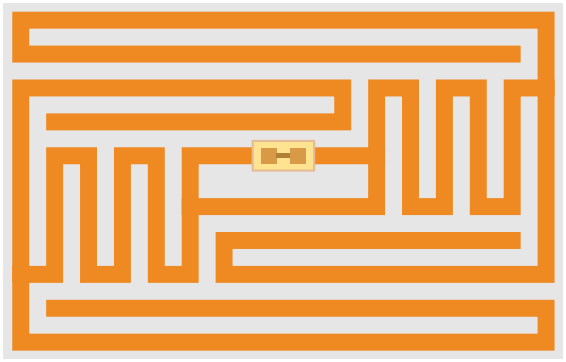
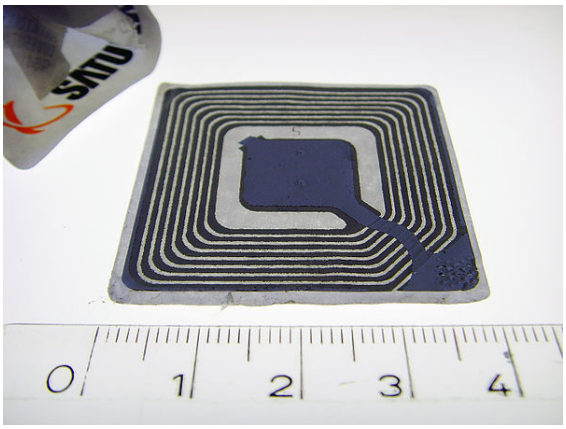
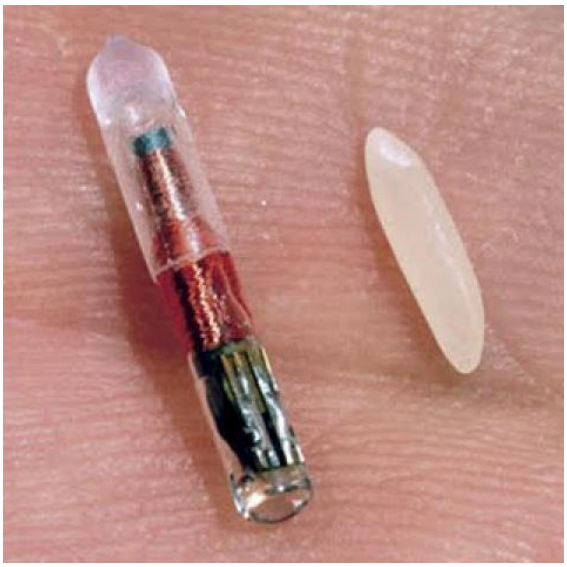
Radio-identification



Une puce de radio-identification EPC utilisée par Wal-Mart





Puce électronique sous-cutanée (par RFID) implantée chez les carnivores domestiques et comparée avec un grain de riz.

La **radio-identification**, le 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)[1].

Les radio-étiquettes sont de petits objets, tels que des étiquettes autoadhésives, qui peuvent être collés ou incorporés dans des objets ou produits et même implantés dans des organismes vivants (animaux, corps humain[2]). 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.

Ces puces électroniques contiennent un identifiant et éventuellement des données complémentaires.(RAD)

Cette technologie d'identification peut être utilisée pour identifier :

- les objets, comme avec un code-barres (on parle alors d'étiquette électronique) ;
- les personnes, en étant intégrée dans les passeports, carte de transport, carte de paiement (on parle alors de carte sans contact) ;
- les carnivores domestiques (chats, chiens et furets) dont l'identification RFID est obligatoire dans de nombreux pays, en étant implantée sous la peau. C'est également le cas de manière non obligatoire pour d'autres animaux de travail, de compagnie ou d'élevage de rente (on parle alors de puce sous-cutanée).

1 Principe

Un système de radio-identification activé par un transfert d'énergie électromagnétique se compose de marqueurs, nommés radio-étiquettes ou transpondeurs (de l'anglais *transponder*, contraction des mots *transmitter* et *responder*) et d'un ou plusieurs lecteurs. Un marqueur est composé d'une puce et d'une antenne.

1.1 Lecteurs

Ce sont des dispositifs actifs, émetteurs de radiofréquences qui vont activer les marqueurs qui

passent devant eux en leur fournissant à courte distance l'énergie dont ceux-ci ont besoin. La fréquence utilisée est variable, selon le type d'application visé et les performances recherchées[3] :

- 125 kHz ;
- 134,2 kHz pour la charge du transpondeur ; 134,2 kHz pour un bit 0 et 123,2 kHz pour un bit 1 pour la réponse du transpondeur dans le cas d'une transmission FSK (Texas Instruments Series 2000) ;
- 13,56 MHz (ISO 14 443 A 1-4, ISO 14443B 1-4, ISO 15693-3 et ISO 18000-3), la plus répandue actuellement dans l'industrie et le grand public pour des applications à portée limitée (badge de transport, de ski, accès bâtiment) ;
- 915 MHz aux États-Unis, de 865 MHz à 868 MHz dans l'Union européenne pour l'UHF (EPCglobal et ISO 18000-6c ; les fréquences et les puissances d'émission dépendent des législations en vigueur) ;
- 2,45 GHz ou 5,8 GHz (micro-ondes), permet des portées de plusieurs mètres, utilisé pour le télépéage notamment.

Une fréquence plus élevée présente l'avantage de permettre un échange d'informations (entre lecteur et marqueur) à des débits plus importants qu'en basse fréquence. Les débits importants permettent l'implémentation de nouvelles fonctionnalités au sein des marqueurs (cryptographie, mémoire plus importante, anti-collision). Par contre une fréquence plus basse bénéficiera d'une meilleure pénétration dans la matière.

L'anti-collision est la possibilité pour un lecteur de dialoguer avec un marqueur lorsque plus d'un marqueur se trouvent dans son champ de détection. Plusieurs algorithmes d'anti-collision sont décrits par les normes (ISO 14443, ISO 15693 et ISO 18000).

1.2 Radio-étiquettes

Ce sont des dispositifs passifs, ne nécessitant aucune source d'énergie en dehors de celle fournie par les lecteurs au moment de leur interrogation. Auparavant, la lecture des puces passives était limitée à une distance d'environ 10 mètres, mais maintenant, grâce à la technologie utilisée dans les systèmes de communications avec l'espace lointain, cette distance peut s'étendre jusqu'à 200 mètres.

Outre de l'énergie pour l'étiquette, le lecteur envoie un signal d'interrogation particulier auquel répond l'étiquette. L'une des réponses les plus simples possibles est le renvoi d'une identification numérique, par exemple celle du standard EPC-96 qui utilise 96 bits. Une table ou une base de données peut alors être consultée pour assurer un contrôle d'accès, un comptage ou un suivi donné sur une ligne de montage, ainsi que toute statistique souhaitable.

Le marqueur est extrêmement discret par sa finesse (parfois celle d'une feuille de rhodoïd), sa taille réduite (quelques millimètres), et sa masse négligeable. Son coût étant devenu minime, on peut envisager de le rendre jetable, bien que la réutilisation soit plus « écologiquement correcte ».

Le marqueur se compose :

- d'une antenne ;
- d'une puce de silicium ;
- d'un substrat et/ou d'une encapsulation.

Notons aussi l'existence des marqueurs « actifs » et « semi-actifs » (aussi appelés BAP, (en) *Battery-Assisted Passive tags*, (fr) *marqueurs passifs assistés par batterie*) qui incluent une batterie.

Les étiquettes actives sont équipées d'une batterie leur permettant d'émettre un signal. De ce fait, ils peuvent être lus depuis de longues distances, contrairement aux marqueurs passifs. Cependant, une émission active d'informations signale à tous la présence des marqueurs et pose des questions quant à la sécurité des marchandises.

Les étiquettes semi-actives n'utilisent pas leur batterie pour émettre des signaux. Elles agissent comme des étiquettes passives au niveau communication. Mais leur batterie leur permet, par exemple, d'enregistrer des données lors du transport. Ces étiquettes sont utilisées dans les envois de produits sous température dirigée et enregistrent la température de la marchandise à intervalle régulier.

Les étiquettes sans puces font aussi leur apparition, c'est l'impression de l'étiquette qui engendre un identifiant unique. D'un coût très faible, ces dernières peuvent être une alternatives au code-barres[4].

2 Contraintes

2.1 Éthique, vie privée

2.1.1 Dans le Monde

Dans les années 2000 dans tous les pays industrialisés, les puces RFID se banalisent très vite. En 2010, l'implantation de micropuces « chez l'homme se pratique (exemple : puce VeriChip ou « *code barre humain* »), avec le risque corrélatif de formes de contrôle de l'individu et de la société »[5], avant même que la législation n'ait eu le temps de s'appuyer sur une réflexion éthique approfondie, notamment concernant les dispositifs actifs ou passifs et de plus en plus miniaturisés (en 2006, Hitachi proposait déjà une puce carrée de 0.15 x 0,15 mm ; plus petite que le diamètre de certains cheveux[6]). Implantables ou implantés dans le corps humain[5], dans ou sur les vêtements

(*wearable computing* ou *cyber-vêtement*), les objets communicants (une société allemande, *Ident Technology*[7], a mis au point des dispositifs faisant de la peau humaine ou animale vivante ou d'autres parties du corps un transmetteur de données numériques)[5], ces puces sont autant d'innovations qui sont aussi sources de questions éthiques et de risques de dérives nouveaux[8],[9].

2.1.2 En Europe

Après un rapport de 2005 sur les nouveaux implants dans le corps humain[10] et après une table ronde organisée par le GEE (Groupe Européen d'Éthique des Sciences et des Nouvelles Technologies)[11] fin 2004 à Amsterdam[12], la Commission européenne a demandé un avis au *Groupe interservice sur l'éthique*, dont le secrétariat[13] est assuré par le BEPA (Bureau des Conseillers de Politique européenne)[14]. Il travaille en lien avec le *Groupe européen d'éthique des sciences et des nouvelles technologies*[15] lequel - à la demande du GEE - a produit, le 16 mars 2005, un avis intitulé *« Aspects éthiques des implants TIC dans le corps humain »*[5].

Les droits fondamentaux concernés sont la Dignité humaine, le Droit à l'intégrité de la personne, la Protection des données à caractère personnel (voir la Charte des droits fondamentaux de l'Union européenne[16]).

La question touche aussi la santé publique, la protection de la vie privée dans le secteur des communications électroniques[17], la législation sur les dispositifs médicaux implantables actifs[18], le consentement et le droit à l'information[19], la protection du génome humain[20], la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[21], les possibles utilisations abusives[22].

En mai 2009, la Commission européenne a publié une Recommandation [23]axée sur la désactivation systématique des tags RFID au point de vente. Pour les applications ne désactivant pas systématiquement les tags, la mise en service de l'application RFID est soumise à la réalisation d'une évaluation d'impact sur la vie privée (EIVP ou Privay Impact Assessment PIA en anglais). En juillet 2014, une norme européenne vient d'être publiée (EN 16571) donnant la méthodologie à suivre pour réaliser une EIVP. Le rapport d'EIVP doit être transmis à l'organisme chargé de la protection des données à caractère personnel (en France, la CNIL) 6 semaines avant la mise en service de l'application.

2.1.3 En France

En France où existe conformément à la législation européenne un droit à l'intégrité physique, la CNIL s'est inquiétée - dans son rapport annuel du 16 mai 2008 - des risques de traçabilité des individus qui n'ont pas accès à leurs données.

2.2 Obstacles

2.2.1 Environnement métallique

La lecture de radio-étiquettes posées sur des objets situés dans un conteneur métallique est plus difficile. Du fait de la présence d'un plan de masse, l'accord de l'antenne du tag est modifié. Ceci peut réduire de manière drastique la distance de lecture. De nouvelles familles de tags intègrent la présence d'un plan métallique dans le design de l'antenne ce qui permet de garder des distances de lecture proches de celles observées sur des supports plus neutres. Dans tous les cas, un tag placé à l'intérieur d'une enceinte métallique ne pourra pas être lu par un lecteur situé à l'extérieur. C'est l'effet de cage de Faraday, qui réalise un blindage électromagnétique.

2.3 Collisions

Lorsque plusieurs marqueurs se trouvent dans le champ d'un même lecteur, les communications sont brouillées par l'activité simultanée des marqueurs.

La détection de la collision est en fait une détection d'erreur de transmission, à l'aide d'un bit de parité, d'une somme de contrôle ou d'une fonction de hachage. Dès qu'une erreur est détectée, l'algorithme d'anticollision est appliqué.

Plusieurs méthodes d'anticollision ont été développées. Voici les quatre principales :

- La méthode fréquentielle : Chaque marqueur communique sur une plage de fréquences différente avec le lecteur. En pratique, c'est inutilisable à grande échelle.
- La méthode spatiale : Avec une antenne directionnelle et à puissance variable, le lecteur va couvrir petit à petit chaque partie de l'espace pour communiquer avec chaque marqueur et l'inhiber, en attendant de le réactiver pour ensuite communiquer avec. En pratique, la présence de deux marqueurs à faible distance l'un de l'autre rend cette méthode inefficace.
- La méthode temporelle : Le lecteur propose aux marqueurs une série de canaux de temps dans lesquels ils peuvent répondre. Les marqueurs choisissent de façon aléatoire le canal de temps dans lequel ils vont répondre. Si un marqueur est le seul à répondre dans ce canal de temps, il est détecté et inhibé par le lecteur. S'il y a plusieurs marqueurs qui répondent en même temps, il sera nécessaire d'effectuer à nouveau cette méthode. Petit à petit, tous les marqueurs sont connus et inhibés ; il suffit alors au lecteur de réactiver le marqueur avec lequel il souhaite communiquer. En pratique, le côté aléatoire fait que la durée de cette méthode est inconnue.

- La méthode systématique : Il existe de nombreux brevets décrivant des méthodes systématiques. Cette méthode consiste à détecter puis inhiber tour à tour tous les marqueurs en parcourant l'arbre de toutes les possibilités d'identifiants (par exemple, le lecteur envoie une requête du type « Tous les marqueurs dont le premier bit d'identification est 1 doivent se manifester. » Si un seul marqueur se manifeste, le lecteur l'inhibe, et s'intéresse ensuite aux marqueurs avec pour premier bit 0, et ainsi de suite). En pratique, cette méthode peut parfois s'avérer longue.

3 Utilisations

Article connexe : Intergiciel pour étiquettes électroniques.

3.1 Marquage d'objets

- Système implanté d'identification et mémorisation : de manière courante, des puces basse fréquence (125 à 135 kHz) sont utilisées pour la traçabilité d'objets (ex : fûts de bière). La traçabilité d'objets tels que des livres dans les librairies et les bibliothèques ou la localisation des bagages dans les aéroports utilise plutôt la classe haute fréquence (13,56 MHz).

- Une utilisation peu connue de la RFID et qui tend à se développer à l'avenir concerne la gestion rationnelle des déchets ménagers, afin de mettre en place une tarification incitative[24]

- Contrôle d'accès : il se fait par badge de *« proximité »* ou *« mains-libres »*.
  Certaines *« clés électroniques »* d'accès sont des marqueurs permettant la protection « *sans serrures* » de bâtiments ou portières automobiles.
  Les badges mains-libres, permettent une utilisation jusqu'à 150 cm (selon le type d'antenne utilisée). Ils peuvent contenir une Identité numérique ou un certificat électronique ou y réagir et permettent l'accès à un objet communicant ou son activation. Utilisé par exemple pour le contrôle d'accès à des systèmes de transports en commun (exemple Passe Navigo)
  Le contrôle d'accès à des bâtiments sensibles est un domaine où le système de radio-identification remplace les badges magnétiques, permettant l'authentification des personnes sans contact. La radiofréquence de la plupart des badges d'accès ne permet qu'une utilisation à quelques centimètres, mais ils ont l'avantage de permettre une lecture-écriture dans la puce, pour mémoriser des informations (biométriques, par exemple).

- Traçabilité distante d'objets (fixes ou mobiles) : Par exemple, des palettes et conteneurs peuvent être suivis dans des entrepôts ou sur les docks) via des marqueurs UHF (ultra haute fréquence).
  À cette fréquence, la lecture n'est théoriquement pas possible à travers l'eau (et donc le corps humain). Cependant lors des *RFID Journal Awards 2008*, l'entreprise Omni-ID a présenté une étiquette RFID lisible à travers l'eau et à proximité de métal, avec un taux de fiabilité de 99,9 %. Des marqueurs micro-ondes (2,45 GHz) permettent le contrôle d'accès à longue distance de véhicules, comme sur de grandes zones industrielles. Ces marqueurs sont généralement actifs.

- Traçabilité d'aliments : Dans la chaîne du froid, des aliments peuvent théoriquement être *suivis* par une puce enregistrant les variations de température.

3.2 Transactions financières

Article détaillé : paiement sans contact.

Les systèmes de **paiement sans contact** tel que des cartes de crédit, des porte-clés, des cartes à puce ou d'autres dispositifs (téléphone mobile...) utilisent la technologie Radio frequency identification et Near Field Communication pour effectuer des paiements sécurisés. Une puce intégrée et une antenne permettent aux consommateurs de payer avec leur carte (sans contact) sur un lecteur au point de vente.

Certains fournisseurs affirment que les transactions peuvent être presque deux fois plus rapides qu'une transaction classique[25]. Il n'y a ni signature, ni saisie du code PIN requis pour les achats de moins de 25 $ US aux États-Unis, moins de CHF 40 en Suisse et moins de 20 € pour la France.

À Hong Kong et aux Pays-Bas des marqueurs en forme de carte de crédit sont répandus comme moyen de paiement électronique (équivalent de Moneo en France). Elles sont également utilisées à Bruxelles (Belgique) comme titre de transport sur le réseau de STIB (voir MoBIB) et désormais en France, à travers les services de paiement sans contact de Cityzi, expérimentés à Nice depuis 2010[26].

3.3 Marquage d'êtres vivants

- Identification de plantes (arbres de la ville de Paris), d'animaux d'élevage (vaches, cochons) ou d'animaux de compagnie comme les chats et les chiens (grâce à une puce installée sous la peau dans le cou), d'animaux sauvages (cigognes, manchots) : ce sont généralement des puces basse fréquence (125 à 135 kHz).

- Relevés scientifiques : des marqueurs sont aussi des moyens de communication pour la collecte des

données issues des relevés scientifiques (monitoring) produits dans un organisme ou par des stations de mesure isolées et autonomes (stations météorologiques, volcaniques ou polaires).

- Chez l'Homme : des radio-marqueurs sous-cutanées, originellement conçus pour la traçabilité des animaux, peuvent sans aucune contrainte technique être utilisés sur des humains. La société *Applied Digital Solutions* propose ainsi ses radio-marqueurs sous-cutanés (nom commercial : VeriChip) destinés à des humains, comme une solution pour identifier les fraudes, assurer l'accès protégé à des sites confidentiels, le stockage des données médicales et aussi comme un moyen de résoudre rapidement des enlèvements de personnalités importantes.
  Combinés à des capteurs sensibles aux fonctions principales du corps humain, ces systèmes sont aussi proposés comme solution intégrée de supervision de l'état de santé d'un patient.
  Une boîte de nuit de Barcelone (Baja Beach Club) utilise des puces sous-cutanées à radiofréquence pour offrir à ses clients VIP une fonction de porte-monnaie électronique implanté dans leur corps même.
  La ville de Mexico a implanté cent soixante-dix radio-marqueurs sous la peau de ses officiers de police pour contrôler l'accès aux bases de données et aussi pour mieux les localiser en cas d'enlèvement[27]

4 Marché des RFID

En 2005, IBM dénombrait 4 millions de transactions RFID chaque jour.
En 2010, ce constructeur évalue à environ 30 milliards le nombre d'étiquettes RFID produites dans le monde et 1 milliard de transistors par être humain[28].

5 Applications

5.1 Applications existantes

- Accès aux transports publics : Marseille (carte transpass), Lille et région Nord-Pas-de-Calais (Pass Pass) , Paris (Passe Navigo), Rennes (carte KorriGo), Reims (Carte Grand R et tickets unitaires), Nancy, TER Lorraine, Troyes (Busséo), Bruxelles (pass MoBIB), Montréal, Luxembourg, Strasbourg (Carte Badgéo), Le Mans (Carte Moovéa), Lyon (Carte Técély), région Rhône-Alpes (Carte OùRA !), Venise (carte imob.venezia), TER Rhône-Alpes, Nimes (cartes Tango) Suisse (Swisspass CFF).
- Télépéages d'autoroutes.
- Contrôle des forfaits de remontée mécanique dans les stations de sport d'hiver.
- Suivis industriels en chaîne de montage.
- Inventaires : Une analyse académique[29] effectuée chez Wal-Mart a démontré que la radio-identification peut réduire les ruptures d'inventaire de 30 % pour les produits ayant un taux de rotation entre 0,1 et 15 unités/jour.
- Saisie automatique d'une liste de produits achetés ou sortis du stock.
- L'office de tourisme des Hautes Terres de Provence (Alpes-de-Haute-Provence) a créé des promenades où les familles vont de lieux en lieux, en glanant des indices que leur dévoilent de faux rochers, dans lesquels sont dissimulés des haut-parleurs, qui se mettent en marche lorsqu'une puce (collée sur un livret « magique ») en est approchée.
- Dans des universités comme Cornell, des cartes à radio-identification permettent aux étudiants de l'université d'accéder sans formalité à la bibliothèque vingt-quatre heures sur vingt-quatre et sept jours sur sept. Les livres sont munis eux aussi de radio-étiquettes, ce qui élimine toute perte de temps administrative lors des emprunts. Plusieurs bibliothèques sont également équipées aux Pays-Bas, où, depuis le 1er janvier 2004, chaque ouvrage acheté comporte une radio-étiquette (à base d'une puce SLI de Philips). En France, plusieurs bibliothèques ont elles aussi franchi le pas et s'équipent de matériels de radio-identification (par exemplela Bibliothèque de Rennes Métropole au Champs Libres). Le mouvement est en réelle accélération, en raison du grand intérêt fonctionnel que présente cette technologie pour les bibliothèques et du prix des étiquettes, en baisse perpétuelle.
- Antivols utilisés dans les magasins.
- La gestion des parcs de Vélib' à Paris et de Velo'v à Lyon, ainsi que de nombreuses autres solutions de Vélopartage et d'autopartage utilisent des puces de radio-identification[30].
- De nombreuses épreuves populaires de course à pied (comme le marathon de Paris ou le semi-marathon Marseille-Cassis) ou de cyclisme (Tour de France) ou de roller utilisent des puces de radio-identification fixées sur une chaussure, le cadre, ou le dossard de chaque participant, permettant ainsi le chronométrage individuel lors du passage des lignes de départ et d'arrivée.
- Identification de livres pour enfants par le Nabaztag: tag pour téléchargement des livres audio correspondants.

- Identification de containers de substances chimiques, de médicaments[31].
- Identification de mobilier urbain, jeux publics, d'arbres d'ornement pour maintenance et suivi[32].
- Échange de cartes de visites lors d'évènements[33]
- Implants corporels[34].
- Suivi d'un cheptel : nourriture, lactation, poids[35].

5.2 Applications potentielles

Les étiquettes « intelligentes » sont souvent envisagées comme un moyen de remplacer et d'améliorer les codes-barres de la norme UPC/EAN. Les radio-identifiants sont en effet assez longs et dénombrables pour envisager de donner à chaque objet un numéro unique, alors que les codes UPC utilisés actuellement ne permettent que de donner un numéro pour une classe de produits. Cette propriété de la radio-identification permet de tracer le déplacement des objets d'un endroit à un autre, depuis la chaîne de production jusqu'au consommateur final. C'est cette propriété qui fait que la technologie est considérée par de nombreux industriels de la chaîne logistique comme la solution technologique ultime à tous les problèmes de traçabilité, notion essentielle depuis les crises sanitaires liées aux filières alimentaires.

Cependant les solutions de radio-identification, bien qu'opérationnelles, souffrent d'un manque de normalisation. La jungle des solutions proposées par les différents fabricants rend la traçabilité universelle difficile à réaliser.

EPCglobal[36] est une organisation qui travaille dans ce sens sur une proposition de standard international afin de normaliser les usages techniques de radio-identification. Le but est de pouvoir disposer d'un système de distribution homogène des identifiants afin de disposer d'un EPC (*electronic product code* ou code produit électronique) pour chaque objet présent dans la chaîne logistique de chaque entreprise du monde.

Les propriétés des radio-étiquettes permettraient également d'envisager des applications à destination du consommateur final, comme :

- un réfrigérateur capable de reconnaître automatiquement les produits qu'il contient, mais aussi capable de contrôler les dates limites d'utilisation optimale (DLUO) des produits alimentaires périssables ;
- l'identification des animaux grâce à l'implantation d'une puce (déjà obligatoire en Belgique et en Suisse pour les chiens et les chats[37]) ; obligatoire en France pour tous les équidés depuis le 1er janvier 2008.
- le marquage des vêtements ;
- l'identification des adresses postales (UAID), des cartes d'identité (INES).
- l'enlèvement des nouveau-nés. En France, la clinique de Montfermeil utilise des bracelets équipés de puce RFID.
- la lutte contre la contrefaçon avec des puces plus difficiles à imiter que les code-barres classiques
- le stade d'avancement d'un produit dans sa chaîne de fabrication (automobile)
- l'identification des produits pour un passage plus rapide en caisse
- l'identification d'utilisateurs de différents biens ou services, comme le rechargement de véhicules électriques[38].

5.3 Galerie

- Bandes de fréquences possibles et légales
- Antennes d'étiquettes UHF et HF
- Matériel d'insertion et puce d'identification animale (fréquence : 2 kHz)
- Lecteur et puce insérée dans le cou d'un chien
- Puce RFID encapsulée, de 5 cm (125 kHz)
- BMicro-puce contenant des données biométriques, insérée dans un passeport.
- Puce RFID passive (Chip Rfid Ario 370DL) en « bouton », adaptée aux uniformes et textiles (résistance aux traitements en blanchisseries)
- Transpondeur *Fast-track* sur un pare-brise, utilisé par exemple pour le péage urbain (accroche velcro)

6 Empreinte environnementale

Article détaillé : Empreinte environnementale de la RFID.

À l'instar de toute production industrielle, la production de puces RFID consomme des ressources naturelles et produit des gaz à effet de serre. Il n'y a malheureusement à ce jour que très peu d'études portant sur l'impact environnemental direct de la production et du recyclage de cette technologie[39].

Cependant, la RFID connaît un essor, notamment pour répondre aux enjeux environnementaux, au sein des chaînes de production, dans la gestion des déchets ainsi que dans le domaine du transport et de la géolocalisation.

Ainsi, par exemple, dans certaines villes européennes, les poubelles résidentielles sont équipées de puces RFID. Les camions poubelles, équipés de lecteurs RFID, identifient les poubelles ramassées grâce à leurs puces [40]. Cette gestion des déchets par RFID permet une meilleure surveillance de leur nature et de leur quantité afin d'optimiser leur traitement.

7 Dangers

Article détaillé : Sécurité de l'information au sein des RFIDs.

Les technologies de radio-identification pourraient s'avérer dangereuses pour l'individu et la société (ex : santé et protection de la vie privée)[41], avec :

- possibilité d'atteinte à la vie privée dans le cas de marqueurs « furtifs » ou accessibles à des systèmes susceptibles de diffuser des informations sur la vie privée ;
- utilisation d'informations contenues par les marqueurs de passeports pour agresser sélectivement et par simple proximité physique les ressortissants de certaines nationalités ;
- « marquage » abusif et facilité de personnes ayant acheté ou emprunté certains types de films, livres (politique, religion, etc.) comme « indésirables » dans les fichiers d'employeurs potentiels ou d'un État répressif (possible à l'heure actuelle sans cette technologie) ;
- problèmes potentiels de « souveraineté numérique/économique » liés à l'infrastructure du réseau EPCGlobal, notamment s'agissant de l'administration, par contrat, de sa racine (onsepc.com) par un acteur privé (américain) ;
- la puce sous-cutanées pose des questions éthiques et de droit à l'intégrité physique. La limitation au volontariat et consentement éclairé n'assure pas de garantie de respect de la vie privée (Cf. charte des droits de l'homme, et en Europe, la Charte des droits fondamentaux de l'Union européenne) ; dans certains contextes des personnes refusant ces étiquettes sous-cutanées risquent d'être victimes de discriminations ;
- identification de personnes par une signature de l'ensemble des étiquettes d'identification par radiofréquences (cartes bancaires, téléphone mobile, pass de transports en commun…) habituellement portées (cf. brevet IBM : Identification and Tracking of Persons Using RFID Tagged Objects par ex.) ;
- au-delà d'un certain seuil de concentration, l'émission de signaux radio-fréquences pourrait s'avérer dangereuse pour la santé (effets suspectés d'un smog électromagnétique croissant...), après la constatation de cancers dans le cas d'expériences sur la souris[42] ou d'interférences pouvant perturber le fonctionnement des appareils bio-médicaux[43].

  Dans un rapport publié le 26 janvier 2009[44], l'AFSSET recommande de poursuivre la veille scientifique sur la recherche d'effets biologiques des rayonnements liés au RFID.

7.1 Protection de l'individu

Article connexe : Vie privée et informatique.

La législation française prévoit une certaine protection de la vie privée en interdisant :

- le contrôle clandestin (toute identification doit faire l'objet d'une indication visible) ;
- l'usage des mêmes appareils pour le contrôle d'accès et le contrôle de présence.

Selon l'association allemande FoeBuD, la législation n'est pas assez restrictive pour la technologie de radio-identification et la protection des informations personnelles[45].

Certaines associations proposent des outils pour se protéger d'une utilisation non autorisée de la radio-identification, tel que RFID Guardian[46].

D'autres associations proposent le boycott de cette technologie qu'elles estiment liberticide[47]. Selon elles, le fichage d'informations non contrôlables dans une carte d'identité électronique serait préjudiciable à la liberté des individus[48].

En 2006 un groupe de hackers a annoncé à la convention bi-annuelle Sixth HOPE à New York avoir cracké (cassé) les sécurités de la fameuse puce sous-cutanée[49]. Ils prétendent aussi avoir pu la cloner[50]. Ils estiment que la législation est trop souple avec cette technologie, au regard de son potentiel d'atteinte à la vie privée et de fuite d'information.

Certains sacs à main possèdent une poche anti-RFID, pour les cartes de crédit et les passeports, qui empêche l'accès non autorisé aux informations personnelles.

7.2 Une sécurité certifiée

L'ANSSI a délivré le 24/10/2013 pour la première fois la Certification de sécurité de premier niveau (CSPN) pour le lecteur RFID LXS W33-E/PH5-7AD, version 1.1 développé par la société Systèmes et Technologies Identification (STid)[51]. Cette certification est destinée à fournir à l'acquéreur potentiel la garantie d'avoir un produit très sécurisé.

8 Notes et références

[1] legifrance.gouv.fr - décision de la Commission générale de terminologie et de néologie sur le terme français *radio-identification*, le 9 septembre 2006 [PDF]

[2] lefigaro.fr “Le premier homme contaminé par un virus informatique”,lefigaro.fr, mai 2010

[3] http://www.guideinformatique.com/fiche-rfid-470.htm

[4] « Identification par radiofréquence », sur *http://iste-editions.fr* (consulté le 18 décembre 2014)

[5] groupe européen d’éthique des sciences et des nouvelles technologies (2005), Aspects éthiques des implants TIC dans le corps humain, Avis du groupe européen d’éthique des sciences et des nouvelles technologies, PDF, 39 pages, consulté 2013-03-09

[6] Hitachi, *World’s smallest and thinnest 0.15 x 0.15 mm, 7.5µm thick RFID IC chip - Enhanced productivity enabled by 1/4 surface area, 1/8th thickness* (ou version pdf) communiqué Tokyo, 2006-02-06, consulté 2013-03-09

[7] Ident Technology

[8] Rafael Capurro(Distinguished Researcher in Information Ethics, School of Information Studies, University of Wisconsin-Milwaukee, USA) 2010, *Ethical Aspects of ICT Implants in the Human Body* présentation (PPT) faite pour l'IEEE au Symposium on Technology and Society (ISTAS10) University of Wollongong, New South Wales, Australia June 7-9, 2010

[9] Vidéo du pr. Rafael Capurro lors de l'ISTAS 10 (10e Symposium IEEE sur les technologies et la société) ; conférence "Ethical Aspects of ICT Implants in the Human Body", consulté 2013-03-09

[10] Dr Fabienne Nsanze (2005), rapport « ICT implants in the human body – A Review », février 2005

[11] Site du GEE

[12] table ronde intitulée [PDF] "The ethical aspects of ICT implants in the human body" du 2004-12-21 (http://ec.europa.eu/bepa/european-group-ethics/docs/publications/tb21dec_ict_en.pdf : PDF, 87 pages)

[13] Secrétariat du GEE (*Groupe interservice sur l'éthique*)

[14] BEPA, *Bureau des conseillers de politique européenne (BEPA)* qui se veut être une « passerelle entre les décideurs politiques de la Commission européenne et les acteurs de la société qui peuvent contribuer utilement à l'élaboration des politiques européennes » (groupe organisé sur 2 piliers "*Outreach*" et "*Analyse*", directement placé sous l'autorité du Président de la Commission)

[15] Commission européenne, et mandat 2011-2016, consulté 2013-03-09

[16] JO C 364 du 18.12.2000, pp. 1 à 22, du 28 septembre 2000, approuvée par le Conseil européen de Biarritz (2000-10-14) et proclamée solennellement à Nice par le Parlement, le Conseil et la Commission le 7 décembre 2000

[17] JO L 201 du 31.7.2002, p. 37 à 47.

[18] rective 90/385/CEE du Conseil, du 20 juin 1990, concernant le rapprochement des législations des États-membres relatives aux dispositifs médicaux implantables actifs (JO L 189 du 20.7.1990, p. 17 à 36.)

[19] Cf notamment la http://conventions.coe.int/treaty/fr/treaties/html/164.htm Convention du Conseil de l'Europe sur les droits de l'homme et la biomédecine], signée le 4 avril 1997 à Oviedo (voir notamment art 5 à 9 et art 10)

[20] Cf. *2228&URL_DO=DO_TOPIC&URL_SECTION=201.html Déclaration universelle sur le génome humain et les droits de l'homme*, adoptée par l'Unesco le 11 novembre 1997

[21] *Convention du Conseil de l’Europe, du 1er janvier 1981, pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*

[22] Cf. point 58 (NTIC) et point 59 (usages abusif des TIC) de la Déclaration de principes du Sommet mondial sur la société de l’information (2003-12-12) sur l'utilisation des technologies de l’information et de la communication (TIC)

[23] « Recommandation Européenne 12 mai 2009 »

[24] « le RFID au service d’une gestion rationnelle des déchets », sur *www.greenit.f*, 12 septembre 2014 (consulté le 30 septembre 2014)

[25] Smart Card Alliance 2003, p. 14

[26] http://www.cityzi.fr/infos/villes/nice/reglez-vos-achats-avec-le-service-m-carte-credit-mutuel

[27] - Mexico’s Rich Embedding GPS-Assisted RFID Tags Under Their Skin In Case of Kidnapping

[28] Smart Objects : IBM Global Technology Outlook 2005.

[29] Recherches RFID portant sur la réduction des ruptures de stock chez Wal-Mart, Radio RFID

[30] filrfid.org - Vélib et radio-identification

[31] Advanco et Sanofi, ou IBIZZ et Pfizer pour la traçabilité des médicaments.

[32] Analogon suivi et maintenance de matériel urbain, jeux publics, arbres d'ornement.

[33] DMD Associates spécialiste de l'échange de cartes de visites électroniques par RFID

[34] Maintag implants corporels.

[35] Maintag contrôle de la lactation.

[36] epcglobalinc.org

[37] Jean-Baptiste Waldner, *Nanocomputers & Swarm Intelligence*, Londres, ISTE, 2007, 242 p. (ISBN 9781847040022)

[38] http://www.avem.fr/actualite-mondial-2010-les-bornes-de-recharge-technolia-1778.html

[39] AFSSET 2008, p. 98

[40] Thomas 2008, p. 1

[41] Dossier futura-sciences. Puce RFID : mythes et réalités du Big Brother miniaturisé - 02/11/2005

[42] Les puces RFID à l'origine de cancers chez les souris

[43] van der Togt R, Jan van Lieshout E, Hensbroek R, Beinat E, Binnekade JM, Bakker PJM, *Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment*, JAMA, 2008 ;299 :2884-2890

[44] Avis de l'Agence française de sécurité sanitaire de l'environnement et du travail - AFSSET, 26 janvier 2009 [PDF]

[45] (de) Association allemande FoeBuD pour prévenir les abus potentiels des radio-marqueurs

[46] Libération/écrans - Interview de Mélanie Rieback (juin 2006)

[47] Pièces et main d'œuvre - RFID : la police totale [PDF]

[48] L'En Dehors - Vers un contrôle social policier sans faille

[49] Annonce de cassage des sécurités de la puce sous-cutanée

[50] VeriChip's human-implatable RFID chips clonable, sez hackers. Engadget 24/07/2006

[51] Liste des produits certifié par l'ANSSI : http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/ Produit certifié :http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/certificat_cspn_2013_08.html

9 Voir aussi

9.1 Bibliographie

- Michel Alberganti, *Sous l'œil des puces, la RFID et la démocratie*, éditions Actes Sud, 2007.
- Philippe Lemoine, « Communication de M. Philippe Lemoine relative à la radio-identification », sur *www.cnil.fr*, CNIL, 30 2003[PDF]
- Pièces et Main d'Œuvre, *RFID : la police totale*, éditions de L'Échappée, 2008, 80 p.
- Michel Alberganti et Pierre Georget, *La RFID : Quelles menaces, quelles opportunités ?*, Prométhée, coll. Pour ou contre ?, Bordeaux, 2008 (ISBN 978-2916623030)
- Étienne Perret, *Identification par radiofréquence : de la RFID à la RFID sans puce*, ISTE Editions, 2014 (ISBN 978-1784050559)
- AFSSET, Les systèmes d'identification par radiofréquences (RFID) - Evaluation des impacts sanitaires, décembre 2008, 1-153 p. (lire en ligne)
- (en) V.M. Thomas, « Environmental implications of RFID », *International Symposium on Electronics and the Environment, 2008. ISEE 2008. IEEE*, mai 2008, p. 1-5 (ISBN 978-1-4244-2272-2, DOI 10.1109/ISEE.2008.4562916)
- (en) Smart Card Alliance, Contactless Payment and the Retail Point of Sale : Applications, Technologies and Transaction Models, mars 2003, 50 p. (lire en ligne [PDF])

9.2 Articles connexes

- Billet électronique
- Communication en champ proche
- Contrôle d'accès
- Contrôle social
- Distance-bounding protocol
- Empreinte environnementale de la RFID
- Exploration de données
- Fichage
- Identité numérique
- Intergiciel pour étiquettes électroniques
- Internet des objets
- Puce sous-cutanée
- Sécurité de l'information au sein des RFIDs
- Système de gestion de cartes à puce

9.3 Liens externes

- (en) Archive of the RFID Consultation Website of the European Commission : a service by CE RFID
- (fr) (en) Centre National de référence RFID
- Portail francophone de la RFID

- Portail des télécommunications
- Portail de l'électricité et de l'électronique

10 Sources, contributeurs et licences du texte et de l'image

10.1 Texte

- **Radio-identification** *Source :* https://fr.wikipedia.org/wiki/Radio-identification?oldid=125208333 *Contributeurs :* Tonnelier, Hemmer, Kelson, Semnoz, Fred.th, HasharBot, Alain Caraco, Raph, Fafnir, Nguyenld, Phe, MedBot, ChrisJ, TigH, Phe-bot, Louis-garden, JB, Ollamh, Nanax, Fylip22, Monster1000, Tintamarre, Yorick, KevinD~frwiki, Valérie75, François-Dominique2, The RedBurn, Jef-Infojef, Ste281, Poppyto, Ofol, StephaneCottin, Bob08, Mogador, Pierre-Étienne Messier~frwiki, Len'Alex, En rouge, Sherbrooke, BrightRaven, Epommate, DocteurCosmos, Wart Dark, ZeMeilleur, Stéphane33, RobotE, Like tears in rain, Romanc19s, David Berardan, Nykozoft, AnoNimes, Probot, Olivier Genest, A3nm, Gzen92, Scls19fr, RobotQuistnix, Sysco, FlaBot, Clicsouris, YurikBot, LeonardoRob0t, Eskimbot, Zelda, Gehel, MistWiz, Jerome66, Bortzmeyer, Passoa15, Litlok, Toutoune25, Zanion, Myst, Mutatis mutandis, Vetruve, Dadu, Freewol, Pautard, LaMerguez, Michel Rousseau, Orel-fr, Cédric Boissière, Esprit Fugace, SashatoBot, Overmac, Mini.fb, MetalGearLiquid, Lamiot, Liquid-aim-bot, Monsieur Fou, Ἐπίκουρος, Tunahead, Stephane.lecorne, NicoV, Thijs !bot, Bibliorock, Bourrichon, Piglop, Kyle the bot, Trex, Cyberic71, Laurent Nguyen, Le Pied-bot, Tannoz, Dauphiné, JAnDbot, Bacchus nx, Arkanosis, Zedh, Manuguf, Jbw, Christian.Mercat, Nono64, Sevenstones~frwiki, Alchemica, Van Rijn, CommonsDelinker, RigOLuche, Numbo3, Olivier Hammam, Wikig, Salebot, GabHor, Speculos, Zorrobot, Stef48, Isaac Sanolnacov, Magmarama, TXiKiBoT, VolkovBot, Cdiot, Yackermann, Nodulation, Jean-Louis Swiners, Cbyd, Reel, Papardelle, Joannaj, Gz260, ArnaudM, SieBot, Hellotheworld, Funto~frwiki, DaBot~frwiki, Cépey, DavidBourguignon, JLM, Zil, Mathieuw, Lilyu, Hercule, DumZiBoT, Gilbertus, Flobel, SniperMaské, HERMAPHRODITE, Michco, Pierre Guillard, Trimégiste, Superjuju10, HerculeBot, Dominiquelazure, WikiCleanerBot, Maurilbert, F1jmm, Leyo, ZetudBot, Bazook, Karenferreirameyers, Maschinenjunge, Guillaume70, Panpan95, Arnaud.trebaol, LaaknorBot, Tanhabot, JackPotte, JeanBono, Oli west, Morcandel, ABACA, GrouchoBot, ChenzwBot, Thefredexperience, JmCor, MagnusA.Bot, Copyleft, Asavaa, Spacebubble, K2R Nolween Leroy, Mikefuhr, Clumsy and stupid, Abracadabra, Xqbot, Obersachsebot, RibotBOT, Rubinbot, GhalyBot, JackBot, Drongou, Bichouille, Dorval28, Coyote du 57, Lomita, TobeBot, Dinamik-bot, Identia, KamikazeBot, GrrrrBot, Gilles.Grimaud, Frakir, EmausBot, Ediacara, Kilith, Orto-Jan, Flocondeneige55, WikitanvirBot, Jules78120, Jules Buech, CocuBot, Ipipipourax, OrlodrimBot, Le pro du 94 :), Ludovic DROUARD, Lechristo, Matthieu.Mastio, Shannah2282000, Hundarja Childeric, CNRFID, Leodegar, Le Bibliophile, Addbot, AméliorationsModestes, RFConception, Siecledigital, Corbac91, Bcag2, Zixiid, Ctetelin, Cyrille.toulet, S.larakeb, Fugitron, Anpanman, Pasum, Vianneydl, Fabienpe et Anonyme : 245

10.2 Images

- **Fichier:Crystal_Clear_app_linneighborhood.png** *Source :* https://upload.wikimedia.org/wikipedia/commons/d/d0/Crystal_Clear_app_linneighborhood.png *Licence :* LGPL *Contributeurs :* All Crystal icons were posted by the author as LGPL on kde-look *Artiste d'origine :* Everaldo Coelho and YellowIcon
- **Fichier:EPC-RFID-TAG.svg** *Source :* https://upload.wikimedia.org/wikipedia/commons/d/d8/EPC-RFID-TAG.svg *Licence :* CC-BY-SA-3.0 *Contributeurs :*
- EPC-RFID-TAG.jpg *Artiste d'origine :*
- derivative work : Sakurambo (talk)
- **Fichier:Fastrak_toll_diagram.jpg** *Source :* https://upload.wikimedia.org/wikipedia/commons/1/1f/Fastrak_toll_diagram.jpg *Licence :* Public domain *Contributeurs :* English wikipédia Fastrak *Artiste d'origine :* Image from California Department of Transportation, originally located at http://www.dot.ca.gov/fastrak/atas.htm.
- **Fichier:Microchip_rfid_rice.jpg** *Source :* https://upload.wikimedia.org/wikipedia/commons/c/c7/Microchip_rfid_rice.jpg *Licence :* Public domain *Contributeurs :* Aucune source lisible par la machine fournie. « Travail personnel » supposé (étant donné la revendication de droit d'auteur). *Artiste d'origine :* Pas d'auteur lisible par la machine identifié. Light Warrior supposé (étant donné la revendication de droit d'auteur).
- **Fichier:Nuvola_apps_ksim.png** *Source :* https://upload.wikimedia.org/wikipedia/commons/8/8d/Nuvola_apps_ksim.png *Licence :* LGPL *Contributeurs :* http://icon-king.com *Artiste d'origine :* David Vignoni / ICON KING
- **Fichier:RFID_Chip_008.JPG** *Source :* https://upload.wikimedia.org/wikipedia/commons/6/63/RFID_Chip_008.JPG *Licence :* CC BY-SA 3.0 *Contributeurs :* Aucune source lisible par la machine fournie. « Travail personnel » supposé (étant donné la revendication de droit d'auteur). *Artiste d'origine :* Pas d'auteur lisible par la machine identifié. Maschinenjunge supposé (étant donné la revendication de droit d'auteur).

10.3 Licence du contenu

- Creative Commons Attribution-Share Alike 3.0