



PAR FRANCIS SYKES (84)

Responsable de l'ingénierie Navigo à la RATP

## La télébillettique : une opportunité pour les transports publics

En se substituant aux traditionnels billets dotés d'une piste magnétique, les cartes sans contact apportent en matière de lutte contre la fraude et d'entretien des matériels des solutions économiques pérennes. Elles ouvrent aussi la voie à de nouvelles fonctionnalités : l'interopérabilité qui permet de loger sur un même support les titres de transport émis par divers opérateurs ; l'achat de billets par Internet ou le téléphone ; le développement de nouvelles offres commerciales.

■ Le rôle du système de billettique d'un réseau de transport est simple : ouvrir l'accès au réseau à toute personne munie d'un droit et le refuser aux autres. Ce droit peut être forfaitaire (abonnements, carte de services, etc.) ou non (tickets unitaires, etc.).

Les revenus de la billettique constituant une ressource financière directe ou indirecte essentielle pour les opérateurs de transports, le bon fonctionnement du système de billettique est primordial.

### Un système flexible et sûr

Le système magnétique de la RATP, et son célèbre ticket cartonné à bande magnétique centrale, est en place en Île-de-France depuis les années 1970.

Au début des années 1990, il s'est

agi de chercher une solution pour lui succéder et répondre à de nouveaux enjeux. L'objectif était de disposer d'un système évolutif, flexible, sûr, ergonomique et financièrement viable tant du point de vue de l'investissement initial

**Un système évolutif,  
flexible, sûr et,  
financièrement viable**

que des coûts d'exploitation et de maintenance. Plusieurs technologies avaient été envisagées et dans certains cas prototypées et testées, dont les tickets magnétiques à haute coercitivité, et l'infrarouge, mais ces technologies ne répondaient que partiellement au cahier des charges.

Les technologies émergentes de couplage inductif communément connues sous l'appellation de RFID<sup>1</sup> caractérisées par une carte téléalimentée par le champ magnétique du lecteur avec lequel elle communique présentaient de nombreux avantages. Notamment, elles permettaient à un voyageur de valider son titre de transport par un geste volontaire.

Les technologies RFID dites de proximité (portée d'une dizaine de centimètres) permettent de s'assurer que le titre de transport qui a été validé est bien celui de la personne située à proximité immédiate de l'équipement de validation, contrairement aux technologies dites de proximité dont la portée est plus importante.

Les équipements magnétiques comprennent des mécanismes précis d'entraînement, de lecture et d'écriture, sollicités au passage de chaque ticket. Le coût de maintenance de ces équipements est donc élevé du fait du nombre de pièces mobiles.

La RFID, par l'absence de pièce mobile dans les coupleurs permet de s'affranchir de ces coûts. L'ar-

chitecture centralisée du système magnétique est seulement réservée aux réseaux fermés.

La sécurité du lien radio offerte par la carte à puce à microprocesseur a rendu possible l'architecture décentralisée RFID indispensable pour les réseaux bus, de dépositaires et autres tiers (automates bancaires, téléphone...).

Ce nouveau système à base de cartes à puce RFID sans contact, appelé aussi télébilletique, ouvre de nouvelles fonctions, aujourd'hui encore sous-exploitées. Nous pouvons citer notamment la possibilité d'intégrer sur un même support un abonnement et un complément de parcours ou la cohabitation de plusieurs abonnements, ce que le système magnétique ne pouvait pas offrir.

Par ailleurs, ces technologies permettent l'usage de cryptographie repoussant les limites de la contrefaçon.

**Pérenniser les investissements**

La longévité d'une rame de métro ou de train se compte en décennies. Il en est de même du système de billettique. Or, la billettique étant la matérialisation des politiques tarifaires, le système est amené à évoluer régulièrement, parfois plusieurs fois par an, au gré des changements de ces dernières et des extensions de réseaux. Un système de billettique doit donc concilier évolutivité et pérennité. Cet objectif ne peut être atteint que grâce à une politique industrielle pensée dans la durée.

Pour la RATP, cette politique s'est traduite notamment par le cofinancement de la première génération de masques<sup>2</sup> de cartes télébilletiques pour amorcer le marché, garantir la compatibilité et ouvrir la concurrence. Ces masques étaient disponibles sous licence. Ces masques s'appuient sur des spécifications ouvertes, connues sous

le nom de Calypso<sup>3</sup>, qui s'appuient à leur tour sur des normes (ISO 14443, 7816 et CEN 1545).

Enfin, cette politique repose sur les technologies émergentes de la carte à puce soutenues par une offre industrielle, confortant ainsi la pérennité du système.

**Une politique industrielle pensée dans la durée concilie évolutivité et pérennité**

**Fraude molle et fraude « high-tech »**

Valider un ticket magnétique dure plusieurs secondes. En revanche, la télébilletique, grâce à la vitesse de traitement par la carte à puce et aux échanges radio optimisés entre la carte à puce sans contact et le lecteur-valideur, assure une validation dans un délai de l'ordre de 200 ms.

Pour ne pas ralentir le flux de voyageurs entrant dans les bus, seuls ceux utilisant des tickets « consommables » doivent valider leurs tickets. Les abonnés dont l'abonnement est matérialisé par un ticket magnétique se contentent

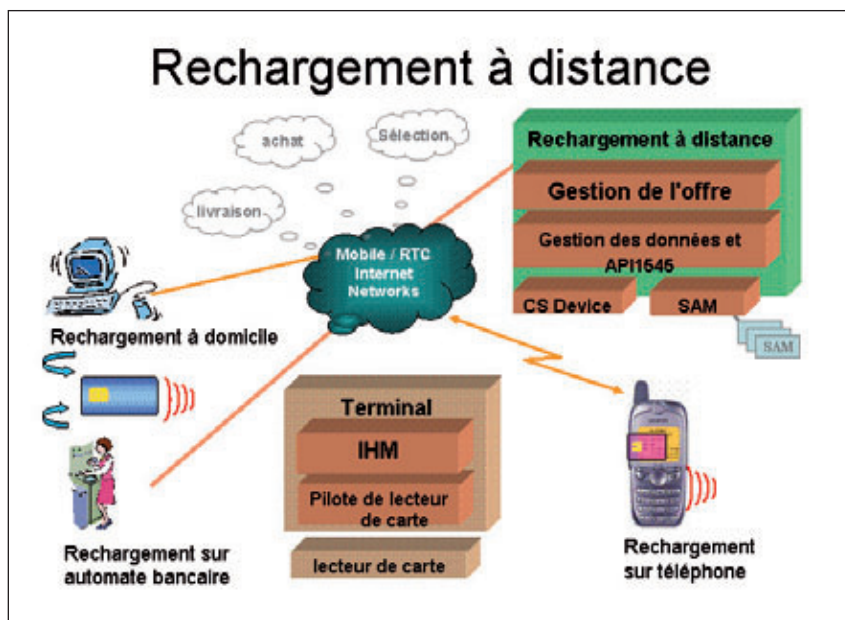
de montrer au conducteur leur abonnement.

Si ces règles minimisent le temps de montée dans les bus, elles ne permettent pas de faire baisser la fraude.

La contrefaçon est une course contre la montre entre les contrefacteurs d'une part et les concepteurs et fournisseurs de technologie d'autre part. Ainsi, quand le système de billettique magnétique

On qualifie de fraude « molle » celle qui consiste à monter à bord d'un bus sans titre de transport, voire avec un abonnement périmé. La télébilletique a permis de mettre en place une politique de validation systématique à l'entrée des bus. Cette politique a eu l'effet escompté d'une baisse significative de la fraude molle, augmentant d'autant les recettes.

a été déployé dans les années 1970, la contrefaçon du ticket magnétique était inexistante. Dans les années 1990, le manque à gagner occasionné par la contrefaçon de billets magnétiques se chiffrait en millions d'euros. Les cartes à puce, grâce à leur cryptographie, sont



beaucoup plus difficiles à cloner. Cependant, toutes les cartes à puce ne sont pas égales devant la contrefaçon, comme en témoignent les attaques récentes de cartes à puce à mémoire sans contact aux Pays-Bas et à Londres.

C'est la conjonction du « progrès » constant des techniques de contrefaçon et de la volonté de garantir la pérennité du système qui a conduit les opérateurs qui ont choisi la technologie Calypso à opter pour des cartes à microprocesseur à haut niveau de sécurité (authentification mutuelle avec les modules de sécurité à puce également, diversification des clés, cloisonnement des zones transport, mécanismes de session-ratification, intégrité, gestion d'aléas anti-rejeux, garantissant une sécurité de bout en bout).

## Commodité et vie privée

Lors de la dernière enquête de satisfaction Navigo, 92 % des clients se sont déclarés satisfaits ou très satisfaits. La rapidité de la transmission, la commodité et le service

**Les données de déplacement sont effacées après quarante huit-heures, délai technique nécessaire à la détection de la fraude**

après-vente sont particulièrement appréciés. En cas de perte ou de vol d'un passe Navigo personnalisé, le voyageur peut faire opposition et se faire fabriquer un nouveau passe qui aura les mêmes droits que le premier. L'identité du premier passe sera alors communiquée aux équipements de validation qui l'invalideront à la première occasion. Cela fournit un service de qualité pour le voyageur qui continue à bénéficier de son abonnement et à l'opérateur de transports qui limite les pertes liées à ce type de fraude, dans la mesure

où le premier passe devient inutilisable pour un tiers.

Un autre type de service, qui satisfait à la fois le client par la flexibilité procurée, et l'opérateur, est la possibilité de souscrire à un abonnement résiliable à tout moment. cela est rendu possible grâce à la faculté d'inhibition de la puce décrite précédemment.

Ne serait-ce que pour gérer le système de billetterie et prévenir la contrefaçon, il est nécessaire de pouvoir distinguer individuellement les passes et objets sans contact qui circulent sur le réseau de télébilletterie. En revanche, constituer une base de données comprenant l'identité du porteur et l'identifiant du passe présente des opportunités mais aussi un danger potentiel si l'on y associe l'usage du passe.

Quant aux dérives potentielles d'un système établissant la correspondance entre identité de passe, de porteur et trajets, les médias imaginent des scénarios de Big Brother. Conformément à la loi Informatique et Libertés, la RATP s'est engagée à effacer les données personnalisées relatives à l'usage des passes de plus de quarante-huit heures, délai technique nécessaire à la détection de la fraude. Les données sont par la suite anonymisées.

Enfin, pour répondre aux attentes des clients ne souhaitant pas que leurs données nominatives soient enregistrées, un passe déclaratif appelé « Passe Navigo Découverte » a été lancé. Cependant, en cas de perte, il n'est pas possible d'établir le lien de propriété. Ce passe n'ouvre donc pas les mêmes possibilités de remplacement.

## La télébilletterie au-delà de la carte

Depuis l'origine du projet télébilletterie Navigo, toutes les cartes

sont émises directement ou indirectement par les transporteurs. Si cela reste envisageable pour les Franciliens qui utilisent, ne serait-ce qu'occasionnellement, les transports publics, des alternatives semblent préférables pour traiter le cas des autres voyageurs occasionnels.



La technologie RFID a gagné d'autres secteurs et notamment la banque (cartes bancaires sans contact, en particulier avec le standard EMV Contactless), la téléphonie mobile (téléphones NFC<sup>4</sup>) et l'identité (contrôle d'accès, cartes d'identité et passeports...). Dans les deux premiers secteurs, les cartes à puce étaient déjà au cœur des produits utilisés par les clients : carte bancaire et carte SIM respectivement.

La technologie commune à toutes ces applications est la norme d'interface RFID ISO 14 443. Les travaux de standardisation du NFC

**Il est possible de remplacer un passe perdu ou volé et de programmer sa désactivation**

Forum et l'initiative française Ulysse ont permis l'émergence d'un standard ouvert permettant l'usage des téléphones portables pour choisir, acheter, télécharger et valider des droits de transport. La RATP a mené des expérimentations avec les trois opérateurs de téléphonie mobile qui ont établi la

faisabilité et l'acceptabilité par les clients de ce service.

Cette fonctionnalité, combinée aux développements d'architectures Java embarquées, permettra de télécharger non seulement des droits de transport mais aussi l'application de transport sous forme d'*applet* JavaCard. Ainsi, un

touriste pourra télécharger l'applet Java Navigo puis, grâce à une application Internet mobile du téléphone (WAP, I-Mode ou autre), les droits lui permettant de voyager en Île-de-France.

L'utilisation de réseaux publics pour le rechargement à distance

exige un très haut niveau de sécurité et impose de fait l'utilisation de composants à microprocesseur et une cryptographie forte.

Ainsi, l'usage de nouveaux supports (cartes multiapplications, téléphones NFC, clés USB...) émis par des tiers permet de couvrir une grande partie des profils de voyageurs occasionnels et d'envisager la suppression complète du système de billettique magnétique.

## La télébillettique dans le monde

Si la France peut être fière des expérimentations de télébillettique menées dans les années quatre-vingt-dix, elle n'a pas été seule dans cette aventure. Ce qui a caractérisé la démarche française, menée à l'origine par la RATP<sup>5</sup>, a été avant tout la volonté d'aboutir à une solution industrielle pérenne et sûre.

La télébillettique est à présent déployée dans de très nombreux réseaux et est devenue la technologie de référence de tout nouveau réseau de billettique, que ce réseau utilise uniquement des cartes comme support sans contact ou bien également des téléphones comme au Japon ou des cartes émises par des tiers.

Les contextes locaux et nationaux ont plus ou moins favorisé le passage du stade de l'expérimentation à celui de la généralisation. Dans de nombreux cas, c'est la facilité de mise en place de bassins d'interopérabilité offerte par les capacités des cartes à puce sans contact qui a suscité le déploiement de réseaux de télébillettique. C'est le cas des Pays-Bas (Trans Link), du Royaume-Uni (ITSO), de la Scandinavie (RKF) et de nombreux autres pays et régions.

La notoriété du système de télébillettique Octopus de Hong Kong est due à son adoption par la grande majorité des Hongkongais et à sa fonction de porte-monnaie électronique.

Cependant, dans de nombreux pays, la gestion d'un porte-monnaie électronique est le monopole de banques.

Si les premiers réseaux ont, pour des raisons

historiques, déployé des cartes utilisant des interfaces RFID non normalisées, nous assistons progressivement à leur substitution par des cartes au protocole ISO 14443. Même au Japon où la technologie Felica, propriété de Sony, domine le marché, l'adoption de cartes conformes à la norme ISO 14443 se profile, grâce à l'adoption de cette norme par l'ICAO. En définitive, ce qui distingue fondamentalement un réseau de télébillettique d'un autre est d'une part le choix de niveau de sécurité de cartes (à microprocesseur ou à mémoire) permettant ou non d'envisager des opérations de rechargement sécurisé à distance (téléphone, automates bancaires, clés USB sans contact ou rechargement sur Internet comme expérimentés actuellement par la RATP) et d'autre part la nature « propriétaire » ou ouverte de la technologie, les deux facteurs influant sur la pérennité et les coûts d'évolution du réseau.



### Une norme internationale et une offre industrielle mature

En quelques années, la télébillettique est passée du stade de l'expérimentation dans quelques villes au stade de la généralisation sur les cinq continents. Cette convergence vers la technologie sans contact s'explique par la combinaison de plusieurs facteurs : la sécurité, l'évolutivité, la fluidité, la fiabilité, le coût, par l'émergence d'une norme internationale adoptée également par d'autres industries et enfin par une offre industrielle mature.

La sécurité accrue qu'offrent les composants à microprocesseur permet déjà au support sans contact de prendre des formes variées (cartes, téléphones, clés USB, etc.), souvent multifonctionnelles, partagées par plusieurs acteurs et rechargeables à distance en toute sécurité donnant à cette technologie une ouverture dont on ne mesure pas encore la portée. ■

1. Radio Frequency Identification.
2. Masque : système d'exploitation d'une puce.
3. Calypso : technologie ouverte de cartes sans contact à microprocesseur adoptée par une cinquantaine de réseaux de transport, dont les évolutions sont gérées par l'Association Calypso Networks Association (CNA).
4. NFC : Near Field Communication, standard international définissant l'application du RFID aux téléphones portables.
5. Sous l'impulsion de son directeur des systèmes d'information et des télécommunications de l'époque, André Ampelas (66).