Analysis of the Latest Trends in Mobile Commerce using the NFC Technology

Mateja Jovanovic, Mario Muñoz Organero

Telematics Engineering Department, University of Carlos III, Madrid
Avenida de la Universidad, 30, 28911 Leganes, Madrid, Spain

***Abstract*— The aim of this research is to propose new mobile commerce proximity payment architecture, based on the analysis of existing solutions and current and future market needs. The idea is to change a Mobile Device into a reliable and secure payment tool, available to everyone and with possibility to securely and easily perform purchases and proximity payments.**

***Index Terms*— mobile commerce, mobile payments, NFC, proximity payments, RFID**

I. Introduction

Mobile commerce (m-commerce) is already being used and implemented as an alternative to many e-commerce services. There are many ways to define it, but simply said, "mobile commerce is a form of electronic commerce that specifically focuses on commerce by the use of Mobile Devices" [1]. This "simply" means that all the services related to commerce are being replaced with adequate Mobile Device services. Having in mind all the advantages of the mobility concept, mostly the fact that customers have their Mobile Devices with them at all times, as well as the fact that it is turning into a serious and secure payment device, it is quite likely that mobile payments will slowly take the leading role in the e-commerce field. Following technologies enable current mobile payment solutions:

- Short Message Service (SMS)
- Unstructured Supplementary Service Data (USSD)
- General Packet Radio Service (GRPS)
- 3G (Third-generation)
- Wireless Application Protocol (WAP)
- J2ME
- Location-Based service (LBS)
- Near Field Communication (NFC)
- Interactive Voice Response (IVR)

Each of these technologies has their own security issues. GSM (Global System for Mobile communication) network infrastructure still represents the most common media of connecting Mobile Devices to Internet, and it is already perceived as insecure. There have been many attacks in years, protection discretions were not fully considered. Having all that in mind it would not be wise to send confidential information, such as protective banking information, across open mobile phone network. This means that a secure mobile payment system has to handle sending secure data through unsecure network. Mobile Payments division can be based on the used technology. Two basic forms of mobile payment regarding these criteria are **Remote payments**, which are mobile phone based and rely on SMS, GSM, UMTS, HSPA, CDMA, WLAN or other technologies, and **Proximity payments**, which can also be mobile phone based (Bluetooth, IrDA) or via contactless card (RFID). These services have the similar demand of authenticating the user of the device, but use different payment techniques, and therefore have to be considered separately regarding implementation and security

Focus of this paper is on the RFID (Radio Frequency Identification) based Proximity Payments using the relatively new Near Field Communication (NFC) technology. The proximity payment concept is not new. Visa and MasterCard have already entered this market with contactless payment cards like PayPass and WavePay. Many mobile phone manufacturers, namely Samsung, Nokia and Apple, have recently vowed to integrate the technology into their future handsets, with NFC-enabled smart phones expected to be more readily available as early as 2012. Company Apple has hired an NFC expert as mobile commerce product manager, which proves that serious companies also consider this technology to be used more in the future [20], while the Nexus S Android phone with an active NFC chip was already presented by Google and Samsung. Nokia's executive Anssi Vanjoki also confirmed that all Nokia smart phones introduced from year 2011 would be equipped by NFC chip, and that they will support both, SWP (Single Wire Protocol) and microSD cards, as well as embedded Secure Element [12].

Many banks, mobile network operators, vendors and independent companies are already implementing this technology and doing a number of trials, but the industry is probably waiting for big companies, such as Apple, Google and Microsoft, to offer their final solution in this field. Observing the current implementation and big companies announcements regarding the NFC technology and proximity payments, there are many possibilities for the final outcome. Having in mind the difficulties of installation and quick implementation of NFC payment chip, the easiest way is just adding the NFC sticker to the back of the phone. This does not require a different phone, or a change of a SIM card, and therefore makes it more convenient for users. The sticker can establish the communication with the Mobile Device using Bluetooth, or have a hardware connection to the devices USB connection port. St Petersburg subway is adding a version of

this kind of payment by the end of 2012. MegaFon, one of three Russian mobile operators is contracted for this project. Users will have to initially activate the service with an operator, and the costs of tickets will be deducted from users phone account. Bank of America is planning NFC stickers in 2011, although they have a parallel running of another field trial program in New York, cooperating with Visa, where the microSD NFC solution is being tested as an alternative option [20]. State-of-the-art shows that many companies have recognized the great potential and are currently researching possibilities, entering joint ventures and doing trial programs in order to test the technology and current market. Observing the current situation there are many factors stopping this process from further faster development, whereas the most important are:

- Lack of a clear standard across the industry
- Interested parties entering joint ventures with biggest profit possibilities, regardless of possible technical inferiority of their solution
- Merchants not willing to buy new payment terminals and offer possibility of NFC payment to customers until there is a critical customer mass
- Users not eager to purchase new NFC Mobile Devices until enough Merchants are offering NFC payments
- Inconvenience of having Mobile Device as a single payment solution because of battery issues and possible call or other mobile network action in progress when payment is required

Aims of the research are:

- Proposing new architecture(s) and a clear standard, based on advantages and disadvantages of the existing systems
- Define roles of all players in each of the proposed architectures
- Estimate relevant players and customers interest in new payment system
- Analyze possible security issues and propose how to overcome them

The scenario consists of connecting users Bank Account with their Mobile Device, and providing a secure way of activating the application for payment and authenticating the device owner each time any kind of payment is engaged. Many companies have recognized a big potential in this technology, while the major concern is lack of a clear security and payment-processing standard across the industry.

Three different proximity payment architecture designs will be proposed and the evaluation will show advantages of each one compared to each other, and against the existing solutions.

II. NFC TECHNOLOGY

NFC (Near Field Communication) is a high frequency technology used for proximity payments in the m-commerce field. It works within the globally available and unlicensed radio frequency ISM band of **13.56 MHz** with a bandwidth of **14 kHz**. The specification details of NFC can be found in ISO 18092. It is a wireless communication technology; the proposed distance between devices is around 3-10 centimetres. The NFC technology is designed for usage in mobile phones. The device can communicate with existing ISO/IEC 14443 smartcards and readers, and with other NFC devices. It is a "read and write" technology, and it allows the high-speed transfer of data between enabled devices.

NFC device can be a reader, but can also simulate the smart card. NFC standards are designed in such a manner that they are backwards compatible with contactless card standards. Communication between NFC device and a smartcard is done through the APDU (Application Protocol Data Unit), executed in the proximity card processor. Standards ISO/IEC 7816-3 AND 7816-4 relate to APDU. Java smart card chip, used by Nokia, communicates using the message-passing model, where the Java chip receives and replies with APDU command and APDU response, respectively [19]

NFC equipped device can operate in two modes: Active and Passive, depending on whether it generates its own field. Active devices have a power supply; passive devices do not. In the active mode the data is sent using Amplitude Shift Keying (ASK), so that the base RF signal is being sent modulated. Each NFC transaction always follows a straightforward sequence of Discovery, Authentication, Negotiation, Transfer, and Acknowledgment. There are three NFC use-cases, depending on operation mode:

- **Card emulation mode**, where NFC device behaves like contactless card
- **Reader mode**, where NFC device is active and reads a passive device
- **P2P (peer-to-peer)**, where two NFC devices communicate and exchange information

Within the NFC classification elements are not referred to as Reader and Tag, but as **Initiator** (Reader part of RFID) and **Target** (Tag part of RFID). In the Active mode Initiator and the Target use their own RF field to communicate using self-generated modulation of self-generated RF field, while in the Passive mode Initiator is the one who generates the RF field, while the Target responds in a load modulation scheme. The Application or a phone MIDlet is in charge of which mode is to be used, and the transfer speed. After the Application is started, the check is performed in order to avoid RF fields Collision, and it will therefore determine whether an external RF field can be detected. It will activate its own RF field if no external field has been found. Target RF field is activated by detecting the Initiators RF field presence.

All the devices have the ability to maintain the communication speed in one of the four bit rates (106, 212, 424 or 828 kbps), or switch one of the remaining three. Carrier frequency stays 13.56 MHz at all times, while the value of minimal un-modulated RF field is 1.5 A/m rms, and maximal un-modulated RF field has a value of 7.5 A/m rms. Initiator produces the RF field in the Passive mode, not bigger then the maximal un-modulated value, to energize the target. Both devices generate an RF field alternatively in the Active mode. There is a thresh-hold value, which defines the point where the external RF field is detected, and its value is 0.1875 A/m. The Initiator and the Target in the Active operation mode both use ASK (Asymmetrical Shift Keying) modulation, with the modulation index 100% for 106 kbps bit rate, and 8 – 30% for bit rates 212 and 424 kbps.

NFC Tag is an ISO 14443 card, which can be a memory card or a microprocessor-based smartcard, holding a specific content. Smart tag can, for example, be embedded into the Smart poster, from where the users with the NFC enabled devices can read information and even receive coupons. Smart poster technical concept defines how to store a phone number, SMS or URL into the tag, and how to transfer them to the NFC reader device. It presents a smart system of interactive dialogue with customers. It makes it possible to make the application in the NFC phone initiate a phone call, send a simple text message or to be directed to a certain web address based on the information obtained from a smart tag. It can be used to download various content, such as e-tickets, ringtones, wallpapers, and videos, get coupons, subscribe to services, etc. NFC Forum, the organisation in charge of NFC standardization, has registered 4 types of NFC Tags [20]:

- Type 1, Innovation Research & Technology TOPAZ chips, proprietary communication protocol on top of ISO 14443-A modulation
- Type 2, NXP MIFARE Ultra-light and Ultra-light C chips, proprietary communication protocol on top of ISO 14443-A modulation
- Type 3, Sony FELICA chips, proprietary modulation and communication
- Type 4, standard ISO 7816-4 smartcards using ISO 14443A or B up to layer 4

Hardware-wise the NFC technology works like RFID, which was invented in 1945 by Léon Theremin as an espionage tool, and uses inductive coupling. This means that magnetic field generated by one side generates electric current in a certain conductor on the other side. The NFC chip has an integrated coil of wire, so that when two NFC chips get close to each other, for example an NFC chip equipped phone and NFC payment station generating magnetic field, the electric current is being generated in the Mobile Device initializing short range radio waves to pass between two devices. NFC chip alone works like a contactless smart card, and in order to work in the "Passive Mode" it is being powered by energy transferred from the reader that generates the RF field by the principle similar to the one explained, where induction creates the electrical current once readers RF field is entered. Security features and data protection features in this type of cards are the same like with contact smart cards [18]. Antennas in RFID are generally used to convert electromagnetic radiation into electrical current, or vice versa. The difference between NFC and the old RFID technology is the improved security; obvious by the fact that two-way communication is being established instead of just sending. An NFC hologram is copy-resistant and can be cancelled if it is stolen. There is a reason to believe that NFC is superior to Bluetooth regarding mobile payments. Even though is has a lower bit rate, NFC is more immune to eavesdropping because of the shorter range, and there are reasons of the speed (the entire process takes just a couple of milliseconds, while the Bluetooth process takes a few seconds), as well as lower pricing, having in mind Bluetooth is much more complex then NFC. NFC wired interface is defined by ECMA-373 standard. Two wires carry two signals, Signal-in and Signal-out. Combinations of these signals define the NFC-WI states between On-state and Off-state, where the Off-state is considered the default state. Switching between these two is called Activating and De-activating, while Escape sequence defines running to Command mode, from the On-state. Working frequency of the NFC technology (fc) is 13.56 MHz, and the clock frequency will vary 7 kHz around. State normally switches to "Off state" when Signal-in and Signal-out both have LOW value for at least 120 μs [14]. Once both, Signal-in and Signal-out carry the Activation sequence, the state will switch to the "On mode". Once the Command state is entered, the exchange is enabled, including: indication of the presence of the RF-field, information about the state of the RF-Collision avoidance and control information to change data rates and communication modes.

Protocols between any two elements within the NFC communication have to be standardized in order to achieve a globally functional and acceptable technology. The NFC technology acknowledgements are received by **ISO/IEC** (International Organization for Standardization / International Electro-technical Commission), **ETSI** (European Telecommunications Standards Institute), and **ECMA** (European association for standardizing information and communication systems). ECMA international is an international organization powered by industry, situated in Geneva, Switzerland, with the aim of making globally accepted standards in ICT field [14]. These standards are even more important in the field of wireless technologies because they help preventing collisions and interferences between the communications in the same frequency range. Standards define all communication modes for Near Field Communication Interface and Protocol (NFCIP) using inductive coupled devices. There are also complementary series of NFC security standards (NFC-SEC), and are used to define a protocol stack that enables application independent and state of the art encryption functions on the data link layer, on top of NFCIP-1. Standards ISO/IEC 18092, ISO/IEC 14443 and ISO/IEC 15693 specify 13,56 MHz as working frequency, but they specify distinct communication modes, defined as NFC, PCD (Proximity Coupling Device), PICC (Proximity Integrated Circuit Card), and VCD (Vicinity Coupling Device) communication modes [14]. The NFCIP-2 Standard specifies the mechanism to detect and select one communication mode out of those four possible communication modes. Principles and algorithms by which an NFCIP-2 (Near Field Communication Interface and Protocol-2) device determines the working mode are defined by ECMA-352 standard. By default, the device has the RF field switched off. If it detects an external RF field, it selects the NFC mode. Otherwise it selects between the PCD or VCD mode. Shared Secret Service (SSE) is establishing shared secret between two users. Secure Channel Service (SCH) uses the shared secret, which is established by SSE, and uses it to standardise the secure channel service to protect all subsequent communication in either direction according to the mechanisms specified by the cryptography standard. Protocol steps are also defined by this standard, and they are:

- Both NFC-SEC users agree upon the KEY. If users did not share any secret beforehand, Elliptic Curve Diffie-Hellman key exchange scheme is used for shared secret between devices. This shared secret is

used to establish the SSE and the SCH. The security parameter of the mechanism is 192 bit.
- KEY confirmation, required for both, SCH and SSE. Key confirmation, data integrity checks and data encryption functions are based on AES. Data confidentiality is ensured by AES with 128 bit key length in CTR mode
- If the service type is SCH - PDU security step is performed
- Termination step (both, SCH and SSE)

III. NFC Proximity Payments

Basic form of proximity payments is the category of off-line micro payments. They represent the first step towards reaching more complex, macro-payment online systems. Contactless smartcards that can work off-line and use only cryptographic protocol protection are no news. The main question is how compromised is the security by the fact that there is no real time bank confirmation required. The answer lies in two facts: Secure Element stored in the device preventing non-authorized users access, and classical Public Key structure which allows only registered parties transfers.

There are three Secure Element (SE) implementations that can be qualified as the possibly secure solution to play the role of actual charge card. Regardless of where the NFC component and the antenna are, what can really make a difference is placing a SE. Possibilities of SE placements are:

- NFC Secure Element on a **SIM/UICC** card
- **Embedded SE**, integrated by phone manufacturer
- **External SE,** such as NFC sticker with Bluetooth of USB connection to Mobile Device, or a **Memory card** (SD or microSD) with embedded SE, or all embedded NFC elements (SE, NFC component and Antenna)

Mobile Device has NFC software, which consists of Java ME program written for MIDP (Mobile Information Device Profile) – **MIDlet**, that runs on phones OS, and one or more **Java Applets** stored on the secure hardware element. Payment and ticketing applications are stored in a Secure Element in the device. Secure Element is a smart card chip, where multiple applications could be stored. Secure Element has a purpose to only accept software from trusted parts that have the private key that allows authentication. The entire process requires only one network connection. Once the issuer registers users phone number and the public RSA key, the X.509 certificate for that public key needs to be issued and sent to the Secure Element of the Mobile Device.

Most convenient solution for mobile network operators is the NFC chip on a SIM card, because it means teaming up of a network operator and any other party, or possibility of "renting" a place on multi-application SIM/UICC. Single Wire Protocol (SWP) is an architecture where SIM/UICC and Secure Element (SE) is actually same Java Card. UICC (Universal Integrated Circuit Card) is the smart card made for GSM and UMTS networks. It normally has a memory space of a few hundred kilobytes. These cards perform the functions of SIM regarding the secure authentication to the radio network, and also perform other applications and functions, possibly even play the role of NFC Secure Element. These UICC cards can literally be rented to other interested parties for storing their applications. There is another scenario how this could work: other parties can create these cards or have them implemented into their devices, and actually rent the mobile operators the space for authentication of the radio network. The future outcome of the events cannot be estimated now with a full accuracy, but it is certain that either of these parties will try to be the card owner and the one who is renting the space, and making the decision about whom to rent it to.

SIM card related solution, which is presented by many Mobile Network Operators and a few companies, such as Oberthur Technologies, propose the NFC antenna and controller embedded into the mobile device and connected to NFC SIM card. "Oberthur Technologies will offer a wide portfolio of Mifare DES Fire-enabled SIM cards to its customers, with free memory ranging from 128KB to 768KB and security level required by EMVCo and Common Criteria certifications" says the company [20]. Orange mobile operator has also announced a deployment of a new generation of SIM cards and handsets for mobile contactless services.

One of the big problems still unsolved seems to be how to meet banks security requirements, and how to simplify the certification cycling between SIM cards and banking Secure Elements. It is obvious that standard SIM needs to evolve in order to meet banking side security requirements. SIM-centric solutions for NFC mobile banking are based on the SIM card which remains the Secured Element for mobile payment, but, instead of using the SIM component to host the payment application, a dedicated component, also located in the SIM plug-in, is used to run the contactless payment application.

Third SE integration possibility is a interesting solution of using a memory card, such as SD or micro SD for implementing the Secure Element (SE), or even both, SE and the NFC Component & Antenna. This solution is of course not applicable to all Mobile Devices, simply because it requires the device equipped by a SD / micro SD card slot. No patent has been accepted as official yet, but there are a few companies that are recognized by certain institutions in the field.

There are several parties that are involved in every electronic payment system. Summarization of the particular roles of each party can be done in a number of manners. According to the Author of this report most correct scenario is represented by IBM Software group, which states that the roles are [21]:

- **Payer** (User, Customer) is an individual or an organization that makes the payment
- **Payee** is a Store or a Service Provider which receives the payment in exchange for providing Payer with a product or a service
- **Banks** are financial institutions (FI) where both, Payer and Payee have the accounts (Payers Account – Issuing Bank, Payees Account – Acquiring Bank)
- **Third Party Trusted Service** provides secure interface with financial networks in order to realise the transaction between Payers and Payees Bank accounts
- **Financial Networks** have the role of transaction network, interconnecting Banks and Third party trusted service

Player categories in the NFC Mobile payment architecture will also fit the mentioned rough role description of electronic payment. Payers are the customers with NFC chip equipped Mobile Device, while the Payee is the provider of services or products with the NFC chip reader equipment. Payers and Payees Banks will naturally have similar roles as in every electronic payment system, which leaves roles of Trusted Third Party Service and Financial Networks to be redefined in the new architecture proposal. New architecture should provide real-time payment processing, as current credit card payments do. Next issues are the mobile payment Transaction Costs. Among all, this will depend on the number of players who participate the payment process, and therefore the fewer players there are – the cheaper these costs will get. This shall be taken under consideration when evaluating three architecture options that will be proposed. Comparison will also be done against current credit card payment system, taking it as the most popular electronic payments reference.

An actual role of all the parties in contactless payments strategy is still not clear. There are a growing number of partnerships, each between different parties, teaming up and increasing the chances of their solution dominance on the market. The parties which are "in the game" are Mobile Devices manufacturers and software developers, Banks, Credit Card companies, Mobile Network Operators and a few of occasional others. A single solution that totally defines the role of all the parties hasn't been accepted yet, and it is quite clear that none of them wants to step out of the race, when it is almost clear that mobile payments are the future. Some partnerships, such as VIVO tech with their OTA (over the air) software and Monetise with the mobile wallet technology, allow clients of various banks to join in. Other solutions are developed either by certain Banks, or in the cooperation with a mobile operator. Example would be the Orange Credit Card by Barclaycard and Orange [7], an application designed to replace users credit card. Even big projects with an aim of replacing credit cards with smartphones, such as ISIS [8] joint venture between AT&T, Verizon and T-Mobile, do not have the clear role of all the parties. Credit Card companies seem to be out of a certain number of these partnerships, but being aware of the situation and the danger of being thrown out of the market they are investing a lot into this area.

IV. NFC Security Issues

Commonly known threats to the NFC security are:

- **Eavesdropping**, where the third party receiving a signal using the antenna
- **Unwanted activation**, which is somewhat similar to eavesdropping. Third party attacker tries to activate the card without the owner's knowledge
- **Data Corruption**, or modifying the data which was transmitted using NFC device using the valid frequency
- **Data Modification**, where the attacker is sending valid, but altered data to the receiving NFC device
- **Data Insertion**, where attacker tries to insert a new message into a NFC communication
- **Man-in-The-Middle-Attack**, where two parties who want to establish communication are tricked into communicating with or via the third party which is therefore enabled to record the entire conversation
- **Denial of service**, where the attacker tries to interfere with the RF field, in order to prevent the transaction

It is eminent that biometrics shall play one of the vital roles in authentication, which is one of the biggest issues of m-commerce. The old system, where given user ID and password, or PIN code are enough to authenticate a person, can be very vulnerable. Additional personal questions bring the security to another level, but there is still a need to perform a type of authentication where the user has to provide something that definitely proves the identity, such as Biometric control. Biometric control may include fingerprint, palm print, unique pattern of the users hand, iris and retina vascular pattern, facial recognition, signature and handwriting, key stroke dynamics, voice recognition and speech patterns.

First level of security on NFC proximity payments is achieved by using Miller and Manchester coding. Manchester bit coding encodes ONE and ZERO in a LOW to HIGH transition in the middle of a bit period. Modified Miller bit coding defines ONE and ZERO by the position of a pulse during one bit period. The pulse is a transition from HIGH to LOW, followed by a period of LOW, followed by a transition to HIGH. On different data rates, where data rate values are around 424 kbps, 212 kbps or 106 kbps, there are certain alterations to bit coding rules. Coding to be applied depends on the baud rate. If the baud rate is 106 kBaud, the coding scheme is the so-called modified Miller coding. If the baud rate is greater than 106 kBaud the Manchester coding scheme is applied. Like Bluetooth, NFC doesn't use a complex and unsuccessful Handshaking protocol. The type of coding applied depends on the coding scheme made in accordance with the two modes of NFC operating modes.

Combination of PIN or password and Biometric protection, such as fingerprint scan are considered to be sufficient, as long as all interfaces between all parties were designed with security concerns for Data corruption and modification.

The problem with the Fingerprint scan is that there are two modes of integration: using an external scanner, which is not too convenient for the user, or having mobile device manufacturers embedding it into their Mobile Devices. Second option might not be an easy solution for phone manufacturers, while it would make a significant improvement to overall Mobile Device security, including the Mobile Payments. Biometrics-specialist Company *Authentechas* from Shanghai, China has announced a new fingerprint sensor only 8mm by 8mm by 1.2mm, designed for the central navigation key of a mobile phone. To date more than 12 million mobile phones have been equipped with the company's biometric security solution, mainly in Japan [20]. Some companies are being the innovators, and are already manufacturing fingerprint scanner equipped Mobile Devices, such as Motorola with the model ES400 Windows Mobile phone.

V. Analysis of players and their roles

Having in mind a great variety of existing technologies, the future of proximity payments will most likely be determined by joined solution of some of the parties in the field. There are several possible scenarios, depending on type of players

involved. Interested parties are: Mobile Network Operators, Banks, Mobile Equipment Manufacturers, Credit Card companies and various third parties. Each of those has profit and predominance in market as primary aim, and therefore participates different kind of joint ventures and supports different types of payment architectures.

There is no doubt that Mobile Network Operators (MNO) have significant role in all kinds of mobile payments. Other parties can easily go around, and make a solution where the role of an MNO comes down to providing GSM and GPRS services required for necessary data traffic only. This way MNOs would be left without the share of the mobile payments market. Having a SIM/UICC card as a "weapon" and knowing it is currently used in most Mobile Devices, MNOs are pushing the idea of having the standard where the NFC Secure Element (SE) is stored on the SIM card, and making the unique charging system where users would be charged using the post-paid scenario for purchased goods and services in the same way they are charged for mobile data and voice traffic. This would mean that users would be getting a unique bill at the end of each month that would include an existing mobile services bill, and everything bought using NFC, and paying it directly to the MNO. If all the other parties let this happen, MNOs could predominate the proximity payment market. Other scenario that would work well for MNOs is having a Secure Element stored on multi-application SIM/UICC, whereas MNO and other parties from a joint venture would each take part. This solution covers joint ventures between MNO and Credit Card companies and a possible Trusted Third party company.

Banks represent another important player where any kind of financial transaction service, such as mobile banking, is involved. Banks have no preferences regarding technical architecture of the system, their interest comes down to making such a solution where another party provides a technical service, and users are charged directly from their bank accounts. Having this in mind, and the fact that users are generally more confident trusting their bank handling their payments, it becomes clear why they represent a significant partner in various joint ventures. Banks might even be offering the proximity payment service to their users in the future, in agreement with Credit Card companies, most probably with the condition of having their application installed on users Mobile Device. Users would likely be allowed to check the current account state using the application, and perform any of the other possible services, such as money transfers and mobile payments, including the ones provided by NFC technology.

Manufacturers of Mobile Devices are apparently a very significant party, because the entire story about mobile proximity payments makes no sense, unless users Mobile Devices are actually equipped with NFC chip, or at least with a SD or microSD card slot where the NFC card could go. Manufacturers like Nokia, Samsung and HTC have already started implementing NFC chips, and the reasons for it are their belief in the success of this technology and interest in profit that it certainly promises.

From the point of view of every device manufacturer probably the biggest advantage is that the entire group of customers interested in using NFC Mobile Payments will need to change their Mobile Devices, once the NFC standards and system architecture is final considering that most promising NFC market options are the ones where device manufacturers are the ones embedding NFC chip, Antenna and possibly the Secure Element into new devices. There are many ways how this could work, and each one is based on cooperation between a Mobile Device manufacturer and one of the payment service providers, most likely MNOs and/or Credit Card companies and Banks. If MNOs get the share of the NFC market, it would be in their best interest to either have SIM/UICC solution available, or offer Mobile Devices equipped with NFC chips to users who want to use this service, with a contract for a certain amount of time, like they're currently doing with voice and data services.

Device manufacturers naturally support the second option, where the success of this service would directly reflect to their profit.

Certain Mobile Device manufacturers and OS designers have a different policy. The biggest representatives of this group are Apple, Microsoft with devices running on Windows Mobile and Google with devices running on Android OS. There is one thing these companies can do differently from others, because they already have databases with users Credit Card and bank account information, which enable them to implement another way of charging users for mobile payments. As mentioned before, Apple has iTunes with 150 million users, Google has Google Checkout and Google Apps Marketplace with 25 million users, and Microsoft has Windows Phone Marketplace with 3 million accounts. NFC technology could enable these three companies to predominate the market by significantly reducing the roles of all other parties from the payment scenario. From their point of view the best form of proximity payments would be the one where the users Mobile Device would come with already installed NFC payment application that connects them to a certain Online Service. Users would use the application to pay for services and products, and would be charged in the similar way to current application purchase charging. Role of MNO's would be taken down to providing necessary data traffic only. Expansion of this idea may be total elimination of Credit Card companies from the process, and connecting users accounts directly to their bank accounts. So far Japanese company DoCoMo co. has been doing it quite successfully, which might give these companies the push to develop the strategy in that direction.

Fourth important party are Credit Card companies. Observing current market, it is quite obvious that Visa and MasterCard are trying their best by joining various companies from NFC field in a number of joint ventures in order to get the share of the market. This is actually quite a logical move from their side, because as mobile payment technologies start to predominate the market in the years to come, there are scenarios where credit cards would become obsolete and unnecessary, and these companies would lose their business.

There are other parties involved, some more important then others. Companies like NXP Semiconductors are doing NFC chip manufacturing on one side, and entering various cooperative works with other companies, such as G&D (Giesecke & Devrient) on Android project, to improve software solutions and architecture. NFC terminals are still not

ready for massive implementation because the manufacturers are somewhat confused by the great variety of different NFC system architecture solutions. Some chip readers are still in beta phase. Many chip readers still do not support NFCIP-2. Even though it has been seven years since the NFC was officially announced the proximity payment technology of the future, most chip reader and terminal manufacturers do not feel confident enough to start mass production of this product. The reasons for this are quite obvious. Since there are so many potential participants, type of the terminal might vary depending on the solution that prevails. This entire concept stops the NFC proximity payments from making a quicker breakthrough.

Other companies, such as Gemalto, Oberthur Technologies and Zapa Technology, are trying to establish the official role of Trusted Third party, or Independent TSM (Trusted Service Manager), having a problem of establishing the right tactics, because they need to enter a number of joint ventures in order to be accepted by other players on one side, but still need to maintain a neutral role on the other. Complexity of Trusted Third party role lies in the fact that it must be neutral, and it has to have following characteristics:

- Needs to accept and support all kinds of applications (Payment, Event Tickets, Transport and others) from any Issuer
- Has to support NFC Mobile Devices regardless of the manufacturer
- Has to support all Secure Element (SE) Issuers

VI. Proposing New Architecture Solutions

A. First Architecture Option

This architecture represents the next step from the current credit card payment architecture. From users point of view, the only difference will be that their Mobile Devices will play the role of the credit card. In the ideal case, Mobile Device manufacturers would include only NFC chip and the antenna to their Mobile Device; SE will be stored preferably to SIM/UICC. Credit Card Companies role stays similar like in current credit card payment system, with added responsibility of authenticating Customers Mobile Device using the applet on Secure Element. Basic design with all interacting parties is shown on Figure 1.

MIDlet on customers Mobile Device simulates contactless smartcard mode, so that POS (Point of Sale) Terminal manufacturers might not need to make new terminals that will be equipped with NFC chip reader. POS Terminals would use the same types of connection to the Credit Card company network as they currently do with credit card payment process: Dial-up or Internet Protocol (IP) whereas the dial-up is a backup option. Consumer also gets the revolving account from a Credit Card company, while the service/product provider gets the merchant account.

Since this architecture has MNOs and Credit Card companies as important players, both would get a piece of the multi-application NFC Secure Element (SE) stored in the SIM/UICC card. This is a significant improvement to current charge card payments in the security area, because two parties will perform authentication before engaging the payment. Assigning a part to Mobile network operators also means enabling the possibility of SMS payment confirmation to both, user and merchant. The Bank where user has the account and the Credit Card company are to provide the Application (MIDlet) for the users Mobile Device.

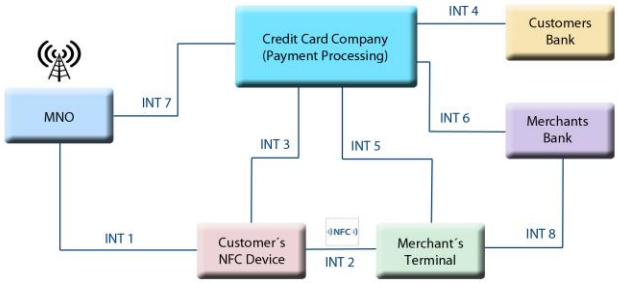

Fig.1 NFC Mobile Payment Architecture 1

Main differences from standard credit card payment system are the interfaces INT1, INT3 and INT7, presence of MNO in the architecture, and the slightly different role of Credit Card company. From users point of view, the main difference between this mobile payment architecture and the previously described Credit Card payment protocol is that user needs to turn the application on the Mobile Device and perform the authentication procedure before the payment. INT2 is where POS terminal is reading a smartcard chip, because upon having the Customer authenticated by Credit Card company and MNO, MIDlet on Mobile Device would be in charge of starting the smartcard-simulating mode.

B. Second Architecture Option

In the Second option Credit Card companies have a less important role. There is another player, Trusted Third Party service, which makes the architecture more secure and global, but also more complex. This might lead to the increase of transaction fees. Focus in this particular architecture is exactly on the Independent Trusted Third Party that has the role of the neutral trusted service. There are two possible solutions regarding the party that performs this role:

- Mobile Network Operator
- Independent Trusted Service Manager (TSM)

In this architecture Mobile Device manufacturer also embeds the NFC chip and the antenna into the device, while the Secure Element (SE) is stored into SIM/UICC card provided by MNO. NFC Payment Application (MIDlet) is to be provided by third party trusted service, including download and life cycle. There are companies trying to get into the market as the independent Trusted Third party, such as Venyon or Gemalto. Each of these two options has its advantages. This means there are two options under this option, but the architecture stays the same with minor changes regarding who is in charge of payment processing, application downloads (if such an option is provided) and management of the payment application life cycle. Interface INT2 of second case architecture is used for Mobile Device to obtain payment information from Merchants POS. In this case Mobile Device and POS Terminal are communicating using LLCP (Logical Link Control Protocol), proposed by NFC forum for P2P communication mode.

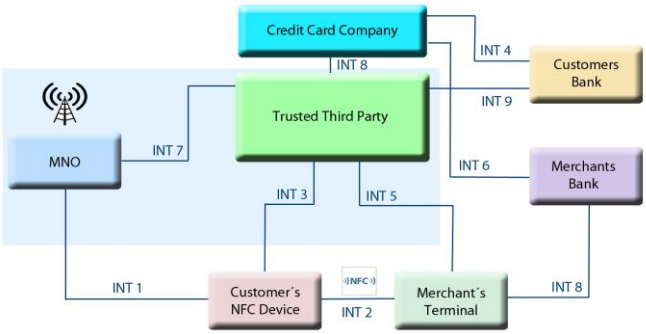

Fig.2 NFC Mobile Payment Architecture 2

Basic design with all the defined interfaces is shown on the Figure 2. Within this architecture a few roles are not final, mostly because a lot depends on the exact party that performs the role of the Trusted Third party. The shaded area represents the architecture alternative where MNO is assigned the role of Trusted Third party. Ideal case will be analysed here, and possibilities will be explained through the payment process description. Roles of individual interfaces will be further elaborated at the end of the process analysis. Typical payment process would consist of following steps:

- NFC equipped Mobile Device owner gets presented with the amount to be paid to the Merchant. User has to turn on the NFC application on the Mobile Device in order to start with the payment.
- Once the application is started, MIDlet activates the NFC chip. Communication with the terminal enables Customers Mobile Device to get the relevant information, such as details about merchant, including his merchant ID, and payment information including the amount.
- When the application has all the important data to process the payment, user has to prove the identity (authentication process). The most basic security procedure requires only the PIN number (Personal Identification Number), but this might not be enough. Biometric confirmation, such as fingerprint scan, should also be performed if users device is designed to perform this kind of authentication. Three applets are stored on SE, used for Customer authentication. MIDlet is used as a proxy between SE and Trusted Third parties Server, whereas the communication between MIDlet and the server uses SSL (Secure Sockets Layer) protocol.
- At this point the Mobile Device sends the data, including the amount to be paid, to the Trusted Third party by INT3 using the MNO data transfer network. In this architectural design the application on the users Mobile Device is to be provided by the third party, including download and the life cycle.
- Besides all the mentioned data and payment amount, users unique application account and credit card information are being sent to Trusted Third party. Along with all this, Request for Authorization is also being sent to the third party's processor network.
- Third party does the relevant checks, and forwards the request for payment to Credit Card company using INT8, which sends it to Customers Bank via INT4 in order to check whether Customer has sufficient funds on the account. Third party and the Customers Bank should also have a previously established agreement (INT9) for security reasons, somewhat like the one Credit Card companies have.
- Upon receiving and authorizing the request Bank checks the available funds on users account and "holds" the required amount, deducting it from the available funds of the users account. Confirmation is then being sent to Credit Card company's server via INT4, and then to Trusted Third party via INT8.
- Using INT3, third party sends the payment confirmation to the users Mobile Device, and the "Payment Successful" message appears on the screen. Funds have still not been transferred to the merchant's business bank account at this point, but they have been temporarily removed from users available funds.
- Merchant's terminal is still waiting for the payment status. There are two ways of realizing this step: either users device can send the confirmation using NFC by INT2 establishing another connection, or the confirmation can come directly from certified third party by INT5. This depends on the final architecture design, mostly regarding the policy of Trusted Third party. Both ways have advantages. While it might be more secure to get the response from the third trusted party, it would require additional communication between the terminal and the third party's server, which is not necessary in the other case.
- At the end of the business day, the merchant sends a request to the Trusted Third party via INT5, which is being forwarded to Credit Card company in order to secure the authorized funds from all the NFC transactions conducted through out the day.
- The total amount of all the NFC payment transactions, minus any processing fees, is then deposited into the merchant's business bank account.

Unresolved question is who is the better option for Trusted Third party, MNO or Independent body with TSM role, such as European companies Gemalto, Oberthur Technologies or Zapa Technology. Payment process will remain the same, with possible logistical changes on some interfaces. When summarized, there are three possibilities.

Mobile Network Operators could take the role of the Trusted Third party. Then the entire area shaded by light blue colour on Figure 2 and the connecting interfaces would be the responsibility of network operator. This way INT1 and INT3 would represent the same process. This solution has some advantages, because majority of smart phone users already have some sort of post paid account with a particular MNO, and the odds are their mobile account is connected to their bank account.

This way the role of MNO would be handling all the described processes that Trusted Third party is in charge in, which is all together a rather complex process.

Each MNO would even need to take over many responsibilities that are currently on Credit Card companies. Even though this solution might seem more convenient to

users, for they would be having a single party providing both, mobile telephony services and credit card functions and transaction fees would be cheaper, the transition process regarding necessary changes on MNO side might take very long if this architecture is to be announced the official NFC mobile payment solution.

C. Third Architecture Option

Third option represents the architecture with an even bigger role of Mobile Device manufacturers and designers of Operating Systems (OS).

Apple will most probably present its NFC mobile payment architecture with the new iPhone in July 2011. The reason so much attention is given to Apple in the Option 3 architecture is that this exact architecture is what everyone expects Apple to introduce. Other possible players in this architecture are Nokia, Google with Android OS and Samsung and HTC as biggest supporting device manufacturers and RIM (Research in Motion) with Blackberry devices.

Google and Apple have been most persistent to entire the mobile payment market lately, and the question is whether they are ready to go into the game with companies like PayPal, which have been in the payment field for more then ten years. Apple is known to be strong on customer service, which is very important in payments, while Google is stronger in technology-driven risk management and has the experience from Google Checkout.

Third option Architecture is shown on Figure 3, and there are only a few, but important differences compared to the first option, shown on Figure 1. In a way the Online Service takes the role of Credit Card companies from the first option, and the joined role of Trusted Third party and Credit Card companies from the second option. This does not mean that Online Service will have exactly the same role like the mentioned parties. First, there is one significant difference in the Architecture Diagram: There is no need for Interface 7, because communication between mobile carrier and Online Service is not necessary here.

MNO will only play the role of providing Internet connection to the Customers Mobile Device in this architecture. This means that connection between Mobile Device and Online Service (Interface 3) is physically realized via Interface 1.

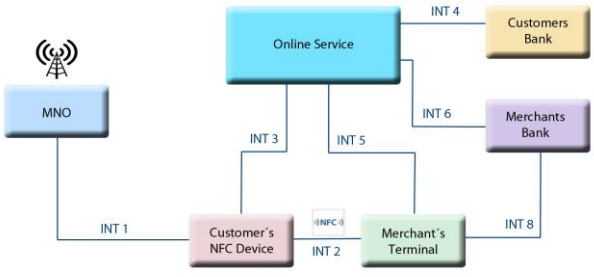

Fig.3 NFC Mobile Payment Architecture 3

Some of basic principles of this architecture are already presented in the Introduction section of this document. The most important player is the company that owns the online store where customer has an account and connects using the NFC Mobile Device, which is in this case OS designer company. Customer needs a Mobile Device equipped with NFC chip and with online service application and a valid account in the online service connected to his credit card.

As presented in the Introduction section, online service can be Apples iTunes, Google's Market Place or other. Application is to be provided by the online service company, which is the case of this architecture the OS designer company.

Typical payment process starts when user decides to pay for the service or product by Mobile Device using NFC technology and online service account. In order to do so, the first step is entering the application and connecting to online service using the existing account information, such as username and password via INT3. Users Mobile Device needs to have an existing connection to Internet, most probably provided by MNO, but in the case of this particular architecture other type of Internet connection is also allowed.

Once user is authenticated to the online service, he needs to read the payment information from the terminal NFC chip via INT2. Once the information is obtained, it gets forwarded to the online service for processing.

Before the user can proceed with the payment, online service needs to perform another authentication to confirm that the user who logged in was the one who requests the payment.

This step is pretty important, because simple PIN authentication might not be sufficient to qualify this system as secure payment method. Out-of-Wallet questions might be a good solution, unless the Mobile Device is equipped by some more reliable technology, such as fingerprint scanner.

Once the online service has the payment information and has authenticated the user, the required amount is charged from users credit card that is connected to online service account, starting by Issuing Bank determining that user has sufficient funds to perform the payment. "Hold" for the transaction amount is placed on the account.

When online service gets the positive response from the Bank, users Mobile Device gets the notification of the successful payment from the online service. The only step missing is notifying the company that provided the paid service or product about the transaction status. Just like in the Second Architecture there are a few options to realise the confirmation. First one is by establishing another NFC session between Mobile Device and the terminal, where the device would transfer signed confirmation provided by online service. Second option is that online service communicates directly to terminal, and notifies about the transaction status.

Mobile Network Operators provide the necessary standard data transfer services only, which means that additional security mechanism has to be implemented by online service for communication between Mobile Device and the service. Credit Card companies could maintain current roles in online services, such as iTunes and Market Place currently use, with the additional business provided by NFC payments. The problem of this architecture still remains determining the party that provides the payment terminals. One of the options is adding the feature to new models of credit card terminals, but this is the issue of accordance between online service, terminal manufacturers and Credit Card companies.

There is another possibility where the OS designers can actually avoid Credit Card companies and design a system where money is being transferred directly from customer's bank accounts to service provider's bank accounts. This concept might not be likely to be implemented in the dear future, having in mind security issues that companies like PayPal who have be doing payment services for more then 10 years have been trying to overcome. This means that credit card payments will continue to be a part of the process, which on the large scale means that this architecture also brings them a lot of profit. More cost effective solution for companies like Apple and Google would be a direct bank transfer, and it is likely that in time they will try to push Credit Card companies out of the game by implementing such a system. Even though their online services have many users, direct bank transfers are different, with a whole other set of issues. First problem is the lack of standard verification process, and lack of international coverage. Even bigger issue is the time banks take to confirm the payment. In certain EU countries, like Spain, it may last up to three weeks. On the other side, there is a possibility that Apple and Google will follow the example of DoCoMo in Japan and also design their own credit card ID and transaction system.

VII. Comparison and Evaluation

The focus of this section will be on evaluating proposed architectures and how these have advanced the current market solutions. Regardless of the NFC system architecture solution that prevails the market, the biggest problem remains solving security issues. Considering the fact that Mobile Device has to be quite close to the chip reader (normally 3-10 cm), sniffing/eavesdropping and "man in the middle" attacks are not considered biggest threats.

On the other hand the problems of user authentication and device-robbery represent issues that can easily make users scared of having their Mobile Devices and credit cards in one single device. For all these reasons it would be rather helpful if standardization bodies, such as ISO, NFC Forum and ECMA could reach a standard, which proposes unique set of characteristics that all Mobile Device designed with NFC mobile payment capabilities have to fulfill. There are two features that would have to be on the list:

- Beside PIN verification Mobile Devices would have to be equipped by a certain type of biometric verification. Fingerprint scanner would be a quite convenient solution for its price and the small portion of space, which is quite important for Mobile Device manufacturers
- Mobile Device manufacturers, NFC chip manufacturers and OS designers would have to agree on entire architecture solution with all parties involved, including MNOs and Trusted Third party (credit card or other) companies

Security issues of the entire payment system may be compared to the issues of current credit card payment system. All proposed architecture options have a few issues in common: Who makes the secure phone application? Who provides chip readers equipped terminals? These answers depend on the architecture, but the most important fact is that all the parties would have to agree upon trusted solution. There are a few possibilities for both, Mobile Device Application and chip-reader Terminals, depending on the exact architecture they can be made/provided by: by MNO, Credit Card companies like the current situation is, Mobile Device manufacturers or other Trusted Third party.

Device robbery or losing the device is significant security issue with a big influence of human factor. Even though customer might never see the device again, there are a few possible solutions. First of all, many of smart Mobile Devices are equipped with GPS chip, which might help user to track the device using some kind of online service. Any unauthorized attempt of activation the NFC services can be a trigger to GPS service activation. Having bank account connected to Mobile Device makes the matter more serious, which is why NFC service providing party should provide user with a possibility to quickly and at all times deactivate all NFC services if the device is stolen/lost, with the possibility to reactivate once the device is found. The security analysis can be divided into following parts: Security design, Vulnerability and risk analysis, Risk mitigation and security policies, Security deployments and monitoring. Security design depends on the mutual coordination of the involved parties. If there are many parties involved, like in first two architecture Options, the disadvantage is that certain parties can design their system and interfaces quite well, and end up with a security compromised solution because other parties, such as device manufacturers, did not make their solution secure enough. On the other hand, there are two parties designing each interface, which should mean increased security concern. Option 1 and 2 are quite comparable with current credit card payment systems, which means that within the last decades most security issues were covered. This makes the Mobile Device security, mostly regarding authentication, the biggest new security issue of all three architectures.

By this point NFC mobile payments have been analyzed from many aspects and suggested as possible breakthrough technology in mobile commerce area. Advantages and possibilities were presented in details in Introduction section.

List of goals of this research, presented in Section I, was made based on NFC technology and current market analysis and possibly encountered implementation problems. This document proposes new architecture with clearly defined roles and global industry standard. By adopting one unique and fully defined architecture, all parties, including users and service and product providers, would be encouraged to start mass production/purchase of NFC payment equipment. What cannot be foreseen are actual possibilities of one of the proposed architectures being globally accepted as a final NFC payment architecture, which mostly derives from such a big number of interested companies.

Three architecture options were proposed, each with a number of advantages and characteristics to be evaluated. Some parts of evaluation are valid for all three options, which will be emphasized. As presented before, evaluation will be done against these criteria:

- Cost efficiency from customer's point of view
- Cost efficiency from phone manufacturers point of view
- Global necessity for this kind of services

- Technical superiority of certain solution
- Integration problems regarding current market
- Future market and development in possible cases

First Architecture represents a single-step logical upgrade from current charge card (Credit and Debit) payment systems, with the focus on the Credit Card companies. There are only two major architecture differences from current credit card payment system: credit cards are replaced with NFC chip equipped Mobile Devices and group of issues regarding chip implementation and phone application.

Second Architecture is an upgrade of First Architecture where the most significant party in the system is Trusted Third service, where the role can be assigned to MNOs (Mobile Network Operators) or rather to an Independent TSM (Trusted Service Manager) Company.

Third Architecture has one major difference from first two options, which is possible elimination of the role of Credit Card companies. Focus is on the Online Service created by joint venture between Mobile Device OS designer and phone manufacturer (or single company in charge of both).

Criterion 1, Cost efficiency from customer's point of view: First option depends on Credit Card companies, and it is likely that transaction costs could stay similar to current Credit or Debit card payments. Second option can be non-cost efficient because of too many parties involved, while a lot depends on the Trusted Third party. If the third party is another independent company, it raises transaction expenses. Best solution from users point of view is the Third option, because the online service is the only party charging for the services, which means lower cost.

Criterion 2, Cost efficiency from device manufacturers point of view: First and Second architecture are definitely worse case for Mobile Device manufacturers because they need to embed NFC component and the antenna into the device, while third party provides NFC payment services. If the NFC technology does succeed, it will work well for them too, because users will be buying new NFC Mobile Devices. Third Architecture is the best-case scenario for them because of participation in the NFC payment transactions. Payment terminal equipment manufacturers on the other side will have similar profit in all three cases, as long as Merchants decide to upgrade their equipment.

Criterion 3, Global necessity for this kind of services: This particular criterion has somewhat been evaluated in this section, and for all three cases this criterion will get the same evaluation. Surveys and trials show that users do need Mobile Payment services because it represents the more convenient and practical way, as also presented in Introduction section. While some parties, like device manufacturers, see this as a great opportunity, some others, like Credit Card companies, participate mostly because of fear of losing current role in electronic commerce dominance.

Criterion 4, Technical superiority of certain solution: All three options have standard issues of Mobile Device vulnerabilities, like having the device stolen. Other then that, First option is similar to current credit card payment system, including advantages and problems. Second option is improved concept in comparison to the first one, because of Trusted Third party handling application download and life cycle. If an Independent Trusted Third party manages issues well, this might be the best technical solution. Third Scenario can be on high technical level if OS designers and Mobile Device manufacturers provide good authentication and secure online service. Issue of Third options is that of too much depends on OS designers.

Criterion 5, System integration problems regarding current market: First architecture would be the easiest to implement of all three solutions, because of current dominating role in electronic commerce. Second architecture problems depend on Trusted Third party service and their solutions, but considering the number of parties participating it would take the longest time to implement.

Third option could be developed rather quickly, even though it could be rather difficult due to the fact that providers of services and products might need terminals with support for each manufacturers online service.

Criterion 6, Future market and development in possible cases: Future market of the First Architecture represents the entire body of credit card users; having in mind that today almost everyone has a Mobile Device. Second option might take a bit longer because the plan is that users get enough confidence in the independent Trusted Third party to start using a new service instead of known credit card services. In the Third architecture, the Online Service Company would immediately have those users who already have the account, and they would easily adopt the new system, whereas winning of new users might be an issue.

Based on the analysis of each of the given evaluation criteria, Table 1 was created. Each of the architecture was marked against all offered criteria by descriptive marks: Low, Medium and High.

Architecture options were only compared to each other in this case, because each one has similar group of advantages comparing to current solutions on the market, defined in Section V.

TABLE I
EVALUATION OF PROPOSED ARCHITECTURE OPTIONS

	Opt. 1	Opt. 2	Opt. 3
Criterion 1	Medium	Low	High
Criterion 2	Medium	Medium	High
Criterion 3	Medium - High		
Criterion 4	Low	High	Medium
Criterion 5	High	Low	Medium
Criterion 6	High	Low	Medium

Even though Third Architecture has slightly better evaluation marks then the other two solutions, it is not likely it will predominate the market. Reasons for this can be explained by complex situation of pushing strong parties, such as Credit Card companies and Mobile Network Operators out of the race.

VIII. CONCLUSION

The aim of this research was to propose new mobile commerce architecture using NFC technology, based on the analysis of existing solutions, encountered problems and current and future market needs. NFC mobile payments have a lot of potential, but the lack of a clear and global standard in the industry is considered one of biggest issues, slowing down the mass-market penetration.

Three entire system architectures were proposed as possible final industry standard. First one represents payment system upgrade by Credit Card companies to enable mobile payments, second one introduces independent Trusted Third party, and the Third architecture relies on Mobile Device manufacturers and OS designers making an Online Service handling NFC payments connecting users mobile phones directly to their bank accounts without Credit Card companies. Each of the Architectures brings a level of progress compared to existing solutions, most of all because they introduce a new clear and global architecture standard and clearly defines the roles of all involved parties. However, it is very likely that the architecture that will predominate the mobile payments market will be a technically inferior one, but introduced by joint venture of companies strong enough to impose it regardless of the competition. Further work and improvements will be possible once big players, such as Mobile Device and OS manufacturers and Credit Card companies make the move.

ACKNOWLEDGMENTS

The research leading to these results has received funding by the ARTEMISA project TIN2009-14378-C02-02 within the Spanish "Plan Nacional de I+D+I", and the Madrid regional community projects S2009/TIC-1650 and CCG10-UC3M/TIC-4992.

REFERENCES

[1] Dwain Chang and Mandy Chin, “Will mobile television be a success?” Sep. 2007.
[2] Martin Newman, M-commerce - Now it really can be called a route to market, Aug. 26th, 2009.
[3] John Leyden “M-commerce - security risks exposed” June 2010
[4] Australian C&C Commission “Shopping on your mobile (m-commerce)” Aug. 2009
[5] Scarlet Schwiderski and Heiko Knospe “Secure M-commerce” Apr. 2008
[6] Jason Ankeny “Doubts in m-commerce security”, May 2009
[7] Ernst Haselsteiner and Klemens Breitfuß “Security in Near Field Communication (NFC), Strengths and Weaknesses” Philips Semiconductors, June 2010
[8] AT&T, Verizon, T-Mobile joined venture - Isis mobile commerce network Web page, Jan. 2011
[9] Lorenzo Stranges, Aymeric Harmand, Jean-Marc Meslin “Oberthur Technologies new SIM-centric solution for NFC mobile payment” Aug. 2008
[10] Finextra, independent information source for financial technology community web page, Oct. 2010
[11] Gauthier Van Damme, Karel Wouters, Hakan Karahan and Bart Preneel “Offline NFC Payments with Electronic Vouchers” Aug. 2009
[12] European Payment Council “White Paper – Mobile Payments” First edition, June 2010
[13] Prof. Min So Kang, Hanyangcyber University “NFC Technical Status and Application” RFID/USN Conference & International Exhibition, Seoul, Nov. 2006
[14] ECMA International, “global ICT and Consumer Electronics standards” Revision 1, Dec. 13. 2010
[15] Heikki Ailisto and the Finish ITEA2 project team, “Physical browsing with NFC technology, VTT Research 2400” Finland, Oct. 2007
[16] EMV, global standard for credit and debit payment cards web page
[17] Jeff Fonseca “NFC Market Update and Technology Overview” NXP Semiconductors, Nov. 2009
[18] Smart Card Alliance Contactless and Mobile Payments Council White Paper “What Makes a Smart Card Secure?” Oct. 2008
[19] NFC Research Lab in Hagenberg, Austria Official Web page, http://www.nfc-research.at/
[20] Near Field Communications Forum Web page
[21] IBM Electronic payment processing for Web businesses, Feb. 2002