EUROSMART
European Smart Card Industry Association

WHAT FUTURE FOR CONTACTLESS CARD SECURITY ?

Alain Vazquez
(alain.vazquez@louveciennes.sema.slb.com)

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Contents

- ☞ Major contactless features : summary
- Contactless major constraints
- Major security issues
  - Tamper resistant device
  - Authentication
  - Integrity
  - Confidentiality
  - Security evaluation (CC, PP, …)
- What future for the contactless card security

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

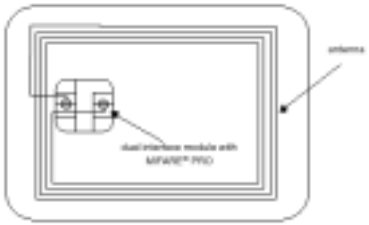
Contactless IC overview

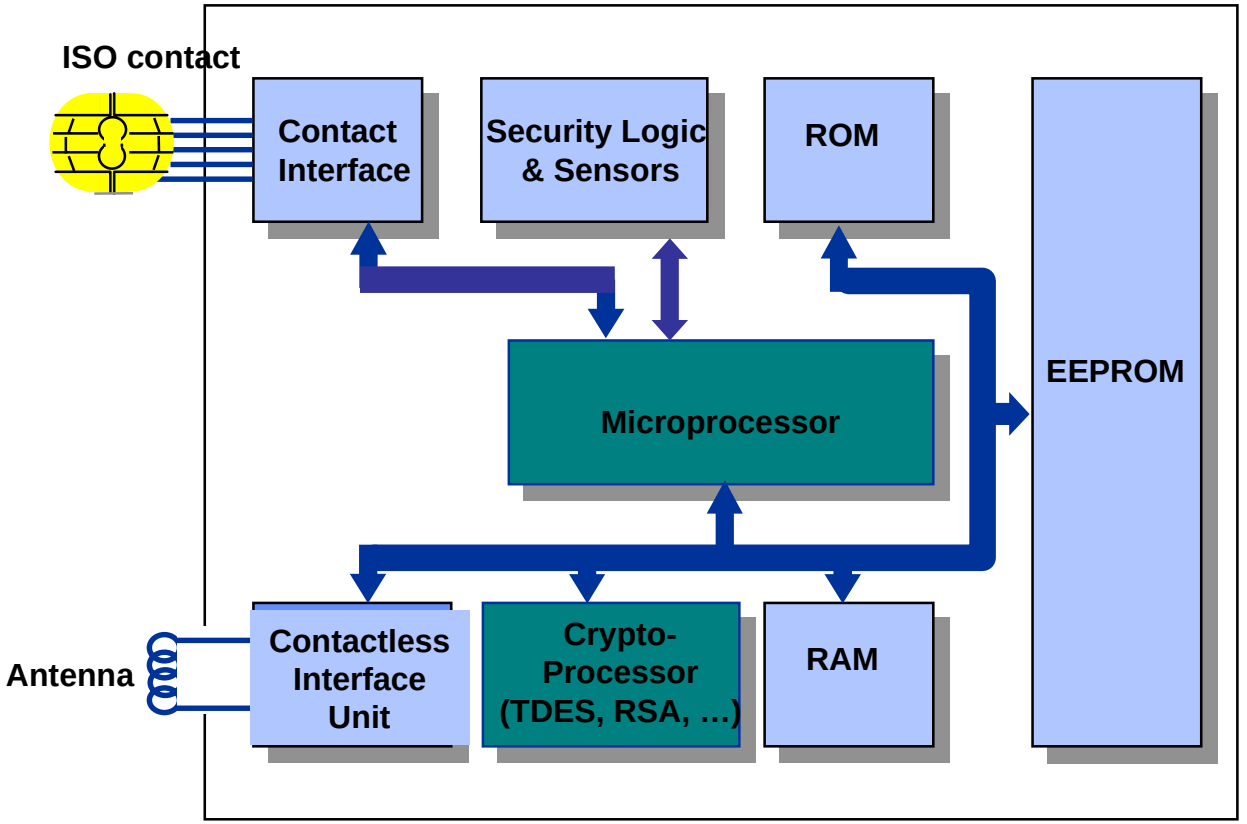
- Based on Smart Card IC with an RF interface (ISO 14443-x)
- Readers supply low impedance electromagnetic field at 13,56 MHz to :
  - Generate power supply for IC
  - Support Clock and data exchange using ASK modulation
- Modulation rate : 100% (type A) or 10% (type B)
- Communication distance (0-10 cm typical)
- High speed serial communication (106 Kb/s – 424 Kb/s)
- Anti-collision protocol
- Extended operating voltage range (typical 2.7 – 5.5 V)

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Diagram (dual interface)

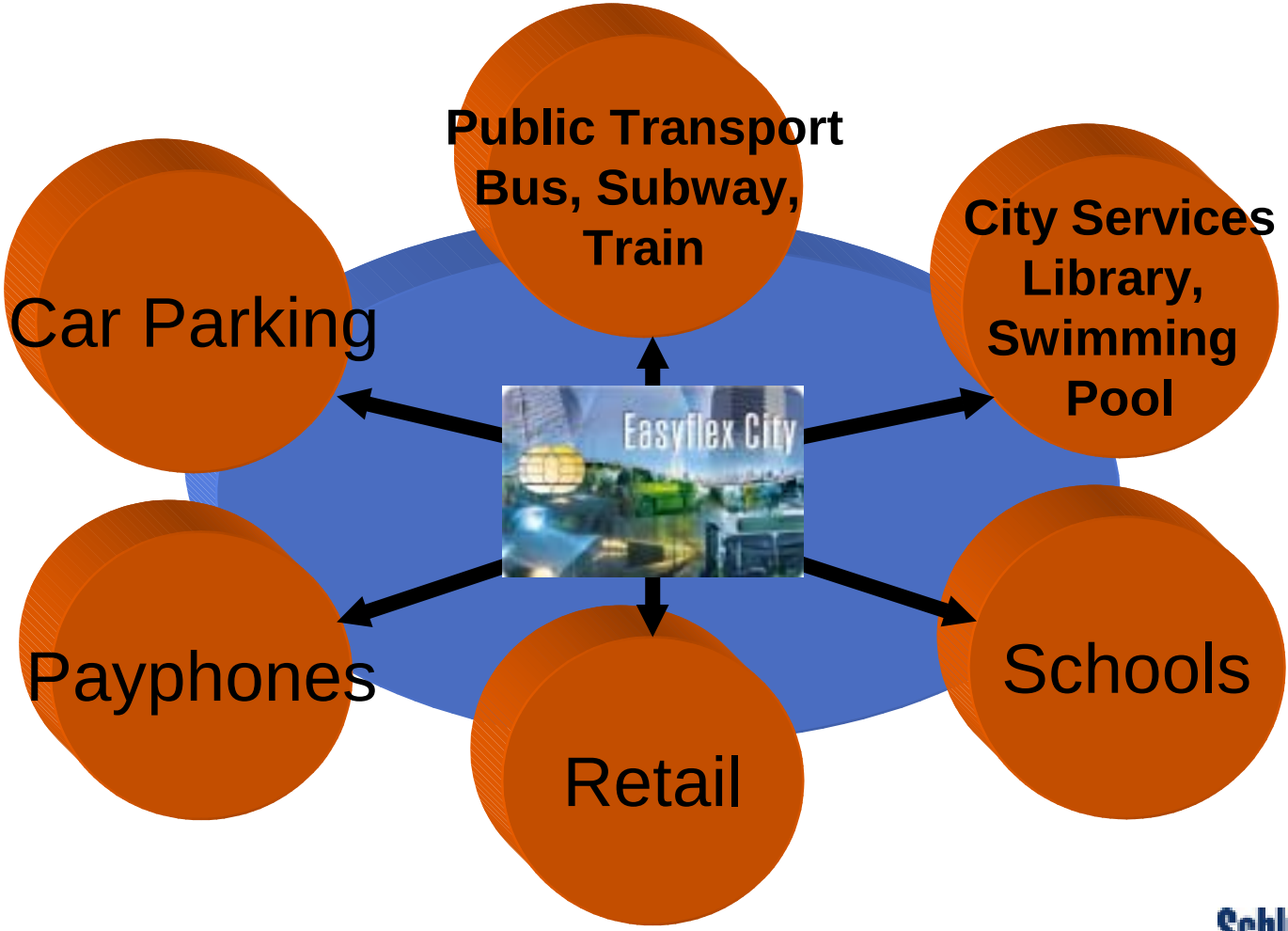




SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Targeted market



SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Contents

- Major contactless features : summary
- ☞ Contactless major constraints
- Major security issues
  - Tamper resistant device
  - Authentication
  - Integrity
  - Confidentiality
  - Security evaluation (CC, PP, …)
- What future for the contactless card security

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Contactless constraints

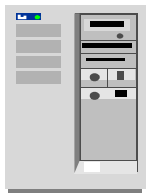
- **Ability to perform a "transaction" within a maximum of 150 ms time including :**
  - **Dialogue establishment with the reader (anti-collision detection)**
  - **Internal computation (which may include cryptographic processing)**
  - **Data exchange (1O6 kb/s) in half duplex**
- **Low power consumption : typically 2 to 5 mW**
  - **Internal CPU clock**
  - **Adapted design technology (submicron)**

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Security attacks

Host

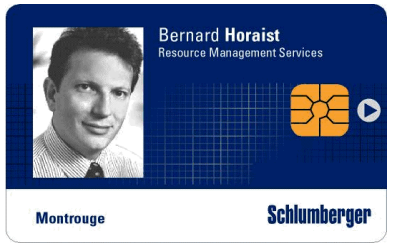


Reader

Man in the middle

Eavesdropping

Tampering



Telepickpocketing

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Contents

- Major contactless features : summary
- Contactless major constraints
- ☞ Major security issues
  - Tamper resistant device
  - Authentication
  - Integrity
  - Confidentiality
  - Security evaluation (CC, PP, …)
- What future for the contactless card security

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Tamper resistant device

- **Tamper resistant device**
  - **Objectives : to prevent the outside from :**
    - **Reading what must be kept secret**
    - **Tampering any stored data**
  - **Contactless attacks**
    - **Most of them are common to "contact only" cards**
    - **Some of them may be re-enforced because of electromagnetic radiation (power, clock, data, …)**

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Attacks 1/2

- Attacks (common with contact cards)
  - Physical
    - Microprobing : access to chip with test or optical means
    - Test mode recovery : recover initial test bit statement
    - Reverse engineering : layout, data, address reconstruction
    - Environmental monitoring ; temperature, light, …
  - Electrical
    - SPA/DPA : statistical attacks based on power analysis
    - Timing : execution time depending on input parameters and secret data involved
  - Logical
    - Software : taking advantage (through the input) of the vulnerability of OS, embedded

EUROSMART
European Smart Card Industry Association

Attacks 2/2

- Attacks (re-enforced by RF interface)
  - Electrical
    - EMA : Electromagnetic Analysis
      - Internal chip radiation
      - RF radiation (13 MHz range)
    - Power drops and short cuts (nota)
      - Available power magnitude highly variable -> chip extended tolerance (2.7 -> 5.5 typical)
      - Clock supply glitches

(nota) intended to corrupt the normal transfer of data between CPU and memory

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Any countermeasures ? 1/2

- **Hardware**
  - Strong protection layers (test mode recovery)
  - Random logic design (reverse engineering recovery)
  - Metal shielding (EMA, light, microprobing, …)
  - Tamper sensors to warn the OS against attacks
  - On chip filters (glitches, transient signals, …)
  - True random generators
  - Unpredictable chip current power consumption
- **Software**
  - Memory address scrambling/memory management (firewall)
  - Random software execution

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Any countermeasures ? 2/2

- **Countermeasures efficiency**
  - To fight against one attack, generally many countermeasures may be required but :
    - Additional hardware modules will increase power consumption
    - Additional software will slow the execution process
  - One compromise must be found between efficiency and contactless requirements (execution time, power requirements)

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Integrity

- **Definition**
  - Confidence that the received data stream is actually the posted stream
- **Mechanisms involved depend on the security level required**
  - Basic protocol feature (Data associated with a CRC check within a frame) eg ISO 14443-4
  - Hash code (one way function)
    - SHA-1 (160 bit code)
    - MD5 (128 bit code)
    - Ripemd (160 bit code)

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Authentication 1/5

- Definition
  - Mechanism that allows you to prove who you are actually
- Mechanisms (security level dependent)
  - ID presentation (identification)
  - Cryptographic techniques
    - Symmetrical (DES encryption, MAC, …)
    - Asymmetrical (digital signature RSA, DSA, ECDSA, …)

Remark : In most cases, authentication and integrity are performed at the same time

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Authentication 2/5

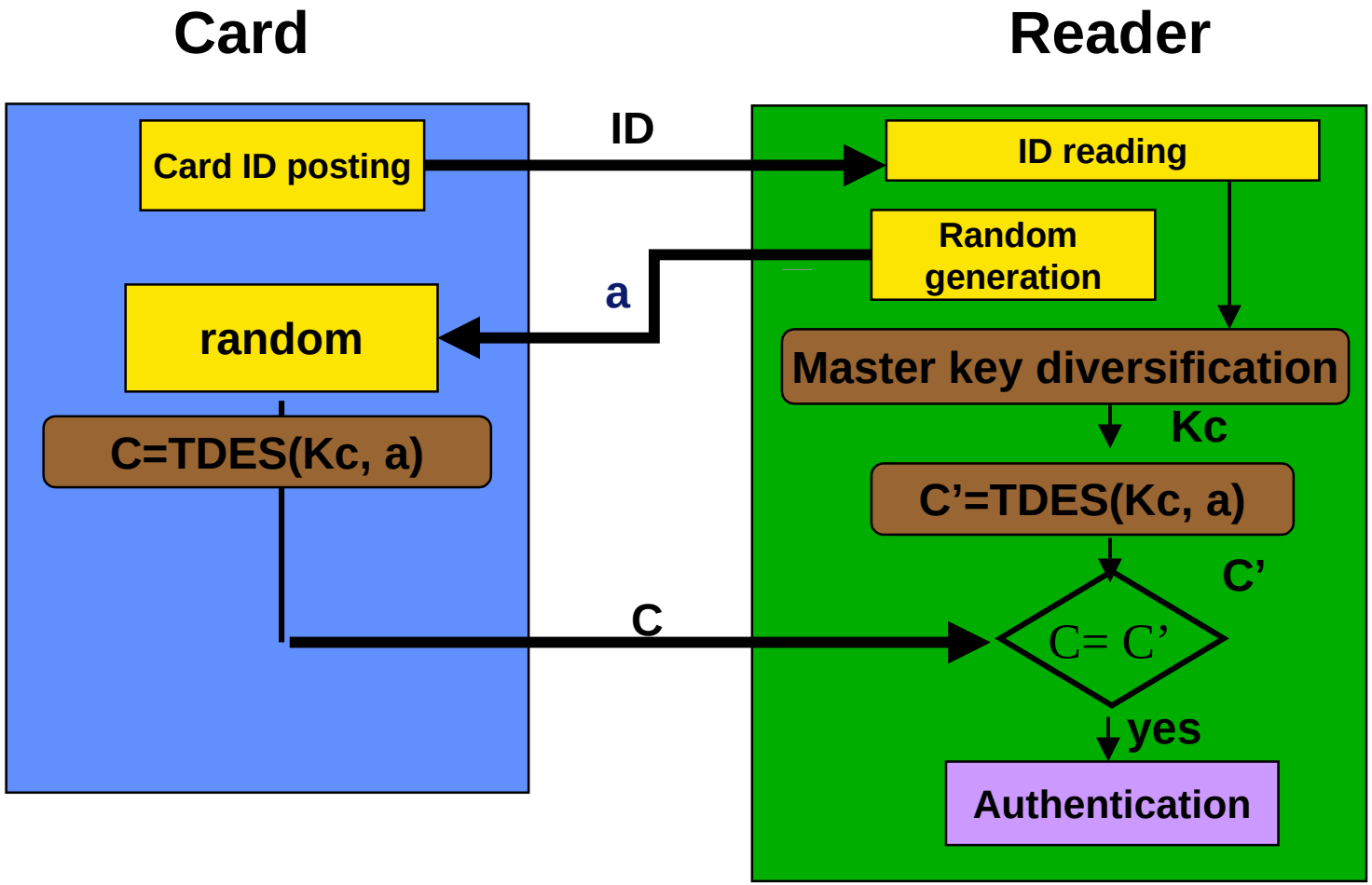
- User by the card (theft prevention)
  - Not feasible in most cases
    - No Pin code typing
    - No biometric mechanisms (e.g. fingerprint)

Nota : If required, authentication can be performed by out of band mechanisms (ex : railway ticket inspector)

- Card vs reader Typical requirements
  - Tranportation : card is authenticated by the reader
  - Finance : mutual authentication is required

SchlumbergerSema

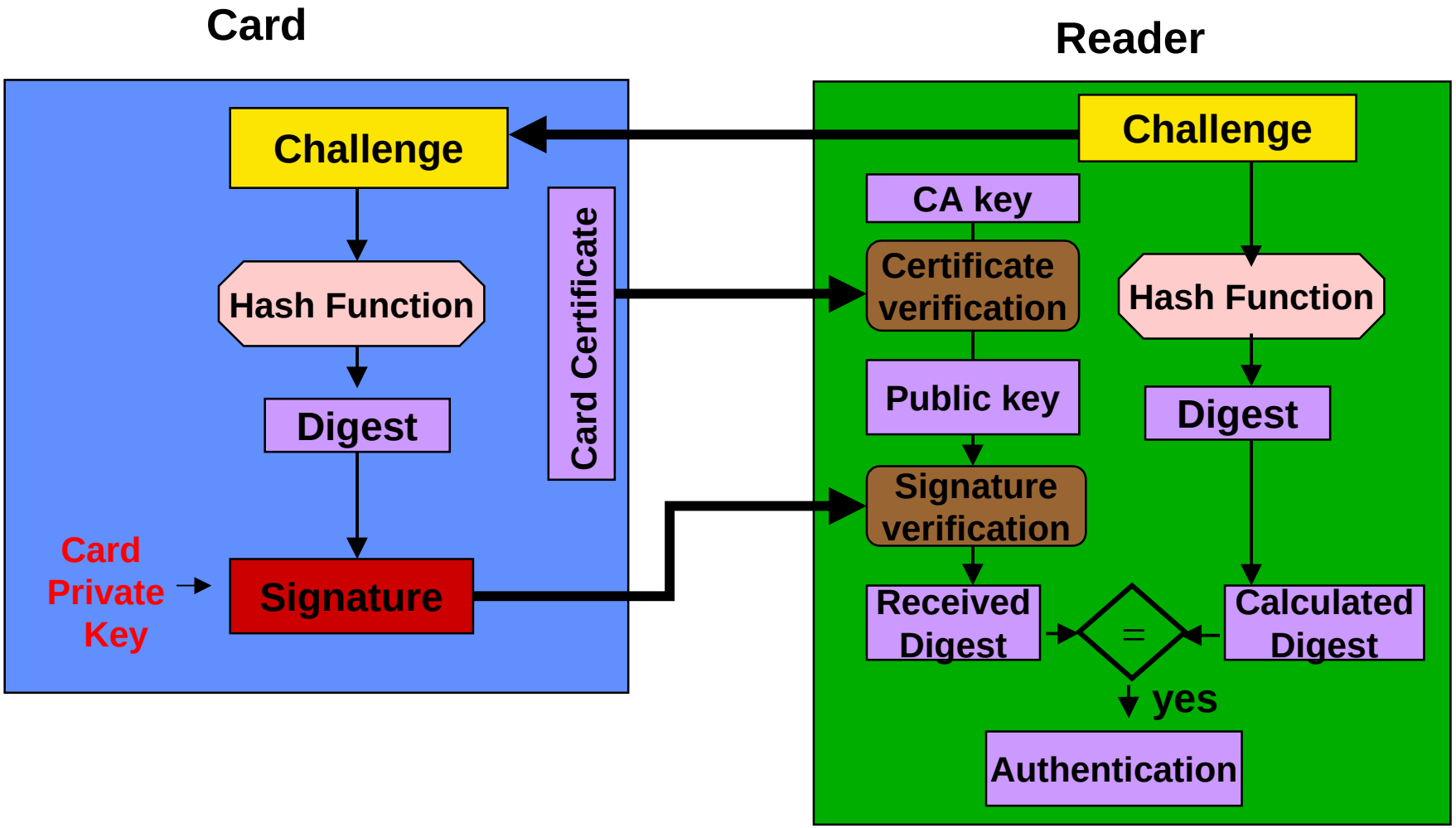
Authentication 3/5



BASIC AUTHENTICATION PROCESS USING A SYMMETRICAL ALGORITHM (CARD AUTHENTICATED BY READER)

EUROSMART
European Smart Card Industry Association

Authentication 4/5



BASIC AUTHENTICATION (AND INTEGRITY) PROCESS USING ASYMMETRICAL ALGORITHM (CARD AUTHENTICATED BY READER)

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Authentication 5/5

- Computation performance (typical)
  - TDES encryption (8 bit CPU) TDES/128 bit key
    - Software : 80/100 ms
    - Cryptoprocessing : 35 µs
  - Digital signature RSA / 1024 bit key
    - Software : not available at company
    - Cryptoprocessing : 85 ms for signature generation

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Confidentiality 1/2

- **Confidentiality**
  - **Objective : to insure privacy of transmitted data between card and reader**
  - **Techniques : Encryption**
    - **Symmetrical key**
      - **Difficult to manage and to share**
      - **Requires a low "computation" power**
    - **Asymmetrical key**
      - **Easy to manage**
      - **Requires a high "computation" power and may require a cryptographic coprocessor**

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Security evaluation

- "Contact Only" cards
  - Some IC are compliant with CC EAL4 augmented
  - Recently, an IC has been announced as being evaluated EAL5 augmented
- Contactless cards
  - Very few products have already been certified CC (ex : ASK IC with a Slb SAM software: EAL1+)
  - Some Protection Profiles have been certified (Assurance level targeted is level 4)

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Contents

- Major contactless features : summary
- Contactless major constraints
- Major security issues
  - Tamper resistant device
  - Authentication
  - Integrity
  - Confidentiality
  - Security evaluation (CC, PP, …)
- ☞ What future for the contactless card security

SchlumbergerSema

Contactless new products 1/2

- New High end products
  - Mifare : Mifare proX : P8RF5016 (dual interface)
  - ST Microelectronics : ST19XR34 (dual interface)
  - Infineon : SLE 88CL320 (Preliminary sheet not yet available)

Contactless new products 2/2

- **Typical product features**
  - Dual interface/ 13,56 MHz, 106 to 424 kb/s/ 10% or 100 % with ASK modulation
  - 8 bit CPU with 32 Kb EEPROM or more
  - On chip crypto processing (TDES, RSA, El Gamal, Elliptic curves, DSS, …)
  - Multiple sensors (voltage, clock, temperature, …)
  - Memory management unit (or firewall)
  - True random number generation
  - Multi-application capabilities

EUROSMART
European Smart Card Industry Association

Company On going activities

- Schlumberger is involved in many comities/Initiatives
  - ISO 14443 (WG8), ISO 7816
  - E-europe (TB3, TB6), ETSI, EESSI, CEN, …
- Full range of OS including a Java platform
- Pilot projects
  - Transport/purse cards (UK, Colombia, Spain, …)
  - City Cards (Brazil, Norway, UK)
  - Corporate/company cards (Club Net/ Japan, KPN (Netherlands, Tokyo University, …)

SchlumbergerSema

EUROSMART
European Smart Card Industry Association

Conclusion

- The future of contactless cards seems to be :
  - Dual interface to ease multi-application/multi-services
  - High security features thanks to on-card cryptoproccessing
  - Opened platform OS (JavaCard, Multos…)

☞ To allow high security level evaluations, attacks related to electromagnetic radiation must be investigated in more details (power attacks, EMA, …)

SchlumbergerSema