Mobile Proximity Payment: Ecosystem and Overview of NFC Technology

Corrado Guidobaldi, MSE, PhD

Abstract

Mobile proximity payment has been discussed for more than a decade, but now it seems close to the maturity and it seems that its mass diffusion has now started.
Expectation for Mobile Payment diffusion worldwide is justified by the fact that in 2010 more than three billion people owned a mobile handset [1]. Mobile commerce is a natural successor to electronic commerce. The capability to pay electronically coupled with a website is the engine behind electronic commerce. Electronic commerce has been facilitated by Automatic Teller Machines (ATMs) and shared banking networks, debit and credit card systems, electronic money and stored value applications, and electronic bill presentment and payment systems.
Mobile payment is a natural evolution of electronic payment that will facilitate mobile commerce. A mobile payment or m-Payment may be defined, for our purposes, as any payment where a mobile device is used to initiate, authorize and confirm an exchange of financial value in return for goods and services. The proximity factor is the most discussed topic in the mobile payment field and promises a revolution in the world of payments.
This article traces the state-of-the-art in mobile proximity payment field and traces the most probable evolution directions.

1. Introduction

Handsets confirm to be worldwide the most promising devices for the diffusion of the Mobile Payment (m-Payment in the following). The main reasons for this are.

1. *Market Penetration*. In Italy, there are 50 mln handsets and 25 mln Credit Cards. In the world, there are 4/5 bln handsets and 1.5/2 bln credit cards.

2. *Portability*. Handset is the preferred object by most people.

3. *Interaction*. Customers can easily interact with their handsets through Graphical User Interface applications while credit cards do not allow this capability.

4. *Credit*. A handset already has credit onboard, that can be used for mobile payment purposes.

It is worth noting that m-Payment services are currently quite widespread around the world. Actually, the term m-Payment is quite ambiguous, since it has been used in different ways in different contexts. M-Payment can indeed be intended as a galaxy of services that rotates around money transactions. Involved technologies are numerous and heterogeneous.
The Mobile Payment ecosystem involves a number of partners, such as:

- banks;

- *Mobile Network Operators* (MNOs);

- service providers;

- technology providers, namely handset suppliers, application providers, SIM suppliers;

- merchants at point of sales;

- *Trusted Service Managers* (TSMs), i.e., intermediary institutions among m-Payment actors that are also responsible for the management of personal data security.

Different business models can be conceived. According to the study of existing m-Payment services, it seems that no entity is strictly necessary in the sense that realistic business models can be designed also if one or more partners are not involved in the value chain. Following, examples of successful cases of m-Payment are discussed.

- *Mobile TopUp*. The handset is used for recharging the credit for voice/data traffic. In this case, usually only the mobile operator and the handset supplier are involved.

- *Car parking*. The handset is used for communicating the start (end) period of car parking. In this case, a service provider is involved delivering a suitable application on the handset.

- *Mobile Money Transfer*. It is used for sending/receiving funds on the mobile phones: a consumer, whose mobile operator offers mobile money transfer in partnership with a service provider, uses his handset to transfer money cross–border to a receiver, whose mobile operator also offers mobile money transfer in partnership with the same service provider. The funds go directly into the receiver's mobile "wallet", or account tied to the mobile handset.

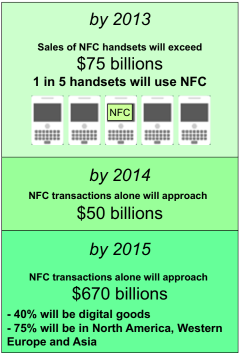
- *Mobile commerce*. eCommerce can be managed by handsets. For instance, eBay transactions can be managed with eBay applications optimized for handsets.

From the above examples, it is clear that the term m-Payment is quite generic. This paper is going to analyze in detail that part of the m-Payment area that is now "bubbling". This area regards the *Mobile Proximity Payment*, i.e., payments carried on with the handset and with the support of a proximity protocol, namely a protocol that allows to complete the payment (the so called *check-out* phase) using the merchant's *Point Of Sale* (POS). A number of mobile payment applications are not part of this area, namely:

- purchases of digital contents from Application Stores,
- donations by handsets,
- payments on web sites that are not optimized for mobile,
- payments by SMS.

During the years, a big number of proximity protocols have been used for experiments regarding the proximity payment. Currently, the most promising seems to be *Near Fierld Communications* (NFC, [2]). NFC has been widely used for a long time in contactless applications, such as access control in buildings and ticketing. Most actors in the business models support this protocol. Members of the NFC Forum, i.e., the standardization forum for this protocol, are hundreds and include the main worldwide players: handset and SIM manufacturers, chipset vendors, MNOs, TSMs, bank services, financial and payment institutions (e.g., VISA), transportation companies (e.g., Transport for London), etc.

Moreover, the main players in the mobile field (e.g., Google, Apple), very large MNOs (e.g., AT&T, T-Mobile, Orange), many financial institutions (e.g., VISA, Mastercard) are going to design their strategies for "attacking" this new and promising sector. Additionally, newcomers and joint-ventures are going to disrupt the equilibrium of mobile commerce in general, enriching the payment experience with new value added services. *Figure 1* shows an estimate of the m-Payment market growth according to a Gplus research [4].



by 2013

Sales of NFC handsets will exceed

$75 billions

1 in 5 handsets will use NFC

by 2014

NFC transactions alone will approach

$50 billions

by 2015

NFC transactions alone will approach

$670 billions

- 40% will be digital goods
- 75% will be in North America, Western Europe and Asia

Source: Adaptation from a Gplus research [4].

Figure 1. Mobile Payment market growth in the next years.

Mobile initiatives around the world reveal a number of key drivers and barriers for the adoption of mobile payments [5], as shown in *Table 1*.

Drivers	Barriers
• Offering added value for consumers and merchants Mobile operators, financial institutions and others Participants in the ecosystem	• Complex value chain with lack of co-operation • Financial regulation • Security/risk issues • Cost • Limited range of mobile payment services • Capable handset • Lack of interoperability across players • Lack of technology standards

Table 1. Driver and barriers for the adoption of mobile payment.

Open points in m-Payment can be summarized as follows:

- which are the most promising services for the start up of the Mobile Payment?

- which is the winning strategy for triggering a virtuous circle? (i.e., after the service start up, how to increase the number of involved customers and service providers?)

- how to let the customer/retailer understand the added value of m- Payment services?

Moreover, the experience of pilots shall be correctly capitalized.
The following sections of this paper address the most common mobile proximity payment business models, the main security concerns, the benefits for the players, some interesting trials and pilots. Some technical details on the NFC technology are discussed in Appendix A.

2. Mobile Payment Business Models

Four potential mobile payment business models have been identified by Smart Card Alliance in 2008 [3], in order to classify the various m-Payment implementation scenarios. This classification is now three years old. Since m-Payment is evolving really fast, three years represent quite a long period and probably there exist trials, pilots and also commercial environments that do not fall into one of the proposed categories. Anyway, the models are clear and still widely used for didactic purposes. One of the commonly cited reasons for the relative lack of success of mobile payments so far, as detailed in [5], is the absence of productive cooperation between key stakeholders, namely the financial institutions and the MNOs. There have been many reasons for this absence of cooperation, some of these (in no order of priority) are:

- desire by players in each industry to diversify from their core businesses;
- debate over who “owns” the customer;
- difficulties around branding in a cooperative model;
- debate over the location of the *Secure Element* (i.e., the architectural component managing security, see *Section 3*) and the inability to arrive at an agreed revenue sharing model.

It is really important for the evolution of the m-Payment market to deploy a number of enclosed services that differentiate m-Payment from the stand-alone credit card.
Moreover, it is necessary to re-design the check-out process for the Mobile Payment: Simply providing a shop with a contactless POS seems really poor and can be not enough for a widespread adoption of m-Payment. Finally, good communication and a “critical mass” of customers are essential for the services.
The four m-Payment business models will be described in the following subsections. However, first it is necessary to better understand a key role in the m-Payment ecosystem: the Trusted Service Manager.

2.1. Trusted Service Manager

A *Trusted Service Manager* (TSM) aims at realizing simple, transparent payments within the m-Payment ecosystem [6].
The core function of the TSM is to securely distribute, provision and manage the life cycle of NFC applications to the *customer base*[1] of MNOs on behalf of service providers. But the TSM role is much broader than supply only the technical capability to provision and personalize NFC applications *Over The Air*[2] (OTA). As a matter of fact, the TSM manages contractual relationships between many mobile network operators and many service providers (*Figure 2*). To this aim, the TSM provides many supporting business services, including customer service, data center hosting and quality assurance.

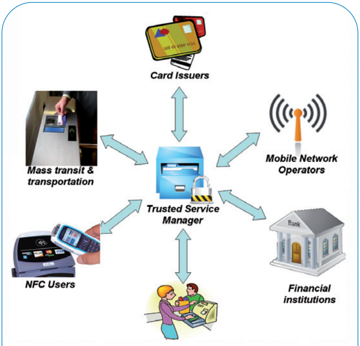


Figure 2. TSM is a service provider that connects all parties involved in an m-Payment, which include card issuers, mobile network operators, retailers, financial institutions, etc., from a neutral standpoint.

The TSM is the entity, in the m-Payment ecosystem, that has a view of the interactions of the customer base with the MNOs and the service providers. This view allows the TSM to provide customer support from both the MNO perspective and the service provider perspective, and enables the management of customer life cycle events such as exchanged, damaged, lost or stolen handsets and associated impact on the service provider accounts previously provisioned. Related to this, there is the responsibility of TSM for managing the life cycles of NFC applications, electronic wallet applications, mobile handsets and Secure Elements.

[1] The customer base is the group of customers and/or consumers that a business serves.
[2] Over The Air is a method of distributing new software updates to handsets or provisioning them with the necessary settings with which to access services such as WAP or MMS.

A key element of the TSM role, as expected by the *GSM Association* (GSMA), is that it is an independent entity serving MNOs and any account-issuing entities such as banks, card associations (such as VISA, Mastercard), transit authorities, merchants, marketing companies and service providers. An independent TSM is crucial to the provisioning of applications to NFC-enabled handsets, since it allows the consumer to have the broadest possible purchasing potential. For instance, a bank working in conjunction with one of the major card associations could issue a handset through a MNO that is essentially a handset hosting a credit card. The card association or the bank might provide the TSM services for that device. Such a partnership might be successful by adding merchant-specific prepaid accounts to those handsets, because these accounts represent ways for consumers to make purchases without using the card association's payment network.

The key point here is that an independent TSM provides NFC-based handsets with many accounts from many different service providers across many carriers and payment networks: this is what will maximize the value of NFC-enabled handsets as a channel for not only consumer purchases, but also targeted marketing.

The customer cannot download applications like games and other utilities, OTA to the handset, without the need for a new business entity, like the TSM, for many reasons. The first and most important is that any application that requires personal information (e.g., a credit, debit or other payment application) requires special handling. The application and personal information must be stored in the Secure Element of the handset and not in the standard handset memory. The technology required to provision and manage applications and personal data on the Secure Element is different from the technology required to download games and non-personalized utilities. The TSM plays a key role in restricting access to applications and data to those with the right access permission.

A payment application and the associated personal data are hosted by a financial institution or third-party processor in a secure data environment that conforms to payment industry security protocols. A core component of this process is, therefore, security key management.

Finally, mobile subscribers must be properly identified, authenticated and authorized before payment applications are provisioned to their mobile handsets: the TSM plays a key role in validating that the customer is who he says he is, that he is a valid customer of a given service provider, and that he has permission to receive a given payment application.

2.2. Collaboration Model

This model is probably the most scalable and desirable and it allows the largest number of opportunities for all stakeholders, including the customers. It supports collaboration among banks, mobile operators and other parties in the mobile payments value chain, including a potential *trusted third party*, namely the TSM.

Payments in this model are processed over the existing financial networks, crediting and debiting the appropriate accounts. This model includes two possible scenarios:

- *Scenario 1*: a MNO, in partnership with a bank, offers a bank-specific mobile payments service;

- *Scenario 2*: MNOs and financial institutions negotiate and set standards for applications that reside on Secure Elements in mobile devices, allowing multiple card types from different banks to be used.

In both cases, NFC-enabled mobile devices and compatible POS devices are deployed. These devices shall meet the standards set by the partner bank and MNOs, and generally speaking they shall support the NFC standard as described in NFC Forum documents and reported in *Appendix A*.

Potential sources of revenues include merchant commissions, merchant and consumer fees, new customer acquisition fees, and marketing fees. The amount paid and collected by each stakeholder is source of considerable contention. Transaction fees, namely those fees that are imposed by financial institutions on each transaction, are currently totally managed by those institutions. It seems really difficult that they can share them with other partners of the m-Payment ecosystem. Also, it is generally expected that merchant fees are split between banks, MNOs, and third-party such as TSMs.

Collaboration model seems to have the greatest potential for long-term success, and it seems the most feasible because it allows stakeholders focusing on their own core competencies, it opens the door for new revenues from incremental services, it drives customer retention and loyalty, and it responds to fundamental demands from customers. A further point of strength is that banks own financial liability while mobile operators own network security.

Figure 3 shows the risk/benefit diagram for the various stakeholders in the Collaboration model. In particular, the TSMs own some risk, and this entitles them to revenues from risk assumption for the provided services.

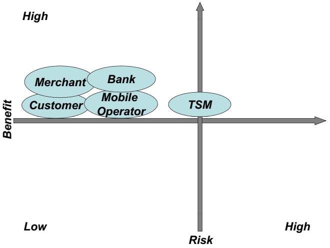


Figure 3. The adoption of a Collaboration model allows the players involved in m-Payment to share risks/responsibilities and benefits.

The technology underlying this model is still in the trial phase in most parts of the world. Although the Collaboration model is ideal because it allows each party to focus on its core competencies, the model has the most complex implementation as it requires agreement on revenue-sharing models.

Many believe that incremental benefits and drivers are not from the payment itself, but from additional services that can be realized through NFC, such as customer loyalty, churn prevention (i.e., preventing customer migration towards competitors), location-based services, and new economic activities unleashed by NFC-driven innovations.

The revenue sharing model is wide open and is determined by the value that partners create for each other. The payment business is much more open than the telecommunication business, and the potential for creative partnering is broad. On the down side, some MNOs report only marginal services being paid with mobile devices due to questions about NFC value proposition and the disputed role of wallet providers (i.e., providers of applications that allow handsets to be used as wallets) and other non-traditional players such as PayPal. The Collaboration model seems the most promising business model.

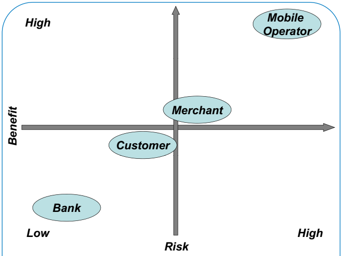


Figure 4. Operators shall assume most of the risks and responsibilities if they prefer the adoption of an Operator-Centric model. In this case, also financial issues shall be managed by the Operator. In return, the Operator gets most benefits.

2.3. Operator-Centric Model

A MNO acts independently in deploying mobile payment applications to NFC-enabled mobile devices. The applications may support a prepaid stored value model or the charges may be integrated into the wireless bill of the customer.

The MNO loads the mobile payment application on the NFC mobile device of its customers. The customer may prepay, or the operator may charge, the existing wireless bill of the customer. Two scenarios are possible:

- *Scenario 1*: the MNO provides the merchant with a wireless POS system;
- *Scenario 2*: the MNO enables the proximity payment application on the NFC mobile device of the merchant.

The Operator-Centric model does not adequately address all business concerns from all associated parties. This model could lead to customer loyalty, increased revenue, and potential reduction in customer turnover.

The Operator-Centric model faces several challenges. Mass adoption from merchants and consumers will be difficult due to:

- concerns of risk, privacy, and fraud;
- need to deploy additional POS equipment at merchants;
- challenges to MNOs regarding billing and customer service requirements.
- lack of business relationships between merchants and MNOs.

Pilots using this model have been launched in Europe and Japan. *Figure 4* shows the risk/benefit diagram for the various stakeholders in the Operator-Centric model.

The primary benefit to MNOs is sole control over the revenue stream. Brand recognition is an additional benefit to the MNO. If the merchant acceptance infrastructure becomes widely available, consumers may consider convenient using the technology and may purchase products or services that are NFC-enabled.

When utilizing this model, MNOs would have ultimate control of the infrastructure and the associated revenues. However, they would also incur the corresponding risks and liability.

MNOs do not have traditional merchant relationships. Acquiring such relationships would require a shift in the business model of the MNO, which is an extremely costly and time consuming activity. Moreover, MNOs should also take care of bad debts, receivables, transaction inaccuracies, and frauds.

2.4. Bank-Centric Model

A bank deploys mobile payment applications or devices to customers and ensures merchants have the required POS acceptance capability. Payments are processed over the existing financial networks by crediting and debiting the appropriate accounts.

The Bank-Centric model extends the existing model used for credit cards into the mobile space.

An issuing bank owns the relationship with the customer and it is responsible for providing their customer with the payment device, in this case an NFC-enabled phone, in much the same way as credit cards are currently distributed. The bank could actually give its clients a fully-featured NFC phone, or, at the other extreme, it could simply provision an existing NFC phone with a suitable payment application.

Implementing the Bank-Centric model is simplified by the fact that the value chain for each participant is relatively clear and easily understood. An issuing bank gets greater client loyalty and more direct contact with their customers in return for the technology investment. The merchant bank gets electronic transactions which would otherwise have been cash purchases. A merchant gets faster transaction times and increased spend. The customer gets convenience and flexibility. *Figure 5* shows the risk/benefit diagram for the various stakeholders in the Bank-Centric model.

Under this business model, only the banks would collect transaction-based fees. This could be either a flat fee or a percentage of the transaction, such as the current interchange fees.

A purely Bank-Centric model is unlikely to be materialized for a number of reasons:

- Banks may be reluctant to invest in another payment model since many of them are rolling out contactless credit and debit cards.
- Partnerships and revenue sharing with MNOs would be impossible to avoid.
- Customers would not want to manage multiple wallets on their phones or have different applications for each of their accounts, resulting in hesitation and slow adoption.
- MNOs would be unwilling to "unlock" NFC on the phone if they do not receive a share of the benefits. This is especially true in Countries where phones are subsidized by the MNO and customers cannot easily switch handsets.
- Banks may be forced to support various operator-specific standards.

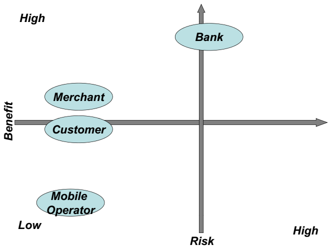


Figure 5. Bank-Centric model is adopted by banks that want to proactively create an m-Payment ecosystem. They assume to get most risks and responsibilities but also most benefits.

The key strength of this model is its easy comprehension.

When a payment is made over the Internet, neither the Internet service provider nor the browser manufacturer takes any fee. So, for mobile payment, a reasonable question is why MNOs should get paid for transporting the transaction or enabling the customer to make the transaction. However, the real struggle with full deployment of the Bank-Centric model is how disruptive the MNOs could be if they choose to take fees. With historically risk-averse banks driving the Bank-Centric model, the full potential of the channel may never be realized. Innovators and facilitators are needed in order to bring in meaningful loyalty programs, smart posters and revolutionary shopping experiences, which are viewed to be key to NFC adoption.

2.5. Peer-to-Peer Model

The Peer-to-Peer model is an innovation created by payments industry newcomers who are trying to find ways to process payments without using existing wire transfer and bank card processing networks.

The ability to send money from one person to another, even across great distances, has existed for many years through providers such as Western Union. While the Internet has made this service even more convenient, the high fees associated with the transfers can make them cost prohibitive and not for every-day use. Internet bill payment services provided by most banks have made remote payments to merchants convenient, but they cannot be used for real-time purchases. Mobile phones with peer-to-peer capabilities overcome these obstacles. Different scenarios are available:

- *Scenario 1*: a provider deploys contactless cards/devices to customers and POS equipments to merchants in a closed loop model;
- *Scenario 2*: a provider deploys a mobile payment application for the NFC-enabled mobile device;
- *Scenario 3*: a peer-to-peer service provider uses an existing online application (e.g., PayPal Mobile). No POS equipment is required.

This model is significantly different from the other models previously discussed.

Service providers must overcome the lack of an existing customer base, lack of payment processing infrastructure and lack of an established brand, and invest a large amount of capital to overcome these obstacles. Established banks and operators have the capital and infrastructure, but fail to see a large revenue opportunity with peer-to-peer payments.

The Peer-to-Peer model is attractive to merchants looking to decrease the costs of processing credit and debit payments, to "underbanked" customers, who have poor access to mainstream financial services and therefore cannot obtain a traditional bank card, and to customers willing to send money to friends and family overseas.

However, this model as well as all payments networks, faces the following main issues:

- providing a significant number of merchant locations to be meaningful to customers;
- ensuring that transactions, whether at POS or online, are convenient for all stakeholders;
- providing sustainable revenue to the banks so that they will drive the transaction volume to this channel;
- educating customers and merchants that the services from peer-to-peer providers shall be as reliable as the credit and debit cards provided by the long-established financial institutions that they trust;
- overcoming negative media reports on money laundering and security;
- resolving disputes and refunds.

Figure 6 shows the risk/benefit diagram for the various stakeholders in the Peer-to-Peer model.

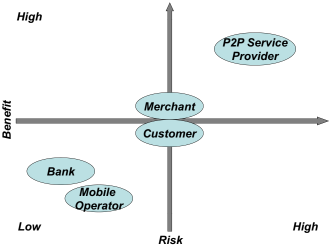


Figure 6. Peer-to-Peer model seems to be the most disrupting one. In this case a "newcomer" P2P service provider, such as PayPal, aims at building a m-Payment ecosystem collecting both risks and responsibilities and catching the benefits.

Additionally, the various stakeholders have different opinions on the Peer-to-Peer model:

- financial institutions are concerned that texting money (i.e., sending money using text messages) at the POS will fail because of lack of speed;
- mobile operators see this as a temporary solution, a good concept that works well for the "underbanked" and for overseas money transfer, but expect little revenue to come from it;
- merchants believe that peer-to-peer payment is compelling since fewer stakeholders simplify implementation and collaboration and the Peer-to-Peer model allows parties to focus on core competencies.

An example of a well-established Peer-to-Peer provider is *PayPal Mobile*. Using a mobile device rather than the Internet, PayPal Mobile leverages eBay's PayPal functionality to allow customers to transfer funds from one PayPal customer to another, to purchase goods on eBay, or to purchase goods online from merchants who accept PayPal as a form of payment.

3. M-Payment Ecosystem Security

Security and confidentiality of sensitive applications and data are the fundamental elements of any payment solution. Financial institutions increasingly seek to mitigate the risk of fraud, in order to protect their customers and hence their own payment franchise.
Enhanced security on credit cards requires the so-called *Secure Element* (SE), namely a chip that stores the payment credentials of the bank (private security keys) and other critical data. One example is the introduction of *Chip and PIN* (EMV chip-based security)[3] on cards in Europe to replace magnetic stripe-based systems.
While the direction for credit card transaction security is clear, the industry is looking for ways to secure m-Payments at a comparable level. The question is, therefore, which SE in the handset are available to facilitate the mass-market introduction of secure mobile payments.
A SE has many features designed to protect the security of the data it stores:

- it is separated from the handset operating system and hardware, and it enables encrypted protocols to enforce access control;
- only authorized programs can access the SE to initiate a transaction;
- there are multiple levels of protection for data stored on the SE and it is protected at the hardware level from snooping or tampering. Moreover, PIN enforcements can be added.

GlobalPlatform [7] a neutral and cross-industry organization, has defined and provided the needed specifications to support three types of Secure Elements, selected as options for NFC mobile. These are:

- *Universal Integrated Circuit* (UICC),
- *Secure Memory Card*,

[3] EMV (Europay, MasterCard and VISA) is a global standard for inter-operation of Integrated Circuit cards (IC cards), POS terminals and ATMs, for authenticating credit and debit card transactions. IC card systems based on EMV are also called Chip and PIN.

- *Embedded* (in the handset) *Secure Element*.

More details can be found in [7]. Also, GSMA delivered a directive on NFC:

- SE shall be placed on the UICC,
- NFC communication device shall be placed on the handset.

Devices hosting the SE shall manage the *Security Domains* (SD). Security Domains can be viewed as black box entities, that support security services such as key handling, encryption, decryption, digital signature generation and verification for the applications of their providers (Card Issuer, Application Provider or Controlling Authority). Security Domains act as the on-card representatives of off-card authorities [8]. SD are used for:

- defining the scope of responsibility of each player,
- ensuring the ownership of the keys of each player,
- hosting dedicated applications: payment, transport, etc.

The Card Issuer has its own SD, called *Issuer Security Domain* (ISD), that has the authorization privileges to:

- create new SD for banks and to allocate memory,
- give authorization privileges to other SDs.

Each bank may have a dedicated Security Domain, called SD_Bank:

- applications belonging to the bank are linked to its SD_Bank,
- the SD_Bank contains a keyset for ensuring confidentiality of the application personalization.

Secure Element must be certified (for instance by VISA or MasterCard). Obtaining the certification is not a simple process, since a number of actors is involved and different actors can require different certifications. Note that chipsets and OSs shall be separately certified. Some certifications have an expiration date, since security attacks are continuously improved.
As detailed above, m-Payment is strictly connected, in most cases, to the presence of a credit card on the handset. Security measures related to the embedded credit card are analogous to those related to a plastic credit card provided with a chip. As a consequence, lost or stolen handsets shall be managed coherently to lost or stolen plastic credit cards. Credit cards can be added on or removed from the handset analogously to the cases in which plastic credit cards can be requested by the customer to the bank and can be refused in a second time.
The Secure Element is designed to prevent malicious applications to access stored credit cards. Additionally, the security of the SE can be enforced by the OS of the handset. A further issue is that someone with a malicious reader could read sensitive date from an NFC-enabled handset. But even if the antenna is on and in proximity (i.e., less than 5 cm) of a reader, payment credentials can only be transmitted from the Secure Element to a payment terminal if the user authorizes the transaction. Finally, the same rules that apply to unauthorized use of plastic credit card, apply to unauthorized use of a credit card stored on the Secure Element, for example, regarding customer liability.

4. Possible Fields of Application of NFC Mobile Payment

This section shortly describes some fundamental applications related to mobile payment. Not all of them are strictly connected with a money transaction, but it is worth noticing that also non-payment applications can represent an enriched user experience that is useful to widespread the benefits of NFC and m-Payment.

4.1. (Micro)Payments

One of the core business for m-Payment with NFC is *Micropayment*. Micropayments are intended as payments whose threshold is quite low, approximately 20€; such threshold may slightly change in the various Countries.
Micropayments can be performed using either online or offline transactions.
Online transactions require electronic authorization for every transaction and the debits are immediately reflected in the account of the customer. The security of the transaction may be additionally enforced with a PIN. The online transaction is generally viewed as superior to the offline debit card because of its more secure authentication system and live status, which alleviates problems with processing lags on transactions. Online transactions are usually more time consuming.
Offline transactions do not require an electronic authorization at the POS. This type of debit card may be subject to a daily limit, and/or a maximum limit. Transactions conducted with offline debit cards require 2-3 days to be reflected on customer's account balance. Offline transactions are usually less time consuming.
Usually, offline transactions are preferred since they are more suitable for small amounts of money and they are faster than online one.
Micropayment is perhaps the most promising but also the most challenging NFC scenario, for many reasons: agreements among MNOs, banks, and financial institutions shall be set up and managed; TSMs shall be set up; contactless POS's shall be distributed; merchants shall be involved and well informed. Another challenging issue is managing the presence of many credit/debit cards and prepaid cards on an NFC handset.
Trials and pilots for micropayment have been done around the world in many Countries and almost every day a press release announces a new pilot. *NFC World* [11] began reporting on developments in NFC communication market in October 2008, and they described over 200 trials, pilots, tests and commercial NFC and related services in 48 countries.

4.2. Ticketing

Scope of ticketing can be quite various: public transportation, cinema, events, etc. (*Figure 7*).
Customers can find many benefits in acquiring tickets with NFC handsets, the most notable being: transaction speed, queue reduction, no need of bringing small change. For these reasons, ticketing seems one of the most promising NFC applications, also because most public transportation networks, at least in the largest cities, are ready for contactless ticketing.

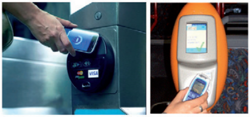


Figure 7. Ticketing and metro access based on an NFC handset.

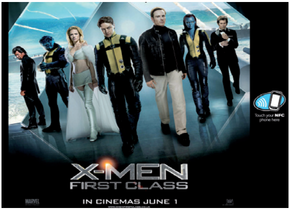
Ticketing applications can be integrated in the Secure Element and driven by an application with an appealing user interface.

4.3. Info Points

Museums and monuments are often described by automatic audio/video guides. This kind of service could also be integrated on handsets hosting NFC technology. Monuments should be equipped with NFC smart tags and the customer, by approaching the handset to the tag, can be redirected on the suitable audio/video guide. The Cityzi project, described in *Section 7.3* also adopted Smart Info points [10].

4.4. Smart Posters and Couponing

Smart postering can be used for receiving detailed information on a product or an event. Interesting use cases are panel information in hyper-stores. It is worth noting that the content of an NFC based smart poster can be dynamically modified and adapted to the context.
Events, such as movies, are usually advertised by trailers. Trailer URLs can be stored in the smart tag hosted in the poster campaigns. For instance, Proxama [9] has announced the launch of an NFC poster campaign in London to support the release of 20th Century Fox's new movie "X-Men First Class" (see *Figure 8*).
Many companies such as *GroupOn* [12] or *Groupalia* [13] and recently, in the US, also Google, give the possibility to access exclusive offers through *coupons*. An evolution could be the diffusion of such offers through a proximity protocol such as NFC. In this case, the customer, passing close to the poster illustrating the offer, can pass the handset close to it and keep the offer (or a discount on a product in which he is interested in).



Source: Adaptation from http://www.nfcworld.com

Figure 8. X-Men campaign by Proxama in London. NFC based smart tag is integrated in the poster.

4.5. Loyalty Cards

Loyalty cards can be embedded in NFC handsets. Points can be caught using the same logic of smart posters. Loyalty card is a widely used instrument for customer loyalty. Currently, customers that use this instrument shall manage a plastic card for each loyalty circuit. NFC handsets allow to store a virtually unlimited number of loyalty cards in the NFC store. Moreover, when loyalty points are converted in discounts or exclusive offers, these can be used directly with the NFC handset during the check-out process.

4.6. Instant Win

Proximity protocols such as NFC can be used for implementing instant win games. The kind of games are currently under investigation in NFC area. For instance, Infordata [14] has developed an innovative system of rewarded game that will establish a new way of communication between companies and their customers.

5. Device Availability

One of the crucial points for the diffusion of NFC is the availability of handsets and USIMs[4] (in case of USIM based SE) supporting NFC. Currently, all the largest handset suppliers are going to distribute handset models hosting NFC technology. Moreover most platforms (e.g., Android, RIM, Windows Mobile, etc.) designed schemes for the support of Secure Element and APIs for the development of Mobile Wallets.
Specifically, at least one model for each brand, supports NFC tech-

[4] A *Universal Subscriber Identity Module* is a software application for UMTS mobile telephony, which runs on a UICC inserted in a 3G handset.

nology and according to the expectations 30% of handsets will support NFC in 2012, 60% in 2013 and most handsets in 2015.
USIM suppliers are still more advanced. NFC USIM hosting Secure Elements for all NFC purposes are already available from all major worldwide USIM suppliers.
The policy of Apple on the support of NFC technology on iPhone 5 is still undisclosed.

6. M-Payment Market Evolution

According to a research by Deloitte [15], the m-Payment market is likely to evolve along four different trajectories, each of which benefits the various key players in a different way (*Table 2*).

6.1. Wait and See

This scenario follows the current trajectory: MNOs, financial institutions, independent payment providers and other players experiment different payment services that provide limited services in specific geographic markets. Limited cooperation between disparate industries and a lack of scale will likely stifle services, fragment offerings, and focus on niche markets.

6.2. Fly Solo

One visionary player with significant market power makes the required investment that stimulates development. NTT DoComo, for example, built a payment platform, developed the payment applications, invested in a bank, gathered a set of merchants together, and provided subsidies to create a contactless payment ecosystem to gain competitive advantage.

6.3. Buddy System

A financial institution and MNOs come together to provide payment solutions where a credit or debit card is embedded as an application in the mobile device. This option allows both parties to share the risks and rewards and develop harmonized, clearly defined business models. A targeted partnership will be better able to focus on the "pain" points, and a small number of partners may be better equipped to address them.
MNOs and financial institutions do not have much experience in collaborating together, and their expectations differ. The buddy system would allow two big players to develop trust while creating a more broad-based coalition.

6.4. Open Federation Alliance

An open federation alliance allows players from different industries to rally around a common vision and use mutually beneficial business models to realize the full potential of mobile payment. MNOs, financial institutions, merchants, handset makers, chipmakers, application providers and a host of others would come together on a standardized platform to provide a portfolio of financial services on mobile devices. A TSM plays the pivotal role of coordinator and integrator managing both the technical aspects of the platform and the business models that govern the alliance.

SCENARIOS	MNOS	FINANCIAL INSTITUTIONS	HANDSET VENDORS	MERCHANTS	CONSUMERS
Wait and see	Gains by innovating disruptive models	Loses by being on the sidelines or acts defensively when credible threat emerges	Limited gain from small scale NFC deployment by carrier	Limited gain from competition to card-based ecosystem	Loses because of fragmented offering and limited availability
Buddy system	Gains from tapping existing payment network and generates incremental revenues	Loses by sharing merchant revenues with carriers unless it is a niche player that expands revenue pie	Moderate gains from NFC deployment to larger customer base	Gains from speeded up transactions but loses from upgrades costs of POS	Gains from merchant acceptance and convenience
Fly solo	Significant risk without commensurate returns	Significant risk without commensurate rewards	Limited gain from small-scale deployment	Limited gains from small scale deployment	Limited gains from low merchant acceptance
Open federation	Significant gains from large-scale mobile payment deployment	Moderate gains from large-scale mobile payment deployment	Significant gains from mass deployment of NFC	Significant gains from mass deployment of NFC and greater competition among payment instruments	Gains significantly because of expanded choice, merchant acceptance and convenience

Source: Adaptation from a Deloitte research [15].

Table 2. m-Payment ecosystem: winners and losers in the various scenarios.

	MARKET	TECHNOLOGY	PROS	CONS	PARTNERS
Google Wallet	The premiere mobile payment platform for Android handset customers	The Nexus 4G is already shipping with NFC chips that will interface with Google Wallet when it launches	Google Wallet will sync with Google Offers, allowing you to take your coupons and savings with you as you shop	No mention of support of VISA. No mention of iPhone support.	Google, Citi Group, MasterCard, First Data, and Sprint
ISIS	ISIS was founded as a coalition among AT&T, Verizon Wireless, and T-Mobile	Will run on any NFC enabled handset supported by the three MNOs	ISIS is working on a mobile wallet system that could store multiple credit/debit cards and allow the customers to pay with any of them	No mention of support of MasterCard, Discover, Amex	VISA and 14 additional banks and financial service providers
Cityzi	Cityzi was founded with the support of French Government (it is a pilot for 3000 users)	Run on Samsung S5230 and potentially on any NFC enabled handset	Open ecosystem with TSMs that allow many MNOs, Banks and Service Providers to join the ecosystem	Limited gains from small scale deployment	4 French MNOs, 3 USIM providers, 2 TSM , VISA, MasterCard, 6 banks, 2 Transport companies

Source: Adaptation from a Gplus research [4].

Table 3. Main m-Payment contenders in the US market.

7. Pilots and Trials

In the next sections, three initiatives, currently under implementation, are presented and discussed. *Table 3* shows the main contenders in the m-Payment sector in the US, according to a Gplus research [4].

7.1. Google Wallet

From a customer perspective, *Google Wallet* (*Figure 9*) is a mobile application that lets the handset be used as a wallet [18]. It stores virtual versions of the existing plastic credit cards on the handset, along with e-coupons, and loyalty and gift cards. Currently, the system is not open, in the sense that there is a fixed set of partners: Sprint (the MNO), Citibank (the card issuer bank), MasterCard and FirstData (the TSM). Google's idea is to make this system open, so that more partners can join the initiative. Currently, Google Wallet is available only with *Nexus S 4G* by Google, branded by Sprint and NFC-enabled. The main aim of Google Wallet is to enable customers to "tap and pay" at physical stores. During the check-out process, the customer taps the handset on the PayPass MasterCard terminal and Google Wallet transmits payment details using a secure, wireless protocol. Google Wallet does not need a network connection to make payments, but the handset needs to be powered on. Additionally, the customer does not see any cost directly connected to the Google Wallet application.

Source: http://www.google.com/wallet

Figure 9. Google Wallet.

Google Wallet supports two types of credit cards: most Citibank cards using the PayPass MasterCard contactless standard and the Google Prepaid Card. The *Google Prepaid Card* is a virtual card powered by MasterCard. This is a purely virtual credit card. Google aims at putting new kinds of virtual cards in Google Wallet.

Due to modification requirements of new partners, the Google Wallet system is continuously evolving.

Google Wallet can be disabled and credit cards can be removed. Personal information is stored into the Secure Element that is embedded in the Nexus S handset; moreover, Google Wallet enforces security by requiring the customer to enter a PIN.

The same rules that apply to unauthorized use of the plastic credit card, apply to unauthorized use of a credit card stored in Google Wallet, for example regarding customer liability.

Google Offers [19] are also related to Google Wallet. Google Offers are deals on products and services at local or online businesses. Offers can be redeemed at most stores, simply showing the offer to the cashier at check out. The cashier will either scan the offer's barcode or manually type it in. A mechanism for automatic redeem is planned. Of course, merchants must have agreed to Google program, by becoming *Google SingleTap merchants:* in this way, their customer are able to pay, redeem offers, and earn loyalty points, all in a single tap of the handset.

Google Wallet is going to establish APIs to:

- allow issuing banks to develop payment instruments to be integrated;
- enable transfer of offers, loyalty programs, receipts, and more at the Points of Sale.

7.2. Isis

Three of the largest US wireless service providers, namely AT&T, T-Mobile USA, and Verizon Wireless, have joined in 2010 to build a nationwide mobile commerce network, called Isis [21], using handsets and NFC technology. By bringing together merchants and consumers, the Isis network promises an enhanced, more convenient, and more personal shopping experience. Specifically, the idea is to constitute an open service that will be available to all merchants, banks, payment networks and mobile operators.

The proposal of Isis is based on four services (*Figure 10*):

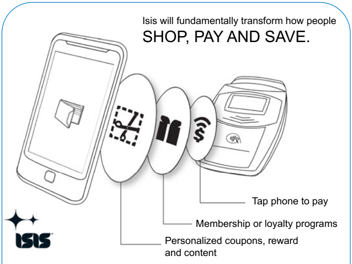
- *pay with handset*: to make a purchase it is sufficient tapping the handset;
- *travel light*: cards and coupons will be embedded in the handset;
- *shop smart and save*: the customer can set preferences to receive offers and savings;
- *see it*: transactions and balances can be consulted by the handset.

Isis expects to introduce its service in key geographic markets starting from the beginning of 2012 [20].

Salt Lake City, Utah is the location for the first trial.

Moreover, Isis has signed up an agreement with Utah Transit Authority (UTA) to make the entire UTA transit system Isis-enabled, marking the deployment of Isis as the first commercially available mobile transportation fare payment program in the US.

Beyond transport services, Isis announced a second trial in the city of Austin, Texas. Before the beginning of the trial, Isis officials demonstrated the technology to Austin merchants. Isis plans to roll out the Austin pilot during the first half of 2012.


Isis will fundamentally transform how people
SHOP, PAY AND SAVE.
Tap phone to pay
Membership or loyalty programs
Personalized coupons, reward and content
ISIS

Source: http://www.paywithisis.com/

Figure 10. The Isis project, a joint venture between AT&T, T-Mobile USA, and Verizon Wireless

Isis recently fundamentally changed the way it plans to bring NFC to market. Isis' original plan, announced in November 2010, called for the venture to develop its own mobile payments service, in competition with the existing payments networks and to recruit its own merchants for the new service. Rather than competing with banks and payments networks, however, the new plan calls for Isis to work with the payments industry to enable US card issuers (VISA, MasterCards, American Express, Discover), brands and merchants to offer NFC-based services to Isis subscribers.

7.3. Cityzi

Cityzi [22] is an NFC trial that has the sponsorship of the French Government. Thanks to the NFC technology, Cityzi promises to Nice inhabitants to use their handsets to pay in shops, enter the tramway, or get some relevant information about monuments. A lot of applications should be offered to customers in the subsequent months, enabling them to link physical and online words.

Nice has won government funding to become the "city of reference" for a pre-commercial phase of NFC testing, involving the local transport operator and three MNOs.

Cityzi started in the Spring of 2010. During the trial 3,000 residents can pay for tram and bus tickets and get information on routes and times using NFC phones. Additional NFC-based services are also available at local museums, cultural events and on the campus of the University of Nice, Sophia Antipolis. Further NFC-enabled services are expected to be rolled out gradually.

Bus and tram operator Veolia Transport and three French mobile operators, namely Orange, SFR and Bouygues Telecom are taking

part in the pilot along with the University of Nice. A number of French banks also took part in the project.
The main goals of the trial are:

- *Payments*. Consumers who purchase an NFC phone are able to make payments at any merchant's, equipped to handle contactless payments. Transactions are secured by PIN if the amount is greater than 25 Euro. MNO credit is used for e-Ticketing, for tickets costing less then 10 Euro.

- *Transport*. Transport tickets can be bought and real-time travel information can be accessed at each bus and tram departure point, in the Nice Region, via 1,500 NFC information points being installed across the local transport network. As well as travel information, the information points will also provide access to information services provided by the city council, events listings and the latest news articles.

- *Information services*. As well as the travel services, additional information services will be available, including an NFC tag-based tour of the old city of Nice.

- *Loyalty points*. Consumers will be able to automatically collect loyalty points when they use their NFC phone to make a purchase.

The French government planned to expand the Cityzi model to 15 French cities of average size in 2012.

8. Conclusions

This paper has analysed technologies, market trends, major players, trials and pilots in the Mobile Proximity Payment field.
What emerge from the analysis is a large number of opportunities available for the players of this ecosystem. Basically, proximity payment is going to revolutionize the payment as we know it today.
Banks, mobile operators, service providers, merchant, financial institution, and other subjects such as Google or PayPal are ready to get in the proximity payment game. All of them are betting on the capillary diffusion of the mobile handset, that is much more wider than the diffusion of credit cards.
Evaluating the winning model and the winning players is really difficult today, since the turmoil is remarkable.
It seems clear that large players such as Google will trace the direction of evolution of this ecosystem, but probably also banks and MNOs will have a primary role.

Biography

Corrado Guidobaldi graduated in Computer Engineering in 2000 and completed his PhD in Computer Engineering in 2004 at University of Naples Federico II. He has been working in the field of artificial vision and pattern recognition since 2000. He is author of several scientific publications in these fields. In 2004, he joined ST Microelectronics (ST Incard) where he worked in R&D for 4 years in the Smart Card field, where he authored 6 patents.
Since September 2007 he works at Altran Italia for the Telecommunications Electronics and Media (TEM) Division.
He is currently engaged as a consultant on behalf of an international Mobile Network Operator.

Acronyms

EMV	Europay, MasterCard and VISA
GP	Global Platform
GSM	Global System for Mobile Communications
GSMA	GSM Association
MNO	Mobile Network Operator
m-Payment	Mobile Payment
NFC	Near Field Communications
OS	Operating System
OTA	Over the Air
POS	Point of Sale
SD	Security Domain
SE	Secure Element
UICC	Universal Integrated Circuit Card

Glossary

- Check out: The process of payment in a store.
- FeliCa: A contactless smart card system from Sony in Japan, primarily used in electronic money cards. The name stands for Felicity Card.
- Secure Element: A smart card module (USIM, Embedded Secure Element or Separated Secure Element like a secure SD memo-

ry card) used for storing and accessing applications and data in a secure manner [6].

- Mobile wallet application: A mobile application that allows to make payments using the phone. Mobile phones needs to have a User Interface (UI) that allows a user to manage accounts and initiate contactless payments. These UI applications turn a mobile phone into something like a wallet full of cards because a mobile phone can contain many "cards" (credit, debit, prepaid gift card, other special stored-value accounts, public transit tickets and merchant-specific loyalty cards, just to name a few). The electronic wallet allows users to select the right card or application when making a purchase. Some mobile handsets being delivered today come with electronic wallet applications already installed [6].

Bibliography

[1]. Mahil Carr. "Mobile Payment Systems and Services: An Introduction". http://www.mpf.org.in/pdf/Mobile%20Payment%20Systems%20and%20Services.pdf

[2]. http://www.nfc-forum.org/home/

[3]. "Proximity Mobile Payments Business Scenarios: Research Report on Stakeholder Perspectives." Smart Card Alliance, 2008.

[4]. Gplus. https://www.gplus.com/Infographic/INFOGRAPHIC-Goodbye-Wallets-How-Mobile-Payments

[5]. Innopay, Telecompaper. "Mobile Payment 2010. Market analysis and overview." Mobey Forum, 2009.

[6]. "Trusted Service Manager: The Key to Accelerating Mobile Commerce". First Data White Paper, 2009.

[7]. "GlobalPlatform's Proposition for NFC Mobile: Secure Element Management and Messaging". White Paper, 2009.

[8]. GlobalPlatform Card Specification v2.2.1.

[9]. http://www.nfcnews.com/2011/05/23/proxama-launches-x-men-nfc-posters

[10]. http://www.cityzi.fr/

[11]. http://www.nearfieldcommunicationsworld.com/list-of-nfc-trials-pilots-tests-and-commercial-services-around-the-world/

[12]. http://www.groupon.it/

[13]. http://www.groupalia.com

[14]. http://openpr.com/news/169311/Instant-Winning-a-new-way-to-communicate-for-companies-and-clients-with-NFC-technology.html

[15]. "Cell me the money: Unlocking the value in the mobile payment ecosystem". Deloitte, 2011. http://www.deloitte.com/us/cellmethemoney

[16]. "Essentials for Successful NFC Mobile Ecosystems". NFC forum, 2008.

[17]. http://mashable.com/2011/07/08/the-future-of-mobile-payments-infographic/#

[18]. http://www.google.com/wallet/

[19]. http://www.google.com/offers

[20]. http://www.nearfieldcommunicationsworld.com/list-of-nfc-trials-pilots-tests-and-commercial-services-around-the-world/#usa

[21]. http://www.paywithisis.com/

[22]. http://www.cityi.fr

Appendix A:
NFC Technology Overview

A number of proximity protocols is currently supported by mobile handsets. The most common are: Bluetooth, 2D code, RFID, NFC. From a theoretical perspective each proximity protocol can be used for performing mobile proximity payments, but currently there is only a real candidate: NFC.

The physical layer of NFC gathers a number of pre-existing contactless protocols already widespread and used for many years for e-Ticketing and e-Access. Thus NFC can be easily used for the interaction with turnstiles. Moreover, the community of partners interested in mobile proximity payment converged to develop a strong security environment based on NFC (see NFC Forum [2] for more details).

When the functions of a contactless card are combined with the wide variety of functions of an handset, the card evolves into a device whose resulting value is greater than just the value of the two devices added together [16]. This new defined device is an NFC mobile handset. It is an intelligent mobile network-enabled device that can connect with other NFC devices in close proximity and that can behave as a contactless credit card.

Customers can access myriad NFC services in their daily lives by having an all-in-one personal device that provides them with a highly personalized and interactive environment.

Compared to a contactless card issued by a single service provider, an NFC handset is a medium where multiple service providers are able to have their own services resident. This is the evolution from the "issuer-centric" model to the "user-centric" model.

It should be noted that the NFC handset alone is not enough for NFC services to be realized. The server systems that communicate with the NFC handset via the operator network are essential to enable remote provisioning of applications resident on the handset. The combination of an NFC handset, the operator mobile network and server systems makes up an NFC mobile system.

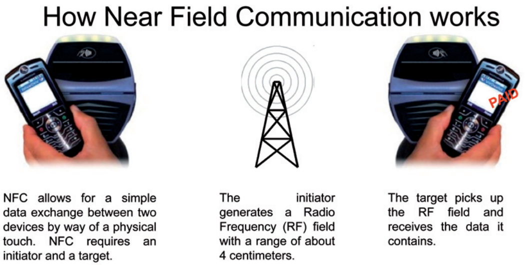
NFC operates in a range from 0 to 10 cm, on a frequency of 13 MHz, and a bandwidth of 424 Kbit/sec (*Figure 11*).

NFC can be used also for aims different from m-Payment but connected to it.

The NFC protocol can be used according to different operating modes. Three different operating modes have been standardized: Reader/Writer mode, Peer-to-Peer mode, or Card Emulation mode [2]. *Figure 12* shows the stack protocols for the three modes.

In the Reader/Writer mode, the NFC device is capable of reading NFC Forum-mandated tag types, such as in the scenario of reading an NFC Smart Poster tag. The Reader/Writer mode on the RF interface is compliant to the ISO 14443 and FeliCa schemes. The NFC device enabled to Reader/Write operating mode can be used to exchange information with other NFC-enabled devices. This mode can be used also for smart poster interaction. Posters can be used for providing information, couponing, advertisement, etc.

In the Peer-to-Peer mode, two NFC devices can exchange data. For example, a customer can share Bluetooth or WiFi link set up parameters or can exchange data such as virtual business cards or digital photos. Peer-to-Peer mode follows the ISO/IEC 18092 standard. A use case can be a Bluetooth headset with NFC support. NFC in this case can be used for pairing devices in an automatic way,



How Near Field Communication works

NFC allows for a simple data exchange between two devices by way of a physical touch. NFC requires an initiator and a target.

The initiator generates a Radio Frequency (RF) field with a range of about 4 centimeters.

The target picks up the RF field and receives the data it contains.

Figure 11. How an NFC handset works [17].

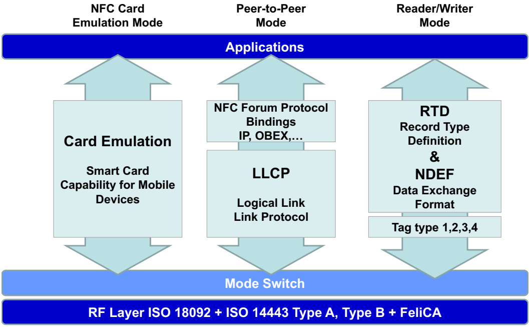


Figure 12. NFC stack protocol according to NFC Forum [2].

just getting them close to each other. Because of the characteristics of the proximity protocol, the handsets can be paired just by putting them in proximity. A further proximity can be used for the unpairing.

In the Card Emulation mode, the NFC device appears to an external reader much the same as a traditional contactless smart card. This enables contactless payments by NFC devices without changing the existing contactless infrastructure.