Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
nationale

Direction centrale de la sécurité des systèmes d'information

Affaire suivie par : Pierre-Michel RICORDEL
01 41 46 37 43

Paris, le 03/12/2003

N° 2356/SGDN/DCSSI/SDS/LCR

NOTE

à

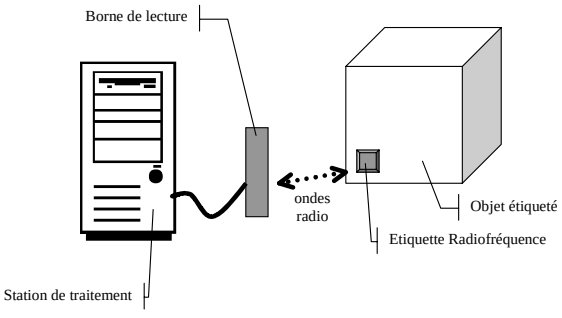
destinataires in fine

Objet : Les Etiquettes Radiofréquence (RFID) et les cartes à puce sans contact

1. Description

1.1. Définition et typologie

Une étiquette radiofréquence est un système électronique chargé de stocker une information utile à l'étiquetage d'un objet auquel il est associé physiquement, et qui peut être lue automatiquement par l'intermédiaire d'ondes radio. L'étiquette n'émet les informations qu'elle contient qu'en présence d'une borne de lecture adaptée.



Une étiquette radiofréquence est composée d'un circuit intégré, d'une antenne, et optionnellement d'une batterie. On distingue deux classes d'étiquettes radiofréquence :

- Les étiquettes actives, qui contiennent une batterie compacte. Ces étiquettes peuvent communiquer sur de longues distances (plusieurs dizaines de mètres), mais ont un coût de revient élevé (plusieurs euros) et une durée de vie limitée (mais qui peut atteindre tout de même une dizaine d'année).
- Les étiquettes passives, qui ne contiennent pas de batterie, et qui puisent leur alimentation électrique directement du rayonnement électromagnétique émis par la borne. Dans ce cas, le signal reçu par l'étiquette sert à la fois de source d'alimentation en énergie et de canal de communication avec la borne. Ce type d'étiquette a un coût de

revient très bas (entre 5 et 50 cents), et une durée de vie virtuellement illimitée, mais sa portée est limitée à quelques mètres au maximum.

Le circuit intégré est composé de trois modules :

- Un module radiofréquence, chargé de la modulation et démodulation des signaux radio, ainsi que de l'alimentation électrique dans le cas des étiquettes passives
- Un module de contrôle, chargé de la gestion du protocole de communication avec la borne de lecture. Les circuits intégrés les plus complexes peuvent également intégrer des processeurs et des cryptoprocesseurs.
- Une mémoire contenant les informations d'étiquetage. Cette mémoire peut être à lecture seule (ROM), à écriture unique (WORM) ou réinscriptible (EEPROM).

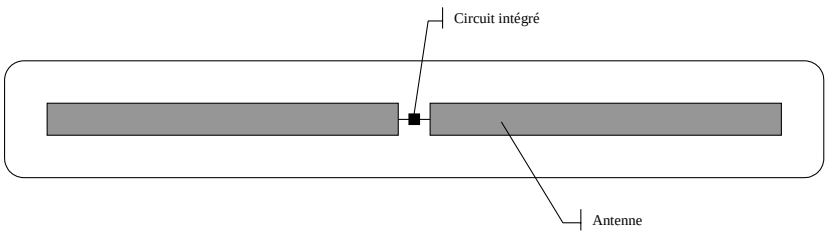
Une étiquette peut également être simplement intégrée à une carte plastifiée associée à un porteur. On parle alors de carte à puce sans contact. On distingue alors quatre types de carte à puce :

- La carte à puce à contact seul (carte à puce classique)
- La carte à puce sans contact, souvent utilisée pour le contrôle d'accès
- La carte à puce bi-mode, bi-puce : c'est une carte contenant à la fois une puce à contact et une étiquette radiofréquence. Ces deux circuits sont indépendant et isolés électriquement, ils ne partagent pas de mémoire, et ne peuvent communiquer entre eux.
- La carte à puce bi-mode, mono-puce : c'est une carte contenant une seule puce, capable de s'alimenter et de communiquer soit par l'interface à contact, soit sans contact. Il est donc possible d'utiliser indifféremment une des deux interfaces pour accéder à la mémoire et aux fonctionnalités du circuit intégré (si la politique de sécurité implémentée le permet).

1.2. Aspect physique

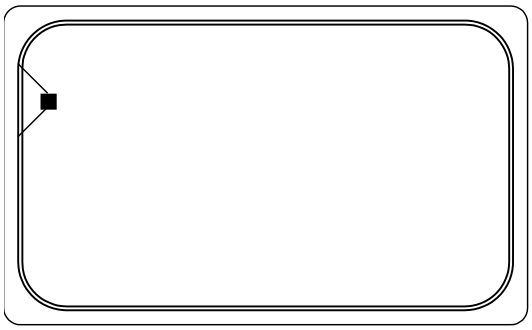
Le circuit intégré proprement dit peut être extrêmement petit : il fait généralement quelques millimètres carrés. Le plus petit circuit commercialisé actuellement est le µ-chip de Hitachi, qui mesure 0,4mm sur 0,4mm.

Cependant, afin d'atteindre une portée suffisante, le circuit intégré doit être associé à une antenne de plus grande taille. La taille de l'antenne dépend de la fréquence radio utilisée, de la portée recherchée, et de la consommation électrique du circuit intégré. Généralement celle-ci varie entre 1et 10 cm (il existe des antennes intégrées au circuit, mais leur portée est très faible : quelques millimètres). Les antennes des étiquettes basse fréquence sont des boucles ou des spirales alors que les antennes des étiquettes haute fréquences sont de simples fils linéaires.



Les antennes peuvent être rigides et incluses dans la masse d'une pièce plastique, ce qui rend l'étiquette insensible à toute dégradation mécanique ou chimique (étiquetage de containers, de châssis de véhicules, de wagons, badge d'accès, implant sous-cutané), mais aussi la rend indécelable pour un simple examen visuel (chaussures, pneus). Pour d'autres applications, les antennes peuvent être flexibles, voire même imprimées avec une encre conductrice, ce qui permet de les intégrer dans des étiquettes adhésives ou des documents en papier (antivols de magasins, billets de banque, passeports, bons).

Dans le cas des cartes à puces sans contact, l'antenne est une spirale faisant le tour de la carte, et reliée à la puce.



1.3. Aspect radioélectrique

Différentes bandes de fréquences sont utilisées pour les communications entre la borne et l'étiquette. Selon la bande de fréquence utilisée, varient : la portée, les caractéristiques de propagation, la forme et taille de l'antenne, le débit de communication, et la complexité technologique du circuit intégré.

D'une manière générale, les communications se font de la manière suivante : La borne émet une onde radioélectrique à une fréquence donnée. Cette onde est captée par l'étiquette qui l'utilise pour son alimentation électrique. Les communications de la borne vers l'étiquette se font par la modulation d'un des paramètres de l'onde : amplitude, fréquence ou phase. Les communications de l'étiquette vers la borne se font par la variation de la charge du champ électromagnétique, imposée par l'étiquette (modulation d'amplitude ou de phase), et mesurée par la borne. De récents développements technologiques permettent à certaines étiquettes de transmettre leurs données sur un autre canal de fréquence que celui de la borne.

On distingue quatre bandes de fréquences utilisées par les étiquettes électroniques :

- Basse fréquence : 125kHz ou moins (antivols de voiture, contrôle d'accès)
- Moyenne fréquence : 13,56MHz (cartes à puce, contrôle d'accès)
- Haute fréquence : entre 850 et 950MHz (UHF) (étiquetage)
- Micro-ondes : 2,4Ghz et 5,8Ghz (péage autoroutier)

Les étiquettes basses et moyennes fréquences utilisent des antennes inductives en forme de spirale. Le fait qu'un couplage inductif avec la borne soit nécessaire à l'alimentation de l'étiquette rend la portée de celle-ci limitée : grossièrement la portée efficace est de l'ordre de grandeur du diamètre de l'antenne de la borne. Au-delà de cette distance, le champ diminue rapidement, et la puissance diminue selon le sixième exposant de la distance. Cependant, au contraire des fréquences plus élevées, les transmissions sont peu influencées par la présence d'eau, d'humidité ou de tissus vivants. L'orientation de l'antenne de l'étiquette par rapport à l'antenne de la base joue un rôle important pour les performances du système, cependant ce problème peut être résolu par l'usage d'antennes plus complexes, générant des champs rotatifs. La portée typique de ce type d'étiquettes est de l'ordre d'une dizaine de centimètres, mais peut aller jusqu'à 1,5 mètres avec une borne équipée d'une ou plusieurs antennes de grandes dimensions.

Les étiquettes haute fréquence et micro-ondes utilisent des antennes du type dipôle, constituée de deux brins conducteurs de part et d'autre du circuit intégré. Cette configuration

rend l'antenne très compacte. La quantité d'énergie reçue dépend de la longueur de l'antenne et de la fréquence utilisée. A ces fréquences, les ondes se propagent relativement loin (la puissance diminue selon le carré de la distance, indépendamment de la taille de l'antenne de la borne) mais sont très susceptibles à la présence d'eau ou de conducteurs à proximité : l'eau et l'humidité absorbent les ondes et dégradent les performances, alors que les objets métalliques réfléchissent, réfractent ou diffractent les ondes. Les réflexions d'ondes peuvent renforcer ou affaiblir les signaux de manière difficilement prévisible selon la disposition relative des antennes et des objets métalliques avoisinants. Ces phénomènes sont dus aux longueurs d'ondes utilisées qui sont relativement courtes par rapport à la taille des objets généralement rencontrés (environ 33cm en UHF, 12cm et 5cm en micro-ondes). L'orientation de l'antenne de l'étiquette par rapport à l'antenne de la base joue un rôle important pour les performances du système, cependant ce problème peut être résolu par l'usage d'antennes plus complexes, générant des champs rotatifs. De plus, à ces fréquences il est relativement aisé de construire des antennes directionnelles, qui permettent de focaliser la zone dans laquelle les étiquettes peuvent être lues, ou d'éviter les interférences entre plusieurs systèmes. Malgré leur sensibilité aux réflexions parasites, la portée de ce type d'étiquette est bien meilleure que pour les étiquettes basses ou moyennes fréquences : de quelques centimètres à une douzaine de mètre, selon la puissance de la borne et la taille de l'antenne de l'étiquette. A ces fréquences, une étiquette active peut porter à plus de trente mètres.

La bande passante (le débit d'information qui peut être transmis par le canal radioélectrique) varie selon les performances du circuit intégré, la fréquence de la porteuse, et la portée espérée. Le débit constaté entre une étiquette et sa borne varie entre environ 10kbit/s et 100kbit/s, mais des vitesses de 1Mbit/s peuvent être atteintes avec des étiquettes actives micro-ondes.

Les puissances émises par les bornes sont limitées par la réglementation. Ces puissances sont relativement faibles, car les bornes sont généralement utilisées en présence de personnes. La réglementation varie selon les pays et les bandes de fréquences, mais sont généralement de l'ordre de 500mW en haute fréquence.

1.4. Aspects logiques

La fonction principale de l'étiquette est de stocker une information et de la transmettre à la borne. Pour cela le circuit intégré de l'étiquette contient un gestionnaire de communication et une mémoire.

Le gestionnaire de communication a la charge d'exécuter le protocole de communication permettant de réguler les communications avec la borne. Selon les implémentations, plusieurs types de protocoles sont présent sur le marché. Pour certains la communication est initiée par l'étiquette (plus efficace pour les applications où les étiquettes sont en mouvement), pour d'autre par la borne (plus efficace pour les applications où les étiquettes sont nombreuses dans un volume délimité). Les communications peuvent être chiffrées ou claires. On rencontre souvent dans les protocoles des mécanismes anti-collision, qui permettent de régler les communications et éviter les interférences ou les conflits lorsque plusieurs étiquettes de se trouvent dans le champ d'une même borne. Ces protocoles anti-collision permettent d'interroger en une seconde jusqu'à 50 étiquettes différentes placées dans le champ de la borne.

La mémoire, du type EEPROM[1], est une mémoire capable de garder des informations pendant au moins dix ans sans nécessité d'alimentation électrique, et qui peut être éventuellement effacée et re-écrite. La quantité de mémoire embarquée varie de 64 bits à plusieurs Kilo-octets selon les applications, les mémoires de grande taille étant plus onéreuses à fabriquer. Généralement, l'espace mémoire est segmenté en plusieurs zones ayant différentes propriétés. Ces zones sont :

[1] Electrically Erasable Programmable Read-Only Memory

- en lecture seule, programmées à la fabrication, contenant généralement un identifiant unique
- en écriture unique (One Time Programmable) : ces zones peuvent être écrites après sortie d'usine par le client, mais ne peuvent plus être effacées ensuite
- en lecture/écriture : ces zones peuvent être effacées et re-écrites par des bornes spécifiques. Les EEPROM étant moins performantes et plus consommatrices en énergie lors d'une écriture que lors d'une lecture, l'écriture exige généralement des bornes spécifiques, et la portée d'écriture peut être plus réduite que lors d'une simple lecture de l'étiquette.

Dans les applications nécessitant des circuits intégrés de petite taille, ou de faible consommation (pour une plus grande portée) le protocole utilisé fait transiter les données en clair sur les ondes. Récemment, les évolutions technologiques permettent d'intégrer des primitives cryptographiques dans les étiquettes radiofréquence, afin de chiffrer les communications, préservant leur confidentialité et leur intégrité. On rencontre des algorithmes de chiffrement par flots, comme dans le protocole Mifare de Philips (algorithme propriétaire CRYPTO1), mais aussi du chiffrement par blocs (DES, DES-X, 3DES), et récemment des algorithmes asymétriques (RSA, ECC). Ces derniers posent encore des difficultés techniques, car ils nécessitent de lourds calculs, or l'alimentation électrique étant très limitée, ces calculs ne peuvent être faits très rapidement. De plus, facteur aggravant, les transactions faites sans contact doivent l'être dans un temps très court, car la continuité de l'alimentation énergétique est incertaine, et les contextes d'utilisations nécessitent souvent un passage rapide de l'étiquette devant la borne (cartes à puces sans contact de transports en commun, acquisition d'objets étiquetés en mouvement). Actuellement, un calcul RSA 1024 bits se fait en environ 250ms pour les meilleures implémentations.

1.5. Normalisation et standardisation

Récemment, un effort de standardisation a été réalisé par l'ISO dans ce domaine. La norme la plus significative est la norme ISO 14443. Deux types de protocoles sont définis : ISO 14443/A, et ISO 14443/B, et la norme est découpée en quatre parties (parts 1-4), certains produit pouvant être compatible avec un sous-ensemble de ces parties. Les quatre parties couvrent les caractéristiques physiques, les puissances radio employées et la signalisation, l'initialisation et le protocole anticollision, et le protocole de transmissions. Alors que le type A est en proche relation avec le protocole propriétaire Myfare de Philips, le type B est plus « libre », et le marché s'oriente progressivement vers celui-ci : la compatibilité ISO 14443/B parts 1-4 deviens de plus en plus généralisée.

En complément de cette norme, qui concerne les communications de proximité (portée d'environ 10cm), s'ajoutent les normes ISO 10536 pour les communications à quasi-contact (*close-coupled*, portée 1cm) et ISO 15693 pour les communications de voisinage (portée 50cm). Toutes ces normes utilisent la fréquence de 13,56Mhz.

D'autres normes ISO et ANSI couvrent les autres bandes de fréquences et divers usages, mais leur influence sur le marché est moindre.

Les cartes à puces bi-mode utilisent à la fois la norme ISO 14443 pour l'interface sans contact, et la norme ISO 7816 pour l'interface à contact.

2. Applications

Les étiquettes radiofréquence ne sont pas une invention récente, et sont déjà utilisées dans de nombreuses applications depuis plus d'une vingtaine d'années. Nous distinguons par la suite les applications historiques, qui sont déjà largement répandues et acceptées, des applications émergentes, et potentiellement problématiques des étiquettes radiofréquence. L'émergence des nouvelles applications est directement liée à la chute du coût de fabrication des étiquettes et à l'évolution technologique permettant d'en diminuer la taille, d'augmenter leurs performances, tout en facilitant la manipulation de grandes quantités d'information à grande échelle.

2.1. Applications historiques

Depuis plus de vingt ans les étiquettes radiofréquence sont utilisées pour marquer des objets. Cependant, leur coût non négligeable (plusieurs euros) restreignaient leur champ d'application. On peut regrouper les applications selon les thèmes suivants :

- Marquage de contenants réutilisables : les étiquettes radiofréquence sont largement utilisées pour marquer les conteneurs de fret maritime ou aérien, les wagons de chemin de fer, les palettes de stockage, les chariots de manutention de lignes de fabrication robotisées, la manutention de colis. Les avantages de cette technologie par rapport à d'autres types de marquages (codes à barres) sont leur résistance aux agressions extérieures (salissures, déchirures) et leur facilité de lecture qui ne nécessite pas une vue directe de l'étiquette
- Contrôle d'accès : les étiquettes radiofréquence sont utilisées dans les badges d'accès, souvent au format de carte de crédit (on parle alors de carte à puce sans contact), ou dans les antivols de voiture (l'étiquette se trouve moulée dans la clef de contact). L'intérêt de cette technologie est qu'elle est simple d'usage et résiste à l'usure et aux dégradations (pas mécanisme en mouvement, comme dans le cas des clefs), et reste difficile à cloner, de par sa simple technicité ou par l'usage de protocoles cryptographiques, par rapport à des clefs physiques, ou même des bandes magnétiques (par exemple, pour le passe RATP NaviGO). Le fait que l'étiquette puisse être lue en mouvement la rend aussi utile pour les applications de télépéage autoroutier (système liber-***t***).
- Marquage d'animaux, d'arbres : ici aussi, c'est la grande durabilité de l'étiquette, sa facilité de lecture à grande distance, et sa grande variété de supports physique (capsule injectable sous la peau, collier, ou sous forme de clou pour les arbres) qui la rendent adapté à ces usages.

2.2. Applications émergentes

Récemment, la baisse du coût de production et l'évolution technologique laissent entrevoir de nouvelles applications pour les étiquettes radiofréquence. Le seuil de rentabilité pour ces applications est généralement estimé à un coût maximal de 5 centimes d'euro par étiquette.

La baisse de ces coûts permet d'envisager d'utiliser les étiquette non pas pour étiqueter les gros contenants, mais les contenus, c'est à dire chaque objet individuellement. L'objectif est de détrôner le code à barres comme moyen privilégié d'identification des produits. Tout comme le code à barres avait révolutionné la grande distribution lors de son introduction, les étiquettes radiofréquence apportent une nouvelle dimension dans la gestion du cycle de vie du produit :

- Sur la chaîne de fabrication : suivi facilité de la production.
- Chez le grossiste : gestion des stocks à l'unité près, sans déballage.
- Chez le commerçant : suivi automatique de l'approvisionnement des rayonnages (étagères intelligentes), antivol, passage à la caisse accéléré.
- Chez le client : transmissions d'informations automatiques aux objets ménagers : date de péremption (réfrigérateur intelligent), temps de cuisson (four intelligent).
- En cas de retour client pour défaut de fabrication, l'article est individuellement traçable.
- Chez le recycleur : l'étiquette peut contenir des informations sur les filières de recyclage à utiliser, ou les types de matières composant le produit.

Contrairement au code à barre, l'étiquette a des applications même après l'achat du produit par le client final, celle-ci est donc parfois intimement liée au produit, moulée dans sa masse plastique. Ainsi certains fabricants de pneus (comme Michelin) intègrent déjà des étiquettes électroniques dans la masse du pneu aux Etats-Unis (faisant référence à la nouvelle réglementation TREAD (Transportation, Recall, Enhancement, Accountability and Documentation) votée par le congrès américain).

De nombreux fabricants ou distributeurs sont en phase d'évaluation, de tests ou de déploiement de ces technologies : Gillette, Coca-Cola, Wal-Mart, Unilever, Philip Morris,

Tesco, Home Depot, GAP, Prada, Proctor & Gamble, Marks & Spencer, Benetton, Michelin, US Postal, Delta Airlines, DoD américain… Certaines estimations font état d'un marché de plus de 500 milliard d'unités.

Un autre domaine d'application émergent est celui de l'authentification de documents officiels (passeports, certificats, diplômes) ou de valeur (billets de banque, bons d'achats). Cette application est envisageable grâce à la miniaturisation des circuits intégrés des étiquettes au point de pouvoir les intégrer dans la trame du papier de manière discrète et sans risque de destruction. Même l'antenne a été miniaturisée, et celle-ci peut être gravée directement sur la puce (ainsi, le µ-chip de Hitachi, mesurant 0,4mm de coté, peut être équipé d'une telle antenne intégrée). La Banque Centrale Européenne étudie la possibilité d'intégrer de telles puces dans les billets d'euro de grande valeur.

3. Problèmes

3.1. Problèmes d'atteinte à la vie privée

Utilisées à des fins de marquage des produits de consommation courante, les étiquettes radiofréquences engendrent deux phénomènes nouveaux, préoccupants pour le respect de la vie privée :

- La singularisation de l'objet de consommation courante : l'espace mémoire des étiquettes radiofréquence est largement suffisant pour numéroter individuellement chaque produit (numéroté sur 128 bits), alors que l'ancien code à barre UPC ne le permettais pas, et surtout la personnalisation des produits est beaucoup plus facile à mettre en œuvre : le code est inscrit électroniquement par une borne plutôt qu'imprimé sur le produit.
- La facilitation de la lecture anonyme : les étiquettes radiofréquences peuvent être lues à distance, sans qu'il n'y ait besoin de contact (carte à puce), ni de vue directe (code à barres). Une borne de lecture peut être facilement dissimulée sous des vêtements ou derrière un mur, et activer l'étiquette sans que son porteur n'en aie connaissance. De plus, cette lecture est facilement automatisable : un lecteur n'a pas besoin d'un opérateur à proximité pour effectuer des saisies.

La combinaison de ces deux phénomènes permet d'associer un individu aux étiquettes qu'il porte (par exemple dans les étiquettes de ses vêtements), puis de le suivre dans ses déplacements. Par exemple, des magasins peuvent énumérer les produits (concurrents ou non) que le client porte, puis utiliser les numéros de série de ceux-ci pour suivre ses visites successives, et utiliser ces informations à des fins de marketing. Un voleur à la tire, un voisin curieux, ou un cambrioleur peuvent obtenir la liste des produits que vous portez, ou que vous avez chez vous, sans infraction.

3.2. Problèmes de contrefaçon, falsification et piratage

D'une manière générale, on peut remarquer que les communications entre une borne et une étiquette sont facilement interceptables. Plus précisément, l'interception des données émises par la borne est extrêmement facile, même à très grandes distances (probablement plusieurs centaines de mètres dans de bonnes conditions), puisque celle-ci émet à une puissance relativement forte, car son rayonnement doit alimenter électriquement l'étiquette. Par contre, le signal de retour, de l'étiquette à la borne, est beaucoup plus faible, et nécessite d'être plus proche de l'étiquette. Cependant, certains protocoles employés actuellement permettent d'obtenir des informations sur l'étiquette en n'écoutant que les émissions de la borne (par exemple, l'écoute du protocole anti-collision par parcours d'arbre, utilisé dans la norme ISO 14443-A, permet d'obtenir indirectement le numéro de l'étiquette), et les ordres d'écriture dans l'étiquette sont facilement interceptés.

De plus, dans le cadre d'une attaque active (où l'étiquette est activée par une borne non autorisée) il est possible d'augmenter largement la portée de l'étiquette. En effet les bornes

standard ont des puissances limitées par la réglementation, leurs antennes sont compactes, et l'électronique employée est issue d'un compromis entre la sensibilité et le coût. Un attaquant utilisant des puissances supérieures, des antennes sophistiquées, et une électronique sensible peut atteindre une portée bien supérieure à celle attendue (peut-être au moins 10 fois plus grandes, mais peu d'expériences de ce type ont été menées). Plus grave encore, certains systèmes de contrôle d'accès peuvent utiliser une puissance d'émission volontairement bridée, donnant l'illusion d'une portée limitée à l'utilisateur, et donc une sécurité accrue (car le badge doit être quasiment en contact avec la borne) alors que celui-ci peut être consulté de beaucoup plus loin avec une borne à forte puissance.

Il faut noter également que, même lorsque les étiquettes radiofréquence sont utilisées dans un cadre de contrôle d'accès ou d'authentification, les protocoles utilisés sont parfois peu résistants à des attaques par rejeu, or ces attaques sont faciles à mettre en œuvre : un badge d'accès pourrait être ainsi cloné par le simple passage à proximité du badge, à l'insu de son porteur. Si un protocole cryptographique plus complexe est utilisé, il reste possible de monter des attaques plus lentes du protocole, par exemple en voyageant à proximité du porteur du badge. L'attaque peut alors durer plusieurs heures de manière imperceptible.

D'une manière plus spécifique, on peut dégager différents problèmes selon le domaine d'application des étiquettes radiofréquence :

- Contrôle d'accès : Outre les problèmes mentionnés précédemment (extension de la portée, possibilité d'attaques par rejeu), il est important de souligner que parfois la sécurité offerte par les badges de contrôle d'accès se limite à la difficulté technique d'accès au médium de communication, c'est à dire la mise en œuvre de systèmes à ondes radio haute fréquence. Ce niveau de sécurité est beaucoup trop faible, il doit être renforcé par l'usage de protocoles d'authentification cryptographiques résistant au rejeu, malgré les contraintes technologiques et économiques soulevées.
- Authentification d'objets de valeur (billets de banque, documents administratifs, etc.) : dans ce cadre, un document ou un objet est authentifié par l'inclusion d'une étiquette radiofréquence inarrachable à celui-ci. L'authenticité est alors assurée par le fonctionnement de l'étiquette, et la délivrance par celle-ci d'éléments numériques d'identification (secret partagé, signature électronique, etc.). Plusieurs problèmes se posent alors : tout d'abord, à l'aide d'une borne adéquate, il est facile pour une personne mal intentionnée de savoir à distance si une personne ou un bagage contient des objets de valeur. De plus, le fait que le contrôle d'authenticité se fasse à l'aide d'un appareillage coûteux et complexe (la borne de lecture), distinct des autres contrôles d'authenticité visuels traditionnels, ouvre le risque du « dédoublement d'authenticité » : comment établir l'authenticité d'un document dont les deux moyens d'authentification se contredisent ? Et quels risques prend-on en n'utilisant qu'un seul moyen d'authentification (visuels seulement dans le cas du transfert de la main à la main, ou radiofréquence seulement dans le cas d'un monnayeur automatique) ?

3.3. Problèmes techniques

Plusieurs problèmes techniques restent encore présents dans ce domaine, et doivent être pris en considération :

- Mauvaise maîtrise des paramètres radioélectriques, des procédés de fabrication et des protocoles : la plupart des fabriquants de circuits intégrés reconnaissent avoir du mal à maîtriser certains les aspects techniques, particulièrement le couple antenne/circuit intégré. Afin d'obtenir les performances voulues (particulièrement la portée maximale), de nombreux cycles d'ajustages sont nécessaires. Cette mauvaise maîtrise se traduit également par des problèmes de compatibilité et d'interopérabilité entre des bornes et les étiquettes de fabriquants différents, et même pour un même fabricant, pour différentes séries de puces. A ce titre, il est significatif de noter que la plupart des sociétés spécialisées dans les étiquettes radiofréquences et les cartes à puces sans contact ont comme corps de métier la conception d'antennes radio (Alien Technology, ASK, …).

Malgré l'emploi des normes ISO dans le domaine, l'interopérabilité ne semble pas garantie, et reste toujours soumise à des ajustements de dernière minute, ou des dégradations de performances.

- Sensibilité à l'environnement radioélectrique : les fréquences utilisées par les étiquettes radiofréquences sont également utilisées par des systèmes électroniques ou industriels (réseaux sans fils, chauffages à induction, signaux de télévision, fours, etc.) susceptibles de gêner ou d'empêcher les opérations d'un tel système dans certains environnement. De plus, comme nous l'avions souligné, les objets métalliques à proximité de la borne ou de l'étiquette perturbent énormément les signaux (pare-brise feuilleté métal, circuits électriques, antenne collée sur un support conducteur, humidité).

4. Conclusion

Les étiquettes radiofréquence, tout comme les téléphones portables, ne sont pas à proprement parler une nouvelle technologie, mais leur utilisation en masse pourrait transformer notre société, et notre relation à l'objet. Chaque objet de la vie courant pourrait ainsi être numéroté et interrogeable à distance, et l'évolution technologique aidant, pourrait former un maillage mêlant intimement objets réels du monde physique et objets virtuels du monde logique.

Cependant, cet optimisme doit être tempéré : de nombreuses difficultés sont rencontrées lors de déploiements en grandeur réelle des étiquettes radiofréquence. Les problèmes techniques persistent : les étiquettes sont très sensibles aux propriétés conductrices du support sur lequel elles sont collées, aux interférences avec d'autres systèmes radioélectriques (notamment les systèmes de télévision, les téléphones portables, les réseaux sans fils), et à l'orientation des étiquettes par rapport aux antennes des bornes. Généralement, le déploiement de nombreuses antennes de borne sont nécessaires afin d'atteindre une bonne couverture. Enfin, le système est facilement neutralisable par l'utilisation de cages de faraday (sous forme de sacs faits de matière conductrice par exemple) empêchant la communication entre l'étiquette et sa borne, ce qui est problématique dans des applications antivol ou de passage à la caisse automatique.

Malgré ces difficultés techniques, la recherche et le développement restent très actif, car le marché est potentiellement énorme, pour les acteurs de la grande distribution, tout comme pour les fabriquants d'étiquettes radiofréquence, mais aussi pour l'industrie informatique, qui devra fournir les applications de gestion de bases de données et de datamining.

Pour les applications de type cartes à puce sans contact, le marché est également important : l'intégration de fonctions cryptographiques et l'apparition des cartes bi-mode ont permis d'aller au-delà du simple domaine du contrôle d'accès, vers des cartes multi-application, sécurisées, permettant d'envisager des applications de paiement, d'identité, de billetterie. Le Japon s'est ainsi déjà doté d'une carte d'identité multifonctions sans contact. Mais l'adoption de ces technologies doit se faire avec précautions: le protocole de communication entre la puce et le lecteur doit plus que jamais être résistant aux attaques en confidentialité, altération et rejeu, puisque le médium de communication radio est ouvert à tous, contrairement au mode avec contact, où une telle attaque nécessite une intervention physique, plus difficile et détectable.

De plus, doit être pris en compte le facteur psychologique de la carte à puce sans contact : les technologies sans fil sont vues avec suspicion, et l'intangibilité des transactions effectuées sans contact les rend suspectes. La peur, justifiée ou non, d'être surveillé, ou abusé par ce système risque de susciter un lever de boucliers de la part du public, si ces puces venaient à être utilisées pour des applications sensibles comme le paiement ou l'identité. Car l'insertion physique d'une carte dans la fente du lecteur reste la dernière trace de la tangibilité de la transaction à l'ère du paiement électronique.

5. Références

The Association of the Automatic Identification and Data Capture Industry : http://www.aimglobal.org

The RFID Journal : http://www.rfidjournal.com
AutoID : http://www.autoid.org/
Alien Technology : http://alientechnology.com
Cryptome : http://www.cryptome.org/rfid-docs.htm