INDUSTRY DE-FACTO STANDARD MEMORY SMART CARD

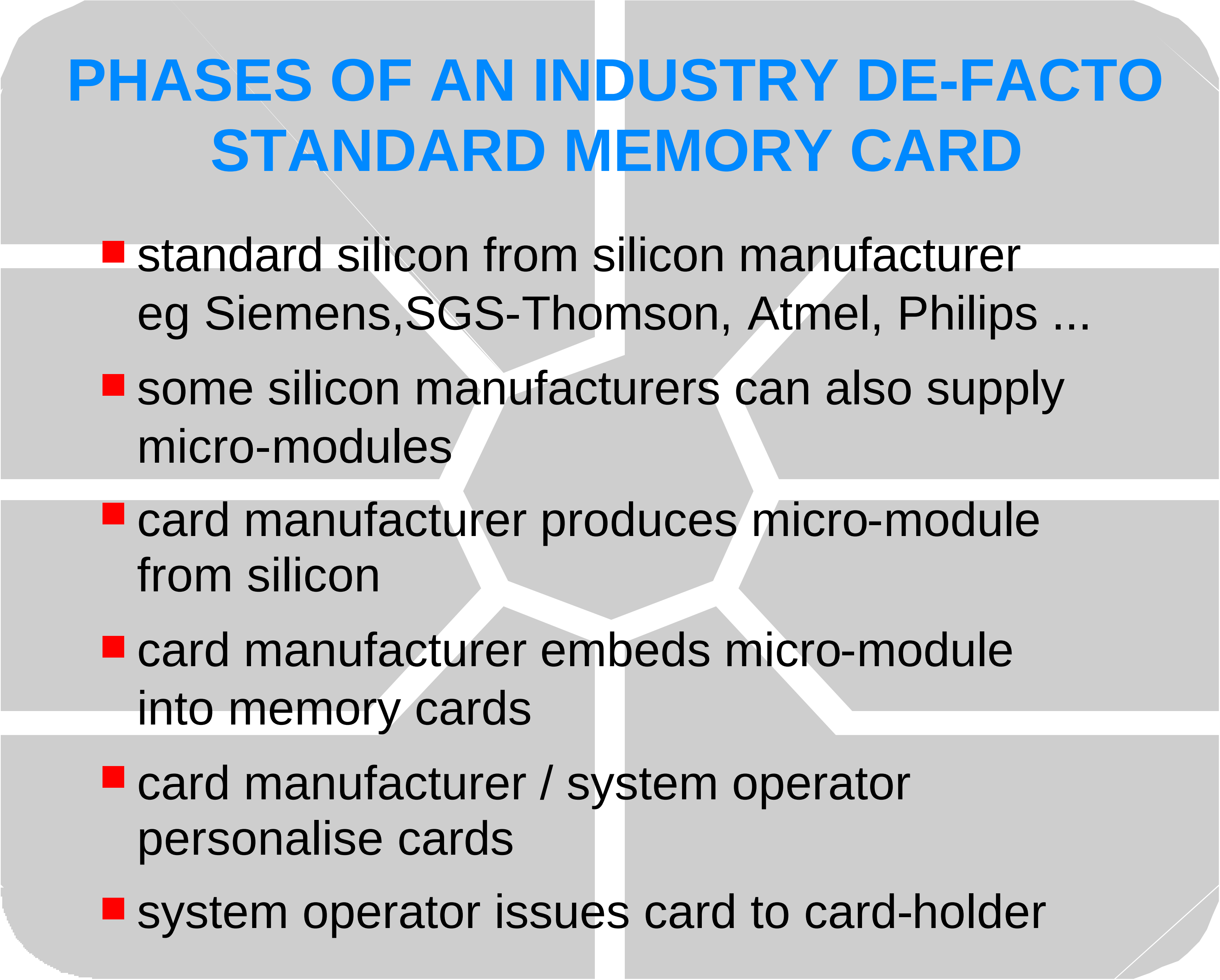
De-facto-standard memory smart card :

cards produced by more than 1 card manufacturer eg GEMPLUS GPM-416

Proprietary memory smart card :

cards produced by only 1 manufacturer

eg GEMPLUS GPM-896



PHASES OF AN INDUSTRY DE-FACTO STANDARD MEMORY CARD

- standard silicon from silicon manufacturer
  eg Siemens,SGS-Thomson, Atmel, Philips ...
- some silicon manufacturers can also supply micro-modules
- card manufacturer produces micro-module from silicon
- card manufacturer embeds micro-module into memory cards
- card manufacturer / system operator personalise cards
- system operator issues card to card-holder

TYPES OF INDUSTRY DE-FACTO STANDARD MEMORY SMART CARDS

- EPROM Telephone Card - 1st generation (T1G)
- EEPROM Telephone Card - 1st generation
- French Telephone Card - 2nd generation (T2G)
- German Telephone Card - 2nd generation (EuroChip)
- I2C Memory Card
- Visa Disposable Store Value Card (416 memory card)

EPROM TELEPHONE CARD (T1G / 256 CARD)

- General
- Specifications
- Memory organization
- Card life phases
- Security features
- Card commands

T1G / 256 CARD - GENERAL

- Silicon from SGS-Thomson ST-1200
- Silicon from Siemens - SLE-3563
- Silicon from Texas - TI-3562
- largest volume - few hundred million cards per year
- lowest priced - approx US $0.60 per card
- used by more than 50 telecom operators world-wide
- usually known as something256 card eg GPM-256, F-256
- sometimes nopt so obvious eg inphone16

T1G / 256 CARD SPECIFICATIONS

- 256 bits of EPROM
- Divided into two fixed areas:
- A 96 bits Identification protected area
- A 160 bits Application area
- Access to each area is controlled by specific security rules
- non-reloadable token card

256 CARD SPECIFICATIONS

- 256 bits of EPROM
- Divided into two fixed areas:
  - A 96 bits Identification protected area
  - A 160 bits Application area
- Access to each area is controled by specific security rules

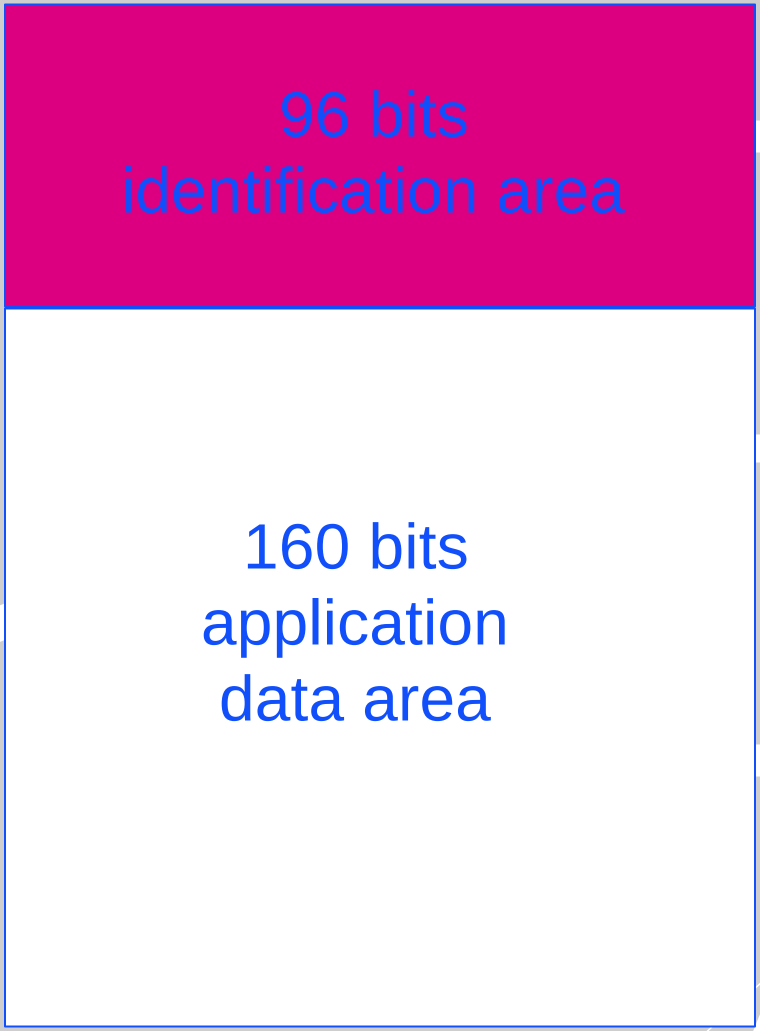
The 256 card is not a reloadable card

ELECTRICAL CHARACTERISTICS

- Synchronous protocol
- 21V programming voltage (VPP) (some card manufacturer has a 5 V version (proprietary)
- 5V supply voltage (VCC)
- Access time
  - Read : 500 ns
  - Write : 20 ms
- Operating range : -10°C to +70°C
- Ten years minimum data retention

Memory Organisation

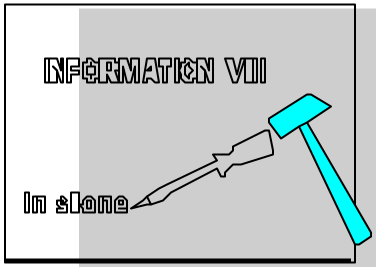
- **memory access is bit by bit**
- **virgin memory state is logic 0**

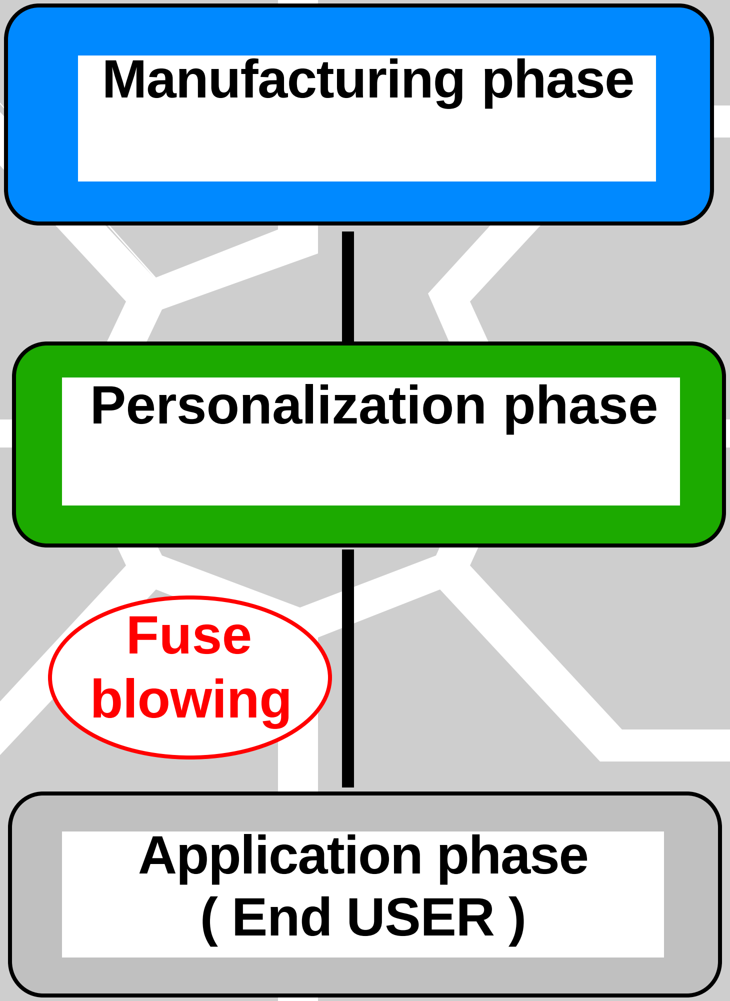


96 bits
identification area

160 bits
application
data area

CARD LIFE PHASES



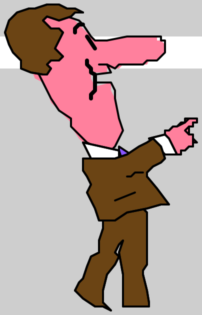


Manufacturing phase

Personalization phase

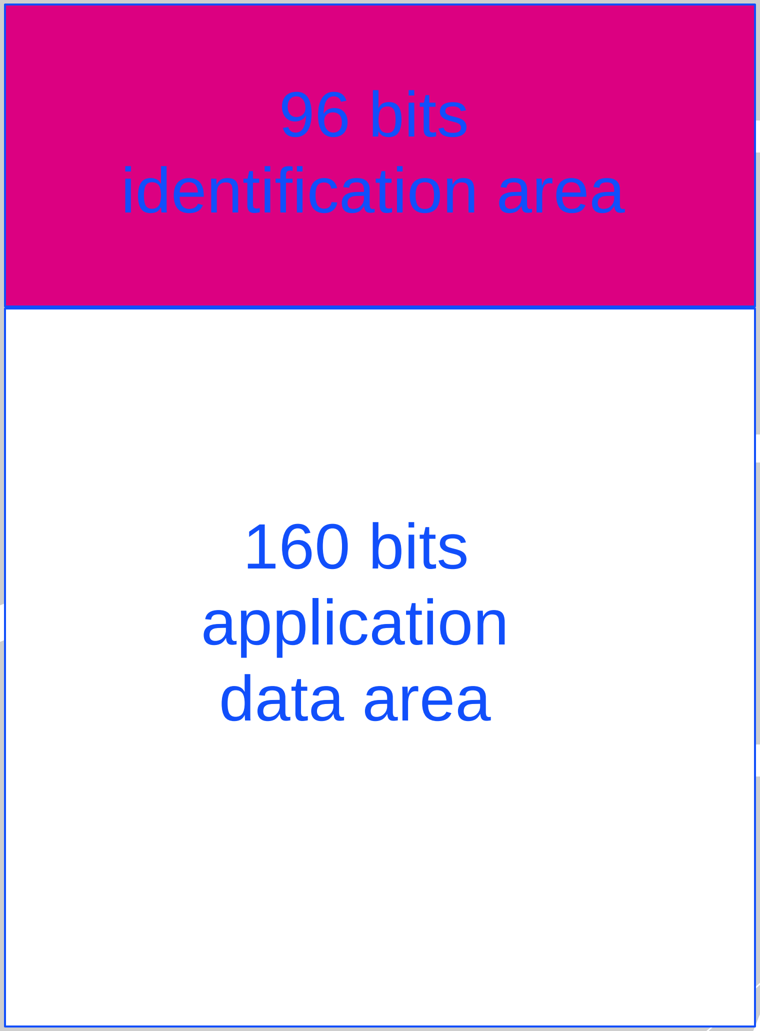
Fuse blowing

Application phase
(End USER)



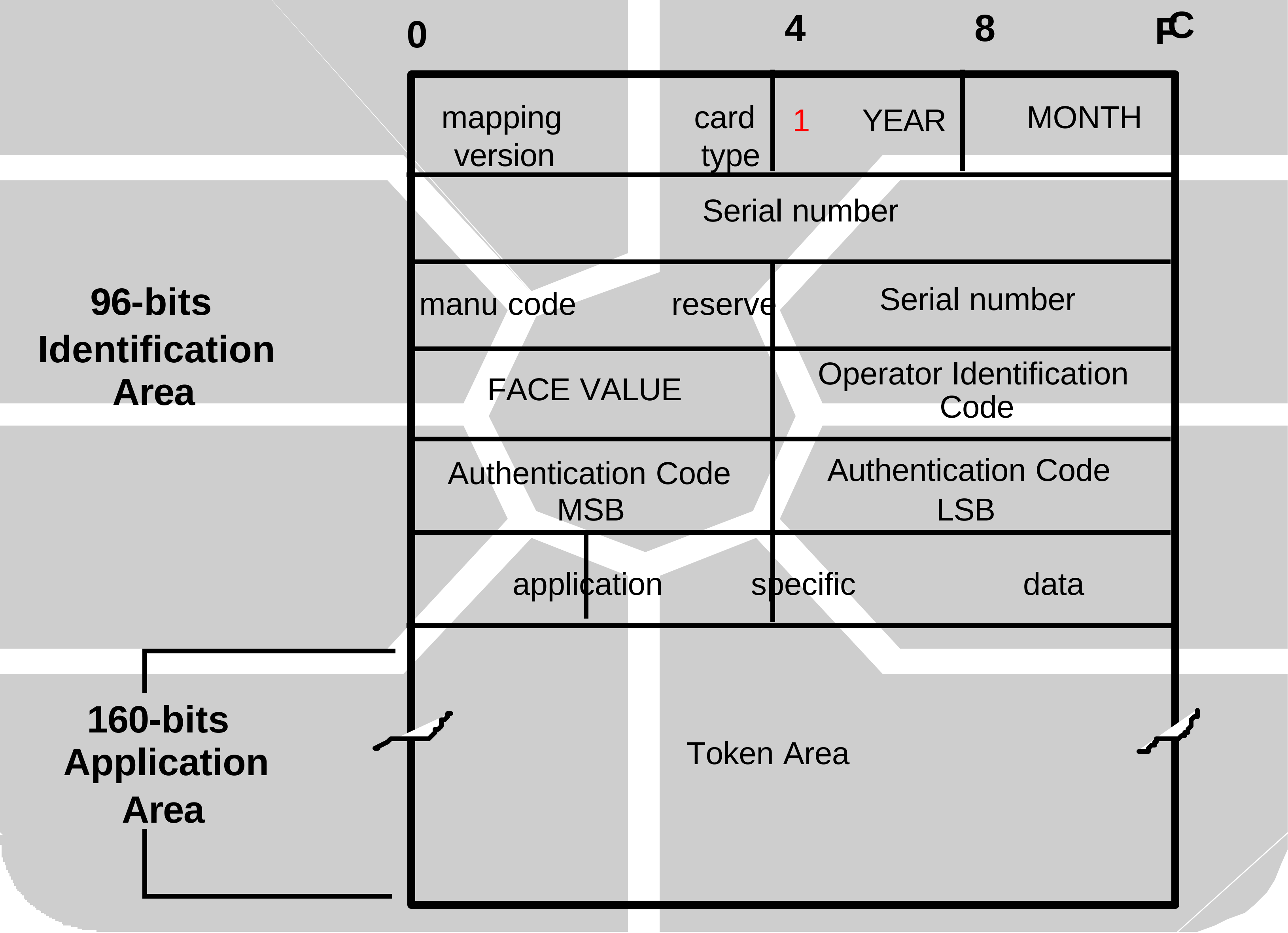
Manufacturing / Personalisation Phase

- manufacturer writes data into identification area
  - manufacturer code
  - issuer code
  - other issuer data
- blow fuse
- destroy extra tokens


96 bits
identification area

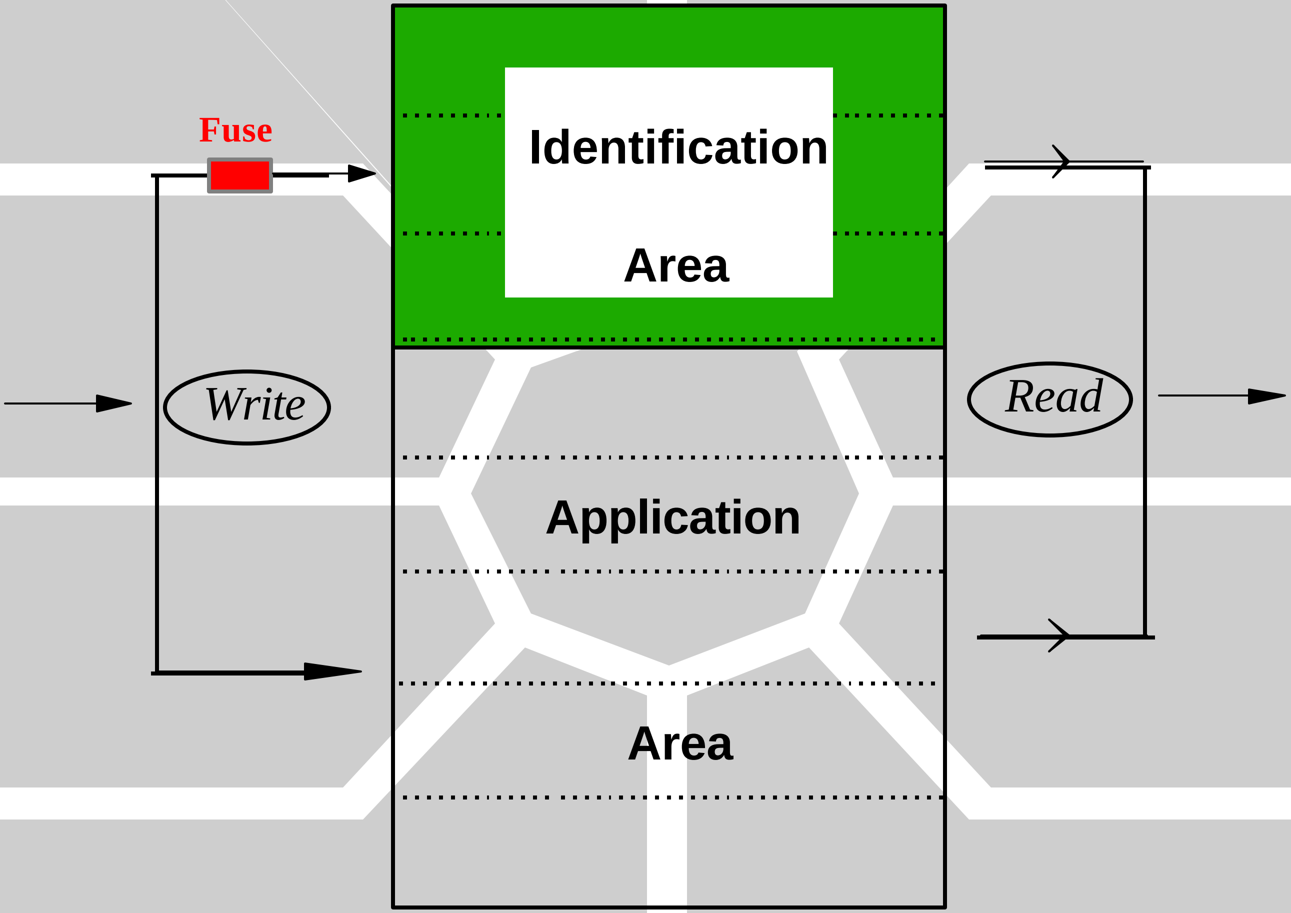
160 bits
application
data area

MEMORY MAPPING EXAMPLE



0		4	8 FC
mapping version	card type	1 YEAR	MONTH
Serial number			
manu code	reserve	Serial number	
FACE VALUE		Operator Identification Code	
Authentication Code MSB		Authentication Code LSB	
application	specific	data	
Token Area			

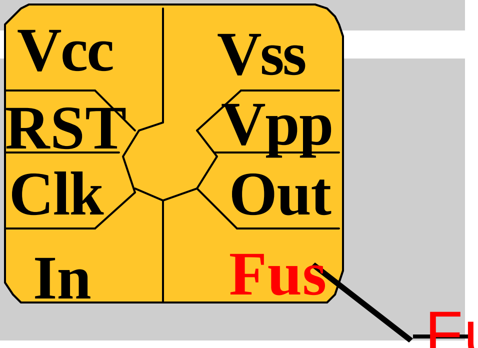
SECURITY FEATURES



Once the fuse is blown, the *Identification area* will be write-protected

FUSE BLOWING

- Done by card manufacturer
- The fuse is blown at the end of personalization.
- When blown, it is impossible to modify or fraud the 96 bits area.
- To blow it :
  - Apply - 40volts on the Fus pin



Fuse control

Blowing a fuse is a irreversible physical mechanism.

CARD COMMANDS

- Two ways to access the memory
  - Physically : By performing the elementary micro-instructions, delivering the various signals on the pins (chip micro instructions)
  - Logically : Through a coupler (reader) by sending high level commands. (reader manufacturer specific commands)

DIRECT PHYSICAL ACCESS

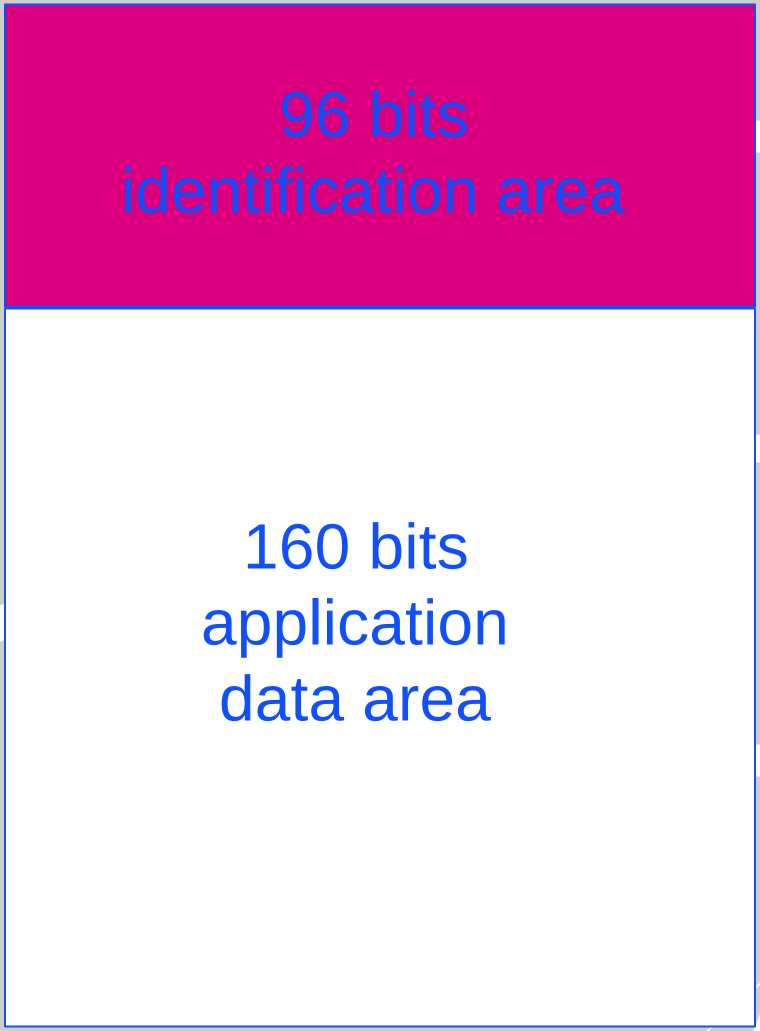
3 Micro-Instructions are used to access the memory

- ***"Reset"***
  - Resets the address counter and ***READS*** the first bit
- ***"Up"***
  - Increments the address counter and ***READS*** the addressed bit
- ***"Program"***
  - ***WRITES*** a "1" at the current address

3 low level commands to access a 256 card

Reset

- **reset micro-instruction makes the address pointer points to the begining of the memory**



96 bits
identification area

160 bits
application
data area

READ A MEMORY BIT

- The "UP" Micro-instruction increments the address pointer and reads the addressed bit.
- To read bit number "N" (N=[0, 255]) :
  - Reset the card (first bit pointed and read)
  - Perform "N" "UP" Micro-instructions.

To read a bit at an address "P" higher than the current one ("N"), it is not necessary to "Reset" the card but only perform "P-N" "UP" Micro-instructions.

WRITE A MEMORY

- The "PROG" micro-instruction writes a "1" at the addressed bit and checks it by presenting the final value on the output pin
- To program bit number "N" (N=[0..255]:
  - Reset the card (first bit pointed and read)
  - Perform N x UP Micro-instructions to point to bit number N
  - Perform a program Micro-instruction.

To write a bit in the first memory area (96 bits) the fuse must be intact.

256 CARD COMMENTS

- 256 card is the lowest priced card, but security offered is very limited
- security relies on the procedural control by chip and card manufacturers
- application not limited to telephone prepaid card applications, but designer's creactivity
- issuer must have control of the terminals to prevent card emulation
- designer must understand the limited security implications
- this card, will in the mid-term be obsoleted