



Le paiement mobile

ABSTRACT

In this paper we aim at describing how mobile payment is developing around the world, what commercial offers are proposed and what technical solutions are applied. In countries where access to financial institutions is lacking, mobile payment developed very fast and continues to grow. In other countries they are a lot of attempts to introduce it, initiated mainly by the Net industry. They are just on the start and the future will show what market share mobile payment will take.

Introduction

Le terminal mobile, qu'il s'agisse du téléphone mobile de base ou du smartphone, est certainement l'un des outils les plus diffusés sur tous les continents : les services qui l'utilisent sont susceptibles d'atteindre rapidement un taux de pénétration significatif. Il a de plus trois qualités essentielles :

- par nature, via les réseaux auxquels il a naturellement accès, il permet d'échanger facilement des données ;
- grâce à la carte SIM qui l'équipe, il est associé à une personne identifiable que son opérateur mobile peut facturer ;
- enfin la carte SIM peut contenir des informations secrètes par exemple des coordonnées bancaires.

C'est pourquoi on a vu se développer des initiatives nombreuses et variées en termes de cible fonctionnelle visant à utiliser le téléphone mobile comme outil de paiement. Les acteurs de ce domaine sont très divers : les opérateurs de réseau mobile visent à prendre place sur un marché qui était celui des banques, les fabricants de terminaux recherchent des revenus récurrents après avoir vendu l'appareil, les acteurs de l'Internet souhaitent bénéficier éventuellement d'une partie des reversements que les vendeurs font à la banque en cas de paiement par carte, la grande distribution peut souhaiter réduire ces mêmes reversements et les banques veulent faire face à tous ces concurrents potentiels.

Dans cet article, nous tenterons de présenter les différents types d'usage actuels et envisagés pour les terminaux mobiles en matière de paiement et de décrire les éléments techniques sur lesquels ils s'appuient.

Panorama des différents usages du terminal mobile en matière de paiement

Les utilisations des terminaux mobiles dans le domaine du paiement sont très variées : elles s'appuient souvent sur des réalisations *ad hoc*, faisant appel aux capacités de communication de données, de visualisation et de traitement que

fournit la gamme de terminaux dont disposent les clients des différents opérateurs. Nous n'avons pas la prétention de donner une liste complète des différents usages mais seulement d'en donner les grands types.

Le rechargement de comptes prépayés et les petits achats sur mobile

Les opérateurs de services mobiles, pour diminuer les risques d'impayés ont développé, dans de nombreux pays, des cartes prépayées qui peuvent être rechargées dans des réseaux de commerçants partenaires : ils ont ainsi créé pour chacun de leurs clients un compte dont ils assurent la gestion. Pour tirer profit de leur capacité à facturer des petites sommes au coût marginal, ils ont également tenté de développer le paiement d'achats par le canal de leurs factures : directement ou via des partenariats, ils se sont efforcés de proposer un catalogue de produits qui peuvent être achetés et payés sur la facture mobile du client. Mais cette approche reste limitée à des achats du type sonneries, fonds d'écran, jeux, car elle impose des montants d'achat faibles et implique des accords entre opérateur et marchands : c'est un contexte difficile à gérer à la fois pour les opérateurs et les marchands qui doivent gérer des accords avec plusieurs opérateurs. Des sociétés intermédiaires entre opérateurs et marchands ont vu le jour, comme par exemple W-HA, filiale d'Orange, qui travaille avec différents opérateurs et fournit des prestations techniques permettant, en particulier, de payer des petits achats sur les factures émises par les opérateurs.

Commerce électronique

Le développement de l'accès à Internet a largement ouvert la porte au commerce électronique dont le chiffre d'affaires en 2014 était estimé à 56,8 Mds d'euros pour la France avec une croissance annuelle dépassant 10 %. Il a donc été nécessaire de développer des moyens de paiement en ligne. A partir d'un ordinateur personnel, la carte de paiement est largement utilisée mais sans code secret : ce

qui rend le système fortement sensible en cas de vol ou de divulgation du numéro de carte. Pour assurer que l'acheteur est bien le titulaire du compte bancaire associé à la carte, les banques s'appuient sur le terminal mobile de l'acheteur dont le numéro est associé au compte en lui envoyant par SMS un code secret qui doit être retourné à la plate-forme de paiement par Internet avant que le paiement puisse être accepté : c'est le système 3D secure qui est de plus en plus utilisé par les marchands en ligne.

Les smartphones donnant accès à Internet, ils se substituent au PC pour faire des achats sur Internet et deviennent peu à peu un outil important de commerce électronique.

Le terminal mobile comme terminal de paiement

La carte de paiement occupe une place très importante dans les paiements effectués en Europe et en Amérique du Nord. La très grande majorité des commerçants en France acceptent le paiement par carte et se sont équipés de terminaux de paiement (TPE) qui doivent disposer d'une connexion aux réseaux bancaires, soit par une ligne téléphonique fixe soit par un accès mobile (GPRS en général) pour permettre d'autoriser la transaction de paiement lorsque l'autorisation est requise. Mais pour certaines catégories de vendeurs, vendeurs occasionnels par exemple, ou pour le paiement à la livraison, il n'est pas économique ou pratique d'utiliser un TPE alors même que beaucoup des clients demandent à payer leurs achats avec leur carte de paiement. C'est pourquoi nombre d'acteurs¹, ont développé sur des smartphones des applications qui couplées en Bluetooth à un petit lecteur de carte de paiement permettent d'encaisser des paiements par carte. C'est la capacité de communication et de traitement du smartphone qui est ici mise en œuvre. Sa limite est, sauf à équiper son smartphone d'une imprimante de tickets, qu'il n'est pas prévu d'édition de ticket en temps réel : par contre le client peut recevoir par mail un ticket-client après sa transaction.

Le terminal mobile comme support de ticket

Dans de nombreux services, le client doit acheter, préalablement à l'accès au service, un ticket, éventuellement par Internet, ticket qui sera vérifié avant ou lors de l'usage du service proprement dit : c'est le cas par exemple des transports. De très nombreuses compagnies aériennes ont mis en place des services de carte d'embarquement dématérialisée via une application chargée sur un smartphone. De même la SNCF permet au client de charger dans son mobile le ticket qu'il a réservé préalablement sous forme d'un code QR².

¹ On peut citer Square ou IZettle et des banques et également des opérateurs mobiles parmi ceux fournissant un tel service.

² Code QR (Quick Response code) : sorte de code barre bidimensionnel

On peut imaginer la même procédure pour des places de spectacle. La seule contrainte est que le vendeur doit avoir le moyen de vérifier que le ticket est bien valide et n'a pas été contrefait. Il faut donc que son personnel ait à sa disposition par exemple un lecteur de code QR pour vérifier sa validité.

Le terminal mobile comme porte-monnaie électronique

Forts de leur expérience dans le domaine de l'alimentation des comptes prépayés, les opérateurs ont été naturellement poussés à étendre les usages de ces comptes vers d'autres usages comme le transfert d'argent de personne à personne ou l'obtention d'argent liquide auprès d'agences. Comme on le verra plus bas, ces offres de paiement mobile ont eu un succès certain dans les pays où l'accès au système bancaire est peu développé. Dans les pays où le système bancaire est très développé, on assiste au lancement de très nombreuses initiatives dans le domaine du paiement mobile. Ce sont ces deux aspects que nous allons développer dans la suite de cet article.

Le paiement mobile dans les pays en développement

Dans les pays où les habitants n'ont que peu accès au système bancaire, comme par exemple dans certains pays d'Afrique, pour pouvoir développer les services téléphoniques, les opérateurs se sont fortement appuyés sur les abonnements prépayés et ont dû développer des moyens de rechargement, soit par recours à des réseaux de partenaires, soit en développant des moyens spécifiques de rechargement, par Internet notamment. Dans quelques pays, il apparut que les crédits de communication étaient spontanément transférés d'un client à un autre, voire revendus et finalement pouvaient servir à des transferts d'argent à l'intérieur de la population. Après un certain nombre d'expérimentations, des opérateurs mobiles africains et multinationaux ont lancé, parfois avec des partenaires bancaires locaux, des comptes prépayés associés au numéro de téléphone mobile : c'est par exemple le cas de MTN, un opérateur sud-africain, avec MTN mobile money ou des opérateurs africains filiales ou partenaires de Vodafone, avec M-PESA ou encore les filiales africaines du groupe Orange avec Orange Money.

Ces services permettent en général :

- de déposer et de retirer de l'argent dans des boutiques partenaires ;
- de transférer de l'argent entre clients du service et vers des personnes non clientes ;
- de payer des factures ;
- d'acheter des crédits de communication mobile ;
- éventuellement de payer des employés : c'est le cas des policiers en Afghanistan avec M-PAISA.



Figure 1 : Une agence M-PESA au Kenya.

Pour faire fonctionner le service, les opérateurs s'appuient sur des réseaux d'agents qui ont pignon sur rue (figure 1) : c'est par leur intermédiaire que les clients peuvent déposer de l'argent sur leur compte mobile et en retirer. Ils jouent un rôle essentiel dans le succès du service. Les transferts entre comptes sont normalement commandés par les clients eux-mêmes à partir de leur téléphone mobile.

Dans les régions concernées, les smartphones et les services de données mobiles (figure 2) sont encore peu développés, même si l'on prévoit une forte croissance : aussi les services offerts actuellement font-ils usage du service de données USSD³ disponible sur la très grande majorité des terminaux mobiles. C'est ce service qui, dans les réseaux mobiles, est utilisé, par exemple, pour interroger son compte mobile ou commander le service de messagerie vocale. Il permet une interaction simple avec l'utilisateur (figure 3) et

³ USSD : Unstructured Supplementary Service Data

des échanges de données entre le téléphone et un serveur de l'opérateur. Avec USSD, les données sont transportées dans le réseau de commande du réseau mobile assurant ainsi une bonne sécurité dans l'échange de données.

Les opérateurs se rémunèrent en faisant payer chaque transaction entre clients. Selon la GSMA⁴, 15 des opérateurs consultés par cette association ont eu un chiffre d'affaires lié au service de paiement dépassant un million d'euros en juin 2015 : parmi ces opérateurs, 12 avaient plus d'un million de comptes actifs durant les trois derniers mois.

Pour les opérateurs mobiles, le paiement mobile permet de fidéliser le client et d'augmenter l'ARPU⁵ de l'ordre de deux euros.

Le développement des offres de service

Les offres de services de paiement mobile se sont très fortement développées depuis 2008 : à la fin de 2015, près de 271 services dans 93 pays ont été identifiés par la GSMA⁶ dont la moitié concerne l'Afrique subsaharienne (figure 4) ; l'Asie du sud, l'Amérique latine et l'Asie Orientale ont vu, ces dernières années, une forte croissance. En décembre 2015, l'ensemble de ces services s'appuyaient sur un réseau de 3,2 millions d'agents déclarés dont un peu plus de la moitié ont été actifs en décembre : ce nombre est très important, il dépasse largement le nombre d'agences bancaires, jusqu'à être dix fois plus nombreux que ces

⁴ GSMA : Association des opérateurs mobiles GSM

⁵ ARPU : Average Revenue Per User ou Revenu mensuel par client

⁶ Pour plus de détails on pourra se reporter au rapport de la GSMA dont sont issues nombre d'informations reproduites dans cet article

http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/04/SOTIR_2015.pdf

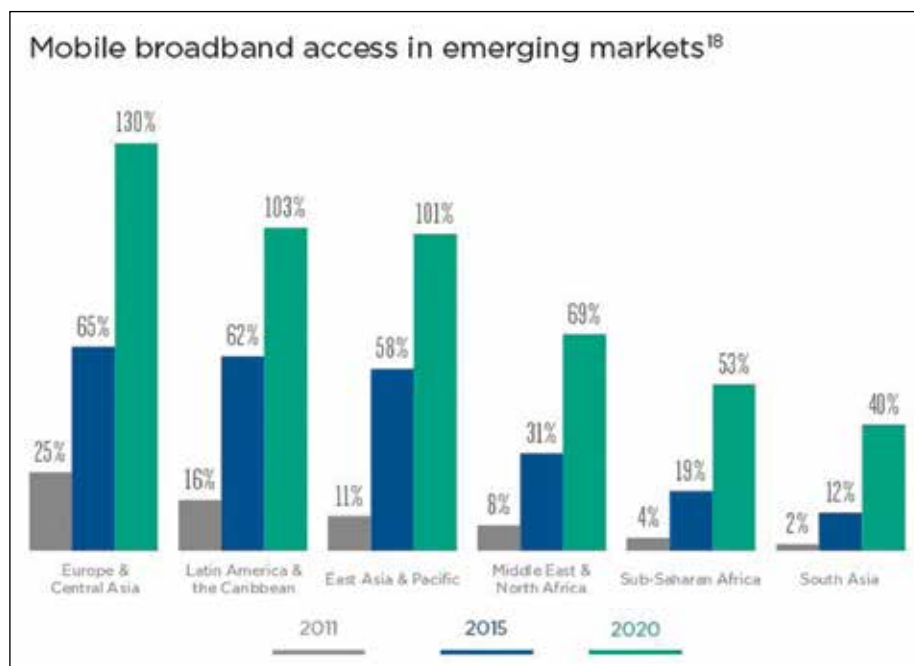


Figure 2 : Pénétration de l'accès mobile haut débit dans les marchés émergents - Source : GSMA.

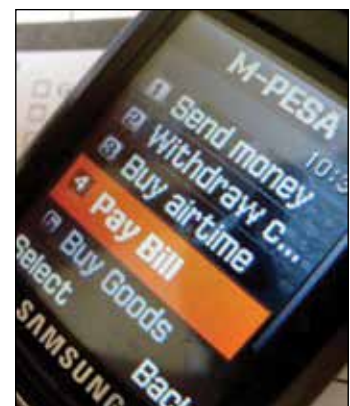


Figure 3 : Exemple d'interface utilisateur en USSD.

Source : Libre Afrique.org.

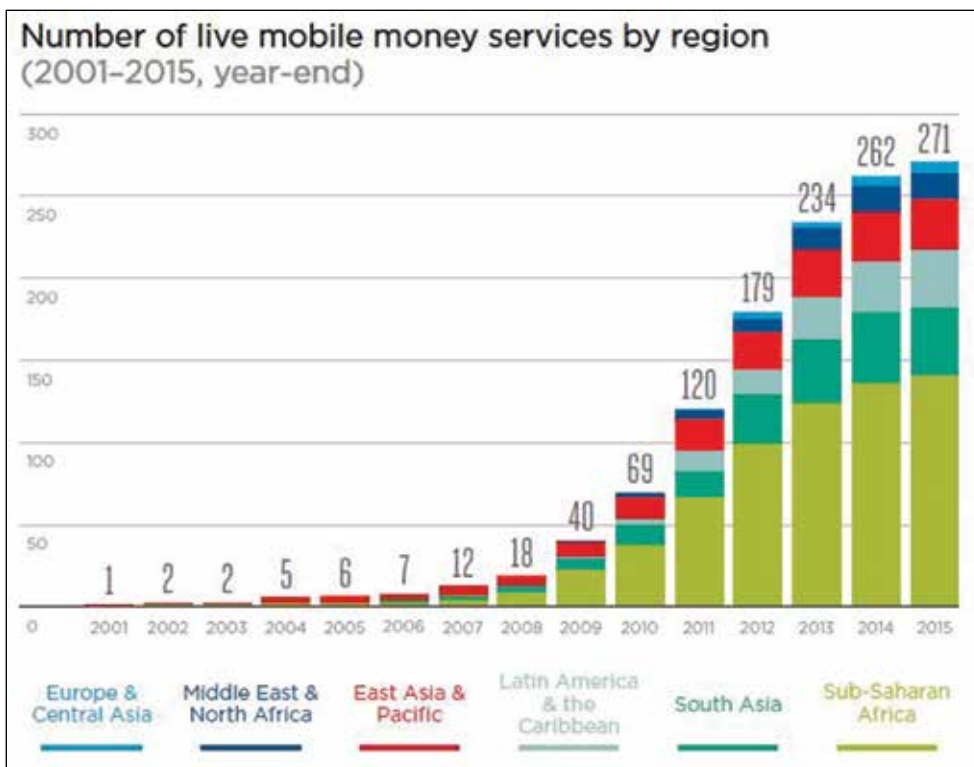


Figure 4 : Évolution du nombre de services de paiement mobile par région – Source: GSMA.

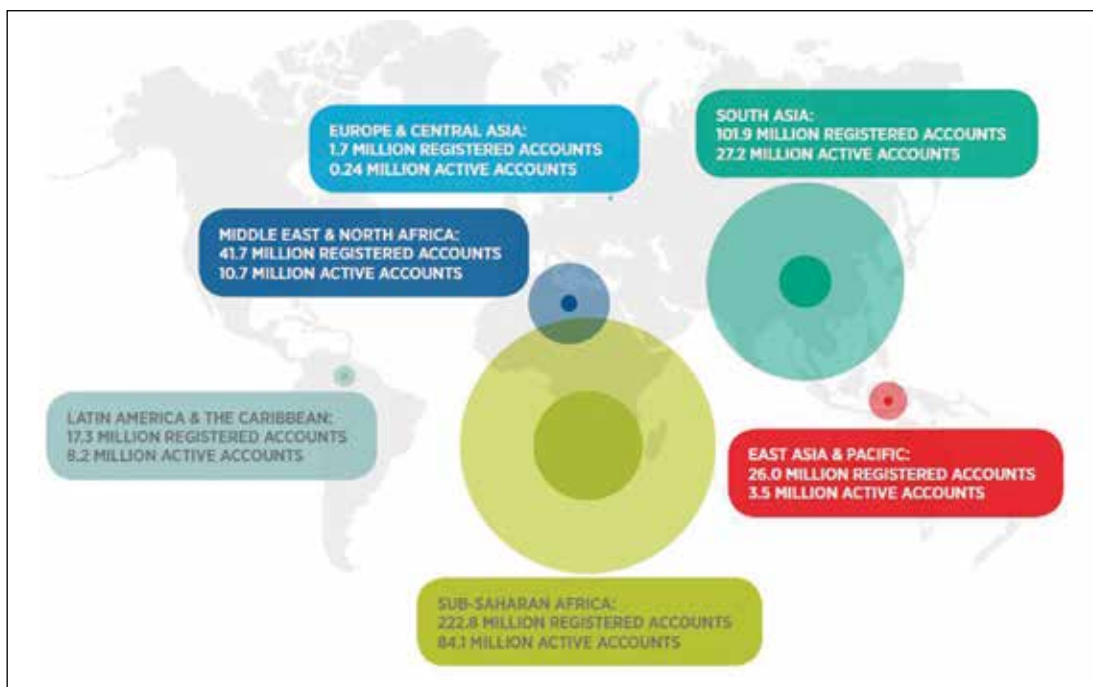


Figure 5 : Nombres de comptes ouverts et actifs (90 jours) par région (décembre 2015) – Source: GSMA.

dernières dans une trentaine de marchés. Dans l'ensemble des pays étudiés par la GSMA, les agents assurent plus de 90 % des sorties d'espèces alors que les distributeurs de billets (ATM) ne représentent que 7,8 %. En 2015, le nombre de comptes de paiement mobile a crû de 31 % pour atteindre 411 millions : 134 millions d'entre eux étaient actifs pendant les derniers 90 jours. A titre de comparaison, Paypal pour l'ensemble du monde affiche

173 millions d'utilisateurs actifs. En moyenne, les opérateurs de service de paiement mobile traitent 33 millions de transactions par jour.

La figure 5 montre que c'est en Afrique subsaharienne que l'on a le plus de comptes ouverts et de comptes actifs : un tiers des abonnements mobiles y sont associés à un compte de paiement mobile. Ce taux atteint 55 % dans l'Est de cette région africaine.

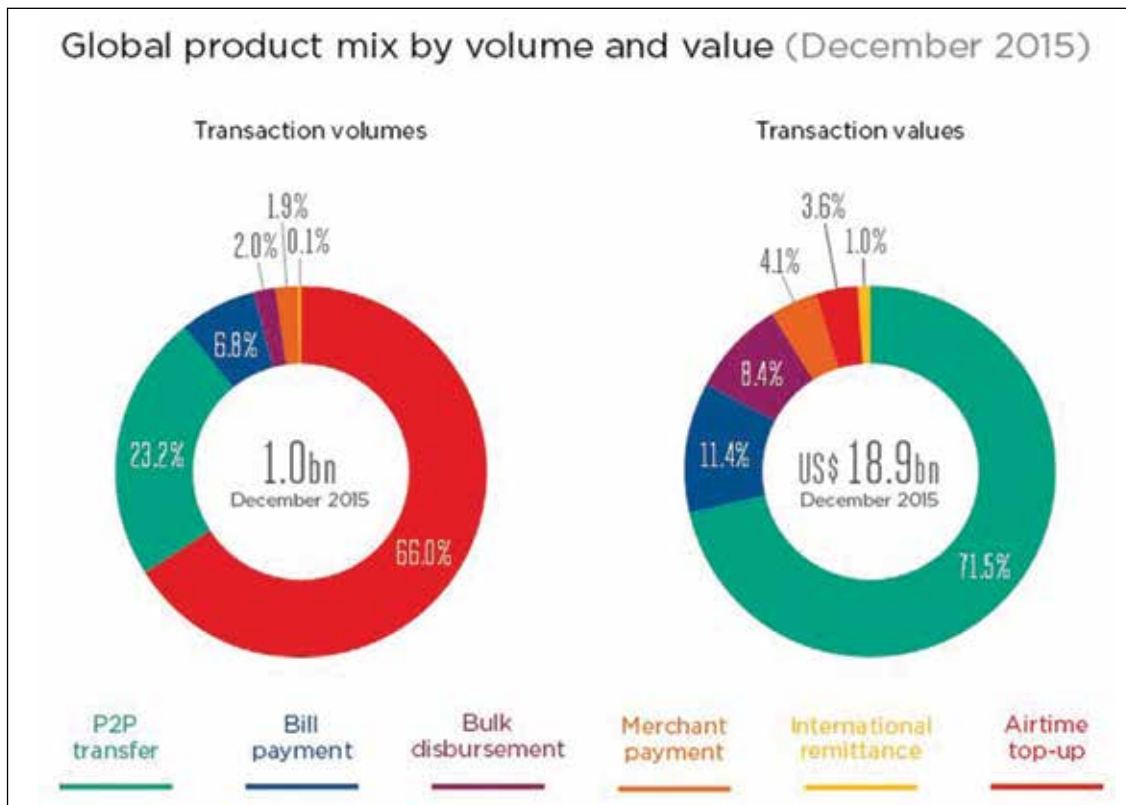


Figure 6 : Usage du paiement mobile – Source: GSMA.

Quels usages pour le paiement mobile ?

L'analyse des usages des services de paiement mobile fait apparaître que le rechargement des comptes mobiles prépayés est le premier en termes de nombre de transactions alors que le transfert d'argent de personne à personne est le premier en termes de volume d'argent transféré (figure 6). Globalement, l'industrie du paiement mobile est en forte croissance puisque, sur l'année 2015, elle a connu une croissance de 31,5 % en valeur.

Les paiements en volume (bulk disbursement) correspondent à l'injection d'argent dans le système sous forme de paiement de salaires ou de versement d'indemnités diverses ; ils représentaient, en 2015, 8,4 % des injections d'argent dans le système. L'expérience du paiement des salaires des policiers par le gouvernement d'Afghanistan montre qu'à la fois le gouvernement et ses policiers y ont gagné en faisant disparaître des employés fantômes et en supprimant des détournements.

Le paiement chez les marchands, bien qu'il soit en forte croissance (+28 % en valeur en 2015), ne représente qu'une faible part des paiements mobiles. Il y a donc là un important gisement de développement pour le paiement par mobile. Une des difficultés réside dans l'équipement des marchands : celui-ci ne peut pas être propre à un système de paiement mobile donné et devrait permettre de recevoir des paiements venant de plusieurs systèmes de paiement mobile ainsi que de cartes bancaires.

Le transfert international de fonds représente globalement un faible volume mais il est en forte croissance (51 %) et les prix des transferts sont en diminution (divisés par 2 en 2015). Compte tenu de la forte diaspora africaine en Europe, qui couramment transfère de l'argent vers leur famille en Afrique, nombre d'opérateurs multinationaux ont étendu à de nombreux pays d'Europe les possibilités de rechargement à distance par Internet et ont ouvert des services de transfert d'argent vers l'Afrique.

Le montant des transactions effectuées est très variable : il varie de 0,7 USD pour la moyenne des rechargements du compte téléphonique à plus de 30 USD en moyenne pour les retraits d'espèces ou les transferts de compte à compte.

Limites et perspectives

Le paiement mobile souffre encore d'un certain nombre de limitations. L'interopérabilité entre les différentes offres de paiement mobile existant dans un même pays et l'interopérabilité avec les banques ne sont pas en général assurées, ce qui limite les transferts de personne à personne ou les paiements chez les marchands. Des initiatives ont été engagées dans un certain nombre de pays pour assurer l'interopérabilité entre les offres, soit en recherchant l'interopérabilité directe des offres prises deux à deux, soit en faisant appel à une plate-forme intermédiaire qui par la même occasion peut assurer l'interopérabilité avec le système bancaire. Le mouvement vers l'interopérabilité peut être accéléré quand

les états souhaitent numériser le paiement des salaires de leurs employés ou des indemnités qu'ils peuvent verser à leurs citoyens. Élargir l'écosystème dans lequel s'intègre le paiement mobile est essentiel pour sa croissance : de nouveaux usages sont à considérer. Dans un certain nombre de pays, des opérateurs de paiement mobile ont engagé des partenariats avec les opérateurs de transport pour permettre le paiement des services de transport par l'intermédiaire de cartes rechargeables qui peuvent être rechargées à partir du porte-monnaie mobile.

Le paiement mobile dans les pays fortement bancarisés

Le contexte des pays fortement bancarisés est évidemment complètement différent de celui des pays en développement. Dans tous les cas, la carte de paiement y a pris une place très importante, les commerçants sont largement équipés de terminaux de paiement capables de lire les cartes de crédit et peu à peu de lire des cartes et des terminaux via l'interface NFC (voir encadré 1). En France, en 2015, il y avait 64,5 millions de cartes bancaires qui ont réalisé plus de 11 milliards d'opérations (source carte bancaire CB) et plus de 1,5 million de commerces équipés d'un terminal de paiement. Le nombre de TPE sans contact croît rapidement (+37 % entre mars 2015 et mars 2016 : source observatoire du NFC et du sans contact) et en mars 2016 plus de

27 % des commerçants sont équipés de TPE sans contact (383 000 en mars 2016). Aux États-Unis, où le paiement par carte est très développé, la transition de la carte à piste magnétique vers la carte à puce est en cours, ce qui complique la question de la mise en place du paiement mobile.

Dans un tel contexte, en plus des usages classiques des terminaux mobiles pour faire des paiements sur facture téléphonique, des rechargements de compte prépayé, pour porter des tickets de transport ou bien pour assurer la sécurité des transactions de paiement par carte sur Internet, on voit de grands acteurs promouvoir des offres de paiement sur smartphone, celui-ci se substituant à la carte de paiement. Pour les clients, elles viennent donc en concurrence avec l'usage de la carte de paiement classique ou sans contact : pour eux, l'intérêt essentiel pourrait être la facilité d'utilisation de l'offre de paiement sur smartphone, en tirant profit de l'usage de plus en plus fréquent de ce dernier dans la vie quotidienne. L'objectif des promoteurs de ces offres est, en plus de réduire les temps d'attente en caisse, de prendre pied sur un marché nouveau mais déjà fort pourvu : leur succès n'est donc pas garanti. Leur approche consiste très majoritairement à réutiliser toute la chaîne de paiement électronique mise en place pour le paiement par carte depuis les terminaux de paiement des commerçants (TPE) jusqu'aux réseaux de données bancaires et à introduire une application spécifique dans les smartphones équipés d'une interface NFC.

NFC CCP

La technique NFC^(a) CCP^(b) est une technique de communication à très courte distance (moins d'une dizaine de cm) dérivée du RFID^(c) et apparue au milieu des années 1990. RFID permet la lecture de badges portés par les entités à identifier. Ceux-ci, lorsqu'ils sont passifs, puisent leur énergie dans le rayonnement radio émis par le lecteur. NFC, normalisé par l'ISO et la CEI offre trois modes de fonctionnement :

- le mode émulation de carte dans lequel le dispositif NFC émule le comportement d'une carte à puce ou d'un badge : on peut ainsi intégrer dans le mobile des services comme l'entrée dans un moyen de transport en commun ou bien le paiement par carte ;
- le mode lecteur qui permet à un dispositif NFC de lire des cartes sans contact ou des badges électroniques ou un autre dispositif NFC. Le dispositif démarre la communication et envoie une commande à la carte ou au badge qui y répond ;
- le mode peer to peer permet à deux dispositifs NFC d'échanger entre eux des données : le transfert de données est alors plus lent que dans les autres modes, à cause des protocoles de dialogue. Mais un premier échange en mode NFC peut être utilisé pour initialiser un autre mode d'échange radio comme Bluetooth ou Wi-Fi quand les échanges sont volumineux.

NFC CCP utilise la bande des 13,56 MHz avec des débits de transfert de données entre 106 et 424 kbit/s. Sur les bases des spécifications ISO/IEC 18032 et 14443, le forum NFC a développé un certain nombre de spécifications pour harmoniser et étendre fonctionnellement le champ d'application du NFC.

^(a) NFC : Near Field Communication.

^(b) CCP : Communication en Champ Proche.

^(c) RFID : Radio Frequency Identification ou Identification Radio Fréquence.

Encadré 1 : Le protocole NFC CCP.

La pénétration de tels services sur le marché dépend donc beaucoup de la conversion du parc des TPE au sans contact et également de la pénétration de smartphones NFC.

Avant de décrire plus avant ces services, il nous faut évoquer d'autres tentatives, assez spécifiques, de paiement par smartphone dont les réseaux de distribution sont les moteurs, notamment aux États-Unis, et dont l'objectif est de réduire les reversements qu'impose le paiement par carte bancaire. Un certain nombre d'initiatives ont été déclenchées aux États-Unis par des groupes de distributeurs. Parmi elles on peut citer CurrentC portée par un consortium de distributeurs MCX qui regroupe de grands noms de la distribution nord-américaine dont Walmart. CurrentC ne s'appuie pas sur le réseau des cartes de paiement mais sur ACH⁷ qui joue le rôle de chambre de compensation pour tous les transferts électroniques de fonds effectués sur le territoire des États-Unis. Dans les boutiques, le client utilisant CurrentC doit démarrer une application spécifique qui, en lisant le code QR affiché sur la caisse du commerçant, accède au montant de l'achat. Le smartphone transmet alors un jeton à la plateforme d'une institution financière qui prend en charge l'accès à ACH. Un autre mode de fonctionnement est disponible, notamment pour payer aux stations d'essence : l'application

⁷ ACH : Automated Clearing House

délivre un code sur le smartphone que le client doit entrer sur le clavier de la station pour déclencher le paiement. CurrentC intègre aussi la prise en charge des programmes de fidélité ainsi que le paiement via des bons de réduction émis par les distributeurs. Ce pourrait être un élément important pour que d'autres distributeurs rejoignent le consortium.

CurrentC est actuellement en test à Columbus (Ohio) et le lancement commercial était annoncé pour 2016 (l'application CurrentC est disponible sur les magasins d'application d'Apple et de Google). A la mi-mai 2016, il a été annoncé que son déploiement était retardé sans préciser une nouvelle date. Par rapport à d'autres offres de paiement mobile, CurrentC paraît relativement complexe à utiliser pour le client et son usage est limité au paiement dans les boutiques affiliées au consortium de distributeurs. CurrentC présente toutefois l'avantage d'être indépendant de la pénétration du paiement sans contact chez les commerçants et de la disponibilité de NFC sur le smartphone du client.

Les offres des acteurs de l'Internet

Apple et Google, ainsi que Samsung ont lancé des offres de paiement par mobile s'appuyant sur les réseaux de cartes de paiement. Orange en France a lancé aussi une offre de paiement mobile en 2015. Les offres des premiers s'appuient

La tokenisation

Les vols de données bancaires des clients d'un certain nombre d'acteurs du commerce en ligne ont conduit l'industrie du paiement par carte à édicter de nouvelles règles de sécurité applicables aux vendeurs qui stockent dans leurs systèmes d'information les données relatives aux cartes de leurs clients (numéro de carte, date d'expiration, cryptogramme visuel...) : ces règles connues sous le nom de PCI-DSS^(a) imposent à ceux-ci des points de contrôle qui sont aussi bien techniques que procéduraux et dont le respect est vérifié par des contrôles d'autant plus sévères que le nombre de transactions effectuées par le commerçant est élevé. C'est le renforcement des exigences de sécurité qui a conduit à appliquer à la carte de paiement le concept de tokenisation pratiqué par les informaticiens déjà depuis quelque temps. Elle consiste à remplacer dans les transactions de paiement, les données que l'on veut protéger – numéro de carte, date de validité, cryptogramme visuel – par un jeton (token) associé à une date d'expiration et un cryptogramme visuel : ainsi la plateforme du commerçant ne stocke que pendant l'allocation du jeton les données sensibles de la carte de paiement, ce qui est autorisé par les normes PCI DSS. Le jeton peut être à durée de vie limitée et doit être renouvelé périodiquement ou bien être permanent : dans ce dernier cas, on parle de « tokenisation statique ». Le jeton a lui-même la forme d'un identifiant de carte de paiement. Ainsi l'attaque des plateformes de commerçant en ligne perd notablement de son intérêt. Les entités qui gèrent la création de jeton et qui conservent la correspondance entre celui-ci et les identifiants réels de la carte client (appelées Token Service Provider) sont, bien sûr, soumises aux exigences de sécurité imposées par PCI DSS et doivent notamment assurer une protection forte des données de correspondance entre jeton et numéro de carte. Les grands réseaux de cartes bancaires comme Visa et Mastercard ont ouvert des services de tokenisation aux États-Unis puis en Europe.

Les promoteurs des offres de paiement mobile se sont évidemment intéressés à cette possibilité qui permet de réduire les risques liés au paiement mobile : elle est parfois appliquée en conjonction avec le concept HCE (Host Card Emulation), décrit plus loin.

^(a) PCI DSS : Payment Card Industry Data Security Standard.

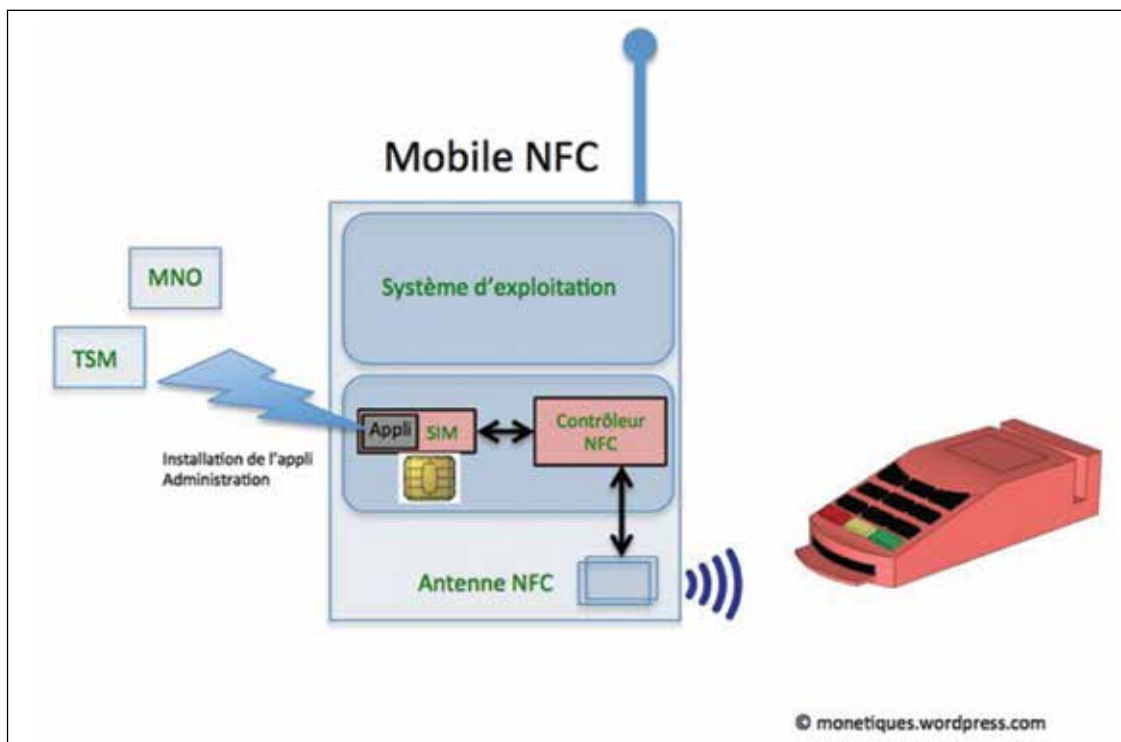


Figure 7 : Le modèle SIM centric – Source site monetiques.wordpress.com.

directement sur le compte de la carte du client alors qu'Orange Cash fait appel à un compte prépayé que le titulaire doit préalablement alimenter à partir de son compte bancaire.

La prise en charge du paiement est assurée dans tous les cas par les réseaux de collecte des transactions par carte. Le terminal mobile doit donc contenir ou avoir accès à un élément sécurisé (SE⁸) comme celui contenu dans la carte de paiement européenne à puce (EMV⁹) : dans celle-ci, cet élément contient des données relatives à la carte (numéro de carte, clés...) qui doivent être protégées contre des accès indiscrets. Dans le cas du paiement mobile par smartphone, ce ne sont pas, en général, les données relatives à la carte du client qui sont utilisées pour les transactions de paiement, mais des données temporaires ou permanentes ayant la même forme que les données des cartes de paiement. Ainsi si le client perd son smartphone, on peut désactiver le paiement mobile sans bloquer l'usage de la carte de paiement du client. Les données bancaires utilisées dans le paiement mobile peuvent être obtenues par tokenisation (voir encadré 2).

Le modèle SIM centric

Dans les terminaux mobiles actuels, la carte SIM qui est fondée sur les mêmes technologies que la carte EMV semble être le lieu naturel où héberger les données bancaires à sécuriser. Ce mode de fonctionnement qu'on appelle "SIM

centric" permet à un terminal de paiement d'accéder via l'interface NFC aux données bancaires contenues dans la carte SIM, de même qu'il peut accéder aux données de la carte EMV. Le principe est que, dès que le contrôleur NFC du smartphone reconnaît une tentative de communication NFC, il route la connexion vers le SE contenu dans la carte SIM. Ce mode de fonctionnement donne une position favorable aux opérateurs mobiles (MNO) car, pour l'heure, ce sont eux qui gèrent et fournissent les cartes SIM de leurs clients. Les MNOs doivent s'appuyer sur des tiers, les TSM¹⁰, non seulement pour éditer les cartes SIM compatibles avec le monde du paiement, mais également pour permettre la gestion du compte du client directement par son smartphone ou assurer d'autres fonctions de gestion spécifiques au service. Le fonctionnement du modèle « SIM centric » est illustré par la figure 7 : au plan de la sécurité, il offre l'avantage de ne pas donner au système d'exploitation du smartphone l'accès aux éléments de sécurité. Mais il est évidemment assez lourd à mettre en œuvre puisqu'il impose au client de se doter d'une carte SIM adaptée au service en plus du chargement d'une application sur son smartphone.

A la mi-2015, la GSMA avait dénombré 67 offres de services de paiement mobile actifs fondés sur un modèle SIM-Centric, promus notamment par des opérateurs mobiles comme Vodafone, Deutsche Telekom et Orange et par des consortiums associant banques et opérateurs comme Enstream au Canada ou bien Valyou en Norvège.

⁸ SE: Secure Element

⁹ EMV: Europay Mastercard Visa

¹⁰ TSM : Trusted Service Manager

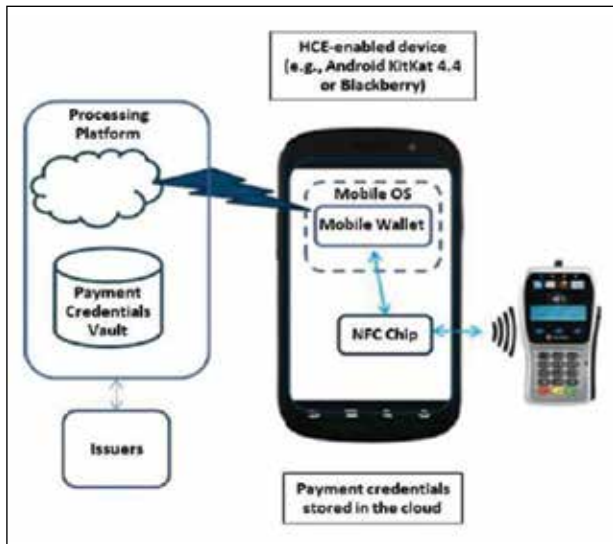


Figure 8 : HCE accès aux données de paiement.
Source : Smart Card Alliance.

Les autres approches

Les acteurs du paiement mobile qui ne sont pas opérateurs, ne disposant pas d'un accès aisé à la carte SIM ont imaginé d'autres approches. La première consiste à créer dans le smartphone l'équivalent du SE : c'est une approche qui n'est accessible qu'aux concepteurs de terminaux. La seconde consiste à utiliser l'émulation de carte hébergée (HCE) décrite ci-dessous.

Émulation de carte hébergée : HCE (Host Card Emulation)

Google a lancé le concept de HCE dans lequel les éléments sécurisés de la carte de paiement ne sont plus stockés dans un élément lié au smartphone, la carte SIM ou bien une

mémoire complémentaire du mobile, mais dans un serveur du cloud. Le contrôleur NFC du smartphone, quand une tentative de connexion NFC est détectée, détermine, en fonction de l'application sollicitant la connexion, si la connexion doit être établie vers un élément sécurisé (SE) interne au smartphone (la carte SIM par exemple) ou bien si elle doit l'être vers le processeur central qui peut alors accéder aux éléments de sécurité du client : ceux-ci peuvent être stockés dans l'application de paiement elle-même ou bien dans une plate-forme externe de haute sécurité. Il est possible pour le smartphone de se connecter périodiquement à cette plate-forme afin de récupérer les éléments de sécurité et les stocker afin qu'elles soient disponibles lors d'un prochain paiement (figure 8).

En couplant cette fonction avec la tokenisation, on se pare contre le risque d'accès frauduleux aux données de paiement du client y compris sur l'interface NFC : seul le jeton est stocké dans le smartphone et est transmis au terminal de paiement.

Le diagramme complet incluant la tokenisation est donné dans la figure 9.

Quelques éléments sur les offres de paiement du marché Apple Pay

Le service Apple Pay a été lancé aux États-Unis en septembre 2014 et en juillet 2015 au Royaume-Uni : c'est un service de porte-monnaie électronique sur iOS, le système d'exploitation de l'iPhone. Il permet de réaliser des paiements via les terminaux de paiement par carte sans contact équipant

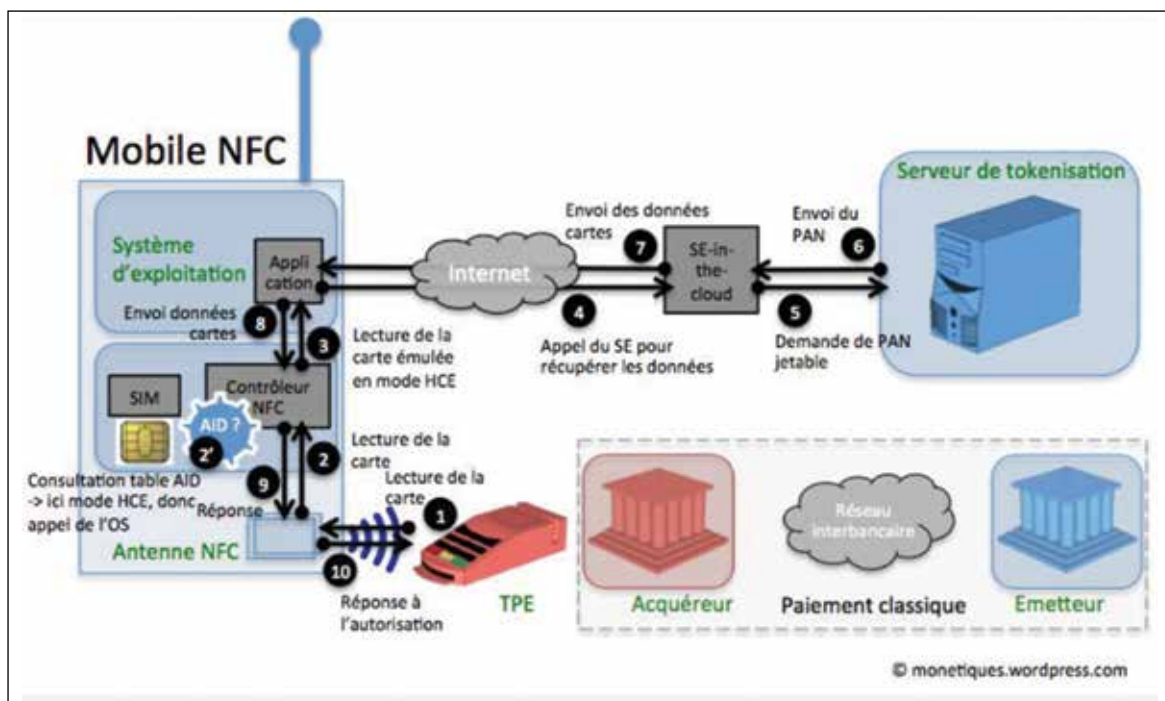


Figure 9 : Principe de HCE avec tokenisation – Source : monetiques.wordpress.com.

les commerçants : en effet, après avoir semblé s'orienter vers l'utilisation de balises (beacons) BLE¹¹, Apple utilise le NFC dont il a équipé ses iPhones à partir de l'iPhone 6. Une application spécifique est à charger dans le smartphone pour pouvoir utiliser le service. Pour l'initialiser, le client photographie sa carte de paiement à laquelle le porte-monnaie est associé et l'iPhone tire de la photo les coordonnées bancaires de la carte et initialise le lien avec le compte du client. Il n'y a pas besoin de disposer d'une carte SIM spécifique : aucun accord n'est donc à trouver avec l'opérateur mobile. L'image de la carte n'est pas conservée dans le terminal. Les données de paiement après tokenisation statique sont stockées dans une puce spécifique de l'iPhone dite "secure element". La sécurité est renforcée grâce au lecteur d'empreinte digitale qui permet au client d'autoriser chaque paiement. Par ailleurs, Apple permet de neutraliser à distance la fonction Apple Pay en cas de perte du terminal.

En termes de modèle d'affaires, Apple a négocié un accord avec les grands réseaux de cartes bancaires et avec un certain nombre de banques qui promeuvent sa solution auprès de leurs clients. Sur le plan financier, Apple aurait obtenu de percevoir une partie du reversement que les commerçants font aux grands réseaux de carte sur chacun des paiements.

Le service a été lancé en Chine en février 2016 en partenariat avec China Union Pay. Le lancement dans le reste de l'Europe fait, semble-t-il, l'objet de discussions avec les acteurs du paiement par carte et la date de lancement devrait être annoncée rapidement.

Android Pay

Le service Google Wallet a été lancé à la fin de 2011 par Google. A l'origine, il permettait de faire des paiements via des TPE NFC et également des transferts d'argent entre comptes Google Wallet et vers des numéros de téléphone ou des adresses mail. Il s'appuie sur un compte bancaire du client.

Les opérateurs mobiles américains, AT&T Verizon et T-Systems ont tenté, par ailleurs, de construire une offre baptisée ISIS qui fut expérimentée en 2013 à Salt Lake City. Renommée SoftCard, la propriété intellectuelle associée à cette offre a été rachetée par Google en 2015 et l'offre a été fermée en mars 2015. Google a intégré cette offre dans une nouvelle offre nommée Android Pay lancée la même année.

Android Pay est une application opérationnelle dans les terminaux utilisant le système d'exploitation Android (version 4.4 et suivantes) : elle a été lancée aux États-Unis en septembre 2015 et permet aux clients d'un certain nombre de réseaux de paiement et de banques de payer leurs achats chez les commerçants avec leur terminal Android à condition que ces derniers acceptent le paiement sans contact. Après

¹¹ BLE: Bluetooth Low Energy

le lancement d'Android Pay, Google Wallet a été restreint aux seuls transferts de fonds entre particuliers.

L'initialisation d'Android Pay peut être effectuée soit, comme chez Apple, en prenant une photographie de sa carte, soit en composant le numéro de carte sur le terminal. Ces données sont tokenisées et stockées dans un serveur sécurisé suivant les principes de HCE. Android Pay permet également de gérer les bons et coupons de fidélité émis par les commerçants et peut être sollicité comme moyen de paiement dans les applications de vente propres aux commerçants (in-app payment). Google a annoncé que le service devrait être disponible au Royaume-Uni en 2016.

Aux États-Unis, d'après les informations disponibles, Android Pay ne prélève aucune commission sur les paiements qui sont faits par son intermédiaire.

Samsung Pay

Samsung Pay a été lancé aux États-Unis par le fournisseur de smartphones Samsung en septembre 2015 après avoir été lancé en Corée du Sud un mois avant. Il s'appuie sur le réseau de paiement par cartes et pour assurer un démarrage le plus rapide possible, Samsung fait appel non seulement au NFC mais également à une technique propre appelée Magnetic Secure Transmission (MST) qui permet à ses terminaux d'interagir avec les lecteurs de carte magnétique qui équipent tous les terminaux de paiement notamment aux États-Unis. Ceci devrait à court terme constituer un avantage concurrentiel pour Samsung. Le service est utilisable par les clients de banques ayant passé un accord avec Samsung Pay. Mais il n'est accessible qu'à des générations de terminaux relativement récentes (Galaxy S6 par exemple). Au plan technique il fait appel aux techniques HCE et tokenisation.

Samsung Pay permet de gérer des bons et des cartes de fidélité et également de retirer de l'argent dans des distributeurs de billets.

Les autres offres

Les offres des grands acteurs de l'Internet ont un peu éclipsé celles mises en place par les banques. En France la plupart des grandes banques offrent un service de paiement mobile : BNP, SG, LBP, CM, CIC... En général il s'agit d'un service fourni en partenariat avec un ou plusieurs opérateurs mobiles selon un modèle SIM centric et seulement utilisable avec des smartphones Android, pris en général dans une liste limitée.

Orange a lancé en fin 2015 le service Orange Cash en France : il tire profit de l'expérimentation menée dans un certain nombre de villes françaises pendant plus d'un an. Bien qu'utilisant les réseaux des cartes de paiement, il ne s'appuie pas directement sur le compte bancaire du client mais sur un compte prépayé ouvert à cette occasion que le client doit alimenter. Le service n'est accessible que par des terminaux

opérant sous Android ou Windowsphone. Il offre la possibilité d'effectuer des paiements sur les TPE sans contact et également de transférer de l'argent de compte à compte. Au plan technique le modèle retenu est le modèle SIM centric : pour l'utiliser le client doit demander à son opérateur une carte SIM capable d'être utilisée avec l'interface NFC. Les données bancaires contenues dans la carte SIM ne correspondent pas à la carte bancaire du client mais à celles du compte prépayé qui est ouvert à la souscription du service pour le compte du client. Deux partenaires interviennent dans la fourniture du service, Wirecard AG qui gère les comptes prépayés et les cartes associées et Oberthur Technologies qui assure le rôle de tiers de confiance. Le montant de chaque transaction ainsi que les montants mensuels et annuels des versements sont plafonnés. Par exemple celui d'une transaction ne peut pas dépasser 300 €. Les versements faits pour alimenter le compte prépayé peuvent ou non, suivant le moyen utilisé, faire l'objet de frais prélevés par Orange. Enfin, Orange Cash peut être utilisé pour des paiements en ligne : pour assurer la sécurité, Orange Cash fournit alors à l'acheteur des identifiants de carte de paiement valables pour une durée limitée. Fin mars 2016, Orange annonçait avoir ouvert 145 000 comptes depuis octobre 2015 et avoir effectué en moyenne 15 000 transactions par semaine.

Patrice Collet est ancien élève de l'École Polytechnique et ingénieur général des télécommunications. Sa carrière l'a conduit de la recherche et développement au CNET qui était alors le centre de recherches de la Direction générale des télécommunications à la Direction générale de France Télécom où il a eu la responsabilité de l'architecture du réseau fixe et son évolution.

Conclusion

Le domaine du paiement mobile est en pleine effervescence. Dans les pays faiblement bancarisés, il connaît un très fort développement, notamment en Afrique. Si les différents acteurs parviennent à rendre leurs offres interopérables entre elles et avec les banques, le paiement mobile devrait trouver une place importante dans le système financier de ces pays. La situation est probablement plus incertaine dans les pays fortement bancarisés : de nombreux acteurs tentent de prendre pied sur ce marché déjà bien pourvu avec des offres très proches les unes des autres au plan fonctionnel. Les conditions sont difficiles : le marché est très segmenté, selon les systèmes d'exploitation des smartphones, selon les accords conclus entre acteurs et banques et selon les liens qui peuvent préexister entre clients et acteurs candidats à la fourniture de services de paiement mobile. Par ailleurs, la vitesse de déploiement de TPE sans contact

pourrait influencer l'adoption du paiement mobile. Enfin, la différenciation par rapport au paiement par carte traditionnelle ou sans contact n'est pas évidente en termes de contenu du service : c'est probablement la facilité d'emploi qui devrait constituer le facteur décisif pour le succès des offres de paiement mobile. Mais nous ne sommes qu'au début de l'histoire : les services n'ont commencé dans les pays développés à être offerts que vers 2014, 2015 ! ■