

La technologie NFC

1 Présentation

La [technologie NFC](#) (Near Field Communication) est une méthode de communication sans fil à courte portée qui permet l'échange de données entre deux dispositifs compatibles NFC. Elle repose sur des champs électromagnétiques pour permettre une communication rapide et sécurisée entre les appareils.

Les appareils équipés de la technologie NFC, tels que les smartphones, les tablettes, les cartes de crédit, les cartes de transport en commun, les clés électroniques, et autres dispositifs, peuvent établir une connexion en approchant simplement l'un de l'autre à une distance généralement inférieure à 4 centimètres.



Les principales caractéristiques de la technologie NFC sont les suivantes :

- Communication bidirectionnelle : NFC permet une communication entre deux appareils, qui peuvent à tour de rôle envoyer et recevoir des données.
- Faible consommation d'énergie : La technologie NFC est conçue pour une utilisation efficace de l'énergie, ce qui la rend idéale pour les appareils alimentés par batterie, comme les smartphones.
- Sécurité : NFC intègre des mécanismes de sécurité pour protéger les données échangées afin d'éviter les fraudes.

- Facilité d'utilisation : La proximité physique requise pour établir la connexion rend l'utilisation de NFC simple et intuitive. Il suffit généralement de rapprocher deux appareils pour qu'ils interagissent.

Les cas d'utilisation courants de la technologie NFC incluent :

- Paiements sans contact : Utilisation de smartphones ou de cartes de crédit équipées de NFC pour effectuer des paiements rapides sans avoir besoin de glisser ou d'insérer une carte dans un terminal.
- Partage de fichiers : Transfert rapide de fichiers, d'images, de vidéos ou de contacts entre deux smartphones compatibles NFC.
- Connexion à des appareils : NFC peut être utilisé pour jumeler rapidement des appareils tels que des écouteurs Bluetooth, des haut-parleurs, des imprimantes, etc.
- Accès sécurisé : Les cartes d'accès NFC sont souvent utilisées pour permettre l'accès à des zones sécurisées dans les bureaux ou les bâtiments.

2 Quelle est la différence entre la RFID et le NFC ?

Le NFC (Near Field Communication) et la RFID (Radio Frequency Identification) sont deux technologies sans fil qui utilisent des champs électromagnétiques pour communiquer entre des dispositifs. Bien qu'ils partagent des similitudes, il y a des différences importantes entre les deux :

- Distance de communication :
 - NFC : La communication NFC a une portée très courte, généralement inférieure à 4 centimètres (1,5 pouce). Les dispositifs doivent être presque touchés pour établir une connexion.
 - RFID : La technologie RFID peut fonctionner sur des distances plus importantes, en fonction du type de tag RFID et du lecteur utilisé. La portée peut varier de quelques centimètres à plusieurs mètres.
- Mode de communication :
 - NFC : La communication NFC est principalement bidirectionnelle. Les dispositifs compatibles NFC peuvent envoyer et recevoir des données l'un de l'autre.
 - RFID : La communication RFID peut être bidirectionnelle, mais dans de nombreux cas, les tags RFID sont passifs, ce qui signifie qu'ils ne peuvent être lus que par un lecteur RFID actif, sans avoir la capacité de répondre.

- Applications :
 - NFC : Le NFC est couramment utilisé pour des applications telles que les paiements sans contact, le transfert de fichiers, l'appairage rapide de dispositifs électroniques, les cartes de transport en commun, etc.
 - RFID : La RFID est utilisée dans une variété de domaines, tels que la gestion des stocks, le suivi d'objets, les badges d'accès pour les bâtiments, la gestion du bétail, les péages autoroutiers, etc.
- Sécurité :
 - NFC : La communication NFC offre un niveau de sécurité plus élevé que la RFID, car elle intègre des protocoles de sécurité pour protéger les données échangées. Par exemple, lorsqu'un smartphone effectue un paiement NFC, des mesures de sécurité sont mises en place pour éviter les fraudes.
 - RFID : Certaines technologies RFID peuvent être vulnérables à des attaques de sécurité, en particulier celles utilisant des fréquences plus basses et ne disposant pas de mécanismes de sécurité avancés.







En résumé, le NFC est une sous-catégorie de la technologie RFID (Annexe 1), mais avec des caractéristiques spécifiques qui le rendent plus approprié pour des applications nécessitant une communication très courte distance et une sécurité accrue. La RFID, quant à elle, est plus polyvalente en termes de portée et d'applications, mais peut-être moins sécurisée.

3 La sécurité des tags

Les tags passifs NFC ne sont qu'une mémoire associée à une antenne, avec éventuellement un processeur pour gérer la communication et la cryptographie. Les tags peuvent être sécurisés en cryptant les données, en vérifiant leur intégrité et en empêchant l'arrachage du tag.

- Le cryptage des données : les données peuvent être sauvegardées cryptées dans la mémoire du tag, à charge au lecteur de les décrypter avec l'application. Les données peuvent aussi être cryptées « à la volée » par le tag, dans le cas d'échange avec des applications de différentes natures. Dans ce cas, le tag devra disposer d'un processeur cryptographique renchérissant son coût.
- L'intégrité des données : afin de vérifier que les données n'ont pas été modifiées ou que le tag n'a pas été remplacé par un faux, il existe des schémas de vérification d'intégrité, qui reposent sur une signature sécurisée (ex : signature RTD du NFC Forum) et/ou une vérification d'intégrité à l'aide d'un service web.
- L'anti-arrachage : pour éviter leur arrachage, les tags peuvent être scellés dans la matière (non conductrice bien sûr) de l'objet taggé, et peuvent comporter des dispositifs d'autodestruction en cas d'arrachage physique, appelés « anti-tearing »

4 Quel tag NFC choisir ?

Autocollants	Cartes	Bracelets
		
Étiquettes encastrées	Porte-clés	Objets connectés
		

On retiendra les tags Ntag21x, tous développés par NXP (ISO / IEC14443 Type A)

Tags	Ntag213	Ntag215	Ntag216
Mémoire totale (bytes)	180	540	924
Mémoire utilisateur (bytes)	144	504	888
URL max. (Caractères)	136	488	872
UID (bytes)	7	7	7
Signature ECC	✓	✓	✓
Séries 32-bit Mot de passe	✓	✓	✓
Miroir ASCII UID	✓	✓	✓
Compteur de scan	✓	✓	✓
Miroir de comptoir ASCII	✓	✓	✓
Verrouillable	✓	✓	✓

Fréquence de fonctionnement : 13.56 MHz

Transfert de données : 106 kbit/s

Conservation des données : 10 ans

Nombre de cycles d'écriture : 100000

5 Lire et écrire un tag NFC avec son smartphone

Utiliser le logiciel NFC tools disponible sous Android et ios.



NFC Tools (4+)
Pour lire vos tags NFC
[wakdev](#)
★★★★★ 4,2 • 725 notes
Gratuit • Inclut des achats intégrés

<https://apps.apple.com/fr/app/nfc-tools/id1252962749>

<https://play.google.com/store/apps/details?id=com.wakdev.wdnfc&hl=fr&gl=US>

Menu de lecture	Menu d'écriture	Menu Autre
<div><div>14:21 Orange F</div><div>NFC Tools</div><div>LIRE ECRIRE AUTRE TÂCHES</div><div><div>SAK 0x00</div><div>Signature Valide (NXP Public Key)</div><div>Protégé par mot de passe Non</div><div>Informations mémoire 180 bytes : 45 pages (4 bytes par page)</div><div>Format des données NFC Forum Type 2</div><div>Taille 21 / 137 Bytes</div><div>Ecriture possible Oui</div><div>Lecture seule possible Oui</div><div>Enregistrement 1 - https://www.github.com/f4goh</div></div></div>	<div><div>14:21 Orange F</div><div>Ajouter un enregistrement</div><div><div>Texte Enregistrer un texte</div><div>URL / URI Enregistrer un lien</div><div>URL / URI Personnalisée Enregistrer une URL / URI</div><div>Unit.Link Partagez tout avec un seul lien</div><div>Recherche Ajouter un lien vers une recherche</div><div>Réseaux sociaux Enregistrer un lien d'un réseau social</div><div>Vidéo Enregistrer un lien vidéo</div><div>Fichier Enregistrer un lien vers un fichier</div><div>Application Enregistrer un lien vers une application</div><div>Mail Enregistrer un e-mail</div></div></div>	<div><div>13:17 Orange F</div><div>NFC Tools</div><div>LIRE ECRIRE AUTRE TÂCHES</div><div><div>Copier un tag</div><div>Copier à l'infini !</div><div>Effacer un tag</div><div>Verrouiller un tag</div><div>Lire la mémoire</div><div>Formater la mémoire</div><div>Définir un mot de passe</div><div>Retirer un mot de passe</div><div>Commandes NFC avancées</div></div></div>

On remarque le type de tag lu (Ntag213) et l'URL enregistré.

Attention le verrouillage d'un tag NFC est définitif, il est alors définitivement bloqué en lecture seule.

6 Lire un tag NFC avec un lecteur et un ESP32

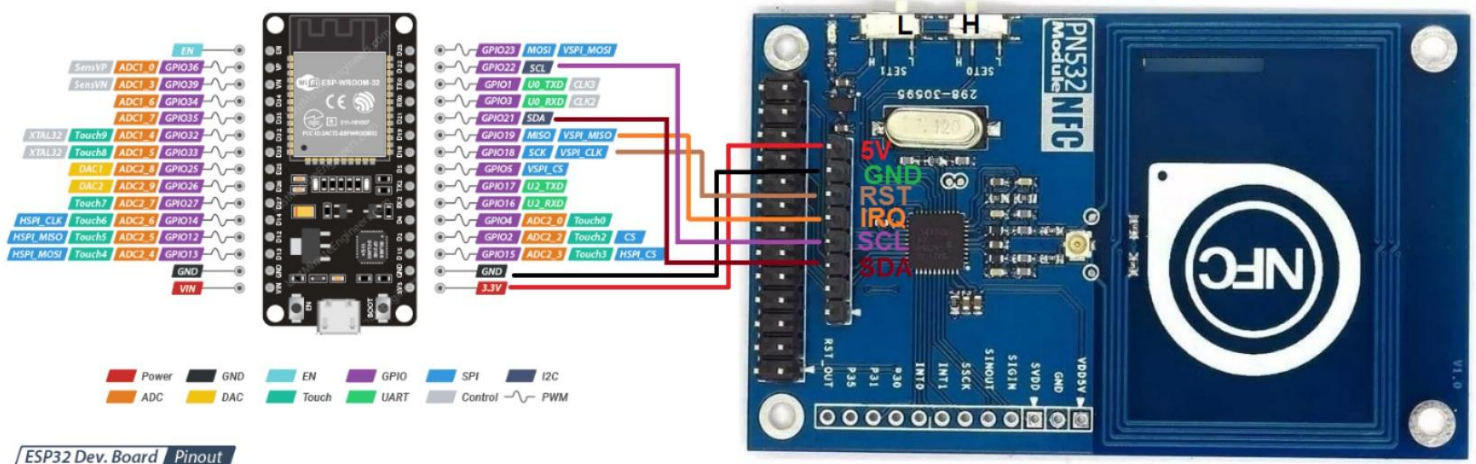


Le module PN535 est un lecteur de tags Mifare NXP. Deux switches permettent de configurer le mode de communication.

Mode	Set0	Set1
UART	L	L
SPI	L	H
I ² C	H	L

Pour la suite le mode retenu est I²C.

Câblage du module avec un esp32



Après avoir créé un projet avec Platform Io

```
pio project init --ide netbeans --board lolin32
```

Installer les bibliothèques suivantes

```
pio lib install "adafruit/Adafruit PN532"
```

```
pio lib install "adafruit/Adafruit BusIO"
```

Un scan du bus I2C permettra de vérifier l'adresse du composant PN532

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00:				--	--	--	--	--	--	--	--	--	--	--	--	--
10:	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
20:	--	--	--	--	24	--	--	--	--	--	--	--	--	--	--	--
30:	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
40:	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
50:	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
60:	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
70:	--	--	--	--	--	--	--	--								

Utiliser le programme exemple de la bibliothèque adafruit PN532 : ntag2xx_read en adaptant les GPIO par rapport à l'esp32

```
#include <Arduino.h>
#include <Wire.h>
#include <SPI.h>
#include <Adafruit_PN532.h>

#define PN532_IRQ 19
#define PN532_RESET 18

Adafruit_PN532 nfc(PN532_IRQ, PN532_RESET);
```

L'exécution du programme avec un Ntag213 devrait afficher une suite de blocs de 4 octets appelés « page »

```
Found chip PN532
Firmware ver. 1.6
Waiting for an ISO14443A Card ...
Found an ISO14443A card
  UID Length: 7 bytes
  UID Value: 0x04 0x03 0x31 0xB2 0xEB 0x6C 0x81

Seems to be an NTAG2xx tag (7 byte UID)
PAGE 00: 04 03 31 BE ..1
PAGE 01: B2 EB 6C 81 //L'identifiant du Ntag213
PAGE 02: B4 48 00 00 H..
PAGE 03: E1 10 12 00 //la valeur 0x12 qui correspond au Ntag213
PAGE 04: 01 03 A0 0C //voir Capability Container
PAGE 05: 34 03 15 D1 4..
PAGE 06: 01 11 55 02 ..U.
PAGE 07: 67 69 74 68 gith //chaque « page » contient 4 octets
PAGE 08: 75 62 2E 63 ub.c
PAGE 09: 6F 6D 2F 66 om/f
PAGE 10: 34 67 6F 68 4goh
PAGE 11: FE 00 00 00 ...
PAGE 12: 00 00 00 00 ....
...
PAGE 40: 00 00 00 BD ...
PAGE 41: 04 00 00 FF ...
PAGE 42: 00 05 00 00 ....
PAGE 43: 00 00 00 00 ....
PAGE 44: 00 00 00 00 ....
```

7 Quelques points de repères dans la documentation constructeur du Ntag21x

https://www.nxp.com/docs/en/data-sheet/NTAG213_215_216.pdf

Page 1 : lien avec les normes ISO

Page 3 : Caractéristiques (déjà décrites dans ce document)

Page 6 : Différences entre les Ntag213, Ntag215 et Ntag216.

Page 11 : Plan mémoire des Ntags

Page Adr		Byte number within a page				Description
Dec	Hex	0	1	2	3	
0	0h	serial number				Manufacturer data and static lock bytes
1	1h	serial number				
2	2h	serial number	internal	lock bytes	lock bytes	
3	3h	Capability Container (CC)				Capability Container
4	4h	user memory				User memory pages
5	5h					
...	...					
38	26 h					
39	27 h					
40	28 h	dynamic lock bytes			RFUI	Dynamic lock bytes
41	29 h	CFG 0				Configuration pages
42	2Ah	CFG 1				
43	2Bh	PWD				
44	2Ch	PACK		RFUI		

Bien observer l'espace disponible pour l'utilisateurs à partir de la « page adr 4 ».

Page 16: Capability Container (CC bytes)

Identifie la taille mémoire du Ntag

IC	Value in byte 2	NDEF memory size
NTAG213	12h	144 byte
NTAG215	3Eh	496 byte
NTAG216	6Dh	872 byte

8 Lire un tag NFC avec un Raspberry PI

Installer les paquets suivants :

```
sudo apt-get update
sudo apt-get install libusb-dev libpcsclite-dev i2c-tools -y
```

Vérifier le lien de la dernière version

<https://github.com/nfc-tools/libnfc/releases/>



```
wget https://github.com/nfc-tools/libnfc/releases/download/libnfc-1.8.0/libnfc-1.8.0.tar.bz2

tar -xf libnfc-1.8.0.tar.bz2

cd libnfc-1.8.0/
```

La commande suivante permet également de vérifier la prise en charge du module PN532

```
./configure -prefix=/usr -sysconfdir=/etc
```

```
Selected drivers:
pcsc..... no
acr122_pcsc..... no
acr122_usb..... yes
acr122s..... yes
arygon..... yes
pn53x_usb..... yes
pn532_uart..... yes
pn532_spi..... yes
pn532_i2c..... yes
pn71xx..... no
```

Compiler et Installer

```
make
```

```
sudo make install
```

Activer l'interface I²C

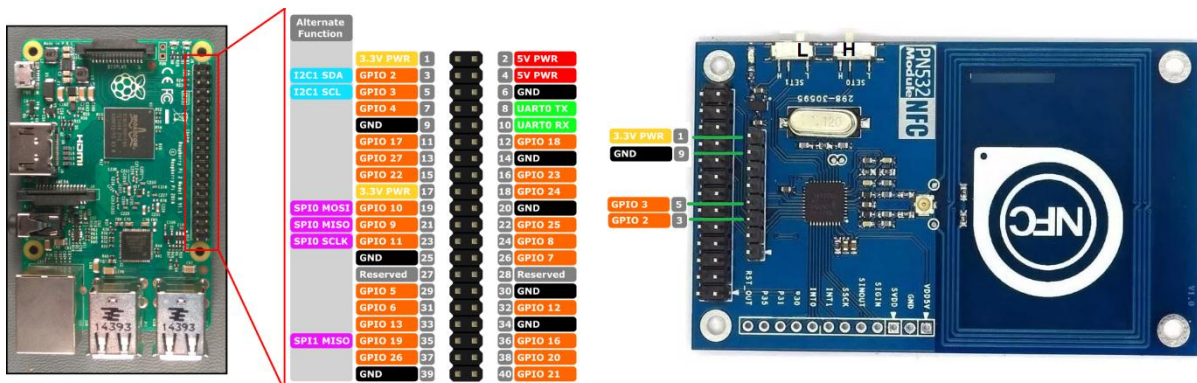
```
sudo raspi-config
```

```
Raspberry Pi Software Configuration Tool (raspi-config)

I1 Legacy Camera Enable/disable legacy camera support
I2 SSH           Enable/disable remote command line access using SSH
I3 VNC           Enable/disable graphical remote access using RealVNC
I4 SPI           Enable/disable automatic loading of SPI kernel module
I5 I2C           Enable/disable automatic loading of I2C kernel module
I6 Serial Port   Enable/disable shell messages on the serial connection
I7 1-Wire        Enable/disable one-wire interface
I8 Remote GPIO   Enable/disable remote access to GPIO pins

<Select>          <Back>
```

Câbler le module sur le Raspberry PI



Vérification de l'adresse du périphérique

```
i2cdetect -y 1
```

```
    0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00:  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --
10:  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --
20:  --  --  --  --  24  --  --  --  --  --  --  --  --  --  --  --
30:  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --
40:  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --
50:  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --
60:  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --
70:  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --  --
```

Créer le fichier de configuration

```
sudo mkdir /etc/nfc
cd /etc/nfc
sudo nano libnfc.conf

# Allow device auto-detection (default: true)
# Note: if this auto-detection is disabled, user has to set manually a device
# configuration using file or environment variable
allow_autoscan = true

# Allow intrusive auto-detection (default: false)
# Warning: intrusive auto-detection can seriously disturb other devices
# This option is not recommended, user should prefer to add manually his device.
allow_intrusive_scan = false

# Set log level (default: error)
# Valid log levels are (in order of verbosity): 0 (none), 1 (error), 2 (info), 3 (debug)
# Note: if you compiled with --enable-debug option, the default log level is "debug"
log_level = 1

# Manually set default device (no default)
# To set a default device, you must set both name and connstring for your device
# Note: if autoscan is enabled, default device will be the first device available in device
list.
#device.name = "_PN532_SPI"
#device.connstring = "pn532_spi:/dev/spidev0.0:280000"
device.name = "_PN532_I2c"
device.connstring = "pn532_i2c:/dev/i2c-1"
```

La commande `nfc-list` affiche seulement l'UID du tag

Attention : placer le tag sur le lecteur AVANT d'exécuter la commande `nfc-list`

```
nfc-list uses libnfc 1.8.0
NFC device: _PN532_I2c opened
1 ISO14443A passive target(s) found:
ISO/IEC 14443A (106 kbps) target:
    ATQA (SENS_RES): 00 44
        UID (NFCID1): 04 78 a2 b2 eb 6c 81
        SAK (SEL_RES): 00
```

Pour pouvoir lire le contenu complet, il faudra utiliser l'API <http://www.libnfc.org/api/>

Il n'y a pas de programme de lecture fourni.

9 Bibliothèque complémentaire Raspberry PI pour lire le contenu des Ntag

La bibliothèque est plus simple à utiliser que l'API libnfc.

Par défaut cette bibliothèque est configurée pour une liaison I²C.

```
git clone https://github.com/soonuse/pn532-lib.git
cd pn532-lib/
cd examples/raspberrypi/
make
ls *.exe

rpi_dump_mifare.exe  rpi_get_uid.exe      rpi_rw_mifare.exe  rpi_write_gpio.exe
rpi_dump_ntag2.exe  rpi_read_gpio.exe    rpi_rw_ntag2.exe

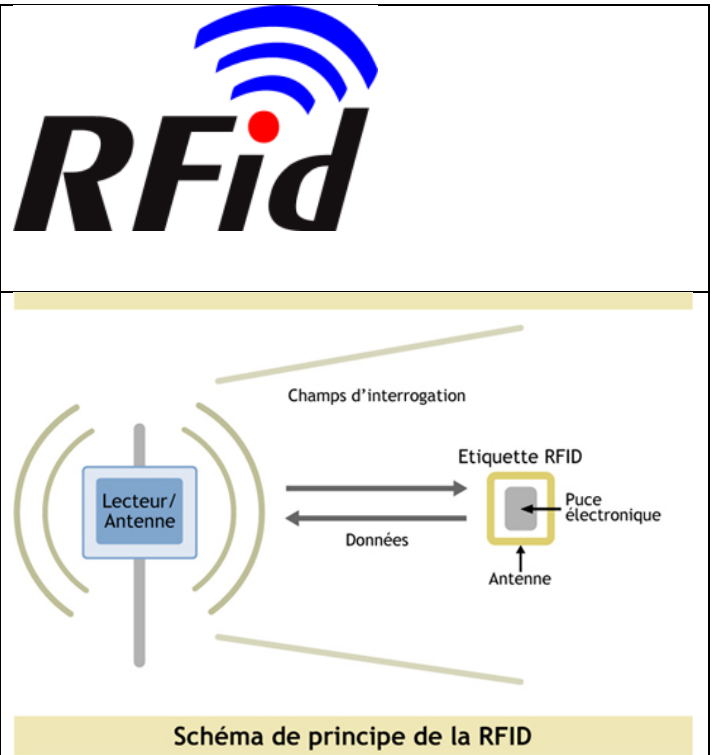
./rpi_dump_ntag2.exe

Hello!
Found PN532 with firmware version: 1.6
Waiting for RFID/NFC card...
Found card with UID: 04 78 a2 b2 eb 6c 81
Reading blocks...
0: 04 78 a2 56
1: b2 eb 6c 81
2: b4 48 00 00
3: e1 10 12 00
4: 01 03 a0 0c
5: 34 03 11 d1
6: 01 0d 55 05
7: 2b 33 33 36
8: 35 31 30 37
9: 32 32 30 37
10: fe 00 00 37
11: 00 00 00 00
```

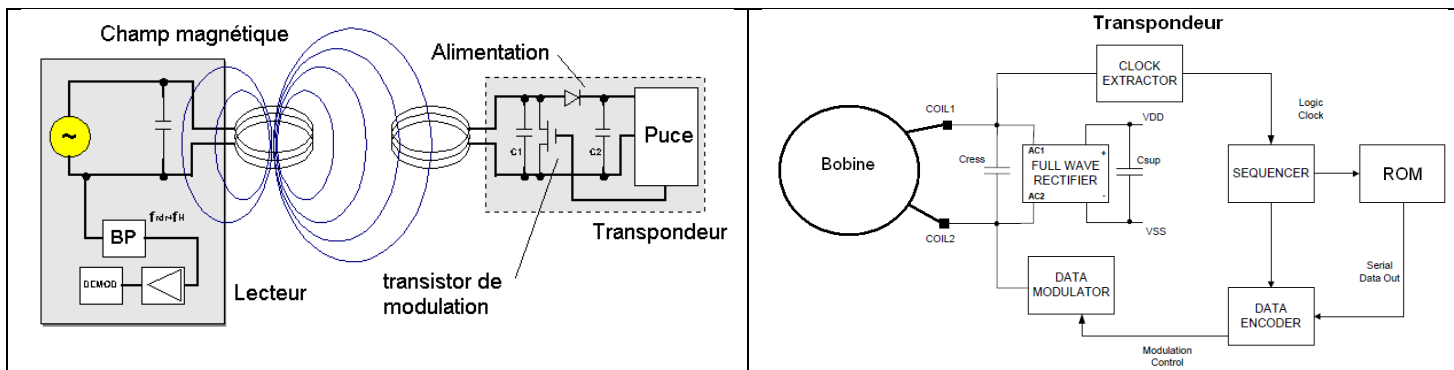
Cette bibliothèque supporte également l'écriture dans les Ntag.

Annexe 1 RFID

La **radio-identification** plus souvent désignée par le sigle **RFID** (de l'anglais **Radio Frequency Identification**) est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » (« RFID tag » ou « RFID **transponder** » en anglais). Les radio-étiquettes sont de petits objets, tels que des étiquettes autoadhésives, qui peuvent être collées ou incorporées dans des objets ou produits et même implantées dans des organismes vivants (animaux, corps humain). Les radio-étiquettes comprennent une antenne associée à une **puce électronique** qui leur permet de **recevoir** et de **répondre** aux requêtes radio émises depuis l'émetteur-récepteur.



Principe : Un lecteur et/ou une antenne envoie un signal radio à une fréquence déterminée. Ce signal, capté par l'antenne de l'étiquette, permet d'accéder aux informations contenues dans la puce électronique de l'étiquette radiofréquence.



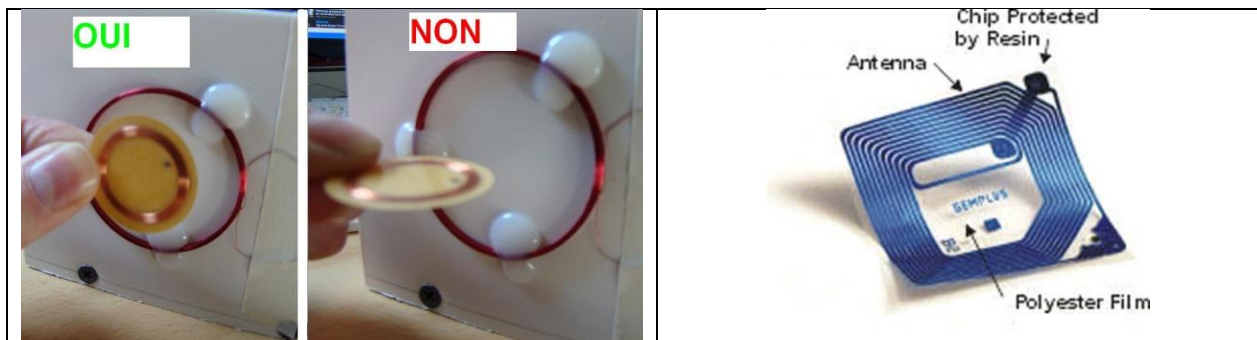
Avec quelle énergie ?

La majorité des puces (tags) ne dispose pas de source d'énergie propre. C'est le signal émis par le lecteur qui permet, via l'antenne, l'échange des données contenues dans la puce. Cela agit comme un transformateur entre le lecteur (primaire) et le tag (secondaire). En captant certaines fréquences, la puce se réveille et émet en retour son numéro d'identification. Ces étiquettes radiofréquences sont dites « passives ».

Gammes de fréquences des tags :

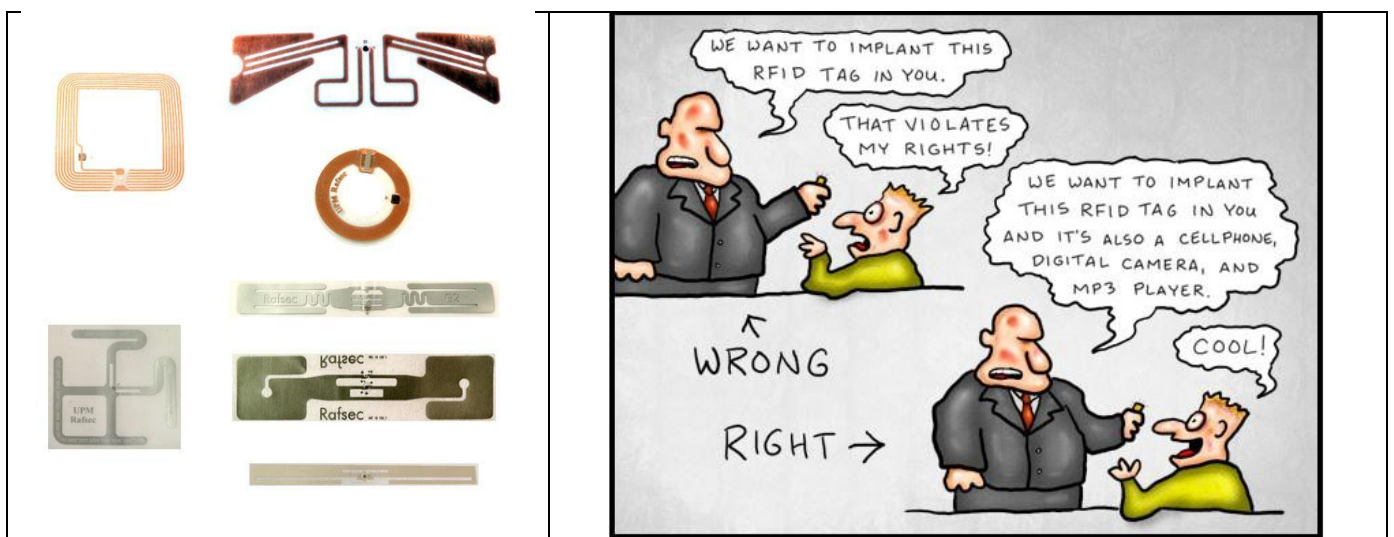
- Basse fréquence 125 à 135 kHz : Identification des animaux, traçabilité d'objets en phase de fabrication, contrôle d'accès par badge de proximité (Challenge robotique), clés électroniques « sans serrures ».
- Haute fréquence 13,56 MHz : Traçabilité des livres dans les librairies et les bibliothèques et pour la localisation des bagages dans les aéroports.
- Micro-ondes (2,45 GHz) : Contrôle d'accès à longue distance des véhicules, comme par exemple sur les grandes zones industrielles.

Ces fréquences offrent des performances différentes, notamment en termes de distance de lecture et de réaction à des environnements humides ou en présence de métaux.



Il existe plusieurs catégories de transpondeurs :

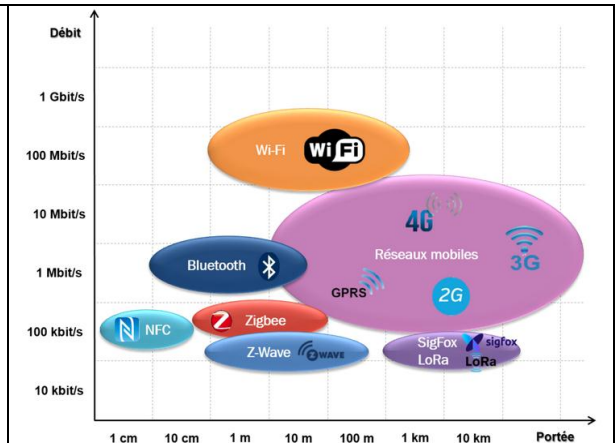
- Les étiquettes en “lecture seule” comportant un numéro d'identification gravé par le fondeur dès la fabrication de la puce. Le numéro peut être lu mais il n'est plus modifiable ;
- Les étiquettes “écriture une fois, lecture multiple”. L'utilisateur peut enregistrer son numéro d'identification unique lors de la première utilisation de l'étiquette. Ensuite, il est seulement possible de lire cette information
- les étiquettes en “lecture réécriture” intégrant des pages de mémoire, en plus du code unique, permettant d'écrire et de modifier de nouvelles données associées.



Annexe 2 : NFC

NFC (Near Field Communication), développée conjointement par Philips et Sony, est une technologie d'identification et d'interconnexion sans contact qui permet une communication sans fil étroite entre les appareils mobiles, l'électronique grand public, les PC et les outils de contrôle intelligents.

NFC est une technologie radio haute fréquence à courte portée. La norme NFCIP-1 stipule que la distance de communication du NFC est inférieure à 10 cm, la fréquence de fonctionnement est de 13.56 MHz et la vitesse de transmission est de 106Kbit/ s, 212 Kbit/ s ou 424Kbit/ s. La norme NFCIP-1 spécifie en détail la vitesse de transmission, la méthode de codec, le schéma de modulation et le format de trame de l'interface RF de l'équipement NFC. Il définit également le protocole de transmission de NFC, y compris le protocole de démarrage et la méthode d'échange de données.



La technologie de communication NFC a évolué à partir de la RFID sans contact et est rétro compatible avec la RFID, qui est principalement utilisée pour fournir une communication M2M (Machine to Machine).

Il existe trois principaux modes de fonctionnement des terminaux NFC :

- Mode actif :

Le périphérique d'origine et le périphérique cible doivent générer des champs RF lors de l'envoi de données l'un à l'autre. Ils ont tous deux besoins de dispositifs d'alimentation pour fournir l'énergie nécessaire pour se transmettre à tour de rôle des signaux.

- Mode passif :

Le périphérique esclave NFC (tag) a besoin d'alimentation. Le dispositif maître utilise son champ magnétique pour fournir l'alimentation au tag et peut échanger des données. C'est le mode le plus utilisé.

- Mode bidirectionnel

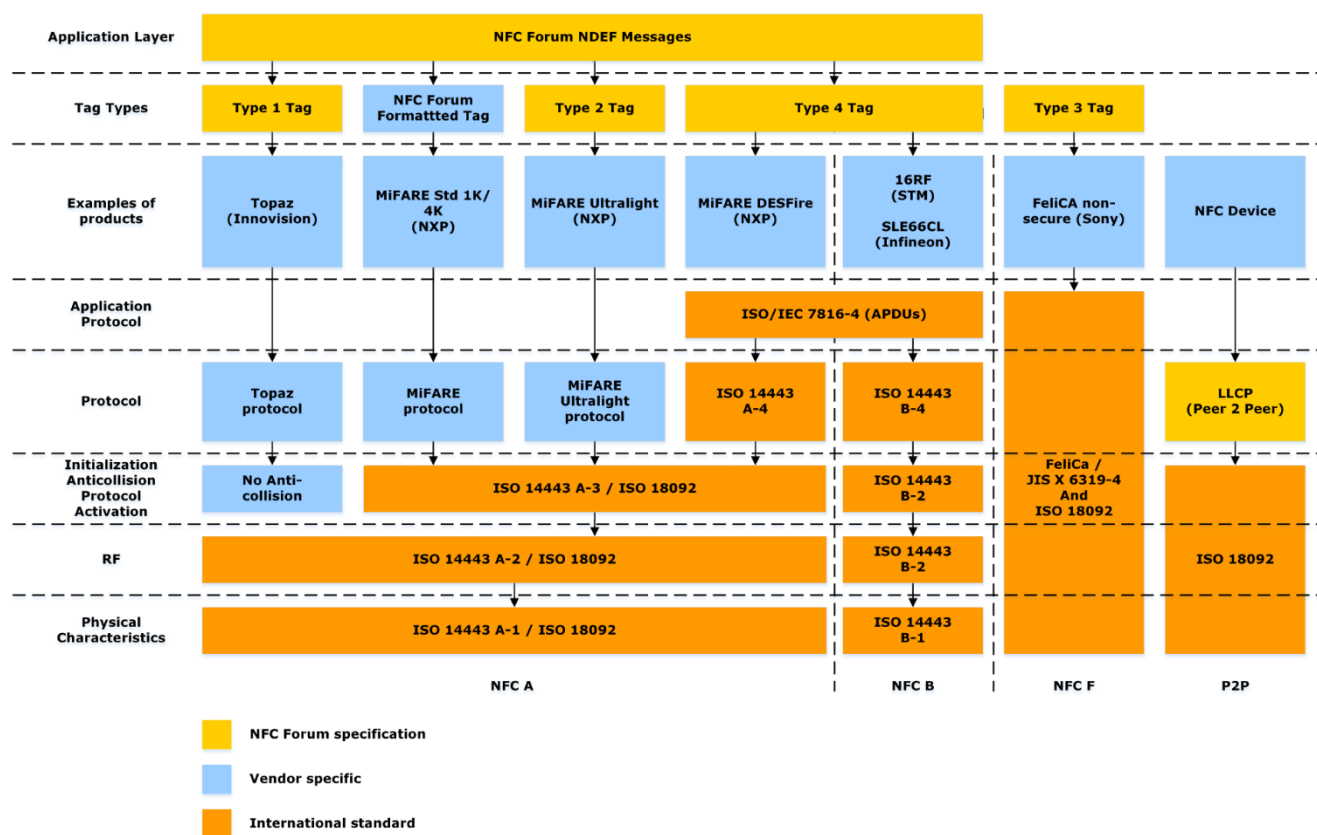
Dans ce mode, les deux appareils NFC sont en mode actif et peuvent activement émettre des champs RF pour établir une communication peer-to-peer (par exemple entre deux smartphone)

La norme NFC

ISO 14443 est une norme internationale bien connue conçue à l'origine pour les cartes à puce sans contact dans les communications radio 13.56 MHz.

Protocole NFCIP-1

Le protocole NFCIP-1 (Near Field Communication Interface and Protocol-1) est un protocole de communication sans fil utilisé dans la technologie NFC. Il définit les spécifications pour permettre la communication entre deux dispositifs NFC en utilisant les fréquences radioélectriques, principalement à 13,56 MHz. Le NFCIP-1 est également connu sous le nom de protocole ISO/IEC 18092.



MIFARE	FeliCa
MIFARE fait référence au type de tag NFC développé par NXP Semiconductor. MIFARE Les étiquettes sont largement utilisées dans les cartes mémoire pour les applications de transport. ISO 14443 définit la pile de protocoles de la couche sans fil au protocole de commande.	FeliCa est une technologie d'étiquette NFC brevetée développée par Sony, largement utilisée dans des applications de paiement et de transport exclusives en Asie.