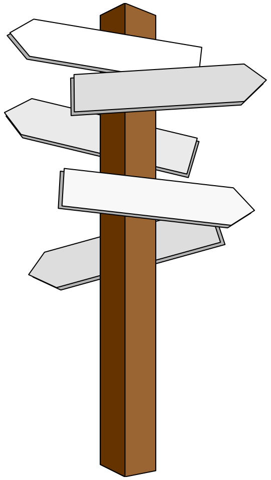
Smart Cards

An introduction on what they are and how they can be used

GEMPLUS™

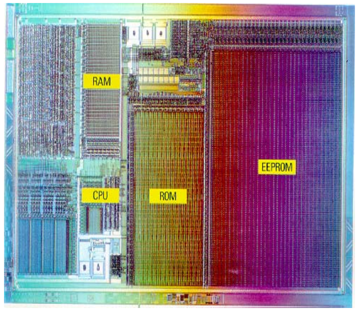
Agenda



- **Introduction to smart cards**
  - Overview
  - What is in a chip?
  - Gemplus know how
  - Types of contact smart cards
  - Why a chip operating system on microprocessor cards ?
- Smart cards and security

What is a Smart Card?

A piece of silicium on a plastic body



Chip

A very secure way of storing a small amount of sensitive data

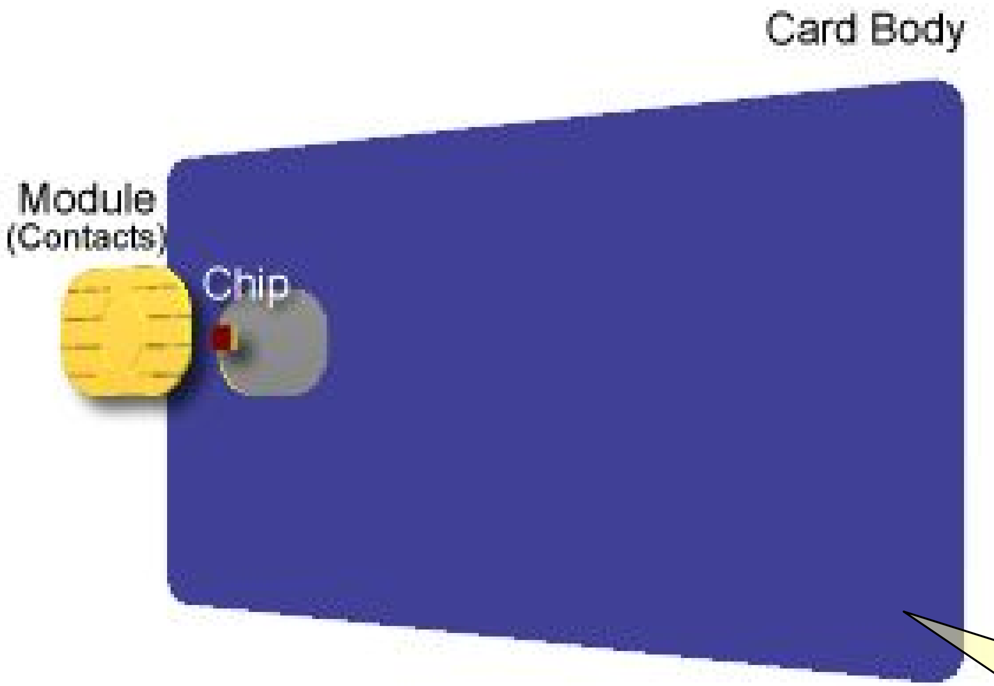
The Smart Card...

- **The smart card stores data and programs**
  - Protection by advanced security features

- **Several types of smart cards**
  - Contact
    - Memory
    - Microprocessor
  - Contactless
  - Hybrid: GemTwin and GemCombi technology

Smart card may mean Microprocessor card only

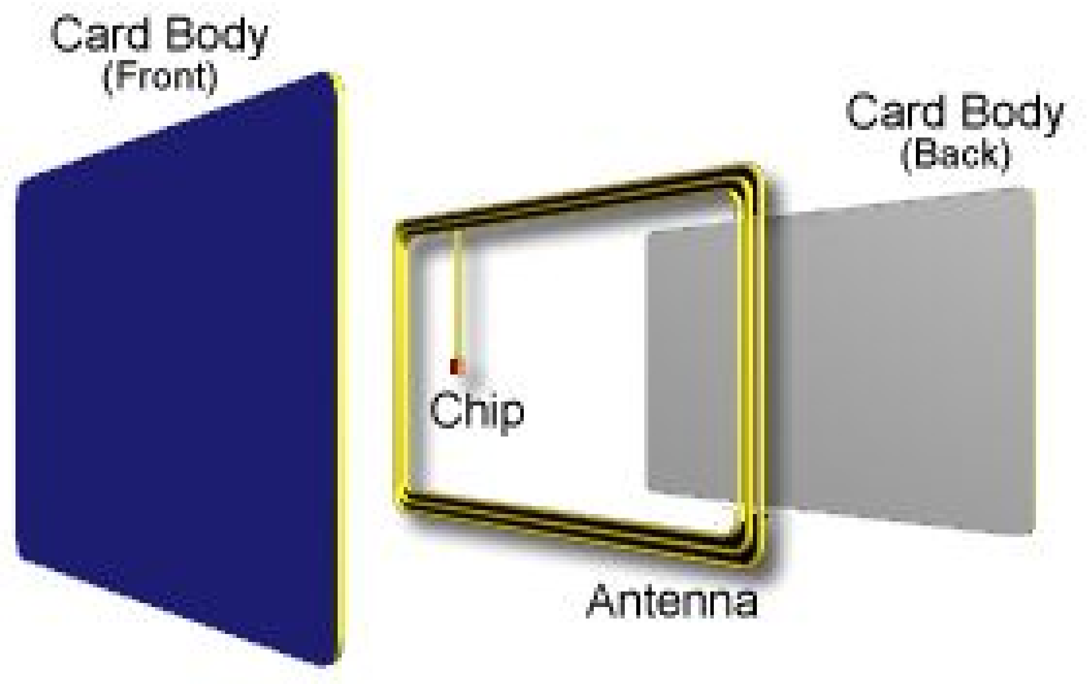
Contact Smart Cards



ISO/IEC 7816

Communication through electrical contacts

Contactless Smart Cards

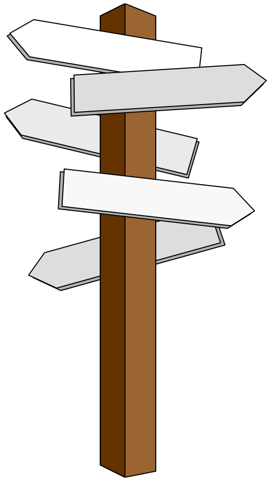


Communication over the air

What is the point of using a card in an application?

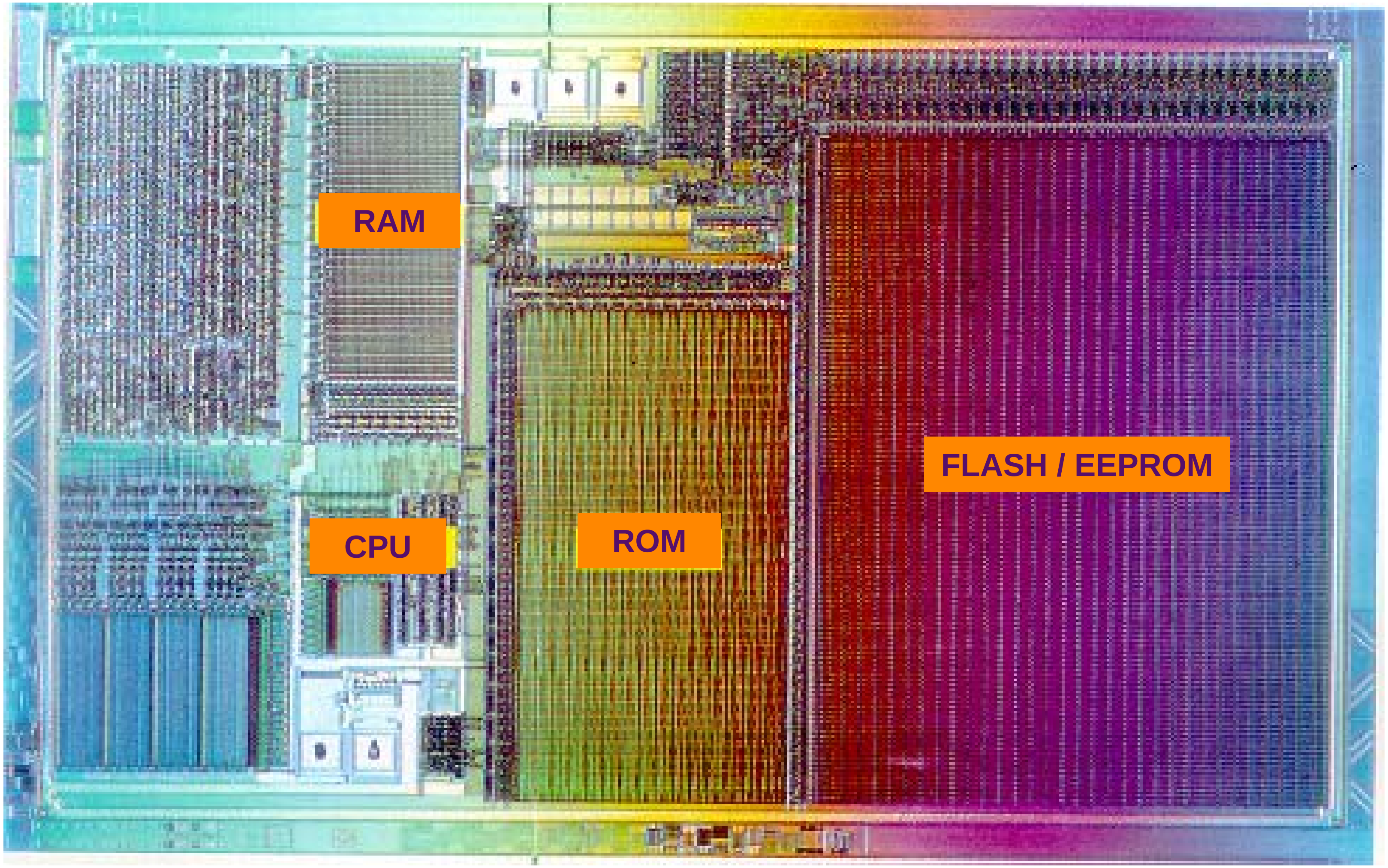
- Security
- Secure off-line transactions
- Easy to use
- Capability to support more than one application
- Portable information
- Marketing tool

Agenda

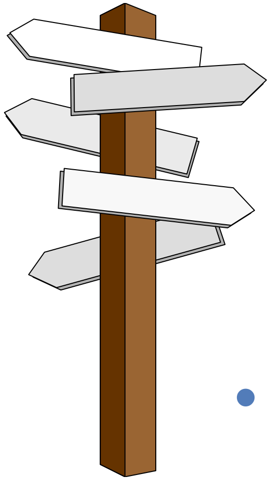


- Introduction to smart cards
  - Overview
  - ☞ **What is in a chip?**
  - Gemplus know how
  - Types of contact smart cards
  - Why a chip operating system on microprocessor cards ?
- Smart cards and security

Microprocessor Card = Microcontroller

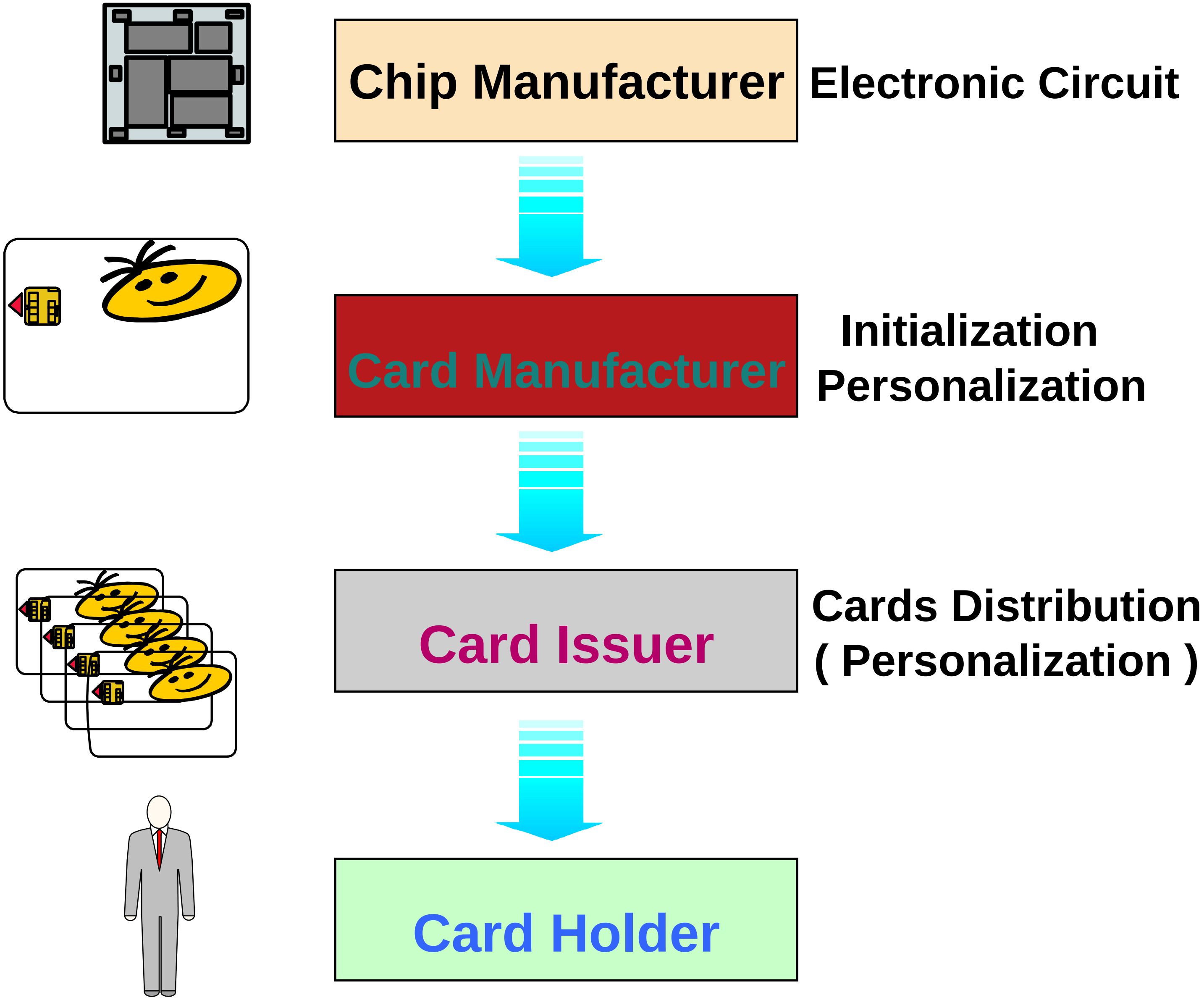


Agenda



- Introduction to smart cards
  - Overview
  - What is in a chip?
  - ☞ **Gemplus know how**
  - Types of contact smart cards
  - Why a chip operating system on microprocessor cards ?
- Smart cards and security

The Players



Chip Manufacturer

Electronic Circuit

Card Manufacturer

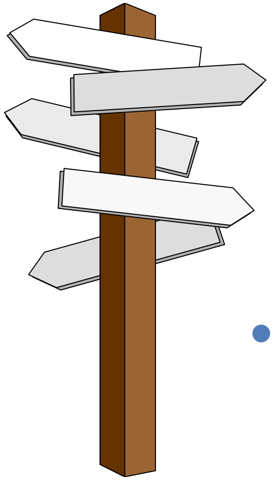
Initialization
Personalization

Card Issuer

Cards Distribution
(Personalization)

Card Holder

Agenda



- Introduction to smart cards
  - Overview
  - What is in a chip?
  - Gemplus know how
  - ☞ **Types of contact smart cards**
  - Why a chip operating system on microprocessor cards ?
- Smart cards and security

Memory Cards

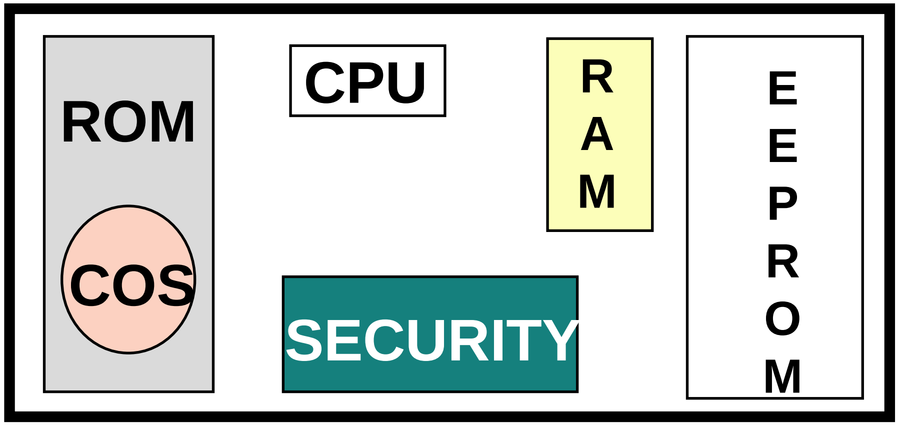
- What for ?
  - Data storage
  - Counter management
- EPROM or EEPROM components
- No microprocessor but some have hardwired logic
- What type of application ?
  - phone cards
  - others...

Microprocessor cards

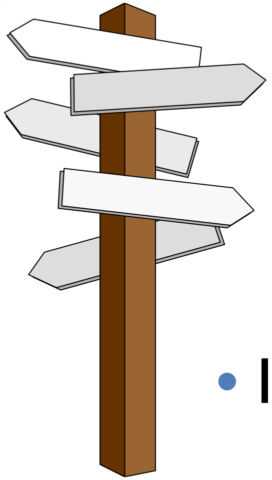
- What for ?
  - Advanced data storage
  - Data processing ("Intelligent" card)
  - High security needs

- Microprocessor card = microcontroller:

- Type of application:
  - e-purse, internet security...



Agenda

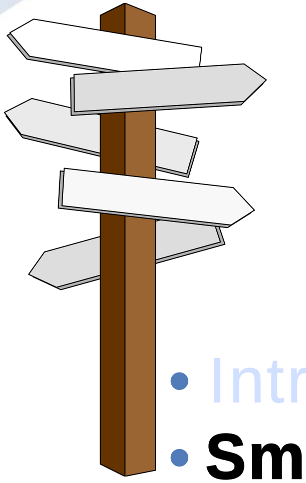


- Introduction to smart cards
  - Overview
  - What is in a chip?
  - Gemplus know how
  - Types of contact smart cards
  - ☞ **Why a chip operating system on microprocessor cards?**
- Smart cards and security

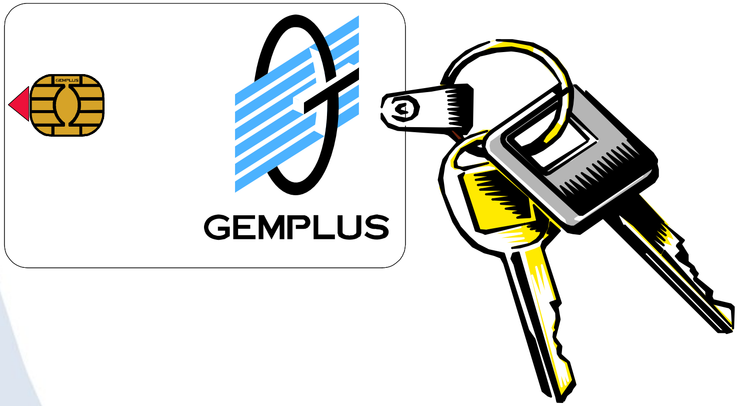
Chip Operating System ⇔ Security

- **Smart card = Black box**
  - Physical device ⇨ Logical device
  - **The COS manages**
    - Predefined & dedicated file structures
      - Key files, secret code file, purse file…
    - A set of dedicated commands
      - Verify, Set Code, Debit, Credit…
    - Cryptographic capabilities
      - DES, RSA…

Agenda



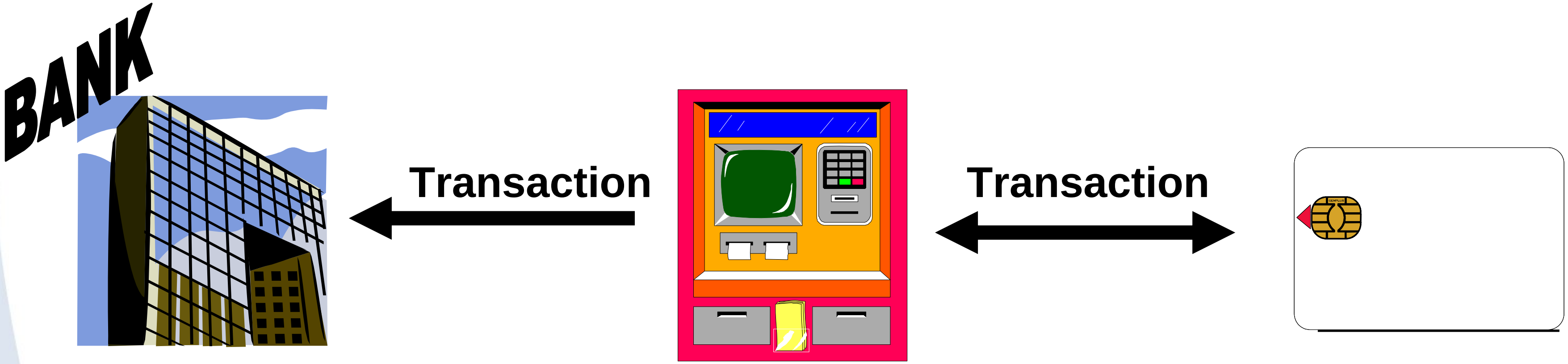
- Introduction to smart cards
- **Smart cards and security**
  - Application security requirements and how can we meet these requirements
  - A few words about cryptography



Authentication

- What is Authentication?
  - Verification that a terminal or a card is genuine

- Authentication - what for?
  - To answer the following questions...



Transaction

Transaction

Is it a real transaction?

Is it a real card?

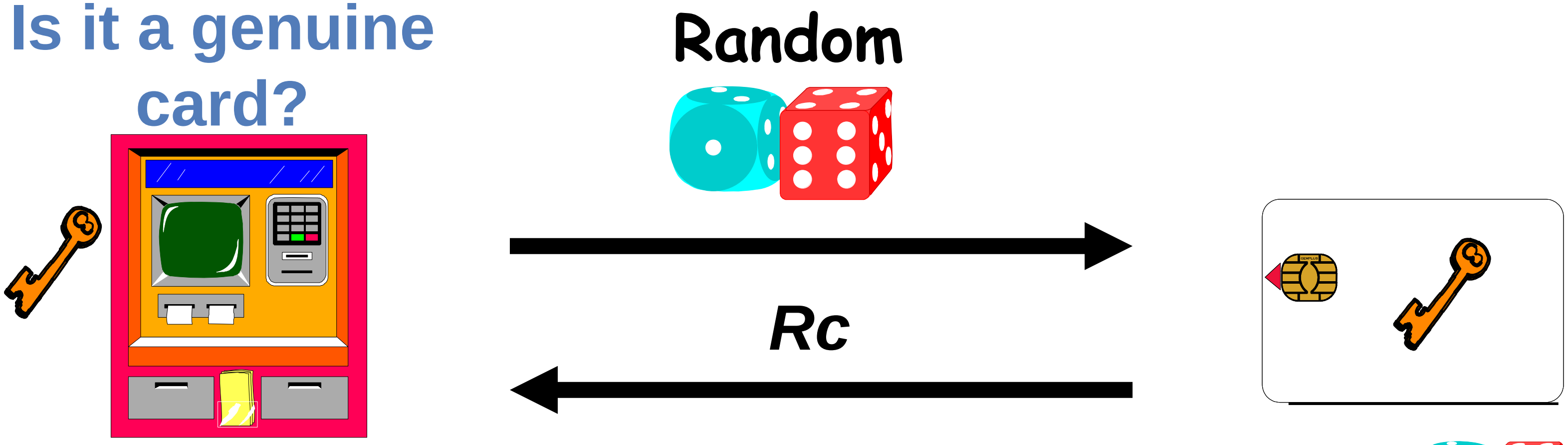
Is it a real terminal?

Meeting The Authenticity Criteria

- Card/Terminal authentication:
  - the terminal/card verifies that the card/terminal knows the right key

- Example:

Is it a genuine card?



Random

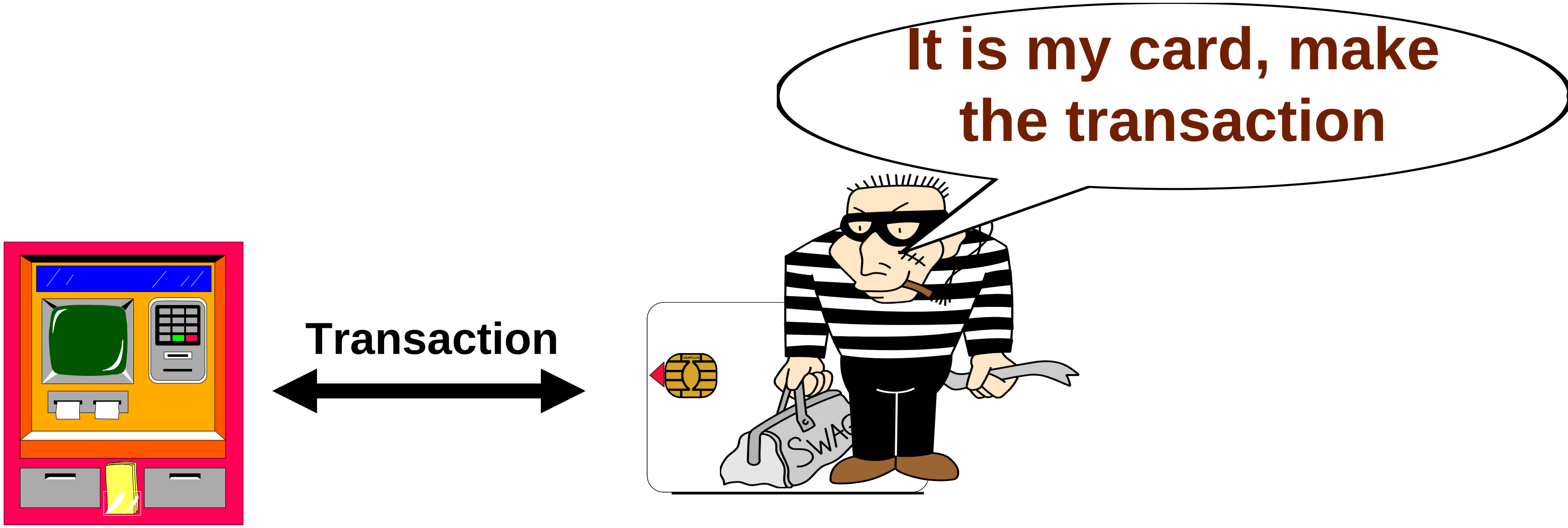
Rc

- ***Rt*** = Algo(🎲🎲 , 🔑)
- ***Rc*** = **Rt ?**

Rc = Algo(🎲🎲 , 🔑)

Identification

- Identification - what for?
  - To verify the identity of the card (serial number, cardholder’s identity...)



Transaction

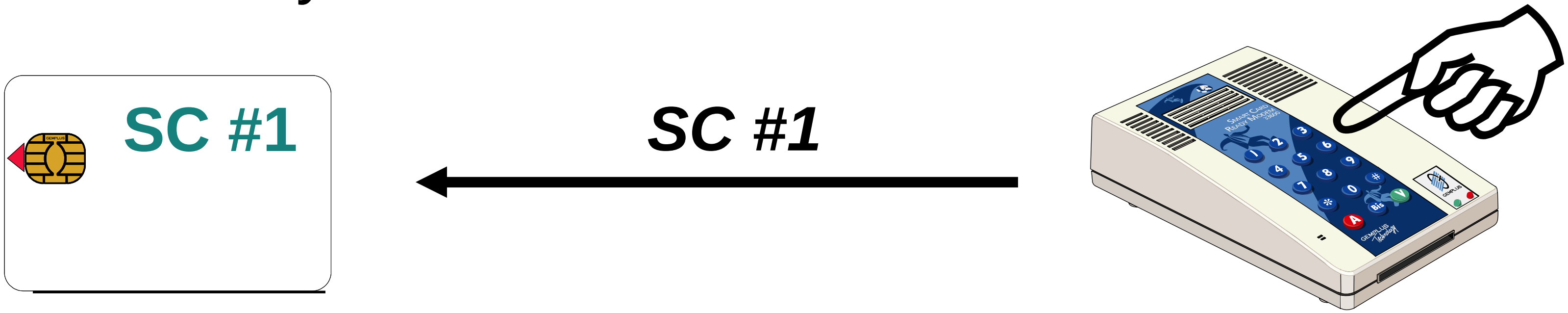
It is my card, make the transaction

Am I talking with the real cardholder?

Meeting The Identification Criteria

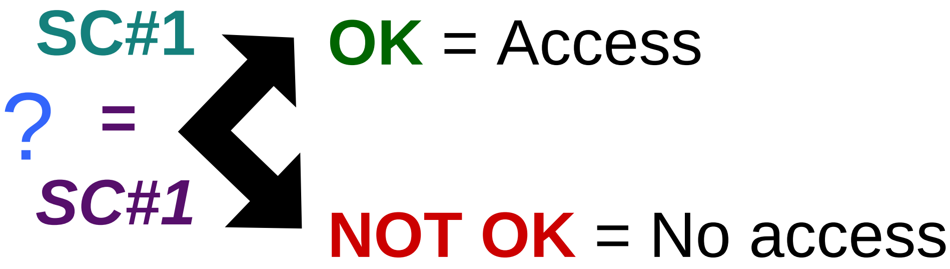
- Stored in the card

- A secret code SC#1 is presented to the card and then checked by the card:



SC #1

SC #1



SC#1

? =

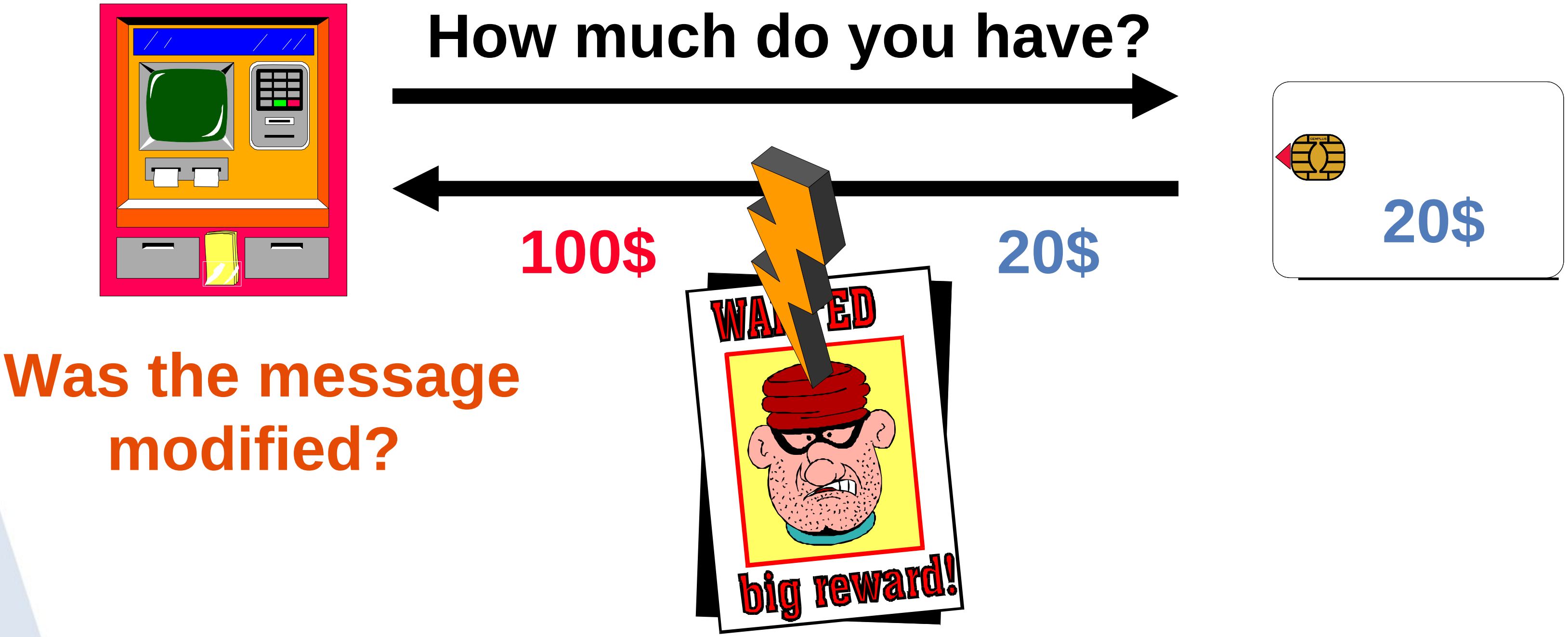
SC#1

OK = Access

NOT OK = No access

Integrity

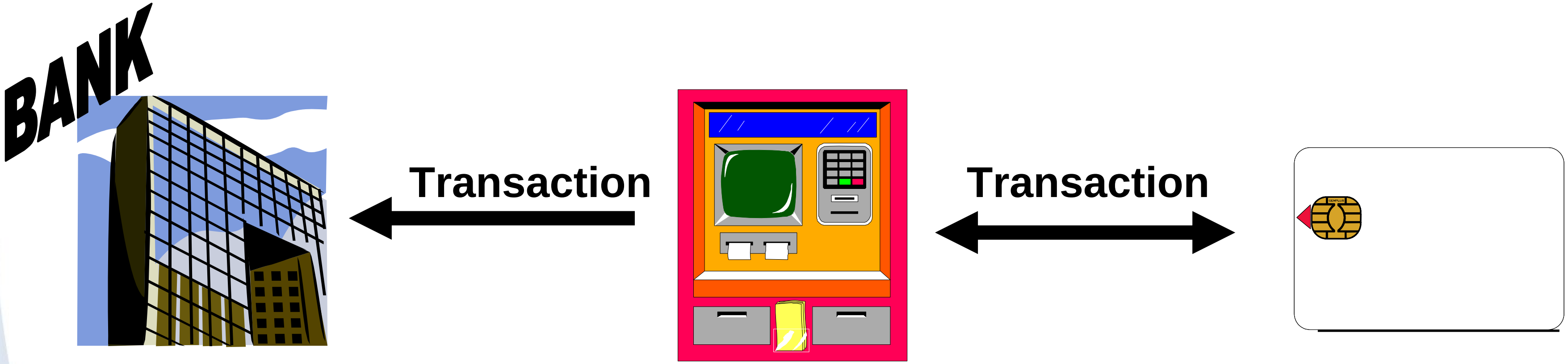
- Integrity - what for?
  - To ensure the message has not been modified
    - Intentionally or unintentionally



Was the message modified?

Non-Repudiation

- Non-repudiation - what for?
  - To prevent the denial of a transaction



Transaction

Transaction

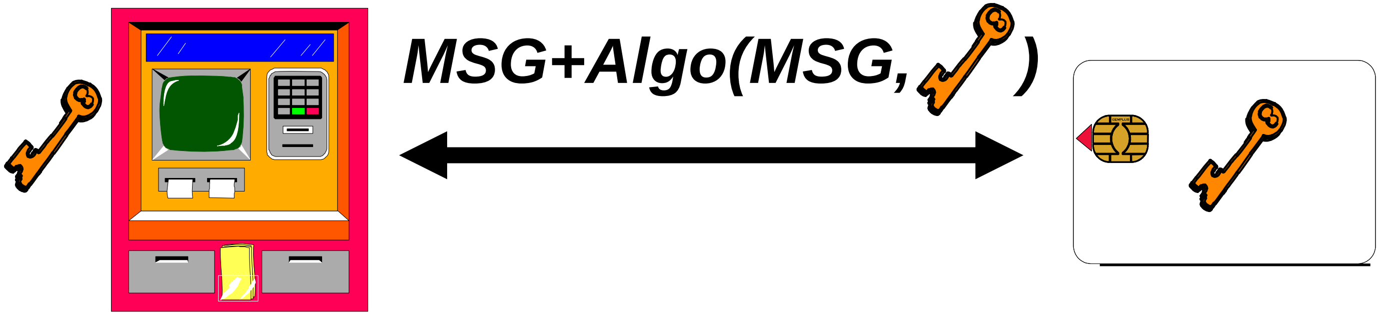
What was the exact content of the transaction?

I never made this transaction!!

Meeting The Integrity And Non-Repudiation Criteria

- Add to the message/transaction (plain text), the result of a cryptographic calculation made on it:
  - Cryptographic checksum
  - Message Authentication Cryptogram
  - Signature...

- The Receiver recomputes the signature with his key and the message he receives



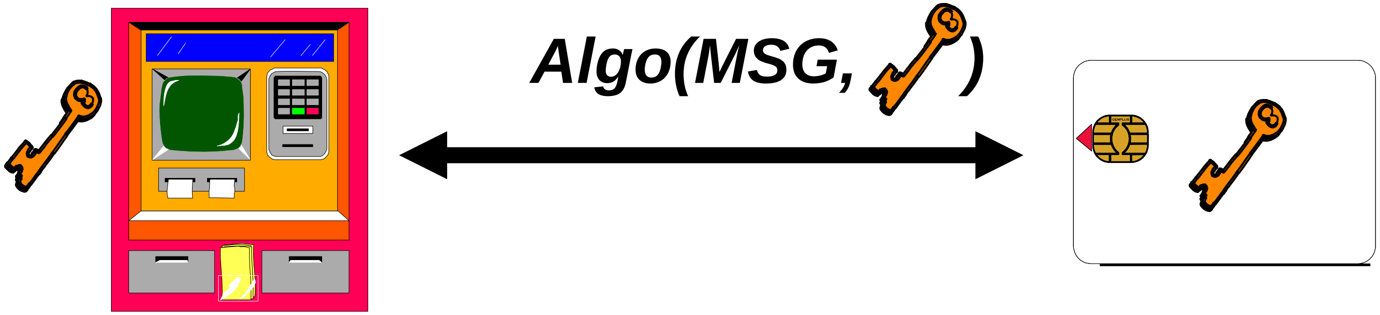
Confidentiality / Privacy

- Confidentiality - what for?
  - To keep information secret from all but those authorized

♋&●□♏♒♋♍♌
?
"Message"
"Message"

Meeting The Privacy Criteria

- The message encrypted



Security of the Chip

- Security Detectors: chip becomes mute when an external attack is detected

- Very difficult to access the chip's internal signals

- Irreversible physical and logical locks after each step in Manufacturing process

Security architecture

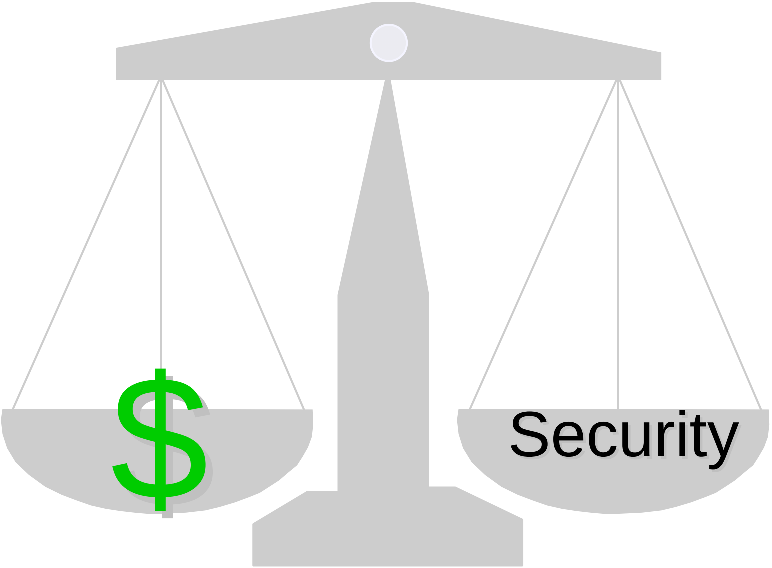
Your application will have the security level of its weakest element!

- Security management
  - Not only on the cards
  - Throughout the application

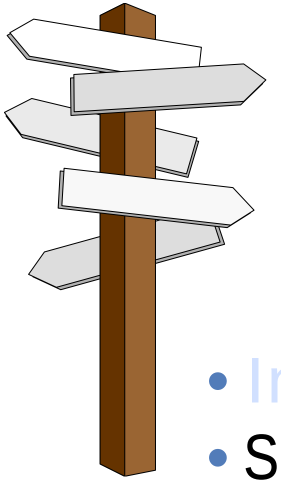
- Good questions when designing security architecture
  - How are system entities authenticated ?
  - How is integrity of system data managed ?
  - How is non-repudiation of data met ?
  - How is system-data kept confidential ?

Summary

- Security functions processed in SAMs
- Audit trail for security functions
- Use security algorithm as part of security scheme
  - authentication
  - signature
    - authenticity
    - integrity
    - non-repudiation
  - enciphering of data
    - confidentiality



Agenda

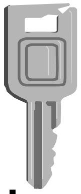


- Introduction to smart cards
- Smart cards and security
  - Application security requirements and how can we meet these requirements
  - ☞ **A few words about cryptography**

Definitions

- Secret Key Algorithm

1 Key



- **Same key for encryption & decryption**

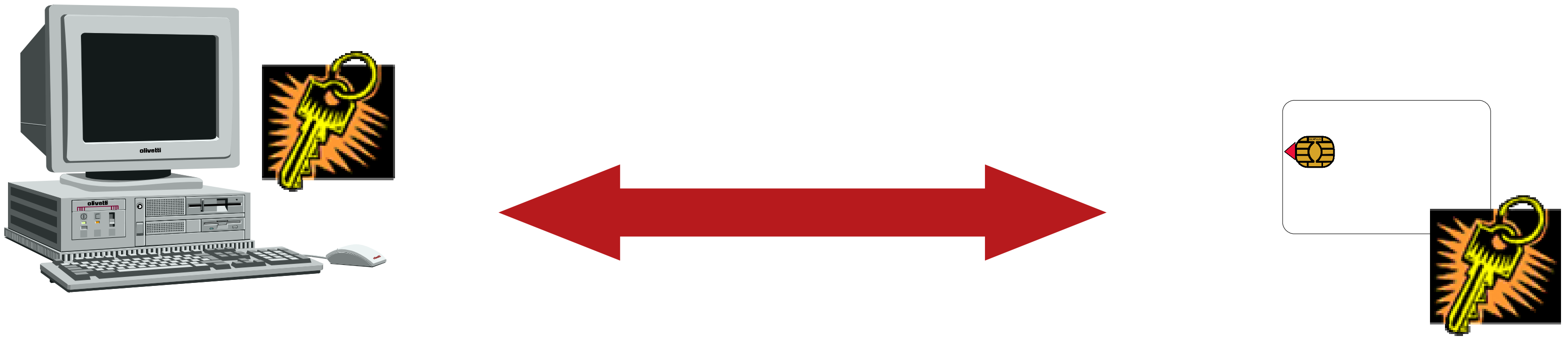
- Public Key Algorithm

2 Keys

- **One key for encryption**
- **Another key for decryption**

Secret Key Principles

- Sender and Receiver share the SAME key

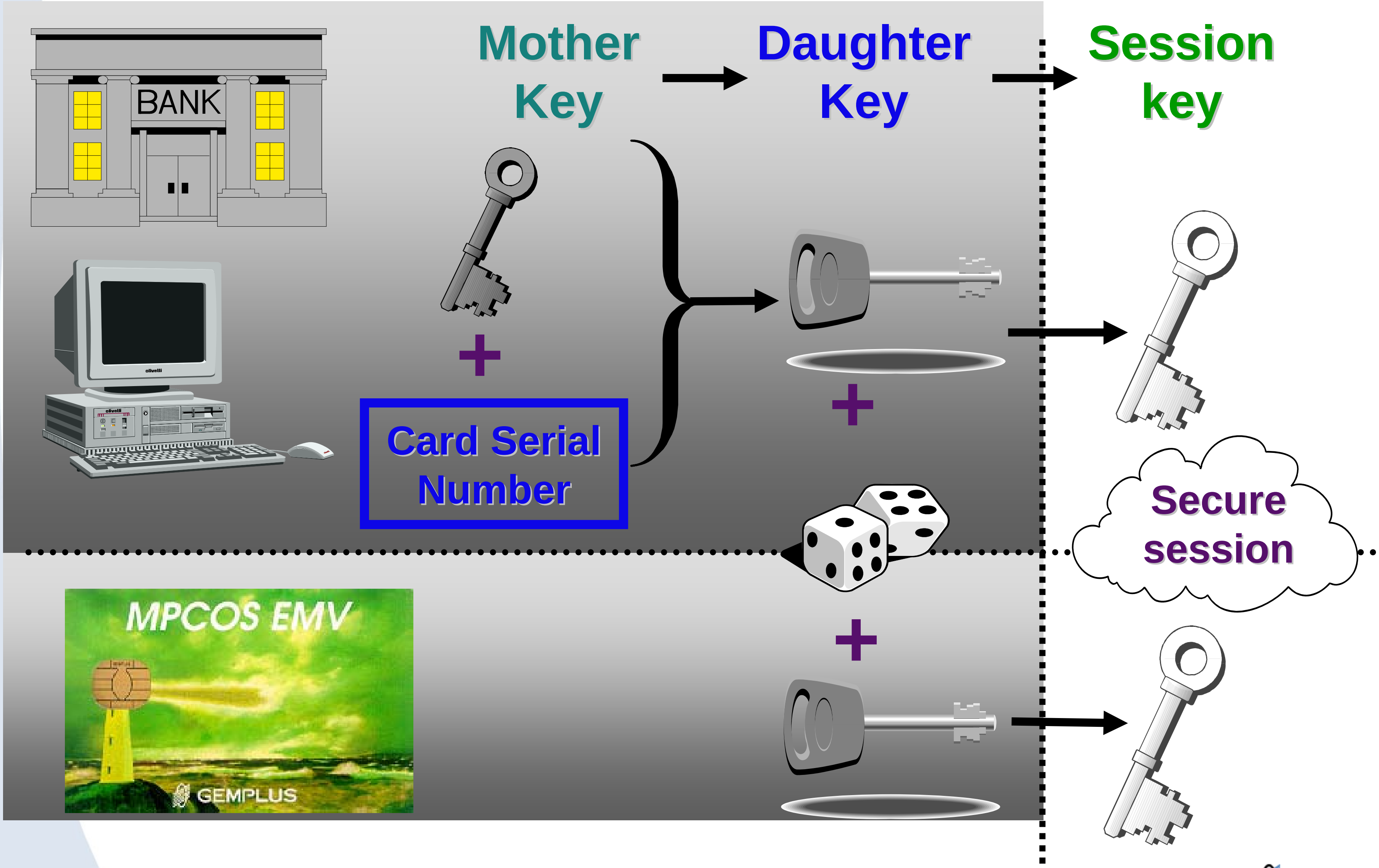


Same key in every card and in every terminal :

KEY DISTRIBUTION IS AN ISSUE!

→ **DIVERSIFICATION**

Key diversification

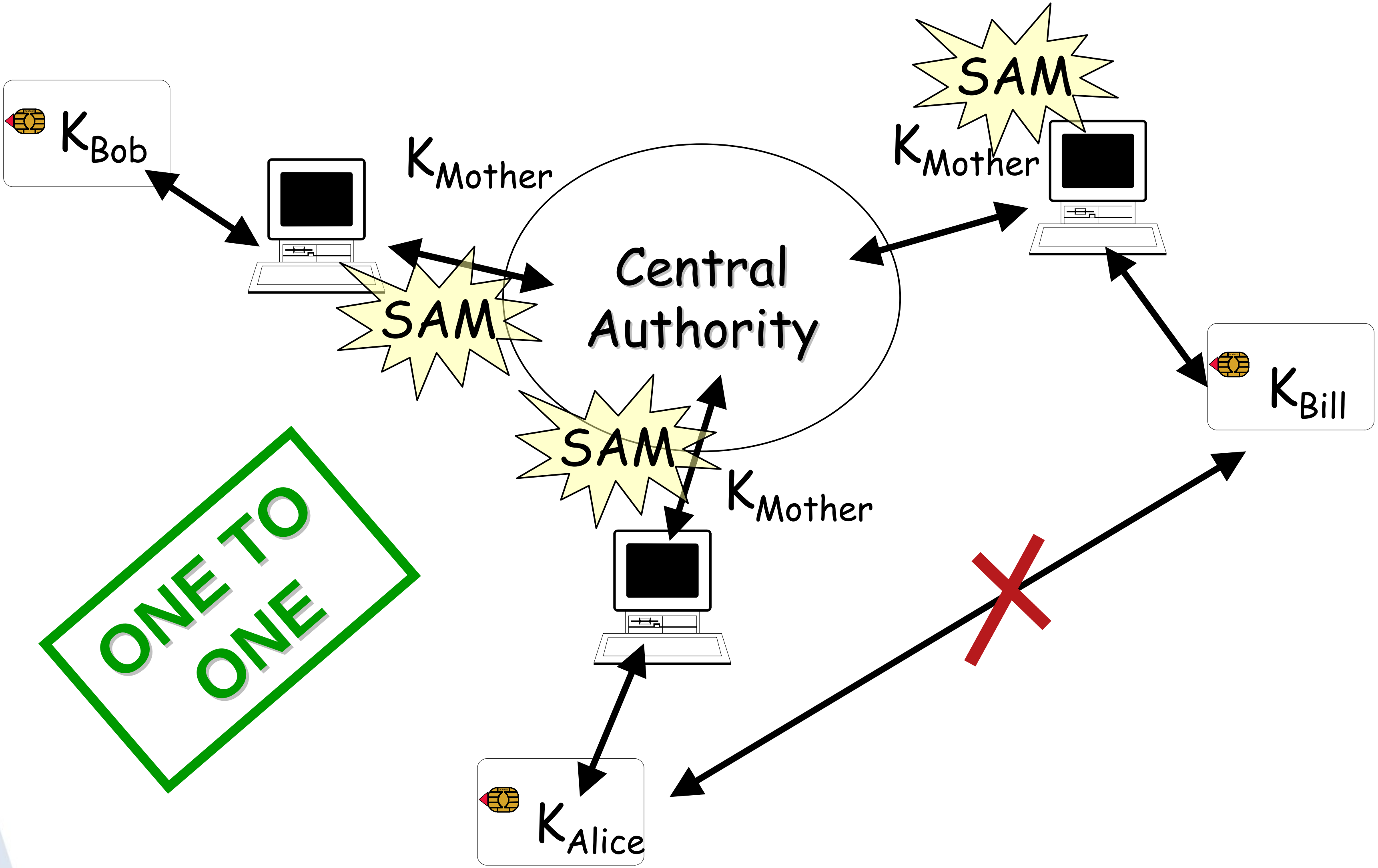


Mother Key → Daughter Key → Session key

Card Serial Number

Secure session

Key Distribution


K_{Bob}
K_{Mother}
SAM
SAM
K_{Mother}
Central Authority
SAM
K_{Mother}
K_{Bill}
ONE TO ONE
K_{Alice}