

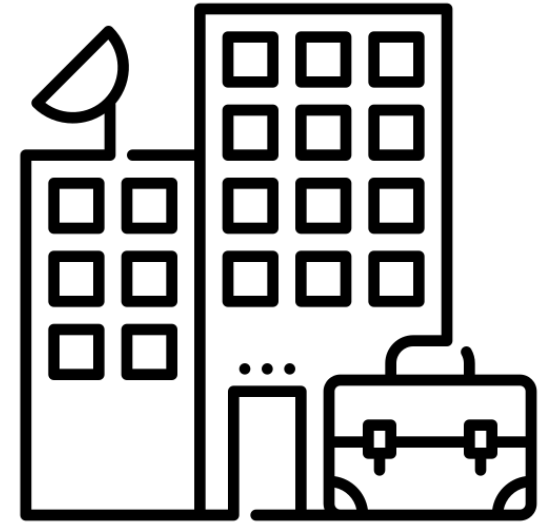
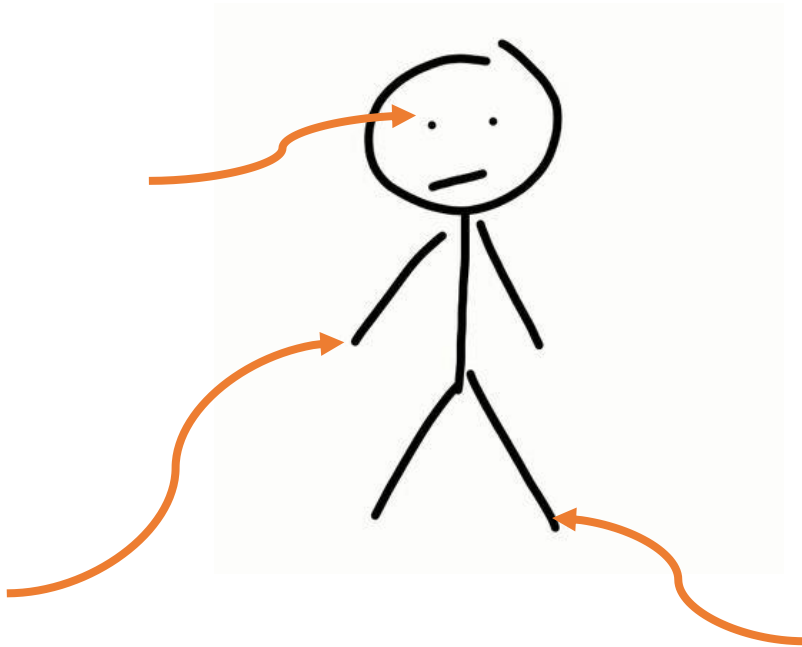
RFID — Les cartes sans contact

Présentation de la techno RF et différents attaques + DEMO

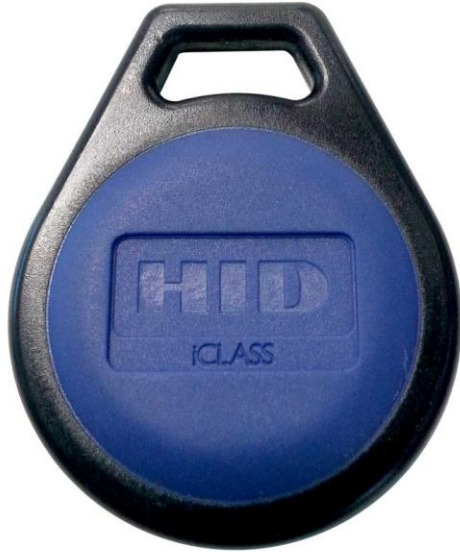
Au Menu

- Introduction « accès RF »
 - Histoire et culture
 - Les différents TAGs
 - Les accès RF
 - En quelques « mots »
 - La conception basique d'une carte RFID
- Comment attaquer ces accès RF
 - Les attaques

Quels sont les services ?



Les TAGs et technologies

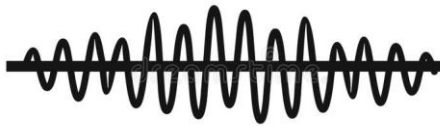


Les domaines de fréquences

- Bases fréquences ou **LF** ($\leq 135\text{KHz}$) – **ISO 14223/1, 18000-2**
- Radio fréquences ou **HF** (fréquences autour de 13,56 MHz) – **ISO 14443, 15693, 18000-3**
- Ultra-hautes fréquences ou **UHF** (de 869-915 MHz) – **ISO 18000-6**
- Micro-ondes ($\sim 2,45\text{ GHz}$) – **ISO 18000-4**

En quelques « mots »:

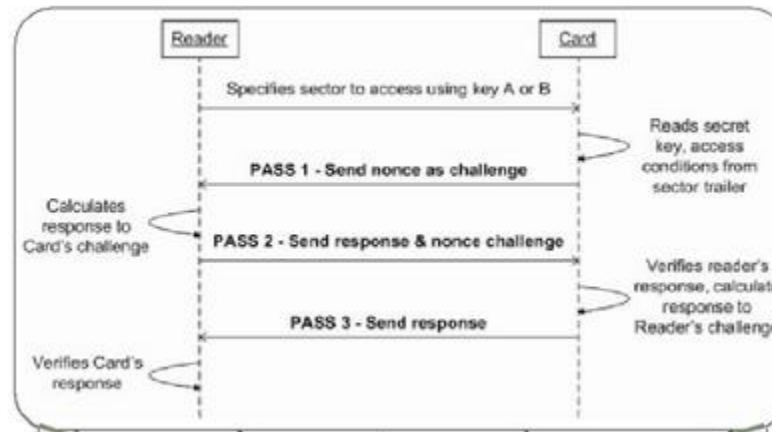
Physique: les signaux



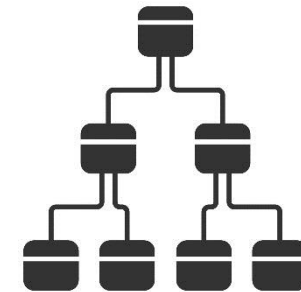
Les données

00101011
01101010
101110101
11011000
10100110

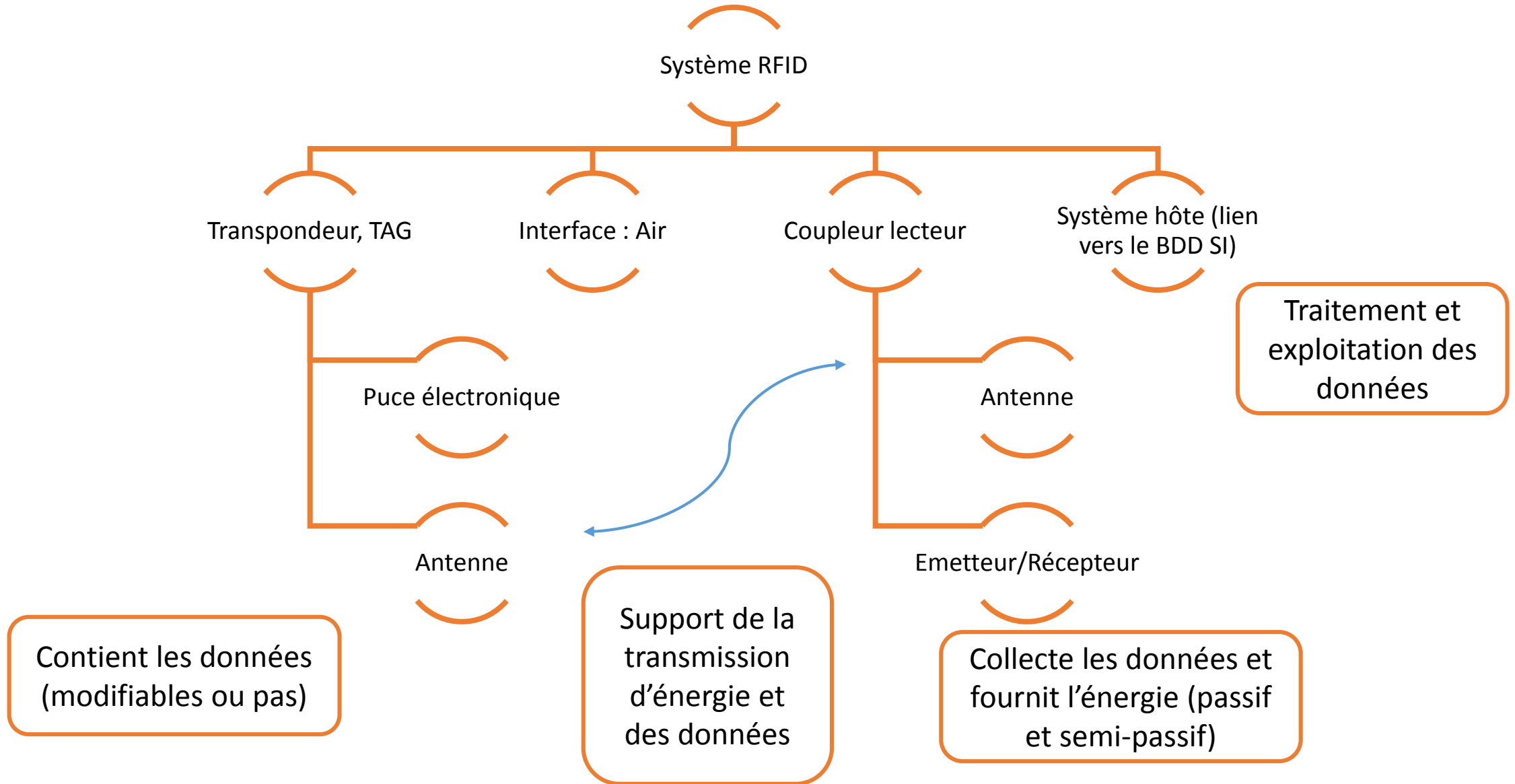
Le protocole



Le système RFID



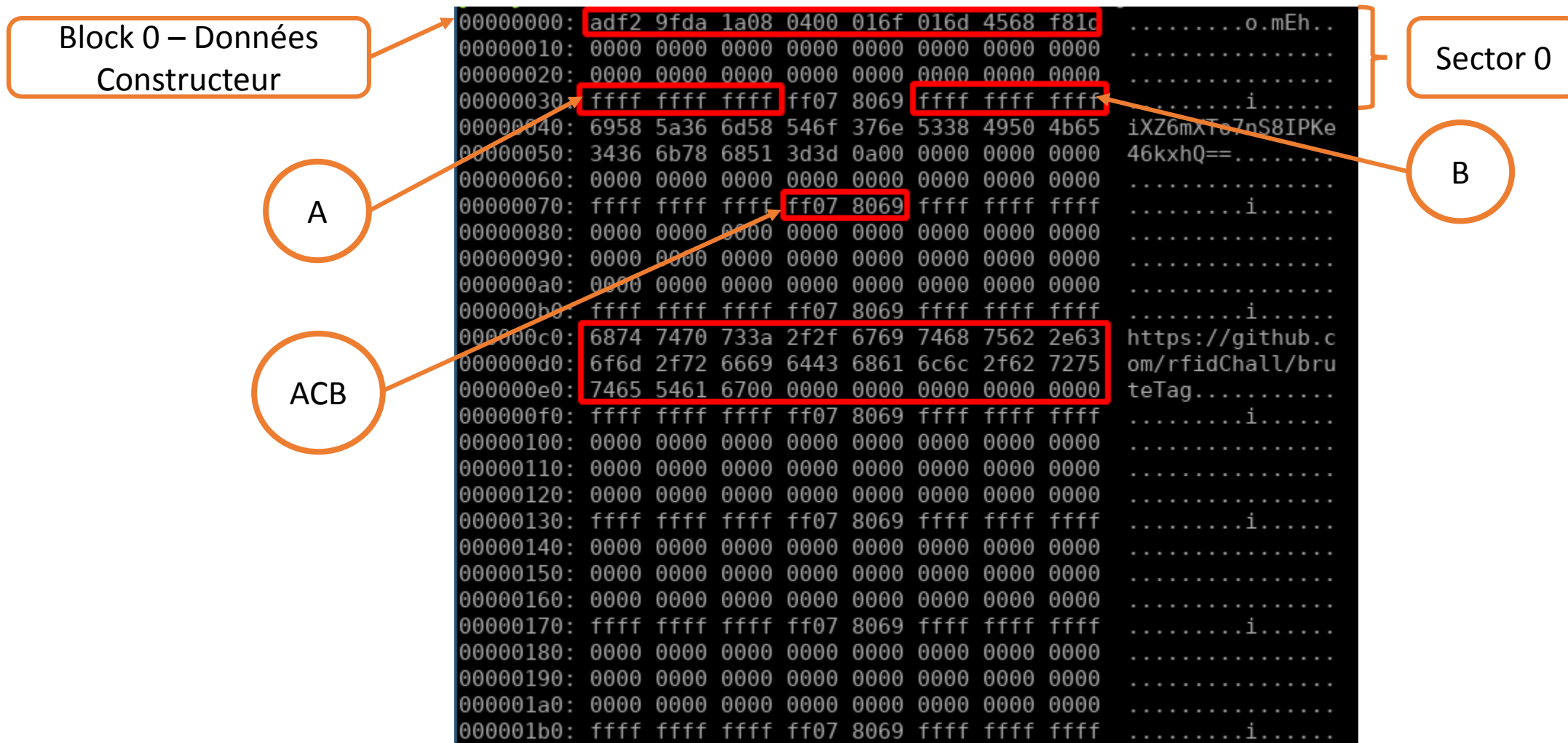
Le système RFID



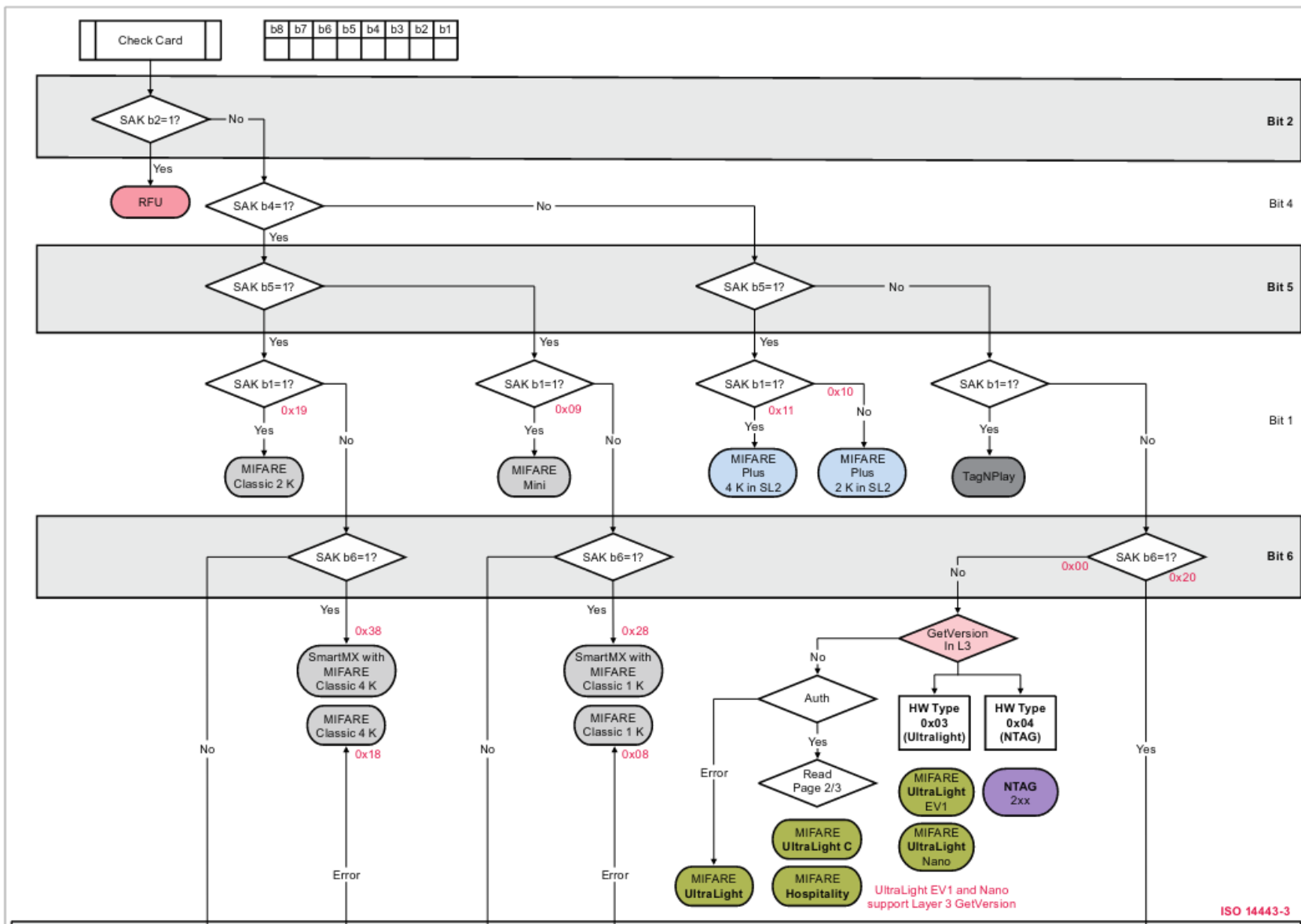
Conception basique d'une carte RFID

- Puce à lecture seule:
 - La puce électronique peut ne contenir qu'un numéro unique gravé par le fondeur de la puce lors de la fabrication (TID Tag Identifier). Si la puce ne possède pas d'autre zone mémoire, on parle de puce en lecture seule.
 - Le TID sert à indexer des informations déportées sur un serveur.
- Puces **WORM** (Write Once, Read Multiple)
 - La puce peut aussi posséder une zone mémoire vierge sur laquelle on peut écrire un numéro (UII Unique Item Identifier ou Code EPC Electronic Product Code par exemple). Ce numéro une fois écrit n'est plus modifiable.
- Puces **MTP** (Multi Time Programmable)
 - Certaines applications nécessitent l'utilisation de tags avec mémoire réinscriptible (**EEPROM**).

La mémoire embarquée d'un TAG



Identification du TAG



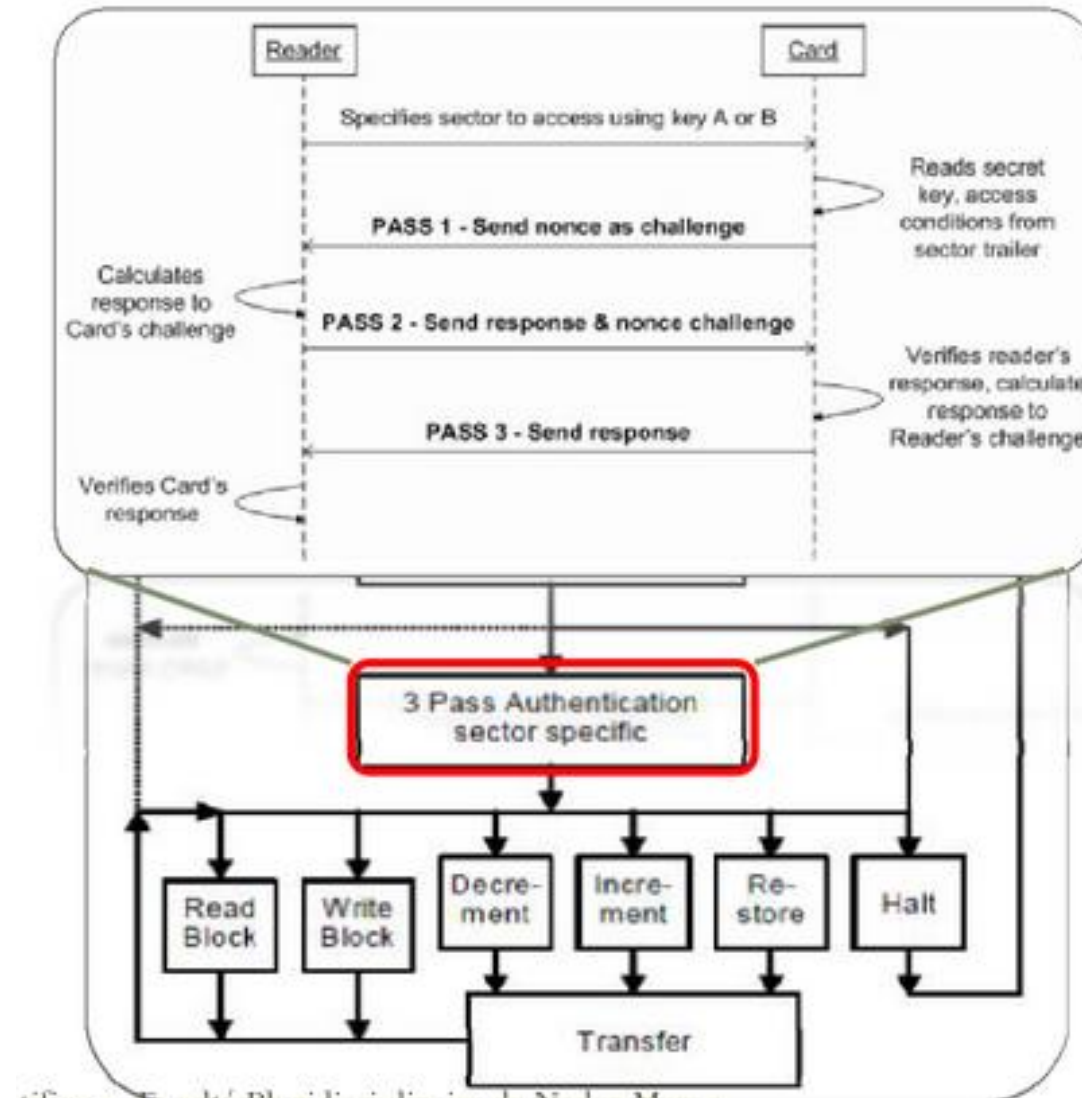
Commandes Mifare

- **Authentication**

- **AUT**<SPACE>**DRT**<SPACE>**FFFFFFFFFFFF**<SPACE>**B**<SPACE>**8**<CR>

- DRT: Authentication mode Direct
 - Key
 - Type
 - Block

Protocole



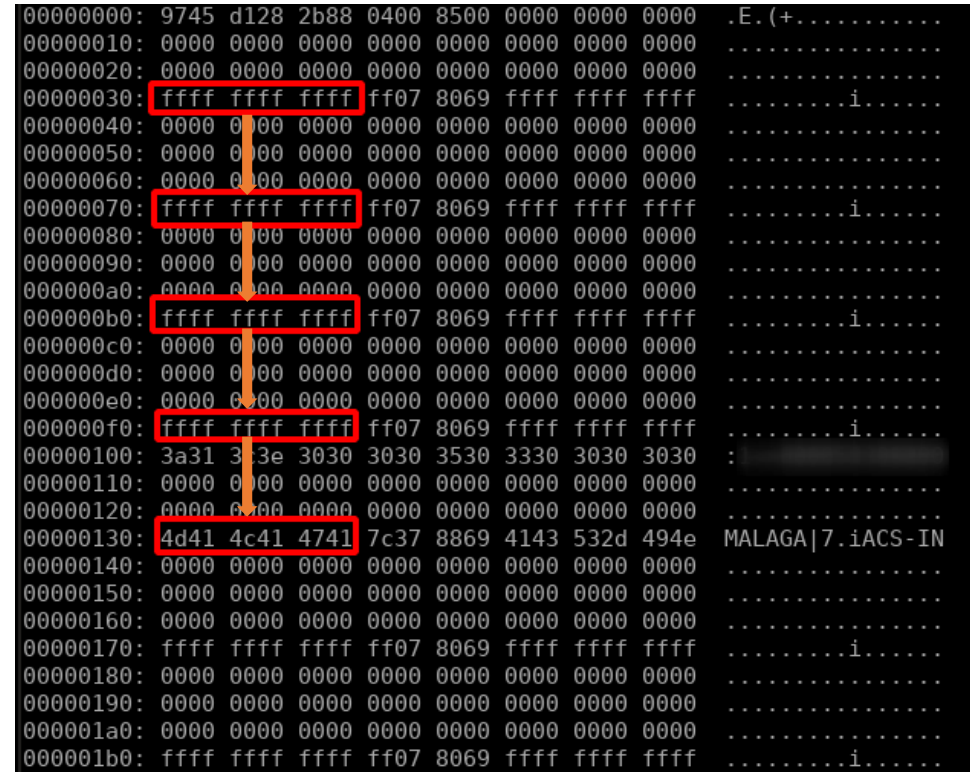
Attaques

- **Darkside Attack:**

- Analyse la **réaction** d'une carte à des messages avec des **mauvaises bits de parité**.
- Réaction: **Erreur** ou **non réponse**.

Attaques

- **Nested Attack:**
 - La **dérivation** des clés par **sector**.



```
00000000: 9745 d128 2b88 0400 8500 0000 0000 0000 .E.(+.....
00000010: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000020: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000030: ffff ffff ffff ff07 8069 ffff ffff ffff .....i.....
00000040: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000060: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000070: ffff ffff ffff ff07 8069 ffff ffff ffff .....i.....
00000080: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000090: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000b0: ffff ffff ffff ff07 8069 ffff ffff ffff .....i.....
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000f0: ffff ffff ffff ff07 8069 ffff ffff ffff .....i.....
00000100: 3a31 3e3e 3030 3030 3530 3330 3030 3030 :
00000110: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000120: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000130: 4d41 4c41 4741 7c37 8869 4143 532d 494e MALAGA|7.iACS-IN
00000140: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000150: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000160: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000170: ffff ffff ffff ff07 8069 ffff ffff ffff .....i.....
00000180: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000190: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000001b0: ffff ffff ffff ff07 8069 ffff ffff ffff .....i.....
```

Plus d'information:

- <https://www.nxp.com/docs/en/application-note/AN10833.pdf>
- <https://github.com/RfidResearchGroup/proxmark3>

Merci !!!

Juan Pablo BARRIGA

juanpablo.becerrabarriga@orange cyberdefense.com