micro and nanoelectronics
microsystem
ambiant intelligence
image chain
biology and health

2008

# RFID and Internet of Things

# Technological Perspectives


François Vacherand

francois.vacherand@cea.fr


leti

MINATEC

cea

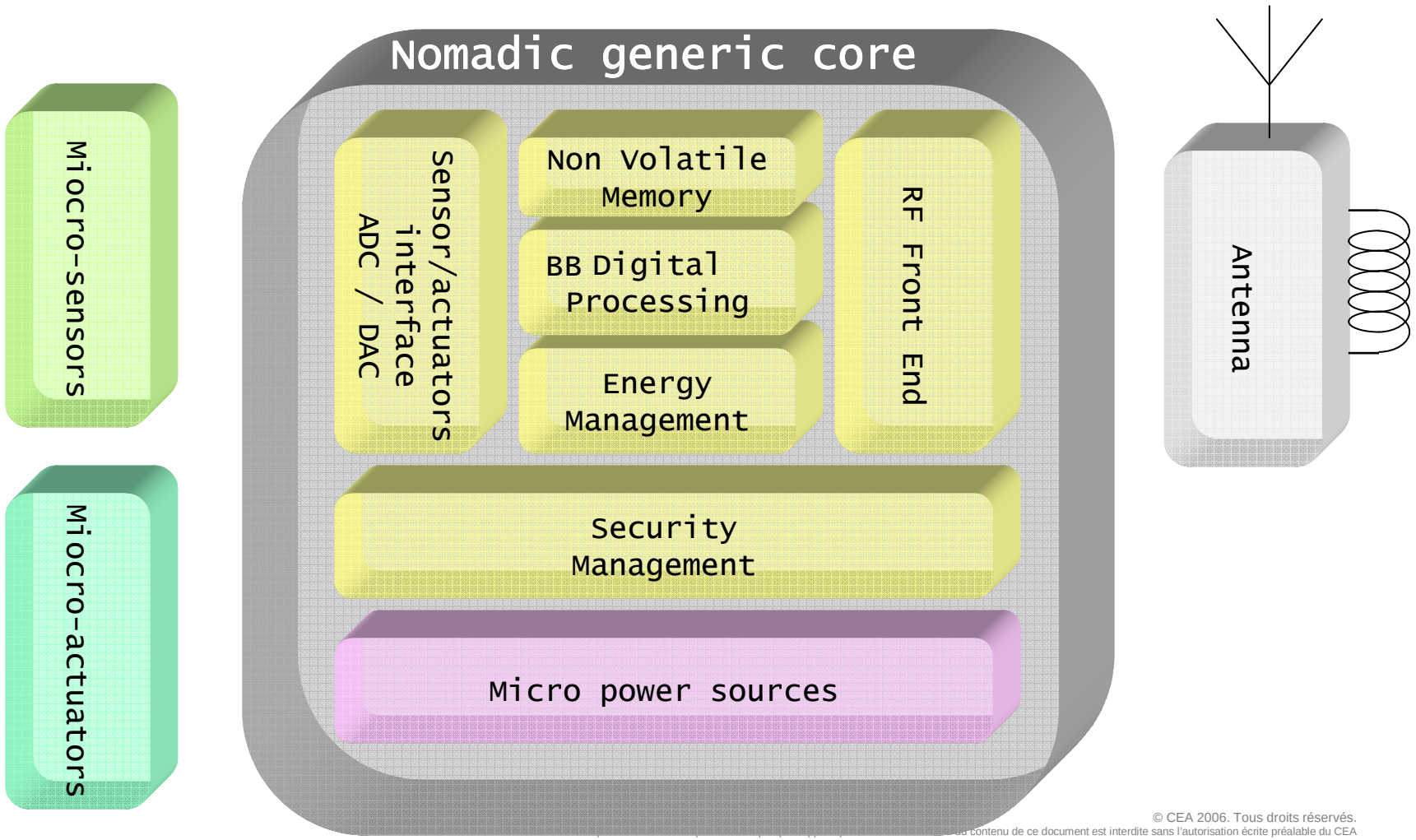
# Presentation plan

- Technological Perspectives of RFID and IoT at LETI
- RFID air interface
  - Large file transfer for large memory
  - Inventory protocols
- RFID Security
  - Security for low resources devices
  - Privacy
- Beyond RFID
  - Micro-sensors
  - Micro-batteries
  - WSN

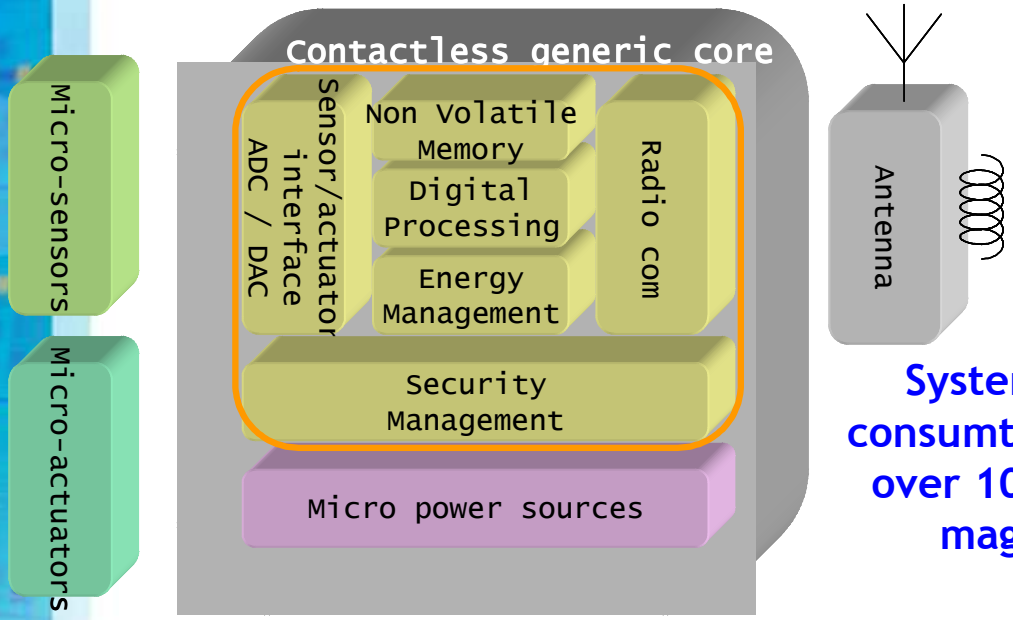
# Presentation plan

- Technological Perspectives of RFID and IoT at LETI
  - RFID air interface
    - Large file transfer for large memory
    - Inventory protocols
  - RFID Security
    - Security for low resources devices
    - Privacy
  - Beyond RFID
    - Micro-sensors
    - Micro-batteries
    - WSN

# Wireless/Contactless Nomadic Devices

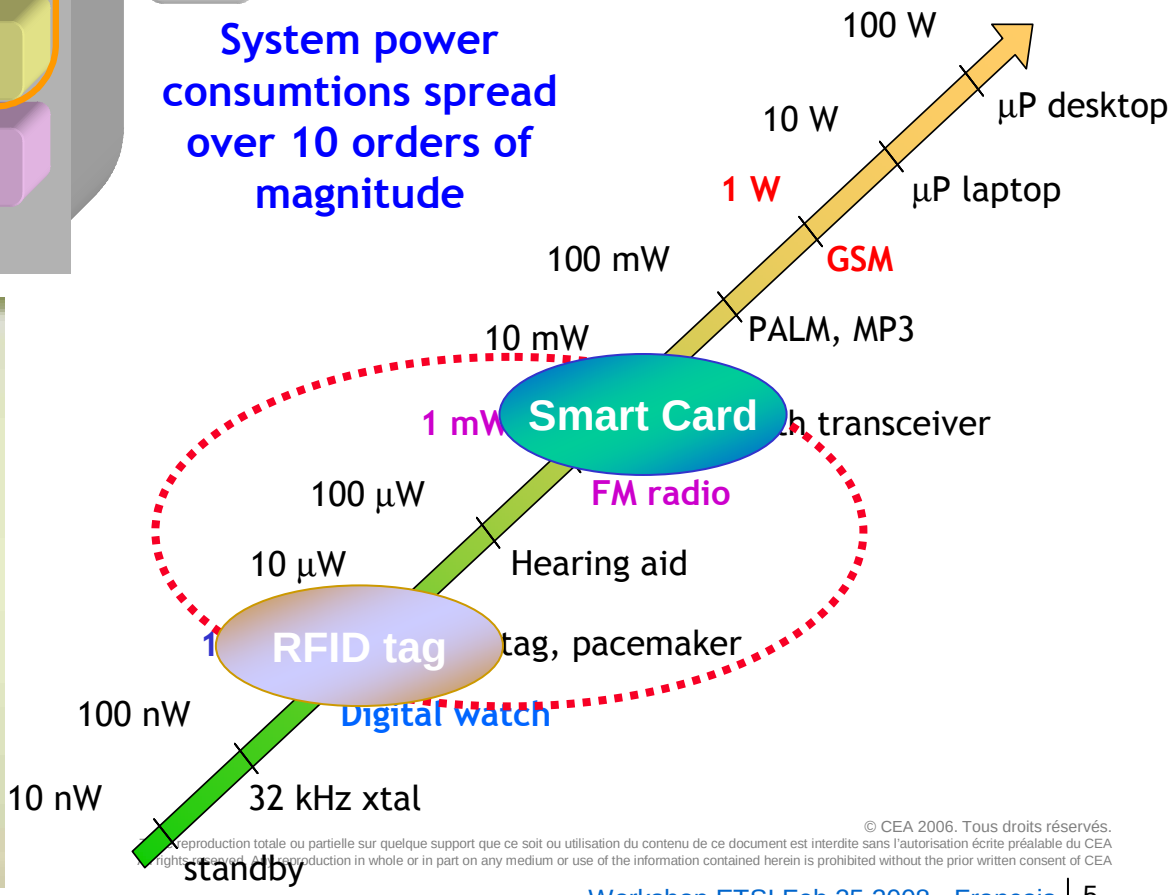


# Autonomous Contactless Devices



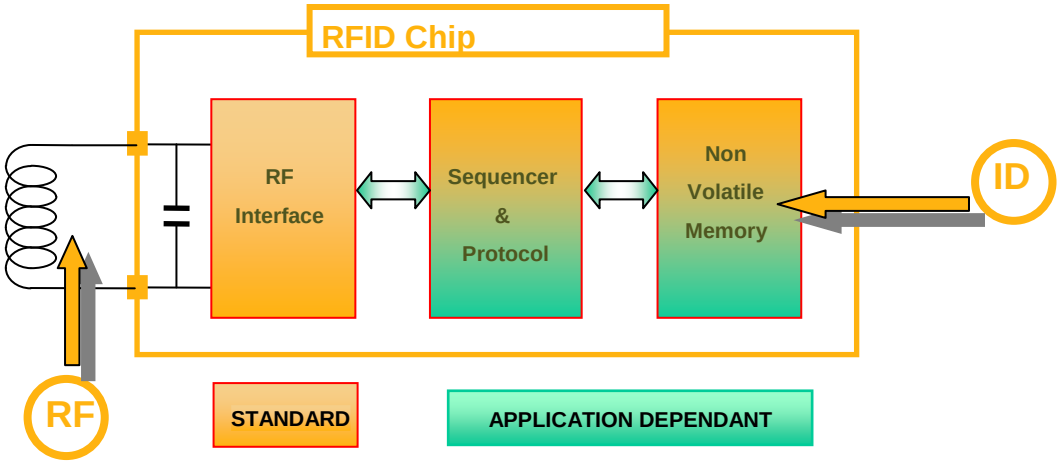

- **Wireless/Contactless**
- **Sensing /actuation**
- **Embedded intelligence**
- **Energy management**

**System power consumtions spread over 10 orders of magnitude**



# *Radio Frequency Identification (RFID)*

- Contactless Identification
  - Person → Smart cards 
  - Items → RFID tags 




- Differences
  - Person: cooperative, unique, biometric
  - Items : passive, multiple, non biometric

# Presentation plan

- Technological Perspectives of RFID and IoT at LETI
- RFID air interface
  - Large file transfer for large memory
  - Inventory protocols
- RFID Security
  - Security for low resources devices
  - Privacy
- Beyond RFID
  - Micro-sensors
  - Micro-batteries
  - WSN

# State of the art air interface (1/3)

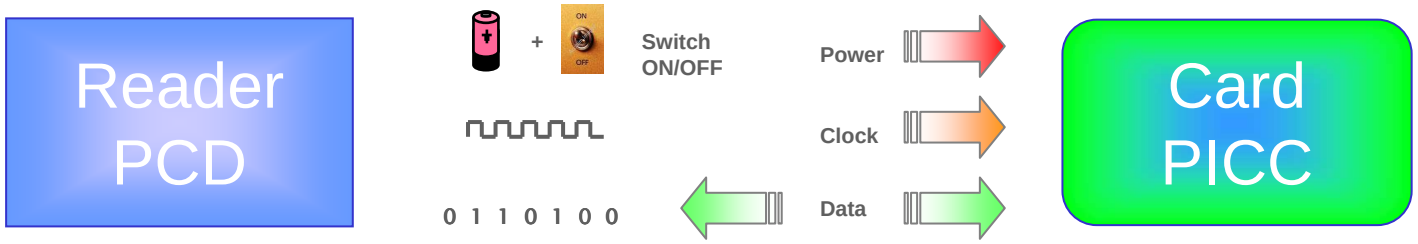
- State of the art (Current standard)

- ISO 14 443 Contactless Proximity Card
  - Contactless air interface between PCD and PICC
- Air interface and data rates
  - Two air interface types: A and B
  - Default data rate at power on: 106 kbps initialisation/anti-collision
  - 2005 amendment: data rates 106,  212, 424 and 848 kbps

- Reader Talks First
- Conformance standard: ISO 10 373-6

# Contactless Paradigm

- Bidirectional Contactless Air Interface




| Reader (PCD) | Parameters | Card (PICC) |
|---|---|---|
| High | Electric Power | Very low |
| High MIPS | Computation Power | Low MIPS |
| Field emission | Electromagnetic | No emission |
| Modulation | TX | Retro modulation |
| High DSP | RX | Low DSP |
| | | |
| Medium | Δ Cost constraint | Very high |

# Towards VHDR air interface: Objecives

- VHDR specifications (applications requirements)
  - Large memory cards
  - Transfer large files
  - Very fast transaction
  - Robustness and security


- System/product constraints
  - Upward compatibility → Use HF band
  - HF bandwidth and spectrum regulation
  - Same coil antenna technology
  - Minimize power
  - Minimize cost

# Towards VHDR air interface: Solution

- VHDR specifications (technical performances)
- Air Interface technical proposal
  - Break the 1Mbps barrier
  - Scalable
  - VHDR proposal: **1.7Mb/s, 3.4 Mb/s, 5.1 Mb/s, . . .**

- **Data rates improvement**
  - From one bit per symbol to multi bits per symbol
- **Scalability**
  - Data rate = f (nb symbols, T symbol) = $\log_2(nb\_sym)/Ts$

# VHDR air interface: Performances

- Technical solution
  - Multi-levels modulation (multi-bits per symbol) for 2 channels
  - Constant envelop modulation (stable power transfer)
    - **Multi Phase modulation**
    - **Higher symbol rate**
  - Data rate = f (nb levels, T symbol) = log2(nb_levels)/Ts

- **PCD → PICC**

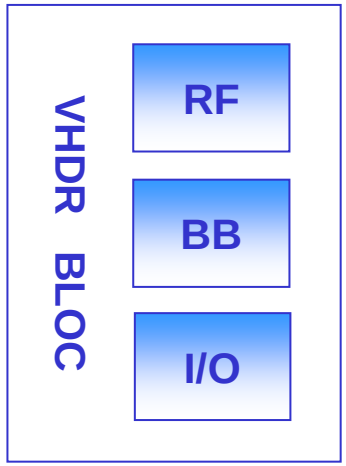
| Phase nb<br>Unitary Δφ | $2 = 2^1$<br>Δφ = 180° | $4 = 2^2$<br>Δφ = 90° | $8 = 2^3$<br>Δφ = 45° | $16 = 2^4$<br>Δφ = 23° | $32 = 2^5$<br>Δφ = 11° | $64 = 2^6$<br>Δφ = 6° |
|---|---|---|---|---|---|---|
| 1 etu = 8/fc = 590 ns | 1695 kbps | 3390 kbps | 5085 kbps | 6780 kbps | 8475 kbps | 10170 kbps |

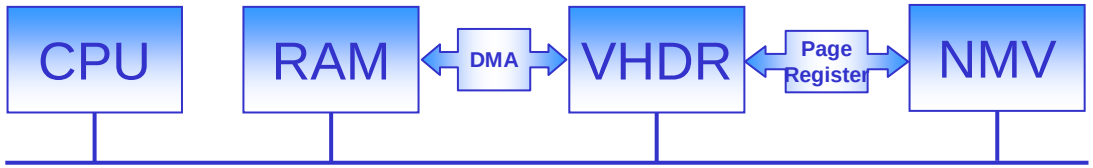
- **PICC → PCD**

| Fsc | Nb phase<br>Ts = 1 etu | $2 = 2^1$<br>Δφ = 180° | $4 = 2^2$<br>Δφ = 90° | $8 = 2^3$<br>Δφ = 45° | $16 = 2^4$<br>Δφ = 23° | $32 = 2^5$<br>Δφ = 11° |
|---|---|---|---|---|---|---|
| *1695 kHz* | 1/fsp = 8/fc= 590ns | 1695 kbps | 3390 kbps | 5085 kbps | 6780 kbps | 8475kbps |

# VHDR Chip Design: Evolution

- VHDR Chip design overview
  - **RF part**
    - Minimize RF and analog
  - **Digital part**
    - Maximize BB digital processing
    - High speed memory transfer

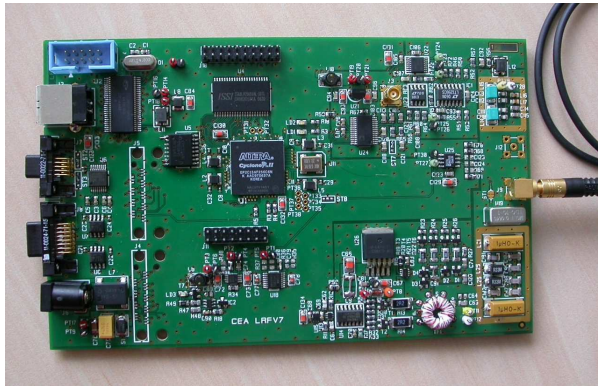


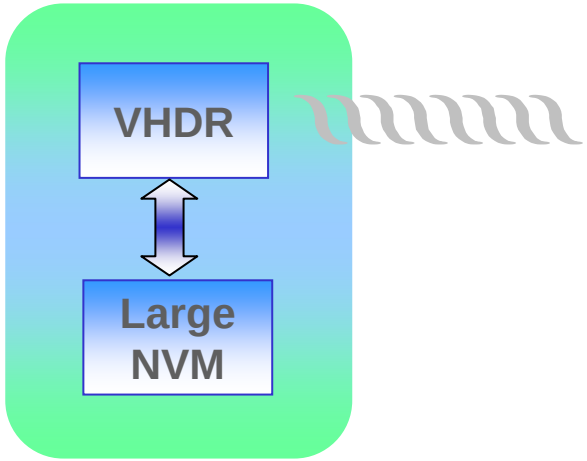

- BB Bloc + bus I/O → No CPU overload for transfer

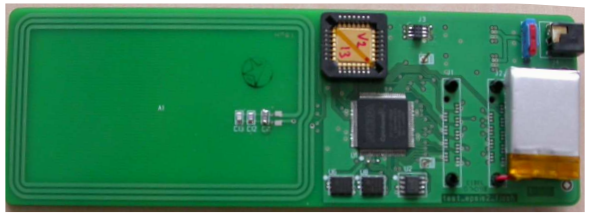
# VHDR Demonstrator

- VHDR Demonstrator
  - Large NVM
  - Medical Images
  - Large file transfer (2MB / 3 sec)



VHDR Reader proto



VHDR Card proto

**Use case: memory token**

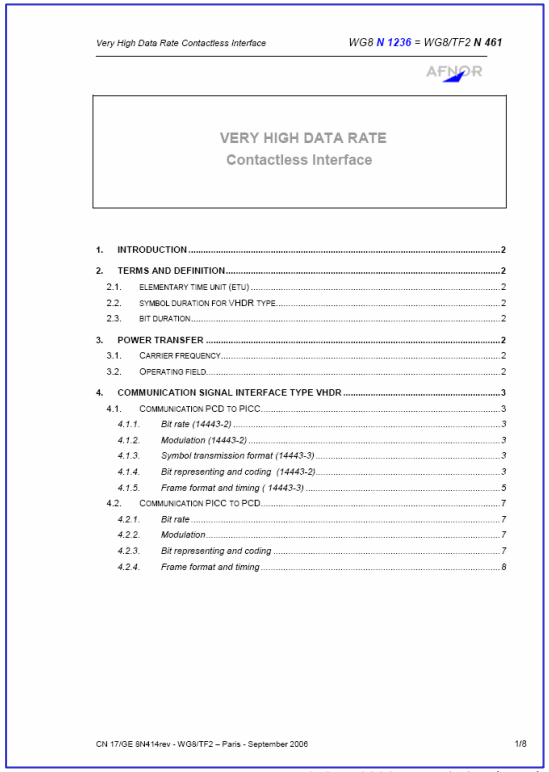
**With large amount of personal data**

# VHDR Standardization

- VHDR ISO technical proposal
  - SC17/WG8/TF2 on VHDR
  - September 2006 French proposal to ISO
  - June 2007, Austrian proposal
  - The 2 proposals are very close
    - Phase modulation

► Toward potential simplification

Only **ONE** scheme beyond 1 Mbps



Very High Data Rate Contactless Interface — WG8 N 1236 = WG8/TF2 N 461

AFNOR

VERY HIGH DATA RATE
Contactless Interface

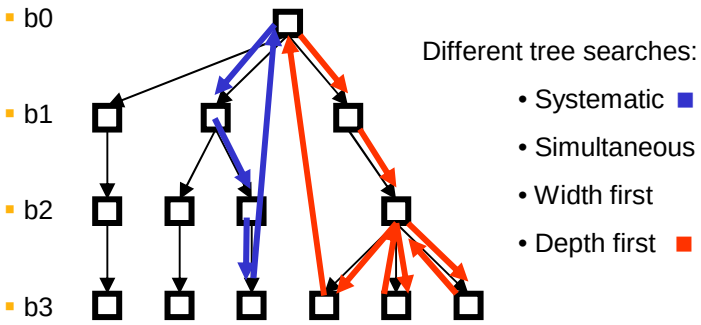


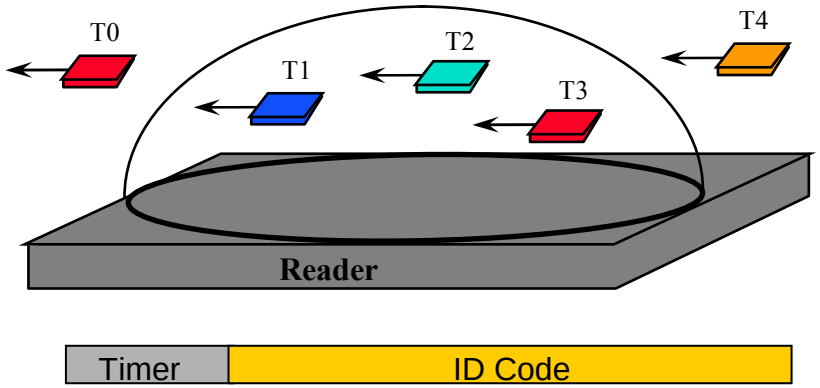
CN 17/GE 8N414rev - WG8/TF2 – Paris - September 2006 1/8

# Electronic Tags: Inventory & Flow

## Inventory Protocol Characteristics

- Determinist Algorithm Characteristics
  - Known Duration: $T_{read}$ = f (Nb Tags, Code Length, Data rate)
  - N-ary Tree Search Algorithms
  - No Random Generator




- Flow management
  - First In - First Read Tag (Timer Header + ID Code)
  - Short Address for Fast Access (8bits for 256 tags)
- Eavesdropping → Anonymity

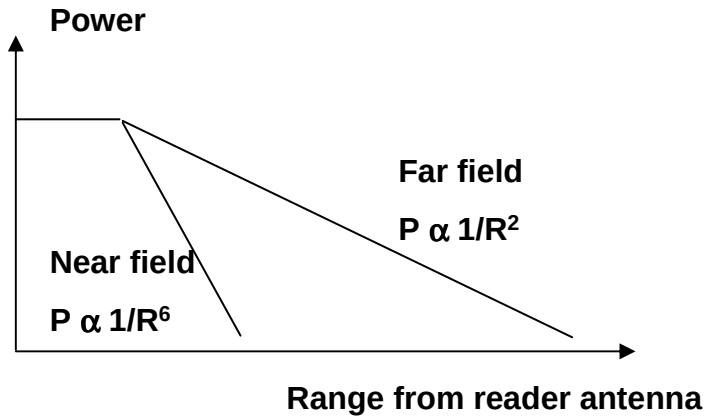
# Presentation plan

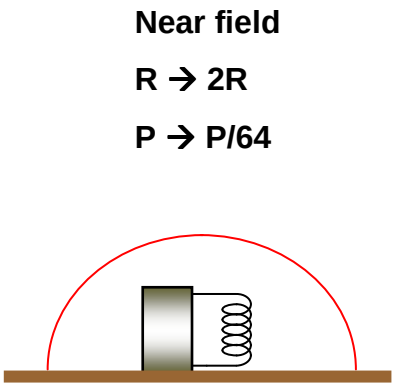
- Technological Perspectives of RFID and IoT at LETI
- RFID air interface
  - Large file transfer for large memory
  - Inventory protocols
- RFID Security
  - Security for low resources devices
  - Privacy
- Beyond RFID
  - Micro-sensors
  - Micro-batteries
  - WSN

# Contactless link
# Near Field Secure Transaction

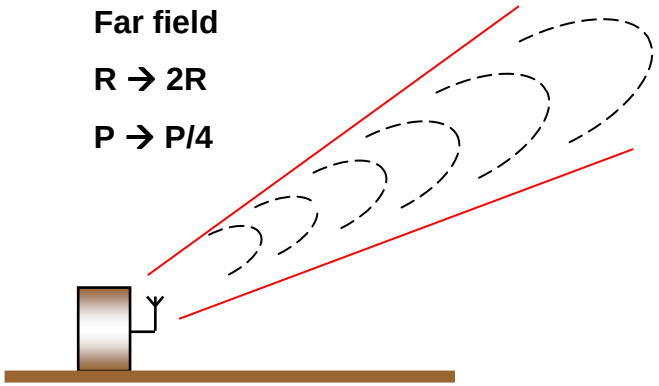
- Near Field (EM) Secure Transaction

  - Near Field → HF band = 13.56 MHz
  - Reduced operating volume
  - Some 10 mW for powering high MIPS
  - Low cost antenna
  - ISO 14 443 and NFC protocols




Smart cards

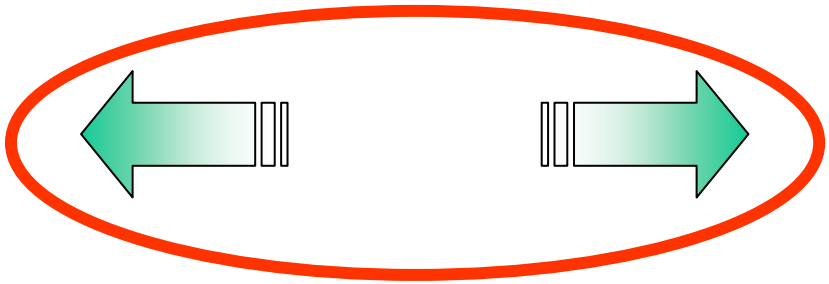


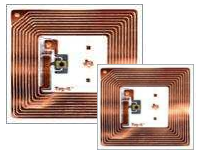

Electronic Tags (UHF)

# Contactless Air Interface

- 3 Main Functions = Power + Clock + Data

- **Reader**
- **Passive: no battery**
- **Unique or multiple**







**Switch ON/OFF**

**Power**

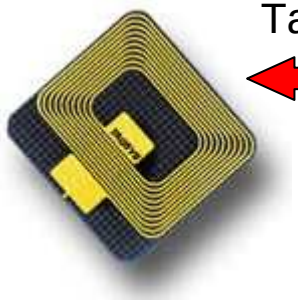
**Clock**

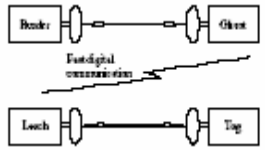
0 1 1 0 1 0 0 0 1

**Data**

# RFID: Security Issues

Tag counterfeiting





Eavesdropping

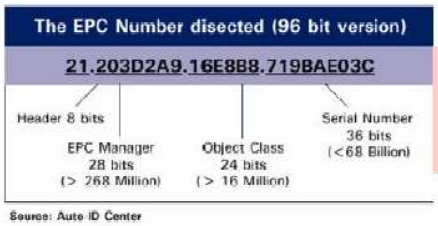
Man in the middle

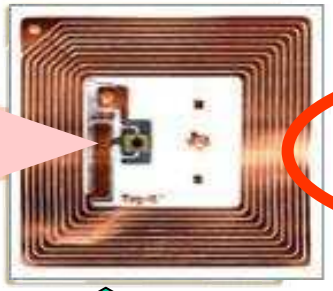
Tag destruction

Relay attack

CPM Guardian

ID Code

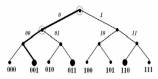


Substitution object/tag

Code modification

Blocking



Jamming

Remote tag control
- Kill command
- Change ID

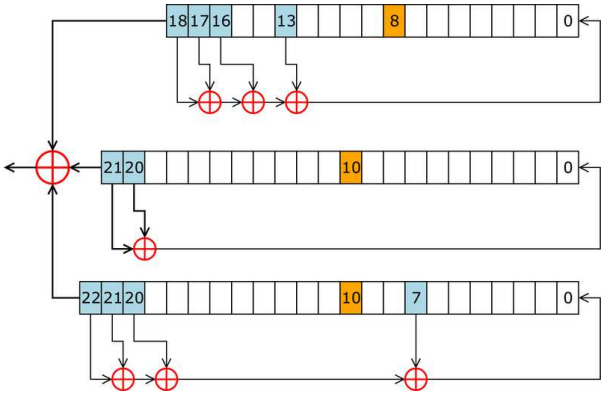
Rogue reader

Telepicpocketing

# Security for low resources devices

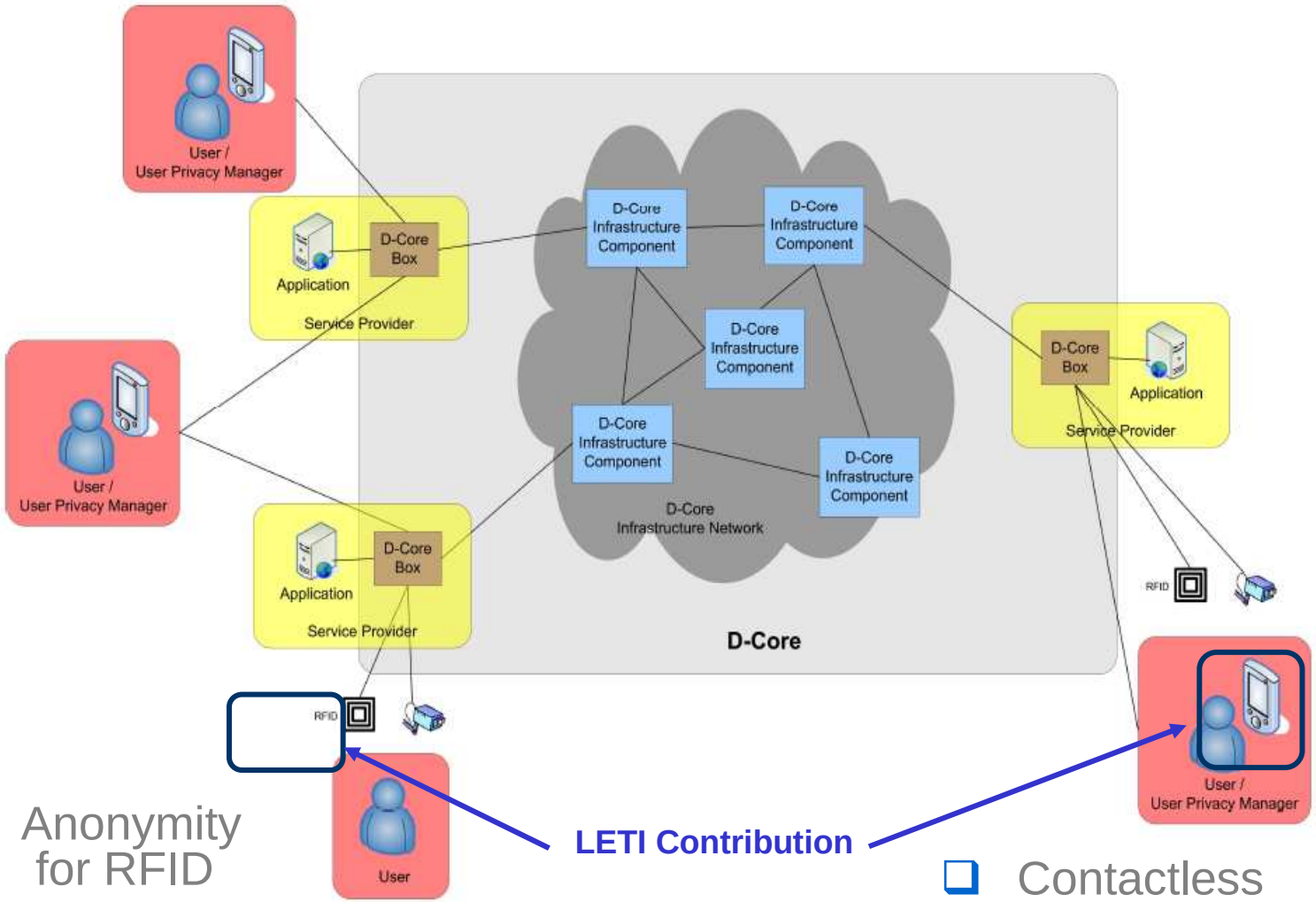
- Ciphering for low resources devices
  - Tag authentication
  - Data information ciphering
  - Privacy Enhancing Technology
  - Low computation capabilities

→ Secure Stream Ciphers




- Relevant algorithm for secure implementation
- Secure LFSR Architecture

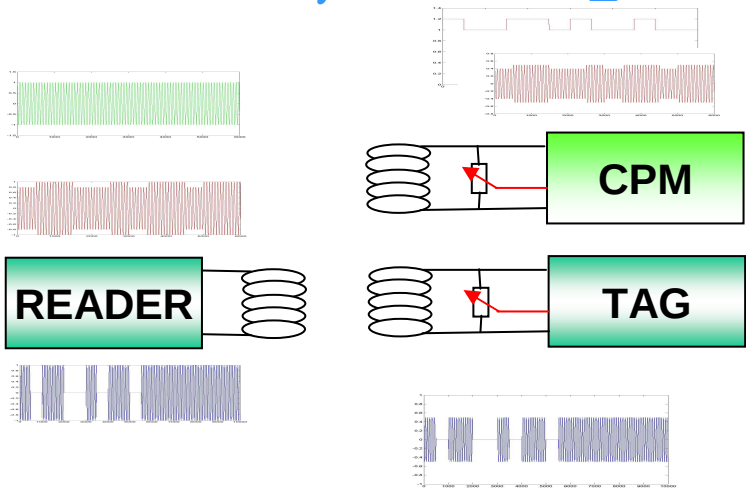
# Privacy Enhancing Technology and RFID




- Anonymity for RFID
- Contactless Privacy Manager

# CPM PET: Contactless Privacy Manager

## CPM functions:



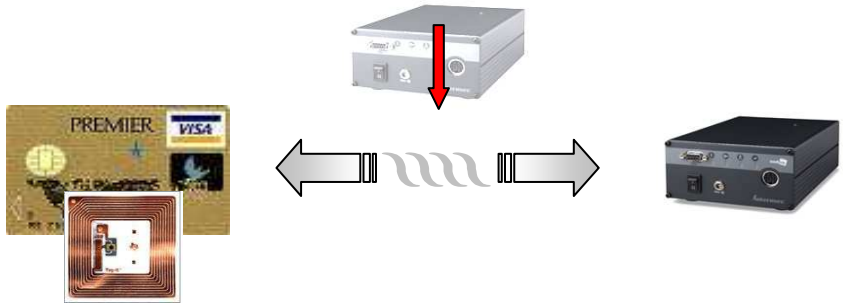

- **Stand alone** nomadic device
- **Embedded** in mobile or PDA

- **EM Spectrum Scanning** for current RFID standards
- Management of **authorized** readers
- Management of **personal** tags and smart cards
- Transaction of **personal data** enabling or disabling
- Reader and tag/smart card **emulator** → NFC and more RF Bands
- Data exchange **interception and control**
- Communication blocking / jamming : **private sphere**
- **Friendly user** interface with messages logging and display

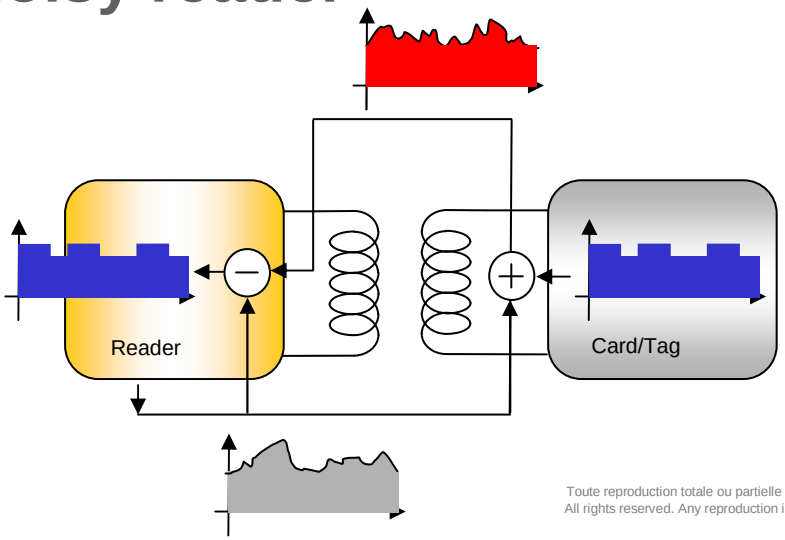
# M2M PET: Low cost tags

## Contactless link protection

- Eavesdropping spying
- Protocol replay
- No Tag over cost
- No Key management




## Noisy reader



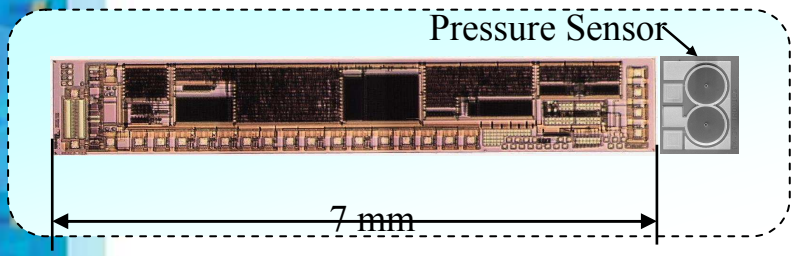

## Low Cost Solutions

- Secure NF Communications
- Jammers → Noisy Reader
- No Shared Secret
- Low cost Tag: No Change

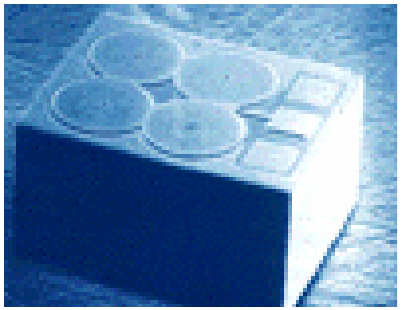
# Presentation plan

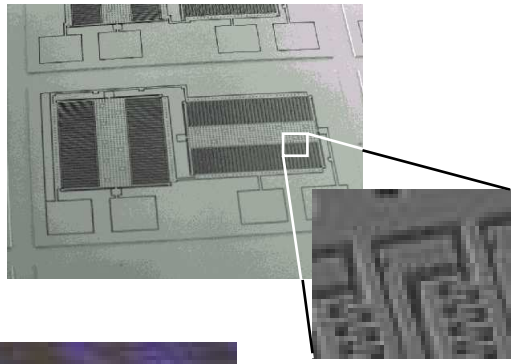
- Technological Perspectives of RFID and IoT at LETI
- RFID air interface
  - Large file transfer for large memory
  - Inventory protocols
- RFID Security
  - Security for low resources devices
  - Privacy
- Beyond RFID
  - Micro-sensors
  - Micro-batteries
  - WSN

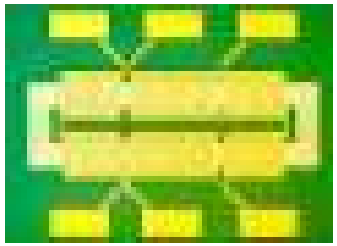
# Micro-Sensors - MEMS - Packaging

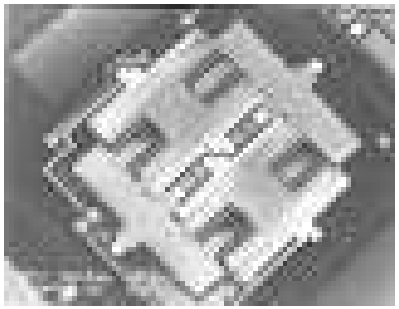



- Accelerometer
- Gyro meter
- Magnetometer
- Pressure

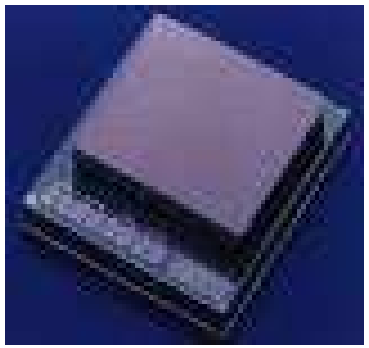






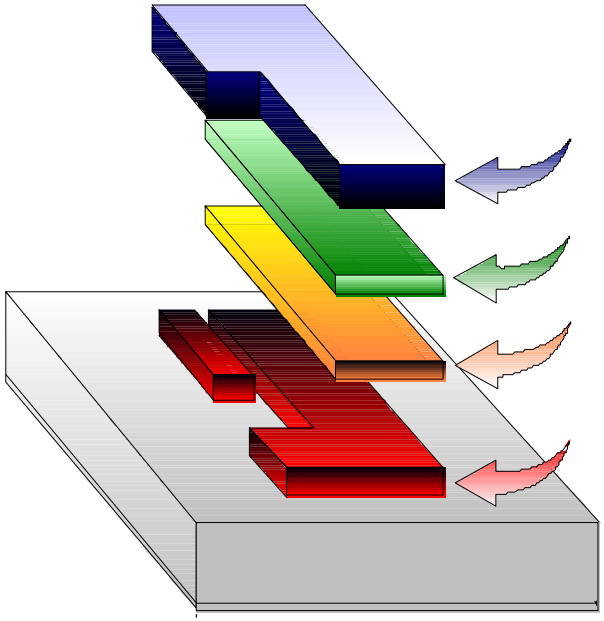
- Micro-packaging



- Micro-Switch

# Above IC Micro battery

## ❑ Above IC Process



Li Anode

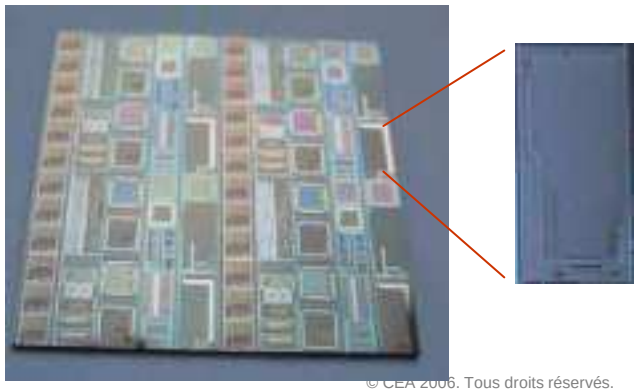
LIPON Solid electrolyte

$TiS_xO_y$ Cathode

Current collector

Substrat (Si)

Above IC micro battery prototype



# RFID Life Cycle

## Security Issues

**Companies assets protection**

**Privacy protection**

**Waste processing**

Reverse engineering:

- Chip tampering

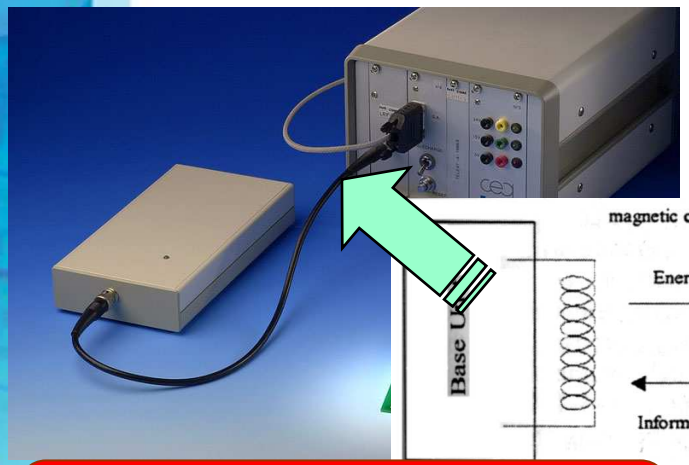
**Utilization**

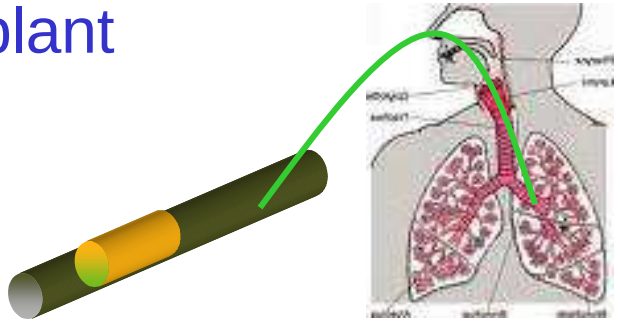
Near reader

- Privacy protection

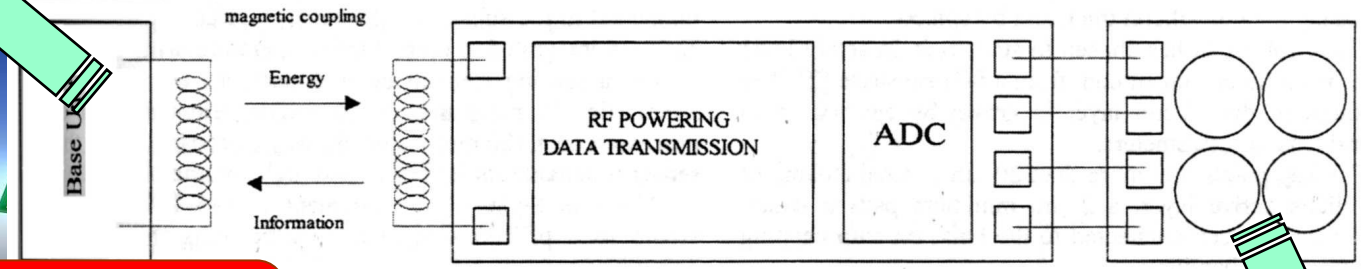
# Medical application: Pulmonary pressure monitoring

- Microsystem implant
  - No wire
  - No battery





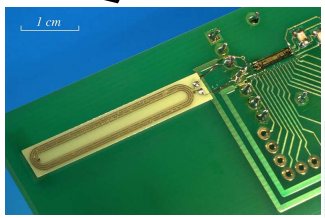
• Catheter 1,5 mm + micro-module

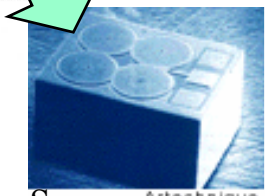



**DATA INTEGRITY**

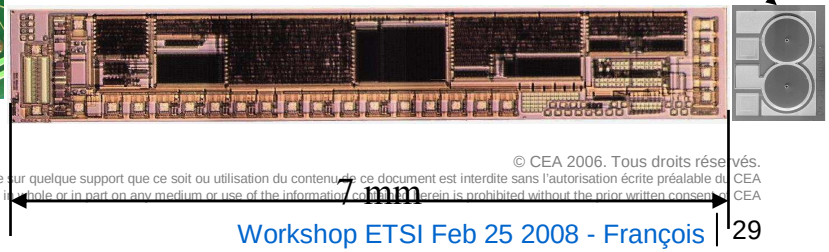
## Characteristics

- Fe= 200Hz, ΣΔ 14 bits
- Capacitive pressure sensor
- Miniaturized antenna



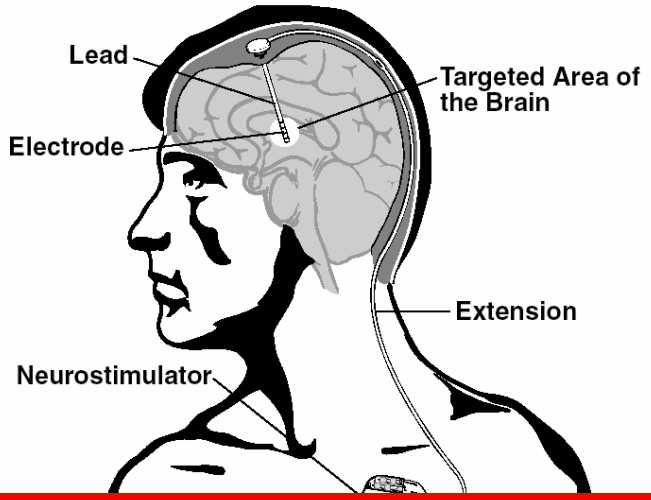



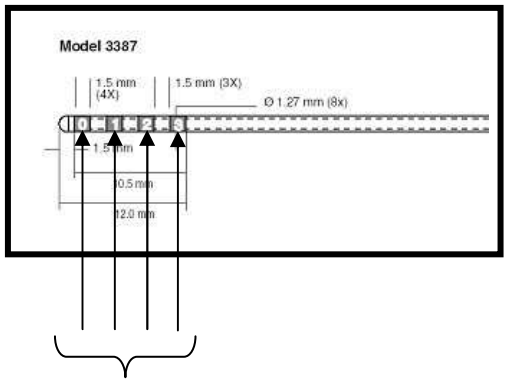
Pressure Sensor Artechnique




Source CEA-LETI

# Medical application: Parkinson Control

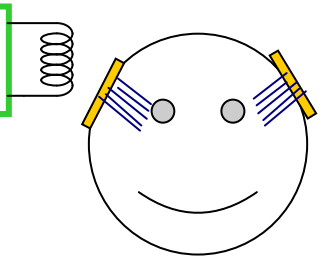



- 4 Electrodes for each probe
- 5 probes embedded for a lobe

**NO REMOTE CONTROL**

Contactless External control

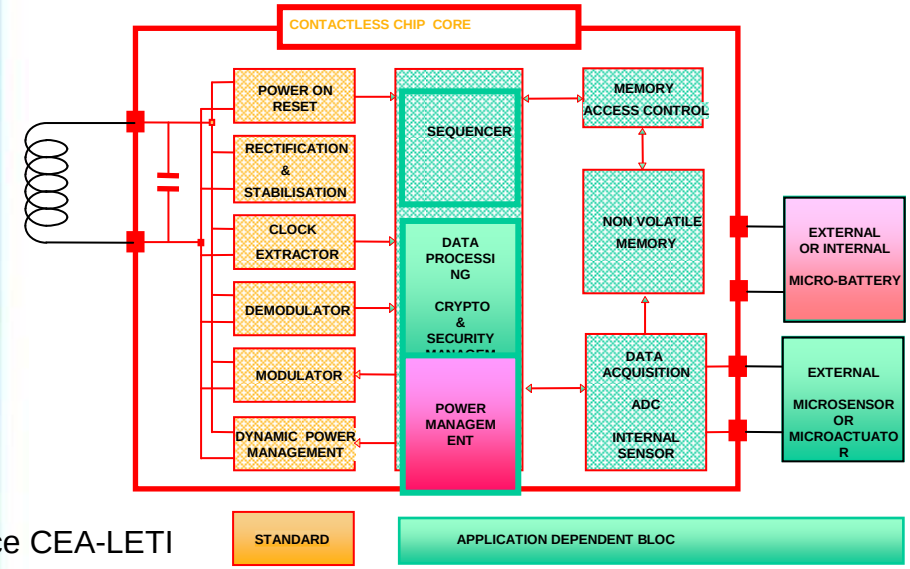


## Characteristics

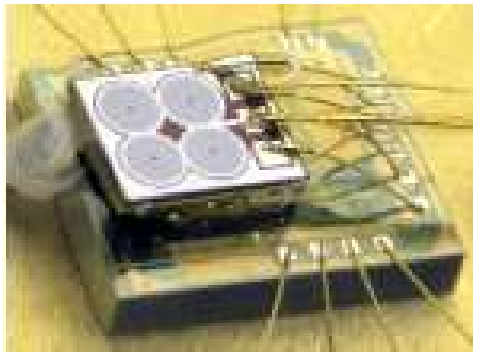
- Embedded electrodes
- External tuning (RFID)
- Chirurgical operation 10H → 2H
- Periodic tuning without operation

Source CEA-LETI

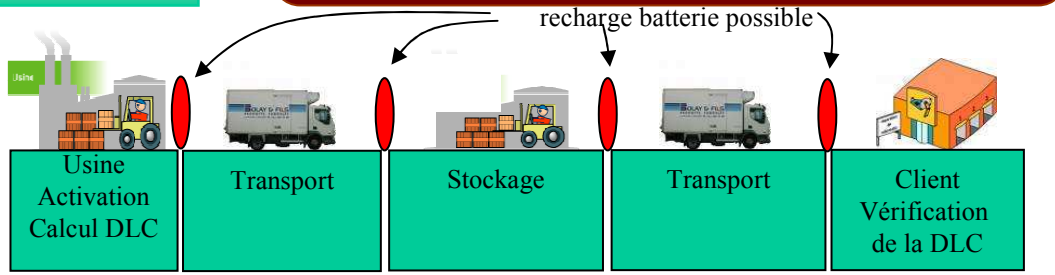
# Health application: Fresh food T° tracking




Source CEA-LETI

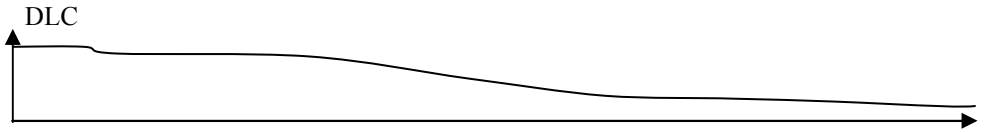


NO DATA TAMPERING





Mémorisation du couple temps/température pour des variations de température significatives




Évolution de la DLC calculée par IDTAG en fonction de la température (Source ID-TAG)

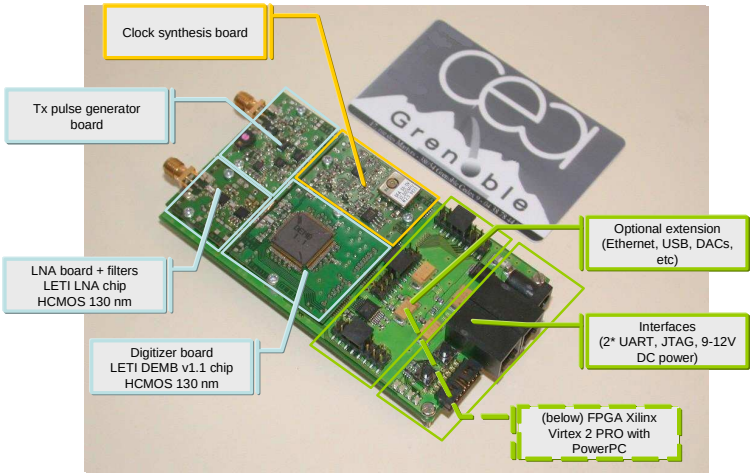
## Characteristics

- Temperature logging
- Embedded sensors
- Embedded battery
- On line information

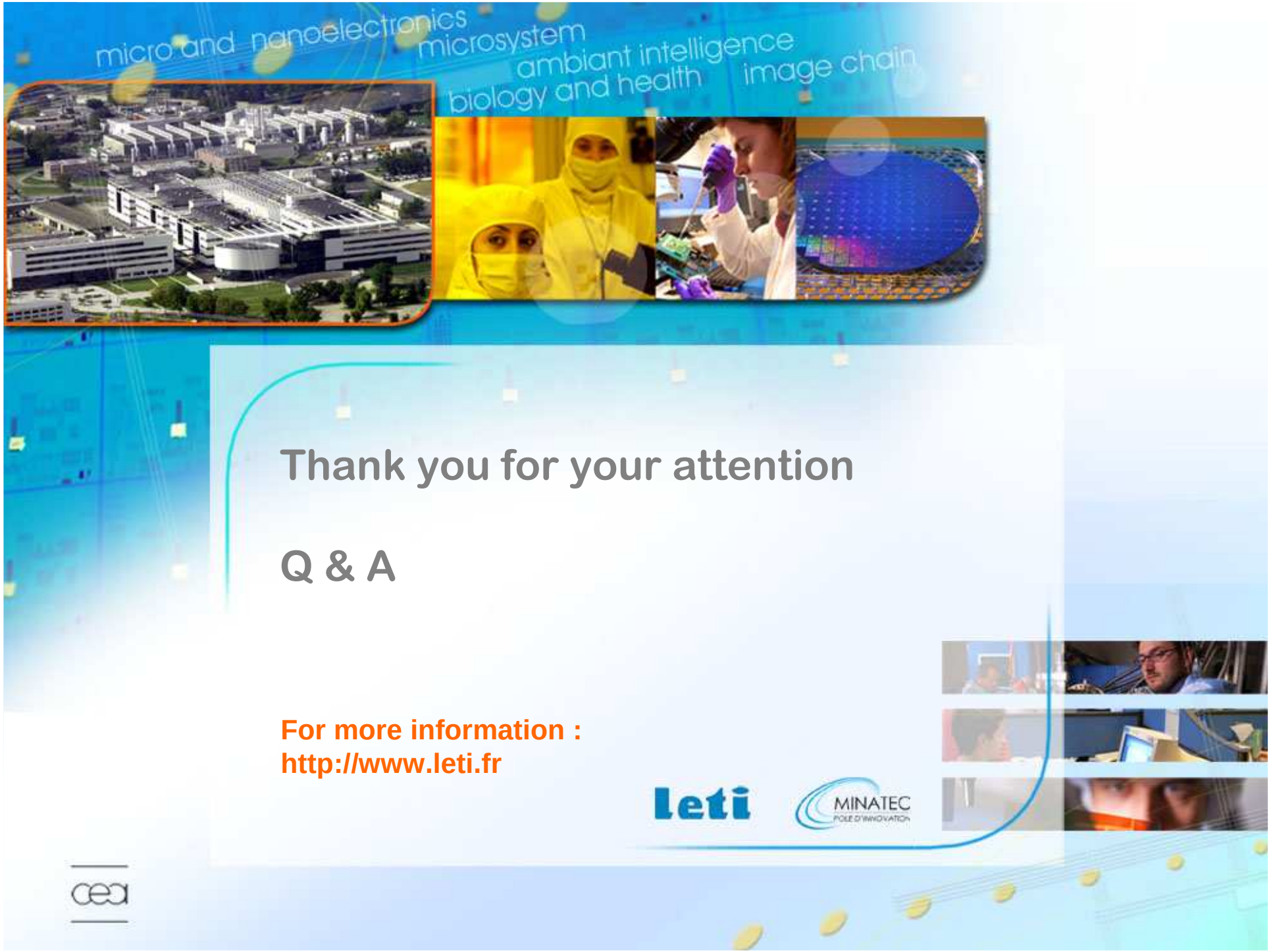
# Wireless Sensors Network

## LétiNode

- Generic Sensor Node (LétiNode)




- Open Platform:
  - Ultra Low Power RF (Zigbee, UWB)
  - Micro sensors
  - Micro batteries
  - Distributed Algorithms : synchro, tracking, MIMO
  - Data Security : PHY, routing, ciphering
  - Integration roadmap
  - Anticipation of standards (IEEE, ETSI)




# Thank you for your attention

## Q & A

**For more information :**
**http://www.leti.fr**

leti

MINATEC
POLE D'INNOVATION

cea