

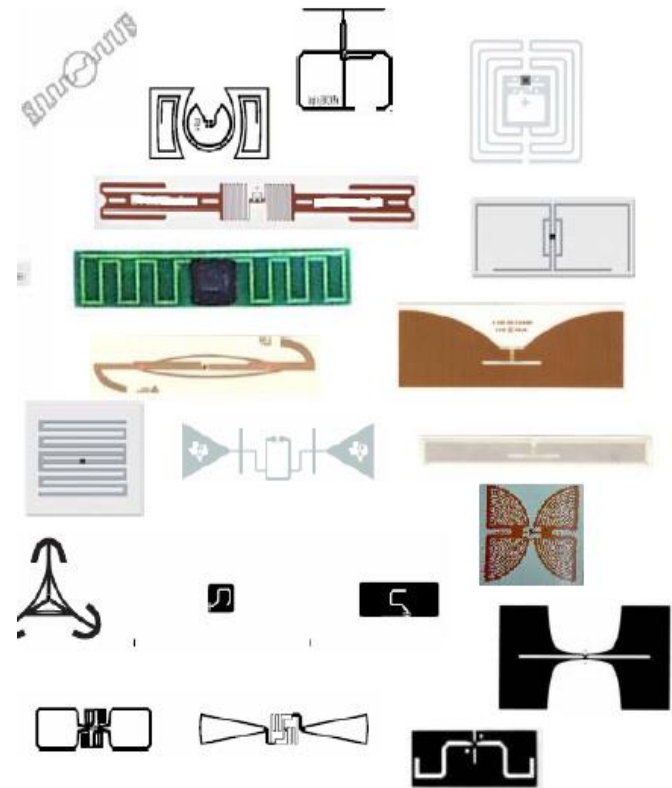
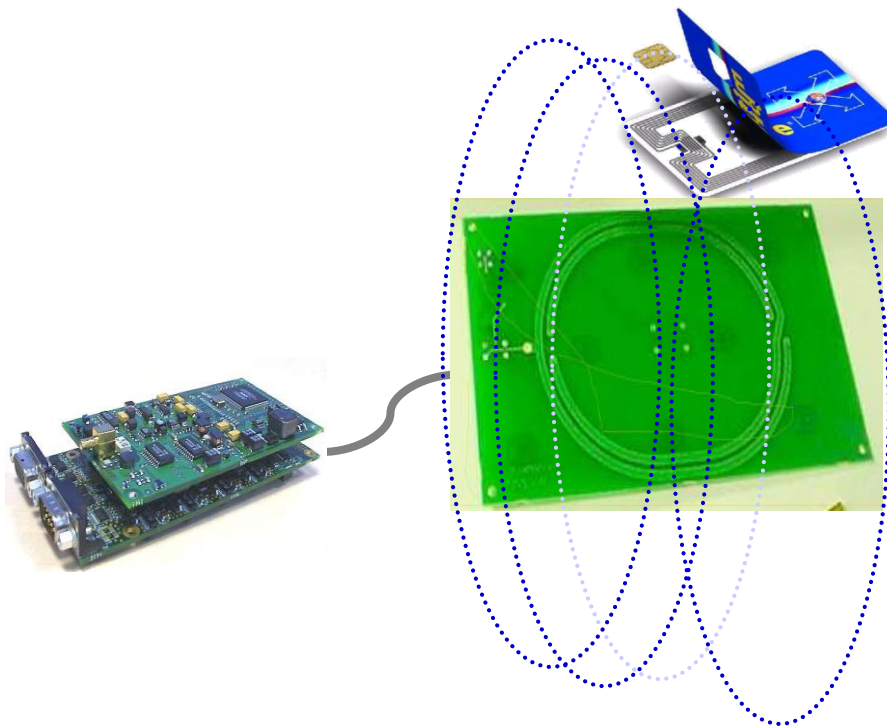
## Sécurité physique et carte à Puces

**Mohamed Senhadji**

senhadji@ensias.ma

# Module II

## Introduction à la techno RFID



- Qu'est ce que la RFID ?
- Un peu d'histoire...
- Carte à puces sans contact
- Classification & état de l'art de la RFID
- Panorama de la standardisation
- Introduction aux cartes à puce sans contact
  - Caractéristiques Physiques
  - Modes de communications
  - Initialisation et Anticollisions
  - Protocoles de transmission

## ➤ Définition :

- ✓ Un ensemble de dispositifs ayant pour fonction d'identifier et de traiter, par ondes radio, les informations contenus dans un ou plusieurs éléments déportés

## ➤ Fonction :

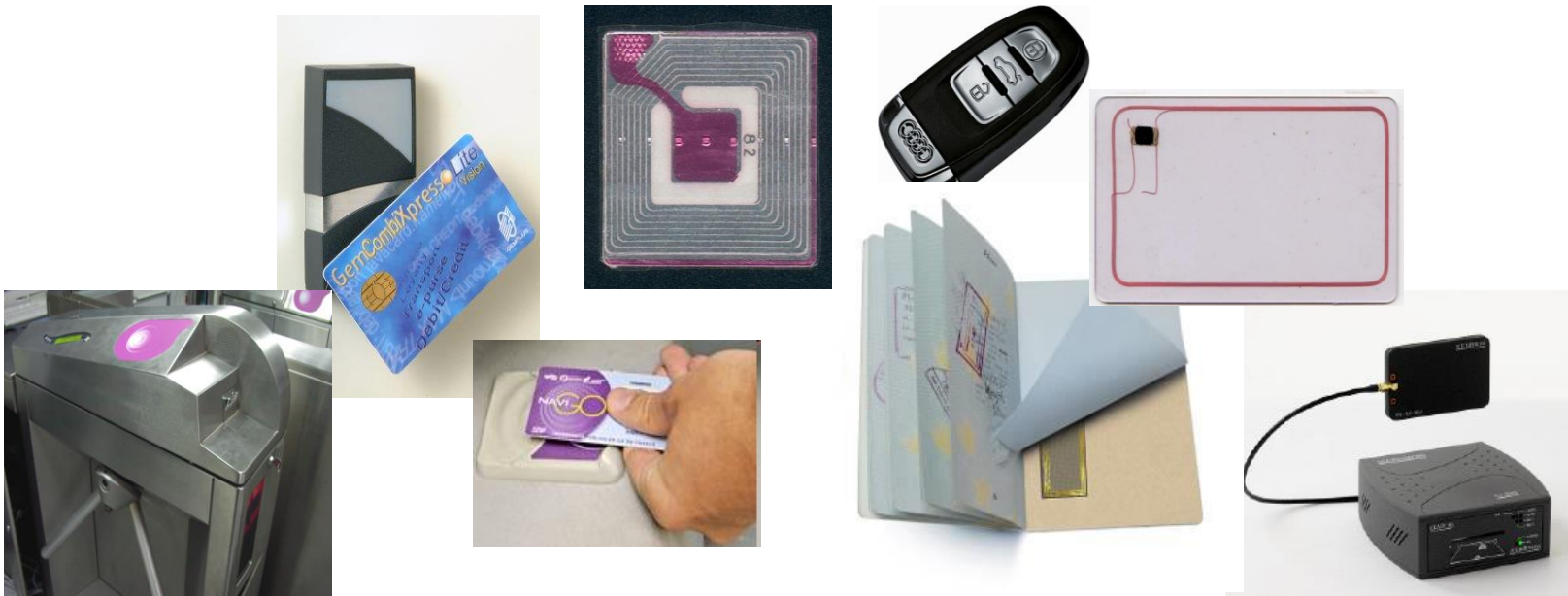
- ✓ Identification automatique et traçabilité des objets
- ✓ Authentification des documents électroniques, sécurité des transactions, etc,

## ➤ But :

- ✓ Réduction des erreurs, de la fraude
- ✓ Rapidité, amélioration des processus, services et produits
- ✓ Sécurité et ergonomie, etc,

# Qu' est-ce que la RFID (2/3)

- Terminologies, applications et environnement variés
  - ✓ Tag, puce RFID, Carte à puce sans contact, Transponder (TRANSmitter / resPONDER), jeton
  - ✓ Lecteur, Terminal, Station Bande de base, Transceiver (TRANSmitter / reCEIVER)



- RFID : Radio Frequency IDentification:
- Confluence de quatre disciplines:
  - ✓ Ondes Electromagnétiques
  - ✓ Micro-électronique
  - ✓ Micro-informatique
  - ✓ Cryptographie
- Trois types de RFID
  - ✓ Objets passifs produisant une interaction avec les ondes électromagnétiques
  - ✓ Objets pouvant mémoriser des données dans une mémoire électronique plus ou moins protégée
  - ✓ Objets possédant une véritable capacité de traitement de l'information

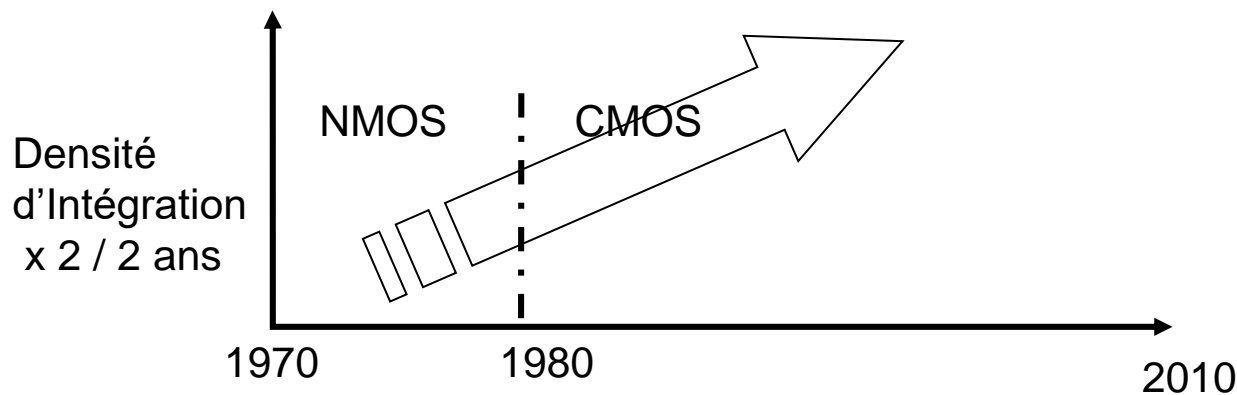
- Qu'est ce que la RFID ?
- Un peu d'histoire...
- Carte à puces sans contact
- Classification & état de l'art de la RFID
- Panorama de la standardisation
- Introduction aux cartes à puce sans contact
  - Caractéristiques Physiques
  - Modes de communications
  - Initialisation et Anticollisions
  - Protocoles de transmission



- Utilisation du Radar durant la seconde guerre mondiale
  - ✓ Identification des avions
  - ✓ Manœuvre des avions entraînant une modification du signal radar retour : un seul bit de reconnaissance → identification amis/ennemis
- H. Stockman, (1948), Communication by means of reflected power



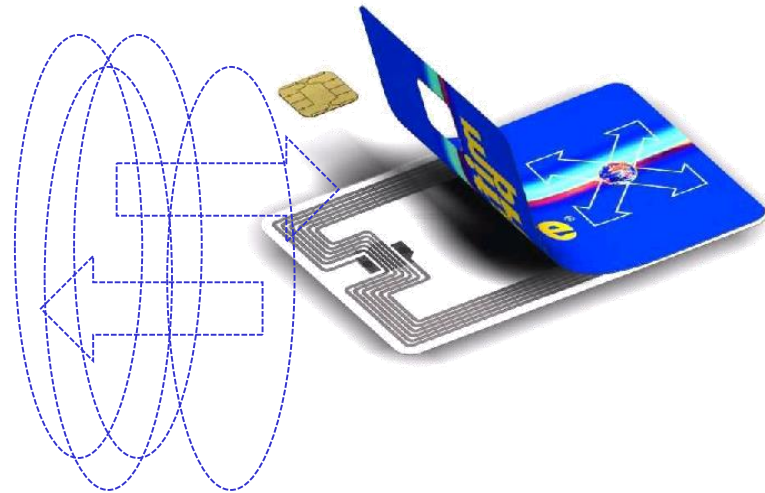
- L'essor de la RFID est lié à celles des technologies CMOS
  - ✓ Multiplication des performances & taille mémoire
  - ✓ Division de la consommation & des coûts
  - ✓ Dimensions des transistors divisées par 2 tous les 2 ans
  - ✓ Complexités des CI & Contraintes technologiques vont de pair
    - Coût R&D multiplié par 3 pour chaque saut technologique
    - Délais importants entre les nouveaux produits sortant des laboratoires de R&D et la production de masse



- Saut technologique CMOS :
  - ✓ Augmentation de fréquence : + 43 %,
  - ✓ Les capacités totales et les tensions d'alimentation - 30 %
  - ✓ La puissance électrique : - 50 %.
  - ✓ Densité de transistor : 100 %
  - ✓ Densité de puissance : 100 %
  - ✓ Densité de courant importante & les porteurs mobiles (électrons) sont très énergétiques
- Caractéristique électrique des circuits CMOS:
  - ✓ Consommation du circuit lors du basculement de la porte logique :  $P = \alpha.f.C.V^2 + V.I_0$ 
    - $f$  : fréquence de l'horloge,  $V$  : alimentation;  $\alpha$  : taux d'activités des portes logiques,  $I_0$  : courant de repos (fuite)

- Qu'est ce que la RFID ?
- Un peu d'histoire...
- **Carte à puces sans contact**
- Classification & état de l'art de la RFID
- Panorama de la standardisation
- Introduction aux cartes à puce sans contact
  - Caractéristiques Physiques
  - Modes de communications
  - Initialisation et Anticollisions
  - Protocoles de transmission

# Cartes à puce sans contact



# Domaines d'applications ...

- Transport de Masse



- Contrôle d'Accès



- Paiement Électronique



- Cartes d'Identités sécurisées
- (e -Passeport, ...)



- NFC

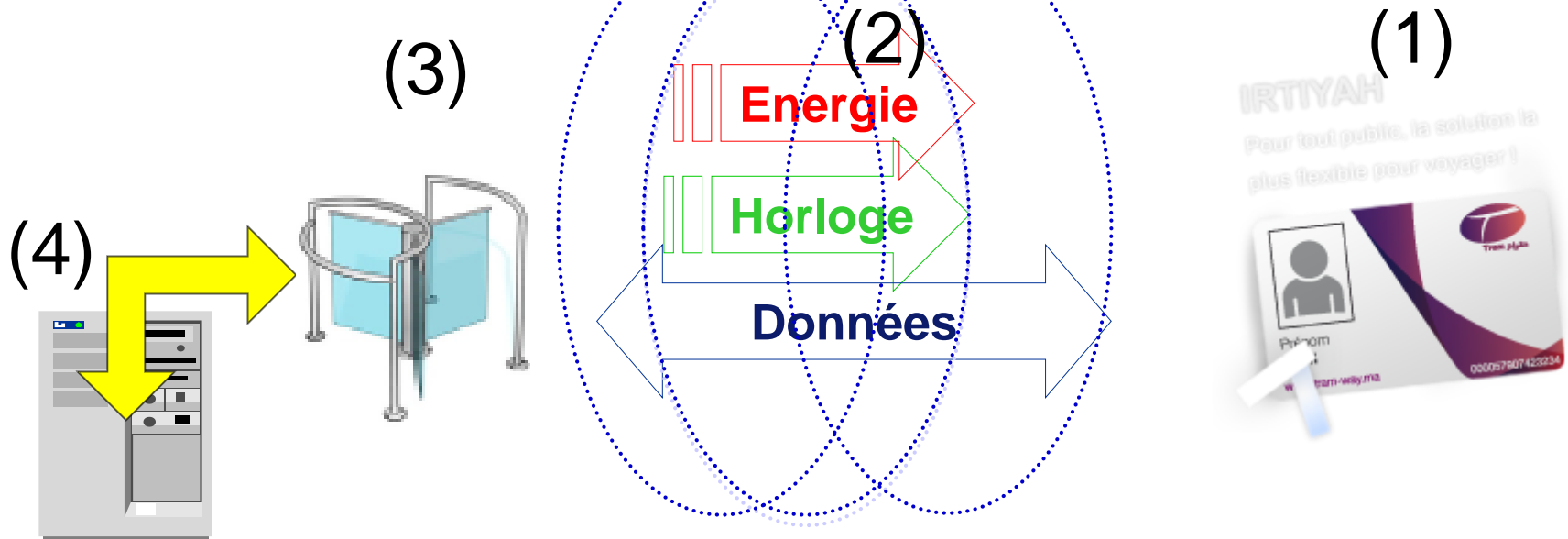


## ➤ Les principales applications RFID

- ✓ Défense & Industrie (automobile, Semi-conducteurs, aviation, etc)
  - Inventaire
  - Localisation et suivi des équipements et des personnes
- ✓ Santé, hôpitaux, Distributions, Luxe, etc
  - Contrefaçon de produits
  - Gestion des stocks
  - Localisation et suivi des équipements et des personnes
- ✓ Grand public, Commerces & finances (Transport, Contrôle d'accès, Banque, loisirs, etc)
  - Gestion & contrôle des flux d'objets et de personnes
  - Paiement électronique, signature électronique
  - Gestion et offre de services

## ➤ 4 entités

- ✓ La carte à puce sans contact ou RFID
- ✓ Le canal de communication (air) ou zone opérationnelle
- ✓ Le lecteur (ou station de base) sans contact
- ✓ Serveur - Middleware et Application Software  
(Traitement des données) : Log, analyse et archivage





- Qu'est ce que la RFID ?
- Un peu d'histoire...
- Carte à puces sans contact
- **Classification & état de l'art de la RFID**
- Panorama de la standardisation
- Introduction aux cartes à puce sans contact
  - Caractéristiques Physiques
  - Modes de communications
  - Initialisation et Anticollisions
  - Protocoles de transmission

- Grande variété des dispositifs, des fonctionnalités, des applications et des usages
- Plusieurs classements possibles. On peut choisir comme critères :
  - ✓ Les fréquences de travail
  - ✓ Les types de transpondeur
  - ✓ Les modes d'activation de l'énergie et de transmission des données

- Classification par gammes de fréquences disponibles
  - ✓ ISM (Industrial-Scientific-Medical)



Fréquences ISM disponibles pour la RFID			
LF / BF	≤	135	<b>KHz</b>
HF / RF	=	13,56	<b>MHz</b>
UHF	=	434	<b>MHz</b>
		860 - 960	<b>MHz</b>
SHF	=	2,45	<b>GHz</b>

- ✓ Corollaires
  - Champ proche et champ lointain
  - Couplage inductif ou électromagnétique
  - Zone opérationnelle ou portée
- Etat de l'art : combinaison de technologies RF + UHF

- Classification par types de transpondeur / puce RFID
  - ✓ Mémoire & logique câblée
  - ✓ Microprocesseur
  - ✓ Composants passifs (circuits résonants RLC)

## ➤ Les puces RFID contiennent des Mémoires Non Volatiles (MNV)

### ✓ Opérations basiques sur les Données:

- Entrée
  - Sortie → délivre des données au monde extérieur 
  - Lecture dans Mémoire Non Volatile (MNV)
  - Écriture ou Effacement dans MNV → modification du contenu 
  - Exécution de fonction Cryptographique
- ✓ Chacune de ces 5 opérations sont reliées à la sécurité HW de la carte.
- Les opérations 2 & 4 sont particulièrement sensibles

## ➤ Etat de l'art :

### ✓ Points faibles :

- Accès à l'écriture
- Endurance et Temps de rétention de l'information (durée de vie 100000 cycles lecture/écriture)

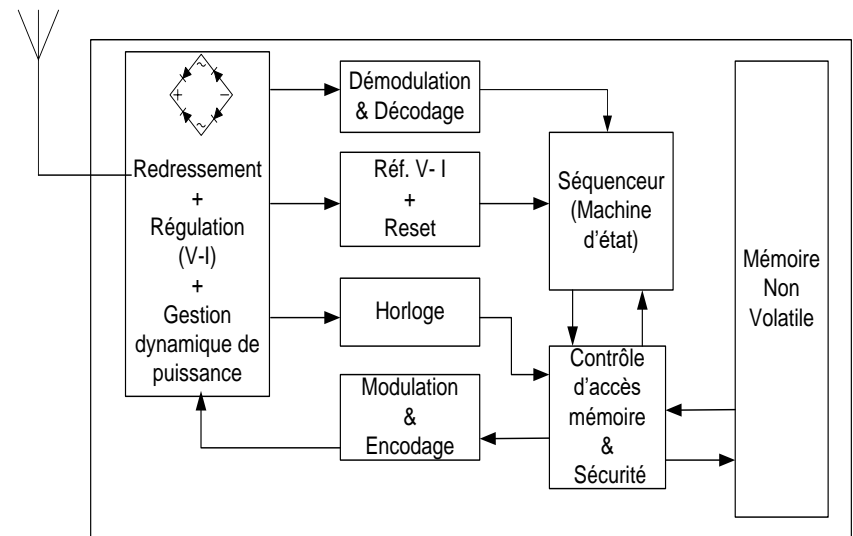
### ✓ Nouvelles technologies FeRAM, MRAM

- Temps d'accès < 100 ns et faible consommation

## • RFID à mémoire

### - Plus values :

- Gestion de puissance
- Démodulation & Décodage



## Comparaison entre FeRAM & EEPROM

---

	FRAM	EEPROM
Size of memory cell	$\sim 80 \mu\text{m}^2$	$\sim 130 \mu\text{m}^2$
Lifetime in write cycles	$10^{12}$	$10^5$
Write voltage	2 V	12 V
Energy for writing	0.1 $\mu\text{J}$	100 $\mu\text{J}$
Write time	0.1 $\mu\text{s}$	10 ms (10 000 $\mu\text{s}$ )

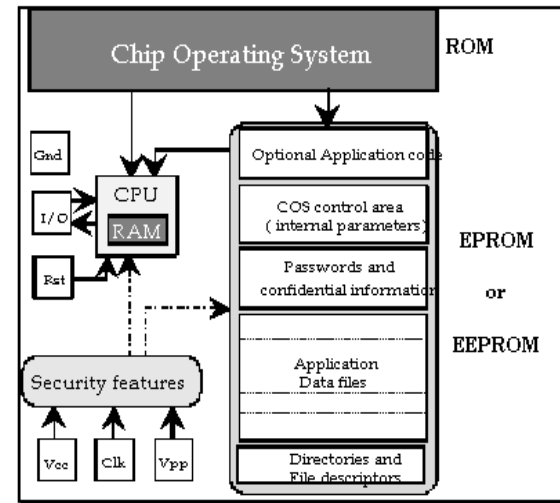
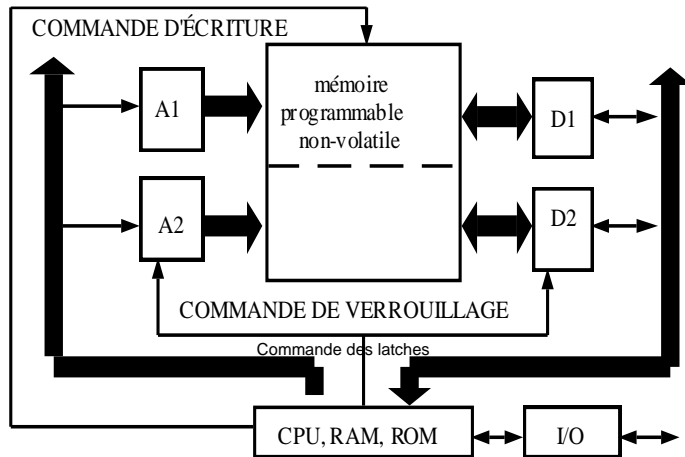
Les données ne sont pas stockées sous forme d'une charge électrique mais d'une charge magnétique. Le changement d'état se fait en changeant le spin des électrons (par effet tunnel notamment).

Cette méthode de stockage possède les avantages suivants :

- la non volatilité des informations ;
- une théorique inusabilité, puisqu'aucun mouvement électrique n'est engagé ;
- la consommation électrique est très minim puisqu'il n'y a pas de perte thermique due à la résistance des matériaux aux mouvements des électrons.
- La MRAM est souvent considérée comme la mémoire « idéale » alliant rapidité, débit, capacité et non volatilité, ce qui peut amener à penser qu'elle entraînera la fin de la hiérarchie des mémoires.



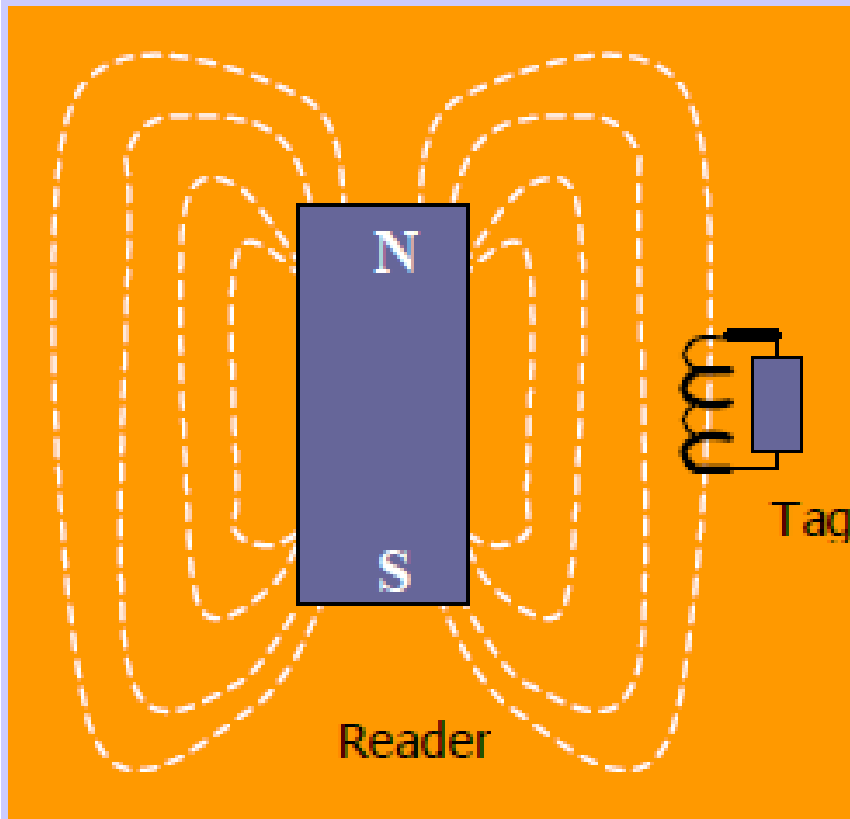
## ➤ RFID à microprocesseur (Carte à puce)



- ✓ SPOM (Self-Programmable One-chip Microprocessor) :  
Déclenchement des routines internes pour protéger leurs données et contrôler tous les signaux logiques et électriques à destination de sa MNV (en particulier les opérations de lecture/écriture).
- ✓ Éléments de sécurités divers, complexes et répartis

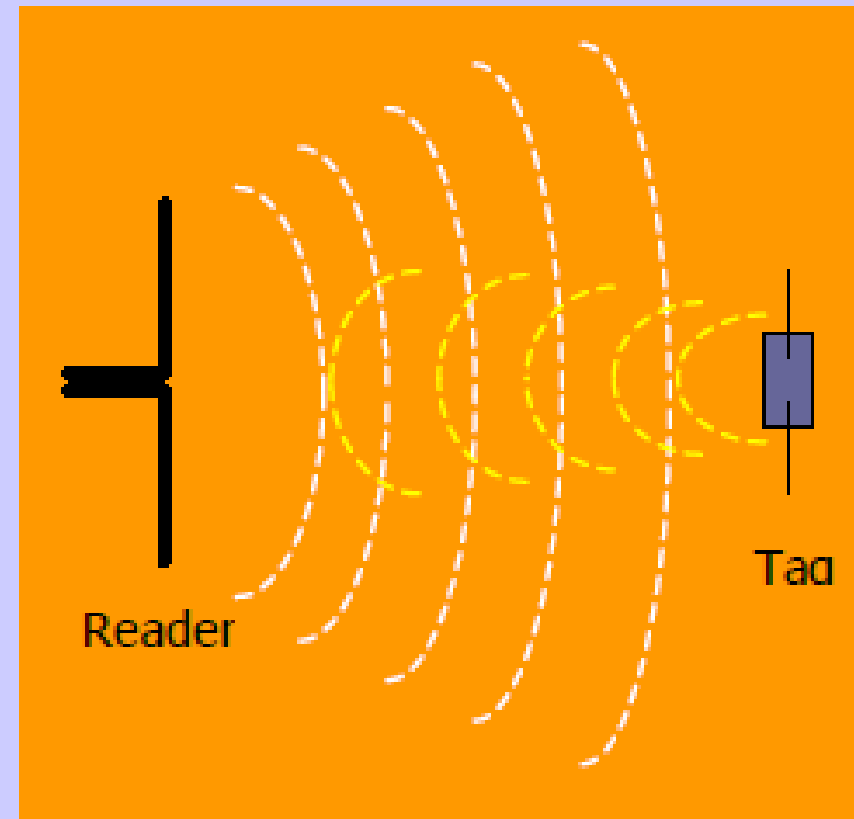
# Near Far Field Power/Communication (9/15)

Magnetic Field (near field)  
Inductive coupling



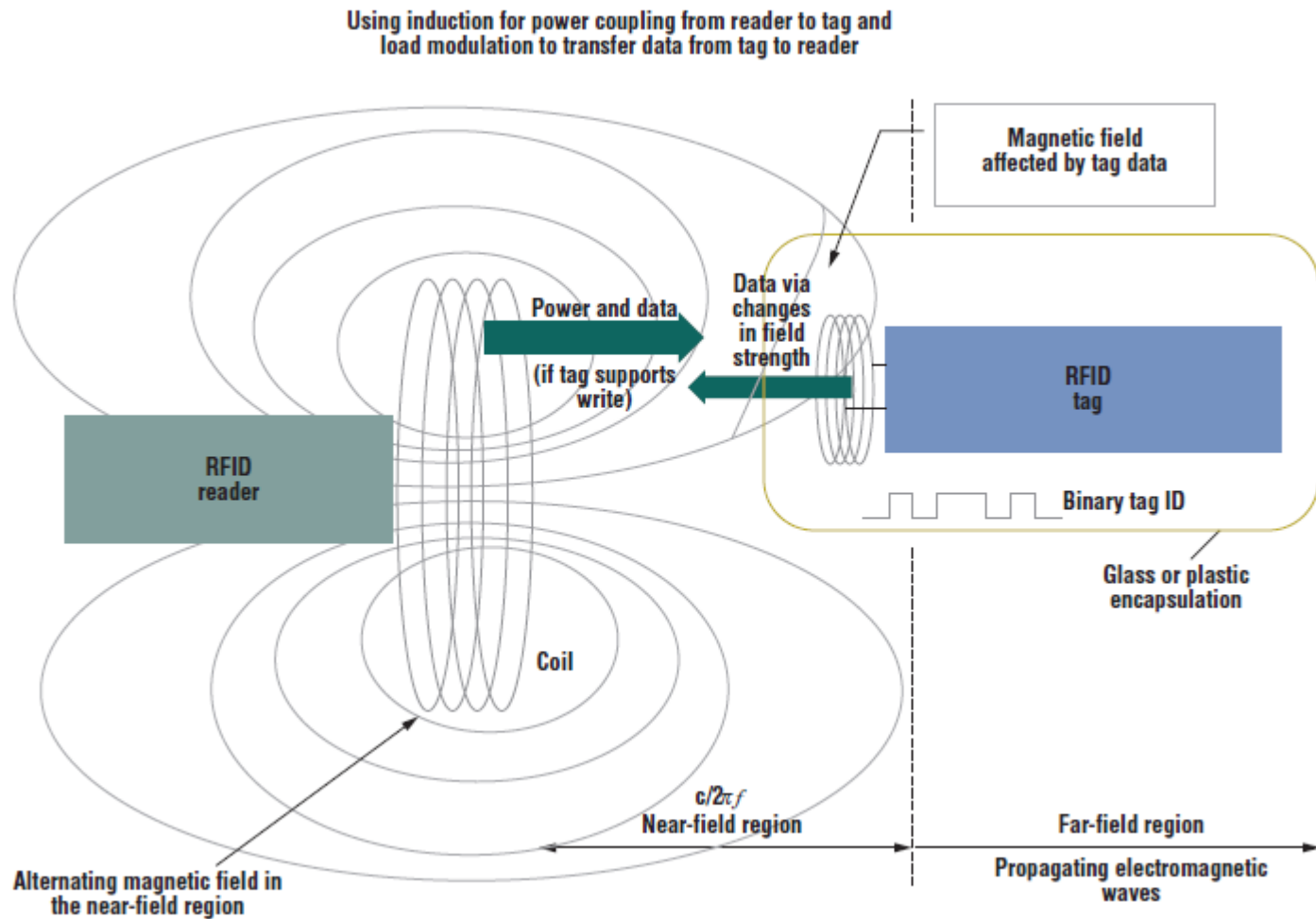
**LF and HF**

Electric Field (far field)  
Backscatter



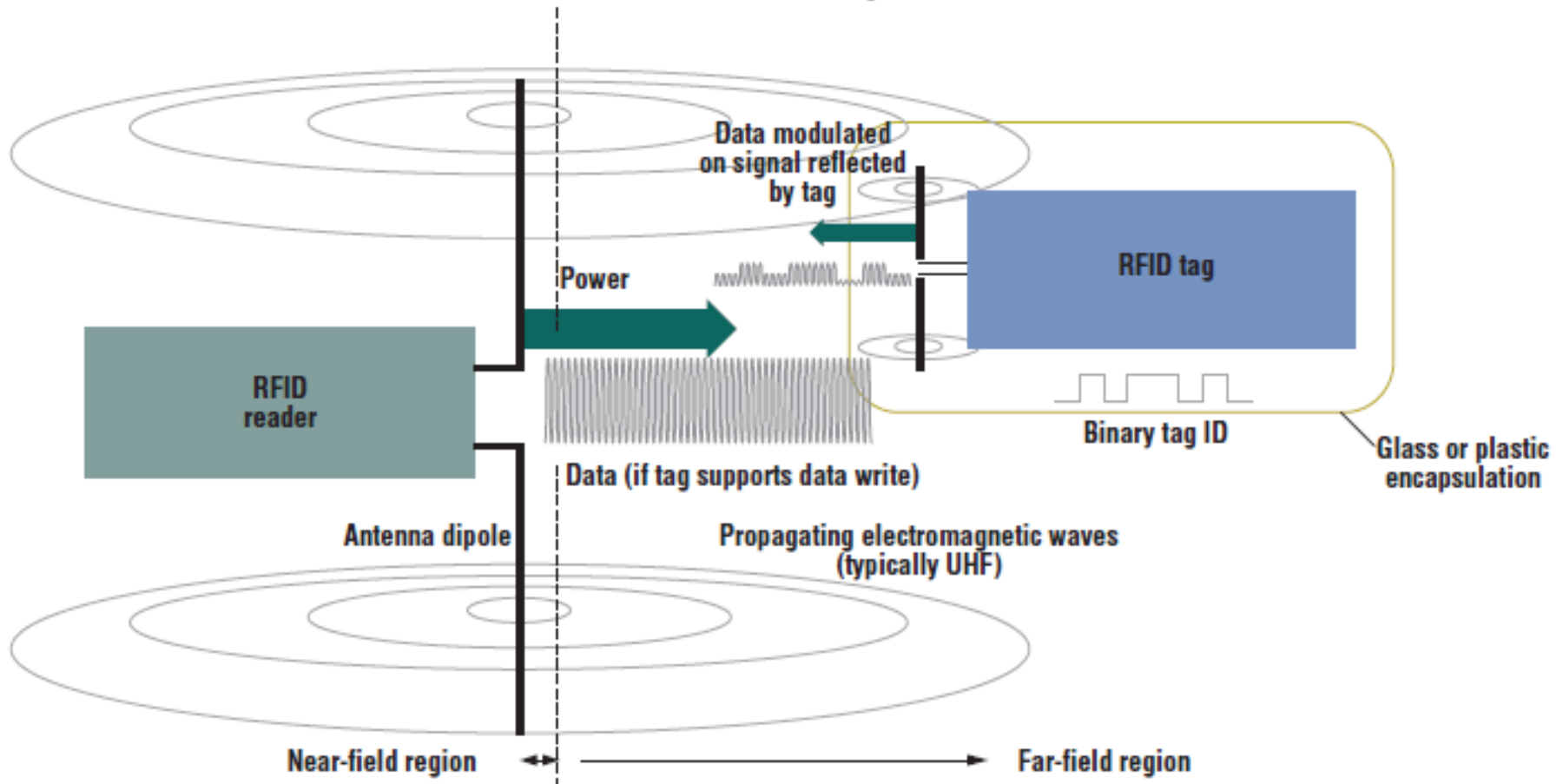
**UHF**

# Near Field Power/Communication (10/15)



# Far Field Power/Communication (11/15)

Using electromagnetic (EM) wave capture to transfer power from reader to tag  
and EM backscatter to transfer data from tag to reader



## ➤ Classification par les modes de transmission de l'énergie

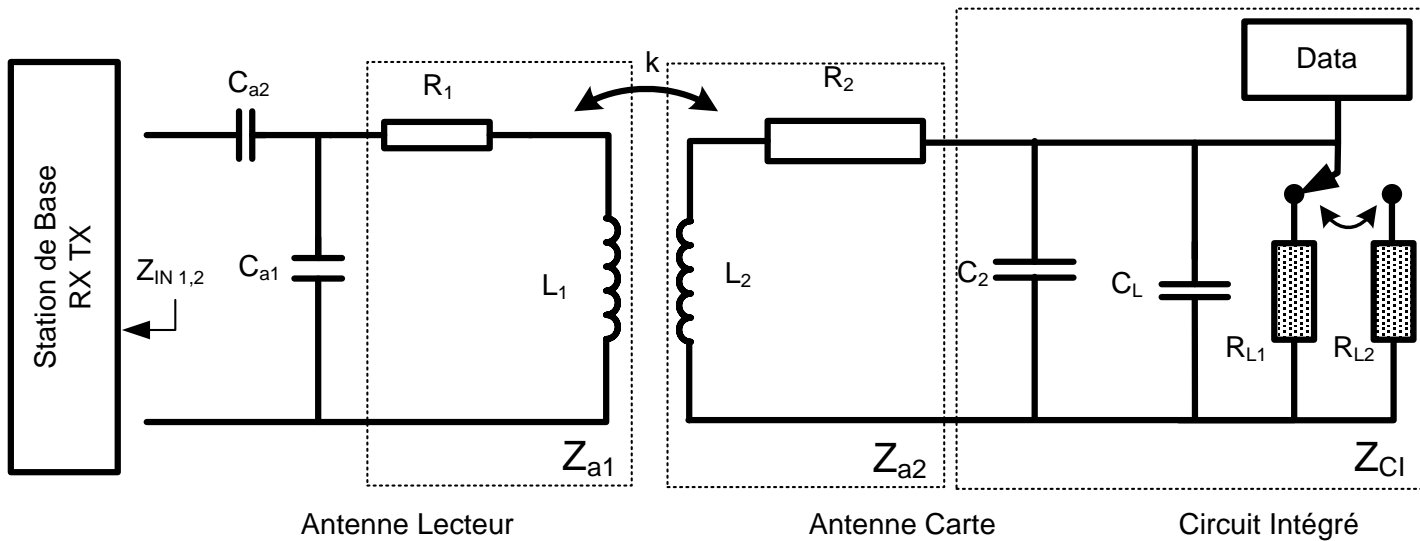
- ✓ RFID passive : la puce RFID est alimentée par l'onde électromagnétique émise par le lecteur.
- ✓ RFID semi-passive : la puce RFID est assistée par une batterie pour alimenter en puissance sa circuiterie et améliorer la sensibilité de son bloc de réception des signaux radios.
- ✓ RFID active : la puce RFID active permet un gain en puissance (+ 20 dBm par rapport aux puces passives)
  - Avantage → améliore la portée
  - Inconvénient → problèmes d'interférences (multiplications des échos radios qui engendrent à leur tour des difficultés de localisations des puces par les lecteurs.
  - Solutions : incorporer des protocoles et des algorithmes qui permettent de corriger, en partie, l'impact de ces interférences multi-chemins mais cela augmente la consommation électrique due à l'activité des portes logiques CMOS

# Classification des Tags (13/15)

**Table 3.4** Characteristics of RFID Tag Classes

Tag Characteristic				
Tag Class    v	Type	Memory	Communication	More Properties
Class 0	Passive	Read-only	Does not initiate communication	The EPC number is encoded onto the tag during manufacture and can be read by a reader)
Class 0+	Passive	Same as class 0, but you can write once	Does not initiate communication	—
Class 1	Passive	Read and write-once	Does not initiate communication	EPC number is not encoded by the manufacturer but can be encoded later in the field
Class 2	Passive	Read and write-once	Does not initiate communication	Encryption
Class 3	Semipassive	Read and rewritable	Does not initiate communication	Class 2 capabilities plus extra such as integrated sensors
Class 4	Active	Read and rewritable	Can initiate communication; power their own communication; tag-to-tag communication possible	Class 3 capabilities plus extras
Class 5	Active	Read and rewritable	Can initiate communication; power their own communication; tag-to-tag communication possible	Class 4 capabilities plus extras

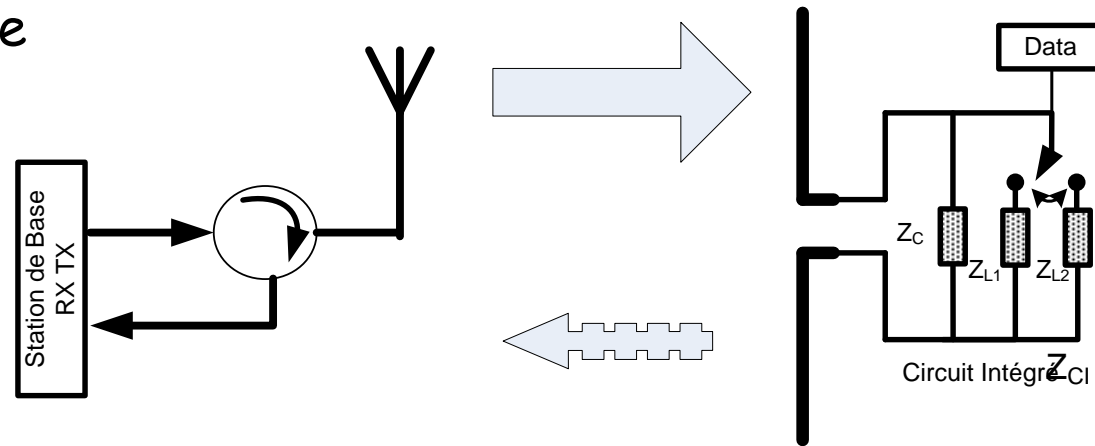
- Classification par les modes de transmission des données
  - ✓ BF & RF : Couplage magnétique et modulation de charge :



- ✓ La puce RFID apparait comme une charge vis à vis du lecteur
- ✓ La puce RFID module sa charge (résistive ou capacitive)
- ✓ Une grande majorité des puces RFID utilisent le mécanisme de modulation d'une charge résistive.

## ➤ Classification par les modes de transmission des données

- ✓ UHF & SHF : Couplage électromagnétique et modulation d'impédance



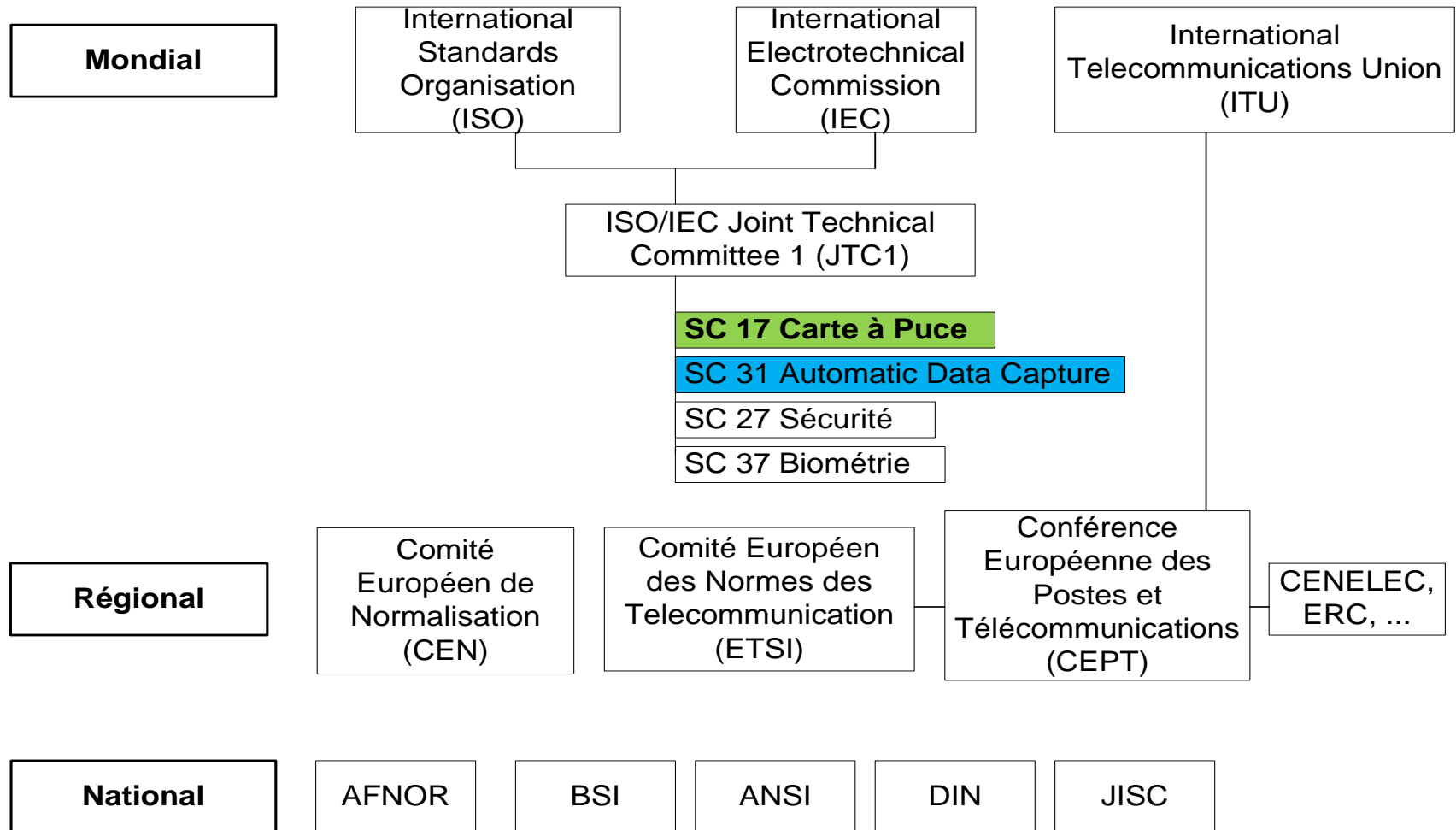
- ✓ Lorsque l'onde incidente émise par le lecteur rencontre l'obstacle RFID, elle est réfléchi.
  - Variation d'impédance qui peut être résistive, capacitive ou les deux à la fois
  - Information : modulation du champ électromagnétique réfléchi



- Qu'est ce que la RFID ?
- Un peu d'histoire...
- Carte à puces sans contact
- Classification & état de l'art de la RFID
- **Panorama de la standardisation**
- Introduction aux cartes à puce sans contact
  - Caractéristiques Physiques
  - Modes de communications
  - Initialisation et Anticollisions
  - Protocoles de transmission

- Deux types de normes:
  - ✓ Normes techniques : elles concernent les produits
  - ✓ Normes applicatives : elles concernent l'utilisation des produits
- Traçabilité des objets ( Smart Label RFID)
- Traçabilité des personnes (Smart Card RFID)

# Panorama de la standardisation (2/7)



## ➤ ITU : Affectation des fréquences ISM (Industrial, Scientific & Medical) par Régions



Fréquences	Région 1	Région 2	Région 3
<b>BF</b>	<b>&lt; 135 KHz</b>	<b>&lt; 135 KHz</b>	<b>&lt; 135 KHz</b>
<b>RF</b>	<b>13,56 MHz</b>	<b>13,56 MHz</b>	<b>13,56 MHz</b>
<b>UHF</b>	<b>865,5 – 869,65 MHz</b>	<b>902 – 928 MHz</b>	<b>860 – 960 MHz</b>
<b>SHF</b>	<b>2,4 – 2,4835 GHz</b>	<b>2,4 – 2,4835 GHz</b>	<b>2,4 – 2,4835 GHz</b>

- ISO 18000 - Radio frequency identification  
for item management - Distance < 1 m
  - ✓ 18 000 - 1 : définition des paramètres standardisés et Architecture de référence
  - ✓ 18 000 - 2 : RFID fonctionnant à < 135 KHz
  - ✓ 18 000 - 3 : RFID fonctionnant à 13.56 MHz
  - ✓ 18 000 - 4 : RFID fonctionnant à 2.45 GHz
  - ✓ 18 000 - 5 : RFID fonctionnant à 5.8 GHz
  - ✓ 18 000 - 6 : RFID fonctionnant de 860 à 960 MHz
  - ✓ 18 000 - 7 : RFID active fonctionnant à 433 MHz



- ISO 15693 - Vicinity card - 13.56 MHz - Distance < 1,5 m
- ISO 14443 : Identification Cards - Contactless Integrated Circuit Cards
- ISO 10373-6
  - ✓ les méthodes et les outils de test et de mesure.



## ➤ Contexte d'utilisation :

- ✓ Les réglementations locales :
  - CEPT, FCC, ETSI, ARCEP (ex ART), etc.
- ✓ L'utilisation locale par d'autres organismes (Militaires, opérateurs, ...)
- ✓ Respect des Normes d'exposition du corps humain aux ondes radio (normes européennes EN)
- ✓ Respect des libertés individuelles des utilisateurs potentiels (CNIL, etc.)

## ➤ Normes RFID & Santé Publique :

- ✓ MPE : Maximum Permissible Exposure
- ✓ SAR : Specific Absorption Rate

- RFID Applications

Application	Standard	Token Resources	Security
Item Tracking	ISO 15693	Memory	Minimal/Low
Ticketing	ISO 15693 ISO 14443	Memory/Logic	Low/Medium
Closed Payment	ISO 14443	Logic	Low/Medium
Open Payment	ISO 14443	$\mu$ -Controller	High
Access Control	ISO 14443	$\mu$ -Controller	High
Identity	ISO 14443	$\mu$ -Controller	High



- Qu'est ce que la RFID ?
- Un peu d'histoire...
- Carte à puces sans contact
- Classification & état de l'art de la RFID
- Panorama de la standardisation
- **Introduction aux cartes à puce sans contact**
  - Caractéristiques Physiques
  - Modes de communications
  - Initialisation et Anticollisions
  - Protocoles de transmission

- Pas de parties mécaniques dans les lecteurs,
- Fiabilité : Pas de dommage physiques pour la carte
- Facilité d'utilisation pour les usagers
- Vitesse de transaction optimum 150ms (à contact 2s)
- Coût de maintenance presque nul
- Passage à la volée

## Contraintes :

- Risque de trous dans le champ
- Transaction en limite de champ
- Nécessité de technologie faible consommation

- ISO 14443 : Identification Cards - Contactless Integrated Circuit Cards
  - ✓ Utilisées dans les Transactions Electroniques Sécurisées (Contrôle d'Accès, Paiement, etc.)
  - ✓ ISO 14443/1 : Caractéristiques Physiques
  - ✓ ISO 14443/2 : Transmission RF (Formes d'Ondes)
    - Les différents type de modulation (type A et B)
    - Le codage
  - ✓ ISO 14443/3 : Initialisation & Anticollision
  - ✓ ISO 14443/4 : Protocoles

# 2 Interfaces RF dans le Standard ISO 14443



	TYPE A	TYPE B
Fabricants	Philips, Siemens, Hitachi	ST Micro, Motorola, Sony
Conception	Cartes RF à logique Câblée	Cartes à Microprocesseur
Débit	106 Kbps	847 Kbps
Fréquence Porteuse	13,56 Mhz	13,56 Mhz
Modulation (Downlink) Lecteur-carte	ASK 100%	ASK 10%
Codage	Miller Modifié	NRZ
Modulation (Uplink) Carte-Lecteur	Mod charge ASK	Mod Phase BPSK
Codage Porteuse	Manchester 847 Khz	NRZ 847 Khz

- Des standards mondiaux
- De bonnes performances de lecture
- Une large offre de lecteurs
- Des mémoires importantes
- Gestion du Multi-application
- Sécurité et protection des données
- Technologie mature (depuis 2000)
- Coût très faible

# ISO 14443

## Part 1 :

### Physical Characteristics

- Ce standard correspond aux caractéristiques mécaniques :
  - Dimension spécifié par ISO 7810
    - 85.72mm x 54.03mm x 0.76mm +/- Tolérance
  - Contrainte de torsion et de flexion
  - Irradiation avec de l'UV, rayon X et les radiations électromagnétiques

- Qu'est ce que la RFID ?
- Un peu d'histoire...
- Carte à puces sans contact
- Classification & état de l'art de la RFID
- Panorama de la standardisation
- Introduction aux cartes à puce sans contact
  - Caractéristiques Physiques
  - Modes de communications
  - Initialisation et Anticollisions
  - Protocoles de transmission



---

# ISO 14443

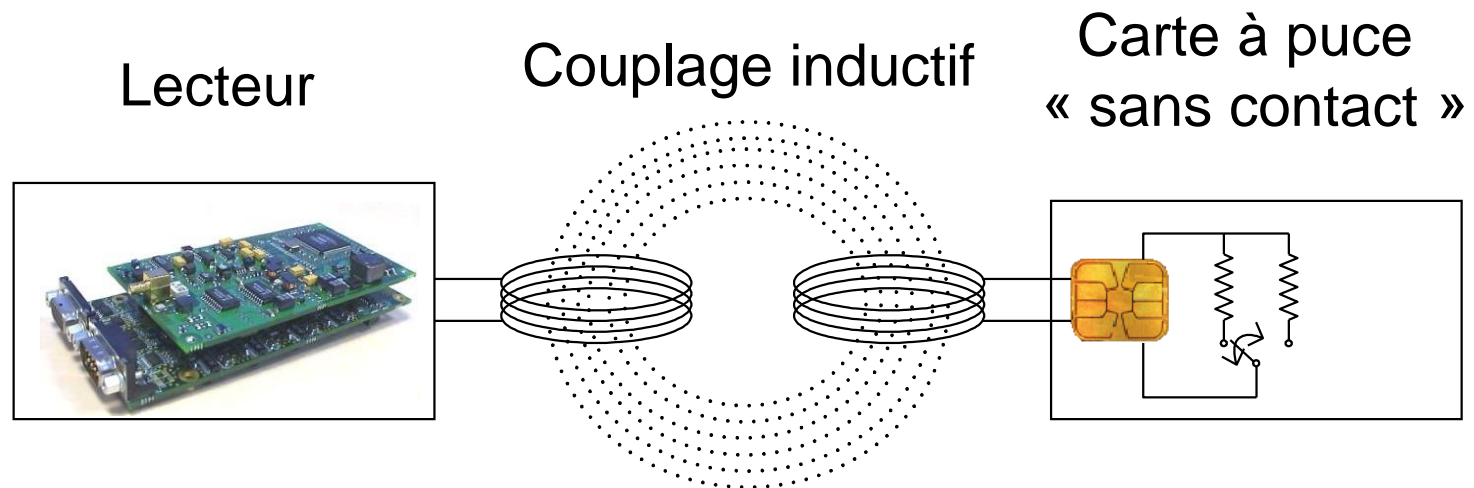
## Part 2 :

### Radio Frequency

### Power and signal interface

# Principe de fonctionnement

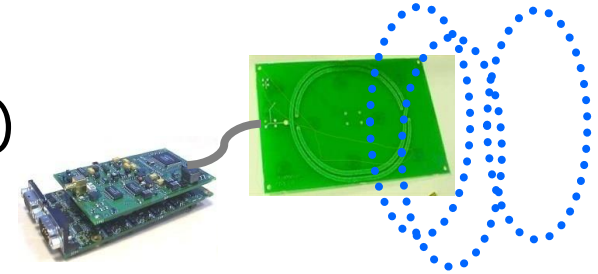
- Choix de la fréquence de travail : 13,56 MHz
- Couplage inductif en champ proche
- Modulation de charge



- => 2 approches:
  - ✓ «Circuits Couplés» : inductance mutuelle, circuit primaire & secondaire (transformateur)
  - ✓ «RF classique» : transmission de données, modulations, etc

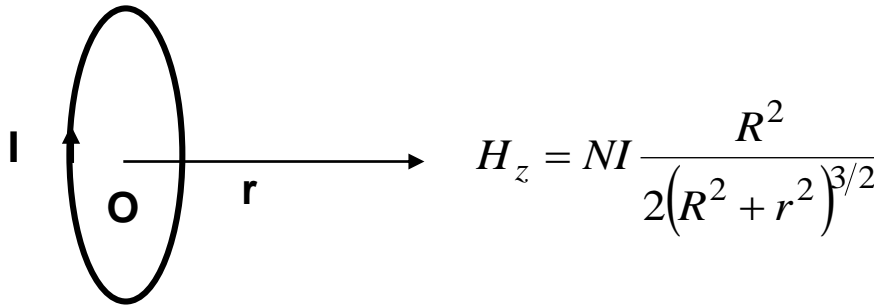
# Le champ électromagnétique

- Propriétés du champ magnétique proche:
  - l'énergie est emmagasinée, et non pas rayonnée
  - Fréquence de travail : 13,56 MHz
  - Long d'onde quasi-stationnaire ( $\lambda \approx 22$  m)
  - découplé du champ électrique
  - décroît en  $1/r^3$



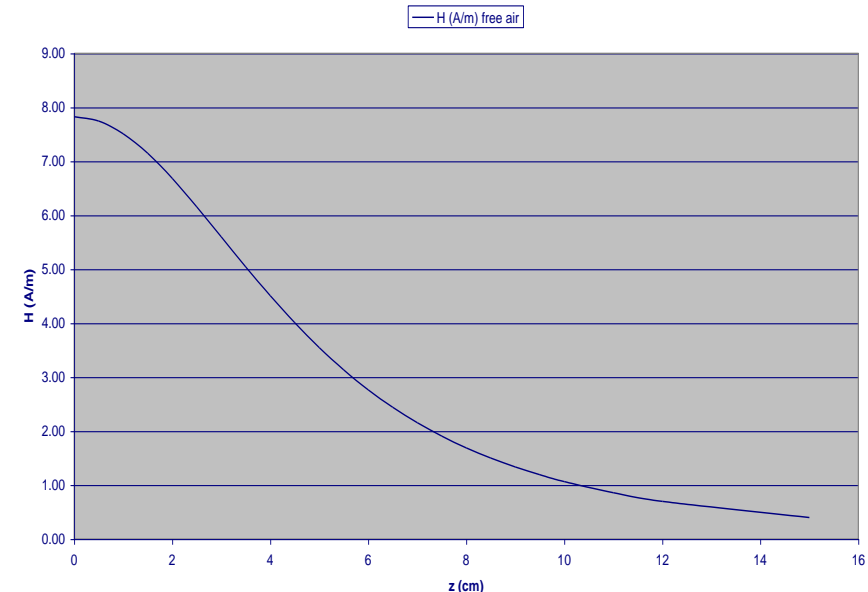
H (A/m) function of distance from Antenna Center axis

Exemple Antenne circulaire :



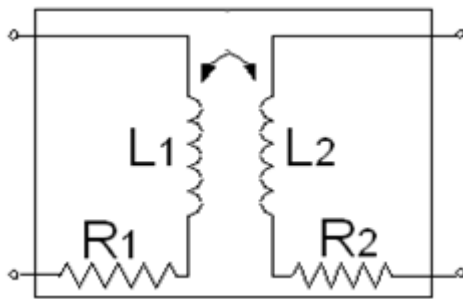
N : nombre de spires

R : rayon de la spire

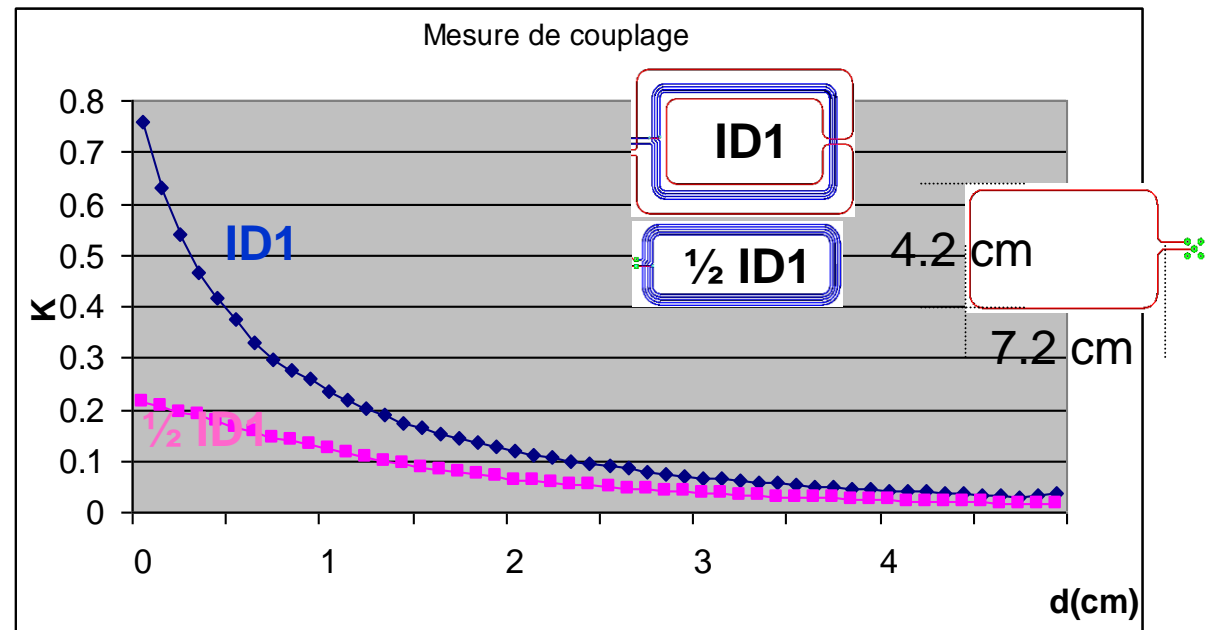


# Le couplage inductif

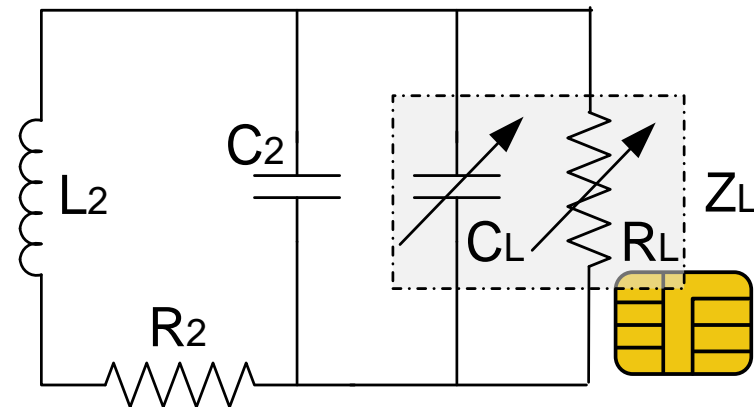
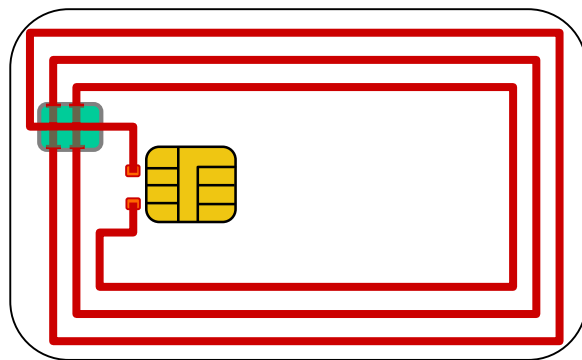
- Le couplage : transmission de l'énergie à distance
  - Inductance mutuelle (Neumann) et Coefficient de couplage



$$k = \frac{M}{\sqrt{L_1 L_2}}$$



## ➤ Modèle électrique équivalent



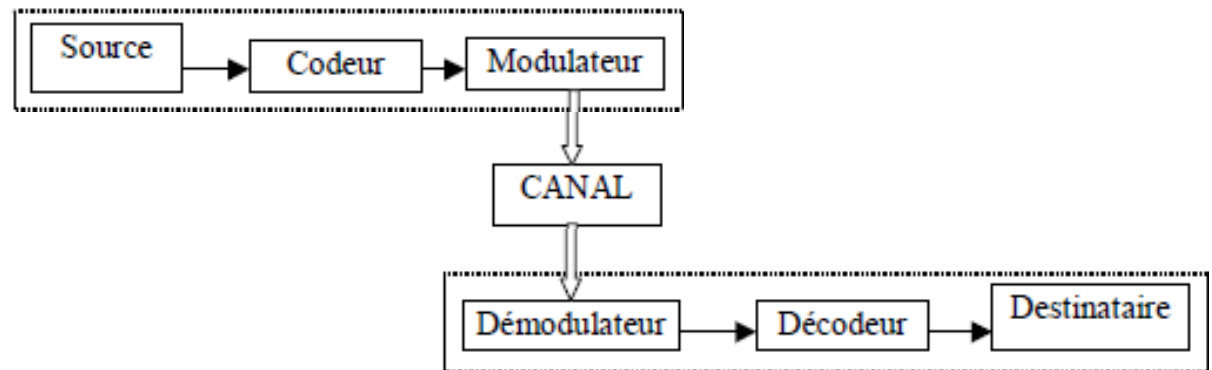
$$Z_{carte} = \frac{1}{\frac{1}{R_2 + j\omega L_2} + j\omega(C_2 + C_L) + \frac{1}{R_L}}$$

# Principe de la modulation démodulation

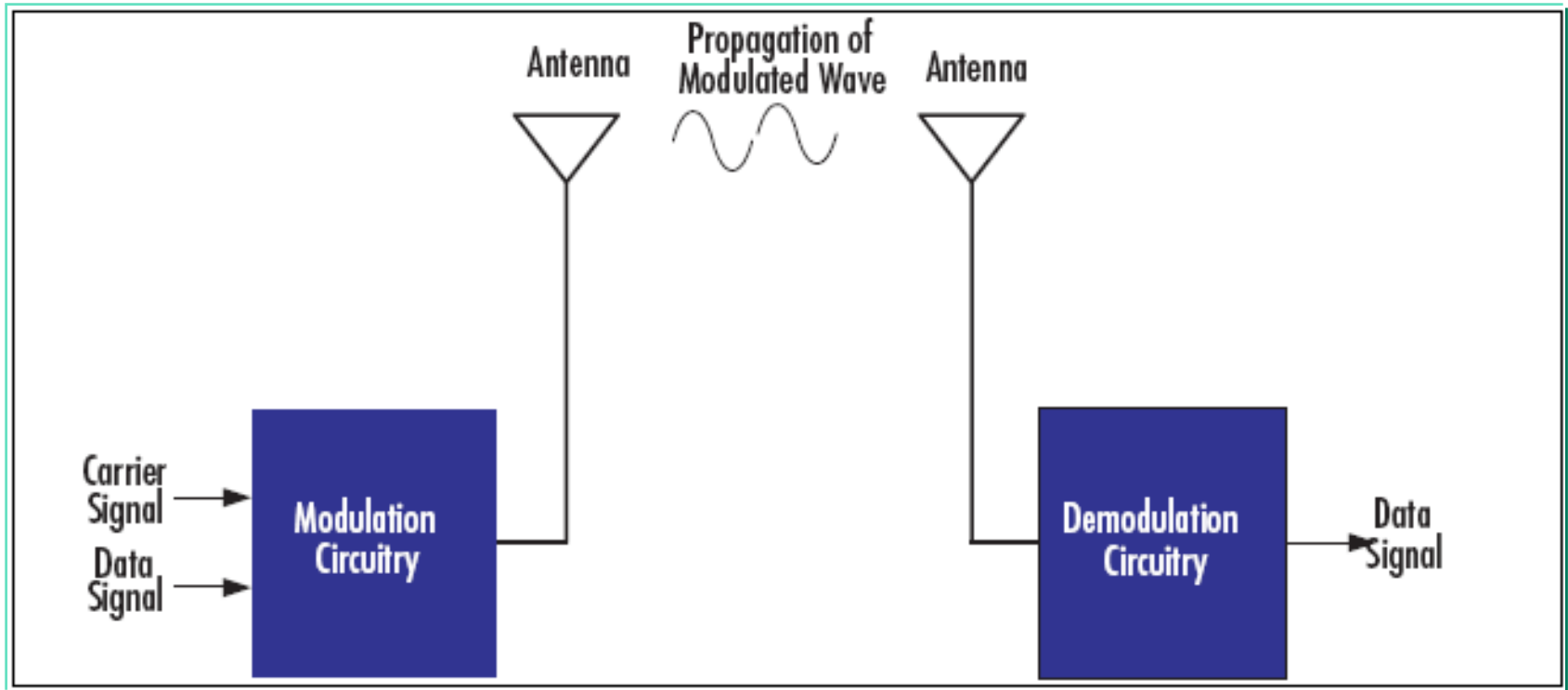


Un système de transmission numérique a les fonctions de base suivantes :

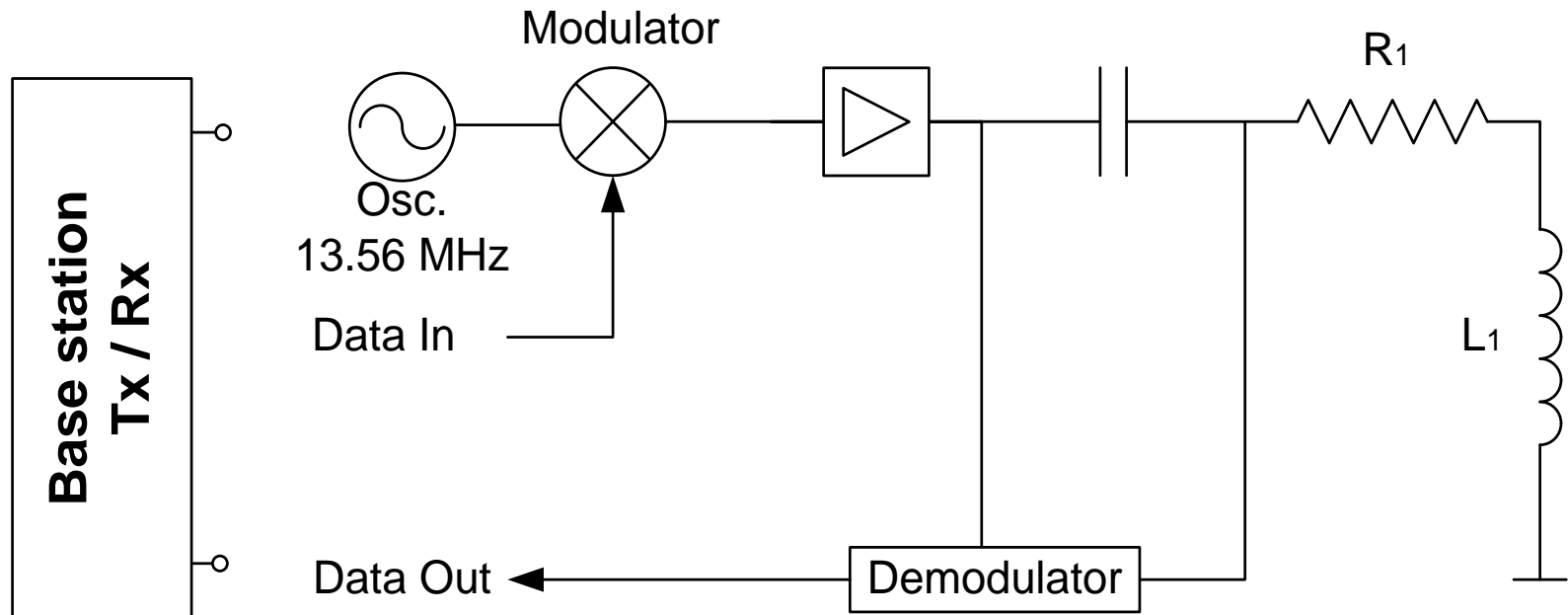
- la source émet un message numérique sous forme d'une suite d'éléments binaires,
- Le codeur peut éventuellement supprimer des éléments binaires non significatifs (compression) ou au contraire introduire de la redondance dans l'information (erreurs),
- La modulation a pour rôle d'adapter le spectre du signal au canal sur lequel il sera transmit,
- Du côté récepteur, les fonctions de démodulation et de décodage sont les inverses des fonctions de modulation et de codage situées côté émetteur



# Communication basé sur la modulation



- Etage RF de la station de base (lecteur PCD : Proximity Coupling Device)



- 2 fonctions :
  - ✓ Fournir de l'énergie (adaptation 50 Ohm)
  - ✓ Transmettre et recevoir des données (bande passante)



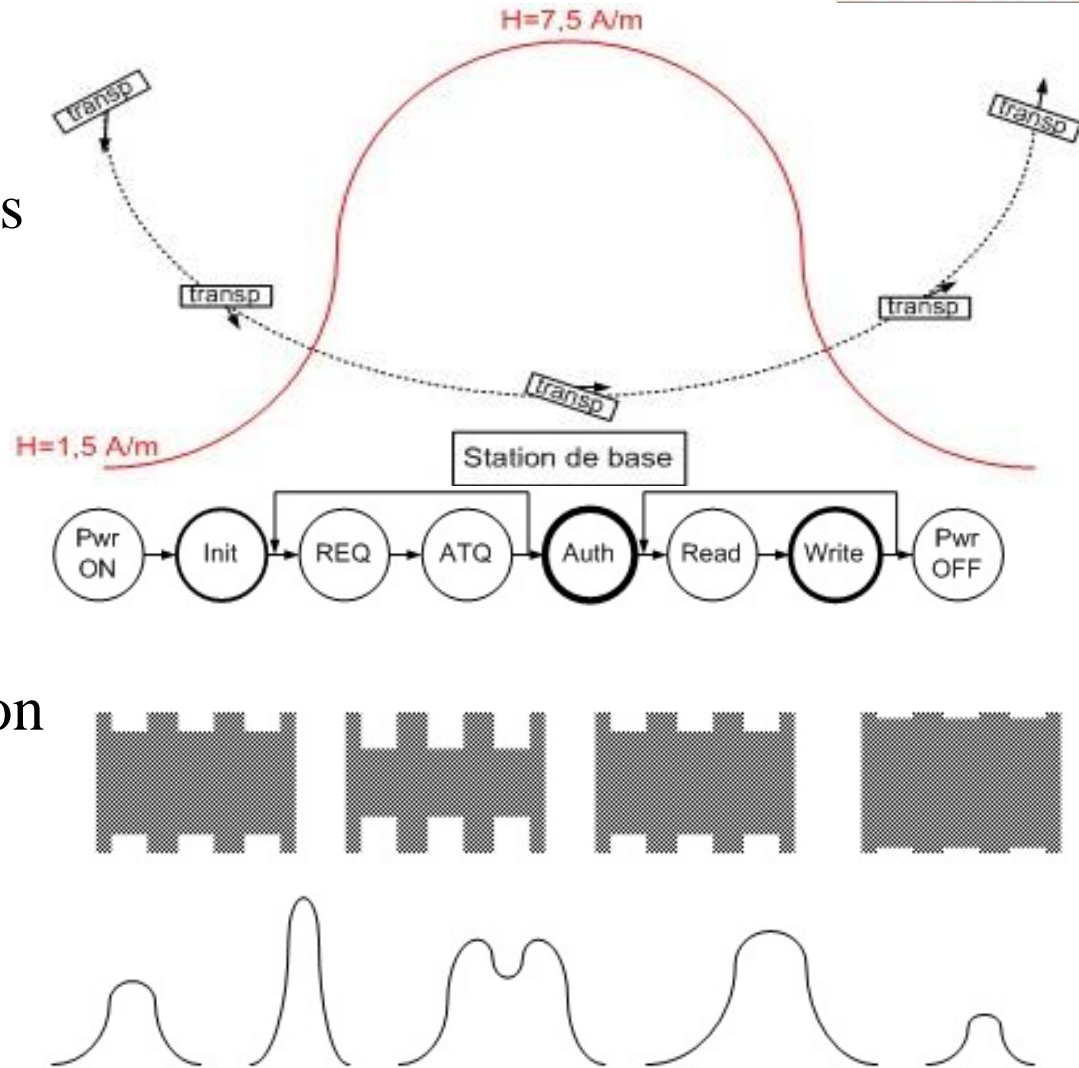
# Synthèses des phénomènes liés à la communication « sans contact »

Variation du champs :  
Phase de Régulation des  
Grandeurs électriques induites  
Échangées OS & CMOS

Phase d'initialisation,  
Authentification et écriture  
en EEPROM

Signaux échangés, modulation  
de charge et changement  
d'impédance

Couplage, bande passante  
Et fréquence de résonance



## ➤ Glossaire :

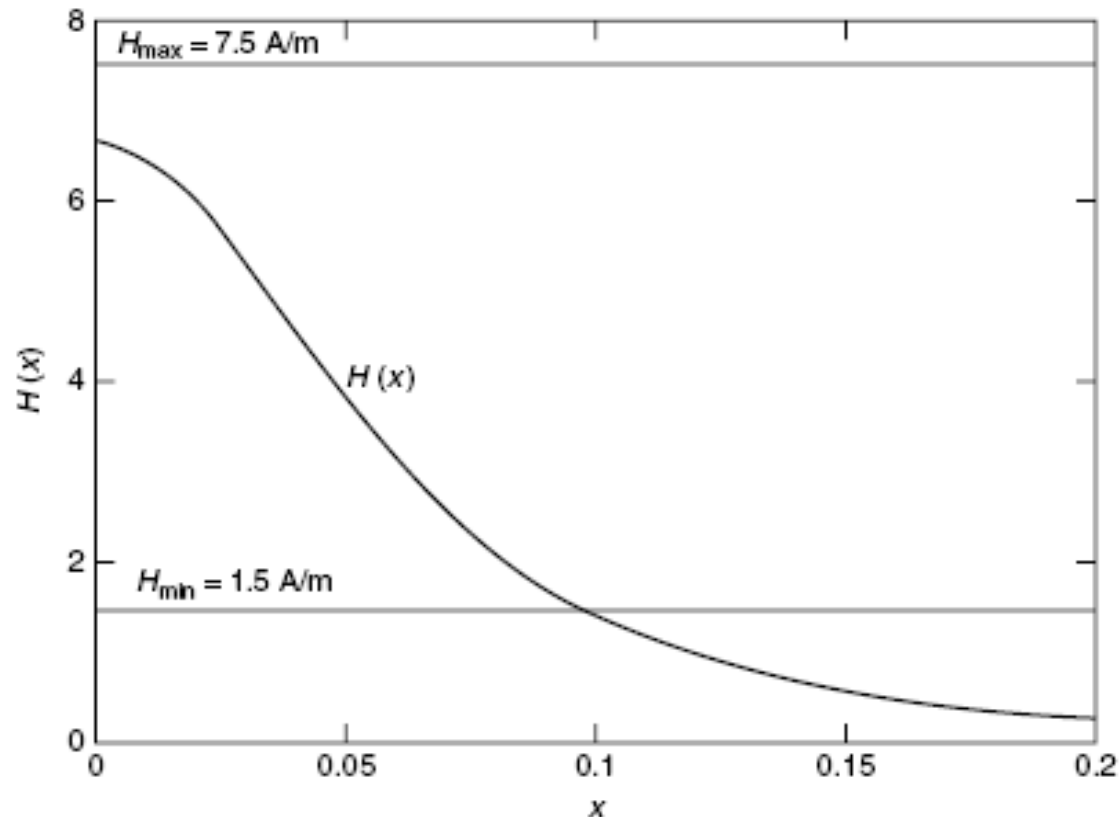
- ✓ PICC : Proximity Integrated Circuit Card (Carte à puce sans contact)
- ✓ PCD : Proximity Coupling Device (Lecteur de Carte à puce sans contact)

## ➤ Dialogue en « Half Duplex » :

- ✓ Activation de la carte par le champ non modulé émis par le PCD;
- ✓ PICC attend une commande du PCD
- ✓ Transmission d'une commande du PCD
- ✓ Transmission d'une réponse du PICC

## ➤ $H_{min} = 1,5 \text{ A/m} < H < H_{max} = 7,5 \text{ A/m}$ ; $f_c = 13,56 \text{ MHz}$

# Courbe Champ magnétique-distance



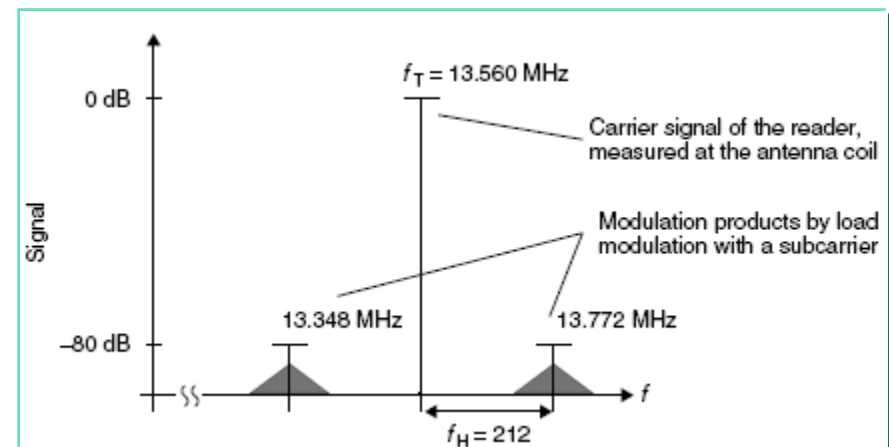
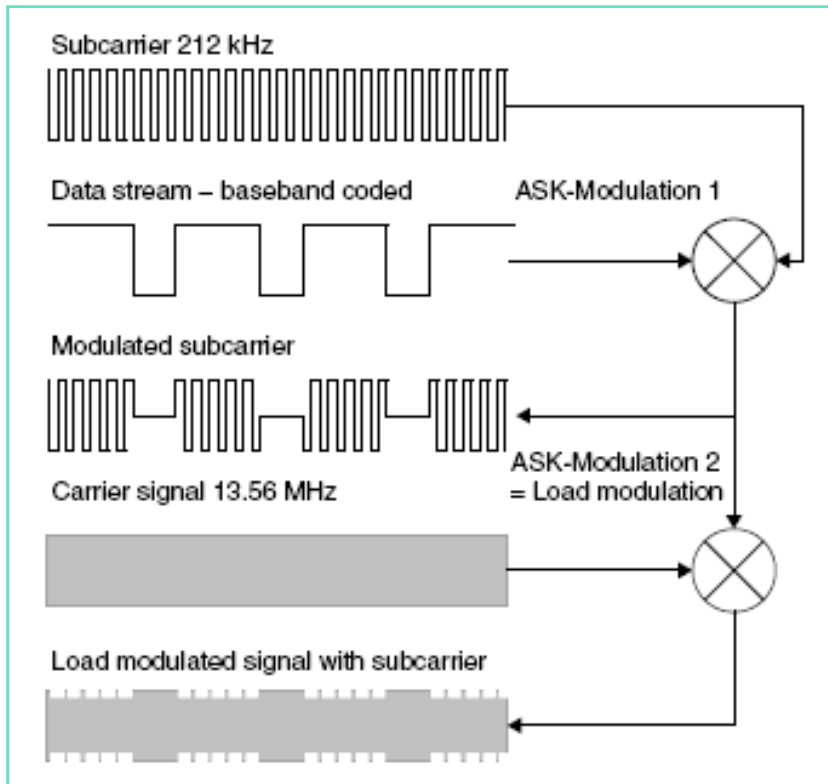
- L'intersection nous donne la distance maximale permettant le couplage lecteur-carte
- 2 technologies Type A & Type B

# ISO 14443

## Mode de communication Type A

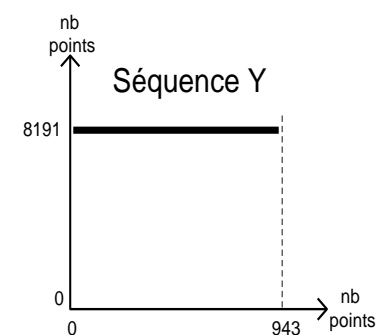
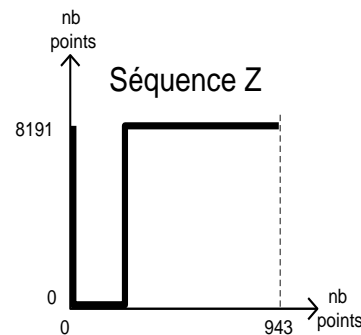
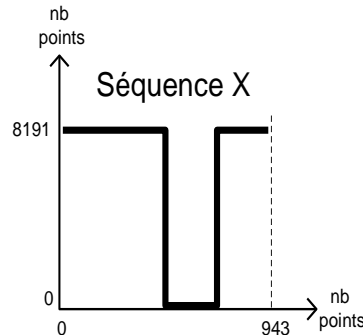
# PCD → PICC - Communication Type A

- Modulation ASK 100%
- Débits possibles = 106, 212, 424, 847 kbits/s
- Débit Binaire :  $f_c/128 = 106$  Kbits/s



## ➤ Codage : Miller Modifié

- ✓ Séquence X
- ✓ Séquence Y
- ✓ Séquence Z



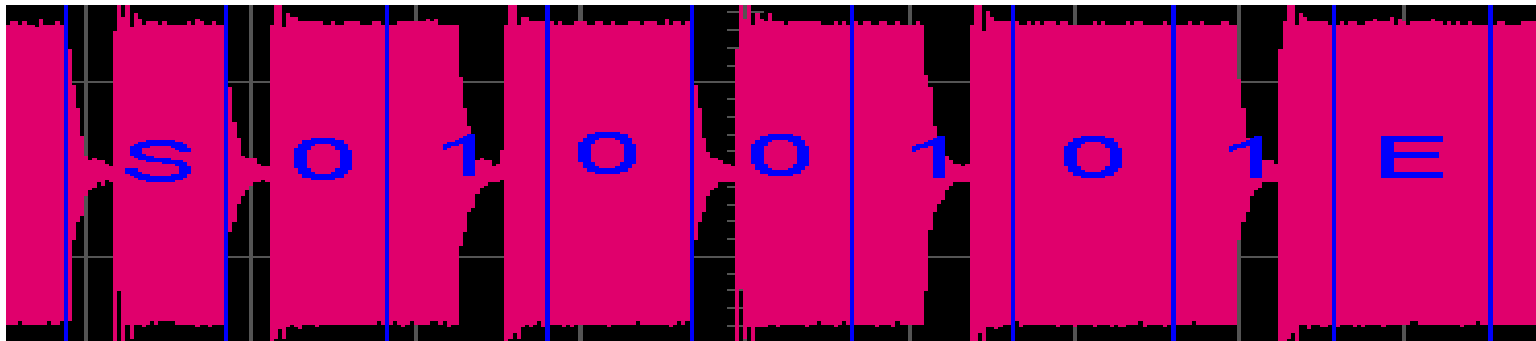
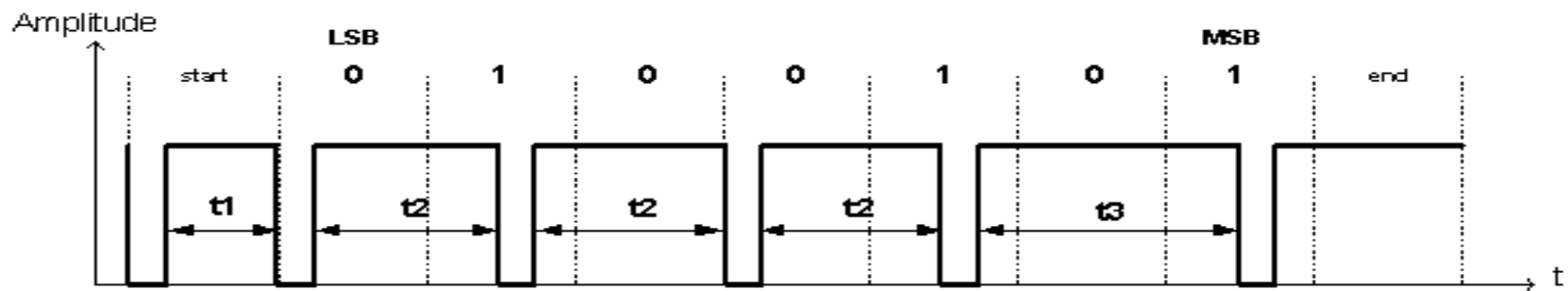
## ➤ Etat « 1 » → Séquence X

## ➤ Etat « 0 » → Séquence Y avec 2 exceptions :

- ✓ Plusieurs zéros de suite, à partir du 2ème zéro → séquence Z
- ✓ 1er bit après le début de la communication → séquence Z
- ✓ Début de la communication → séquence Z
- ✓ Fin de la communication « 0 » suivi de la séquence Y
- ✓ Pas d'information : au moins 2 séquences Y

# PCD → PICC - Communication Type A

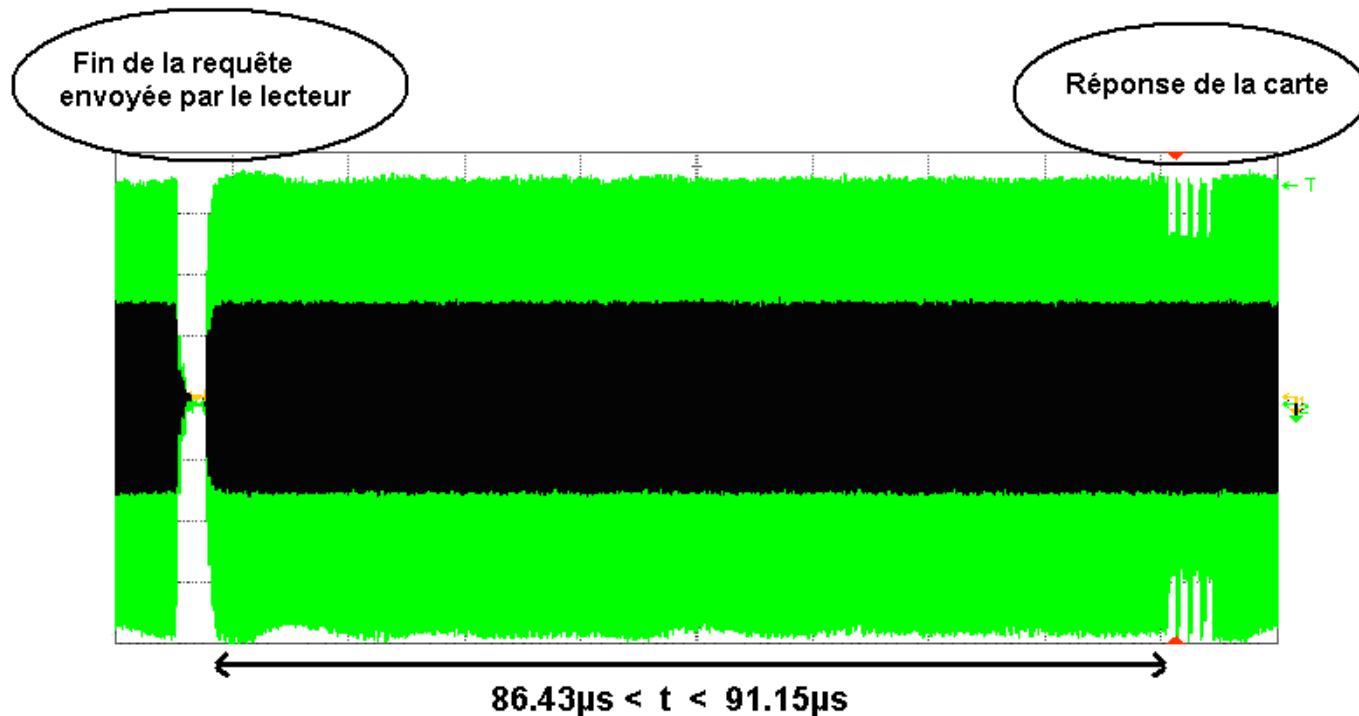
- Exemple de Requête envoyée par le PCD en permanence : Cmd WUPA (Wake UP type A) : « 101 0010 » ou 0x52



- ✓ Débit binaire :  $f_c/128$  soit une fréquence de 106Kbit/s  
⇒  $9.44\mu s$  pour 1 bit.

# PCD → PICC - Communication Type A

- Entre la requête du PCD et la réponse du PICC il y a un temps de pause qui est effectué, ce temps varie en fonction de la commande envoyée par le PCD

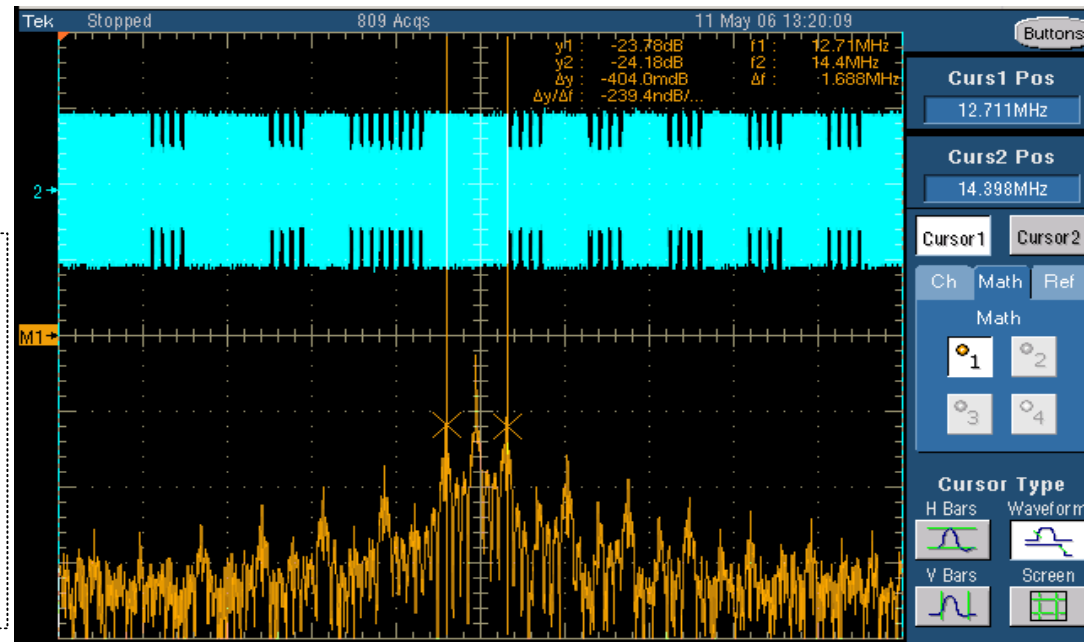
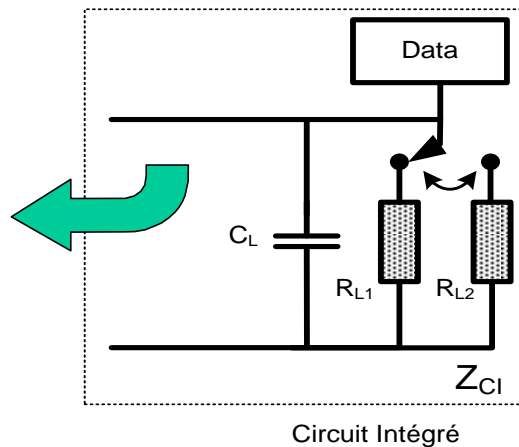
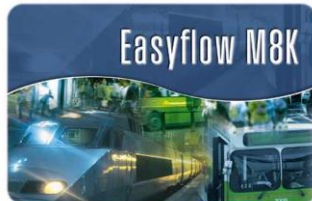




# PICC → PCD - Communication Type A

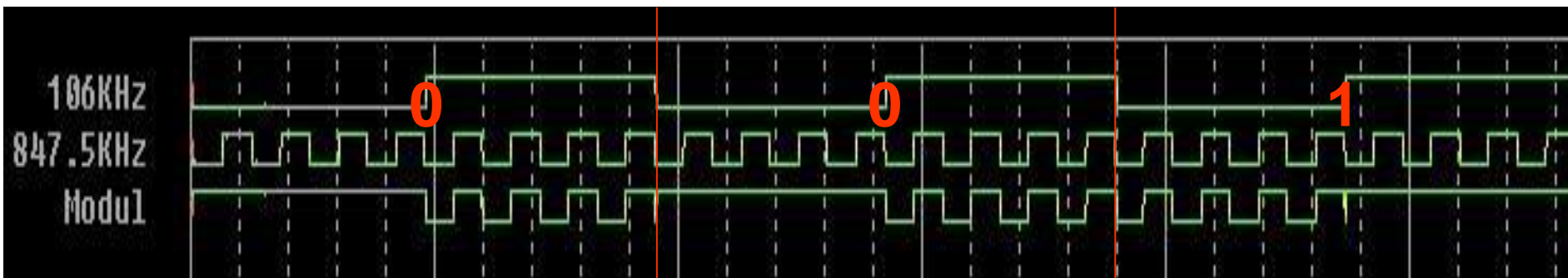
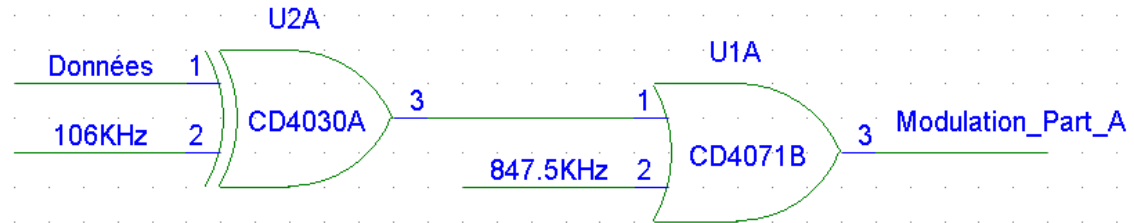
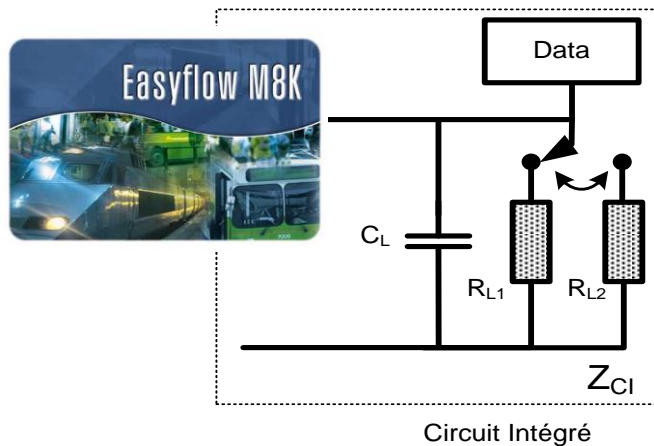
## ➤ Modulation de charge

- ✓ Sous porteuse  $f_s = f_c / 16 = 847 \text{ KHz}$
- ✓ Amplitude  $\leq 30/H_{1,2} \text{ (mVpeak)}$  où H est la valeur rms du champ magnétique (A/m)

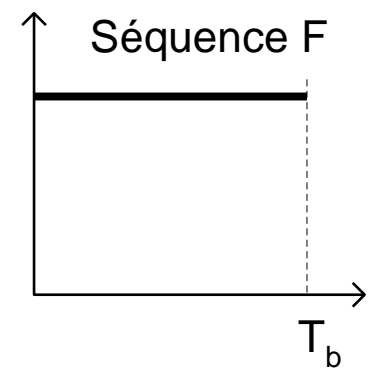
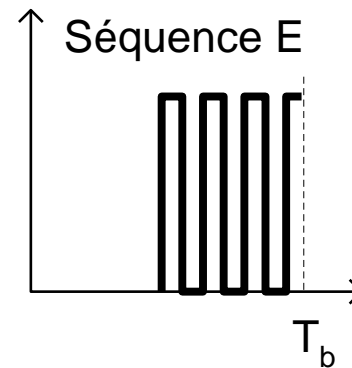
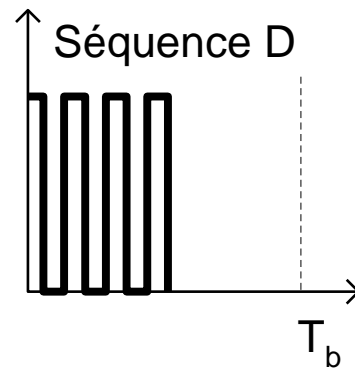


# PICC → PCD - Communication Type A

## ➤ Modulation de charge OOK (On/Off Keying)

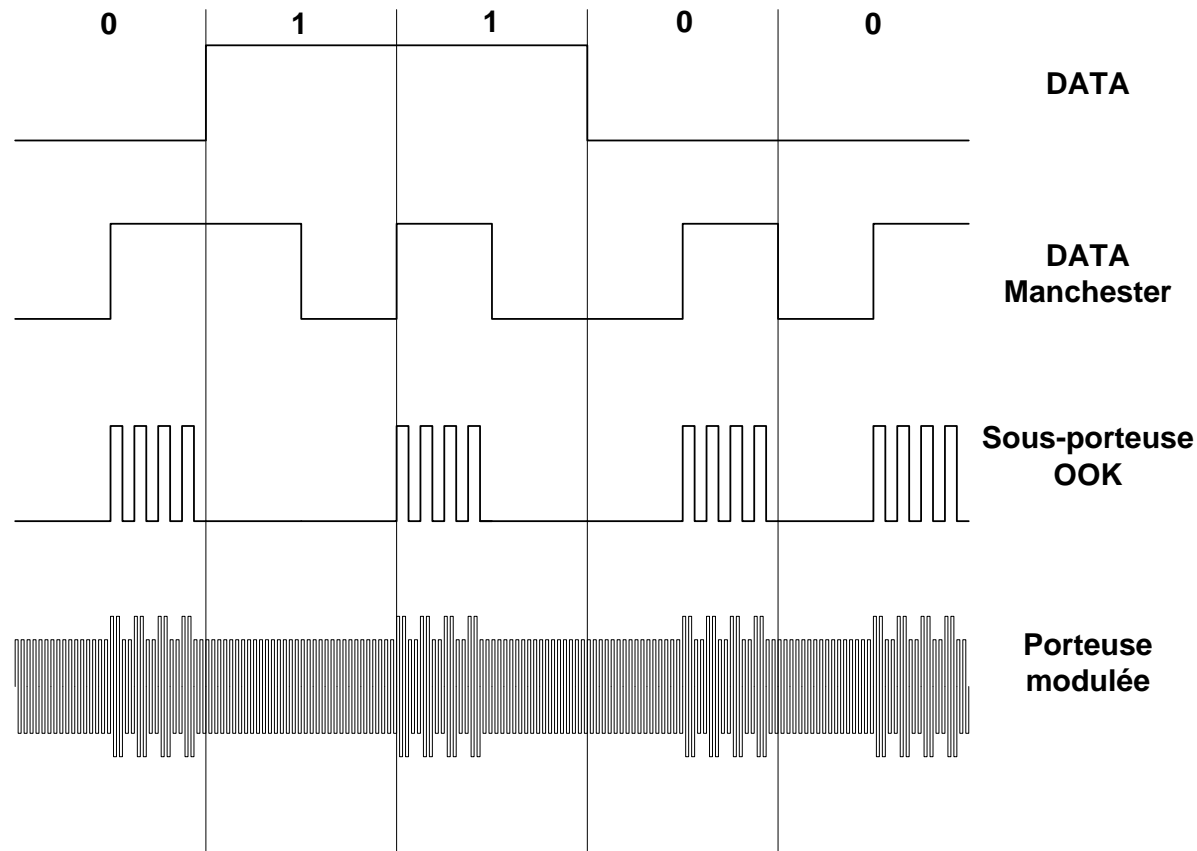


- Codage Manchester :
  - ✓ Sous porteuse modulée OOK

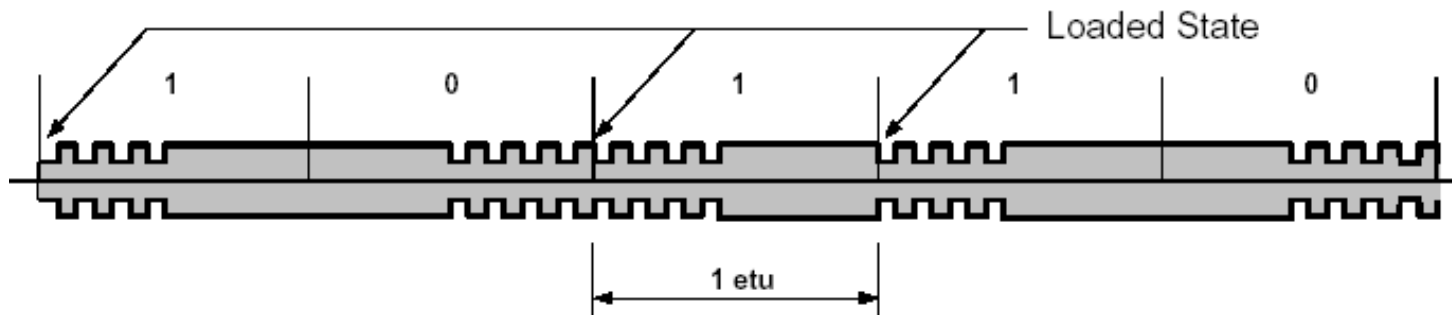


- Avec
  - ✓ Etat « 1 » → Séquence D
  - ✓ Etat « 0 » → Séquence E
  - ✓ Début de la communication → Séquence D
  - ✓ Fin de la communication → Séquence F
  - ✓ Pas d'information → Absence de sous-porteuse

## ➤ Codage Manchester



- Exemple : Réponse d'un PICC après un REQ A :
  - ✓ ATQA « 1 00100000 0 00000000 0 1 »

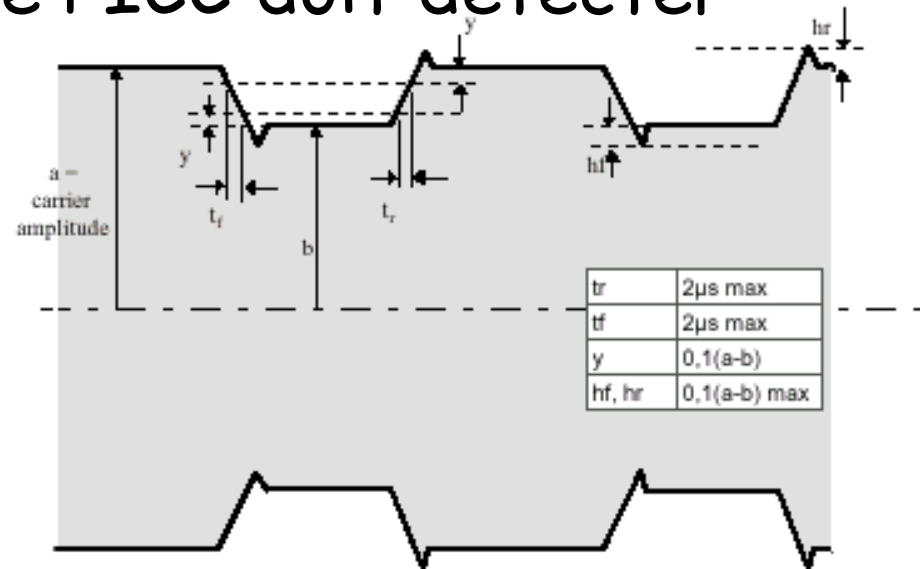
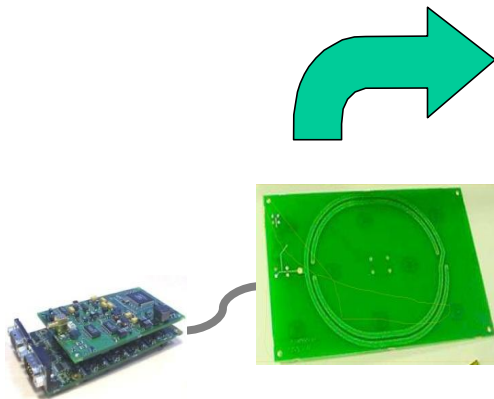


---

# ISO 14443 Mode de communication Type B

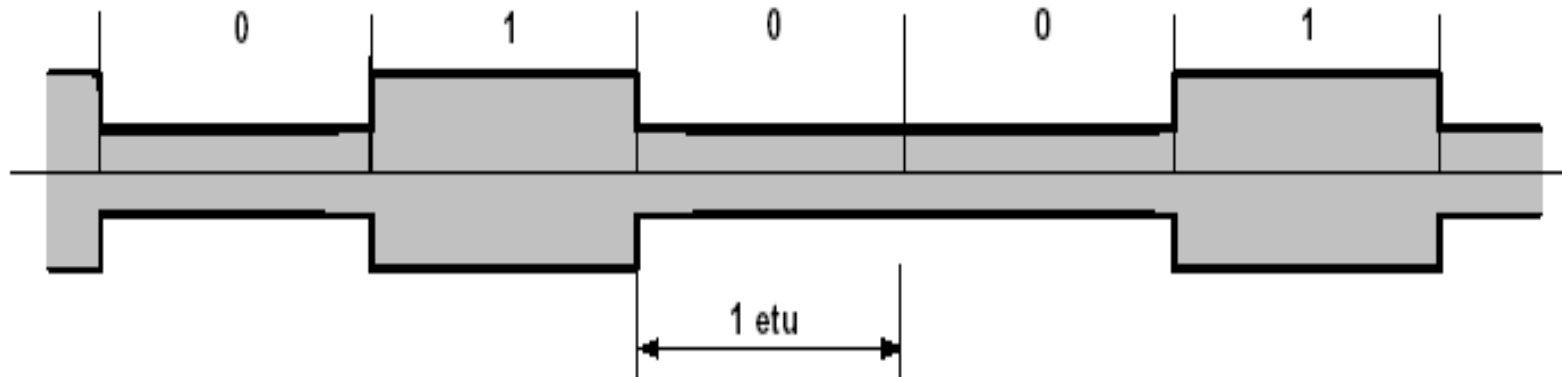
# PCD → PICC - Communication Type B

- Modulation ASK 10%,
  - ✓ Indice de modulation toléré entre 8% et 14%
- Débit Binaire :  $f_c/128 = 106 \text{ kbits/s}$ 
  - ✓ Débits possibles = 106, 212, 424, 847 kbits/s
- Forme d'onde que le PICC doit détecter



## ➤ Codage NRZ (No return to Zero)

- ✓ 1 Logique : Amplitude haute du champ de la porteuse
- ✓ 0 Logique : Amplitude Basse du champ de la porteuse

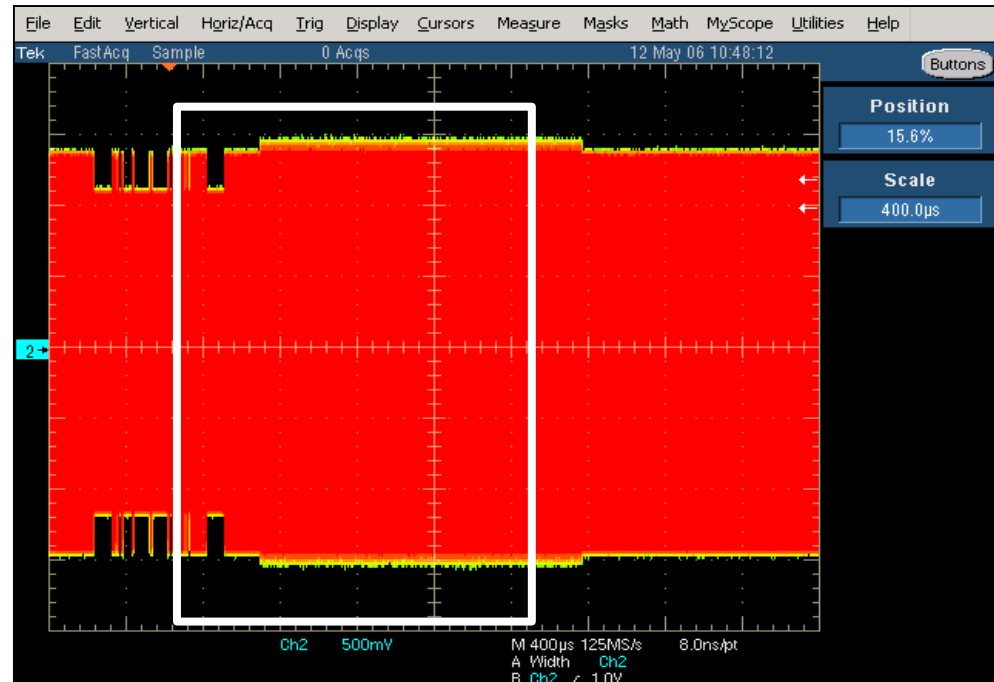
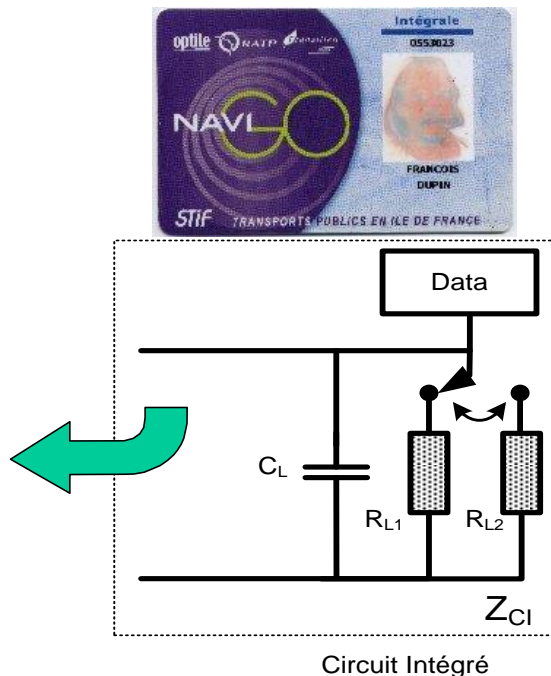




# PICC → PCD - Communication Type B

## ➤ Modulation de charge

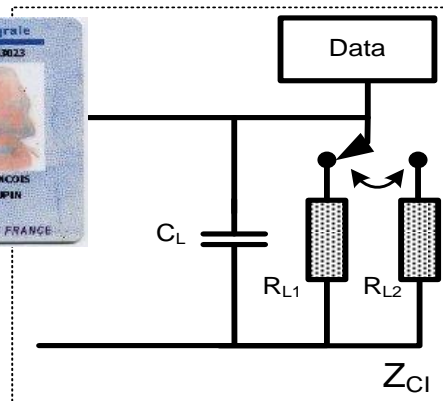
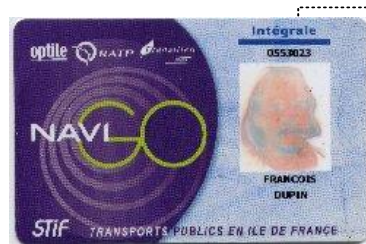
- ✓ Sous porteuse  $f_s = f_c / 16 = 847 \text{ KHz}$
- ✓ Amplitude  $\leq 30/H_{1,2} \text{ (mVpeak)}$  où  $H$  est la valeur rms du champ magnétique (A/m)



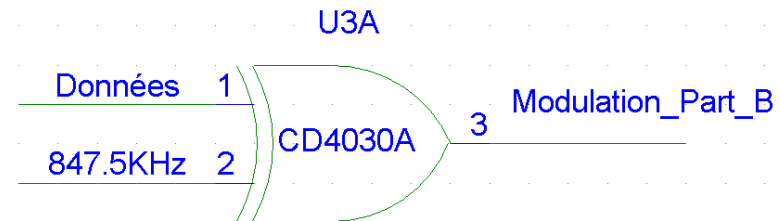
# PICC → PCD - Communication Type B

## ➤ Modulation de charge

- ✓ Codage NRZ-L avec modulation sous-porteuse en BPSK
  - Etat « 1 » → Phase =  $0^\circ$
  - Etat « 0 » → Phase =  $180^\circ$

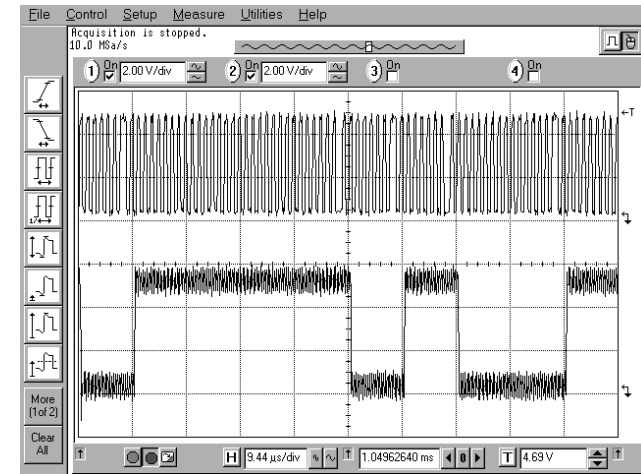
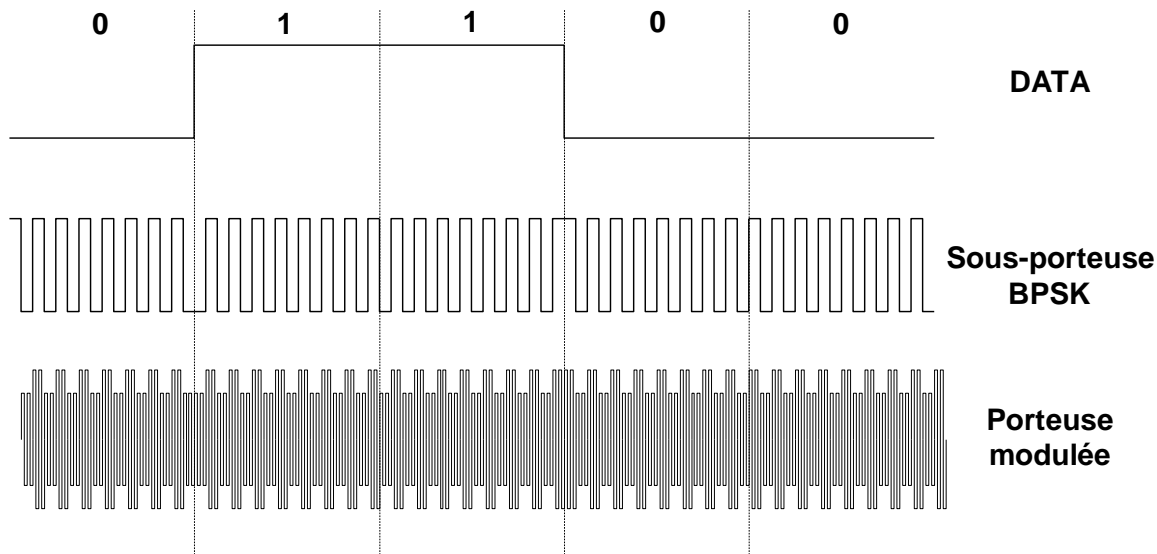


Circuit Intégré



# PICC → PCD - Communication Type B

## ➤ Exemple



# Recap : Data transfert PCD-PICC

PCD → PICC	Type A	Type B
Modulation	ASK 100%	ASK 10% (modulation index 8%–12%)
Bit coding	Modified Miller code	NRZ code
Synchronisation	At bit level (start-of-frame, end-of-frame marks)	1 start and 1 stop bit per byte (specification in Part 3)
Baud rate	106 kBd	106 kBd

PICC → PCD	Type A	Type B
Modulation	Load modulation with subcarrier 847 kHz, ASK modulated	Load modulation with subcarrier 847 kHz, BPSK modulated
Bit coding	Manchester code	NRZ code
Synchronisation	1 bit frame synchronisation (start-of-frame, end-of-frame marks)	1 start and 1 stop bit per byte (specification in Part 3)
Baud rate	106 kBd	106 kBd

- Qu'est ce que la RFID ?
- Un peu d'histoire...
- Carte à puces sans contact
- Classification & état de l'art de la RFID
- Panorama de la standardisation
- Introduction aux cartes à puce sans contact
  - Caractéristiques Physiques
  - Modes de communications
  - Initialisation et Anticollisions
  - Protocoles de transmission

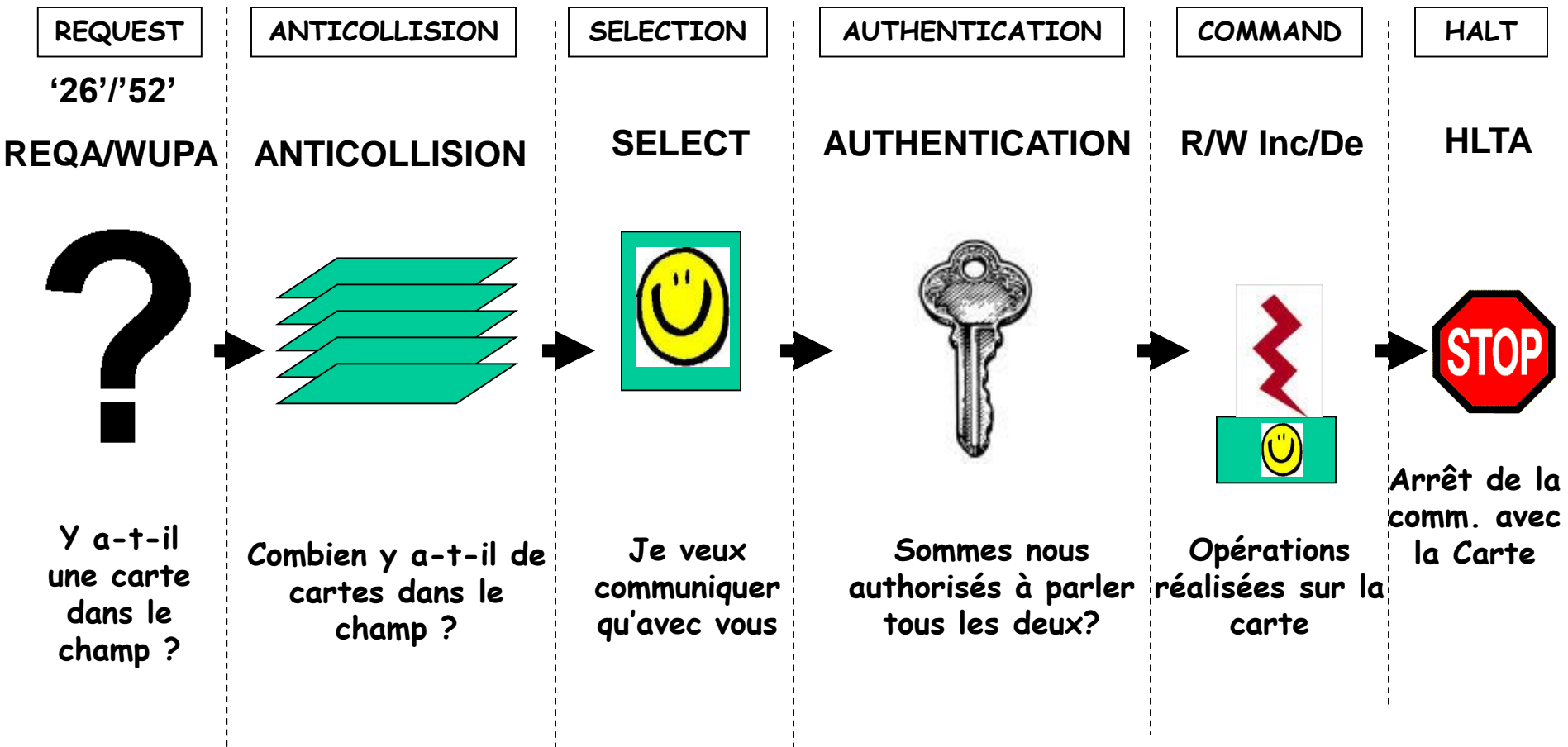
# ISO 14443 Part 3 : Initialisation et Anticollision Type A

- L'acteur principal est le lecteur
  - ✓ Mode maître-esclave



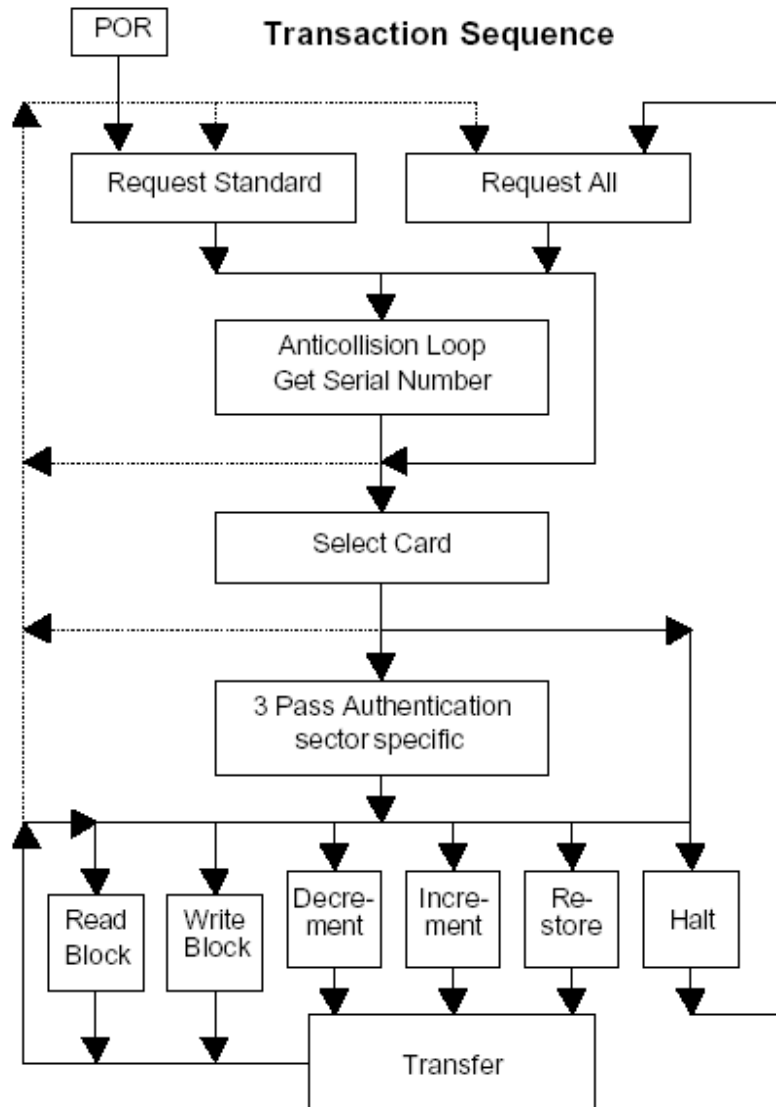
- Carte : passive → elle dépend du lecteur
- Le lecteur initie la communication :
  - ✓ Il envoie une commande à la carte
  - ✓ Il attend une réponse de la carte
  - ✓ FDT : temps entre deux trames, synchronisation

# Exemple de transaction - Type A





# Exemple de transaction - Type A



## Typical Transaction Time

### Identification and Selection Procedure

3 ms without collision  
+ 1 ms for each collision

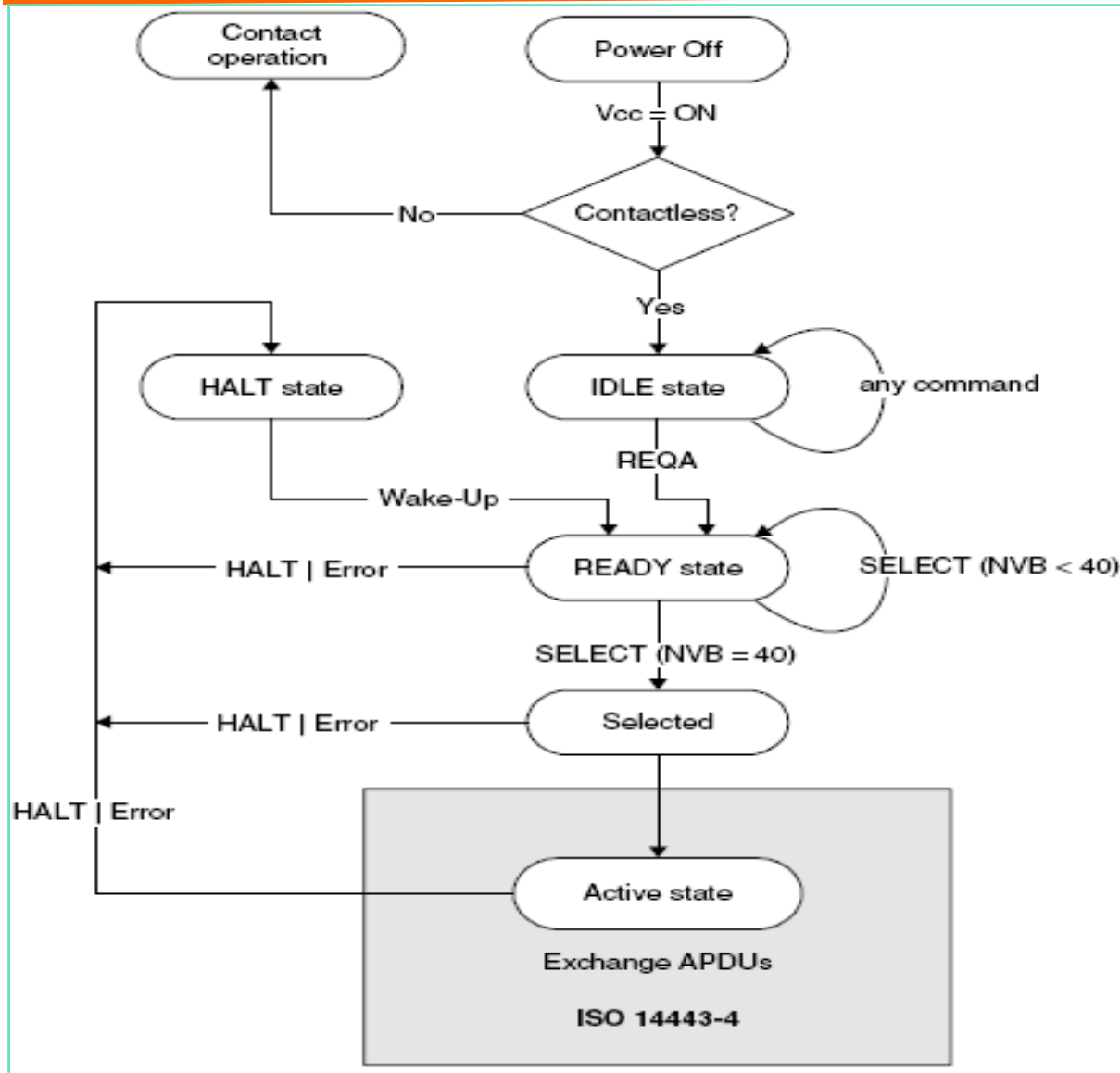
### Authentication Procedure

2 ms

### Memory Operations

2.5 ms read block  
6.0 ms write block

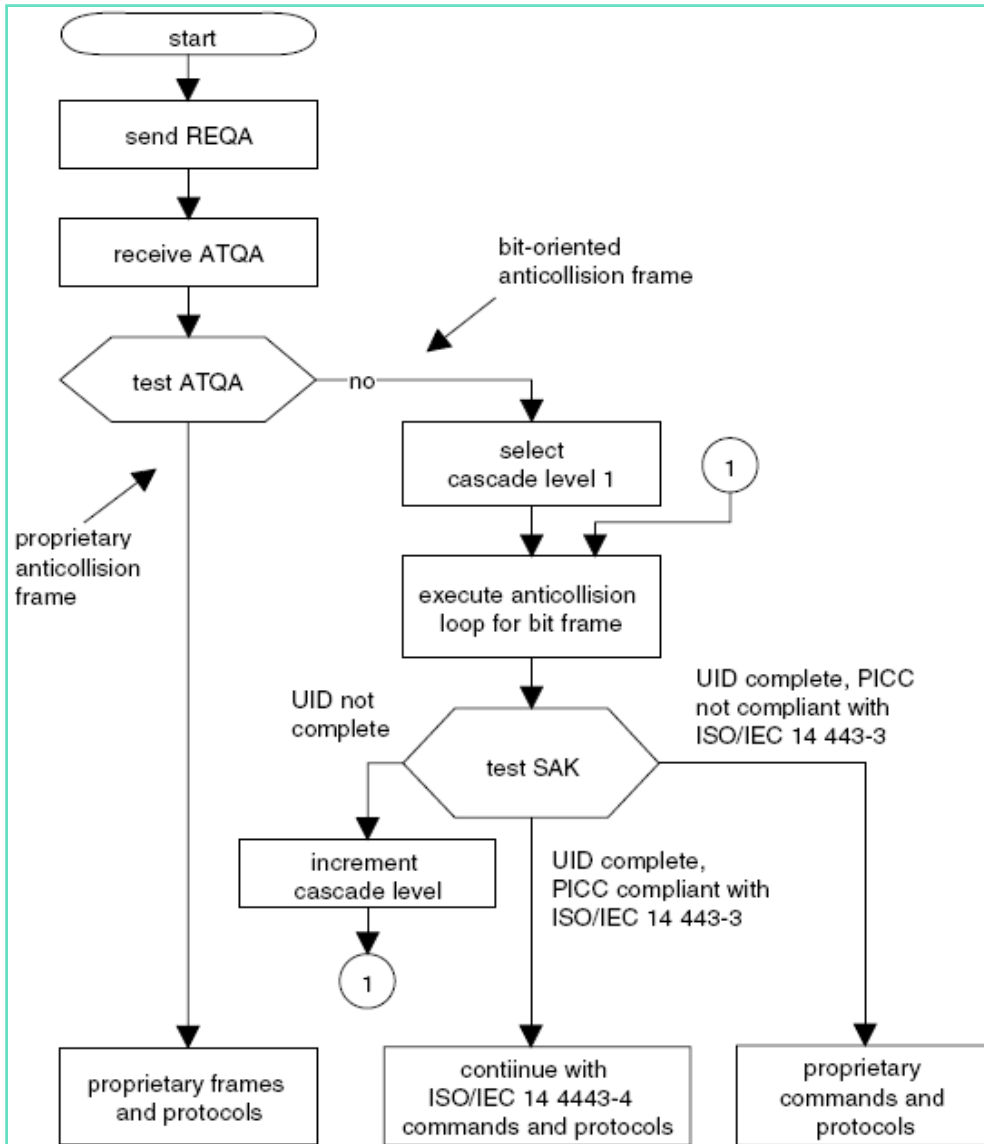
# Diagramme d'état de la carte - Type A



Etats de la carte :

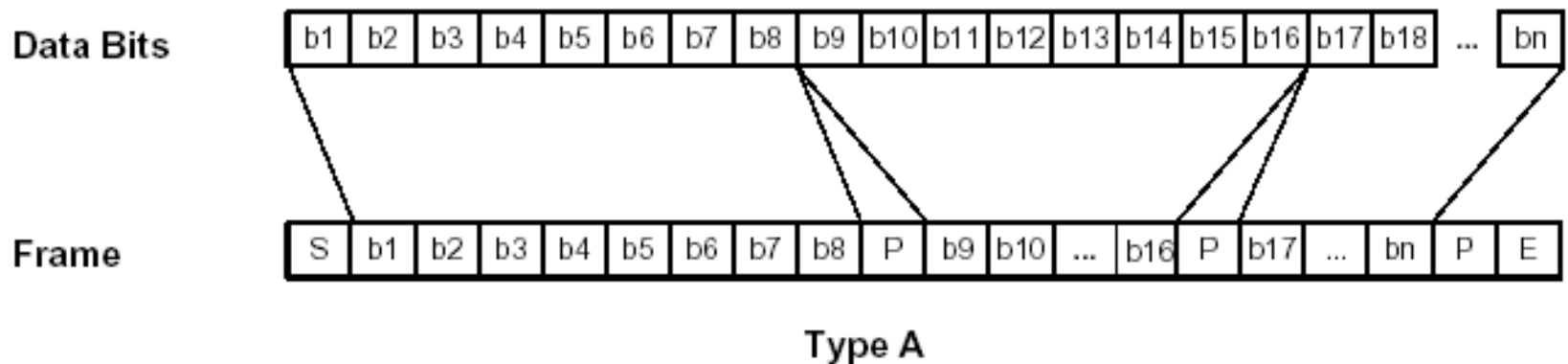
- POWER OFF
- IDLE
- READY
- ACTIVE
- HALT

# Diagramme d'état lecteur/carte - Type A



- Commandes utilisées par le Lecteur pour gérer la Communication multicartes :
- REQA : les cartes concernées répondent avec ATQA
  - WAKE-UP
  - SELECT
  - ANTICOLLISION
  - HALT

- 2 types de trames
  - ✓ Trames courtes utilisées dans la phase d'initiation de la communication (utilisé uniquement par le PCD)
  - ✓ Trames standards utilisées pour le reste de la communication
- LSB est transmis en premier



## ➤ Trames courtes pour initier la communication

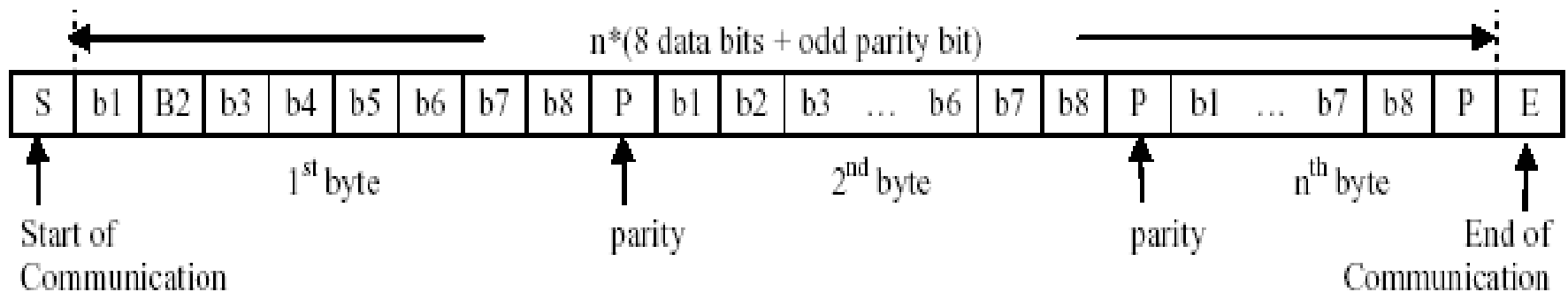
	LSB							MSB	
S	b1	b2	b3	b4	b5	b6	b7	E	

## ➤ Commandes utilisées :

- ✓ REQA : la station de base envoie systématiquement, en boucle cette commande pour vérifier s'il y a des cartes dans son champ
- ✓ WUPA : reveiller une carte qui a été mise en veille par une commande HALT

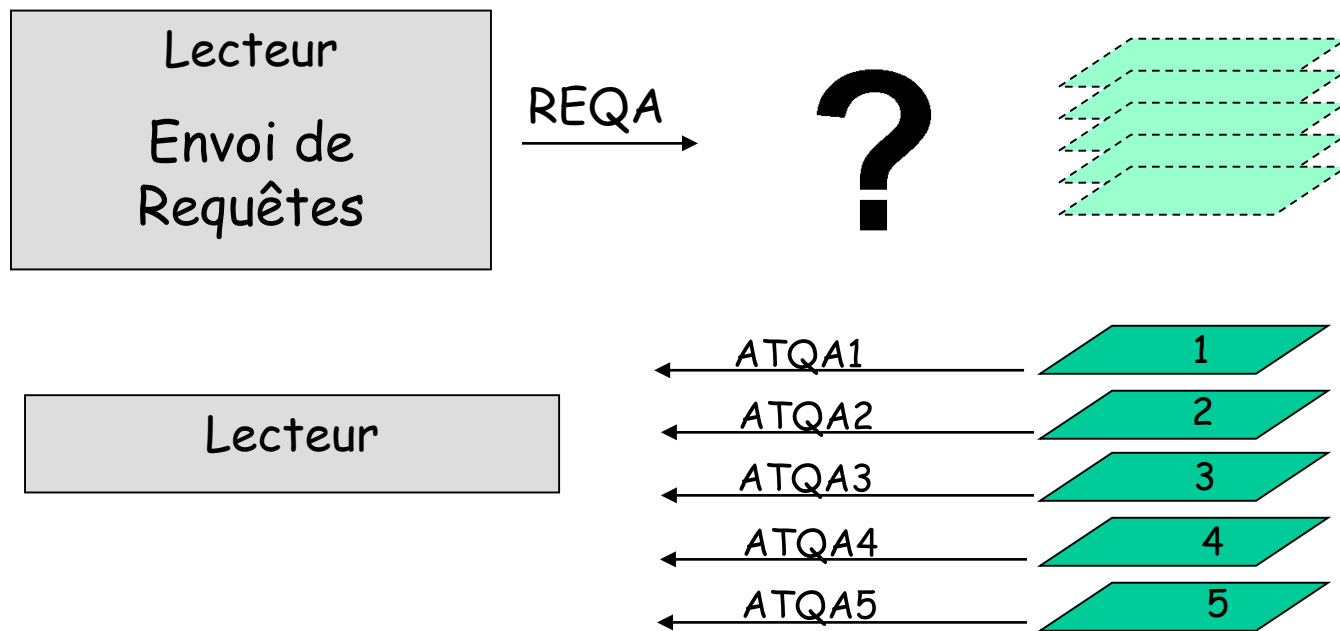
➤ La trame standard est utilisée pendant tout l'échange d'information entre station de base et transpondeur :

- ✓ Bit de Start (S)
- ✓ Bits (LSB first)
- ✓ Bits de parité prennent la valeur « 1 » si le nombre de bits à « 1 » dans l'octet qui les précède est pair
- ✓ Bit de Stop (E)



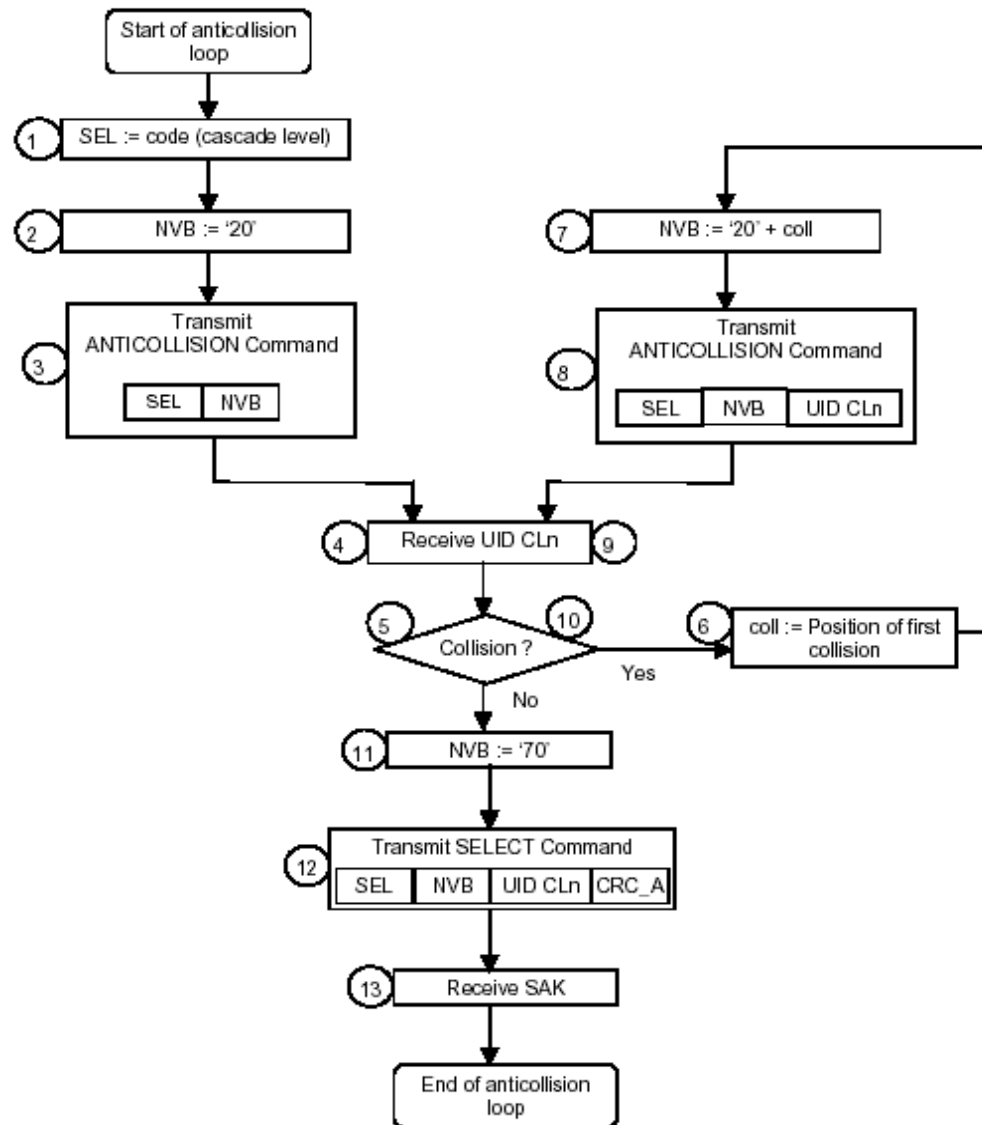
- La carte est dans le champ,
  - ✓ Power-on Reset
  - ✓ Etat Idle
- Le lecteur envoie une requête, indiquant qu'il cherche à communiquer avec une carte.
- 2 types de Requête :
  - ✓ REQA '26' : initialisation de la communication
    - Y a t-il une carte dans le champ?
  - ✓ WUPA '52' : même rôle que REQA, elle sert à réveiller les cartes qui ont été mises en veille auparavant avec une commande HALTA
- Attente de la réponse de la carte.
  - ✓ Si pas de réponse envoie d'une deuxième REQA
  - ✓ Temps mini entre deux REQA =  $7000 / f_c$

- Toutes les cartes dans le champ doivent transmettre leurs data de manière synchrone





# Boucle anticollision - Type A



## ➤ Réponse synchrone avec le lecteur d'une carte type A

MSB								LSB							
b16	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1
RFU								UID size bit frame		RFU	Bit frame anticollision				

## ➤ ATQA (trame standard) de 2 octets contient :

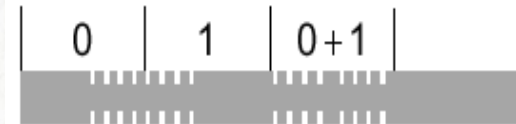
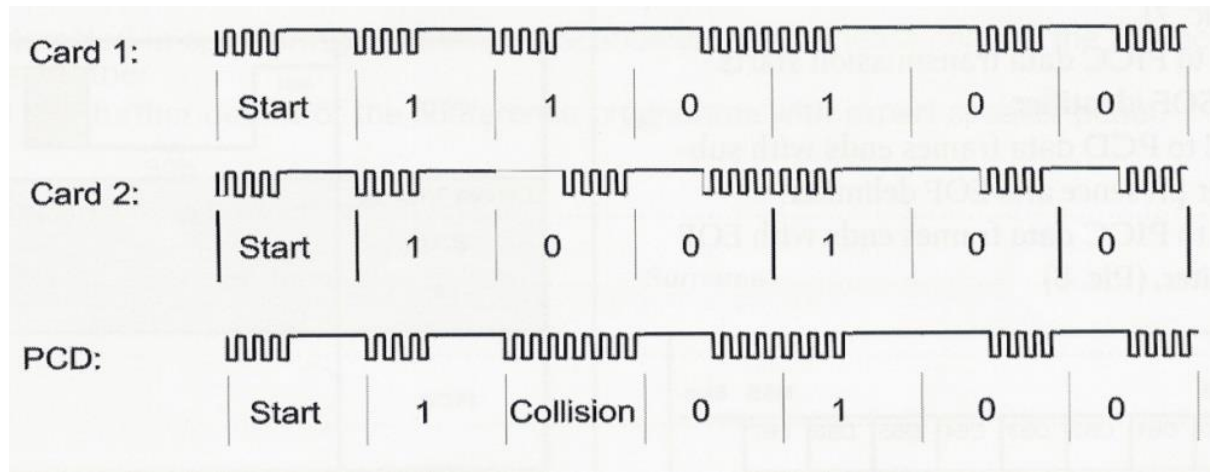
- ✓ la taille de l'UID (Unique IDentification Number) de la carte:
  - Single UID → 4 octets (b7 = 0 et b8 = 0)
  - Double UID → 7 octets (b7 = 1 et b8 = 0)
  - Triple UID → 10 octets (b7 = 0 et b8 = 1)
- ✓ Le bit de trame anticollision : un seul bit doit être à « 1 »

b5	b4	b3	b2	b1	Signification
1	0	0	0	0	Bit frame anticollision
0	1	0	0	0	Bit frame anticollision
0	0	1	0	0	Bit frame anticollision
0	0	0	1	0	Bit frame anticollision
0	0	0	0	1	Bit frame anticollision

## ➤ La procédure Anticollision est initiée pour lire l'UID de la carte

# Principe de l'anticollision - Type A (1/2)

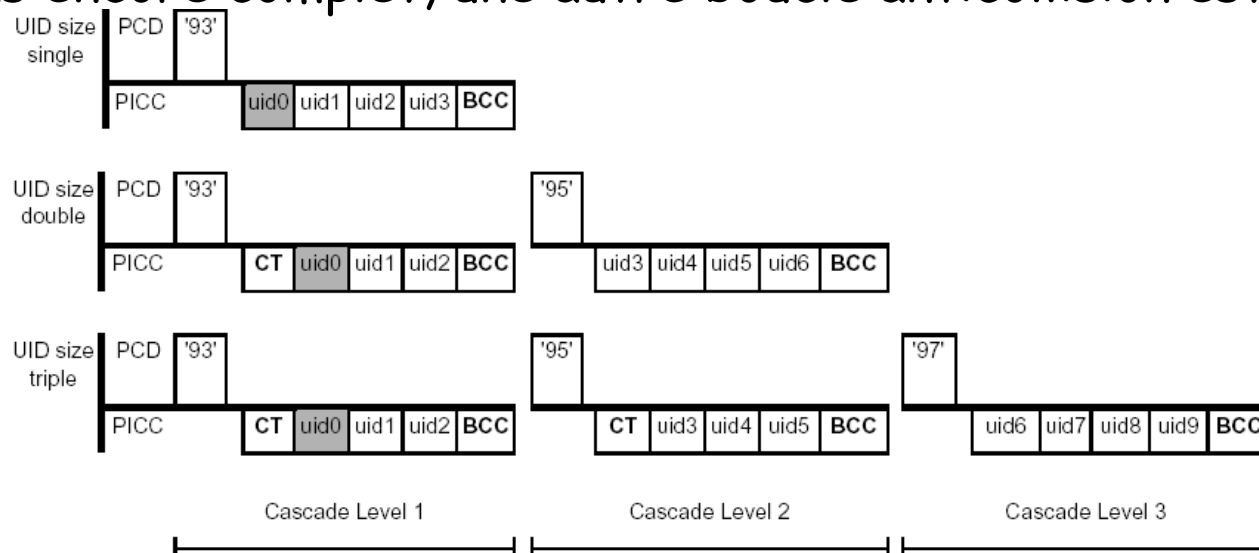
- La collision est détectée au niveau du bit, grâce au codage manchester.



- Méthode déterministe qui repose sur le temps maximum nécessaire pour sélectionner une carte unique qui doit être bien défini et ne doit pas varier avec le temps
  - ✓ → Identification par un numéro unique

# Principe de l'anticollision - Type A (2/2)

- UID (Unique IDentification Number)
  - ✓ 40 bits de data Max.
  - ✓ Lecture en cascade suivant la taille de l'UID (info contenu dans ATQA)
- La boucle d'Anticollision peut avoir plusieurs niveaux de cascades qui dépendent de la taille du UID
  - ✓ Le paramètre CT (Cascade Tag=88) indique que l'UID reçu n'est pas encore complet, une autre boucle anticollision est requise.



# Trame anticollision - Type A (1/4)

- La commande ANTICOLLISION contient les champs suivants :

SEL	NVB	Données UID CL <sub>n</sub>
8 bits	8 bits	0 à 40 bits

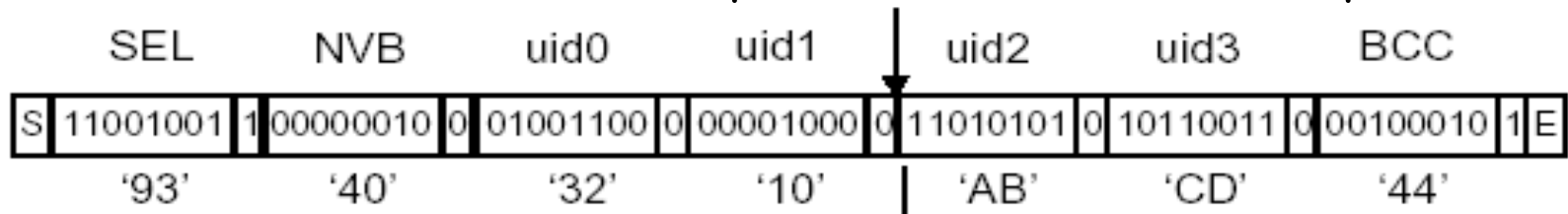
- ✓ SEL (select code; 1 octet), pour demander à la carte d'envoyer son UID qui peut avoir plusieurs tailles (Cascade Level CL)
- b1 indique le mode d'anticollision choisi par le lecteur
  - b2 et b3 indique le niveau de cascade sélectionné

b8	B7	B6	b5	b4	b3	b2	b1	Value	Signification
1	0	0	1	0	0	1	1	'93'	Selection of CL1
1	0	0	1	0	1	0	1	'95'	Selection of CL2
1	0	0	1	0	1	1	1	'97'	Selection of CL3

# Trame anticollision - Type A (2/4)

## ➤ La boucle anticollision est utilisée :

- ✓ Envoi de trames standards de 56 bits partagés en 7 octets.
- ✓ Bit de Start (S), Bit de Stop (E), 8 bits data, 1 bit de parité



## ➤ La trame est divisée en 2 partie

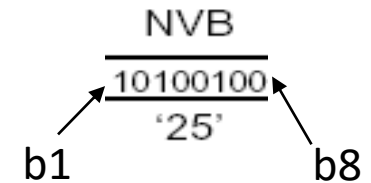
- ✓ Part 1 : transférer data de PCD vers PICC (min = 16 bits; max = 55 bits)
- ✓ Part 2 : transférer data PICC vers PCD (min = 1 bits; max = 40 bits)
- ✓ La division dépend de la place de la boucle de l'anticollision:
  - A l'intérieur d'un octet (cas Split Byte)
  - Après un octet complet (cas Full Byte)

## ➤ La direction de transmission entre lecteur et carte peut être inversée après que le nombre désiré de bits ait été envoyé.

- La commande ANTICOLLISION contient les champs suivants :
  - ✓ SEL
  - ✓ NVB (Number of Valid Bits; 1 octet), comme dans le processus de l'anticollision, chaque bit transmis est vérifié, NVB indique le nombre d'octets transmis du PCD vers le PICC après qu'une collision ait eu lieu.
  - ✓ Au début de la communication, le lecteur assigne NVB = '20', il ne transmet que 2 octets qui sont NVB et SEL forçant ainsi toutes les cartes à répondre avec leur UID (CL1)

# Trame anticollision - Type A (4/4)

- Codage du NVB
  - b1 à b3 appelé 'bit count'
  - b4 à b8 appelé 'byte count'



b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	1	0	x	x	x	x	byte count = 2
0	0	1	1	x	x	x	x	byte count = 3
0	1	0	0	x	x	x	x	byte count = 4
0	1	0	1	x	x	x	x	byte count = 5
0	1	1	0	x	x	x	x	byte count = 6
0	1	1	1	x	x	x	x	byte count = 7
0	1	0	0	x	x	x	x	byte count = 8
x	x	x	x	0	0	0	0	bit count = 0
x	x	x	x	0	0	0	1	bit count = 1
x	x	x	x	0	0	1	0	bit count = 2
x	x	x	x	0	0	1	1	bit count = 3
x	x	x	x	0	1	0	0	bit count = 4
x	x	x	x	0	1	0	1	bit count = 5
x	x	x	x	0	1	1	0	bit count = 6
x	x	x	x	0	1	1	1	bit count = 7



# Boucle anticollision - Type A (1/4)

PCD	PICC	Cascade Level
REQA	Réponses synchrones	
	ATQA1	
	ATQA2	
	ATQA3	
SEL '93'    NVB '20'	Les cartes dans le champs doivent transmettre les UID	CL1

# Boucle anticollision - Type A (2/4)

- Les cartes dans le champ envoient leurs UID de manière synchrone

PCD			PICC							
SEL	NVB		Réponse synchrone	UID0 – CL1						
'93'	'20'									
			UID01	0	0	0	1	1	1	1
			UID02	0	0	0	1	0	1	1
			UID03	0	0	0	0	1	1	1
Première collision au 4 <sup>ème</sup> bit – le lecteur assigne '1' à la place de la collision										

# Boucle anticollision - Type A (3/4)

PCD										PICC									
SEL	NVB	UID CL1								Réponse synchrone	UID0 – CL1								
‘93’	‘24’	0	0	0	1	-	-	-	-										
Les cartes avec les premiers bits corrects de l’UID envoient la partie manquante																			
										UID01	0	0	0	1	1	1	1	1	
										UID02	0	0	0	1	0	1	1	1	
Collision au 5 <sup>ème</sup> bit - le lecteur affecte ‘1’ à la place de la collision																			

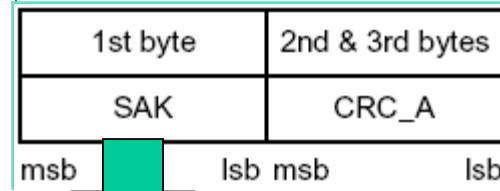
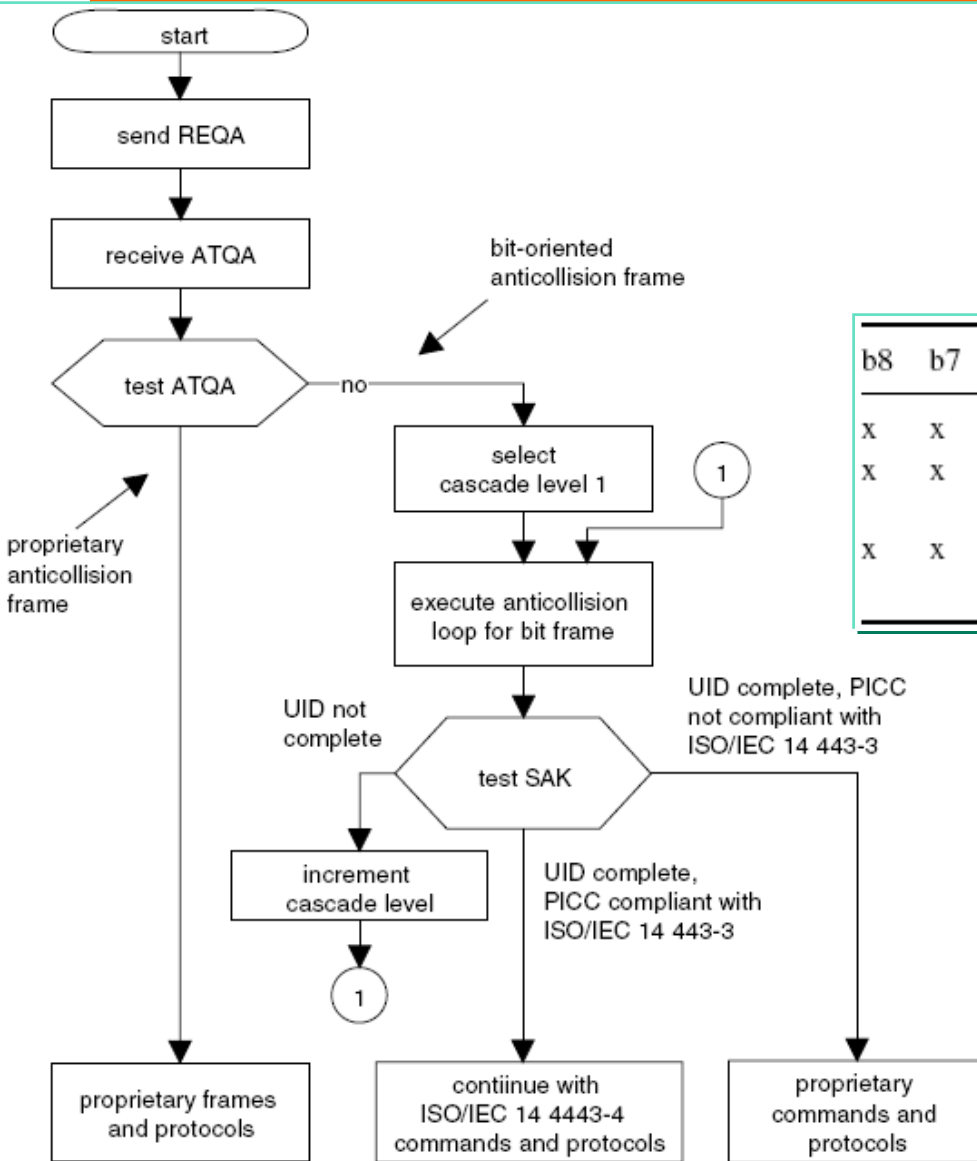
PCD										PICC									
SEL	NVB	UID CL1								Réponse synchrone	UID0 – CL1								
‘93’	‘25’	0	0	0	1	1	-	-	-										
Les cartes avec les premiers bits corrects de l’UID envoient la partie manquante																			
										UID01	0	0	0	1	1	1	1	1	
Plus de collision -																			

# Boucle anticollision - Type A (4/4)

PCD										PICC					
SEL	NVB	UID CL1									UID – CL1				
‘93’	‘25’	0	0	0	1	1	-	-	-						
La carte sélectionnée N°1 va envoyer les autres UID : UID0, UID1, UID2, UID3															
										UID0	UID1	UID2	UID3	BCC	

PCD								PICC	
SEL	NVB	UID0	UID1	UID2	UID3	BCC	CRC_A		
‘93’    ‘70’									
La carte sélectionnée va envoyer l’accusé de réception le SELECT ACKNOWLEDGE									
								SAK	CRC_A
								xx0x x1xx	

# Diagramme d'état lecteur/carte - Type A



b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	1	x	x	Cascade bit set:: UID incomplete
x	x	1	x	x	0	x	x	UID complete, PICC complies with ISO/IEC 14 443-4
x	x	0	x	x	0	x	x	UID complete, PICC does not comply with ISO/IEC 14 443-4

# Exemple : anticollision Type A (1/4)



PCD to PICC →

← PICC to PCD

Request

REQA →

'26'

← ATQA PICC 1  
1000 0000 0000 0000

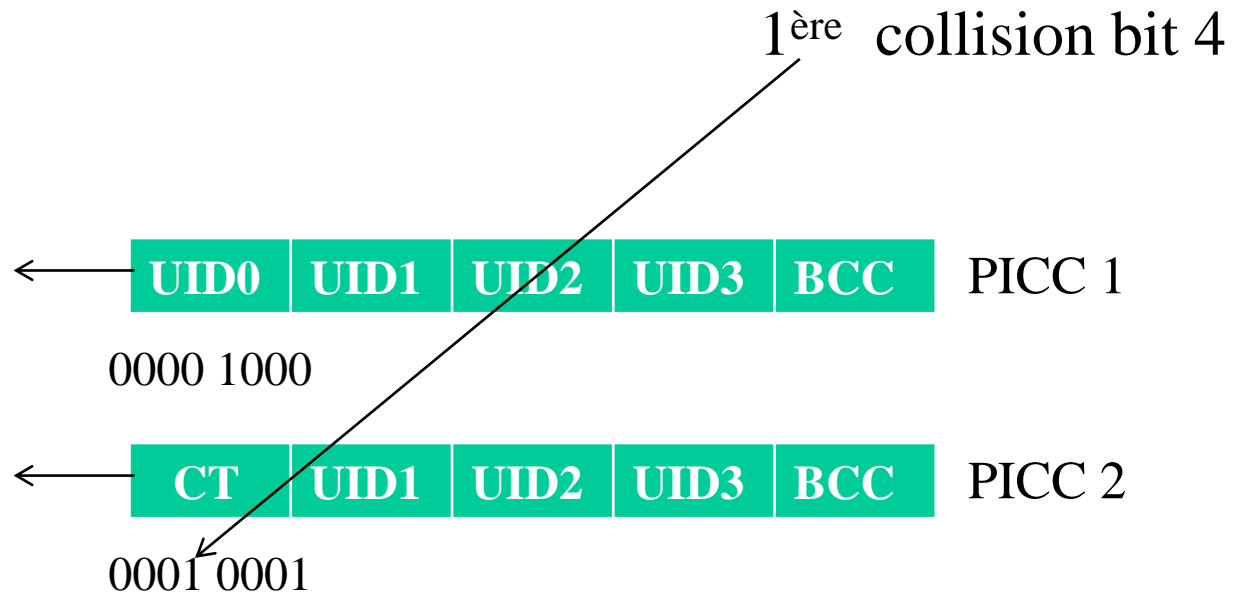
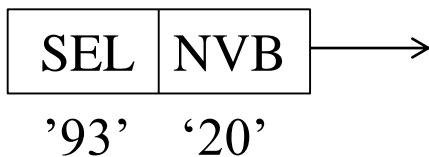
← ATQA PICC 2  
1000 0010 0000 0000

# Exemple : anticollision Type A (2/4)

PCD to PICC →

← PICC to PCD

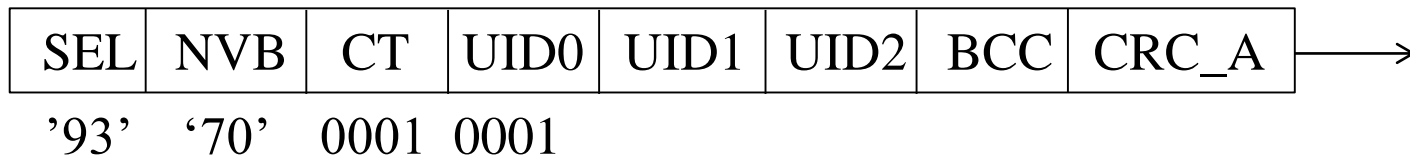
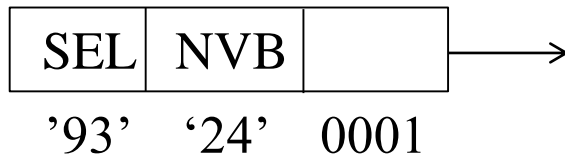
Boucle anticollision : Cascade Level 1



# Exemple : anticollision Type A (3/4)

PCD to PICC →

← PICC to PCD





# Exemple : anticollision Type A (4/4)

PCD to PICC →

← PICC to PCD

Boucle anticollision : Cascade Level 2

SEL	NVB
'95'	'20'

 →

← 

UID3	UID4	UID5	UID6	BCC
------	------	------	------	-----

 PICC 2

SEL	NVB	UID3	UID4	UID5	UID6	BCC	CRC_A
'95'	'70'						

← 

SAK	CRC_A
-----	-------

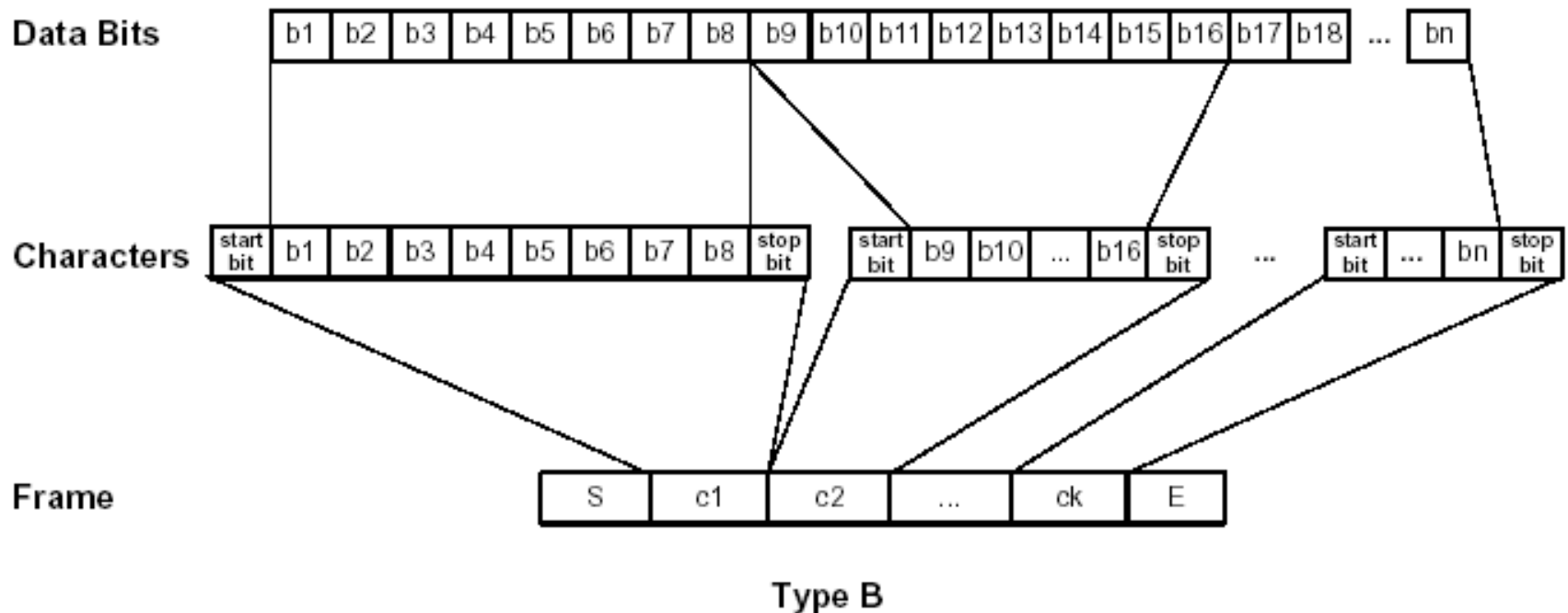
 PICC 2  
xx0x x1xx

---

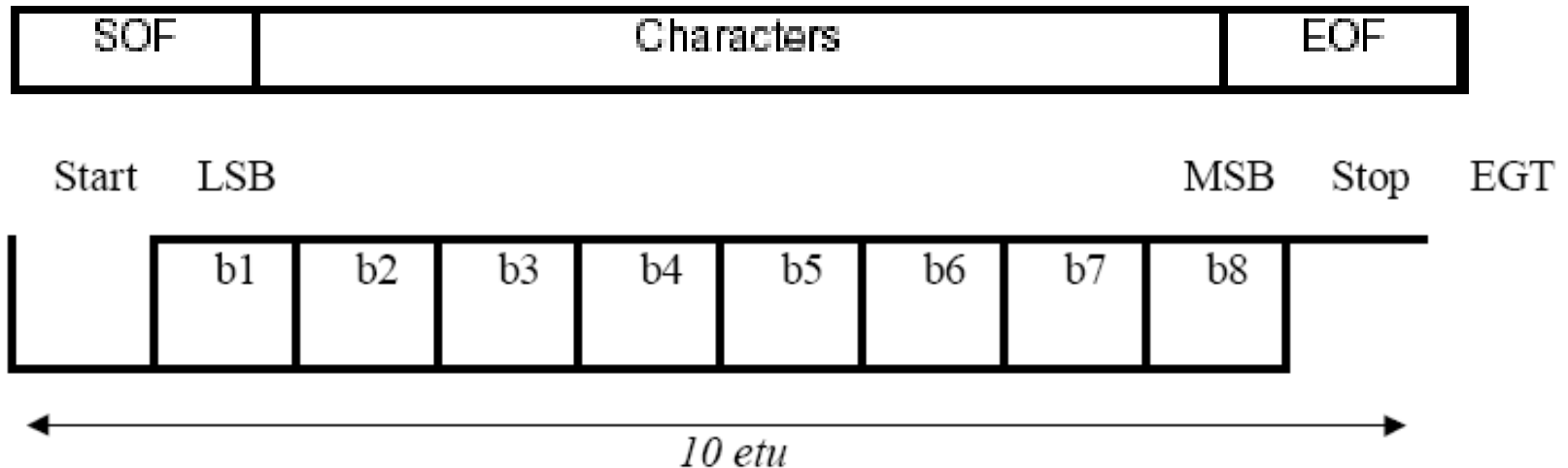
# ISO 14443 Part 3 : Initialisation et Anticollision Type B

# Format Frame - Type B (1/6)

- Un seul type de format
- Utilisé par les cartes et les lecteurs
- LSB transmis en premier



## ➤ Format d'un caractère

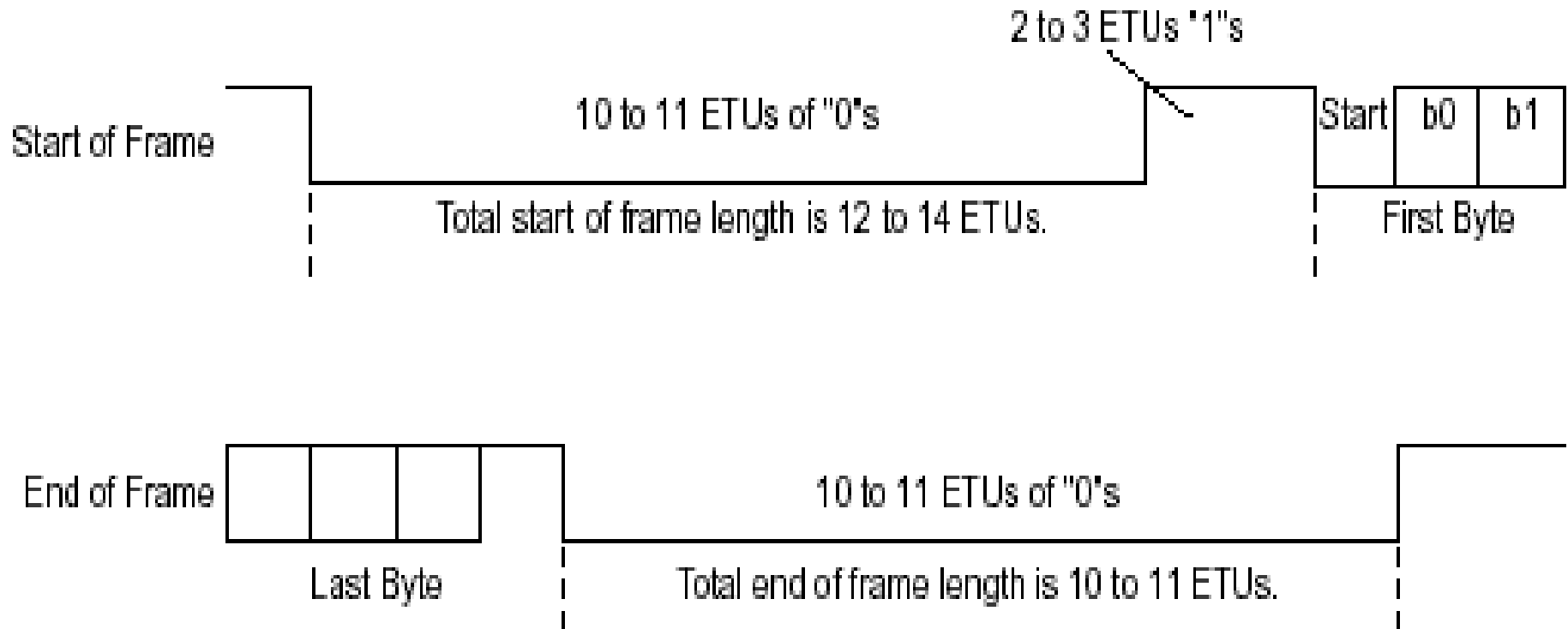


## ➤ EGT (Extra Guard Time) est le temps qui sépare deux caractères.

- ✓ PCD vers PICC entre 0 et  $57\mu s$  (0 à 6 etu)
- ✓ PICC vers PCD entre 0 et  $19\mu s$  (0 à 2 etu)
- ✓ etu : elementary time unit (durée d'un bit)

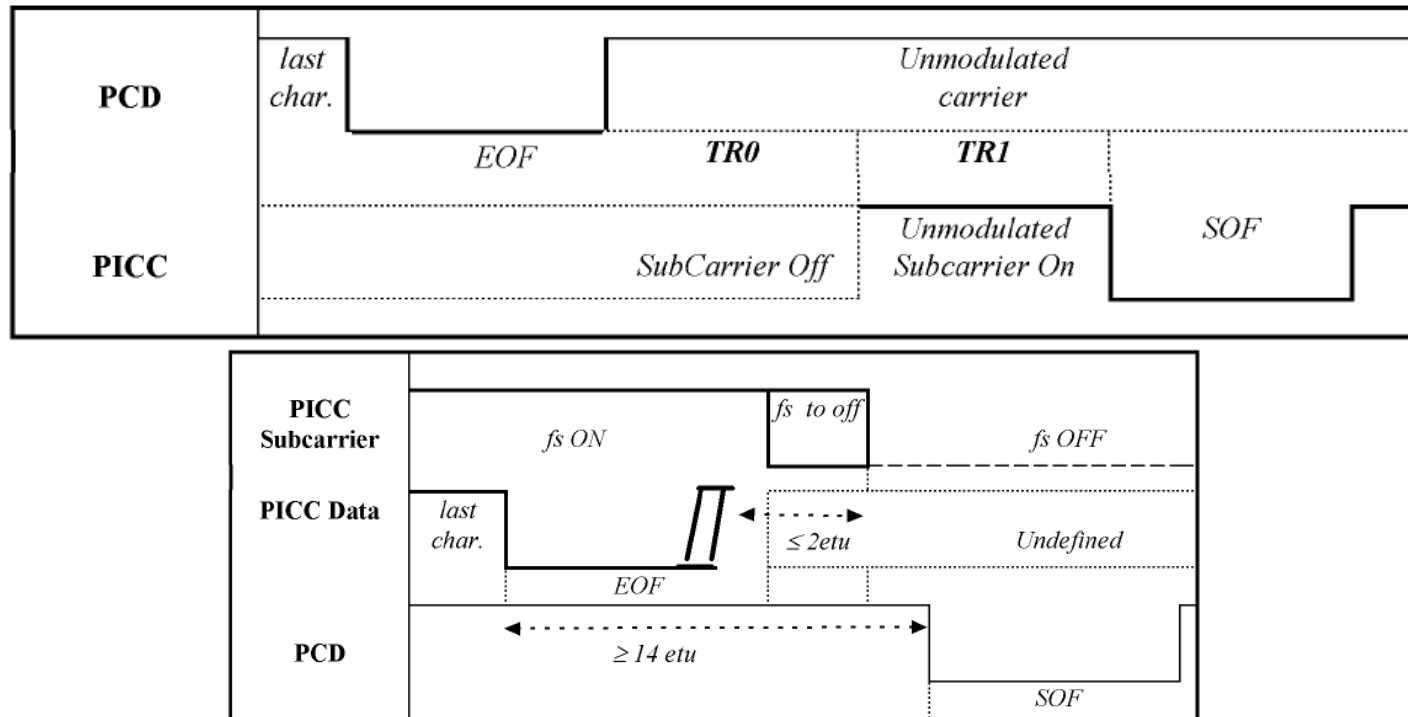
# Format Frame - Type B (3/6)

- Start of Frame (SOF)
- End of Frame (EOF)



# Format Trame - Type B (4/6)

## ➤ PICC vers PCD sous-porteuse et SOF

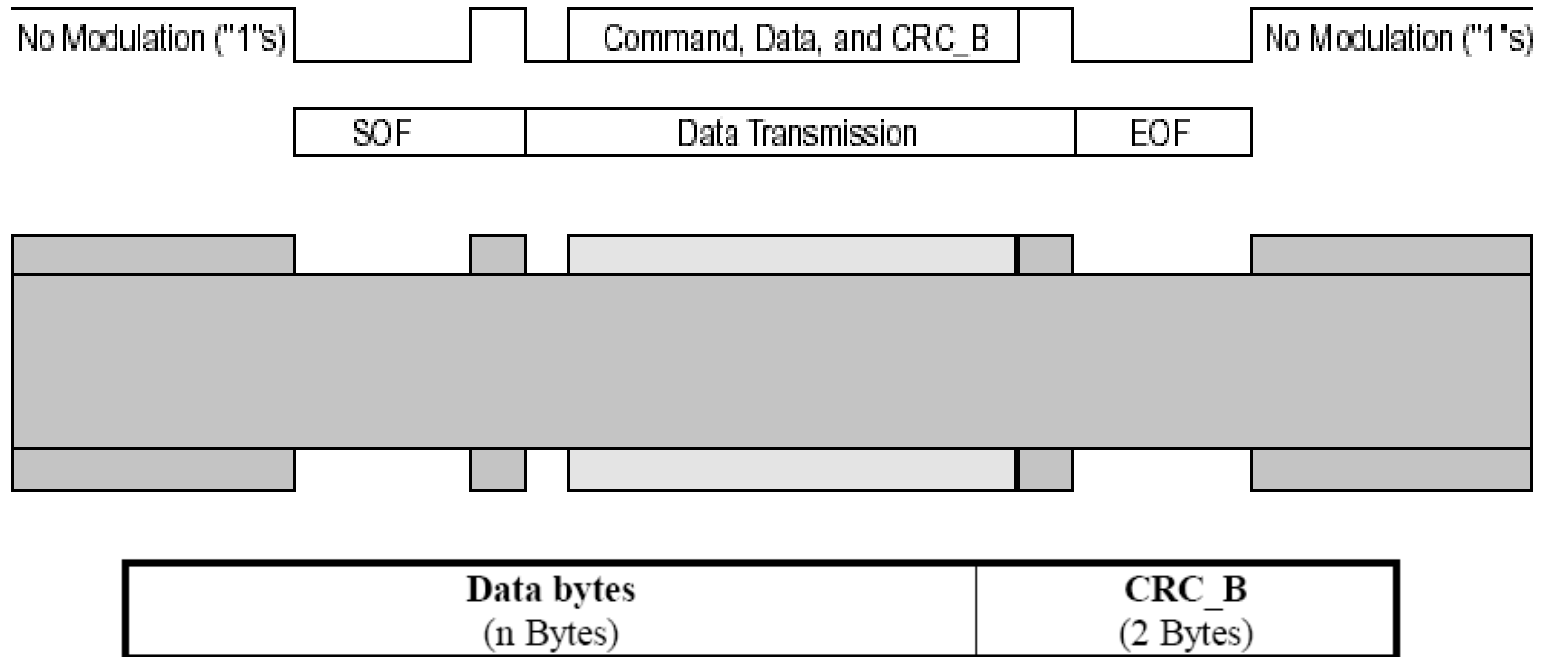


## ➤ PICC vers PCD sous-porteuse et EOF

- ✓ Le PICC ne doit pas s'arrêter avant la fin d'EOF et pas au delà de 2 etu après l'EOF.
- ✓ Le délai minimum (FDT) entre le début du EOF du PICC et le début du SOF du PCD doit être de 14 etu

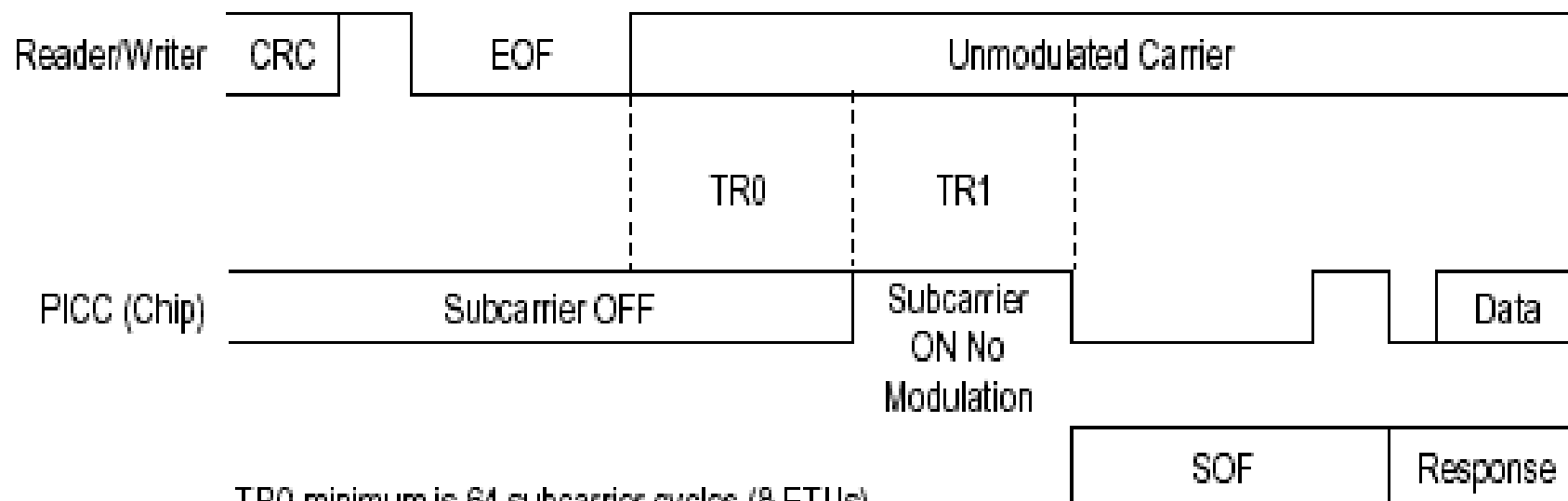
# Format Frame - Type B (5/6)

- Une frame est considérée comme correcte si elle est reçue avec un CRC\_B valide (défini par la norme 14443 et ISO/IEC 3309).



## ➤ FDT du PCD vers PICC

✓ TR0 et TR1



TR0 minimum is 64 subcarrier cycles (8 ETUs).

TR0 maximum is 32 ETUs for ATQB only.

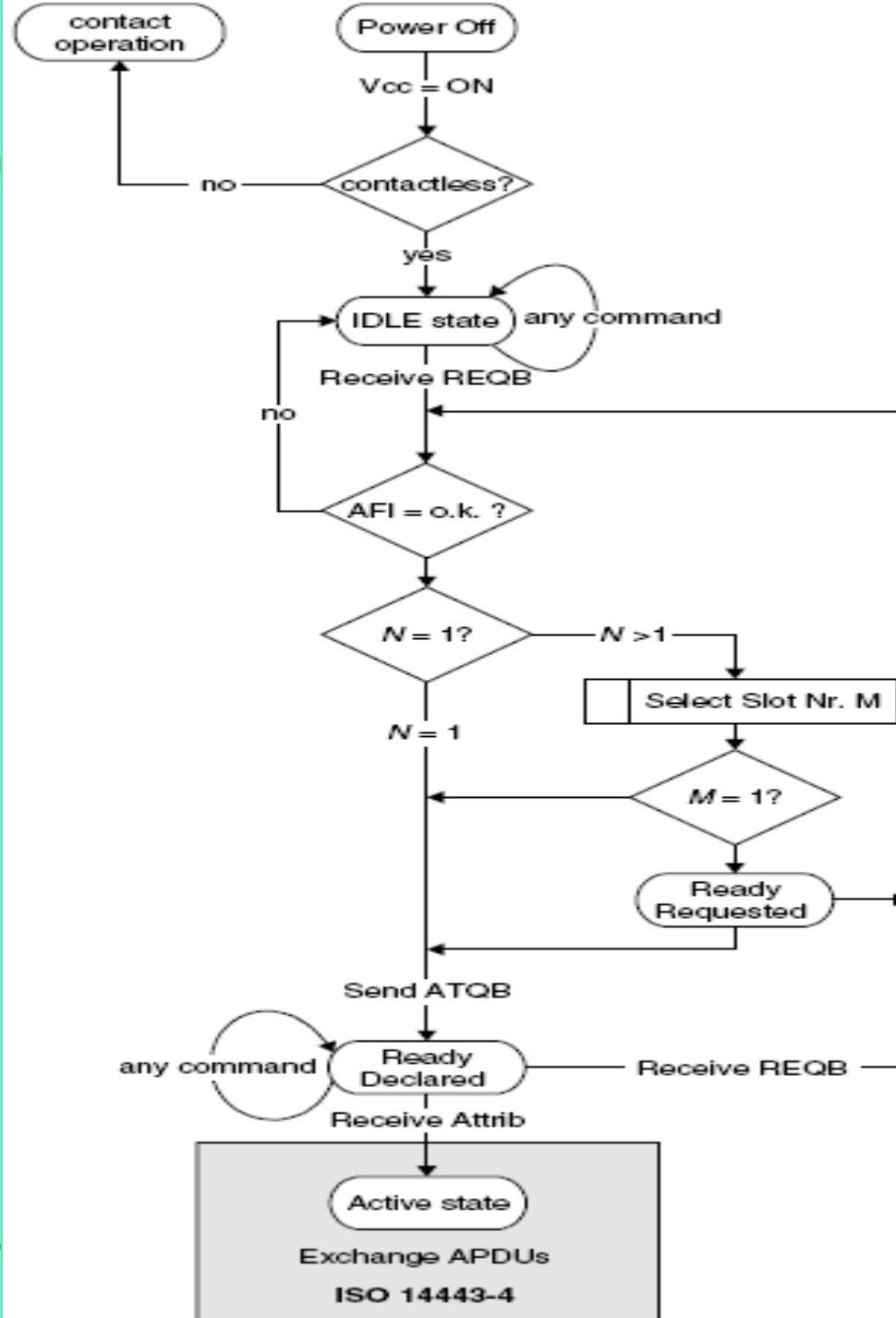
TR0 maximum is FWT for all other commands.

TR1 minimum is 80 subcarrier cycles (10 ETUs).

TR1 maximum is 200 subcarrier cycles (25 ETUs).



- L'anticollision est contrôlé par le PCD (maître-esclave), qui permet de séparer les transmissions des PICC dans le temps. Le PCD ne permet qu'à une seule carte de dialoguer
  - ✓ Solution Pseudo - déterministe
    - Multi-time slot pour la réponse du PICC : chaque carte n'a le droit de répondre que dans une plage. Si le nombre de plage est grand, le PCD trouve presque toujours une plage dans laquelle une seule carte a répondu, et elle est choisie..
  - ✓ Solution Probabiliste
    - Simple slot avec une probabilité de réponse du PICC : il y a une seule tranche, mais, chaque carte tire au sort pour décider si elle répond ou non. La probabilité est majorée par  $1/N$
  - ✓ Autre solution combinant les deux approches



- Le PCD envoie des trames REQB/WUPB d'invitation à émettre (mode polling). La porteuse réveille la carte qui passe à l'état Idle.

Apf	AFI	PARAM	CRC
1 Byte	1 Byte	1 Byte	2 Bytes

- ✓ Apf : Anticollision Prefix, a une valeur réservée : (05h) utilisé pour marquer les plages horaires (slot marker)
- ✓ AFI (Application Family Identifier) de 1 octet pour présélectionner la ou les cartes que le PCD sait traiter.
- ✓ PARAM définit le nombre de plages horaire (slots) disponibles

## ➤ AFI (Application Family Identifier)

AFI bit 7–bit 4 Application group	AFI bit 3–bit 0 Subgroup	Comment
0000	0000	All application groups and subgroups
—	0000	All subgroups of an application group
‘X’	‘Y’	Only subgroup Y of application group X
0001	—	Transport (local transport, airlines, ...)
0010	—	Payments (banks, tickets, ...)
0011	—	Identification (passport, driving licence)
0100	—	Telecommunication (telephone card, GSM, ...)
0101	—	Medicine (health insurance card, ...)
0110	—	Multimedia (internet service, Pay-TV)
0111	—	Games (casino card, lotto card)
1000	—	Data storage (‘portable files’, ...)
1001–1111	—	Reserved for future applications

## ➤ PARAM

Para <i>M</i> byte (bit 2–bit 0)	Number of slots <i>N</i>
000	1
001	2
010	4
011	8
100	16
101	Reserved for future applications
11x	Reserved for future applications

# Anticollision - Type B (1/9)

- La station de base propose N plages horaires où les cartes à puce présentes peuvent répondre (N = 1, 2, 4, 8 ou 16)
  - ✓ Si N = 1, la carte transmet un ATQB et se met en mode Ready
  - ✓ Si N > 1, la carte engendre un nombre aléatoire R entre 1 et N

Reader	REQB N = 1		REQB N = 4
PICC #1		ATQB	R = 2
PICC #2		ATQB	R = 4
PICC #3		ATQB	R = 1

- Si  $R = 1$ , la carte transmet un ATQB et se met en mode Ready
- Si  $R > 1$ , deux options sont possibles :
  - ✓ Option 1 (approche probabiliste) : pour les cartes qui n'ont pas de sélection de plages horaires spécifiques,
    - la carte se met en mode Idle et se boucle jusqu'à avoir  $R = 1$
    - Autre possibilité, le PCD met  $N$  à la valeur 1
  - ✓ Option 2: pour les cartes qui permettent la sélection des plages horaires. Dans ce cas, la carte attend de recevoir la commande Slot Marker avec un nombre correspondant à une plage horaire (Nombre de la plage =  $R$ ) avant de transmettre l'ATQB et de se mettre en mode Ready

# Anticollision - Type B (3/9)

Reader	REQB N = 1		REQB N = 4		SM2		SM3		SM4	
PICC#1		ATQB	R = 2			ATQB				
PICC#2		ATQB	R = 4							ATQB
PICC#3		ATQB	R = 1	ATQB						

- Format de la commande Slot Marker  
 $AP_n$  : Anticollision Prefix = \$n5

$AP_n$	CRC_B
1 byte	2 bytes

$n$	Slot number
0001	2
0010	3
0011	4
...	...
1110	15
1111	16

- Si le PCD ne détecte pas un ATQB, il transmet immédiatement le Slot Marker suivant

- Une fois la séquence d'anticollision terminée, la station de base sélectionne un transpondeur par son PUPI (Pseudo-Unique Picc Identifier)
- PUPI est l'identificateur du PICC durant la boucle d'anticollision et met les autres PICC en attente pendant qu'elle communique avec lui.
  - ✓ PUPI peut être fixe ou aléatoire généré par la carte après un Power Reset
- Le PICC adressé par son PUPI envoie l'ATQB et se met en mode actif



- La réponse ATQB envoyé par le PICC au PCD fourni au lecteur les informations sur les paramètres importants de la carte :
  - N° de série de la carte (PUPI)
  - Interface Contactless (Protocol Info)
    - Débit max de communication
    - Taille des trames réceptionnées par la carte
  - Paramètres des Applications (Application Data)
    - Information sur les applications disponibles sur la carte

# Anticollision ATQB - Type B (6/9)

- La trame ATQB envoyée par le PICC en réponse au REQ B/WUPB a le format suivant :

APa	PUPI	Application Data	Protocol Info	CRC_B
'50'	4 bytes	4 bytes	3 bytes	2 bytes

- Format du champs Application Data

AFI	CRC_B (AID)	Number of applications
1 byte	2 bytes	1 byte

- Number of applications :
  - b7-b4 : nombre d'appli AFI
  - b3-b0 : nombre total d'applications dans la carte

- Format du champs Protocol Info

Byte 1	Byte 2				
Bit_Rate_capability	Max_Frame_Size	Protocol_Type	FWI	ADC	FO
8 bits	4 bits	4 bits	4 bits	2 bits	2 bits

- Champs FO :
  - b2b1 = 1x : PICC supports NAD
  - b2b1 = 1x : PICC supports CID
- Champs ADC (Application Data Coding)
- Champs FWI : Frame Waiting Integer (0-14)
  - spécifie le temps max nécessaire pour que la carte démarre la transmission en réponse au PCD
  - Permet le calcul du FWT(Frame Waiting Time)

# Anticollision ATQB - Type B (8/9)

- Format du champs Protocol Info

Byte 1	Byte 2				
Bit_Rate_capability	Max_Frame_Size	Protocol_Type	FWI	ADC	FO
8 bits	4 bits	4 bits	4 bits	2 bits	2 bits

- Champs Protocol Type :
  - b4b3b2b1 = 0001 : PICC supports ISO:IEC 14443-4
  - b4b3b2b1 = 0000 : PICC does not support ISO:IEC 14443-4
- Max\_Frame\_Size : limité par la taille de la mémoire du PICC

Max_Frame_Size code in ATQB	0	1	2	3	4	5	6	7	8	9-F
Maximum frame size (bytes)	16	24	32	40	48	64	96	128	256	RFU>256

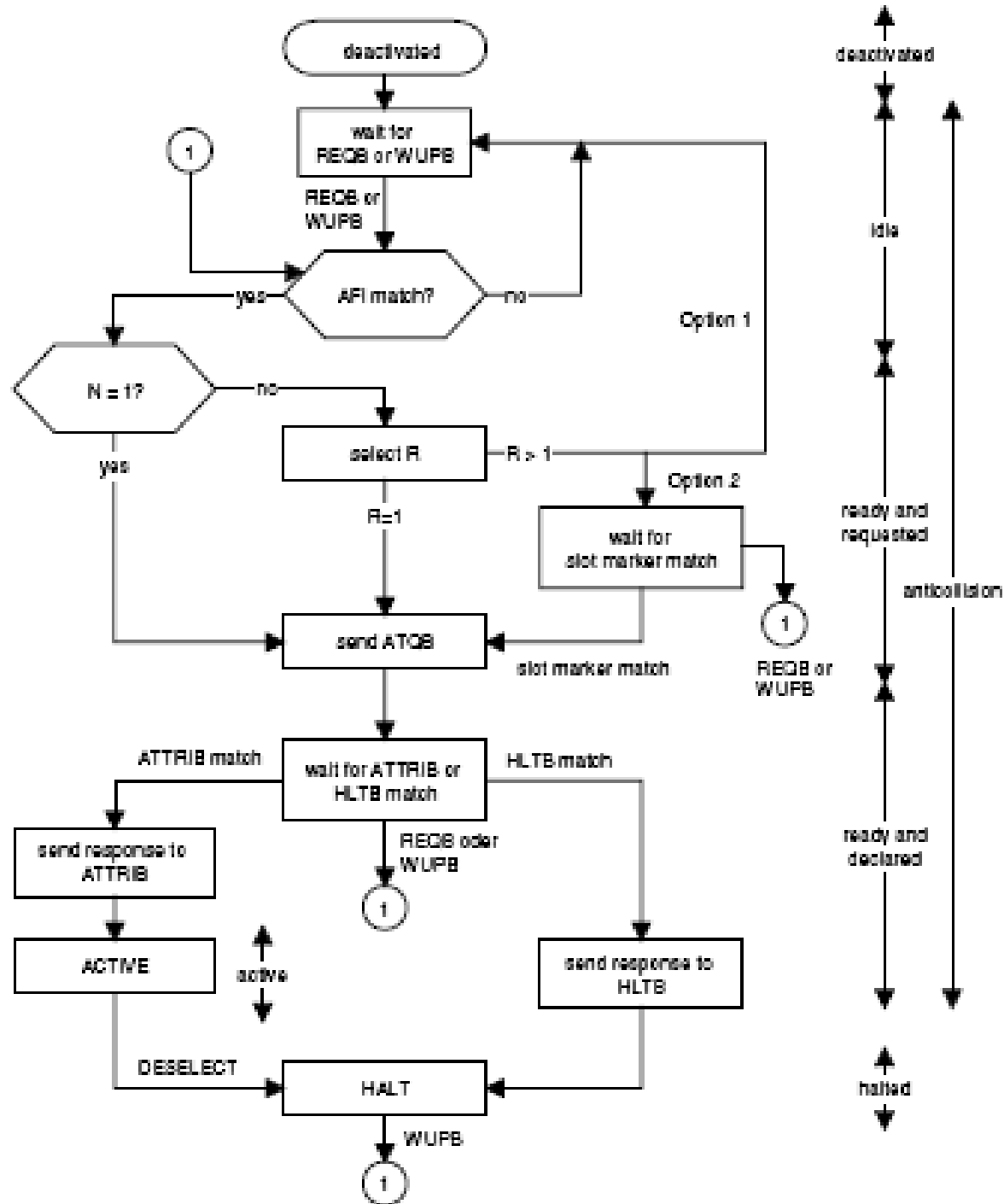
# Anticollision ATQB - Type B (9/9)

- Format du champs Protocol Info

Byte 1	Byte 2				
Bit_Rate_capability	Max_Frame_Size	Protocol_Type	FWI	ADC	FO
8 bits	4 bits	4 bits	4 bits	2 bits	2 bits

- Bit\_Rate\_Capability :

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	PICC supports only 106 kbit/s in both directions
1	X	X	X	0	X	X	X	The same bit rate in both directions
X	X	X	1	0	X	X	X	PICC to PCD: 1 etu = $64/f_C$ , 212 kbit/s supported
X	X	1	X	0	X	X	X	PICC to PCD: 1 etu = $32/f_C$ , 424 kbit/s supported
X	1	X	X	0	X	X	X	PICC to PCD: 1 etu = $16/f_C$ , 847 kbit/s supported
X	X	X	X	0	X	X	1	PCD to PICC: 1 etu = $64/f_C$ , 212 kbit/s supported
X	X	X	X	0	X	1	X	PCD to PICC: 1 etu = $32/f_C$ , 424 kbit/s supported
X	X	X	X	0	1	X	X	PCD to PICC: 1 etu = $16/f_C$ , 847 kbit/s supported



# ATTRIB - Type B (1/4)

- ATTRIB est transmis par le PCD au PICC pour sélectionner la carte

'ID'	Identifier (PUPI)	Param 1	Param 2	Param 3	Param 4	Higher Layer Inf.	CRC_B
1 byte	4 bytes	1 byte	1 byte	1 byte	1 byte	0 or more bytes	2 bytes

## • Format Paramètre 1 :

b8	b7	b6	b5	b4	b3	b2	b1
Minimum TR0		Minimum TR1		EOF	SOF	RFU	

Minimum TR0 : définit le temps minimum avant de répondre à une commande du PCD

Minimum TR1 : définit le délais minimum Entre l'activation de la sou-porteuse et le début de la transmission

b8	b7	Minimum TR0
0	0	Default value
0	1	$48/f_s$
1	0	$16/f_s$
1	1	RFU

b6	b5	Minimum TR1
0	0	Default value
0	1	$64/f_s$
1	0	$16/f_s$
1	1	RFU

# ATTRIB - Type B (2/4)

- ATTRIB est transmis par le PCD au PICC pour sélectionner la carte

'ID'	Identifier (PUPI)	Param 1	Param 2	Param 3	Param 4	Higher Layer Inf.	CRC_B
1 byte	4 bytes	1 byte	1 byte	1 byte	1 byte	0 or more bytes	2 bytes

- Format Paramètre 2 :

- ✓ bits b4-b1 spécifient la taille max de la trame qui peut être reçu par le PCD

Max_Frame_Size code in ATTRIB	0	1	2	3	4	5	6	7	8	9-F
Maximum frame size (bytes)	16	24	32	40	48	64	96	128	256	RFU>256

- ✓ Bits b8-b5 sont utilisés Pour sélectionner le débit Binaire dans les deux directions

b8	b7	b6	b5	Meaning
0	0	x	x	PICC to PCD: 1 etu = $128/f_C$ , bit rate is 106 kbit/s
0	1	x	x	PICC to PCD: 1 etu = $64/f_C$ , bit rate is 212 kbit/s
1	0	x	x	PICC to PCD: 1 etu = $32/f_C$ , bit rate is 424 kbit/s
1	1	x	x	PICC to PCD: 1 etu = $16/f_C$ , bit rate is 847 kbit/s
x	x	0	0	PCD to PICC: 1 etu = $128/f_C$ , bit rate is 106 kbit/s
x	x	0	1	PCD to PICC: 1 etu = $64/f_C$ , bit rate is 212 kbit/s
x	x	1	0	PCD to PICC: 1 etu = $32/f_C$ , bit rate is 424 kbit/s
x	x	1	1	PCD to PICC: 1 etu = $16/f_C$ , bit rate is 847 kbit/s



# ATTRIB - Type B (3/4)

- ATTRIB est transmis par le PCD au PICC pour sélectionner la carte

'ID'	Identifier (PUPI)	Param 1	Param 2	Param 3	Param 4	Higher Layer Inf.	CRC_B
1 byte	4 bytes	1 byte	1 byte	1 byte	1 byte	0 or more bytes	2 bytes

- Format Paramètre 3 :
  - ✓ bits b4-b1 confirment le type de protocole supporté par le PCD

b4	b3	b2	b1	Meaning
0	0	0	1	PICC supports ISO/IEC 14 443-4
0	0	0	0	PICC does not support ISO/IEC 14 443-4

- ✓ Les autres bits sont positionnés à « 0 »

# ATTRIB - Type B (4/4)

- ATTRIB est transmis par le PCD au PICC pour sélectionner la carte

'ID'	Identifiant (PUPI)	Param 1	Param 2	Param 3	Param 4	Higher Layer Inf.	CRC_B
1 byte	4 bytes	1 byte	1 byte	1 byte	1 byte	0 or more bytes	2 bytes

- Format Paramètre 4 :
  - ✓ bits b4-b1 appelé CID (Card Identifier) qui définit le N° logique de la carte sélectionnée (de 0 à 14). Si la carte ne supporte pas le CID, le paramètre est positionné à « 0 »
  - ✓ Les autres bits sont positionnés à « 0 »
- Format Higher Layer Inf :
  - Champs utilisé lorsqu'on veut utiliser des commandes de niveau supérieur

- Le PICC répond à chaque ATTRIB valide (PUPI et CRC\_B correctes)
  - ✓ CID: Card Identifier (Optionnel)
  - ✓ MBLI (Maximum Buffer Length Index) que le PICC envoie au PCD pour lui signaler la taille max de sa mémoire tampon d'entrée, évitant ainsi au PCD de saturer la mémoire du PICC par l'envoi en surnombre de trames.
    - Si MBLI = 0, la carte ne fournit aucune information sur la taille de son buffer interne.

Byte 1		Bytes 2–n	
MBLI	CID	Higher-layer response	CRC_B
1 byte		Optionally 0 or more bytes	2 bytes

# Anticollision Exemple-Type B (1/4)

## PCD

Début de la séquence anticollision :  
Application transport, AFI = '10'  
Nombre de slots (N)=1

*Transmit REQB*

Apf	AFI	Param	CRC	CRC
'05'	'10'	'00'	xx	xx

PICC 1

PICC avec application transport,  
AFI = match, N =1

*Transmit ATQB*

PICC 2

PICC avec application santé,  
AFI = no match  
Attendre prochain REQB/WUPB

PICC 3

Multiapplication PICC  
AFI = match, N =1

*Transmit ATQB*

PCD

Collision détectée  
Modifier numéro du slot : N =4

# Anticollision Exemple-Type B (2/4)

*Transmit REQB*

Apf	AFI	Param	CRC	CRC
'05'	'10'	'00'	xx	xx

→ PICC 1

PICC avec application transport,  
AFI = match  
Sélection R (aléatoire) entre 1 & N  
R=2, attendre slot marker 2

PICC 2

PICC avec application santé,  
AFI = no match  
Attendre prochain REQB/WUPB

PICC 3

PICC avec application transport,  
AFI = match  
Sélection R (aléatoire) entre 1 & N  
R=1, transmettre dans le slot 1

*Transmit REQB*

PCD ←

# Anticollision Example-Type B (3/4)

## PCD

En fonction de l'application,  
le PCD a le choix entre la sélection du PICC3  
Sans l'envoi de slot marker ou  
Envoie de nouveau slot marker

*Transmit REQB* → PICC 1

Apn	CRC	CRC
'15'	xx	xx

PICC avec application transport,  
AFI = match  
R =2, transmet sur le slot 2

*Transmit ATQB*

PICC 2

PICC avec application santé,  
Attendre prochain REQB/WUPB

PICC 3

Multiapplication PICC  
Attente HALT ou ATTRIB

PCD ←

# Anticollision Exemple-Type B (4/4)

## PCD

Le PCD a maintenant la réponse de deux PICC. Dans cet exemple il continu a envoyer des slot markers.

*Transmit slot marker for slot 3 : no response*

*Transmit slot marker for slot 4 : no response*

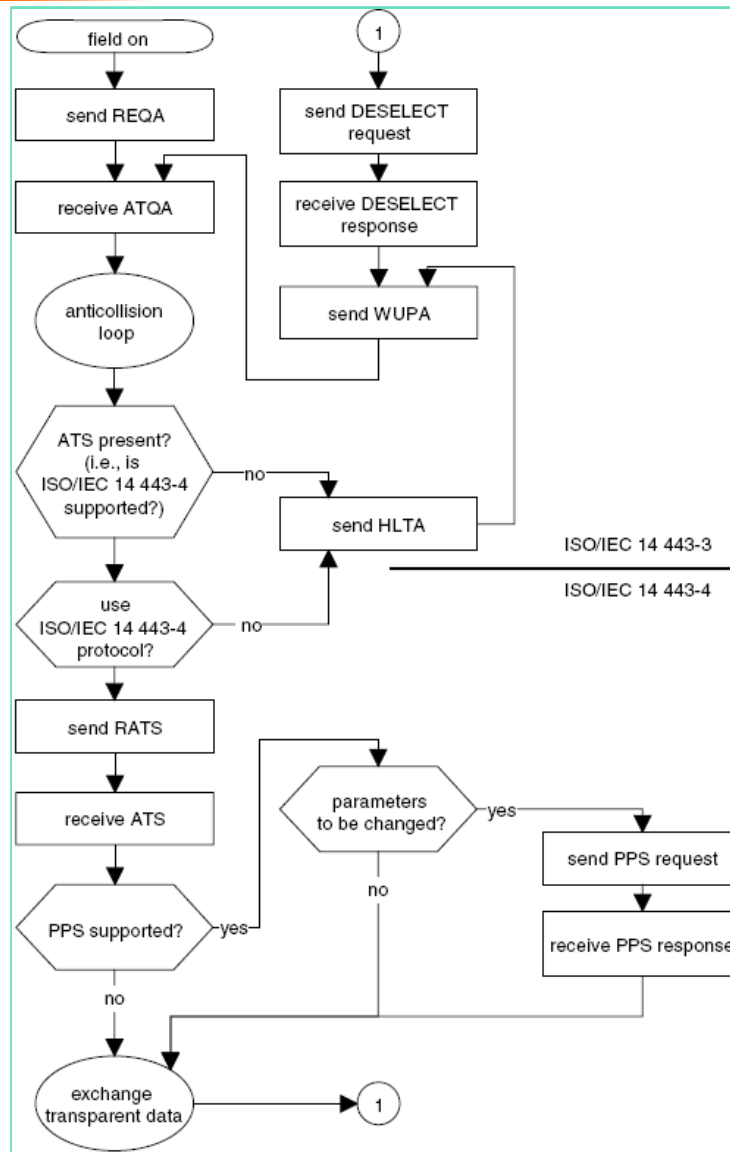
## PCD

Le PCD décide de sélectionner PICC1 (Application transport) en utilisant la Commande ATTRIB. Il peut aussi utiliser la commande HLTB pour arrêter PICC3

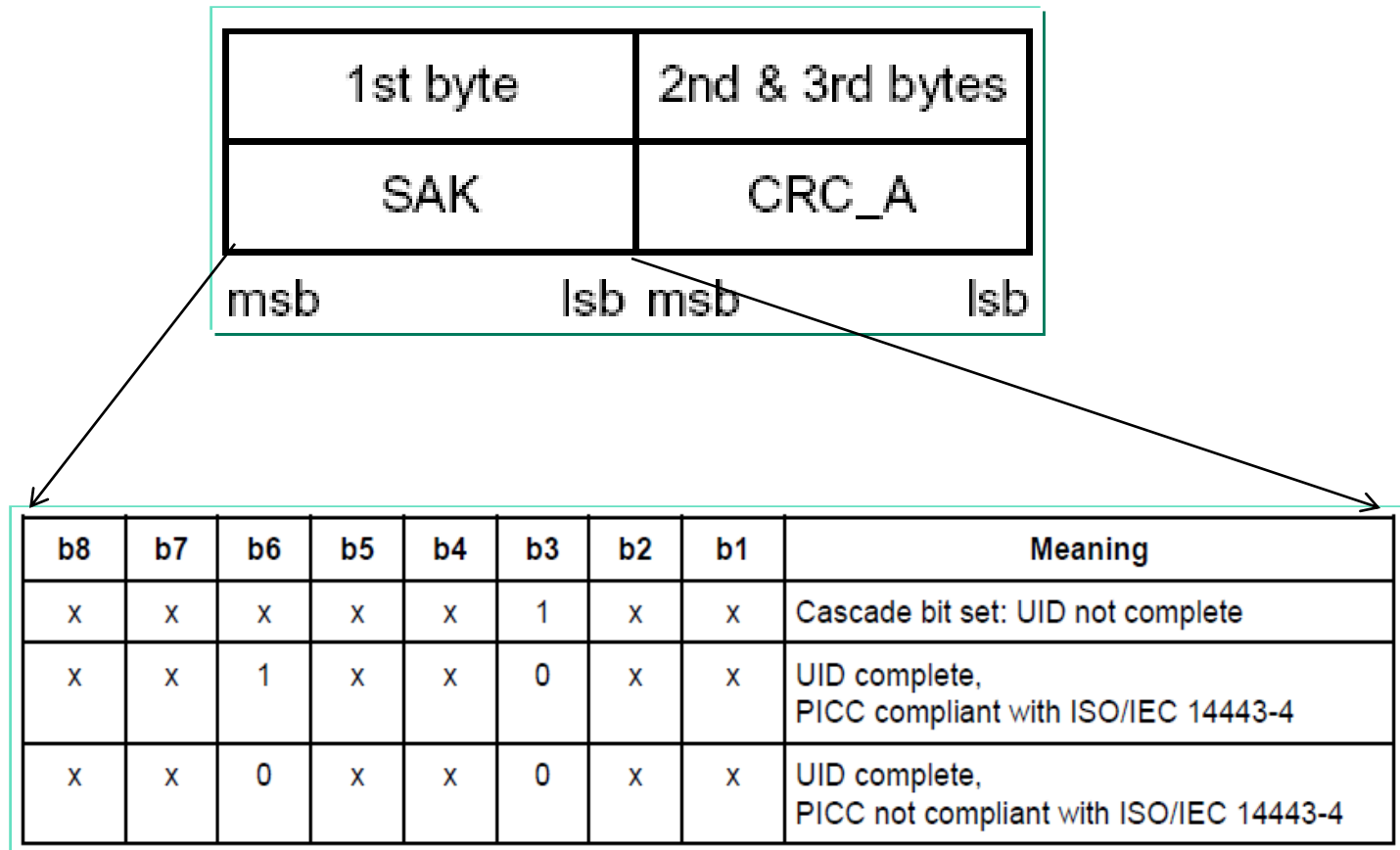
- Après l'initialisation et la boucle d'anticollision, la communication est établie entre le PCD et le PICC pour la lecture, l'écriture et le traitement des données.
- Type A : des informations supplémentaires sur la configuration du protocole (débits binaires possibles, taille max des blocs de données, etc.) doivent être transférées.
- Type B : la configuration du protocole a été transférée lors du processus d'anticollision (ATQB & ATTRIB), le protocole peut commencer immédiatement



# Protocole d'activation du PICC Type A (1/4)

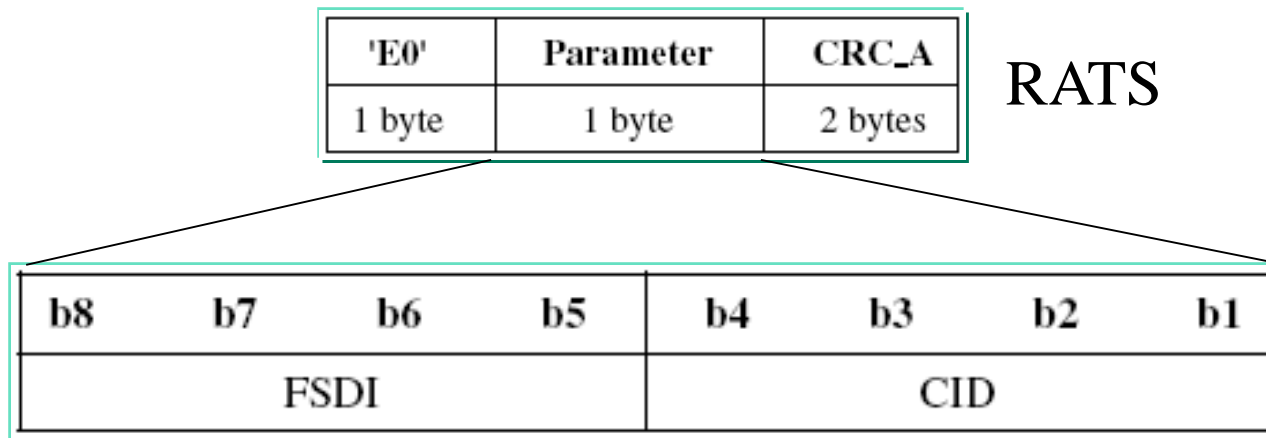


- Confirmation de Select par SAK (Select Acknowledge) après la boucle de l'Anticollision



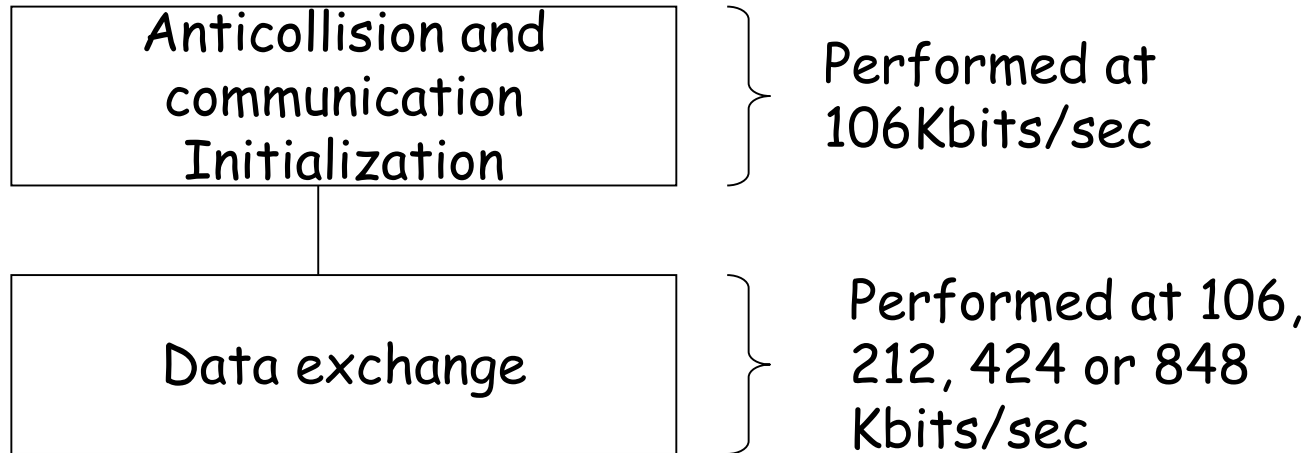
- Le lecteur demande un RATS (Request for an ATS) constitué en deux parties :
  - ✓ b8-b5 FSDI (Frame Size Device Integer) : Taille max d'une frame qu'une carte peut envoyer à un lecteur (PCD)
  - ✓ b4-b1 CID (Card Identifier) : N° logique de la carte sélectionnée entre (0-14).

Le PCD peut maintenir plusieurs cartes Type A dans un état Selected en même temps et peut adresser une carte individuellement via son CID



- Après avoir reçu un ATS (Answer to Select) de la carte, deux possibilités :
  - ✓ La carte détectée n'est pas compatible et/ou le protocole n'est pas supporté par le lecteur
    - La carte est mise en mode HALT
  - ✓ Le protocole indiqué dans l'ATS , est utilisé pour la transmission des data. Le protocole peut aussi être renégocié via la commande PPS (Protocol Parameter Selection)
- ✓ ATS identifie les paramètres supportés par la carte :
  - ✓ Taille maxi de la trame,
  - ✓ débit dans les 2 directions,
  - ✓ Temps d'attente entre les trames,
  - ✓ Supporte NAD et CID.

- La séquence d'activation est décrite par le diagramme d'état de la norme 14443-3
  - ✓ Si la carte reconnaît un ATTRIB Valide elle transmet une réponse à l'ATTRIB et se met en mode ACTIVE.
  - ✓ Dans l'état ACTIVE, la carte a un CID (Card Identifier) assigné par la commande ATTRIB.
- Les paramètres nécessaires aux transmissions de données sont spécifiés et échangés durant la phase d'initialisation et du processus de sélection. (ATQB & ATTRIB)



- Activation avec :
  - ✓ PPS (Protocole & Parameter Selection) request pour Type A
  - ✓ Attrib pour Type B
- Peut être sélectionné dans les deux directions (ex: 848/ 212)

- Le PICC est mis à l'état HALT, une fois que les transactions entre le PICC et le PCD sont terminées
- La désactivation se fait avec la commande DESELECT

- Qu'est ce que la RFID ?
- Un peu d'histoire...
- Carte à puces sans contact
- Classification & état de l'art de la RFID
- Panorama de la standardisation
- Introduction aux cartes à puce sans contact
  - Caractéristiques Physiques
  - Modes de communications
  - Initialisation et Anticollisions
  - **Protocoles de transmission**

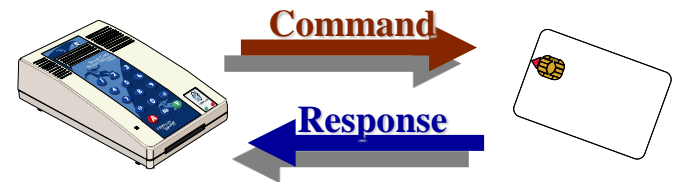


# ISO 14443

## Part 4 :

### Protocole de transmission

- Le protocole débute après un ATR ou un PPS réussi
- T=0 est le premier protocole à être normalisé durant le développement initial de la carte à puce. Il est le plus utilisé.
- La carte communique avec le lecteur en échangeant des messages APDU (Application Protocol Data Unit)
  - ✓ Transmission en Half-Duplex : Transfert de data (longueur variable) dans une seule direction sous le contrôle des octets de protocoles envoyés par la carte.
  - ✓ Caractères asynchrones, Orienté octets (c'est la plus petite unité traité par le protocole)



- Un message est composé d'une
  - ✓ Commande initié par le lecteur vers la carte
  - ✓ Réponse : de la carte vers le lecteur

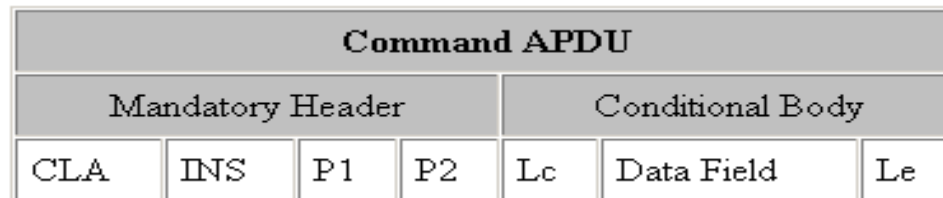
## ➤ Format des commandes APDU :

### ✓ Préfixe obligatoire de 4 octets

- CLA : Classe d'instructions, identifie l'application et les commandes associées
- INS : Code d'instruction
- P1 et P2 : Paramètres de l'instruction

### ✓ Corps optionnel de longueur variable

- Lc : Nombre d'octets présents dans le champ données de la commande
- Séquences d'octets (dont le nombre d'octets est égal à la valeur de Lc) dans le champ données de la commande.
- Le : Longueur maxi du champ de données de la réponse

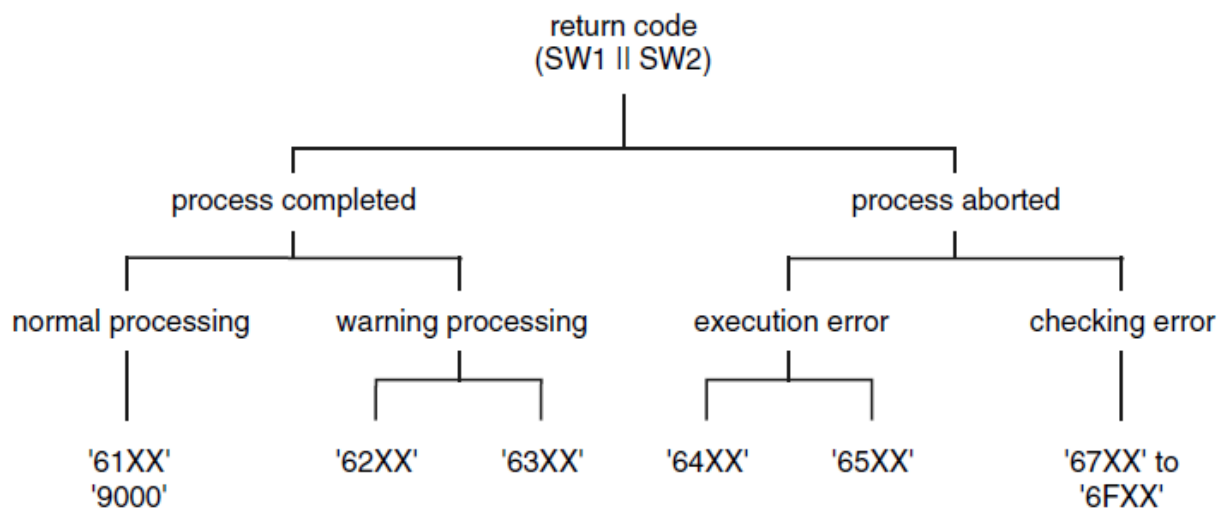


## ➤ Format des réponses APDU :

- ✓ Champ conditionnel
  - Séquences d'octets reçus dans le champ données de la réponse
- ✓ Suffixe obligatoire de deux octets d'états (status bytes) notés SW1 et SW2 qui donnent l'état de la carte après traitement de la commande.

Response APDU		
Conditional Body	Mandatory Trailer	
Data Field	SW1	SW2

## ➤ Structure générale des octets d'états SW1 SW2 :

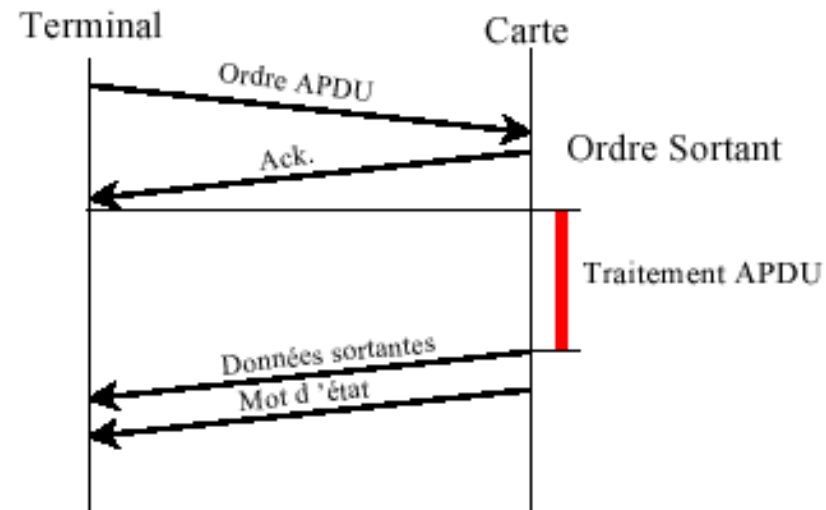


SW1 SW2	Status
0x90 0x00	OK
0x6E 0x00	CLA Error
0x6D 0x00	INS Error
0x6B 0x00	P1, P2 Error
0x67 0x00	LEN Error
0x98 0x04	Bad PIN
0x98 0x40	Card blocked

## ➤ Case 1

✓ Pas de données de commandes, Pas de données de réponse

- COMMAND: CLA INS P1 P2
- RESPONSE: SW1 SW2



## ➤ Case 2 : Commande sortante

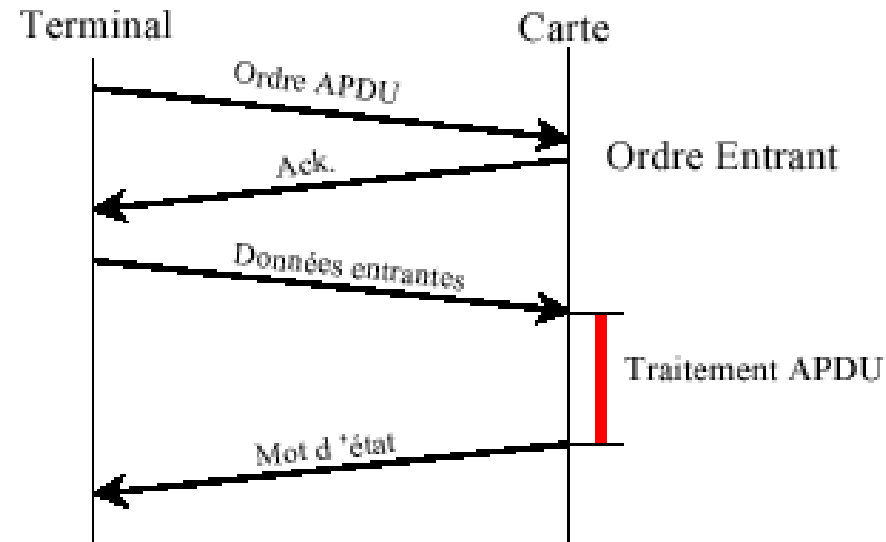
✓ Pas de données de commandes, données de réponse envoyées

- COMMAND: CLA INS P1 P2 Le
- RESPONSE: Data (jusqu'à Le octets) SW1 SW2

## ➤ Case 3 : Commande entrante

- ✓ Card reçoit des données de commandes, Pas de données de réponse

- COMMAND: CLA INS P1 P2 Lc Data (exactement Lc octets)
- RESPONSE: SW1 SW2



## ➤ Case 4

- ✓ Card reçoit des données de commandes, et envoie des données de réponse

- COMMAND: CLA INS P1 P2 Lc Data (exactement Lc octets) Le
- RESPONSE: Data (jusqu'à Le octets) SW1 SW2

- Octet *CLA* : indique la structure et le format pour une catégorie de commandes et de réponses APDU
  - ✓ Quelques exemples d'applications définis dans les doc. Normatifs (Normes 7816 - 3/4/7/8)
    - BC = carte de crédit françaises, cartes vitales française
    - A0 = cartes SIM
    - 00 = cartes Monéo (porte monnaie en France), Master Card, Visa

Class	Application
'0X'	Standard commands compliant with ISO/IEC 7816-4/7/8
'80'	Electronic purses compliant with EN 1546-3
'8X'	Application-specific and company-specific commands (private use)
'8X'	Credit cards with chips, compliant with EMV
'A0'	GSM mobile telecommunication systems compliant with GSM 11.11



- Octet INS : spécifie l'instruction de la commande
- Quelques exemples :
  - ✓ 20 = vérification du PIN
  - ✓ B0 = Lecture
  - ✓ D0 = Ecriture
  - ✓ A4 = Sélection du répertoire (Directory)
  - ✓ C0 = Demander une réponse

## ➤ Octets de procédure:

- ✓ Lorsque la carte reçoit les 5 octets de command header, elle retourne un ACK (acknowledgement) dans la forme d'un octet de procédure décrit dans le tableau suivant.
- ✓ L'octet NULL demande de réarmer la temporisation WT (« je suis encore là »). WT est indiquée en réponse à la RAZ.
- ✓ SW2 suit toujours SW1
- ✓ Si Commande rejetée, SW1 est envoyé au lieu de ACK

Nom	Valeur	Signification
ACK	INS	Transmettre les data
	INS $\oplus$ 'FF'	Transmettre l'octet suivant
	INS $\oplus$ '01'	Transmettre les data, activer VPP(Obsolète)
	INS $\oplus$ 'FE'	Transmettre l'octet suivant , activer Vpp (Obsolète)
NULL	'60'	Relancer la temporisation
SW1	'6X'	(pour X>0) SW2 suit
	'67'	P3 incorrect
	'6B'	P1 et/ou P2 incorrect(s)
	'6D'	INS inconnu ou invalide
	'6E'	CLA non supporté
	'6F'	Erreur non précisée
	'9X'	SW2

- Protocole par blocs
  - ✓ Détection d'erreur par checksum
  - ✓ Correction par répétition de blocs numérotés.
  - ✓ Chaînage qui permet de fragmenter l'APDU entre plusieurs blocs successifs
- Le premier bloc est envoyé par le lecteur et le suivant par la carte
- Chaque bloc commence par un champ obligatoire :
  - ✓ Prologue field
  - ✓ Data
  - ✓ Champ de contrôle

prologue field			information field	epilogue field
node address NAD	protocol control byte PCB	length LEN	APDU	EDC
1 byte	1 byte	1 byte	0 ... 254 bytes	1 ... 2 bytes

## ➤ format :

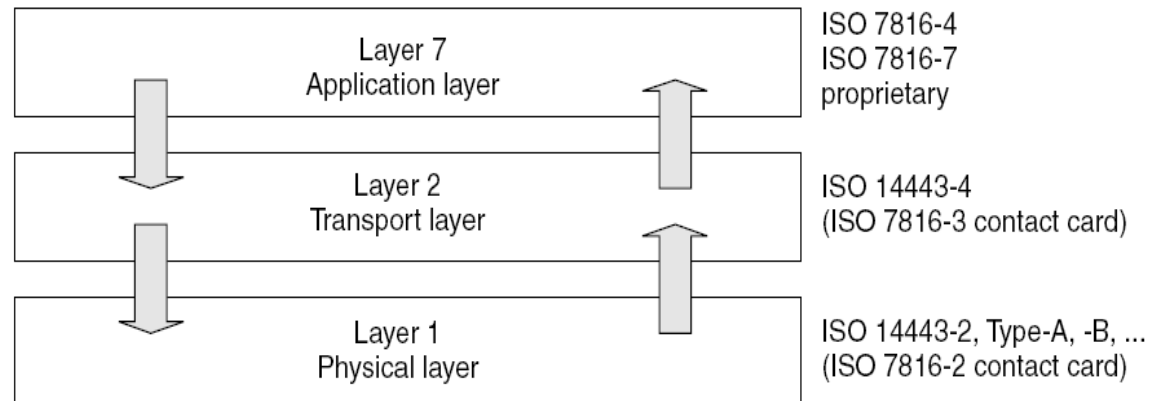
- ✓ NAD = adresse du destinataire, adresse sources
- ✓ PCB = type de trame encapsulée et chainage des trames
- ✓ LEN = longueur des données encapsulées (0 à 254 octets)
- ✓ INF = données : APDU ou autre
- ✓ EDC = contrôle d'erreur sur toute la trame : en général LRC (XOR de tous les octets le précédant)

## ➤ Le protocole définit trois types de blocs

- ✓ Bloc d'Information (I-Block) : transport de l'information pour être utilisée dans la couche applicative.
- ✓ Bloc de Réception (R-Block) : transport l'acquittement positif ou négatif. (le champ INF est absent)
- ✓ Bloc de Supervision (S-Block) : échange l'information de contrôle entre le lecteur et la carte (WTX, DESELECT).

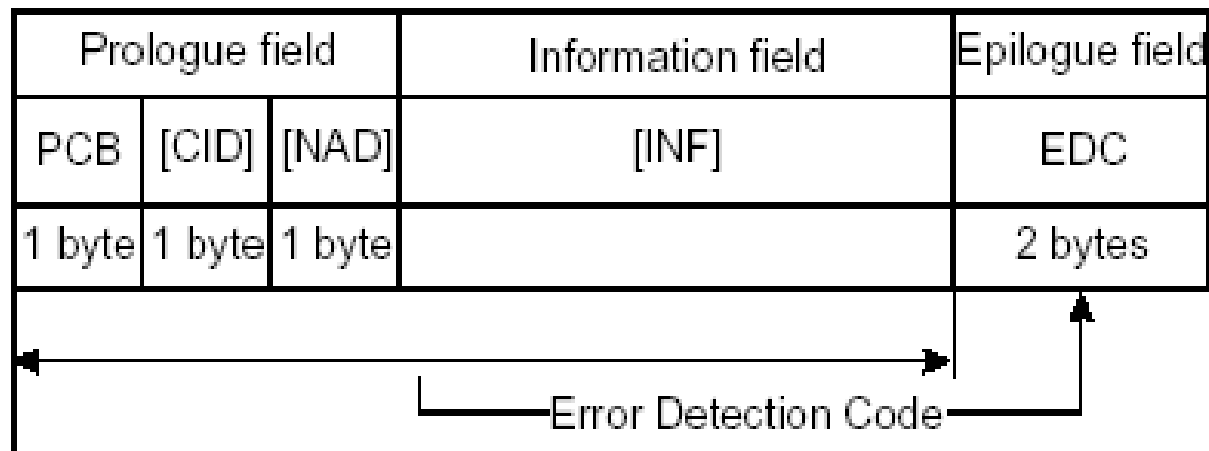
# Protocole T = CL (1/4)

- Protocole utilisé pour les cartes à puce sans contact.
- Structure du protocole basé sur celui de T = 1 (ISO 7816-3) des cartes à puce à contact.
  - ✓ Défini dans la norme ISO 14443-4
  - ✓ N'est pas utilisé dans les technologies propriétaires (Mifare, Felica, etc.)
- Pour faciliter l'intégration du protocole dans l'OS des cartes à puce, en particulier celle duales, on définit un protocole T = CL.



- La transmission des données des cartes ISO 14443 peut être représentée suivant le modèle des couches OSI
- La structure des données utilisées dans la couche applicative est identique à celles des cartes à contacts.
  - ✓ Les données de la couche applicative sont encapsulées dans les trames du protocole de la couche transport
- Les couches 3 et 6, utilisées pour les réseaux complexes pour déterminer et acheminer les paquets de données, ne sont pas utilisées ici.

# Protocole T = CL (3/4)



## ➤ Format :

### ✓ Prologue

- PCB : Protocol Control Bytes (Obligatoire)
- CID : Card Identifier (Optionel)
- NAD : Node Address (Optionel)

✓ INF : INFormation field, (APDU ou autre commande propriétaire), (Optionel)

✓ EDC: Epilogue field, CRC A or B, contrôle d'erreur sur toute la trame (Obligatoire)

- Le champs PCB

Bit	I-block PCB	R-block PCB	S-block PCB	
			DESELECT	WTX
b8	0	1	1	1
b7	0	0	1	1
b6	0 (1 is RFU)	1	0	1
b5	1 = chaining	0 = ACK, 1 = NAK	0	1
b4	1 = CID follows	1 = CID follows	1 = CID follows	
b3	1 = NAD follows	0 (no NAD)	0 (no NAD)	
b2	1	1 (0 is RFU)	1 (0 is RFU)	
b1	block number	block number	0 (1 is RFU)	



- Qu'est ce que la RFID ?
- Un peu d'histoire...
- Carte à puces sans contact
- Classification & état de l'art de la RFID
- Panorama de la standardisation
- Introduction aux cartes à puce sans contact
  - Caractéristiques Physiques
  - Modes de communications
  - Initialisation et Anticollisions
  - Protocoles de transmission

---

# Module III

## Techno Mifare

### Cartes & Lecteurs

- Architecture et fonctionnement d'une carte
- Organisation Mémoire
- Gestion de la sécurité
- Architecture du lecteur
- Jeux de commandes
- Application Porte Monnaie
- Application code PIN Embarqué

## ➤ S. ELRHARBI

- ✓ [elrharbi@telecom-paristech.fr](mailto:elrharbi@telecom-paristech.fr)
- ✓ INFRES - 2010
- ✓ ELECINF 359

## ➤ J. LEROUX

- [leroux@enst.fr](mailto:leroux@enst.fr)
- INF 359

## ➤ A. RAMARAMI

- ✓ IT Security Architect
- ✓ Capgemini ESEC, Paris, France
- ✓ CEO of CryptoDisk, Boston USA