

L'enquête

Le 04 novembre 2008

Internet des objets

Les objets communicants veulent être verts et sûrs

Par Cyrille Chausson, cyrille.chausson@leMagIT.fr

L'essentiel :

Tous les analystes s'accordent à dire que le sans-contact et l'ensemble des usages qui y sont liés, comme le paiement mobile, seront à coup sûr une des prochaines générations de technologies qui bouleversera le quotidien des consommateurs. Des travaux sur la récupération d'énergie et la sécurité tournent à plein dans les laboratoires français pour préparer le terrain à un marché prometteur.

Face un contexte d'expansion future et d'explosion des usages – comme nous le laissait entrevoir le [Forum Ocova](#) -, les laboratoires de recherche, épaulés par les pôles de compétitivité en Europe, planchent sur le développement de la technologie NFC (Near Field communications), son évolution, son amélioration et sa pérennité. Avec en filigrane, la volonté de répondre aux besoins des constructeurs et des fournisseurs de services pour qui le « commerce sans contact » représente une manne lucrative (voir encadré : **Un secteur dans les starting-blocks**). Leur objectif : combler les lacunes qui freinent la propagation du sans-contact. Parmi leur champs d'action prioritaire, les chercheurs planchent sur la récupération d'énergie, de façon à entourer la puce d'une couche de services et de la rendre plus intelligente. Pour au final, rassurer l'ensemble de la chaîne de production.

Considéré par l'industrie comme le standard de facto pour équiper les puces sans contact et orchestrer les usages de liaisons de proximité, la norme NFC, qui fonctionne aussi bien en mode actif (échange entre terminaux) que passif (lecteur ou émulateur de carte - voir encadré : **Un mode Peer-to-Peer pour orchestrer les échanges entre terminaux**) séduit. Notamment par sa simplicité d'utilisation. De par son faible rayonnement (pas au-delà d'une dizaine de centimètres – avec une efficacité optimale allant jusqu'à 4 cm), la technologie NFC implique une démarche volontaire du détenteur de l'appareil, généralement un téléphone portable. Ce qui est considéré par les défenseurs de la protection des données personnelles comme un acte primordial dans l'acceptation des usages.

Priorité n°1 : capter l'énergie

En dehors du couplage puce / lecteur, mécanisme de base reste un des travaux centraux et permanents dans les laboratoires, la priorité n°1 est bien celle de l'alimentation, résume Claude Tételin, leader du groupe traçabilité du pôle SCS (Solutions Communicantes Sécurisées). Et pour cause : elle constitue le nerf de la guerre dans la bataille de l'autonomie du « tag » (la puce).

« Nous essayons de récupérer l'énergie là où elle est, explique-t-il. D'abord en piochant dans l'environnement, avec l'énergie solaire, puis en s'intéressant à l'énergie dégagée par le corps humain. »

C'est aussi ce sur quoi planche le CEA de Grenoble dans son laboratoire, le

Leti. Au centre de ses travaux sur les objets communicants, des prototypes de micro-batteries (Above IC Micro battery), dont le but est de placer en superposition une source d'alimentation sur la puce, et ce en respectant les standards des semi-conducteurs CMOS. Pour François Vacherand, qui dirige le labo, cette solution présente un double intérêt : « cette batterie permet de fournir suffisamment d'énergie (quelque 100 à 200 micro-ampères par cm carré) pour alimenter deux fonctions : un mécanisme d'autodéfense qui vise à sécuriser les données en les effaçant en cas de menaces, et une horloge interne pour dater les éléments contenus dans la puce. » Le Leti planche également sur une architecture de composants capable de récupérer de multiples sources d'énergie : thermique, mécanique ou issues de vibration.

Un secteur dans les starting-blocks

Les chiffres du marché des solutions NFC sont plutôt optimistes : 700 millions d'utilisateurs de technologie NFC (Near Field Communications – norme associée au sans-contact) intégrée dans les téléphones portables d'ici à 2013, prédit le cabinet Juniper Research. Mieux, les ventes de puces NFC passeront de 650 000 en 2007, à 6,5 millions en 2008, prévoit ABI Research, pour exploser d'ici à 2013, à plusieurs centaines de millions. C'est dire si les constructeurs de téléphones mobiles, considérés comme l'un des supports premiers pour héberger la sainte puce, ont l'intention de se pencher sur son intégration.

De cette adoption technologique devrait découler un décollage côté services. La France a inauguré [le premier forum des services sans contact](#). Sa mission : fédérer industriels et consommateurs autour des problématiques de développements des usages du NFC.

...pour sécuriser l'infrastructure et les transactions

Elément indissociable pour rassurer les consommateurs, la sécurité des transactions réalisées entre terminaux NFC. Et lorsqu'on aborde le sujet du paiement par mobile via NFC, l'une des conditions qui fera éclore la technologie. Sur ce terrain, force est de constater que l'analyse ne peut être que prospective, commente Laurent Besset, consultant chez I-Tracing. « Les standards sont récents et les architectures pas encore bien définies (...) ». D'autant que la dématérialisation des paiements et des transactions sans contact associent les différentes failles de sécurité inhérentes à chaque secteur, celles du paiement traditionnel avec contact et celles associés aux radio-communications. C'est ainsi que les chercheurs se focalisent sur des parades contre le vol ou la destruction de terminaux, ou encore contre les attaques relais et la manipulation ou l'interception des données lors d'une transaction. L'idée est donc de placer des procédures d'authentification, de validation, de chiffrement ou encore de brouillage de signal, « quitte parfois à perdre en simplicité (d'usage, ndlr) », souligne Claude Tételin. Parmi les travaux de son équipe sur le sujet, « l'ajout d'une procédure d'identification par code PIN ». Une manipulation commode qui rassure.

De son côté, le Leti travaille à des algorithmes de chiffrement très peu gourmands en énergie, ainsi que, du côté des données personnelles, à un système de gestion de vie privée sans contact (CPM – Contactless Privacy Manager). Ce dernier doit notamment détecter la présence de lecteurs à proximité et appliquer des procédures de sécurité, pré-définie. Le CEA étudie également un système de brouillage pour « faire du bruit » sur les communications entre deux dispositifs sans contact.

Si l'alimentation et la sécurité constituent deux axes de recherche primordiaux, les centres de R&D sont encore aux prises avec le degré d'acceptation de la technologie NFC, et plus largement des usages du sans contact, comme le paiement mobile. Le sans-contact, qui constitue la clé de voute, avec la RFID, de l'Internet des objets doit encore murir. Et les laboratoires transférer le résultat de leur travaux vers l'industrie, comme le soulignait Yann Bidault, chef de projet du Forum Ocova.

Un mode Peer-to-Peer pour orchestrer les échanges entre terminaux

Sous forme de micro-puce électronique au rayonnement maximum d'une dizaine de centimètres, le standard ISO NFC repose sur le principe du couple lecteur / puce. On approche la puce d'un lecteur qui émet un champ magnétique et capte les informations alors enfermées dans la puce. On appelle cela l'émulation de cartes, à l'image du pass Navigo de la SNCF et de la RATP. Le terminal, généralement un téléphone portable, peut également se transformer en lecteur (on parle d'émulation de lecteur) et lire les puces NFC insérées par exemple dans du mobilier urbain. Ces deux usages fonctionnent alors en mode passif.

Mais là où NFC est considéré comme la technologie phare du sans contact, c'est qu'elle a également la capacité à fonctionner en mode actif. Dans ce dernier cas, il faut comprendre que la puce peut faire office de lecteur et d'étiquette. A titre de comparaison, le rapport maître / esclave disparaît pour donner lieu à un échange Machine-to-Machine dans lequel chaque appareil est autonome et actif. C'est dans ce dernier mode, que les spécialistes nomment également mode Peer-to-Peer, que réside un des enjeux majeurs du NFC; le mécanisme qui devrait faire décoller les communications d'objet à objet, de machine à machine, d'applications de paiement à téléphones. Une des forces de NFC tient enfin à sa compatibilité avec RFID, autre norme du sans-contact et terme générique souvent utilisé pour qualifier l'ensemble des technologies de radio-fréquence.