

# Labo SSI

Recherche sur la technologie RFID :



|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 1  |

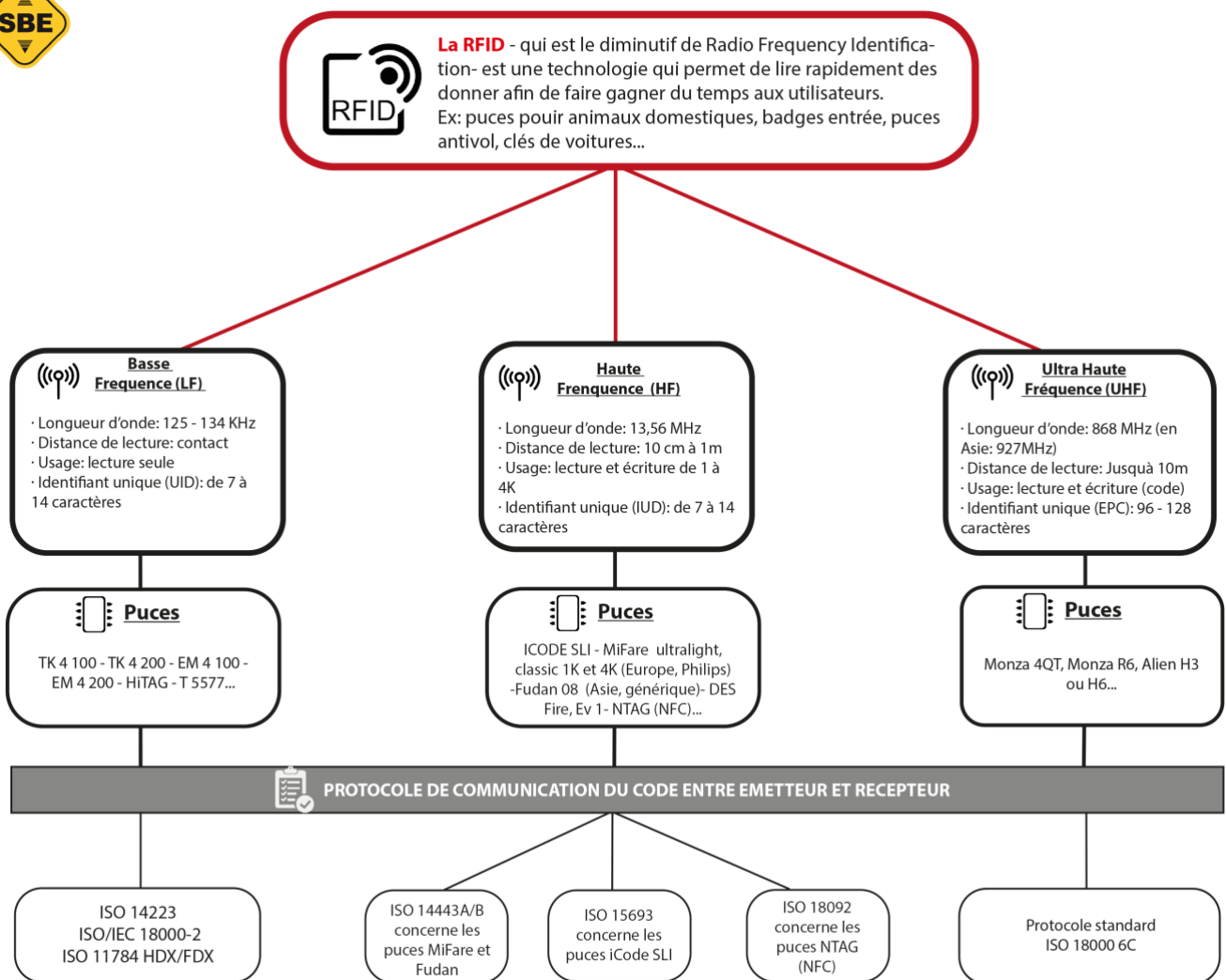
## Sommaire :

|            |   |           |
|------------|---|-----------|
| <b>1.</b>  | <b><i>Introduction :</i></b>  | <b>3</b>  |
| <b>2.</b>  | <b><i>Qu'est-ce que la technologie RFID</i></b>   | <b>4</b>  |
| <b>2.1</b> | <b><i>Quelles sont les différents types d'utilisation de la technologie RFID ?</i></b>          | <b>5</b>  |
| <b>2.2</b> | <b><i>Comment fonctionne-t-elle ?</i></b>   | <b>6</b>  |
| <b>2.3</b> | <b><i>Quels sont les différentes fréquences utilisées pour la RFID ?</i></b>                    | <b>7</b>  |
| <b>2.4</b> | <b><i>Les différents types de puce RFID ?</i></b>   | <b>9</b>  |
| <b>2.5</b> | <b><i>Comment est géré stockage sur les tags ?</i></b>  | <b>10</b> |
| <b>2.6</b> | <b><i>Les puces les plus utilisé ainsi que les autres puces disponibles sur le marché ?</i></b> | <b>11</b> |
| <b>2.7</b> | <b><i>Quels sont les sécurités mise en place ?</i></b>  | <b>13</b> |
| <b>3.</b>  | <b><i>Comment récupérer les informations d'un badge ?</i></b>                                   | <b>14</b> |
| <b>3.1</b> | <b><i>Comment dupliquer un badge ?</i></b>  | <b>15</b> |
| <b>3.2</b> | <b><i>Comment modifier un badge ?</i></b>   | <b>16</b> |
| <b>4.</b>  | <b><i>Annexe :</i></b>  | <b>17</b> |

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 2  |

## 1. Introduction :

Nous avons effectué un travail de recherche sur la technologie RFID et ses systèmes de sécurité. Nous aborderons les points suivants : la fréquence utilisée, son fonctionnement, les différents types de puces. Voici un schéma explicatif qui regroupe les principales informations que nous avons pu trouver en ligne sur cette technologie.



sbedirect.com

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 3  |

## 2. Qu'est-ce que la technologie RFID

La technologie RFID (Radio-Frequency Identification) est une méthode de communication sans fil qui permet l'identification et le suivi d'objets, d'animaux ou de personnes à l'aide d'étiquettes RFID.

Ces étiquettes contiennent des puces électroniques et des antennes qui émettent des signaux radiofréquences pour communiquer avec un lecteur RFID.

La technologie RFID joue un rôle crucial dans la concrétisation de l'Internet des Objets (IoT), facilitant la connexion entre les objets de manière aisée et sécurisée.

La technologie RFID peut être expliquée en deux composantes principales : les étiquettes RFID et les lecteurs RFID.

Les étiquettes RFID, également appelées transpondeurs, sont équipées d'une puce électronique et d'une antenne. Ces étiquettes émettent des signaux radiofréquences lorsqu'elles entrent en contact avec un lecteur RFID.

Les lecteurs RFID, quant à eux, émettent des signaux radiofréquences pour interroger et recevoir des données des étiquettes à proximité.

Le spectre de fonctionnement de la RFID comprend différentes fréquences radio, avec des fréquences basses, hautes et ultra-hautes. Chaque fréquence a ses propres caractéristiques et applications spécifiques.

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 4  |

## 2.1 Quelles sont les différents types d'utilisation de la technologie RFID ?

Plusieurs fabricants se partagent le marché et proposent **des puces de plus en plus performantes**. Cette technologie est aujourd'hui standardisée et présente dans beaucoup d'objets du quotidien.

Cartes RFID et badges RFID :

- Identification des personnes
- Contrôle d'accès en entreprise
- Transports Cartes de fidélité

Étiquette PVC sans contact RFID :

- Identification & traçabilité
- 3 formats d'étiquettes RFID normes ISO
- Une technologie RFID performante et abordable
- 4 types de puces RFID disponibles

Étiquettes et stickers :

- Identification des biens
- Stockage et inventaire
- Lutte contre la contrefaçon
- Traçabilité des produits
- Promotion dans les événements

Bracelets :

- Identification des personnes
- Paiement sans contact
- Promotion dans les événements

Porte-clés et tags :

- Accès à des résidences, locaux et parking
- Badge RFID d'accès en entreprise

Puces sous-cutanées :

- Identification d'animaux

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 5  |

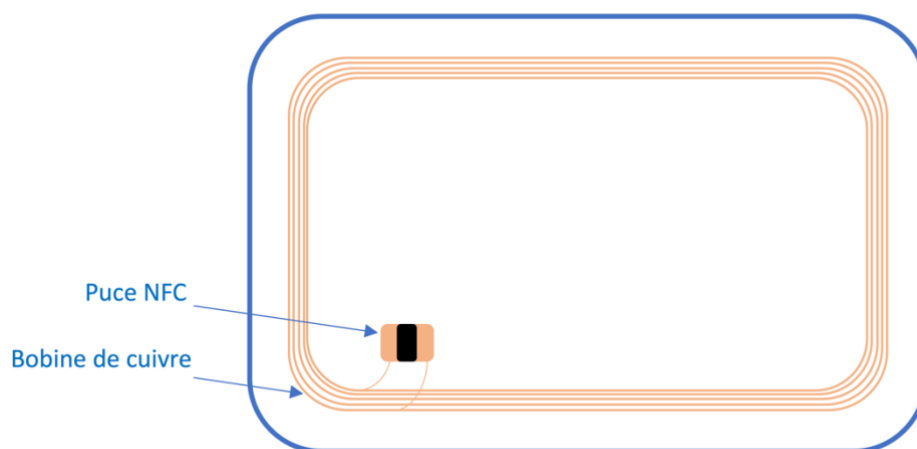
## 2.2 Comment fonctionne-t-elle ?

Un badge RFID est généralement constitué de deux composants principaux : la puce RFID et l'antenne. Voici une description de ces composants :

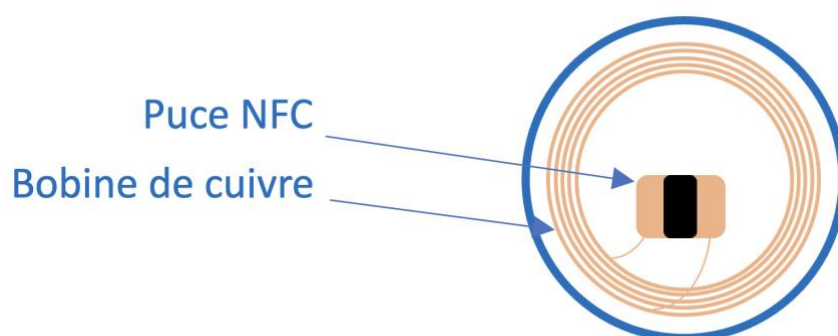
- L'antenne RFID est un composant essentiel du système. Elle est généralement constituée d'un fil conducteur, souvent en cuivre, qui est enroulé de manière spécifique pour former une bobine. La forme de l'antenne dépend de la fréquence à laquelle le système RFID fonctionne.
- La puce RFID est le cerveau du badge. Elle contient des informations spécifiques telles qu'un identifiant unique, des données d'authentification, des numéros de série, etc. La puce peut être de type passif (n'ayant pas de source d'alimentation propre, mais plutôt alimentée par l'énergie du champ radio émis par le lecteur RFID) ou active (dotée de sa propre source d'alimentation, généralement une petite batterie).

Voilà des schémas qui représente la constitution d'un badge :

Badge rectangulaire :



Badge rond ou étiquette :



|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 6  |

## 2.3 Quels sont les différentes fréquences utilisées pour la RFID ?

La **fréquence est la caractéristique qui permet d'établir la communication** entre la puce et l'antenne.

Toutes les puces sur le marché n'ont donc pas la même fonctionnalité.

Les puces se différencient en grande partie par la fréquence de fonctionnement et la distance de lecture.

Plus la fréquence est élevée, plus la distance de lecture s'agrandit. En fonction de ces éléments, la puce sera plus ou moins puissante et plus onéreuse.

Trois types de fréquences sont utilisés pour les puces RFID :

- Basse fréquence (125Khz),
- Haute (13,56 Mhz)
- Très haute fréquence (UHF).

| Types de fréquence   | Fréquence de fonctionnement | Distance de lecture (m) | Taux de transfert | Normes                          |
|----------------------|-----------------------------|-------------------------|-------------------|---------------------------------|
| Basse fréquence      | < 135 kHz                   | 0.5                     | 1kb/s             | ISO 142231 ISO 18000-2          |
| Haute fréquence      | 13,56 Mhz                   | 1                       | 25kb/s            | ISO 14443 ISO 15693 ISO 18000-3 |
| Très haute fréquence | 863 à 915 Mhz               | 3 à 6                   | 28kb/s            | ISO 18000-6                     |

Tableau des différentes fréquences utilisé pour la technologie RFID

RFID LF (Basse Fréquence) :

- Contrôle d'accès : Utilisée pour les clés de voiture sans contact et les badges d'entrée, garantissant un accès sécurisé et pratique.
- Suivi des animaux : Employée pour identifier et suivre les animaux domestiques ou de ferme, essentiel pour la gestion vétérinaire.
- Applications médicales : Utilisée pour le suivi des instruments chirurgicaux, améliorant la sécurité et l'hygiène médicale.

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 7  |

#### RFID HF (Haute Fréquence) :

- Paiements mobiles et billetterie électronique : La technologie NFC facilite les transactions sans contact et la gestion de billetterie électronique.
- Bibliothèques et documentation : Idéale pour le suivi des livres et documents, automatisant les prêts et retours.
- Gestion des dossiers médicaux : Suivi des dossiers médicaux et gestion des médicaments dans les hôpitaux.
- Contrôle d'accès : Utilisée pour les badges d'identité dans les entreprises, similaire à la RFID LF mais sur une plus grande échelle.

#### RFID UHF (Ultra-Haute Fréquence) :

- Commerce de détail : Gère les inventaires en suivant les articles dans les magasins ou entre les sites.
- Logistique : Facilite le suivi des cargaisons en temps réel, de l'usine à la livraison.
- Fabrication : Suivi des produits en production, optimisant les opérations et minimisant les interruptions.

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 8  |



## 2.4 Les différents types de puce RFID ?

Les puces RFID peuvent être classé dans différentes classes :

| Classe                           | Tag           | Fonction   | Avantages / inconvénients   |
|----------------------------------|---------------|--|---|
| <b>Classe0</b><br><b>Classe1</b> | Passif        | Lecture de l'identifiant unique  | Moins onéreux que les tags actifs, utiles pour un gros volume de marchandises à lire à courte distance. Cependant, la distance de lecture est aussi un frein car le lecteur doit être à proximité.                                    |
| <b>Classe2</b>                   | Passif        | Fonctions additionnelles : lecture, écriture avec mémoire                      |   |
| <b>Classe3</b>                   | Semi-passif   | Tags assistés par une batterie   | Plus performant et moins onéreux que la RFID active. En revanche, l'incertitude repose sur la fiabilité en cas de traçabilité.  |
| <b>Classe4</b>                   | Actif         | Communication sans transiter par un serveur central                            | Technologie autonome grâce à son énergie propre, ce qui permet une lecture à longue distance. Les inconvénients sont : le coût des étiquettes et leur durée limitée, la faible sécurité des ondes émises et leur impact sur la santé. |
| <b>Classe5</b>                   | Interrogateur | Alimentent les tags de classe 0 à 3 et communiquent avec les tags de classe 4. |   |

Tableau des différents types de puce RFID

Exemple concret du mode passif de la RFID :

*Une étiquette RFID est attachée à un produit en magasin. Lorsque cette étiquette entre en contact avec un lecteur RFID à la caisse, le lecteur génère un champ électromagnétique qui alimente l'étiquette en énergie. L'étiquette répond ensuite en transmettant les informations stockées sur la puce au lecteur RFID, permettant ainsi la lecture rapide et efficace des données du produit lors du processus d'achat.*

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 9  |

## 2.5 Comment est géré stockage sur les tags ?

| Mifare Mapping |              |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|----------------|--------------|-------|------|------|------|-------------------|---|---|---|-----------|---|----|----|----|----|
| Sector 0       | block 0      |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         | UID0  | UID1 | UID2 | UID3 | Manufacturer DATA |   |   |   |           |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 1       | block 1      |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 1       | block 2      |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 1       | block 3      |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         | KEY A |      |      |      | ACCESS BITS       |   |   |   | USER DATA |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 14      | block 4      |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 14      | block 5      |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 14      | block 6      |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 14      | block 7      |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         | KEY A |      |      |      | ACCESS BITS       |   |   |   | USER DATA |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 14      | block 56     |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 14      | block 57     |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 14      | block 58     |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 14      | block 59     |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         | KEY A |      |      |      | ACCESS BITS       |   |   |   | USER DATA |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 15      | block 60     |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 15      | block 61     |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 15      | block 62     |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |
| Sector 15      | block 63     |       |      |      |      |                   |   |   |   |           |   |    |    |    |    |
|                | Byte number  | 0     | 1    | 2    | 3    | 4                 | 5 | 6 | 7 | 8         | 9 | 10 | 11 | 12 | 13 |
|                | Name         | KEY A |      |      |      | ACCESS BITS       |   |   |   | USER DATA |   |    |    |    |    |
|                | Value (HEXA) | 0     | 0    | 0    | 0    | 0                 | 0 | 0 | 0 | 0         | 0 | 0  | 0  | 0  | 0  |

La carte MIFARE Classic est divisée en secteurs, chacun contenant 4 blocs de données. Chaque bloc de données peut contenir jusqu'à 16 octets de données. La carte a un total de 16 secteurs, ce qui donne une capacité de stockage maximale de 640 octets.

Le mappage de la mémoire de la carte MIFARE Classic est le suivant :

Secteur 0, bloc 0 : Contient l'identifiant unique de la carte (UID). L'UID est une chaîne de 4 octets qui identifie de manière unique la carte.

Secteur 0, bloc 1 à 3 : Non utilisés.

Secteur 1 à 15, bloc 0 : Contiennent une clé de sécurité. Les clés de sécurité sont utilisées pour protéger les données stockées sur la carte.

Secteur 1 à 15, bloc 1 à 3 : Contient des données d'utilisateur. Les données d'utilisateur sont des données personnalisées qui peuvent être stockées sur la carte par l'utilisateur.

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 10 |

## 2.6 Les puces les plus utilisées ainsi que les autres puces disponibles sur le marché ?

Les badges les plus utilisés sont les badges MIFARE, c'est la technologie de carte à puce sans contact la plus répandue dans le monde. Ils sont fabriqués sur la base d'un composant fourni par la société NXP. Le MIFARE est le standard de la carte RFID.

| Type                      | Fréquence | Stockage                                | Caractéristiques   |
|---------------------------|-----------|---|--|
| <b>Mifare Ultralight</b>  | 13,56 Mhz | 512 bits<br>(64 octets = 64 caractères) | Lecture seule. Pas de bloc de sécurité comme dans le MIFARE Classic. Utilisé principalement pour les tickets jetables.<br><b>Classe 0/1</b>  |
| <b>Mifare classic 1K</b>  | 13,56 Mhz | 768 octets (768 car.)                   | Bloc de sécurité. Possibilité de lire ou écrire des données mais aussi d'incrémenter ou de décrémenter des valeurs. Distance d'écriture de 10 cm. Première version du MIFARE.  |
| <b>Mifare classic 4K</b>  | 13,56 Mhz | 4 ko (4096 car.)                        | Bloc de sécurité. Possibilité de lire ou écrire des données mais aussi d'incrémenter ou de décrémenter des valeurs. Distance d'écriture de 10 cm.<br><b>Classe 2</b>   |
| <b>Mifare DESFire Ev1</b> | 13,56 Mhz | 2ko, 4ko ou 8ko                         | Transmission de données sans contact sans besoin d'énergie ni de batterie. Cette puce dispose d'un plus haut niveau de sécurité par rapport aux autres. La carte embarque 28 applications dont chacune supporte 32 fichiers. La taille de chaque fichier est définie au moment de la création. Produit pratique et flexible. |

Tableau des différents types de puce Mifare

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 11 |

Et voici d'autres puces disponibles sur le marché :

| Fréquence      | Type de puce                 | Caractéristiques  |
|----------------|------------------------------|---|
| <b>125 KHz</b> | EM 4200 (EM Microelectronic) | 128 bits en lecture seule, basse fréquence sans contact avec dispositif d'identification. Elle vient remplacer petit à petit EM4100/4102 et EM4005/4105. Très faible consommation d'énergie et hautes performances. Classe 0/1                                |
| <b>125 KHz</b> | EM 4100 (EM Microelectronic) | 64 bits en lecture seule programmable, basse consommation. Puce de petite taille pour une meilleure implémentation. Classe 0/1  |
| <b>125 KHz</b> | T 5577 (Atmel)               | 363 bits. Puce à lecture et écriture depuis un lecteur. Classe 2  |
| <b>125 KHz</b> | HiTag (NXP)                  | De 64 bits à 2048 bits. Efficace dans la transmission de données dans des environnements complexes. Plusieurs versions, dont le HiTag S, HiTag 2 et HiTag 1. La différence se fait essentiellement dans la taille de mémoire et la fonction lecture/écriture. |

Tableau des autres puces RFID utilisés

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 12 |

## 2.7 Quels sont les sécurités mise en place ?

Les systèmes RFID sont soumis aux mêmes menaces de sécurité que les autres systèmes informatiques. Les menaces les plus courantes sont les suivantes :

- La confidentialité : les données stockées sur les tags RFID peuvent être interceptées et lues par des personnes non autorisées.
- L'intégrité : les données stockées sur les tags RFID peuvent être modifiées ou corrompues par des personnes non autorisées.
- La disponibilité : les systèmes RFID peuvent être rendus indisponibles par des attaques de déni de service.

Pour protéger les systèmes RFID contre ces menaces, plusieurs mesures de sécurité peuvent être mises en place :

- L'utilisation de clés de chiffrement : les données stockées sur les tags RFID peuvent être chiffrées pour les protéger contre l'interception.
- L'utilisation de techniques d'authentification : les lecteurs RFID peuvent être authentifiés avant qu'ils ne puissent lire ou écrire des données sur les tags RFID.
- L'utilisation de techniques de cryptage : les données stockées sur les tags RFID peuvent être cryptées pour les protéger contre la modification ou la corruption.
- La mise en place de contrôles d'accès : seuls les utilisateurs autorisés doivent avoir accès aux données stockées sur les tags RFID.

Voici quelques exemples concrets de mesures de sécurité mises en place sur les systèmes RFID :

- Dans les applications de gestion des stocks, les tags RFID peuvent être chiffrés à l'aide d'une clé de chiffrement partagée par le lecteur et le système de gestion des stocks.
- Dans les applications de contrôle d'accès, les lecteurs RFID peuvent être authentifiés à l'aide d'une carte à puce ou d'une clé USB.
- Dans les applications de traçabilité des produits, les tags RFID peuvent être cryptés à l'aide d'une clé de chiffrement unique pour chaque produit.
- La mise en place de mesures de sécurité appropriées est essentielle pour protéger les systèmes RFID contre les menaces.

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 13 |

3. Comment récupérer les informations d'un badge ?

Cette ligne de code sert à récupérer les informations d'une étiquette NFC, en forçant l'extraction des clés A et B, puis de l'enregistrer dans un fichier .dmp ou .mfd

Ici nous utilisons « mfoc-hardnested » :

- F : force the hardnested keys extraction
- O : file in which the card contents will be written



Ensuite nous pouvons utiliser soit mfdread qui est un fichier python permettant de lire les fichiers .mfd

```
$ ./mfdread.py ./dump.mfd
File size: 4096 bytes. Expected 64 sectors

UID: 33bd9d3f
BCC: 2c
SAK: 98
ATQA: 02
```

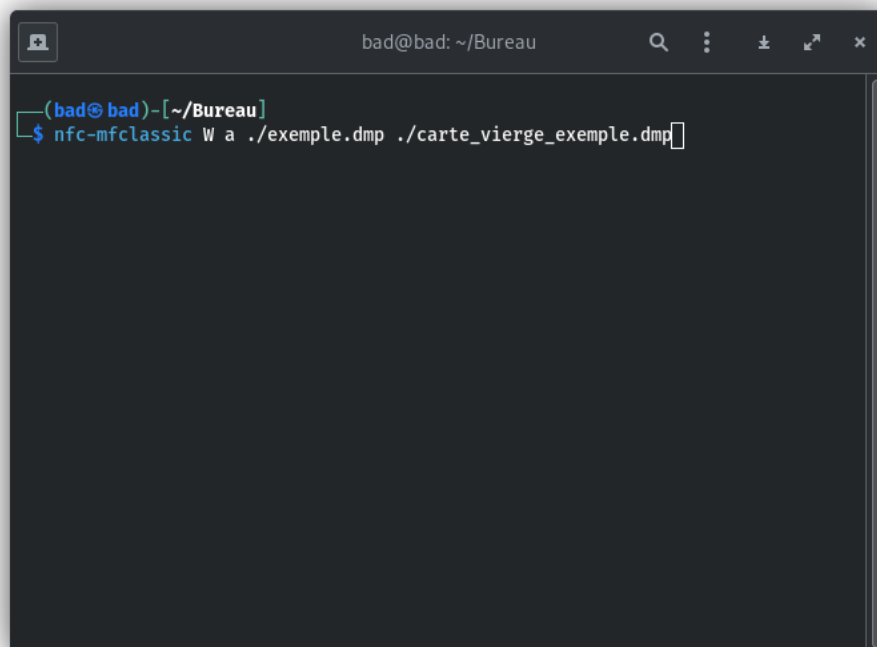
|        |       | Key A                             | Access Bits | Key B       |
|--------|-------|-----------------------------------|-------------|-------------|
| Sector | Block | Data                              |             | Access Bits |
| 0      | 0     | 33bd9d3f2c980200648f841441502212  |             | 100         |
|        | 1     | 090f1808000000000000003010000400b |             | 100         |
|        | 2     | 00000000400c400c400c400c00040005  |             | 100         |
|        | 3     | a0a1a2a3a4a5787788c17db82a7f6825  |             | 011         |
| 1      | 0     | 418d50c98d7f962462004c800000ffcc  |             | 100         |
|        | 1     | 1fa1014100d101c060000000049a2a9f  |             | 100         |
|        | 2     | 1fa1014100d101c060000000049a2a9f  |             | 100         |
|        | 3     | 2735fc18180778778800bf23a53c1f63  |             | 011         |
| 2      | 0     | 3065061730077220296012505b74c05d  |             | 100         |
|        | 1     | 68c701da24c027ece0ee9a99c0caadb1  |             | 100         |
|        | 2     | c82591842f0b8304a2a068d1f4e016e7  |             | 100         |
|        | 3     | 2aba9519f574787788ffc0ba1f2d7368  |             | 011         |
| 3      | 0     | 6c135ade77c0f7a11f09ad059d45720c  |             | 100         |
|        | 1     | 3c0dc85010e3ef723bfad584c4ad509d  |             | 100         |
|        | 2     | 040e821625f14168040ed8ee61a8f635  |             | 100         |
|        | 3     | 84fd7f7a12b6787788ffc7c0adb3284f  |             | 011         |
| 4      | 0     | 420d53f9bdc3362461004c800000bc18  |             | 100         |
|        | 1     | 1f51014100d101c09000004240280bdce |             | 100         |
|        | 2     | 1f51014100d101c09000004240280bdce |             | 100         |
|        | 3     | 73068f118c1378778800207f3253fac5  |             | 011         |
| 5      | 0     | 000000000000000000000000000000    |             | 110         |
|        | 1     | 0177000090722029653352020202020   |             | 110         |
|        | 2     | 000000000000000000000000000000    |             | 110         |
|        | 3     | 186d8c4b93f908778f02ff11108c2057  |             | 011         |

### 3.1 Comment dupliquer un badge ?

Une fois que les données du badge NFC sont stockées, il suffit de forcer l'écriture de ce badge sur un autre badge vierge, où le secteur 0 peut être modifié pour changer l'UID du badge. Il faut donc d'abord enregistrer les données du badge vierge également, pour pouvoir les comparer et les remplacer par les nouvelles données.

Ici nous utilisons « nfc-mfclassic » :

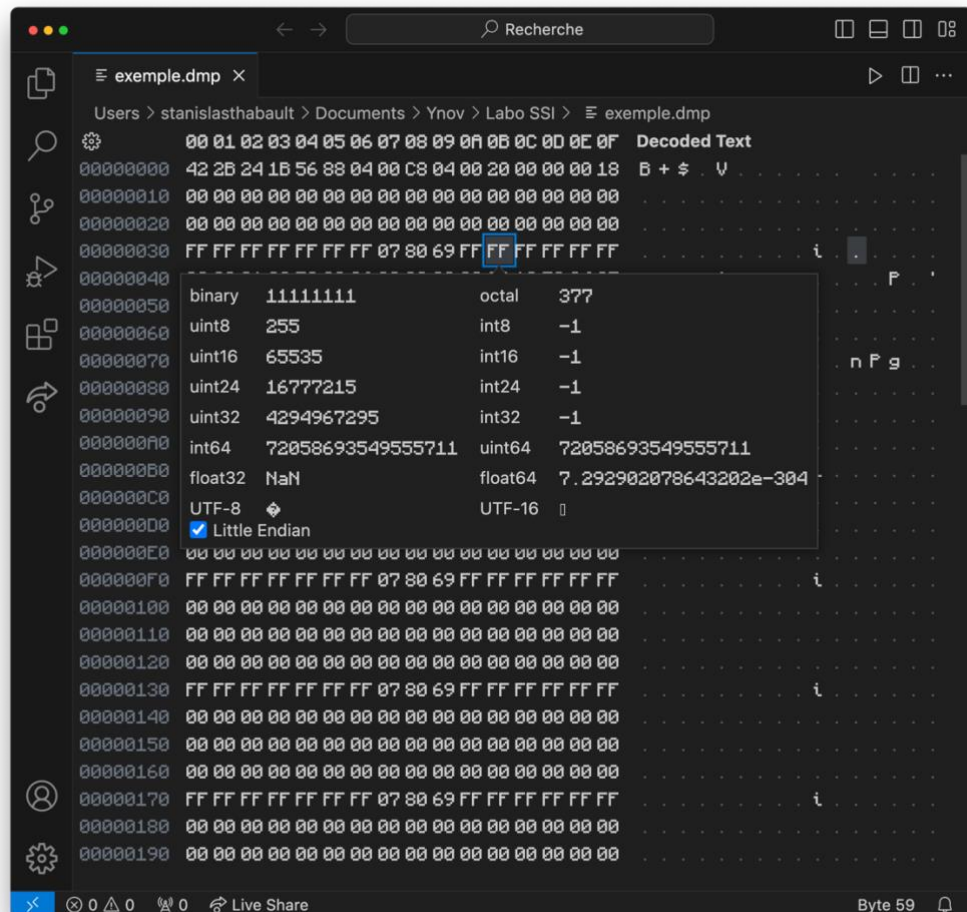
W : unlocked write to card  
a : select key a ; Halt on errors  
b : select key b ; Halt on errors

A terminal window with a dark background. The title bar shows 'bad@bad: ~/Bureau'. The prompt is '(bad@bad)-[~/Bureau]'. The command entered is '\$ nfc-mfclassic W a ./exemple.dmp ./carte\_vierge\_exemple.dmp'.

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 15 |

## 3.2 Comment modifier un badge ?

Pour modifier un badge, il suffit d'installer l'extension « Hex editor » sur Visual Studio Code et de changer les valeurs en hexadécimal.



|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 16 |



#### 4. Annexe :

<https://www.diffchecker.com/oBZz96PD/>  
<https://www.dipolerfid.fr/blog-rfid/qu-est-ce-que-nfc>  
<https://sbedirect.com/fr/blog/article/comprendre-la-rfid-en-10-points.html>  
<https://blog.androz2091.fr/copy-nfc-card/>  
<https://github.com/zhovner/mfdread>  
<https://github.com/nfc-tools/mfoc-hardnested>  
<https://github.com/nfc-tools/libnfc>

Pierre STACKE

|                                 |               |    |
|---------------------------------|---------------|----|
| Labo SSI                        | Recherche NFC | V1 |
| Tom MALLOR & Stanislas THABAULT | 2023          | 17 |