Les systèmes d'identification radio (RFID)
— fonctionnement, applications et dangers —

Nicolas Seriot, IL–2005B, Yverdon-les-Bains

13 janvier 2005

Résumé

Nous étudions ici différents aspects de la technologie RFID (*Radio Frequency IDentification*), qui consiste à utiliser des champs électromagnétiques et des ondes radio pour alimenter à distance et communiquer avec des étiquettes.

Après avoir situé la RFID par rapport à d'autres systèmes d'identification automatique, nous exposons son fonctionnement général et faisons un tour d'horizon des nombreuses variantes utilisées, puis évoquons les problèmes techniques ou de sécurité que l'on peut rencontrer.

Nous examinons également quelques applications de la RFID et notamment la norme EPC, qui est sur le point de remplacer le code barre traditionnel. Enfin, nous terminons cette étude par un aperçu des dangers que la RFID peut faire peser sur le respect de la vie privée.

Mots clés : *Identification radio, Auto ID, RFID, EAN, EPC.*

Table des matières

1 Introduction

La technologie RFID (*Radio Frequency IDentification*) — ou identification par fréquence radio — fait partie des technologies d'identification automatique, au même titre que la reconnaissance optique de caractères ou de codes barre. Le but de ces technologies est de permettre l'identification d'objets ou d'individus par des machines.

La technnologie RFID a la particularité de fonctionner à distance, sur le principe suivant : un lecteur émet un signal radio et reçoit en retour les réponses des étiquettes — ou *tags* — qui se trouvent dans son champ d'action. Il existe une variété presque infinie de systèmes RFID ; différents types de mémoire, différentes fréquences, différentes portées, différents types d'alimentation... (voir section 3)

La technologie RFID est utilisée depuis longtemps et à large échelle, notamment dans les secteurs de la logistique, la protection contre le vol ou encore l'identification des animaux. Pendant longtemps, le prix des étiquettes RFID, leur encombrement ainsi que le manque de normalisation ont limité leur développement.

Aujourd'hui, en 2005, après des années de recherche, de miniaturisation et d'efforts de normalisation, la technologie RFID vit une étape majeure de son développement. D'une part, on sait maintenant produire des étiquettes de moins d'un demi-millimètre. D'autre part, les industriels viennent de se mettre d'accord pour adopter le standard EPC (voir section 5), qui s'apprête à compléter puis remplacer les codes barre pour créer un « Internet des objets ». Maintenant que la technologie est au point, il reste encore le problème des coûts de fabrication, qui toutefois ne cessent de baisser.

Les entreprises technologiques et les industriels ont largement financé la recherche, notamment par le biais du *Auto-ID Center* au *Massachusetts Institute of Technology* (MIT). L'identification sans contact est devenue un champ de recherche interdisciplinaire indépendant, qui mêle des domaines tels que les technologies radio, les technologies des semi-conducteurs, la protection des données, la cryptographie ou la téléinformatique. Le marché des systèmes RFID est en très forte croissance, de l'ordre de 30% par an. On prévoit que les ventes de systèmes RFID passeront de 900 millions $US en 2000 à 2650 millions $US en 2005 (Krebs, [1]) et que ce nombre explosera quand les *tags* RFID marqueront chaque objet vendu par la grande distribution.

La technologie RFID, alors qu'elle est en train d'investir la vie quotidienne, reste méconnue du grand public. La documentation disponible reste relativement succinte et les informations sont parfois contradictoires. Les enjeux sont pourtant majeurs, car la RFID peut bouleverser notre vie quotidienne. Pour toutes ces raisons, autant que par intérêt pour les systèmes d'identification et les disciplines qui y sont afférentes, nous avons choisi de nous pencher sur la technologie RFID et tenté d'en synthétiser les aspects les plus saillants.

2 Les systèmes d'identification automatique

Les systèmes RFID font partie des technologies d'identification automatique, que l'on appelle aussi AIDC (*Automatic Identification and Data Capture*). Voici quelques-unes des ces technologies, qu'il est important de connaître pour comprendre le fonctionnement des systèmes RFID.

2.1 Le code barre

Omniprésents dans notre vie quotidienne, les codes barre dominent les systèmes d'identification automatique depuis plus de 20 ans.

Le code barre est un code binaire représenté par une séquence de barres vides et de barres pleines, larges ou étroites, disposées parallèlement. La séquence peut être interprétée numériquement ou alphanumériquement. Elle est lue par balayage optique au laser, c'est-à-dire d'après la différence de réflexion du rayon laser par les barres noires et les espaces blancs. On utilise actuellement une dizaine de types de codes barre différents, sans compter les codes barre à deux dimensions — mais s'agit-il encore de codes barre ?

Le code barre le plus courant est le code EAN (*European Article Number*) — figure 1 —, créé pour répondre aux besoins de l'industrie alimentaire en 1976. Le code EAN est une évolution de l'UPC (*Universal Product Code*) américain, introduit aux États-Unis dès 1973 ; UPC et EAN sont compatibles entre eux.

Fig. 1 – Un code barre EAN (*European Article Number*)

Le code EAN est composé de 13 chiffres : l'identifiant du pays, l'identifiant de la société, le numéro de l'objet chez le fabriquant et un numéro de contrôle. Voir la figure 2[1].

Malgré son grand âge, le code barre conserve des avantages importants comme son coût quasiment nul et sa large diffusion. En revanche, il présente plusieurs inconvénients : il est fragile, doit être lu de manière optique et peut être remplacé par quelqu'un de mal intentionné. De plus, il ne peut pas être modifé à distance, contient peu d'informations et n'a bien sûr aucune capacité de traitement de données.

[1]Pour une explication détaillée du codage EAN : http://www.barcodeisland.com/ean13.phtml. Pour consulter la base EAN : http://www.ean.ch/gepir/client_f.asp

76	.	10807	.	07030	.	9
Système		Fabriquant		Produit		CS

Système	Suisse
Fabriquant	Coop, CH-4002 Basel
Produit	Chocolat en poudre bio, 250g
CS	check sum (somme de contrôle)

FIG. 2 – Structure d'un code barre EAN. — Le numéro *système* indique généralement le pays, mais pas toujours ; il peut aussi bien indiquer le type de produit, c'est notamment le cas pour les livres (978–979) et les périodiques (977). La liste des codes système est disponible sur http://new.ean.ch/french1/08_EAN-International/01-prefix.html.

2.2 La reconnaissance optique de caractères

La reconnaissance optique de caractères (*Optical Character Recognition*, OCR) est utilisée depuis les années 1960. Elle fonctionne avec des polices de caractères conçues pour être lisibles aussi bien par les hommes que par les machines. On l'utilise aujourd'hui dans le domaine administratif et les services bancaires, notamment pour l'encaissement de moyens de paiement, tels que les chèques ou les bulletins de versement.

Si les système OCR ne sont pas plus répandus, c'est notamment dû à la complexité des lecteurs et à leur prix élevé .

2.3 Les *Smart cards*

Une *smart card* (« carte intelligente » ou « carte à puce »), est un système électronique de stockage de données, éventuellement avec une capacité de traitement (carte microprocesseur) qui, par commodité, est incorporé dans une carte en plastique de la taille d'une carte de crédit. Les premières *smart cards* sont apparues en 1984, sous la forme de cartes téléphoniques prépayées. Pour fonctionner, les *smart cards* doivent être placées dans un lecteur, qui entre en contact avec la surface de contact de la *smart card*. Le lecteur fournit à la *smart card* l'énergie et la pulsation d'horloge. Les transferts de données entre le lecteur et la carte se font par une interface série bidirectionnelle (port E/S).

Un des principaux avantages des *smart cards* est que les données qui y sont stockées peuvent être protégées contre les accès (lecture et/ou écriture) non désirés. Les *smart cards* simplifient et sécurisent de nombreux services, à commencer par les transactions financières. En 1992, 200 millions de *smart cards* avaient déjà été produites dans le monde. En 1995, ce chiffre était de 600 millions, dont 500 millions de cartes mémoire et

100 millions de cartes à microprocesseur. Le marché des *smart card* représente donc un des secteurs à plus forte croissance de l'industrie micro-électronique.

Les *smart cards* comptent plusieurs inconvénients, basés sur la nécessité du contact et des manipulations : elles sont vulnérables à la corrosion et la poussière. Les lecteurs qui sont utilisés fréquemment (cabines téléphoniques, automates à billets...) tombent en panne et sont chers à entretenir. De plus, les lecteurs accessibles au public ne peuvent pas être protégés contre le vandalisme.

On distingue deux types de *smart cards* : les *cartes mémoire* et les *cartes à microprocesseur*.

2.3.1 Les cartes mémoire

Les cartes mémoire fonctionnent sur le principe d'une machine à états ; on accède à la mémoire — généralement une EEPROM — selon une logique séquentielle. Elles peuvent contenir des algorithmes de sécurité simples. Les fonctionnalités des cartes mémoire sont généralement optimisées pour une application spécifique. Les applications sont assez rigides, mais les cartes sont bon marché ; on les utilise dans des applications à large échelle, là où le coût est un facteur essentiel.

2.3.2 Les cartes à microprocesseur

Cartes à microprocesseur Comme leur nom l'indique, les cartes à microprocesseur contiennent un microprocesseur, connecté à une mémoire segmentée (segments ROM, RAM et EEPROM). Voir aussi la section 3.6, page 11.

La ROM Elle comprend un système d'exploitation pour le microprocesseur. Le contenu de la ROM est inséré lors de la fabrication de la puce ; il est identique sur toutes les puces issues du même lot et ne peut pas être modifié.

L'EEPROM Elle contient les données et le programme relatif à l'application. La lecture et l'écriture de cette zone mémoire est contrôlée par le système d'exploitation et se fait après la fabrication.

La RAM C'est la mémoire temporaire de travail du microprocesseur. Les données stockées dans la RAM sont perdues quand l'alimentation électrique est interrompue.

Les cartes à microprocesseur sont très pratiques, puisque l'on peut facilement intégrer plusieurs applications différentes dans une même carte (multi-applications).

Les cartes à microprocesseur sont surtout utilisées dans les applications qui demandent un certain niveau de sécurité, comme les cartes pour téléphones GSM ou les cartes de type « porte monnaie électronique ». La possibilité de programmer les cartes à microprocesseur favorise l'adoption rapide de nouvelles applications.

2.4 Les systèmes RFID

Les systèmes RFID sont très proches des *smart cards*. Comme sur les *smart cards*, les données sont stockées sur une puce électronique (*tag*). Cette puce peut être de type « machine à états » ou contenir un microprocesseur, elle peut avoir différents types de mémoire. Par contre, à la différence des *smart cards*, il n'y a pas de contact physique entre la puce et le lecteur ; l'alimentation électrique de la puce se fait par induction électromagnétique. Les données sont aussi transmises selon ce principe, ainsi que par réflexion des ondes radio (voir la section 3.2). C'est bien de là que vient le nom de cette technologie : *Radio Frequency IDentification*.

2.4.1 Historique

1940 La notion de RFID (identification par fréquences radio) date de la 2ème guerre mondiale ; il est lié au développement de la radio et du radar. Pour savoir si les avions qui arrivaient dans l'espace aérien britannique étaient amis ou ennemis, les alliés plaçaient dans leurs avions d'imposantes balises, ou transpondeurs, afin de répondre aux interrogations de leurs radars. Ce système, dit IFF (*Identify : Friend or Foe* ; de nos jours, le contrôle du trafic aérien reste basé sur ce principe), est la première utilisation de la RFID. La première étude dont on dispose sur le sujet est un travail Harry Stockman [2], qui sera suivi notamment par les travaux de F. L. Vernon [3] et ceux de D.B. Harris [4]. Ces deux derniers articles sont considérés comme les fondements de la RFID et décrivent les principes qui sont toujours utilisés aujourd'hui.

1970 Durant les années 1960 et 1970, les systèmes RFID restent une technologie confidentielle, à usage militaire pour le contrôle d'accès aux sites sensibles, notamment dans le secteur nucléaire.

1980 Les avancées technologiques permettent l'apparition du *tag* passif. L'absence de source d'énergie embarquée rend le *tag* moins coûteux. Le *tag* reçoit son énergie par le signal du lecteur. Les distances de lecture obtenues sont de quelques centimètres.

À la fin des années 1970, la technologie se répand dans le secteur privé. Une des premières applications commerciales est l'identification de bétail en Europe. Dès le début des années 1980, plusieurs sociétés européennes et américaines se mettent à fabriquer des *tags* RFID.

1990 Début de la normalisation pour une interopérabilité des équipements RFID.

2004 Le *Auto-ID Center* du MIT devient *EPCglobal* (voir la section 5), une organisation dont le but est de promouvoir la norme EPC (*Electronic Product Code*) — sorte de super code barre stocké dans un *tag* RFID —, élaborée par les universitaires et adoptée par l'industrie.

Pour un historique complet et très bien documenté de la RFID, voir [5].

3 Fonctionnement

On a tendance à réduire les systèmes RFID au rôle de « codes barre du futur ». Mais les systèmes RFID existent en d'innombrables variantes ; il n'est pas possible de les présenter toutes. Nous allons plutôt décrire leur principe général, puis quelques façons de les distinguer, ce qui devrait donner un bon aperçu de leur diversité et de leur fonctionnement.

3.1 Composition d'un système RFID

Un système RFID se compose de deux éléments : l'étiquette (*tag*) et le lecteur (figure 3).

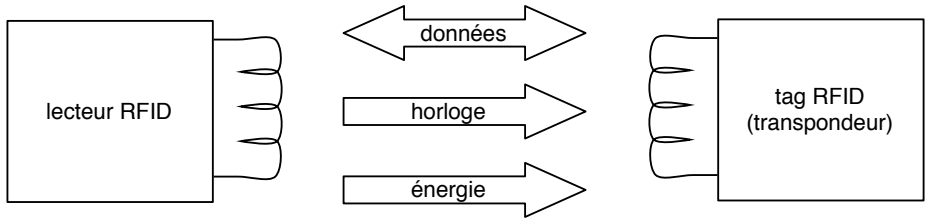

FIG. 3 – Le lecteur et le transpondeur sont les principales composantes de tout système RFID.

3.1.1 Le *tag*

Le *tag* (étiquette) — appelé aussi transpondeur, pour *trans*mitter–res*ponder* — comprend une puce, dotée d'une mémoire, reliée à une antenne bobinée. Le plus souvent, le *tag* est collé sur un film en plastique ou moulé dans une carte au format carte de crédit.

3.1.2 Le lecteur

Le lecteur, selon la technologique utilisée, peut lire mais aussi écrire des données sur le *tag*. Il émet des ondes radio et des champs magnétiques, puis écoute les réponses des *tags* qui se trouvent dans son champ de lecture. Le lecteur contient typiquement un module radio (émetteur et récepteur) et une interface de contrôle. La plupart des

lecteurs fournissent une interface supplémentaire de type RS 232 pour transférer les données reçues à d'autres systèmes (PC, robots, etc.).

3.2 La communication

Quand le transpondeur, qui ne possède généralement pas d'alimentation propre, n'est pas dans le champ d'action d'un lecteur, il est totalement passif. L'énergie, les données et les pulsations d'horloge nécessaires à l'activation et au fonctionnement du transpondeur lui sont fournies par le lecteur. On distingue deux cas, qui peuvent se recouvrir : la communication par champs électromagnétiques et la communication par ondes radio.

La communication par champs électromagnétiques Dans le cas des basses fréquences — moins de quelques MHz — un courant alternatif dans l'antenne du lecteur induit du courant dans l'antenne bobinée du *tag*, ce qui éveille et alimente la puce. La puce effectue les opérations pour lesquelles elle a été conçue, puis créé une modulation d'amplitude ou de phase sur la fréquence porteuse. Le lecteur reçoit ces informations, qu'il transforme en code binaire. Dans l'autre sens, du lecteur vers la puce, les informations circulent selon le même principe, par modulation sur la porteuse. Plus la fréquence est basse, plus le nombre de tours de l'antenne bobinée nécessaires à la création d'un voltage suffisant est important. Cela augmente la complexité et les coûts de fabrication.

La communication par ondes radio Sur d'autres systèmes RFID, notamment si la fréquence utilisée dépasse quelques MHz ou que le *tag* se trouve au-delà d'une certaine distance du lecteur, les données ne peuvent plus être transmises par modulation ; on utilise alors la réflexion des ondes radio. L'électronique du *tag* modifie l'impédance de l'antenne, renvoyant une partie des ondes radio au lecteur. Le lecteur, doté d'un capteur très sensible, décode les données du *tag* d'après le type de réflexion reçu.

On distingue également les communications *full duplex / half duplex* et les communications séquentielles. En mode *full* et *half duplex*, le *tag* diffuse ses informations dès qu'il se trouve dans le champ du lecteur. À l'inverse, dans les procédures séquentielles, le *tag* qui se trouve dans le champ du lecteur est activé brièvement, à intervalles réguliers.

3.3 L'alimentation

Les *tags* passifs Les *tags* passifs ne disposent pas de leur propre source d'énergie ; toute l'énergie nécessaire à leur fonctionnement leur est fournie par le lecteur.

Les *tags* semi-actifs ou actifs Les *tags* semi-actifs fonctionnent comme les *tags* passifs, sauf qu'ils comportent une batterie. Cette batterie ne sert qu'au fonctionnement du microprocesseur ou à la rétention des données. Les systèmes actifs[2], peuvent émettre

[2]Voir le consortium industriel *Smart Active Label Consortium*, qui promeut les *tags* RFID actifs : http://www.sal-c.org/.

des données de manière autonome. Ils ont de meilleures portées, de meilleures capacités de calcul et des mémoires plus importantes, mais ils ont aussi une espérance de vie plus courte, sont plus gros, plus et plus chers à produire.

3.4 Les fréquences

Les systèmes RFID génèrent et réfléchissent des ondes électromagnétiques ; ce sont donc des *systèmes radio* (voir en annexe, page 25) et, à ce titre, ils sont soumis à une législation stricte. Les systèmes RFID doivent notamment veiller à ne pas perturber le fonctionnement des autres *systèmes radio* : (télévision, services de secours, services radio maritimes et aériens, téléphones mobiles, etc). On ne peut, en principe, utiliser que les plages de fréquences spécifiquement réservées aux applications industrielles, scientifiques ou médicales. Ces plages de fréquences sont appelées ISM (*Industrial–Scientific–Medical*).

En plus des fréquences ISM, on utilise les plages de fréquences en dessous de 135 kHz ($<$ 400 kHz pour l'Amérique du Nord, du Sud et le Japon). En effet, en raison de la basse fréquence de l'horloge, le transpondeur nécessite peu d'énergie, ce qui favorise une portée élevée. Le taux de pénétration dans l'eau et les matériaux non métalliques est aussi meilleur.

Plus la fréquence est élevée, plus la vitesse d'horloge permettra des calculs rapides, comme des applications cryptographiques. De même, une bande passante plus large permettra des débits plus élevés. Pas contre, la portée se trouve réduite et la transmission est plus sensible aux interférences.

Les principales plages de fréquences utilisées par les systèmes RFID sont les basses fréquences (125 et 134.5 kHz) et les fréquences ISM : 6.78 MHz, 13.56 MHz, 27.125 MHz, 40.68 MHz, 433.92 MHz, 869.0 MHz, 915.0 MHz (pas en Europe), 2.45 GHz, 5.8 GHz et 24.125 GHz.

La plage de fréquences la plus utilisée est de loin 13.56 MHz (haute fréquence). Suivent ensuite 134.5 kHz (basse fréquence), puis 2.45 GHz (micro-ondes) et 868/915 MHz (UHF).

3.5 La portée et le couplage

On distingue trois types de couplages entre le lecteur et le *tag*. Le couplage est étroitement lié à la fréquence et à la portée du système, qui peut varier de quelques millimètres à plus de 15 m.

Close coupling systems (« systèmes à couplage rapproché ») Ces systèmes ont une portée très faible, jusqu'à 1 cm. Ils fonctionnent avec des champs électromagnétiques, jusqu'à 30 MHz. L'énergie disponible est importante et permet d'utilisation d'un microprocesseur. On retrouve donc ces systèmes dans des applications qui utilisent le chiffrement, comme le verrouillage de portes et les cartes avec des fonctions de paiement. Ces systèmes sont de moins en moins importants sur le marché.

Remote coupling systems (« systèmes à couplage distant ») La portée de ces systèmes va jusqu'à 1 mètre. Ils fonctionnent aussi avec des champs électromagnétiques, par induction. Ces systèmes représentent plus de 90% des systèmes RFID vendus actuellement. Les fréquences généralement utilisées sont 135 kHz et 13.56 MHz. Quelques applications particulières (Eurobalise[3]) fonctionnent à 27.125 MHz.

Long-range systems (« systèmes longue portée ») Ces systèmes portent à plus d'1 mètre. Les *tags* sont trop éloignés pour fonctionner par induction. En revanche, ils réfléchissent les ondes radio. Ces systèmes fonctionnent en UHF à 868 MHz (Europe), 915 MHz (USA) et sur les micro-ondes à 1.5 GHz et 5.8 GHz. La portée des transpondeurs passifs est de 3 mètres, tandis que les transpondeurs actifs, qui comportent une batterie, atteignent plus de 15 mètres.

Les avancées scientifiques permettent chaque année de diminuer la quantité d'énergie nécessaire à l'alimentation des étiquettes. C'est pour les mêmes raisons qu'un PDA peut fonctionner avec des piles alors qu'il a la même puissance de calcul qu'un PC du milieu des années 1980. Chaque années, les systèmes RFID peuvent être concus avec une meilleure portée, puisque les étiquettes consomment moins à la même fréquence.

3.6 La mémoire

Les capacités mémoire des transpondeurs RFID vont normalement de quelques bytes à plusieurs kilobytes. Le cas des « transpondeurs 1 bit » est particulier : une information binaire permet de signaler au lecteur deux états : « le transpondeur est dans le champ » et « le transpondeur n'est pas dans le champ ». C'est peu, mais c'est suffisant pour des fonctions de surveillance ou de signalement. Un transpondeur 1 bit n'a pas besoin de puce électronique, il peut être fabriqué à un coût très bas. Les transpondeurs 1 bit sont généralement utilisés en *Electronic Article Surveillance* (EAS) pour protéger les biens dans les magasins et les entreprises. Les marchandises qui n'ont pas encore été payées portent un *tag*, qui sera détecté par le lecteur installé à la sortie du magasin.

Les mémoires peuvent être en lecture seule, mais aussi en lecture/écriture. Dans les systèmes très simples, les données du transpondeur, en général un simple numéro de série, sont écrites sur la puce lors de la fabrication et ne peuvent pas être modifiées.

[3]Eurobalise : système européen de contrôle ferroviaire.

À l'inverse, dans les systèmes plus complexes, le lecteur peut écrire des données sur le transpondeur. On utilise principalement trois type de mémoire :

Les EEPROMs (*Electrically Erasable Programmable Read-Only Memory*) consomment beaucoup d'énergie durant les opérations d'écriture et le nombre de leurs réécritures est limité — typiquement entre 100'000 et 1'000'000 fois.

Les FRAMs (*Ferromagnetic Random Access Memory*) consomment 100 fois moins d'énergie que les EEPROMs, et le temps d'écriture est 1000 fois plus bref. Pour l'instant des problèmes de fabrication ont retardé la diffusion des FRAMs sur le marché.

Les SRAMs (*Static Random Access Memory*), particulièrement répandues dans les systèmes à micro-ondes, sont très rapides à écrire. Par contre, la rétention des données nécessite une source d'énergie permanente, fournie par une batterie auxiliaire.

Dans les systèmes programmables, les accès mémoire doivent être autorisés par la puce elle-même, en lecture comme en écriture.

3.7 Le format des tags

On trouve des *tags* RFID de toutes formes et de toutes tailles. En voici quelques uns, présentés aux figures 4, 5, 6, 7, 8 et 9.

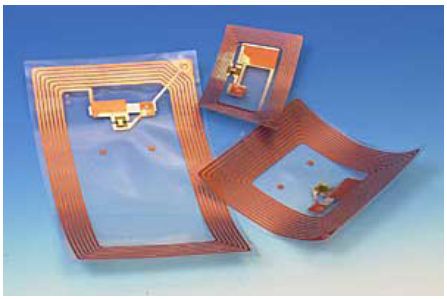

FIG. 4 – Ici, le transpondeur et l'antenne sont fins et souples, collés sur un autocollant. Source : Texas Instruments

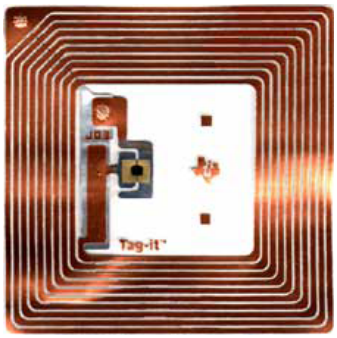

FIG. 5 – Sur cette photo, on distingue bien le transpondeur au centre, entouré d'une antenne de cuivre bobinée. Source : Texas Instruments

3.8 La capacité de traitement de l'information

On distingue trois types de systèmes : les *low-end*, les *mid-range* et les *high-end systems*, allant d'une cpacité de traitement simplement inexistante aux puces les plus sophistiquées, embarquant des coprocesseurs spécialisés.

FIG. 6 – Ce *tag* est conçu pour être injecté sous la peau des animaux. Il est moulé dans un tube de verre de 1 à 3 cm. Source : Verichip

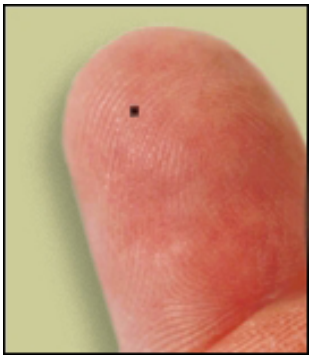

FIG. 7 – Les RFID peuvent être miniaturisés à l'extrême. Ces *tags*, fabriqués par Hitachi, mesurent 0.25 mm^2 ; ils sont pratiquement invisibles. Source : hitachi.com

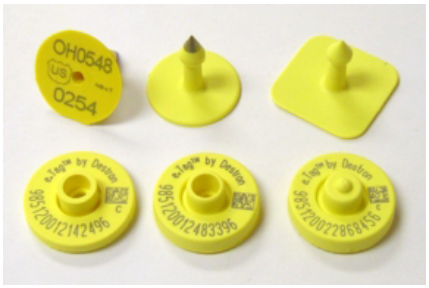

FIG. 8 – Les *tags* sont souvent ronds, éventuellements percés d'un trou pour mieux les fixer. Source : nationalband.com

FIG. 9 – Un lecteur RFID. Source : opticonusa.com

Low-end systems Les systèmes EAS — *Electronic Article Surveillance*, ou surveillance électronique d'articles — contrôlent la présence d'un transpondeur dans la zone d'interrogation du lecteur, généralement un portail. On classe aussi parmi les *low-end systems* les transpondeurs avec une micropuce mais en lecture seule (*read-only*). Les données de ces transpondeurs sont encodées de manière permanente ; elles consistent généralement en un numéro de série unique de quelques bits. Ces systèmes fonctionnent sur toutes les fréquences. Les portées sont généralement grandes du fait de la faible consommation d'énergie. On les utilise là où l'on a besoin de peu de données, par exemple pour remplacer les codes barre, comme en logistique, dans l'identification de palettes, de containers ou de bouteilles de gaz (ISO 18000), mais aussi pour l'identification des animaux (ISO 11785).

Mid-range systems Dans cette catégorie, on trouve plusieurs systèmes à mémoire réinscriptible, et donc de nombreuses applications différentes. La taille des mémoires

varie de quelques bytes aux EEPROMs de plus de 100 Kbytes (transpondeurs passifs) ou SRAM (transpondeurs actifs, avec batterie). Ce sont des machines à états, sans microprocesseurs. Les transpondeurs peuvent traiter des commandes simples pour lire et écrire des données. En général, ils suivent aussi des procédures anticollision, de manière à ce que plusieurs transpondeurs qui se trouvent dans le champ d'action d'un même lecteur au même moment n'interfèrent pas les uns avec les autres et communiquent avec le lecteur les uns après les autres. Certains de ces systèmes implémentent aussi des procédures cryptographiques d'authentification. Ces systèmes fonctionnent sur toutes les fréquences.

High-end systems Ces systèmes sont généralement munis d'un microprocesseur et d'un système d'exploitation (*Smart Card OS*). Le microprocesseur facilite la réalisation d'applications complexes, d'algorithmes de chiffrement et d'authentification. Il existe même des *smart cards* équipées d'un coprocesseur cryptographique ; le temps de calcul s'en trouve grandement réduit et les *smart cards* peuvent servir dans des applications qui nécessitent un chiffrement solide, comme les porte-monnaies électroniques ou les systèmes de tickets pour les transports publics. La plupart de ces systèmes fonctionnent à 13.56 MHz. La transmission des données est décrite dans le standard ISO 14443.

3.8.1 Autres classifications

On pourrait aussi classer les systèmes RFID selon la procédure utilisée par le transpondeur pour renvoyer des données au lecteur, le type de codage binaire et d'autres critères encore. On retiendra qu'il existe une multitude de systèmes, qu'il faut choisir selon l'usage que l'on veut en faire, en étudiant les aspects suivants : portée, environnement électromagnétique, réglementation, prix, interopérabilité, capacité de traitement, capacité mémoire, sécurité (voir section 3.9). On voit aussi que les lignes de partage se recoupent et que les spécifications ne sont pas nettes. Le secteur est en effet trop jeune pour être parfaitement normalisé.

3.9 La sécurité

Les enjeux relatifs à la sécurité des *tags* RFID sont nombreux et importants. Le concepteur de systèmes RFID rencontre les mêmes problèmes que celui qui conçoit des cartes à puces (voir 2.3) : comment empêcher qu'un attaquant puisse lire, modifier ou fabriquer, voire dupliquer les données d'un *tag*, de manière à perturber le système et éventuellement obtenir frauduleusement un accès à un bâtiment ou un service ? Il s'agit d'un problème complexe qui ne connaît pas de réponses parfaitement satisfaisantes.

Dans le cas des systèmes RFID, le fait que les échanges de données se font par ondes radio, ou champs électromagnétiques, ajoute une dimension supplémentaire au problème. D'une part, les menaces qui pèsent sur les *smart cards* avec contact physique sont renforcées par le fait qu'un attaquant peut interagir avec un *tag* RFID à distance, sans même que son propriétaire légitime ne s'en rende compte. D'autre part, il existe une nouvelle

menace, qui pose un défi de taille aux concepteurs : comment empêcher un attaquant d'intercepter la communication radio, pour ensuite « rejouer » la transaction en imitant le *tag* original, un peu à la manière d'Ali Baba devant la grotte des voleurs ?

Il est facile d'imaginer des scénarios catastrophiques pour les acteurs qui utiliseraient des systèmes de paiement électronique mal sécurisés...

Lors de la conférence de sécurité informatique *Blackhat 2004*, un consultant allemand, Lukas Grunwald, a présenté le logiciel libre RFDump[4], qui permet de lire et de modifier différents types de *tags* RFID. Il existe également une bibliothèque[5] de fonctions en langage C écrite par le français Loïc Dachary, libre elle aussi, pour dialoguer avec les *tags* RFID.

3.10 Les problèmes techniques

La technologie RFID, si elle a un petit côté « magique », ne fonctionne pas sans problèmes ; en voici quelques uns, strictement limités au domaine technique.

3.10.1 L'orientation des antennes

Les tags RFID ne nécessitent pas de liaison optique pour fonctionner, mais les lecteurs ne peuvent pas communiquer normalement avec un *tag* dont l'antenne est orientée perpendiculairement à l'antenne du lecteur. On constate le même effet quand on essaie de recevoir une station radio très faible avec une petite radio portable. Si plusieurs produits sont disposés au hasard dans un chariot à commissions, certains seront orientés de telle sorte qu'ils seront invisibles par le lecteur.

Si les produits marqués ne peuvent pas être réorientés, il faut alors modifier l'orientation du lecteur ou construire des antennes moins sensibles à l'orientation. Une autre approche est de mélanger les données de plusieurs lecteurs orientés de manières différentes. On peut encore installer plusieurs antennes et les connecter au lecteur l'une après l'autre, ce qui est certainement la solution la plus économique.

3.10.2 Les collisions

Les premiers *tags* RFID, fabriqués dans les années 1960, fonctionnaient sur de basses fréquences. De nos jours, des fréquences élevées, typiquement sur la bande UHF, améliorent la capacité d'un lecteur à lire plusieurs *tags* se trouvant dans son champ de lecture, car le taux de transfert est plus grand et les données de chaque *tag* sont transmises plus rapidement, réduisant la probabilité de collision entre les données de chacun des *tags* — typiquement lors de la lecture des produits dans un chariot de supermarché.

[4] http://www.rf-dump.org/
[5] http://savannah.nongnu.org/projects/rfid/

Pour réduire les chances que deux *tags* émettent en même temps (collision), les *tags* utilisent un protocole anti-collision pour contrôler la fenêtre de temps durant laquelle chacun répond ; ce temps dépend du numéro unique des tags.

3.10.3 Les lecteurs multiples

La plupart des lecteurs RFID ne sont pas conçus pour fonctionner en présence d'un autre lecteur qui scannerait les tags en même temps. L'ISO est en train d'établir des normes à ce sujet.

3.10.4 Les normes

Le développement de standards est la responsabilité du comité technique de l'ISO. L'ISO est l'union internationale des institutions nationales de standardisation, comme la DIN (Allemagne), l'ANSI (USA), l'AFNOR (France) ou la SNV (Suisse).

Les tags RFID fonctionnent selon des normes comme l'ISO 14443 (13.56 MHz) ou EPCglobal 96-bits (915 MHz) (voir section 5). Dans un monde idéal, toute l'industrie adopterait la même norme. Pour des raisons commerciales, ce n'est pas le cas. Par exemple, Wal-Mart utilise EPCglobal alors que Nokia, le plus grand fabriquant de téléphones portables dans le monde, prépare un téléphone qui inclut un lecteur RFID, mais qui fonctionne avec la norme ISO 14443. Vraisemblablement, on va vers l'utilisation de lecteurs comprenant plusieurs normes...

3.10.5 Les matériaux d'emballage

Les ondes radio peuvent être perturbées par certains emballages, notamment les métaux ferreux.

3.10.6 Les coûts

Le problème principal des systèmes RFID reste leur coût de fabrication. Aujourd'hui, en 2005, un *tag* passif pour étiqueter les produits coûte environ 0.25 $US. Or, cela n'a pas de sens de placer un tel *tag* sur un produit qui coûte à peine plus cher. On estime que les *tags* RFID pourront se répandre dans la grande distribution quand on pourra les produire pour 0.05 $US.

3.10.7 Le format des données

Le format des données renvoyées par les *tags read-only* est standardisé, mais les *tags* inscriptibles fournissent une mémoire flash que l'utilisateur peut utiliser à sa guise. Il y aurait avantage à normaliser la manière dont les données sont représentées, notamment pour que différents partenaires puissent traiter les données enregistrées par les autres. Le format XML serait un bon candidat, mais pour l'instant la mémoire disponible (typiquement 2 Kbits) incite plutôt à l'utilisation d'un format de données plus compact.

4 Applications

Les systèmes RFID sont utilisés depuis plusieurs années, dans des applications relativement classiques. Récemment, les évolutions technologiques ont favorisé leur apparition dans des domaines moins classiques, ce qui soulève d'importantes questions relatives au respect de la vie privée, de la protection des données et des libertés individuelles.

On a déjà évoqué, en examinant les différents types de systèmes RFID, certaines applications courantes comme les systèmes anti-vol dans les magasins (section 3.6), le contrôle d'accès (section 3.7), la logistique, l'identification du bétail (figure 6) et des des animaux de compagnie. La RFID sert également à identifier les bagages dans les aéroports[6], les livres dans les bibliothèques, les documents dans les entreprises, à faire payer les conducteurs aux péages, à relever les données de capteurs, à effectuer des micropaiements[7], à emprunter les transports publics à Londres, Paris[8] ou Venise ou les remontées mécaniques dans les stations de ski. La plupart de ces utilisations sont largement documentées sur Internet, nous ne les décrirons pas en détail ici.

Ces applications se généralisent rapidement. La guerre en Irak a été l'occasion[9] pour l'armée américaine d'utiliser les systèmes RFID à large échelle. Tous les tickets[10] vendus pour la prochaines coupe du monde de football, qui se tiendra en 2006 en Allemagne, seront porteurs de *tags* RFID. Il existe même des machines à laver[11] capables d'indiquer quel est le meilleur programme de lavage en fonction du linge qui se trouve à l'intérieur.

Les *tags* RFID peuvent aussi faire bien plus que simplement renvoyer un numéro ; ils peuvent par exemple être associés à des capteurs et mémoriser les températures de stockage d'une viande, de manière à prévenir les risques d'avarie. Ils peuvent aussi profiter de capacités de calcul (voir 3.8) pour trouver des applications encore insoupçonnées.

5 Le *Electronic Product Code* (EPC)

5.1 Introduction

Parmi toutes les applications des RFID, il en est une qui a longtemps constitué une sorte de fantasme ultime : c'est l'attribution d'un code individuel à chaque objet. Les principaux groupes industriels viennent d'adopter une norme en ce sens, l'*Electronic Product Code* (EPC). Il s'agit d'une tentative ambitieuse de créer un réseau global, normalisé, permettant d'étiqueter et de suivre tout ce qui peut être expédié, stocké ou

[6] http://www.securitymagazine.com/CDA/ArticleInformation/features/BNP__Features__Item/0,5411,116832,00.html

[7] Par exemple la carte *Octopus*, utilisée à Hong-Kong : http://www.octopuscard.com/eng/.

[8] Voir la carte *Navigo*, http://www.ratp.fr/corpo/service/navigo.html.

[9] http://www.eetimes.fr/at/news/showArticle.jhtml?articleID=19504772

[10] http://www.infoworld.com/article/04/01/15/HNrfidsoccer_1.html

[11] http://www.i4u.com/article2134.html

vendu. En fait, l'EPC permet virtuellement de numéroter tous les objets de la planète. Le but est bien sûr pour les industriels d'anticiper la demande, de réduire les stocks, de prévoir les pénuries, bref, les perspectives économiques sont énormes.

La norme EPC a été élaborée en étroite collaboration avec le monde académique, par le *Auto-ID Center*[12], un centre de recherche basé au MIT créé et largement financé par les industriels, avec des laboratoires dans les plus prestigieuses universités du monde. Les laboratoires continuent désormais leurs recherches sous un autre nom, tandis que le *Auto-ID Center* est devenu *EPCglobal*[11], une institution dont le but est de promouvoir et d'encourager l'utilisation de la norme EPC.

Comme le code barre EAN (figure 2), l'EPC (figure 10) est un nombre. Il est plus long que le code EAN et, au lieu d'être imprimé sous la forme de barres parallèles, il est stocké dans un *tag* RFID. Deux boîtes de conserve ont le même code barre EAN, mais des codes EPC différents. En fait, seuls les derniers bits diffèrent, car ils identifient le produit de manière unique ; chaque boîte de conserve a son propre numéro ! On peut se représenter le code EPC–96 comme un code EAN avec un identifiant unique en plus.

De grands acteurs comme IBM adhèrent à l'EPC. IBM fabrique des logiciels qui utilisent le standard EPC pour synchroniser les données entre les systèmes informatiques de sociétés qui travaillent ensemble, éliminant ainsi des erreurs coûteuses et des problèmes de sécurité.

Notre manière de faire des achats s'en trouvera à coup sûr modifiée et l'on risque bien, d'ici quelques années, de faire nos courses dans des supermarchés sans caisses mais dont les lecteurs RFID débiteront nos cartes de crédit automatiquement. C'est d'ailleurs déjà une réalité aux États-Unis dans certaines stations services et commerces de détail[13]. Maintenant que la technologie est presque prête, le principal obstacle demeure les coûts de fabrication, qui restent de l'ordre de 20 centimes, même si de nouvelles technologies comme les encres conductrices[14] permettent déjà des baisses très importantes. Le but est d'atteindre un prix d'un centime par *tag* EPC. On prévoit que la généralisation de ce nouveau standard prendra au moins cinq ans encore ; de nombreuses sociétés devront adapter les logiciels qui gèrent leurs *supply-chain*, puis appliquer les *tags* à chaque palette, carton et emballage.

On peut aussi se demander si la perspective d'une adoption généralisée du système EPC est bien réelle… elle l'est ! Il suffit de savoir d'une part que les membres de EPCglobal (EAN International, Uniform Code Council, Coca-Cola, Pepsi, Gillette, Procter & Gamble, Wal-Mart, Hewlett-Packard, Johnson & Johnson, …) produisent 10% de tout

[12] http://www.autoidcenter.org/
[13] http://www.speedpass.com/
[14] http://www.organicid.com/

01	.	0000A89	.	00016F	.	000169DC0
Header		EPC Manager		Object Class		Serial Number
8 bits		28 bits		24 bits		36 bits

Header	version du standard EPC utilisé
EPC Manager	code du fabriquant
Object Class	type de produit, par ex. « cannette de Coca-Cola, 330 ml »
Serial Number	numéro unique : « cette cannette de Coca-Cola »

FIG. 10 – Structure du code EPC–96 bits — ce code permet de représenter 79 *milliards de milliards de milliards* d'objets différents, un peu moins en pratique du fait du contrôle d'erreur.

ce qui est produit dans le monde. De plus, Wal-Mart, la plus grande chaîne de supermarchés des États-Unis (chiffre d'affaire 2002 : 244.5 *milliards* de dollars) et le Département américain de la défense (DoD)[15] — deux organisations gigantesques — ont exigé l'un comme l'autre de leurs principaux fournisseurs qu'ils utilisent des tags RFID sur chacune de leurs palettes ou de leurs cartons dès janvier 2005.

5.2 L'architecture du réseau EPC

Le nouveau standard EPC ne spécifie pas seulement un format commun pour les numéros des produits mais crée un système complet, un réseau d'informations que certains appellent « l'Internet des objets » (« *Internet of things* »). Ce réseau se compose des éléments[16] suivants :

Le code EPC *Electronic Product Code* — ce code identifie chaque objet de manière univoque. En fait, le code agit comme une clé dans une base de données, il est un « pointeur » vers les informations associées au produit.

Le service ONS *Object Naming Service* — il s'agit d'un service informatique qui, à la manière des serveurs de noms (DNS) qui routent l'information sur Internet, indique où se trouve l'information sur les objets.

Le langage PML *Product Mark-up Language* — c'est un langage, basé sur XML, qui permet de décrire les objets, notamment des caractéristiques telles que dosage, date de péremption, type de lavage machine, couleur, incompatibilités entre médicaments, etc. Il est aussi prévu pour décrire des données dynamiques, telles que volume, température, pression...

[15] http://www.defenselink.mil/releases/2003/nr20031023-0568.html

[16] Toutes les spécifications sont disponibles sur http://www.epcglobalinc.org/standards_technology/specifications.html.

Le logiciel Filter (anciennement Savant) Filter est un logiciel distribué, présent sur chaque point de vente ou de traitement, qui agit comme un « filtre » et communique avec d'autre « filtres » situés ailleurs. Filter s'occupe entre autres de « lisser » et homogénéiser les données, de coordonner les lecteurs RFID, de savoir quelles données communiquer, ou non, et à qui, de maintenir un système de cache, de permettre la surveillance de l'état du système... bref, il s'agit du système nerveux du réseau EPC.

6 Droits et libertés des citoyens/consommateurs

Les systèmes RFID (voir la section *Applications*, page 17), s'ils peuvent simplifier la vie, sont autant de menaces pour le respect de la vie privée et des libertés individuelles. En effet — les informaticiens le savent bien — les applications les plus inoffensives en apparence, comme les cartes de transports publics, laissent des traces du passage de l'individu dans le système informatique. Ainsi, l'administrateur du système et d'autres personnes encore, autorisées ou non, peuvent potentiellement avoir accès à l'historique des déplacements d'un individu : où était-il ? à quelle heure ? où allait-il ?

Dans un supermarché, le porteur d'une carte de fidélité contenant[17] un *tag* RFID peut être suivi ; ses déplacements intéressent certainement beaucoup les cadres du magasin, par exemple ceux qui décident du placement des produits, d'autant plus qu'ils disposent de l'historique de ses achats ; tout cela peut constituer un puissant dispositif de recoupement marketing.

En Suisse, à Genève, les badges des participants au *Sommet mondial de la société de l'information* en 2003 comportaient[18] des *tags* RFID (« *de quoi établir une cartographie complète des personnes présentes selon leurs affiliations ou affinités* » selon Stéphane Koch), sans que les participants n'en soit informés, ce que la loi Suisse exige pourtant.

Pour Katherin Albrecht, directrice de l'association CASPIAN[19], l'un des principaux risques est l'identification d'un individu par les *tags* RFID qu'il porte : « *Si les chaussures que je porte sont associées à mon identité, on peut tracer mon parcours et me suivre partout où je vais dans le monde* ». Elle imagine encore d'autres dangers : « *Un aspirateur pourrait cesser de fonctionner s'il détecte que les sacs qu'on veut y mettre ne sont pas de la marque du fabriquant, et cela pourrait être le cas pour tous les appareils utilisant des consommables, notamment les imprimantes.* »Notons cependant que ce dernier problème n'est pas propre aux tags RFID.

Dans certains cas, les clients doivent signer un document dans lequel ils renoncent à leurs droits à la protection des renseignements personnels ; c'est le cas par exemple

[17] Voir l'histoire de la carte *METRO* : http://www.spychips.com/metro/scandal-payback.html.
[18] http://www.zdnet.fr/actualites/technologie/0,39020809,39134545,00.htm
[19] CASPIAN : *Consumers Against Supermarket Privacy Invasion and Numbering*

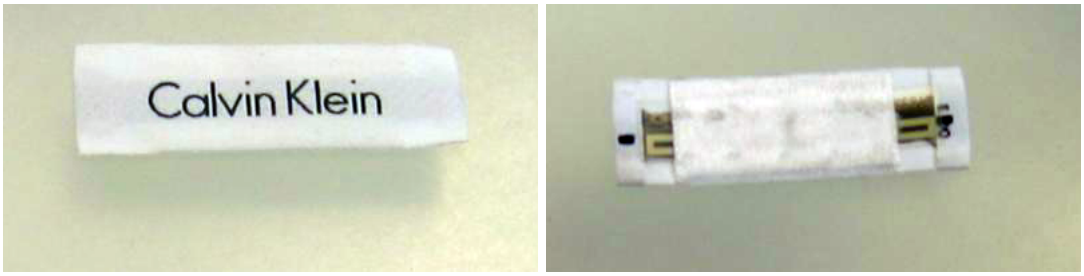

FIG. 11 – Un *tag* RFID dissimulé dans l'étiquette d'un vêtement. Source : spychips.com : http://www.spychips.com/press-releases/checkpoint-photos.html.

dans l'un des plus vastes parcs d'attraction européens, le *Legoland* au Danemark, où des bracelets électroniques rapportent la position des enfants toutes les 8 secondes[20].

Les clients de sociétés privées peuvent refuser d'acheter des biens et services s'ils le souhaitent. Il est plus difficile à un salarié de s'opposer au port d'une carte qui permet de le localiser en temps réel, ou de porter un vêtement[21] contenant une puce RFID.

Il est aussi des applications discutables que l'on ne pourra plus éviter car elles s'imposeront à tous, non plus seulement aux clients de certaines sociétés privées ou à certains salariés, mais à tous les citoyens. On pense aux *tags* RFID dans les documents officiels comme les passeports. D'ici 2006, les passeports américains devront inclure une puce[22] de 64 Ko qui ne contiendra pas seulement un numéro mais aussi des données personnelles telles que la date de naissance et des données biométriques, accompagnées d'une photo au format JPEG, le tout étant non chiffré[23], c'est-à-dire accessible à quiconque muni d'un lecteur RFID se trouvant à quelques mètres. Ces données seront donc lisibles par des escrocs, mais aussi par des hôteliers peu scrupuleux, qui pourront les revendre.

On pense aussi à d'autres systèmes RFID que les citoyens ne pourront pas éviter, comme les plaques minéralogiques[24] ou les systèmes de surveillances des écoliers. C'est par exemple le cas dans le district de Stampa au Texas, où les écoles enregistrent[25] les heures d'arrivée et de départ de 28'000 écoliers, porteurs de puces RFID.

C'est aussi le cas des billets de banque. La Banque Centrale Européenne (BCE) envisage depuis longtemps déjà de placer des *tags* RFID dans les fibres des billets de

[20] http://www.eetimes.fr/at/news/showArticle.jhtml?articleID=19504447
[21] http://www.usatoday.com/tech/news/surveillance/2004-08-30-rfid-uniforms_x.htm
[22] http://www.wired.com/news/privacy/0,1848,65412,00.html
[23] http://www.schneier.com/blog/archives/2004/10/rfid_passports.html
[24] http://allafrica.com/stories/200408040339.html
[25] http://query.nytimes.com/gst/abstract.html?res=F50814F9395B0C748DDDA80994DC404482

banque[26]. Cela permettra de les compter très rapidement, de savoir d'où ils viennent, où ils ont été scannés pour la dernière fois, de lutter contre le blanchiment ou d'éviter les demandes de rançon... On peut imaginer que certains billets pourront être invalidés, en cas de vol par exemple. Il y aura bien sûr de nombreux avantages, mais aussi de nouveaux problèmes, avec des questions comme « qui peut savoir quoi ? ». Est-ce que le marchand d'une boutique pourra savoir combien d'argent le client qui rentre a sur lui ? et le voleur au coin de la rue ? par qui ces données pourront-elles être utilisées ? Toutefois, les billets de banque constituent un environnement très hostile pour une puce électronique et rien n'est encore sûr et la BCE n'a encore rien décidé.

Au-delà même de ces applications discutables, certains considèrent que les *tags* RFID constituent *intrinsèquement* une menace pour la vie privée, parce qu'ils peuvent être lus à l'insu de leur porteur, qui lui-même n'a aucun moyen de savoir qu'il est porteur d'un ou plusieurs *tags* ! Il est vrai que pour l'instant rien n'oblige les distributeurs à indiquer aux consommateurs la présence de *tags*, qui sont parfois incorporés dans l'emballage même des produits, et non pas seulement collés dessus.

Une étape supplémentaire est en train d'être franchie avec l'implantation de *tags* sous la peau des humains. Depuis octobre 2004, l'agence de sécurité sanitaire américaine (*Food and Drug Administration*) autorise[27] les hôpitaux à implanter des *tags* RFID dans le corps des patients, à des fins de suivi médical. De même, 18 officiers de police de la ville de Mexico sont équipés[28] d'une puce dans le bras, fabriquée par *Verichip*[29], ce qui leur permet d'accéder au fichier central de la police, mais les expose aussi à de possibles mutilations de la part de criminels souhaitant accéder à ce fichier...

Les associations américaines comme CASPIAN ou l'*Electronic Frontier Foundation*[30] sont parmi les opposants les plus farouches aux *tags* RFID. En effet, les consommateurs/citoyens américains ne sont pas protégés par des institutions telles que la Commission Nationale Informatique et Liberté (CNIL) française. CASPIAN a élaboré un projet[31] de loi pour protéger les consommateurs.

En Allemagne, l'association *FoeBuD*[32] a conçu un appareil permettant de repérer les *tags* RFID.

[26] http://www.wired.com/news/privacy/0,1848,59565,00.html
[27] http://www.technovelgy.com/ct/Science-Fiction-News.asp?NewsNum=199
[28] http://www.spychips.com/press-releases/mexican-implant-correction.html
[29] http://www.4verichip.com/
[30] http://www.eff.org/Privacy/Surveillance/RFID/
[31] http://www.spychips.com/press-releases/right-to-know-summary.html
[32] http://www.foebud.org/rfid/

7 Conclusion

L'adoption générale et rapide d'une technologie (les ordinateurs personnels, les téléphones portables) se produit au moment où cette technologie fonctionne bien, où les prix sont suffisamment bas et la demande assez grande. Cette heure a sonné pour la RFID. Il reste bien sûr des défis (prix, standardisation, sécurité) mais les systèmes RFID sont sur le point de se répandre massivement.

L'utilisation des RFID pour le suivi des hommes, des animaux et des produits va permettre d'optimiser de nombreux processus industriels, de minimiser les stocks et d'améliorer un certain nombre de services tels que les transports publics par exemple. D'autres usages sont encore à inventer, car on présente souvent le *tag* RFID comme une « étiquette intelligente » ou le « successeur du code barre » mais les RFID sont capables de bien plus que ça (voir la section 3).

« L'internet des objets » (section 5 page 17), résultat d'années de recherche, pose de nombreux défis notamment logiciels, à la fois dans le traitement et l'analyse des montagnes de données qui seront disponibles que dans l'adaptation des infrastructures existantes au réseau global EPC.

La technologie RFID présente toutefois des problèmes techniques (section 3.10 page 15) mais aussi des problèmes de sécurité (section 3.9 page 14) et des problèmes de respect de la sphère privée (section 6 page 20). Ces problèmes, inhérents à toute technologie, sont cette fois particulièrement importants, de par les possibilités de suivi de chaque objet et de chaque personne. Il est aussi dans l'intérêt des industriels de résoudre ces problèmes, sans quoi la RFID pourrait rencontrer une éraction de rejet de la part des consommateurs.

Nous pensons que, comme d'autres sciences capables de changer le monde (nucléaire, manipulations génétiques), la RFID va susciter des débats passionnés, avant d'être encadrée par des législations particulières. Seulement, pour que le débat ait lieu, il est nécessaire que le grand public connaisse puis comprenne cette technologie et soit sensibilisé à ses dangers, ce qui suppose encore un long travail de vulgarisation.

Références

Livres

[1] Klaus Finkenzeller,
RFID Handbook : Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition,
John Wiley & Sons, Ltd., England, 2003,
ISBN 0-470-84402-7
Site web : http://rfid-handbook.com/english/

Articles

[2] Harry Stockmaby,
Communication by Means of Reflected Power,
Proceedings of the IRE, pp. 1196–1204, October 1948

[3] F.L. Vernon, Jr.,
Application of the Microwave,
Homodyne, IRE Transactions on Antennas and Propagation AP-4, 110 (1952)

[4] D. B. Harris,
Radio transmission systems with modulatable passive responder,
Brevet.

[5] Historique de la RFID
http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf

Sites web de référence

[6] http://rfidjournal.com/

[7] http://rfidbuzz.com/

[8] http://rfidlog.com/

[9] http://rfidnews.org/

[10] http://www.rfidgazette.org/

Organismes

[11] EPCglobal
http://www.epcglobalinc.org/

[12] Association for Automatic Identification and Mobility
http://www.aimglobal.org/technologies/rfid/

[13] Auto-ID Labs
http://www.autoidlabs.org/

8 Annexes

Fréquences radio

Fréquences [Hz]	Longueur d'onde λ [m]	Nom	Abbréviation
3 – 300	10^{8} – 10^{6}	extremely low freq.	ELF
300 – 3 k	10^{6} – 10^{5}	ultra low freqency	ULF
3 k – 30 k	10^{5} – 10^{4}	very low freqency	VLF
30 k – 300 k	10^{4} – 10^{3}	low freqency	LF
300 k – 3 M	10^{3} – 10^{2}	medium freqency	MF
3 M – 30 M	10^{2} – 10^{1}	high freqency	HF
30 M – 300 M	10^{1} – 10^{0}	very high freqency	VHF
300 M – 3 G	10^{0} – 10^{-1}	ultra high freqency	UHF
3 G – 30 G	10^{-1} – 10^{-2}	super high freqency	SHF
30 G – 3000 G	10^{-2} – 10^{-4}	extremely high freq.	EHF