Mobile Payment Ecosystems in Transition

Matti Penttilä[1], Erkki Siira[1], Maarit Tihinen[1]
[1]*VTT Technical Research Centre of Finland Ltd, PO BOX 1000, 02044 VTT, Finland*
Maarit.Tihinen@vtt.fi

ABSTRACT: *One of the most prominent mobile payment technologies of interaction paradigms is Near Field Communication (NFC), which provides simple and secure two-way communication between electronic devices. However, NFC-based services have not increased as expected. In this paper, the NFC payment ecosystems are introduced and reasons to why their use has not rapidly become more prevalent are discussed. The presented research results are summarised from business case studies that were carried out in various Finnish companies during the period 2012-2015. The results showed that the sustainable and feasible solutions are based on recognised standards and open ecosystems; national, proprietary or otherwise restricted solutions do not work. Accordingly, it was recommended to start with Value Added Service (VAS) systems as these involved fewer security requirements. Finally, the analyses pointed out that tokenisation offers light security version for most of services in the business and it was experienced a remarkable way for promoting the mobile payment services.*

KEYWORDS *-Mobile payment, Near Field Communication, Payment ecosystem, Value Added Services*

I. Introduction

Mobile devices and the services they offer have become an essential part of our lives. Today we usually carry a device that has lots of processing power, a big and clear display and ability to be constantly online. Throughout its short history the mobile phone has integrated other devices into itself, e.g. only few people carry around a separate camera or a digital music player any more. The mobile industry has been eyeing the wallet as the next victim of integration. Mobile payment generally refers to payment services operated under financial regulation and accessed from or via a mobile device. Digital transactions are already succeeding in web environments, and bringing them to the mobile device environment is seen as a natural progression. One characteristic of mobile payments is the fusion of new technologies like mobile banking, mobile wallets, SMS payments, biometric payments and Near Field Communication (NFC) [1]. As financial transactions with mobile devices are encouraged and brought into public use, the ability to interact with the real world is becoming an increasingly important function for the device.

There are a few interaction paradigms that mobile devices can use to interact with the real world [2]: scanning, pointing and touching. Scanning as a paradigm is based on finding the presence of local hotspots by omnidirectional or wide beam communication, usually based on radio frequencies. Pointing and touching interaction paradigms come naturally to humans and are thus easy to understand for users. The most prominent technology within the touching paradigm is NFC, that is, a very short range communication protocol that provides simple and secure two-way communication between electronic devices. Communication between two NFC-compatible devices occurs when they are brought within four centimetres of one another: a simple wave or touch can establish an NFC connection. NFC is a blend of cell phone and smart card technology and NFC-equipped devices work either in card emulation mode, peer-to-peer mode or reader-writer mode [3].

The first NFC phone was released in February 2006 and there were high hopes that the technology would be adopted quickly by mobile devices and also by the payment and ticketing industry. At that time, payment and ticketing use cases were considered to be the most important use cases and this has not changed during the nine years of NFC adoption. The NFC-based services did not, however, take off as expected [1, 4]. There are several reasons for this slow growth. This paper analyses the main obstacles to the success of NFC-based payment, it also introduces some contemporary mobile payment schemes and proposes a new approach on which the payment ecosystem could be built. Based on the analysis, we present some considerations for open mobile NFC-based payment and Value Added Service (VAS) ecosystems. This research was conducted between 2012 and 2015 as part of the Digital Services (DS) program (http://www.digital-services.fi), which was

facilitated by DIGILE (http://www.digile.fi), one of Finland's Strategic Centers for Science, Technology and Innovation.

The literature survey shows that NFC payment ecosystems and elements have been researched and discussed from various perspectives such as: introducing payment ecosystem models [5], main components of NFC ecosystems [6], business models [1], and assessments of payment systems [4]. However, only some of the research is focused on the transition of mobile payment ecosystems. Thus, in this paper, trends and changes in mobile payment ecosystems are based on experiences from business cases. In addition, the paper summarises the viewpoints for promoting NFC payment ecosystems.

This paper is organised as follows. In chapter 2, the research design and research questions are presented. Chapter 3 provides an overview of the NFC payment research and ecosystems. In addition, analysis of the challenges of mobile payment ecosystems is discussed. Chapter 4 presents the first real-life examples of mobile VAS business cases, which are considered a prominent path towards payment services. In chapter 5 the research results are concluded.

II. Research design

This paper is based on the research results within the DS program, realised as a PACE –project (NFC Payment Ecosystem project) that started in 2012. The actual work of the DS program was divided into four areas: small and medium enterprises services, financial services, educational services, and wellness services. The research introduced in this paper was processed under 'financial services'. At the beginning of the PACE project, it was recognised that offering NFC as a service was challenging due to 1) overall complexity of NFC, 2) a lack of active development with value-added NFC services and an end-to-end approach, and 3) limited support of NFC reader infrastructure at point of sale. Based on several meetings and workshops among the partners of the PACE project, the main conclusions were summarised as the following research questions: 1) Why have NFC payment ecosystems not become more general faster? 2) How could we advance an open global NFC payment ecosystem?

To find answers to the research questions, a literature survey was conducted by using publicly available information such as academic journals and conference articles. In addition, regular project meetings and workshops were utilised for directing the research and activities of the PACE -project. The idea of the PACE project was to develop an end-to-end NFC service concept for easy distribution and validation of various types of digital credentials. The developed system enables users to receive and store, e.g., loyalty cards to their NFC phones via simple APIs and use these credentials easily with various acceptance points. Starting the creation of a payment ecosystem from VAS instead of traditional money transfer was seen as a more prominent approach.

This article provides evidence from various single case studies. A case study research approach [7] was selected as it emphasises the ability of case studies to examine complex and unrepeatable circumstances and, in this way, to gather information for the creation of new knowledge [8]. During the PACE project, several business cases were developed and piloted in real environments of case companies. The close co-operation with industrial partners in the PACE project ensured that the research, case studies and produced deliverables focused on the most challenging issues faced by industry. In this paper, the main findings of the research are introduced and discussed in detail.

III. NFC PaymentEcosystems

NFC is a short-range, wireless connectivity technology that evolved from a combination of existing contactless identification and interconnection technologies. It was considered to be a great facilitator for proximity interactions between different devices [4]. There are several commonly known NFC payment ecosystems in the world, e.g., Apple Pay, Cityzi, Google Wallet, Mobile PayPass of MasterCard, OsaifuKeitai, SoftCard, UnionPay, and Visa Paywave. Today, contactless schemes are successfully deployed in quick-service and transaction-intensive industries such as public transportation. However, NFC mobile payment solutions have been lagging behind their expectations [1, 9]. Even if NFC mobile payment solutions have not achieved early expectations, it is evident that there will be a proliferation in their use in the future [10]. One of the strongest driving forces is the public's ever-increasing dependence on, and demand for, smart phone functionalities.

3.1 Introduction to the literature studies

In the literature, NFC payments have been studied from various points of view. For example, Ozdenizci et al.[11] analysed the status of NFC research and pointed out that it has mainly focused on technical aspects and applications of NFC. According to their survey, NFC ecosystems were analysed only in seven papers of which most are presented in this sub-chapter. In their paper, Madlmayr et al.[12] discussed the management of NFC ecosystems from a technological point of view. In addition, Kerem et al.[5] presented a role-based service level NFC ecosystem model and Benyó et al.[13] introduced the StoLpaN view on NFC ecosystems. StoLpaN is a pan-European consortium that aims to establish a secure interoperable operating environment for NFC services. Furthermore, Schamberger et al.[6] analysed the main components of an interoperable NFC mobile payment ecosystem. In addition, Kanniainen[14] demonstrated how industrial participants can position themselves in the mobile payment value chain and select the ideal secure element option.

Moscoso et al. [15] presented in their paper a graph-based analysis of market players and their relationships in two NFC payment ecosystems: SoftCard (formerly ISIS) and Google Wallet. According to Moscoso et al.[15]SoftCard is trying to increase the use of NFC services by providing their customers with NFC-enabled devices; Google on the other hand is attempting to gain momentum by co-operating with retailers to provide a working system for their customers.

Ondrus&Pigneur[4] presented an assessment of NFC in the context of a payment market. They collected their research data from experienced mobile payment experts from the Swiss industry. Ondrus&Pigneur[4] surveyed the preferences for payment technology and evaluated the organizational aspects of mobile payments. The findings of their research show that Swiss industry experts were quite enthusiastic about the future of NFC. Furthermore, Chae&Hedman[1] introduced a business model framework for NFC-based mobile payment solutions by using a comparative case study method to investigate Google Wallet and SoftCard (formerly ISIS), and their underlying business models. The findings of Chae&Hedman[1] suggest the importance of focusing on the aspect of scalability. Gannamaneni et al. [16] have studied why some mobile payment platforms have failed since 2000. They highlight four cases, none of which has a technological background in NFC, but the reasons for failure are similar across the cases.

3.2 Introduction to technical background

The NFC concept is based on integrating existing Radio Frequency Identification (RFID) technology, especially, ISO 14443-based, NXP-owned MIFARE and Sony-owned FeliCa portable consumer devices which are both widely distributed contactless smart card families. The legacy of earlier standards gives NFC compatibility benefits with existing RFID applications as it is often possible to operate with old infrastructure, even if the RFID card or reader is replaced with an NFC-enabled mobile phone. NFC is capable of emulating both RFID readers ("reader/writer mode") and RFID tags (“card emulation mode”). NFC hardware can include a secure element for improved security in critical applications such as payments. Using hardware secure elements in NFC devices offers a transaction speed that cannot be achieved when a transaction needs to go through the mobile device’s operating system. This is crucial in the ticketing use case where strict time limits are in place ensuring a smooth user experience at mass transit bottlenecks like gates in subways.

Ownership of secure elements is the subject of perhaps the most heated discussion concerning NFC as owners of the Secure Element (SE) can set the rules and fees for the rest of the ecosystem. It is important to point out that technically it has been possible to have several applications in a simple plastic smart card, but due to economic reasons these multi-application cards have never been able to gain traction. Because of the cryptography there is only one set of keys to the secure element and thus only one party can install applications on it. Plastic smart cards have been cheap enough to produce and distribute so all parties have chosen to have their own cards. The situation is different in the mobile phone environment as there can be only one secure element in the device and it must be sufficient for all parties.

In addition to the reader/writer and card emulation modes, there is an NFC-specific NFCIP-1 mode (“peer-to-peer mode”), defined in the ECMA-340 standard [17]. This mode is intended for peer-to-peer data communication between devices and in this mode, NFC is comparable to other short-range communication technologies, e.g. Bluetooth including Low Energy specifications, and IrDA (Infrared Data Association),

although the physical data transfer mechanism is different. In this respect, NFC can be seen as a rival of these technologies, even though it can also complement them. [18]

3.3 Roles and advantages

Moore [19] defined the business ecosystem as "An economic community supported by a foundation of interacting organizations and individuals." The ecosystem enables its members to move towards shared visions to align their investments, and to find mutually supportive roles [19]. In this paper, an ecosystem is understood as a collection of entities (businesses and organizations) that aim to provide an overall solution or application. Another characterization of business ecosystems can be described as a network of firms, which collectively produce a holistic, integrated, technological system that creates value for customers. The ecosystem concept emphasises its members' contribution to the system's functionality and their dependency on each other in the survival and evolution of the ecosystem [20]. In a business ecosystem the actors are intelligent and able to perform planning and predict the future. The business ecosystem's aim is to create and share value and innovations [21]. The simplified idea of business ecosystem is that business will evolve into a complex network structure where key players enhance network stability. The primary goal of a business ecosystem is to create new value through the increased volume and variety of information, services, and products available to the customer. In an ecosystem, companies should have a common (shared) vision for the targeted market space. Ecosystems emphasise relationships and permit companies to create new values that no company could achieve alone [22]. Thus, a business actor is a company or an individual acting in an ecosystem in one or several roles. A business role is the role a company plays in the ecosystem. Business ecosystems constantly evolve so that roles are changed, but the system as a whole persists.

In the platform point of view, Eisenmann et al.[23] classify different platform actors into three categories. It does not acknowledge the relative position of the stakeholders in one category but is helpful in recognising the abstract dimensions of the domain. Eisenmann et al. [23] have recognized the following categories: sponsor level, platform level and user level. Actors on the sponsor level are the stakeholders who get to decide platform participants, exercise property rights, etc. Actors on the platform level are the technical partners that are responsible for creating the technology and being the contact point between the sponsor level and user level. The user level actors are consumers and merchants. Gannamaneni et al. [16] have analysed why some mobile payment platforms have failed and their understanding of how mobile payment stakeholders are positioned in Eisenmann et al's[23] platform level framework. Both Eisenmann et al's[23] and Gannamaneni et al.'s [16] work has been included in Figure 1.

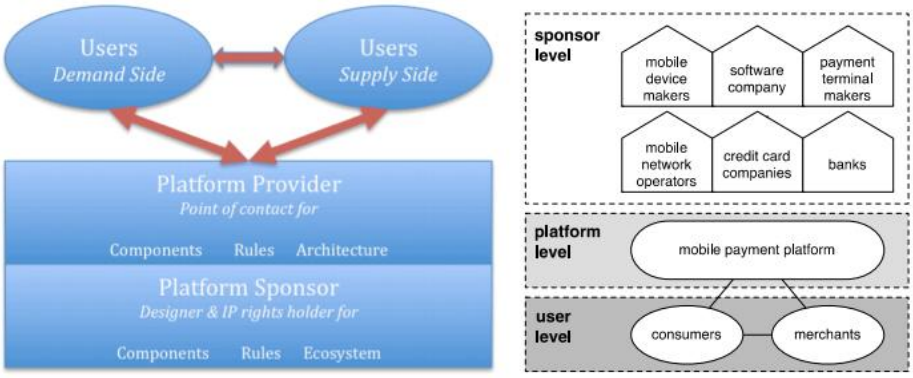

Fig.1. Elements of platform-mediated network and mobile payment platform in the relevant network. (Adapted from [16, 23]).

Gannamaneni et al.[16] do not specifically address the NFC payment ecosystem which has the same sponsor level and user level as general mobile payment usually does, but has a platform level that is unique to the NFC payment ecosystem. Continuing Gannamaneni et al.'s [16]research, Ondrus[24] has studied how different secure element solutions affect the NFC mobile payment ecosystem. Table 2 (below) presents the key roles of an NFC payment ecosystem and other related roles.

Table 2.Roles within the NFC ecosystem. Adapted from ([5, 16, 25, 26, 27]).

Role		Function
Application provider		Develops mobile NFC payment applications. Usually is not in contact with the end users but the front end is sponsor-level stakeholder, e.g. a bank. This role overlaps with mobile wallet provider.
Bank	Acquiring bank	Processes payments on behalf of a merchant. Usually this role is filled by credit card company, e.g. Visa or MasterCard.
	Issuing bank	Issuing bank has the customer contact and issues card association branded payment cards directly to consumers.
Chipset Manufacturer		Provides the integrated circuit components that are needed in NFC devices. Role of chipset manufacturer is diminishing as standardisation has gone forward and there is competition in terms of which manufacturer the chipset is bought from.
Component and tag Manufacturers		Make devices capable of supporting communication logic and communicating with new form factors.
Consumer		The consumer is the reason the ecosystem exists, he or she pays the final bill. The consumer needs to gain a monetary or usability benefit for the ecosystem to flourish.
Mobile device manufacturer		Manufactures and sells NFC-enabled handsets. In device-centric, secure element model the manufacturer is the central player who controls the payment ecosystem by owning the critical hardware.
Merchant		Functions as consumer's counterpart in the NFC payment transaction.
Mobile Network Operator (MNO)		Maintains network infrastructure, provides data connectivity to users, offers user authentication and user care for data connectivity service. In the SIM (Subscriber Identity Module)-centric secure element model the MNO is the central player who controls the payment ecosystem by owning the critical hardware.
Mobile Wallet Provider		Develops wallet and/or application and User Interface to manage NFC applications. The wallet or application can be pre-installed or downloaded via an application store or Internet. In some cases can also be a bank.
Point of Sale (POS) Provider		Manufactures the POS terminal that holds the software used at the checkout. Terminals usually provide a set of different payment possibilities to reduce the amount of devices the merchant needs.
Secure element owner		Handles ownership of the secure element.
Service Provider		Enables users to subscribe to and receive their personalized contactless cards, provides services to users.
Token Service Provider		Is responsible for handling the tokens that are distributed and processed. Payment provider can implement their own tokenisation services, but there is the possibility to use a specific partner for this. Especially for smaller providers. Not a mandatory role in the host-card emulation ecosystem model.
Trusted Service Manager (TSM)		Provides a contact point between network operators, service providers and NFC phones and provides the functionality of remote multi-application management. The TSM role has been created to reduce the natural ecosystem dominance of the secure element owner and to make it easier for the service providers to deploy their software to different secure elements with different owners.

In the mobile payment ecosystem model presented by the GSM Association [28], the MNO is considered to be one of the key actors, but solutions also exist [29] to bypass the operator to make more profit for the other actors in the ecosystem. To decrease the amount of actors and thus make more profit, in Host Card Emulation (HCE)-based payments, the role of Trusted Service Manager (TSM) and in direct payments the role of banks have been removed.

Several advantages can be recognised in terms of the different actors /roles in the ecosystem that NFC can enable. For example, network operators can get more income due to increased network traffic or renting space on SIM cards. At the same time, merchants get new and effective advertising channels, e.g. by pushing targeted coupons over the air using relationship management tools. NFC also provides fast handling of small payments. From the end-user viewpoint too NFC provides several advantages. It offers faster and easy payment with mobility, convenience and better security [30]. Generally, end-users may reduce the number of plastic cards and paper coupons in their physical wallets. They can carry as many credit and bonus cards in their wallet as they need and be ready to use them when the opportunity arises.

3.4 Ecosystems in transition

There are roughly three types of NFC-payments: physical SE-based payments, HCE-based payments and 'direct' payments that do not involve financial institutions. The three NFC-payment types are presented in more detail below.

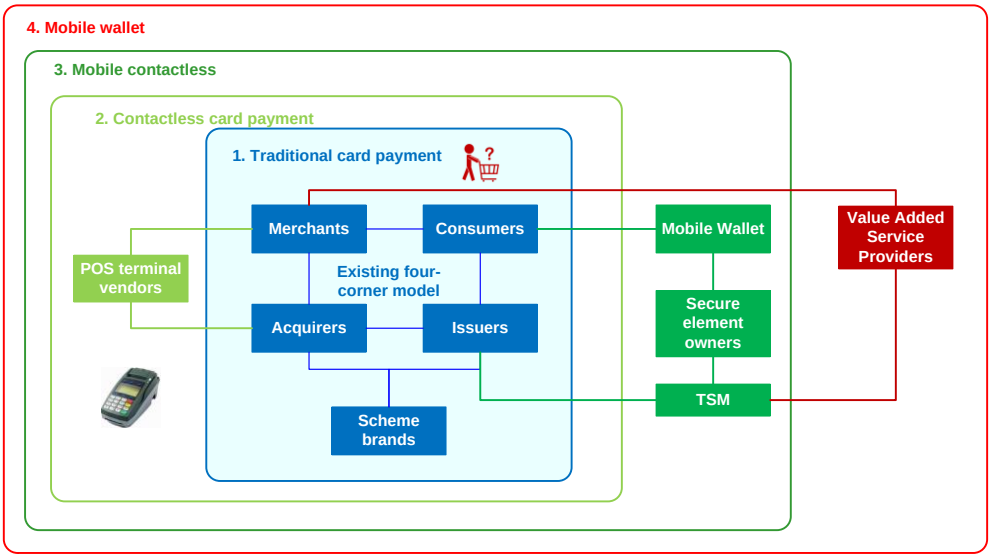

Fig.2. From traditional card payment to mobile wallet.(Adapted from [31]).

Figure 2 presents the key elements of existing and emerging payment models. The traditional four corner model (1. In blue) is in the middle. The first extension in light green adds the contactless cards and the POS terminals capable of reading them to the model. This does not change anything in the business model. The transactions via the cashier are a little more fluent than in the traditional model with magnetic stripes or chips. The next sphere, (3) in dark green, changes the business model more dramatically depending on the use of Secure Element. If the Secure Element (SE) is located in the SIM chip, the Mobile Network Operator (MNO) enters the picture, as it is the owner of mobile SIM. MNO may participate in revenue sharing by charging transactions or traffic. MNO may also rent the space for the SE on the SIM.

In MNO-centric model, the ecosystem requires the use of an entity called Trusted Service Manager (TSM). TSM is a neutral broker between MNOs and service providers. It creates a remote interface for service providers so that they can seamlessly deploy the applications to different MNOs' Secure Elements, which in turn hides the diversity of operators and technology. The TSM can also be the actor that is really in contact with the customer SIM through the security keys provided by the operators [32]. The Mobile Network Operator (MNO) maintains network infrastructure, provides data connectivity to users, offers user authentication and user care for data connectivity services. The Point-Of-Sales (POS) terminal can be used as a mobile device (mPOS), which makes a solution lighter and cheaper. It is typically used for inventory management, electronic payment, and queue busting. [33]

The red sphere (4) adds mobile wallets and value-added services to the picture. The mobile payment in sphere 3 can be located in the phone in a simple application or in Mobile Wallet. Value-added services may be in individual applications or collected into Mobile Wallet with single sign-in.

A mobile wallet is the digital equivalent to the physical wallet we already have in our pockets today. It is a container in which to store digitized valuables for authorization. These valuables grant permission for usage or access to goods, services or places. They can include personal identification like an ID or social security card, driving license, health insurance cards, payment cards, loyalty cards, website access or login data, and so forth. They can be non-personal means of authentication like tickets for public transport or events, car and hotel keys, gift cards and coupons. In Figure 2, "mobile wallet" means a digital wallet that enables you to make payments without having to locate your credit or debit card. The idea of the mobile wallet is to encompass all physical wallet functionalities in a mobile device. To create mobile wallet, the mobile wallet user has to: 1) create a

digital wallet with a mobile wallet provider, and 2) activate the mobile wallet on their mobile device by downloading the provider's corresponding application. Once the user has a mobile wallet application, he/she can start using the mobile device to make payments at any merchant with, e.g. an NFC reader, available at checkout. [34]

As Figure 2 shows, the area in which innovation could, potentially, build a common ecosystem model and make a profit is the area of Value-Added Services (VAS) and mobile wallet. The technology behind the solutions already exists. Transfer from traditional card payment requires introducing new business actors like VAS providers, TSMs (Trusted Service Managers), Secure Element owners and POS terminal vendors.

In 2013, Google announced the introduction of Host Card Emulation (HCE)-technology that is available in its Android operating system. HCE represents a new alternative to "traditional" NFC payments. In HCE, the payments application is on the phone's Operating System (OS), the "host," and interacts directly with the Cloud system and the NFC controller (see Figure 3). In HCE a card issuer does not have to use the SIM (Subscriber Identity Module) or another secure element to make contactless NFC mobile payments. With a suitable software-based payment solution, HCE provides another option for implementing NFC payments. Compared with physical Secure Element (SE)-based NFC payment implementations, HCE has its upsides, but also comes with its own limitations. For example card emulation will not work when the device is off. Figure 3 below presents the differences between physical SE-based NFC Payment and HCE-based NFC-payments. [9]

First, NFC devices were implemented in device-centric models where the device manufacturer owned the secure element and got to decide who could install software on it. In Western countries, this model was challenged by operators who wanted to use their SIM/UICC chip as the secure element. After a few years of trying the device manufacturers gave up and implemented SIM-centric devices. SIM being the secure element did not reduce the complexity of the overall ecosystem and the industry has been trying to solve it in several ways.

In recent years, HCE has been the most promising effort capable of solving some of the problems that have been encountered in SIM-centric and device-centric secure element models. Trying to get these models to work has already taken years and no real breakthrough has been achieved. It may be that neither of these models has a real commercial future in open markets where one company does not dominate the ecosystem. HCE on the other hand tries to solve the complexity problems these previous models had. It provides independence from traditional actors and offers more flexibility in terms of how mobile payment can be made. In addition to the emergence of HCE, consumers are already being introduced to the "payment by touch" paradigm, thus the education of consumers may be easier this time around. The lack of high security in HCE may make some payment use cases impossible, but on the other hand, by lowering the bar in terms of payment creation, it allows value-added services to be created without the heavy burden of the previously security-driven payment ecosystem. It is important to keep in mind that HCE is still a young technology and needs to mature before it can be adopted into wider use, but the technology problems can be solved easier than the challenges in the business models.

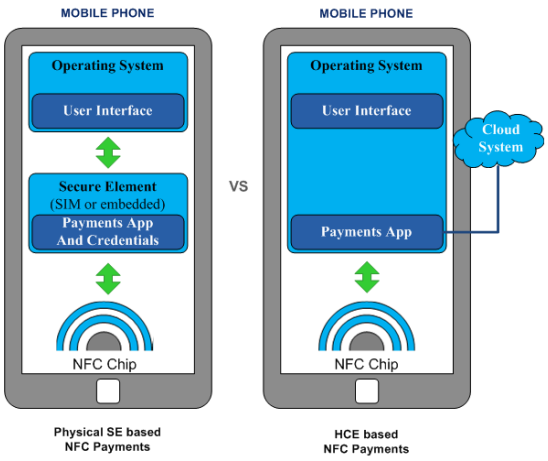

Fig.3. Physical SE-based NFC Payment vs. HCE-based NFC payment. (Adapted from [9]).

It is clear that broad adoption of HCE would mean many changes in the mobile payments landscape as it gives different entities more freedom to decide to what extent they want to work with other players in the value chain. HCE will in future be an important driver behind NFC-based mobile payment adoption as well as other services, but understanding the market dynamics and the control points will be essential to success [9]. Table 3 summarizes the advantages and disadvantages of HCE.

Table 3. Pros and cons of HCE (based on [9])

Consideration	**Physical SE-based solution**	**HCE solution**
Issuing /provisioning	Requires provisioning of the payment app and credentials to a physical SE (Secure Element) on the phone. May need a new SIM card.	Payment app can be downloaded from the app store. Payment credentials supplied as needed by the solution.
Security	Very secure, chip-based, tamper-resistant environment.	Need to manage risk of exposing the payment app to malware and viruses. Need risk-based authentication to ensure a legitimate device and that users can access payment credentials. Security ensured by utilising limited-use payment credentials (e.g. tokens, transaction keys) and other risk mgmt. techniques.
Current OS support	Android, Blackberry, Windows	Android 4.4 KitKat or later, Blackberry OS10
User experience	Seamless. Works with lower power or without any user interaction.	Without access to fast network, users may experience slow transactions (4.-full cloud solution). Tokens have to be delivered to the phone ahead of the transaction (risk of not having a token if the phone cannot connect to the network). Battery power may be required.
Transaction support	Currently for physical POS (Point of Sales; card present) only	Physical POS and e/m-commerce (card present or not)
Business model	Complex ecosystem and business model; issuers need agreements with both SE owners and TSM (Trusted Service Manager) suppliers.	Fast time-to-market, no need for complex issuer-MNO-TSM negotiations. However issuers may want to partner with HCE-solution providers or utilise third-party token service providers.

Tokenization of payment is becoming the standard method for mobile payment with HCE/NFC – technology. HCE is inherently less secure than physical secure element solutions and the security of payment data in the device cannot be trusted in the way that has been traditionally necessary. There are many methods of tokenisation, but in general terms; it is the process of substituting the secret account number with a single-use token, the use of which may be limited by the consumer device, channel or merchant. This reduces the impact of data breaches significantly. If the token is interrupted in one merchant's system it does not affect payments to other merchants. Token Service Provider (TSP) is a role that is not mandated by the ecosystem, but if it is used, its role is to generate single-transaction tokens from the static account number and to check their acceptance. Either way, transaction-specific data (token or session keys) will need to be distributed and managed [35]. The role of the TSP has been shown in Figure 4, along with how it fits into the traditional card payment ecosystem.

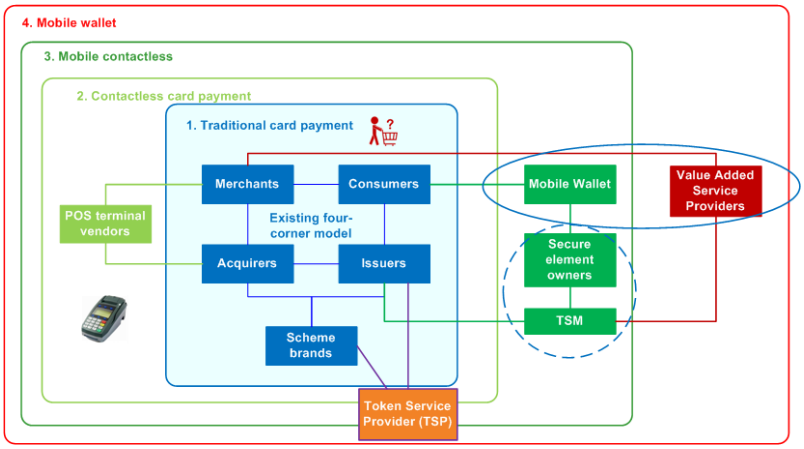

Fig.4. Token-secured mobile payment and VAS

In direct NFC-payments, the involvement of the bank is not needed. Payment is made using a mobile wallet and adding the payment to the phone bill, directly from phone to phone.

3.5 Discussion of identified challenges

Contactless mobile payment ecosystems have generally been slow to grow in number. The added value the contactless technology offers the end user compared to existing payment systems has clearly not been sufficient for end users to go to the trouble of acquiring such payment capabilities. Users may not even be aware that their mobile devices support contactless payment. Thus the model of acquisition has been emphasised from the payment ecosystem side. From the business side, contactless mobile payment ecosystems are formed mostly from already existing parties. This has led us to a situation where several entities in the ecosystem already have customer contacts. For example, the bank has its own customers, operators have their own customers and device manufacturers have their own customers. All these parties want to retain their own ability to directly connect and sell services to customers, but they do not want the responsibility of the role of help desk when something goes wrong with the system. A general ecosystem for contactless mobile services is lacking and the co-operation between different actors in the ecosystem is problematic [36]. Globally, one-country ecosystems or ecosystems that are based on one company do not work. Country-specific systems can be very functional in the specific context, but due to cultural and other differences they are often not generalizable or transferrable to other countries [37]. On a global scale, ecosystems based on one company do not work, e.g. due to trust issues. This has recently been rectified to some extent as technologies like HCE have enabled the creation of a global ecosystem (i.e. standards are shared and everyone has full control over distribution).

Gannamaneni et al.[16] have studied why some mobile payment platforms have failed, identifying five major reasons from four different use cases. Firstly, there is malfunctioning collaboration, which concerns non-diverging views of the different industries that are together creating novel ways to pay. Known cases can be found within transportation ticketing. You cannot buy a ticket from A to B but you need to buy separate tickets from the operators connecting A and B, e.g. the bus, train, ferry or other means of transportation. The second reason is no win-win business model; how parties agree on the division of profits, with parties feeling that they give more than they get from the cooperation. The paradigmatic case here is the attempts made by MNOs to enter the payment market. It has been very difficult to prove that the added parties in the payment ecosystem could reduce costs more than they would induce them. The third reason is the lack of support and promotion, which relates to how financial institutions play and active part in development but lack incentives to push it further. They join to keep control of things but do not foster further development of mobile payment platforms. One example of such a failure is the NFC payment ecosystem that requires (sometimes substantial) investment in the POI and cashier system. If this was solely the duty of the merchant, such investment would be neglected. The fourth reason is inadequate technologies and standards, which has to do with going to market prematurely, when the technology behind the service is not sufficiently mature or widely adopted for the mobile payment service to flourish. When the NFC phones have been tested with the readers, the success rate (especially on the first attempt) has been low. In time-critical services, such as mass transportation ticket validation, this has

created serious problems. The antennas have not been standardized or implemented adequately. The fifth and last reason is low value compared to existing solutions which relates to merchants and consumers not gaining sufficient benefit to move from more traditional ways of payment to the new mobile payment platform. A very well-known reason in payment ecosystems: the EMV plastic card is reliable, secure, efficient and easy to use. Why replace it with a novel and uncertain system that may require some learning as an entry threshold?

The challenge for payment interoperability and ecosystem lock-in has decreased after credit card companies introduced their own contactless payment to market. Existing contactless terminals are accepting payment from different ecosystems, thus increasing the market impact in the future. There is still limited availability of contactless payment enabled terminals. This dilemma is expected to disappear soon; in 2014 ca. 416 million NFC phones were shipped and the number is expected to reach 1.2 billion by 2018 [38].

Ecosystems themselves are not open and due to the systemic complexity of secure payment, the payment domain has not attracted small and flexible companies to challenge the existing parties. In addition, the current ecosystem actors do not want new actors in the ecosystem as it increases complexity and decreases profits [39, 40]. HCE as a technology is promising an easier way to make payments, so in future this dynamic may change.

Newcomers to the payment market like Google or Apple try to disrupt the payment business just as they have done in several other domains. For example, Google does not charge any fees for the use of their payment platform but they make their business from analysing transactions and selling that information for more directed advertising. Competing with "free" has always been difficult. New business models have their own frictions and in traditional domains like payment, the Google advertisement-based business model has as yet not been very well accepted.

Lack of technological maturity and incompatibility of devices have been major reasons for the slow adoption of contactless mobile payment [3]. Now that contactless technology has matured to a phase where interoperability and low cost have been secured, competition within ecosystem is beginning. For users the choice of mobile phone platform seems to be the most crucial one in determining which camp he or she is going to end up in.

In different domains payment faces different preconditions. For example, in public transportation, the speed of the transaction is crucial [41]. If payment is too slow, the flow of passengers is disturbed and queues form. The hard limit of 0.5 seconds per payment transaction has usually been advertised for public transportation. Several mobile payment transactions fail to achieve this, especially where transaction processing requires a network connection. In retail, the need for a loyalty card, couponing and vouchering infrastructure is present. The lack of a common standard to address these non-payment services has slowed adoption in the retail domain. [42]

IV. Business case experiences and analysis

In this chapter we are exploring paths towards more general payment methods and ecosystems through NFC value-added services which have been piloted in several business cases in the PACE project in Finland 2012-2015. The business cases were carried out in various Finnish companies – Bonwal (http://www.bonwal.fi/en/), Fara (http://fara.no/en/home/), IDcontrol (http://www.idcontrol.fi/en/index), Ideavoima (http://www.ideavoima.fi/), Juvenes (http://juvenes.fi/en-gb/restaurantsandcafeterias.aspx), SeamChip (https://www.seamchip.fi/), and UniCom (http://www.unicom.fi/index.php?page=home) – which are introduced in this chapter. Most of the PACE cases have been piloted or implemented in real industrial environments.

The NFC ecosystem for contactless payments has been well defined and standardized in cross-industry collaboration within the payments industry, e.g. EMVco (https://www.emvco.com/); mobile operators, e.g. GSMA (http://www.gsma.com); coordination bodies for banks, e.g. European Payment Council (http://www.europeanpaymentscouncil.eu/) and Mobey Forum (http://www.mobeyforum.org), handset vendors and key technology forums like Global Platform (http://www.globalplatform.org) and ETSI (http://www.etsi.org). Several successful NFC payment trials around the world have proven the acceptance of NFC payments by end-users and merchants. Rollout of payment terminals with contactless functionalities, contactless payment cards and mobile phones with NFC has enabled commercial launches of mobile NFC

payments. However, NFC payments alone are not enough. A wide variety of value-added NFC services like loyalty cards, coupons, vouchers, gift cards, event tickets, access keys, etc need to be in end-users' mobile wallets in order to make the NFC business case feasible for all players in NFC ecosystems. The overall complexity of NFC service architecture has slowed down the take-off of NFC-based value-added services. There is no common and open solution to NFC-based service provision for service providers or coherent user experience for end-users.

The PACE cases were focused on loyalty (SeamChip, Ideavoima), vouchers (SeamChip, Bonwal), tickets (Fara), mobile payments for predefined products (Juvenes, UniCom), and access rights (IDcontrol). We have tried to understand the benefits or success of each service by categorising the key factors of the services through the experiences gained in the PACE cases. The identified key factors of the services are categorized as follows: location of the credential; means of issuing credentials; means of payment; payment or methods of using various vouchers and tickets. These are addressed and discussed in the following paragraphs.

Location of the credential is important as the manager of possession has a lot of power over use. If the credentials are on the card, the issuer has a control to load and use as with a traditional travel card. It is logically the same with a card on a device. In validation there is no need for online connection to the back-office server. This has been necessary in public transport, where the network connection has not been guaranteed. If the validation of the payment has to always be done by the issuer (or its authorised/acquiring operator), the card on the device does not need to have more than an identity or secured identity readable by a validating terminal/POS. This may be done online in a timely fashion via a POS-delivered "list of closed cards and terminals", which prevents transactions.

Means of issuing credentials is essential because customers appreciate simple, straightforward ways of obtaining their credentials. Traditional methods included getting them by mail or collecting them from service points such as banks. Digital credentials may also be loaded at the authorized point of sales, a kiosk requiring physical contact as in the case of travel cards. They may be loaded to the user's network account. If the customer has a local writing device, (like an NFC chip on the gadget) the credential may be downloaded via the net and written to the card or device. The most convenient way to access the credential is to get it directly onto the mobile device by OTA with the necessary security measures.

The simplest *means of payment* is prepaid which may be printed on paper, loaded on the chip on plastic, or loaded digitally on an electronic device. This has no risks for the issuer or the merchant. The sum has already been received from the customer in advance. The customer always suffers in this deal; some prepaid credentials are never used. In fact, many prepaid schemes live within this unused, prepaid margin. The next most secure way of payment is payment by telephone, where the MNO SIM and possession of the device form the credibility basis. The transaction is sent to the MNO, which adds the cost to the telephone/MNO bill. The issuer's and acquirer's risk is put on the MNO. From the validation point of view, the "post-paid" method is just as simple. Transactions are authorised for strong identity holders, who will receive bills according to and after their use of services. This system simplifies, e.g. transportation payment clearing, remarkably.

QR is currently a popular identification *method of various vouchers and tickets*: the reader checks the unique code from the print or device display. It has a straight evolution path to NFC credentials, where the reader checks the credential from the card or device. Validation can be done locally or in the back-office. The issuing and security mechanisms are light and secure compared to other carriers.

Juvenes is a Tampere-based company that runs restaurants and cafeterias. Juvenes also offers catering and event organising services as well as printing services. In the PACE business case Juvenes serves 2000 lunches during a peak hour in one restaurant. The operating profit of one selling event is so slow that every cent counts. That is why the general payment methods (bank card, credit card and cash) are not feasible. Bonwal and Juvenes have created a payment system based on JavaCard that can be distributed to cards and NFC phones. This minimizes the issuing costs as well as reduces the time of payment, which are both critical factors for Juvenes' business.

Unicom Consulting Oy specializes in electronic payment and customer loyalty systems. Unicom offers solutions for membership, loyalty, ticketing and payment systems. In the PACE business case, the UniCom solution for the City of Oulu's lunch canteens allows for passing the cashier, which is of course the fastest payment method. Payment can be prepaid or take place after billing, which is very flexible for the user. The

back-end system keeps records on all the transactions and receipts, which makes it easy to control both money transfers and diet.

IDcontrol is a Finnish company focusing on physical or structural identification. IDcontrol provides access control, visitor management and ID-products to enhance a company's security. In the PACE business case, IDcontrol issued the credential – in this case access rights – via delivery over the air to the phones of the client. In the case of hotels, but especially with cottage renting, the management of keys is an enormous job. If the system can deliver access rights directly to the clients' telephones, enabling the opening of selected locks during the defined time period, all access system management can be practically automatized. This implies substantial savings as well as reduced errors, since the keys cannot be lost.

Seamchip is a Finnish company offering JavaCard based services [43] to a wide range of customers: companies, clubs, societies and event organisers. It is especially popular among SMEs and other small actors, who cannot afford loyalty, campaign or ticketing schemes of their own. The Seamchip concept offers many company-related benefits and services in one NFC-card or mobile app. One card can serve several companies as Seamchip handles back-office services. The merchant gets CRM and a direct channel to his loyalty customers via internet or mobile. He can also provide tickets or access rights (e.g. gym). The customer is treated the same way independent of company size or sector. The service provider can provide targeted info to his customers, who in turn can customise the loyalty benefits for him/herself.

The case studies in the PACE project have shown the power of value-added services, especially claiming credentials, when rolling out contactless services (blue oval area in the Figure 4). Both QR and NFC-based validation methods have been smooth and efficient. Using a mobile wallet to store services has been successful. In future research we have to consider the mobile wallet, which creates a new dilemma for the ecosystem: who is the owner of wallet? Does it create yet another player in the game? What does it mean for revenue sharing? Can the wallet be used to reduce costs?

V. Conclusion

In big picture, NFC payments have not taken off as predicted. All cases are unique, but they share common traits that explain why adoption of the service has been slow. NFC Payment services have been a great success in ecosystems where the keystone role in the system has been evident; the technologies have been imposed and the client potential has been actualised to a wide customer base. This type of scenario has taken place in more closed markets with very strong actors, e.g. in Japan and Korea. It has, however, resulted in problems regarding the extension of the services. They have not been open enough for the other players; national success stories have not grown globally.

The great number of stakeholders in the payment ecosystem slows down the take-off of the business as the number of contacts and contracts increases. Small national ecosystems such as Iceland and Estonia have been effective as the number of key actors has been limited and threshold investments moderate. They can often reach remarkable market coverage in relatively short periods. The developers of new initiatives have underestimated the strength of the current payment ecosystems. The system is not in crisis, it is functioning fluently, and customers were previously very used to card based payment systems. Mobile payment requires investments by users, operators and merchants. Savings in operational costs may, however, be marginal, so the return on investment may be delayed.

The standardisation bodies and NFC promotion companies have repeatedly stated that the technology is ready and easy to use. However, practical experience has shown that user experiences within the varying networks, devices, operating systems and POS systems have not been rewarding. Even small inconveniencies and obstacles in the introductory phase may prolong the take-off of the service dramatically. If the customer is king, the monarch has rejected payment difficulties.

These results elucidate answers to the first question research question set in the paper. The second question has been addressed in Chapters 3 and 4. The three main findings are as follows.

National, proprietary or otherwise restricted solutions do not work. They may have faster take-off with limited numbers of actors, but later they face major obstacles in the globalised world. There are so many different types of actors in the payment sector that in the end the restrictions limit the whole market or incur excessive costs because of overlapping or parallel systems. The only sustainable and feasible solutions are based

on recognised standards and open ecosystems. Without these, the critical mass of customers, merchants, banks, payment operators and device manufacturers is never achieved.

Right from the start, developing the end-to-end secure payment eco-system has been a bumpy road and has required huge investments and an enormous number of contracts to make it fly. That is why even the strongest companies have met overwhelming problems upon entering the payment business. Therefore we have recommended starting with VAS systems, where one can get into the market with fewer security requirements. In our PACE cases the customers and the entire market responded very positively. The customers have become accustomed to use their devices and apps, and the merchants have achieved better service levels with clear savings.

With its long track record, mobile contactless payment systems are again in the spotlight after Google announced its HCE solution in 2013. It answers a few of the biggest problems the previous systems have had, but the world is still waiting to see if the new technology advancements will endure the test of time and gain user acceptance. In general, HCE offers a higher flexibility and lighter security than secure element-based systems, resulting in its application in use cases that can benefit from these features. To circumvent the lower security of HCE systems a tokenization scheme is used to reduce the possible risk of security breach. It is deemed sufficient in several major cases and thus it substantially lowers the threshold for payment services.

To avoid common pitfalls, the PACE project took a different approach to payment than is usually employed. Instead of general payment the project focused on value-added services that do not require complex processes, multiple stakeholders and expensive infrastructure investment. Value-added services like loyalty schemes, access control, ticketing, vouchers, etc. are easier to roll out and are still powerful enough to succeed at a local level. Several details differ from solution to solution, but few of these appear to be the more important decisions. They are location of credentials; means of issuing credentials; means of payment; payment or using credentials and collecting usage data.

VI. Acknowledgements

We would like to thank Tekes, the Finnish Funding Agency for Innovation (http://www.tekes.fi/en), and DIGILE (http://www.digile.fi) for enabling and funding this research. We would also like to thank the companies: Bonwal, Fara, IDcontrol, Ideavoima, Juvenes, SeamChip, and UniCom, for their co-operation during this study.

References

[1] Chae, JS. &Hedman, J. (2015). Business Models for NFC based mobile payments. Journal of Business Models, 3(1).

[2] Välkkynen, P., Korhonen, I., Plomp, J., Tuomisto, T., Cluitmans, L., Ailisto, H. & Seppä, H. (2003). A user interaction paradigm for physical browsing and near-object control based on tags. In Mobile HCI, Physical Interaction Workshop on Real World User Interfaces. Udine, Italy, pp. 31-34.

[3] Al-Ofeishat, HA.,&Rababah, M.A.A.AL. (2012). Near Field Communication (NFC). International Journal of Computer Science and Network Security, 12(2), 93-99.

[4] Ondrus, J. &Pigneur, Y. (2009). Near field communication: an assessment for future payment systems. Information Systems and E-Business Management, 7(3):347-361.

[5] Kerem, OK.,Coskun, V., Ozdenizci, B. &Aydin, MN. (2013). A Role-Based Service Level NFC Ecosystem Model. Wireless Personal Communications, 68(3): 811-841.

[6] Schamberger, R., Madlmavr, G. &Grcchenia, T. (2013). Components for an interoperable NFC mobile payment ecosystem. The 5th International IEEE Workshop on Near Field Communication (NFC), Zurich, Switzerland, pp. 1-5.

[7] Yin, RK. (2009). Case Study Research: Design and Methods. The 4th edition, Los Angeles, Sage Publications.

[8] Järvinen, P. (2012). On Research Methods. Tampereenyliopistopaino, Tampere, Finland.

[9] Mobey Forum (2014). The Host Card Emulation in Payments: Options for Financial Institutions. White Paper, 25 p. Retrieved August 31, 2016, from http://www.mobeyforum.org/w/wp-content/uploads/20141118-Mobey-Forum-HCE-Report-FINAL.pdf.

[10] Du, H. (2013). NFC Technology: Today and Tomorrow. International Journal of Future Computer and Communication, 2(4), pp. 351-354.

[11] Ozdenizci, B., Aydin, MN., Coskun, V. & Ok, K. (2010). NFC research framework: a literature review and future research directions. The 14th IBIMA Conference, pp. 23-24.

[12] Madlmayr, G., Langer, J. &Scharinger, J. (2008). Managing an NFC ecosystem. The 7th International IEEE Conference on Mobile Business, 2008. ICMB'08. Pp. 95-101.

[13] Benyó, B., Vilmos, A., Fordos, G., Sódor, B. &Kovács, L. (2009). The StoLpaN view of the NFC ecosystem. IEEE Wireless Telecommunications Symposium (WTS 2009) pp. 1-5.

[14] Kanniainen, L. (2010). Alternatives for banks to offer secure mobile payments. International Journal of Bank Marketing, 28(5): 433 – 444.

[15] Moscoso, O. Z., Lekse, D., Smith, A. & Holstein, L. (2012). Understanding the current state of the NFC payment ecosystem: A graph-based analysis of market players and their relations. ISSN: 1390-6542 Enfoque UTE, 3(2):13-32.

[16] Gannamaneni, A., Ondrus, J. & Lyytinen, K. (2015). A Post-Failure Analysis of Mobile Payment Systems. Proceedings of 48th Hawaii Internaltional Conference on System Sciences. Honolulu, HI United States pp. 1159-1168.

[17] ECMA-340 standard. Near Field Communication Interface and Protocol (NFCIP-1) 3rd edition June 2013. Retrieved August 31, 2016, from http://www.ecma-international.org/publications /files /ECMA-ST/Ecma-340.pdf.

[18] Tuikka, T. (2009). NFC Technology and Reference Applications. In: Tuikka T, Isomursu M (eds): Touch the Future with a Smart Touch, VTT Research Notes 2492, Espoo 2009, pp. 33-38.

[19] Moore, JF. (1996). The Death of Competition: Leadership & Strategy in the Age of Business Ecosystems. New York, Harper Business. 320 p.

[20] Mäkinen, SJ. &Dedehayir, O. (2012). Business ecosystem evolution and strategic considerations: A literature review. The 18th International Conference on Engineering, Technology and Innovation, 18-20 June 2012, pp.1-10.

[21] Iansiti, M. &Levien, R. (2004). Strategy as ecology. Harvard Business Review, March, 1-10.

[22] Gossain, S. &Kandiah, G. (1998). Reinventing value: The new business ecosystem. Strategy & Leadership, Nov/Dec 1998, 26(5):28-33.

[23] Eisenmann, T., Parker, G. & Van Alstyne, M. (2008). Opening Platforms: How, When and Why? Harvard Business School Entrepreneurial Management Working Paper No. 09-030.

[24] Ondrus, J. (2015). Clashing over the NFC Secure Element for Platform Leadership in the Mobile Payment Ecosystem. Proceedings of the 17th International Conference on Electronic Commerce (ICEC'15), New York, United States.

[25] Mobey Forum (2011). Business Models for NFC Payments. White paper. 64 p. Retrieved August 31, 2016, from http://www.mobeyforum.org/business-models-for-nfc-payments/.

[26] NFC Forum (2008). Essentials for Successful NFC Mobile Ecosystem. White paper.

[27] Morgan, D. (2012). An Introduction to Mobile /NFC Ecosystems. Smart Card Alliance Mobile & NFC Council Webinar. Retrieved August 31, 2016, from http://www.smartcardalliance.org/resources/webinars/nfc_app_ecosystem/20120927_NFC_Application_Ecosystems.pdf.

[28] GSMA (2007). Pay-Buy-Mobile Business Opportunity Analysis - Public White Paper. Retrieved August 31, 2016, from http://www.gsma.com/digitalcommerce/wp-content/uploads/2012/03/gsmapbmwhitepaper112007.pdf.

[29] Clark, S. (2013) Samsung and Visa announce NFC payments plan that cuts out the carriers. NFC World. Retrieved August 31, 2016, from http://www.nfcworld.com/2013/02/25/322691/ samsung-and-visa-announce-nfc-payments-plan-that-cuts-out-the-carriers/.

[30] Zmijewska, A. (2005). Evaluating wireless technologies in mobile payments-a customer centric approach. In: ICMB2005- IEEE International Conference on Mobile Business, pp. 354-362.

[31] Pilkama, M. (2013). From Card Payment to Mobile Contactless (presentation). CAC card academy Conference, April 16, 2013, Helsinki, Finland.

[32] Ouoba, J. & Siira, E. (2013). Many Faces of Mobile Contactless Ticketing. Proceedings of the Second International Conference on Smart Systems, Devices and Technologies (SMART 2013), June 2013, Rome, Italy, pp. 23 – 28.

[33] Smart Card Alliance (2011). The Mobile Payments and NFC Landscape: a U.S. Perspective. White paper.

[34] Palermo, E. (2013). Mobile Payment Options: 3 Types Explained. BusinessNews: May 10th 2013. Retrieved August 31, 2016, from http://www.businessnewsdaily.com/4469-mobile-payment-types-explained.html.

[35] GSMA (2014). HCE and tokenisation for payment services. Discussion paper. Retrieved August 31, 2016, from http://www.chyp.com/wp-content/uploads/2015/01/GSMA-HCE-and-tokenisation-for-Payment-Services-paper_WEB.pdf.

[36] Benyó, B. (2009). Business process analysis of NFC-based services. IEEE International Conference on Computational Cybernetics (ICCC 2009). IEEE pp. 75-79.

[37] Amoroso, DL. & Ogawa, M. (2011). Japan's Model of Mobile Ecosystem Success: The Case of NTT DoCoMo. Journal of Emerging Knowledge on Emerging Markets, 3(1) Art. 27, 17p.

[38] IHS (2014). NFC-Enabled Cellphone Shipments to Soar Fourfold in Next Five Years. Retrieved August 31, 2016, from http://press.ihs.com/press-release/design-supply-chain/nfc-enabled-cellphone-shipments-soar-fourfold-next-five-years.

[39] Moore, JF. (1993). Predators and Prey: A New Ecology of Competition. Harvard Business Review, May-June 1993 pp.75-86.

[40] Herzlinger, RE. (2006). Why innovation in Health care is so hard. Harvard Business Review, 84(5):58-66, 156.

[41] Kevin, C., Millar, A. & Mc Garvey, C. (2012). Near field communication. International Journal of Electrical and Computer Engineering (IJECE), 2(3):371-382.

[42] Dyer, K. (2013). GSMA calls for feedback on NFC loyalty and coupon proposals. Retrieved August 31, 2016, from http://www.nfcworld.com/2013/05/10/323971/gsma-calls-for-feedback-on-nfc-loyalty-and-coupon-proposals/.

[43] Oracle home page (2016). Java Card Technologies. Retrieved August 31, 2016, from http://www.oracle.com/us/technologies/java/embedded/card/overview/index.html.