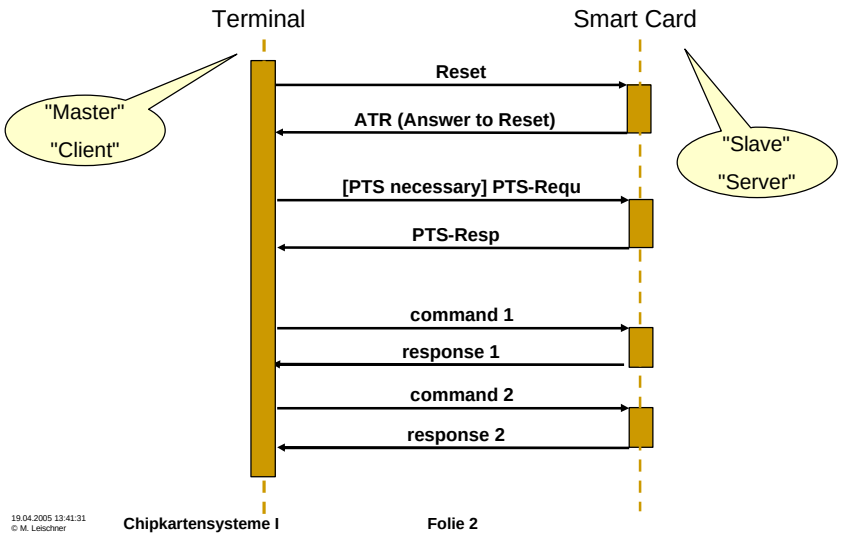
Modul 3

Kommunikation Karte/Terminal

Grundschema Chipkarten-Protokoll

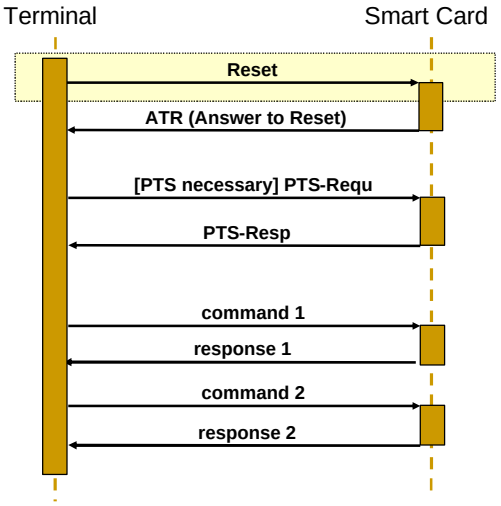


Activation Sequence and Reset

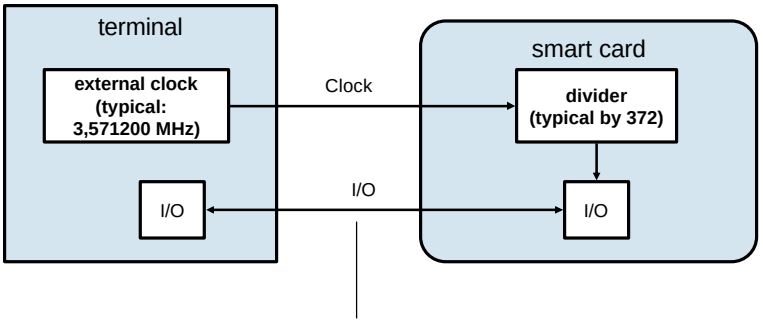
Activation sequence (driven by the terminal):

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

etu (elementary time unit)

Definition

- **1 etu (elementary time unit) =**
  Zeitdauer für die Übertragung eines Bits in Abhängigkeit von Taktfrequenz, einem Umrechnungsfaktor ("Teiler") und einem Justierfaktor.

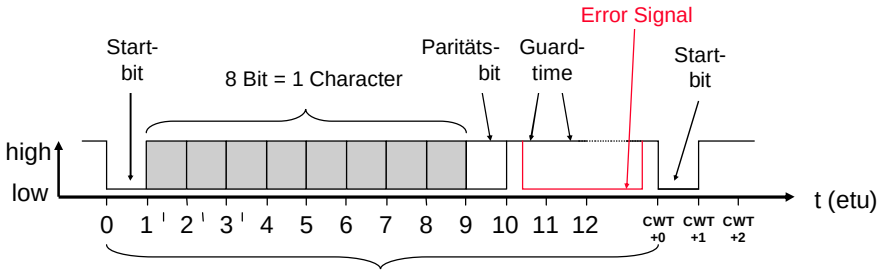
$$1\ etu = \frac{F}{D} \cdot \frac{1}{f}$$

F = Umrechnungsfaktor (*clock rate conversion factor*, "Teiler"): Standardwert = 372

D = Justierfaktor (*baud rate adjustment factor*): Standardwert =1

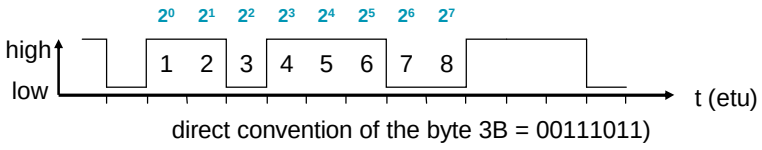
f = Taktfrequenz (*frequency*): Standardwert =3,571200 MHz

Übertragung eines Zeichens

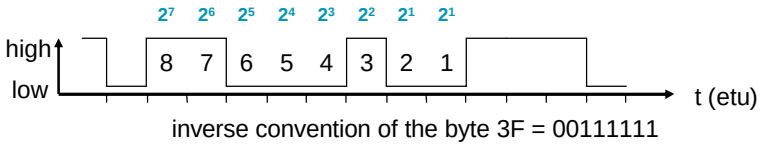


mindestens 12 Bitzeiten, d.h. Guardtime=2

direct/inverse convention

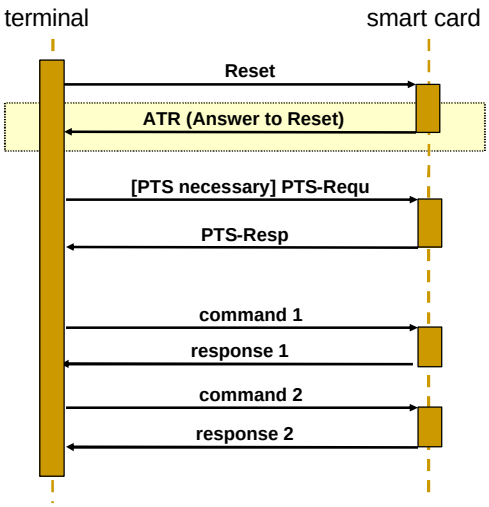


direct convention of the byte 3B = 00111011)



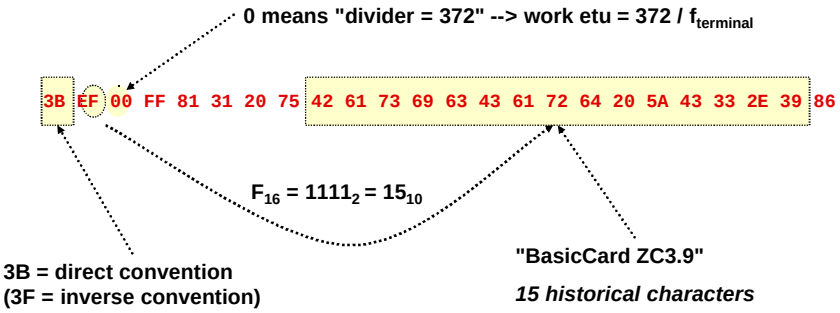
inverse convention of the byte 3F = 00111111

Answer to Reset

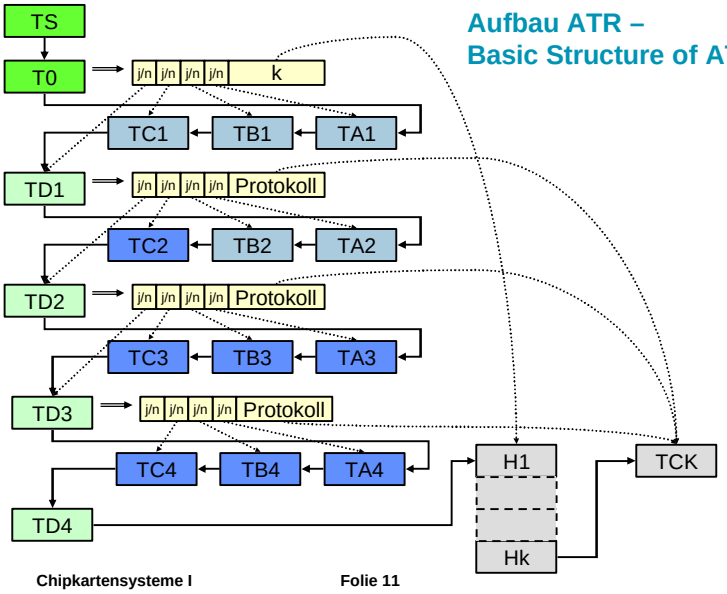


An Example of an ATR (Answer to Reset)

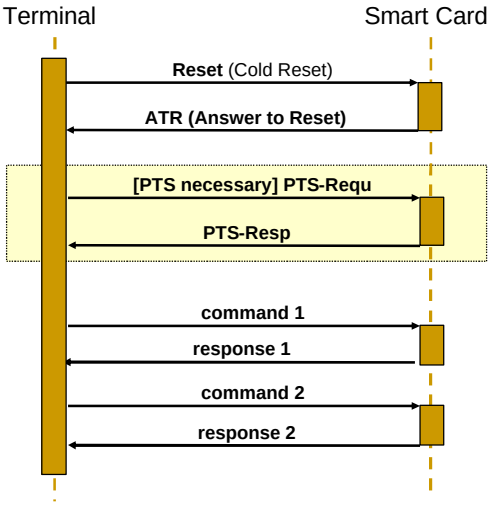
The ATR of the enhanced BasicCard ZC3.9:



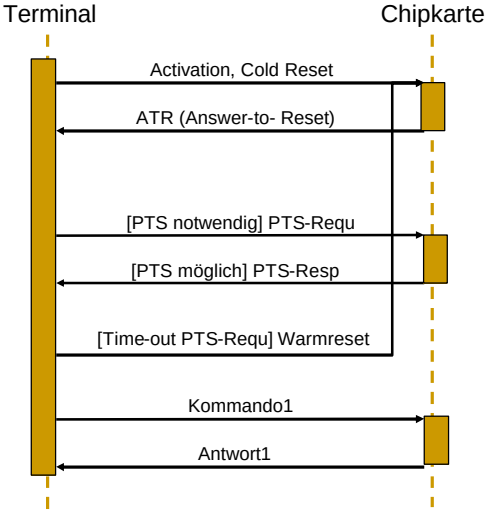
Aufbau ATR – Basic Structure of ATR



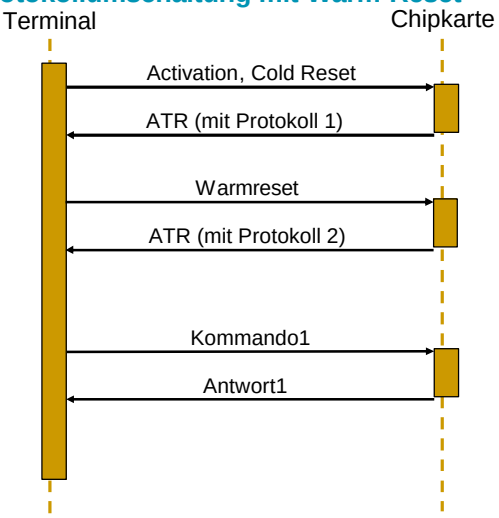
Protocol Type Selection



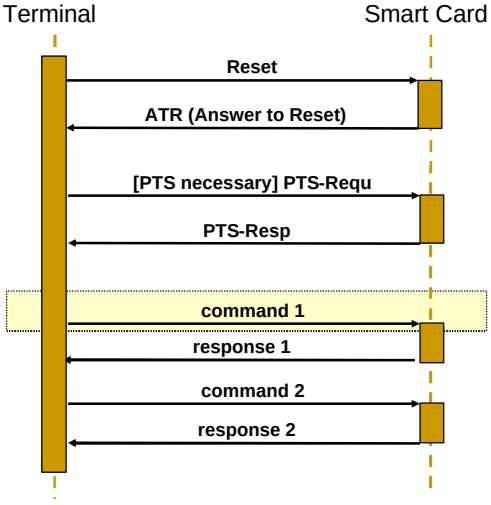
Initialisierungsprotokoll (ATR und PTS)



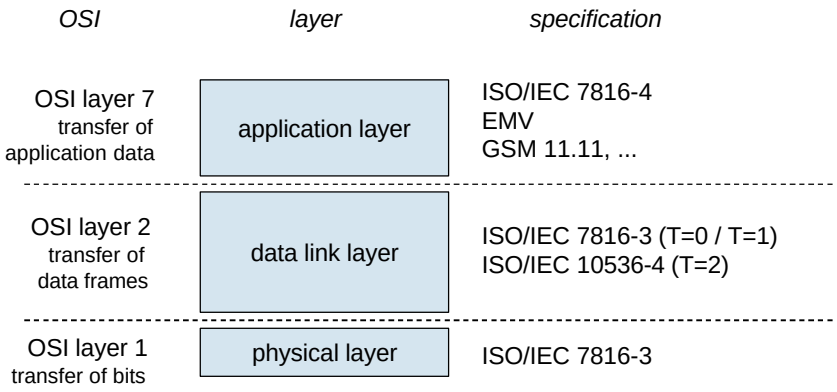
Scenario: Protokollumschaltung mit Warm-Reset



Sending a Command



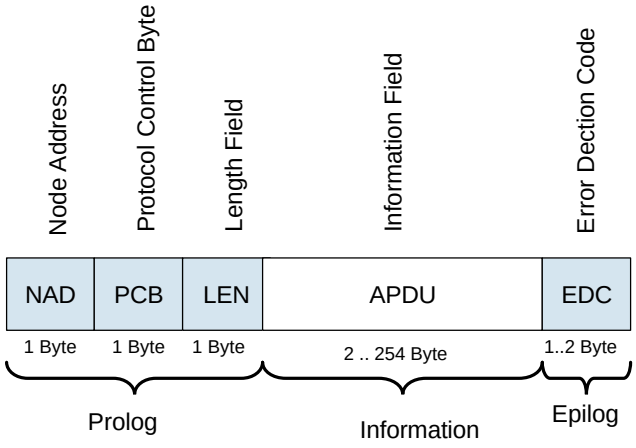
Layered Communication Model for Smart Card Data Transfer



Transmission Layer (Data Link Layer, Übertragungsschicht)

Protokoll	Norm	Bedeutung
T=0	ISO/IEC 7816-3	halbduplex, asynchron byteorientiert
T=1	ISO/IEC 7816-3	halbduplex, asynchron blockorientiert
T=2		vollduplex, asynchron blockorientiert (in Normierung)
T=3		vollduplex
T=4		halbduplex, asynchron byteorientiert Erweiterung von T=0
T=14		

Aufbau T1-Übertragungsblock

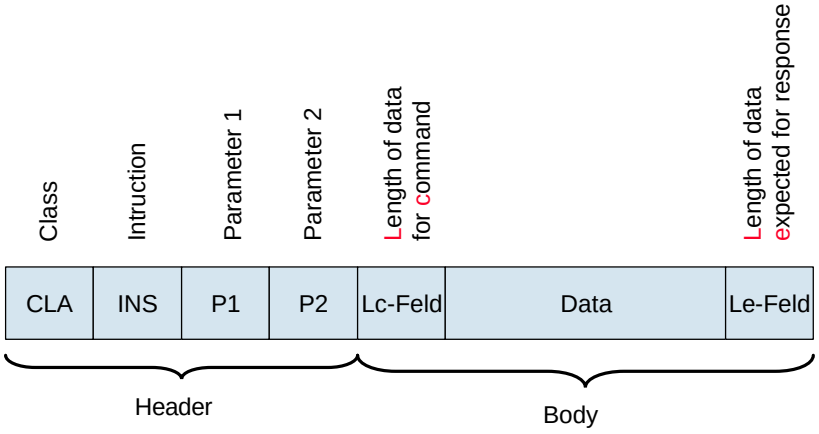


T1-Protokoll

- **Timing**
  - **Zeichenwartezeit (CWT):**
  - **Blockwartezeit (BWT)**
  - **Blockschutzzeit (BGT**
- **Blockverkettung:**
  Entspricht der Fragmentierung bei IP. (erlaubt nur bei I-Blöcken)
- **Fehlerbehandlung:**
  - **Längenprüfungscode (XOR-Verknüpfung, Standard für T=1 Implementierungen) o.**
  - **Ein CRC-Prüfsummenverfahren zum Teilerpolynom x**16+x**12+x*5+1**

  Zusätzlich wird noch ein Sendefolge/Empfangsfolgezähler modulo 2 eingesetzt.
- **Die Fehlerbehandlung in drei Eskalationsstufen:**
  - **Stufe 1: Bei Empfang eines fehlerhaften Blocks antworten mit einem R-Block, der die Wiederholung der Übertragung des letzten Blockes anfordert.**
  - **Stufe 2: Führt Stufe 1 nicht zum Erfolg, so wird über einen S-Block eine Resynchronisationsanfrage an den Sender geschickt.**
  - **Stufe 3: Auslösen eines Resets .**
  - **Stufe 4: Nach dreimaligen Versuch: Fehlermeldung.**

Aufbau command-APDU



4 Fälle der APDU-Struktur

Fall 1: Lc fehlt --> kein Datenfeld
Le fehlt --> keine Daten in Antwort (nur SW1, SW2)

Header

Fall 2: Lc fehlt --> kein Datenfeld

Header	Le-Feld

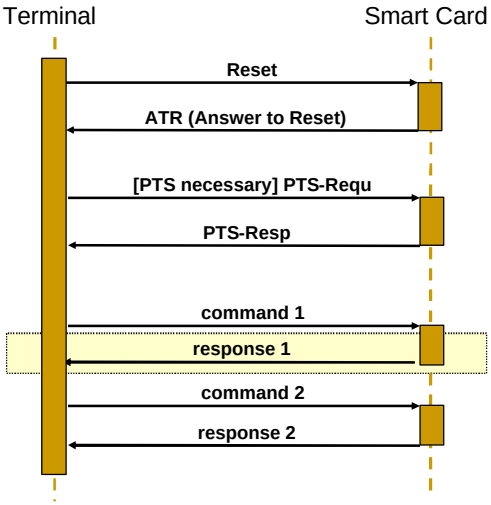
Fall 3: Le fehlt --> keine Daten in Antwort (nur SW1, SW2)

Header	Lc-Feld	Data

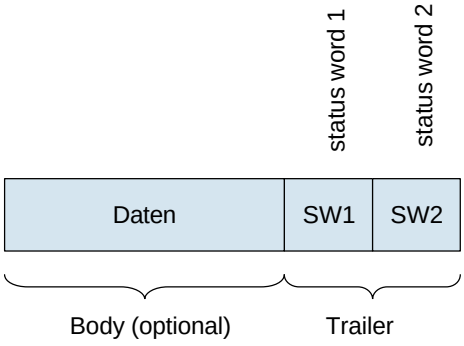
Fall 4: Daten in Kommando und Antwort

Header	Lc-Feld	Data	Le-Feld

Sending a Response



Aufbau Response-APDU



Classification Scheme for the Return Code (SW1, SW2)