TECHN 37

Publication périodique de Smals

Janvier 2014

Le b.a.-ba de la RFID

Origines, Technologies et Applications

1. Introduction

Tania Martin est titulaire

septembre 2013, elle est employée comme consultante à la section Recherche de Smals. Spécialiste en cryptologie, elle étudie la possibilité

solutions et technologies utiles pour le secteur des soins de santé et pour la sécurité sociale.

Contact: 02 787 56 05

Tania.Martin@smals.be

,

(RFID[1]) / authentifier à distance et sans contact visuel des transpondeurs, communément appelés « tags » ou « étiquettes ». « lecteur », serait plus approprié de le nommer « interrogateur ».

a sa propre vision. Cependant, deux caractéristiques fondamentales ressortent systématiquement : chaque tag possède un unique identifiant, et les tags répondent aux requêtes faites par des lecteurs mais ne peuvent pas communiquer entre eux. En mai 2009, la Commission européenne a publié la définition suivante dans sa recommandation 2009/387/EC [1] :

« L'identification par radiofréquence (RFID) [est] l'utilisation d'ondes électromagnétiques rayonnantes ou d'un couplage de champ réactif dans une portion de radiofréquences du spectre pour communiquer vers ou à partir d'une étiquette selon différents schémas de modulation et d'encodage afin de lire, de façon univoque, l'identité d'une étiquette de radiofréquence ou d'autres données stockées sur celle-ci. » (Article 3.a).

Une telle définition ne permet toutefois pas de lever toutes les ambiguïtés. En particulier, la limite entre la RFID et les cartes à puce sans contact reste floue. Les industriels de la carte à puce préfèrent généralement faire une distinction entre les deux concepts car le terme RFID

. ,

. Enfin, on voit depuis peu la NFC[2] se détacher de la RFID. Or, de certaines normes de la RFID. Elle se distingue néanmoins par le fait que tout dispositif NFC typiquement un GSM peut se comporter à la fois comme tag et comme lecteur. Deux GSM peuvent alors communiquer entre eux en utilisant la NFC pour échanger des raisonnables, sans nécessité de couplage, contrairement au Bluetooth par exemple.

Ce document ne parlera que de RFID, en englobant également les autres formes de technologies basées sur les radiofréquences, comme la NFC ou les cartes à puce sans contact.

[1] *Radio Frequency IDentification*.

[2] *Near Field Communication*.

La structure du présent document est la suivante. La section 2 présente brièvement les origines de la RFID. La section 3 introduit la technologie RFID, en particulier les caractéristiques physiques des tags. La section 4 donne quelques exemples concrets . Enfin, la section 5 conclut ce document.

2. Origines de la RFID

Bien que la RFID ait grandi de façon exponentielle ces dernières années, son histoire prend racine au milieu du 20e .
la conception du système IFF[3]
alliés durant la Seconde Guerre Mondiale. Il est impossible de lier la création de la RFID à une personne en particulier, mais il est cependant clair que Charles A. Walton y contribua grandement avec la publication de nombreux brevets, en particulier celui enregistré en 1973 sur un transpondeur passif [2].

,

radiofréquence. Les années 80 ont marqué
technologie sans contact avec les premières applications commerciales, comme
.

Pourtant, la RFID a réellement pris son envol dans les années 90, en particulier avec la vente massive du tag Mifare Classic[4] [3] développé par Mikron (acheté par Philips ,)
millions de copies ont été vendues depuis son introduction sur le marché. Le grand public a
, ,
e les passeports électroniques.

3. La technologie RFID

,
des systèmes basés sur la RFID aux caractéristiques des tags et standards existants.

3.1. Architecture d'un système RFID

Comme représenté sur la figure 1, un système RFID est généralement composé de trois types de dispositifs : , -plan communément appelé *back-end*. Ces entités interagissent ensemble via des protocoles de communication où des messages sont échangés dans (. .
authentifier les tags du système).

[3] *Identify Friend or Foe*.

[4] Lancé en 1995, le tag Mifare Classic a été le premier produit RFID
une carte à puce sans contact, permettant la production massive de ce tag et contribuant à son succès. À titre , était présent dans plus de 80 % du marché des solutions de billettiques sans contact en 2012.

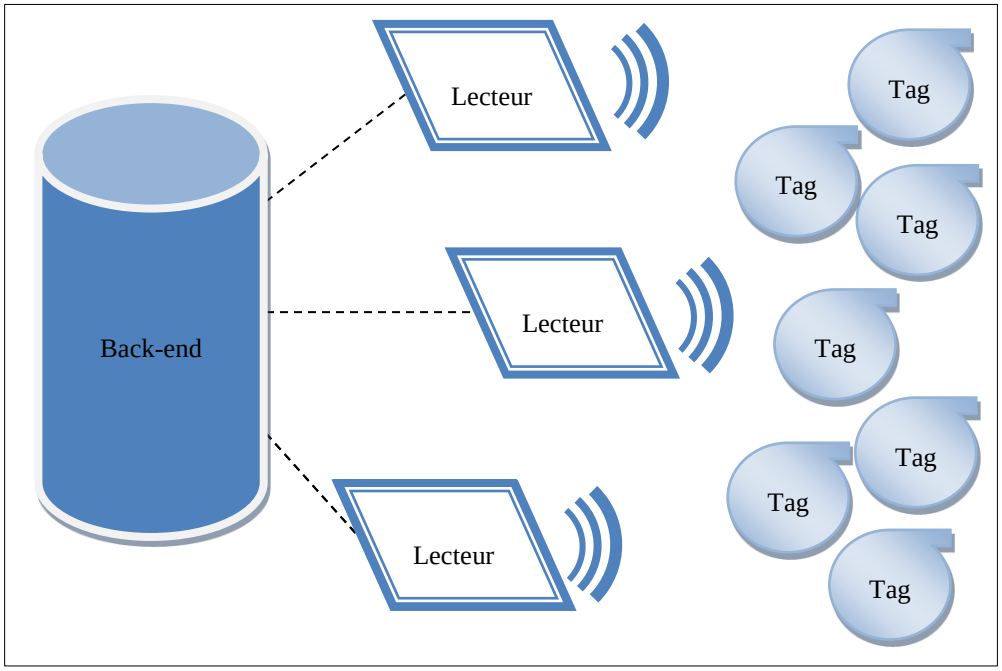

Figure 1 : une architecture RFID typique

Tag RFID

, -à-dire un circuit intégré couplé avec une antenne comme représenté en figure 2, incorporé dans un objet distant. Il peut avoir différentes sources entation, soit la sienne, soit celle fournie par un lecteur RFID. Sa mémoire peut varier de quelques centaines de bits (comme pour les tags EPC[5] [4]) à quelques kilo-octets (comme des cartes à puce sans contact [5] [6]).

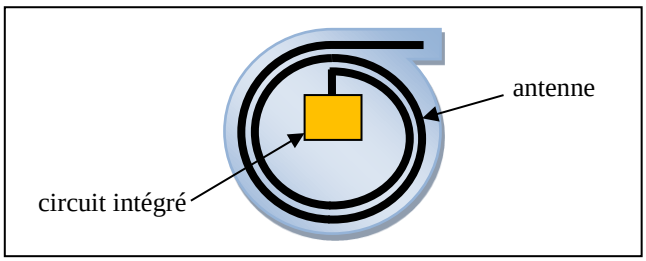

Figure 2 : représentation simplifiée d'un tag RFID

Il peut y avoir différents niveaux de capacités de calcul. Certains tags ne peuvent accomplir , de la cryptographie symétrique, des fonctions de hachage ou même de la cryptographie asymétrique.

Un tag est généralement dit « violable » ou encore « falsifiable », et un attaquant peut . Enfin, sa distance de

[5] *Electronic Product Code*.

communication se situe entre quelques centimètres à quelques décimètres. Les diverses caractéristiques des tags RFID sont détaillées à la section suivante.

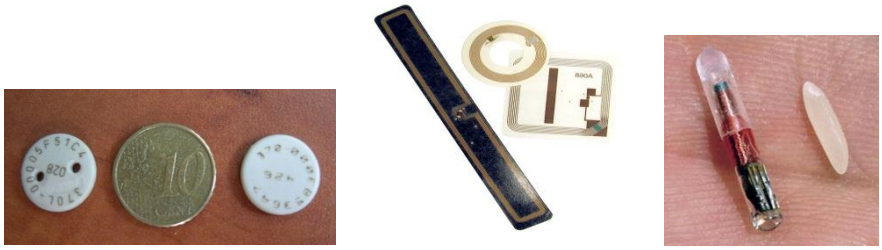

Figure 3 : différents types de tags RFID (crédits : Sancho, Grika, LightWarrior/WikimediaCommons)

Lecteur RFID

Un lecteur est un transreceveur. Il peut communiquer avec un tag quand ce dernier est dans son champ électromagnétique. Il peut aussi communiquer a
back- (. . Ethernet ou Wi-Fi).

un tag. Ses capacités de calcul celles
. (. .) (. .
smartphone) et est généralement considéré comme étant inviolable.

Back-end

Le back-end contient habituellement une base de données qui stocke les informations relatives à chaque tag et lecteur du système (p.ex. les identifiants des tags). Cependant, le back-end peut aussi être une sorte de switch qui ne fait que transférer les communications entre les lecteurs. Dans tous les cas, le back- .

Note : un back- . ,
,
rôle de back-end. utres systèmes, le back-end et les lecteurs sont connectés tous ensemble via un canal sécurisé et peuvent donc être vus comme une seule et unique entité, simplement nommée « lecteur ».

3.2. Caractéristiques des tags RFID

Établir une classification complète de la technologie RFID est difficile étant donné le nombre de caractéristiques qui doivent être considérées pour définir un tag.
e définir les
besoins technologiques et, par la suite, type de tag le plus approprié. Les principales caractéristiques des tags RFID sont représentées sur la figure 4 et décrites ci-dessous.

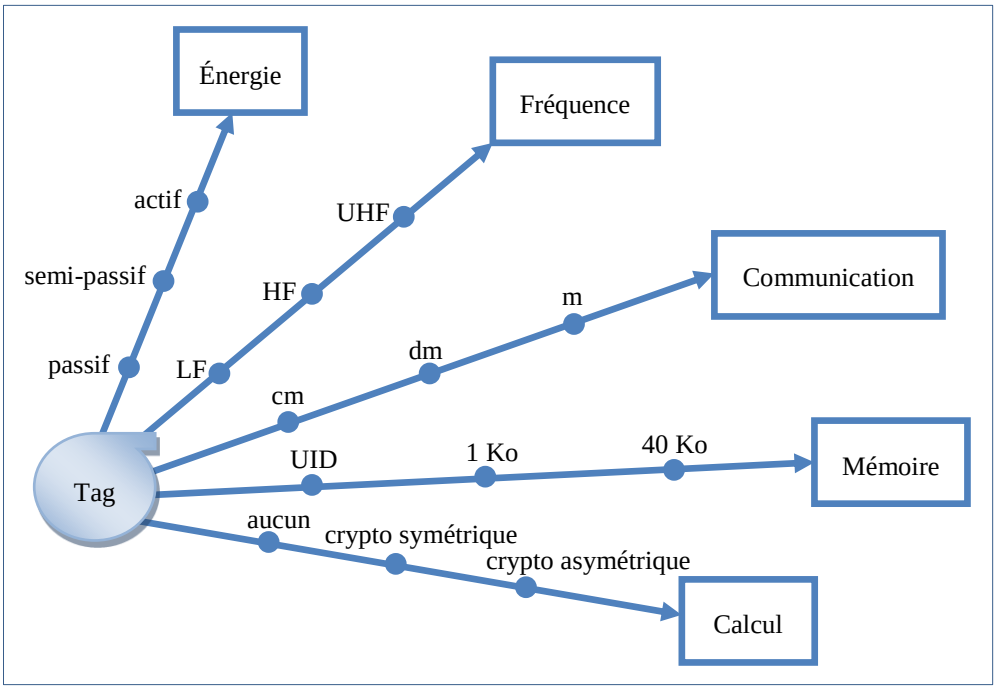

Figure 4 : principales caractéristiques d'un tag RFID

Source d'énergie

.

alimentés par leur propre batterie pour leurs calculs internes et leurs communications avec les lecteurs sont dits « actifs ». Les tags alimentés par le champ électromagnétique des lecteurs sont dits « passifs ». Enfin, les tags sont dits « semi-passifs » quand ils utilisent leur . Ce dernier type de tags est beaucoup moins présent sur le marché que les autres.

Note : la terminologie actif/passif/semi-passif est pas liée à la puissance de calcul ou à la , mais seulement à la façon dont il est alimenté.

passifs, et le simple terme « RFID » est généralement utilisé pour les désigner. Par exemple, les tags pour le tatouage animal, pour remplacer les codes-barres, pour les passeports ou les tickets de transports publics sont , actifs. Dans la suite de ce document, le terme « tag(s) RFID » fera référence aux tags passifs.

Fréquence

La technologie RFID fonctionne essentiellement dans cinq bandes de fréquence définies par le standard ISO/IEC 18000 [7]. Ces fréquences sont listées ci-dessous, accompagnées des .

- 124 135 kHz (LF[6]) : identification animale.

[6] *Low Frequency*.

- 13,56 MHz (HF[7]) : , , .
- 433 MHz (UHF[8]) : .
- 860 960 MHz (UHF) : chaîne logistique.
- 2,45 GHz (UHF) : péage autoroutier, identification de conteneurs.

Trois de ces cinq fréquences sont clairement les plus utilisées pour les applications RFID déployées. La première est la fréquence 124 135 kHz (LF) car elle permet une bonne pénétration dans les environnements métalliques et liquides. La deuxième est la fréquence 13,56 MHz (HF) car elle fournit au tag suffisamment opérations cryptographiques. La dernière est la fréquence 860 960 MHz (UHF) car elle offre de meilleures distances de communication dans le cas des tags passifs.

Évidemment, le choix de la fréquence est plus complexe que ce qui est présenté ici et , , les bandes de fréquence selon le pays où est déployée ou encore les coûts de production.

Distance de communication

Plusieurs paramètres influent sur la distance de communication entre un tag et un lecteur, , , , , . Pour les , en fonction des bandes de fréquence.

- Basse Fréquence (LF) : quelques centimètres.
- Haute Fréquence (HF) : quelques centimètres à quelques décimètres.
- Ultra-Haute Fréquence (UHF) : quelques mètres.

Note : ces distances sont données selon les standards et spécifications des fabricants. Cependant, plusieurs études ont démontré que ces distances peuvent être considérablement augmentées avec un matériel de lecture adéquat [8] [9].

Mémoire

Comme pour les autres paramètres, la quantité de mémoire disponible sur un tag dépend des . [9] du tag. Cet identifiant est en principe déterminé par le fabricant et ne peut plus être modifié par la suite. Outre cet UID, le tag possède généralement de la mémoire EEPROM[10] , -octets. Cette mémoire peut exceptionnellement être beaucoup plus importante, par exemple de 30 à 70 kilo-octets pour un passeport électronique.

[7] *High Frequency*.

[8] *Ultra-High Frequency*.

[9] *Unique IDentifier*.

[10] *Electrically Erasable Programmable Read-Only Memory*.

Capacité de calcul

Les tags sont clairement très limités en termes de calcul. Certains ne peuvent exécuter que de simples opérations logiques (p.ex. comparer un mot de passe reçu avec un autre stocké). , 90 cryptographiques, typiquement un algorithme de chiffrement par flot[11]. , il est plus que commun de trouver des algorithmes de chiffrement par bloc[12] tels que 3DES[13] ou AES[14] sur les tags passifs. Encore onéreux bien que disponibles sur le marché, certains tags passifs peuvent aussi réaliser de la cryptographie asymétrique, par exemple pour les passeports électroniques.

Il existe donc un large éventail de tags avec diverses capacités de calcul, que les intégrateurs chercheront à minimiser pour une application donnée.

3.3. Standards

, couche physique, de la couche communication ou de la couche application, représentées sur la figure 5. Cette section présente les principaux standards liés à la technologie sans contact.

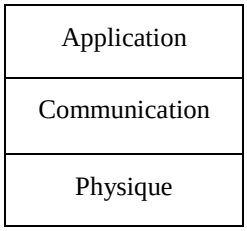

Figure 5 : modèle en couches simplifié pour la RFID

ISO/IEC 14443 [10] et ISO/IEC 15693 [11]

Ces standards couvrent les couches physique et communication de la bande de fréquence 13,56 MHz et constituent la pierre angulaire de la plupart des applications qui ne reposent pas sur des normes propriétaires.

Le standard ISO/IEC 14443 est dédié aux tags de type *proximity* (distance de 10), / 15693 tags de type *vicinity* (80 centimètres). Par exemple, [15] [12] sont basés sur le standard ISO/IEC 14443.

[11] Type de chiffrement symétrique (i.e. la même clé est utilisée pour chiffrer et déchiffrer un message) où le texte à chiffrer est additionné bit à bit à une suite dite chiffrante, cette dernière étant elle-même dérivée de la clé.

[12] Type de chiffrement symétrique où le texte à chiffrer est découpé en blocs de taille fixe (p.ex. 128 bits) et chaque bloc est chiffré avec la clé.

[13] *Triple Data Encryption Standard*.

[14] *Advanced Encryption Standard*.

[15] *International Civil Aviation Organization*.

EPC Class 1 Gen 2 [4]

Le déploiement des tags à très bas coût a été propulsé par -ID Center, un consortium créé aux États- 1999. ,
Network et des différents Auto-ID Labs, a pour but de standardiser et promouvoir la RFID dans les chaî . 1 2
Network est maintenant largement déployé et suivi par de nombreux industriels. Il couvre les trois couches (physique, communication et application).

NFC

La NFC est une technologie de communication sans fil qui opère dans la bande de fréquence 13,56 MHz. Elle prov [16] créé en 2004 par Sony, Philips et Nokia, et maintenant composé de plus de 150 membres.

Cette technologie est compatible avec la RFID en particulier avec le standard ISO/IEC 14443 . Par conséquent, deux appareils NFC, typiquement des GSM, peuvent communiquer en utilisant la technologie RFID. Cela autorise des communications à faible débit et de courte distance qui sont établies beaucoup plus rapidement que des communications Bluetooth ou Wi-Fi.

Le standard ISO/IEC 18092 [13] définit les principales caractéristiques de la NFC et propose un format précis (NDEF[17]) pour stocker et échanger les informations. Il a pour but appareils NFC.

,
NFC est simplement une extension de certains standards de la RFID. Les problèmes de sécurité de la NFC sont donc similaires à ceux de la RFID. Cependant, les solutions pour résoudre ces problèmes peuvent être différents, par exemple en tirant parti des capacités .

Note : il est possible de développer une application compatible avec la technologie NFC sans nécessairement utiliser des GSM, en restant dans un modèle lecteur-tag comme décrit précédemment.

4. Exemples d'application

Les applications industrielles reposant sur la RFID sont multiples et variées. Elles peuvent être regroupées en trois catégories : ( ) , ( ) i de production et (iii) application sécurisée. Cette section présente chaque domaine et les illustre avec des exemples concrets de la vie de tous les jours.

4.1. Contrôle d'accès

.
,
inconnue jusque-là. , avec des passes infrarouges, puis avec des cartes à bande magnétique, et finalement avec des cartes à puce avec contact.
carte dans le lecteur, ce qui représente une perte de temps significative, en particulier dans le

[16] http://www.nfc-forum.org/

[17] *NFC Data Exchange Format*.

. , , les lecteurs étant directement accessibles et souvent vandalisés. La technologie RFID offre la possibilité de réduire ces problèmes et de
dans une carte, une clé ou encore un bracelet. Ainsi, les utilisateurs ont simplement besoin
.

Ticket de ski

Le contrôle a grandement bénéficié de la technologie RFID. Il suit généralement le standard ISO/IEC 15693 qui autorise une distance de communication légèrement plus grande que le standard ISO/IEC 14443. La RFID facilite la vie du skieur : il ; il positionne simplement son passe (potentiellement dans sa poche) devant le lecteur.
un atout pour les compagnies de remontées mécaniques car cette technologie accélère le flux des skieurs tout en maintenant un contrôle systématique.

Figure 6 : remontées mécaniques de ski basées sur la RFID (crédit : Baileypalblue/WikimediaCommons)

Automobile

Depuis 90,
renforcer la sécurité du contrôle . Un tag RFID incorporé dans la clé de voiture peut conducteur s
approche. Dans ces systèmes, la RFID peut également être utilisée comme solution pour le démarrage de la voiture : lorsque le conducteur introduit sa clé dans le barillet de , tag RFID. Si ce dernier
présent, le démarrage sera refusé par la voiture. Ces systèmes anti-démarrage sont généralement basés sur les bandes de fréquence LF comprises entre 100 et 135 kHz.

Péage autoroutier

ancienne. Comme
pour les stations de ski, le but est de faciliter la vie des conducteurs et de la compagnie. Le ère du péage.
Certains systèmes autorisent même le conducteur à passer à pleine vitesse le péage. La compagnie ici aussi gagne en efficacité tout en réduisant ses coûts. La RFID automatise les contrôles, ce qui permet à la compagnie de réduire son effectif en postes .
Comme la distance de lecture exigée est relativement grande (environ 5 mètres), une
.

Transports publics

, pour le voyageur et la société de transport. Le voyageur gagne en simplicité : il est plus simple pour lui de passer son ticket

. ,

distances parcourues, le voyageu
traversées : .

de son infrastructure que le simple comptage du nombre de voyages effectués. La technologie RFID permet également à la compagnie de réduire la contrefaçon de tickets car il est plus difficile de produire de faux tags RFID que de faux tickets en papier.

De nos jours, un grand nombre de villes ont opté pour un système de transports publics basé sur la RFID, par exemple Bruxelles, Paris, Londres, Amsterdam, Berlin, New York ou encore Hong Kong. À Bruxelles, la société de transports publics STIB a lancé en 2008 son système RFID de billettique, appelé « MOBIB »,
système basé sur des cartes à bande magnétique. MOBIB repose sur le standard Calypso [14], lui-même déjà en place dans plus de 20 pays.

Figure 7 : portillon RFID dans une station de métro (crédit : ProtoplasmaKid/WikimediaCommons)

4.2. Pistage et suivi de production

Dans le domaine de la logistique, la RFID est la nouvelle alternative aux codes-barres qui fournit deux avantages majeurs. Le premier est la distance de lecture. En effet, les codes-

,

de lire un . Cette caractéristique
: une passe suffit pour scanner toutes les palettes se trouvant dans un conteneur, et le statut des stocks peut être vérifié en temps réel. Le deuxième avantage de la RFID est sa meilleure résistance aux éléments externes et détériorations. Clairement, si un code-barres est plié, déchiré ou recouvert de poussière, sa lecture devient impossible. Les conditions de lecture jouent également un rôle important. Par exemple, un code-
lumière.

Identification animale

80.
technologie est utilisée pour ,
. Les tags sont attachés aux oreilles des animaux ou encore incorporés dans des bagues ou colliers, en fonction . La RFID peut servir à
santé, par exemple pour contenir des épidémies la plus fameuse étant la maladie de la vache folle ou, plus récemment, la grippe porcine. Une telle utilisation de la RFID nécessite une interopérabilité complète entre les différentes compagnies de production.
cela que certains standards ont été créés, / 11784 [15] / 11785 [16] qui reposent sur la bande de fréquence LF 134,2 kHz.

.
grain de riz et sont injectés en sous- .
chocolatée et sont ingérés par les animaux.

, [18] comme organisme de .
, identification canine peut se faire via un tag RFID implanté en sous-cutané . Ce tag contient simplement un numéro 15 -ci est interrogé par un lecteur. nt une base de données de tous les numéros , ainsi que les données spécifiques de chaque animal (p.ex. âge, race) et les données personnelles de chaque propriétaire (p.ex. nom, adresse, téléphone).

Figure 8 : animal portant un tag RFID accroché à son oreille (crédit : Haslam/WikimediaCommons)

Bibliothèque

La RFID facilite le prêt de livres et la gestion des stocks dans les bibliothèques. Elle /
replacé sur les étagères. De plus, e portiques aux sorties de la , enregistré peut déclencher une alarme.
Les bibliothèques utilisent typiquement la technologie RFID avec la bande de fréquence HF 13,56 MHz basée sur le standard ISO/IEC 15693.

18 .

Figure 9 : système RFID pour une bibliothèque (crédit : LIU/WikimediaCommons)

Suivi dans une chaîne logistique

à utiliser la RFID pour la gestion de sa chaîne logistique. Ce projet a commencé en 2003 lorsque Walmart a imposé 2005. Le coût étant trop élevé pour les fournisseurs, Walmart a révisé ses attentes à la baisse et demandé que seules les palettes soient équipées de tags RFID. Les tags utilisés par Walmart 1 2 deux mètres.

4.3. Application sécurisée

Passeports électroniques

. Les tags incorporés dans la couverture des passeports répondent au standard DOC 9303 [12] de pour la couche application et au standard ISO/IEC 14443 pour les couches inférieures.

Les informations du détenteur du passeport sont stockées dans des groupes de données, appelés « DG[19] ». En particulier, le DG1 contient toutes les données écrites sur la zone du passeport destinée à la lecture automatique, appelée « MRZ[20] ». Un exemple de MRZ est donné à la figure 10 avec le . Dans la figure 11 détaillant la MRZ, on y retrouve entre autres le nom et la date de naissance . Le DG2 contient la photo du détenteur du passeport, et le DG3 principalement utilisé en Europe stocke ses empreintes digitales.

[19] *Data Group*.

[20] *Machine Readable Zone*.

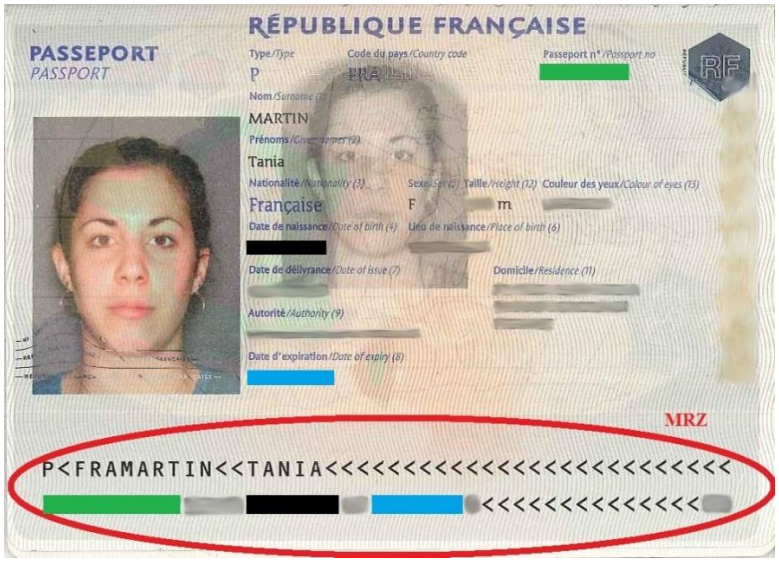

Figure 10 : MRZ d'un passeport français

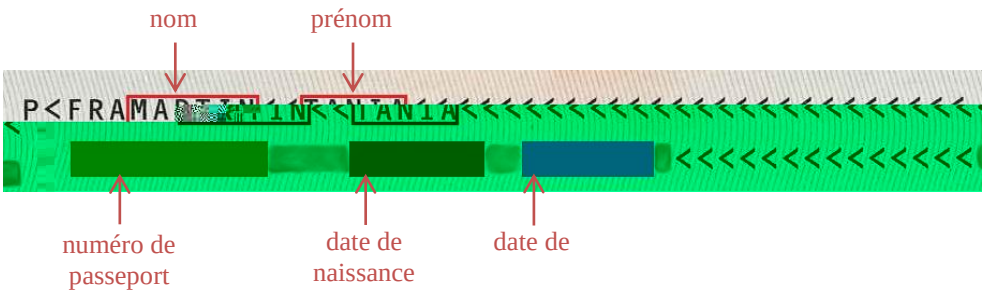

Figure 11 : détail d'une MRZ

mécanismes[21]. La lecture des données est aussi protégée par un protocole [22], appelé « BAC[23] ». Sans détailler BAC, il faut néanmoins retenir que n complète du protocole requiert la connaissance de la deuxième ligne de la MRZ du passeport. Ceci
pour pouvoir accéder au contenu du tag. Les passeports stockant les empreintes digitales , EAC[24] », qui ne permet .

[21] La description de ces mécanismes est hors du cadre de ce document. Le lecteur intéressé pourra consulter [17] pour obtenir plus de détails.

[22] , procédure par laquelle un lecteur RFID est .

[23] *Basic Access Control*.

[24] *Extended Access Control*.

Paiement sans contact

Une application récente basée sur la RFID est le paiement sans contact. Elle a déjà été

montants. Un des exemples les plus connus est le Speedpass, introduit en 1997, permettant aux conducteurs américains de payer leur carburant par paiement sans contact aux stations Exxon, Mobil et Esso. Dans ces systèmes, les tags RFID sont incorporés dans des porte-clés et opèrent sur la bande de fréquence LF 125 kHz.

Figure 12 : tag RFID incorporé dans le porte-clés Speedpass (crédit : Atkinson/WikimediaCommons)

Les principaux groupes bancaires MasterCard, American Express et Visa ont également investi dans de telles applications. Depuis le début des années 2000, chacun développe son propre système de paiement sans contact qui, contrairement au Speedpass, opère à la bande de fréquence HF 13,56 MHz avec le standard ISO/IEC 14443.

Le paiement sans contact est aussi un domaine en plein boom pour la NFC, particulièrement dans le cas des transports publics. De nombreux pays comme la France, le Japon ou les États-Unis testent les solutions NFC pour centraliser toutes les cartes des utilisateurs sur leur GSM. Selon les firmes, cela va grandement faciliter la vie des utilisateurs. Le GSM sera alors à la fois une carte de crédit, un abonnement aux transports publics, une carte

besoin de son portefeuille, mais seulement de son GSM.

Figure 13 : paiement à un distributeur de boissons via NFC (crédit : Alecrim/WikimediaCommons)

5. Conclusion

. en une multitude de technologies différentes, avec divers standards et caractéristiques physiques. La RFID se retrouve dans de nombreuses applications mises sur le marché public .

Avec ce déploiement à grande échelle, il est donc
RFID. Cette invasion dans le quotidien soulève de grandes interrogations et craintes de la part des consommateurs et des autorités vis-à-vis du respect de la vie privée. Ceci est en particulier dû au fait que les tags sont incorporés dans des objets portés par des personnes. Les tags RFID peuvent-ils révéler des informations qui pourraient nuire à la vie privée du porteur du tag ? La RFID peut-elle aider les compagnies à récolter des informations sur les consommateurs ? La RFID peut-elle servir à tracer voire traquer les consommateurs et leurs habitudes ? Y a-t-il assez de mécanismes de sécurité mis en place et utilisés dans les systèmes RFID ? Si oui, sont-ils suffisamment efficaces ? Un prochain Techno pourrait évoquer cette problématique de la vie privée dans les systèmes RFID.

6. Bibliographie

[1] European Commission (Viviane Reding), "Commission recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification," *Official Journal of the European Union*, vol. L(122), pp. 47--51, May 2009.

[2] C. A. Walton, "Electronic Identification and Recognition System". U.S. Patent 3,753,960, 14 August 1973.

[3] NXP Semiconductors, "Mifare Smartcards ICs," [Online]. Available: http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/.

[4] EPC Global Inc., "Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.2.0," October 2008. [Online]. Available: http://www.epcglobalinc.org/standards/.

[5] Infineon, "Contactless SLE 66 Family," [Online]. Available: http://www.infineon.com/.

[6] NXP Semiconductors, "DESFire Tags," [Online]. Available: http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/mifare_desfire/.

[7] International Organization for Standardization, "ISO/IEC 18000: Information technology - Radio frequency identification for item management," ISO, 2008.

[8] G. Hancke, "Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens," *Journal of Computer Security*, vol. 19(2), pp. 259--288, March 2011.

[9] P.-H. Thevenon, «Sécurisation de la Couche Physique des Communications Sans Contact de Type RFID et NFC,» 2012.

[10] International Organization for Standardization, "ISO/IEC 14443: Identification cards - Contactless integrated circuit cards - Proximity cards," ISO, 2001--2008.

[11] Internation Organization for Standardization, "ISO/IEC 15693: Identification cards - Contactless integrated circuit(s) cards - Vicinity cards," ISO, 2000-2009.

[12] International Civil Aviation Organization, "Machine Readable Travel Documents, Doc 9303, Part 1, Machine Readable Passports, Fifth Edition," ICAO, 2003.

[13] International Organization for Standardization, "ISO/IEC 18092: Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol," ISO, 2004.

[14] Innovatron, "Calypso Electronic Ticketing Standard," 1993.

[15] International Organization for Standardization, "ISO/IEC 11784: Radio frequency identification of animals - Code structure," ISO, 1996.

[16] International Organization for Standardization, "ISO/IEC 11785: Radio frequency identification of animals - Technical concept," ISO, 1996.

[17] G. Avoine and J.-J. Quisquater, "Passport Security," in *Encyclopedia of Cryptography and Security (2nd Ed.)*, Springer, 2011, pp. 913--916.