Technology Assessment

Near Field Communication

Convenience takes a great step forward. But what about the footprints we leave?

14 October 2008

Christian van ’t Hof and Wouter Schilpzand

Rathenau Instituut

Rathenau Institute

P.O. Box 95366
2509 CJ The Hague
The Netherlands

Telephone: 0031 70 342 15 42
E-mail: info@rathenau.nl
Website: www.rathenau.nl

The Rathenau Institute focuses on the influence of science and technology on our daily lives and maps its dynamics; through independent research and debate.

Preferred citation:
Hof, C. Van ‘t and W.F. Schilpzand, “Near Field Communication. Convenience takes a great step forward. But what about the footprints we leave?” The Hague, Rathenau Institute, 2008

Near Field Communication

Convenience takes a great step forward. But what about the footprints we leave?

Authors:
Christian van ‘t Hof - Rathenau Institute
Wouter Schilpzand - Technical University Eindhoven

October 2008

Preface

A single chip embedded in a mobile phone can now provide services ranging from payment to access, loyalty points and information retrieval. Near Field Communication (NFC) promises users the ability to 'just tap and go'. Lying behind this seemingly simple device, however, is a complex mix of organizational and technological developments that is only just beginning to take shape. The convergence of so many applications and providers gives rise to the obvious question, how will this innovation benefit its users? NFC allows for the merging of data relating to payments, locations and communications, and there is clearly potential for developing new services. It is necessary to ask, however, who will be managing users' personal data, and to whom will users be able to turn if things go wrong? These questions have yet to be answered.

This research forms part of the Rathenau Institute's project on the 'Digitalization of Public Places', which analyses the societal impact of upcoming digital technologies in the public domain. The concept of identity management is central to our analysis. Having described this concept, NFC technology and the players involved, we focus on two case studies involving NFC applications: those of Payter and Rabo Mobiel. We look at how technological and organizational convergence has occurred in practice; we consider the implications for users who want to manage their identities in an increasingly digitalized public space; and we ask whether government can play a role in helping users to do so.

The research is performed by Wouter Schilpzand, under supervision of Christian van 't Hof of the Rathenau Institute. They have written this report, with comments from Rinie van Est. Illustrations are made by Eva Broekhuizen. We thank the respondents who were willing to share their knowledge and opinion on NFC. They are listed in appendix 2. As research on a technical subject such as NFC cannot do without many technical abbreviations, we compiled a list alongside explanations in appendix 1.

Content

1 Research aims and context

This research on Near Field Communication (NFC) forms part of the Rathenau Institute's project on 'The Digitalization of Public Places', which analyses the societal impact of the increasing use of digital technologies in the public sphere. Our analysis focuses on the relationship between physical and virtual public places, between physical and virtual identities, and between digital convergence (that is, the convergence of applications and networks) and organizational convergence. The concept of identity management is central to analysing these relationships. In this chapter, we describe how this concept can be used to analyse NFC.

1.1 The context: managing identities in a digitally converging world

Cyberspace used to be heralded as a 'free space' in which one could escape earthly constraints. Now, as we surround ourselves with a plethora of digital devices for communication, navigation, access, and payment, cyberspace instead seems to be a virtual layer of our everyday physical space. Information and communication are increasingly becoming connected to times and places. Our virtual identities are developing beyond mere nicknames or e-mail addresses; increasingly detailed images are emerging of where we have been, what we have done, and, in essence, who we are. How, then, should we manage our identities in an increasingly digitalized world?

Living in a digitally converging world

At the end of the last millennium, cyberspace was feted as a virtual world that was free from the constraints of time and space. Regardless of one's location or the time of day, one could communicate with whomever one wanted, whenever one wanted, and access a seemingly limitless amount of information. Following Gibson's description of cyberspace (Gibson, 1984), one's point of access to the network was independent of one's cyberpresence, and one's virtual identity would continue to exist even after one had logged off. Users enjoyed unlimited mobility in cyberspace: they could be active in different places at the same time, and make friends with people that they would otherwise never have met and compile information from libraries all over the world.

This freedom from time, space, and other 'real world' constraints remains an important theme in cyberspace. We use terms such as 'surfing the web' or 'accessing the Internet' on a daily basis, so as to distinguish the real world from cyberspace. However, a new dimension to cyberspace is currently developing. Increasingly, parts of cyberspace are becoming linked to the physical world, as digital networks act to accommodate location-based services. The virtual world is no longer a separate entity that one can take time to explore, putting one's real-world activities temporarily on hold. Increasingly, cyberspace has become something that we both move and live in.

In a vision that complements the original idea of cyberspace, while it incorporates the new pervasiveness of digital networks, the International Telecommunications Union (ITU) has coined the phrase, the 'Internet of things' (Srivasatava et al, 2005). While this phrase does acknowledge the interconnectedness of things in the real world, it does not address the role of users in the network. Recently, the European Union (EU) incorporated the role of users in its vision of the Internet, which it termed the 'Internet of people'. Still, limiting our vision to the Internet alone could lead us to overlook other

digital networks that are converging into this same network. Perhaps the best concept for capturing the notion of users being in constant contact with multiple interconnected networks converging on mobile user terminals has arisen from research conducted by the Rathenau Institute in Japan: namely, the idea of the Ubiquitous Network Society (Schilpzand and Van 't Hof, 2008).

The concept of a Ubiquitous Network Society denotes convergence at three levels: those of applications, networks, and the organizations that support them. Phones, Internet access, messaging services, navigational devices, electronic payment and access cards all converge into the same hand-held devices, through the Internet Protocol. In this way, many previously separate service providers have been brought together. In short, in the Ubiquitous Network Society, users are constantly surrounded by forms of digital media that communicate with every user via one integrated network. Information thus becomes personalized and location-based by default.

NFC as an identity manager

In this digitally converging world, information about what were previously separate services is increasingly becoming linked. A user who is in almost constant contact with multiple digital networks might well wonder whether he or she has maintained any privacy. Given that the concept of privacy is quite problematic, owing to its subjective and ambiguous aspects, we have chosen to focus on the concept of identity management (Van ‘t Hof, 2007). We have found identity management to be a much richer concept than in its original sense as a technical concept used by service providers, offering a protocol for identifying users signing on to systems and authorizing access to services. Here, we use identity management in a more sociological sense, and focus on what actually happens to the profiles that people build up in information systems. We therefore define identity management as how persons, when interacting with a system, define what is known and what is not known about them to others using the system, and how this relates to what the system owner knows about them.

Other than the concepts of privacy and data protection, identity management can be used to analyse trade-offs for both users and providers of information systems. We have used this concept in case studies of Radio Frequency Identification (RFID) systems in both Europe (Van ‘t Hof, 2007) and Japan (Schilpzand and Van ‘t Hof, 2008). With RFID systems, such as transport cards, office access, or payment systems, users are often unaware of the considerable profiles that are built up in service providers’ databases. These profiles provide system owners with the possibility of feedback, and thus of a measure of control. For example, public transport cards can be used to analyse travel behaviour or inform direct marketing. That is not to assume, however, that this development is devoid of potential user benefits. Best pricing schemes, whereby users receive reductions for performing certain actions, can bring user benefits. Also, many users appear to value the security features that come with being tracked. Given that the technology does not dictate the use, however, it is characterized by ongoing negotiations between providers and users about who can gather what personal data to which purpose.

RFID smart card systems often offer users an anonymous service. In Japan, when Mobile FeliCa brought RFID technology to mobile phones, applications lost this neutrality and became personalized by default. This lack of anonymity also holds true for NFC. To subscribe to NFC services, one needs to identify oneself to the system’s owners. Subsequently, user profiles are generated on a personalized basis. Compared with the ‘traditional RFID’ in tokens or smart cards, NFC has the potential to take identity management issues to a new level, not only because of personalized services, but also because these services will become increasingly integrated.

1.2 The research

We decided to focus on NFC in this study because it is a technology in which many interesting developments are coming together. A number of applications are converging in mobile phones and are communicating via the same networks, prompting organizations to work together and users to take an active stance in managing their identities. Although empirical evidence for these developments is scarce, focusing on the Netherlands reveals two case studies that can shed light on how NFC convergence may unfold in the near future.

Research aims and questions

The aim of this study was to analyse NFC from an identity management perspective, and to sketch the roles played by businesses, users and the government in the digitalization of public space. We therefore posed the following research questions:

1. What is the current state of NFC development in the Netherlands?

What is the current state of the technology? What are the prospects and the estimated chances of success? What are the time frames set by companies involved? What kind of technical issues need to be overcome? (see conclusions: paragraph 6.1)

2. What kinds of identity management issues are raised by businesses involved in NFC?

Do technological and organisational convergence go hand in hand? Who is currently managing which personal data and how will this change in the near future? What are the perceived benefits of managing these customer identities? (see conclusions: paragraph 6.2)

3. What kinds of identity management issues are raised for users of NFC?

What kinds of personal data are generated in NFC systems? To what extent can users manage their identities by themselves? Are there technological options which may be beneficial to users, but are not taken into account by the companies providing NFC? (see conclusions: paragraph 6.3)

4. Is there a role for government in NFC developments?

Are identity management issues being resolved in the best interests of NFC users, or is there a need to secure these interests? Are there any areas where the market is failing in the current development of NFC, where the government needs to step in? Do current laws governing the use of personal data need to be reviewed in the light of NFC developments? (see conclusions: paragraph 6.4)

Case selection and methodology

Over the past three years, a number of small NFC trials have been carried out that are relevant to this research. In cooperation with KPN and NXP Semiconductors, among others, the Japanese bank, JCB, launched a mobile payments pilot in ten shops around Amsterdam's World Trade Center in September 2006. Approximately 100 JCB cardholders were given an NFC-equipped phone. At time of writing, the pilot was still underway, but had not expanded significantly since it had been launched (Stil, 2007; Paymentsnews.com, 2006). Roda JC, a Dutch Premier League football club, experimented with NFC during the 2005-2006 football season. Fifty loyal fans received NFC phones that could be used to gain access to the stadium and to pay for beverages and items from the club's shop (Emerce, 2005). JC Decaux, a firm that hosts outdoor advertising in bus stops and on billboards, has used NFC in a trial to monitor its staff's progress with work. The employee had to tap an NFC tag on his or her worksite, which

was then registered in an NFC phone. This allowed the employee's progress to be measured at the end of the day (Steegstra, 2008).

In home healthcare, meanwhile, Nedap Healthcare has developed an NFC-based application that allows care workers to upload patient information onto their phones. Using the network, the phone then downloads work schedules for each patient, and allows the care provider to tick off tasks that have been performed. At the end of 2007, Nedap had sold 11,000 NFC phones offering this application, with the largest purchaser being the home care provider Meavita (Balaban, 2007). NFC serves two purposes in this context. The first is to automate the process of checking and ticking off the relevant task on the schedule. The second objective is to automate the filing system used by care providers to make insurance claims. Nedap's product has gone beyond the pilot phase, and has become one of Europe's largest NFC-enabled services in terms of the number of users.

These trials have taken place in specific contexts, using NFC to address a particular scenario or problem in a closed environment. For the purpose of this study, we focus on NFC applications that involve broader identity management issues, on the grounds that these are aimed at daily practices in public places. Only two examples meet these criteria: namely, Payter, the scheme run by the firm of the same name; and the nameless Minitix-based scheme run by Rabo Mobiel. While these were not the first NFC pilots to be carried out in the Netherlands, these two firms stand out for the reason that they have used NFC to experiment with options for integrating services. Their systems actively explore NFC's potential in areas such as payment, ticketing, and content retrieval. In both cases, the schemes are poised for short-term rollout, and promise to be the start of something bigger.

Two case studies were conducted in order to shed light on the research questions listed above. We examined two NFC-based systems that are testing how NFC might be used to offer a wide range of services. Expert interviews held in the course of the research form the prime source of information for this report. Interviews were conducted with experts who are either directly or indirectly involved with developments in NFC technology. Not only did we interview the developers of the two systems, but we also discussed developments with security experts and policy advisors. A list of interviews held can be found in Appendix One. We also conducted a survey of the literature, in order to supplement the knowledge gained in these interviews. Hands-on experience provided a final means of data gathering. Our participation in the Payter pilot allows us to describe the Payter system from a user's perspective.

The introduction of NFC applications is currently at a precarious stage. At the request of some of the interviewees, we have not quoted actors' opinions of others. Given the generosity with which the respondents shared their knowledge, we would be loath to put them in potentially awkward situations.

2 How NFC works

NFC combines many different technologies: Radio Frequency Identification (RFID), Global System for Mobile Communications (GSM) technology, local networks, databases, and the Internet. These technologies work together when a user holds an NFC device close to another NFC device. In doing so, a seemingly simple gesture triggers a complex technological process. This process demands the involvement of many different organizations, so as to allow all of the technologies to communicate with one another in a single language. In this respect, as this chapter explains, in the case of NFC, the process of technological convergence goes hand-in-hand with organizational convergence.

2.1 NFC in practice

NFC enables users to exchange information by holding their mobile phones within 20 centimetres of NFC logos. Due to the fact that the communication range is so small, the user – in principle, at least – initiates all forms of communication. NFC technology integrates three functions with which consumers are already familiar: smart cards (such as ID-, debit- or access cards); the accessing of digital content (such as clicking with a mouse); and the establishment of communication between two devices (Bluetooth, for example).

Figure 1: NFC as a smart card

In card-emulation mode, an NFC device functions as a proximity card. In this mode, the NFC tag remains passive and awaits a signal from a reader/writer in the environment. When a user approaches a read/write terminal, the latter initiates a communication. This mode is suited to functions such as payment, ticketing, and access.

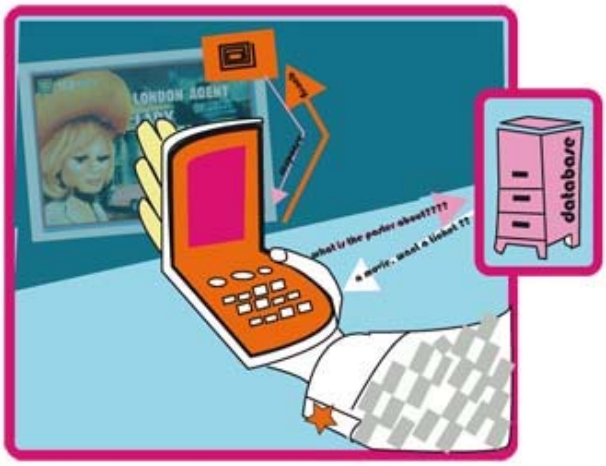

Figure 2: NFC for content retrieval

When using NFC to access digital content, a user will tap an NFC tag with his or her NFC handset. The typical use scenario for this function is known as ‘smart postering’. The user's NFC phone initiates the communication, and the tag sends back its content. Typically, this content will be brief, such as a URL, a few sentences of text, or the initiation of a phone call. In this mode, the user’s NFC device works actively and initiates the communication.

Figure 3: communication between NFC devices

NFC can be used to establish a connection between two devices, such as a mobile phone and a PC. The connection can either be used to transfer data using the NFC connection, or it can be used as a means of setting up another type of wireless connection, such as Bluetooth. The NFC Forum’s promotional presentations envisage this technology being used to transfer files such as photos or meeting agendas between NFC-equipped devices. Another potential use would be transferring funds from one electronic purse to another.

2.2 NFC’s technological components

NFC involves the convergence of many different technologies: RFID, GSM, local networks, customer databases and the Internet. Although each of these platforms has a separate language, shared standards allow them to communicate. Moreover, a new element has been added to the NFC technology chain, that of the ‘secure element’

(SE). This feature continues to be one of the major unresolved issues surrounding NFC. It should be noted that not all NFC-enabled services require all of the elements listed above. The images show the different layouts for the three ways in which NFC systems can be used. Card emulation (Figure 1) requires an active terminal with network access. Tag reading for content retrieval (Figure 2), meanwhile, may only involve an NFC handset and a tag. In some cases, the tag will refer to information stored online, and will trigger the option to open a web page via the mobile device. Lastly, an NFC system can consist of just two coupled devices (Figure 3). This is the case, for example, if two users decide to share holiday pictures or contact details using NFC. Given that various new services may be added in future, however, many different technologies may need to be aligned from the start.

NFC as the next step for RFID

NFC was mainly developed by Philips (later NXP) and Sony from 2002 onwards, and can be perceived as the next step in the development of RFID: that is, tags which can be read from short distances and used in smart cards or for identifying products. An RFID tag contains a small chip and an antenna to communicate on radio frequency. The chips are generally passive, which means that they are powered through induction in their antennae from signals in RFID readers. When an RFID chip is scanned, it provides a code that serves as a key for unlocking information about the chip's identity from a central database.

NFC works on the same proximity principle, and uses the same frequency as smart cards (13.56 MHz). The major difference, however, is that NFC serves both as an RFID reader and as a tag, and the chip is incorporated in a mobile phone. The degree of technical novelty is quite imperceptible to the user. Indeed, users appear to perceive NFC simply as an additional function of their mobile phones (Wendt, 2008). From a technological perspective, however, an NFC system is more than a chip that has been added to a phone or other form of terminal, whether this is fixed or mobile. Like RFID, an NFC system consists of two communicating chips: a network and a database. The chip is used as an identifier that unlocks information stored in a database, the type and extent of which depends very much on the nature of the service that is provided. Content can range from payment transaction histories to train timetables.

Embedded tags do not require much physical infrastructure. The tags only measure a few centimetres on each side and are almost as thin as paper. As such, they can be placed inside virtually any object. Simple tags can be obtained quite cheaply and have been commercially available for some time. As NFC penetration remains prohibitively low, smart postering has only been used in a handful of instances to date. When NFC breaks through, however, smart postering is likely to become a popular means of providing NFC services, given that implementation is relatively inexpensive.

NFC terminals present a different case, however, as they require both power and access to a (local) network in order to function. NFC systems are interoperable with contactless payment and ticketing infrastructures, due to NFC's backwards compatibility with Mifare and FeliCa. NFC's diffusion is thus facilitated in settings where a contactless reader is already operative, on the grounds that the costs of offering an NFC service are then lowered considerably. One example, described further in Chapter 5, is that of NFC ticketing at Rotterdam Zoo, which is offered by Rabo Mobiel using WheretoCard's contactless infrastructure.

NFC and GSM

By embedding the NFC chip and reader in a mobile phone, NFC technology builds on RFID by adding a screen, a keyboard, and network connections. This enables users to review past transactions or top up credit, whenever and wherever they wish to do so. Second, using mobile phones means that users have access to new functions using a familiar device and interface. In 2005, the number of mobile Internet subscriptions in the Netherlands exceeded the number of inhabitants (CBS, 2008a). When NFC stakeholders agree on a model for integrating chips and tags in handsets (an issue that we examine further below), there will be a rapid diffusion of NFC technology. Equipping a line of handsets with NFC costs between two and five euros per handset. While few users are likely to specifically request an NFC phone, the low price may stimulate the diffusion of NFC handsets even before NFC services have become widely available (Desertine, 2008). As we shall explain further in the section on NFC security, however, using a mobile phone as also carries risks.

NFC and the Internet

Currently, most handsets are equipped with the necessary technology and applications for accessing the Internet. While mobile Internet use in the Netherlands is not widespread when compared with East Asia, for example, the rate of use is steadily increasing (CBS, 2008b). Smartphones enabling users to check their e-mail are gaining in popularity, and an increasing number of websites are being adapted for viewing on tiny mobile screens. The increasing availability of technologies such as UMTS, HSDPA and WiFi has also meant a steady increase in connection speeds, enabling fast mobile Internet access.

Many NFC services require a mobile connection to the Internet in order to function. As explained above, this connection is most often made via an application on the handset, but it is also possible to establish a link to a web page. In general, according to Logica's Michel Bayings, data packages are not excessively large, and relatively slow GPRS connections are not perceived to present an obstacle to NFC use (Bayings, 2008).

NFC and other networks

While it is possible to integrate NFC well into existing networks, network access may need to be provided for. Take, for instance, NFC's role as an alternative means of payment. Network access to the PIN infrastructure is available at many points of sale in the Netherlands. The connections used by the PIN system can also be used for NFC terminals, meaning that no new networks have to be developed and installed. For functions such as access and ticketing, however, installing connections can be quite costly if no network connection has yet been established.

NFC and customer databases

There are two markedly different forms of service provider databases, depending on the type of service rendered. First, there are databases that hold information that can be accessed by users. This is the case, for example, with smart posters or other tagged items. Second, there are databases that store information about users. These databases are used for services in which NFC is used as a card emulator, mainly for payment, ticketing, and access. Such databases record the time, place and nature of a transaction. In most cases, users will be able to access at least some parts of their own files, enabling them to check their transaction histories, for example.

Given that NFC's unique selling point is its potential to integrate different services, these databases and their profiles have the potential to become very rich indeed. For example, a service provider offering both payment and public transport services would

be able to build user profiles encompassing data on both the time and place of shopping, and of users' movements.

NFC and its secure element

In order to identify a user and keep track of sensitive information such as their debit account and identification data, data need to be encrypted and stored in a secure place. This is known as the 'secure element', or SE. There have been proposals to embed SE chips in three different locations: in the phone, on the SIM, or on an external memory card, such as a micro-SD card. All three options serve the interests of different stakeholders and have both advantages and disadvantages. As such, where to locate the SE has proved to be one of the major unresolved issues hindering handset dissemination, an issue that we examine further in the next chapter.

3 The actors and issues involved in NFC

Owing to its unique mix of business development and technological innovation, the Netherlands offers an interesting case study for the development of NFC. First, the Dutch company NXP (formerly Philips Semiconductors) is a world leader in the manufacture of RFID and NFC chips. Second, the abundance of mobile communication devices in such a small country means that both telecoms companies and hand-held device manufacturers have a strong foothold in the market. A final factor is that electronic payment systems, especially those that use the PIN infrastructure, became prevalent throughout the Netherlands much earlier than in surrounding countries. Despite this unique mix, as we will see further below, getting different corporate cultures and high-tech devices to speak one language has been a challenging process.

3.1 The actors involved in NFC

Philips and Sony have spearheaded the development of NFC technology since 2002. Both companies have enjoyed considerable success with their RFID smart card systems, which are known as Mifare and FeliCa respectively. Philips' Mifare tags are used worldwide in smart cards for payment and ticketing. Sony's FeliCa, meanwhile, is mainly used in East Asia, notably in Japan, Hong Kong and Singapore. Unlike RFID card technology platforms, NFC technology is not proprietary, and potential users can adopt standards and specifications. When analysing both companies' omnipresence in the RFID and NFC fields, it is hard to avoid coming to the conclusion that they are doing much more than simply producing chips on demand; they are both seeking any opportunity to stimulate a growing market for NFC.

The NFC Forum, which was established in 2004 by Philips and Sony in conjunction with Nokia, is responsible for standardization and specification development. The Forum now has over 150 members, and aims to promote NFC by developing specifications that will ideally become international standards. The intention is to ensure that NFC devices and services are truly interoperable, and to promote the introduction of NFC services to the market. Considering the dominant roles played by NXP and Sony in the NFC development process, it will come as little surprise that NFC standards are backwardly compatible with both Mifare and FeliCa (NXP press release, 2004). Backward compatibility means that while NFC devices work on both Mifare and FeliCa, these latter two systems do not necessarily work on an NFC system. It should be stressed that this compatibility only exists in a technical sense. For functional compatibility, NFC applications need to be interoperable.

The NFC Forum has had considerable success in standardizing NFC technology. The NFC interface and protocol (often abbreviated as NFCIP) have been formalized in both ISO and ECMA standards, notably the 2004 standard, ISO 18092 / ECMA 340. Standardizing the air interface was just the beginning of the process. In the second half of 2006, specifications for formats for data sharing between NFC devices and tags were established. As NFC tags had to be compatible with Mifare and FeliCa, the Forum created a set of mandatory tag formats based on the ISO standard for proximity cards (ISO 14443) and Sony's FeliCa, and standardization of these is pending. Having undertaken an analysis of potential security threats to NFC, the NFC Forum is now also

developing encryption standards for secure NFC communication.

Standardization of the technology is only the start: to ensure interoperability and the smooth functioning of NFC applications, NFC functions also need to be standardized. Payment services offer a good example of this. The development of mobile payment systems has forced banks and mobile telecoms operators to cooperate and to establish a common standard for mobile payments. European banks have established the Mobey Forum for this purpose, whereas telecoms operators use the GSMA. Standardization expert Professor Jan Smits of the Eindhoven University of Technology in the Netherlands foresees difficulties ahead. He suggests that even if participating organizations are likeminded, it can be very hard to establish shared standards. Banks and telecoms operators have very different cultures; while banks aim to establish trust, telecoms companies focus on short business cycles (Smits, 2008).

At the time that this research was undertaken, there were fewer than 1000 NFC users in the Netherlands. These functioned as a testbed of potential users who were willing to take part in field tests. When, then, do companies predict that a critical mass of genuine users will emerge? In general, few disagree with the idea that NFC will break into the mass market at some point. The timing of this breakthrough is a controversial issue, however. First, one should note that forecasts regarding the number of NFC-enabled handsets differ widely, and in planning their NFC-related operations, actors use very different predictions with respect to NFC handset diffusion. Logica, for example, estimates that in 2011, 30% of new handsets will be NFC-enabled (Bayings, 2008). Schuitema's Van Mierlo, on the other hand, assumes that this number will be as high as 70% (Van Mierlo, 2008). Meanwhile, in an NFC Forum presentation, ABI Research estimated that there would be 500 million NFC-enabled handsets in 2011 (NFC Forum, 2007). In comparison, Nokia expects the total number of mobile phone subscriptions worldwide to exceed three billion for the first time in 2008. NXP offers a much more conservative estimate, predicting that only 10% of new handsets will be NFC-enabled in 2013 (Desertine, 2008).

3.2 Technological and organizational issues

With the convergence of so many applications in one hand-held device, the management of personal data becomes a tremendous challenge. Various issues relating to data protection and ownership have yet to be resolved. First, as mentioned above, there is ongoing controversy over where to place the Secure Element (SE) for the NFC data. The SE contains sensitive data, such as encryption keys for secure applications. Second, the sheer abundance of data flows calls for some form of management, possibly in the form of a new actor, a so-called ‘Trusted Service Manager’ (TSM). The identity and mandate of this actor are still matters of debate, however. Finally, even if and when these two issues are resolved, data protection will remain a sensitive issue.

The location of the Secure Element

Three potential locations are suggested in proposals for SE chip placement: namely, embedded in the phone, on the SIM, or on an external memory card, such as a micro-SD card. All of these proposals serve different stakeholders’ interests, and have both advantages and disadvantages. An alternative approach would be for an intermediary company to manage the SE, wherever the latter had been located on the phone.

Of the three scenarios, embedding the SE in the mobile phone would allow service providers the most freedom. It is unlikely that handset builders would attempt to charge service providers for using the SE. This option is supported by the Mobey Forum, the

international association responsible for promoting mobile financial services that is backed by many banks, and to date this has been the model chosen for introducing NFC phones. The SE is embedded in the phone in both the Nokia 6131 NFC model and in the new Nokia 6212 NFC model that will be launched in the summer of 2008. The disadvantage of this option, however, is that it gives little impetus to the integration of NFC in phones. Handset manufacturers do not stand to make money from NFC, but they do face (limited) costs. Discounting interoperability issues, in the absence of consumer demand driving phone sales, handset manufacturers will see few advantages for themselves, and will be unlikely to push the large-scale introduction of NFC. For users, moreover, there is the added disadvantage that many people change their phones relatively frequently. Opting for this scenario would thus necessitate addressing the portability of NFC applications. It is also unlikely that telecoms operators would be receptive to this idea; if SEs were embedded in phones, then the role played by telecoms operators would be substantially reduced to that of merely ensuring that data was flowing correctly from A to B.

Mobile network operators and their industry association, the GSMA, instead support a second option, that of embedding the SE on the SIM that is located in all GSM phones. In a smart move that has increased participating actors' support for the fledgling technology, the NFC Forum has sought close cooperation with the GSMA in developing specifications for applications. In 2006, 19 actors joined to form the GSMA Mobile NFC project, a group that included KPN. Perhaps most notably, this working group has developed a communication standard for the NFC chip in the phone and the SE on the SIM card, known as the Single Wire Protocol (SWP). The GSMA is using the SWP to actively experiment with developing a scheme for NFC-based mobile payment, called Pay-Buy Mobile. Placing the SE on the SIM is clearly advantageous for consumers, offering easy portability in an environment in which users tend to change their phones more often than their SIMs. The SIM's capacity might prove to be a limiting factor, however. This model places service providers at the greatest disadvantage. Telecoms operators are planning to let the capacity on SIMs to service providers in much the same way that real estate owners let apartments in buildings. According to Rabo Mobiel, telecoms operators plan to charge service providers between four and five euros per application per user (Armstrong, 2008c). Various actors, especially those striving for an open and accessible NFC system, have expressed dissatisfaction with this model.

A third option would be to embed the NFC SE in an external memory card, such as a micro-SD card. This would have the advantages of easy portability and significant capacity. However, few phones are equipped with a slot for an external memory card, and this option lacks backing from a powerful interest group. As such, this third option may well be overlooked.

An alternative would be for an intermediary company to manage the SE, regardless of where it had been placed. This solution was suggested by our research in Japan. In Japan, the Mobile FeliCa SE is embedded in the phone. When a user changes phones, an intermediary firm moves all of the secure data and applications to the new phone. This intermediary, Japan's TSM, was deliberately established to manage all Mobile FeliCa-generated data and to offer clients a single point of access in case of problems. Such an organization does not yet exist in the Netherlands.

From a user's perspective, a non-proprietary SE placement would be the best option. A lack of SE 'ownership' would ensure the fewest barriers to the initiation of NFC services. Few barriers to entry would also lead to a greater range of services offered, enhancing freedom of choice for consumers. An accessible SE might also stimulate

user involvement, whereby users could design their own services to share with others. This scenario, which resembles the Web 2.0 concept, would offer users the richest NFC experience. Going for a non-proprietary solution would mean ruling out the SIM option, and the other two options would best suit this scenario. Still, having an SE embedded in the phone would be the least desirable option with regard to portability. If the SE were to be placed on the SIM, however, telecoms operators could offer users the option of transferring the SE's contents when switching users. For easy portability, embedding the SE on an external memory card would be the ideal situation. As suggested above, however, the disadvantage would be that memory card slots are not universally available in mobile phones.

The Trusted Service Manager

Even if one were to solve the various problems relating to technology, interoperability, and chip placement, one major obstacle – the role of the TSM – would remain. The convergence of applications has created a need for a new, intermediary actor. In simple terms, the role of this actor would be to prevent conflicts between different applications and technological solutions. For example, if a user were to install two payment applications, the TSM would need to establish a protocol to prevent both applications from being charged at the checkout. The TSM would need to ensure that NFC applications functioned on all platforms. The figures below set out the TSM's basic task of reducing data flow and compatibility complexity. One would not necessarily need to establish a new organization in order to establish a TSM. Several firms – mainly system integrators, including Gemalto, Atos Origin and Logica – have suggested that they could assume the role.

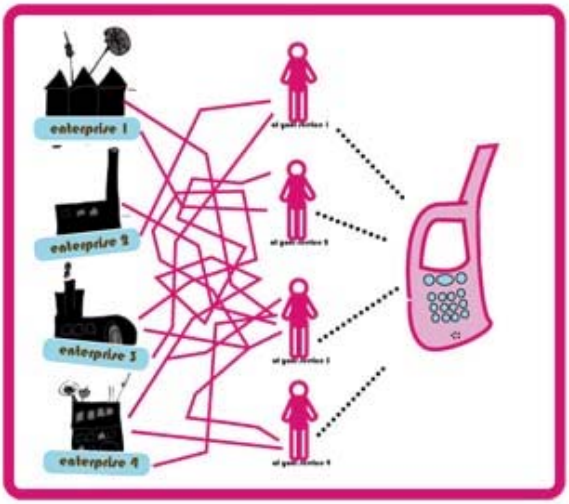

Figure 4: NFC on current networks may lead to chaos

A TSM would not be required during the initial phases of introducing small-scale services, experimenting, and learning. At this stage, the number of users, phone types and applications would be limited. All of the major players see the TSM as a necessary aspect of a large-scale rollout, however, as the potential for encountering different kinds of interoperability problems would then increase dramatically.

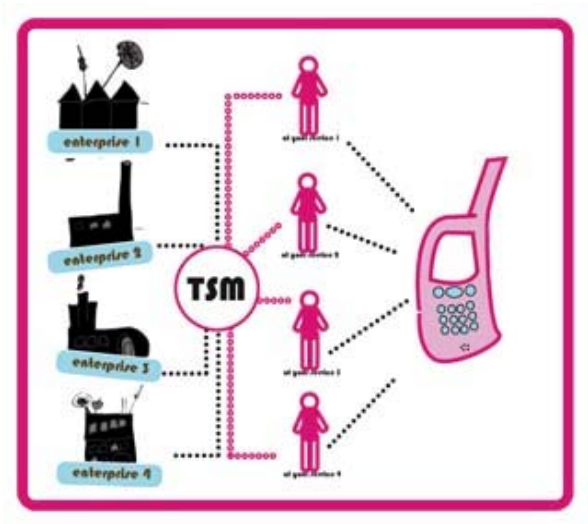

Figure 5: A TSM as intermediary for all networks

Various stakeholders with different backgrounds, most notably KPN, Logica and Rabo Mobiel in the Netherlands, have put significant effort into creating a TSM. The lengthy process has been characterized by discussions and compromise, as consensus is needed on what the TSM should do, how it should do it, and which organization would be best suited to the role. Also, the outcome of the (as of yet) unresolved chip placement issue will shape the TSM's tasks and roles, meaning that it will be hard to reach consensus until a solution has been found to this technological problem. If the SE-on-the-SIM option emerges as the dominant solution, notes Rabo Mobiel's Armstrong, then the TSM will face a daunting task. The TSM would then be the single point where service providers could access every telecoms operator's customers. As such, the TSM would need to ensure correct key management between all customers, with all their different phones (potentially amounting to hundreds), SIMs and telecoms providers (over 60 in the Netherlands alone). Armstrong predicts that this would be a logistical nightmare (Armstrong, 2008c). Most TSMs would be local organizations, representing NFC actors on a national or even regional level. In the case of internationally compatible NFC services (desirable, for example, for airlines or large payment schemes), TSMs would also face the enormous and complex task of cooperating to ensure that all data ended up in the right place.

Given that the TSM discussion is far from reaching a conclusion, it is currently unclear what the TSM's tasks will be. Certainly from a user's perspective, the TSM could play a valuable role. Logica notes that if NFC were to take off, many different companies would be represented on one user's mobile phone. In this case, the consumer would be unsure of whom to turn to if a malfunction occurred. In an NFC system, the TSM would be the obvious candidate for providing users facing difficulties with their phones with a single point of reference (Bayings, 2008).

Moreover, as stated above in the section on the SE's location, the TSM could assume responsibility for NFC portability. As such, it could transfer users' NFC applications from one phone to another, or even replace a user's NFC applications in the event of loss or theft. Furthermore, a TSM could offer a portal for the secure download of NFC applications. The TSM's role also proves interesting from an identity management perspective. Offering services such as replacing a user's NFC applications would entail the TSM managing the user's NFC application portfolio.

Data protection and security

Whenever personal data are exchanged, governments play a role in both protecting citizens from harm and monitoring data to promote the security of others. As a result, data protection laws ensure that users know which actors handle their personal data and for which purposes, and address the need to protect this data from abuse. The exchange and monitoring of data have also prompted data retention laws, which oblige providers to store data on payment and communication in the event that these are needed to aid police investigations.

The fact that NFC – which is personalized by default – creates a much more intimate relationship between consumer and service provider than most RFID solutions suggests that NFC might warrant extra attention from data protection policy makers. Such technology might allow companies to build up detailed consumer profiles and adapt pricing and marketing efforts accordingly, while consumers remain unaware of their methods. Despite this, the Dutch Data Protection Agency (the *College Bescherming Persoonsgegevens*, here abbreviated as the CBP) so far sees no reason to treat NFC differently from RFID, as NFC is in essence a member of the RFID family. The CBP has seen little progress in the RFID and NFC fields, and these topics were not included in the organization's 2008 working programme as a result (Nas, 2008).

With regard to the illegal use of data, concerns remain about the security of NFC devices. According to one article published by Philips, the main security risks associated with NFC are eavesdropping and data modification, both of which, it is argued, are easily countered using current key management systems (Haselsteiner, and Breitfuß, undated). Not everyone agrees with this view, however. It is believed that the mobile phone is the weakest link in an NFC system (Hoepman, 2008, Armstrong, 2008). Jaap-Henk Hoepman, IT security specialist at TNO, cites one security weakness as the fact that the NFC chip does not have its own interface. Instead, the NFC chip uses the mobile phone's interface and is thus commanded indirectly. This means that it is possible to install malware between the tag and the mobile, creating a phoney interface. As such, users have absolutely no way of knowing whether commands are being processed correctly (Hoepman, 2008).

Finally, as of 2008, Dutch data retention laws oblige actors to store data on phone conversations, Internet traffic and electronic payments for at least a year in an easily-retrievable format, on the grounds that the police may need to access them. The companies interviewed for our research project believe that these data retention laws are not applicable to NFC, even though the latter involves all three types of data flow mentioned above. If it turns out that the new laws do apply, however, then it remains to be seen how much effort will be needed in order to comply.

4 Payter: when money becomes information

In August 2007, Payter started operating in Rotterdam city centre. Roughly 50 locations, including shops, bars, restaurants and a parking garage, began to accept payment with Payter using NFC-equipped mobile phones. Starting with around 500 users, by May 2008 the scheme had expanded to around 700 users (Starkenburg, 2008). Payter's vision focuses on customer loyalty and advertising, while payment services are seen as a 'necessary evil'. In a bid to achieve a critical mass, Payter provides new users with a complimentary Nokia 6131 NFC phone, and offers stores subsidized infrastructure. Payter has been portrayed as a pilot, an image that leaves room for experimentation and that has perhaps prompted a more forgiving user response to start-up glitches and hiccups. The scheme's rollout is permanent, however, and at the time of writing, Payter was expanding to other Dutch cities.

4.1 The actors involved

Payter is a start-up firm that is backed by the investment agency, Borghols. Thanks to its start-up nature, the firm is versatile and agile, and able to plan, launch and expand its activities rapidly. Payter perceives its independence from banks and mobile network operators to be one of its key assets, allowing it to open up its system to every interested potential user. In addition, independence allows Payter to act quickly, unbound by the routines and rules imposed by vested interests and business culture.

Payter's founders have a background in the development of loyalty programmes and gift certificates, and their relationship with their investor dates from this period. Payter's vision and business model also reflect this background. The company's slogan, 'Your phone as a wallet' (Hendriksen, 2008), refers to the wallet in the broadest sense of the word; not only as a form of mobile payment, but also in terms of loyalty, coupons and content retrieval. Payter does not aim to make money by offering money, but by offering advertisement solutions that use both the wallet and the phone alike.

A promotional video on Payter's website clearly sets out the company's vision of the future. Payter aims to become a system for mobile payment and ticketing, intertwined with on-demand advertising. The company is also developing peer-to-peer payment, so that vendors can create mobile points of sale. Payter's vision is fully centred on loyalty and advertising. Mobile communication and mobile payment are tools for allowing consumers to interact directly with advertisers, and vice versa. Loyalty systems can be easily integrated with and used in NFC systems, with automatic point collection or price reductions at the checkout.

The benefits to business are obvious, as advertisers are offered a direct link to consumers. In this way, coupons retrieved from interactive commercials on television and from smart posters are stored on the user's phone. These coupons are only stored if the user so wishes. The user's phone has to physically approach the embedded tags containing the coupons via a near touching point, and the user has to give consent by tapping the poster or the interactive television set. As Payter's business model is entirely advertising-based, the company is able to offer payment at virtually no cost. Carpenter claims to be able to deliver payment for free. Rather than risk clashing with

the Dutch banks that own the PIN system, however, Carpenter has decided to offer payment at rates comparable with those for PIN (Carpenter, 2008).

In the long run, Payter aims to become an open framework offering potential service providers a system for making secure mobile applications. For example, a company could use the Payter system to establish an NFC loyalty system. In this case, a user could open the Payter applet on the phone and choose from one of the payment functions offered via Payter by Maestro, Cirrus, or other such schemes. Carpenter sees the Netherlands as a test market for this long-term vision. He is busy opening an office in Dubai, and is conducting negotiations with a view to starting a project in Spain.

Payter is backed by private investors, a fact that leaves many other actors relatively sceptical about the model's durability. As a start-up firm in a start-up field, unlike many of the well-established companies experimenting with NFC, Payter lacks a historical context. Other actors find it hard to assess how serious Payter is, whether the system is durable, or whether it is a mere means for investors to make a 'quick buck'. This seems to generate a feeling among some actors that might best be described as mixture of slight unease and curiosity. When Payter first sought media attention with news of its launch (memorably one day before the Rabo Mobiel pilot was due to give its press conference), some actors were concerned that should Payter fail, this would reflect badly on other NFC initiatives.

Moreover, given that Payter claims to have developed an advertising-driven business model, most actors are surprised by the fact that Payter's clients pay a monthly fee. For many other actors, the old saying, 'seeing is believing', holds true in this case. On the other hand, some have praised the speed and agility of Payter's operations, which stem from its start-up nature. Both NXP and KPN have applauded Payter for shaking up the market and for instilling a sense of urgency in the other players.

4.2 Payter in practice

When applying for Payter's services, customers complete a form with their personal details, and provide a copy of their personal identification. The signed contract allows Payter to withdraw funds from users' bank accounts when users top up their credit. Users agree to pay a monthly administration fee of €2.50. Until recently, Payter also charged €0.70 each time users recharged their accounts, but this fee was dropped in April 2008.

Payter uses a prepaid system that works in a similar way to Chipknip. Users have to charge their accounts before they can spend any money, and can top up their credit via mobile Internet, using the applet on the phone. Users have to identify themselves twice in order to charge their accounts: first when opening the Payter applet, and second when confirming the top-up. It should be stressed that unlike the Japanese applications studied in this research, Payter stores the value in a database, rather than on the phone itself. This practice lessens the risk of skimming. When using the Payter applet to check one's transaction history or current balance, the phone's mobile Internet connection briefly connects to the Payter server.

In order to conduct a transaction with Payter, a user enters a PIN code to open the application on their mobile phone. Touching the Payter terminal, which is recognizable by its logo, initiates the transaction. The transaction is subsequently confirmed on the mobile phone's keypad. Tag reading, such as via smart posters, only requires tapping.

About 50 shops, restaurants, and bars accept Payter as a payment method. Some shops, such as the supermarket chain Albert Heijn, have installed Payter terminals at all checkouts, while others provide more limited services. Albert Heijn has demonstrated the greatest enthusiasm for experimenting with Payter. As of May 2008, billboards promoting weekly recipes and featuring smart tags have been placed at the entrances of participating stores. By tapping smart tags, users can send SMS messages to receive text messages containing lists of recipe ingredients. At the same time, users receive e-mails containing cooking instructions. Payter's users also receive Albert Heijn's sponsored magazine via the mail, which features the same tagged recipes. This is the first smart postering application that Payter has supported.

Besides being used in shops, Payter is also accepted in the Q-park parking garage at the Beursplein in Rotterdam. Q-park, in cooperation with SKIDATA, had previously used NFC for parking during a pilot at an Amsterdam-based garage in 2006 (Libbenga, 2006). The Q-park procedure is as follows. When entering the garage, users tap the terminal with their phones in order to register their arrival. When exiting, customers choose either to tap the terminal at the exit, which automatically calculates and deducts the parking fee, or to tap the payment terminal and pay cash, thus using the phone like a ticket. When settling transactions with Payter, users automatically collect Payter's loyalty points under the 'Tsjing' scheme. Users can then use these points to buy gifts from the Payter shop. Launching Tsjing has enabled Payter to gain experience with creating NFC loyalty, experience that the company may use in the future when hosting other companies' loyalty schemes.

4.3 Payter: into the near future

The first Payter wallet was very basic, allowing users to review the current balance and recent transactions, and providing a button for topping up the account. When Tsjing was launched some months after the start of the payment service, Payter installed an additional applet alongside the wallet. In May 2008, the original payment and loyalty applets were replaced with a single applet that had been developed and distributed over the air in partnership with the Singapore-based firm, Cassis. From a user's perspective, this update was similar to updating software on a PC: customers received a text message, pushed an 'agreement' button, and the download and installation proceeded automatically. In addition to integrating the payment and loyalty applets, the new wallet offers some of the services featured in the company's promotional video. Payter now provides a coupon section in which users can download and access coupons, which typically offer reductions on products for a limited time period. For the time being, Payter is offering coupons via its wallet and its website, but it is likely that the product will be extended to smart posters and other media.

Together with launching its new wallet, Payter has upgraded its back-end system so as to be able to handle one million users, and to accommodate payments made at 120,000 shops (Carpenter, 2008). This upgrade will occur on the eve of the expansion of operations to five large cities in the Netherlands. In the second half of 2008, Payter will start operating in Amsterdam, Den Haag, Utrecht, Eindhoven and Arnhem. It is not yet known what the scale of the rollout will be, and how many stores will participate.

Payter has purchased a large number of Nokia 6131-type NFC phones for future users. The firm intends to follow a similar strategy to that which it adopted in Rotterdam, offering free phones to users who commit to using the system on a regular basis. However, being limited to a single type of phone is thought to present an obstacle to the rapid diffusion of NFC technology. As an interim solution, Payter will shortly offer users add-on NFC tags that can be fitted into non-NFC phones. Acting as unique

identifiers, these non-integrated tags will offer users card emulation services (in Payter's case, this means payment and loyalty). Tag detection is not possible with add-on tags, as the latter do not support an active mode. While phone and tag cannot communicate directly when a tag is placed onto a non-NFC phone, Payter's system is very back-end based as it is. Most data are stored in databases that users' mobile phones connect to, rather than on users' phones. Given the fact that Payter's payment processing system is back-end based (that is, value is not stored on phones, but in Payter's database), peer-to-peer payments – when they do become available – will not be genuinely peer-to-peer, as they will be filed in the database and logged.

Payter is less than enthusiastic about the payment aspect of its system. The company perceives offering payment as a necessary part of creating value for users, but the process is complex and offers Payter few advantages. The company would prefer to focus on advertising and leave the payment aspect to others. Despite this – and this view is frequently expressed by NFC actors – it is necessary to provide payment facilities in order to create an NFC system that will catch on with users. The expectation is that users will not acquire NFC phones and subscribe to NFC services on a large scale unless a mobile wallet is part of the deal. As suggested above, Payter wishes to become a platform that can be used by others to provide services. Rabo Mobiel's Chief Technical Officer (CTO), Dan Armstrong, is sceptical about this aim: 'the only true asset banks have is trust. They will not risk using a system developed by a firm that does not (yet) hold the explicit trust of banks' (Armstrong, 2008c).

So long as Payter fails to find a partner that will take care of the payment aspect of its business, Payter will provide the service itself. It is likely that Payter will continue to operate a prepaid system, as the company has no ambition to become a bank. The latter would require going through the difficult process of obtaining an EGI licence. Moreover, Payter is somewhat sceptical about the organizations involved with payment. In many respects, the company is keen to remain on good terms with the banks, as failing to do so could have negative consequences. Payter's payments are handled by Equens, a large payment processing firm that is reputedly heavily influenced by the banks. The same holds true for CCV Holland, the company providing shops with point-of-sale terminals. Given that Dutch banks are CCV's prime customers, CCV would be unlikely to engage in activities that would conflict with the banks' interests.

4.4 Identity management issues

The Payter application features a convergence of services: payment, loyalty systems, and coupon-based and value-added advertising. The latter service features an advertised product, such as Albert Heijn's recipes. Coupon-based advertising allows users to load coupons onto their Payter accounts via the Internet or smart posters. Payter has also promised a ticketing service, but so far, this has not been established. The convergence of payment and services is an interesting concept; in the process, money becomes loaded with increasing amounts of information. The trend started in the 1980s with the advent of cashless transactions, when the time, place, and nature of a transaction could be logged. Payter's system adds an extra layer of information: money, or rather the payment system, becomes a marketing tool. Payter offers payment services with the express goal of creating a customer base that advertisers can then target.

Has this convergence of applications caused organizational change? We would argue that it has, to a certain extent. No organizations in the Netherlands offer payment in such a way, using payment as a tool in an advertisement-based concept. Offering services in order to build a platform for advertising is not new, however, and the

Internet offers many examples of this strategy. Google provides many of its services for free, for instance, while exposing users to advertising. One can also find real-world examples, such as those free newspapers that update readers on current affairs and are funded by advertising. Payter has taken this model a step further and made it more personal. Rather than offering advertisers a platform for broadcasting ads, Payter offers a means of directly contacting consumers.

From an identity management perspective, the notion of addressing advertising to individuals is an interesting one. Users only receive ads when they tap the relevant tags, thereby giving their consent. In this respect, the identity management trade-off is an obvious one. Users receive a direct reward for expressing their willingness to interact with a service provider. Rather than being subject to the steady background noise of advertising in the public arena, users can actively decide which ads they are willing to receive and which they are not.

The NFC model developed by Payter has a distinct advantage over RFID smart card systems. At the touch of a button, users can request to view a list of recent transactions. This offers them more information about how they have used the application. The fact that such knowledge is not exclusive to service providers places user and provider more on an equal footing than is the case for most RFID cards.

With a view to identity management, Payter's intention to become a platform offering many different services does warrant attention. There are certainly user benefits to having integrated services across a wide range of functions, and having one actor ensuring that everything is working as it should. Using a single system for diverse services, however, creates a potential risk in the form of a large digital footprint: that is, one database containing data on many different aspects of consumer behaviour.

From a user’s perspective, it is important that the consequences of tapping a tag are always made clear. In the case of Payter’s tags in Albert Heijn, for instance, customers are contacted via their private e-mail addresses, as well as via messages on their phones. Users should always be made aware of what will happen when they tap a tag. Data provided to a service provider for administrative purposes may simply be used for getting users’ feedback, for example, or for marketing purposes. Although such uses are adequately covered by data protection legislation, they should be monitored carefully. Law enforcers might also request access to data, so as to undertake surveillance activities. Even though the intention is to serve the good of the community, such uses should not go unchecked. The saying, *Quis custodiet ipsos custodes?* (who watches the watchmen?), is clearly highly relevant here.

On the other hand, Payter might also offer users an opportunity to shield their spending data from the government. One interesting scenario might arise if users were able to exchange loyalty points using an NFC peer-to-peer function. In this case, users could exchange points at rates that they had set themselves. On a large scale, this could lead to informal exchange rates by which different kinds of points could be exchanged. Moreover, if loyalty points were to become easier to spend and could be exchanged for real items, this could lead to a scenario in which people could use them as virtual currency for paying for goods or services, thus enabling users to dodge taxes. While with peer-to-peer money transactions, payments are logged in the payment service provider’s back-end system, no such regulations cover loyalty systems.

Logging loyalty transactions as such is a relatively straightforward process, as – in a similar way to payment – points are moved from one back-end account to another. However, registering an exchange, whereby one scheme’s loyalty credits are

exchanged for another scheme's credit, is not so simple. Kleijmeer (2008) of De Nederlandsche Bank mentions that if such a scenario were to arise, loyalty points could possibly enter the money domain, and a much stricter regulatory environment would ensue. The likelihood of such a scenario, Kleijmeer notes, is reduced by the fact that most loyalty programmes are characterized by rapid inflation. Airmiles, for example, represented much more value ten years ago than they do today.

5 Rabo Mobiel: reducing cash payments while maintaining trust

The Dutch bank, Rabobank, launched Rabo Mobiel in 2006 as a locus for long-term innovation. The company developed a system based on MiniTix, Rabobank's system for digitally processing small payments. Rabo Mobiel conducted several pilots in different settings, including vending machines, a snack bar, and, in the most extensive pilot to date, a supermarket. Rabobank is aiming to reduce the costs associated with small cash purchases. Evidently, Rabo Mobiel is in less of a hurry than Payter. As a bank, trust is Rabobank's main asset. The importance of launching a product quickly should be balanced, in Rabo Mobiel's view, with the need to create a viable NFC system.

5.1 The actors involved

Banks are interested in mobile banking and mobile payments for two reasons. First, given that mobile phone prevalence and functionality continue to increase, banks are keen to offer mobile services so as to make banking more accessible and therefore more attractive to customers. The result, it is hoped, will be improved customer relations and loyalty. 'When young people go out, they return home if they've forgotten their mobile phone. If they've forgotten their wallet, they borrow some money from friends,' says René Bruinsma, a senior manager at Rabo Mobiel. Rabo Mobiel offers mobile phone subscriptions with low calling rates to individuals with Rabobank accounts. The second reason is that making cash payments is very expensive. In the EU, 82% of transactions in shops are still conducted using cash (Hensen, 2007). It is estimated that in the EU, the handling and logistical costs associated with cash payments annually approach 50 billion euros.

Rabobank has created a system, MiniTix, for processing small payments in a digital environment. MiniTix can be used in different settings, including online and mobile payments. In using MiniTix, Rabobank hopes to emulate the success of 'Rabo Direct Betalen', an online payment system that has been adopted by other Dutch banks under the 'iDEAL' brand. An online MiniTix wallet is already available to customers who do not have a Rabobank account. Rabobank has ambitious plans for MiniTix. If enough support can be gained from other Dutch banks, Rabobank will offer MiniTix as an alternative means of payment processing in the Single European Payment Area (SEPA). The two current payment processing systems that comply with SEPA demands, Mastercard and Visa, are both based in the US. MiniTix, Rabobank promises us, is just as well-suited to the job as its rivals, is cheaper, and is based in Europe.

According to Dan Armstrong, Rabo Mobiel's CTO, it is the cooperative character and lack of stockholder interference that make long-term initiatives such as Rabo Mobiel possible. Unlike Payter, Rabo Mobiel has taken a cautious approach, developing many small pilots and involving many different stakeholders. Typical of this approach is the fact that the pilot partners joined via the RFID Platform, the RFID and NFC industry association for the Netherlands. This platform was responsible for external

communication on the Molenaarsgraaf trial (see further below). Furthermore, the platform helped to hold the group together.

For small-scale tests using vending machines, Rabo Mobiel collaborated with brands such as Febo (snacks), Coca Cola, and their associates. The largest pilot was led by Schuitema, a company specializing in the logistics of fast-moving consumer goods. Schuitema identified a suitable location at a supermarket in Molenaarsgraaf, and was tasked with integrating NFC readers into the information terminal in both their back-office system and in a bottle-return machine. Schuitema had previously piloted new technology in cooperation with the RFID Platform in the form of the Vers Schakel project, which had applied RFID to the supply chain. The company sees NFC as a technology that has the potential to make consumers' lives easier. Retailers, meanwhile, can benefit from NFC in two ways, says Van Mierlo: by strengthening customer loyalty, and by saving money due to sleeker logistics.

Rabobank provided payment traffic capabilities linking the store and the bank, and communicated with the payment processor, Currence. Together with Banksys, a payment terminals supplier, Rabobank was responsible for integrating the contactless reader into its system. Rabo Mobiel supplied half of the pilot participants with a mobile phone, while the telecoms operator KPN supplied the other half. KPN also brought practical knowledge to the project: the company had built up experience in NFC payments as a partner in an ongoing payment pilot in Amsterdam's World Trade Center (WTC), together with the Japanese bank, JBC.

KPN expects NFC to benefit its business in a number of ways. The company is closely involved in the GSMA's plan to place the SE on the SIM, thus giving ownership of the SE to telecoms operators. Furthermore, KPN aims to learn how to become an NFC system and infrastructure provider. For instance, the company plans to install and host NFC payment installations in shops, and to provide the necessary infrastructure. One of NFC's intangible benefits, suggests KPN, is that NFC supports the business of being a telecoms operator by strengthening the prevalence and position of mobile handsets (Steegstra, 2008).

In the Molenaarsgraaf pilot, NXP (formerly Philips Semiconductors) provided the NFC readers and the supporting infrastructure. The company also assisted with developing the necessary NFC applications. As suggested above, NXP is one of the firms that had originally developed NFC and had established the NFC Forum, and is a major stakeholder in NFC chips and systems. In a bid to help the market take off, NXP is actively helping to set up pilots, bring interested parties together, and provide information about the technology. NXP's Desertine (2008) states that most actors now understand what NFC is and what it can do. In his opinion, the pilot phase is nearing its end, and NFC services now need to be developed and implemented.

Logica was tasked with the daily management of the pilot and was paid for this role, unlike the other actors involved. Logica developed the mobile phone application and, together with Rabobank, developed and integrated the payment application. Logica is interested in NFC for two reasons. First, as a consultancy, Logica is actively developing use cases for other companies. One of the main lessons that the company has learned, in this respect, is that it will be a long time before there is a mass diffusion of NFC technology.

5.2 Rabo Mobiel in practice

Rabo Mobiel has conducted several pilots using NFC transactions. The first test commenced in May 2007, in cooperation with Coca Cola and Cap Gemini. A Coca Cola vending machine was equipped with an NFC reader, allowing users to purchase drinks using NFC-enabled phones (and the appropriate MiniTix application). The vending machine was piloted in 19 different locations between April and October 2007. Another small-payments NFC trial was conducted at a snack bar owned by the Febo franchise, where a vending machine was equipped with an NFC point of sale. Febo's owners' interest in the pilot had been triggered by a Rabo Mobiel commercial the previous year, which had shown people in the street being asked if they could imagine using a mobile phone to buy a snack. The one-day pilot aimed to test two things. First, a hot snack vending machine is obviously a challenging environment for sensitive electronics. Dealing with the high temperatures involved proved to be one issue of concern, but this problem was eventually solved. The other aim was to test consumers' abilities to use the system. Clearly, hot snack vending machines owe their popularity to the speed with which consumers can obtain snacks. Using a mobile phone to buy a snack thus had to feel very instinctive for consumers if it was to have any chance of success. Users responded well to the process, in which they only had to tap the terminal and no further confirmation was required.

Rabo Mobiel has launched its latest NFC product at Diergaarde Blijdorp Zoo in Rotterdam. In this context, NFC is used for access and content retrieval, as users with NFC phones and Rabo Mobiel contracts can buy tickets to the zoo online. Information about the purchased tickets is then linked to the user's NFC account. Then, when entering the zoo, an NFC terminal checks the tickets and grants access. In the zoo, NFC tags at certain locations provide extra information about animals or offer premium content, such as seal ringtones. As the Rotterdam branch of the Rabobank is one of the zoo's main sponsors, the two companies enjoy a good relationship. The electronic ticketing company WheretoCard had earlier provided Blijdorp with e-tickets, and had installed an NFC reader for smart cards, meaning that no additional infrastructure was necessary. The smart tags were provided by Yoonison, a firm that offers personalized data-carriers, such as magnetic cards and smart cards.

The biggest NFC trial to date has been the 'PINnen met je mobiel' (PIN with your mobile phone) pilot, in which NFC played the role of a bankcard in a supermarket. Rather than working with the MiniTix wallet for small payments, this time, costs were directly debited from users' bank accounts. From a user's perspective, the system worked exactly like the PIN system. One touched the payment terminal with the phone, and then entered one's PIN number into the terminal. In addition to using NFC phones for checkout payment, customers could also use their phones to store the deposit value of returned bottles. Using an NFC terminal in the supermarket, this sum could either be wired to the owner's bank account, or it could be donated to charity. The pilot lasted six months and involved 100 participants, who rapidly caught on to the idea of payment using mobile phones. Learning to use NFC when returning empty bottles proved to be a little trickier but, according to Logica's Michel Bayings, this did not deter users (Bayings, 2008). On the contrary, this function proved very popular once users had understood the procedure.

The 'PINnen met je mobiel' pilot was on a different scale from the other pilots described above. Not only did 100 users participate for six months, but the scheme also involved many firms in addition to Rabo Mobiel. Participants included Schuitema, one of the RFID Platform's founders and owner of the Dutch supermarket chain, C1000; KPN, the largest mobile network operator in the Netherlands; systems integrator Logica MC;

NXP Semiconductors; and the Dutch RFID Platform. The pilot was a cooperative affair that took quite a long time to prepare and execute. Bart Schermer, who was then secretary to RFID Platform Nederland, the RFID industry organization in the Netherlands, recalls the long preparatory period. The consulting firm Logica, then Logica CMG, was one of the first actors to express an interest in NFC. Other firms, whose interest had been raised, insisted that the pilot should occur under the RFID Platform banner, so as to ensure equality between partners. Two potential pilot scenarios were developed: the first using NFC for ticketing, payment and information in a theatre, and the second using NFC in a supermarket. The supermarket scenario was chosen on the grounds that large numbers of customers do not return to theatres on a regular basis (Schermer, 2008).

Each party in the pilot bore its own costs, plus every party donated around 20,000 euros for shared expenses. Logica made the biggest expenses claim, as for this company the exercise was as much a business case as a pilot. The process leading up to the pilot was a lengthy one. The partners, with their different backgrounds and corporate cultures, had been discussing different possibilities for eighteen months when Van Mierlo, Schuitema's representative, assumed the lead. Rabo Mobiel had not existed when the partners first met and decided to cooperate; instead, Rabobank belonged to the group and provided the bank transactions. It was agreed that KPN would take responsibility for telecoms operations, supplying participants with NFC mobile phones. Rabo Mobiel's subsequent launch temporarily created a stir in the project team, as suddenly two telecoms operators were present. It was decided that each company would supply half of the customers with phones.

The aims of the trial were to learn about the maturity of the technology, to find a way to use as much of the existing infrastructure as possible, to learn how NFC might benefit both consumers and suppliers, and to study users' reactions (PINnen met je mobiel, 2008). The pilot used NFC in two ways: namely, for payment at the checkout, and for storing the deposit retrieved when a customer returned empty bottles. In the process, the participants agreed that the pilot's conditions should remain very similar to situations and procedures with which consumers were already familiar.

Molenaarsgraaf was chosen for the pilot for two reasons. First, all of the project partners could easily reach Molenaarsgraaf, due to its central location in the Netherlands. Second, as a supermarket in a small community, the C1000 in Molenaarsgraaf had a solid base of loyal customers who enjoyed a relationship of trust with the local owner. The supermarket manager was relatively keen for the pilot to take place. Participants aged between 18 and 68 were selected so as to represent both sexes and various ages. Some modifications had to be made to the shop floor: cash registers were fitted with a contactless point of sale; the bottle-return machine was equipped with an NFC reader; and an information and transaction terminal was erected in the centre of the shop.

The 100 participating shoppers used NFC phones to tap the bottle machine once they had returned their bottles, so as to load the deposits onto their phones. Users could then choose to use this deposit in one of three ways: they could use the transaction terminal to transfer the money to a charity; transfer it to their Rabobank account; or could proceed to the checkout and use the value of the deposit to reduce their shopping bill. Then, at the checkout, the phone functioned as a bankcard, using the PIN infrastructure to debit a user's bank account. As the pilot partners had opted to stay as close to shoppers' existing routines as possible, users validated transactions by keying their PIN numbers into the payment terminal, not into their phones. The application on

the mobile phone, which had been created by Logica, logged transactions so that users could view their shopping histories.

All of the actors involved were surprised at the ease with which users adopted the technology. A group of users even approached the organizers after the pilot had finished, explaining that they were disappointed that the scheme had ended and enquiring whether it could be continued. Satisfying this latter request proved to be impossible, as the pilot system was insufficiently integrated into existing systems, and the various components were only linked to the few computers that ran the applications. BSIS, Schuitema's IT service organization, concluded that greater integration would be needed between front- and back office systems in order to provide permanent NFC services.

Although the survey that was conducted at the end of the pilot is not statistically sound, due to the small size of the sample, it does provide us with some insights into users' responses. Schuitema's Van Mierlo tells us that participants consistently used their NFC phones for frequent transactions, with an average of more than three a week. About 20% of users required assistance when first using the system. Most found using their phone as a bankcard easy enough, but the procedure for using NFC to store deposits at the bottle-return machine proved to be slightly more counterintuitive. Despite this, the deposit function also yielded good results, and was met with a high level of user satisfaction. The two features that customers valued most highly were the increased speed of payment at the checkout and the NFC deposit function (customers often lose or forget to reclaim paper deposit tickets) (Van Mierlo, 2008).

5.3 Rabo Mobiel: into the near future

Most of the people we interviewed for this research agreed that the NFC trial phase is over. This is not a view that is held by Rabo Mobiel, however, and the company is planning further trials. In June 2008, Rabo Mobiel launched the first mobile MiniTix application. It is likely that this downloadable Java application will also be used as the interface for Rabo Mobiel's future NFC services. The second half of 2008 will see Rabo Mobiel launch a new range of NFC pilots and products. A large-scale payment trial in partnership with Albert Heijn is planned for the second half of the year, in which NFC in conjunction with MiniTix will be used for self-scanning checkout, and which will involve 500 users.

2008 will also see the introduction of some new NFC-enabled ticketing and access products. Starting in the summer of 2008, NFC (as well as Mifare-enabled smart cards) will be available at bicycle storage systems in three cities. Later in 2008, Rabo Mobiel will launch NFC parking in combination with access to museums in four cities. These ticketing and access solutions will be based on the system that was developed for Diergaarde Blijdorp, and will initially only be accessible to visitors with Rabo Mobiel accounts. Rabo Mobiel will also launch an NFC mobile loyalty programme, in cooperation with two existing loyalty programmes and four major retailers. These trials will be used to build up Rabo Mobiel's ability to move into rollouts (Armstrong, 2008a). The company is taking a cautious approach, as there are many challenges to be overcome.

Rabo Mobiel is not an overly popular telecoms operator, and has only sold a few hundred of its handsets. Armstrong is dissatisfied with the current Nokia model, the 6131 NFC. He regards it as a mediocre phone in most respects: decent, but not spectacular. Neither does Armstrong have high expectations of the new Nokia NFC phone that is to be launched at the end of the summer of 2008, the 6212 Classic.

Armstrong is particularly surprised by Nokia's decision to use a so-called 'candy bar' design (as opposed to the foldable 'clamshell' design), as opening a phone is a good way of mimicking opening one's wallet when engaging in an NFC transaction. On the positive side, Armstrong notes that to date, Nokia has launched at least two NFC phones with the SE integrated in the phone, rather than on the SIM or on a memory card. As a potential NFC user on a significant scale, Rabo Mobiel would prefer NFC to be embedded in the phone rather than in the SIM, so as to keep service providers' costs down. Having to pay NFC rent to mobile network operators is seen as a potential obstacle to the diffusion process.

Being both a bank and a telecoms operator, Rabobank via Rabo Mobiel is well-placed to engage in the mobile payment market. This dual identity allows Rabo Mobiel to integrate telecoms and banking perspectives when developing its vision on NFC. It also helps to stimulate the diffusion of mobile payment technology, as there is an existing consumer base consisting of people with first, a Rabobank bank account and second, a Rabo Mobiel phone.

Rabo Mobiel has two goals with respect to its NFC pilots. First, the company aims to gain experience with NFC as a means of payment, access, ticketing and content retrieval. Second, the company intends to create a viable NFC system. In Rabo Mobiel's view, NFC technology should be both cheap and accessible to potential service providers and users. Integral to this vision, as discussed in Chapter Two, is the TSM's role – a view that is shared by most actors in both the banking and the telecoms sectors. Having a TSM will be necessary if NFC is to become an 'open' system involving many service providers and millions of users. Rabo Mobiel estimates that a TSM structure will emerge in 2009. The company predicts that a significant diffusion of NFC technology will only occur after this development, meaning that a critical mass will eventually form around 2011 (Bruinsma, 2008).

Like many other actors, KPN expects NFC payment to be the main factor stimulating the mass adoption of NFC technology. KPN's Steegstra points out that building a successful business case around payment is not a simple matter. Steegstra concludes that while there is little controversy regarding NFC's future role, the timescale remains unclear. For the time being, KPN sees two factors limiting NFC adoption. The first is the limited availability of NFC handsets, with only one model being commercially available and just a few others available for pilots. Steegstra's (2008) view is that handset manufacturers are tending to watch one another and wait for increased demand. The second limiting factor is the need for a TSM. KPN argues that a TSM is necessary for creating clarity for companies in areas such as application standards, what payment services should look like, and how they should operate. KPN has been very active in the process of setting up a Dutch TSM, but there has been limited progress to date, and the company fears further hurdles and a considerable period of time before success is achieved.

NXP does not share KPN's rather despondent view of the TSM. Setting up a TSM is a lengthy process, but Desertine thinks that progress has been made. In his view, compared with some other countries, the Netherlands faces a significant task in implementing NFC technology, as contactless infrastructure is still relatively scarce. In those environments where services are already offered via contactless cards, migration to NFC will be relatively straightforward.

Bayings from Logica MC does not anticipate a major rollout of NFC systems within the next two years. In the meantime, in his view, service providers should aim to develop use scenarios for small groups of users with which the service provider interacts on a

regular basis. To illustrate this approach, Logica cites a scenario that it has developed for KLM, by which frequent flyers can use NFC for checking in, boarding, and everything in between. Moreover, as an experienced system integrator, Logica is interested in becoming a TSM. Bayings (2008) foresees a significant role for the payment processor companies Currence and Equens, and urges them to take a more active approach.

Partly in cooperation with Logica, Schuitema is now developing two additional NFC services. The first consists of using NFC to unlock a shopping trolley, while the second consists of using NFC to provide information about products' ingredients in shops, by placing tags on shelves containing information about additives and allergens. Despite this, Van Mierlo predicts that organizational hurdles will delay the widespread diffusion of NFC handsets, and sees payment services as the key factor driving user adoption. As a potential NFC service provider, Schuitema is unenthusiastic about the GSMA's proposal to put the SE on a chip and then let SE capacity. He would prefer an open system that allows for a low threshold in the provision of NFC services.

5.4 Identity management issues

With regard to identity management, the Rabo Mobiel NFC system perhaps raises fewer concerns than Payter's approach. Rabo Mobiel does not share Payter's intention to offer many different services that are integrated with advertising. However, Rabo Mobiel's services are by default offered on a personalized basis, as users have to identify themselves in order to access services. Payment is always conducted on a personalized basis; opening a MiniTix wallet, for example, requires users to identify themselves using an e-mail address and a phone number. Consumers using the Diergaarde Blijdorp ticketing scheme have to identify themselves using their Rabo Mobiel telephone numbers in order to buy online NFC tickets. In a similar way to Payter, therefore, the relationship between service provider and user becomes more intimate.

This raises the question whether all users benefit equally from managing their identities using hand-held devices. In the case of mobile phones, the largest group of non-users is that of elderly people. Their reasons for not using mobile phones vary from feeling that they do not need to, to finding it too difficult to learn, and finding it physically difficult to operate a mobile phone. One surprising result from the Molenaarsgraaf pilot, however, was that the scheme had a high acceptance rate among older people. Apparently, even those older people who had not previously used a mobile phone were enthusiastic about using a phone as a PIN card (Wendt, 2008). The high adoption rate for this group can perhaps best be explained by the strong relationship of trust between the customers and the supermarket manager. In the absence of such a direct, trust-based relationship, one could hardly expect NFC to appeal to people who could not (or would not) normally use a mobile phone. Operating mobile phones does require some digital literacy and, in the absence of this, NFC technology becomes unusable.

Two of NFC's traits and its envisioned use mitigate the seriousness of this potential digital divide, however. First, for the foreseeable future, NFC is only intended as an alternative to existing systems or as a means of delivering premium content. In this sense, it makes little sense to push for use. Granted, users might miss out on NFC coupons or other price reductions, but that is the extent of the problem. A second mitigating factor relates to NFC's intuitiveness as a form of technology. Either the service is offered in the same way as before (for example, using a phone as a bankcard), or the service is activated by movement. In both scenarios, little learning is

required on the part of the user – an aspect of NFC that proponents of the technology are keen to emphasize.

One of the observations made by Rabo Mobiel during its Coca Cola pilot was that some people with NFC phones avoided getting too close to the vending machine, in case it initiated a transaction. This type of misunderstanding might be relatively insignificant while NFC technology remains scarce, but when the technology is widely available, users need to be (made) aware of the fact that NFC terminals usually have short reading ranges. On the other hand, the read range can be expanded to up to half a metre when a more powerful reader is used. Powerful readers could potentially be used to eavesdrop on people in an unauthorized fashion, implying that users should not be over-confident about devices' short reading ranges. Users need to be aware that NFC devices can behave as readers *and* as tags, and that just like with Bluetooth or any other wireless communication technology, having an 'always on' connection leaves people vulnerable to unauthorized reading.

The attempt to establish a TSM also raises identity management issues. If the TSM is an intermediary between service provider and user, then where will users' personal data be stored? Will the service provider maintain its own data, or will it be (partly) outsourced to the TSM? A further TSM-related issue is that of the role of data retention laws with regard to NFC communications. Most actors consider it unlikely that NFC transactions *per se* will be subject to data retention legislation (including, for example, Bayings and Bruinsma). However, as an NFC tap is often the start of a communication over another network, this technology is expected to generate a significant amount of mobile Internet traffic. Tapping a smart poster, for instance, might refer the user to a website or a phone number, both of which are subject to data retention laws. As such, data retention issues will become the responsibility of the telecoms operator that enables the Internet traffic to store these data, rather than that of the service provider. Depending on the TSM's eventual mandate and how data retention legislation develops, the TSM may also become (partly) responsible for data retention. At present, however, it is unclear how this scenario will unfold.

6 Conclusion: managing identity in NFC environments

Although it is still in its infancy, NFC offers interesting insights for the study of managing identities in a rapidly digitalizing public environment. With so many technologies and applications coming together in hand-held devices, many different suppliers are currently collaborating to agree on common standards. Who will manage which data on users remains a contentious issue, however. Each of the various actors involved – telecoms operators, chip manufacturers, mobile phone suppliers, and banks – brings its own interests, technical standards and organizational culture to the negotiating table. It seems unlikely that a consensus will be reached in the near future. Meanwhile, users and government have so far played a marginal role in the process. By further elaborating the concept of identity management, this chapter suggests that now is the time for governments and users to become involved. We thus ask, which roles can companies, users, and governments play in managing identities in an increasingly digitalized public arena?

6.1 NFC beyond the pilot phase

This study suggests that NFC trials in the Netherlands have proved to be successful, and will be followed up with further studies and products. Payter's successful rollout in Rotterdam and its plans to expand to several other cities appears to be particularly promising. Although the company still calls its scheme a 'pilot', Payter's application has progressed beyond the testing phase and appears to be permanent. On the other hand, should Payter fail, other NFC service providers, such as Rabo Mobiel, would feel the backlash. Even the most optimistic suppliers think that it will be several years before the majority of handsets are NFC-enabled, let along actually used for that purpose. For NFC to take off, many issues will first need to be addressed that may appear technical in nature, but in fact reflect a power struggle over who is going to manage the identities of NFC users.

First, there is the issue of the Secure Element (SE), whereby important data (for example, on identification and encryption keys) can be shielded from the outside world. Will this element be built into phones, into SIMs, or into an additional card (an SD or smart card)? Each of these three options serves the interests of one or another of the actors involved.

Second, in order to integrate all of the applications, networks and data flows, a new intermediary needs to be established: the Trusted Service Manager (TSM). Will the TSM merely be an intermediary, supporting the smooth flow of data from one to another? Or will the TSM also play an important role in promoting smooth collaboration and competition among suppliers, and help customers switch from one supplier to another? And if the TSM does become a point of ultimate technological and organizational convergence, and plays a dominant role, then which actor will be responsible for ensuring that it is doing its job well?

Third, once more people start using NFC, it is likely that there will be increasing attempts to hack into people's phones, eavesdrop, and commit identity theft and other cybercrimes. Although suppliers claim that NFC is safe, computer security experts view NFC as a 'mixed bag': while there are more entries to be broken into, greater computer power is also needed to seal it off. In theory, any device can be broken into as long as enough effort is made. Only practice will prove whether it to be a criminal business case.

Finally, the process of setting up a TSM demands an overall architecture for data exchange. Currently, there are many different flows of user data, and every application has its own identification mechanism and a separate organization handling the data. For instance, a customer's phone calls are not automatically linked to a customer's purchases. In future, will NFC evolve into an application which requires users to sign-on just once, thus linking everything to one single identity (one number and one database containing all personal data), or will a more versatile form of identity management prevail?

6.2 Suppliers: converging and competing

At the present time, many technology and service suppliers are coming together to make NFC work, in a seemingly fluent collaboration of commercial titans. While in this trial phase each participant is playing its role, whether as a bank or as a telecoms operator, it remains to be seen how competition among other suppliers will evolve in a growing market. Will telecoms companies joining at a later stage benefit equally from offering NFC as a new service? Will the banking system evolve into one compatible Single European Payment Area- (SEPA-) based currency exchange, or will delays in reaching standards stifle innovation? Will it be profitable for handset manufacturers to add NFC technology to their phones? Will NFC operate in a free, competitive market, or will a few big players dominate the game?

Resolving the issues surrounding the SE and the role of the TSM appears to be crucial. If the SE is placed in the handset, this could shift the balance of power in favour of handset manufacturers – if, of course, the latter perceive there to be sufficient commercial benefit in adopting the technology. Mobile network operators, on the other hand, perceive significant advantages to be gained from putting the SE on SIMS, thus allowing them to govern the technology. If this were to happen, then the network operators might gain so much dominance in the market by locking-in customers and overcharging for services, that other actors might see few benefits in the technology. Other options, such as placing the SE on a SD- or add-on smart card, lack a strong business case, as they lack strong stakeholder support and may prove to be too much of a hassle for users. One further option that might be worth considering, in order to break the deadlock, would be to appoint an intermediary to manage the SE.

At this early stage in NFC deployment, two business models have emerged. The first, Payter, is mainly based on marketing. Payment is seen as a 'necessary evil' for building customer relationships. Service providers can use the resulting elaborate consumer profiles to target marketing efforts and develop location-based services. Customers, meanwhile, profit from discounts, customized offers, additional product information and above all, convenient currency. Still, whether this model will prove to be profitable for both service providers and users remains to be seen. Second, Rabo Mobiel's business model, which involves customer loyalty and reducing costly cash payments, also has to prove its value. The high cost of cash has traditionally been an important source of bank income. Moreover, trust, one of the banking sector's key assets, could be eroded if NFC becomes just another channel for spam, malware and other digital annoyances.

Then again, both of these business models are still in their infancy. The nature of new ways of making money out of customer identities will be highly dependent upon which companies decide to step into the game.

6.3 Users: actively managing their identity

Initial feedback on users' experiences appears to be positive. Payter's users are staying loyal, and more cities are joining the scheme. Meanwhile, Rabo Mobiel users in Watergraafsmeer wanted the pilot to continue, including elderly customers who had never previously carried a mobile phone. When people are given the option of having new features on their mobiles, it appears that convenience is the key. Regardless of this, however, how much control do people really have over their personal data in such situations? Suppliers did not really address this issue in trial evaluations. From a user's perspective, receiving an e-mail after having held their NFC device close to a smart poster might appear to be just another aspect of the service, but it does demonstrate that NFC integrates their personal data. Profiles on spending, location and information retrieval are linked with users' phone numbers, bank account numbers, Social Security numbers, copies of passports, and e-mail addresses. Increasingly, money is becoming loaded with personal information. This may be a relatively insignificant issue in the case of a pilot that only involves a few people and a few transactions, but once a critical mass has been reached, marketing has the potential to evolve into an invasive control mechanism.

On the other hand, NFC provides users with more tools for managing their identities themselves. First of all, users can avoid the hassle of arranging increasing numbers of smart cards in their wallets by simply downloading them onto their phones, which come with keyboards, screens and Internet connections. The technology also makes it easier to monitor which organizations are keeping track of users' spending and choosing who may reward it with coupons. Moreover, carrying an RFID reader offers users the ability to read smart environments, rather than being read themselves. With the exception of smart posters, this function has yet to be fully explored. For example, a consumer might use a reader to check whether groceries or smart cards have tags inside them, find out which kinds of tags these are, or perhaps even scan the environment to find out which actors are monitoring them.

If the issues surrounding the SE and the TSM are eventually resolved, then the stage will be set for broader user experiences involving NFC. However, solutions that appear to be logical and beneficiary for the actors involved may not prove to be in the customers' best interests. For example, placing the SE on the SIM card may prove to be advantageous for mobile network operators, but users might experience the result as a lock-in that limits their choice of service provider. All in all, a non-proprietary solution to the SE placement issue would offer consumers more freedom of choice, but would also raise the issue of who would then oversee this freedom. In addition, the existence of too much choice may lead to confusion. Making it the user's responsibility to decide where the SE is placed could result in a Kafkaesque nightmare in which consumers went from one provider to another with a handful of chips. This is where the TSM could play a pertinent role: the TSM would manage the SE, regardless of where it had been placed on the device, allowing customers to avoid having to care or even know about the issue.

Moreover, the TSM could emerge as a single service contact point for users. In addition to integrating data flows for all of the companies involved and resolving the SE issue, it could provide a help desk for users seeking assistance with malfunctioning devices or changing their provider, bank or device, and also monitor who does what with users'

personal data. All of these functions would indeed amount to a highly integrated identity manager. On the other hand, however, if all of these responsibilities were to be awarded to a single party, to what extent would users be able to trust the TSM? Although the companies that are currently applying for the role, such as Logica MC, Gemalto and Atos Origin, have good track records with other companies, they lack a profile among consumers.

6.4 Government: supporting innovation and consumer protection

Until now, the story of the development of NFC in the Netherlands has been one of large enterprises, ambitious start-ups, and some willing customers. Our analysis has revealed little evidence of government interference. The Dutch Ministry of Economic Affairs and the Dutch Data Protection Authority, for example, both appear to perceive NFC as little more than RFID on mobile phones, and neither seems to see a need for additional policy measures. Our analysis demonstrates that so far, despite the complexity of bringing together a great deal of personal data, money and organizational challenges in one hand-held device, the free market has functioned quite well. It is possible that NFC will prove to be one area in which the Netherlands is at the forefront of innovation, which would obviously be a position to nurture. Still, there remains a need to establish whether Dutch users will benefit from the technology and whether, at some stage, the market might need a helping hand. Stimulating innovation therefore ought to go hand-in-hand with consumer protection. Moreover, current government regulation concerning personal data protection may need to be reviewed if it proves to be unfeasible once NFC takes off on a large scale.

First, there is the deadlock between mobile network operators, banks and handset manufacturers regarding where the SE should be placed, and regarding the role of the TSM. It will take time to build sufficient trust between the relevant actors to allow tasks to be delegated to the TSM. Would it be possible for the Ministry of Economic Affairs to support these negotiations, or perhaps play an important role in setting criteria for a good TSM? It would also be pertinent for policymakers to start considering NFC's implications for legislation regulating the telecoms market, cornerstones of which are free competition and keeping prices low. What if telecoms essentially ceases to be simply about supporting phone and Internet communication, and becomes a sector that deals with payment, location-based marketing, profiling, information retrieval and the like? In this case, legislation would not only need to address how to keep prices low and consumer choice high, but also to address who is managing identity in an increasingly digitalized public arena.

Second, as NFC brings together a great deal of personal data on spending and communication, it may become necessary to review the applicability of current regulation on personal data protection. On the one hand, data protection regulation protects users from businesses; while on the other, law enforcement agencies are seeking more opportunities for gathering personal data for investigative purposes. When so many parties are involved, whom might users or law enforcement agencies turn to for control over these data? In some cases, it might prove difficult to enforce personal data protection legislation. For example, if a user were to receive unwanted e-mail after having touched an NFC terminal, to whom would they turn? It may also be difficult to enforce data retention legislation. Currently, data on phone conversations, Internet traffic and electronic payments need to be stored for at least a year in a retrievable format, in case the police need to access them. The companies interviewed for our research believe that, with the exception of NFC-generated Internet use, data

retention laws do not apply to NFC. We are of the contrary opinion that, as the technology simultaneously involves payment, phones and Internet, the legislation does apply. It is unlikely, though, that any of the providers are taking this possibility into account when building networks and databases. One could also take the opposite view of the issue: if data retention were to become an unfeasible task in an NFC environment, then would we still *want* data retention laws?

This study has shown how a unique combination of large companies and small start-ups has provided the Netherlands with a new form of mobile communication. In the near future, we will see increasing numbers of people tapping their phones to perform transactions, retrieve information, and access services. Given this fact, now is the time to reconsider what this seemingly simple technology implies for the identities that we are building up in an increasingly digitalized public space. NFC is undoubtedly a great step forward in terms of convenience, but what about the digital footprint that we will leave?

7 Summary (in Dutch)

Betalen, toegang, informatie opvragen en punten sparen – het kan allemaal met Near Field Communication in de mobiele telefoon. Even het toestel tegen het leesapparaat - “bliep!” - en gaan. Achter deze ogenschijnlijk eenvoudige handeling gaan echter complexe organisatorische en technologische ontwikkelingen schuil. De eerste proefprojecten zijn succesvol en het aantal gebruikers neemt toe, maar er moet nog heel veel gebeuren wil NFC op grote schaal gebruikt worden. Het Rathenau Instituut heeft daarom in dit rapport *Near Field Communication. Convenience takes a great step forward. But what about the footprints we leave?* een Technology Assessment verricht naar deze snel opkomende technologie. Hoe werkt NFC en hoe ver is de ontwikkeling? Wat zijn de kansen en wat zijn mogelijke bedreigingen voor de bedrijven en gebruikers? Ligt hier een rol voor de overheid?

NFC en Identity Management

Het onderzoek voor dit rapport is onderdeel van het project *Digitalisering van de openbare ruimte* waarin we analyseren hoe de samenleving verandert onder toenemend gebruik van digitale middelen in de openbare ruimte. Centraal begrip in die analyse is het concept Identity Management, ofwel, hoe gebruikers van informatie en communicatie systemen door hun gebruik definiëren wat anderen wel of niet over hen weten en welk beeld de aanbieders van die systemen daarmee krijgen van hun gebruikers. Bij Near Field Communication gaat het dan vooral over consumentenprofielen op basis van wie, waar, wanneer, wat doet en in hoeverre gebruikers het beeld dat daaruit ontstaat zelf kunnen beïnvloeden. De empirische basis van dit onderzoek bestaat met name uit interviews met mensen die betrokken zijn bij NFC proefprojecten.

NFC is een convergentie van verschillende digitale toepassingen

Technologisch gezien is NFC een convergentie van verschillende digitale technologieën: RFID (Radio Frequency IDentitification, de contactloze chips in smart cards en producten), PIN (electronische betaalstructuur die werkt met Personal Identification Number), GSM (Global System for Mobile Communications) en internet. Bij betaling werkt de NFC in de mobiele telefoon hetzelfde als een gewone contactloze betaalkaart, die uitgelezen wordt door een leesapparaat, afrekent via de PIN structuur en kan worden opgeladen via een internetverbinding. Bij het uitlezen van informatie is de verhouding omgekeerd: de NFC chip in het toestel leest een chip in de omgeving (bijvoorbeeld een *smartposter*) en zoekt aanvullende informatie via internet. Een derde toepassing, directe communicatie tussen twee toestellen, wordt vooralsnog niet gebruikt. De standaarden om deze communicatie mogelijk te maken zijn nu vastgelegd en kunnen door iedereen worden gebruikt, waardoor zich vele andere toepassingen in het verschiet liggen.

Eerste proeven met NFC zijn geslaagd

In Nederland zijn er diverse proefprojecten geweest in besloten omgevingen. Twee projecten in Nederland zijn voor dit onderzoek interessant vanwege hun schaalgrote en diversiteit aan toepassingsgebieden: Payter en Rabo Mobiel. Payter is een betaaltoepassing die tijdens dit onderzoek door 500 proefpersonen getest werd in 50 winkels in Rotterdam. Volgens de enquêtes van Payter zijn de gebruikers positief, met name over het gebruiksgemak. Dat gold ook voor het tweede proefproject, Rabo Mobiel, dat onder andere getest werd in een supermarkt. Beide systemen werden

geïntroduceerd als betaalmiddel, maar de achterliggende motivatie van de aanbieders is echter een geheel andere. Payter ziet betaling als een noodzakelijk kwaad om mensen aan NFC te helpen, terwijl zij uiteindelijk een platform willen creëren voor spaarpunten en marketing. Rabo Mobiel daarentegen ziet NFC vooral als een manier om kleine transacties goedkoper te maken (contanten zijn logistiek gezien duur) en de band met de Rabobank klanten te versterken door aanvullende diensten.

Bedrijven zien nieuwe verdienmodellen, maar botsen op belangentegenstellingen
De proefprojecten wijzen uit dat de techniek werkt, de eerste klanten tevreden zijn en de weg vrij is voor veel innovatieve diensten. Achter de ogenschijnlijk eenvoudige toepassingen ging een complex proces schuil van technologische en organisatorische convergentie. Door het samensmelten van RFID, GSM, internet en PIN komen veel uiteenlopende belangen samen in het ene toestel: fabrikanten van mobiele toestellen (Nokia), chip fabrikanten (NXP), Mobile Network Operators (KPN), banken (Rabobank), winkelketens en tussenpersonen. Ze zijn al een behoorlijk eind gekomen nu de verschillende apparaten dezelfde taal spreken. Met name de fora zijn hier belangrijk geweest: NFC forum, Mobey Forum, GSMA en RFID Platform. De standaard die hieruit is voortgekomen is bewust open: iedere dienstverlener kan er in principe gebruik van maken. Vanuit het oogpunt van Identity Management zijn twee problemen nog niet opgelost: de plaatsing van het *Secure Element* en de oprichting van een *Trusted Service Manager*.

Het Secure Element (SE) is de plek in het toestel waar data wordt opgeslagen over de gebruiker, zoals identificatie codes, encryptie en tegoeden. Deze data mogen alleen door de aanbieder worden ingezien of gewijzigd worden en moeten daarom afgeschermd worden voor de gebruiker en derden. De locatie van het SE stuit op tegengestelde bedrijfsbelangen, want wie het SE beheert, beheert in wezen de toegang tot de gebruiker. Het SE kan op de SIM kaart worden gezet van de telecom provider. Die optie wordt sterk gesteund door hun belangenbehartiger, de GSMA. Deze optie zal echter een drempel kunnen opwerpen voor andere NFC dienstverleners, aangezien de telecom hen waarschijnlijk hoge tarieven zullen rekenen voor het gebruik van hun SIM. Voor de gebruiker is deze optie ook niet optimaal: als die wil overstappen naar een andere telecom provider, moet het SE op de een of ander manier worden overgezet op de SIM van de nieuwe provider.

Andere opties voor de locatie van het SE stuiten op praktische bezwaren of hebben geen sterke partij die die optie kan afdwingen. Zo kan het SE in het toestel worden ingebouwd, maar dan zit de gebruiker dus aan dat toestel vast. Het kan op een externe chipkaart worden gezet, maar dan verliest het toestel veel functionaliteit. Sommige toestellen hebben een ingang voor kleine verplaatsbare geheugenkaartjes (Mirco SD), maar als het SE daarop wordt gezet sluit dat weer gebruikers van andere soorten toestellen uit. Bovendien is er geen sterke speler die daar belang bij heeft. Het lijkt er dus op dat de SE op de SIM optie het gaat winnen en dat een belemmering kan zijn in de ontwikkeling van NFC.

Met zoveel organisaties en toepassingen in één apparaat blijkt onder de betrokken partijen behoefte te zijn aan een zogenaamde *Trusted Service Manager*. Dat is een intermediair die het dataverkeer bijeenbrengt en aanspraakpunt is voor al die betrokken partijen. Als er steeds meer aanbieders en gebruikers komen en er is nog geen TSM, dan dreigt een logistiek drama in dataverkeer en zal de positieve stemming rondom NFC snel omslaan. Enkele bedrijven hebben zich al aangeboden, maar wie het wordt en welke taken precies bij de TSM komen te liggen en aan welke eisen die moet voldoen is onduidelijk.

Gebruikers zullen meer actief hun identiteit moeten managen
De eerste reacties zijn positief, maar dat is slechts indicatief. Het ging immers om enkele beperkte toepassingen waarbij proefpersonen hun toestel gratis kregen. Niettemin kan gesteld worden dat gebruiksgemak overheerst. Vanuit het oogpunt van Identity Management kan geconstateerd worden dat hun transacties steeds meer persoonlijke data genereren. Anders dan bij smart cards is een NFC toepassing per definitie persoonsgebonden, aangezien het verbonden is aan het rekening nummer en telefoon abonnement. Bij PIN betalingen was het alleen de bank die inzicht kreeg in de transactie (tijd, plaats en soort betalingen), terwijl bij NFC meerdere organisaties kunnen mee kijken. Met die informatie kunnen vrij gedetailleerde klanten profielen worden opgebouwd en aanbiedingen worden gedaan. Vraag is of elke gebruiker zich daarvan bewust is en dat eigenlijk wel wil.

Daar staat tegenover dat het NFC toestel ook voor de gebruiker zelf meer Identity Management opties biedt. Vergeleken met huidige betaalsystemen is NFC een kaart met toetsenbord, beeldscherm en internetverbinding. Dat biedt meer mogelijkheden om bij te houden hoeveel tegoed en spaarpunten er zijn. Bovendien kan de gebruiker de wildgroei aan pasjes en inlogcodes indammen; die kunnen allemaal op dat ene toestel onder dezelfde inlogcode. De echte winst voor de gebruiker komt echter pas als NFC meer als leesapparaat gebruikt kan worden in plaats van alleen uitgelezen wordt. Smartpostering is een begin, maar vele toepassingen liggen in het verschiet. Bijvoorbeeld het uitlezen van RFID chips in producten (checken op allergenen), bewegwijzering (download route) of smartcards (controleren wat de aanbieder doet met de informatie).

Ook voor de gebruiker zal de plaats van het Secure Element en de rol van een eventuele Trusted Service Manager gevolgen hebben. Wordt het SE beheert door de telecoms, dan heeft de gebruiker weliswaar een bekende dienstverlener maar wordt hij enigszins beperkt in zijn keuze vrijheid. Overstappen wordt moeilijker en andere dienstverleners kunnen belemmerd worden in de toegang tot de gebruiker. Plaatsing in het toestel is eveneens niet wenselijk, want gebruikers wisselen vaker van toestel dan van telecom provider. De optie met externe geheugenkaarten kan gezien worden als te ingewikkeld. Onduidelijkheid over de locatie van het SE is eveneens onwenselijk. Vraag is of de TSM wellicht ook richting de klant hierin een rol kan spelen. Die zou bijvoorbeeld kunnen aanbieden het SE over te zetten en zo drempels voor gebruikers en aanbieders weg te nemen.

Overheid moet stelling nemen in beheer persoonsgegevens
De twee proefprojecten laten zien dat de vrije markt tot nog toe goed werkt: bedrijven zien kansen voor nieuwe verdienmodellen en de gebruikers waarderen de nieuwe diensten. Vraag is of die markt op grote schaal goed blijft functioneren of toch een helpende hand behoeft. Een overheid, bijvoorbeeld het ministerie van Economische Zaken of de mededingingsautoriteit, kan niet beslissen waar het SE moet komen of wie de TSM wordt, maar kan wel de onderhandelingen scherp in de gaten houden. Dreigt één partij alle anderen te overheersen? Zijn er mogelijke oplossingen die het belang van de consument dienen, maar niet een grote partij achter zich hebben staan?

Het belang van innovatie moet daarbij afgewogen worden tegen de huidige regelgeving rondom persoonsdata. Met NFC komt veel voorheen gescheiden informatie samen (betaling, locatie, communicatie, internetten, etc.), terwijl het niet altijd duidelijk zal zijn wie welk deel beheert. De overheid zal enerzijds de gebruiker willen beschermen tegen oneigenlijk gebruik van die data middels de Wet Bescherming Persoonsgegevens. Anderzijds zal de overheid ook graag zelf inzicht hebben in die data voor opsporingsdoeleinden, bijvoorbeeld middels wetgeving voor dataretentie. Echter naar

wie kan de overheid toe voor welke data te beschermen, dan wel te benutten? Ook hierbij is de rol van een eventuele TSM essentieel. Wordt dit de plek waar alle data samenkomt en dus ook de wetgeving gehandhaafd wordt? Wordt de TSM de intermediair die aanwijst waar de overheid moet zijn voor welke data? Of zal met NFC de stroom data zo onoverzichtelijk en onbeheersbaar dat we ons moeten afvragen of de wetgeving zelf aanpassing behoeft?

Dit onderzoek laat zien hoe een uniek samenspel van grote en kleine bedrijven in Nederland een nieuwe toepassing voor de mobiele telefoon van de grond heeft gekregen. Binnenkort zullen we meer en meer mensen zien die hun mobiele telefoon ergens tegenaan houden om te betalen, toegang te krijgen of informatie op te vragen. Dit is het moment om ons te realiseren wat deze ogenschijnlijk eenvoudige handelingen betekenen voor de virtuele identiteit die we bij ons dragen in de publieke ruimte. NFC belooft een grote stap voorwaarts in gebruiksgemak, maar wie let nog op de voetsporen die we ermee achterlaten?

Appendix 1: Abbreviations

GPRS	General Packet Radio Service is a packet oriented Mobile Data Service available to users of Global System for Mobile Communications (GSM) and can be used for services such Short Message Service (SMS), Multimedia Messaging Service (MMS), and for Internet communication services such as email and World Wide Web access.
GSM	Global System for Mobile Communication, the most common standerd used for mobile phones
GSMA	GSM Association: the global trade association representing over 750 GSM mobile phone operators across 218 countries of the world. In addition, more than 200 manufacturers and suppliers support the Association's initiatives as key partners
KPN	KPN, a Dutch fixed-line and mobile telecommunications company
NFC	Near Field Communication: a wireless communication technology, which used radio frequencies to communicate on short distances (mostly less than 20 centimetres). It is currently applied in mobile phones fore payment and information retrieval
NXP	Next eXPerience Semiconductors is the name for the new semiconductor company founded by Philips
RFID	Radio Frequency Identification: a wireless communication technology used in smartcards and product identification. An RFID chip consists of a micro chip with an antenna. The antenna is shaped as a coil which generate power from the received signal
SD card	Micro SD is a format for removable flash memory cards. It is derived from SanDisk TransFlash and is used mainly in mobile telephones
SE	Secure Element: the place in the NFC device where sensitive information such as their debit account and identification data is encrypted and stored. There have been proposals to embed the SE in the phone, on the SIM card, or on an external memory card, such as a micro-SD card
SIM	Subscriber Identity Module (SIM) is part of a removable smart card for mobile phones
WiFi	Wireless Fidelity is the trade name for the popular wireless technology used in home networks, mobile phones, video games and more

Appendix 2: Interviews

Armstrong, D. May 16th 2008c. Chief Technical Officer, Rabo Mobiel

Bayings, M. April 18th 2008, Mobile & RFID Solutions Consultant, Logica

Bruinsma, R. May 16th 2008, Senior Manager, Products & Services, Rabo Mobiel

Carpenter, B. April 21st 2008, Founder Payter

Desertine, M. April 28th 2008, Manager, Business Development RFID EMEA, NXP

Hendriksen, I, April 2008, Chief Compliance Officer, Payter

Hoepman, J.H., April 22nd 2008, Senior Scientist, TNO

Kleijmeer, R. April 2008, Payment and Settlement Systems Policy Department, De Nederlandsche Bank

Mierlo, R. van April 28th 2008, Director, Central Logistics and Innovation, Schuitema

Nas, S. April 2008, College Bescherming Persoonsgegevens

Schermer, B. May 6th 2008, partner Considerati and former secretary to the RFID Platform Netherlands

Steegstra, L. April 25th 2008, Manager, Innovation Business Market, KPN

Teepe, W. May 19th, 2008, Computer Security Group, Radboud Universiteit Nijmegen

Appendix 3: References

Anonymous, March 18th 2004, Nokia, Philips and Sony establish the Near Field Communication (NFC) Forum, NXP press release. Accessed online on May 21st, 2008, http://www.nxp.com/news/content/file_1053.html.

Anonymous, August 12th 2005, Mobiele telefoon vervangt clubcard Roda JC, accessed online on May 26th 2008 http://www.emerce.nl/nieuws.jsp?id=772108

Anonymous, October 12th 2006, JCB's Amsterdam NFC mobile payment pilot, accessed online on May 26th 2008.
http://www.paymentsnews.com/2006/10/jcbs_amsterdam_.html

Anonymous, February 14th, 2007, Near Field Communication Technology and the Road Ahead, NFC Forum. Accessed online on January 15th, 2008, http://www.nfc-forum.org/resources/multimedia/NFC_Forum_14Feb07_Press_and_Analyst_Briefing_Slides.pdf

Anonymous, 2008, Pinnen met je mobiel, Amersfoort: Schuitema.

Anonymous, 2008a, Verbinding in context, Voorburg: CBS. Accessed online on June 24th, 2008. http://www.cbs.nl/NR/rdonlyres/72671723-2FCF-408B-BD47-0E2C7DF5763D/0/200802eyeart.pdf

Anonymous, 2008b, De digitale economie 2007, Voorburg: CBS. Accessed online on June 24th 2008. http://www.cbs.nl/NR/rdonlyres/17750841-7775-4CE7-A122-1BD52991C8C5/0/2007p34pub.pdf

Anonymous, undated, Near Field Communication white paper, ECMA International. Accessed online on May 25th 2008.
http://www.ecma-international.org/activities/Communications/2004tg19-001.pdf.

Aarts, E. and Marzano, S. 2003, The New Everyday: Views on Ambient Intelligence, Rotterdam: 010 Publishers.

Armstrong, D. April 6th 2008a, Rabo Mobiel, presentation at Mobile Monday Amsterdam. Accessible online at
http://www.mobilemonday.nl/2008/04/06/momoment-momo-5-dan-armstrong/

Armstrong, D. April 14th 2008b. Rabo Mobiel overview, presentation at Emerce Insight banking. Accessible online at
http://www.slideshare.net/Emerce/dan-armstrong-rabo-mobiel-407309

Balaban, D. November 1st 2007, Making house calls with NFC mobile phones, accessed online on May 26th 2008.
http://www.cardtechnology.com/article.html?id=20071101R3SAXMD3

Beugelsdijk, R., October 2006, RFID. Veelbelovend of onverantwoord? Den Haag: College Bescherming Persoonsgegevens. Accessed online on April 15th, 2008 at
http://www.cbpweb.nl/downloads_av/av29.pdf?refer=true&theme=purple

Gibson, C. 1984, Neuromancer, New York: Ace Books.

Haselsteiner, E. and Breitfuß, K. undated, Security in Near Field Communication, Philips semiconductors

Hendriksen, I. March 2008, untitled, presentation at Mobile Monday Amsterdam, accessed online on May 27th 2008. http://www.mobilemonday.nl/page/2/

Hoepman, J.H. and Siljee, J. October 23rd 2007 Beyond RFID: the NFC security landscape, Groningen: TNO.

Hensen, C. August 29th, 2007, Ongevraagde betaalexperimenten; Bedrijven zien veel in betalen met mobieltje, consumenten vooralsnog niet, Rotterdam: NRC Handelsblad.

Hof, C. van ‘t, 2007, RFID & Identity Management in Everyday Life. Striking the Balance between Convenience, Choice and Control. The Hague: Rathenau Institute.

Libbenga, J. April 5th 2006, Proef met contactloos parkeren, accessed online on May 27th 2008. http://www.emerce.nl/nieuws.jsp?id=1231954

Schilpzand, W. and Van 't Hof, C. 2008, RFID as the Key to the Ubiquitous Network Society, The Hague: Rathenau Institute.

Smits, J. March 31st 2008, Mobile and Banking: a natural fit?, presentation at mobile Monday Amsterdam, accessed online on May 25th, 2008.
http://www.mobilemonday.nl/index.php

Srivastava, L. et al., 2005, The Internet of Things Geneva: ITU Report.

Starkenburg, J. May 16th 2008, Smart Tags sturen boodschappenlijstje naar mobiel, accessed online on May 27th 2008. http://www.emerce.nl/nieuws.jsp?id=2555994

Stil, H. March 3rd 2007, Rabo Mobiel is....., Amsterdam: Het Parool.

Stil, H. March 3rd 2007, mobiel betalen, Amsterdam: Het Parool.

Wendt, W. April 1st, 2008, Mobile payment and transaction pilots, presentation at Mobile Monday Amsterdam, accessed online on May 25th, 2008, accessed online on May 25th, 2008 http://www.slideshare.net/momoams/momo5-logica-336466/.