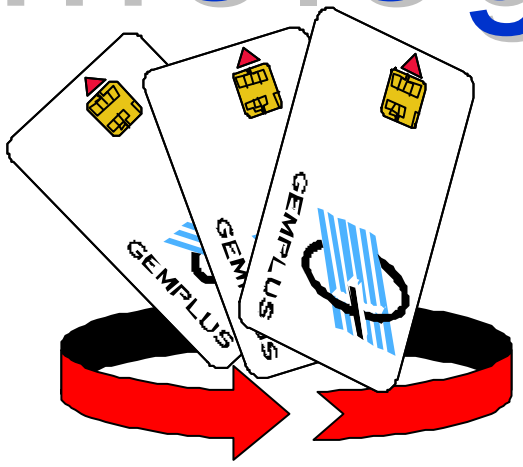
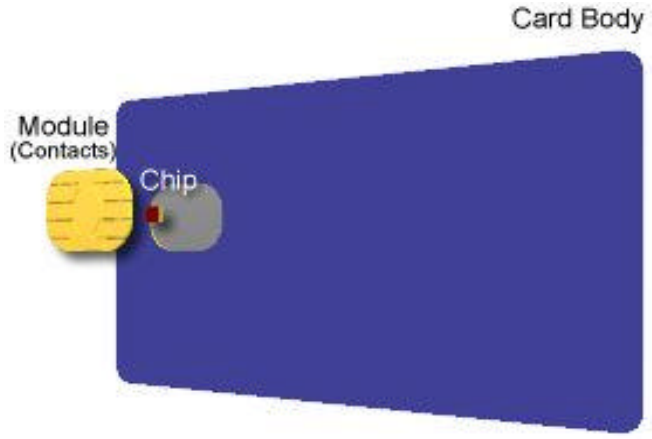
Advanced Course on Smart Card Technology



Part 1 :

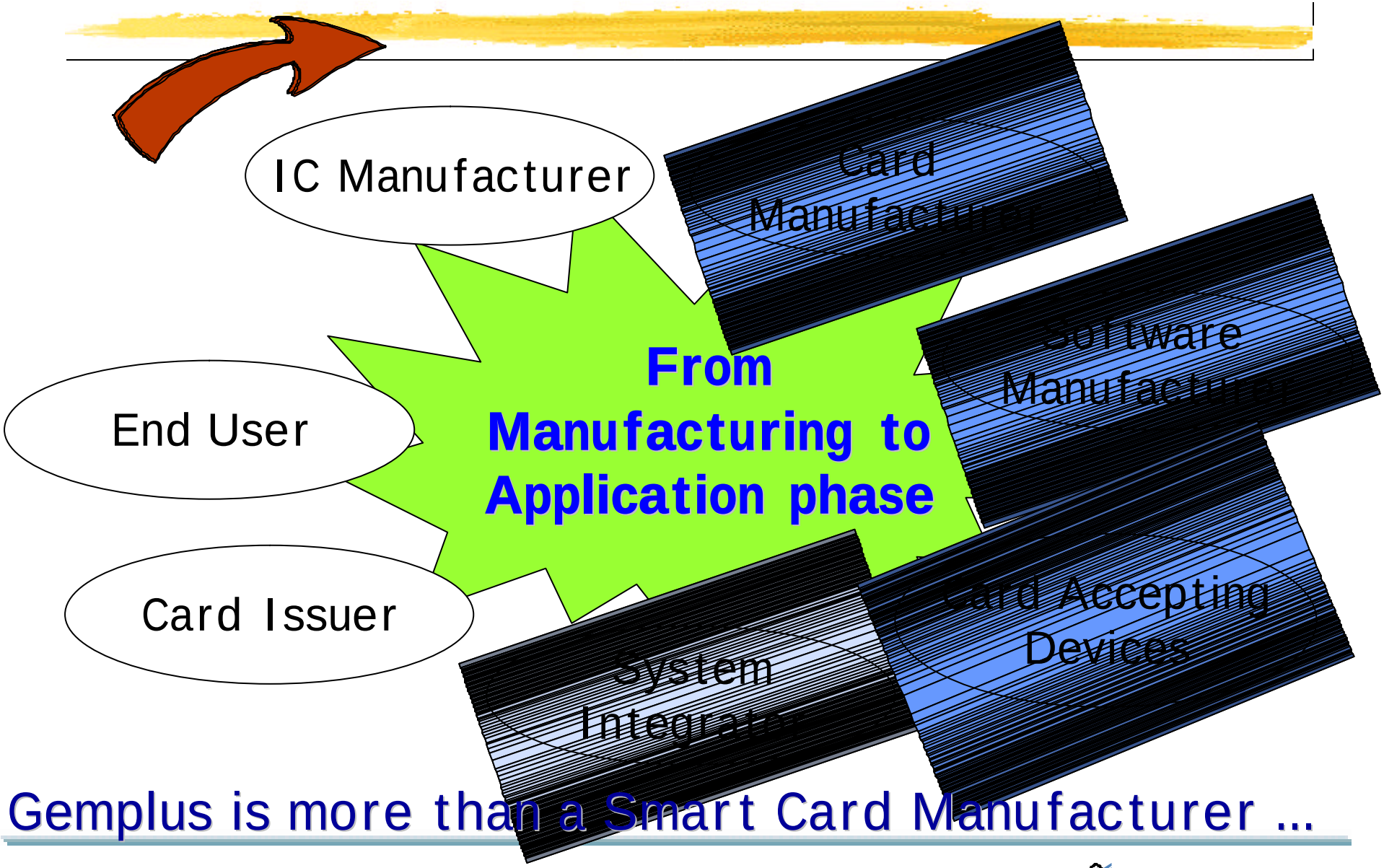
Smart card basics (cont)



A Smart Card is a part of an

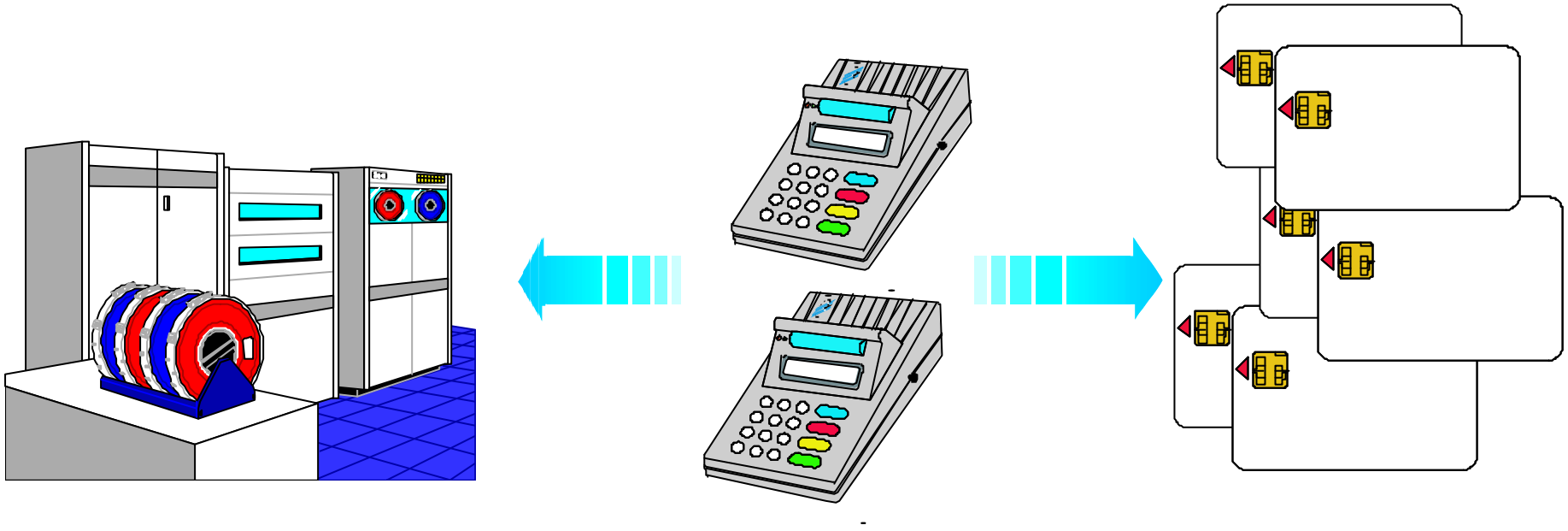
Application

Card Life Cycle



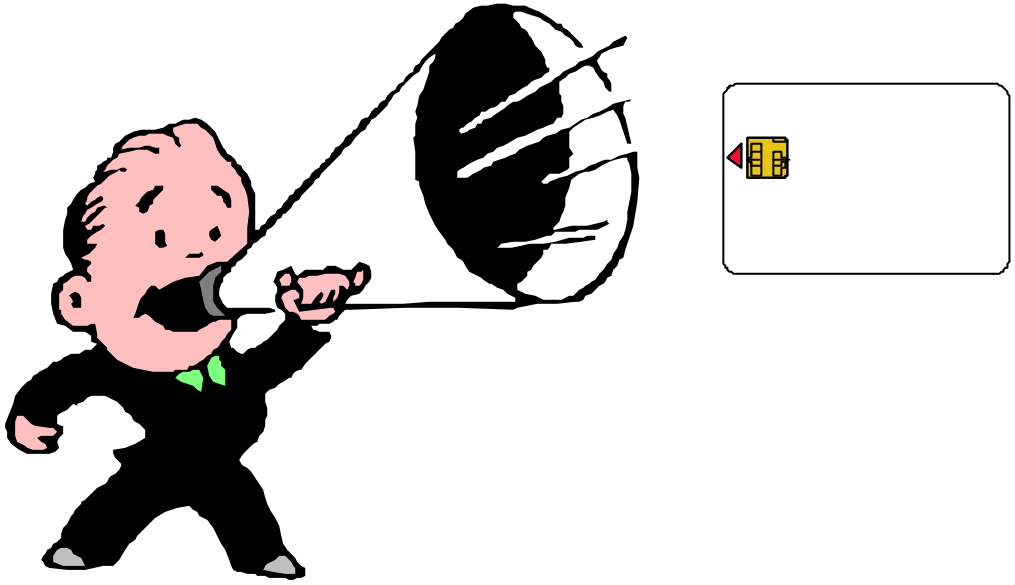
Gemplus is more than a Smart Card Manufacturer ...

Application Players



HOST **READERS** **CARDS**

How to communicate with a smart card ?



Application Software

- Application software developed for customer's needs
  - Design to communicate with card users
  - The fixed program of a microprocessor card (also referred to as OS) is held in ROM and is called the mask.
- Different cards produced on the same microprocessor chip by using different masks.
  - The mask performs application functions, e.g., reducing the value of a purse. Application logic is contained in the mask, e.g., a smart credit card will not complete the transaction until the terminal has executed the correct sequence of checks.

Card OS Structure 1/2

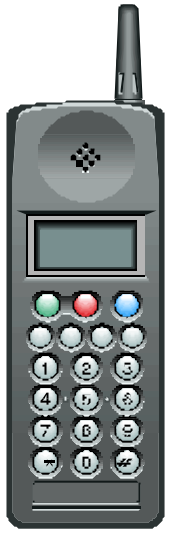
- **From a security point of view, a microprocessor card operating system consists of a set of layers.**
  - **Data access control:**
    - The innermost layer is concerned with handling an access to individual fields and how those fields can be manipulated.
  - **File manager:**
    - File manager deals with the DF (dedicated file)- EF (elementary file) structure and the access rules for those files.
  - **Command handling:**
    - The command manager interprets commands and checks whether that command is valid at this point of the operation.

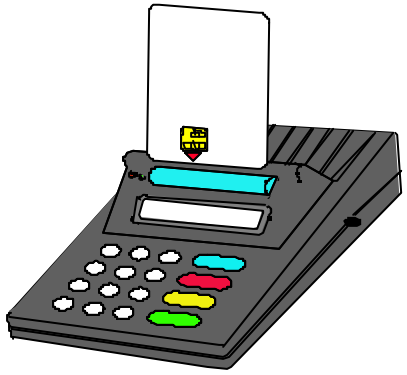
Card OS Structure 2/2

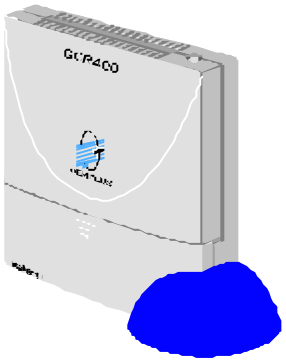
- **Outmost layers:**
  - **Secure messaging:**
    - The functions of this layer are defined by the ISO 7816-4, which is designed to provide both authentication and confidentiality when data are exchanged between reader and card.
  - **The transport manager**
    - Provides the low-level communication functions required by ISO 7816-3.
- **This structure provides a very high level of confidence in the ability to protect data stored on a card under all normal operating conditions.**

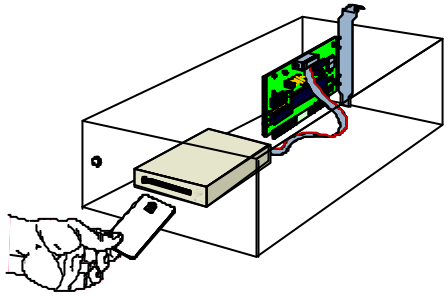
Reader

- Link **between:**
  - **the** host
  - **the** cards



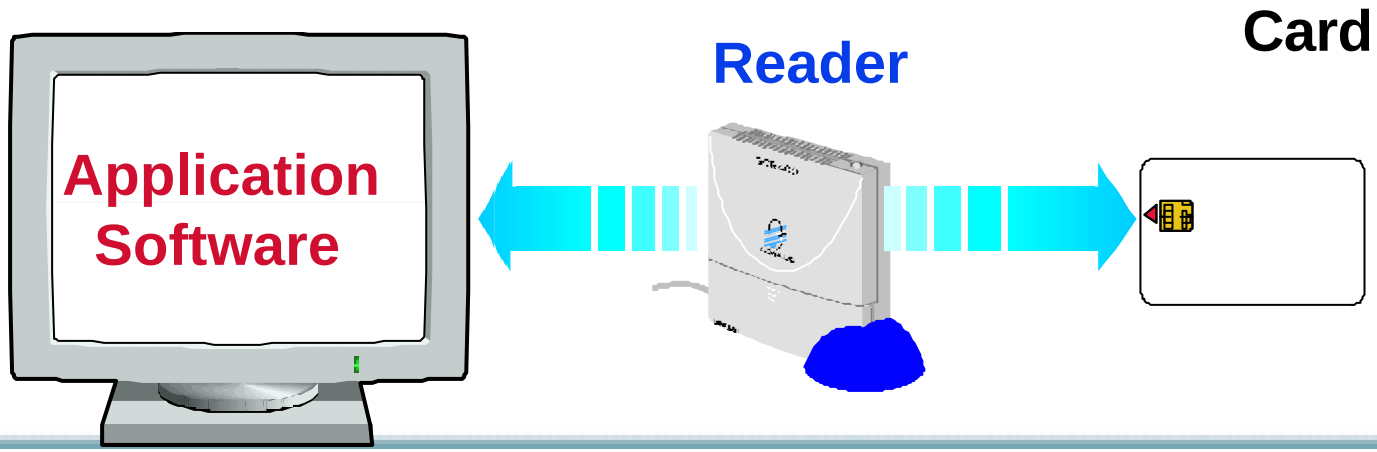






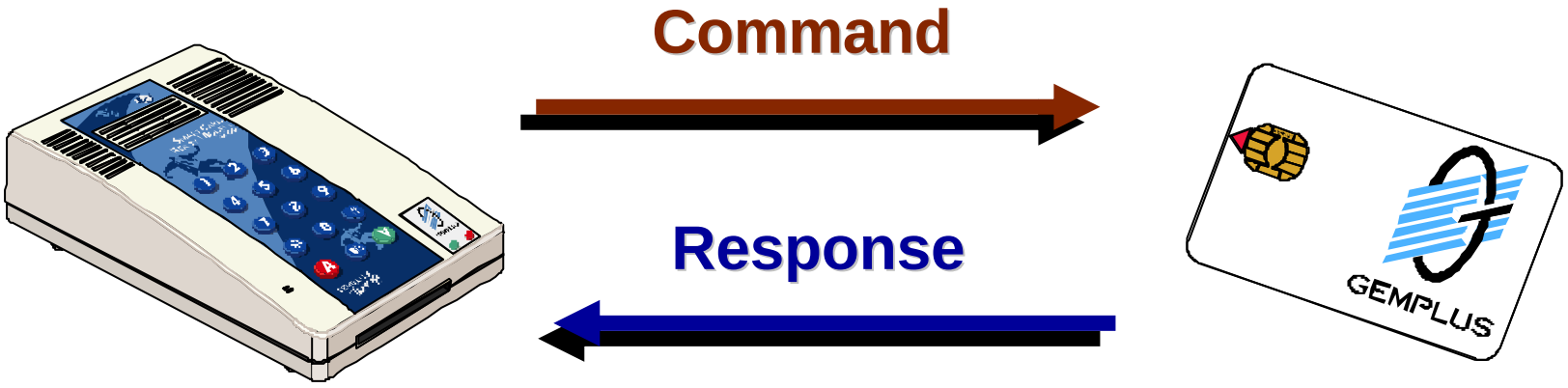
Role of the Reader

- The reader is the interface between the card and the application
  - **It serves as a** translator
  - **It accepts the messages**
    - from the card and
    - from the application software



Messages

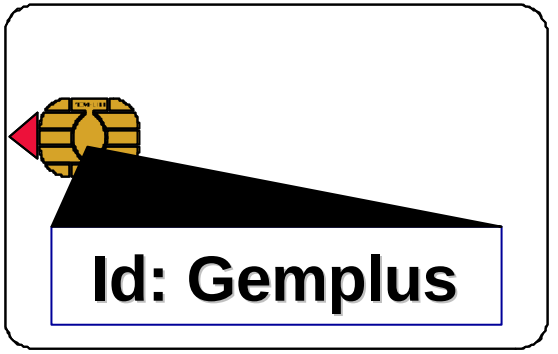
- **The card communicates with the reader by exchanging messages**
- **A message is either**
  - a Command **: From the reader to the card**
  - a Response **: From the card to the reader**



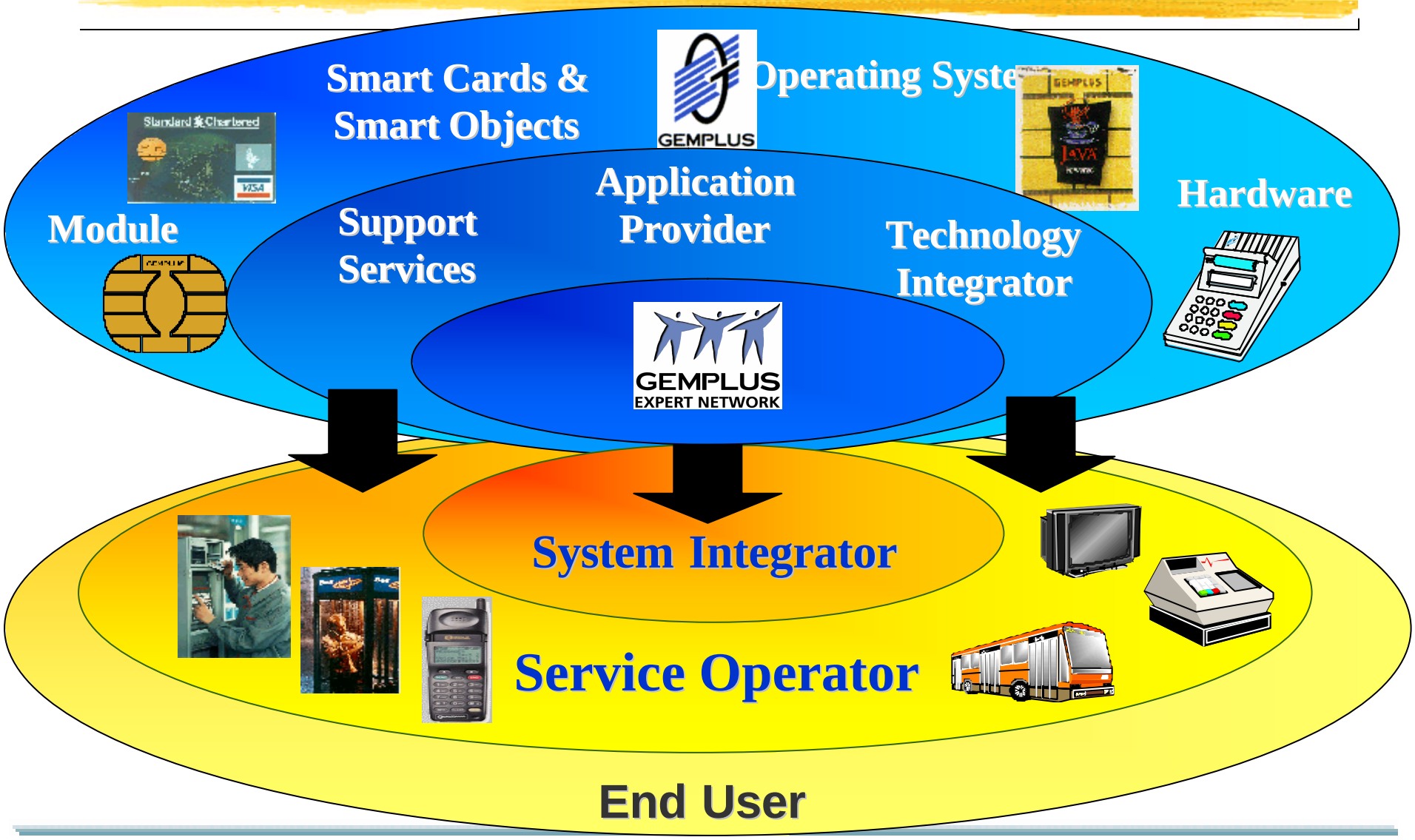
Example

Read Name

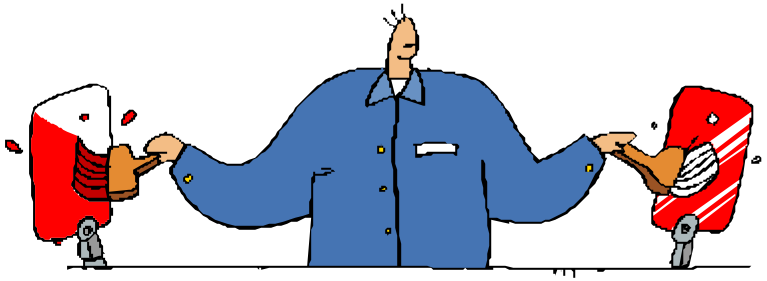
Gemplus



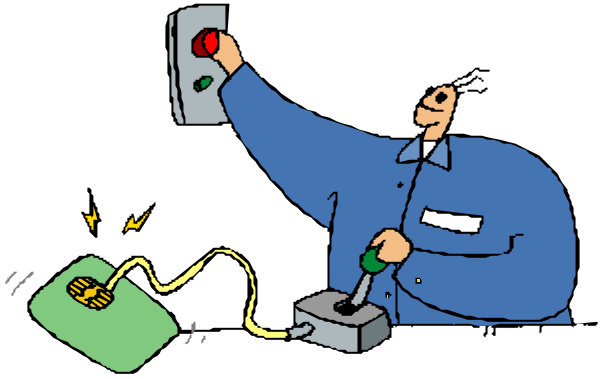
Positioning



Smart Card Personalization

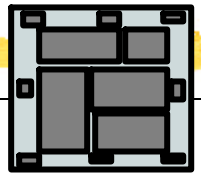


Artwork

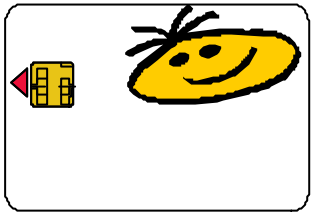


Electrical

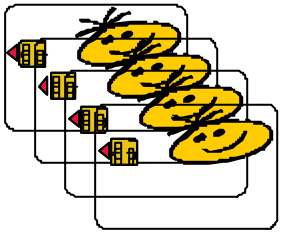
The Players



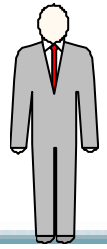
Chip Manufacturer — Electronic Circuit



Card Manufacturer — Initialization, Personalization



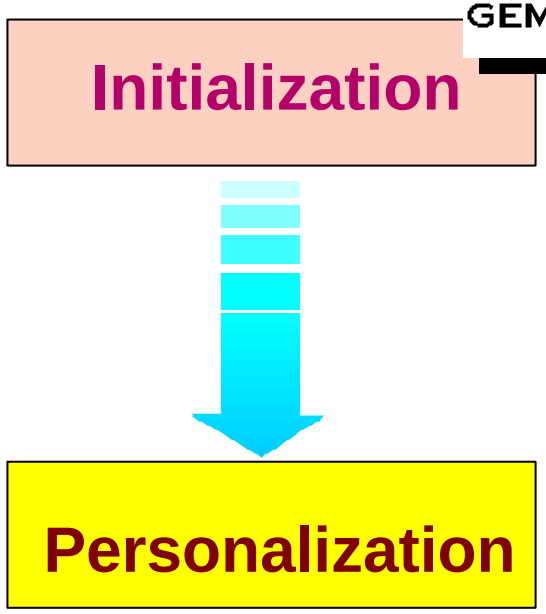
Card Issuer — Cards Distribution (Personalization)



Card Holder

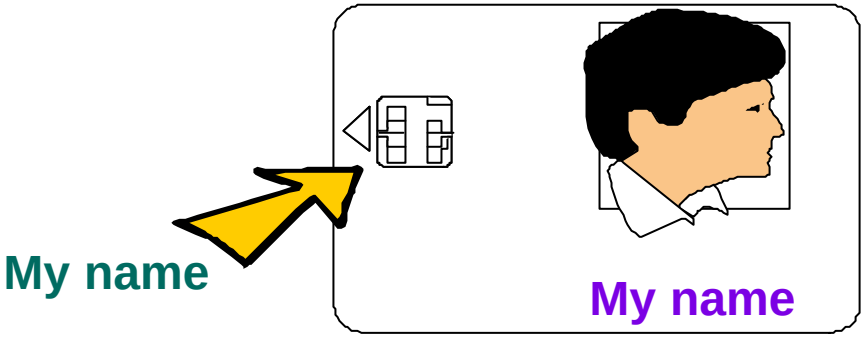
Gemplus Know-How

- Initialization
  - **Card associated with issuer**
  - **Security conditions**
- Personalization
  - Application profile **into every card. The card belongs to one given application.**
  - Cardholder profile **into the card: name, identification number...**



Card personalization

- **Electrical Personalization**
  - **Private / personal data**
  - **Template / file structure**
  - **Diversified keys**
- **Mechanical Personalization**
  - **Photos, holograms, magnetic stripe encoding...**
  - **Embossing**
  - **Text printing**
- **Input file / output file**
- **Packaging & shipping**
  - **Mailer with PIN**



Making each card unique !