Kartentypen

Types of Cards
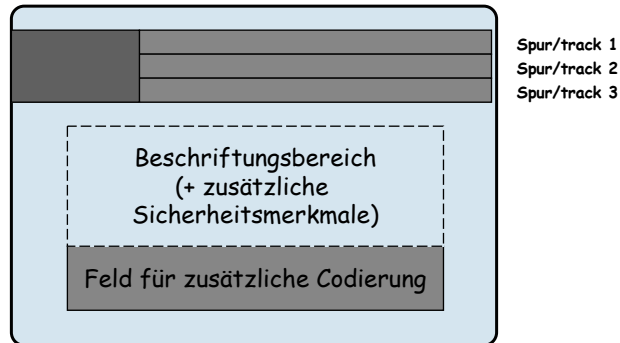

Hochgeprägte Karten / Embossed Cards

4 x 27 characters reserved for cardholder's name and address

19 characters reserved for ID number

region 1

region 2
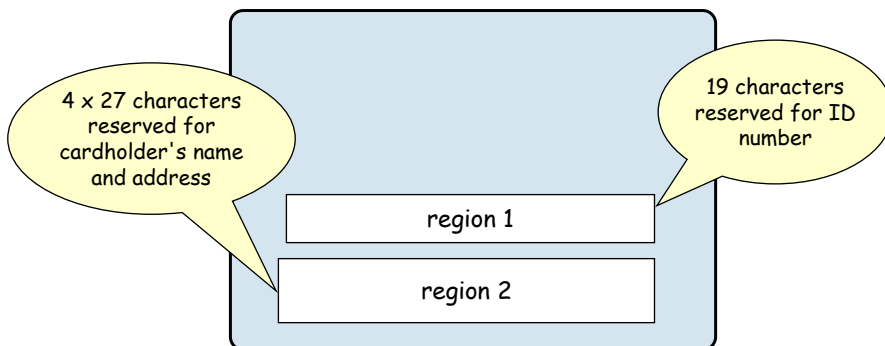
Magnetstreifenkarte / Magnetic-strip Cards

Spur/track 1
Spur/track 2
Spur/track 3

Beschriftungsbereich
(+ zusätzliche
Sicherheitsmerkmale)

Feld für zusätzliche Codierung

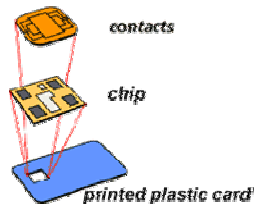
What is a Smart Card ?

<u>Definition</u>

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

o   either a memory chip or

o   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.

contacts
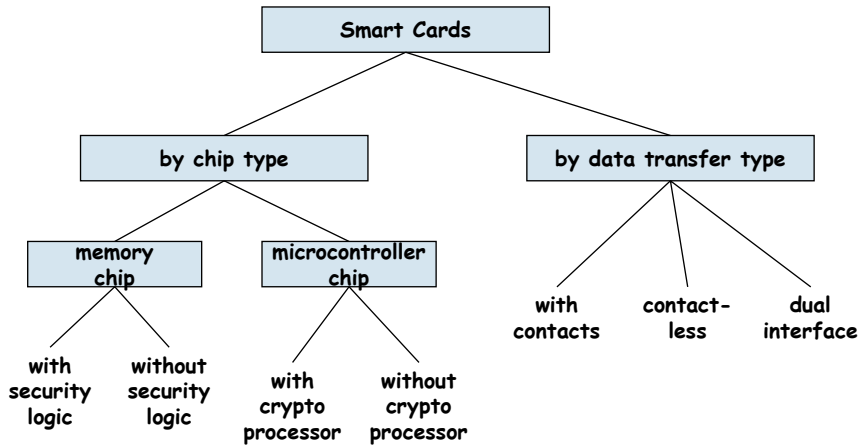
chip

printed plastic card

25 March 1974:

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

Classification Chart for Smart Cards

```
                      ┌──────────────┐
                      │ Smart Cards  │
                      └──────┬───────┘
              ┌──────────────┴──────────────┐
        ┌─────────────┐              ┌──────────────────────┐
        │ by chip type│              │ by data transfer type│
        └──────┬──────┘              └──────────┬───────────┘
        ┌──────┴──────┐
  ┌──────────┐  ┌────────────────┐
  │ memory   │  │ microcontroller│
  │ chip     │  │ chip           │
  └────┬─────┘  └───────┬────────┘
```

memory chip:
- with security logic
- without security logic

microcontroller chip:
- with crypto processor
- without crypto processor

by data transfer type:
- with contacts
- contact-less
- dual interface

by W. Rankl / W. Effing

© M. Leischner

Arten von Chipkartenspeicher / Memory Types

o ROM (read-only memory)
o PROM (programmable read-only memory)
o EPROM (erasable programmable read-only memory)
o EEPROM (electrically erasable programmable
            read-only memory)
o Flash-EEPROM
o FeRAM (ferroelectric random-acces memory)
o RAM (random access memory)

NetLab:
o Enhanced BasicCard ZC3.9:
   8K EEPROM, 256 bytes RAM
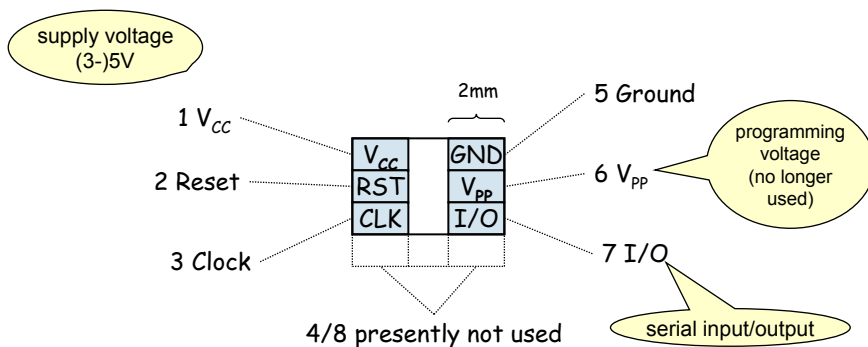o Professional BasicCard ZC4.5A: 30K EEPROM, 1K RAM

© M. Leischner

Platzbedarf für ein Bit /
area required for a single bit cell

Fest-platte	Haar	ROM	FRAM	EEPROM	RAM
0,0005		1	2	4	16
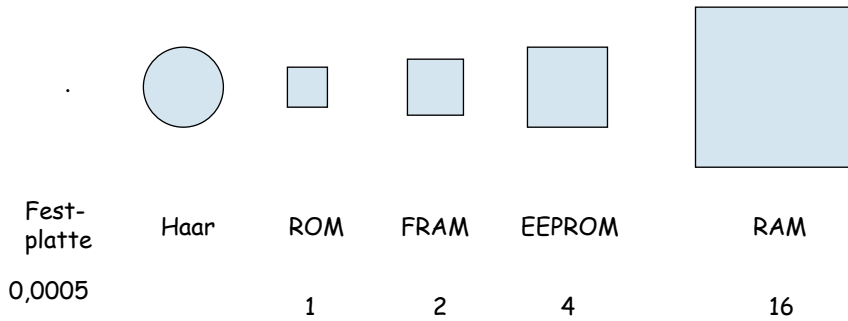
© M. Leischner

Quelle: Rankl/Effing

Kontaktfelder einer Chipkarte (ISO 7816-2) /
Smart Card Contact Areas (ISO/IEC 7816-2)

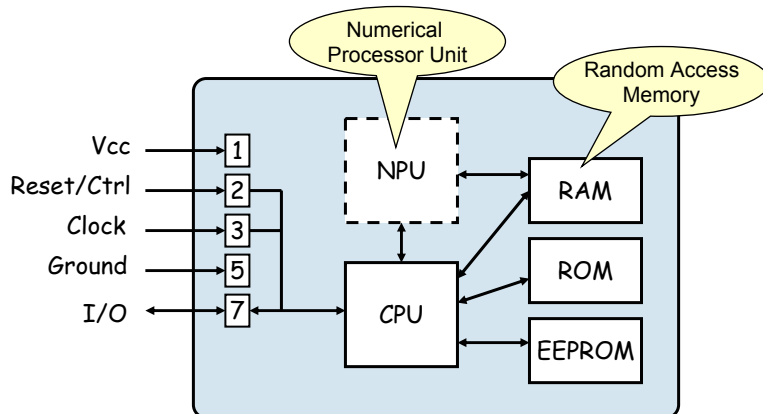supply voltage (3-)5V

2mm

1 V_{CC}

5 Ground

2 Reset

6 V_{PP}

programming voltage (no longer used)

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

3 Clock

7 I/O

4/8 presently not used

serial input/output

© M. Leischner

Architecture of a Memory Card

Electrically
Programmable
Read Only Memory

Vcc — 1
Reset/Ctrl — 2
Clock — 3
Ground — 5
I/O — 7

access,
address and
security
logic

EEPROM

ROM

Read Only
Memory
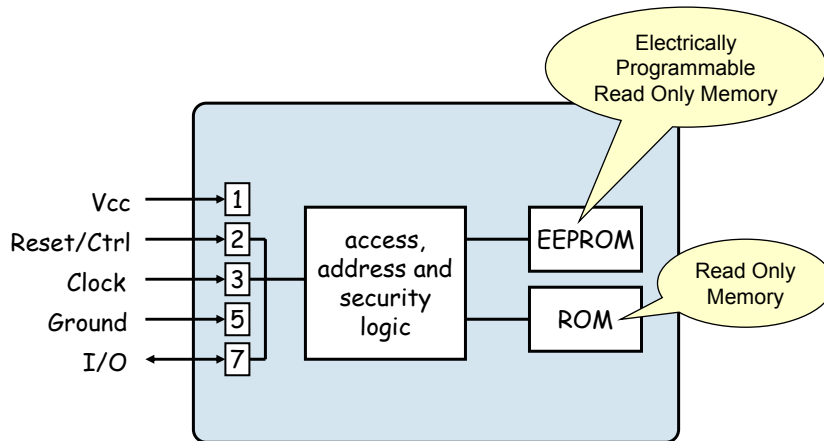
© M. Leischner

Architecture of a Microprocessor Card

Numerical
Processor Unit

Random Access
Memory

Vcc — 1
Reset/Ctrl — 2
Clock — 3
Ground — 5
I/O — 7

NPU

RAM

CPU

ROM

EEPROM

© M. Leischner

Architecture of a Contactless Microprocessor Card

antenna

energy, reset		1	Vcc	1	Co-Pro-cessor	RAM
clock	2	Reset/Ctrl	2		ROM
	3	Clock	3		
	5	Ground	5	CPU	
comm.	7	I/O	7		EEPROM

4 problems to solve:
- energy transfer
- transmission of clock signal
- data transfer to the smart card
- data transfer from the smart card
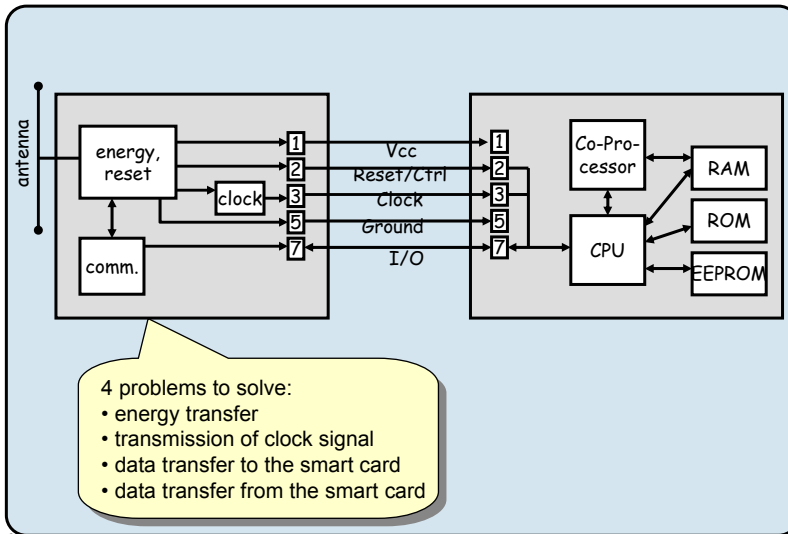
Architektur kontaktlose Chipkarte (Kombikarte) / Architecture of a dual interface card

Vcc 1
Reset/Ctrl 2
Clock 3
Ground 5
I/O 7

Antenne

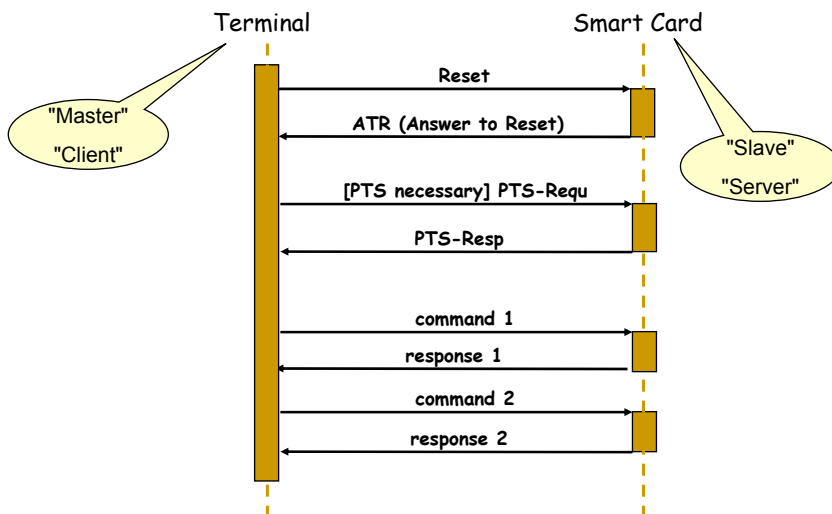| Energie Reset | | 1 | | 1 | Co-Pro-zessor | RAM |
Takt	2		2		ROM
	3		3		
	5		5	CPU	
Komm.	7		7		EEPROM
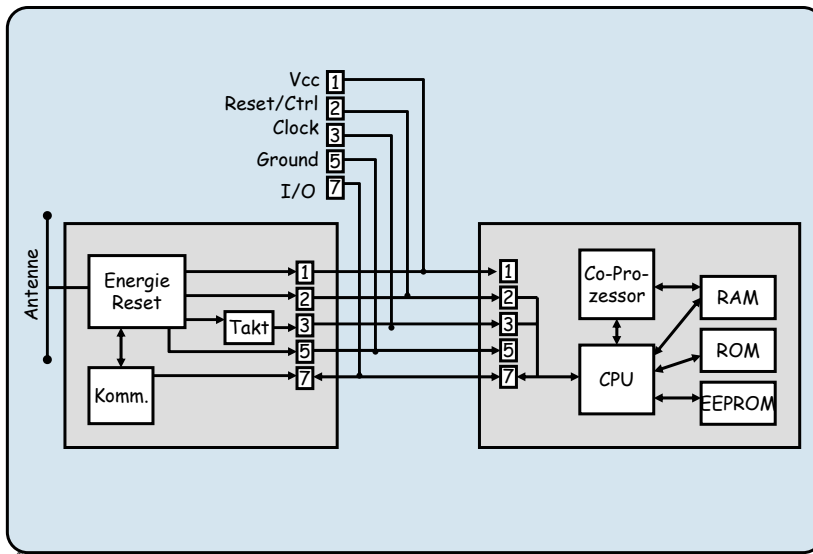
Kommunikation Karte/Terminal

Smart Card Communication

© M. Leischner

Overview: Smart Card Data Transfer

Terminal   Smart Card

"Master"
"Client"

"Slave"
"Server"

Reset

ATR (Answer to Reset)

[PTS necessary] PTS-Requ

PTS-Resp

command 1

response 1

command 2

response 2

© M. Leischner

Layered Communication Model for Smart Card Data Transfer

OSI	layer	specification
OSI layer 7 transfer of application data	application layer	ISO/IEC 7816-4 EMV GSM 11.11, ...
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
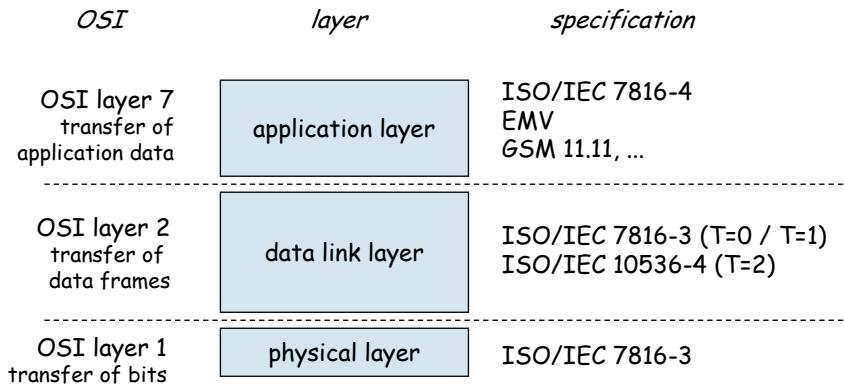
© M. Leischner

Activation Sequence and Reset

Terminal   Smart Card

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

Reset

ATR (Answer to Reset)

[PTS necessary] PTS-Requ

PTS-Resp

command 1

response 1

command 2

response 2
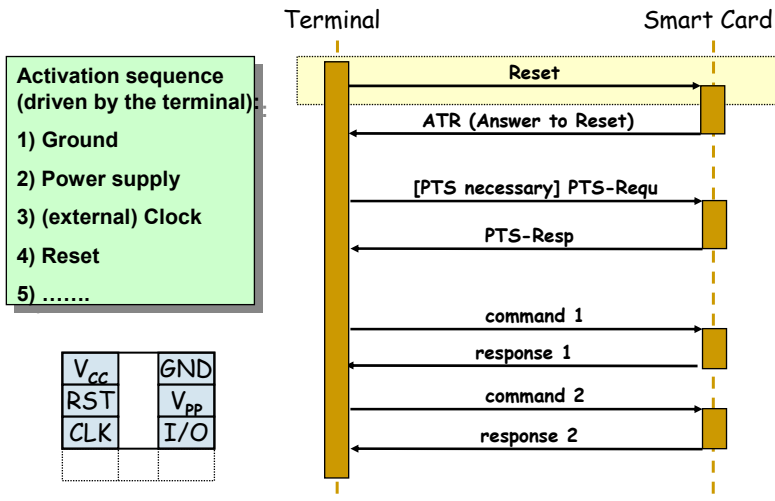
© M. Leischner

Physical Layer - Transmitting a Bit

```
┌─────────────────────────────┐                    ╭──────────────────────────────╮
│         terminal            │                    │         smart card           │
│  ┌──────────────────────┐   │    Clock           │   ┌──────────────────────┐   │
│  │ external clock       │   │ ────────────────►  │   │     divider          │   │
│  │ (typical:            │   │                    │   │ (typical by 372)     │   │
│  │ 3,571200 MHz)        │   │                    │   └──────────────────────┘   │
│  └──────────────────────┘   │                    │            │                 │
│                             │       I/O          │            ▼                 │
│         ┌───────┐           │ ◄────────────────► │      ┌───────┐               │
│         │  I/O  │           │                    │      │  I/O  │               │
│         └───────┘           │                    │      └───────┘               │
└─────────────────────────────┘                    ╰──────────────────────────────╯
```
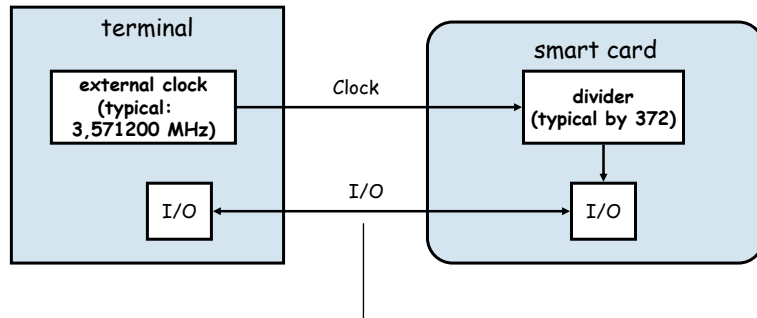
data transmission rate = 3571200 / 372 = 9600 bit/s

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

Transmission of a Character (Byte)

Answer to Reset

terminal   smart card

Reset

ATR (Answer to Reset)

[PTS necessary] PTS-Requ

PTS-Resp

command 1

response 1

command 2

response 2
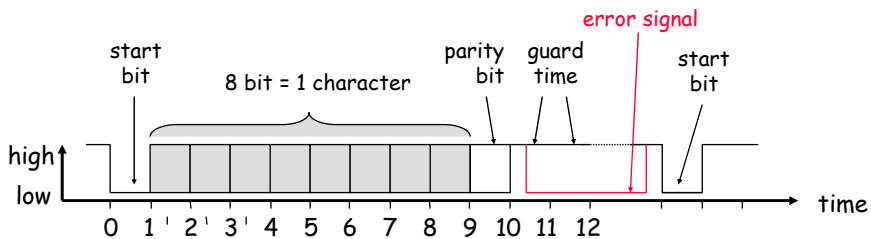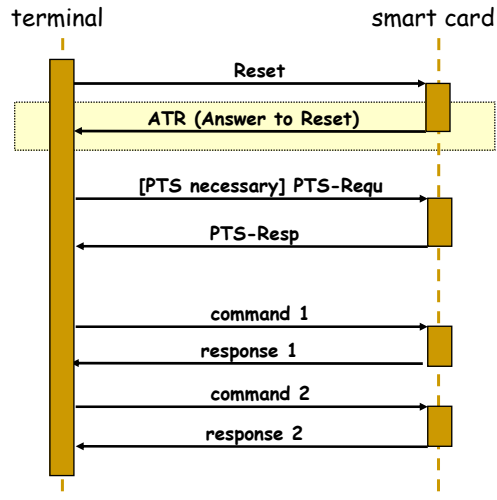
© M. Leischner

An Example of an ATR (Answer to Reset)

The ATR of the enhanced BasicCard ZC3.9:

0 means "divider = 372" --> work etu = 372 / $f_{terminal}$

3B EF 00 FF 81 31 20 75 | 42 61 73 69 63 43 61 72 64 20 5A 43 33 2E 39 | 86

$F_{16} = 1111_2 = 15_{10}$

3B = direct convention
(3F = inverse convention)

"BasicCard ZC3.9"

15 historical characters
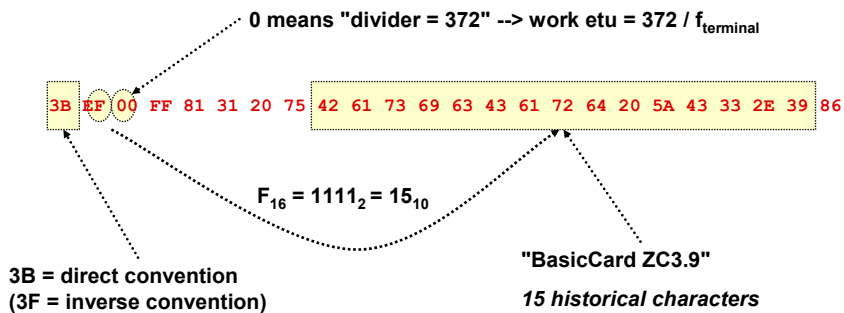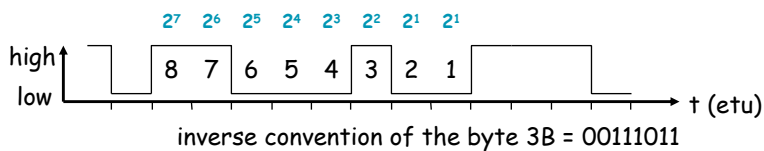
more about the ATR: practice with Martina Kannen

© M. Leischner

Aufbau ATR – Basic Structure of ATR
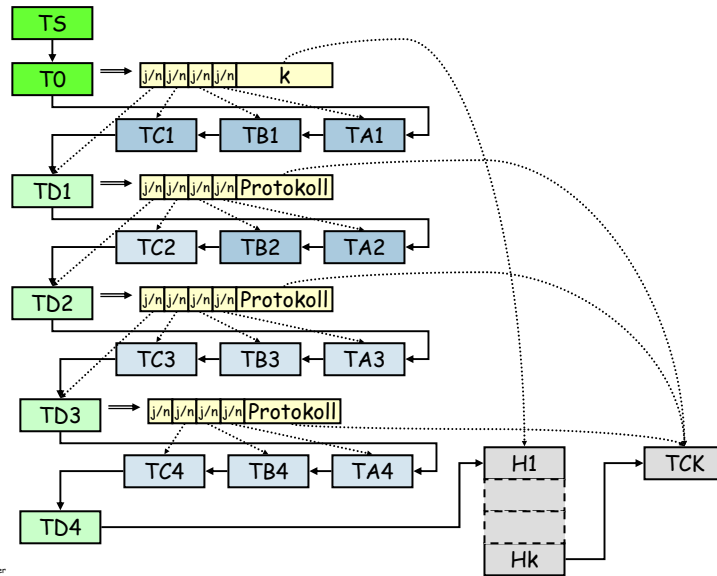
© M. Leischner

direct/inverse convention

2^0 2^1 2^2 2^3 2^4 2^5 2^6 2^7

high

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

low

t (etu)

direct convention of the byte 3B = 00111011)

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^1

high

| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

low

t (etu)

inverse convention of the byte 3B = 00111011
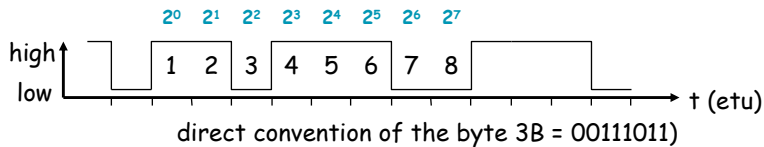
© M. Leischner

Protocol Type Selection

Terminal — Smart Card

- Reset
- ATR (Answer to Reset)
- [PTS necessary] PTS-Requ
- PTS-Resp
- command 1
- response 1
- command 2
- response 2
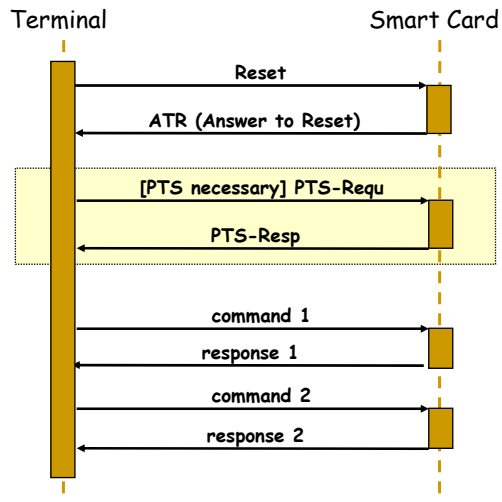
© M. Leischner

Sending a Command

Terminal — Smart Card

- Reset
- ATR (Answer to Reset)
- [PTS necessary] PTS-Requ
- PTS-Resp
- command 1
- response 1
- command 2
- response 2
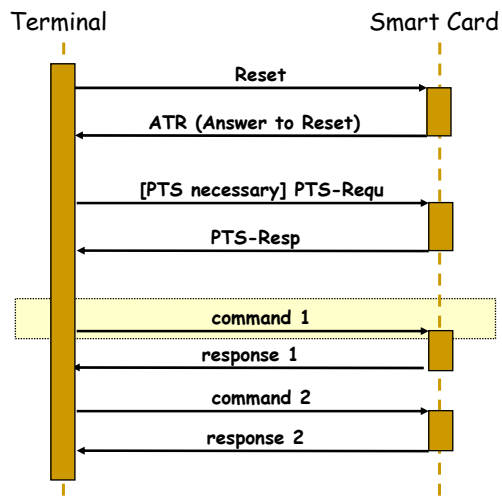
© M. Leischner

Structure of a T1 Transfer Block

NAD	PCB	LEN	APDU	EDC
1 Byte	1 Byte	1 Byte	2 .. 254 Byte	1..2 Byte

- NAD: node address
- PCB: protocol control byte
- LEN: length field
- APDU: information field
- EDC: error dection code

prolog — command APDU — epilog
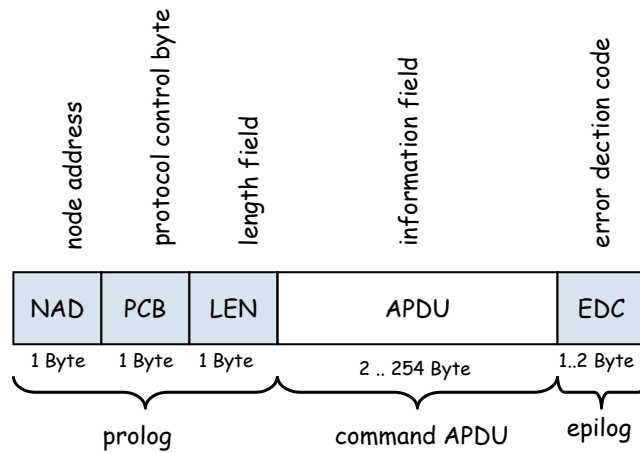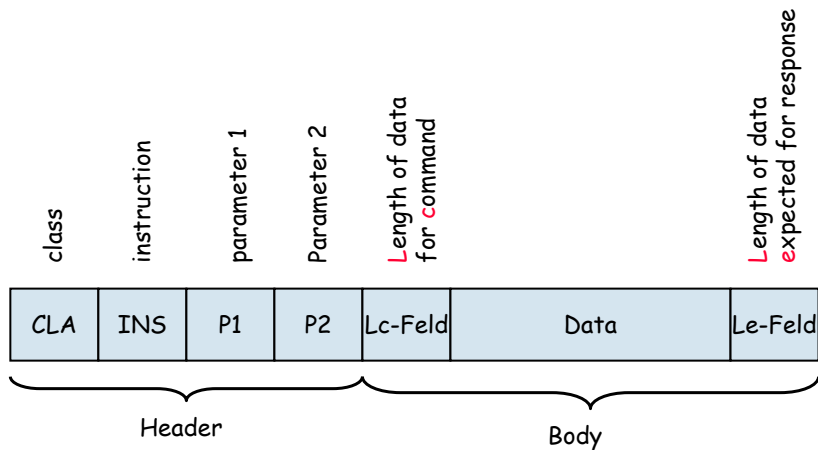
The T1 protocol offers a transparent, block-oriented, asynchronous half-duplex protocol with error handling

© M. Leischner

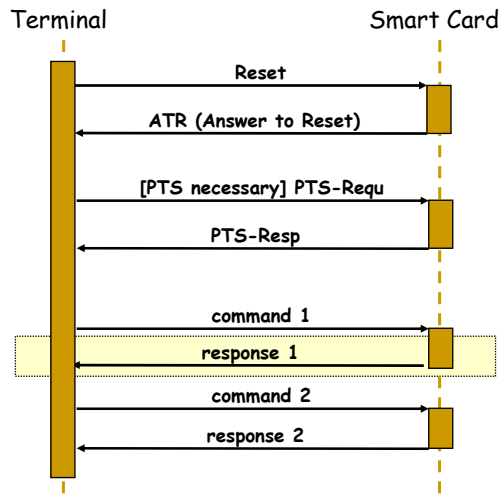# Structure of a Command APDU

CLA	INS	P1	P2	Lc-Feld	Data	Le-Feld

- CLA: class
- INS: instruction
- P1: parameter 1
- P2: Parameter 2
- Lc-Feld: Length of data for command
- Le-Feld: Length of data expected for response

Header — Body

© M. Leischner

Sending a Response

```
      Terminal                        Smart Card
         |                                 |
         |------------ Reset ------------->|■
         |<------- ATR (Answer to Reset) --|
         |                                 |
         |---- [PTS necessary] PTS-Requ -->|■
         |<--------- PTS-Resp -------------|
         |                                 |
         |---------- command 1 ---------->|■
         |<--------- response 1 -----------|
         |---------- command 2 ---------->|■
         |<--------- response 2 -----------|
         |                                 |
```

Structure of a Response-APDU

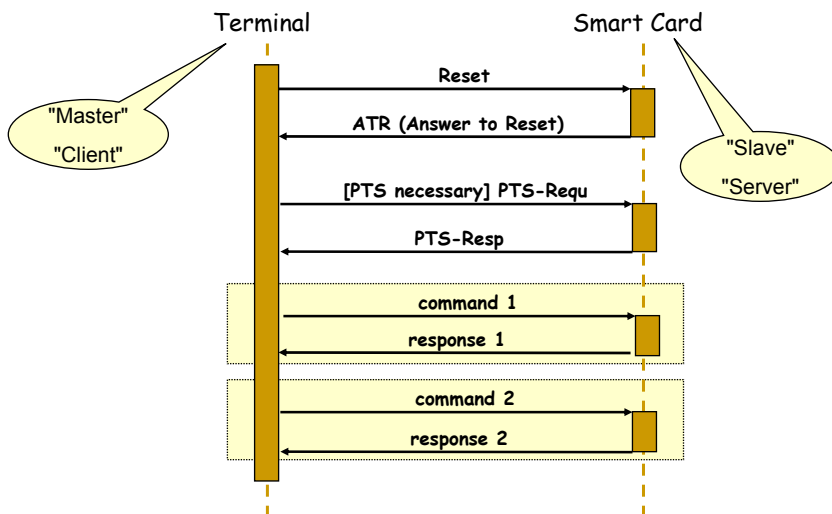| Data	SW1	SW2
	status word 1	status word 2
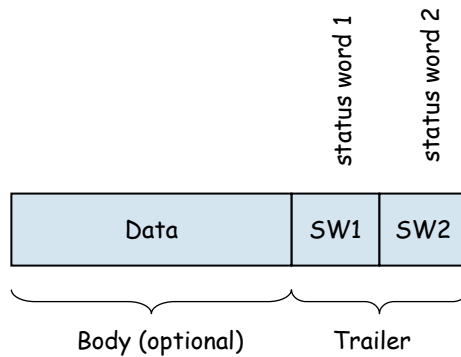
Body (optional)   Trailer

Classification Scheme for the Return Code (SW1, SW2)
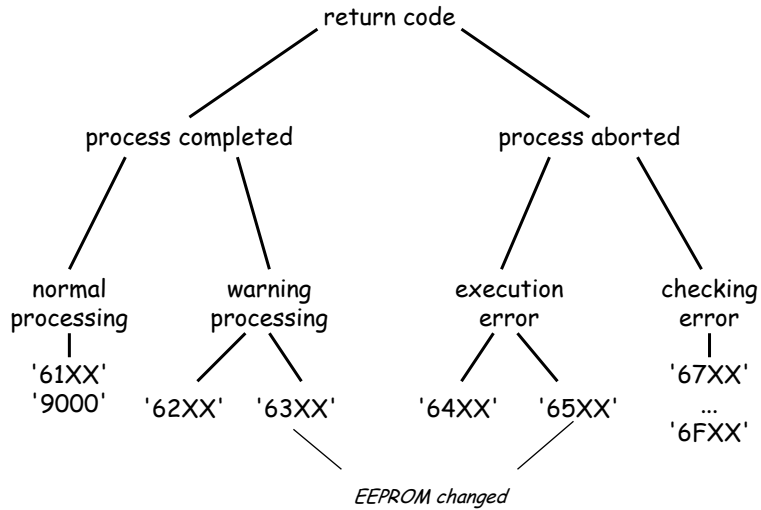
© M. Leischner

Master / Slave Communication

© M. Leischner

ENDE

END