Industry De-facto Standard Memory Smart Card

De-facto-standard memory smart card :

Cards produced by more than 1 card manufacturer

e.g. GEMPLUS GPM-416

Proprietary memory smart card :

Cards produced by only 1 manufacturer

e.g. GEMPLUS GPM-896

Phases of an Industry De-facto Standard Memory Card

- Standard silicon from silicon manufacturer e.g. 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 personalize cards
- System operator issues card to cardholder

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 e.g. GPM-256, F-256
- Sometimes not so obvious e.g. 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 controlled by specific security rules

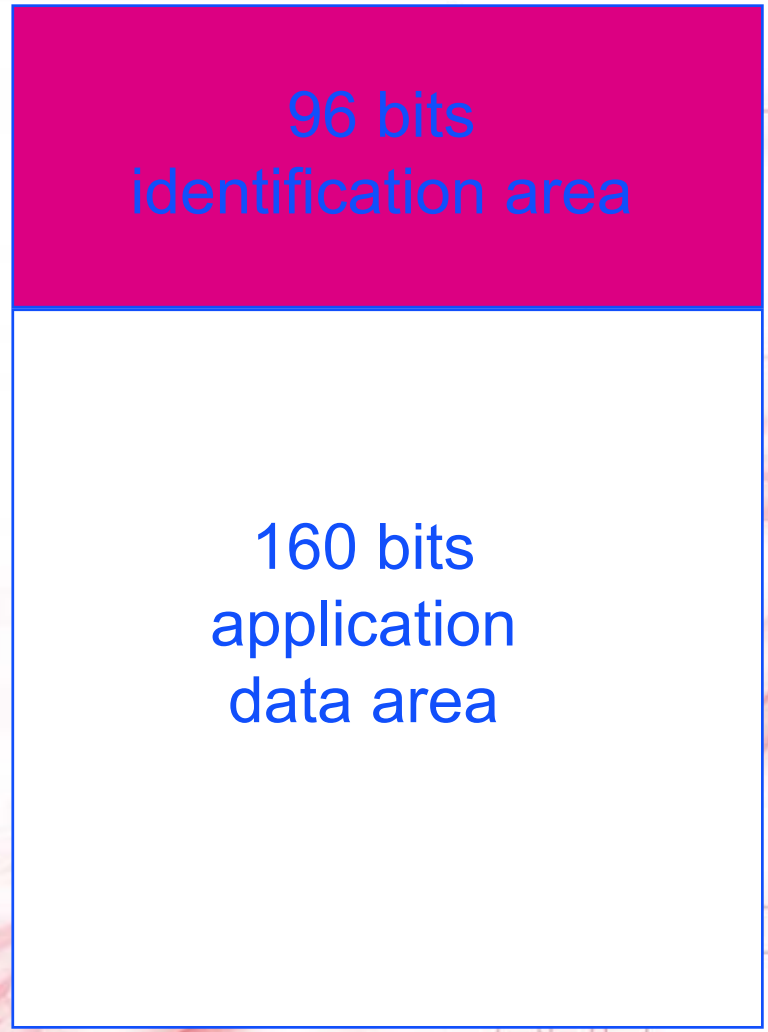
The 256 card is not a reloadable card

Electrical Characteristics

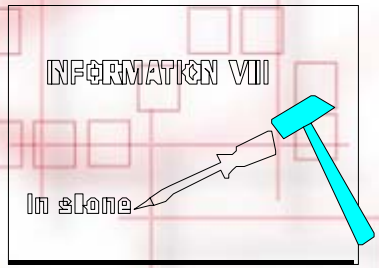
- Synchronous protocol
- 21V programming voltage (VPP) (some card manufacturer has a 5 V version (proprietary)
- 5V supply voltage (VCC)
- Access time
  - Read : 500 ns
  - Write : 20 ms
- Operating range : -10°C to +70°C
- Ten years minimum data retention

Memory Organization

- Memory access is bit by bit
- Virgin memory state is logic 0



Card Life Phases

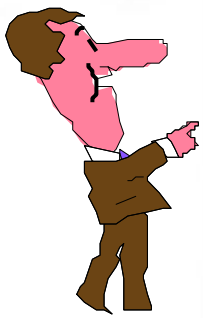


Manufacturing phase

Personalization phase

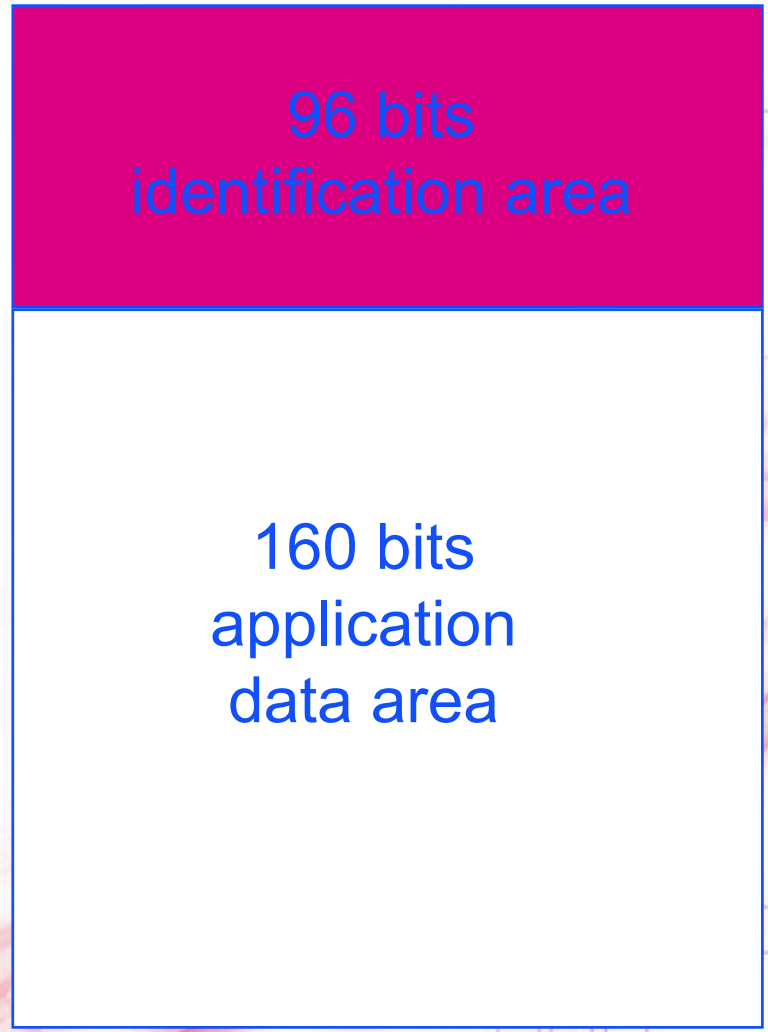
Fuse blowing

Application phase (End USER)

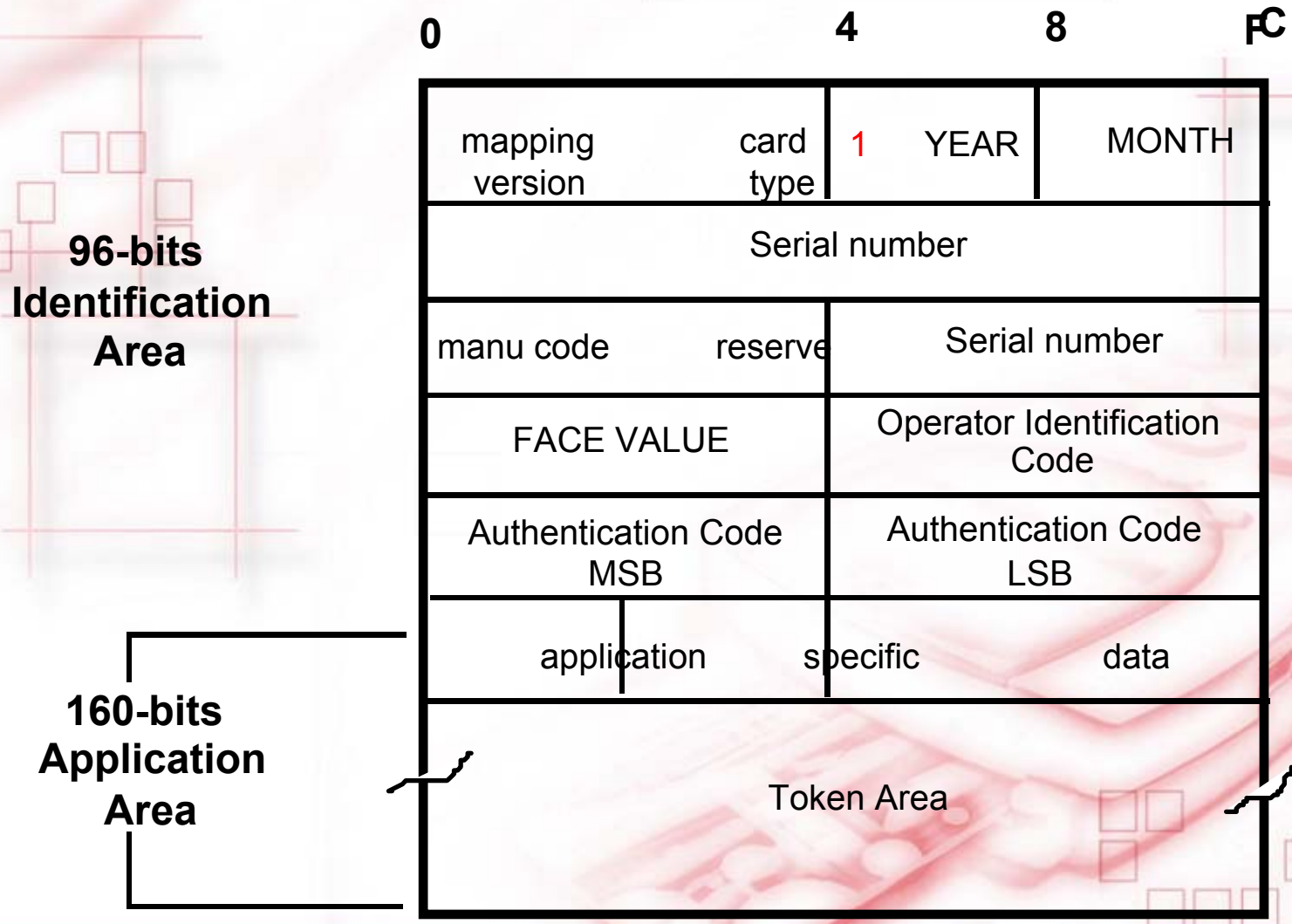


Manufacturing / Personalization Phase

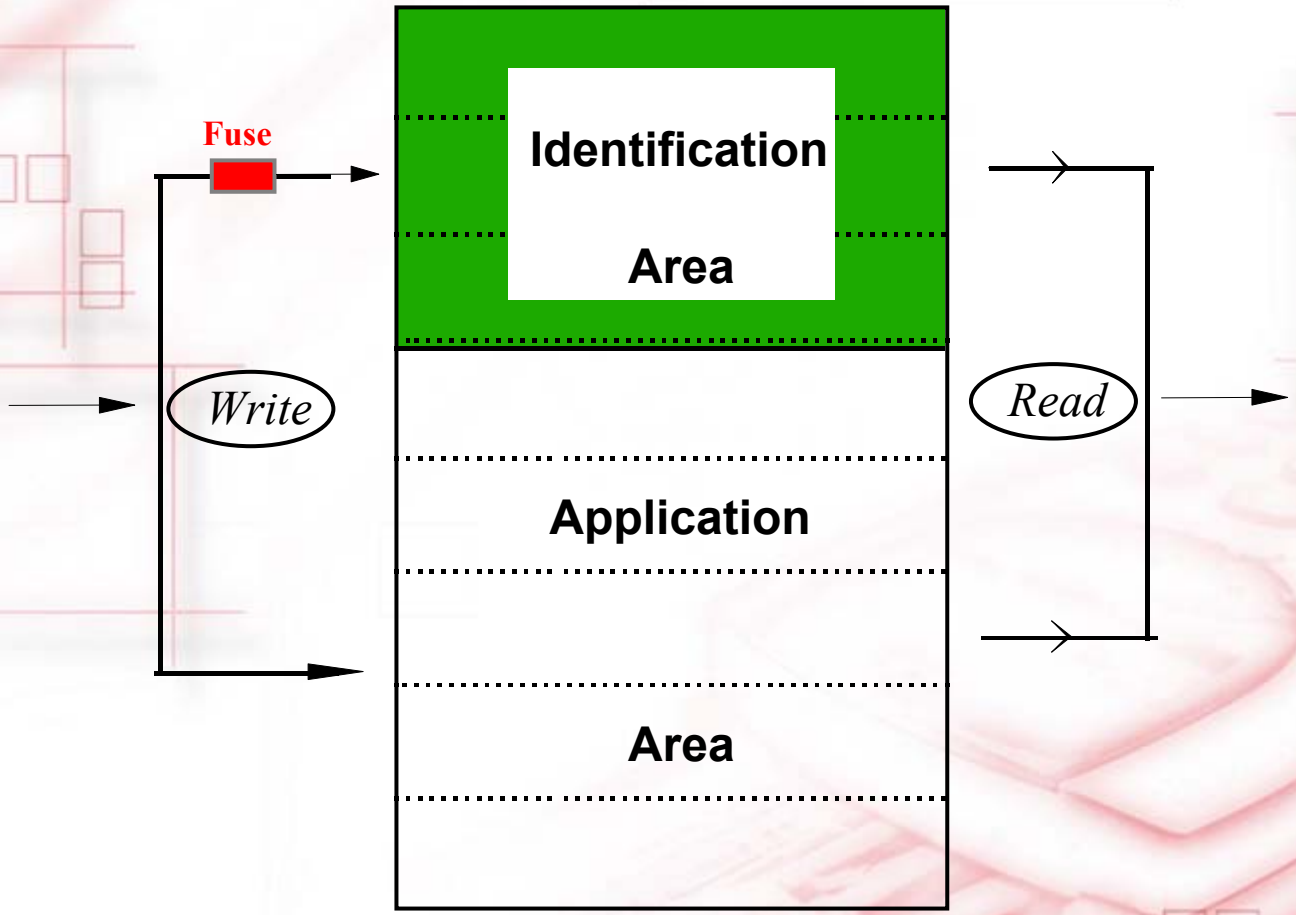
- Manufacturer writes data into identification area
  - Manufacturer code
  - Issuer code
  - Other issuer data
- Blow fuse
- Destroy extra tokens



Memory Mapping Example



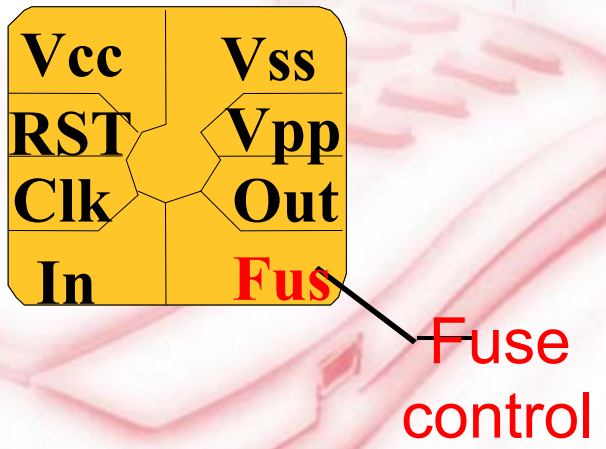
Security Features



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



Blowing a fuse is an 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

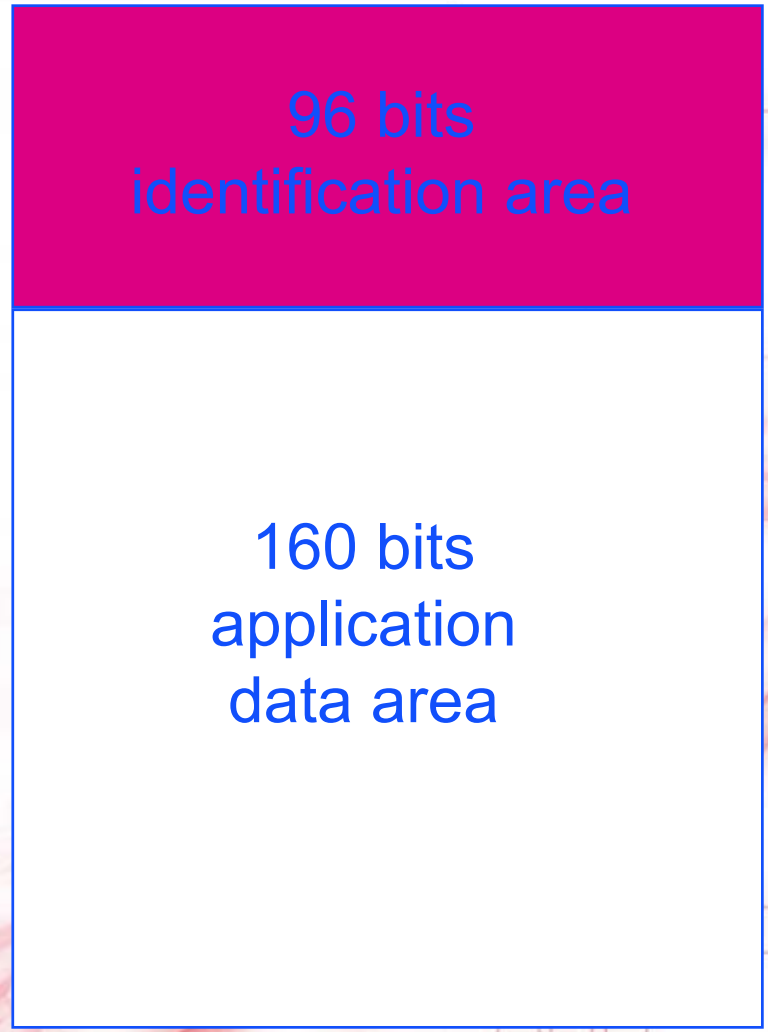
3 Micro-Instructions are used to access the memory

- ***"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 beginning of the memory



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 creativity
- 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 obsolete