
# The Mobile Money Revolution

## Part 1: NFC Mobile Payments

ITU-T Technology Watch Report
May 2013

Mobile money refers to financial transactions and services that can be carried out using a mobile device such as a mobile phone or tablet. These services may or may not be linked directly to a bank account. Previously, recharging your mobile meant adding more airtime but now increasingly you will be able to add money to it, keep all your credit cards and loyalty coupons, access your bank account and use it like your ordinary wallet for payments. Innovations in mobile money could lead to a drastic change in the way people pay for goods and services in the near future. This report surveys and analyses the innovations in the mobile payments landscape and their likely impact on future standardization activities.

The rapid evolution of the telecommunication/information and communication technology (ICT) environment requires related technology foresight and immediate action in order to propose ITU-T standardization activities as early as possible.

**ITU-T Technology Watch** surveys the ICT landscape to capture new topics for standardization activities. Technology Watch Reports assess new technologies with regard to existing standards inside and outside ITU-T and their likely impact on future standardization.

**Acknowledgements**

This report was written by Venkatesen Mauree of the ITU Telecommunication Standardization Bureau in collaboration with Gaurav Kohli (intern at the ITU).

The authors are grateful for the support given by colleagues at the ITU Secretariat. The authors would like to thank the following persons for their feedback: Mr Gunnar Camne from GSMA and Mr Zhao Ping, ITU-T Study Group 2.

Please send your feedback and comments to tsbtechwatch@itu.int.

The opinions expressed in this report are those of the authors and do not necessarily reflect the views of the International Telecommunication Union or its membership.

This report, along with other Technology Watch Reports, can be found at http://www.itu.int/techwatch.

Cover picture: Shutterstock

Technology Watch is managed by the Policy & Technology Watch Division, ITU Telecommunication Standardization Bureau.

**Call for proposals**

Experts from industry, research and academia are invited to submit topic proposals and abstracts for future reports in the Technology Watch series. Please contact us at tsbtechwatch@itu.int for details and guidelines.

# Table of contents

*Page*

# 1. Introduction

Money has evolved several times in human history from the days of the barter trade, from coins to paper, then plastic and now phones. About 15 years ago, the mobile phone was used for making calls, playing simple games and texting friends. Today, mobile phones can be used to access the Internet, make video calls, take photos, find your location on a map, purchase transport tickets, and even for banking, among many other applications. Through advances in mobile technology and near-field communications (NFC), innovation in the area of financial services is changing the way we pay for goods or services or send money overseas, replacing the wallet with the smartphone.

NFC is a wireless communication technology that permits data transfer over distances of up to 10 cm based on the ISO/IEC 18092 standard. Based on Radio Frequency Identification (RFID) technology, it has been used in various industries including retail, automobile, medical, transportation and manufacturing. The primary uses of NFC are to:

- Connect electronic devices, such as wireless components in a home office system or a headset with a mobile phone;
- Access digital content, using a wireless device such as a cell phone to read a "smart" poster embedded with an RFID tag;
- Make contactless transactions, including those for payment, access and ticketing.

The main drivers behind the success of mobile money are the explosive growth in the number of mobile devices and the fall in the cost of computing power, which have lowered the barriers to new entrants in this field. Mobile money (m-money) is quite versatile and can support a variety of services, in particular, person to person (P2P) money transfers, which are of significant value for emerging economies.

Broadly speaking, m-money refers to financial transactions and services that can be carried out using a mobile device such as a mobile phone or tablet. These financial transactions and services are sometimes referred to as mobile financial services and may or may not be linked directly to a bank account. The year 2012 turned out to be a very busy year for mobile money, with a number of articles in the news and companies like Starbucks announcing their mobile money plans each week.

The terms "m-money", "mobile financial services" and "e-money" are used quite often in technical reports and in the media. Their meanings in this report are clarified at an early stage (See Box 1) in order to avoid any possible confusion.

**Box 1: M-money, mobile financial services and e-money**

M-money and mobile financial services have the same meaning in this report. They both refer to financial transactions and services that can be undertaken using a mobile device such as a mobile phone or tablet.

E-money is the electronic alternative of cash. The European Union defines e-money as a "*monetary value as represented by a claim on an issuer, which is stored electronically and issued on receipt of funds for the purposes of making payments transactions and is accepted by other legal entities other than the issuer*" (Article 4(5) of Directive 2007/64/EC).

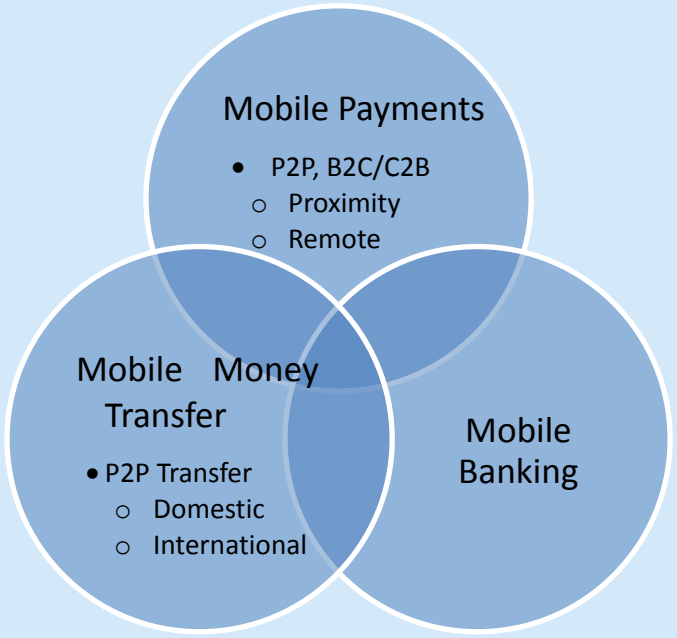
This first part of a two-part report on mobile money in the Technology Watch Report series focuses on innovations in the mobile payments landscape, and in particular on NFC contactless mobile payments and the likely impact on future standardization activities. The second part of the report will focus on mobile money transfer and mobile banking services and their link to enabling financial inclusion.

## 2. Types of mobile financial services

There are three main types of mobile financial services (see figure 1 below) with some degree of overlapping among the functionalities offered by applications in each category:

- Mobile payments;
- Mobile money transfer; and
- Mobile banking.

**Figure 1: Types of mobile financial services**




Mobile payments cover many types of transactions which fall into two categories: transactions with a remote merchant or proximity payments at the merchant site.

Mobile money transfer is also a broad term and in this report refers mainly to the transfer of money from one individual to another. The transfer can be domestic or international and can also be called a "peer to peer" (P2P) payment. When the transfer is international, it is referred to as an international remittance. Mobile banking allows users to manage their bank accounts remotely from their mobile devices.

Currently there is no standard definition of the terms mobile money transfer, mobile payment and mobile banking. There are some proposed definitions from industry associations (e.g. GSMA and Mobey Forum) and the European Union but there is no agreement on a common definition. This report focuses mainly on innovations in mobile payments. The next issue of the Technology Watch report will focus on mobile money transfer.

## 3. Types of mobile payment

Mobile payments refer to P2P and consumer-to-business (C2B) transactions for physical goods and services that are made using a mobile phone. Mobile payments are now present in every sphere of our life in developed economies, in the retail industry, transport sector, and entertainment and leisure activities. In developing countries mobile payments are used mainly for P2P payments and remittances but are also increasingly being used for utility bill payments and purchase of goods.

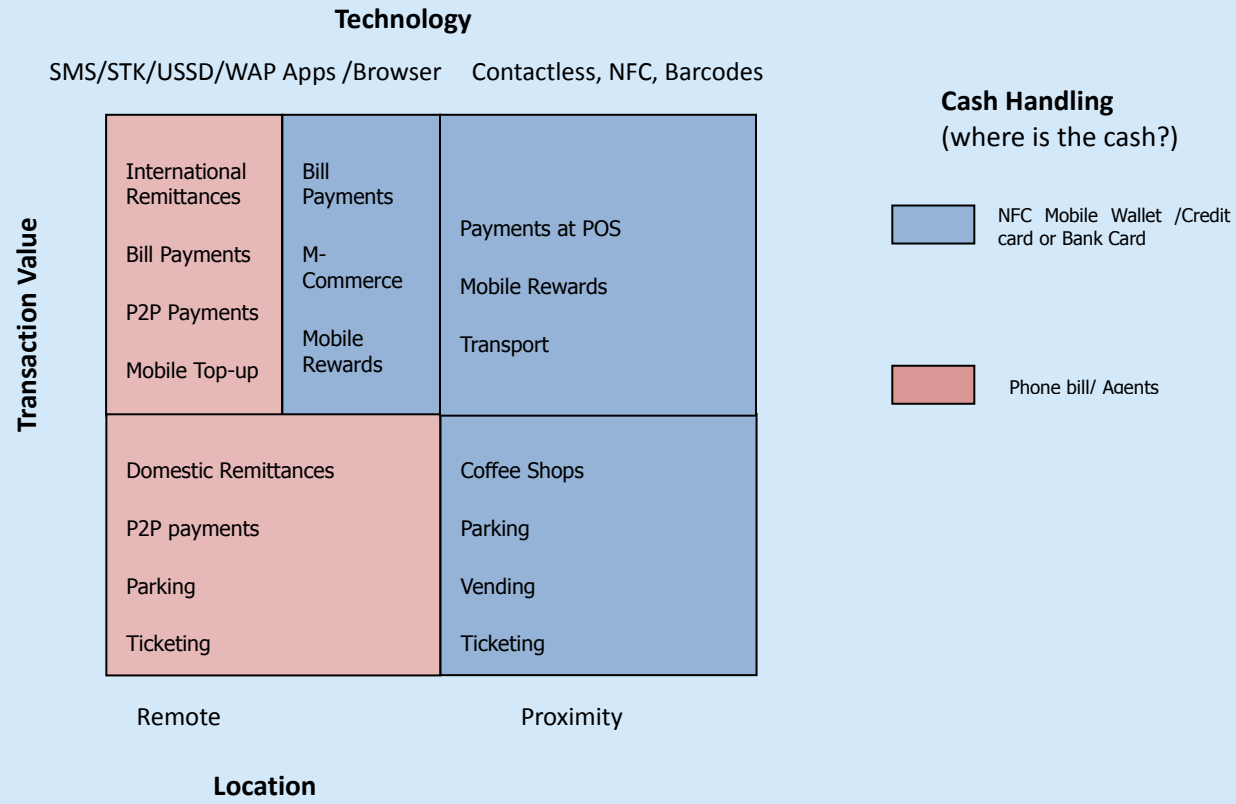
There are two types of mobile payments: proximity and remote. Figure 2 shows the different types of mobile payment services and their applications. Most B2C/C2B solutions provide an alternative to cash transactions and have the potential to change consumer behaviour in fundamental ways. B2C solutions rely on either a mobile operator-centric or bank-centric business model. The mobile handset interface is the crucial business driver as it allows the consumer to pay for everything and so has to be very user friendly and easy to use.

**Figure 2: Types of mobile payment services**

| | P2P | C2B/B2C |
|---|---|---|
| Proximity | | Mobile wallets (Contactless payments)<br>Mobile as a Point of Sale[1] (POS) |
| Remote | P2P Payments<br>Domestic transfers<br>International remittances | M-commerce<br>Mobile bill payments |

P2P mobile payments are private transactions between two persons. Commercial platforms may be involved in the transaction, but the transaction is a direct one between two persons. The most common transactions are transfers of funds. International remittances are viewed as a subset of P2P payments as they are usually one-way transactions. They have huge potential in developing countries.

**Figure 3: Mobile payments spectrum**




*Source: Smart Card Alliance Payments Council: Mobile Payments and NFC Landscape: A US Perspective. 2011, http://smartcardalliance.org/resources/pdf/Mobile_Payments_White_Paper_091611.pdf*

Figure 3 shows the various types of mobile payment services that are available, differentiated by technology, location, transaction value and cash handling function. Mobile payments can use a number of different technologies to perform a transaction. Remote payments will usually make use of short message service (SMS), Wireless Application Protocol (WAP), a browser, or a mobile application. Proximity payments, on the other hand, would be based on technologies such as bar codes or a contactless interface to chip-enabled payment technology, such as NFC-enabled mobile phones. Remote mobile payments and proximity mobile payments differ by virtue of the location of the mobile device and the merchant, as well as the nature of the transaction. A remote mobile payment is one in which the payer does not interact directly with the merchant. In a proximity payment, on the other hand, the mobile device interacts in some way with a physical POS device to obtain the consumer's payment information and complete the transaction.

The transaction value also influences the choice of mobile payment technology. In general, mobile payments fall into one of two transaction value categories. Micropayments are those with a value of less than USD 10–25. Examples include purchase of ring tones, parking charges, transport tickets and payments in coffee shops. Some examples of transactions that would exceed USD 25 in value are P2P international remittances, web purchases, bill payments and retail purchases.

The way in which cash is handled during the transaction also differs according to the technology. In some cases, the phone is a mobile wallet and provides access to the user's credit card or bank account information. In other cases, the credit card or bank card can be accessed by the mobile phone via a reader to carry out the payment transaction (e.g. Square). In other situations, for example in P2P payments (e.g. M-PESA), the cash is loaded through an agent into a virtual account linked to the phone number which is then used for payments. In other cases, the value of the transactions can be charged to the user's phone bill.

# 4. Proximity payments

Proximity payments are the main payment method for B2C transactions and involve the use of a mobile phone either as the equivalent of a credit or debit card (mobile wallet) or as a point-of-sale (PoS) terminal. Proximity payments have been implemented in developed economies and in some emerging economies. With the growth of smartphones usage in emerging economies, there is no doubt that it will gradually make its way in those markets as well.

## *4.1 Mobile Wallet*

This is the most common type of mobile money service in the news. An electronic account held on the mobile device known as a "mobile wallet" has various functional features such as converging deposit accounts, credit accounts, loyalty accounts, merchant accounts, gift cards and coupons stored on the mobile device with a remote communication facility for use anywhere, anytime. In developed countries, the mobile wallet can also be conceived as a container for different payment instruments, such as cash and cards. The mobile wallet is a menu on the phone which provides access to different payment instruments and payment account information. This method typically uses "tap and go" (i.e. the user taps his/her mobile device for payment instead of the credit card) or the smartphone's built-in near-field communication (NFC) wireless technology to facilitate payment for goods and services using a mobile device in much the same way as a credit card. There are also methods other than NFC for implementing mobile wallets.

This system is faster and more convenient than cash (people are more likely to forget their wallets than their mobile phones). An NFC-enabled mobile device is a medium which enables multiple service/card providers to have their own services resident within a mobile phone.

**Box 2: Google Wallet**

Google Wallet works with an NFC-enabled device. Users can tap the phone to an NFC terminal at checkout and use any credit or debit card (Visa, MasterCard, American Express, Discover) with the Google Wallet app on a smartphone. Google Wallet is available on major mobile networks in the United States such as T-Mobile, Sprint, AT&T and Virgin Mobile. Google Wallet has partnered with outlets where consumers can shop and just use their phones to tap payments on POS devices that are PayPass-enabled. The mobile wallet can also be used to make online payments to partner merchants by accessing the Google Wallet account through a WAP browser. When a user makes a payment using Google Wallet, Google actually pays the merchant and then processes the transaction with the customer's selected credit or debit card, so neither the merchant nor the phone operating system ever obtains the customer's payment card information. Google Wallet is PIN protected against fraud, and if the phone is stolen, the customer can remotely manage the Google Wallet to disable the account by logging online.

There are also other implementations based on software and QR[1] codes. NFC-enabled mobile devices can enable a range of services such as ticketing, payments, loyalty, couponing, access control and identity.

Google initiated Google Wallet (Box 2) with Sprint's Nexus S and is now available on phones from Sprint and Virgin Mobile. Since the release of the first version of Google Wallet, Google has partnered with more than 25 retailers, and linked up with MasterCard PayPass, which enables payments at more than 200 000 retail locations across the United States. The main objective of Google's strategy is to build a payments "ecosystem" around Google Wallet similar to Android. Google is trying to create an open standard that will be adopted by various stakeholders, such as MasterCard, network operators, handset manufacturers, merchants and the banking industry. In August 2012, Google announced a new, cloud-based version of the Google Wallet that supports all credit and debit cards from Visa, MasterCard, American Express and Discover. This will enable customers to use their cards when shopping in-store or online with Google Wallet. With the new version, the mobile wallet can be remotely disabled from the Google Wallet account on the web.

**Box 3: YESpay cloud payment platform**

YESpay International Limited and YES-wallet.com Limited have developed a cloud based payment platform using a cloud-based NFC contactless card emulation service conforming to Visa PayWave and MasterCard PayPass standards and offering a convenient and efficient payment solution for merchants and consumers. The partnership allows pre-paid/gift-card related businesses, merchants, and mail order houses to implement the contactless card payment system without having to make heavy upfront investment by using the Pouch cloud service. YESpay contributes by providing payment terminals based on NFC reader/writers and payment processing services for merchants. YES-wallet is a digital wallet (referred to as Pouch) which complies with the PayWave or PayPass standard virtual payment cards cloud system.

The cloud-based Pouch PayPass/PayWave NFC payment solution does not use the mobile phone's Secure Element or the baseband memory to store the security keys related to the issued card. Instead it uses the YES-wallet.com secure PCI-DSS level-1 certified data centre to manage the security keys related to the issued PayPass/PayWave virtual cards.

Credit card companies MasterCard and Visa are also quite active in this field. MasterCard in August 2012 signed a five-year deal with Everything Everywhere in the European market, which will see the two companies working to develop a co-branded, contactless NFC payments solution. MasterCard is partnering with Deutsche Telekom in Germany and elsewhere in Europe, with Turkcell in Turkey, and has been working with Orange on QuickTap, the first commercial NFC payment service in the United Kingdom. The ISIS mobile

[1] QR stands for Quick Response and is a cell phone readable bar code that can store website URL's, plain text, phone numbers, email addresses and other alphanumeric data. It is standardized under ISO 18004.

wallet is being promoted by AT&T, T-Mobile and Verizon Wireless. The ISIS mobile wallet holds virtual versions of credit and debit cards on the mobile device. The wallet can be accessed only by composing the unique four digit PIN code. All sensitive data are stored on a chip on the mobile phone (the "Secure Element" (SE)[2]). ISIS mobile wallet was launched on 23 October 2012 in the United States.

Apple's Passbook, which was released in September 2012 with the iOS 6, is another type of digital wallet designed to store membership cards, tickets, boarding passes and coupons, amongst other such items on the user's mobile phone. Unlike the Google Wallet, it is not used for making payments but for storing tickets, coupons, cards or boarding passes on the iPhone. In addition, Passbook does a few things which paper and plastic cannot do, like sending alerts and pop ups to be readily accessed at the user's location. For example, in the case of a boarding pass for a flight, if the boarding gate has changed, the system will update in the background and push the new information to the user's lock screen to alert him or her of the change. In the United States, Passbook is already being used for digital ticketing. The ticket bought using the iPhone is kept in the Passbook wallet and the user scans the phone to get access.

In China, NFC mobile wallets are also getting a lot of attention. China UnionPay is the dominant player in China for NFC mobile payments and is collectively owned by the banks. China UnionPay now has agreements with 157 banks, laying a good foundation for its mobile payments services. In May 2011, ChinaUMS, one of its subsidiaries, also received a government licence for third-party payments. In June 2012, China UnionPay and China Mobile signed a partnership agreement on mobile payments, promising to collaborate in this field. China's leading mobile carriers - China Mobile, China Telecom and ChinaUnicom - have each established their own mobile payments subsidiaries. All three have strong mobile subscriber populations, control access to millions of mobile devices, and see mobile payments as an additional revenue stream. The mobile carriers, however, are pursuing different paths. In May 2010, China Telecom and China Unicom aligned with China UnionPay's 13.56 GHz standard, while China Mobile continued to push its 2.4 GHz solution. In addition, China Mobile made a major move to acquire a 20 per cent stake in the Shanghai Pudong Development Bank, with which it recently launched a mobile banking/payments platform. E-commerce service providers Alipay, Tenpay, and YeePay all have large active user bases and are looking to use the power of smartphones and applications as a relatively easy way to break into mobile payments.

In the Republic of Korea, SK Telecom and Korea Telecom (KT) are the main players in NFC mobile payments. SK Telecom has partnered with Visa whilst KT joined with MasterCard to launch NFC mobile payment services. In 2010, SK Telecom launched the Smart Wallet which is available on an NFC enabled phone with USIM based services for membership cards and coupons. In 2011, the Grand Korea Alliance, which includes mobile network operators (MNO), handset manufacturers, card issuers and government agencies, opened an NFC shopping mall in the Myeondong area in Seoul. This enabled shoppers to make NFC-based payments at 200 outlets, order drinks, and download coupons and transit information from smart posters. The service could also be used for peer-to-peer NFC payments and transport ticketing.

In Japan, NTTDoCoMo dominates the mobile contactless payments landscape. DoCoMo and Sony jointly developed the contactless FeliCa[3] (Felicity card) chip which is being used to create the iD mobile wallet inside the phone. NTTDoCoMo has also subsidized the installation of readers at the national level and developed strategic partnerships with banks, retailers and merchants. In October 2012, NTTDoCoMo announced a partnership with MasterCard which will integrate the iD mobile wallet with MasterCard's Paypass to enable NTTDoCoMo subscribers to make purchases overseas. NTTDoCoMo, KDDI and Softbank have formed the Japan Mobile NFC Consortium to align the country's standards for NFC with international ones.

[2] Secure Element is a smart-card chip in the mobile device onto which an app can be downloaded and installed. Examples are microSD cards and Universal Subscriber Identity Module (U-SIM).

[3] FeliCa : It is a contactless RFID smart card system from Sony in Japan.

## 4.2 Mobile Phone as a PoS

Mobile phones can also be used to accept payments from others, i.e. to process credit card payments without the need for NFC capability. The biggest players in this space are Square (which has partnered with Visa) and VeriFone. The limited availability of NFC-enabled handsets has posed a challenge to widespread consumer adoption of mobile payment. However, credit card and technology companies have developed a contactless payment system that is contained on a microSD card and can equip smartphones with SD card slots with contactless payment capability. This technology is seen as a transitional solution until NFC-embedded smartphones are widely introduced by mobile phone handset makers.

Square (see Box 4) offers a free credit card reader and application that connects to your iPhone, iPad, or Android device. It charges a simple flat rate of 2.75 per cent for all cards, including American Express. VeriFone's PAYware Mobile works with iPhone but a USD 49 activation fee is required, the encrypted card reader must be bought separately, and there are in addition standard merchant fees that vary depending on the transactions. Groupon, an online discount and advertising company, has also come up with a similar payment application similar to Square, called Groupon payments service, and is charging lower fees.

In Hungary, a cloud-based service is operated by mobile payments company Cellum in partnership with MasterCard and is handling 1 million transactions per month. Users scan QR codes to make payments authenticated with a PIN which matches information stored locally in an application on the handset with information stored remotely on a server.

In the Czech Republic, the three mobile network operators partnered with the top four banks to launch a mobile-wallet service called Mobito, whereby retailers key in the user's mobile number on their POS device and users receive a notification via either USSD[4] or a downloaded app, which they authenticate with a PIN. Mobito has NFC enablement on its roadmap, but has kicked off with this cloud-based solution because NFC is not yet a mass-market proposition.

**Box 4: Square**

*Twitter* founder Jack Dorsey introduced *Square,* a mobile payment service that is being viewed as a disruptive innovation which could create a new market and value network. It has revolutionary features, such as no elaborate hardware installations. The Square Card reader is only 1 inch tall and can be carried in the pocket. It can simply be plugged into a mobile device's standard 3.5mm headphone mini-jack and can be used for swiping credit cards, and no merchant account is required. There are no monthly fees or set-up costs. The app is free as well as the Square Card Reader, and free shipping is offered to clients. Square has two main applications, Pay with Square and Square Register, which currently work on smartphones that must run on iOS 4.1 or Android 2.2 or later operating systems, to be able to use these Square applications. Pay with Square allows customers to view merchant menus, make mobile payments, receive virtual receipts, and discover other Square-enabled merchants. Square Register is point of sale software aimed at replacing traditional credit card terminals and cash registers. The Pay with Square application allows customers to buy items directly from their mobile device without having to reach for a credit card. Customers just need to provide their name at the check-out. Merchants will know the customer's name as they will see the name and a picture of the customer on their registers and can accept payments with a simple tap of a button. Square's Technology is PCI compliant and VeriSign certified and uses strong encryption on its devices including SSL and PGP. Card numbers, magnetic stripe data, or security codes are not stored on Square client devices.

[4] USSD: Unstructured Supplementary Service Data.

## 5. Remote payments

Remote payments are initiated with a mobile device independent of the consumer's or merchant's location. Remote payments will be considered in more detail in Part 2 of the Technology Watch Mobile Money Report.

Remote payments can be classified as follows[5]:

a. P2P domestic transfers and payments : payments made to individuals for informal services (e.g. purchasing a second-hand item) or for formal services (e.g. self-employed car mechanic).
b. International remittances in the form of mobile money transfers across international borders.
c. Person-to-business (P2B): payments to businesses for purchases of physical goods and services, but excluding digital goods (such as ring tones).
d. Business to person (B2P) payments, such as salaries and wages or reimbursement of employee expenses.
e. Mobile bill payments: payments usually made for utilities such as those for gas, electricity, and water and other similar services normally, but not always, incurred on a recurring basis.
f. Carrier billing: payments for purchases of digital goods such as software applications from third parties that are downloaded directly onto the mobile device. The payments are billed directly by the mobile operator providing the service. Several payment companies have partnered with mobile operators, including Cashlog, Fortumo, BOKU, and Bango. They offer software development kits that developers can integrate into their applications. Carrier billing typically uses a two-factor authentication method. The user enters his mobile number and receives a one-time password via a text message to complete credentials. This eliminates even friendly fraud (for example, someone who knows you uses your number) as the buyer must have the device in-hand to complete the purchase.

## 6. Proximity NFC mobile payment ecosystems

A number of stakeholders are involved in the proximity NFC mobile payments business. For example, in a B2C transaction, the following stakeholders would be involved: the customer (payer) and the merchant, the mobile network operators (MNO), financial sector institutions (e.g. banks), payment networks (e.g. Visa, MasterCard), a trusted service manager, the mobile device manufacturer, and software and service providers (e.g. wallet developers). Table 1 shows the expectations of the different stakeholders involved.

[5] Asli Demirguc-Kunt, L. Klapper. (2012). Measuring Financial Inclusion. World Bank.

**Table 1: Expectations of stakeholders in the NFC mobile payments ecosystem**

| Stakeholder | Expectations |
|---|---|
| Merchant | • Faster transaction time<br>• Low or zero new investment and usage cost<br>• All in one open interoperable devices (e.g. POS) with backward and forward compatibility<br>• Integration/simplification of existing payment approaches<br>• High security and trust in the service<br>• Possibility of customizing the service (e.g. adding loyalty schemes)<br>• Real-time status of mobile money transactions |
| Consumer | • Minimal learning curve<br>• Better and personalized service<br>• Trusted and secure solutions (at technical and social level)<br>• New service is available everywhere<br>• Low or zero additional cost of usage<br>• Interoperability at the POS and the ability to transfer money across different service providers and banks<br>• Real-time transaction status overview<br>• Being able to pay "anywhere," "anytime" and in any currency<br>• Person-to-person transactions |
| Mobile Network Operator (MNO) | • Potential to add value to existing services<br>• Increase customer loyalty<br>• New revenue channels<br>• Increase average revenue per user |
| Mobile Device Manufacturer / Service Developer | • Large market adoption of new embedded hardware/software features of the devices<br>• Open, interoperable, widely-used standards<br>• Low cost of new technologies/features to be integrated<br>• Low time-to-market<br>• Multi-application capability<br>• New relationships with banks/MNOs/payment networks |
| Bank | • Branding and customer loyalty<br>• New customers<br>• Ownership or co-ownership of the new payment application<br>• Secure and trusted payment service<br>• Integration/use of existing infrastructure and payment methods |
| Payment Network | • Secure authentication<br>• Integration/use of existing infrastructure<br>• Secure processing of payments |
| Trusted Service Managers | • Secure payment channel<br>• Provide service to banks and MNO |

*Source: Adapted from S. Karnouskos, Mobile payment: a journey through existing procedures and standardization activities, Communications Surveys & Tutorials, IEEE , vol.6, no.4, pp.44,66, Fourth Quarter 2004*

For MNOs, m-money means increasing the number of customers and average revenue per customer. Most of the available deals are thus based around increasing customer loyalty to increase revenue from telephone services. By controlling the authentication of contactless payments on phones, MNOs aim to get a slice of the revenue generated by these payments. MNOs can charge SIM-space rental fees to NFC application providers such as banks, retailers and transport companies.

Trusted service managers (TSMs) are intermediaries between MNOs and service providers and are involved only in NFC mobile payments. For example, Gemalto acts at the TSM for Vodafone NFC mobile payments. The main role envisaged for the TSM is to help service providers securely distribute and manage contactless services for their customers using the networks of mobile operators. One important TSM responsibility is to manage the cryptographic keys and system used to securely communicate the payment information from the financial institution to the consumer's mobile device.

In NFC mobile payments the relationships between stakeholders can differ depending on the route adopted for implementing the secure element (SE). The SE is a smart card chip equipped with cryptographic processor to provide authentication and security for storing payment applications. A mobile device can implement the SE in the following ways (see Table 2):

- Universal Integrated Circuit Card (UICC) Removable
- Embedded
- MicroSD Removable

**Table 2: Differences in implementations**

| UICC Removable | Embedded | MicroSD Removable |
|---|---|---|
| SE on UICC | Embed NFC SE on device | MicroSD has NFC capabilities (including controller, antenna and cryptographic processor) |
| SIM Cards require upgrades to use UICC that supports NFC | Done during manufacture of phone | Can be used on non-NFC enabled phones. |
| UICCs created that support NFC controller and antenna | Does not provide portability of the microSD or UICC | |

The entity which controls the distribution of the SE has a direct effect on the possible NFC payment provisioning paths and on stakeholder relationships.

# 7. Security of mobile payments

All cases of online use (proximity mobile payments, remote mobile payments and mobile money transfer) require secure transactions to protect against eavesdropping or modification of the communication between the device and the server.

## *7.1 Characteristics of secure mobile payment transactions*

A secure mobile payment transaction has the following characteristics:

- Confidentiality: the confidential information must be secured from unauthorized persons, processes or devices. For SMS payments, the confidential information is stored at the merchant's level. The security of the transaction is as secure as the security of the merchant.
- Authentication: ensures that parties with access to a transaction are trusted.
- Integrity: the information and systems have not been altered or corrupted by intruders
- Authorization: verifies that the user is allowed to make the requested transaction. With post-billing SMS, authorization is an issue but with PIN-based SMS-payment systems, security is better.
- Availability: it must be accessible for authorized users at any time. This is a tricky situation in P2P SMS-based systems, as the receiving party's mobile device must be switched on for the transaction to be completed.
- Non-repudiation: ensures that the user must not deny that he has performed a transaction, or provide proof if such a claim is made. There is no 'proof of delivery' incorporated in the SMS protocol. This can be resolved, but at additional cost.

## 7.2 M-money security concerns

M-money transactions pose two primary security concerns:

a. How to keep information secure if a mobile phone is lost or stolen, and
b. How to keep information secure when it is transferred from consumer to recipient.

With regard to the first security issue, two-factor authentication is currently used to verify the mobile phone's proper user. Before making any m-payment, the user will typically register the phone, which acts as the "token", with the bank or mobile service provider offering the m-money service (the first factor) and then confirm the payment with a PIN or password (the second factor). Thus, to initiate an m-payment, the user must have both the right phone and know the correct password. In proximity contactless mobile payments, the mobile device is used as the token for the two-factor authentication.

As regards the second issue, the situation depends on whether the payment is made via proximity or remote mobile payment. Proximity m-money payment uses the same security features as contactless payment cards to secure information passed from customer to merchant. The security of the transaction will depend on the location of the mobile payment application which is used to store the user's data such as payment account information and passwords. The location of the mobile payment application needs to be secure and is considered in Section 7.3. Cryptograms are used to confirm the validity of the transaction and encrypt the data during transmission.

## 7.3 Securing the mobile payment application

There are two possible options for securing mobile payment applications:

a. The Trusted Execution Environment (TEE); and
b. The Secure Element (SE)

**Table 3: Payment Application Location**

| Type of mobile services | Payment Application Location and storage of encryption keys | | Requires Trusted User Interface |
|---|---|---|---|
| | SE | TEE | |
| NFC Contactless Payments | | | |
| Mobile as POS | | | |
| Mobile authentication | | | |
| Remote Payments | | | |

Recommended

The SE is tamper-resistant and thus provides a high security level for the data. It is used to store sensitive payment and user credentials for offline proximity payment (e.g. Mobile as PoS). Since it is a dedicated hardware component, the SE requires integration with the platform hardware. This type of implementation requires a lot of time to develop and is quite expensive. Many NFC enabled phones come wired with a connection between the NFC chip and the SIM card called Single Wire Protocol (SWP), allowing specially adapted SIM cards to be loaded on the phone which can act as an SE. Because of its reliability in authenticating users immediately and offline, the SE is particularly suited to NFC transactions, which are performed on the spot. Any kind of offline transaction also requires an SE in combination with the Trusted User Interface.

TEE is a hardware-protected environment that runs in the phone's main processor and alongside the main operating system of the smartphone. It is an isolated area in the smartphone which connects to critical device resources without passing through the operating system. It allows critical data and code to be isolated from any malware-type attacks in the smartphone's open environment, without requiring any new

hardware component. Sensitive code is executed in this isolated and protected environment, and critical data stored in this area are encrypted. One of the unique capabilities of the TEE is its ability to implement a Trusted User Interface.

The Trusted User Interface enables secure authentication through a secure channel with the Secure Element or a server and non-repudiation for financial transactions performed on smartphones. It controls the screen and keyboard and/or touchpad, isolating them from the operating system, thus providing secure authentication and non-repudiation. TEE includes cryptographic as well as key-storage and management functionalities. It also includes secure mass storage, which can be used to store transaction logs and passwords in a private area.

The TEE efficiently protects sensitive data stored on the device and can therefore enable all online uses such as NFC contactless mobile payments, mobile as POS, and remote mobile payments (see Table 3). With the TEE, all these uses can benefit from hardware-based security, while maintaining flexibility and ease of deployment.

### *7.4 Storing encryption keys and payment information in the cloud*

Cloud computing holds the potential to overcome some of the security challenges of m-money and has been attracting interest of late. PayPal has invested in the cloud payment model. The advantage of the cloud payment model for NFC contactless payments lies in the keys, and the fact that personal information related to the credit/debit card is not stored on the phone but in the cloud. The risk is therefore less for a consumer who loses his or her mobile phone. The only problem with cloud computing is the reliability of the network infrastructure. If a problem occurs in the network before the completion of the transaction, the customer could incur additional charges, especially for credit card transactions.

## 8. Standardization

Mobile NFC payment is an area where standardization work is attracting a lot of attention. The work is being undertaken mainly by standards development bodies such as the International Organization for Standardization (ISO), European Telecommunications Standards Institute (ETSI), and by ICT industry and financial institutions, either independently or in partnership (e.g. SmartCard Alliance, Electronic Transactions Association, Mobey Forum, GSMA, Global Platform, EMVCo[6] and NFC Forum). At the level of the International Telecommunication Union (ITU) work has focused mainly on securing mobile financial services and on harmonizing frequency ranges used by RFID as a particular type of short-range devices (SRDs) requiring operation on a global or regional harmonized basis. This section provides an overview of ongoing standardization activities in this field at the international level.

Although the way of accepting payments on POS terminals from NFC cards or devices has been standardized, the same cannot be said for loyalty points and vouchers. Each NFC POS deployment requires adaptation of the software on each payment terminal and integrating each terminal with the retailer's back-end loyalty-scheme and the offers and customer relationship management systems. This is not only time-consuming but costly.

### *8.1 NFC contactless mobile payments industry forums*

A number of players from the ICT industry, standardization bodies and financial services sector are involved in the standardization of NFC contactless mobile financial services (e.g. SmartCard Alliance, Electronic Transactions Association, Mobey Forum, GSMA, Global Platform, EMVCo and NFC Forum, ETSI and ISO).

[6] EMV Co stands for EuroPay, MasterCard and Visa.

The Mobey Forum, NFC Forum, Global Platform and GSMA have been quite active in the development of specifications and best practices for NFC contactless mobile payments.

Global Platform is a cross-industry, not-for-profit association which identifies, develops and publishes specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology[7]. Global Platform has developed a set of specifications for mobile networks that use the same security best practices for moving data in the physical world to moving data through the mobile networks. The Global Platform specification 2.2 defines multiple security domains (the TEE and Trusted User Interface) that use authorized and delegated management to allow an application to be loaded into the secure element.

The NFC Forum develops specifications for NFC devices that are based on the ISO/IEC 18092 contactless interface, ensuring interoperability among devices and services. The different operating modes of NFC devices are based on the ISO/IEC 18092 NFC IP-1 and ISO/IEC 14443 contactless smart card standards (i.e. reader/writer mode, peer-to-peer mode and card emulation mode). The NFC Forum has issued a number of specifications (about 16 in 2012)[8], for the different operating modes. The N-Mark trademark has been developed as a universal symbol for NFC, so that consumers can easily identify NFC-enabled products as well as the locations where NFC services are available[9]. It has two main objectives:

- To inform consumers that NFC services are available on mobile devices and other consumer electronics; and
- To indicate where to touch to enable NFC services.

The mobile telecommunication operators have focused on driving the standardized deployment of mobile NFC, using the SIM as the secure element to provide authentication, security and portability. GSMA has focused on the development of SIM specifications to support NFC and certification and testing standards to promote interoperability. The big debate in the industry has been about where, in phones equipped with NFC, to locate the SE for storing payment information. The GSMA has been pushing for the UICC to become the standardized component for storing sensitive data in NFC-equipped mobile phones, whilst other organizations advocate embedding it in the phone or embedded micro SDs. Privacy and security are assured by storage of the payment application within the UICC. GSMA is working together with EMVCo to ensure the relevant security requirements are met.

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. In the United States, the EMV Migration Forum is a new independent organization created by the Smart Card Alliance to support the coordination of the implementation steps required to migrate successfully from magnetic stripe technology to secure EMV contact and contactless technology. The focus of the Forum is on topics that require some level of industry cooperation and/or coordination to migrate successfully to EMV technology in the United States.

## *8.2 ISO*

NFC, the near-field communication standard that uses the 13.56 MHz frequency band for contactless proximity mobile financial services, was certified by ISO/IEC as an international standard in December 2003 (ISO 18092, 21481). ISO is working towards the development of ISO 12812, a standard for mobile financial services, which, is expected to address:

- Security and data protection for mobile financial services
- Financial application management

---

7 Source : http://www.globalplatform.org/.

8 Source : http://www.globalplatform.org/.

9 Source: http://www.nfc-forum.org/resources/N-Mark/.

- Mobile person-to-person payments
- Mobile person-to-business payments
- General requirements for mobile banking applications.

The work is being undertaken in ISO working group 10, *Mobile banking / payments*, in technical committee ISO/TC 68, *Financial services*, subcommittee SC 7, *Core banking*. ISO will also examine successful models in nations where bank accounts, and therefore debit and credit cards, are rare – such as M-PESA in Kenya, a mobile phone-based money transfer service that allows branchless banking – to ascertain whether they can be incorporated into the standard.

## 8.3 European Commission Directive on Payment Services (PSD)

The Directive on Payment Services (PSD) is being established by the European Commission to provide a single framework for payment standards and obligations, resulting in the Single European Payments Area (SEPA). The SEPA territory consists of 32 European countries[10] and also includes countries which are not part of the euro area or European Union. The SEPA initiative aims to overcome technical, legal and market barriers between countries in order to create a single market for retail payments in euros and will include a SEPA card standardization programme as well as one for mobile money services. However, progress has been slow, with countries disputing the regulatory requirements to be imposed on non-banks, and many missing the first deadline for implementation. Such disagreements show the difficulties in translating national payment approaches into regional policy.

Payment standards that are being established for debit and credit transfers include the following[11]:

- The payment account identifier must be the IBAN.
- The standard for message format must be the ISO 20022 XML standard.
- The remittance data field must allow for 140 characters. Payment schemes may allow for a higher number of characters, unless the device used to remit information has technical limitations relating to the number of characters, in which case the technical limit of the device applies.
- Remittance reference information and all the other data elements provided must be passed in full and without alteration between PSPs in the payment chain.
- Once the required data are available in electronic form, payment transactions must allow for fully automated electronic processing at all stages of the payment chain (end-to-end straight-through processing).
- Payment schemes must set no minimum threshold for the amount of the payment transaction in respect of credit transfers and direct debits but are not required to process payment transactions with zero amount.
- Payment schemes are not obliged to carry out credit transfers and direct debits exceeding €999 999 999.99.

The European Payments Council[12] (EPC) is facilitating cross-industry cooperation between payment providers and MNOs in the elaboration of guidelines and standards under the PSD.

## 8.4 ITU

At the level of ITU, Study Group 13 (Future Networks) has developed two Recommendations related to securing mobile financial services. Recommendation ITU-T Y.2740 elaborates approaches to developing system security for mobile commerce and mobile banking in the next generation networks (NGNs). It

[10] See list of countries: http://www.ecb.europa.eu/paym/sepa/about/countries/html/index.en.html.

[11] See: http://www.ecb.europa.eu/paym/sepa/elements/standards/html/index.en.html.

[12] EPC is the coordination and decision-making body of the European banking industry in relation to payments. It consists of 74 members representing banks, banking communities and payment institutions.

describes security requirements for mobile commerce and mobile banking systems, based on four specified security assurance levels. It outlines probable risks in mobile commerce and mobile banking systems, and specifies means for risk reduction. Recommendation ITU-T Y.2741 specifies the general architecture of a security solution for mobile commerce and mobile banking in the context of NGN. It describes the key participants, their roles, and the operational scenarios of the mobile commerce and mobile banking systems. It also provides examples of implementation models for mobile commerce and mobile banking systems.

ITU-T Study Group 2 is currently working on the development of a Recommendation on Telecom Finance, which will provide an overview of mobile money services from the operators' perspective to enhance the customer experience in telecom service and strengthen B2B, C2C and B2C financial infrastructure.

As with other wireless communication technologies, spectrum availability is the key factor for RFID functioning and global deployment. The ITU Radiocommunication Sector (ITU-R) is continuing its studies to achieve harmonization for SRDs in response to Resolution ITU-R 54-1. Recommendation ITU-R SM.1896 contains frequency ranges to be used as recommended ranges for SRD applications requiring operation on a globally or regionally harmonized basis, such as RFID. These frequency ranges include but are not limited to ISM bands identified in the Radio Regulations. In addition, Report ITU-R SM.2255 outlines the key standards, operating parameters and frequency bands for the deployment of RFIDs in various administrations and includes information on harmonization possibilities.

Recommendation ITU-T X.668 (ISO/IEC 9834-9) allows the referencing of schemes using the object identifier (OID) system developed by ITU-T and ISO/IEC in the 1980s and widely deployed in, for example, e-commerce applications. This allows a tag placed on a billboard poster to be read with a mobile phone and makes it easy for the user to get additional multimedia (text, graphics, even voice or video) information about the content of the poster. ITU-T X.668 is the first and key stage in the standardization process, with the next stage of work focusing on specifications of the system and protocol that will associate the multimedia information to an ID (a.k.a. ID resolving). It was jointly authored by experts from ITU-T Study Group 17 (with input from SG 13 and SG 16) and ISO/IEC.

# 9. Conclusion

With the rapid adoption and growth in mobile technologies worldwide, mobile money services are being adopted all over the world, albeit in different ways in the developed and developing worlds. Mobile money will be used increasingly in the future to complement cash, cheques, credit cards and debit cards. Moreover, it can also be used for payment of bills (especially utilities and insurance premiums) with access to account-based payment instruments such as electronic funds transfer, Internet banking payments, direct debit and phone bills. The scope of m-money has also expanded beyond just goods and services. Mobile payment processing must be global (i.e. what works in United States should also work in Asia, Europe, the Middle East and Africa). The only way to ensure that processing is uniform is to develop and adopt global standards.

As has been shown, the interest in mobile money is evident, standardization efforts are ongoing, and the search for the right business models and successful approaches is ongoing. This proves that the area is active and of great interest, but also indicates that we are still at the beginning of a long road.

The ITU could play an important role in this ongoing standardization work. ITU-T Study Group 17 could also address some of the security issues related to mobile money payments using the cloud.

ITU-T Technology Watch surveys the ICT landscape to capture new topics for standardization activities. Technology Watch Reports assess new technologies with regard to existing standards inside and outside ITU-T and their likely impact on future standardization.

**Previous reports in the series include:**

Intelligent Transport Systems and CALM
ICTs and Climate Change
Ubiquitous Sensor Networks
Remote Collaboration Tools
NGNs and Energy Efficiency
Distributed Computing: Utilities, Grids & Clouds
The Future Internet
Biometrics and Standards
Decreasing Driver Distraction
The Optical World
Trends in Video Games and Gaming
Digital Signage
Privacy in Cloud Computing
E-health Standards and Interoperability
E-learning
Smart Cities

http://www.itu.int/ITU-T/techwatch

Printed in Switzerland
Geneva, 2013
Photo credits: Shutterstock®