LE MAGAZINE
D'ASPROM
(www.asprom.com <http://www.asprom.com>)

TRIMESTRIEL - 45 €

n°37
Août 2009
Septembre 2009

NUMÉRO SPÉCIAL SUR LES COMMUNICATIONS SANS FIL DE PROXIMITÉ

MINIATURISATION ULTIME DE SYSTÈMES : NANOMACHINES ET MOTEURS MOLÉCULAIRE

Roland DUBOIS
Publications de ASPROM
7, rue Lamennais -75008 PARIS
Tél. 06 07 02 83 93 - Fax. 01 42 89 82 50
Rédacteurs : Jean-Claude BASSET, Pierre COTTIN, Jean-Claude FRAVAL, Guy GIRARDETTI, Maurice MORDANT, Patrice ROUSSO
Prix du numéro : 45 € - Abonnement : 152 €.

Maquette : Patrick Perrault.
Mise en page, composition, impression : Imprimerie DÉJAGLMC. 01 34 45 22 22

Les communiqués de presse et les invitations aux conférences de presse sont à envoyer à :
Roland DUBOIS
Veille Technologique
3, rue de la Pléiade
94240 L'haÿ les Roses

VEILLE TECHNOLOGIQUE

LE PRÉSENT NUMÉRO ABORDE DEUX DOMAINES TECHNOLOGIQUES FORTS PROMETTEURS : LES COMMUNICATIONS SANS FIL DE PROXIMITÉ ET LES NANOTECHNOLOGIES.

La technologie de communication sans fil de proximité est utilisée dans plusieurs domaines d'application où d'ailleurs elle porte des noms différents. Elle se nomme « RFID » pour faire la traçabilité de biens matériels ou d'animaux, elle prend le nom de « sans contact » pour effectuer du contrôle d'accès de personnes dans les bâtiments ou dans les transports publics, ou pour réaliser des paiements ; elle devient « NFC » lorsque embarquée sur un téléphone portable elle permet de gérer le contrôle d'accès de personnes dans les bâtiments ou dans les transports publics, ou des paiements.

Parmi toutes les technologies dites RFID, l'une d'entre elles, décrite par le standard ISO/IEC 14443, a permis au cours de ces dernières années de développer des applications très variées, et particulièrement différentes les unes des autres. De nouvelles technologies sont en développement sur la thématique des systèmes d'identification et de traçabilité sans contact. Parmi celles qui émergeront à court/moyen terme, on peut citer actuellement : les interfaces air pour augmenter les débits des cartes à puces sans contact ; les antennes dites 3D permettant de lire une étiquette dans n'importe quelle position ; les micro-capteurs téléalimentés, la gestion de l'énergie via la récupération de puissance disponible, la conversion et le stockage ; la protection des communications sans contact pour prévenir la fraude et protéger la vie privée.

Le NFC (Near Field Communication) est une évolution des diverses technologies « sans contact » appliquées à des équipements électroniques grand public. Le NFC est une technologie permettant à n'importe quel appareil d'émettre un champ à courte portée (inférieure à 10 cm) pour échanger des informations. Aujourd'hui, un des appareils phares, pressenti pour embarquer la technologie NFC, est le téléphone mobile. L'intérêt est que l'utilisateur a toujours son téléphone mobile sur lui, et le taux de diffusion du téléphone mobile est un atout.

Pour faire connaître les standards, les technologies, les usages, les applications, mais aussi les défis et les enjeux autour des « communications sans fil de proximité », ASPROM a organisé deux journées sur ce thème avec quelques uns des meilleurs experts des grandes organisations, mais aussi de jeunes entreprises innovantes. Veille technologique a demandé à ces experts de vous faire partager leur expérience dans ce domaine.

Dans l'évolution constante vers la miniaturisation des dispositifs électroniques et mécaniques, les molécules jouent un rôle de plus en plus important. Dans le cadre de ses travaux sur la miniaturisation ultime des systèmes, le CEMES a conçu des nanomachines et des moteurs moléculaires, qui constituent de véritables prouesses technologiques. Cet article fait suite à un séminaire qu'avait organisé ASPROM sur les nanotechnologies.

Roland DUBOIS

SOMMAIRE DES ACTUALITÉS

COMMUNICATION SANS FIL DE PROXIMITÉ

NANOTECHNOLOGIE

COMMUNICATIONS SANS FIL DE PROXIMITÉ

Technologie de communication de proximité et qualification

Par Christophe CHANTEPY, Responsable RFTLab
(Christophe.chantepy@esisar.grenoble-inp.fr)

La technologie de communication de proximité, à des fins d'identification et de transaction de données, fait-elle partie des technologies du futur ou du passé ? Difficile de répondre par l'affirmative à une telle question mais il est à noter qu'elle est en pleine évolution. Ce qui peut être remarqué, c'est que la technologie de communication de proximité par radio fréquence est utilisée dans plusieurs domaines d'application où d'ailleurs elle porte des noms différents. Elle se nomme « RFID » pour faire la traçabilité de biens matériels ou d'animaux, elle se nomme « sans contact » pour faire du contrôle d'accès de personnes dans les bâtiments ou dans les transports publics, ou pour faire des paiements ; elle se nomme encore « NFC » lorsque embarquée sur un téléphone portable, elle permet de gérer le contrôle d'accès de personnes dans les bâtiments ou dans les transports publics, ou des paiements . Ces quelques lignes d'entrée en matière risquent fort de faire grincer les dents des puristes qui verront ici une confusion totale, et peut-être une vision plus globale et simplifiée pour les non-initiés. Mais rappelons qu'en ce qui concerne la fréquence de fonctionnement à 13,56 MHz, les équations de Maxwell restent les mêmes quelque soit le domaine d'application !

Il est bon de préciser à ce moment que pour la traçabilité par RFID, il existe un grand nombre de solutions technologiques : différentes fréquences (>135 kHz, 13,56 MHz, 433 MHz, 860-960 MHz, 2,45 GHz) pour lesquelles des normes ISO de protocole de communication existent, des systèmes actifs et des systèmes assistés par batterie.

Ces « nouvelles technologies » d'identification et de communication ont débuté dans les années 90 par le démarrage des travaux de normalisation avec dans l'ordre historique : le sans contact, la RFID, le NFC… à suivre le MIIM mais on y reviendra plus tard. Attachons-nous tout d'abord à la technologie Inductive à 13,56 MHz qui est bien maîtrisée en France et en Europe depuis plusieurs années mais pas encore vraiment déployée.

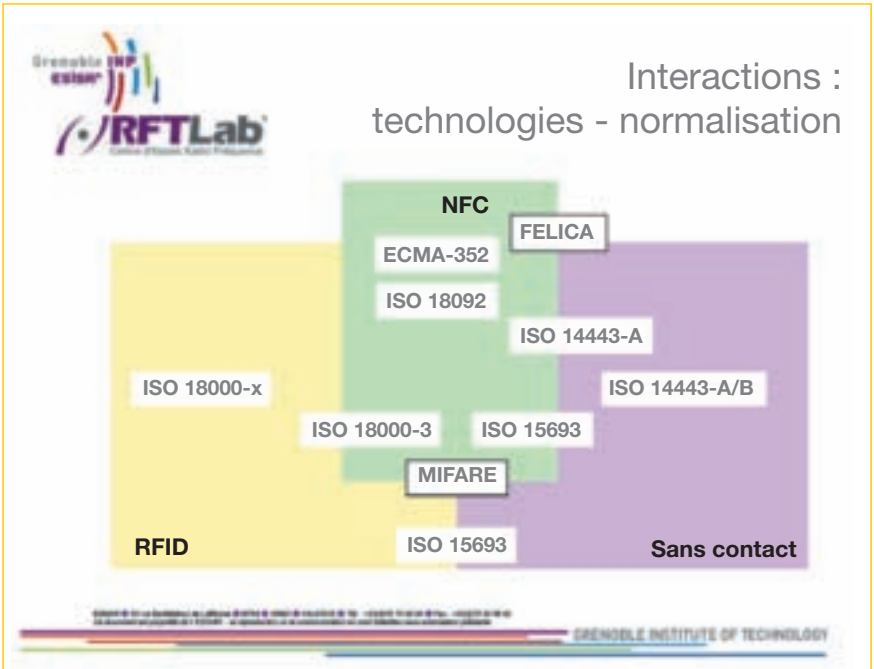


Fig. 1 : interactions entre les technologies et les normes

Le schéma de la figure 1 présente les interactions entre les technologies et les normes (seules les principales normes de protocole de communication sont citées).

On retrouve les normes émanant de l'ISO, de l'ECMA ainsi que des standards propriétaires de Sony et NXP (Philips).

Déploiement et développement des technologies :

Le déploiement de ces technologies reste encore marginal (exception pour le transport) sur le territoire français mais semble être en évolution au vu des nombreux pilotes qui voient le jour depuis ces 2 dernières années. POURQUOI ? Est la question légitime que nous pouvons nous poser au sujet du manque de vraies applications. Plusieurs réponses peuvent être émises pour l'ensemble des technologies :

1. finalisation et adoption des normes,
2. technologie nouvelle,
3. technologie de rupture,
4. interopérabilité.

1. Finalisation et adoption des normes

Comme toutes technologies de communication, il est nécessaire de définir des normes de protocole afin de remplir cette fonction de transfert d'information dans les meilleures conditions. Cette normalisation, se basant sur les nouvelles technologies, est en évolution permanente afin de prendre en compte le développement technique, les contraintes d'utilisations et les intérêts économiques privés. Cela se remarque par le nombre d'amendements existants sur l'ISO 14443 ou les travaux actuels sur l'ISO 18000-6.

Les marchés (les acheteurs) sont frileux quant à acheter une solution technologique non stable ; en effet il reste difficile de justifier le choix d'une « solution propriétaire » sans garantir de pérennité par une double source.

Cette période de flou semble aujourd'hui se terminer et laisse espérer une évolution importante des marchés.

COMMUNICATIONS SANS FIL DE PROXIMITE

2. Technologie nouvelle

Ces technologies de communication de proximité ne sont pas nouvelles dans leur principe mais le sont dans leur intégration et leur utilisation. C'est là que se situe la difficulté de ces technologies qui sont amenées à évoluer afin de s'adapter aux utilisations potentielles qui peuvent en être faites. Or cette évolution, ou adaptation permanente, donne l'impression que ces technologies ne sont pas abouties et par voie de conséquence pas fiables pour une utilisation industrielle. Cela impacte directement sur le coût des produits proposés qui reste encore élevé pour faire le choix d'une modification complète des systèmes existants.

3. Technologie de rupture

Ces technologies remettent en cause de nombreuses choses dans une application donnée : le processus métier, la gestion des données, l'architecture et l'infrastructure existantes, les habitudes humaines,…

Deux exemples peuvent être cités, le premier est le paiement sans contact qui est une étape supplémentaire à la dématérialisation de l'argent et qui soulève certains problèmes de sécurité (intégrité, confidentialité, disponibilité, non répudiation, authentification). On note également le coté « High Tech » qui passe encore difficilement dans notre société, contrairement au Japon.

Le second exemple est la traçabilité des biens de consommation qui se veut unitaire et mondiale, d'où les problèmes de gestion et de sécurité des informations.

4. Interopérabilité

L'interopérabilité est la capacité que possède un produit ou un système, dont les interfaces sont intégralement connues, à fonctionner avec d'autres produits ou systèmes existants ou futurs et ce sans restriction d'accès ou de mise en œuvre.

Cette notion d'interopérabilité très simple à comprendre et à appréhender pour un système de communication filaire par la vérification du protocole de communication, des niveaux de signaux admissibles, devient bien plus complexe pour un système RF et particulièrement un système de communication de proximité autoalimenté. Ces paramètres sont alors variables en fonction de facteurs externes qui rendent l'interopérabilité plus complexe à vérifier…

Sur le plan du développement, les systèmes continuent d'évoluer afin d'intégrer les dernières avancées technologiques ou de s'adapter aux futures utilisations potentielles auxquelles elles sont promises. On peut citer les développements actuels suivants :

- les méthodes et processus de fabrication d'antennes à base d'encre et de nanotechnologie,
- l'électronique imprimée,
- les transpondeurs « chipless »,
- la miniaturisation des transpondeurs,
- les systèmes de récupération d'énergie pour alimenter des capteurs ou des organes de sécurité,
- des méthodes de protection,
- l'évolution des protocoles de communication pour l'augmentation des débits,
- l'intégration et la multiplication des facteurs de forme des transpondeurs.

Les tests de qualifications :

L'interopérabilité, introduite précédemment, est un point essentiel du déploiement de ces technologies. Comment développer un service sans garantir un fonctionnement fiable et constant, quel que soit l'origine des éléments constituants le système : coupleur et transpondeur ?

Difficile d'expliquer à un utilisateur, comme AIRFRANCE par exemple, que le système d'identification des bagages aura des performances de détection de l'ordre de 95 % dans certaines conditions (type de transpondeurs, type de lecteur, environnement, lieu,…) et des performances inférieures à 60 % dans d'autres !

Autre exemple, les utilisateurs des transports en commun qui doivent sortir leur nouvelle carte d'accès de leur portefeuille ou de leur sac à main alors que cette opération n'était pas nécessaire avec l'ancienne version.

Comme nous l'avons décrit précédemment, la notion d'interopérabilité est plus complexe dans un système RF et ne suffit pas à garantir les niveaux de performances attendues.

Pour illustrer cela, il suffit de suivre les nombreux travaux en cours sur la norme de tests ISO 10373-6 pour le sans contact qui doit prendre en compte les évolutions des technologies (composants, antennes, matériaux, systèmes de sécurité..) mais aussi des utilisations avec notamment le facteur de forme des transpondeurs (des antennes) qui impacte fortement sur le couplage magnétique et donc sur les paramètres de la transmission (transfert d'énergie, niveau de modulation, timing,…).

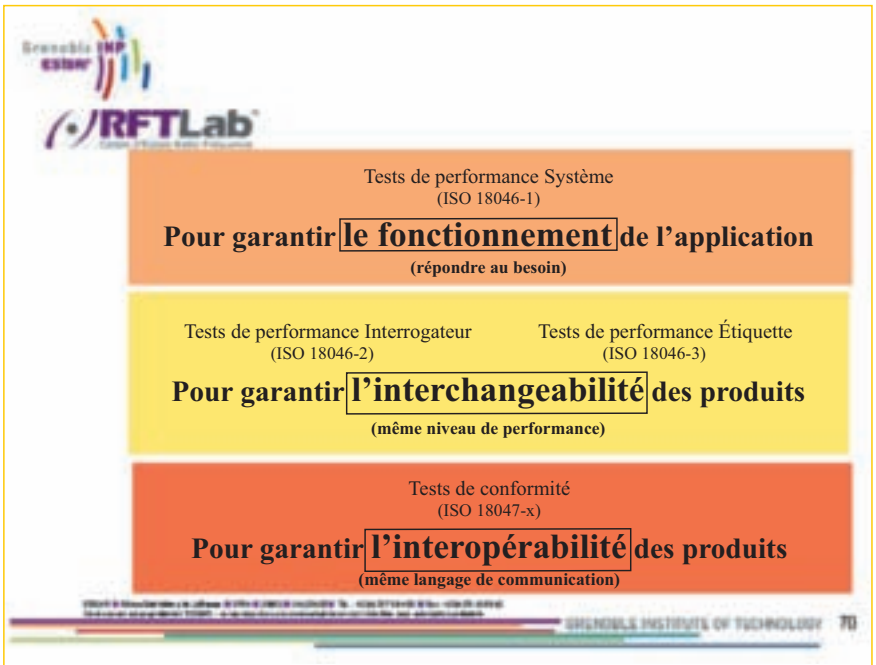


Tableau 1 : Les points clés de la certification : les normes

Ces problématiques se retrouvent à l'identique pour le NFC avec l'intégration sous diverses formes des antennes dans les téléphones.

Afin de répondre à cela, une approche différente a été initiée au sein de la commission de normalisation sur les RFID CN31 en introduisant une notion de conformité au protocole de communication (interopérabilité) et surtout une notion de performances (interchangeabilité) dont voici le détail dans *le tableau 1 :*

Ces normes permettent d'évaluer les performances RF des systèmes de communication et ainsi de prédire ou de corriger les problèmes potentiels.

Le RFTLab® travaille depuis plus de 9 ans sur ces problèmes de tests RF liés aux technologies de communication de proximité. Il est notamment à l'origine des normes de performances en RFID série ISO 18046-x.,

Le RFTLab® a développé des compétences et des moyens d'investigation spécifiques *(figure 2).*

Le RFTLab® réalise des essais de caractérisation avancés, avec la capacité de prendre en compte les éléments de l'applicatif pour la qualification des produits.

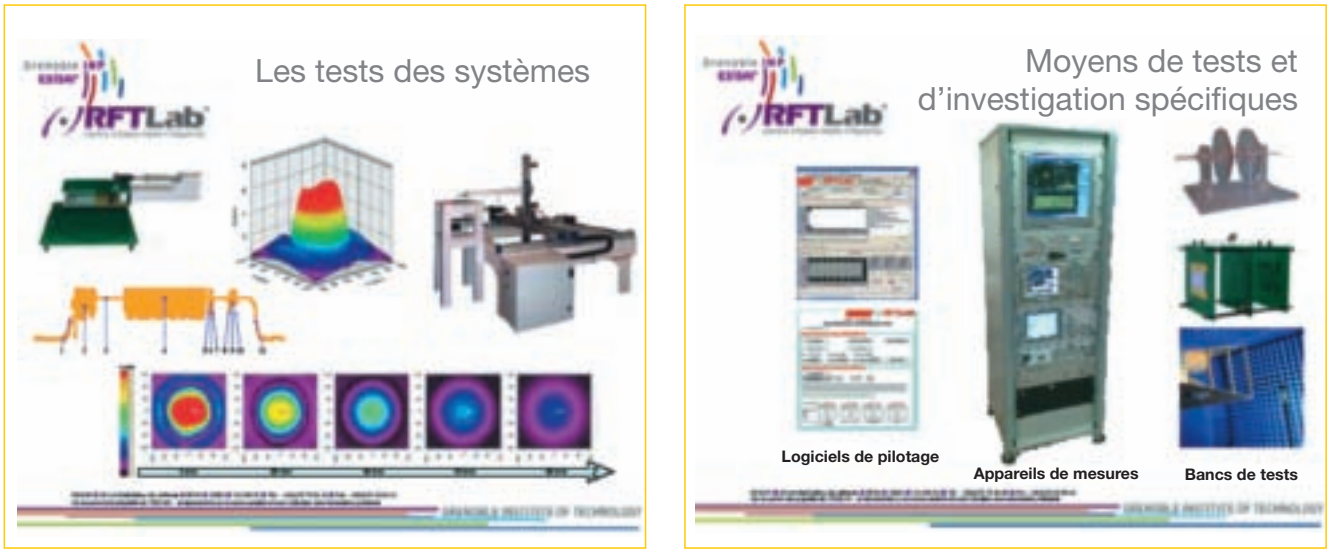


Fig 2 : Le RFTLab® a développé des compétences et des moyens d'investigation spécifique

BULLETIN D'ABONNEMENT A VEILLE TECHNOLOGIQUE

Je souhaite recevoir "VEILLE TECHNOLOGIQUE" pendant 1 an, soit 4 numéros au prix de 152 € TTC.
Règlement établi à l'ordre de ASPROM : 7, rue Lamennais 75008 PARIS - FRANCE.

☐ Chèque bancaire ☐ Virement bancaire ☐ Autre

Nom : _____ Prénom : _____

Fonction : _____

Société et adresse : _____

_____

_____

Téléphone : _____ Fax : _____ E-mail : _____

Signature :

COMMUNICATIONS SANS FIL DE PROXIMITÉ

La technologie sans contact de proximité IS0 / IEC 14443 Une fondation solide pour un vaste champ d'applications

Cet article a été rédigé à partir des notes prises lors de la conférence de Jean-Paul CARUANA de GEMALTO

Parmi toutes les technologies dites RFID, l'une d'entre elles, décrite par le standard ISO/IEC 14443, a permis au cours de ces dernières années de développer des applications très variées, et particulièrement différentes les unes des autres. Sa souplesse d'implémentation, ses performances et ses caractéristiques principales ont permis son utilisation dans tous les segments de marché des applications sécurisées au travers de projets variés. Ce sont :

- des applications transports dont les caractéristiques sont grande vitesse (transaction de courte durée) et faible quantité d'information échangée,
- des applications de contrôle d'accès sécurisées ou non,
- des applications de paiement qui nécessitent sécurité et confidentialité,
- des applications gouvernementales d'identité telle que le passeport électronique qui transfère un grand volume de données.

Cette technologie a permis le développement d'applications à succès mondial tel que Paypass[1] (Paiement), Calypso[2] ou Mifare[3] (Transport), Desfire[4] (Transport , Access Control), ICAO[5] (Travel Document e-Passport).

Les raisons d'un succès

Les succès de l'ISO/IEC 14443 s'explique d'abord par les performances de cette technologie : débits d'information de 106 Kb/s à 847 kb/s, absence de latence entre échanges, distances de fonctionnement de 0 à une dizaine de centimètres. Cette technologie, à très faible coût, permet d'alimenter de simples petites mémoires jusqu'à de complexes crypto-processeurs DES, RSA ou encore AES.

La technologie ISO/IEC 14443 répond à un réel besoin : pour être mise en œuvre, elle nécessite une action volontaire de l'utilisateur ; elle implique de mettre en relation deux objets pour initialiser une transaction.

La technologie ISO/IEC 14443 présente une indépendance totale quant à l'usage. Initialement définie pour des formats cartes, elle est avantageusement utilisée dans les passeports biométriques, Dongle USB, porte-clés RFID ou téléphones portables

L'ISO/IEC 14443 est un standard mondial, complet, accompagné de méthodes de test simples et peu coûteuses, ce qui permet à des laboratoires indépendants de contrôler des produits indépendamment des constructeurs. C'est un standard qui intéresse de nombreux acteurs industriels.

Un standard vivant

Les premiers travaux concernant la définition de ce standard ont commencé en 1994. Pendant une longue période, ces travaux n'ont intéressé que les spécialistes, ce qui a permis d'élaborer sérieusement ce standard avant sa publication en 2000 - 2001 *(Tableau 1)*.

Par la suite, l'ISO / IEC 14443 a été amendé à de nombreuses reprises *(Tableaux 2, 3 et 4)*, ce qui est tout à fait normal dans la vie d'une norme. Les amendements concernent notamment les applications bancaires et de passeports électroniques.

Et maintenant….

L'ISO/IEC 14443 continue de s'améliorer au travers de processus d'amendements. En 2006, il a été procédé à la révision quinquennale du standard avec l'intégration de l'ensemble des amendements effectués au cours des cinq années précédentes. Il a été lancé la création de Class de produits.

L'ISO/IEC 14443 fournit les briques de base technologique utilisables par des applications et d'autres standards (ISO/IEC 18092, les spécifications ECMA, les spécifications NFC (NFC Forum). Elle est supportée par un nombre croissant d'autres standards : standard PC/SC, Bluetooth (appairage).

1994 : start of works on "Remote coupling cards"

1995 : share between Proximity (14443) and Vicinity (15693)

1996-1999 : main technical choices (types A and B) and ballots

2000-2001 : publication of the 4 parts of ISO/IEC 14443 and associated test methods, ISO/IEC 10373-6

2001-2002 : draft amendment for optional types C, D, E, F and G

2002 : definitive abandonment of this amendment

Tableau 1 : Les différentes dates de développement de la norme ISO / IEC 14443

1 **PayPass** de MasterCard utilise la technologie de paiement sans contact. Ainsi, au lieu d'insérer ou de glisser la carte dans la fente du lecteur, le client n'a qu'à la placer ou à l'agiter devant le lecteur du terminal. La carte ne quitte jamais sa main. Régler un achat avec PayPass, c'est le moyen le plus simple de payer.

2 **Calypso** et son pendant parisien Navigo est une carte à puce sans contact qui sert de passe-partout dans le métro, les bus ou les tramways.

3 **MIFARE** est une des technologies de carte à puce sans contact les plus répandues dans le monde avec 500 millions de cartes et 5 millions de modules de lecture/encodage. La marque, lancée par Philips, est propriété de la société NXP. **MIFARE** est basée (partiellement ou complètement selon les modèles) sur l'un des standards ISO décrivant les cartes à puce sans contact: la norme ISO/IEC 14443 de Type A fonctionnant à 13,56 MHz. La technologie est intégrée à la fois dans les cartes et dans les lecteurs/encodeurs.

4 La carte **MIFARE DESFire** est une version spéciale de la plate-forme **NXP SmartMX**. Elle est vendue préprogrammée avec le système d'exploitation **DESFire** (ou **DESFire operating system**). Il s'agit d'un logiciel générique qui offre globalement les mêmes fonctions que celles des cartes *MIFARE Standard* (soit 4 ko de stockage répartis sur 16 zones) mais avec une plus grande flexibilité, une sécurité accrue avec du Triple DES et une communication plus rapide.

5 L'**ICAO** (International Civil Aviation Organization) a défini plusieurs standards de passeports et visas électroniques s'appuyant sur les technologies de puces sans contact.

Standard	Publication	Pages
ISO/IEC 14443-1:2000 Proximity cards - Physical characteristics	13/04/2000	5
ISO/IEC 14443-2:2001 Proximity cards - Radio frequency power and signal interface	28/06/2001	11
ISO/IEC 14443-3:2001 Proximity cards - Initialisation and anti-collision	01/02/2001	48
ISO/IEC 14443-4:2001 Proximity cards - Transmission protocol	18/01/2001	34
ISO/IEC 10373-6:2001 Test methods – Proximity cards	31/05/2001	24

Tableau 2 : ISO/IEC 14443, ISO/IEC 10373-6 – Résumé

	WD[6]	CD[7]	FCD[8]	FDIS[9]	IS[10]
Optional communication types 14443-2 AMD1	2000-11	2001-032002-01: definitive abandonment			
Optional high bit data rates 14443-2 AMD2 14443-3 AMD1	2003-06	2003-07	2003-11	2004-10	2005-01
Optional very high bit data rates 14443-2 AMD3 14443-3 AMD2 14443-4 AMD2	2005				
Clarification of RFU handling 14443-3 AMD3 14443-4 AMD1	2003-09	2004-07	2004-10	2005-04	2005-08

Tableau 3 : Résumé des amendements du standard de base

6 WD : Working Draft
7 CD : Committee draft (première étape)
8 FCD final committee draft (seconde étape)
9 FDIS : Final draft International standard (troisième et dernière étape)
10 IS : International standard (publication)

	WD	CD	FCD	FDIS	IS
Logical card test methods 10373-6 AMD1	2002-02	2002-07 2002-10 2004-10	2003-07 2004-07	2005-04	2005-08
Improved RF test methods 10373-6 AMD2	2002-02	2002-07	2002-10	2003-03	2003-09
Logical reader test methods 10373-6 AMD3	2002-02	2003-07 2004-07	2003-11 2004-10	2005-04	2005-08
Additional RF test methods 10373-6 AMD4	2004-09	2004-10	2005-04	2005-10	2006-02
High bit rates test methods 10373-6 AMD5	2004-09	2004-10	2005-04	2005-10	2006-02
Very high bit rates test methods 10373-6 AMD6	2005				

Tableau 4 : Résumé des amendements concernant les méthodes de test

COMMUNICATIONS SANS FIL DE PROXIMITE

Perspectives Technologiques en RFID Intelligente

Par François VACHERAND,
CEA-LETI MINATEC

De nouvelles technologies sont en développement dans les laboratoires de R&D du CEA-LETI sur la thématique des systèmes d'identification et de traçabilité sans contact. Parmi celles qui émergeront à court/moyen terme, on peut citer actuellement :

- les interfaces air pour augmenter les débits des cartes à puces sans contact et « memory tokens » passifs,
- les antennes dites 3D permettant de lire une étiquette dans n'importe quelle position,
- les micro-capteurs téléalimentés,
- la gestion de l'énergie via la récupération de puissance disponible, la conversion et le stockage.,
- La protection des communications sans contact pour prévenir la fraude et protéger la vie privée.

Ces cinq avancées majeures sont les plus prometteuses pour l'évolution des performances et des fonctionnalités des micro-systèmes d'identification et de traçabilité sans contact industrialisables à court ou moyen terme. Elles permettent tout à la fois de proposer des systèmes autonomes performants et sécurisés tout en prenant en compte les facteurs sociétaux incontournables que sont la gestion de l'énergie et la protection des libertés individuelles.

La première avancée concerne l'augmentation des débits pour les systèmes sans contact de proximité dédiés à l'identification des personnes (carte à puce). L'objectif est de proposer un lien de communication numérique à débit de données nettement supérieur à ce qui se fait actuellement (106 kbps à 848 kbps) afin de pouvoir transférer rapidement des fichiers entre la carte et le lecteur. Les applications visées sont l'identification biométrique, le téléchargement d'applets Java ou de fichiers multimédia, et bien évidemment celles utilisant le standard NFC.

Pour cela, le LETI a développé une interface air spécifique très haut débit (VHDR) , compatible avec les produits déjà normalisés. La transmission sans contact développée permet de gagner un facteur 10 sur les débits actuels et possède une plage de fonctionnement de106 Kbps à 6,78 Mbps. La solution implémentée sur le composant téléalimenté et le lecteur associé *(figure 1)* repose sur une technique de modulation de phase multi-niveaux avec un étage de réception à haute sensibilité.

Un démonstrateur comprenant le lecteur très haut débit et un circuit intégré regroupant les fonctions d'émetteur/récepteur très haut débit et de téléalimentation a été validé à la vitesse de 6,78 Mbps. Des travaux sont en cours pour atteindre les 10 Mbps. Ce démonstrateur transmet des images de 2 Mo en 3 secondes. Une proposition d'extension de la norme actuelle (ISO 14443) est en cours de discussion à l'ISO.

Figure 1 : Prototype du composant intégré et du lecteur VHDR

La seconde avancée vise à faciliter le déploiement des étiquettes RFID. Elle a comme objectif de pouvoir lire de façon automatique les étiquettes dans n'importe quelle position tout en évitant l'encombrement des antennes tunnel ou portique. Pour résoudre ce problème, le LETI a développé une technique originale basée sur une association d'antennes planaires et d'émission de signaux qui combinent les champs électromagnétiques émis de façon à recréer des champs tournants en 3D *(figure 2)*.

L'avantage de ce dispositif est double : il occupe moins de place qu'une antenne tunnel ou portique et il laisse libres deux axes. Ainsi les objets étiquetés peuvent se déplacer sur un plan.

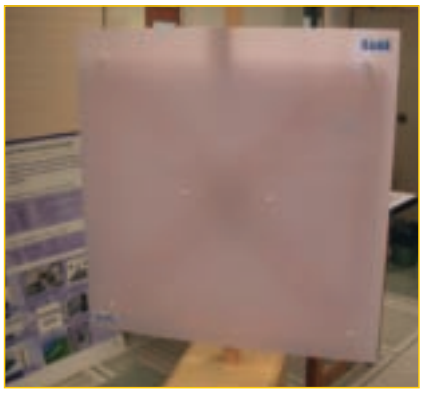


Figure 2 : Antenne plane générant un champ électromagnétique 3D.

La troisième avancée importante dans le domaine de la traçabilité est la possibilité de surveiller une grandeur physique telle que la température, la pression ou l'accélération. Les utilisations potentielles vont du contrôle alimentaire de la chaine du froid au suivi du colisage. L'arrivée de micro-capteurs performants, économiques et à très faible consommation permet d'envisager la réalisation de microsystèmes de traçabilité, actifs par nécessité, mais bon marché et à grande autonomie.

Les micro technologies, en particulier silicium, permettent aujourd'hui l'industrialisation en volume de ce type de composants. On dispose ainsi maintenant de micro-capteurs de type : capteurs de température, de pression, accéléromètres, gyromètres, magnétomètres *(figure 3)*. L'utilisation de ces micro-dispositifs peut se faire sous deux formes : soit l'acquisition directe et au vol par activation instantanée par un lecteur, soit par enregistrement continu du profil d'une grandeur physique pour contrôle temps réel ou a posteriori.

La quatrième avancée est le corollaire de la précédente. Le suivi continu d'une grandeur physique nécessite de disposer en permanence d'une source d'énergie électrique *(figure 4)*. Afin de diminuer les coûts de maintenance, il

Figure 3 : Exemple de micro-capteurs intégrés: pression, gyromètre et magnétomètre

est aussi primordial que ces microsystèmes soient autonomes. C'est pourquoi des travaux importants ont été conduits pour introduire trois fonctions liées à la gestion de l'énergie : la récupération d'énergie ambiante d'origine non électrique, la conversion en énergie électrique et le stockage *(figure 5)*.

La récupération d'énergie se fait sur une source d'énergie disponible dans l'environnement du microsystème : mécanique (vibrations), rayonnement (photovoltaïque) ou thermique. Une miniaturisation de l'élément sensible va permettre la capture de la puissance disponible directement dans la puce. Un convertisseur va fournir en sortie cette puissance sous forme électrique et une micro-batterie va stocker soit au niveau de la puce, soit au niveau du microsystème cette énergie ainsi récupérée.

L'objectif est de pouvoir alimenter en permanence certaines fonctions d'un circuit électronique telles que le contrôle de la sécurité des données sensibles ou l'acquisition de données capteurs entre deux passages devant un lecteur sans contact par exemple. Enfin, le LETI a aussi développé une électronique de contrôle de charge et de décharge ultra basse consommation afin d'optimiser au mieux l'énergie disponible.

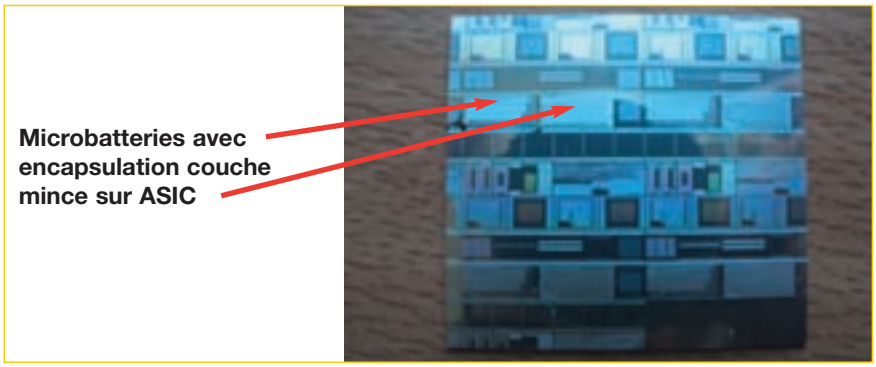


Figure 4 : Prototype de micro-batterie déposée sur tranche de silicium

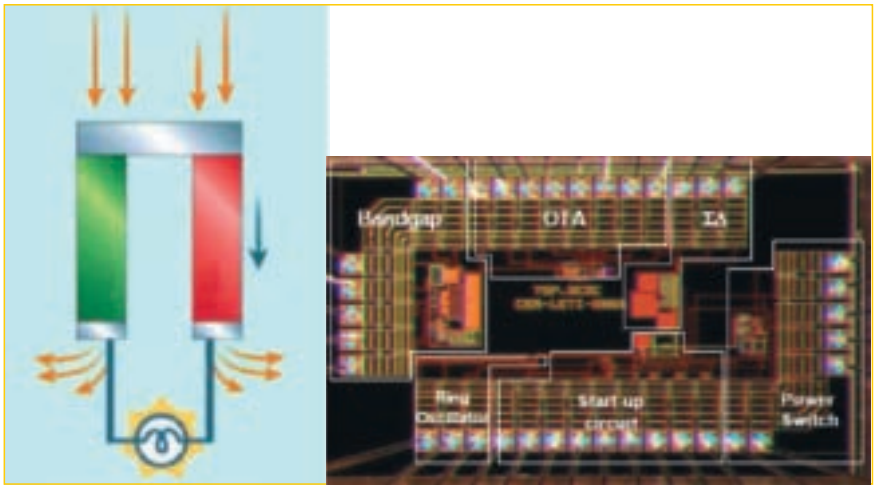


Figure 5 : Systèmes de récupération de l'énergie thermique et conversion DC/DC : principe et composant intégré

La dernière avancée, et non des moindre en ce qui concerne le déploiement à grande échelle, est le renforcement de la protection des libertés individuelles vis-à-vis de l'usage des nouveaux objets communicants tels que les cartes à puces sans contact, les étiquettes RFID ou les terminaux NFC. Il s'agit de protéger les données personnelles manipulées par ces objets. Dans ce cas on cherche à se prémunir de deux menaces : le vol de données personnelles à travers la communication sans contact et la traçabilité potentielle de l'utilisateur de l'objet via le protocole utilisé.

Dans ce domaine, le LETI a développé un système simple et économique permettant d'établir une communication sécurisée entre une carte ou une étiquette sans modification de ces dernières. Le principe repose sur un lecteur émettant un signal bruité quand le dispositif sans contact lui transmet des messages *(figure 6)*. Le lecteur étant le seul à connaitre le bruit qu'il émet, est donc le seul à pouvoir le soustraire par traitement et ainsi retrouver l'information transmise par le dispositif sans contact. Ainsi un lecteur espion ne peut pas récupérer les informations transmises par l'utilisateur de la carte ou du tag.

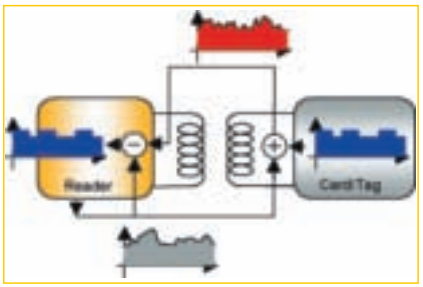


Figure 6 : Lecteur bruité : principe et prototype.

A propos du LETI

Le LETI est un laboratoire public de recherche appliquée appartenant au CEA et situé dans le pôle MINATEC de Grenoble. Ses deux objectifs fondamentaux sont l'innovation technologique et le transfert industriel. Au sein de ses 6 départements, plus de mille chercheurs étudient et développent de nouveaux procédés micro-électroniques ainsi que des systèmes électroniques innovants, basés sur ces micro-technologies émergentes. Les principaux domaines d'application sont le multimédia, les transmissions numériques, les objets communicants, la sécurité des composants électroniques et la santé.

COMMUNICATIONS SANS FIL DE PROXIMITE

NFC ET GLOBALPLATFORM

Envie de comprendre ?

Par Mathieu AMIEL - Consultant MONETECH

INTRODUCTION

Depuis quelques temps le NFC fait couler beaucoup d'encre et anime les médias autour des nouveaux services que cette technologie propose : paiement, ticketing, fidélité, contrôle d'accès … Tout ce petit monde qui remplit aujourd'hui portefeuille et sac à main pourrait se retrouver embarqué dans un seul téléphone mobile dans votre poche. Autant d'applications du quotidien qui pourraient bien changer beaucoup de nos habitudes de vie et de consommation.

Une course commence donc pour fournir à tout un chacun ces services. Mais différentes problématiques jusque là inconnues apparaissent. Certaines émanent de l'utilisateur : est-ce que je peux avoir confiance en une carte bancaire présente dans mon téléphone ? Quand je prends le bus, je paie avec ma carte bleue ou ma carte de transport ? Et si on me vole mon mobile ?

D'autres proviennent des différents fournisseurs de services : comment puis-je discuter avec une entreprise qui a une expérience métier très différente, avec ses propres contraintes si différentes des miennes ? Comment être sûr que la sécurité du service que je déploie n'est pas altérée par l'application de mon nouveau "voisin" ?

Le NFC bouscule un monde de frontières bien établies mais ce n'est pas pour cela qu'elles doivent s'effondrer. Il faut pouvoir accompagner les fournisseurs de services dans la redéfinition de ces frontières et dans la mise en place de processus communs répondant à ces problématiques.

VOUS AVEZ DIT NFC. MAIS QU'EST-CE QUE C'EST ?

Le NFC (Near Field Communication) est une évolution des diverses technologies « sans contact » appliquées à des équipements électroniques grand public. La technologie sans contact est déjà utilisée depuis plusieurs années dans notre quotidien notamment dans les transports en commun ou pour du contrôle d'accès.

Le NFC est une technologie permettant à n'importe quel appareil d'émettre un champ à courte portée (inférieure à 10 cm) pour échanger des informations.

Aujourd'hui, un des appareils phares pressenti pour embarquer la technologie NFC est le téléphone mobile.

L'intérêt est que l'utilisateur a toujours son téléphone mobile sur lui, et le taux de diffusion du téléphone mobile est un atout.

Technologiquement le téléphone mobile présente également l'avantage d'embarquer un élément sécurisé qui peut être soit la carte SIM déjà présente ou alors un élément sécurisé distinct et complémentaire. Les deux schémas d'architecture coexistent *(voir Figure 1 et Figure 2)*

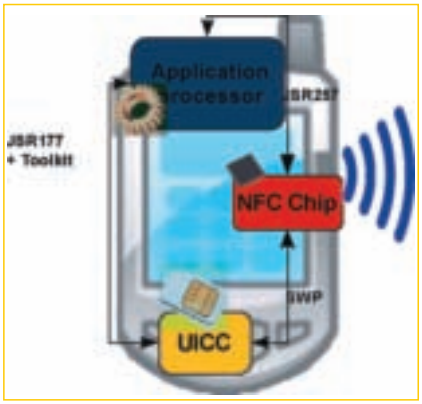


Figure 1 : Architecture SIM centric

Quelles sont les nouvelles problématiques ?

Les processus existant sur les cartes à puce apportent un niveau de sécurité approprié au contexte de chacun des fournisseurs de services, notamment dans le domaine de l'émission et de la remise de la carte au client.

Demain qu'en sera-t-il ?

Ces services doivent être installés dans l'élément sécurisé du téléphone qui est déjà en votre possession. Le but est donc d'utiliser des propriétés communicantes du téléphone pour les installer une fois le téléphone en service.

Il faut donc définir de nouveaux procédés de diffusion aux utilisateurs tout en respectant le niveau de sécurité attendu par chacun des fournisseurs.

CE QUI EXISTE : JAVACARD & GLOBALPLATFORM

Deux briques technologiques sont disponibles afin de répondre à ces problématiques : **JavaCard** et **Global Platfom**.

JavaCard tout d'abord …

Toutes ces problématiques ne sont pas entièrement nouvelles. Une standardisation était déjà nécessaire pour permettre à différents fournisseurs de services d'utiliser des cartes à puces provenant de différents fabricants de cartes.

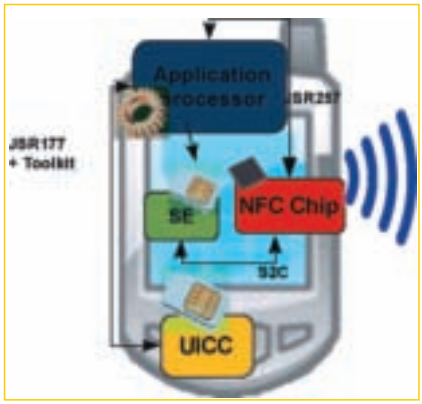


Figure 2 : Architecture avec Secure Element complémentaire

Tout d'abord, standardiser l'exécution et le langage de programmation des services sur la carte. A ce propos la technologie Java a déjà de l'avance puisque c'est déjà son ambition sur des plates-formes micro. SUN (aidé par le JavaCard Forum) s'est donc attaqué à l'embarqué et a fait de JavaCard un standard de développement incontournable sur carte à puce. On peut ainsi uniformiser les développements *(voir Figure 3)*.

Avec JavaCard, les applications développées deviennent interopérables, complètement indépendantes de la carte qui la porte.

… et GlobalPlatform

C'est aussi l'ambition de GlobalPlatform (GP) depuis bientôt 10 ans d'émettre des spécifications visant à uniformiser les développements et les cycles de vie des plates-formes de manière interopérable, fiable et flexible, pour des cartes multi applicatives et correspondant à plusieurs modèles économiques.

GP est un organisme de spécification international qui regroupe des industriels, des sociétés de service, des opérateurs comme Gemalto, Oberthur, Visa, MasterCard, France Telecom et bien d'autres. L'organisme s'est aussi ouvert aux sociétés de conseil comme Monetech.

Le schéma multi applicatif décrit dans les spécifications permet de faire cohabiter sur la même carte des applications bancaires, télécoms ou transports. Une application n'est plus forcément gravée dans le silicium de la carte lors de sa fabrication, mais peut être chargée et paramétrée a postériori, voire supprimée sans altérer le cycle de vie de la carte. Un émetteur de carte peut donc faire valoir une multitude de services et offrir de l'espace sur sa carte pour y intégrer des applications compatibles, correspondant aux normes JavaCard et GP.

Toutes ces fonctionnalités impliquent de nouveaux besoins de sécurité et c'est un point très important des spécifications : définir une architecture permettant la gestion sécurisée des applications et leur étanchéité les unes par rapport aux autres.

La carte va donc être partitionnée en plusieurs coffres-forts, qu'on appellera « Security Domains » (SD). Chaque coffre-fort contient sa propre combinaison pour être ouvert, qu'on veuille y mettre ou y enlever du contenu. Cette combinaison prend la forme d'un ensemble de trois clés cryptographiques que l'on nomme un « Keyset ». On peut alors attribuer un coffre-fort à chacun. Ainsi une banque aura les clés de son coffre, mais pas celle du coffre voisin concernant un agent de transport, ou pire, le coffre d'une banque concurrente. Les informations contenues sont garanties contre les regards indiscrets ou les utilisations frauduleuses.

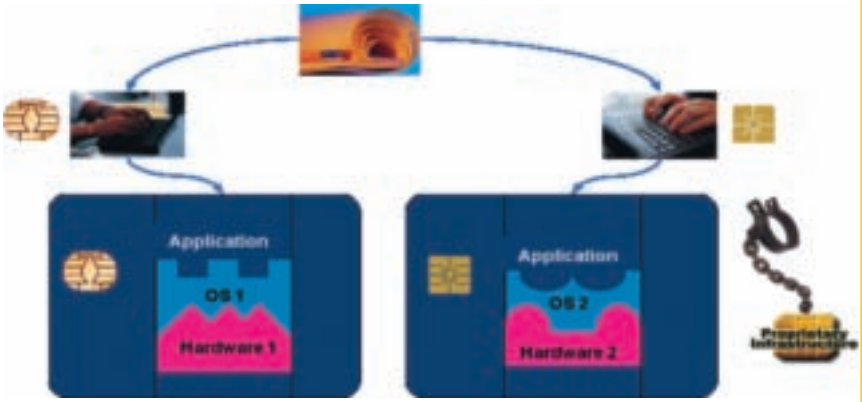


Figure 3 : Uniformisation des développements

L'émetteur de la carte est le seul à posséder un SD spécifique (Issuer Security Domain) qui permet de gérer le cycle de vie des applications de la carte (chargement, suppression, activation…) sans pour autant accéder à leurs données.

L'aspect critique de ce concept de coffre-fort est d'être sûr que la seule entité qui possède sa combinaison est son propriétaire ou un de ses partenaires de confiance. Cette problématique devient cruciale avec l'arrivée du NFC et la multiplication des acteurs dans ce nouvel écosystème.

Pour cela, GP définit des rôles, dont voici les plus importants :

- Propriétaire de l'application : définit et maintient les spécifications de l'application.
- Fournisseur d'applications : fournit les éléments nécessaires pour charger une application (code, données, clés, certificats, données de personnalisation). C'est lui qui propose des services au porteur de la carte.
- Gérant du SD : se charge de gérer les SD sur la carte.
- Autorité de contrôle : gère les échanges avec une éventuelle tierce partie dans le cadre des déploiements.
- Emetteur de la carte : c'est lui qui a la responsabilité de la carte GP. Il peut être la seule entité à pouvoir charger, installer, personnaliser ou associer à un nouveau SD une application. Mais il peut aussi déléguer ces fonctions à une tierce partie, comme le fournisseur d'application par exemple, avec l'aide du gérant de SD. Il fournit l'utilisateur final et est responsable de l'intégrité du processus d'émission de la carte. Il détermine un éventail d'applications pouvant fonctionner sur sa carte et gère les droits des applications qu'il autorise à s'installer sur sa carte.
- Utilisateur final / Porteur de carte : reçoit la carte en vue d'utilisation.
- Activateur de Carte : s'occupe de la pré-personnalisation, principalement des SD de l'émetteur et de l'autorité de contrôle, ainsi que de ceux des fournisseurs d'applications. Il va donc définir le niveau de sécurité de chacune de ces entités et préparer la carte à recevoir du contenu applicatif.
- Loader : charge les applications sur la carte et peut personnaliser les applications selon les directives de l'émetteur, du fournisseur de services tout en respectant les politiques de sécurité. Il a aussi la possibilité de charger des clés dans un SD.
- Fabricant de cartes : fabrique les cartes destinées à l'émetteur.
- Fabricant de puces : fabrique les wafers et est chargé de placer la partie statique de la carte (ROM).

Chaque rôle définit et implique un niveau de responsabilité. Tous les acteurs se retrouvent concernés et chacun sait à quoi se référer pour délimiter son rôle.

Installer les applications dans la carte

Prenons l'exemple d'une banque et d'un transporteur qui voudraient installer leurs applications sur une carte SIM émise par un opérateur télécom présente dans le mobile NFC d'un client *(voir Figure 4)*.

Sur ce schéma très simple on voit apparaitre les différents rôles :

- L'émetteur est dans le cas de notre exemple l'opérateur télécom. Détenteur des clefs de l'ISD, il peut

charger les applications bancaire et transport ainsi que les clefs dans les SD Banque et Transporteur et endosse à ce titre le rôle de loader.

- Les fournisseurs de service sont dans le cas de notre exemple la Banque et le Transporteur, ils sont les propriétaires de leur application ainsi que les gérants de leur SD dont les clefs leur ont été transmises par l'opérateur télécom. Ces dernières lui permettent d'établir un canal sécurisé avec son application détaillé dans le paragraphe suivant.

Sécuriser la communication avec les applications : le Secure Channel

Un Secure Channel est un canal sécurisé entre le fournisseur de service et son application indépendamment de l'environnement traversé qui peut être varié, ouvert, non sécurisé (Over The Air à travers les réseaux mobiles, Internet, …).

Pour ouvrir un Secure Channel il faut s'assurer de l'identité de chacune des deux entités (fournisseur de service d'un côté, son application dans la carte de l'autre), et offrir la capacité de rendre la communication confidentielle. Il faut donc que les deux entités partagent un secret : les clés du coffre.

Pour éviter que les clés aient à voyager, GP prévoit un protocole d'ouverture de session qui est basé sur :

- l'échange et le calcul de données aléatoires,
- l'utilisation de compteurs de transactions pour éviter que la même sécurité soit applicable plusieurs fois et qu'un tiers puisse ainsi rejouer l'authentification,
- les clés du SD auquel appartient l'application.

Le protocole le plus utilisé à l'heure actuelle est le Secure Channel Protocol 02 (SCP02). Il permet d'authentifier chacun des correspondants et de rendre les données confidentielles jusqu'à la carte, qui décryptera elle-même les messages *(voir Figure 5)*.

Reprenons le schéma précédent en y introduisant deux nouvelles hypothèses :

Les fournisseurs de service :

- ne veulent pas communiquer leurs clés à l'émetteur.

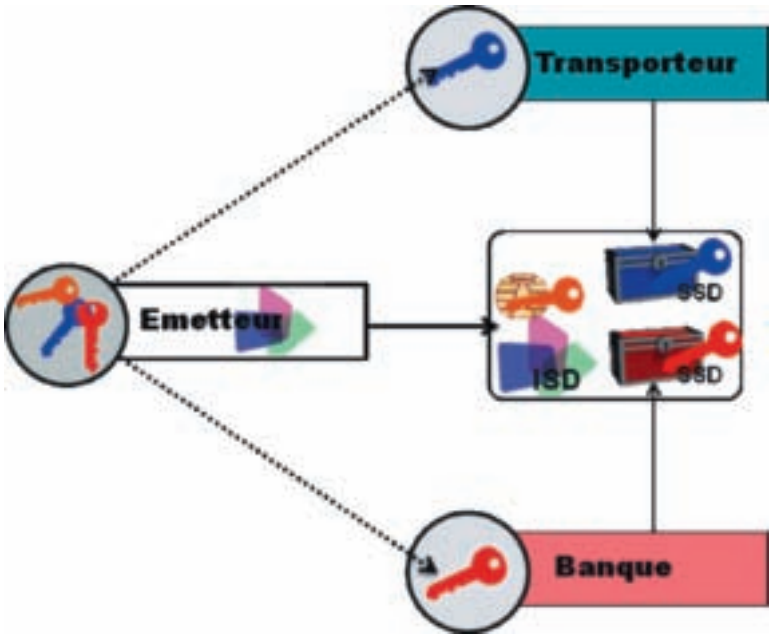


Figure 4 : Installation simple d'un service

- veulent utiliser SCP02 pour garantir la confidentialité de leurs données.

Les deux fournisseurs ont établi un lien sécurisé. Il n'est pas spécialement prévu que SCP02 passe par le réseau des opérateurs téléphoniques. Or c'est le canal qui va être utilisé pour parler avec la carte du porteur (chargement et évènements au cours du cycle de vie de l'application)

Il faut donc rajouter l'opérateur dans la cinématique de façon à gérer le service. Jusqu'ici les opérateurs téléphoniques et les fournisseurs de service sur carte (non SIM) n'utilisaient pas de structures ni de processus communs. GP permet donc de passer sur le réseau de l'opérateur sans modifier la sécurité *(voir Figure 6)*.

COMMENT GP REPOND IL AUX PROBLEMATIQUES DU NFC ?

Les fournisseurs de service n'ont d'une part pas l'habitude de cohabiter sur une même puce et d'autre part vont devoir charger et suivre leur service à distance.

Voilà en quoi le NFC apporte de nouvelles contraintes. Un fournisseur de service quel qu'il soit doit avoir le moyen d'administrer son service à distance en utilisant les canaux de communication du téléphone.

Grâce à GP chaque fournisseur de service dispose d'un espace qui lui est propre et qui réunit les critères de sécurité, sur la carte, mais aussi pendant le transport des informations en proposant des protocoles de cryptage, comme SCP02.

GP fournit également les outils nécessaires à la gestion à distance d'un service sur un élément sécurisé.

Ainsi un fournisseur de service va pouvoir :

Figure 5 : Secure Channel Protocol (SCP02)

- charger son service à distance,
- l'installer et le paramétrer,
- le personnaliser,
- bloquer / débloquer le service.

La carte se transforme en un minuscule disque dur pouvant accueillir des applications gérées à distance, paramétrables et effaçables de manière sécurisée, tout en s'affranchissant du mode de communication utilisé.

Ce qu'il faut pour permettre à votre mobile de devenir un jour votre porte monnaie, votre carte de bus … votre couteau suisse de tous les jours.

Les spécifications GlobalPlatform couvrent plus de cas d'utilisations, et divers modèles de déploiement.

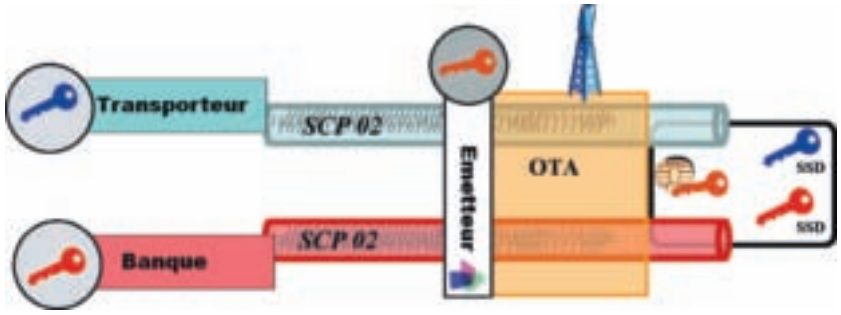


Figure 6 : Canal OTA sécurisé

Volontairement cet article n'en traite qu'une petite partie. Depuis plus de 5 ans Monetech accompagne ses clients dans la spécification et la réalisation de projets à base de GP.

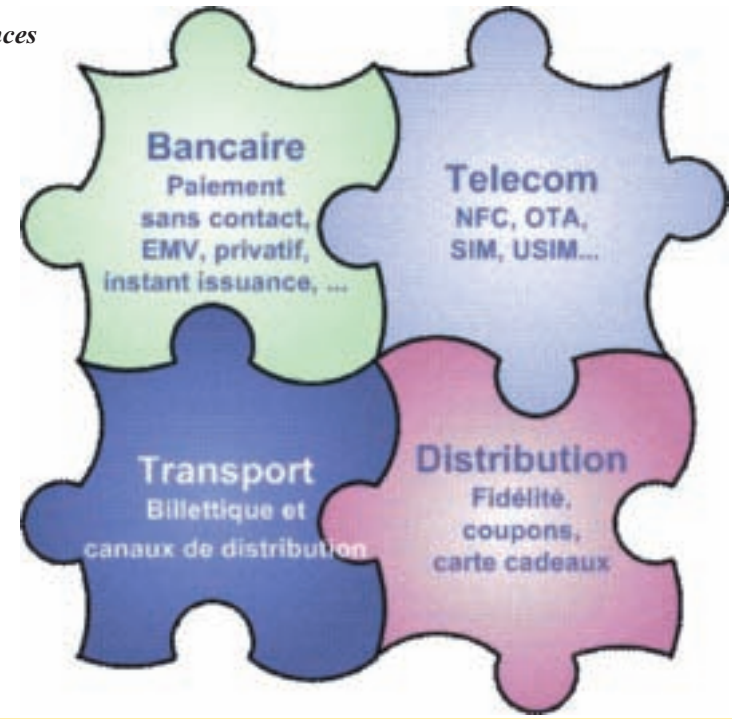
Pour plus de renseignements nous vous invitons à visiter notre site internet sur **http://www.monetech.fr** et le site officiel de GP, **http://www.globalplatform.org.**

MONETECH EN DEUX MOTS

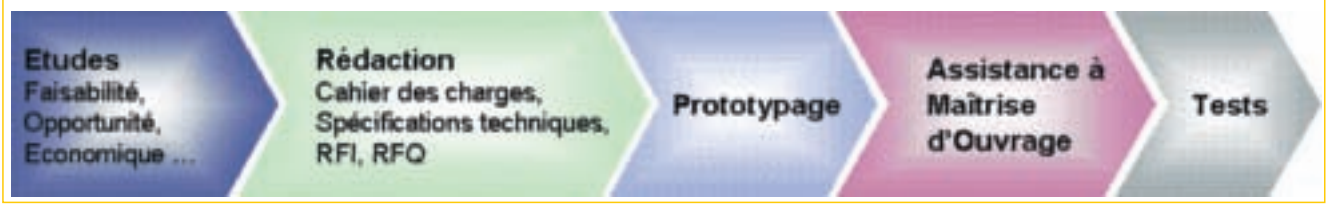
Nous sommes…

- un cabinet de conseil indépendant,
- spécialisé dans les nouvelles applications utilisant la carte à puce, le sans contact et le NFC,
- avec comme mission d'accompagner nos clients dans la réussite de leurs projets innovants.

Nos domaines de compétences



Nos missions



Mieux nous connaître ? www.monetech.fr

COMMUNICATIONS SANS FIL DE PROXIMITE

NFC : Communication en champ proche Les aspects normalisation

Par Yves THORIGNÉ, Expert à ORANGE LABS

La technologie NFC : principales caratéristiques

La technologie NFC (Near Field Communication) est issue du monde des cartes à mémoire sans contact. Celles-ci sont maintenant devenues familières pour le grand public, principalement par l'usage qui en est fait dans les transports en commun, comme par exemple la carte Navigo en région parisienne.

Le NFC s'en distingue par des caractéristiques techniques qui ont été ajoutées, et surtout par la nature du marché auquel elle s'adresse. En effet, le NFC va s'intégrer dans des équipements électroniques grands publics comme les téléphones mobiles, les appareils photos et les ordinateurs personnels. Le NFC présente donc les mêmes propriétés techniques que les cartes sans contact: les débits binaires sont de l'ordre de quelques centaines de Kbits/s, la distance de communication est inférieure à dix centimètres. Son usage est associé à un geste intuitif et rapide: on met son mobile à proximité d'une borne sans autre action demandée.

Dans les systèmes de cartes sans contact, l'élément portable est la carte, la borne (ou lecteur sans contact) est un élément fixe (comme ceux qui sont installés dans les équipements des transports en commun). Un équipement NFC répond à ces deux modes : carte et lecteur, et un troisième mode est aussi défini, appelé Peer to Peer qui est une association des deux autres modes (lecteur et carte).

Afin d'assurer son adoption par les acteurs du marché, le NFC a entraîné une grande variété d'activités de normalisation. Le NFC a d'abord été spécifié au sien de l'ECMA, puis les travaux de normalisation se déroulent essentiellement au NFC forum, à l'ETSI, à l'ISO et à GlobalPlatform. En complément, d'autres organismes participent à ces actions de normalisation. Ainsi, la GSMA (GSM Association) au travers de White papers, donne des recommandations techniques qui servent ensuite de guide pour l'édition de standards.

Les couches protocolaires du NFC sont représentées *(figure 1)*.

Description des couches protocolaires

La partie radiofréquence est composée des normes ISO/IEC 18092 et 14443 *(voir diagramme de la figure 2)*.

La norme ISO 18092 est composée de la norme ISO 14443 type A (pour les parties 2 et 3) et du système Felica (pour les parties radiofréquence et initialisation du protocole). L'ISO 18092 définit en complément le mode actif, qui permet à chaque équipement d'être alternativement lecteur puis carte, l'autre équipement étant alors dans le rôle inverse (lecteur / carte). Le but est de pouvoir augmenter la distance de communication.

Au niveau fonctionnel, le protocole d'échanges de données de la norme ISO 18092 est identique à la partie correspondante de la norme ISO 14443. Le comité ISO/JTC1/SC6 a la responsabilité de l'ISO 18092. Initialement, cette norme a été spécifiée par l'ECMA, elle est devenue norme ISO par une procédure d'approbation accélérée dite "fast-track". La référence ECMA est NFCIP-1.

Des travaux d'harmonisation entre les normes NFC et les normes ISO 14443 sont en cours. Il s'agit d'une part, de définir les conditions d'interopérabilité au niveau radiofréquence et d'autre part, de réaliser l'harmonisation au niveau des protocoles. Ainsi, il est envisagé de permettre le mode Peer to Peer au-dessus de la norme ISO 14443 (Pour l'instant ceci n'est défini qu'au-dessus de l'ISO 18092).

Sur la figure 2, sont représentées les normes ISO 18092 et ISO 14443. Elles sont indiquées dans la figure 1 par la couche intitulée "couche radiofréquence ISO 18092, 14443 type A & B".

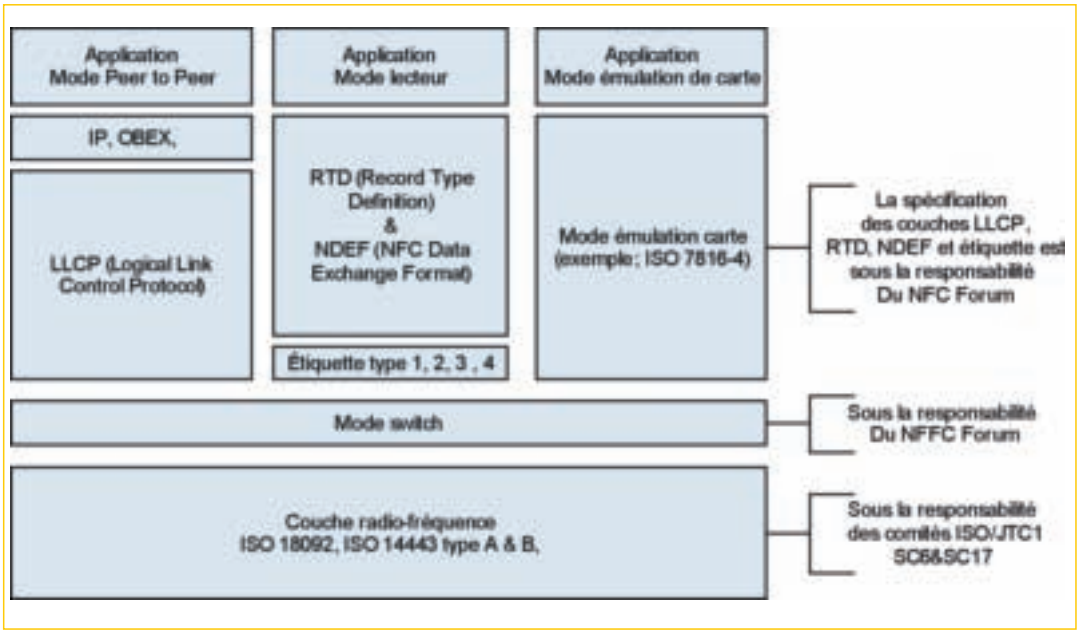


Figure 1: Couches protocolaires du NFC

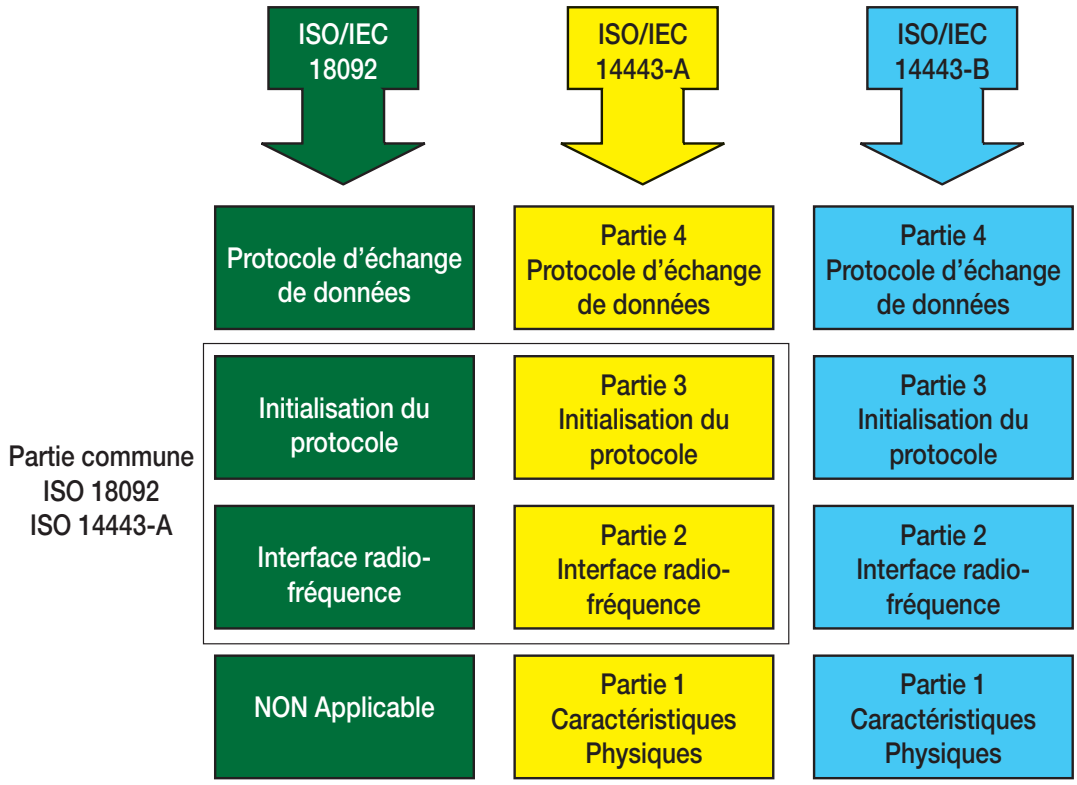


Figure 2 : Couches protocolaires des normes ISO 18092 et ISO 14443

La correspondance entre les spécifications ECMA et les standards ISO est représentée sur la *figure 3* :

La couche mode switch *(voir figure 1)* permet la gestion des différentes technologies radiofréquences ainsi que la gestion des deux modes lecteur et carte (le mode Peer to Peer est l'association de ces deux modes et n'a donc pas d'incidence sur cette couche). En mode lecteur, l'équipement NFC va émettre un signal radiofréquence dans chacune des trois technologies (par exemple suivant la séquence suivante : ISO 14443 type A puis ISO 14443 type B puis Felica). De même en mode carte, l'équipement va pouvoir détecter l'une des trois technologies.

La couche placée au-dessus du mode switch dépend du mode de fonctionnement (Peer to Peer, lecteur ou carte). Pour le mode Peer to Peer, une couche liaison de données (OSI couche 2) est définie. Elle permet en particulier de rendre symétrique la communication car les normes ISO 18092 et 14443 sont de type maître-esclave, seul le maître peut émettre des données. Pour le mode lecteur, quatre types d'équipements pouvant être lus sont définis: il s'agit des étiquettes types 1 à 4. Un protocole de communication a été spécifié afin d'échanger d'une façon simple les données: il s'agit des spécifications NDEF et RTD. La lecture d'une étiquette se limite à lire un message contenu dans l'étiquette. La définition du format de ce message permet l'interopérabilité entre les équipements NFC en mode lecteur et les étiquettes compatibles NFC Forum. Les applications sont de différentes natures, la plus prometteuse étant le smart poster qui permet par exemple d'accéder à un site Internet à partir d'une URL contenue dans l'étiquette. Pour le mode émulation de carte, la couche protocolaire dépend de l'application placée au-dessus. Elle n'est pas spécifiée par le NFC Forum. Cette couche est soit conforme au standard ISO 7816-4 (commun avec les cartes à mémoire à contact), soit propriétaire (comme le protocole de communication des cartes Mifare, celles-ci sont conformes à la norme ISO 14443 partie 2 et 3, mais pas partie 4).

Implémentation de la technologie NFC dans les téléphones mobiles avec la carte UICC (carte SIM).

Les applications liées au NFC appartiennent pour la majeure partie au domaine des transactions électroniques comme le paiement ou la télé-billettique. Ce type d'application requiert un élément de sécurité basé sur un composant carte à micro-circuit. Le téléphone mobile contient un tel dispositif: la carte SIM. L'implémentation du NFC dans les téléphones mobiles contient trois éléments : l'antenne, le NFC controller (noté NFC dans le schéma représenté sur la *figure 4*) et la carte SIM.

Le comité ETSI/SCP (Smart Card Platform) a défini deux normes pour l'interface NFC Controller et la carte SIM. Il s'agit du TS 102 613 et du TS 102 622. Dans l'architecture retenue, la couche radiofréquence ainsi que les couches protocolaires des normes ISO 18092 et ISO 14443 sont intégrées dans le NFC controller (couches protocolaires représentées *figure 2*). Les couches de plus haut niveau sont implantées dans la carte SIM (cas de la couche ISO 7816-4). Pour la mise en œuvre de l'interface entre le NFC Controller et la carte SIM, le principe retenu est basé sur une communication avec une seule connexion, qui est bidirectionnelle full duplex. TS 102 613 spécifie l'interface physique et protocolaire de bas-niveau appelée Single

Wire Protocol (SWP). Afin d'assurer une communication full duplex sur un seul fil, un principe original a été choisi: le maître (NFC Controller) émet les données par un signal en tension alors que l'esclave (Carte SIM) émet les données par un signal en courant, ce qui permet ainsi de pouvoir échanger des données de part et d'autre simultanément. TS 102 622 est une spécification de plus haut niveau pouvant d'ailleurs s'implanter sur une autre liaison de données que le SWP. Elle est constituée de deux parties: un noyau et un ensemble de services propres au NFC. Le noyau est un protocole qui permet d'ouvrir plusieurs connexions logiques simultanément, et d'intégrer aussi une fonction SAR (Segments and Reassembly) pour pouvoir contrôler le début et la fin de message. La seconde partie est spécifique au NFC, elle permet de transporter les messages relatifs au NFC, pour le support des trois modes fonctionnels: Peer to Peer, lecteur et émulation de carte. Ce comité travaille à la définition d'une API (Applications Programming Interface) afin de permettre aux fournisseurs d'applications de pouvoir développer leurs logiciels d'une façon interopérable (donc capables de fonctionner sur toutes les cartes SIM). GlobalPlatform prend en charge les aspects téléchargement et installation des applications dans la carte SIM.

La GSMA, qui regroupe principalement les opérateurs mobiles, a publié plusieurs white papers donnant des directives pour la technologie NFC. En particulier, le document "Mobile NFC Technical Guidelines" a décrit un ensemble de recommandations qui ont facilité l'émergence de consensus entre les différents acteurs de la normalisation.

Les activités de normalisation du NFC sont réparties entre plusieurs organismes. Des actions de coordination entre ces entités ainsi que la volonté affichée des acteurs du secteur ont permis d'élaborer un ensemble cohérent et complet de normes et de spécifications. Les résultats obtenus facilitent l'adoption de cette technologie par le marché, avec en premier lieu celui des téléphones mobiles.

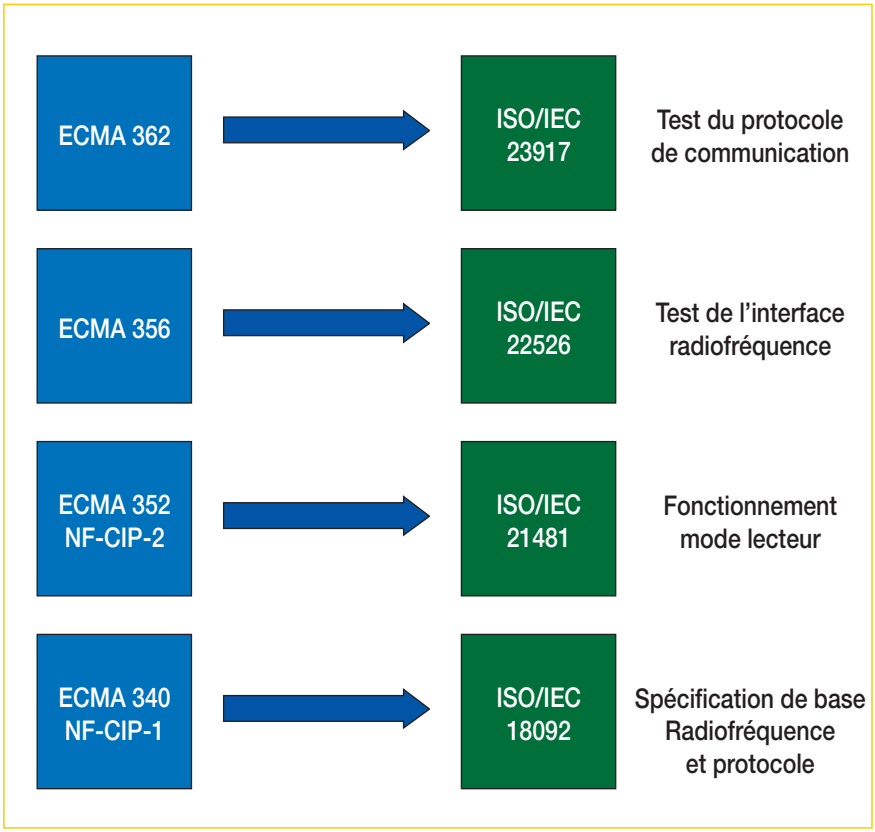


Figure 3 : Correspondance entre les spécifications ECMA et les normes ISO

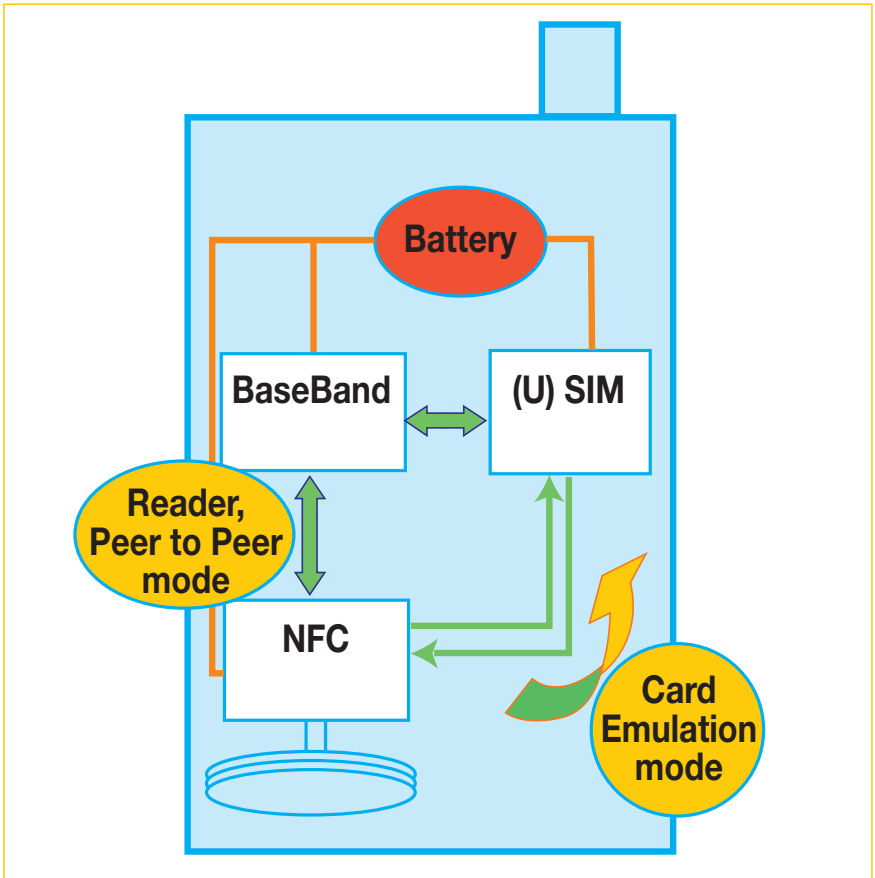


Figure 4 : Architecture NFC d'un téléphone mobile

NFC : Certification fonctionnelle

Par Eric Nizard, Directeur de LIC, Président d'EESTEL

NFC est une technologie de communication radio de proximité à 13,56 MHz qui, d'une part fédère plusieurs autres technologies pré-existantes dites "legacy" ayant chacune pour origine un industriel particulier (Philips-NXP, Sony, Infineon…), d'autre part propose ses propres protocoles et formats d'échange.

Cette multiplicité technique et cette multiple paternité rendent la normalisation de NFC particulièrement complexe.

Au moins cinq instances de normalisation et de standardisation sont actives :

- l'ISO IEC,
- le NFC Forum,
- l'ECMA,
- l'ETSI,
- la GSM Alliance.

La normalisation ISO/IEC

C'est la seule normalisation officielle de NFC.

Elle s'applique à la technologie : radio, physique, logique.

Le principal initiateur a été Philips à partir de 2004.

La norme ISO/IEC 18092 spécifie NFCIP-1 pour l'interface de Proximité (quelques centimètres)

Elle redéfinit dans le contexte NFC les normes ISO 14443 et JIS6319-4 (Felica).

Elle propose un nouveau mode de communication active avec une double génération de champ magnétique, à chaque extrémité.

Elle introduit un nouveau protocole de transmission NFC appelé Peer2Peer.

Mais elle ne définit pas la compatibilité avec la norme ISO/IEC 14443-4.

La norme ISO/IEC 21481 spécifie NFCIP-2 pour les interfaces de proximité et de "vicinité" (quelques dizaines de centimètres), cette dernière étant héritée de la norme ISO 15693.

La spécification est incomplète et une mise en œuvre strictement conforme n'en garantit pas pour autant une interopérabilité totale.

S'agissant des méthodes de tests, l'ISO a produit deux normes de haut niveau, c'est-à-dire non directement exploitables :

- ISO/IEC 22536 (NFCIP-1 RF interface),
- ISO/IEC 23917 (NFCIP-1 Protocol).

Un complément d'ingénierie appropriée à chaque cas d'application est nécessaire pour aboutir à un service de tests complet.

La standardisation du NFC Forum

Le Forum NFC qui regroupe les principaux acteurs industriels de ces technologies produit une normalisation appliquée et dont l'importance est croissante depuis 2 ou 3 ans.

Il est né peu après la publication des normes ISO/IEC précédemment citées, avec comme objectif une interopérabilité applicative.

Les premiers standards NFC Forum sont sortis en 2007.

L'ECMA

Le Programme de travail NFC de l'ECMA traite des thèmes techniques suivants :

- les communications sans fil de proximité (à 13,56 MHz) pour interconnecter périphériques et ordinateurs (famille technologique RFID),
- les normes ECMA-340, NFCIP-1, 2002, l'interface NFC et le Protocole (ISO/IEC 18092) qui couvre l'ISO 14443-4 et Felica,
- l'ECMA-352, NFCIP-2, 2003, pour relier NFCIP-1, 14443-B et 15693,
- l'ECMA-356, 2004, NFCIP-1 - pour les méthodes de tests relatives à l'interface radio,
- l'ECMA-362, 2004, NFCIP-1 - pour les méthodes de tests de protocole.

L'ECMA travaille actuellement à améliorer :

- la sécurité,
- les débits,
- l'interopérabilité,
- le contrôle de la fourniture d'énergie,
- la couche "liaison de données".

L'ETSI

L'ETSI standardise NFC comme une technologie télécom.

Elle a produit des normes connexes à la norme NFC :

- HCI (Host Controller Interface) - ETSI TS 102-622 v7 (Février 2008). Cette interface assure la communication entre une carte SIM et un hôte externe pouvant être une carte ou un serveur applicatif ; il couvre les couches logiques 3 et 4 et utilise la technologie NFC
- SWP (Single Wire Protocol) - ETSI TS 102 613 Release 7 (Oct. 2007). Ce protocole assure la communication entre une carte SIM et le contrôleur NFC à l'intérieur du téléphone

Quelle est la typologie des acteurs de NFC ?

- ***des organismes de normalisation (ou de standardisation)*** :
  - ETSI
  - NFC Forum

- GSMA Association
- ECMA

• ***des fabricants de puces :***

- NXP pour SONY …,
- Inside Contactless (plutôt –B),
- Innovision (Tags NFC de type 1),
- ST,
- TI,
- ATMEL …

• ***des fabricants de téléphones mobiles :***

- Nokia,
- Sony.

• ***des Opérateurs de services :***

- Opérateurs de téléphonie mobile,
- Municipalités (Oulu en Finlande, Caen, …),
- Opérateurs de Paiement (Master Card, Visa…).

Quant à la certification, c'est une condition nécessaire à la réussite d'une technologie sur le terrain.

Pour NFC, la certification doit s'appuyer sur la constitution d'un schéma de certification sous la responsabilité d'une autorité de certification qui délivre des labels aux fournisseurs de produits, garants de l'interopérabilité des terminaux NFC et de leur non dégradation sur le terrain *(figure 1 et figure 2)*.

Pourquoi la certification est-elle nécessaire ?

La certification est la condition du succès durable d'une technologie sur le terrain.

Elle est source de confiance pour le marché : les industriels, les opérateurs, les autorités de normalisation …

Son efficacité n'est valable qu'à l'intérieur d'un même écosystème.

Pourquoi la certification NFC est-elle un casse-tête ?

Il y a, de fait, plusieurs autorités de normalisation ou de standardisation.

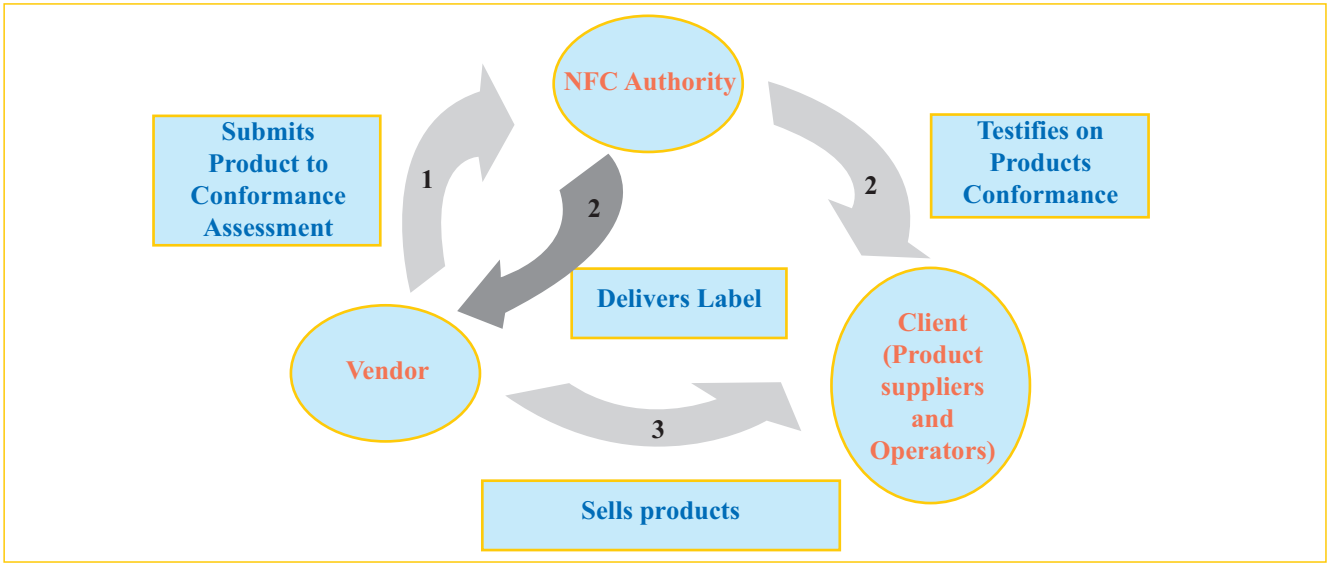


Figure 1 : Acteurs et rôles dans la certification

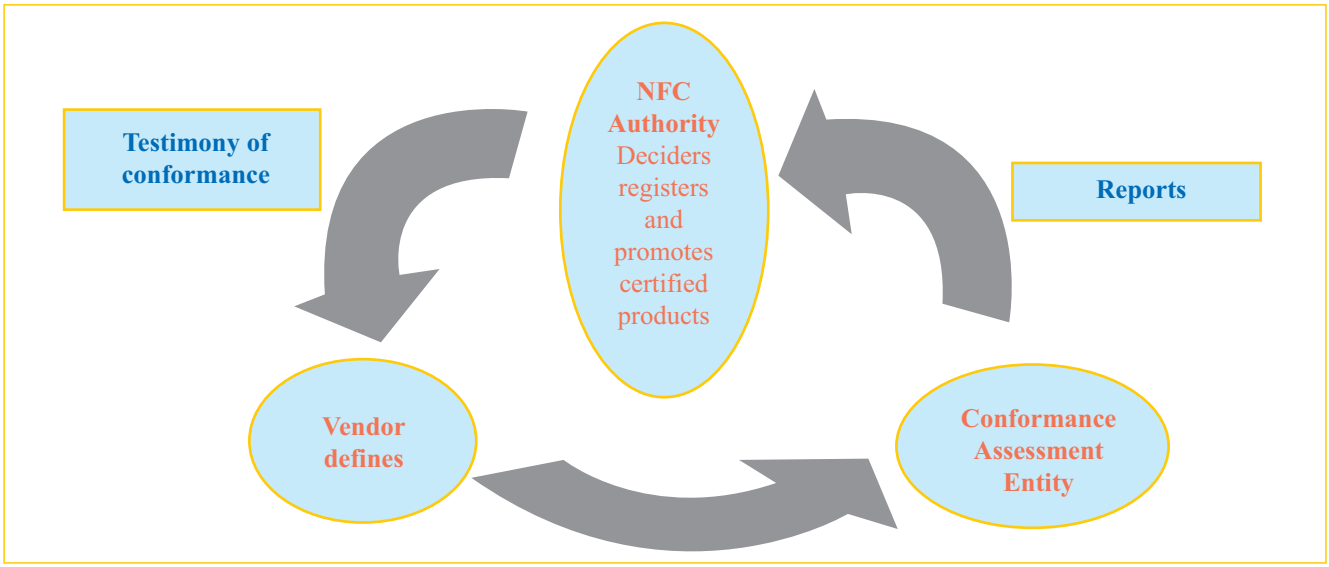


Figure 2 : Documents de certification échangés

Cette technologie s'adresse à des marchés différents (Télécommunications, paiement, transports, marketing de terrain).

De plus les "time to market" sont différents de même que les rythmes d'innovation selon les marchés.

Les durées des cycles de vies des produits sont différentes :

- pour les matériels,
- pour les logiciels de communication (et les middlewares en général),
- pour les applicatifs.

Les conséquences de problèmes d'interopérabilité n'ont pas le même degré de criticité selon les marchés (paiement vs télécommunications).

Qu'est-ce qui pourrait fonctionner ?

Pour que les activités de certification de l'écosystème puissent fonctionner, il convient d'avoir une approche dissociée des produits.

Pour les parties à cycle de vie long et ayant des enjeux forts (exemple : monétique) :

- définir des îlots applicatifs et les faire contrôler par les Opérateurs des services qui les utilisent,
- viser à réutiliser les produits en fonction des différents facteurs de forme ("form factors"),
- bâtir des schémas de certification consistants.

Pour les parties à cycle de vie plus court (exemple : télécommunications) :

- alléger la certification pour favoriser l'innovation

Tests fonctionnels NFC

Pour une technologie de communication de proximité telle que NFC, au-delà des tests purement électriques, il est nécessaire de mettre en œuvre des tests fonctionnels et de protocoles, toujours pour accroître la confiance.

Les tests fonctionnels doivent garantir que :

- les équipements sont interopérables,
- aucun équipement, aucune carte à puce ne sera endommagé sur le terrain,
- la gestion des collisions sera efficace par rapport à l'application ciblée.

Un schéma de tests fonctionnels comprendra des tests radio, des tests de protocoles et des tests applicatifs.

Il se composera, conformément à la norme ISO 9646, de tests abstraits, de méthodes de tests, d'un outillage de tests (constitué d'un moteur et de scripts). En fonction du volume de certifications visé, ces tests pourront être opérés par des laboratoires de tests accrédités et pourront être complétés par des audits permettant de contrôler le fonctionnement des études et de la production des industriels.

S'appliquant spécifiquement à la technologie NFC, la difficulté en la matière est double :

- d'une part, la combinatoire technique de configuration d'un terminal NFC se décline en combinatoire de tests,
- d'autre part, les rythmes d'innovation entre l'industrie de la téléphonie mobile et celle du paiement électronique sont totalement différents et les schémas de tests doivent en tenir compte.

A propos de l'informatique communicante (LIC)

LIC est une société de conseil et d'ingénierie en systèmes sécurisés de transactions électroniques :

- carte à puce,
- EMV,
- carte sans contact,
- RFID – NFC,
- Certification.

L'activité de LIC se situe au confluent de la stratégie technique, des projets et de la qualité :

- conseil – études – accompagnement,
- architecture,
- expertise,
- ingénierie de Certification - qualité,
- transfert de technologie - formation.

En matière d'ingénierie de certification, LIC couvre les activités suivantes :

- études de certification,
- validation de spécifications (contribution à la mise à jour des spécifications de référence permettant une meilleure qualité et testabilité de ces spécifications),
- méthodologie de tests,
- tests de certification : ISO 7816, EMV – EMV CL, ISO 14443, NFC,
  - spécifications de tests de conformité (jeux de tests) au standard considéré,
  - spécifications de tests d'interopérabilité,
  - spécifications de tests de performance.
- conception de l'architecture du banc de tests,
- choix, pilotage, contrôle et accompagnement des industriels développant des outils de certification,
- pilotage et contrôle de la mise en œuvre de qualification des outils de tests,
- animation technique de comités de certification,
- pilotage, contrôle et accompagnement des laboratoires de tests dans la mise en œuvre de leurs outils et méthodes,
- expertise de résultats d'homologation de type à partir des rapports de tests et des traces obtenus des outils de test.

Enfin, Eric Nizard, Directeur de LIC, est président d'EESTEL (Experts Européens des Systèmes de Transactions Electroniques) et vice-président du GIXEL (Groupement des industries électroniques).

I-TRACING
La Traçabilité Intelligente

Sécurité des paiements NFC

Par Laurent BESSET, I-TRACING

A l'heure où beaucoup s'accordent sur le fort développement à moyen terme du commerce mobile et où un consensus technologique semble s'installer autour des technologies sans contact, NFC en tête, utilisateurs et experts s'interrogent légitimement sur la sécurité de ce type de paiement.

Beaucoup d'autres questions sur le futur du paiement sans contact restent bien sûr sans réponse (business model à définir entre Banques et MNO (Mobile Network Operators), bataille autour de l'emplacement de l'application de paiement entre MNO et constructeurs, vitesse de renouvellement du parc d'équipements, etc.), mais le dernier obstacle à son adoption par le grand public, comme à celle de tout service financier, sera celui de la confiance.

Le paiement NFC, comment ça marche ?

En dépit de possibles variations, les processus de paiement NFC restent relativement génériques :

- Le client dispose d'un mobile « équipé NFC » et contenant une application de paiement (carte bancaire ou/et porte-monnaie électronique), le marchand possède un terminal de paiement « équipé NFC »,
- Au moment de régler un achat, le client passe son mobile à proximité du terminal qui établit une communication radiofréquence avec le mobile et lit les informations fournies par l'application (identifiants de compte, plafonds, etc.),
- La transaction peut faire l'objet d'une demande de confirmation et d'une authentification du client sur son mobile,
- Le terminal de paiement du marchand communique si nécessaire avec les réseaux bancaires (l'autorisation de transaction pouvant être donnée directement par l'application de paiement pour les plus petits montants).

Quelles failles de sécurité pour les paiements NFC ?

En toute logique, les failles de sécurité potentielles d'un paiement NFC sont à la convergence de failles déjà connues pour les paiements par carte bancaire « avec contact », et d'autres, propres aux environnements sans contact en général et à la technologie NFC en particulier :

- vol du téléphone mobile, i.e. du moyen de paiement,
- destruction de l'application de paiement, i.e. du moyen de paiement,
- sécurité de l'application de paiement et de ses données,
- déni de service,
- interception et manipulation des données confidentielles échangées lors d'une transaction,
- attaque-relais (man-in-the-middle).

Un niveau de risque réel limité… pour l'instant

Concernant les failles analogues à celles du paiement « avec contact » que sont le vol et la destruction du moyen de paiement, ainsi que la sécurité de l'application de paiement, force est de constater que le paiement NFC peut difficilement être jugé plus vulnérable :

- authentification complémentaire sur la SIM (ou tout autre SmartCard) avant d'accéder à l'authentification de paiement,
- possibilité de désactiver à distance la ou les applications du téléphone grâce aux plates-formes OTA des opérateurs (ou d'un tiers de confiance),
- portage de la norme EMV aux cartes sans contact assurant un niveau de sécurité applicatif au moins équivalent aux cartes avec contact.

Quant aux attaques propres à la communication NFC entre le téléphone et le terminal de paiement, hors le déni de service, elles restent difficiles et souvent plus théoriques que pratiques :

- complexité et limites de manipulation liées aux schémas de modulation de fréquence et aux codages employés,
- possibilité pour tout équipement actif NFC de scanner le champ magnétique durant la transmission afin de détecter les attaques et, le cas échéant, mettre fin à la transmission,
- sécurisation du flux en amont, au niveau de l'application EMV (authentification des équipements et autorisation des transactions à base de certificats et de clés asymétriques).

La sécurité ne peut et ne doit donc pas être considérée aujourd'hui comme un obstacle réel à l'adoption et à la diffusion du paiement NFC. Cela ne signifie pas pour autant que la menace n'existe pas et que le sujet doit être laissé au bord du chemin.

En effet, la plupart des normes et protocoles sous-jacents étant très récents ou encore à l'étude, il est difficile de préjuger de la manière dont ils seront implémentés. Or la pratique montre régulièrement que les failles de sécurité proviennent bien plus souvent d'un défaut d'implémentation technologique que d'un défaut de la technologie elle-même.

Il est également primordial de ne pas sous-estimer l'attrait croissant que constitueront ces nouveaux flux financiers, attrait qui ne manquera pas d'augmenter les moyens consacrés au piratage et donc la probabilité de trouver de nouvelles failles de sécurité.

COMMUNICATIONS SANS FIL DE PROXIMITÉ

MobiNear
Discover the Digital World around you

Les technologies de communication sans-fil de proximité (Bluetooth, WiFi, NFC & BlueNFC)

par Christian CHABRERIE, PDG - Fondateur de MOBINEAR

La société MobiNear est spécialisée dans les communications de proximité autour du mobile (typiquement entre un mobile et une borne interactive en magasin). Trois types de technologies de communication sans fils de proximité sont utilisés :

- Bluetooth,
- WiFi,
- NFC (i.e. "Near Field Communications" en anglais).

MobiNear a développé une technologie brevetée appelée BlueNFC qui permet de proposer des applications de type NFC avec des terminaux Bluetooth standards (près de 80 % du parc en France).

BlueNFC permet des applications de type "NFC-like" avec des mobiles Bluetooth standards.

Marché mondial des technologies Sans-Fil

Avec 53 % du parc mondial des Mobiles (2007), Bluetooth est devenue la 2ème technologie sans-fil après le GSM.

La Figure 1 illustre l'adoption des principales technologies sans-fil au niveau mondial. On constate que le GSM est de loin la première technologie déployée (avec près de 4 milliards d'abonnés). Le Bluetooth vient en deuxième position et équipe déjà (i.e. depuis 2007) plus de la moitié des mobiles (au niveau mondial). De plus, la croissance continue puisqu'aujourd'hui, en Europe occidentale, la technologie Bluetooth est présente dans plus de 80 % des mobiles vendus. Enfin le WiFi est principalement utilisé pour les applications de type ordina-

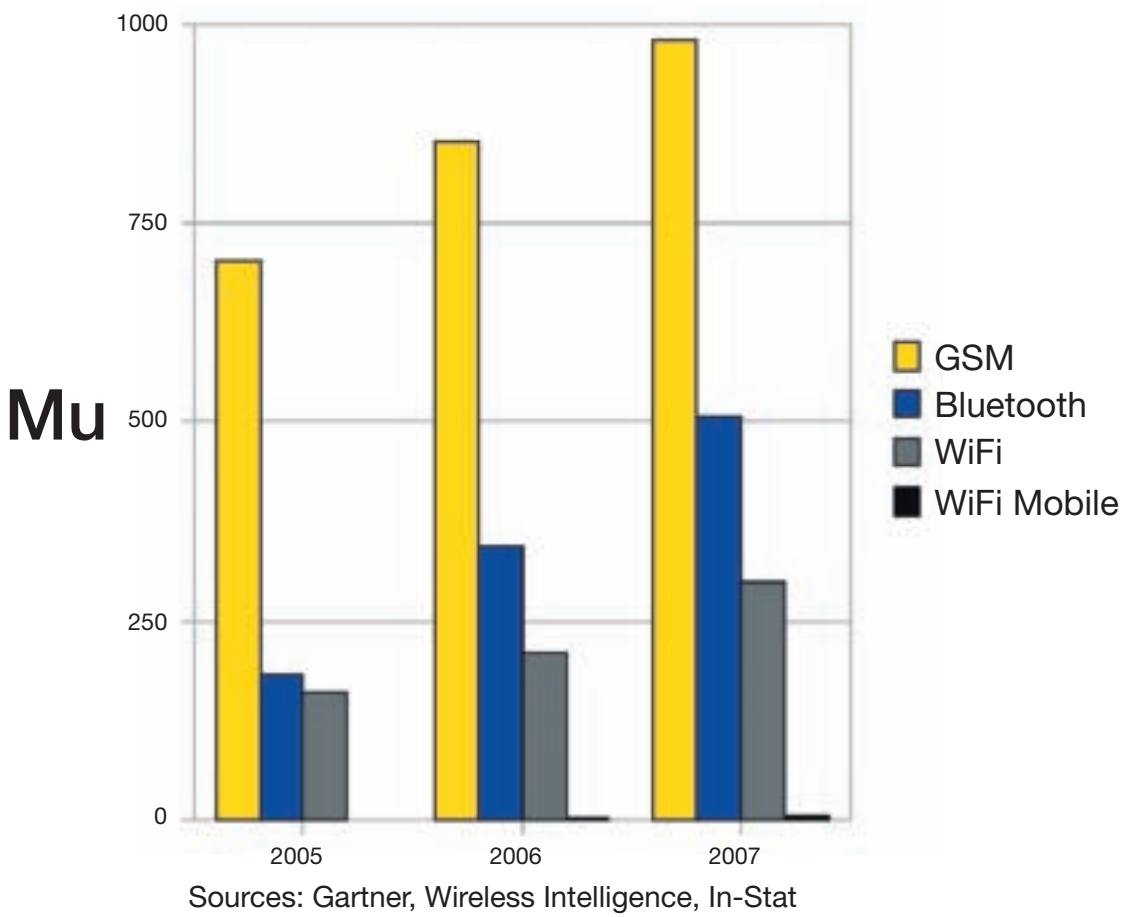


Figure 1 : Adoption des technologies sans-fil
(livraisons annuelles mondiales de circuits intégrés par types de technologies).

teur portable. Au niveau mondial, le WiFi dans les téléphones mobiles représente moins de 5 % du parc. Les bornes MobiNear sont toutes compatibles Bluetooth & WiFi.

Les Technologies de communications mobiles de proximité

La Figure 2 illustre les technologies de communications mobiles hors Voix, Data & SMS.

Le Bluetooth est majoritairement représenté avec plus de 50 % du parc installé mondial (53 % en 2008, Source Gartner), et plus de 80 % des ventes en Europe occidentale. Le taux d'équipement augmente encore et devrait atteindre plus de 85 % du parc mondial en 2011 (Source Gartner). Le plus fort taux d'équipement mondial se trouve en Espagne, notamment à cause de la législation locale qui impose un kit main libre pour passer des appels en voiture. Le Bluetooth n'est pas uniformément réparti sur la planète. A l'origine c'était un nom de code entre Nokia et Ericsson. C'est donc en Europe qu'il est logiquement le plus présent dans les terminaux mobiles. En Asie, la Chine et la Corée du Sud sont les zones à plus forte densité de mobiles Bluetooth, le Japon représentant moins de 5 % du parc mondial. Les Etats-Unis représentent environ 20 % du parc mondial. Ce faible taux de pénétration devrait rapidement connaître une forte croissance notamment sous la pression légale de certains Etats qui devraient rendre les car-kits obligatoires. La MobiNear Box est compatible avec tous les mobiles Bluetooth.

Le Flashcode est un code-barre 2D (différent des QR-Codes japonais). Il est basé sur une application installée sur les mobiles qui, à partir d'une image d'un code, renvoie typiquement vers des liens (i.e. URL) internet mobile. Il est à noter que, en France, environ 10 % des utilisateurs de mobiles sont mobinautes (c'est-à-dire qu'ils se sont connectés au moins une fois dans le dernier mois).

Le WiFi, au niveau mondial, a un taux de pénétration d'environ 5 %. On peut également distinguer le WiFi du WiFi "ouvert", la différence entre les deux correspondant typiquement aux terminaux UMA qui disposent d'un circuit intégré WiFi à bord, mais dont le logiciel est bridé pour se connecter uniquement aux bornes des opérateurs. Donc si on considère les terminaux WiFi "ouverts", on constate qu'ils représentent moins de 5 % du parc, mais sont en forte croissance. La MobiNear Box est compatible WiFi.

L'Ultra White Band (i.e. UWB) et le WiMax sont cités pour mémoire. Il est à noter que les nouvelles versions de Bluetooth visent à le rendre inter-opérable avec WiFi, NFC, UWB et les applications faible consommation (i.e. Bluetooth Low-Power).

Enfin, le NFC est annoncé avec un taux de pénétration dans les mobiles de 20 % du parc en 2012 par l'AFMM (Association Française du Multimédia

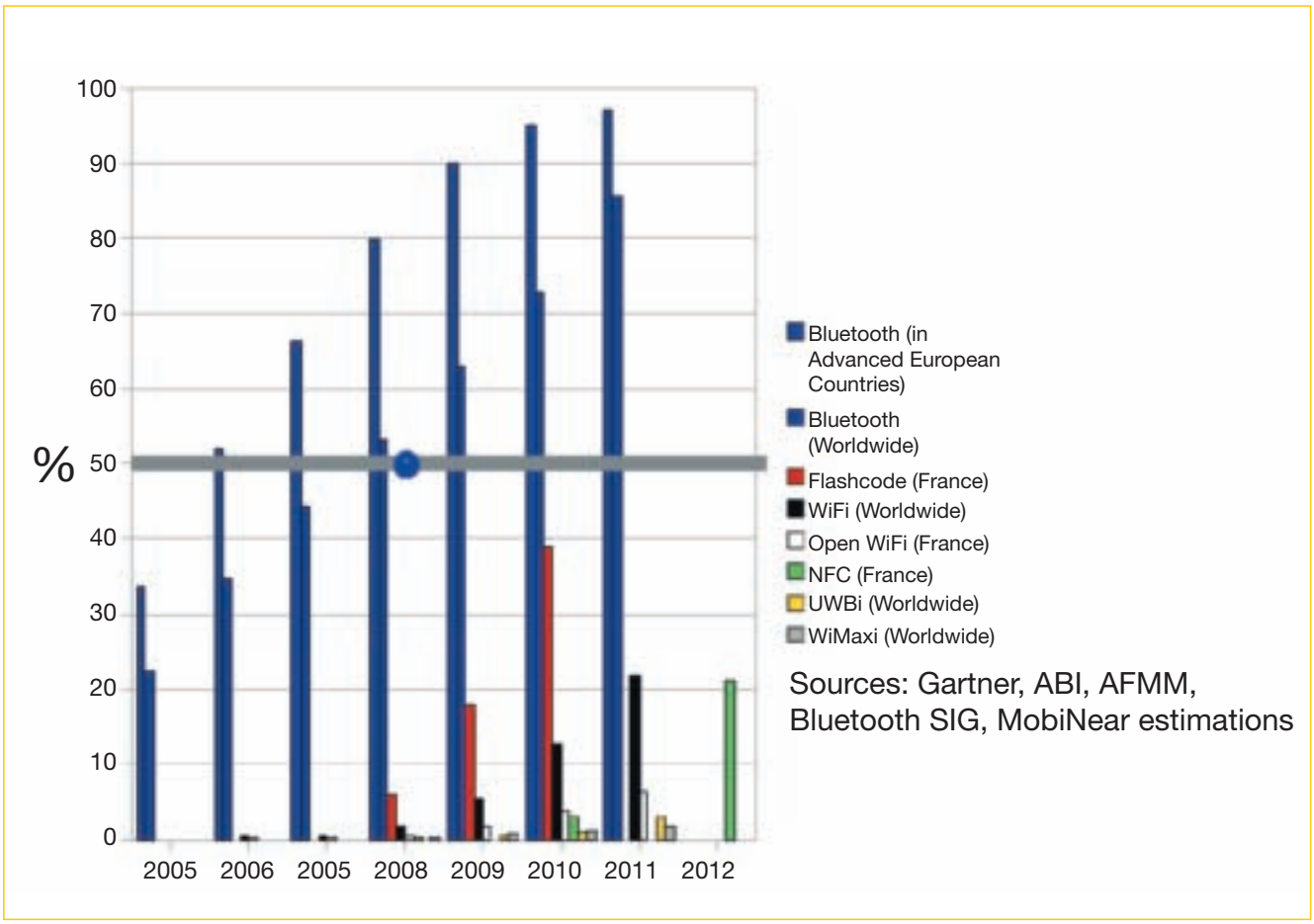


Figure 2 : Technologies de communications mobiles (hors Voix, Data & SMS)

Mobile). Notons que l'AFMM a reporté cette estimation d'un an cette année.

La technologie BlueNFC de MobiNear, permet de déployer dès aujourd'hui, à grande échelle, des usages de type NFC avec des terminaux Bluetooth standards.

Pourquoi BlueNFC ?

La technologie BlueNFC permet de déployer massivement des usages de types NFC sur des terminaux Bluetooth standards sans modifier le matériel, le logiciel ou les applications installés sur ces terminaux à bord du terminal. Partout en Europe, le parc compatible le jour du lancement est supérieur à 50 %. Et c'est plus de 80 % du parc installé compatible en France pour un lancement commercial en 2010.

Si on compare BlueNFC (i.e. Bluetooth Near Field Communication) et NFC (i.e. Near Field Communication), BlueNFC a 8 ans d'avance sur le marché. En effet, le taux de pénétration NFC est estimé à 20 % en 2013 ce qui correspond au taux de pénétration avéré du Bluetooth en 2005. La portée programmable du BlueNFC résoud également les problèmes de double ou triple Taps du NFC. De plus, les très forts volumes ont permis une érosion des prix des chipsets Bluetooth. Enfin, le débit Bluetooth est environ 10 fois supérieur à celui du NFC et permet donc l'envoi de contenus multimédia.

C'est pourquoi, BlueNFC peut être une étape vers les usages NFC mais avec un déploiement rapide à large échelle.

Comparaison des technologies

Le Tableau 1 compare les technologies Bluetooth, BlueNFC et NFC. La technologie BlueNFC réduit logiciellement la portée du Bluetooth d'une dizaine de mètres à une dizaine de centimètres pour mimer des usages de type NFC. Puisque BlueNFC est une technologie logicielle, la zone de détection est bien évidemment programmable. Le taux de transfert en Bluetooth environ 10 fois supérieur à celui du NFC.

Comme BlueNFC est une technologie 100 % logicielle, elle peut être ajoutée très rapidement aux lecteurs existant. Notre vision du meilleur lecteur est qu'il doit être multi-mode et au moins bi-mode, c'est-à-dire qu'il supporte à la fois NFC (ISO A, B & B') & Bluetooth (V1, V2 & BlueNFC).

	Bluetooth	BlueNFC	NFC
Type de réseau	Point à Multipoint	Point à Multipoint	Point à Point
Portée	10 m	< 0,1 m - 10 m & Programmable	< 0,2 m
Vitesse	721 kbits/ 3 Mbps	721 kbits/ 3 Mbps	424 kbits/s
Temps de connection	6 s	Typ : 3 s 1 - 6 s	< 0,1 s
Compatibilité RFID	Non	Non	Oui
"Zéro" click	Non	Oui : logicielle	Oui : logicielle
Sécurité	Non	Oui : logicielle & SIM	Oui : logicielle & SIM

Tableau 1 : Comparaison des technologies Bluetooth, BlueNFC et NFC.

Suite aux nouvelles recommandations sur le Bluetooth, BlueNFC a reçu un avis positif de la CNIL.

Applications des Technologies de communication sans-fil de proximité (Bluetooth, WiFi, NFC & BlueNFC)

Les technologies de communication sans-fil de proximité permettent la relation client sur le lieu de vente (i.e. CRM In-Situ) *(tableau 2)*.

Les usages pouvant être proposés sont par exemple :

- diffusion de contenus multimédia (audio-guides, bandes-annonces, ...),
- Smart Poster : affiches interactives pour mobilier urbain,
- paiement en magasin,
- carte de fidélité,
- coupons,
- optin,
- publicité ciblée,
- mesure de fréquentation.

MobiNear est une start-up créée le 23 Janvier 2007 qui a fait sa première levée de fonds le 31 Janvier 2007 auprès de Business Angels du secteur, dont Henri Seydoux (le PDG - Fondateur de Parrot, leader mondial des car-kits Bluetooth) qui est administrateur de MobiNear.

	SMS	Bluetooth	e-mail
Localisation	Partout	Magasin	Maison
Support	Mobile	Mobile	PC
Multimédia	Non	Oui	Oui
Taux de lecture d'un message	100 %	100 %	15 %
Coût par message d'utilisation du canal	"Cher"	"Gratuit"	"Gratuit"

Tableau 2 : Comparaison des canaux CRM.

COMMUNICATIONS SANS FIL DE PROXIMITÉ

De nouvelles technologies mobiles pour une ville interactive

par Laetitia GAZEL ANTHOINE, CEO CONNECTHINGS

Les technologies mobiles - code barres 2D, NFC... - apportent des solutions pour rendre les espaces urbains interactifs en utilisant l'écran des téléphones mobiles. Quels seront les services dans la ville ? Quels modeles économiques ? Quels acteurs et leur positionnement ? Retour sur les premières implémentations et expérimentations menées dans le monde.

Connecthings rend la ville interactive

Les services mobiles proposés par Connecthings apportent une nouvelle expérience dans la ville : le piéton simplement équipé de son téléphone mobile pourra désormais recevoir de l'information multimédia pertinente venant répondre à ses besoins d'informations ; en effet, dans de nombreuses situations, la plupart d'entre nous ont eu besoin d'obtenir des informations souvent fastidieuses voire même impossibles à trouver : devant un monument, dans une grande surface, un aéroport ou un salon d'exposition, ou même à un arrêt de bus.

En s'appuyant sur les nouvelles technologies intégrées aux téléphones mobiles, Connecthings apporte les solutions pour rendre l'environnement interactif et fournir sur le téléphone portable de l'utilisateur des services et informations contextualisés

Tourisme et Culture : ezStroll

ezStroll est un service mobile développé par Connecthings, permettant aux touristes de découvrir une ville. Depuis des points d'accès (datamatrix, tags NFC) déployés sur des mobiliers urbains à proximité de points d'intérêts et monuments de la ville, le touriste accède sur son téléphone portable à un guide multimédia géolocalisé : textes, images, plans, mp3, parcours thématiques. Il est donc possible d'offrir un service aux touristes étrangers dans leur langue maternelle et de fournir sur son téléphone mobile un contenu adapté à son profil. Enfin, de la même manière qu'il fournit à la demande de l'information culturelle géolocalisée, le service mobile ezStroll est également capable d'assurer la diffusion vers les touristes ou les habitants d'annonces municipales ou encore d'offres promotionnelles contextualisées dans le temps et l'espace.

Ces annonces sont créées et gérées à partir de l'outil de gestion de contenu et du média planning développés par Connecthings.

Mobulles Transport

En scannant les tags déployés sur le réseau de transports publics (aux arrêts de bus, dans les stations de métro) avec son téléphone portable, le voyageur accède directement à l'information correspondant à sa localisation : trafic des lignes, interconnexions, temps d'attente.

Grâce à l'outil de gestion de contenu de Connecthings, l'information voyageur peut être modifiée et enrichie en temps réel, par point tag ou réseau de tags et des annonces municipales et promotionnelles peuvent être ajoutées.

Le contenu affiché sur le téléphone mobile de l'usager comprend :

- des informations sur la disponibilité des correspondances à une station précise ou dans ses environs,
- les horaires des prochains passages à la station et sur la ligne où se trouve l'utilisateur,
- des messages d'informations et / ou de la publicité géolocalisés et donc en adéquation avec l'environnement direct de l'usager.

Des espaces indoor interactifs

Connecthings développe les services mobiles des salons d'exposition, de centres commerciaux, de musées... Grâce à des points d'accès déployés dans l'espace, les visiteurs accèdent au service mobile géolocalisé :

- plan indoor interactif développé par Connecthings,
- moteur de recherche des exposants, de produits, de biens, avec visualisation du résultat sur le plan,
- fiches exposants, fiches produits.

Tous ces services géolocalisés sont rendus possibles par la plate-forme logicielle développée par Connecthings. Cette plate-forme intégrant un outil de gestion de contenu (CMS) et un média planning permet de créer et de gérer toutes les annonces contextualisées de manière simple et efficace.

A propos de Connecthings

Créée en 2007, Connecthings développe une plate-forme de gestion de tags et de contenus contextualisés - fonction du temps et de la localisation. Le cœur de métier de Connecthings est de développer et commercialiser des solutions permettant de déployer des réseaux de tags dans l'espace public et d'y associer des informations contextualisées accessibles sur les téléphones portables. Les tags lisibles par les téléphones mobiles, s'appuient sur une ou plusieurs technologies : le code barre 2D, les puces NFC, le SMS ou simplement des coordonées GPS.

Connecthings fournit les outils pour :

- créer des contenus géolocalisés et planifiés dans le temps,
- gérer des parcs de tags visualisés sur des cartes,
- développer et adapter des applications aux écrans et navigateurs des téléphones portables.

WENEO : DES « SMART CARDS » AU « SMART OBJECTS »

Les « Smart Objects » au cœur de la révolution des services internet dans le monde du Transport, de l'Entreprise, du Bancaire et des Telecoms

Par Bruno BERNARD, NEOWAVE

Figure 1 : De la carte téléphonique à mémoire aux "Smart Objects"

Un « Smart Object » est un objet personnel, portable et communicant qui permet à son possesseur de s'identifier dans son environnement et/ou au sein d'une communauté.

Dans la lignée des cartes à puce, il lui permet aussi de réaliser des transactions en toute sécurité. Se présentant sous le format d'une clé USB *(figure 1)*, les Weneo de Neowave constituent une première génération de Smart Objects qui se veulent briser les limitations de la carte à puce en termes de connectivité (PC et Web), de capacité mémoire et capacité de traitement. Combinant dans un seul produit, la carte à puce, son interface RFID, son lecteur intégré et de grandes capacités de mémoire Flash, les Weneo constituent un nouvel e-media transactionnel.

Analyse du besoin du marché

Dans les dix dernières années, dans le monde du transport public, du paiement, de la gestion d'accès en entreprise, les solutions à base de cartes et de tickets sans contact ont apporté fluidité, fiabilité, sécurité et facilité d'usage dans des domaines où les évolutions technologiques se font à long terme. Cependant, faute d'infrastructure lecteur, ces applications sont coupées du monde du PC et de l'internet, et en conséquence des services associés. Par ailleurs les pilotes NFC ont démontré l'intérêt du grand public pour les solutions de dématérialisation, mais ceux-ci n'ont pas à ce jour entrainé de déploiements faute de mobiles NFC en volume et de business modèle bien établi.

TRANSPORT : la dématerialisation « tout de suite »

Dans le monde du transport, pour l'opérateur, les bénéfices de la dématérialisation du titre de transport se confirment.

On le voit avec le succès de l'e-ticketing dans le monde du transport aérien ou encore de l'IDTGV au niveau de la SNCF.

Grâce aux Weneo *(figure 2)*, fini les files d'attente interminables au guichet ou aux automates de distribution et de rechargement. En effet, l'usager peut réaliser ces opérations directement de chez lui sur son PC, ou de tout autre PC connecté, et ceci à n'importe quelle heure du jour ou de la nuit.

Pour l'usager, c'est une facilité d'usage, un gain de temps et de sécurité. Il peut ainsi réaliser ses transactions calmement, sans se déplacer et avec la possibilité d'en vérifier la validité sur le Weneo connecté à son PC.

Figure 2 : « Avec les Weneo Pass, plus de perte de temps au guichet ou aux automates »

Comme on l'identifie lorsqu'il se connecte, l'usager peut recevoir des messages personnalisés de la part de l'autorité organisatrice ou de l'opérateur comme l'annonce de travaux sur la ligne qu'il emprunte tous les jours. Le Weneo devient alors un véritable outil de communication entre l'opérateur et l'usager : l'opérateur peut promouvoir ses services et en informer l'usager tout comme l'usager peut avoir un contact client privilégié : exprimer ses besoins, requêtes, réclamations et satisfaction.

Un autre axe d'innovation à considérer est celui de l'utilisation de la plate-forme ouverte et multi-applicative du Weneo. Cette plate-forme permet d'envisager de combiner plusieurs applications répondant à des besoins identiques d'une communauté d'utilisateurs. Autour de l'application de base que constitue le transport public, on pourra ainsi venir greffer par exemple :

- pour une mairie ou une entreprise : l'accès physique et logique (réseau), une solution de porte-monnaie électronique, applications de productivité personnelles avec la Flash embarquée,
- pour des collégiens : un chéquier livre et spectacle, la gestion des présences, la consultation sécurisée des notes, l'accès à l'espace numérique de travail,
- pour une université : l'accès physique et logique (réseau), Moneo comme solution de porte-monnaie électronique, transmission de fichiers de travail …

Une des forces du concept Weneo est de pouvoir utiliser les puces déjà qualifiées par les opérateurs et par conséquent de rendre les Weneo parfaitement compatibles avec des infrastructures mises en place. De plus le business modèle reste inchangé pour l'autorité organisatrice qui garde le lien direct avec son client. L'ère de la dématérialisation est définitivement ouverte et ceci dès aujourd'hui. De nombreux pilotes sont actuellement en cours dans

plusieurs villes et régions dont notamment le pilote commercial lancé par la SNCF en novembre 2008 sur son réseau TER.

Contrôle d'accès logique et services RFID : la solution de convergence

Dans l'entreprise, le monde de l'accès physique et celui de l'accès logique étaient bien séparés car gérés par des entités différentes. Aujourd'hui, de plus en plus, la notion de protection de l'entreprise devient globale entraînant un besoin de convergence entre les deux mondes. Entrer de manière non autorisée, dans l'enceinte de l'entreprise ou entrer dans le réseau de l'entreprise sont devenus des actes tout aussi graves l'un que l'autre, de même que voler du matériel, des documents ou encore des identités. Les Smart Objects Weneo se veulent un des outils de convergence au service de l'entreprise grâce à une combinaison unique d'applications assurant un haut niveau de protection en contrôle d'accès logique et physique, tout en pouvant se coupler à d'autres applications utiles dans la vie quotidienne de l'employé.

Le contrôle d'accès physique dans les entreprises est basé depuis de nombreuses années sur des cartes, et les solutions sans contact (ISO14443) prédominent dans ce marché. La plate-forme ouverte du Weneo permet là aussi d'utiliser des puces dont l'interface RFID offre la compatibilité avec les principaux standards du marché du contrôle d'accès physique comme Mifare, Legic, Diester, STID…. et les principales applications de l'entreprise comme la gestion des présences et le porte-monnaie électronique. De plus, le Weneo Pass avec la photo d'identité permet de réaliser un contrôle visuel pour un gardien en plus du contrôle par les points d'accès RFID. La version numérique de la photo pourra aussi être stockée de manière sécurisée dans la mémoire du Weneo pour un niveau de sécurité accru.

Le contrôle d'accès au réseau de l'entreprise et la gestion des identités et des droits dans l'entreprise étaient réservés aux grandes entreprises et aux entreprises de haute sécurité, on voit maintenant que la demande s'étend aux PME. En effet, des solutions comme celles qui sont embarquées dans le Weneo s'appuient sur les standards informatiques du monde du PC et ne nécessitent donc pas d'installation et de mise en œuvre complexes. Les services de protection de réseau et de données *(figure 3)*, proposés par neowave incluent :

- Windows Logon sécurisé,
- authentification web,
- accès VPN sécurisé,
- Email sécurisé,
- cryptage des données…

Figure 3 : Services de protection de réseau et de données, proposés par neowave

Le fait de cumuler les deux fonctions dans un seul support permet de résoudre un problème de sécurité connu : en effet les employés ont tendance à laisser leur solution (carte, token,...) de contrôle d'accès logique active sur le poste de travail, lorsqu'ils s'absentent pour prendre un café ou même lorsqu'ils quittent l'entreprise le soir. Comme le Weneo Pass leur est nécessaire pour passer les contrôles d'accès, ils sont amenés à prendre leur Weneo pour sortir de l'entreprise et ainsi désactiver automatiquement leur poste de travail.

La plate-forme ouverte du Weneo permet d'ouvrir le champ des applications utiles pour l'employé de l'entreprise :

- PME Moneo ou privatif,
- Gestion des présences,
- Productivité personnelle (grâce à la mémoire Flash),
- Accès au Transport public,
- …

BANCAIRE : une solution d'authentification forte

Les solutions mises en œuvre dans le transport peuvent aussi s'appliquer dans le monde du paiement. Ainsi le Weneo peut devenir un Porte-Monnaie Electronique que l'on pourra consulter et recharger directement sur Internet. Par ailleurs les Weneo constituent une solution innovante d'authentification forte. Les Weneo se présentent comme la plate-forme idéale pour mettre en place des solutions d'authentification multi-facteurs qui peuvent s'adapter aux diverses demandes de ce marché en plein développement : compatibilité 3D Secure, application double ou triple facteurs d'authentification.

TELECOM : WENEO, le smart compagnon

Le « mobile paiement » fait l'objet de beaucoup d'intérêt dans les media suite aux multiples pilotes NFC réalisés à travers le monde. Dans la mouvance de la dématérialisation, ces pilotes ont montré l'intérêt du grand public de pouvoir réaliser des transactions avec leur mobile, objet qu'ils portent en permanence avec eux. Cependant, il n'est pas certain que « tout le monde » souhaite « tout faire » avec son mobile, peu à peu l'idée d'utiliser un Smart Object compagnon du mobile fait son chemin. Il permettra à son possesseur de répartir ses applications entre son mobile et son Weneo NFC à sa guise *(figure 4)*. Le mode lecteur du Weneo NFC permettra de réaliser le lien entre le mobile et le monde du Web et du PC. Grâce à la liaison NFC, plus simple à mettre en œuvre que celle d'autres protocoles de communication, l'utilisateur pourra mettre à jour, synchroniser, faire des transactions, répartir les applications sur son mobile avec une interface utilisateur optimale : celle de son PC.

Figure 4 : Répartition des applications entre son mobile et son Weneo NFC

Une plate-forme ouverte et une architecure performante

Construite autour d'un processeur 32 bits, la plate-forme Weneo *(figure 5)* offre une grande puissance de traitement et une grande capacité à gérer des environnements complexes. Vu du PC, le Weneo se présente comme :

- un lecteur de carte à puce PCSC/CCID,
- un CD-ROM,
- un Flash drive .

La fonction CD-ROM permet d'embarquer les drivers du Weneo, qui peuvent être chargés automatiquement sur le PC si nécessaire. Elle permet aussi de lancer en auto-exécution des programmes au démarrage des applications. On pourra ainsi programmer une adresse URL cible qui sera automatiquement accédée lors du lancement de l'application.

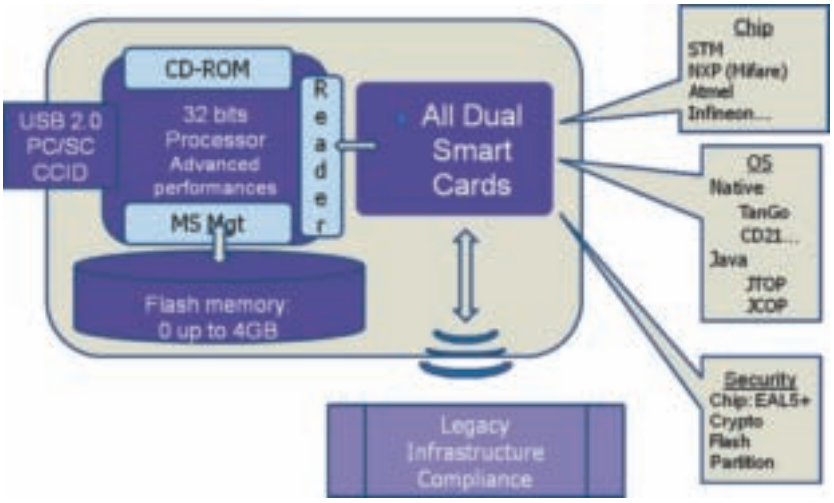


Figure 5 : Plate-forme Weneo

La plate-forme ouverte permet d'interfacer le lecteur intégré avec toutes les cartes duales existantes et même d'en implanter plusieurs dans le Weneo.

Neowave a aussi développé les briques logicielles nécessaires à l'interfaçage des serveurs web qui sont destinées à réaliser des transactions avec des Weneo et les autres produits de dématérialisation.

CONCLUSION

Avec les Smart Objects, c'est un nouvelle ère qui s'ouvre pour les cartes à puce et c'est un nouveau média qui se crée *(figure 6)*. Les services qu'ils peuvent rendre à leur possesseur et la facilité d'usage en font des objets qu'une partie des utilisateurs de carte à puce vont adopter et s'approprier. On va ainsi voir se déployer des services autour de cet objet pour des communautés d'utilisateurs qui ont des usages et des besoins communs : étudiants,

Figure 6 : Avec les Smart Objects , c'est un nouvelle ère qui s'ouvre pour les cartes à puce et c'est un nouveau média qui se crée

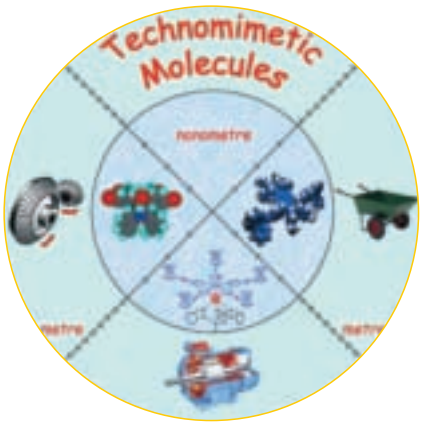
lycéens, employés d'une entreprise ou d'une collectivité locale. Les premiers tests faits par la SNCF, la RATP ainsi que l'ensemble des pilotes en cours dans les différentes villes et régions de France et d'Europe montrent que la voie est ouverte pour la démultiplication des Smart Objects et que l'on va les trouver prochainement dans notre poche accroché à notre trousseau de clé ou à notre mobile…

NANO-TECHNO-LOGIE

Miniaturisation ultime de systèmes : nanomachines et moteurs moléculaires

Par Dr Gwenaël RAPENNE Groupe Nanosciences, Centre d'Elaboration de Matériaux et d'Etudes Structurales - (UPR CNRS), 29 rue Jeanne Marvig, BP 94347, F-31055 Toulouse Cedex 4, France.

Dans l'évolution constante vers la miniaturisation des dispositifs électroniques et mécaniques, les molécules jouent un rôle de plus en plus important grâce à l'art de la synthèse multi-étapes qui permet aujourd'hui au chimiste de préparer des molécules "sur-mesure" avec des formes prédéterminées et des mouvements ou des fonctions programmées. Dans la stratégie de type "bottom-up", qui consiste à partir d'une molécule la plus simple possible et de lui ajouter des fonctions de plus en plus complexes, les machines et moteurs artificiels ont émergé en tant que nouveau champ de la chimie moléculaire. Ceci a été rendu possible grâce au développement de nouvelles techniques d'analyse, en particulier de la microscopie en champ proche qui permet d'observer une molécule unique, d'étudier ses mouvements et de la manipuler.



Mon projet dans le Groupe NanoSciences du CEMES s'est développé autour du contrôle du mouvement de rotation à l'échelle moléculaire. Pour celà, nous avons conçu et synthétisé des molécules technomimétiques, c'est-à-dire des molécules transposant des objets du monde qui nous entoure à l'échelle moléculaire, y compris les mouvements dont ces objets sont le siège. Nous avons ainsi synthétisé des *engrenages moléculaires*, une *brouette moléculaire* ainsi qu'une famille de *moteurs moléculaires*. Ces molécules ont été ou seront étudiées par des techniques de microscopie en champ proche (AFM et/ou STM).

Un moteur moléculaire

1. Principe de fonctionnement

Dans le domaine des nanosciences, l'un des défis à relever est la conception et la construction d'un moteur moléculaire de taille nanométrique. Un moteur rotatif est une machine qui, de manière continue, transforme une énergie en produisant un travail via un mouvement de rotation unidirectionnel contrôlé. Celui que l'on va présenter ici a été pensé pour être adressé individuellement, le but étant de le déposer entre deux électrodes distantes de quelques dizaines de nanomètres.

Les moteurs moléculaires synthétisés jusqu'à présent ont été étudiés en solution. Leur comportement est celui d'une assemblée de molécules et non de la molécule unique. L'originalité de notre moteur est qu'il a été élaboré dans le but d'être déposé sur une surface d'alumine entre deux nanoélectrodes métalliques (nanojonction). Ceci implique entre autres que la molécule soit particulièrement rigide. Notre stratégie est représentée *Figure 1*.

Le schéma de principe de notre moteur est représenté ci-dessous. Le groupement électroactif (GE) à proximité de la cathode devrait être réduit et la répulsion électrostatique devrait conduire à la rotation d'un cinquième de tour de la partie supérieure de la molécule. Le fragment réduit (chargé négativement, en noir) devrait être attiré par l'anode et lui céder son électron. Entre temps, un autre groupement électroactif devrait se placer au voisinage de la cathode, il serait alors réduit et ainsi de suite.

Du point de vue de sa structure chimique, ce moteur est composé de trois parties, avec une structure générale en tabouret de piano. La première est un socle tripodal constitué de trois pieds, fonctionnalisé de manière à se lier de manière covalente à la surface isolante dans laquelle seront enterrées les deux électrodes de la nanojonction. La seconde est une plate-forme aromatique ayant 5 groupements électroactifs accrochés de manière linéaire et rigide. Entre ces deux parties, un métal de transition joue le rôle de rotule. La partie supérieure sera libre de tourner alors que la partie inférieure restera immobile, accrochée à la surface. Cette molécule devrait alors convertir une énergie électrique en un mouvement contrôlé de rotation à l'échelle de la molécule unique.

2. Un tourniquet organométallique avec effet d'engrenage

Dans le schéma de synthèse de notre molécule cible, le complexe de ruthénium représenté ci-dessous est un intermédiaire clef. L'atome de ruthénium est la rotule qui va permettre la rotation. La partie inférieure est constituée d'un ligand trisindazolylborate qui a vocation à être fonctionnalisé pour être accroché sur une surface, il constitue le stator. Le plateau supérieur, par la présence des cinq atomes de brome, est prêt à recevoir les groupements électroactifs.

Un mouvement intéressant y a été mis en évidence. Du fait de la gène stérique imposée par les trois pieds du ligand tripode, la rotation du plateau supérieur (rotation aléatoire provoquée par l'agi-

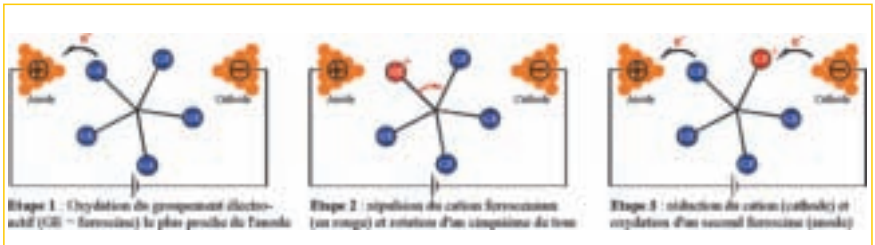


Figure 1 : Schéma de principe pour un moteur moléculaire unidirectionnel.

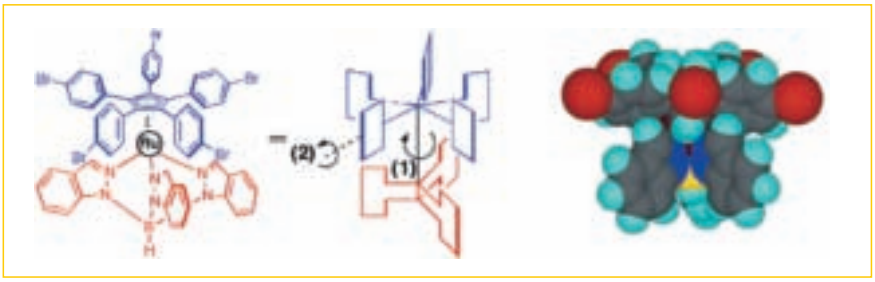


Figure 2 : Dans le précurseur pentabromé, la rotation libre du ligand supérieur par rapport au ligand inférieur (rotation 1) entraîne la rotation des pales (rotation 2)

tation thermique) entraîne la rotation des pales (les 5 groupements para-bromophényle). Cette molécule se comporte donc comme un tourniquet moléculaire avec un effet d'engrenage. Une étude théorique appuyée par une étude RMN à température variable a montré que la barrière de rotation (rotation 1) était très faible, de l'ordre de 4 kcal.mol^{-1}.

3. Synthèse de la partie active d'un moteur moléculaire

Après quelques étapes supplémentaires de synthèse, nous avons obtenu la molécule ci-dessous comprenant cinq groupes électroactifs de type ferrocène, des groupements électroactifs qui s'oxydent facilement et de manière réversible.

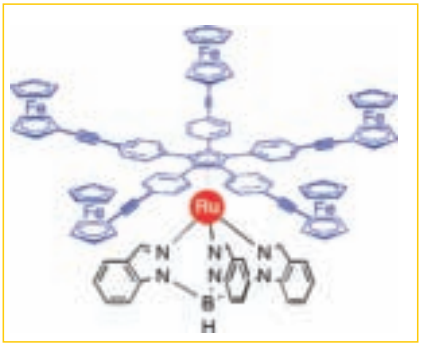


Figure 3 : Partie active d'un moteur moléculaire

Afin que cette molécule soit utilisée comme moteur moléculaire, certains paramètres ont été contrôlés. (i) Le potentiel d'oxydation des ferrocènes doit être inférieur au potentiel d'oxydation du ruthénium, afin que le ruthénium reste inerte lors de l'oxydation des ferrocènes. (ii) L'électrochimie du complexe a montré que son oxydation est réversible ce qui prouve la robustesse du complexe. (iii) Aucune bande d'intervalence n'a été observée ce qui montre que la communication électronique entre les ferrocènes, si elle existe, est très faible. En effet, pour l'objectif qui est le nôtre, les transferts d'électrons intramoléculaires sont à éviter puisqu'ils conduiraient au passage d'électrons entre les deux électrodes sans rotation de la partie supérieure de la molécule. (iv) Des calculs DFT et des expériences RMN à T° variable ont montré que la barrière de rotation du rotor est très faible (de l'ordre de 4 kcal.mol^{-1}).

4. Introduction de fragments isolants

Pour obtenir un mouvement de rotation il faut que le temps caractéristique de la rotation d'un cinquième de tour soit nettement inférieur à celui du transfert électronique intramoléculaire entre deux groupements électroactifs. En effet, dans le cas contraire les électrons passeraient à travers le rotor *via* le squelette carboné sans entraîner de rotation de l'ensemble *(Figure 4)*. L'introduction de fragments isolants dans chaque bras du rotor permet de diminuer le couplage électronique entre les groupements électroactifs et ainsi de localiser la charge sur un groupement électroactif oxydé.

Nous avons donc décidé d'insérer des fragments isolants (complexes de type trans-platine) dans chacun des cinq bras du rotor. Le platine présente de plus l'avantage de maintenir la rigidité de l'ensemble tout en augmentant de manière significative le diamètre de la molécule qui passe ainsi de 2 à 3 nm ce qui est un point positif pour son observation par microscopie en champ proche. De plus, l'électroneutralité de la molécule finale est préservée ce qui est essentiel pour l'étape de dépôt. D'autre part, ces complexes de platine sont plans carrés et permettent ainsi de garder la linéarité des bras tout en isolant les cinq groupements électroactifs du rotor. Une stratégie de synthèse modulaire a permis d'obtenir la molécule représentée *Figure 5*.

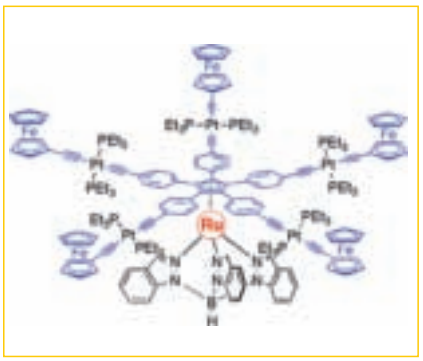


Figure 5 : Moteur moléculaire intégrant des fragments isolants.

Un travail analogue a été fait en utilisant le fragment bicyclo[2,2,2]octane. Le rôle isolant du fragment bicyclo[2.2.2]octane a été évalué théoriquement. Les calculs ont montré une diminution d'un facteur 12 du couplage électronique pour la molécule intégrant le fragment isolant. La synthèse du moteur incorporant le fragment isolant bicyclo[2.2.2]octane a été achevée *(Figure 6)*. On a maintenant une molécule de près de 4 nm de diamètre.

5. Introduction de groupes d'ancrage

Afin de pouvoir déposer le moteur sur des surfaces et ainsi pouvoir l'étudier par microscopie en champ proche, nous avons développé la synthèse de ligands tris(indazolyl)borates intégrant des fonctions ayant une affinité importante pour deux types de surfaces. D'une part, afin de visualiser notre molécule sur des surfaces métalliques

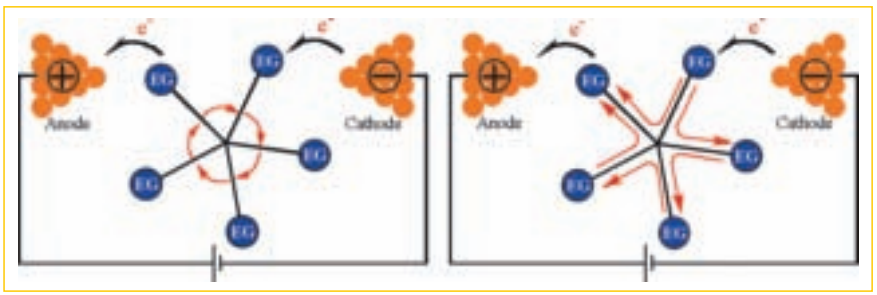


Figure 4 : A gauche le comportement souhaité c'est-à-dire que le transport des électrons conduise à une rotation du rotor. A droite, le comportement à éviter c'est-à-dire que le transport des électrons par transfert électronique intramoléculaire se produise sans mouvement du rotor (pseudo rotation).

avec un microscope à effet tunnel, nous nous sommes orientés vers des fonctions thioéthers qui sont connues pour interagir fortement avec des surfaces d'or. D'autre part, afin de pouvoir accrocher cette molécule sur une surface d'alumine entre deux nanoélectrodes, des fonctions esters ont été choisies. En effet, la fonction ester est connue pour interagir fortement avec des surfaces d'oxyde métallique, la déprotection spontanée des fonctions esters générant alors des groupes acides carboxyliques qui s'y lient de manière covalente. Les deux ligands fonctionnalisés sont représentés *Figure 6*.

Après avoir synthétisé leurs complexes de ruthénium modèles avec un ligand cyclopentadiényle non substitué pour vérifier leurs propriétés de coordination, ces ligands tripodes fonctionnalisés ont été intégrés à notre moteur.

Ayant en main tous les éléments constitutifs de notre moteur, nous avons ensuite synthétisé les molécules représentées sur la *Figure 7*. Il s'agit de deux moteurs prêts à être déposés sur une surface d'alumine entre deux nanoélectrodes avec ou sans isolant ainsi que le moteur à accrocher sur une surface métallique (à droite).

Les perspectives de ce travail sont maintenant d'observer ces complexes par microscopie en champ proche puis de construire les nano-électrodes nécessaires à leur fonctionnement. Des résultats préliminaires ont été obtenus, ils montrent en effet un mouvement de rotation contrôlable.

Une brouette moléculaire

De récentes avancées dans l'imagerie et la manipulation de molécules uniques ont stimulé la synthèse de molécules présentant des propriétés électroniques particulières mais aussi des propriétés mécaniques inédites à cette échelle. Dans le cas d'une brouette macroscopique, la pousser permet d'induire la rotation de la roue. Notre but est ici de transposer ce comportement à l'échelle moléculaire. Ce projet est directement connecté au projet de "moteur moléculaire" puisqu'il est fondamental de pouvoir identifier un mouvement de rotation sur une surface, en particulier un mouvement de rotation unidirectionnel.

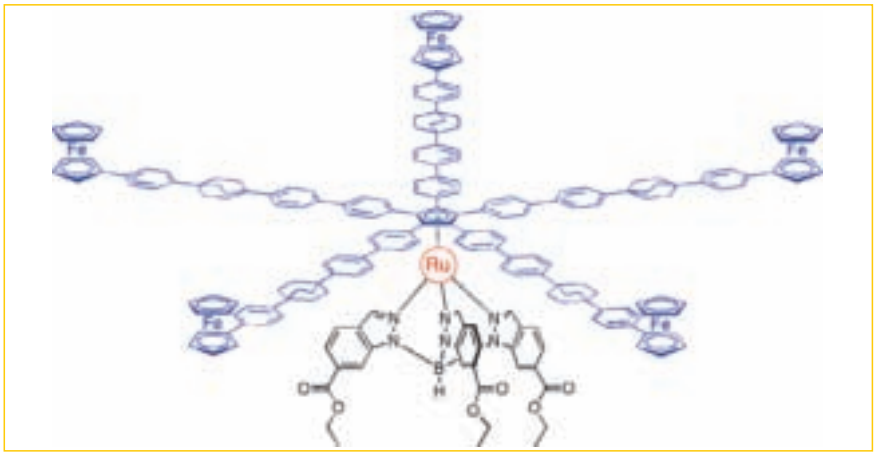


Figure 6 Synthèse du moteur moléculaire intégrant le fragment isolant bicyclo[2,2,2,]octane

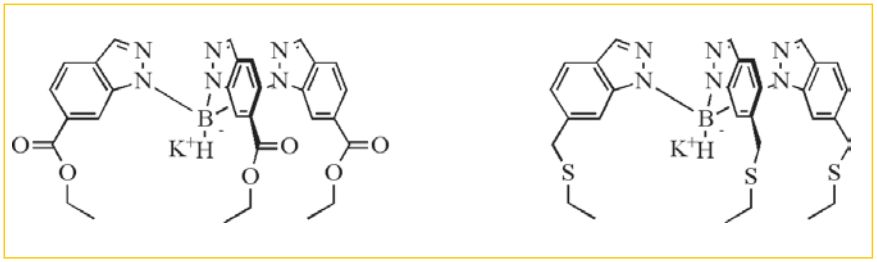


Figure 7 Nouveaux ligands tris(indazolyl)borates fonctionnalisés.

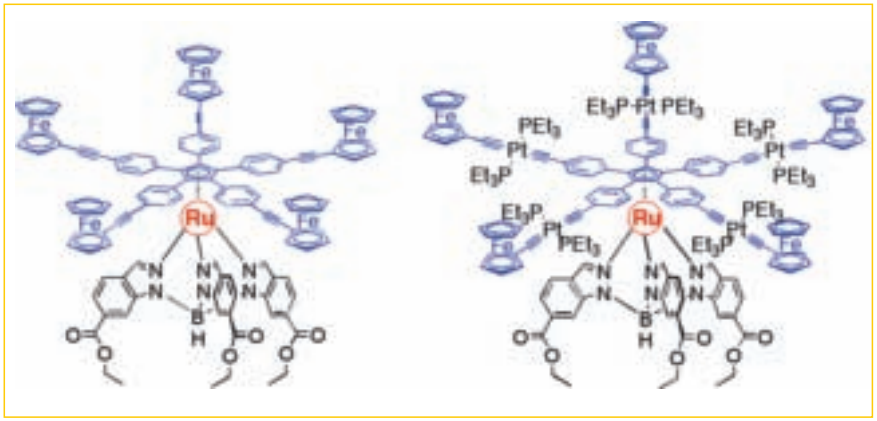


Figure 8 Famille de moteurs synthétisés intégrant un stator fonctionalisé.

Figure 9. Structure chimique de la brouette moléculaire (à gauche), son analogue macroscopique (au centre) et une vue en modèle CPK de sa modélisation moléculaire.

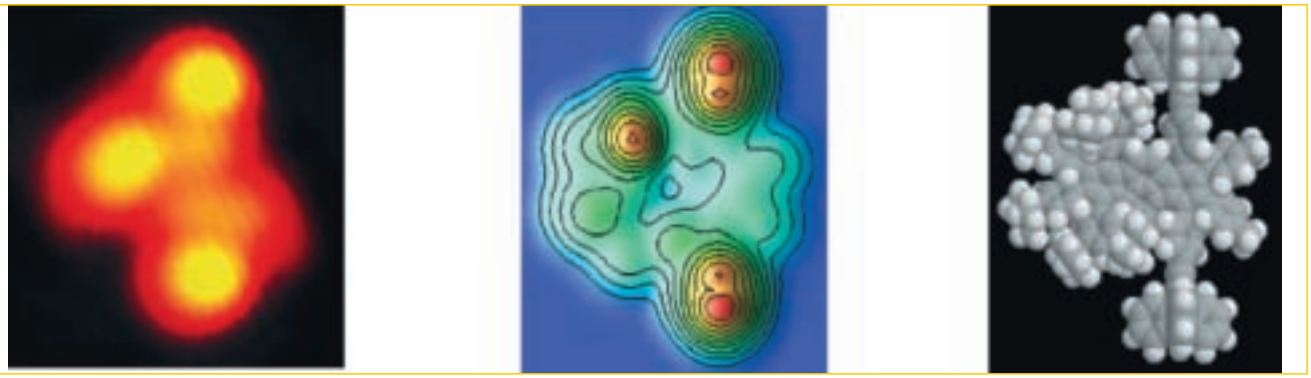


Figure 10 : Premières images de la brouette. A gauche l'image expérimentale, au centre, l'image calculée (méthode ESQC) obtenue à partir du modèle représenté à droite.

1. Design et synthèse d'une brouette moléculaire

Par analogie avec une brouette, nous avons ainsi imaginé une molécule contenant un châssis constitué d'une plate-forme polyaromatique rigide (et donc facilement manipulable par la pointe du STM), deux essieux indépendants comprenant : **2 roues**, **2 pieds** pour isoler le corps de la molécule de la surface et **2 poignées** pour manipuler la molécule avec la pointe du STM. Nous avons opté pour deux roues au lieu d'une pour des raisons synthétiques évidentes. La molécule synthétisée est représentée *Figure 8*.

Les fragments triptycène jouent donc le rôle de roues et les triple liaisons sont nécessaires pour permettre aux roues de tourner. Suivant une stratégie basée sur des séquences de doubles réactions de Knoevenagel et de Diels-Alder, la brouette a été obtenue après 15 étapes avec un rendement moyen par étape de 75 % ce qui correspond à un rendement global de 1,3 %.

2. Dépôt et observations d'une brouette moléculaire par STM

Déposée sur une surface de cuivre, la molécule adopte une conformation différente de celle en phase gazeuse, néanmoins, tous les éléments constitutifs (roues, pieds, poignées) peuvent être reconnus sur l'image calculée. Après dépôt, des images de cette molécule sur une surface de cuivre (100) ont été obtenues par STM. La molécule a été identifiée par comparaison avec son image calculée.
Jusqu'à présent, il n'a pas été possible de manipuler cette molécule sur cette surface de cuivre pour reproduire au niveau moléculaire le comportement mécanique d'une brouette, c'est-à-dire transformer un mouvement de translation appliqué à la molécule en un mouvement de rotation des roues. Il semble que malgré ses pieds, elle interagisse fortement avec la surface, et que l'action de la pointe ne soit pas suffisante pour la faire bouger. Des études sont en cours sur d'autres surfaces plus rugueuses, et nous envisageons également d'utiliser des surfaces d'isolants sur métal (tel que NaCl sur cuivre) où l'interaction devrait être plus faible.

3. Mise en évidence de la rotation d'une roue triptycène

Comme le montre la modélisation sur la partie gauche de la *Figure 11*, les fragments triptycènes sont des molécules 3D constituées de trois pales à 120° l'une de l'autre, elles peuvent donc jouer le rôle de roues.

L'étude de la molécule-essieu terminée par deux roues triptycènes ci-dessous a permis de mettre en évidence la rotation des roues sous l'action de la pointe du microscope à effet tunnel *(Figure 11)*. Il s'agit d'une première qui a été possible grâce à l'analyse ultrafine du courant passant de la pointe à la surface lors de la manipulation.

Ces roues présentent toutefois un désavantage intrinsèque, leur aromaticité les conduit à interagir fortement avec les surfaces d'étude. Afin de construire des nanovéhicules équipés de plus de 2 roues, nous avons donc besoin de les remplacer par des roues à la fois plus rigides et moins couplées avec la surface. Ces travaux sont actuellement en cours.

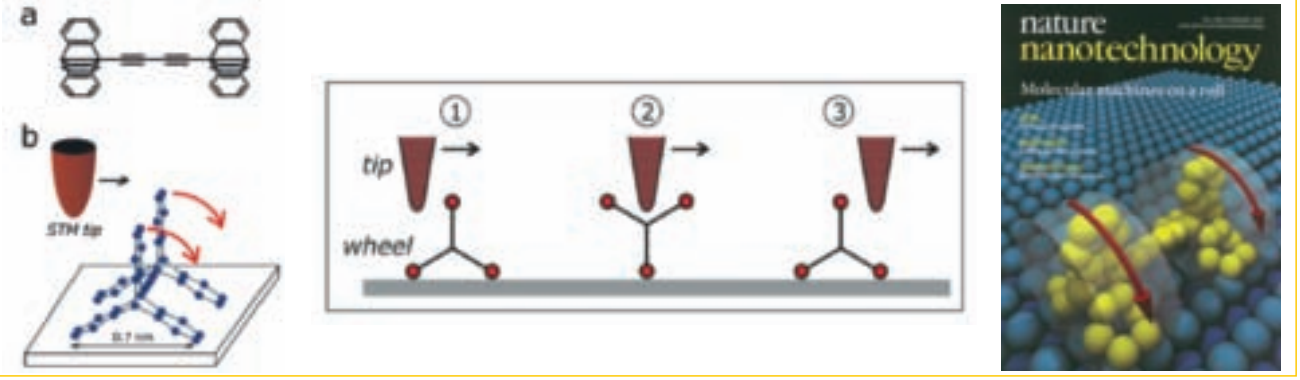


Figure 11 : Molécule-essieu contenant un axe linéaire terminé par deux roues triptycènes (a) et mouvement de rotation mis en évidence (b). Etape (1) la pointe du STM approche de la molécule. Etape (2) La rotation de la roue démarre. Etape (3) La pointe est passée de l'autre côté de la molécule en ayant entraîné une rotation de 120°.

Besoin d'évoluer ?

Devenez...

... Consultant

SAP, BI BusinessObjects, Qualification Logicielle

... Expert

Virtualisation / DBA Microsoft, UNIX ORACLE

... Développeur

ABAP - NetWeaver, .net, JAVA

Fitec vous propose

15 formations Métier

conçues et réalisées avec les éditeurs
SAP, BusinessObjects, HP Software, Microsoft

Consultant Finance et Comptabilité SAP FI/Co	40j	Administrateur Virtualisation Microsoft	45j
Consultant Achat et Administration des ventes SAP MM/SD	40j	Administrateur UNIX ORACLE	40j
Consultant Qualification Logicielle	40j	Administrateur Base de Données Microsoft SQL	45j
Consultant Testing HP for SAP	40j	Développeur JAVA J2EE JBoss	30j
Consultant BI BusinessObjects-SAP	40j	Développeur Microsoft .Net - SharePoint	35j
Consultant BI Microsoft SQL	45j	Développeur SAP ABAP - NetWeaver	40j
Consultant Service & Asset Management	40j	Consultant AMOA en environnement Finance	40j
Consultant Network & Systems Management	40j		

Contactez

Nelly MIMOS (n_mimos@fitec.fr)

01 55 70 80 90

(www.fitec.fr/metiers)

fitec
FORMATION & CONSEIL

Possibilités de financement global et partiel (Fafiec, Pôle emploi...)

MOODY CERTIFICATION ISO9001 FRANCE

CERTIFICATION
ISO9001
N° 2008012029

ffp

Membre de la FFP