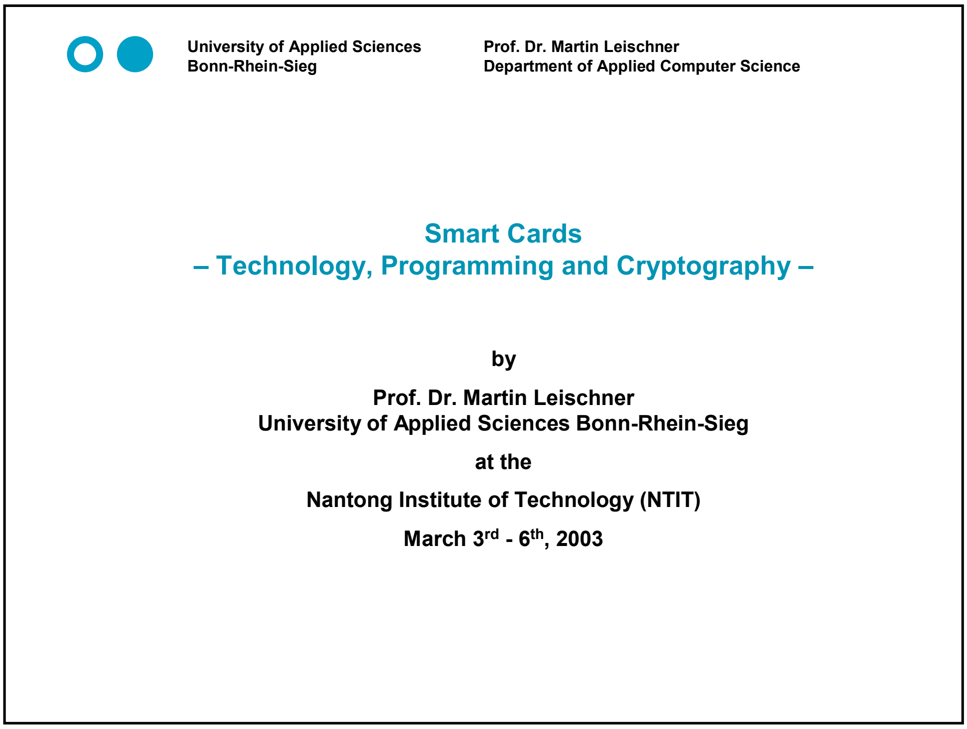


Smart Cards
– Technology, Programming and Cryptography –

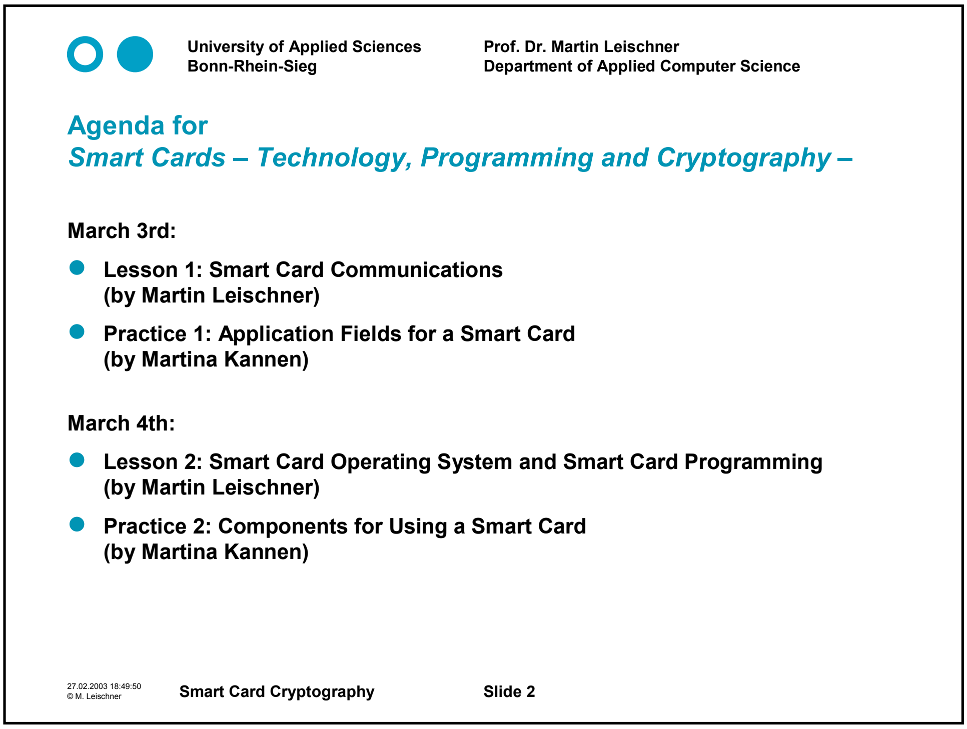
by

Prof. Dr. Martin Leischner
University of Applied Sciences Bonn-Rhein-Sieg

at the

Nantong Institute of Technology (NTIT)

March 3rd - 6th, 2003



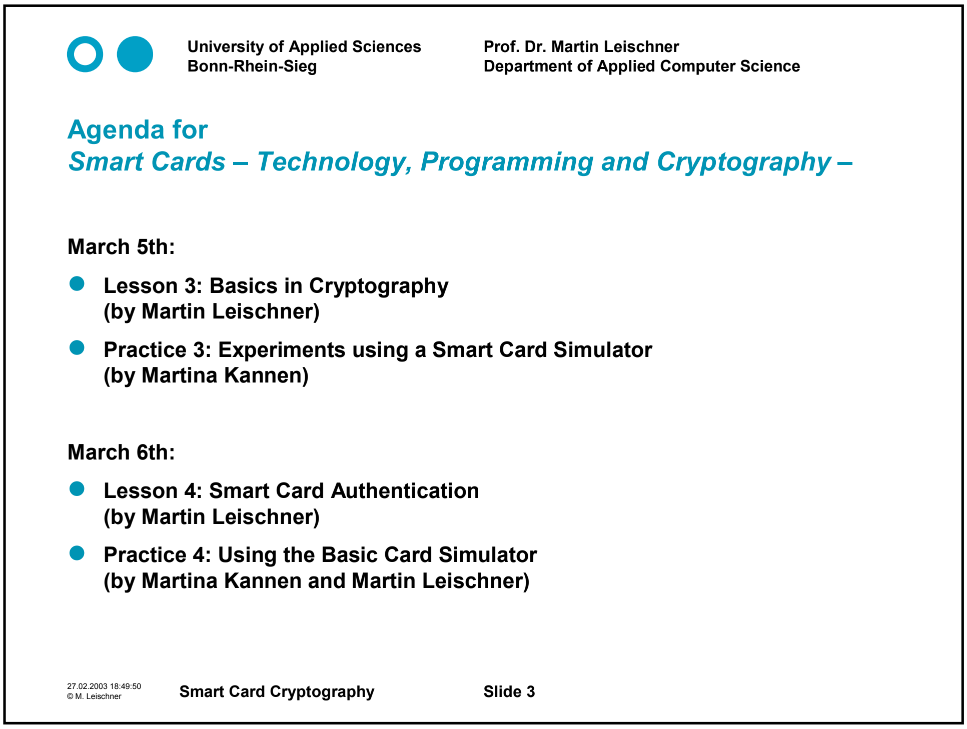
Agenda for
Smart Cards – Technology, Programming and Cryptography –

March 3rd:

- Lesson 1: Smart Card Communications
  (by Martin Leischner)
- Practice 1: Application Fields for a Smart Card
  (by Martina Kannen)

March 4th:

- Lesson 2: Smart Card Operating System and Smart Card Programming
  (by Martin Leischner)
- Practice 2: Components for Using a Smart Card
  (by Martina Kannen)



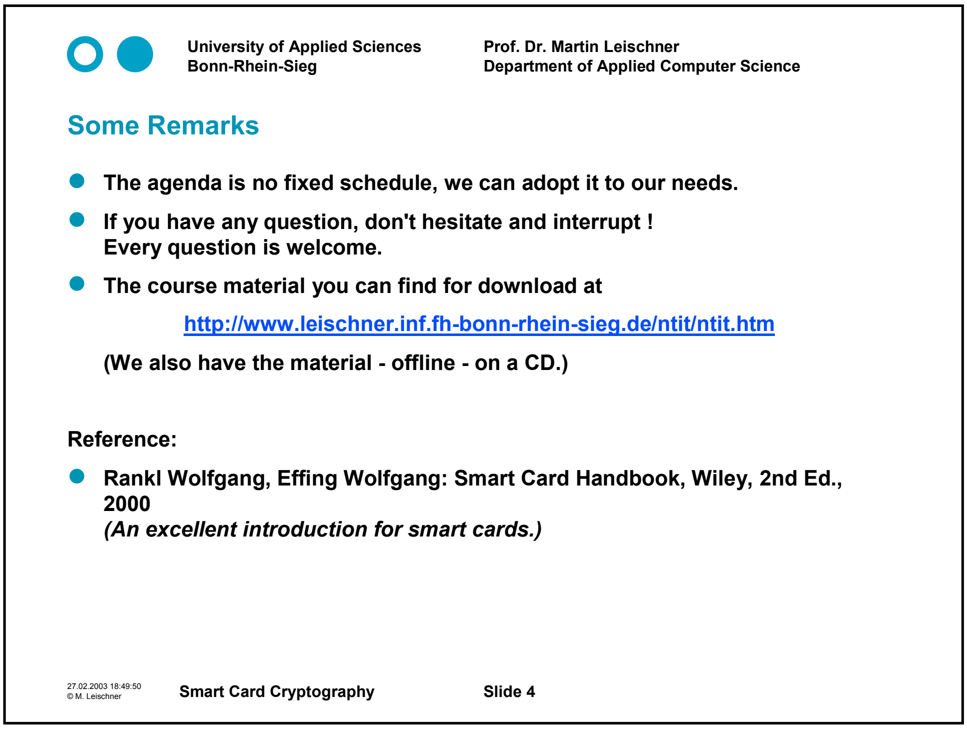
Agenda for *Smart Cards – Technology, Programming and Cryptography –*

March 5th:

- Lesson 3: Basics in Cryptography
  (by Martin Leischner)
- Practice 3: Experiments using a Smart Card Simulator
  (by Martina Kannen)

March 6th:

- Lesson 4: Smart Card Authentication
  (by Martin Leischner)
- Practice 4: Using the Basic Card Simulator
  (by Martina Kannen and Martin Leischner)



Some Remarks

- The agenda is no fixed schedule, we can adopt it to our needs.
- If you have any question, don't hesitate and interrupt !
  Every question is welcome.
- The course material you can find for download at

  http://www.leischner.inf.fh-bonn-rhein-sieg.de/ntit/ntit.htm

  (We also have the material - offline - on a CD.)

Reference:

- Rankl Wolfgang, Effing Wolfgang: Smart Card Handbook, Wiley, 2nd Ed., 2000
  (An excellent introduction for smart cards.)

Introduction: Smart Card Basics

Just the very basics

Application Fields of a Smart Card

- **Public Card Phones:**
  substituting coin operated telephones
- **Mobile Communications:**
  personal SIM card enabling the use of numerous mobile phones by the same user.
- **Banking & Retail:**
  an effective method of combating fraud and credit card theft.
- **Electronic Purse:**
  providing a rechargeable or disposable card containing electronic cash.
- **Public Transport Cards:**
  no more need for paper tickets
- **Digital Signatures:**
  for E-Business

For more information and examples:
--> see exercise given by Martina Kannen

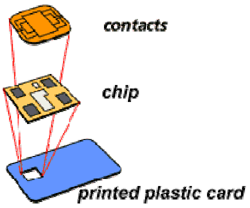
What is a Smart Card ?

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.

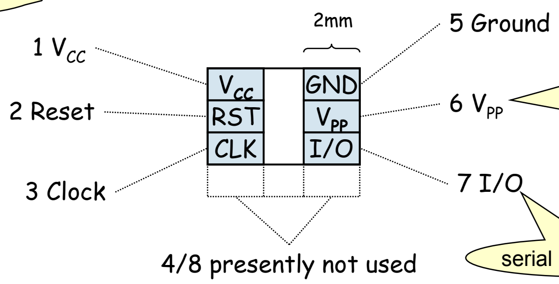


25 March 1974:

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

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

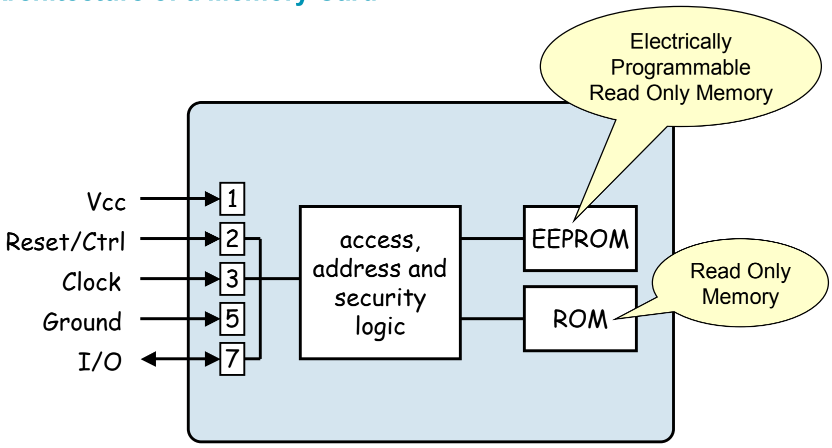
supply voltage
(3-)5V



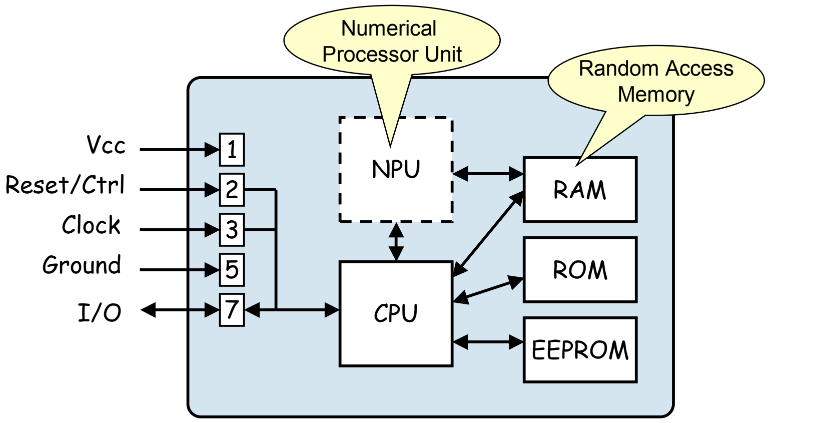
programming voltage (no longer used)

serial input/output

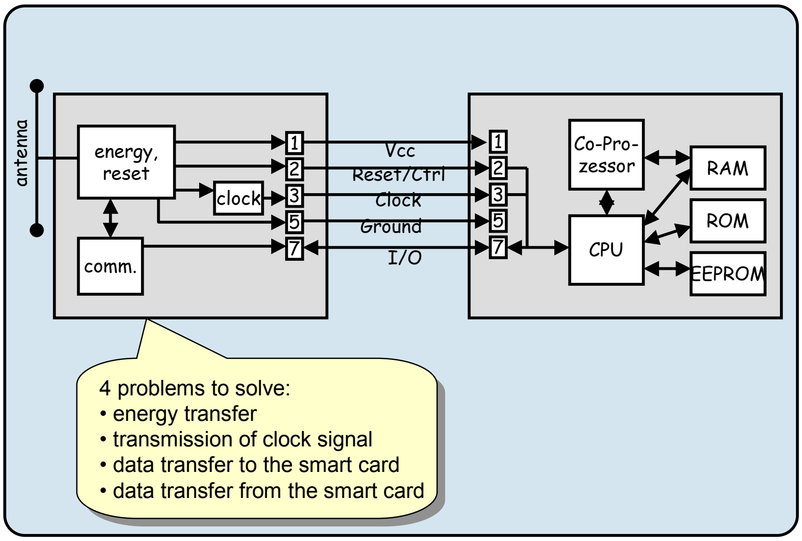
Architecture of a Memory Card


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

Architecture of a Microprocessor Card



Architecture of a Contactless Microprocessor Card

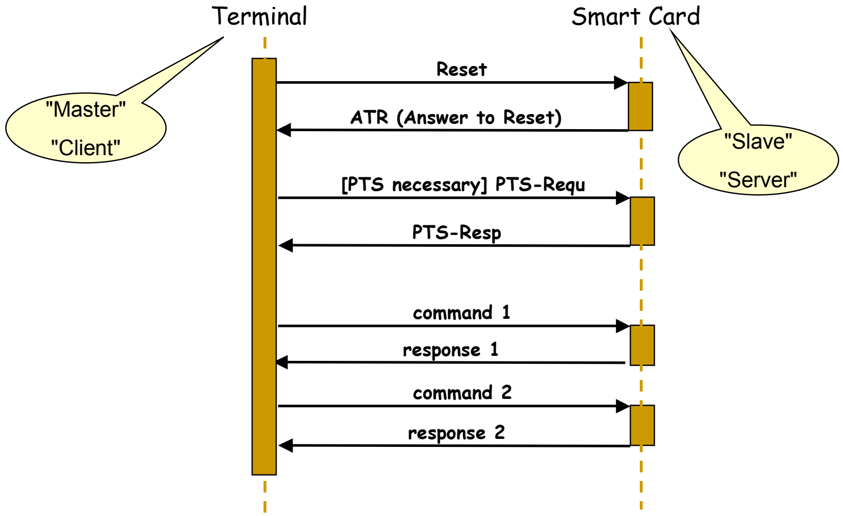


4 problems to solve:
- energy transfer
- transmission of clock signal
- data transfer to the smart card
- data transfer from the smart card

Lesson 1: Smart Card Communication

- Overview: Smart Card Data Transfer
- Activation Sequence and Reset
- Physical Layer - Transmitting a Bit
- Data Link Layer - Transmitting a Frame
- Application Layer - Transmitting a Commands

Overview: Smart Card Data Transfer



Layered Communication Model for Smart Card Data Transfer

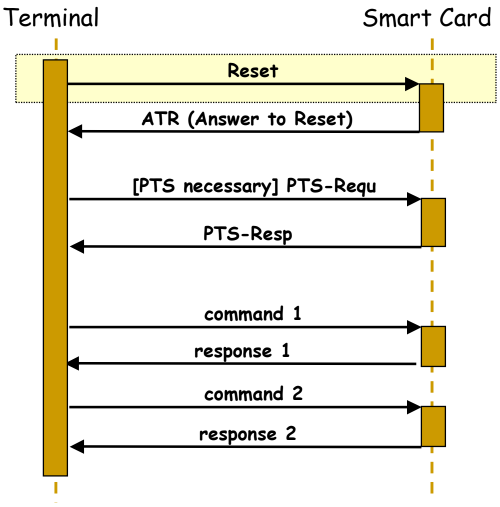
OSI	*layer*	*specification*
OSI layer 7 transfer of application data	application layer	ISO/IEC 7816-4 EMV GSM 11.11, ...
OSI layer 2 transfer of data frames	data link layer	ISO/IEC 7816-3 (T=0 / T=1) ISO/IEC 10536-4 (T=2)
OSI layer 1 transfer of bits	physical layer	ISO/IEC 7816-3

Activation Sequence and Reset

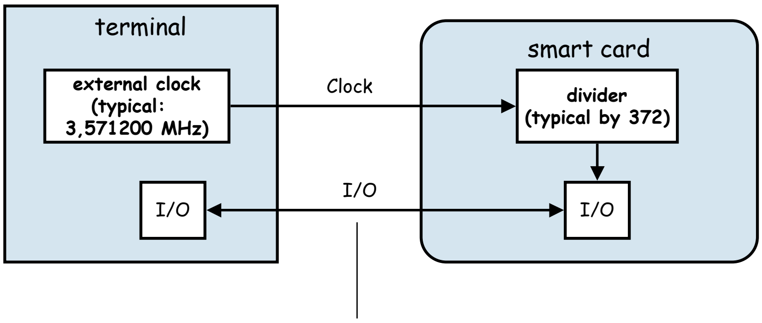
Activation sequence (driven by the terminal):

1) Ground
2) Power supply
3) (external) Clock
4) Reset
5) ....

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



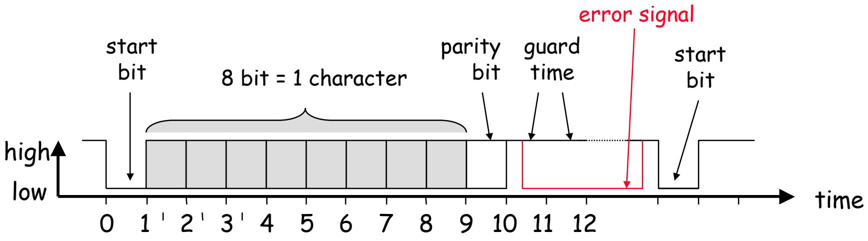
Physical Layer - Transmitting a Bit



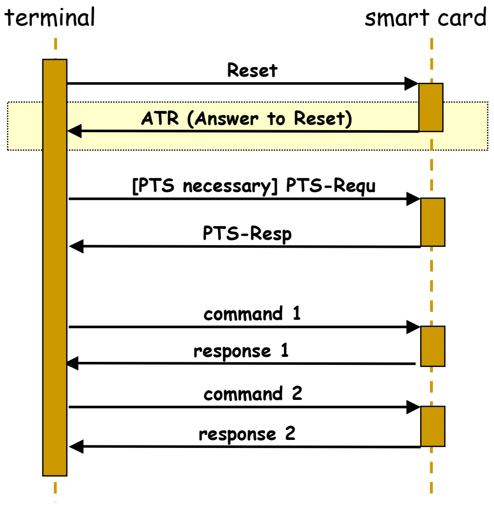
data transmission rate = 3571200 / 372 = 9600 bit/s

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

Transmission of a Character (Byte)

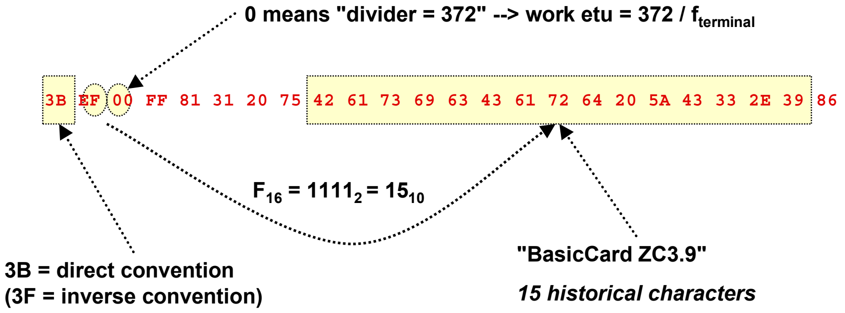


Answer to Reset



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
```

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

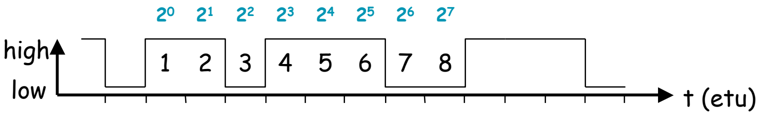
3B = direct convention
(3F = inverse convention)

"BasicCard ZC3.9"

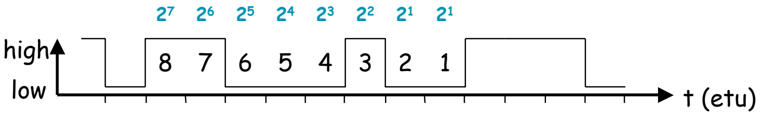
15 historical characters

more about the ATR: practice with Martina Kannen

direct/inverse convention

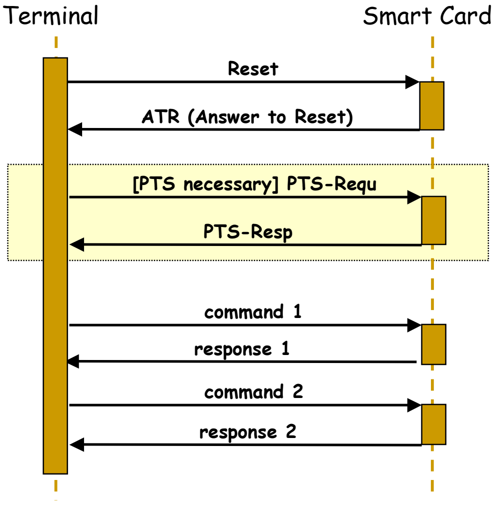


direct convention of the byte 3B = 00111011)

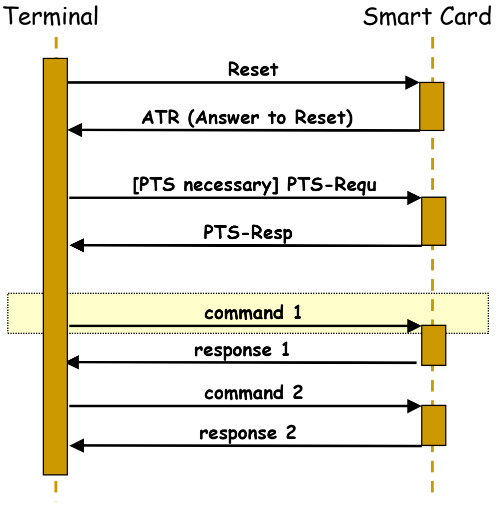


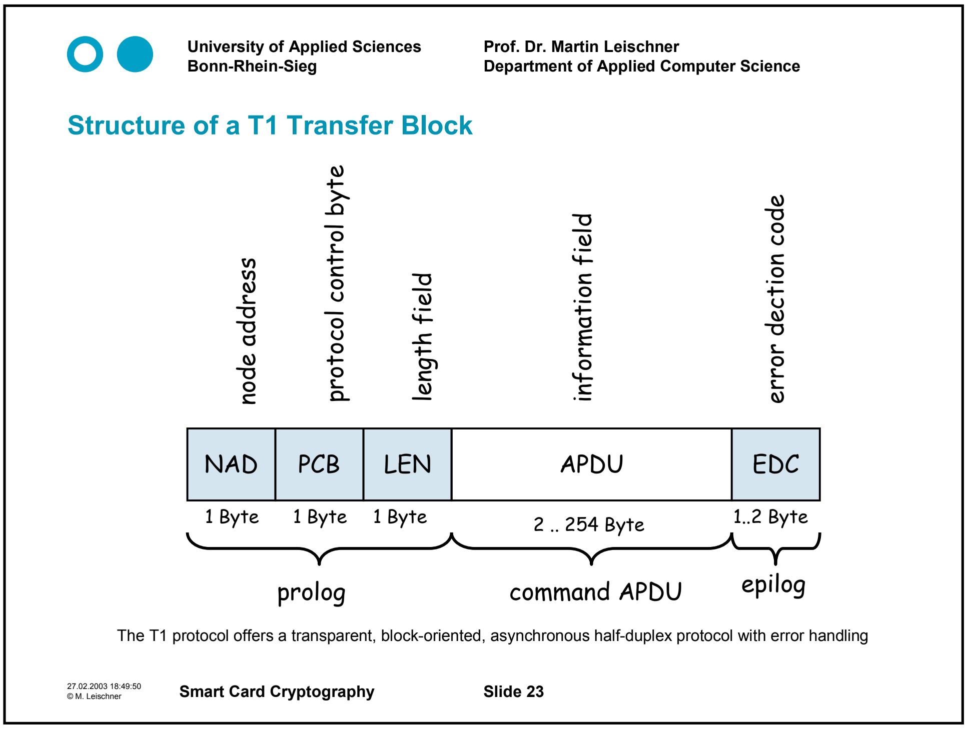
inverse convention of the byte 3B = 00111011

Protocol Type Selection



Sending a Command





University of Applied Sciences
Bonn-Rhein-Sieg

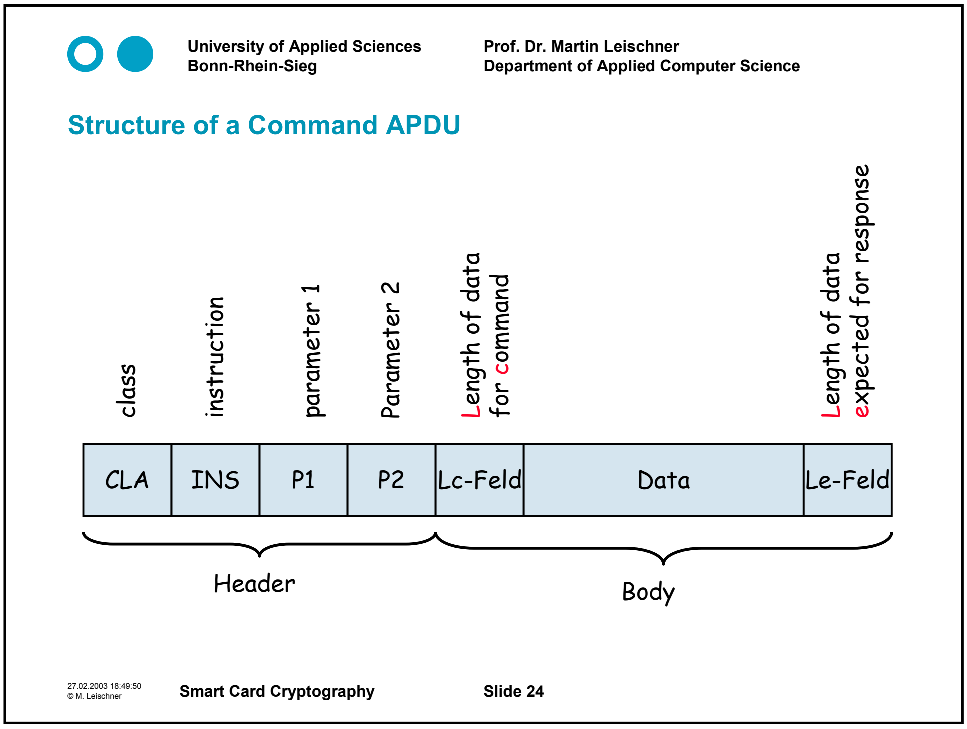
Prof. Dr. Martin Leischner
Department of Applied Computer Science

Structure of a T1 Transfer Block

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

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

27.02.2003 18:49:50
© M. Leischner



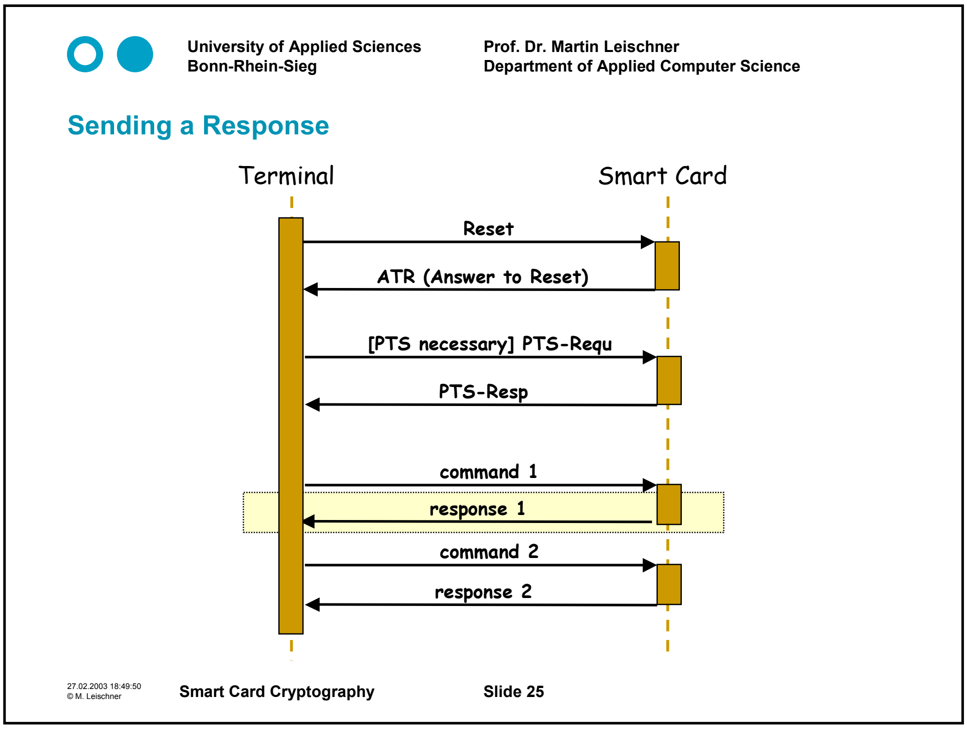
University of Applied Sciences
Bonn-Rhein-Sieg

Prof. Dr. Martin Leischner
Department of Applied Computer Science

Structure of a 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		

27.02.2003 18:49:50
© M. Leischner



Sending a Response

Terminal

Smart Card

Reset

ATR (Answer to Reset)

[PTS necessary] PTS-Requ

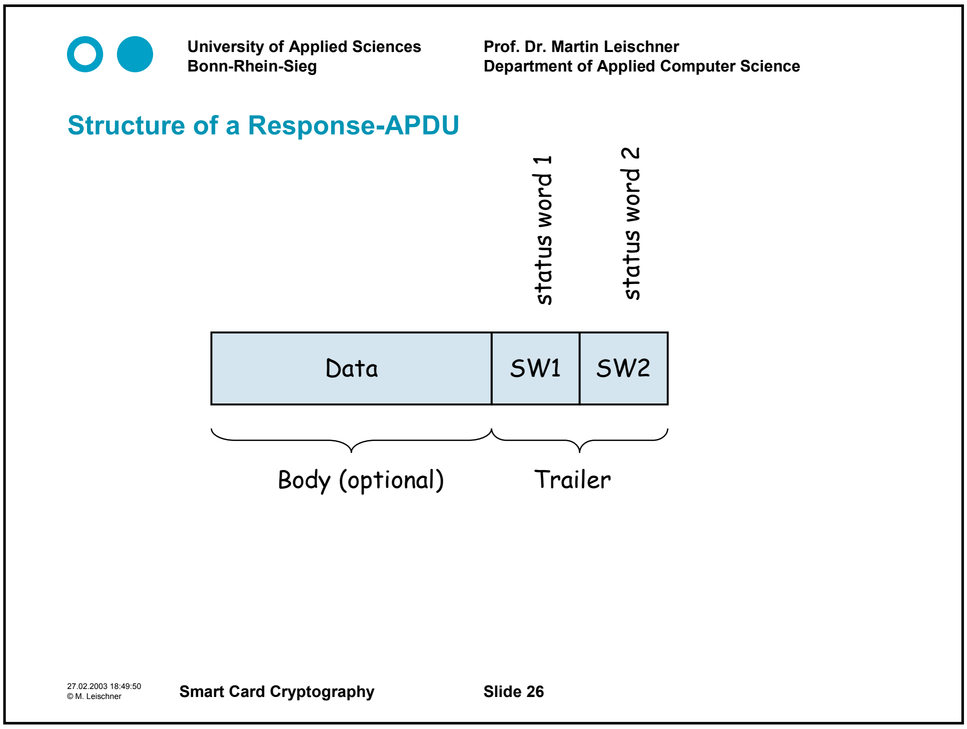
PTS-Resp

command 1

response 1

command 2

response 2



Structure of a Response-APDU

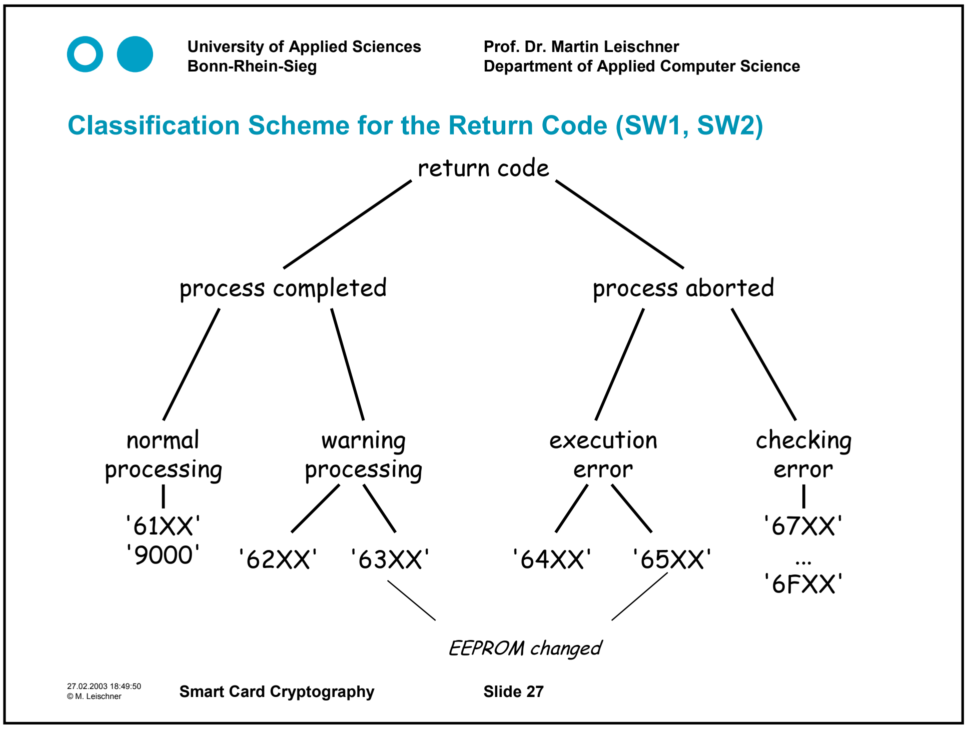
status word 1

status word 2

Data	SW1	SW2

Body (optional)

Trailer



Classification Scheme for the Return Code (SW1, SW2)

return code

process completed

process aborted

normal processing

'61XX'
'9000'

warning processing

'62XX'

'63XX'

execution error

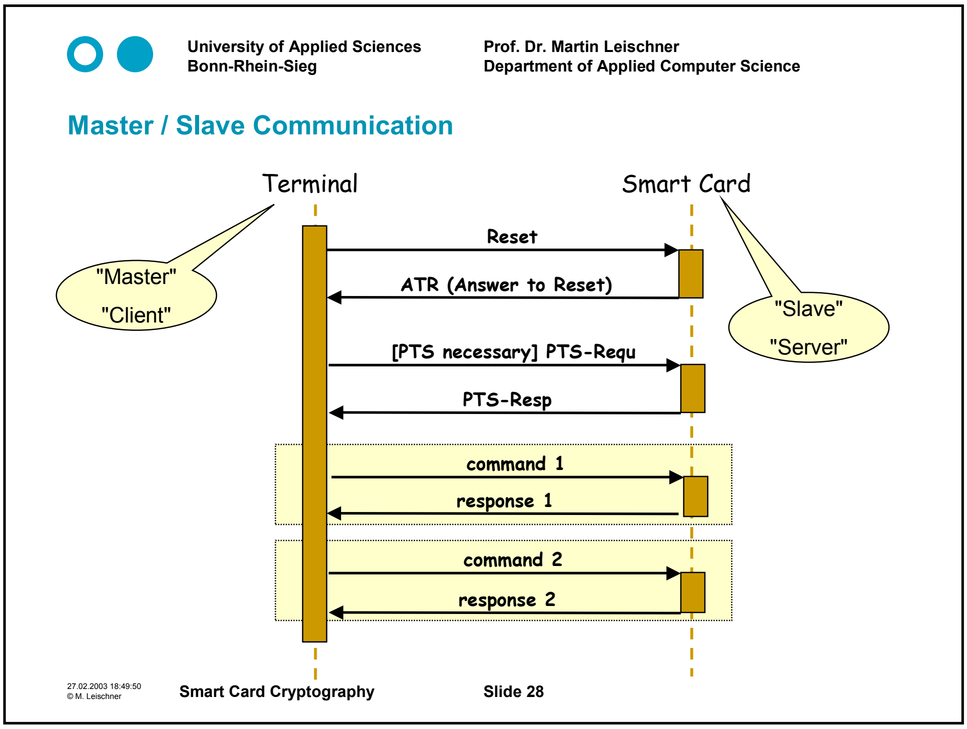
'64XX'

'65XX'

checking error

'67XX'
...
'6FXX'

EEPROM changed



Master / Slave Communication

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