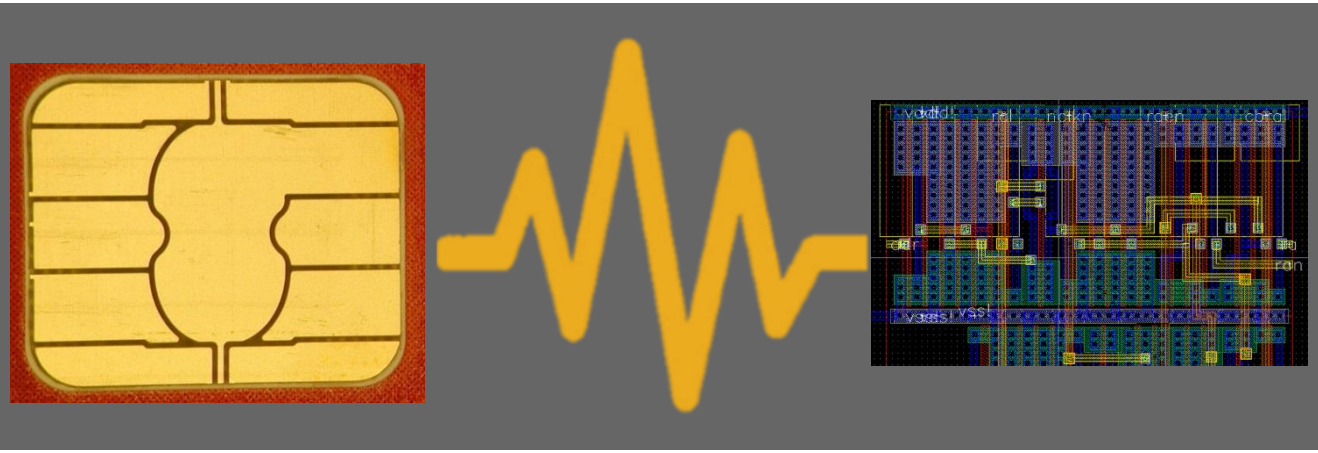
FROM RESEARCH TO INDUSTRY

cea tech

leti

SMARTCARD SECURITY

Charles GUILLEMET | ITSEF Technical Manager | 2016-2017
CEA Grenoble – charles.guillemet@cea.fr



LECTURES AGENDA

- L1: 26/10/2016 (Today) | 9:45 - 13:00
- L2: 07/12/2016 | 8:00 – 13:00
- L3: 14/12/2016 | 8:00 – 13:00
- L4: 11/01/2016 | 9:45 – 13:00

OVERVIEW OF LECTURE

- **What is a smart card?**
  - From the Design to the Application
- **Applications example :**
  - EMV
  - Mifare
- **Faults attacks**
- **Side channel analysis**

WHAT IS A SMARTCARD ?

- **Pocket-sized card**
  - With embedded integrated circuits
- **Communication**
  - Contact ISO 7816
  - Contactless ISO 14443

WHAT IS A SMARTCARD ?

- **Used for various applications**
  - Identification
  - Authentification
  - Data storage
  - Application processing

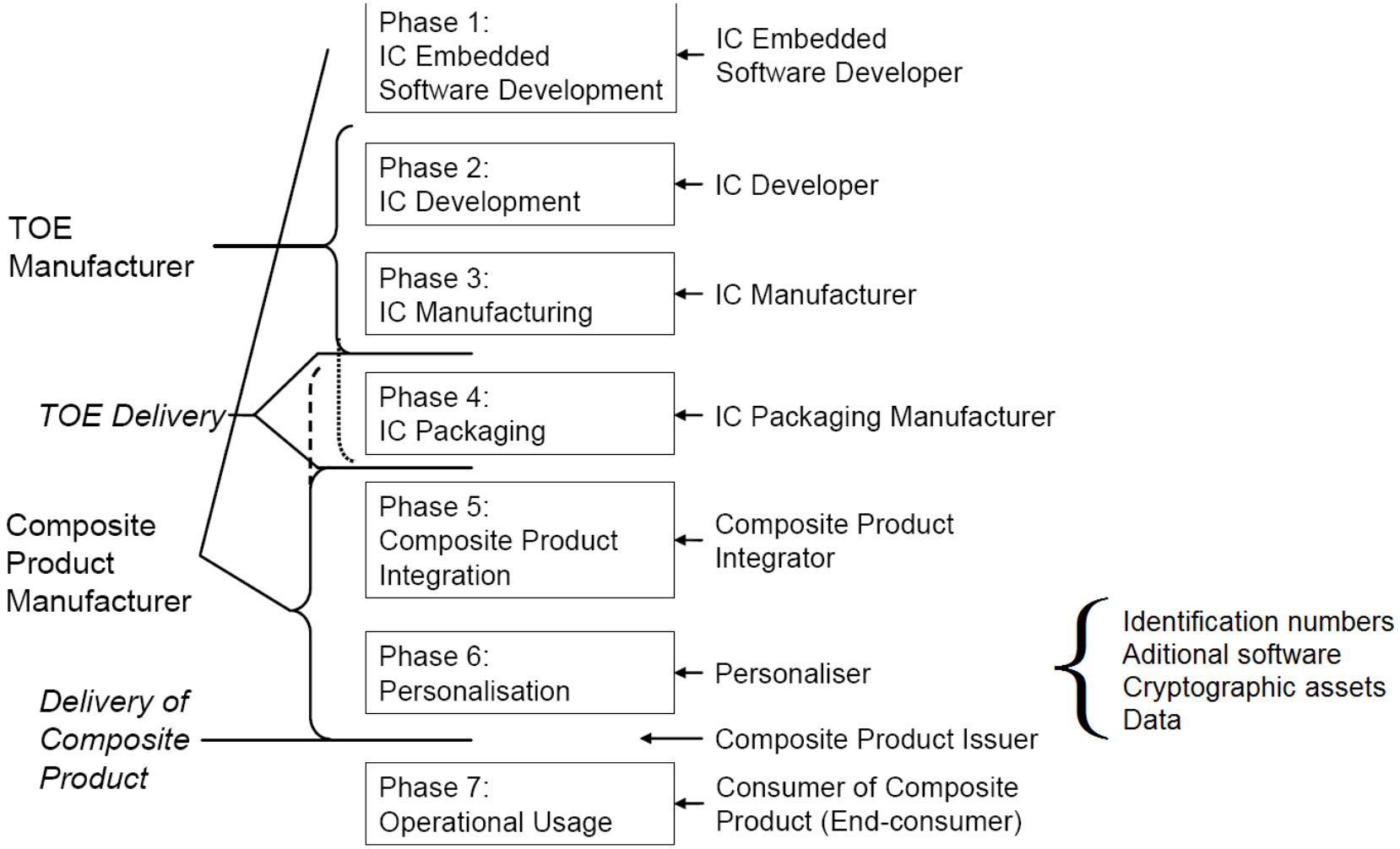
WHAT IS A SMARTCARD ?

- **Usage examples**
  - EMV cards
  - MIFARE tokens
  - Health Care cards
  - Ski resort Tokens
  - Passport
  - PayTV card
  - SIM cards
  - Public transportation
  - …

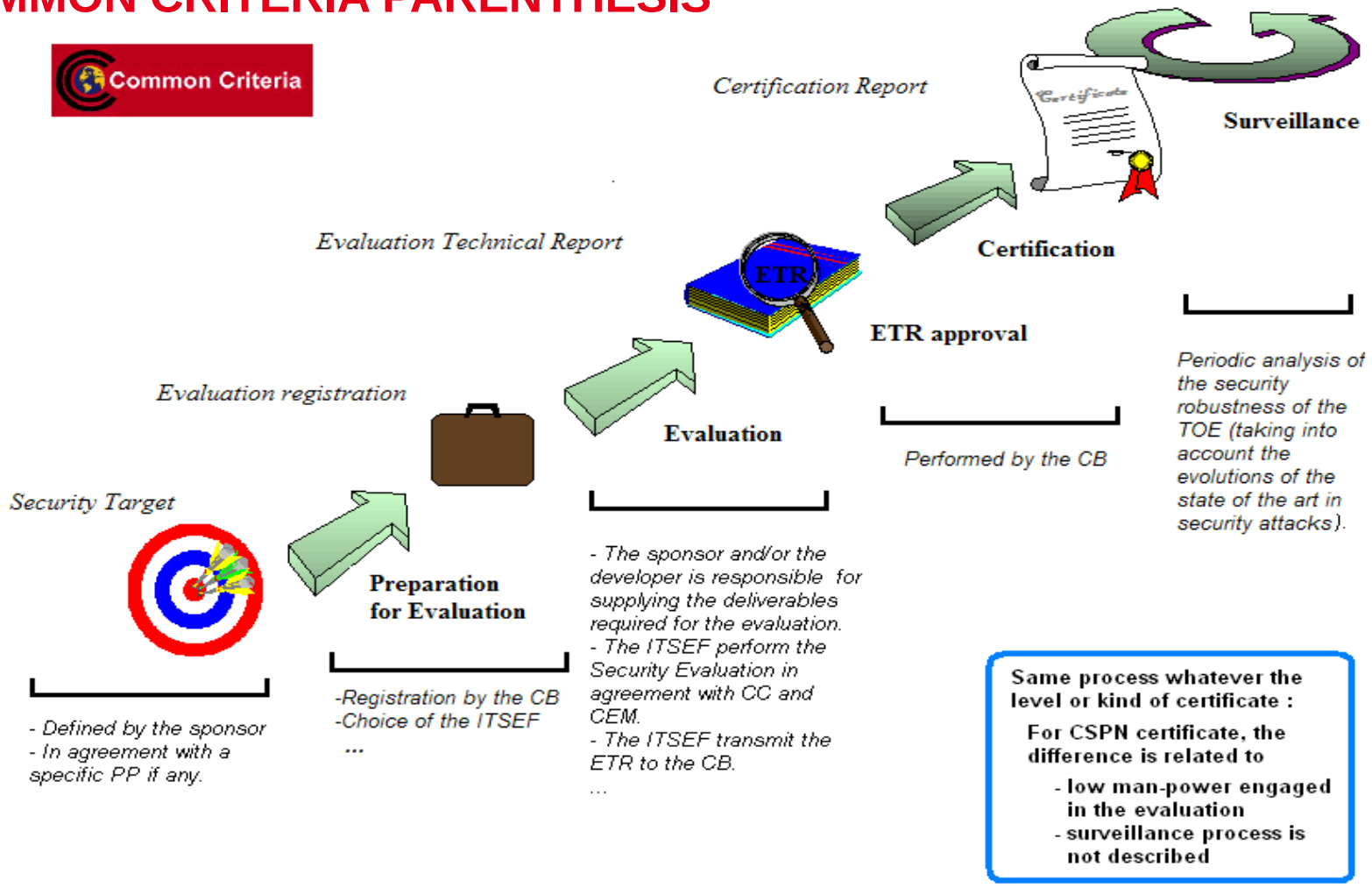
WHAT IS A SMARTCARD ? ACTORS

- **Main IC actors**
  - Samsung
  - Infineon
  - NXP
- **Smaller IC actors**
  - Tiempo
  - Starship
  - others,
- **Embedded software developper**
  - Gemalto
  - Morpho (ex: Safran)
  - Oberthur
  - Giesecke & Devrient
- **Certifcation bodies**
  - CC: ANSSI, BSI, CESG, …
  - EMVCo
  - Mifare
  - …

SMARTCARD LIFE CYCLE (COMMON CRITERIA)



COMMON CRITERIA PARENTHESIS



COMMON CRITERIA - OVERVIEW

- **7 level of security (EAL1-7)**
- **TOE – SFR – TSF - SM**
- **Assurance components**
  - ADV
  - AGD
  - ALC
  - ASE
  - ATE
  - AVA
- **AVA : 5 levels of security**
  - AVA_VAN.1 to 5

WHAT IS A SMARTCARD ?

- **Threats**
  - Attacker has a physical access
  - Listen
  - Perturb
  - Modify

- **Not an HSM in a bunker / data farm !**

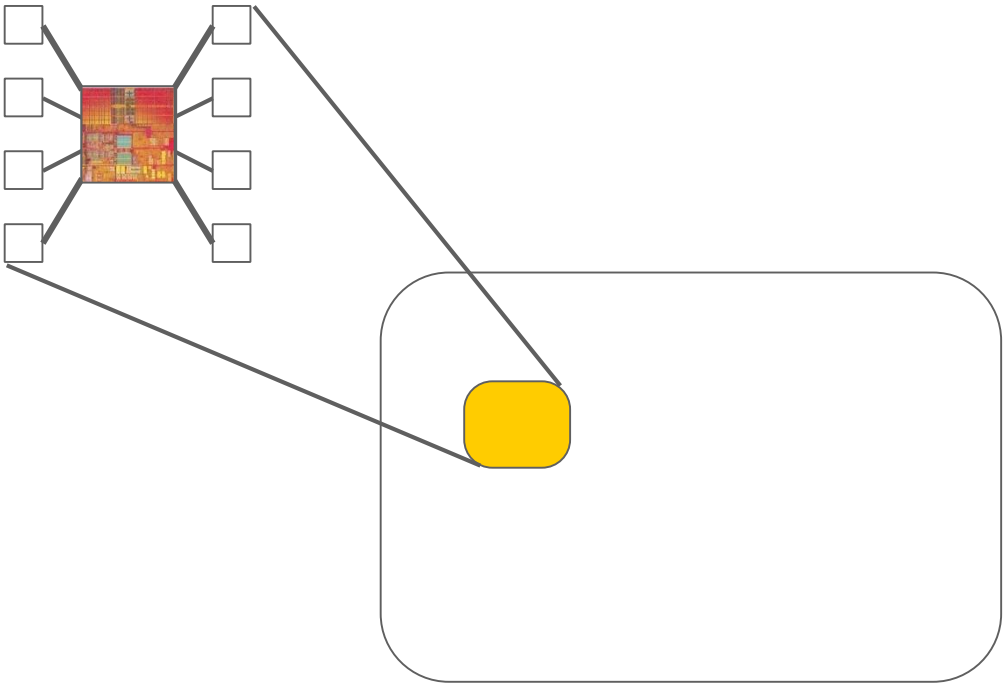
WHAT IS A SMARTCARD ?

- **CPU (MCU)**
  - ARM
  - Proprietary instruction set
- **Memories:**
  - ROM
  - RAM
  - EEPROM / Flash
- **Crypto-processors : DES, AES, multiplier…**
- **Communication interface : serial bi-directionnal I/O line, RF, USB…**

On the same silicon!

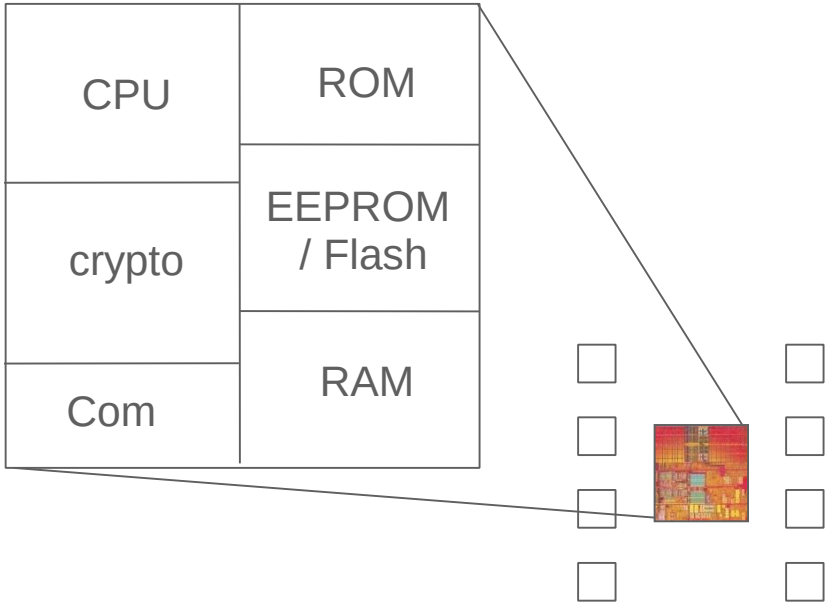
WHAT IS A SMARTCARD ?

- The Micro module



WHAT IS A SMARTCARD ?

- **The architecture**



WHAT IS A SMART CARD?

- **Design of a smart card**
  - memory blocks
  - analogical part
  - numerical part
    - language used for dev. : VHDL, Verilog
- **Embedded software**
  - application example
  - development : assembly language, C, C++, JAVA

EMBEDDED SOFTWARE

- **Source Code : C, C++, ASM**

- **Compilation gcc, keil**
  - Target: depends on CPU the Instruction set
  - ARM 8-bits, 16-bits, 32-bits (v5,v7…), MIPS
  - Other proprietary instruction set

- **Javacard**
  - JVM (compiled for the target : CPU + accelerators)
  - Applets

WHAT IS A SMART CARD – DESIGN OVERVIEW

- **1. Architecture Scheme**
- **2. Design**
  - Analogic
  - Digital
- **3. Synthesis**
- **4. Floor Planning**
- **5. Place And Route**
- **6. Tape-Out**

EDA tools
(Electronic Design Automation)

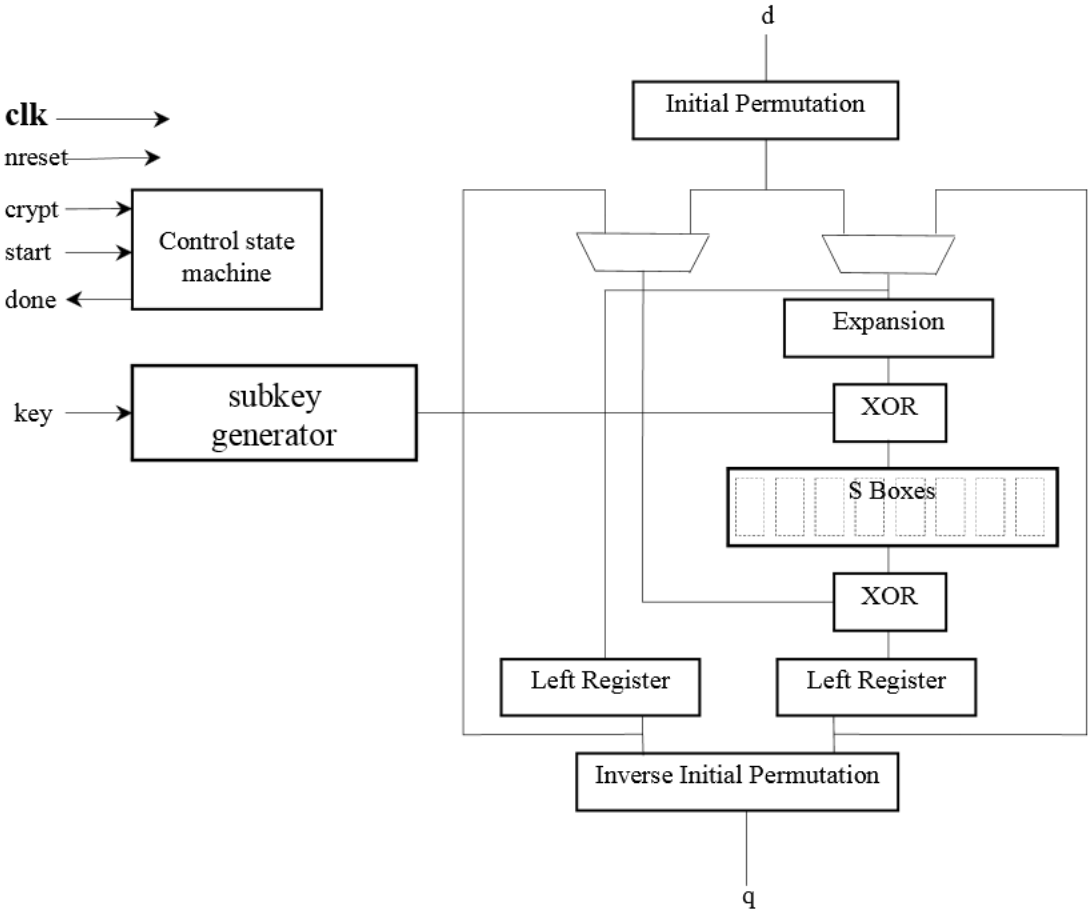
TESTS
TESTS
TESTS

This is not software:
Bug is not option

Long time process: very costly

WHAT IS A SMART CARD – DESIGN OVERVIEW (1/5)

- 1. Architecture Scheme (DES example)



WHAT IS A SMART CARD – DESIGN OVERVIEW (2/5)

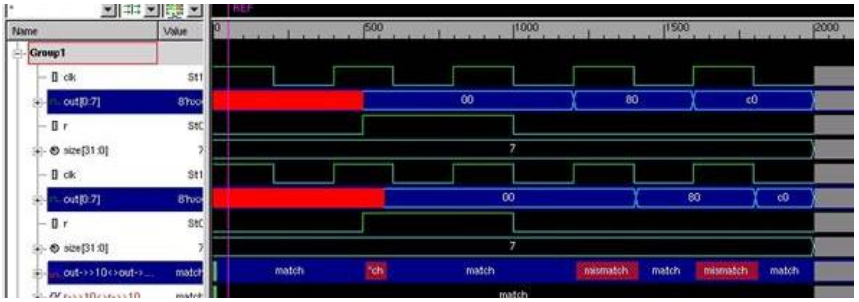
- 2. Design – simple Verilog example (Sbox1)

```
module Sbox_Rom1(S1_INPUT, S1_OUTPUT);
    input  [6 : 1] S1_INPUT;
    output [3 : 0] S1_OUTPUT;
    wire   [6 : 1] S1_INPUT;
    reg    [3 : 0] S1_OUTPUT;
    wire   [6 : 1] S1_SELECT;
    assign S1_SELECT = {S1_INPUT[6], S1_INPUT[1], S1_INPUT[5 : 2]};

    always @(S1_SELECT)

     begin
       case (S1_SELECT)
            6'b000000: S1_OUTPUT <= 4'hE;
            6'b000001: S1_OUTPUT <= 4'h4;
            6'b000010: S1_OUTPUT <= 4'hD;
            6'b000011: S1_OUTPUT <= 4'h1;
            6'b000100: S1_OUTPUT <= 4'h2;
            6'b000101: S1_OUTPUT <= 4'hF;
            6'b000110: S1_OUTPUT <= 4'hB;
            6'b000111: S1_OUTPUT <= 4'h8;
            ....
       endcase
     end
```

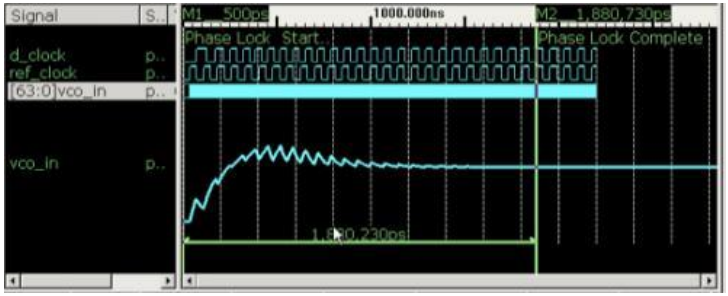
=> TESTS: Verilog/VHDL simulation

WHAT IS A SMART CARD – DESIGN OVERVIEW (3/5)

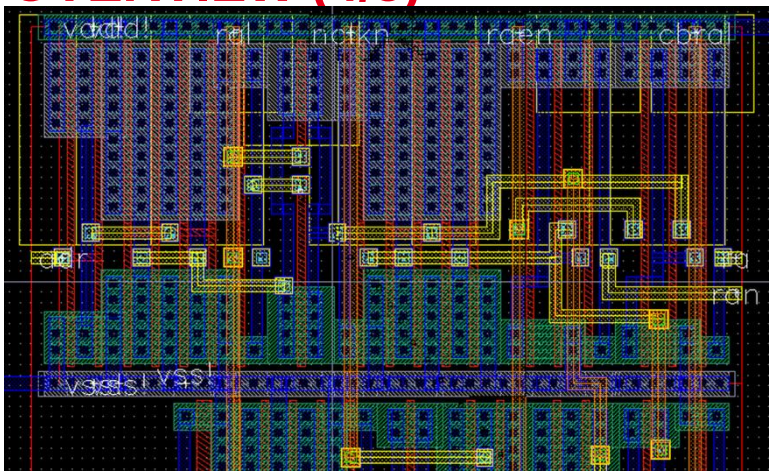
- **3. Synthesis**
  - Kind of compilation
  - From Verilog/VHDL code source
  - To Netlist File
- **TESTS: Netlist Simulation**



- **Spice Simuation**
  - Electrical simulation
    - EDP/Differential equations solving at each step of time



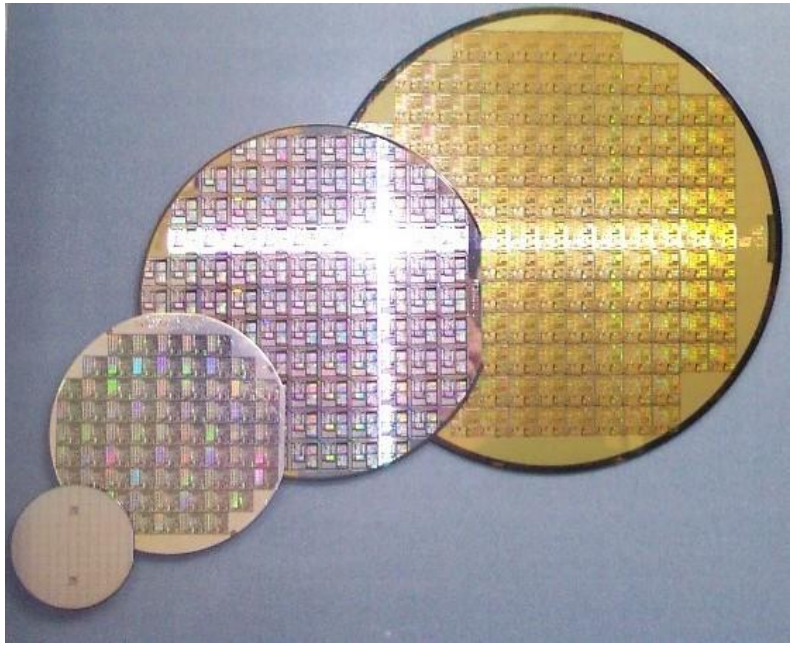
WHAT IS A SMART CARD – DESIGN OVERVIEW (4/5)



- **4. Floor Planning**
  - From the netlist
  - To a 2D plan
- **5. Place And route**
  - Cells are placed on the floor plan
  - Routing
  - Design Rules Check / Layout Versus Schematic
  - Parasitics extraction
  - TESTS: simulation

WHAT IS A SMART CARD – DESIGN OVERVIEW (5/5)

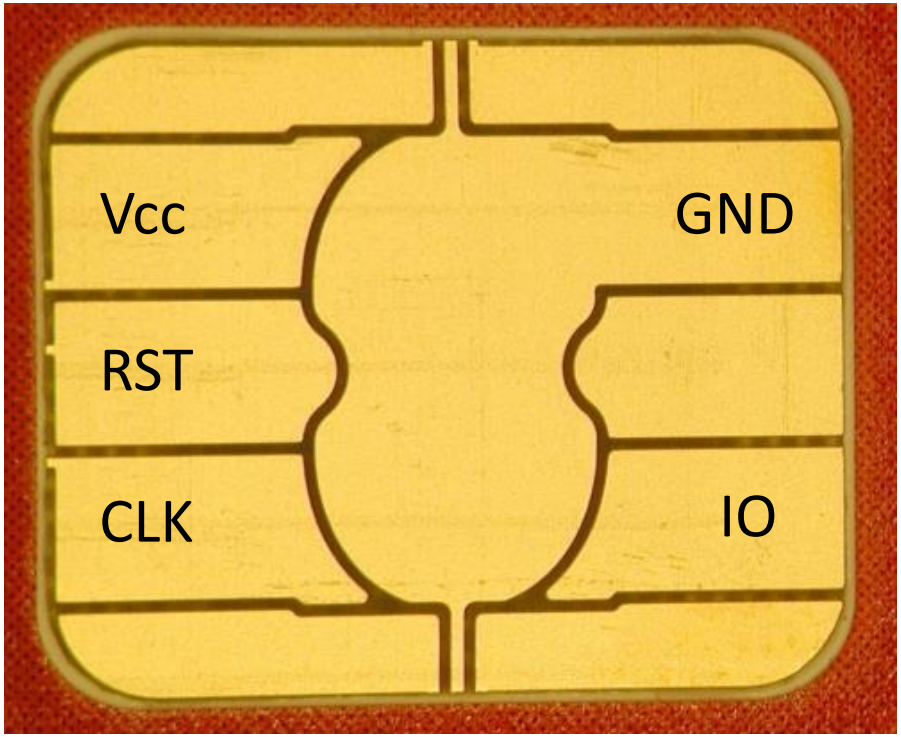
- **5. Tape-Out**
  - GDS sent to the foundry
  - Wafer
  - Tested
  - Cut
  - Packaged



WHAT IS A SMART CARD – A WORD ON TECHNOLOGY NODE

- 130nm, 90nm, 65nm, 45nm, 32nm, 22nm, 14nm
- Smallest half-pitch of contacted M1 lines in the fabrication process
- Defines the size of cells
- Smaller implies
  - Less power consumption
  - Faster electronic
  - Less silicon => cheaper production
  - New techno => lot of investments => more expensive
- **TSMC, Global foundery, UMC, Samsung, Intel, …**

WHAT IS A SMART CARD? MICRO-MODULE: PINS



SMARTCARD ACTIVATION SEQUENCE

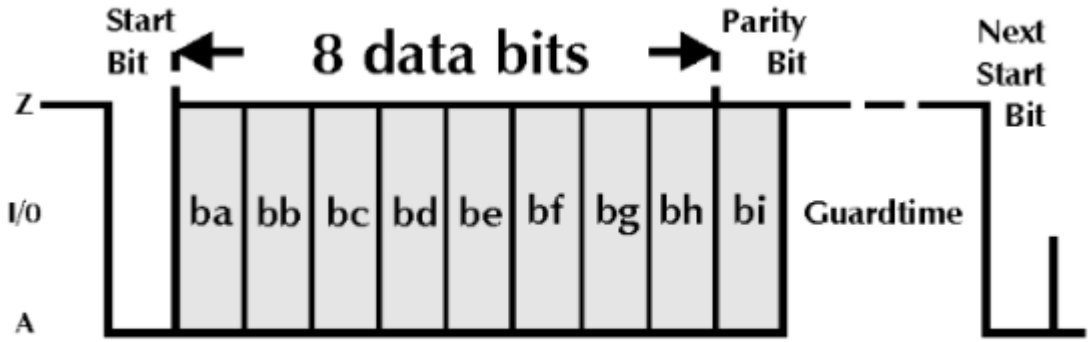
- 1. RST low
- 2. Apply VCC
- 3. Put IO in receive mode
- 4. Apply CLK
- 5. RST High

ISO 7816-3

- **ATR**
  - Contains several data
  - TS, T0, clock frequency, convention, …

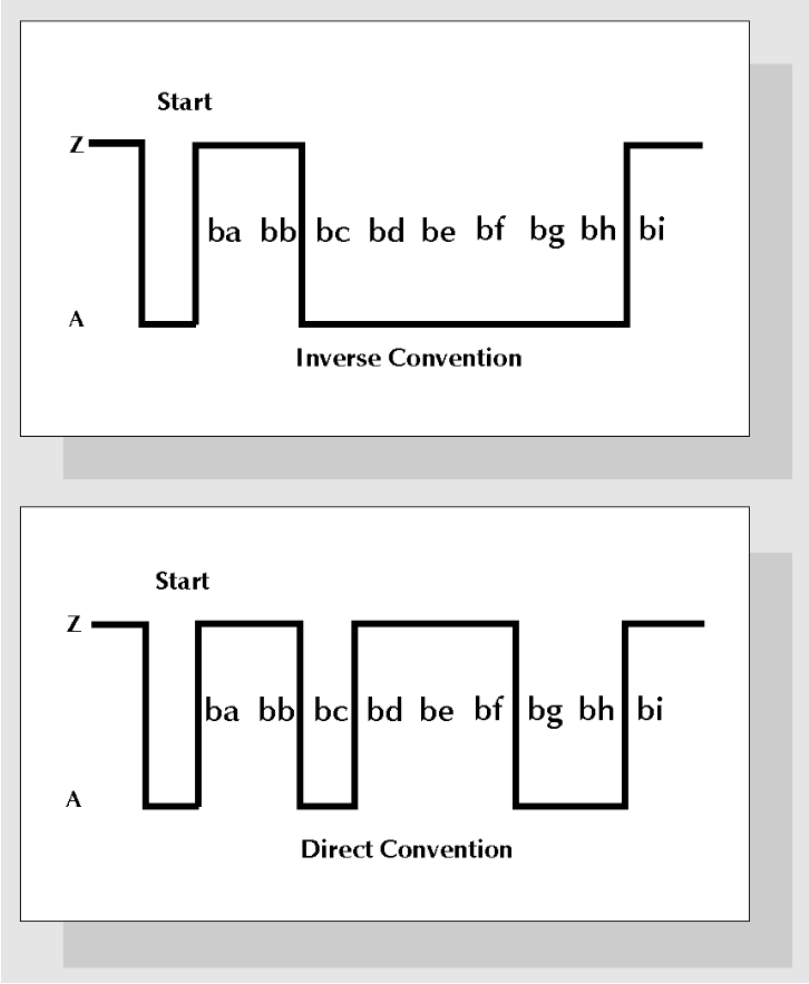
- **Indirect mode**
  - Z → 0, A → 1
  - Msb first

- **Direct mode**
  - Z → 1, A → 0
  - Lsb first

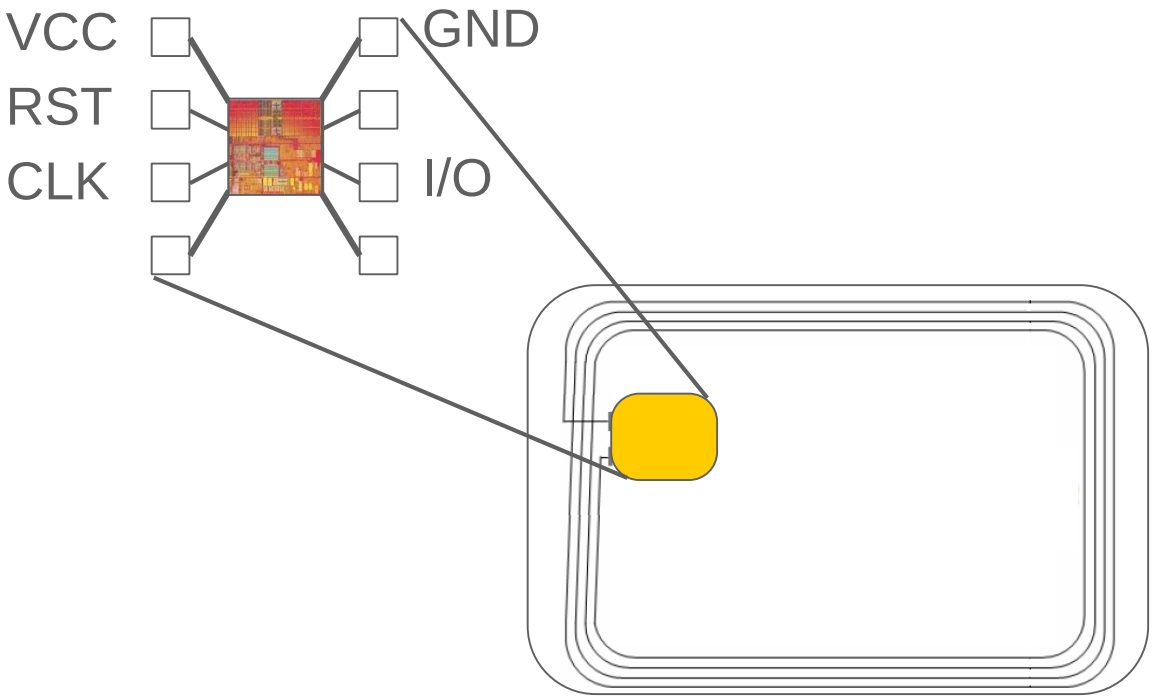


$$1\ \text{etu} = \frac{372}{f}$$

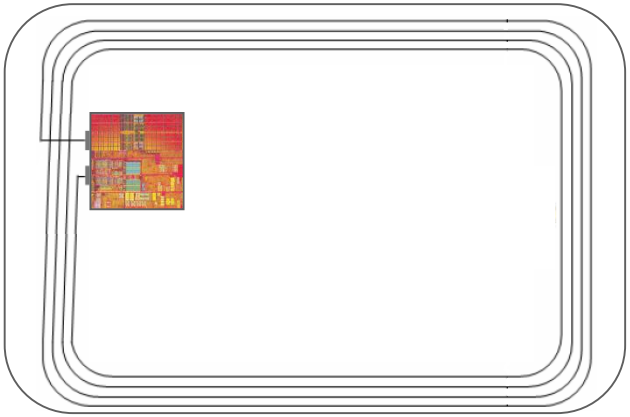
ISO 7816-3 TS CHARACTER



WHAT IS A SMART CARD?
CONTACT AND CONTACTLESS DUAL MODE



WHAT IS A SMART CARD… CONTACTLESS MODE



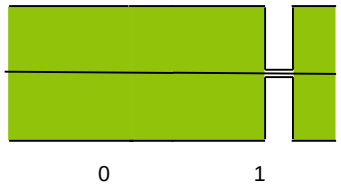
ISO 14443

- **Proximity coupling (< 10cm)**
- **Two types**
  - Type A (Philips MIFARE)
  - Type B (Others: STM, MOTOROLA)
- **EM Field**
  - Carrier @ 13.56 MHz
  - EM amplitude field H_{min}=1.5 to H_{max}=7.5 A/m
- **Terminology**
  - PCD: Proximity Coupling Device (Reader)
  - PICC: Proximity Integrated Circuit Card (Card)

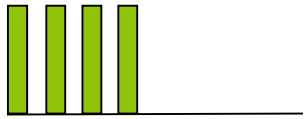
ISO 14 443-2 TYPE A - PHY & MAC LAYERS

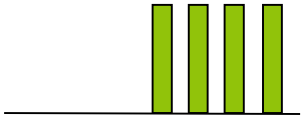
Modulation & Coding (Type A)

- **Forward link**
  - 100%-ASK (OOK)
  - Logic 1 : Modified Miller with pause on carrier
  - Logic 0 : No pause



- **Return link**
  - Load modulation of a sub carrier
  - Frequency of sub carrier = Fc/16 = 848 kHz
  - Logic 1 : first half bit with sub carrier modulation
  - Logic 0 : second half bit with sub carrier modulation



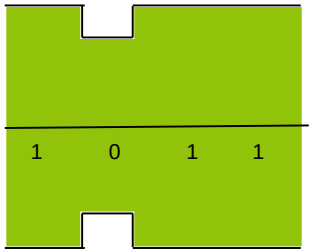


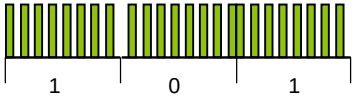
Data rate: 106 kbps

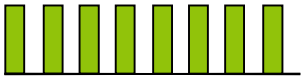
ISO 14 443-2 TYPE B - PHY & MAC LAYERS

Modulation & Coding (Type B)

- **Forward link**
  - 10%-ASK [8% – 14%]
  - Coding: NRZ-L
    - Logic 1 : Carrier high field amplitude (No modulation)
    - Logic 0 : Carrier low field amplitude
- **Return link**
  - Load modulation of a sub carrier Fc/16 = 848 kHz
  - BPSK NRZ-L
    - Logic 1: sub carrier phase + 0°
    - Logic 0 : sub carrier phase + 180°

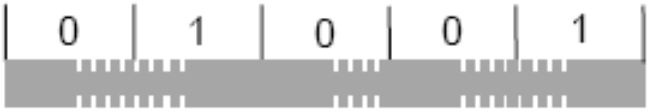






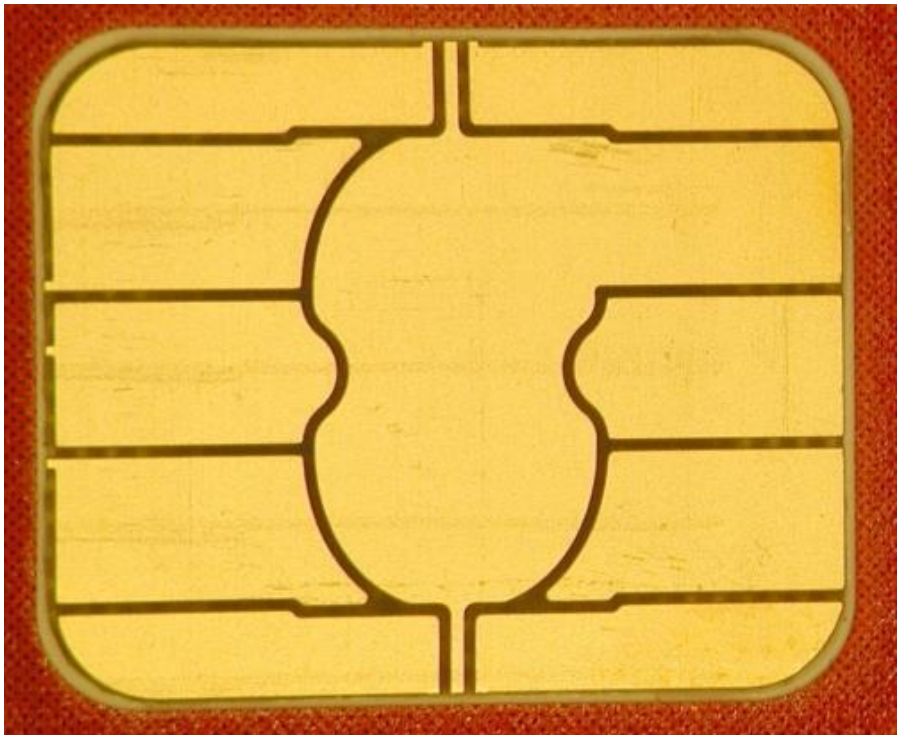
Data rate: 106 kbps

ISO 14443

	Type A	Type B
PCD to PICC	ASK 100% Modified Miller, 106kbit/s 	ASK 10% NRZ, 106kbit/s 
PICC to PCD	Load Modulation Subcarrier $f_c/16$ OOK Manchester, 106kbit/s 	Load Modulation Subcarrier $f_c/16$ BPSK NRZ-L*, 106kbit/s 

Example communication signals for Type A and Type B interfaces

WHAT IS A SMART CARD? MICRO-MODULE



WHAT IS A SMART CARD…