Thomas Zefferer: "A Survey and Analysis of NFC-based Payment Solutions for Smartphones". In IADIS International Conference e-Society 2013, pp. 275-282, IADIS, 2013.

A SURVEY AND ANALYSIS OF NFC BASED PAYMENT SOLUTIONS FOR SMARTPHONES

Thomas Zefferer
Secure Information Technology Center - Austria
Inffeldgasse 16a, 8010 Graz, Austria

ABSTRACT

The recent emergence of smartphones and mobile communication technologies has caused a significant shift towards mobile solutions in many aspects of our daily life. Motivated by this general trend and facilitated by the integration of NFC technology into modern smartphones, stakeholders from the mobile communication sector and from the financial sector have recently started to roll out NFC based mobile payment solutions. These solutions allow customers to pay cashless at points of sale using their NFC enabled smartphones. However, most of these solutions have not managed to make the breakthrough so far and suffer from low user acceptance rates. This is surprising as NFC based payment solutions are usually beneficial compared to other payment methods in terms of usability.

In order to find out the reasons for this observable lack of user acceptance, this paper analyzes existing NFC based payment solutions and identifies their strengths and weaknesses. For this purpose, NFC based payment solutions from all over the world have been surveyed. Based on this survey, a set of distinctive features has been derived. These features have then been used to classify and analyze the surveyed payment solutions. The conducted analysis process has revealed useful findings, which can be used to improve future NFC based payment solutions, and which can help to introduce NFC into other security sensitive fields of application.

KEYWORDS

Mobile payment, smartphone, NFC, Secure element

1. INTRODUCTION

Applications that make use of mobile communication technologies have significantly gained importance during the past years. Powered by the introduction of new and powerful mobile end devices and by the development of mobile broadband communication networks, an emerging trend towards mobile solutions can be observed in various fields of application. This shift towards mobile services can also be observed in various security sensitive fields of application such as electronic payment (e-payment) or electronic government (e-government). The integration of mobile technologies into e-payment and e-government applications has become commonly known under the terms mobile payment (m-payment) and mobile government (m-government), respectively. Mobile payment solutions usually allow customers to use their mobile phones to pay cashless at points of sale. Google Wallet (Google, 2012), which has been introduced by Google in the USA in 2011, is a representative example of mobile payment solutions.

During the past years, smartphones have turned out to be the most relevant and most frequently used end devices for m-payment and related services. Beside typical mobile communication facilities, modern smartphones integrate various additional technologies that allow for the implementation of powerful applications. The various technologies supported by modern smartphones can not only be used to improve the functionality of mobile applications. Some of these technologies are also suitable to improve the security and usability of mobile solutions.

A popular technology that has the potential to improve the security and usability of security sensitive mobile applications is *Near Field Communication (NFC)*. NFC is a wireless short-range communication technology closely related to *Radio Frequency Identification (RFID)* technology. On smartphones, NFC is typically integrated together with a *Secure Element (SE)*. An SE is a simple but highly secure hardware unit that can be used to securely store data and to carry out cryptographic operations. In combination with an SE, NFC represents a powerful technology to improve the security of mobile applications.

The potential of NFC on smartphones has already been recognized. Google Wallet is but one of many NFC based m-payment services that have been introduced during the past years. Similar m-payment solutions that make use of smartphones' NFC capabilities have been introduced all over the world. While the number of NFC based m-payment solutions is constantly growing, the user acceptance of these solutions often remains below expectations. At the same time it can be observed that NFC is less frequently used in other security sensitive fields of application such as m-government. This is surprising, since most security sensitive fields of application share several common requirements regarding security and usability.

In order to find reasons for the obvious lack of user acceptance of NFC based payment solutions and in order to analyze the potential of NFC for other fields of application, we have surveyed existing mobile payment solutions based on NFC. Thereby, focus has been put on solutions that have been designed and developed for smartphones. In this paper, we first provide a brief introduction to NFC and its integration into modern smartphones. We then present the results of the conducted survey and discuss different NFC based payment solutions. Subsequently, we propose a set of distinction criteria to classify the surveyed solutions. From the applied classification and analysis process we finally derive and discuss findings that can help to improve future NFC based m-payment solutions and to leverage NFC technology also in other security sensitive fields of application.

2. NFC ON SMARTPHONES

NFC is probably one of the most promising smartphone technologies that can be used for the implementation of secure and usable mobile payment solutions. Actually, NFC is not a new technology but has already been introduced in 2002. Mainly fostered by the two companies NXP and Sony, NFC is based on RFID technology, which has also been developed mainly by these two companies. Established RFID standards define the transmission of data between a powerful reader device and a simple RFID tag. The RFID tag is usually completely supplied by an external electromagnetic field. This field is generated by the reader device and also used to read data from and write data to the tag using standardized modulation techniques. Due to these technology inherent limitations, RFID based communication is typically extremely limited in terms of distance and bandwidth. The main advantage of RFID is however the automatic and immediate communication set-up. A reader device can communicate with any compliant tag whenever the tag is within the reader's range. RFID tags are therefore suitable as a replacement for barcodes and to store simple information such as URLs. Popular RFID standards are MIFARE (ISO, 2008) developed by NXP and FeliCa developed by Sony.

NFC can be seen as development of RFID and combines the established standards MIFARE and FeliCa. Relevant NFC standards are ISO/IEC 18092 (ISO, 2004) and ISO/IEC 21481 (ISO, 2005). In contrast to RFID, NFC does not define fixed roles for (active) reader devices and (passive) tags. Every NFC device can be operated in three different modes. An NFC device can act both as passive tag (card-emulation mode) and as reader device (reader/writer mode). Additionally, two NFC enabled devices can also directly communicate with each other (peer-to-peer mode). This way, NFC is suitable for much more application scenarios compared to simple RFID solutions but still features the same communication properties such as short-range, low bandwidth, and immediate communication set-up.

Although NFC has been available for about ten years, this technology has not been able to reach the mass market so far. Amongst others, reasons have been a lack of appropriate end user devices and a very limited set of potential use cases and concrete NFC based applications. This situation has changed, when smartphone manufactures have recently started to integrate NFC into their products. Smartphones integrate various powerful technologies, which can be combined with NFC to implement new and powerful services and applications. In this context, especially *Secure Elements (SE)* have turned out to bear a great potential for NFC based smartphone applications. An SE is a secure hardware module that supports the secure storage of confidential data and the execution of cryptographic operations. Secure elements are basically comparable to smart cards (Rankl et al., 2004). However, while the functionality of a smart card is usually determined during the manufacturing process, the functionality of secure elements can also be determined and modified after deployment. For this purpose, a *Trusted Service Manager (TSM)* is able to securely access an already deployed secure element in the field and to securely install special applications on the SE in order to modify its functionality.

NFC and SE are a powerful combination that allows for the realization of secure smartphone applications. Fig. 1 illustrates the general architecture of NFC enabled smartphones. In this architecture, the *Baseband Controller* represents all smartphone components that are required to execute the mobile operating system. Usually, the Baseband Controller does not implement highly secure security measures and is hence potentially vulnerable to malware. The *NFC Controller* complements the Baseband Controller and implements an analogue frontend to the smartphone's *Antenna*, which is used to communicate with external NFC devices. The NFC Controller also implements a digital interface to the Baseband Controller. The Baseband Controller uses this interface to access the smartphone's NFC interface. This can be necessary when the smartphone is operated in the reader/writer mode or in the peer-to-peer mode.

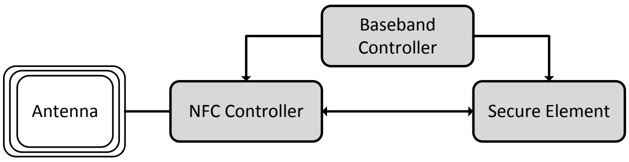

Figure 1. Architecture of NFC enabled smartphones

For security sensitive applications, the *Secure Element (SE)* is of special importance. The SE implements hardware based security measures and is thus resistant to malware residing on the smartphone. As shown in Fig. 1, the SE is separated from the Baseband Controller and is equipped with an own interface to the NFC Controller. This way, there is a secure path between the smartphone's NFC interface (Antenna) and the SE, bypassing the potentially insecure Baseband Controller. The direct path between Antenna and Secure Element allows the smartphone to be operated in card-emulation mode. In this mode, external reader devices can directly access the SE through the smartphone's NFC interface. The card emulation mode is of special relevance for most NFC based payment solutions that are surveyed in the next section.

3. NFC BASED M-PAYMENT SOLUTIONS

A key characteristic of RFID and NFC based communication technologies is their short operating range. The two communicating devices (reader and tag) need to be in close proximity in order to be able to exchange data. This might appear to be a drawback form a functionality point of view. From a security point of view, the limited operating range is actually a benefit as it prevents NFC devices from being used and accessed unnoticed by the legitimate device owner. Several payment solutions make use of this inherent feature of RFID and NFC technology. For instance, MasterCard PayPass (MasterCard, 2012) or Visa PayWave (Visa, 2012) allow users to pay cashless in stores simply by tapping a contactless RFID enabled smart card on a special payment terminal (tap-and-go). An additional authorization such as a PIN is not necessary. This improves usability, but on the other hand reduces security. Thus, these kinds of payments are usually subject to rather low transaction limits.

MasterCard PayPass and Visa PayWave have originally been designed for contactless smart cards. Enabled by the growing availability of NFC enabled smartphones, several solutions have recently been introduced, which are based on the backend systems of MasterCard PayPass and Visa PayWave, but replace the contactless smart card by an NFC enabled smartphone. Such a solution is for instance offered by the Russian mobile network operator MTS in cooperation with MasterCard and the Russian banking institution MTS (NFC World, 2012). Customers are supplied with a special NFC antenna and a special SIM card, which assumes the role of a secure element. Antenna and SIM card can be used to extend existing mobile phones with NFC and SE functionality. The enhanced devices can then be used to carry out MasterCard PayPass based transactions up to 1000 RUB at points of sale equipped with appropriate MasterCard PayPass terminals.

A similar smartphone based m-payment solution that relies on MasterCard PayPass technology has been introduced in Turkey. This solution is called Cep-T Cüzdan (Turkcell, 2012) and has been developed by the Turkish mobile network operator Turkcell. Cep-T Cüzdan allows customers to carry out MasterCard PayPass transactions using their NFC enabled smartphones. Similar to the Russian mobile network operator MTS, Turkcell supplies its customers with add-on solutions to extend older mobile phones with NFC technology.

Moneto (Moneto, 2012) is another mobile payment solution that makes use of smartphones and allows for conducting contactless MasterCard PayPass transactions. Moneto is based on an NFC enabled microSD card developed by the companies DeviceFidelity and Spring Card Systems. This way, this solution is applicable on any smartphone that features an appropriate slot for microSD memory cards and does not require the smartphone to feature NFC. The microSD card also features a SE, which is used to store security sensitive data such as the PIN that can be used to protect financial transactions.

The probably most discussed NFC and smartphone based m-payment solution is Google Wallet (Google, 2012). Google Wallet is the result of a joint initiative of Google, MasterCard, the US mobile network operator Sprint, Citibank, and FirstData. The basic idea of Google Wallet is to provide users with a smartphone app (Google Wallet App) that acts as virtual wallet and stores different kinds of virtual cards such as credit cards, prepaid cards, or loyalty cards. Similar to the above mentioned m-payment solutions from Russia and Turkey, Google Wallet makes use of the existing MasterCard PayPass infrastructure to process transactions. To pay cashless at points of sale, users select a card in their Google Wallet App and tap their NFC enabled smartphone on the MasterCard PayPass terminal. In contrast to other MasterCard PayPass based m-payment solutions, users need to enter a secret PIN into the Google Wallet App in order to authorize the transaction. Although recent security reports have revealed that this PIN is not appropriately protected under certain circumstances (viaForensics, 2011; The Smartphone Champ, 2011), this additional authorization step adds more security to the entire solution.

When introduced in 2011, Google Wallet stored security sensitive data (credit card numbers, etc.) in a secure element residing on the user's smartphone. Full access to the secure element was only provided via NFC and required mutual authentication. This way, only FirstData being the operator of the backend systems was able to access the secure element during a financial transaction through the smartphone's NFC interface. Other smartphone applications were not able to access the secure element and its data. In autumn 2012, Google has suddenly changed the basic architecture of Google Wallet. According to an official announcement (Google Commerce, 2012), Google Wallet now stores security sensitive data centrally on Google servers. Although the introduction of Google Wallet has caused a stir, its success has remained below expectations so far. Main reasons are Google Wallet's limitations regarding supported mobile networks, mobile end devices, and credit cards. The combination of these limitations has significantly reduced the circle of potential customers and has prevented a breakthrough of Google's m-payment solution so far.

ISIS (ISIS, 2012) is another NFC based m-payment solution and follows a similar approach as Google Wallet does. Equally to Google Wallet, ISIS allows users to virtualize payment cards on their smartphones and to use these virtual cards to carry out cashless payments at points of sale. Similar to Google Wallet, ISIS makes use of a secure element and requires the user to enter a secret PIN in order to authorize a payment. However, there are also several differences between ISIS and Google Wallet. ISIS is not restricted to a certain mobile network operator but is supported by the three major US mobile network operators AT&T, Verizon, and T-Mobile. Furthermore, ISIS supports most major credit card brands according to official announcements. The most relevant difference between Google Wallet and ISIS from a technical point of view is the realization of the SE. While Google Wallet relies on an SE that is based on a hardware chip being integrated directly in the smartphone, ISIS makes use of SIM cards to implement the functionality of an SE. This provides ISIS more flexibility regarding the choice of appropriate end devices. ISIS is currently piloted in the US cities of Austin and Salt Lake City.

While Google Wallet and ISIS are – at least for the time being – mainly intended for the US market, NFC based m-payment solutions have also been introduced in other countries all over the world. Japan and South Korea can actually be seen as pioneers in NFC based payment solutions. While contactless payment methods are only slowly gaining popularity in America and Europe, NFC payments are already well established in Japan and South Korea. In Japan, NFC based payment methods have evolved from contactless ticketing systems for public transportations. Later, these tickets have been enhanced by simple electronic purse functionality to allow users to purchase goods at special kiosks. Popular brands of such combined contactless ticketing and electronic purse solutions available in Japan are Suica (JR East, 2012b) or PASMO (JR East, 2012a). Recently, these solutions have also been ported to smartphones. This allows customers to store tickets on their NFC enabled smartphones and to use their mobile communication devices as contactless electronic purses.

A similar solution is available in South Korea. Also in South Korea, the established mobile payment solution T-Money (Korea Smart Card Co., 2012) has evolved from a contactless ticketing system for public transportations, which has later been extended by prepaid based payment functionality. Nowadays, T-Money is also available on mobile phones. In contrast to the Japanese solutions Suica and PASMO, T-Money implements a proprietary communication standard, which is similar but not directly compatible to NFC.

While RFID and NFC based mobile payment solutions have already been available in Japan and South Korea for several years, Europe is only slowly catching up. However, there are already a few NFC based mobile payment solutions available in different European countries. Beside the already mentioned solutions from Russia and Turkey, NFC based payment methods have recently attracted attention also in Austria, Germany, and the UK.

In Austria, the company Paybox, which has already gained experience with SMS based m-payment solutions, has recently piloted an NFC based payment solution that allows users to pay at selected points of sale using their NFC enabled smartphones (Paybox, 2012). Security sensitive data has been stored in a secure element implemented by the mobile phone's SIM card. For this purpose, Paybox has collaborated with the Austrian mobile network operator A1. For mobile phones without NFC support, Paybox has offered its customers a sticker containing an NFC antenna and an integrated SE. Similar to MasterCard PayPass based solutions, it has been sufficient to tap the NFC enabled mobile phone or the NFC sticker on an appropriate reader device at the point of sale. In autumn 2012, Paybox announced to not prolong the pilot and to withdraw the service by end of 2012 due to a lack of acceptance (Paybox, 2012).

Another NFC based mobile payment solution is currently being piloted in Austria by Raiffeisen Bank International (RBI). The solution is called CardMobile (Raiffeisen Bank International, 2012) and has been developed for the Apple iPhone. As the iPhone does not feature NFC support, CardMobile requires the user to equip the smartphone with a special protective cover that contains an NFC antenna and a SE. CardMobile supports two types of transactions. Micropayments up to 20€ can be conducted simply by taping the iPhone on an appropriate reader device at the point of sale. Payments above this limit are carried out as Visa V Pay transaction (debit) and require the user to additionally enter a PIN.

Contactless payment methods are currently also piloted in Germany. The girogo service (EURO Kartensysteme, 2012), which allows customers to carry out financial transactions up to 20€ without entering a PIN on a prepaid basis, is currently tested in the German cities Hannover, Braunschweig, and Wolfsburg. So far, this service is limited to special issued smart cards and not available on smartphones.

In the UK, the mobile network operator Orange and the credit-card issuer Barclaycard have launched the NFC based payment solution Quick Tap in 2011 (Orange, 2011). Quick Tap is also based on a prepaid model and allows customers to charge their mobile phone with up to 100£. Customers can then pay at points of sale amounts up to 15£ simply by taping their mobile phone on an appropriate reader device. Quick Tap also requires the user to install a special smartphone app. This app provides the user with information on the current balance and optionally with the opportunity to protect payments by entering a secret PIN.

Beside Europe, NFC based payment methods have also been introduced and piloted in other regions of the world. NFC based payment solutions for smartphones have for instances been introduced in Canada by Rogers Communications and CIBC (SureTap) (Rogers Communications, 2012), or in New Zealand, where the mobile network operator 2degrees and the payment company snapper have introduced the payment system Touch2Pay (2degrees, 2012).

4. ANALYSIS

The conducted survey on existing NFC based mobile payment solutions has revealed that these solutions are quite heterogeneous and differ in several aspects. A thorough analysis and comparison of existing solutions hence requires a classification of existing solutions with respect to these criteria. We define criteria and distinctive features of current NFC based mobile payment solutions in this section. Based on the identified distinctive features we then classify the surveyed payment solutions and derive findings that can be useful for the development of future NFC based m-payment solutions and for the introduction of NFC based solutions into related fields of application.

4.1 Definition of Classification Criteria

Despite their heterogeneity, all surveyed mobile payment solutions share some common features. All solutions allow customers to pay cashless at points of sale. For this purpose, the points of sale have to provide an appropriate infrastructure. This infrastructure typically includes an appropriate reader device, which is connected to the backend systems of a central payment system. All surveyed payment solutions have also in common that they make use of NFC or closely related wireless communication technologies to allow for a contactless payment process. Customers can initiate (and in some cases even complete) a payment simply by tapping a mobile NFC device on the reader device at the point of sale. Furthermore, all solutions rely on some kind of hardware based SE that is used to store and process security sensitive information.

Despite these similarities, existing solutions differ in various technological and organizational aspects. We propose the following set of distinctive features to classify existing NFC based mobile payment solutions.

- **Realization of the SE:** The SE represents a key component of all NFC based payment solutions. Especially on smartphones, secure elements can be realized in different ways. The realization of the SE influences the usability of the entire solution and also affects the set of involved stakeholders. Hence, the realization of the SE is an important classification criterion for NFC based payment solutions.
- **Transaction authorization:** The main benefit of NFC based payment solutions is usability. Customers can carry out transactions simply by taping an NFC device on an appropriate reader device. In order to not disturb this so called tap-and-go experience, most solutions do not require customers to additionally authorize transactions e.g. by entering a secret PIN. As this potentially decreases security, the type of provided transaction authorization is also a relevant classification criterion for NFC based payment solutions.
- **Type of payment:** NFC basically defines the communication technology used by the customer to interact with the payment system. However, the use of NFC does not limit the type of payment. The conducted survey has shown that NFC is typically used for credit card, debit, and prepaid payments. Of course, not all surveyed solutions support all kinds of payment. Hence, the set of supported types of payment is another interesting classification criterion for NFC based payment solutions.
- **Stakeholders:** The development and operation of NFC based payment systems usually requires the collaboration of different stakeholders. Depending on the concrete technical implementation, such solutions require the collaboration of banking institutions, credit card companies, smartphone manufactures, trusted service managers, or mobile network operators. At the same time, a growing number of involved stakeholders potentially reduces the profit for each single stakeholder. Hence, the set of stakeholders being the main drivers behind the development and operation of an NFC based payment solution is another interesting classification criterion.

4.2 Classification

Based on the proposed classification criteria, we have classified the surveyed mobile payment solutions. The results of this classification process are shown in Table 1. For each surveyed solution, the four criteria defined above have been analyzed separately. Findings that can be derived from this classification process are discussed in the next subsection.

Table 1. Classification of surveyed NFC based mobile payment solutions

Payment system	SE Realization	Transaction authorization	Type of payment	Stakeholders
MasterCard PayPass	Smart card	None, PIN	Debit, credit, prepaid	Credit card company
Visa PayWave	Smart card	None, PIN	Debit, credit, prepaid	Credit card company
Google Wallet	Hardware module	PIN	Credit, prepaid	Smartphone OS manufacturer, bank, credit card company, MNO, payment

				infrastructure operator
ISIS	SIM	PIN	Debit, credit, prepaid	MNO
Paybox NFC	SIM, sticker	None	Debit, phone bill	MNO
Touch2Pay	SIM	None	Prepaid	MNO, payment company
MTS Money NFC	SIM	None	Debit	MNO, bank, credit card company
Moneto	microSD	PIN	Prepaid	Hardware manufacturer, payment company
Cep-T Cüzdan	SIM	None	Credit	MNO, bank
girogo	Smart card	None	Prepaid	Bank
suretap	SIM	None	Credit	MNO, bank
Quick Tap	SIM	PIN	Prepaid	MNO, credit card issuer
Suica/PASMO	Smart card	None	Prepaid	Public transportation operator
T-Money	SIM	None	Prepaid	Payment company
CardMobile	microSD	None	Prepaid	Bank

4.3 Findings and Lessons Learned

The conducted survey on existing NFC based payment solutions and the applied analysis process has revealed several interesting findings. First of all, the conduced survey has shown that NFC and secure elements have evolved to mature technologies that are basically suitable for the development of secure and usable mobile payment solutions. In this context, the short range of NFC based communication has turned out to be an interesting security feature. As users need to intentionally tap their personal NFC device on a reader device to initiate a payment process, additional security measures are often not implemented. Of course, these kinds of tap-and-go transactions that do not require additional authorizations by the user are usually limited to micropayments. The conducted classification process has also shown that in many cases, convenient tap-and-go transactions are furthermore restricted to prepaid payments. In general, it seems that providers of NFC based payment solutions definitely want to make use of NFC's potential to improve the usability and efficiency of payment processes. However, they are also well-aware of the reduced security caused by a missing additional transaction authorization.

For NFC based m-payment solution, the risk can easily be controlled by defining appropriate transactions limits or by restricting the payment solution to prepaid payments. Table 1 shows that this strategy is successfully applied all over the world. If NFC based solutions shall be developed in other security sensitive fields of application, similar risk-limiting strategies need to be applied. The concrete strategies to be implemented of course heavily depend on the actual field of application and require a thorough risk assessment.

Another interesting finding of the conducted classification and analysis process pertains to the implementation of the secure elements and its influence on involved stakeholders. The implementation of the secure element is a major design decision for all NFC based payment solutions. Table 1 shows that in many cases the SIM card is used as secure element. This seems reasonable, as SIM cards are basically available in and compatible to all GSM based mobile phones. Table 1 also shows that in most SIM based solutions mobile network operators (MNO) are involved in the development and operation of these solutions. Other stakeholders typically prefer alternative SE implementations in order to remain independent from MNOs. The appropriate choice of an SE realization is hence not only a question of technical feasibilities, but also a strategic issue. If a SE can be implemented without the help of MNOs, profits do not need to be shared with MNOs neither.

In general, the complex ecosystem of involved stakeholders is one of the biggest challenges of NFC based payment systems. The large number of stakeholders renders the development of strategies and business plans, which satisfy the demands of all parties, difficult. So far, the given complexity has led to collaborations between different stakeholders and to the development of different heterogeneous solutions all over the world. It remains to be seen which approaches will succeed in the end. In any case, the increasing deployment of NFC based payment solutions is a great opportunity also for other security sensitive fields of application as it offers great potential for synergies and joint solutions.

5. CONCLUSIONS

The emergence of smartphones and the recent integration of NFC technology into these powerful mobile end devices have paved the way for the development of contactless payment solutions. These solutions allow customers to pay cashless at points of sale. A heterogeneous ecosystem of different NFC based m-payment solutions has evolved during the past few years.

In this paper, a representative subset of these solutions has been surveyed. In order to facilitate a classification and subsequent analysis of this heterogeneous set of existing solutions, distinctive features have been identified and appropriate classification criteria have been defined. By applying these criteria to the surveyed solutions, several interesting findings could be derived. These findings can help to improve the acceptance of future NFC based m-payment solutions and to introduce NFC also in other security sensitive fields of application.

REFERENCES

2degrees, 2012. *Touch2Pay – with Snapper Mobile*. http://www.2degreesmobile.co.nz/touch2pay.

EURO Kartensysteme, 2012. Girogo. http://www.girogo.de/.

Google Commerce, 2012. *Use any credit or debit card with Google Wallet*. http://googlecommerce.blogspot.co.at/2012/08/use-any-credit-or-debit-card-with.html.

Google Inc., 2012. *A smart, virtual wallet for in-store and online shopping – Google Wallet.* http://www.google.com/wallet/.

ISIS, 2012. *Welcome to ISIS*. http://www.paywithisis.com/.

ISO, 2004. *ISO/IEC 18092:2004*. http://www.iso.org/iso/catalogue_detail.htm?csnumber=38578.

ISO, 2005. *ISO/IEC 21481:2005*. http://www.iso.org/iso/catalogue_detail.htm?csnumber=40261.

ISO, 2008. ISO/IEC 14443-1:2008. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39693.

JR East, 2012a. *PASMO*, http://www.pasmo.co.jp/en/.

JR East, 2012b. *Suica*. http://www.jreast.co.jp/e/pass/suica.html.

Korea Smart Card Co., 2012. *T-Money*. http://eng.t-money.co.kr/.

MasterCard, 2012. *MasterCard PayPass*. http://www.paypass.com/.

Moneto, 2012. Moneto. http://www.moneto.me/.

NFC World, 2012. MTS launches commercial NFC payments service in Russia. http://www.nfcworld.com/2012/05/23/315880/mts-launches-commercial-nfc-payments-service-russia/.

Orange, 2011. Quick Tap. http://shop.orange.co.uk/mobile-phones/contactless/.

Paybox, 2012. *Paybox NFC*. http://www.paybox.at/7377/Privat/Produkte--Tarife/paybox-NFC.

Raiffeisen Bank International, 2012. CardMobile. www.r-card-service.at/cardmobile.

Rankl, W., Effing, W., 2004. *Smart Card Handbook.* John Wiley & Sons, USA.

Rogers Communications, 2012. *Introducing sureTap*. http://www.rogers.com/web/content/suretap?setLanguage=en.

The Smartphone Champ, 2011. *Second major security flaw found in Google Wallet….rooted or not no one is safe*. http://thesmartphonechamp.com/second-major-security-flaw-found-in-google-wallet-rooted-or-not-no-one-is-safe-video/.

Turkcell, 2012. *Turkcell Cüzdan*. http://www.turkcell.com.tr/bireysel/servisler/Sayfalar/turkcell-cuzdan.aspx.

viaForensics, 2011. *Forensic security analysis of Google Wallet*. https://viaforensics.com/mobile- security/forensics-security-analysis-google-wallet.html.

Visa, 2012. *Visa PayWave*. http://www.visaeurope.com/en/cardholders/visa_paywave.aspx.