gemalto

Contactless smartcard activation without the cardholder agreement

Carine Boursier, Pierre Girard, Christophe Mourtel

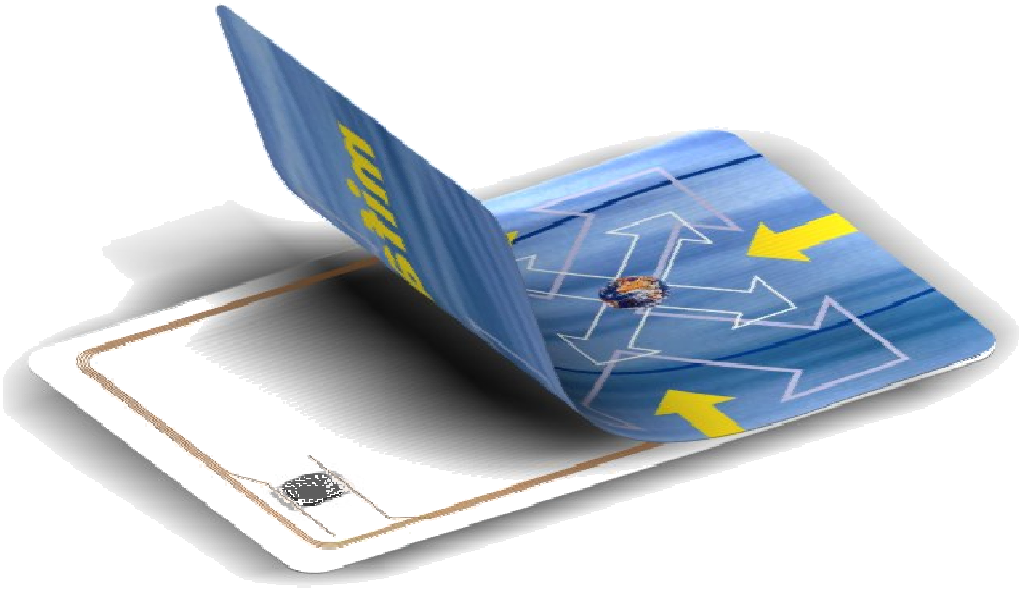
SSTIC – Rennes – 4th june 2008

Summary

- What is Contactless ?
- ISO 14443
- Application
- Security
- Risks
- Solutions

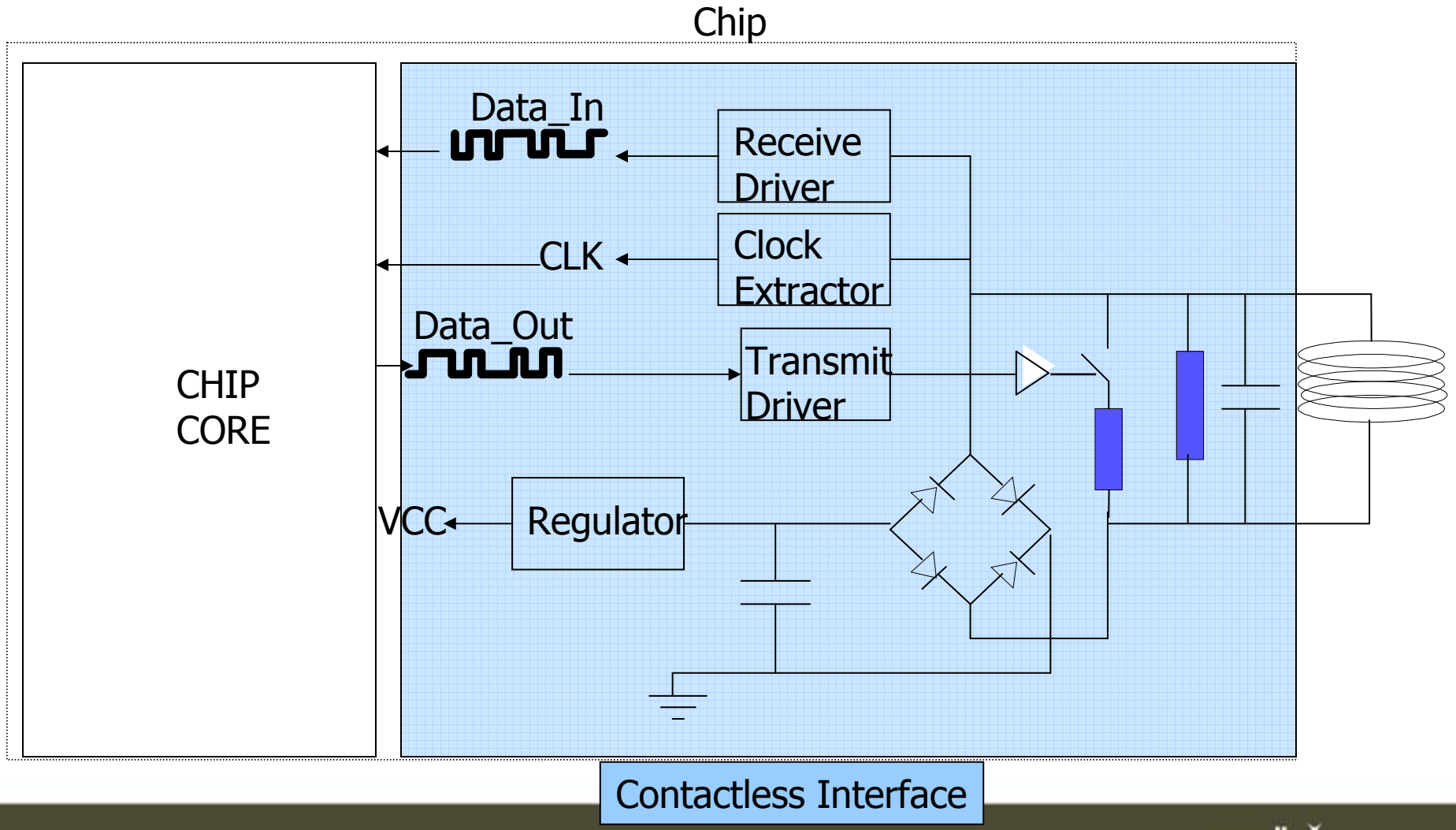
CONTACTLESS Products: BASIS

What is a contactless smartcard?

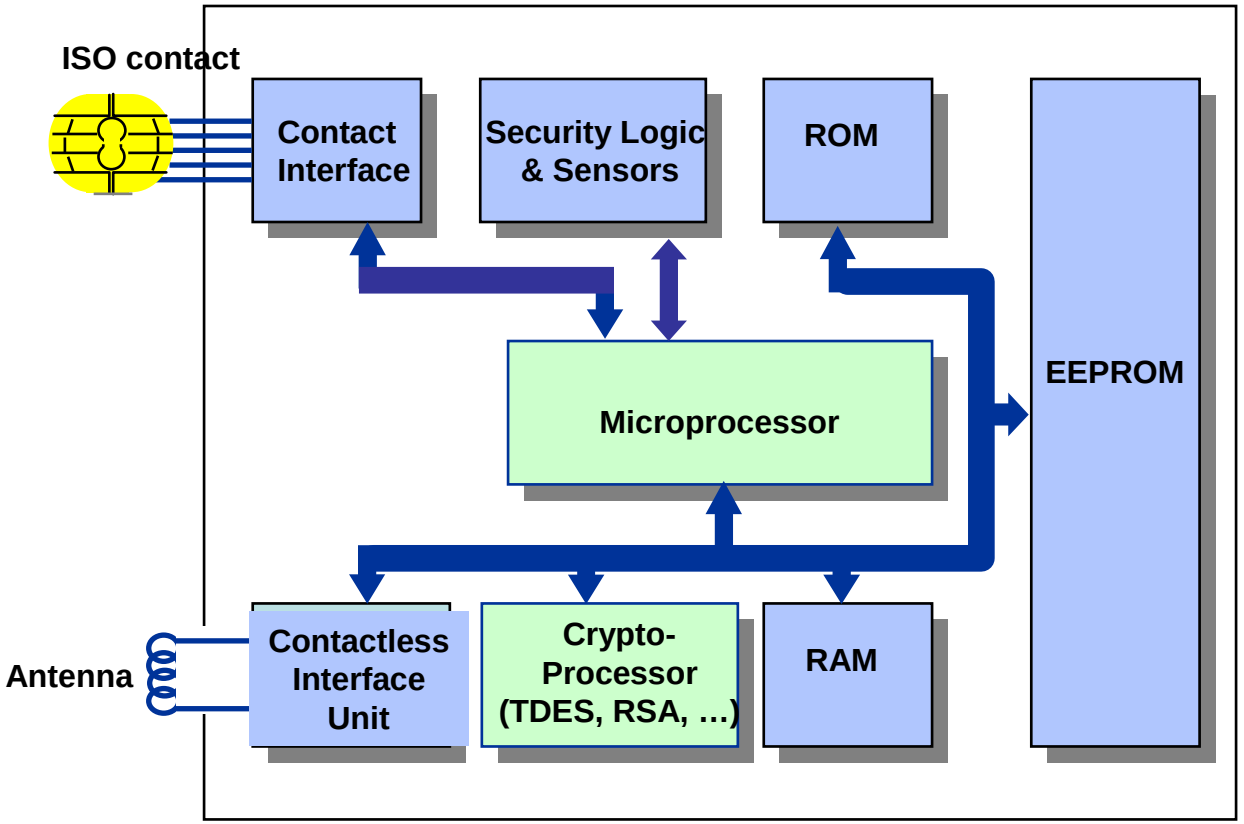


- Products without battery.
- Powered by a magnetic field (13.56 MHz).
- Use microprocessor products only.
- Working distance between 0 to 10 cm.
- Smartcard resonance frequency : 14 to 19 MHz.
- Data transmitted by field modulation (Half duplex).
- Compliant with the ISO/IEC 14443 norm.

Contactless Interface structure



Product Architecture

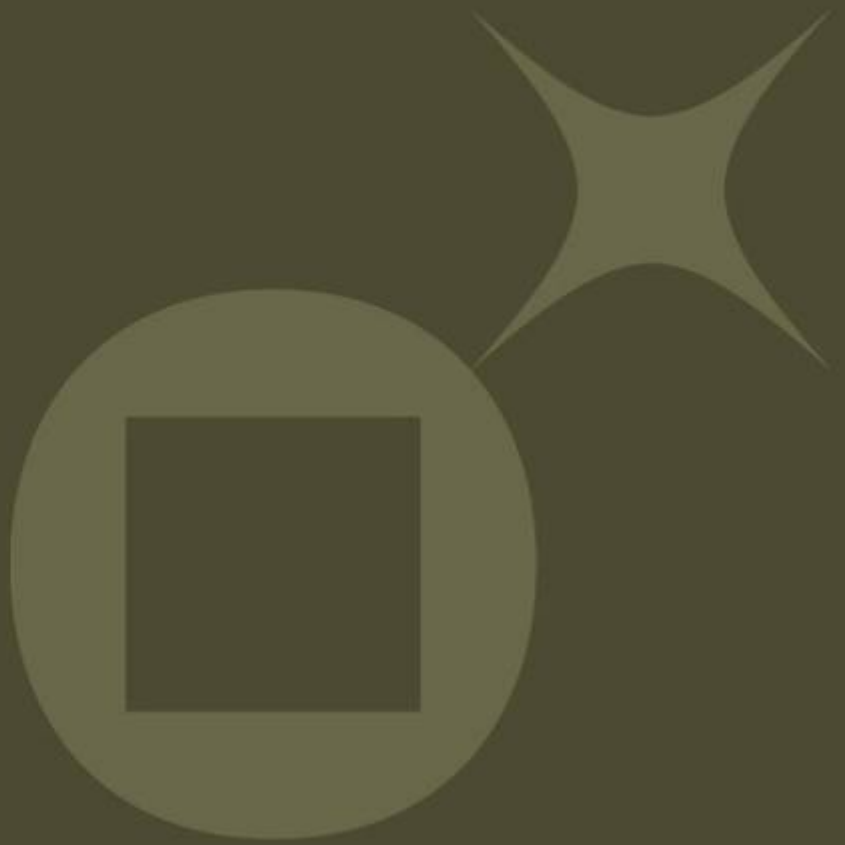


gemalto

ISO/IEC 14443

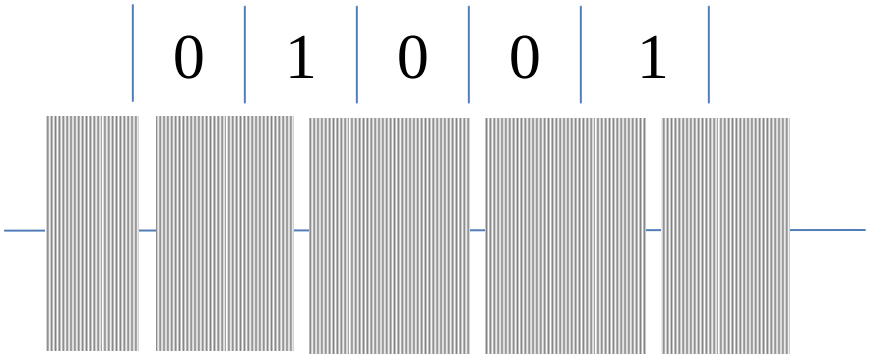
Contactless

Proximity cards



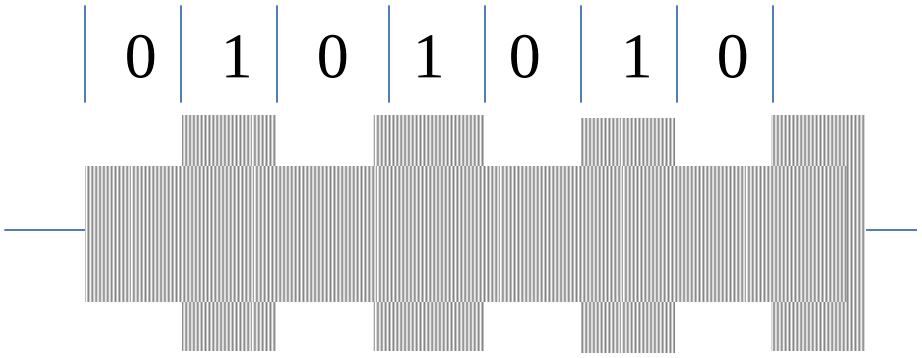
14443
Uplink communication
Reader->Smartcard

Type A



100% ASK
Carrier interruption :3µs
Modified Miller
106 kbit/s

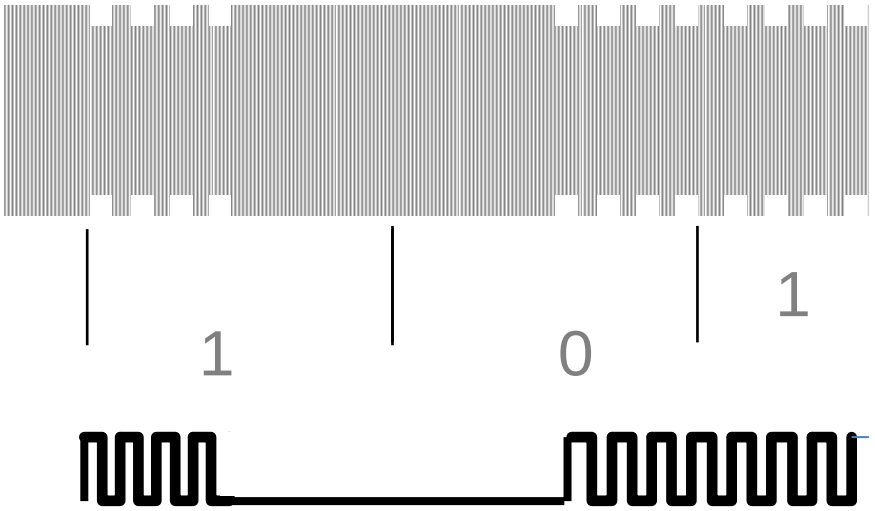
Type B



10% ASK
NRZ-L
106 kbit/s

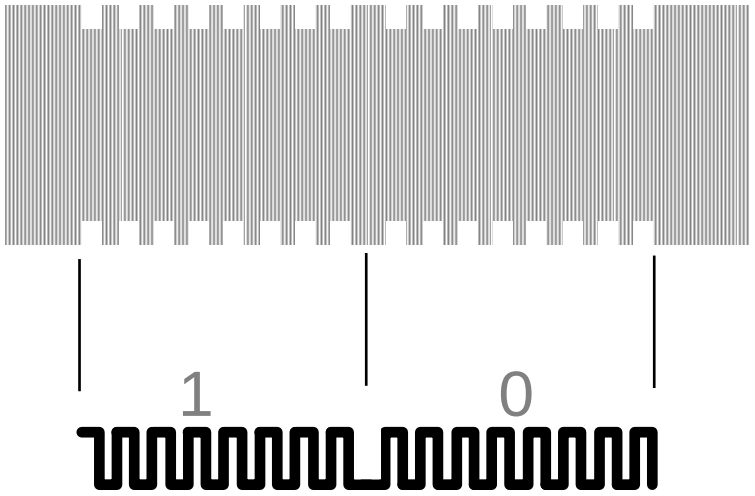
14443-2
Downlink Communication
Smartcard -> Reader

Type A

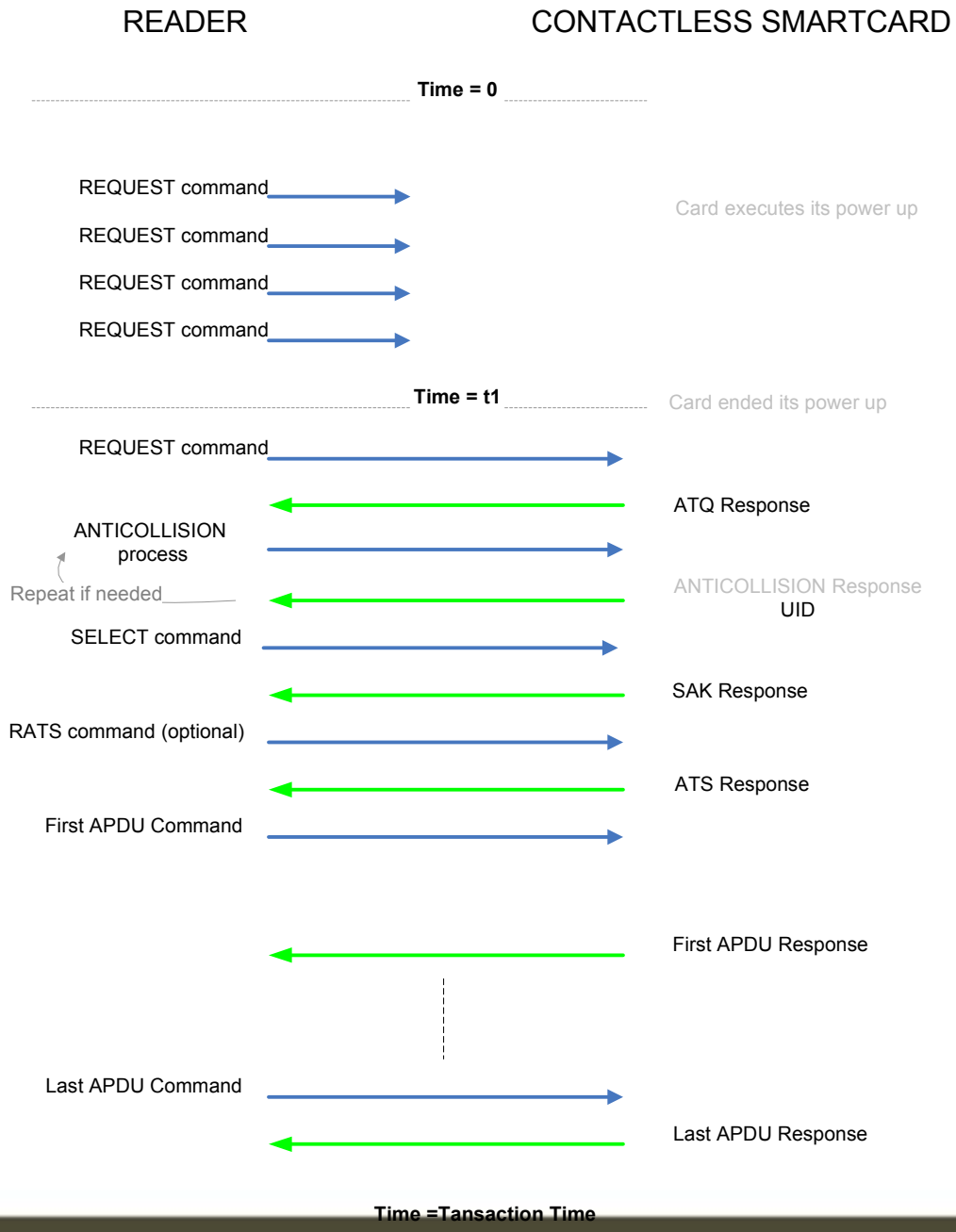


Load modulation
Subcarrier fc/16 (847Khz)
OOK
Manchester, 106kbit/s

Type B



Load modulation
Subcarrier fc/16
BPSK
NRZ-L, 106kbit/s


READER
CONTACTLESS SMARTCARD
Time = 0
REQUEST command
REQUEST command
REQUEST command
REQUEST command
Card executes its power up
Time = t1
Card ended its power up
REQUEST command
ATQ Response
ANTICOLLISION process
Repeat if needed
ANTICOLLISION Response UID
SELECT command
SAK Response
RATS command (optional)
ATS Response
First APDU Command
First APDU Response
Last APDU Command
Last APDU Response
Time =Tansaction Time

Sensitive data exchanged during smartcard activation

- Type A : UID (Unique identifier) 4, 7 or 10 bytes
  - unique chip identifier
  - fix value (default setting)
  - allow tracability
- Type B : PUPI (Pseudo Unique PICC Identifier) 4bytes
  - unique chip identifier
  - fix value (default setting)
  - allow tracability

AFI (Application Family Information) 1 byte
smartcard selection by application family

Application data 4 bytes
information sent by smartcard to inform reader which application are installed

Applications using Contactless

- Acces Control
  - Require cardholder identification (ID,PIN CODE)
  - Memory products
  - Proprietary implementation
  - Mifare (NXP product) is widely used

- Transport
  - Require a short transaction time (150 to 250 ms).
  - Calypso (Paris, EU town)
  - Octopuss (Hong-Kong) based on Felica (sony technology)
  - Mifare utilisation (London, Bombay, Moscow, Beijin, Sao Paulo...)

- Payment
  - Require security
  - Microcontroler products
  - Proprietary scheme (Paypass, Visa contactless Payment)

- Identity
  - Require security, cardhloder identification, big memory size for biometric parameter strorage
  - Microcontroler products
  - ICAO specification – e-Passport, e-Visa

gemalto

SECURITY

Main risks classification

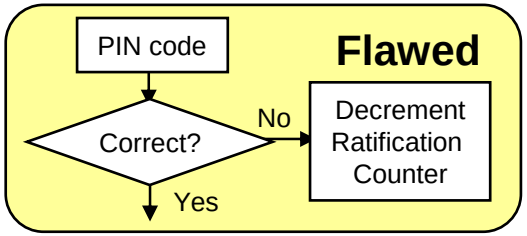
- Two kinds of risks are defined
  - Passive attacks
    - No actions are required on system
    - No modifications on data are possible
  - Active attacks
    - Actions on system are required
    - Modifications on data exchanged/stored are targeted

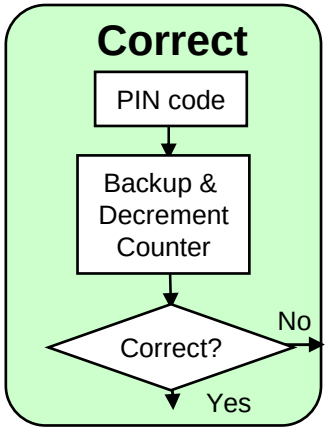
Well kowned and controled vulnerabilities on smartcard

Software attacks

PASSIVE attacks

Implementation flaw exploitation



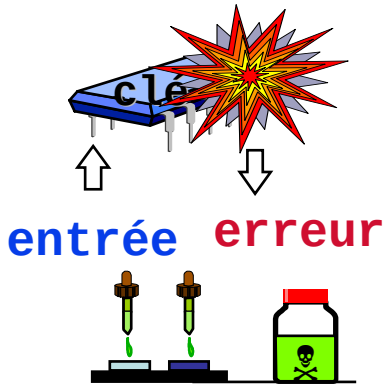


Fault attaks

ACTIVE attacks

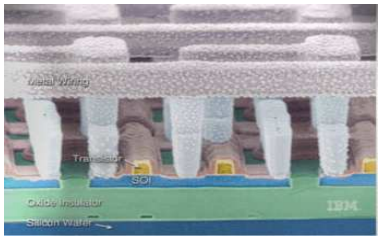
With physical perturbation:

- Vcc, clock,
- temperature, UV
- light, X-Ray, …



Invasive Attacks

ACTIVE attacks



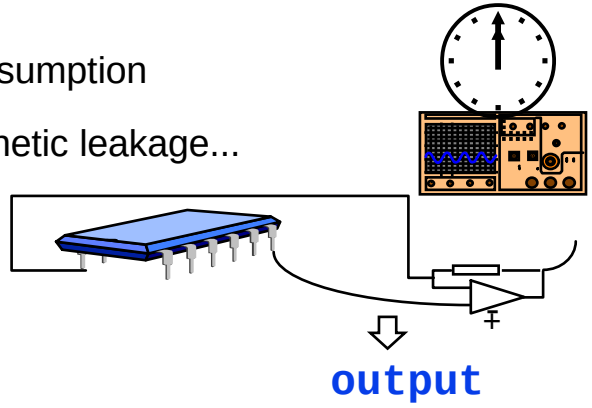
- Probing on buses
- … or through protection layers
- ROM memory reverse
- Track reconstruction or cutting

Side Channel Analysis

PASSIVE Attacks

Signal captation and recording:

- Time
- Current consumption
- Electromagnetic leakage...



Other risks for contactless products

- Data eavesdropping
  - Ability to listen and eavesdrop data exchanged between the reader and the smartcard during the transaction.
  - Passive attack
  - Security issue

    If data exhanged during the transaction can be understood (no security implementation).
  - Potential attacks

    Secret and data captation

    Application cracking

    Cloning

Other risks for contactless products

- Tracking
  - Ability to eavesdrop data exchanged between the reader and the smartcard during the smartcard activation.
  - Passive attack
  - Privacy issue

    If each smartcard has a unique and diversified parameter (UID, PUPI).

    Remarks: ISO1443 allows random value. Only mandatory for e-passport application.
  - Potential attacks

    Cardholder tracking and identification

    Victim targeting

Other risks for contactless products

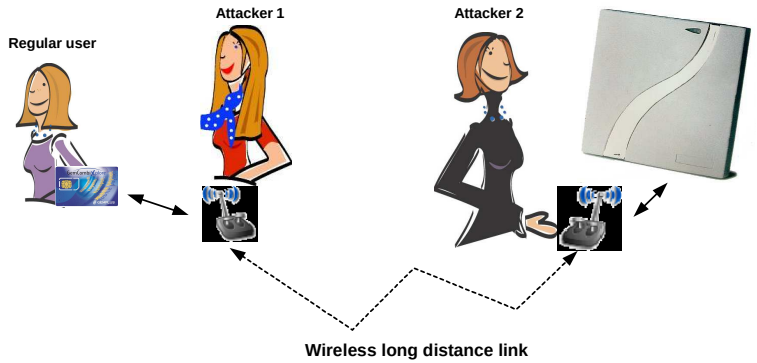
- Active scanning
  - Ability to activate and communicate with a smartcard with an unauthorized reader and without the cardholder agreement.
  - Active attack
  - Privacy and security issue
    - Allow (UID, PUPI) recovery.
    - Application data and cardholder recovery.
  - Potential attacks
    - Cardholder tracking and identification
    - Victim targeting
    - Application cracking

Other risks for contactless products

- Relay attack
  - Ability to propagate an information over the physical limitation distance.
  - Active attack
  - Security issue
  - Potential attacks

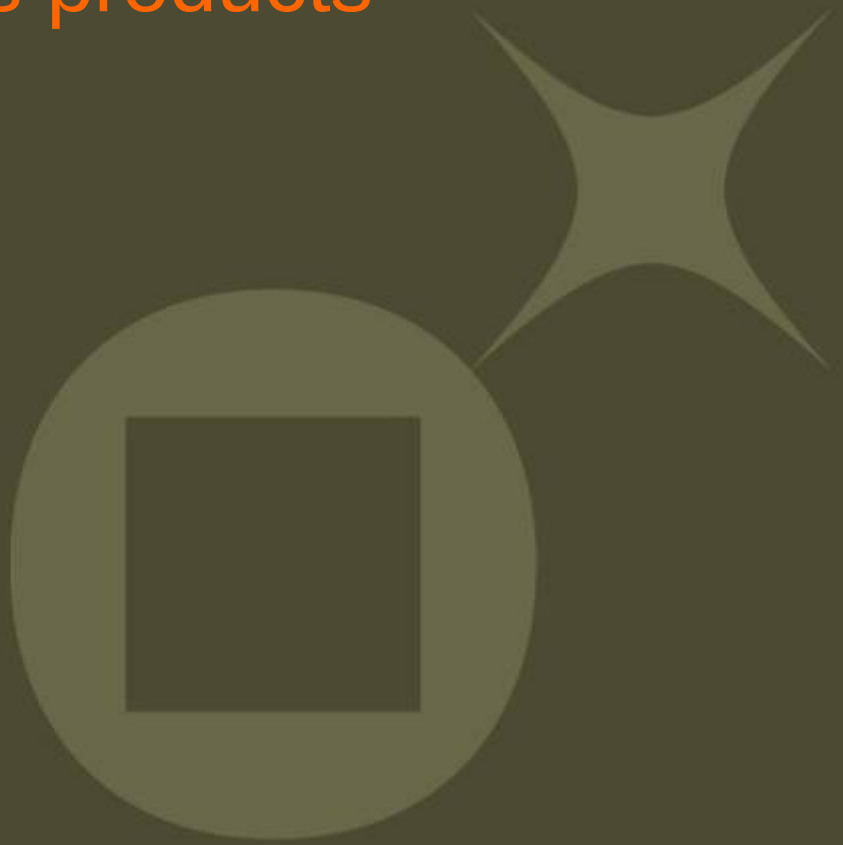
    Smartcard utilisation beyond the physical limitation

    Man in the middle attack.



gemalto

Attacks on contactless products related on WEB



Attack on Texas Instrument product (RFID product)

- •.Sniffing the product 
- •.Cracking the product 
- •.Use a fake product to start a car 
- •.Use a fake product to buy gasoline 

Principle:

Break algorithm encryption

Read chip content and copy content in a blank chip

Emulate a chip behavior

Solution:

Use a secure channel scheme.

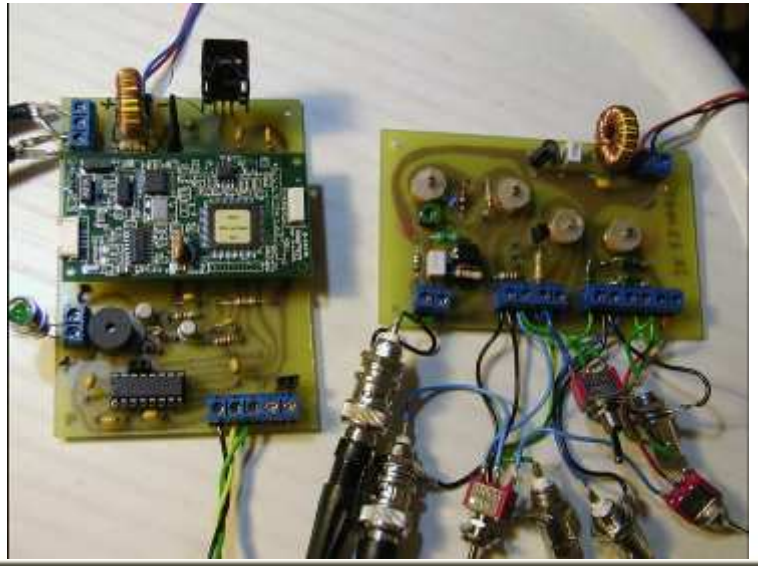
Use stronger encryption and not a proprietary algorithm.

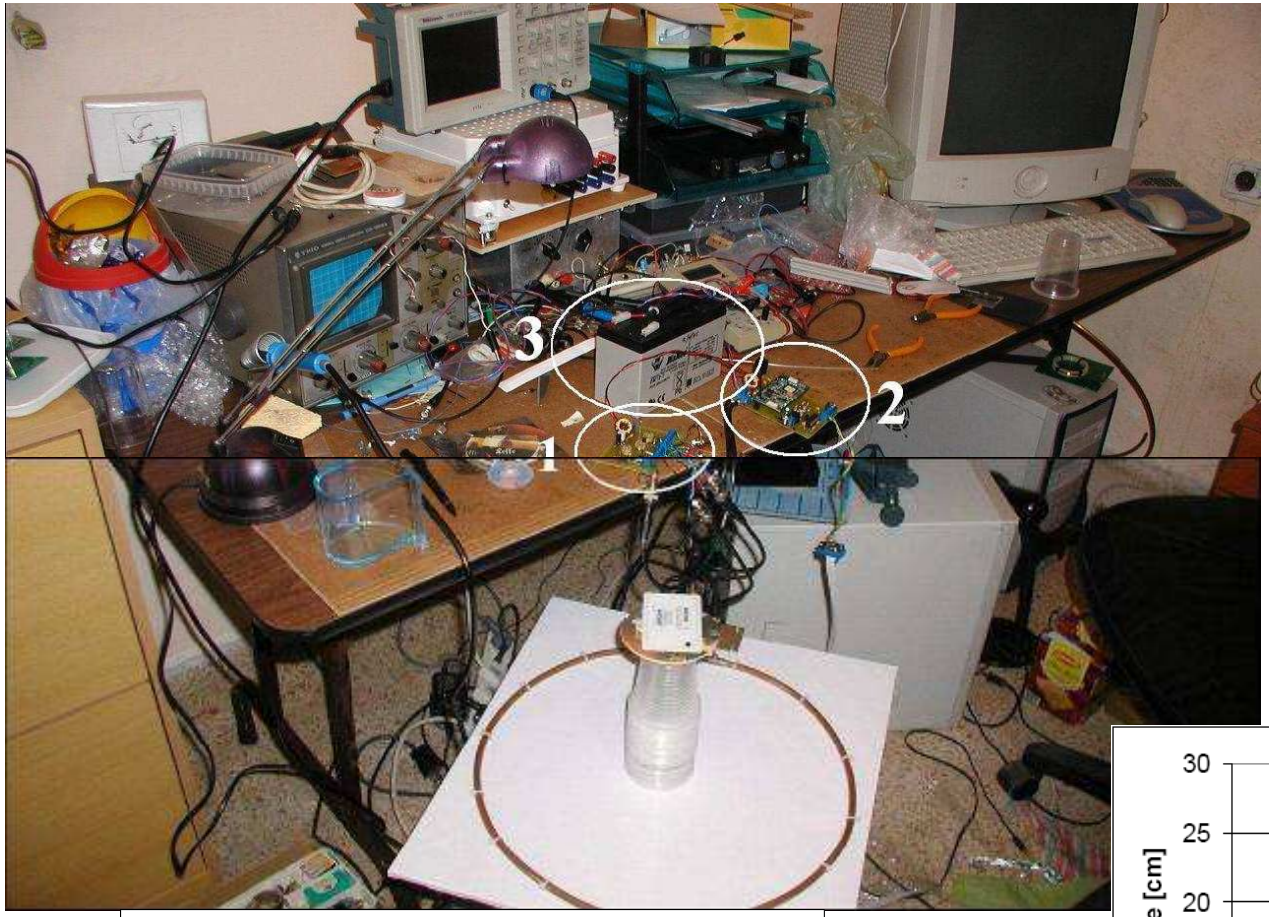
Use contactless smartcard.

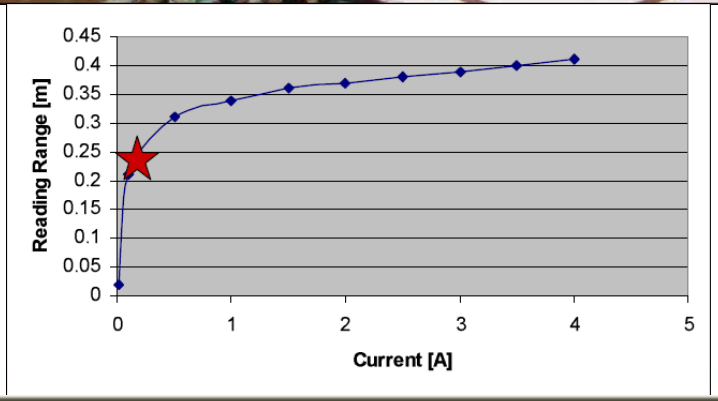
How to Build a Low-Cost, Extended-Range RFID Skimmer

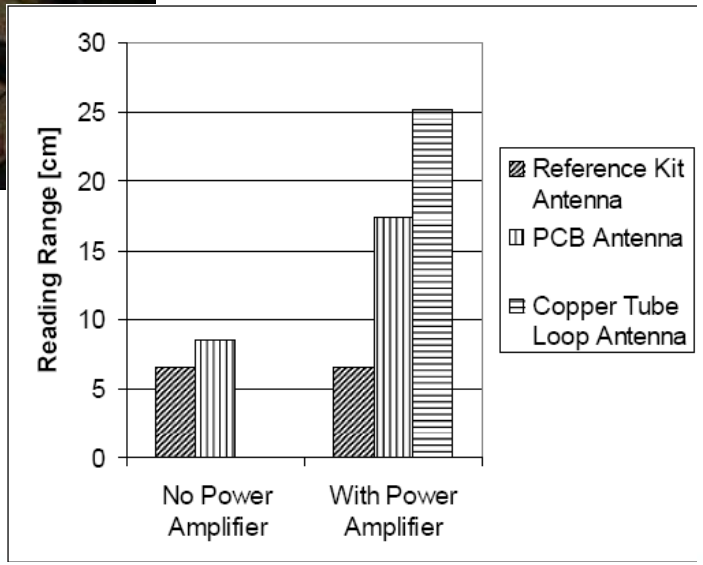
- Authors: Ilan Kirschenbaum, Avishai Wool

- System able to read a ISO 14443 card from a distance of 25cm with an antenna of 40 cm diameter with a reader powered with a 12 V DC battery. Total cost around 100$.




3
2
1


Reading Range [m]
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
0
1
2
3
4
5
Current [A]

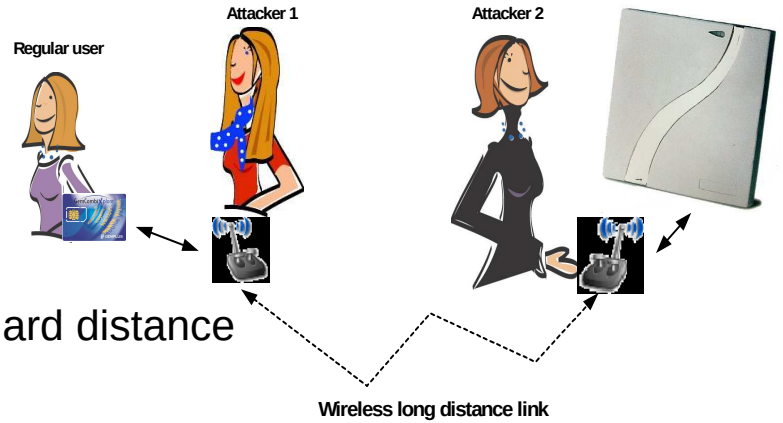

Reading Range [cm]
30
25
20
15
10
5
0
No Power Amplifier
With Power Amplifier
Reference Kit Antenna
PCB Antenna
Copper Tube Loop Antenna

A Practical Relay Attack on ISO 14443 Proximity Cards

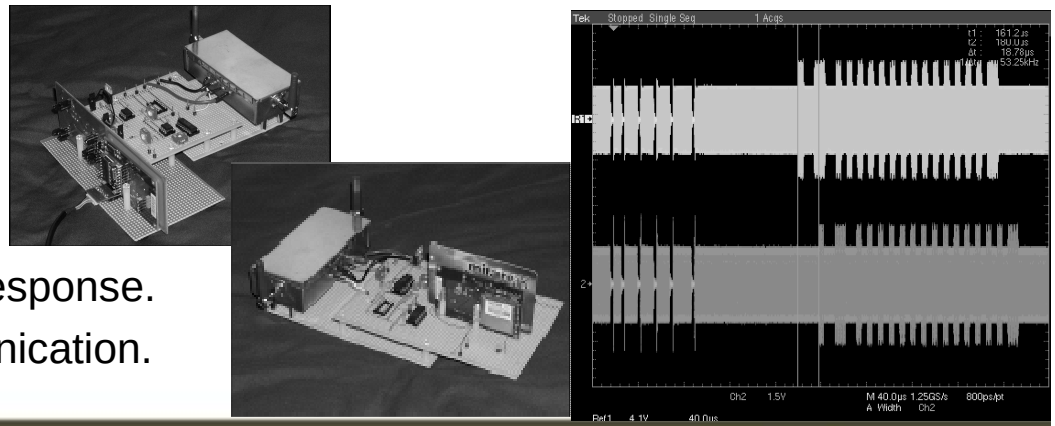
- Authors: Gerhard Hancke

- Relay attack demonstrated on mifare card but works on all contactless product.

- The delay time is around 20 to 25 µs.



- Principle:
  - Establish a transaction farther than standard distance



- Solution:
  - Impose and control the time response.
  - Block an un-authorize communication.

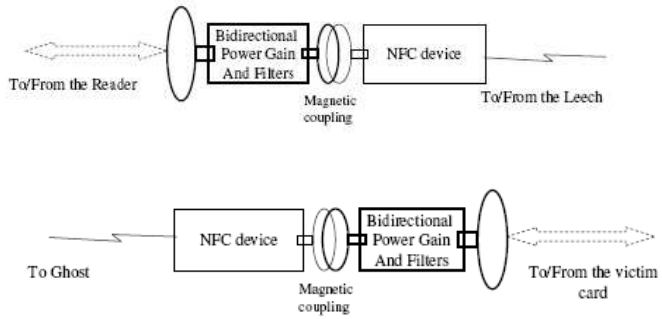
Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems

- Authors: Ziv Kr and Avishai Wool

- Distance between reader and ghost : 50 cm

- Distance between leech and card: 50 cm

- Principle:
  - Relay chip answer farther than standard distance



- Solution:
  - Impose and control the time response.
  - Block an un-authorize communication.

Method	Property			
	Max Distance	Extra Cost (beyond NFC)	Availability	Attacker Knowledge
Standard	10 cm	0$	High	Low
Current + Antenna	40 cm	$< 100$$	High	Medium
Current + Antenna + Software	50 cm	$< 100$$	Medium	High
Current + Antenna + Signal-Processing	55 cm	$> 5000$$	Low	Very High

TABLE I

Forging of ePassports

- Authors: Lukas Grunwald, aug 2006

- Principle:
  - read chip content and copy content in a blank chip

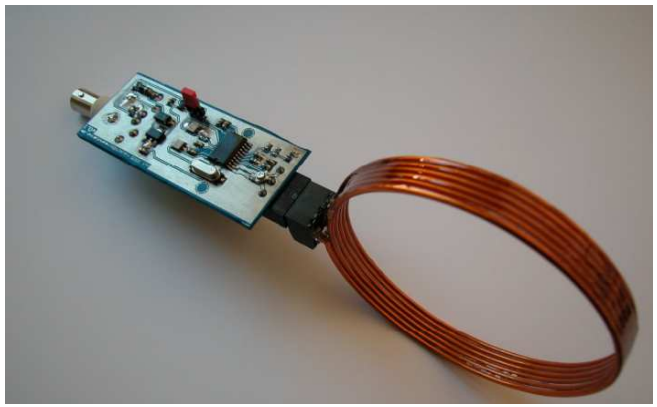
- Solution:
  - Use always the chip and compare content with passport booklet content.
  - Scanners at the border always verify optical features and chip data content.
  - Implementation of Basic Acces Control mechanism (Secure channel and data encryption).

ePassport to fire bombs

- Authors: Mahaffey &Hering, aug 2006
- Principle:
  - Bomb connected to a reader triggered when a passport comes in range
- Solution:
  - Use variable UID no traceability.
  - Use Basic Access Control.
  - Shielding of US passports (needs improvement).

How to sniff RFID

- Authors: Milosch Meriac www.rfiddump.org
- Build a sniffer for all ISO 14443 chip
- Gives detail to build an antenna for 10 €.
- Hope to have an electronic for a full duplex sniffing able to catch data between 3 and 5 meters
- Hope to « replace a tag » with this system.
- Principle:
  - Spy out and manipulate unprotected data using a mobile reader
  - Software can be downloaded from the internet
  - Potential fraud on product pricing via modified article number
- Solution:
  - Protect the data access



Mifare Cracking: little security, despite obscurity

- Authors: Karsten Nohl, Henryk Plotz

- Mifare algorithm partially reversed and cracked
- Mifare secret key recovery (application diversification)

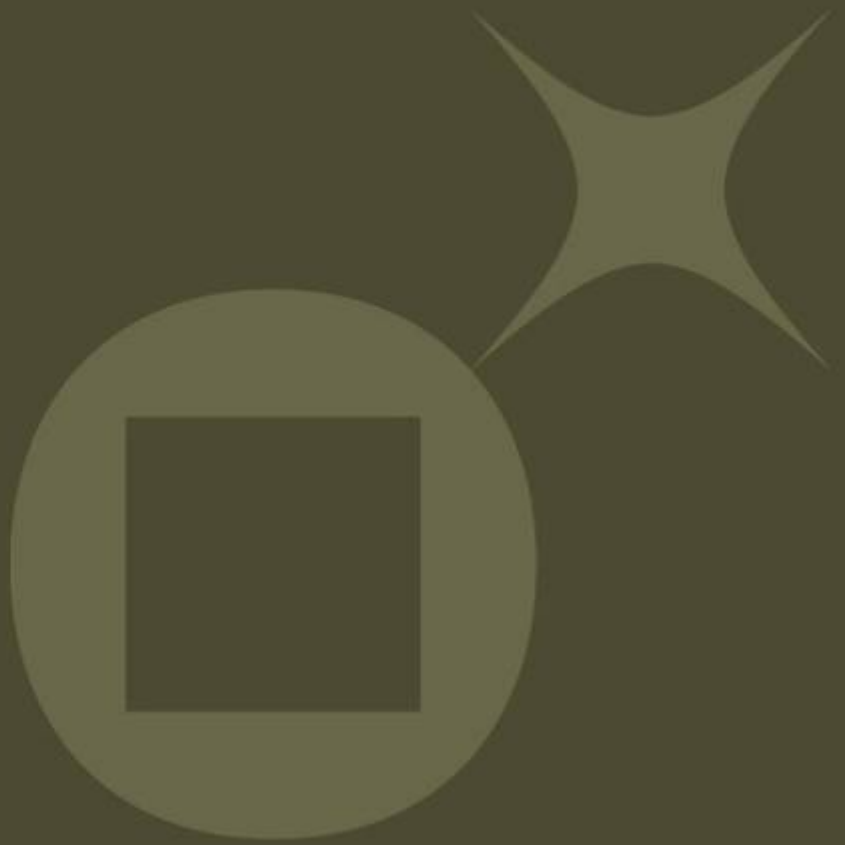
Solution:

Improve the mifare security.

Use a public algorithm. “Obscurity is not a good way to make security”.

gemalto

Solutions



Usual propositions

- Faraday cage:
  - Prevent an illegal communication.
  - Inefficient during legal communication.
- Push Button:
  - Prevent an illegal communication.
  - Inefficient during legal communication.
- Data scanning on cardbody – ICAO solution.
  - Prevent an illegal communication.
  - Data are used for communication encryption.

  All these solutions reintroduce a cardholder agreement

Smart solutions

- Environmental sensors:
  - Sensors are embeeded in reader and in smartcard (light, temperature, movment, accelerator…).
  - Reader and smartcard exchange trough secure communication the sensors value.
  - Communication is establish only if the same environment is shared

  - Prevent a relay attack, eavesdropping attack and active attack
  - Efficient during legal communication. (secure channel)

- Close coupling:
  - A close coupling with an other device operate a communication validation.

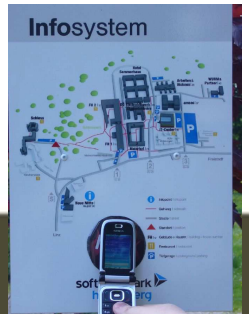
  - Prevent an illegal communication.
  - Efficient during legal communication.

  These solutions reintroduce also a cardholder agreement

Next class of attack

- NFC objects attack
  - NFC (Near Field Communication) enables contactless communication in smart object.
  - A special device embeeded in the phone allows it to emulate a contactless smartcard.
  - A reverse function transforms the phone in a contactless reader.
  - Risks:
    - hostile applet could modified the phone behavior (ie the smartcard content).
    - Everyone will have a contactless reader – easier ability to read and eavesdrop contactless product.
  - Attacks:
    - All attacks already described
    - NFC phone attack related in : ***Collin Mulliner Attacking NFC Mobile Phones -EUSecWest 2008***

      smart object reading and attack allows:
      - Tracking
      - Trojan download
      - Phone misused



Conclusion

- The smartcard activation without the cardholder agreement is the bottleneck of the contactless products security.
- Solutions exist to prevent attacks. Some are common with all smart objects (secure channel, data ciphering, pin code) other are specific.
- Contactless smartcards could at the end be as secure as contact products. Example e-passport.

Questions ?

- Thank you

Christophe.mourtel@gemalto.com