DÉCOUVREZ LA NFC ET LES TAGS RFID : LE GROS MINIMUM À SAVOIR

Hackable n° 10 (/Hackable/HK-010) | janvier 2016 | Bodor Denis (/auteur/Bodor-Denis)

Cartes d'abonnement, tickets de parking, paiement sans contact, étiquettes de produits, antivols... Autant de domaines et d'applications où la communication sans contact prend chaque jour davantage de place et où se mélange joyeusement toute une collection de termes, parfois (souvent) utilisés à tort et à travers. Avant de nous lancer dans l'aventure, un passage obligé par la case « introduction » est totalement indispensable pour savoir exactement de quoi on parle !

Le mot « NFC » s'est depuis quelques années bien installé dans le langage courant, ainsi que « RFID ». Il est important en revanche de ne surtout pas tout mélanger, car il s'agit bien de deux choses distinctes même si technologiquement voisines et s'empruntant mutuellement certaines caractéristiques. Le but de cette introduction est de vous permettre de clairement distinguer quelles technologies sont désignées lorsqu'on évoque des termes comme NFC, RFID, ISO14443, NDEF, Mifare, NTAG... Le tout sans avoir à lire des centaines de pages de documentation ou spécifications de normes complexes.

1. LA BASE : LE RFID

Passons tout d'abord les fantasmes de type « les boîtes de raviolis RFID vont nous pister où qu'on aille » et penchons-nous surtout sur ce qu'est effectivement cette technologie. À la charge de chacun, ensuite, fort de connaissances techniques non imaginaires, d'avoir une réflexion personnelle et d'en tirer des conclusions concernant l'impact sur sa propre vie.

RFID pour *Radio Frequency IDentification* est un ensemble de normes et standards définissant une technologie permettant de mémoriser des données sur un support et de les faire transiter à distance sans connexion matérielle. Le plus souvent, ceci prend la forme de **marqueurs** désignés par les termes **tags RFID**, **radio-étiquettes** ou **transpondeur RFID**, pouvant se matérialiser de différentes façons : badges, autocollants, porte-clés, capsules sous-cutanées, cartes, disques plastiques à coller ou visser, ou encore embarqué directement dans un objet comme un outil, un jouet, un appareil domestique ou une peluche.

L'objectif initial de ces objets est avant tout de permettre une identification, mais comme nous allons le voir, dans les faits, les usages vont bien au-delà. Tout ce qui répond à cette définition peut être qualifié de technologie RFID, sous certaines conditions. L'une d'entre elles concerne la fréquence en œuvre qui peut être (liste non exhaustive) :

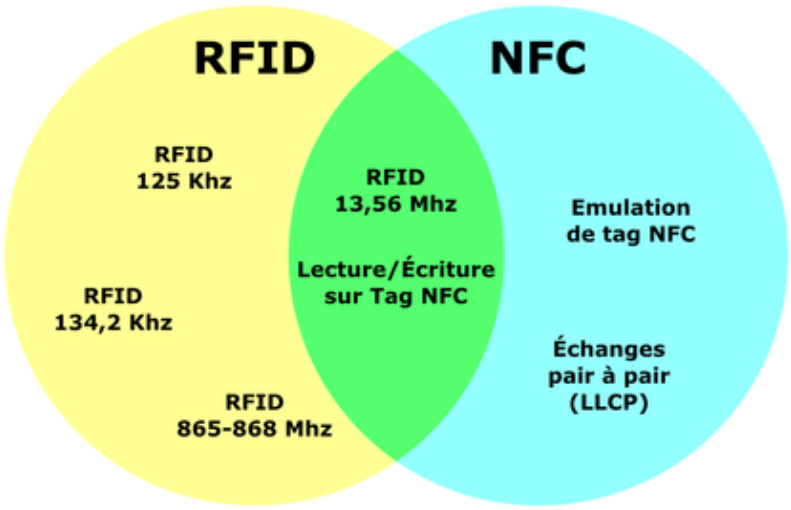
- Basse fréquence ou LF (*Low Frequency*) : à 125 ou 134 Khz ;

- Haute fréquence ou HF (*High Frequency*) : généralement 13,56 Mhz ;

- Ultra-haute fréquence ou UHF (*Ultra High Frequency*) : 865 MHz à 868 MHz (CE), et tantôt 2,4 Ghz ;

- Supra-haute fréquence ou SHF (*Super High Frequency*) : 5,8 GHz (généralement réservée pour les applications nécessitant une portée importante).

Ces fréquences sont utilisées pour deux choses : transmettre des informations et alimenter ce que nous appellerons désormais le tag RFID ou simplement le tag. J'écarterai de mes explications les tags actifs et semi-actifs alimentés par ailleurs et de plus en plus rares (sauf lorsqu'on parle de pair-à-pair). Ce qui nous intéresse ici, ce sont les tags dits passifs.



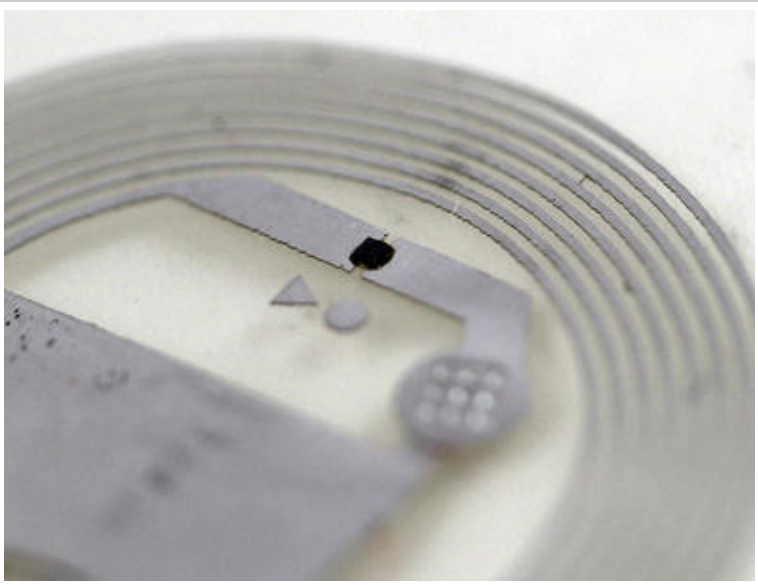
(https://connect.ed-diamond.com/sites/default/files/articles/hackable/hk-010/82824/NFC_RFID_diff1.png)

RFID et NFC sont deux choses distinctes, reposant sur des normes et des standards bien définis. La première chose à savoir sur ces technologies consiste à de ne pas les confondre et ne jamais utiliser un terme à la place de l'autre.

Ceux-ci sont constitués de deux principaux éléments : une antenne et une puce électronique (ou *die* en anglais). La puce est alimentée par induction électromagnétique selon un principe connu depuis plusieurs générations. Prenez une bobine, faites-y passer un courant alternatif et placez une autre bobine à proximité. Le champ magnétique apparaissant et disparaissant dans la première bobine va induire un courant alternatif dans la seconde. C'est exactement le même principe de fonctionnement qu'un transformateur, à la différence que les deux bobines ne sont pas fixes et que le champ magnétique s'étend dans l'air et non dans une carcasse (ou tôles feuilletées). Le procédé a fait l'objet de nombreuses expérimentations très popularisées dès la fin du 19ème siècle par un certain... je vous le donne en mille... Nikola Tesla ! Les proportions en œuvre étaient cependant toute autre que celles des tags RFID (cherchez « tour Wardenclyffe » pour vous faire une idée). C'est également ce même principe qui est utilisé avec les smartphones modernes proposant un système de recharge sans fil.

L'énergie ainsi transmise, qui est modulée par l'émetteur, permet d'alimenter une puce dédiée à cet usage qui en retour va pouvoir répondre en réfléchissant une partie du rayonnement électromagnétique (phénomène de rétrodiffusion) ou en l'absorbant. Nous avons donc une communication bidirectionnelle, *half duplex* (HDX) ou réception puis envoi pour le tag, et *full duplex* ou envoi et réception simultanés pour l'émetteur, qu'on désigne plutôt par le terme PCD pour *Proximity Coupling Device* (le tag étant dans la nomenclature un PICC ou *Proximity Integrated Circuit Card*).

Un tag est donc un véritable concentré de technologie reposant sur des décennies de recherches et d'expérimentations et bien plus qu'une simple puce dans une petite étiquette, une carte ou un porte-clés. En dehors de l'aspect énergétique, cette technologie doit également prendre en compte un problème majeur que l'on retrouve dans la documentation désigné par le terme « collision ». En effet, lorsque plusieurs tags (PICC) se trouvent dans le champ du lecteur (PCD) les communications se mélangent et des techniques particulières doivent être utilisées pour contourner ces effets : les algorithmes d'anti-collision.



(https://connect.ed-diamond.com/sites/default/files/articles/hackable/hk-010/82824/rfid_ultra_macro_chip1.jpg)

Ce petit carré noir de moins d'un millimètre de côté est le circuit intégré formant la partie intelligente d'un tag (ici un NXP NTAG213). Celui-ci est alimenté par l'antenne en spirale qui l'entoure et lui permet également de communiquer.

Les fréquences, les techniques de modulation de signaux, les algorithmes de communication et d'anti-collision et bien d'autres choses encore, forment ensemble une série de normes et de standards. C'est cet ensemble qui est désigné sous le terme RFID.

2. LA NORME : LE NFC

Les mots « NFC » et « RFID » ne sont pas interchangeables. Utiliser maladroitement l'un à la place de l'autre est tout à fait comparable au fait de confondre CD et DVD.

La technologie NFC pour *Near Field Communication* ressemble au RFID, mais n'en est pas, car encadrée par d'autres standards et normes (regroupés sous les désignations ISO/IEC 14443-1 à ISO/IEC 14443-4). Ces normes décrivent quelque chose s'approchant du RFID, mais imposent un certain nombre de restrictions tout en couvrant des points ignorés par les normes RFID. Ceci concerne les caractéristiques physiques (14443-1), l'interface d'alimentation et de gestion radiofréquence (14443-2), l'initialisation et l'anti-collision (14443-3) et enfin le protocole de transmission (14443-4).

(https://connect.ed-

diamond.com/sites/default/files/articles/hackable/hk-010/82824/rfid_lot_tags1.jpg)

Une petite partie d'une collection assez classique de tags de toutes sortes, Mifare Classic, Mifare Ultralight, NTAG203, NTAG213, Mifare DESFire... et de toutes formes, cartes, stickers, porte-clés...

Ne vous inquiétez pas, si vous ne comptez pas fabriquer de lecteurs ou de tags, nous n'avez pas besoin de comprendre le contenu de ces normes et ces caractéristiques. En revanche, savoir qui fait quoi sous quelle désignation est absolument indispensable pour ne pas faire d'erreur et se retrouver dans une impasse lors de vos expérimentations.

Ceci commence par la fréquence utilisée qui, en NFC, se bornera à 13,56 Mhz. Les tags LF RFID 125 Khz ou 134,2 Khz (utilisés pour le marquage des animaux) ne sont donc **PAS** des tags NFC.

Pour communiquer sur cette fréquence, le lecteur et le tag utilisent une modulation. Deux types de modulation sont couverts par la norme sous les noms ISO 14443-A et 14443-B ou plus simplement des lecteurs type A ou B et des tags type A ou B. Bien entendu, un lecteur type A ne pourra pas communiquer avec un tag type B et inversement. Il est donc important en choisissant votre matériel de prendre ceci en considération et d'opter pour un périphérique capable de gérer les deux types (ainsi que d'autres dont nous parlerons plus loin). Notez qu'il existe également un type F, presque exclusivement utilisé au Japon (cartes Suica pour le réseau ferroviaire).

Le type de modulation A ou B est indépendant du protocole (décrit par 14443-4) qui est grossièrement la façon de communiquer. Un peu comme pour des échanges entre personnes : le type est la langue utilisée, le protocole est « bonjour, question, formule de politesse ».

Voilà pour ce qui est de la communication et des protocoles, mais ce n'est pas tout. Parmi les tags , il faut également distinguer différents types en fonction des fonctionnalités qu'ils proposent :

- Le type 1 dispose d'un UID (*Unique IDentifier*), un numéro unique par tag, assimilable à un numéro de série, mais valable parmi la totalité des tags produits tous fabricants confondus. Ce type est également verrouillable en lecture seule. Le tag Topaz d'Innovision (maintenant Broadcom) est un exemple de tags de type 1.

- Le type 2 possède l'UID, est verrouillable et ajoute l'anti-collision permettant de solutionner le problème de la lecture simultanée de plusieurs tags. Les Mifare Ultalight et Ultralight ainsi que NXP NTAG213 par exemple sont des tags de type 2.

- Le type 3 n'a pas d'UID, mais est verrouillable en lecture seule et dispose des mécanismes anti-collision. Le Sony FeliCa est de type 3.

- Le type 4 est l'aîné de la famille avec l'UID, le verrouillage, l'anti-collision et la possibilité d'avoir un contenu actif, le tag lui-même peut modifier son contenu (et non simplement le PCD). Un tag NXP DESFire est une implémentation d'un tag de type 4.

Enfin, un dernier point important qui fait que la technologie en œuvre peut être qualifiée de NFC concerne le mode de communication. Le standard décrit, pour un lecteur (PCD), deux modes possibles. Le premier est celui que j'ai détaillé dans la partie RFID où la communication est initiée par un périphérique et l'autre répond en modulant le champ magnétique fourni par l'initiateur. Le second mode est actif et le champ magnétique est produit alternativement de part et d'autre de la communication, chaque périphérique désactivant son émission pour recevoir des données. Ce second mode permet par exemple à deux smartphones disposant de fonctionnalités NFC de s'échanger des informations, l'un jouant le rôle de lecteur (initiateur) et l'autre de tag (cible). Ces échanges peuvent avoir lieu de pair à pair (LLCP pour *Logical Link Control Protocol*) ou avec un des périphériques émulant un tag.

Il faut bien comprendre que les produits, objets et tags disponibles, doivent être vus comme des « implémentations ISO/IEC 14443 » ou répondant à cette norme, de manière totale ou partielle. Quelques exemples d'implémentation sont le passeport biométrique, les cartes de transport type Calypso (qui sont de type B', un type B mais avec un protocole propriétaire), la carte d'identité allemande, les cartes de paiement sans contact EMV (*Europay MasterCard Visa*) et bien entendu, les périphériques et tags officiellement compatibles NFC, selon le *NFC Forum*.

Ces considérations de compatibilité et désignations associées sont certes pénibles et peu enjouantes, mais c'est le bagage minimum pour éviter les écueils. À titre d'exemple, pour en revenir à la thématique propre du magazine, certains modules ou shield pour Arduino sont capables de lire toutes sortes de tags, mais ne sont pas compatibles NFC.

(https://connect.ed-diamond.com/sites/default/files/articles/hackable/hk-010/82824/rfid_carte_a_puce1.jpg)

Les tags peuvent prendre la forme de cartes au format standard. Il est même possible de combiner plusieurs technologies avec ici à droite une carte intégrant un tag Mifare DESFire, une puce JCOP (JavaCard) et, au dos, une piste magnétique HiCo.

C'est le cas des modules construits autour de la puce RC522 (MFRC522 de NXP plus précisément), car celle-ci est en réalité un composant pour **lecteur** de tags NXP Mifare (Classic, Mini, Ultralight, DESFire, etc.) et ne peut agir qu'en tant qu'initiateur et non de cible. Ce n'est donc pas une solution NFC, mais juste un périphérique pour lire et écrire les tags RFID NXP Mifare. Il ne faut donc pas s'étonner du fait que ce composant ne soit pas supporté par des bibliothèques permettant le support NFC (comme les NFC-tools pour la Pi) alors que le PN532, également à la base de certains modules et shields et du même fabricant, le sera parfaitement.

3. NFC C'EST AUSSI UN FORMAT DE DONNÉES

Pour résumer, nous avons des objets qui utilisent des fréquences modulées pour communiquer selon certains protocoles, le tout classé proprement par types et libellé de tout un tas de désignations cryptiques (et encore, je vous en ai épargné la plupart). C'est un peu comme quand on range son bureau, si déjà on décide de mettre de l'ordre et d'organiser, autant le faire totalement. Le NFC Forum ne s'est donc pas limité à l'aspect matériel, mais a également défini un format pour les données stockées ou échangées.

La façon dont les données sont stockées physiquement dans un tag NFC est dépendant du tag lui-même, de la technologique utilisée, du modèle et du constructeur. Certains tags utilisent des blocs de 4 octets appelés pages, d'autres des secteurs de 4 blocs de 16 octets et d'autres encore une architecture qui rappelle les fichiers d'un disque dur. Pour que tout le monde puisse échanger des données convenablement, se place au-dessus du stockage physique un format unique : NDEF pour *NFC Data Exchange Format*, ou en français, un format d'échange de données NFC.

Ce format décrit des **messages** NDEF constitués d'un ou plusieurs **enregistrements** NDEF. Ces enregistrements ne contiennent pas uniquement les données utiles (*payload* dans le jargon), mais bien d'autres choses comme le type de type d'enregistrement (non ce n'est pas une faute de frappe, c'est le TNF pour *Type Name Format*), si c'est un morceau d'un enregistrement (CF), s'il s'agit du début (MB) ou la fin (ME) d'un message, la taille des données utiles, le type d'enregistrement (en fonction du TNF), éventuellement un numéro... et finalement les données utiles.

C'est la même logique que celle d'un format graphique dans lequel on trouve non seulement la liste des couleurs de chaque pixel, mais également toutes les informations permettant de traiter l'image en tant que telle (taille, densité, palettes, métadonnées, etc.). Ici, c'est simplement un peu plus riche et générique, car un tag NFC peut contenir énormément de choses différentes.

À titre d'aperçu, prenons un cas particulier avec un enregistrement ayant le champ TNF à `0x01`. Ceci indique qu'il s'agit d'un enregistrement de « type bien connu » (ça sonne mieux en anglais : « *Well-Known Type* » ou WKT). De ce fait, le type précisé dans l'enregistrement aura un sens précis et standardisé où chaque valeur possible fait partie d'une nomenclature appelée RTD (*Record Type Definition*). Si nous prenons le type `0x55` (qui correspond au caractère `U`), l'enregistrement est utilisé pour stocker un URI ou *Uniform Resource Identifier*, autrement dit une chaîne définissant quelque chose. Et ce quelque chose peut, par exemple, être une adresse mail (`0x06` pour `mailto:`)...

Si là vous n'avez pas encore décroché, félicitations ! Mais sachez que cet exemple ne concerne qu'un TNF (`0x01`), un type d'enregistrement (`0x55`) et un code URI (`0x06`). Il y a une quantité de codes URI, une demi-douzaine de « types bien connus » (WKT) et 7 TNF (types de type). S'ajoute encore à cela le TNF `0x04` précisant qu'une « nomenclature » externe (*NFC Forum External Type*) peut être utilisée et donc décrite en dehors des spécifications du NFC Forum.

Étant donné la complexité ou plus exactement la densité du sujet et la masse d'informations à assimiler, il n'est pas question pour un usage comme le nôtre de devoir lire et retenir des pages et des pages de spécifications. Exactement de la même manière qu'il ne vous est pas nécessaire de comprendre le format JPEG ou PNG pour manipuler des images sur un PC ou un Mac, nous n'aurons pas besoin de maîtriser le format NDEF pour faire usage de la technologie NFC.

Comme pour les images, seuls quelques points importants sont à retenir et en particulier le fait qu'un tag NFC contient toujours des données NDEF qui sont davantage que de simples données utiles. Si un tag ne contient autre chose que du NDEF, ce n'est pas un tag NFC. Encore une fois, voyez cela comme un support optique : si un CD ne contient pas des données formatées CDDA (alias Red Book), ce n'est pas un CD audio, même s'il s'agit bien un CD et que de la musique y est enregistrée.

4. LES DIFFÉRENTS TAGS

À ce stade, vous pouvez vous demander ce qu'est finalement effectivement un tag NFC et la question est parfaitement légitime. La réponse est simple : c'est un tag répondant aux spécifications NFC et contenant des données formatées NDEF, rien de plus.

Matériellement, comme le disent clairement les documentations de NXP pour ces composants, c'est juste une puce compatible avec les normes définissant un tag type 1, 2, 3 ou 4. Et ceci ne signifie absolument pas que vous ne pouvez qu'y inscrire des données NDEF. Ainsi, ceux qu'on trouve généralement dans le commerce sont des tags ayant une désignation définie par leurs fabricants. Il n'y a pas de tags NFC « tout court ». Un NTAG213 et un Mifare Ultralight, de NXP sont des produits différents, mais tous les deux peuvent être des tags NFC type 2 s'ils contiennent les bonnes données.

Le NFC Forum ayant été formé par les principaux acteurs sur le marché que sont NXP, Sony, et Innovision/Broadcom, il n'est guère étonnant que les tags commercialisés et se trouvant un peu partout proviennent principalement de ces constructeurs avec, en tête de liste NXP. Sans oublier, bien entendu les fabricants de clones et de produits compatibles comme Infineon Technologies (ex-Siemens) ou Fudan Microelectronics (il existe même des tags produits sans licence, disposant de fonctionnalités hors normes, comme des UID réinscriptibles).

Pour expérimenter ces technologies, vous aurez besoin d'un lecteur (ou *reader* qui est aussi un périphérique d'écriture, mais c'est là la désignation courante, un peu comme les *lecteurs* de disquettes d'antan), mais aussi et surtout de tags, de formes et de modèles les plus variés possibles de préférence.

Ainsi, parmi les produits les plus courants nous avons :

- Les *Mifare Classic* de NXP qui ne sont pas à proprement parler des tags compatibles NFC (voir ci-après) mais ce sont, sans le moindre doute ceux qu'on trouve littéralement partout. Ceux-ci se déclinent en deux tailles, 1k (752 octets utiles) ou 4k (3440 octets utiles), parfois respectivement désignés par « S50 » et « S70 ».

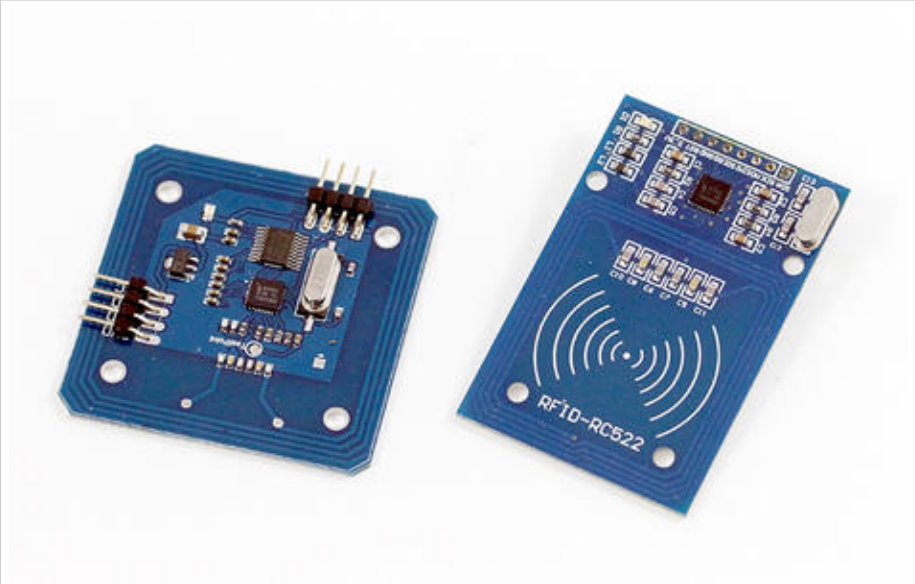
- Les *Mifare Ultralight* également de NXP qui cette fois respectent intégralement les standards NFC et peuvent être utilisés dans des tags NFC de type 2. Initialement créés pour les applications à faible coût, on les retrouve généralement dans des solutions à durée de vie limitée, embarquées dans des supports peu robustes comme les tickets de parking.

- Les NTAG210/213/215/216 sont très proches des *Mifare Ultralight*, mais ont été développés spécifiquement par NXP pour un usage en tant que tags NFC type 2 de 48, 144, 504 et 888 octets utiles. On peut voir ce modèle comme le successeur de l'Ultralight pour les usages NFC.

- Les *Mifare DESFire* sont des tags plus évolués intégrant un microprocesseur et toute une logique interne ainsi qu'un système d'exploitation et différents mécanismes de protection avancés. Une évolution du produit est disponible sous le nom *Mifare DESFire EV1* ajoutant encore des fonctionnalités et corrigeant certains problèmes de sécurité. Les DESFire sont totalement compatibles avec les normes du NFC Forum pour une utilisation en tag NFC de type 4.

Je pense qu'on peut parler ici d'une réelle domination de NXP, du moins pour l'Occident. En effet, Sony et sa technologie FeliCa, qui est compatible NFC (parce que la compatibilité FeliCa est incluse dans le standard), est massivement utilisé dans les pays asiatiques (Japon, Chine, Thaïlande, etc.) ainsi que de façon éparse pour certaines applications dans le reste du monde.

On trouve ensuite tout un tas d'autres tags pouvant ou non être compatibles NFC Forum, tantôt reposant sur des technologies connues sous un autre nom. C'est le cas par exemple des Samsung TecTiles, reposant sur NXP Mifare Classic. Mais on trouve également du Texas Instrument Tag-it HF Plus, du NTAG203, du MIFARE Plus, etc.



(https://connect.ed-diamond.com/sites/default/files/articles/hackable/hk-010/82824/rfid_modules_rc5221.jpg)

Deux modules généralement vendus comme « compatibles NFC », reposant sur le circuit intégré RC522. Au sens strict du terme, il ne s'agit pas de NFC puisque ce composant ne peut émuler un tag, mais plutôt d'un simple lecteur de tags NXP Mifare.

Mes recommandations concernant la composition d'une petite collection de tags tiennent en peu de choses : le bien nommé Mifare Classic est le tag le plus facile à trouver et le moins cher, il est donc presque indispensable (malgré ses écarts à la norme). Mais par souci de respect des normes, quelques Mifare Ultralight et NTAG213 (ou 203, 210, 215, 216) forment un complément pertinent. Et enfin par curiosité, on pourra tenter d'obtenir un ou des Mifare DESFire, FeliCa et autres modèles plus exotiques.

5. MIFARE CLASSIC ET LES PETITS ÉCARTS À LA NORME

Les tags Mifare Classic ne datent pas d'hier et étaient déjà utilisés avant même que l'on parle de NFC avec autant d'ardeur. La technologie utilisée est historiquement celle de la société Mikron (le nom MIFARE signifie d'ailleurs « *MIkron FARE Collection System* ») acquise par Philips, maintenant NXP, il y a presque 20 ans.

On retrouve les tags Mifare Classic sous une quantité incroyable de formes et de formats. C'est une technologie vastement installée, mais il ne s'agit pas véritablement de NFC. En effet, les Mifare Classic sont bel et bien des tags ISO/IEC 14443-A, mais ils ne respectent pas l'ensemble des spécifications du NFC Forum et en particulier ISO/IEC 14443-4 au bénéfice d'un protocole propriétaire propre aux puces du constructeur (et que partiellement ISO/IEC 14443-3).

La conséquence directe de cet état de fait est un problème de compatibilité. Le protocole utilisé étant non standard, seuls les composants NXP (ou compatibles sous licence) peuvent communiquer avec les tags Mifare Classic. Dans les faits si nous prenons l'exemple des périphériques Android, seuls les smartphones équipés de puces NXP peuvent lire et écrire des tags Mifare Classic en plus de ceux pleinement compatibles NFC. Les Google Nexus 4, 5 et 6, par exemple, intègrent un contrôleur NFC Broadcom (BCM20793 ou BCM20795) qui est compatible NFC Forum… et uniquement compatible NFC Forum. Ces smartphones ne permettent pas la manipulation de tags Mifare Classic, mais uniquement de tags qui sont également 100% compatibles NFC Forum (comme les NTAG, Mifare DESFire ou Mifare Ultralight).

Notez cependant que sur un smartphone équipé d'une puce NXP, il est tout à fait possible d'utiliser un tag Mifare Classic comme un tag NFC et donc de le formater et d'y placer des données NDEF. Tout fonctionnera exactement de la même façon et sera totalement transparent pour vous. Le tag en question, toutefois, ne sera lisible et donc utilisable que sur les smartphones également équipés d'une puce NXP.

Enfin, il est important de préciser que les Mifare Classic malgré les mécanismes de sécurité en place ne doivent plus être considérés comme des solutions sûres. Il existe plusieurs techniques, attaques et implémentations permettant de déjouer ces sécurités et d'accéder frauduleusement au contenu du tag.

6. LE MATÉRIEL

Nous avons déjà parlé de la constitution minimale d'une collection de tags. Si le domaine vous apparaît divertissant après quelques essais, vous verrez sans le moindre doute votre collection rapidement s'étoffer de toutes sortes de choses (attention, il y a un petit effet Pokemon dans RFID/NFC). Ceci aussi bien au travers d'achats en ligne via des boutiques et sites d'enchère que par d'autres moyens. Il y a fort à parier que toutes les cartes dans votre portefeuille vont passer au test systématique, mais ce n'est pas tout…

(https://connect.ed-diamond.com/sites/default/files/articles/hackable/hk-010/82824/rfid_acr122u1.jpg)

Le « lecteur » ACR122U d'ACS est le périphérique USB le plus populaire et le plus facile à trouver, mais c'est aussi celui qui posera tantôt problème et obligera à une déconnexion/reconnexion en raison d'un firmware peu stable.

Vous vous souvenez lorsque vos parents vous disaient qu'il ne fallait pas ramasser ce qui traîne par terre dans la rue ? Hé bien c'est faux ! Ne leur en voulez pas, il ne pouvaient pas savoir. Tantôt les tickets jetables embarquent une antenne et une puce NFC (de l'Ultralight le plus souvent), mais il peut aussi s'agir d'emballages divers, de cartes soi-disant non rechargeables, de badges égarés, de titres de transport, etc.

Mais le plus important n'est pas tant la collection de tags que le matériel permettant de les manipuler. La trousse à outils idéale, selon moi, est la suivante (par ordre d'importance) :

- Un smartphone Android disposant de fonctionnalités NFC, de préférence avec une puce NXP offrant un accès aux tags Mifare Classic en plus du standard NFC Forum. Si vous êtes un utilisateur d'iPhone, pas de chance. Chez Apple, la « révolution » NFC n'arrive qu'avec l'iPhone 6 et en version « limitée » uniquement aux fonctionnalités qui semblent profiter à la firme de Cupertino. L'offre logicielle sur plateforme Android est, pour peu que l'on dispose d'un appareil compatible, absolument fantastique. À titre personnel, bien qu'utilisant un non-smartphone Samsung E1200 (prix : 15€, autonomie : 1 mois), je conserve et chéris mon Samsung Galaxy Nexus et sa puce NXP PN544 pour cette raison précise (ainsi qu'une tablette Nexus 7 2012 intégrant une puce NXP PN65).

- Un « lecteur » NFC USB qui pourra être utilisé aussi bien sur PC/Mac qu'avec la Raspberry Pi. Deux lecteurs se partagent généralement la vedette avec d'un côté l'ACR122U d'ACS pour quelques 30€ et de l'autre le SCL3711 de SCM/Identive entre 40€ et 50€. Le premier est littéralement la solution la moins chère, mais présente tantôt un comportement instable bien connu. Le produit SCM/Identive est généralement un meilleur choix, plus stable et de bien moindre encombrement.

- Un module ou shield Arduino construit autour d'un PN532. Ce circuit intégré de chez NXP est compatible NFC et est donc capable non seulement de lire et d'écrire les Mifare Classic ainsi que les tags compatibles NFC (FeliCa inclus), mais également d'agir comme une cible NFC en pair-à-pair et en émulation. Le PN532 peut être interfacé en liaison série, SPI ou i2c. Il est donc important de choisir un module proposant de préférence les trois connectiques ainsi qu'une configuration des tensions (5V et 3,3V). De cette manière, un seul module vous suffira pour toutes vos expériences aussi bien sur Raspberry Pi que sur Arduino, Ti Launchpad, etc. Un tel module vous coûtera entre 15€ et 20€.

- Un module ou shield basé sur une puce RC522. Ce contrôleur RFID n'est **pas** compatible NFC au sens strict du terme puisqu'il ne sait agir qu'en tant qu'initiateur dans une transaction. Il ne pourra pas vous permettre un fonctionnement pair-à-pair avec un smartphone par exemple, mais sera bien utile avec une carte Arduino pour lire toutes sortes de tags (ISO/IEC 14443-A/Mifare). Comme le PN532, il peut être interfacé en série, SPI et i2c, et par-dessus tout, il présente un avantage crucial : un tel module coûte moins de 3€ !

En termes de budget, le smartphone ou la tablette idéalement compatible reste l'élément le plus coûteux s'il vous faut envisager une telle acquisition. Des périphériques d'occasion se trouvent entre 50€ et plus de 150€ selon l'état. Vous passer d'une puce NXP ne sera pas un problème, mais mettra les populaires tags Mifare Classic hors de votre portée. Le smartphone NFC Android n'est en rien indispensable, mais apporte un confort très important en faisant office de système portatif fiable, ne serait-ce que pour vérifier vos expérimentations sur Arduino ou Raspberry Pi.

(https://connect.ed-

diamond.com/sites/default/files/articles/hackable/hk-010/82824/rfid_module_pn5321.jpg)

Exemple de module à base de PN532 pouvant être interfacé avec une carte Arduino via une connexion série, SPI ou i2c. Celui-ci est vendu par ElecFreaks, mais il en existe de nombreux modèles.

Notez qu'il existe une solution permettant d'utiliser des lecteurs ACS avec une tablette Android disposant de fonctionnalités USB hôte. Ce support appelé « *External NFC Reader Service* », disponible via le *Play Store*, est vendu 20€ ! Nous ne pouvons vous confirmer son fonctionnement, car nous ne l'avons pas testé pour une raison évidente : 30€ d'ACR122U + 20€ d'applicatif + le temps de développement (il ne s'agit pas d'une application, mais d'un service)... Il est plus simple et économique de se trouver un smartphone compatible d'occasion. Prenez simplement garde, certains modèles utilisent une antenne NFC placée dans la batterie (Galaxy Nexus) et les batteries « compatibles » et économiques ne l'intègrent pas.

Le lecteur USB lui est à envisager de la même manière, avec une souplesse un peu plus réduite puisqu'il ne disposera pas des applications clés en main et nécessitera l'ajout d'un PC/Mac (de préférence sous GNU/Linux) ou d'une Pi, ce qui reste handicapant pour une utilisation nomade. Un module PN532 pourra être connecté à un PC/Mac ou une Pi de façon à permettre une utilisation comparable à celle d'un lecteur USB, mais ceci demandera un peu de bricolage, soit par la connexion directe (série, SPI ou i2c), soit via un adaptateur USB/série.

(https://connect.ed-diamond.com/sites/default/files/articles/hackable/hk-010/82824/rfid_scl37111.jpg)

Le périphérique USB SCM SCL3711 est un produit compact et réputé en termes de stabilité de fonctionnement (par rapport à l'ACR122U). C'est le « lecteur » généralement recommandé si l'on souhaite explorer les technologies NFC et RFID 13,56 Mhz.

Comme dans toutes expérimentations, il est important d'avoir une référence sûre. Ainsi même si les modules à 3€ à base de RC522 sont fort séduisants, en cas de difficulté, vous ne saurez pas si le problème vient de vous, de votre code, du tag, du module, de la configuration... Vous serez dans le noir.

CONCLUSION

Longue, pénible et pas forcément très ludique... Voilà qui peut parfaitement qualifier une introduction aux technologies RFID et NFC comme celle que vous venez de subir. Mais cela reste un coût relativement modeste au regard de la richesse et de la rigidité des standards, mais aussi et surtout des possibilités qui vous sont maintenant accessibles. Nous ne sommes pas vraiment descendus dans le terrier du lapin blanc, car il y a

énormément de choses à dire, en particulier sur le stockage des données sur différents types de tags. C'est là un autre avantage du NFC, il permet de se placer à un niveau d'abstraction où seules les données importent, le reste étant laissé à la charge des bibliothèques, des outils et des applications. Nous voici enfin prêts pour nous lancer dans l'aventure. Allons-y !

Étiquettes :
RFID (/search/node?field_ct_article_tags_target_id_selective%5B0%5D=72568),
NFC (/search/node?field_ct_article_tags_target_id_selective%5B0%5D=72569),
Mifare (/search/node?field_ct_article_tags_target_id_selective%5B0%5D=72570)

Article précédent (/Hackable/HK-010/Creer-une-horloge-a-aiguille-originale-amperemetre)
Article suivant (/Hackable/HK-010/Quelles-applications-Android-utiliser-pour-explorer-RFID-et-NFC)

AU SOMMAIRE DU MÊME NUMÉRO

PAR LE MÊME AUTEUR

VITE FAIT : CRÉER UN THERMOSTAT D'AMBIANCE PROGRAMMABLE (/HACKABLE/HK-032/VITE-FAIT-CREER-UN-THERMOSTAT-D-AMBIANCE-PROGRAMMABLE)

Hackable n° 32 (/Hackable/HK-032) | janvier 2020 | Bodor Denis (/auteur/Bodor-Denis)

Domotique (/search/node?Domaines%5B0%5D=72455)

Dans ma nouvelle maison, j'ai découvert les joies du chauffage au fioul et les limitations d'un système de régulation de la température intérieure le plus simpliste qui soit. La simplicité a ses avantages, et le fioul aussi, mais lorsqu'on regarde sa facture, on se rend rapidement compte que cette simplicité a un coût, qui peut être important. Pour régler le problème, j'ai décidé de faire rapidement évoluer mon installation, avec l'aide d'une ...

ÉDITO (/HACKABLE/HK-032/EDITO)

Hackable n° 32 (/Hackable/HK-032) | janvier 2020 | Bodor Denis (/auteur/Bodor-Denis)

De Noël à mars... Avez-vous remarqué qu'il y a un climat de crise énergétique ambiant en ce moment ? Tout devient économe en énergie, les ampoules à filament ont laissé place aux leds dans les rayons des magasins et petit à petit dans les rues, de manière générale les choses énergivores sont devenues le mal incarné car, comme dirait la pub, « ce n'est pas Versailles ici ». ...

MODULE INTERFACE I2C POUR ÉCRAN LCD (/HACKABLE/HK-032/MODULE-INTERFACE-I2C-POUR-ECRAN-LCD)

Hackable n° 32 (/Hackable/HK-032) | janvier 2020 | Bodor Denis (/auteur/Bodor-Denis)

Électronique (/search/node?Domaines%5B0%5D=72452)

Les afficheurs LCD alphanumériques disposant d'une interface compatible HD44780 (composant Hitachi à l'origine) se pilotent tous de la même façon et peuvent avoir différentes caractéristiques et tailles : une ligne de 8 caractères, quatre lignes de 20 caractères, deux lignes de 16 caractères, etc., tantôt avec rétroéclairage, tantôt sans. ...

ÉDITO (/HACKABLE/HK-031/EDITO)

Hackable n° 31 (/Hackable/HK-031) | octobre 2019 | Bodor Denis (/auteur/Bodor-Denis)

Dans la vie, il y a ceux qui savent être « open » et ceux qui ne savent pas. ...

CONVERTISSEUR HDMI VERS VGA (/HACKABLE/HK-031/CONVERTISSEUR-HDMI-VERS-VGA)

Hackable n° 31 (/Hackable/HK-031) | octobre 2019 | Bodor Denis (/auteur/Bodor-Denis)

Électronique (/search/node?Domaines%5B0%5D=72452) **Audio/Vidéo (/search/node?Domaines%5B0%5D=72453)**

L'intérêt premier d'un convertisseur HDMI vers VGA est de permettre l'utilisation de matériels plus anciens avec des cartes et équipements modernes. Le cas typique ici est, bien entendu, de recycler un vieil écran VGA comme moniteur pour une carte Raspberry Pi. Ceci ne sera pas nécessairement très intéressant pour une

utilisation « desktop », mais sera parfaitement viable pour le jeu, l'émulation, la création d'un media center ou ...

CRÉER, ÉCRIRE, LIRE ET DÉCODER UNE IMAGE SPIFFS D'UN ESP8266 (/HACKABLE/HK-031/CREER-ECRIRE-LIRE-ET-DECODER-UNE-IMAGE-SPIFFS-D-UN-ESP8266)

Hackable n° 31 (/Hackable/HK-031) | octobre 2019 | Bodor Denis (/auteur/Bodor-Denis)

Électronique (/search/node?Domaines%5B0%5D=72452)

L'espace de stockage SPIFFS des ESP8266 est très pratique, mais il arrive tantôt qu'on se retrouve dans une situation où l'on souhaiterait vraiment récupérer les données stockées, sans avoir à bidouiller un croquis, au risque de faire une fausse manipulation et de tout perdre. Fort heureusement, le support ESP8266 (et ESP32) de l'environnement Arduino est composé d'un ensemble d'outils, qui peuvent être utilisés individuellement. ...

1 (?page=0%2C0) 2 (?page=0%2C1) 3 (?page=0%2C2) 4 (?page=0%2C3) 5 (?page=0%2C4)
6 (?page=0%2C5) 7 (?page=0%2C6) 8 (?page=0%2C7) 9 (?page=0%2C8) Suivant › (?page=0%2C1)

()