

## Le RFID aux Etats-Unis

Publié le jeudi 19 janvier 2006

Voir en ligne : <https://www.france-science.org/Le-RFID-aux-Etats-Unis,7713.html>

### 1. Introduction

Le nom RFID recouvre en fait un ensemble de technologies et d'applications très variées. Portée, bande de fréquences utilisée, prix, encombrement, consommation d'énergie sont des facteurs qui les différencient. Davantage que des équivalents au code barres interrogeables par ondes radio (ou smart labels ou EPC pour Electronic Product Code), les marqueurs RFID peuvent fournir des informations issues de capteurs, ou des données enregistrées et modifiables. Des systèmes plus évolués permettent aussi une communication entre marqueurs. Un système RFID est ainsi constitué de marqueurs/capteurs, de lecteurs, le cas échéant d'un réseau sans fil connecté à un réseau classique, d'un middleware adapté à l'utilisation (collecte des informations, intégration etc.), de services adaptés à l'emploi considéré, côté utilisateur final, ainsi que d'outils de gestion. Aux Etats-Unis, la technologie RFID se répand à une vitesse accélérée ces dernières années. Il est annoncé qu'elle représenterait une activité de plusieurs milliards de dollars (engendrant des économies de plusieurs milliards de dollars dans les chaînes logistiques). La technologie qui suscite le plus d'intérêt actuellement est celle qui utilise les ultra hautes fréquences, bon compromis entre vitesse de lecture, portée, présence de plusieurs marqueur et coût. Un cap important a été franchi fin 2004 avec l'adoption de l'EPC Generation 2 (initialement mis au point par Intermec Technologies, Everett-Washington, la version d'origine EPC ayant été créée par le MIT Auto-ID Lab) comme norme ouverte par l'EPC Global, ainsi que celle du portefeuille complet de la norme ISO/IEC 18000:2004, complété par ISO/IEC TR 24710:2005.

### 2. Applications déployées

Des composants RFID sont utilisés pour le péage autoroutier sur de nombreux réseaux et comme carte de paiement pour certaines stations d'essence Exxon. Cette technologie est également utilisée pour l'identification des animaux (au départ en 125 kHz, puis en 134,2 kHz standard international). Le RFID est notamment utilisé par suite du "National Farm Animal Identification and Records", qui a concerné plus d'un million de têtes de 1999 à 2004. Par ailleurs, plusieurs sociétés proposent des systèmes RFID (incompatibles) pour l'identification des animaux de compagnie, qui sont bien répandus (plusieurs millions). La technologie est surtout utilisée à très grande échelle pour la gestion de la chaîne logistique : Wal-Mart, la plus grande chaîne de grande distribution, requiert depuis 2005 de ses 100 plus gros fournisseurs la présence de marqueurs RFID sur les cartons et, depuis janvier 2006, le demande à ses 300 plus gros fournisseurs. Wal-Mart fait partie de EPCGlobal, une alliance d'industriels qui vise à promouvoir l'utilisation de RFID et EPC pour la gestion de la chaîne logistique. EPC est un système d'identification des produits reposant sur RFID, similaire au code barres, mais qui contient (en sus des codes du fabricant et de la classe du produit) un code permettant d'identifier les produits d'une même série. Le Department of Defense (DoD) exige de ses 43.000 fournisseurs, depuis le printemps dernier, le marquage RFID des marchandises destinées à deux de ses centres de dépôt. Le code d'identification des tags peut-être EPC ou un code spécifique au DoD. Les tags sont à ultra haute fréquence (autour de 900 MHz). Le DoD expérimente par ailleurs certains systèmes RFID très complets pour la localisation du matériel : des marqueurs actifs permettant une communication à plusieurs centaines de mètres, des systèmes munis de GPS, d'autres combinant RFID à un système de communication par satellite (SACOM Iridium). Des systèmes RFID sont également utilisés pour le contrôle d'accès à certaines installations militaires (par exemple le Fort McPherson, siège de l'état major de l'armée de terre). Au-delà, certaines bibliothèques l'utilisent aussi pour la gestion des emprunts et retours ; dans certains aéroports la technologie est employée pour le suivi des bagages et des passages aux inspections de sécurité. Elle est par ailleurs assez bien utilisée pour les badges d'authentification. L'agence hospitalière du ministère des anciens combattants (dont le réseau hospitalier dessert 5 millions de personnes) a commencé en 2005 à mettre en usage le RFID pour le suivi des médicaments.

### 3. Quelques exemples d'applications en développement ou à venir

La FDA (Food and Drug Administration) recommande d'équiper les palettes de médicaments de systèmes RFID dans le but de lutter contre la contrefaçon, un séminaire consacré à cette question aura lieu les 8 et 9 février 2006. Des études sont en cours pour connaître l'effet du champ créé par l'utilisation de RFID sur certains médicaments. Certains hôpitaux testent des systèmes s'appuyant sur RFID : principalement pour le suivi du matériel (et éviter les vols), du personnel, des patients, visiteurs (localiser et vérifier les accès), parfois pour l'identification des médicaments et des patients, voire pour des capteurs sur les patients. VeriChip a développé une puce RFID destinée à être implantée sous le tissu adipeux, la seule à avoir reçu l'agrément de la FDA. Elle peut-être utilisée pour l'identification des patients dans les hôpitaux (une soixantaine d'établissements utilisent cette technologie), mais aussi pour authentifier les accès etc.. Le Department of Homeland Security teste des formulaires d'entrée et de sortie du territoire I-94 (formulaires pour les ressortissants dispensés de visa) équipés de marqueurs RFID depuis l'été 2005 et pour un an environ. Ces marqueurs passifs, interrogeables sans authentification contiendront uniquement un identifiant, qui sera lié aux informations personnelles contenues dans une base de données. Le DHS a par ailleurs équipé une centaine de postes frontière terrestres (avec le Mexique et le Canada) de voies RFID (programme FAST) où peuvent passer des chargement qui ont été pré contrôlés au départ. American Express et Mastercard ont lancé des cartes de paiement dotées d'une puce RFID. De tels systèmes peuvent être intégrés dans les téléphones (système dit NFC pour Near Field Communication) ; Motorola a annoncé de tels produits.

#### **4. Les passeports RFID**

Le gouvernement américain a exigé des pays dont les ressortissants peuvent entrer aux Etats-Unis sans visa qu'ils mettent en place des passeports numériques équipés de données biométriques avant octobre 2005. Le "Enhanced Border Security and Visa Entry Reform Act" de 2002 requérait la mise en place d'équipement aux points d'entrées aux Etats-Unis, mais ces équipements ne sont toujours pas prêts (problèmes de compatibilité). Le gouvernement souhaite équiper les passeports américains d'un système RFID d'ici à octobre 2006, mais rien n'est encore finalisé : les choix techniques ne sont pas encore arrêtés et des conflits légaux consécutifs au choix des fournisseurs sélectionnés pour tests après appel d'offre auront retardé le processus. Pour éviter que ces passeports RFID ne soient interrogeables en permanence, ils seraient recouverts d'une sorte de cage de Faraday et, surtout, comporteraient un système d'autorisation utilisant une cryptographie asymétrique pour l'interrogation des données (mais selon certains experts la sécurité serait compromise par une clef qui resterait inchangée sur la durée de vie d'un passeport).

#### **5. Réglementation**

Aux Etats-Unis, c'est l'Office of Engineering and Technology (OET) de la Federal Communications Commission qui est responsable de la mise à jour des règlements pour tout ce qui concerne l'emploi privé des fréquences (la National Telecommunications and Information Administration étant en charge des emplois par l'administration fédérale). Les systèmes RFID sont régulés selon la section 15 des règles de la FCC : en contrepartie du libre accès aux fréquences considérées, les équipements doivent répondre à des critères stricts édictés par l'OET, notamment sur la puissance d'émission, le champ électromagnétique créé et la stabilité qui implique des contraintes en terme de portée. Les appareils les plus courants utilisent les basses fréquences (autour de 125 ou 134,2 kHz), les hautes fréquences (autour de 13,56 Mhz : utilisée à l'échelle mondiale), les ultra hautes fréquences (autour de 463 Mhz et entre 868 et 956 Mhz) ou les micro ondes (autour de 2,45 Ghz ou 5,8 Ghz). La portée varie selon les équipements utilisés de l'ordre du centimètre à plusieurs centaines de mètres.



Un problème d'uniformité des réglementations des fréquences au niveau mondial

Les industriels souhaitent un produit qui puisse être autorisé mondialement pour l'application gestion de la chaîne logistique, alors que les fréquences autorisées varient suivant les pays. La FCC a autorisé ODIN (l'un des leaders en intégration de systèmes RFID aux Etats-Unis) à utiliser dans ses laboratoires les fréquences autorisées en Europe ou au Japon (mais pas aux Etats-Unis), pour favoriser la présence américaine sur ces marchés, mais aussi le développement de produits pouvant fonctionner mondialement, nécessaires pour la gestion logistique.

#### **6. Problèmes posés par les composants RFID**

Respect de la vie privée :

La FTC (Federal Trade Commission) a organisé en mars 2005 une table ronde. Ce fut l'occasion d'observer la diversité des avis sur la question. Certains industriels avaient déjà établi des règles de bonne conduite pour la protection de la vie privée des consommateurs (par exemple les "EPCGuidelines"). Ainsi les produits portant un marqueur RFID doivent informer le consommateur de cette présence, et le marqueur doit pouvoir être désactivé avant la sortie du magasin. Certains groupes souhaitent une réglementation dans le domaine. Plusieurs projets de lois étatiques et fédérales souhaitent encadrer l'utilisation de RFID afin de limiter son impact sur les problèmes relatifs à la vie privée.

Sécurité :

La faible sécurité de certains produits introduits sur le marché peut par ailleurs être sujet d'inquiétude : des chercheurs de John Hopkins University sont parvenus à "pirater" le système Digital Signature Transponder (DST) de Texas Instruments utilisé entre autre par ExxonMobil SpeedPass et par des clés de voitures (en raison d'une taille de clé cryptographique trop faible : 40 bits). De fait, les classes 0 à 2 définies par la norme EPC (composants passifs) correspondent à une sécurité faible, nonobstant la faible portée associée. Il faut atteindre les classes 3 (semi passif) et 4 (actif) pour que le niveau de sécurité soit satisfaisant. Le Government Accountability Office (GAO) est sensibilisé à ces risques et a publié en mai 2005 un rapport sur le sujet, dans lequel il met en évidence le fait que les administrations qui se sont engagées dans l'emploi de RFID n'ont pas pris sérieusement en compte, à une exception près, les risques en matière de sécurité et en matière de protection de la vie privée, et pointe l'insuffisance des contre-mesures envisagées. Dans le même ordre d'idée, le "think tank" RAND a enquêté auprès de six grandes entreprises qui utilisent des puces RFID dans leurs locaux (contrôle d'accès et au-delà). Une seule avait formulé par écrit les règles d'emploi et de déploiement, mais à l'attention du service de sécurité. Les employés se trouvaient donc dans l'ignorance des implications et limites de l'emploi de cette technologie.

Fiabilité :

Avant un emploi massif et efficace il faudrait trouver une solution aux problèmes techniques mis en évidence lors des expériences. Les taux de reconnaissance diminuent fortement lors de la présence de nombreux marqueurs (problèmes d'interférences et d'alimentation par champ électromagnétique insuffisante dans le cas de marqueurs passifs) ; les ondes sont fortement atténuées par le métal et l'eau. Il est parfois nécessaire d'adapter l'emballage des produits pour le rendre compatible avec une utilisation RFID...

## **7. Recherche & Développement**

Dans l'ensemble la plus grande part des travaux consacrés au RFID ou tirant partie du RFID relève actuellement de la recherche applicative, ce qui n'est pas très surprenant. Cela va jusqu'à des travaux dont le propos est de réduire le coût de fabrication des composants RFID tout en augmentant leur capacité. Une autre caractéristique importante est que les travaux relatifs au RFID sont souvent des travaux portant sur des réseaux de composants sans fil (pas tous RFID), avec intégration dans le Web. En effet, dès que l'on sort du cadre 'un code objet lu par un lecteur, puis lecture d'un autre code objet', un système rassemblant des composants RFID doit être vu comme un réseau sans fil, en règle générale intégré dans le réseau Internet. A cet égard, la recherche sur les RFID a de nombreux liens avec celle sur les réseaux sans fil ou avec celle sur le "pervasive computing". Par ailleurs, pour des composants actifs dont la capacité va nettement au-delà du code barre, la recherche de base est très étroitement liée à celle portant sur les systèmes embarqués (modèles logiques, travail sur l'autonomie etc.).

Recherches centrées sur le RFID :

On peut relever que, si certaines universités ont créé des centres de longue date, à commencer par le MIT, il y a une floraison de nouveaux centres consacrés au RFID. Tous ces centres viennent s'ajouter à une infrastructure de recherche qui, notamment du côté industriel, est déjà significative : centres de Sun Microsystems, Texas Instrument (dont l'unité Sensors & Actuators, mais sans la partie RFID, vient d'être vendue à LLC), Intel, Seattle et Berkeley, Wal-Mart, IBM (pour le middleware), Microsoft (qui a même créé un RFID Council), etc. Du point de vue industriel Dallas (notamment TI et Sun, tandis que pour IBM c'est Zürich) apparaît comme étant le centre principal pour ce qui est du RFID au sens strict, ce à quoi l'on peut ajouter le MIT Auto-ID Lab et ses partenaires industriels.

Les principaux thèmes de recherche qui apparaissent sont :

- les logiciels embarqués des composants, à considérer comme une partie de la recherche sur les systèmes embarqués.
- l'amélioration du hardware : amélioration de la portée et de la directivité des antennes, maîtrise des interférences, de l'autonomie (alimentation solaire, reposant sur les vibrations, les flux d'air, voire les gradients de température / pression), miniaturisation (un nouveau domaine est le recours à des nano-composants) ...
- la prise en compte des interférences entre puces RFID ("tag anti-collision") ou entre lecteurs RFID ("reader anti-collision"), question rendue accrue par le déploiement d'applications qui comportent un grand nombre de composants ou par la proximité d'un grand nombre de lecteurs, à portées croissantes, avec des sensibilités différentes au bruit, etc.
- la conception et l'architecture des composants RFID, voire des systèmes (réseau de composants + middleware + applications), ce qui commence par l'intégration dans le monde du RFID des techniques (outils de conception etc.) qui se sont développées dans le domaine des puces et des systèmes embarqués, mais également la prise en compte de nouveaux matériaux (silicium sur isolant, silicium pressé) utilisés pour les microprocesseurs.
- les problématiques liées aux réseaux de systèmes RFID (gestion d'ensemble par des outils Web adaptés etc.) et au trafic que représentent les données d'un très grand nombre de capteurs (routage, évitement des collisions, gestion adaptative du trafic etc.). Cela va jusqu'à des réflexions sur un réseau global rassemblant toutes sortes d'objets équipés : 'Internet of things' et autres IrisNet.
- le middleware pour les RFID, en particulier l'intégration des données envoyées par de grands nombres de capteurs RFID, les services Web pour piloter des applications RFID...
- la sécurité des informations (concernant la vie privée etc.) dans les systèmes RFID.
- les recherches portant sur l'application du RFID, dans le domaine de la santé (suivi de patients, aide aux handicapés), celui de l'environnement (réseaux de suivi de zones naturelles), celui du bâtiment (domotique, suivi de structures), l'automobile (suivi des composants et contrôle) etc.

Les centres qui apparaissent comme les plus actifs, outre ceux listés ci-dessus, semblent être :

- le MIT via le MIT Auto-ID Lab et son rôle dans les Auto-ID Labs et dans EPC Global.
  - Intel et ses partenaires universitaires.
  - un ensemble d'universités réparties à travers le pays : UCLA (CENS et WINMAC), UCB, Harvard (projet CodeBlue pour le suivi médical de patients), Carnegie Mellon, Université de Columbia (centre WICAT, système MoteTrack), Ohio University, Virginia University, Urbana Champaign (essentiellement pour la thématique réseau), Université de Washington, GeorgiaTech (aide aux aveugles).
- Les financeurs sont, outre les industriels (probablement en premier lieu), la NSF, la DARPA, les NIH et de puissantes fondations liées au monde de la santé (association Alzheimer ou AAHSA par exemple) pour les applications correspondantes du RFID.

Un rapport d'ambassade plus détaillé paraîtra très prochainement.

La version pdf du présent article est également disponible au téléchargement à l'url [http://www.bulletins-electroniques.com/rapports/smm06\\_004.htm](http://www.bulletins-electroniques.com/rapports/smm06_004.htm)

#### Source :

- La norme ISO/IEC 18000:2004 : <http://www.iso.org/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=ISO%2FIEC+18000>
- La norme ISO/IEC TR 24710:2005 : <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=38820&ICS1=35&ICS2=40&ICS3>
- EPC Global : <http://www.epcglobalinc.org>
- Programme NAIS : <http://animalid.aphis.usda.gov/nais>
- [http://www.acq.osd.mil/log/rfid/DoD\\_Suppliers\\_Passive\\_RFID\\_Information\\_Guide\\_v9.pdf](http://www.acq.osd.mil/log/rfid/DoD_Suppliers_Passive_RFID_Information_Guide_v9.pdf)
- Expérimentation du DoD : [http://www.govworks.gov/vendor/RFP\\_docs/60916\\_A6\\_BPA.doc](http://www.govworks.gov/vendor/RFP_docs/60916_A6_BPA.doc)
- [http://www.securitymanagement.com/library/gao05345\\_rfidreport1205.pdf](http://www.securitymanagement.com/library/gao05345_rfidreport1205.pdf)
- Contrôle d'accès au Fort McPherson : <http://rfid.idtechex.com/knowledgebase/en/casestudy.asp?freefromsection=121>
- Le séminaire de la FDA : <http://www.fda.gov/bbs/topics/NEWS/2006/NEW01293.html>

- Applications médicales : <http://medicalconnectivity.com/categories/rfid/> I-94
- RFID : <http://www.dhs.gov/dhspublic/display?content=4720>
- La section 15 des règles de la FCC : <http://www.fcc.gov/oet/info/rules/part15/part15-91905.pdf>
- Le rapport de la FTC suite à sa table ronde "Radio Frequency Identification : Applications and Implications for Consumers" : <http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf>
- Piratage du DST : <http://rfidanalysis.org/DSTbreak.pdf>
- Le rapport du GAO : "Information security - Radio Frequency Identification Technology in the Federal Government" : <http://www.gao.gov/new.items/d05551.pdf>
- Enquête de la RAND : [http://www.rand.org/pubs/research\\_briefs/RB9107/index1.html](http://www.rand.org/pubs/research_briefs/RB9107/index1.html)

Centres consacrés au RFID créés en 2005 :

- Le Radio Frequency Identification Center of Excellence (<http://www.engr.pitt.edu/site/rfid>) a ouvert en octobre dernier à l'université de Pittsburgh (chargé aussi de gérer le portefeuille de brevets RFID de l'université, laquelle est un des principaux centres du domaine avec le MIT).
- Le RFID Lab de l'Université du Wisconsin à Madison, adossé sur un groupe d'industriels, se positionne aussi comme centre de test pour les nouveaux marqueurs RFID (<http://www.uwrfidlab.org>).
- Le RFID Research Group de l'université du Nord Texas à Denton (<http://www.txcdk.org/rfid>).
- Le RFID Research Center, fortement pluridisciplinaire, (<http://itrc.uark.edu/view.asp?article=242>) vient d'ouvrir au sein de l'université d'Arkansas (le financement associe notamment Tyson Foods et Wal-Mart, ainsi que des dons matériels de grands industriels, dont Intel, Cisco-Eagle et Microsoft).
- Le tout nouveau Center for food distribution and retailing de l'université de Floride (<http://cfdr.ifas.ufl.edu>), pour lequel le RFID est un axe majeur (là encore clairement très applicatif). <http://www.intel.com/research>
- Le projet CodeBlue : <http://www.eecs.harvard.edu/~mdw/proj/codeblue>
- Le système MoteTrack : <http://www.eecs.harvard.edu/~konrad/projects/motetrack>

#### **Pour en savoir plus, contacts :**

- <http://www.rfidjournal.com>
- <http://www.rfidgazette.org>
- <http://www.rfidnews.org>
- <http://www.gcn.com>

Code brève

ADIT : 31714

#### **Rédacteur :**

Jean-Philippe Lagrange, [attache-stic.mst@ambafrance-us.org](mailto:attache-stic.mst@ambafrance-us.org)

Sébastien Morbieu, [sebastien.morbieu@ambafrance-us.org](mailto:sebastien.morbieu@ambafrance-us.org) (MS&T)