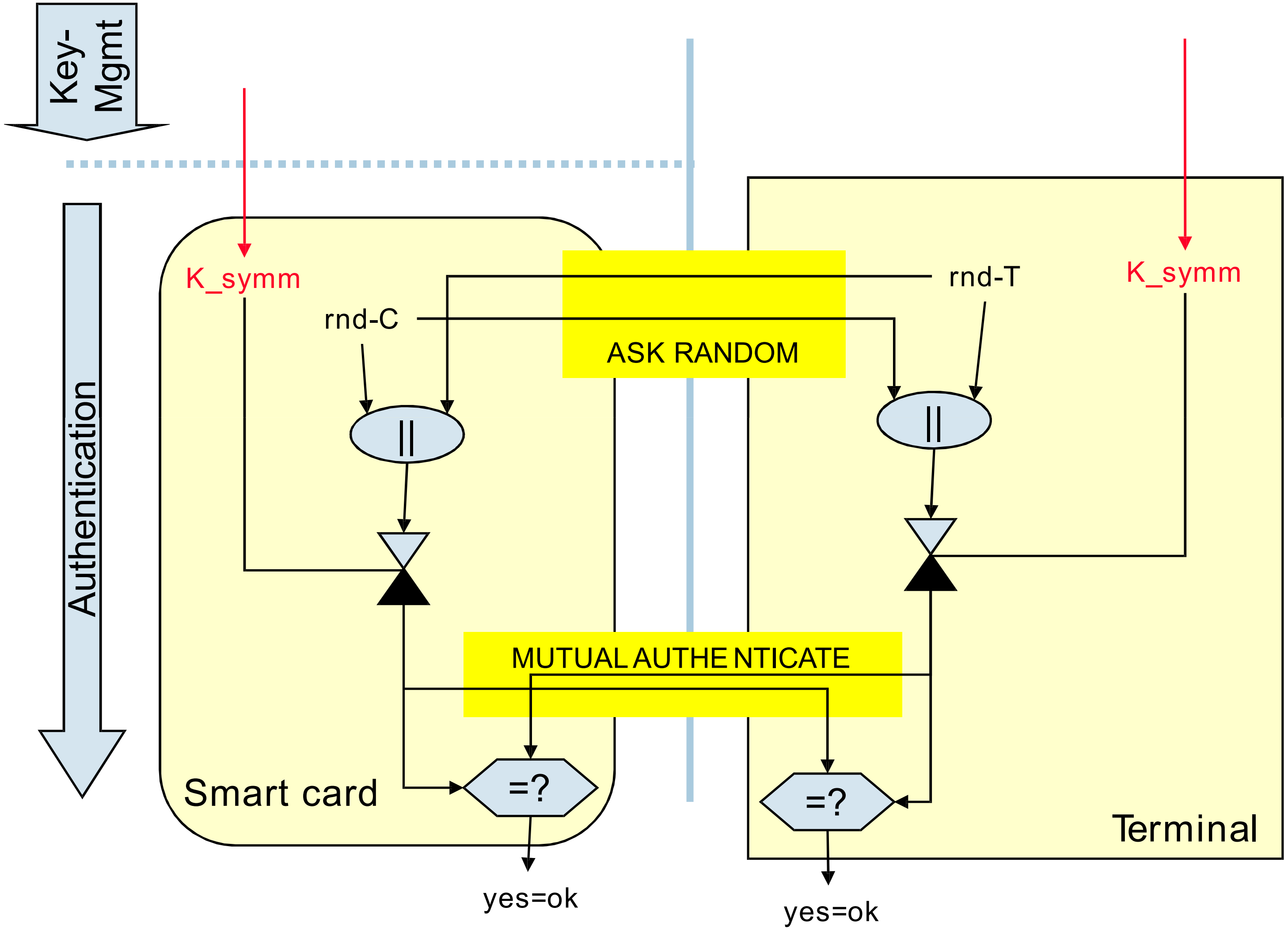
One-sided, symmetric, static authentication



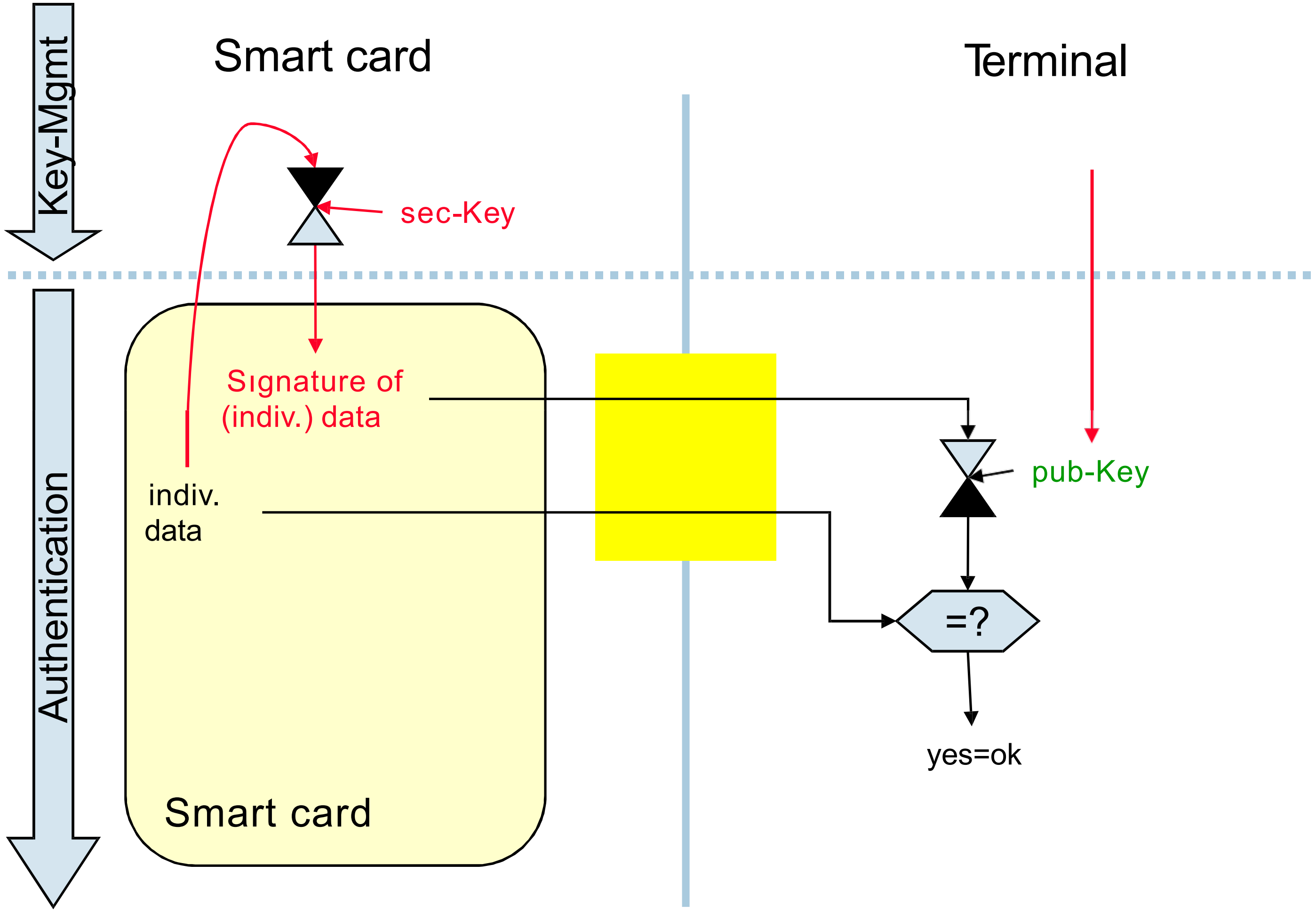
One-sided, symmetric, dynamic authentication



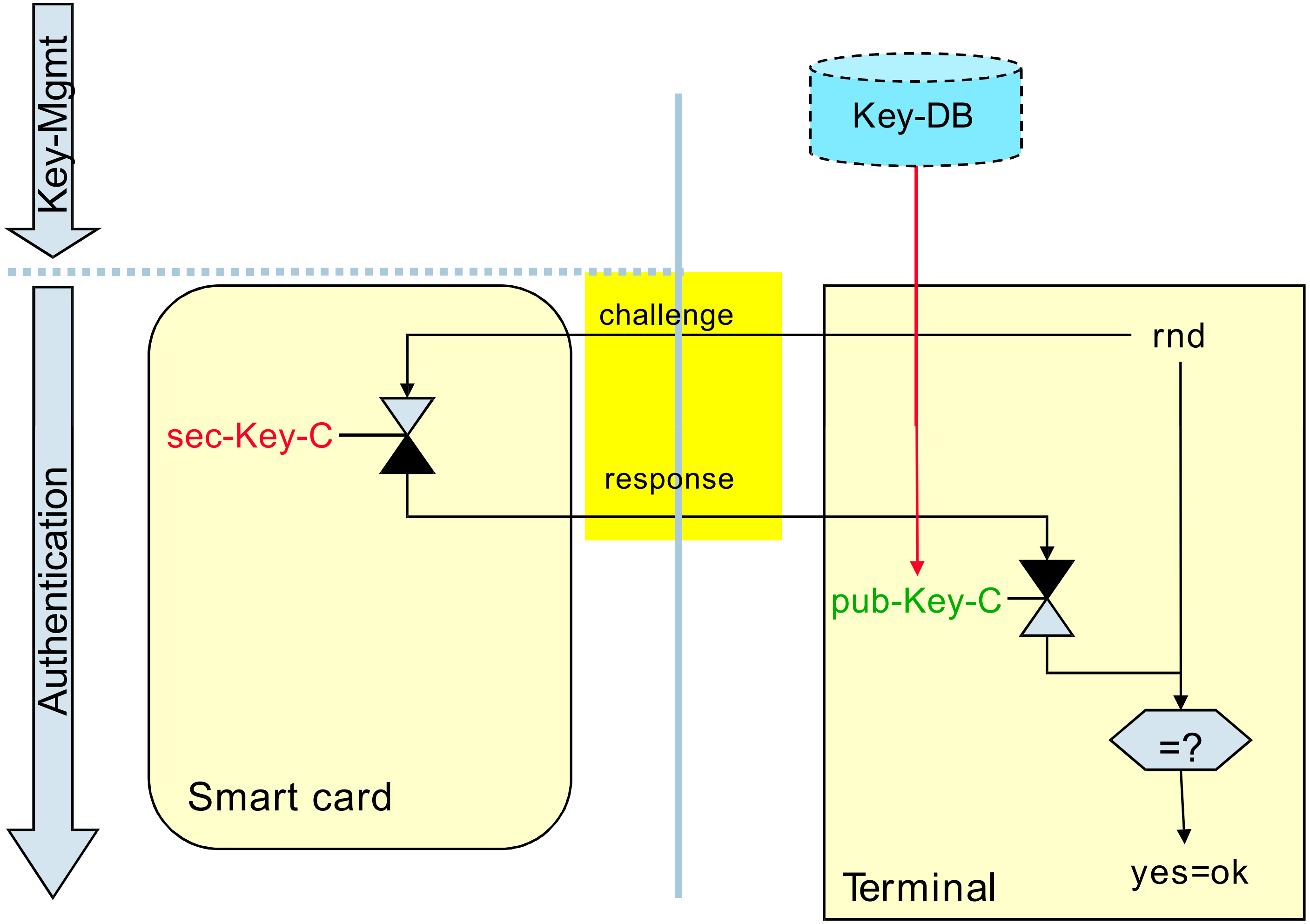
Mutual, symmetric, dynamic authentication



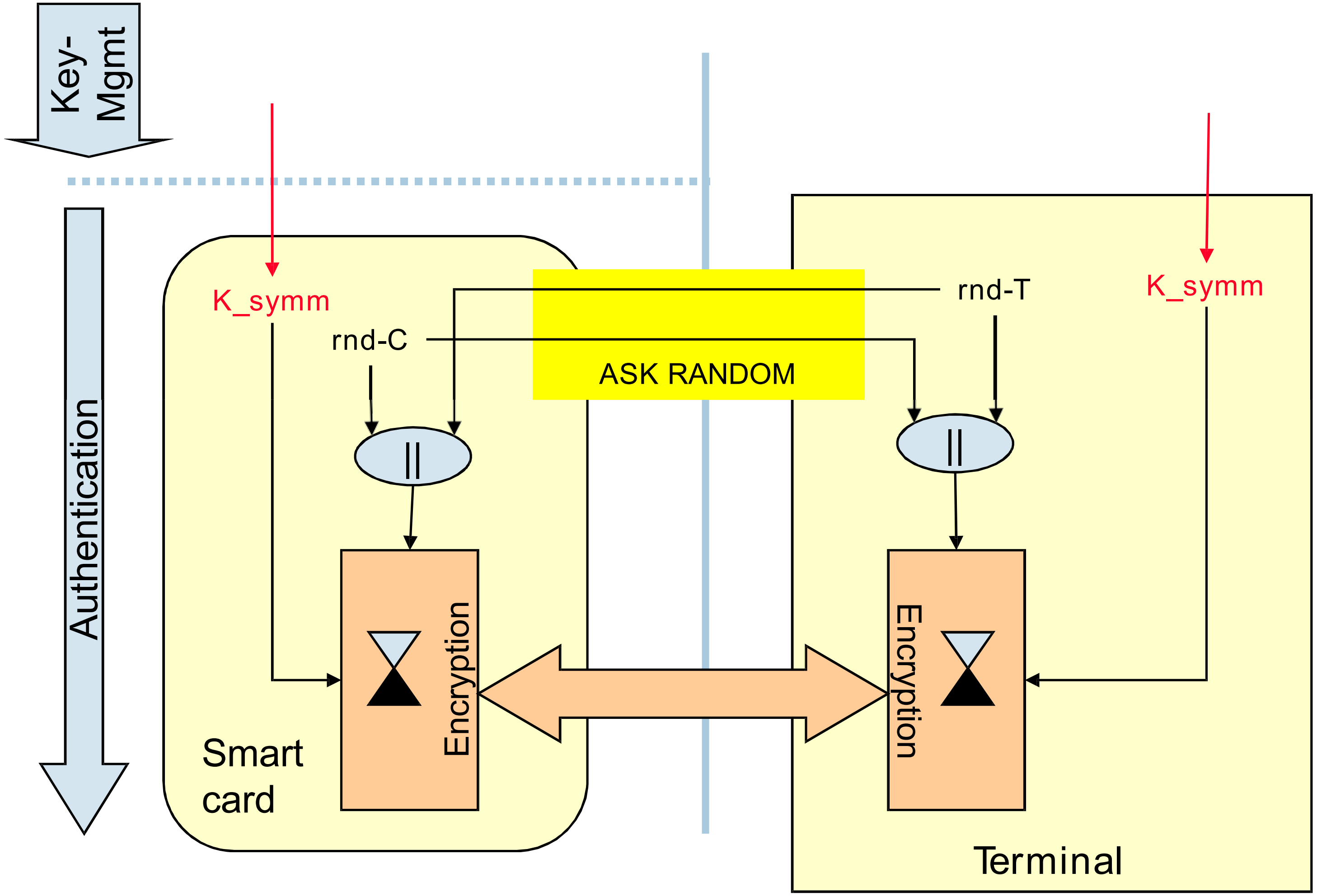
One-sided, asymmetric, static authentication with global keys



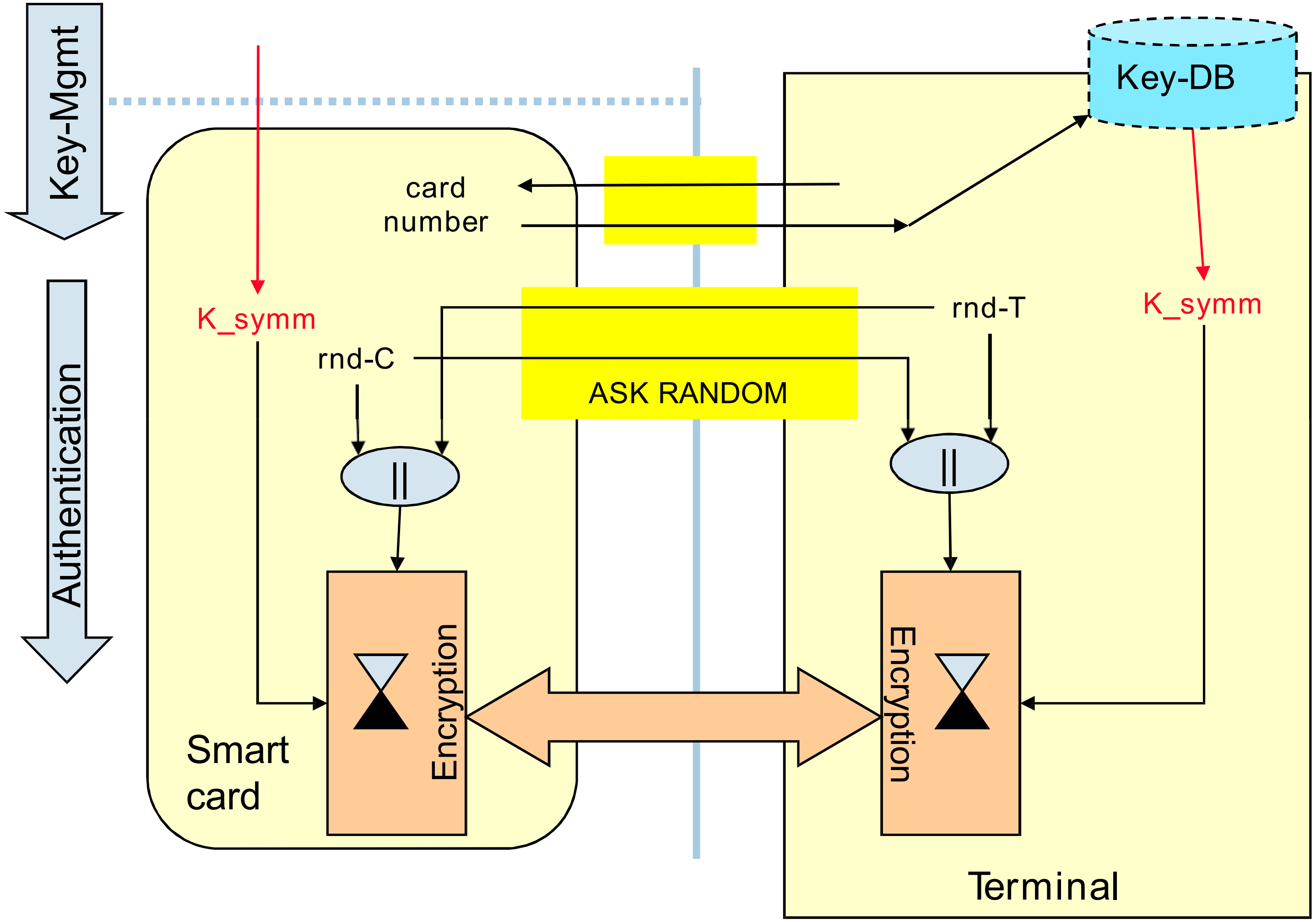
One-sided, asymmetric, dynamic authentication



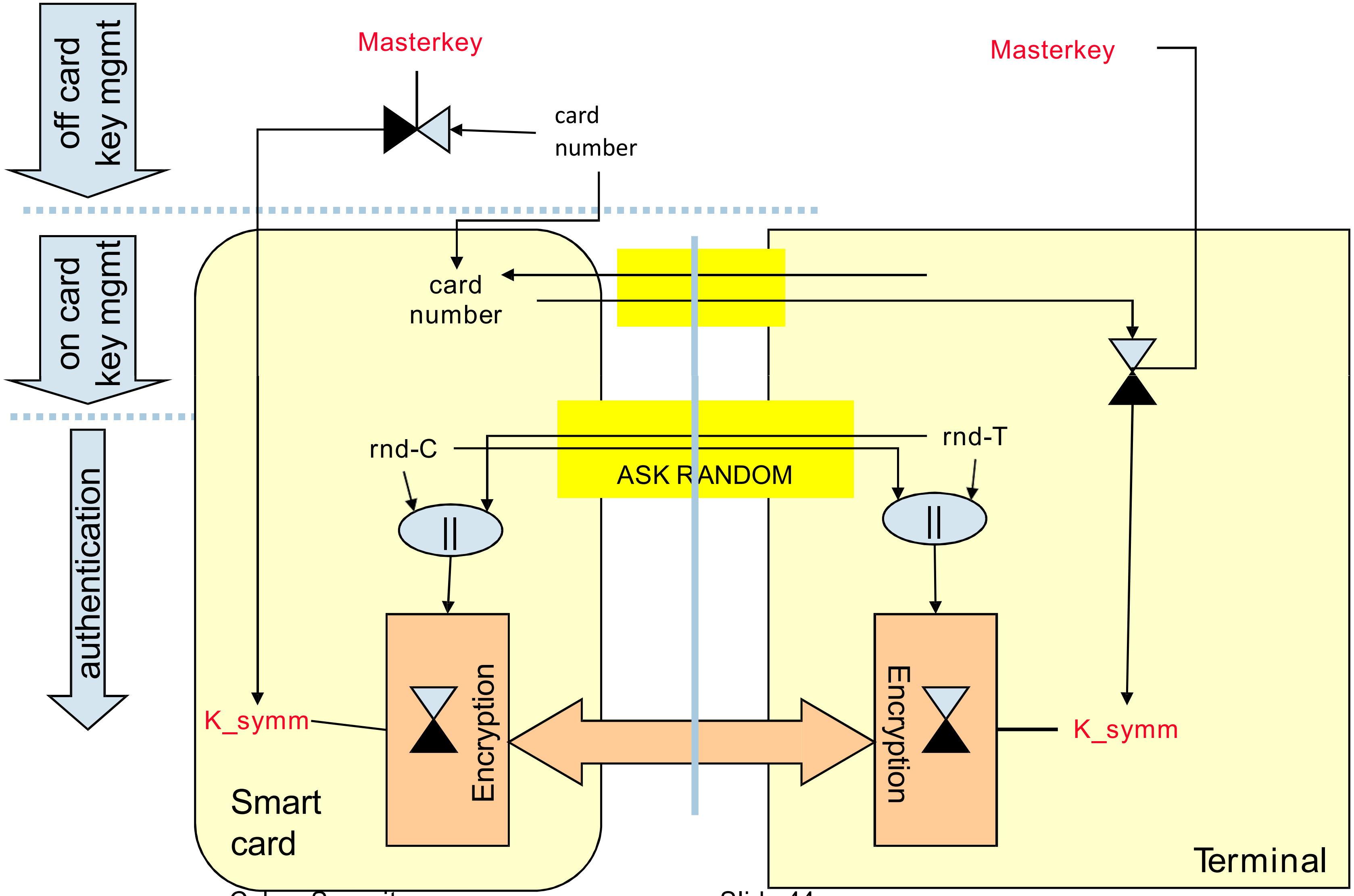
Mutual, symmetric, dynamic authentication and encryption



Mutual, symmetric, dynamic authentication with key management and encryption



Mutual, symmetric, dynamic authentication with *master key* and encryption


off card key mgmt
on card key mgmt
authentication
Masterkey
card number
Masterkey
card number
ASK RANDOM
rnd-C
rnd-T
||
||
Encryption
Encryption
K_symm
K_symm
Smart card
Terminal