BREAKTHROUGHS IN THE EUROPEAN MOBILE PAYMENT MARKET

Atos Origin™

CONSULTING > SOLUTIONS > OUTSOURCING

White Paper

Written by Laurent Bailly and Bernard Van der Lande

Contents

Executive Summary

Mobile payment has yet to fulfil its potential. The time is now right for the mobile phone to step up and become an everyday, convenient payment method.

Technological advances, such as the new generation of mobile devices, the emergence of contactless payments, IP everywhere and 3G, coupled with the adoption of the new legal framework for payments and the creation of the Single Euro Payment Area (SEPA) means the future for mobile payment has never been more promising.

The future of mobile payment will likely belong to contactless technology
Still in its pilot stage in Europe, Near Field Communication (NFC) contactless payment is a huge opportunity for proximity payment, as it addresses both the cash and card payment markets.

Collaboration between stakeholders is key
Standardisation and business model issues need to be resolved through strong collaboration between mobile operators, banks and retailers, so as to limit the number of rival solutions, which would inhibit mobile contactless payment adoption.

Mobile remote payment will prosper in the short term
The technology for mobile remote payment is already mature with opportunities beyond mobile content, such as pre-paid top-up and electronic bill payment. For mobile operators, it provides new opportunities to drive additional revenue via mobile shopping and payment traffic. The market is also accessible to banks and new entrants. In fact, with Paypal Mobile and Google Checkout arriving on mobile phones, Internet giants already represent a common threat to the incumbent telecoms operators and banks.

Mobile remote and proximity payment are converging
Mobile remote payment technology and NFC proximity technology will be soon be complementary. A good example of this is m-ticketing: using a remote m-payment service, users can buy and download an m-ticket on their mobile phone, before swiping the phone over an NFC-enabled gate.

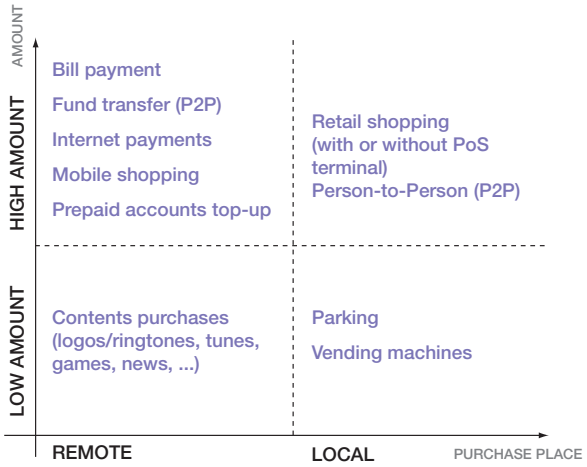
INTRODUCTION TO MOBILE PAYMENT

What is mobile payment?

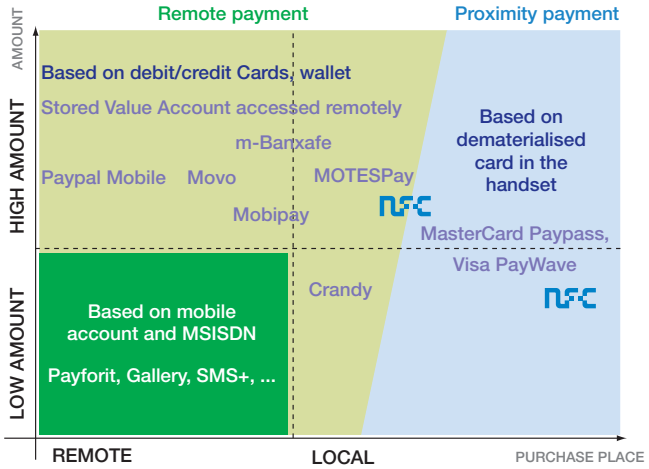
For the purposes of this document, mobile payment is defined as:

Payment for products or services between two parties for which a mobile device, such as a mobile phone, plays a key role in the realisation of the payment.

The mobile payment market can be segmented into categories and into a combination of micro/macro-payment and remote/local mobile payment situations:



Atos Origin differentiates between remote and proximity payment:



Mobile remote payment

Remote payment covers payments that take place online, in which the mobile phone is used as a device to authenticate personal information stored remotely. But remote payment solutions can also be used for transactions that take place locally, such as face-to-face and vending machine transactions.

In the case of low-value purchases, such as ring tones or mobile content, mobile operators have already developed solutions based on the phone number (MSISDN) for user authentication. The transaction is recorded on the user's mobile phone bill, and the merchant is reimbursed by the mobile operator. This is also called 'billing-on-behalf-of', and is mainly used for small transactions, as the level of security is low (network authentication only). This is already common in most European countries.

For higher-value purchases, a mobile payment transaction can be processed in various ways:

> Credit/debit card – payment is processed, for example, by entering card information on a secured WAP interface.
> Wallet / stored value account – card payment can also be processed indirectly using a wallet, which stores a user's key information, such as the card number and expiration date, bank account details etc. This is particularly useful for WAP mobile shopping. One step further, a stored value account can be offered to the customer, which can be topped up using traditional payment methods, such as debit cards and credit transfer. Security is an important issue, and PIN code for authentication is required. Encryption for transport – over WAP, IVR, SMS, USSD – is a plus. Activation of the customer and enabling the link between the mobile MSISDN and the card number is also crucial to ensure reliability.

Atos Origin believes that this area represents significant opportunities today.

Mobile proximity payment

Proximity payment refers generally to contactless payments in which the payment credential is stored in the mobile and is exchanged over the air, based on NFC technology, with a dedicated and compatible payment terminal. In other words, the mobile acts as a contactless payment card, thus becoming a new payment form factor.

However, contactless payment could also be used remotely, for example, to make an online purchase by swiping the mobile over a contactless NFC reader plugged in to the PC.

Mobile contactless payment is likely to have a bright future in shops and at vending machines.

Finally, it is worth noting that the divide between remote and proximity payment is narrowing. More detail on the concept of converged mobile payment can be found later in this document.

Near Field Communication

Mobile proximity payment relies on contactless technology called near field communication (NFC).

NFC is an easy-to-use, short-range wireless technology. It is quickly becoming the technology of choice for operators, handset manufacturers, credit card companies and public transport operators around the world for contactless transactions, including secure payment and ticketing, because of its strong consumer appeal and ease of use.

NFC has been jointly developed by Philips and Nokia. NFC is a combination of contactless identification and interconnection technologies that enables secure short-range communication between electronic devices, such as mobile phones, PDAs, computers and payments terminals via a fast and easy wireless connection. NFC operates in the 13.56 MHz frequency range, over a distance of, typically, a few centimeters and combines the functions of a contactless reader, a contactless card and peer-to-peer functionality on a single chip. It is an open interface platform that allows fast and automatic set-up of wireless networks, which also works as a virtual connector for existing cellular, Bluetooth and wireless 802.11 devices. NFC is compatible with Sony's FeliCa card and the broadly established contactless smart card infrastructure based on ISO 14443 A, which is used in NXP's MIFARE technology. www.nfc-forum.org

WHY THE TIME IS RIGHT FOR MOBILE PAYMENT

Since the beginning of the 21st century, there have been a lot of mobile payment initiatives. Some, such as DualSlot handsets and Simpay, were not successful because they lacked a clear business model and/or infrastructure costs.

Technological advances

Today, the market has seen a number of changes that make the mobile payment proposition more attractive and more realistic than ever before:

> Contactless technology is now a reality and is already used in millions of cards worldwide, such as debit/credit cards, underground/subway tickets, access devices, and so on. Making it available on mobile phones is the obvious next step. Successes in Asia have shown that there is a strong business case for contactless mobile payment.

> Network capacities and device capabilities have increased substantially; and the adoption rate of mobile phones has reached almost saturation point in Europe. Today, mobile phones are an integral part of daily life for many people and have joined keys and wallets as 'must have' items before leaving the home.

The impact of regulation

The creation of the Single Euro Payment Area (SEPA) in 2000 and the easing of restrictions on payment operators will improve the chances of success for mobile payment across Europe.

New entrants to the payment market, without having the status of a traditional credit institution (as defined in the European directive 2000/12/CE), will be able to act either as:

> Electronic money issuer – the entrant must have an electronic money- issuer license, defined by directive 2000/46/CE, allowing it to manage low-value payments, based on an online stored-value account.

> Payment Service Provider (PSP) – the entrant must have the status of a Payment Institution (PI), as defined in article 6 of the European directive on payment services in the internal market, adopted in April 2007.

Specifically, this directive allows new players (mobile operators, department stores, etc) to be recognised as PSPs, and operate in direct competition with traditional financial/credit institutions, provided they comply with the requirements set out in the directive. They will be able to offer:

> Cash deposits
> Cash withdrawals
> Direct debits
> Credit transfers
> Payments initiated by a card or a similar device
> Credit (for a maximum 12 month period).

Many competitors already own electronic money-issuer licenses in Europe, from internet giants like Paypal and Google, to start-ups like Crandy, Luup or Tunz.

Some telecom operators already own a banking license (Mobilkom in Austria, for example) have a subsidiary with financial status, or have built partnerships with PSPs or banks.

SEPA will increase the flexibility to perform credit transfer and bank card payments throughout Europe, and will build on this by internalising mobile payment.

SEPA may also have a huge impact on payment tools that are used in association with the mobile phone: credit transfer could be an alternative to traditional credit/debit card schemes, as mobile phone technology is already standardised throughout Europe.

MOBILE REMOTE PAYMENT

Outlook and opportunities for mobile remote payment

Payment can be made either at the micro or macro level; each level requires very different technology and levels of security.

Mobile remote micro-payment
Micro-payment (payments worth €10 or less) for goods and services, such as ring tones and games, is already a mature market in most European countries. They are provided by mobile operators, with payment being made mostly via premium SMS/WAP using mobile operators' billing infrastructures. Such micro-payments have proved to be an extremely lucrative source of revenue.

Since payment amounts are low and the merchant's fee for mobile content relatively high, mobile operators have accepted the payment risk, based on their basic authentication of the user and their billing systems, without any collaboration with the banks for online authorisation.

New payment schemes have appeared either proprietary to one mobile operator (Orange World, Vodafone Live!, iMode) or are the result of collaboration between mobile operators.

One of them is UK-based Payforit, which allows mobile phone users to purchase low-value goods and services from the internet and charge them to their mobile phone. Under the Payforit scheme, mobile internet billing requests are no longer handled by individual mobile service providers, but by a trusted party, known as an 'Accredited Payment Intermediary'. Similarly, Gallery in France is a multi-operator scheme that enables the purchase of content via a WAP portal.

On an international level, however, there has been less success. Simpay was supposed to provide a single platform to deal with the routing, clearing and settling of cross-border payments made with mobile phones.

Before its collapse in June 2005 because of the exit of T-Mobile, one of its four founding members, Simpay was considered a genuine threat to card issuers and card schemes. One problem with Simpay was the high cost of its infrastructure, especially when offset against the value the system would add. The German company withdrew from Simpay in favour of furthering the payment systems it developed on its own. The collapse of Simpay further underlined the need for cross-industry involvement in a mobile payment solution.

Atos Origin believes that in the future competition in the Internet and mobile content micro-payment space will increase. The introduction of new payment solutions could bypass mobile operators' 'billing-on-behalf-of' systems, and instead will be based on stored-value accounts, with lower fees for merchants.

Beyond mobile content and services, initiatives have appeared across Europe allowing subscribers to pay for parking at vending machines and for bus rides. Most use SMS to order the product/service, and in the case of bus rides use it as proof of purchase.

Some mobile operators agree to bill those items on their pre/post-paid accounts, but others are reluctant to do so because of the lower merchants' fees.

A typical m-parking scenario sees a customer, upon arrival at the airport, send a formatted SMS containing his car registration number and the parking area number. The parking stewards are equipped with PDAs connected to a server. By typing the car registration number into the PDA, the steward can verify if the car is appropriately registered. The user is then billed via the mobile operator, or the user's bank or stored value account is debited.

There are a number of different initiatives around m-parking; such as easy-park, mpark, parkline and Crandy, which have been developed in collaboration with parking device manufacturers in several cities throughout Europe.

Mobile remote macro payment
For remote macro payments, the mobile is linked to a payment card (credit/debit card) or an account (bank account and/or store account) via an activation/ enrolment process and is used afterwards as an authenticator of remotely-stored information.
There are various opportunities for mobile remote macro payments:

Topping-up a mobile pre-paid account – this is done via the handset, meaning customers do not need anymore to go to the shop to purchase a voucher. For mobile operators, this is a far less expensive topping-up method than scratch cards and represents huge cost savings.

Mobile shopping – whereby the mobile phone is used as a shopping and payment channel. Shopping channels could be based on IVR, SMS or WAP/iMode.

Access to the mobile store can be facilitated by tag reading, whereby the user swipes the mobile phone across a tag (printed on a poster or in a magazine) that links them to a website to purchase a product.

There are two kinds of tag:
> ***Bar code tag*** – a typical scenario would see the user scan the bar-code near his favourite product in a magazine, using his mobile phone embedded camera. He is then redirected to the related product on the merchant's WAP site, where he can get more information on it and purchase it.

> ***NFC tag*** – the same principle as the bar code tag, but the NFC tag is read by the NFC-enabled mobile phone.

Ticketing applications in which dematerialised tickets are ordered, paid for and delivered on the mobile (by MMS containing a bar code or in an NFC-transport application) have been piloted by some European railway companies (SNCF Tikefone, Deutsche Bahn).

Although the above are emerging opportunities with limited penetration, Atos Origin believes that mobile shopping will become significant in the near future, thanks largely to two key enablers:

> Tag reading, as it makes access to the product or service very simple, which will encourage impulse buys

> Physical ticket dematerialisation, as it enables new services to be delivered over the air i.e. m-tickets and m-coupons.

Mobile banking: the option to sell/buy stock, conduct credit transfers, check bank balances, or pay bills via a mobile handset. Various market surveys reveal that there is much consumer interest in the possibility of mobile banking.

Some European banks have already started using the GSM channel to conduct banking operations and have enjoyed some success.

Bill payment: SMS bill delivery and payment has already been proposed by some mobile operators and utility companies. Atos Origin believes this could represent a significant business opportunity, provided such projects are developed with convenience for the user firmly in mind.

Internet shopping: via a PC, whereby a user can authenticate their transaction via their mobile handset rather than having to enter their credit card details.
There is a still a significant number of consumers that do not feel comfortable entering credit cards details online, for whom mobile authentication could be an acceptable alternative.

The mobile device could also be used as an authentication method for 3D-secure card payments online. In this case, the user still enters their card details via the Internet and validates the transaction on their mobile phone. Caixamovil has launched a service to process on a mobile phone the 3D-secure authentication of a card internet payment.
Atos Origin believes the opportunity to use the mobile handset for internet payments will grow exponentially in the near future because of the liability shift from the acquiring side to the issuing side in 3D-secure card payments. This means that the banks are responsible for the fraud generated by the cards they issue, and will be more and more reluctant to authorise payments that have not been authenticated.

P2P: (person to person) refers to payment between two persons via their GSM. The success of P2P on the internet is largely driven by online auctions; the challenge for mobile P2P is to find an equivalent application. mPOS or international fund transfer could be that one:

mPOS: refers to a specific case of P2P in which the mobile payment service is marketed to professionals and to low-segment mobile merchants without point-of-sale (POS) payment terminals, for which mobile payment could prove a cheaper alternative to electronic payment terminals.

In Belgium alone, surveys show that there is the potential to target 200,000 professionals, which represents 1.5 billion cash transactions. Therefore, the opportunity across Europe is huge.

Against this backdrop, Belgian banks and telecoms companies have decided to address this market by offering a mobile electronic payment solution without fixed costs. The merchant pays only a fixed fee for each transaction.

The merchant initiates the transaction via a SIM toolkit menu entry in his mobile device, entering the amount due and the customer's phone or reference number. The customer then receives a signature request on his mobile handset and validates it by entering his PIN. Both receive a confirmation of the transaction via SMS. Transactions are performed directly by debiting the customer's bank card and crediting the merchant account while, payment costs – including communication costs – are billed by the telecom operators using the SMS premium infrastructure.

The acquiring process for merchants wishing to take advantage of this solution is simple – no paper contract, quick and free registration via the Internet – to ensure operational resources are minimised. The solution is ideal for small businesses and independent operators (doctors, dentists, architects, accountants, plumbers, electricians, delivery companies, taxi drivers etc).

International fund transfer for migrant communities: another potentially promising application for P2P mobile payment services is the capability to send money abroad.

With an estimated 191 million migrant workers around the world, and with the business potential for international remittance of 257 billion USD in 2005 (according to the UN and the World Bank respectively), international fund transfers via mobile phone represent a significant opportunity for mobile operators across Europe.

The Mobile Money Transfer mechanism endorsed recently by the GSM Association and Mastercard could soon lead to a faster development of operator-driven mobile fund transfer systems world wide.

An additional new opportunity for mobile operators is to bring financial services to developing countries, where the number of 'unbanked' (or underbanked') people with mobile phones is much higher than the banked population. Vodafone's M-Pesa in Kenya is a good example of those emerging opportunities, enabling mobile subscribers to deposit or withdraw cash at a branch of the mobile operator, top-up their prepaid account and transfer money to another customer using their mobile phone.

Existing macro payment initiatives

Different initiatives have already been launched in remote macro-payment areas, either by Internet payment providers, such as Paypal Mobile or Google Checkout Mobile; or by new electronic money issuers such as Crandy, originally based in Germany, Luup in the Nordic countries, Tunz in Belgium and Mobile2Pay in the Netherlands. Others have been initiated by banks, such as Paybox in Germany and Austria and MOVO (Caisse d'Epargne) in France; and some have been collaborations between banks and mobile operators – Mobipay in Spain and mBanxafe in Belgium, for example.

These initiatives usually focus on a limited number of m-payment opportunities. For example, Paypal mobile focused on P2P payments and mobile shopping via SMS; Crandy focused on vending and parking solutions; MOVO focused on P2P and credit transfer payments; while Luup and Tunz concentrated on internet payments.

Mobipay and mBanxafe try to cover a broader range of remote macro payment opportunities.

Many mobile operators have developed specific solutions dedicated to topping-up prepaid accounts.

Security issues

Typically, security levels relating to mobile payment do not match the standards required by a bank or card issuer in order for them to assume the risk of payment. There is also the common end-user perception that many mobile payment solutions are fraught with insecurities.

Authentication is usually based on the customer's MSISDN and, eventually, a PIN code to validate the transaction. This is provided by SMS either during the initiation of the transaction or during an Interactive Voice Response session generated by the payment server after the initiation of the transaction. This is the case for most of the current solutions e.g. Paypal mobile, MOVO, Paybox, Crandy.

In the case of Mobipay, security is based on the USSD communication protocol, which is controlled by the mobile operators.

The PIN is requested and transported by USSD. This makes the solution more secure, provided that the USSD servers are processed by a Trusted Party. A joint venture has been formed between the Spanish mobile operators and many of the Spanish banks that manage the solution.

Authentication can also be based on hardware with a secure element incorporated into the mobile device. This is the case in Belgium with mobile banxafe. An agreement between telecoms companies and banks has seen a specific signature applet hosted on every new SIM card issued. This secure technology layer means mobile payments follow the same standards of security as chip card payments, and are considered as secure as card-present transactions. Replacing the existing SIM cards should take approximately four years. Currently, 25% of Belgian SIM cards are equipped with this technology.

The presence of a specific applet on the SIM maximises convenience for the user, as it can be used for a variety of m-payment applications.

Activation/registration – a hurdle for mobile payment adoption

Activation consists of linking payment credentials to the mobile phone. The activation/registration process is a major obstacle for the success of any macro mobile payment solution.

This process should be made as easy as possible for the end user but it must also be secure. The payment service provider must ensure that the payment information provided by the user during the registration process actually belongs to them, otherwise the transaction will not be secure.

In this context, it is important to develop a single solution that allows the various stakeholders to pursue the business opportunities available. A single registration would allow customers to benefit from all of the services on offer.

With many solutions, registration takes place on the mobile payment service provider's website. The customer fills in a form and provides his personal details as well as card or account information.
In order to verify the payment information provided, the mobile PSP could process an initial payment, for a minimal amount, with a reference that the customer will receive via his account/card statements. He will then have to re-enter this reference on the mobile PSP in order to complete the registration process. This loop is used to prove that he is the owner of the payment information he provides.

In alternative solutions, the customer has to sign a contract and has to show the cards he wants to link with his GSM. Of course, this manual process is much more time-intensive.

In Belgium, accounts are activated via the ATM network and the POS terminals in the telecom shops. Special applications on ATM and POS terminals have been developed, allowing customers to insert their bank card and enter their mobile phone number before keying the bankcard PIN to validate the link.

In future, activation could be conducted using the same strong authentication tools that bank are deploying for web banking throughout Europe.

The business case for mobile remote payment

The business case for mobile remote payment will differ depending on the roles and contributions of the different stakeholders – be they banks, mobile operators or new players.

In the micro payment area for content, mobile operators have already generated significant value by creating solutions themselves, based on their existing billing systems. As the margins are usually very high, competition has begun to appear from new players that have applied for an electronic money issuer license. Financial institutions are very passive in this area because of a lack of experience and the inadequacy of their traditional payment methods i.e. debit/credit cards, in this market.

With regard to the macro payment area, there have been few significant developments by mobile operators or financial institutions. New players, such as Crandy or Paypal, have started to market their own solutions to provide mobile payment, in which the role of the mobile operators is very limited.

The business case for mobile operators

Atos Origin believes that mobile operators can build a strong case for remote mobile payment by proposing a single, secure and convenient solution. Indeed, mobile remote payment generate traffic both at the point of purchase and at the point of payment authentication, while providing an enjoyable user experience. Remote mobile payment could also offer significantly lower pre-pay top-up costs compared with traditional top-up scratch cards and e-vouchers.

Collaboration with at least one financial institution would enhance the business case for mobile operators, as they have little experience in risk management for high-value payments. Any operator aligning itself with a bank or similar organisation would increase customer confidence, as customers often trust a financial institution more than a mobile operator when it comes to security.

In addition, mobile operators have control over their networks, SIM, handsets and customers base, allowing them to maximise their role and share of revenues in the m-payment value chain.

Roles for the mobile operator in the remote payment scenario could include:

> Hosting a secure (bank) signature application in the SIM, and provide specific menus or interface development (Java based)
> Act as an authentication for third parties, such as banks. This role, however, will usually be sub-contracted to a trusted third-party processor that complies with security requirements of the stakeholders
> Transport between the handset and the mobile payment service provider
> Communicating new payment services to end-users and merchants
> In collaboration with the mobile payment service provider, provide registration and acquiring services for customers and merchants
> Provide the mobile payment service provider with use of its billing infrastructure

The combination of the roles means there is significant potential for mobile operators to claim their share of the mobile payment transaction.

The business case for the banks

The business case for the financial institutions will rest on a new generation of electronic transactions. These transactions are based on their traditional payment methods, on which they will be able to claim acquisition and interchange fees. Additionally, mobile devices could offer them a new, convenient and secure banking channel.

Mobile remote payment – key factors for success

User convenience
The benefits to end-users are clear – being able to pay for goods and services via mobiles devices will give consumers enormous freedom. Of course, the shopping phase will feel different, as remote mobile payment could be applied to broad range of services and scenarios (face-to-face payments, internet payments). However, it is important to provide a similar user experience for the validation of the mobile transaction.

Perception of security and trust
It is important to adopt the appropriate level of security, which will allow organisations to take full advantage of the business opportunities while at the same time giving end users confidence in the security of the service.

End users must trust the payment service provider behind the solution. Various market surveys already indicate that financial institutions are seen as more trustworthy than other organisations so, in this context, a collaborative solution could be a progressive option.

Registration / activation process
As discussed earlier, the registration phase is a major hurdle for any mobile payment solution.

The process should be free, simple and secure. It is important that the same process opens the doors to all business opportunities. One user could decide to register for one application and later discover that he can also directly benefit from other applications without a new registration.

Definition of right business models
We have already stressed the fact that collaboration between mobile operators and financial institutions would be mutually beneficial. Both would be able to re-use their existing infrastructures in the development of new payment solutions, and they will be able to share the risk and the costs of launching them.

It is important, therefore, that all of the organisations involved in developing a solution devise a business model for each of the business opportunities they will be pursuing.

The business model should outline what each stakeholder should be paid – in accordance with their investment and how much value their role adds to the initiative. Various market surveys in Belgium show that end users may also be prepared to accept paying, at least in part, for m-payment services.

Local-level standardisation
Currently there are no standards in existence for remote mobile payment and most of the existing initiatives have been developed in a three-box model. This means the customer and the merchant must be registered on the same mobile payment platform in order for a transaction to be made.

This is sufficient to address some of the services outlined earlier in this paper, such as as the prepaid account top-up, but not enough for others. The essence of a payment instrument is its universality. Standardisation must be achieved at least at country level to take advantage of most of the opportunities that remote mobile payment offers. This can be achieved by the adoption of the same technical platform at national level by the different stakeholders, or by defining a common ‘standard technical interface’ and business model, including interchange rules.

What will certainly be necessary will be the re-routing of the end user to his mobile payment provider for validation of the transaction, initiated by a merchant registered with another mobile payment provider. The 3D-secure protocol promoted by VISA and Mastercard for secure Internet transactions will definitely be a source of inspiration for the standardisation of remote mobile payment.

Communication and marketing efforts
Last but not least, one of the most critical factors for success is a compelling communications and marketing plan to generate interest in any new payment solution.

Changing customer habits is no mean feat and requires significant investment – even if the new solution addresses consumer need and could make their lives easier.

With such considerable investment costs in mind, collaboration between mobile operators and financial institutions is even more important.

MOBILE PROXIMITY PAYMENT

Contactless market outlook

Lying in most wallets and purses today are credit and debit cards, loyalty cards, travel tickets/cards, health cards – and all from different issuers with their own brands and logos. The future of the mobile phone is to become a wallet, on which users will be able to store several dematerialised eCards from different issuers with their own brand and logos.

Mobile contactless technology enables not only the dematerialisation of a contact card into the handset, but it also adds value to the end-user's experience by adding interactivity via a screen and a keypad. Additionally, it gives access to related online services, reached via the mobile data network (GPRS/UMTS, SMS/MMS), and through mobile specific functions, such as geo-location.

Mobile contactless technology provides flexibility for service providers (banks, retailers, transport companies) to update over-the-air (OTA) their contactless application (payment, loyalty, ticket; e-money).

Contactless technology is already a reality

There are millions of cards in circulation all around the globe, including credit cards, electronic purses, access devices, travel and event tickets, and many more. In the transport sector, contactless cards for travel tickets are a reality. Obvious examples include "Navigo" in Paris for RATP, and "Oyster" in London, which has issued more than 10 million contactless cards since its launch in 2003.

In the payment sector, Visa, MasterCard and Amex have already established their own contactless protocols – PayWave, PayPass and ExpressPay respectively. According to MasterCard, there are now 51 million merchant locations worldwide that accept PayPass payments. In the UK, Visa announced the launch of an NFC card in autumn 2007 for small transactions of less than £10, where no PIN code will be required.

We will soon witness the launch of the multi-services contactless card. In the UK, a deal between Barclays and Transys has put Barclaycard and Oyster into single contactless card, allowing passengers using public transport in London to make quick, contact-free, cashless payments and travel around the Capital using one card.

Integrating contactless technology in to the mobile world

Asia is the first region in the world to understand the tremendous benefits of contactless payments and is leading the global market with Korea and Japan following closely behind. In Japan, more than 30% of NTT Docomo mobile handsets are contactless, enabled with Felica (Sony technology), and have integrated the ePurse application, EDY (Euro Dollar Yen), and the eTicket Suica (Super Urban Intelligent Card)/Japan Railway & Japan Airlines since 2004.

In Europe, the pilot phase for mobile contactless payments began in 2006 with payment, transport and loyalty applications. As of May 2007, the main European NFC experiments (not exhaustive) are:

> In Germany, Nokia, Philips and Vodafone conducted a ten month experiment in Hanau. The NFC mobile phone was used as a travel ticket and loyalty card for the public transport authority, the Rhein-Main-Verkehrsverbund.

> France has seen a number of initiatives from both the banking and mobile operator sectors:
- Orange launched the "NFC Caen" pilot with Cofinoga and Vinci Park in Caen in 2005-2006, which was a multi-services contactless trial, for parking and private payments
- Credit Mutuel launched a payment trial with Mastercard in late 2006 with Sagem and Gemalto.
- RATP began a mobile contactless ticketing trial with Bouygues at the end of 2006, putting the Navigo contactless card into the handset
- MOTESpay, launched in 2007, is an NFC payment pilot that involves French banks Caisse d'Epargne and Banques Populaires, NXP, Atos Worldline, Caen University, the Groupement des Cartes Bancaires (French national card scheme) in Caen
- P€gasus is a 2007 joint initiative between the french mobile operators, Visa, Mastercard and the main french banks to experiment with universal contactless payment in a collaborative approach.

> In the Netherlands, JCB, the Asia-based global payment brand, launched in September 2006 a contactless mobile payment pilot that targeted approximately 100 card members located in Amsterdam, and merchants in and around the city's World Trade Center. Also unveiled in 2007 was a new pilot from Rabobank, Orange and Banksys for payment and loyalty.

The business case for proximity payment

The NFC eco-system is extremely complex, with a lot of different stakeholders aiming to take their share of the revenue. Mobile contactless payment is one application among many. A global overview of the main stakeholders in the NFC eco-system, and the role they could play in the near future, can be found below:

Mobile operators: mobile contactless payment provides a means to add value to their commercial offering with new services that will, potentially, allow them to increase their Average Revenue Per User (ARPU) thanks to new revenue that could come from other different sources, such as:

> Transaction fees
> Renting space on the handset or SIM card
> Data traffic (mainly from over-the-air downloads)
> Managing service providers' applications
> Providing financial services (see "Disruptive strategies could emerge" section, to follow)

Mobile contactless will also reduce churn, as when customers get all these new services on their mobile phone, moving to another Mobile Network Operator (MNO) must be carefully though through.

Banks: mobile contactless payment will reduce cash handling (for micro-payment) and plastic card issuing costs (for macro-payment). But it also offers the opportunity to offer more interactive services, linked to online banking services, like providing credit at the point of purchase.

Merchants: contactless payment helps to speed up transaction time as well as generating more transactions, especially for micro-payments, and also reduces cash handling.

A Mastercard study showed increased spending of 19% per PayPass account, compared with accounts for which consumers have only been issued tradtitional cards. It also indicated consumers with PayPass cards or fobs are using them 29% more often than those with non-PayPass cards, and that the average transaction size of a PayPass payment is smaller than for transactions made with magnetic strip cards, replacing cash as a means to make smaller purchases.

Mobile contactless payment could also reveal new opportunities for loyalty programs, especially with an eCoupon that could be stored in the handset and consumed at the checkout by swiping the phone.

Transport operators: many transport operators already offer contactless cards for use on their network. As the infrastructure is already deployed, the transport sector is the preferred one to launch mobile contactless services on a large scale. Putting an eTicket into the mobile phone helps increase customer satisfaction, making daily travel easier. And replacing tickets and contactless cards with contactless applications that can be downloaded to the handset will significantly reduce ticket issuing costs.

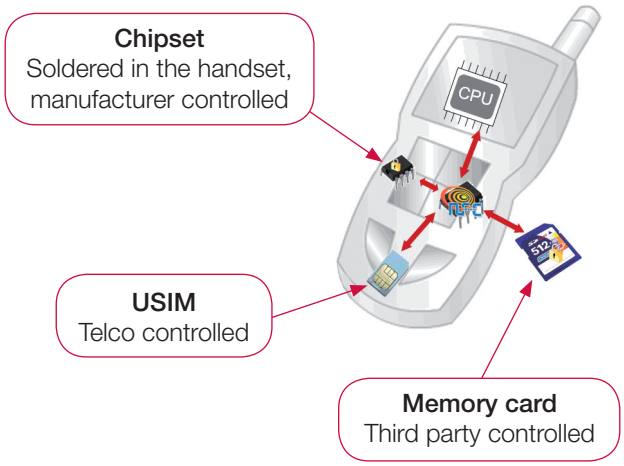
Ticket vendors: event organisers, museums and cinemas that sell tickets via the Internet or over a mobile network can now send tickets directly to the purchaser via their NFC-enabled handset, making the purchasing of tickets much faster and possible from any location. Additionally, purchasers can be fast tracked into the event when they arrive, rather than waiting in queues. Event organisers can also use these applications for more interactive services, such as providing additional information about the event.

Other business opportunities could emerge, such as access granting – using the mobile as a key to securely unlock the home/office door in the physical world, or as a strong authentication token for remote access (eCommerce, eBanking, eGovernement).

While it is clear that the potential of mobile contactless payment is significant for everyone involved, there are still questions concerning the business model and value sharing. Discussions in this area are ongoing in Europe, thanks to a number of pilots taking place.

The place of the contactless application within the handset

NFC applications must be able to be downloaded and co-exist independently on the handset in a secure way. The Secure Element (SE) is a generic term that describes the place where a mobile contactless application is stored securely in the handset. One of the current debates is over the placement of the secure element within the phone, whether this would be included in the SIM card or be a separate entity – an embedded soldered chipset or a removable hardware (memory card), and issued potentially by a non-mobile operator. Issues such as business model and strategy are in discussion between stakeholders, and must be resolved before mass deployment is possible.



The need for a trusted third party

One key consideration is way the applications could be added to, and managed, within the secure element. The GSMA, a telecom-industry driven association, which represents more than 700 mobile operators around the world, has suggested the creation of a new role – the 'Trusted Service Manager,' while the Mobey forum, a financial-industry driven association to develop mobile usage for the financial services, is speaking of a 'Platform Manager'. So, both MNOs and banks are encouraging the creation of this "trusted third party" role, which would provide a single point of contact for all service providers wanting to put their applications onto NFC phones (m-payment, m-loyalty, m-ticket).

The trusted third party would have a 'master key' to the secure element and also manage the secure downloads of the applications onto the secure element. They would also help manage the services, once there. The trusted third-party would also be responsible for invoicing, as well as offering support to service providers.

In Belgium for instance, in the context of mobile remote payment, Atos Worldline already plays a similar role with its m-Banxafe solution, managing the secure download of keys in the SIM for all the MNOs and the banks.

Depending on the country, the TTP services platform could be run by the mobile operator itself, a consortium of operators / service providers, or by an independent trusted third party, like Atos Worldline. The exact role and responsibility of the trusted third party is currently under construction, thanks to various trials happening throughout Europe.

Mobile proximity payment – key factors for success

Collaboration

During the last few years, financial institution investment and effort has been focused on new payment technology for contact cards (EMV cards and PoS terminals upgrade). The introduction of NFC-enabled phones and contactless cards would require a major overhaul of the infrastructure (PoS card readers to upgrade/change to NFC).

On the other hand, mobile operators must finance and market NFC-enabled handsets and certainly the secure element (SIM card or otherwise). Even if, according to ABI Research, NFC enabled handset sales worldwide do grow from 500,000 in 2006 to 450 Million in 2011 (30% of total sales), mobile operators must have a clear ROI or this exciting, mobile contactless dream will collapse.

There is no doubt that collaboration is needed in order to share revenue; however, it is also needed to share risks and investments, which are especially important in Europe where there is no contactless payment infrastructure in place. In Japan, remember, the ePurse application, EDY, and the eTicket Suica contactless cards already existed before being dematerialised into NTT DoCoMo handsets. In Europe, the case for mobile contactless payment is still under construction through several trials and pilots. It is important to remember that contactless payment is only one potential contactless application, and that the ROI be considered globally and include other applications, such as m-ticketing, m-loyalty and m-access.

Branding

Dematerialisation of the card must not let the brand or logos disappear. Physical cards provide the link between the customer and the brand – if the card is to effectively be put in to the handset, the link must be preserved via the user interface.

Trust between mobile operators and banks

Trust between mobile operators and service providers is key; service providers need guarantees in terms of security, confidentiality and service quality. The role of a trusted third party (or Trusted Service Manager) is a good way to build a trusting relationship.

Bringing value to the merchant and the end-user

It is perhaps obvious, but merchant and customer are the main clients of both banks and mobile operators. Whatever the business model, the resulting solution should improve the existing payment instruments, or at least equal them, in areas such as:

- ***Ease of use*** – if the execution of a mobile payment is not as easy to use as existing payment methodologies, it will not be adopted. This includes the registration or activation phase for the customer.
- ***Speed*** – transactions must be able to be completed within a reasonable timeframe.
- ***Price*** – the price for having the option to pay for goods and services via a mobile device must be acceptable to users and merchants
- ***Security and privacy*** – both in terms of real and perceived. Merchants and customers must be protected against fraudsters and hackers, and must feel confident that the system is secure.
- ***Unlocking*** – changing of bank or MNO should be achievable.

Standardisation for broad acceptance and availability

For mass-market take-off, standardisation is crucial to allow interoperability with merchant payment terminals via a standard hardware and software interface. One of the barriers to the widespread implementation of contactless payment in Europe is the current lack of EMV protocol for contactless.

Today, MasterCard Paypass protocol consists of dematerialising the card's magnetic strip in the contactless card/handset. EMV contactless protocol integration is still being developed, driven by payment players such as Visa, MasterCard and EMVCo. Some technical standardisation issues have yet to be solved, such as the connection between the secure element and the NFC chip inside the mobile phone.

Until now, pilots focused on proprietary solutions that worked locally, within a specific town, with a specific handset and a specific card. There is still a lot of work to achieve in order to reach a true universal mobile proximity payment.

Standardisation is key at least in country, but with SEPA's intent to standardise card payments in Europe, it is difficult to imagine a mobile contactless payment system that wouldn't be SEPA compliant.

Mobile remote / proximity payment convergence

Remote payment should not be seen as a separate business opportunity; synergies between remote and proximity payment can reinforce the opportunity.

A typical scenario is the Smart Poster: the mobile phone reads the NFC tag located on a poster for a concert, and then redirects to a WAP site on which the user can buy a ticket for the concert. A dematerialised eTicket is then stored securely in the user's handset. The final step is for the user to wave the mobile phone in front the NFC-enabled concert gate, which will then grant access to the concert hall and allows the user to by-pass queues.

Contactless mobile proximity payment is often seen today as a wallet that stores dematerialised e-cards. This is not mandatory, however: MOTESpay is a good example of convergence, as consumers can use their remote wallet by swiping their mobile phones over a local NFC reader (the merchant must be online).

Plugging an NFC reader in to a PC is another possibility to make transactions on the Internet using the same mobile handset used in the proximity world.

Finally, some players that are providing remotely-accessible stored value accounts, such as Paypal (which has already launched a Visa credit card in the UK), could propose a plastic card or a dematerialised e-Card in the mobile handset to spend the stored value account e-money in a proximity store.

Collaboration or competition?

As mentioned above, the mobile operators' role in the NFC ecosystem is at least to provide access to the NFC-enabled phone through their service platform. Applied to payment, this means the ability for any 'service provider' (i.e. bank) to store and use a dematerialised debit/credit card in the NFC handset.

At this stage, some operators are thinking of being e-card issuers themselves. NTT DoCoMo, for example, issued its top subscribers with both a physical and virtual card 'DCMX', a dematerialised credit card stored in Sony-Ericsson handsets, through 'iD', DoCoMo's branded platform for storing and using e-credit cards in DoCoMo handsets.

The platform is open to the cards of other issuers, in addition to DoCoMo's DCMX series of credit cards. Because the NFC infrastructure roll-out will take a long time, we observe some innovative strategies that will see physical plastic cards issued in addition to a dematerialised e-card, stored in the handset and which can be used on traditional card reader. These will be used for those outlets that are not yet equipped with NFC readers. In addition, issuing a physical card helps to increase loyalty and can provide new financial revenue (interchange and credit fees).

Finally, of course, this card and e-card will be compatible for remote payment, on the internet or mobile.

So, beyond being enablers of m-payment through the handsets and network, mobile operators could provide their own payment service. Future mobile payment offerings from telecom companies could rely on what Atos Origin calls a '**quintuple play**' offering, the m-payment function being an additional offer of the so-called quadruple play package (Internet, telephony, TV, mobile).

On the other hand, some disruptive strategies could emerge from non-mobile companies, such as banks or retailers, which already offer not only financial or loyalty cards, but also mobile services to their customers through MVNO agreement. They could offer a '**killer bundle**' that include their customised mobile handset and m-payment instruments.

In the Netherlands, for example, Rabobank launched Rabo Mobile in 2006, and in a release, Piet van Schijndel, Member of the Executive Board of Rabobank Nederland said: "Mobile phones are the wallets of tomorrow. Rabo Mobile lets you transfer funds between payment, savings and investment accounts and transfer funds to another account – quickly, easily and safely. Plus it will be possible within the foreseeable future to use mobile phones for contact-free payments."

Future of mobile proximity payment is taking shape today through various pilots in Europe, and either in a collaboration mode – which is preferred – or competition mode, Atos Origin believes that players able to offer a unique set of coherent mobile payment instruments either remotely (mobile, internet) or locally (NFC e-card, physical card) will bring value to their customers, and will gain a strong competitive advantage.

Conclusion

Today, the mobile payment environment has opened up to several types of industry players: card schemes, mobile operators, banks, electronic money issuers, Internet giants, IT companies, new start-ups, alliances between banks and mobile operators (Mobipay, m-banxafe). The list goes on.

We are entering a pivotal moment in the history of m-payment, which is set to take off thanks to technical (NFC maturity) and regulatory (SEPA) breakthroughs. However, it cannot be over-stated that collaboration between mobile operators and banks is imperative for mobile NFC payment to become a mass-market reality.

It is evident that while this may be the future of mobile payment, there are also significant opportunities in the mobile remote payment arena, which new entrants are targeting actively.

Also, remote and proximity payment are complementary and converging; they are addressing different business opportunities and offering synergy which will add tangible value for the different stakeholders involved in their development.

For further information please contact:
laurent.bailly@atosorigin.com or bernard.vanderlande@banksys.be

About Atos Origin

Atos Origin is an international information technology services company. Its business is turning client vision into results through the application of consulting, systems integration and managed operations. The company's annual revenues are EUR 5.4 billion and it employs over 50,000 people in 40 countries. Atos Origin is the Worldwide Information Technology Partner for the Olympic Games and has a client base of international blue-chip companies across all sectors. Atos Origin is quoted on the Paris Eurolist Market and trades as Atos Origin, Atos Euronext Market Solutions, Atos Worldline and Atos Consulting™.

About Atos Worldline

Atos Worldline is a major European player in the processing of large-volume electronic exchanges, specialising in electronic payment services, CRM and e-services (internet, voice and mobile services). With the focus on technological innovation, Atos Worldline implements its solutions in processing or integration mode. On December 7th 2006, Atos Origin announced the acquisition of Banksys and Bank Card Company (BCC), creating a European leader in Payment Services, with combined pro forma 2006 revenues of EUR 630 million and 4,000 employees.

1517-0707