KEMI-TORNIO UNIVERSITY OF APPLIED SCIENCES

The study of business opportunities and value add of NFC applications in security access control solutions

Harri Niemelä

Master´s thesis of the Degree Programme in International Business Administration

Master of Business Administration

TORNIO 2011

CONTENTS

ABSTRACT

Niemelä, Harri 2011. The study of business opportunities and value add of NFC applications in security access control solutions. Master´s Thesis. Kemi-Tornio University of Applied Sciences. Business and Culture. Pages 59. Appendices 2.

Since wireless technologies and electrical identification is already our everyday life, it is naturally to utilize latest technologies and in this case Near Field Communication technology to security access control purposes what we meet in our life at work, shops and everywhere where security of people, goods or premises are highly taken into account. The aim of this thesis is finding out economic possibilities to use Near Field Communication technology into security access control management.

This work studied the economic aspects and possibilities of implementing NFC technology into security access control segment. Information was collected of current situation and what kind of applications was currently available and expected to succeed in the future. After dealing with these aspects, there were negative and positive impacts evaluated what NFC would be security access control solutions. The study has been conducted through interviews, document analysis and extent observations.

A general usability of NFC was discovered and the factors of value-adding possibilities were seen. These success factors were pinpointed and limitations of technology summarized. Different aspects was described to making profitable business with customized products, concentrate market leaders or direct products to mass market.

The results of the study shows the guidelines and opportunities to utilize NFC at access control as economic point of view. This thesis can be used as a source of information for security access control by Original Equipment Manufacturers or service provider companies. NFC technology is ready to be used, but customers are not sure about the benefits and possibilities of it. It was seen also that new technology business possibilities are requiring increased co-operations between security service providers and security management companies.

Keywords: NFC technology, access control, security.

ABBREVIATIONS

B2B	Business to Business
B2C	Business to Consumer
EU	European Union
IP	Internet Protocol
IS	Information System
IT	Information Technology
MNO	Mobile Network Operator
NFC	Near Field Communication
RFID	Radio Frequency Identification
ROI	Return on investment
VTT	Technical Research Centre of Finland
Saas	Software as a service

INTRODUCTION

The development in wireless and computing sectors has been enormous during the past years. New products and services come out at an increasing pace to compete for market positions. “Technological innovations enable fundamentally new value propositions and transform current business structures as they change the earning logic and involve cooperation of companies from many industry sectors. Traditional sources of revenue are about to become commodities and the industry players are seeking new business opportunities.” (Ovum 2000, 61; Sikiö 2001,1) It can be seen that networking between industry sectors is increasing and new opportunities are giving value for operators.

The main aim of this thesis is to find out business opportunities and to study the economic aspects of NFC technology in the security access control business solutions. NFC brings new value-adding features to the current devices, and may facilitate a change in a way mobile and NFC devices are used. It has also a potential to increase their use, and it may generate a lots of new business opportunities including new service concepts. This work studies utilizing possibilities for NFC in security management business.

Firstly, I will evaluate NFC technology readiness from commercial point of view for other Original Equipment Manufacturer devices. I find answers to question of how the market for the current NFC solutions might be beneficial, add value and usable to use at security access control business in the future. The starting point for this study is the NFC technology, i.e. how currently and in the future it might be used in security access control solutions.

The technology brings companies from these and other industry sectors together to develop products in cooperation and thereby unifies the industries. There may be new players rising and maybe some old ones fading as new business opportunities emerge. Some of the new players may find new roles in the sector but some of them may take over roles of the current players. What the potential of NFC to cause these changes is remains to be seen as the standard develops but predictions can already be made to figure the potential effects. (Sikiö 2001, 2.)

1.1 Background

The term security management covers two different terms “Safety” and “Security”. Safety means accidental casualties and accidents which for example can be work, traffic, home, fire or product safety related. “Security” means intentional damages and relating criminal, terrorism or business security. Exception to this is information security where will be included accidental and criminal related risks.

Requirements of increasing security have arisen in Europe especially after highly visible and tragic events in Madrid and London. While responsibility for security rests largely with the national activities, the EU has also started planning research activities. As the general justification “Technology alone can not assure security, but security can not be assured without the support of technology” (Naumanen & Rouhiainen 2006, 4). Nowadays there is lot of research looking for usable solutions, not only technology oriented. This means adaption of new technologies into security management. Business security ensuring has been seen production and service operations security which generally includes buildings, premises security and also system information security management. There are measurement ways (due diligence) to recognize risk and this will be even more necessary in the future business from global environment. Critical objects ensuring affects benefits that there will be avoided production stops, service stops which have direct impacts to business results and reputation as a operator in own business sector.

Security industry has been split into four different segments, i.e. overall security management (identifying, positioning and data transmission), information network and system protection and also physical protection to those. Access control is a major factor when planning the overall security management guidelines. At the same time it is affecting flexibility of moving premises and it is used in the future as integrated solutions to building automation and other systems when controlling environment temperature, lighting together with security ensuring.

According to VTT Security Research, reference there is already now noteworthy entrepreneurship related to security. Although some of the companies are currently only operating in Finland, others are already international leaders in their area. The importance of security area is increasing and remarkable potential for new growth business areas can already be identified. This however also requires an increase in

research efforts. (Naumanen & Rouhiainen 2006, 4.) Several of these companies are pioneers of creating new technologies and their business opportunities.

NFC technology is becoming currently increasingly popular and several OEM manufactures are interested in the usability of it parallel with other wireless communication methods. There are a very few studies, how this technology can be utilized for future requirements and especially in security management solutions concerning how this detection technology creates new business opportunities from system and security points of view.

When NFC technology is, for example, a part of a mobile phone or another wireless device, these devices can be utilized in a competitive way by integrating services to it. One of the biggest drivers globally is NFC Forum, non-profit making association which has gathered several OEM manufacturers´ advances to develop applications, ensuring interoperability and educating the market about NFC technology. This association has been formed 2004, and there is at the moment 140 members where front-line mobile manufacturers Nokia, Samsung and for example Microsoft. (NFC Forum 2011)

The new NFC technology in combination with mobile communication could largely improve the usability, convenience, security and financials of a range of customer services. There is a lot of technical incompatibility of the solutions on the markets, challenges would be a business model settings what satisfies stakeholders. Currently the wide application potential of NFC and the long value chain of the services and vendors needs to be harmonized or interoperable solutions will not gain market acceptance. (Vilmos 2004, 1.)

My employer Schneider Electric Buildings Finland is interested in finding possibilities to take technology into use by integrating it to their systems and support NFC for access control solutions. They are looking for value-adding applications for the future, when Schneider Electric Buildings Finland is developing solutions from OEM and from service point of view to different parties domestically. Schneider Electric is interested in commercial and technological aspects of international markets in parallel with their product concepts. They have technology roadmap for building management solutions where access control is one part of it. New technologies are evaluated an updating is done regularly. This study is concentrating on the current situation and evaluates business opportunities for NFC technology. This evaluation is utilizing new innovative

ideas and is linking outcomes of the study to the future product roadmaps inside the company.

Security management access control and NFC terms and abbreviation are listed in the beginning of the thesis. This gives a reader an understanding what technology terms relating especially technology point of was used generally. There are some basic security management terms included as which are necessary to know when talking about business opportunities at this security management sector.

The purpose of this study is to examine the value the NFC technology adds and to analyze the effects it may have on the value network of the ICT sector. The focus is on the business side of NFC instead of a detailed description of the specification. The technical characteristics and the basic idea of the technology are introduced to give a general idea of the functionality of the technology and to form a basis for presenting the future application visions.

The value-adding to NFC is looked from the perspective of security access control management. The geographic perspective of the study is rather general. It is not tied up to one single country because ICT sector is very international. However, the challenges of international markets are discussed in general, because at the moment as NFC is still at the level that it is more interesting to look at the nature of the possible effects in general.

The perspective is, however, more European in the sense that the original Porter's value chain concept is discussed to provide the basic idea of value creation. However, the focus is on the reconfiguration of value chain to value network and on the effect that the development of information technology has on it. There are also several other drivers, such as the convergence of industries and globalization, transforming the way value is created, but in this study the focus is on the effects that a new technology may have instead of all the other drivers. The implications that new technologies, such as the Internet, have previously had on value chains give an idea of what kinds of changes may be expected as NFC enters the market.

1.2 Research aims and research questions

This research studies the business possibilities and the economic aspects of implementing NFC applications into the security access control solutions. Research

questions are concerned with economic possibilities of the NFC technology, benefits to older technologies because the current detection technology is widely used and is still competitive from the cost point of view. The aim was to prepare information to be used in a decision making when planning possibilities for NFC based services or solutions.

The new detection technologies such as NFC offering new business opportunities and requires co-operation between operators different ways than traditionally vertically or horizontally. Markets are changing and these opportunities bring new players to the industry. Therefore, to be able to plan for the future, possible effects of arising technologies have to be examined and alternatives known so that the most can be taken out of the coming market situation. The aim of this thesis is to find out how NFC technology affects to the value network of the security industry and how it may affects in general opportunities. The objective of the work can be translated into the research questions as follows.

The main research questions are as follows:

1. *What is meant by business opportunities in security access control solutions for the NFC technology?*

This question will be answered in the literature review part of this thesis in chapter 5.

2. *What kind of security access control solutions for NFC technology can be beneficial?*

This question will be answered in Chapter 5 based on the literature analysis and Chapters 6 and 7 comparing the theory to the observations and interviews.

3. *Are there limitations and will the economic aspects and other benefits of using NFC technology be enough to validate the costs?*

This research question will be answered in Chapters 4, 5 and 6 which are based on the interviews, NFC workgroup study and the own experience.

4. *What is the value of the NFC standard in the security access control business area?*

This question will be answered in Chapter 4 where there is a theoretical summary of the technology and in Chapter 6 which analyses the observations.

1.3 Research informants, data and methods

Theory was gathered from literature, handbooks and studies dealing with NFC technology generally or discussing the field of security management. The persons interviewed were chosen with work experience that they have enough experience and vision of this topic. There were persons from the security management business. The aim was to gather through interviews enough information, emphasizing the quality not to the quantity of the interviews. The analysis of interviews was done and supplemented with knowledge and practical experience (15 years) of the author in the field of wireless technologies and security access control solutions.

To do this, I needed information about the current situation and what kind of devices and applications were needed and in which situations they would be used. Theory analysis, theme interviews and observations will be summarized from economic point of view. Thereafter, it is essential to assess the negative and positive impacts that the introduction of NFC technology would bring to the security access control management solutions. This gives overview what are the expectations and limitations regarding the usability of the NFC technology usability at area. Finally, future possibilities for NFC at security management solutions at access control are studied.

It is increasingly important to meet and satisfy customer needs as the competition today becomes tougher and tougher. From the vast array of product and brand choices customers choose the ones that they believe will deliver the most value to them. They form value expectations on products and as acting on them they learn whether the offers live up to their expectations, which affect their satisfaction and repurchase probability. (Kotler 1994, 36; Sikiö 2001, 10.) In order to a company to succeed in the market it needs to offer increasingly value to customers than its competition, which means that it has to be able to cost-effectively offer products that customers value, and these products have to meet the requirements of use as well. (Andrews & Hahn 1998, 9)

Theme interviews as a research method were selected as an appropriate in the area where a few studies have been done and the amount a published information is limited. I am using consensual theme interviews which give a free hands to interviewee in the

defined area to give own thoughts and expertise to it. (Hirsjärvi & Hurme 2001, 35.) Theory based analysis and personal experience of the author will be used supplement and evaluate the information obtained through theme interviews.

Theme interview is a semi-structured interview by finnish. Interviewing will be done within predefined frame – some of aspects have been decided beforehand, but conversation is generally free. The aim is to find new information. Analyzing interviewed information and contents was done against theory based on research questions. (Hirsjärvi & Hurme 2001, 33.)

Interviewees were chosen from security management and information technology companies. Security management companies are operating as security system developers and sellers or detection technology developers and sellers. Information technology companies are working with NFC technology developers or solution providers. The interviewed persons were working in international sales, development or expertise positions in their organization.

1.4 Structure of thesis

This study paper is divided into three main sections. The first section approaches the research methods, NFC technology overview and general information of security access control; secondly there is value of new technologies and utilizing NFC technology from commercial point of view. This third part focused summarizing on evaluating economic value-adding and business readiness at security access control business solutions based on observation, interviews and conclusions. These aspects were examined by utilizing theory available in this field and interviewing experts of these fields.

2 NEAR FIELD COMMUNICATION TECHNOLOGY

In this part the intention is to give basic overview of NFC technology. This part describes NFC functional operating modes, applications and possibilities research subject. It is clarifies to understand the NFC technology and definitions behind these technical terms and related phenomenon.

2.1 NFC technology background

In March 2004, a new interconnection technology, Near Field Communication (NFC Forum 2011), was launched by Sony, Philips and Nokia with the establishment of the NFC Forum. The NFC Forum is a non-profit industry association for advancing the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs. NFC is a short range (max. 20 cm), standards based wireless connectivity solution, based on RFID sensor technology that enables active and/or passive communication between electronic devices in close proximity. NFC allows people to use the simple act of touching or placing their device close to something, another device or an RFID tag to initiate the desired service. This is making to use any form of electronic “service” and other interactions easier accessible to people, whatever their age or ability.

NFC secures, while the initiation of “service” handshake is always under user controlled. It removing the user need to perform complex manual operations. Once the connection is established – within milliseconds – information can be exchanged between the two devices using either NFC directly or via another wireless technology.

2.2 Operating modes

The technology has three operating modes, namely 1) Reader – when the NFC enabled device reads a passive RFID tag, 2) Card emulation – when an external reader reads the content of the NFC chip and 3) P2P which means that both communicating devices are in active mode, sending and receiving messages to each other. In this mode, NFC is comparable to other short-range communication technologies such as Bluetooth, Wibree and IrDA, although the physical data transfer mechanism is different. (VTT 2007, 13.) In this respect, NFC can be seen as a rival of these technologies, even though it can also complement them. NFC can open a connection between two devices that are brought close to each other, and the actual communication will then occur by Bluetooth or WLAN.

The legacy of earlier standards gives NFC compatibility benefits with existing RFID applications, such as access control or public transport ticketing. It is often possible to operate with old infrastructure, even if the RFID card or reader is replaced with an NFC-enabled mobile phone, for example. This is possible because of NFC.s capability to emulate 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. For example, a credit card could be integrated into a mobile phone and used by contactless credit card readers over NFC. (VTT 2007, 13.)

NFC has even greater potential when it is combined with mobile communication. Integrating NFC chip into a mobile handset the combination of proximity and remote communication is achieved opening further new perspectives. NFC is a standard technology that has recently achieved commercial availability via NFC chips, modules, mobile phones and PDAs. NFC is also backed by the leading mobile phone manufacturers and its deployment and chip development will be strongly driven via its integration into cellular handsets. For example, standardised interfaces to SIM cards and to dedicated security chips, as well as chip level integration of NFC with Bluetooth can be expected in the near future.

2.3 Applications

NFC is new technology – but due to its compatibility with existing contactless and smart card standards it can rely on the available infrastructure. There is practically no entry barrier from this perspective and the application potential of NFC is practically limitless. Compatible contactless technology is already used for payment transactions, ticketing, access control, content download, to set up connectivity for higher speed communication protocols without manual configuration and further implementations are planned for loyalty applications, ID card.

The contactless smartcard is a great improvement compared to its contact sister as it allows simpler, faster, increasingly convenient and cheaper interaction with the reader devices. The combination of mobile handset with NFC interface further improves the usability of the services and makes traditional contactless smartcard practically obsolete. The mobile NFC allows over the air access to the applications, which could facilitate remote download, management, update-recharge and deletion of the service

profiles and content, but more than that, it also provides the support of the phone resources.

The use of handset power, screen and keyboard opens new functions to existing services. The capability checking the status of the services or to request the recharge without the need to find a service station, or to exchange a ticket with a friend are all such functions which are not supported by existing contactless applications but are greatly increasing the value of service. (Vilmos 2004, 2)

There are motivators to financial sector to drive NFC technology applications. Main motivating reasons can be seen. Firstly, the fear that Mobile Network Operators are taking control of an area that has traditionally been in the hands of the financial sector is keeping financial institutions on their focus and under management. Management of the customer information is so valuable that the financial sector wants to keep hold of it. If the payment transaction is carried out with a payment application residing on the SIM card of mobile phone, MNOs would control and manage customer information, which raises concerns among financial institutions. In addition, the brand visibility of the card associations is threatened, if payment is handled using payment application in a SIM card. There are also positive implications in transformation from card to mobile phones. Traditionally, financial institutions have to bear the costs of issuing the physical cards and those costs could be decreased if accounts would reside in mobile phone payment platform.

A second motivating reason for investing in contactless/mobile payment technology is the competition between different financial institutions. Card associations are trying to find a way to differentiate their product offering from those of their competitors. Actors are also competing for the first mover´s advantage, which may provide additional competitive advantage in a form of large installed customer base and good brand reputation. However, financial institutions are driving contactless payment with smart cards in the first place; they already have in mind to move to real mobile payments that are handled using mobile phones. Contactless infrastructure that is built to be used with contactless payment cards should be either directly or with small changes be compatible with mobile payment conducted with NFC-enabled handsets. Therefore the change from contactless payment to mobile phone-based mobile payment can be done quite swiftly if

there is enough willingness and co-operation between needed stakeholders. (VTT 2007, 55.)

2.4 NFC device possibilities

NFC technology has evolved from a combination of contactless identification and interconnection technologies including RFID and it allows connectivity to be achieved very easily over distances of a few centimeters. Simply by bringing two electronic devices close together they are able to communicate and this greatly simplifies the issues of identification and security, making it far easier to exchange information. There are several manufacturers in different fields who are supporting NFC in their devices.

Near field communication NFC lends itself ideally to a whole variety of applications. For example it utilizes following possibilities:

- Mobile phones, PDAs, etc
- Personal computers
- Check-out cash registers or "point-of-sale" equipment
- Turnstiles
- Vending machines
- Parking meters
- ATMs
- Applications around the office and house, e.g. garage doors, etc

A further application that was proposed was that NFC connections could be used to configure the connection between two wireless devices. All that was required to configure them to operate together wirelessly would be to bring them together to effect the NFC "connection". This would initiate a set-up procedure; communication could take place over the NFC interface to configure the longer range wireless device such as Bluetooth, 802.11 or other relevant standard. Once, set up the two devices could operate over the longer range allowed by the second communication system.

NFC near field communication is ideally placed to provide a link with the contactless smart card technology that is already used for ticketing and payment applications. It is broadly compatible with the existing standards that have been set in place. Accordingly it is quite possible that NFC enabled devices could be used for these applications as well.

Numbers of NFC pilots in all regions have been done or are running. However, there is very little, if any, proper business and economic research available on how the different stakeholders benefit from NFC and what are the real costs and return of investment (ROI). Also as stated by the respondents “neutral analysis reports are missing entirely, all of them are twisted towards a group of players” or “happily written advertising articles are not useful; we are interested in concrete examples how and what did you do to make it work”. In other words, it needs to be justified why NFC would be better than the current smart card-based systems or e.g. cheap paper based tickets. If the benefits can not be made concrete it will be difficult to defend complex business models or new costs caused by the NFC ecosystem such as transaction charges, OTA and application management. From this perspective it can be argued, that besides the testing of technical functionality and use-case concepts, the NFC pilots in the future should concentrate on business models, money flows, concrete benefits and real costs. This would also create the basis for robust business cases and mass market feasibility, which are needed to encourage different stakeholders to make investment decisions. According to the primary data the real business examples and descriptions of best practices, were seen as especially important by financial institutions and system integrators. (Huomo 2008, 12.)

3 SECURITY ACCESS CONTROL GENERAL

3.1 Access control

This part describes security access control functionalities and basic detection operating modes. Access control is a system which enables an authority to control access to areas and resources in a given physical facility or computer-based information system. An access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure.

Access control is, in reality, an everyday security solution. A lock on a door is essentially a form of access control. A PIN on an ATM system at a bank is another means of access control. The possession of access control is of prime importance when persons seek to secure important, confidential, or sensitive information and equipment.

Item control or electronic key management is an area within (and possibly integrated with) an access control system which concerns the managing of possession and location of small assets or physical keys. Physical access by a person may be allowed depending on payment, authorization, etc.

In physical security, the term access control refers to the practice of restricting entrance to a property, a building, or a room to authorized persons. Physical access control can be achieved by a human (a guard or receptionist), through mechanical means such as locks and keys, or through technological means such as access control systems like the premises. Within these environments, physical key management may also be employed as a means of further managing and monitoring access to mechanically keyed areas or access to certain small assets.

Physical access control is a matter of whom, where, and when. An access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. Historically this was partially accomplished through keys and locks. When a door is locked only someone with a key can enter through the door depending on how the lock is configured. Mechanical locks and keys do not allow restriction of the key holder to specific times or dates. Mechanical locks and keys do not provide records of the key used on any specific door and the keys can be easily copied or transferred to an unauthorized person. When a

mechanical key is lost or the key holder is no longer authorized to use the protected area, the locks must be re-keyed.

Electronic access control uses computers to solve the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. The electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked.

3.2 Security access control systems

When a credential is presented to a reader, the reader sends the credential's information, usually a number, to a control panel, a highly reliable processor. The control panel compares the credential's number to an access control list, grants or denies the presented request, and sends a transaction log to a database. When access is denied based on the access control list, the door remains locked. If there is a match between the credential and the security access control list, the control panel operates a relay that in turn unlocks the door. The control panel also ignores a door open signal to prevent an alarm. Often the reader provides feedback, such as a flashing red LED for an access denied and a flashing green LED for an access granted.

The above description illustrates a single factor transaction. Credentials can be passed around, thus subverting the access control list. For example, Alice has access rights to the server room but Bob does not. Alice either gives Bob her credential or Bob takes it; he now has access to the server room. To prevent this, two-factor authentication can be used. In a two factor transaction, the presented credential and a second factor are needed for access to be granted. The second factor can be a PIN, a second credential, operator intervention, or a biometric input.

3.3 Security access control detection credentials

A credential is a physical object, a piece of knowledge, or a facet of a person's physical being, that enables an individual access to a given physical facility or computer-based information system. Typically, credentials can be something you know (such as number or PIN), something you have (such as an access badge), something you are (such as a biometric feature) or some combination of these items.

The typical credential is an access card, key fob, or other key. There are many card technologies including magnetic stripe, bar code, Wiegand, 125 kHz proximity, 26 bit card-swipe, contact smart cards, and contactless smart cards. Also available are key-fobs which are compact than ID cards and attach to a key ring. Typical biometric technologies include fingerprint, facial recognition, iris recognition, retinal scan, voice, and hand geometry.

Credentials for an access control system are typically held within a database, which stores access credentials for all staff members of a given firm or organization. Assigning access control credentials can be access control system components. An access control point, which can be a door, turnstile, parking gate, elevator, or other physical barrier where granting access can be electrically controlled. Typically the access point is a door.

An electronic access control door can contain several elements. At its most basic there is a stand-alone electric lock. The lock is unlocked by an operator with a switch. To automate this, operator intervention is replaced by a reader. The reader could be a keypad where a code is entered, it could be a card reader, or it could be a biometric reader. Readers do not usually make an access decision but send a card number to an access control panel that verifies the number against an access list. To monitor the door position a magnetic door switch is used. In concept the door switch is not unlike those on refrigerators or car doors.

Generally only entry is controlled and exit is uncontrolled. In cases where exit is also controlled a second reader is used on the opposite side of the door. In cases where exit is not controlled, free exit, a device called a request-to-exit (REX) is used. Request-to-exit devices can be a pushbutton or a motion detector. When the button is pushed or the motion detector detects motion at the door, the door alarm is temporarily ignored while the door is opened. Exiting a door without having to electrically unlock the door is called mechanical free egress. This is an important safety feature. In cases where the lock must be electrically unlocked on exit, the request-to-exit device also unlocks the door.

4 VALUE CHAIN AND VALUE NETWORKS AT NEW TECHNOLOGIES

4.1 Value of information system

In this chapter it is reviewed value chain and networks behind it. What are obstacles for new technologies and what ways technological innovations to be utilized for new businesses. The security market is partly driven by the increased vulnerability of modern complex society. Cost-effective production and delivery systems combined with dependence on the availability and reliability of IT systems implies that companies become increasingly vulnerable to operational shutdowns. The IT sector development is propelling higher technical content in technology-related sectors as enables these sectors to become increasingly efficient. Continued technological development leads to increasingly efficient solutions and lower prices.

Value gives customer competitive advantage for others. Values are splitted basic cost and total cost what is evaluated against whole economic cost to service or equipment what received. This includes costs of acquiring, using and maintaining.

In the industrial economy added value was defined as selling price less the cost of purchased raw materials and it was created and added sequentially in the value chain. (Porter 1985, 39) Final customers were seen as destroying the value which producers had created for them. Value creation is interpretative action and customer based on it evaluation to their customers. I find out that what is added value of NFC refers to technologies what are currently used and characteristic in industry at the moment. The added value to the participants of the value network of the ICT sector is seen mainly through emerging business opportunities. (Sikiö 2001, 4) At the same time the value creation is considered synchronic and interactive, and customers take part in the value creation as they co-invent it with their suppliers and their own customers. (Ramirez 1999, 49-51)

Value network can be created complex ways when processes are utilized with different operators, companies are using several products which are integrated together with different linkages. That means tight relationships between co-operators. Products might unique design and share values for both operators and sharing competitive advantage for co-operators. At this phase, it might increase new business segments.

The term value chain is often used to refer to the system in which value is created, disregarding the actual structure of the system. In other words, in some cases the term value chain is used rather generally without emphasizing the structure and it then may refer to a chain or a network. In this study the term value chain is used only when talked about a linear chain, and as the most of the value creation today is interactive and involves multiparty relationships the term value network is preferred. The studied network is an industry value network that includes several actors who can generally be seen pursuing a common goal. The purpose is not to describe a network for producing one single product but to illustrate the basic structure of the industry value network and NFC's effects on it.

Complex products often result in greater service content. There is a requirement that the product should complement the customers existing operations in an effective manner. In order to operate to satisfaction complex products require regular supervision and maintenance. In this matter, majority of products are complemented with associated services.

An Information system can be defined as an interconnected set of information resources under the same direct management control that shares common functionality. An information system normally includes hardware, software, information, data, applications, communications, and people. Many of business areas IS has a purely supporting role. Information technology, which is only one sector of IS, is used to efficiently handle everyday routine tasks, such as billing. This is the same in the different business areas. IT has replaced manual work in many areas, but the monetary value of this change is difficult to count.

4.2 Characteristics for technological innovations

Innovations in the high-tech industry often differ from those in other industries. They are often complicated and require increasingly from the customers. They are also hardly predictable when it comes to forecasting which ones will make a break-through and which ones will vanish. The diffusion of the innovations generally follows the same pattern of a very slow start and an explosion at a certain point. Technological innovations have several aspects in common, and these aspects are contemplated through some theories in this chapter to provide an understanding of the nature of technological innovations and change. (Sikiö 2001, 12)

There is lot of new innovations what increase customer value-adding for existing problems, problem comes the ways that those are economic competitive from price point of view. At the same time when replacing current solutions with new innovations, there comes new market space and demand of hidden features and solutions. This increases operator value adds to customer when showing future thinking when utilizing ways of doing solutions.

As the innovations in the high-tech industry are often discontinuous by nature, they require, unlike continuous innovations that are upgrades to existing products, consumers to change their current modes of behavior. Therefore, the attitude of consumers towards the adoption is a significant factor affecting the diffusion, and it can be described with the technology adoption life cycle in Figure 1. (Moore 1999, 12 ; Sikiö 2001, 15.) In the cycle, consumers are distinguished from each other by their characteristic response to discontinuous innovations, and grouped into innovators, early adopters, early majority, late majority and laggards. The cycle presents that technology is absorbed in stages corresponding to the psychological and social profiles of these various segments. (Moore 1999, 9-13 ; Sikiö 2001, 15.)

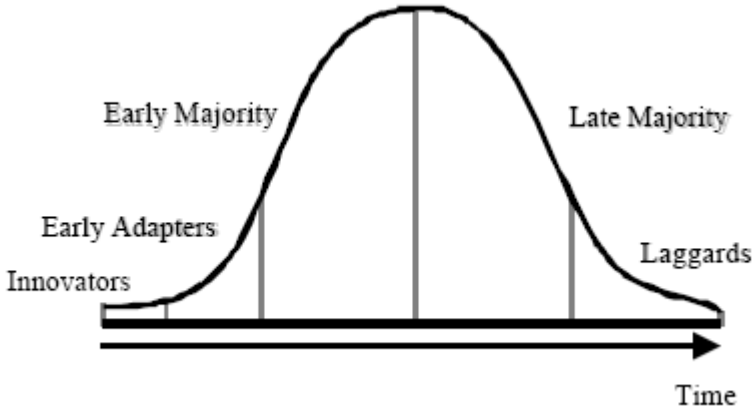

Figure 1. Technology adoption life cycle (Moore 1999, 12 ; Sikiö 2001, 15)

First there is a small group of adopters and as the technology evolves the products move up the performance curve until they begin to satisfy the bulk of users' performance demands and threaten increasingly sophisticated market segments. (Christensen 1998, 36 ; Sikiö 2001, 15) An example of this kind of diffusion is mobile telephony that was

adopted by a fairly small group of users until it became performance and price-competitive against wire line telephony (Christensen 2000, 25; Sikiö 2001, 15) and expanded so that it today partly replaces the wire line telephony.

The slow diffusion at the beginning and the explosion of user base of many technological innovations at a certain point can also be explained by the theory of network externalities or effects. Many information technologies follow the principles of this theory, as the value of a product to one user depends on how many other users there are. (Sikiö 2001, 15) These technologies tend to exhibit long lead times followed by explosive growth, which results from positive feedback: as the user base grows, increasingly users find adoption worthwhile. Eventually, if the diffusion is successful, the product achieves critical mass and takes over the market. Prime examples are communications technologies, such as the Internet, which exhibited this pattern.

4.3 Information technology and value chain

The current information technology environment is created and elaborated by several drivers. Development of information technology drives changes to value chain; it creates new utilized possibilities managing solutions and complicated processes. The convergence between different industries affects value chain and it increase values from operators to end-customers.

Market point of view, nowadays companies can born as global in the beginning when same concept can be copied a quite widely and localize when necessary. This kind of behavior reshape customer to require specified services which are customized locally. It is creating pleased customers when best practices are available to use and add value to their operating ways.

Value chain is not able respond to the all requirements themselves what is coming from turbulent environment. A fundamental problem concerns the definition of value. According to De Rose (1994, 13; Sikiö 2001, 11) Porter considers value and a competitive price to be the same thing, and he ignores the value in use, which includes excessive costs that result from unmet quality or time requirements. (De Rose 1994, 15 ; Sikiö 2001, 21) A reason for this is that the perspective of Porter’s value chain is rather product-oriented as he defines value as a sum of contribution of each activity in the production process to the final product.

Normally there are seen problems to show the value to customer and they are not able to evaluate cost and other benefit what are getting when operation comes increasingly effective. Customer wants to maximize improvements and try to avoid processes where there has not value in their eyes. The activities of value chain causes difficulties to operators achieve all these requirements and getting customer satisfaction parallel when needs to achieve cost-effectiveness. Integrated processes are giving increasingly space from functional point of view for solutions but at the same time increase complexity of the products and operators. That means co-operation with different operators and between industries.

Co-operation between design and engineering from technical point of can be managed and highlight targets when necessary. Challenges are coming when these technical changes need to integrate business systems where complexity of different solutions is changing fastly and there is not one-way to go. Solutions and services utilize operator's new ways to act in the value chain. Companies are forced to focused develop information technology together with their product offers in the value chain.

4.4. Advantages of value networks

Nowadays vertical integration benefits are reduce cost structure and it enables highly integrated product offerings from IT companies. IT companies are offering customized products for example Saas model, which same concept can copied and offered several customers, at the same time administration cost are lower when that is taken care by centralized way.

Electrical ways of communication has decreased costs between companies and value networks have utilized new kind of services and operation models. At the same time, these networks are flexible, scaling can be done faster comparing vertically integrated companies. Quality of integration is challenge where companies are focusing and get services what are acceptable level when offering products to mass markets. Companies which are developing their services and products together with horizontal partners are able to change their acting to customer and tune services in short term using power of knowledge from wide area.

Companies are able to focus in their key capabilities and strengths in value networks. Their have possibilities to outsource activities where they don't see as their key business areas. Outsourced services, they can develop co-operation relationships with top partners when increasing their own value proposition. This kind of collaboration means capabilities offering successful products in terms of new technologies linked together with products, services or combined solutions with innovative way.

Key competence value is depending customer feedback and real value can be evaluated based on market feedback and response. Even resources between networked companies are not enough if there is not real demand for the product or service. Companies must evaluate their current products value chain and which ways they are able to provide a new value for customers and major advantage in cost, service or asset productivity with flexible ways. This will be key factor also at security industry in the future.

These new value adding services and networks are decreasing material costs and at the same time resources are used increasingly efficiently. When these joint modes are working efficient ways, cycle times are shorter, quality of service improves and product value can be seen clearly. This means better impression to customer and market point of view. A information technology allows all participants closer contact surface to each other and helps them to control increasingly complex products and systems.

4.5 Environmental affects to value creation

Companies are forced quick decisions when industry environmental changes are happening fastly and technology development affects into the value networks. In that turbulent environment their roles are changing and giving space for innovative re-thinking. This brings value to customer and executes their decisions when choosing operators, system solutions and products. Until recently, also vertical integration has been used to reduce transaction costs and to provide lower cost structures. (Copacino 1999, 8) Vertical integration is one of value creation ways and differs from competitors.

New technologies are often used to swap one solution directly for another in order to save the customer money. One option can be to expand the value network and find way offer new value to customer. When integrate a new feature with innovative way, the overall service can be expensive, but customer pays more when system is used

effectively way. New system features helps operative actions - quality and reliability of operations.

New value proposition is generated by composed of elements that are aggregated from suppliers or employees and supplied forward after combining to customer. New technologies can enable disaggregation of the different elements and feed increasingly valuable offers to customer. These kinds of business model changes create benefits to customers. A new technology offers possibilities to operator's interactive co-operation when developing value networks and services. Digital development and customer activity changes whole thinking of services, entire industry sector solutions are blurring with new technologies and changing traditional ways and products. Value of the new services is based existing value propositions and when new offerings are set to customer and how they receive these into their current ways. There is big difference in company level and even globally, what is usability and attitude for new technologies and innovations. Those who are forerunners with new technology products and innovations, have possibility to use that position in their business development as competitive advantage.

Existing value chain knowledge and evaluation needs to do closely and breakdown of costs clear when developing efficiency and cost reductions with new technologies. Competence of employees and customers are affecting too when thinking digital innovations usability from business point view and part of the business models. Complexity of the product means partnerships with new kind of suppliers and channel thinking when creating business models and back office support to them. Strategic alliances between companies are increasing and even loosing alliances between companies become general globally, not only domestically.

4.6 Utilizing value network to the security sector

As many firms are moving at least some of their value-creating activities to the new electronic space to add significant value to customers (Cartwright & Oliver 2000, 22 ; Sikiö 2001, 33), increasingly companies appear to compete for positions in the security market. As a result, the way value is created and the sources of revenue are transforming in the industry. As the access technologies have become faster and increasingly affordable like NFC technology, the use of the connecting networks has

increased and changed, and the value chain has converted to a network that is too large and complex for anyone to “own”.

Today’s innovative value networks include large and smaller specialized players, whom are operating with specialized areas and their key competencies, are narrow and a quite typical nowadays. Those operators whom are integrating successfully new innovative products and partnering, can gain market share in traditional security sector when involving new products into current solutions in the security sector. The players with old technologies are predictable in their activities and customer are looking for re-thinking which way they are gaining advantages for current solutions and openness for innovations.

The obstacles between wireless and security sector are disappearing, which means that several new organized operators are entering to another business segment. Security companies are looking for and ensuring that they have capabilities to provide IP services in their networks and develop new business models based on IP product possibilities. Over the network services are cost effective to customer and flexible but there is some limitations which are relating information security especially accessing to system. Internet is creating challenges to employees what comes to usability and information security.

4.7 Wireless and cloud computing technologies on the security value network

Cloud computing services and wireless technologies development are continuing security value network. Smartphone users are increasing and it will force operators to develop new content offerings to online and real-time point of view. This is making great opportunities to operators and new players entering to market, plan to gain earnings and customer relationships with new technology based solutions. This causes, that market become increasingly competitive and co-operation increasing when complex systems needs to several players knowledge to set-up and maintain reliable way.

NFC is one of the technologies which are creating new opportunities when used in customers´ operations for example through mobile. Customer can use NFC to utilize services with secured way and fastly from field point of view. The PDA devices are changing accessibility to internet and services. They are able using any kind of data

when accessibility available to web, mobile commerce solutions helps managing services and it is not dependent place and time.

Smartphone devices are gaining capabilities in level where those can use like PCs. It is creating possibilities even increasingly innovative business models. Mobile commerce services changes also security industry value network and new companies entering into business. This causes that new companies are gaining market share and old ones looses their share. Wireless services integrated into systems are driving costs lower and IP based solutions are overtaking old analogy based systems.

The applications of NFC are piloting projects to different channels to interest customer and building new business models beside old solutions. These services have been informative services and content pinpointed to share information which is related to locate person, share commercial information or ticketing services. There is a looked best practice to offer in the future significant advance comparing other similar technology which in NFC case is Bluetooth. At the moment system integrators are investing money to development where they get earnings later on in future.

The terms of applications, operators challenge is to identify needs from customer and utilize new value through NFC information services. It means understanding current customer infrastructure and offer services what customer requiring. These services need to be reliable and functionality working properly in the beginning. The operators which are able to customize services are succeeding; this is relating security sector and NFC technology products.

4.8 NFC on the value network

There has been a lot of talk and marketing whirl about NFC and even though the development has been fast, not much has happened yet. Standardization is still going on and there are many open questions, as well as prospective standards competing for the dominant position. The players of the ICT sector, including device manufacturers who are striving to get products to the market, and some of them are in a hold position and waiting for something to happen. Meanwhile, they develop solutions for other technologies and are ready to apply them to NFC once they get some kind of a signal from the market to start acting.

Many companies can thus be considered to be rather reactive in their actions. It may be a smart strategy as there are several prospective technologies, and long-term proactivity requires considerably large resources. “Only large companies can afford to try to create markets and keep on proactively.” Therefore, especially for smaller companies it may be wise to react fast as the first sign of a business opportunity appears. However, the reaction has to be fast enough because along with innovativeness, time to market may become decisive in captivating markets.

The changes that may occur in the value network of the security sector can be seen to come as a chain reaction, one change leading to another. As NFC provides convenience of use to devices and applications, as well as makes the user interface of multiple devices simpler, it is likely to increase the number of users. The increased convenience of interconnecting devices may also change the type of the used devices and the way they are used. As the user base grows, the demand for related services is likely to increase, especially as their use is increasingly convenient with the better devices.

At the same time, content provision becomes easier since basically anyone can deliver content over NFC. NFC may also solve locally or together with the third generation network technologies the existing bottleneck that prevents good content from entering the market because it enables the delivery of larger content over the wider band.

In many situations NFC services can be created and used without any national telecom operator as the data transmission is only local. It is likely that there will appear smaller local operators that either manages their own local communication or that of a number of local actors. Traditional operators are, therefore, likely about to confront competition from new directions. It can be expected that the amount of provided content will increase and its nature change as well as the number of actors increase. All this is likely to lead into increased traffic and complexity of the networks and higher need for coordination of the activities.

5 NFC ADDED VALUE TO BUSINESS MODELS AT SECURITY ACCESS CONTROL

It was already discussed in the chapters 2 and 3 that NFC and access control, and this has made many companies to consider take into account NFC in their business models. This chapter summarizes business models at security access control and clarify beneficial possibilities.

5.1 Benefits of security and NFC

Currently it has been seen that the smart cards industry makes continued progress in the worlds of NFC technology. NFC technology is a trusted communication way to access control solutions when needs to identify person, placement, and access rights. At the same time, this identification way provides multiple other ways to cost-effectively use one technology and its applications through different service providers. This makes the technology attractive for organizations.

The added value of NFC in most service visions is based on locality. The provision of the services can be truly local as the services can be created and distributed locally. As the service provider knows where the user is, it can distribute content that is very local by nature and especially valuable when received in the particular location. An example of this is the concept of love beeper or increasingly widely interest recognition, in which a person can define characteristics of an interesting person in an Internet database or to a smart device, and get a signal when someone meeting the requirements is within the reach of NFC. As the purpose is to find a match as s/he is nearby, the information is especially valuable when received at the right moment. This feature can be used for example area guard services when making watch round or sharing security instructions newcomers.

Locally valuable are also all kinds of informative systems, current info services as well as guidance systems. As NFC enables the delivery of information to an exact location, it may become interesting to many users and service providers. For example, receiving instructions as entering an unfamiliar office building or visiting a new city may be quite helpful.

NFC applications and data can be stored on a mobile or NFC device in an unencrypted or encrypted form, depending on their sensitivity. Security is central especially in banking and payment services, whether it be a some Euros for a local travel card or larger amounts, for example when customers pay for purchases using their mobiles almost similarly as their credit cards. This sensitive information – customer data, account and credit card numbers, balance details – must be stored securely on a medium in the NFC device.

The medium offering the best security for storing data is the SIM card at mobile phone. At the initiative of Vodafone and Giesecke & Devrient (G&D), a standard specification is currently being developed for an NFC-enabled SIM card to be used as a secure storage element. It will ensure interoperability between SIM card, mobile phone operators, mobile phone manufacturers, and service providers. G&D has the security architectures needed for NFC systems. Thanks to its familiarity with the interests of all market players, from mobile phone operators through credit card organizations and financial institutions to providers of mobile services and service providers such as transport companies, G&D is now forging links wherever they are needed to grow the deployment of NFC. (Grassie 2010, 1.) Another prerequisite to the success of NFC is that the applications being controlled by the technology must be simple and flexible to use.

For example, in a mobile phone, the NFC applications and data (such as a credit card function) are managed on the secure storage element ‘over the air’. If a bank customer wants to pay with their NFC mobile phone, the bank arranges for the NFC payment application to be downloaded onto the storage element over the air. If the customer later switches bank or alters the data required to use the services, these details can be updated via the mobile phone network. The advantage to users is that they don’t need to physically go to the bank or to a store to perform the update. Updates are secure and flexible, saving money and time – for both customer and service provider. Venyon, the joint venture started by G&D and Nokia at the end of last year, provides the server platforms required to manage NFC applications conveniently and securely over a mobile network. (Grassie 2010, 2)

5.2 Access control and NFC pilot

An access control and NFC trial were conducted from October 2006 to February 2007 by VTT. The problem for which the case application was constructed originated from the key management problem of the city of Oulu. Distributing keys to facilities for temporary use, gathering them back, and monitoring and preventing misuse of the keys is a problematic issue. Keys can disappear by accident or intentionally, but the locks for facilities, to which the key had access, are expensive to change and cannot be changed every time the key is lost. However, when a key is lost there is a risk that someone who should not have access to the facility has the key. (VTT 2007, 41-44.)A block diagram is shown in Figure 2. (VTT 2007, 27)

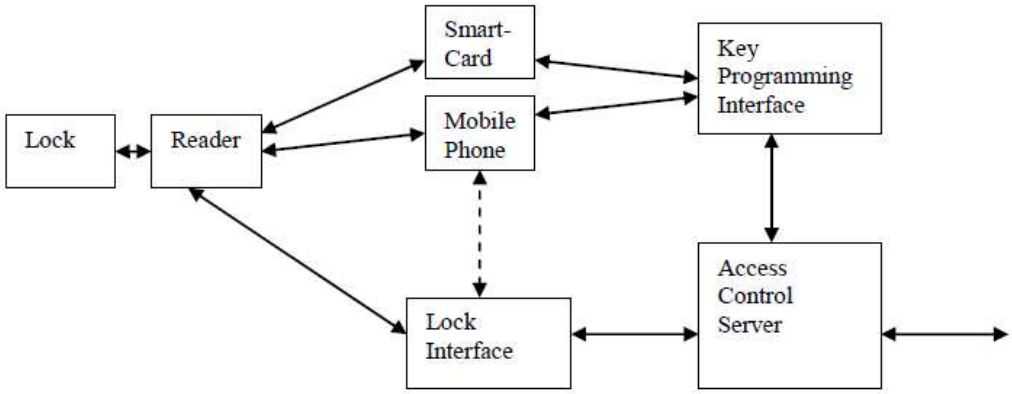

Figure 2. A general view of the parts of an electronic access control system. (VTT 2007, 27)

The access control server on the right is where the logic of the system resides. It has an outward interface for reporting and management. This might be either a local user interface or a network connection to another system. The access control server has two other interfaces towards the system: a lock interface for speaking with the readers and locks, and a key programming interface for issuing and retracting the keys. The key programming interface towards a smartcard-based system is typically a station for writing or printing the access cards. It will be a physical location such as the security personnel's office. For a mobile phone-based system, it will most likely be an over-the-air link to the mobile phone.

The physical access control tokens will be the smartcards or mobile phones of the users. The user will open a door or gain the relevant access by presenting this token to a reader. Communication with the reader will, for the purpose of this paper, be over a short range RF-interface, typically according to the 13.56MHz ISO 14443 standard.

The lock will be in connection with the access control reader, either by being integrated into the same unit, or by electric wiring. Finally, the lock and reader will be able to communicate with the back-end system. Firmware updates and blacklists of keys are two examples of communication that work this way. Another important communication that is routed this way will be the reporting of who opened the door and when. In some systems this communication route can be handled through either the SmartCards or the mobile phones, as shown by the dotted line.

In a typical case, data is communicated from the object (sensor) to the microcontroller of an NFC server using serial communications. The measurement can be started when an NFC phone acting as an NFC initiator comes nearby. Then the data is sent to the phone. Another possibility is that the NFC server constantly receives data from the sensor, and the latest result is sent when NFC server is touched by a phone. It is also possible to use the NFC server as a stand-alone data logger, which sends a larger amount of data to the phone when required. When compared to the reading of tags the fundamental difference is that the data content is not static, and the data can also be processed at the sensor end. The data source can of course also be something other than an actual sensor, and there can also be a back-end system involved. However, many applications are possible with local communications alone.

The peer-to-peer communication mode of NFC is suitable for these kinds of operations. Often it is preferred to have low current consumption on the sensor end. This is especially true when a wired power supply is not used, such as in case of battery powered devices. The best power efficiency is achieved by setting the sensor end to NFC passive target mode while the phone is set to NFC initiator mode to read the sensor.

Using this kind of arrangement, the sensor does not need to generate the carrier signal, but it can communicate back to the initiator using load modulation (modulating the carrier generated by the initiator, i.e. the phone). This is the same method that is used in

passive RFID tags. This approach minimises the current consumption at the sensor end, not only during communications but also while waiting for the start of communications. Another advantage of this approach is that the peak current is kept low at the sensor end, enabling operation, for example, from small coin-cell batteries with restricted peak current capability.

Figure 3. NFC server enables using a mobile phone as the user interface for non-UI devices. (VTT 2007, 34)

Another use scenario is related to using a mobile phone as a UI for devices that are not equipped with a UI themselves. Typically there is bidirectional data communications. For example, the value set to a thermostat could first be read by touching the thermostat with a mobile phone and value to be shown on screen. (VTT 2007, 33) Then, a new value could be typed using a mobile phone keypad, and the old value could be replaced with a new one by touching the thermostat with the phone, see Figure 3. (VTT 2007, 34). Here, peer-to-peer communication mode is the most natural choice, the phone taking the role of the initiator.

In this kind of mobile application, the user benefits from the physical browsing concept: the desired action can be triggered by a simple touch. In an ideal situation, no key presses or browsing of menus is required, or at least this is kept to a minimum for example confirmation by a key press may be necessary. This is contrary to the case where a short range radio would be used instead of NFC. This would inevitably lead to a increasingly complicated selection process at the phone. In case of short-range radios,

it is also difficult to implement ultra-low power sensors with low latencies. Of course, the requirement of touching an object is not feasible or convenient in all applications, however. (VTT 2007, 33)

The study shows following results: Participants saw a possibility to use a mobile phone in a versatile way as positive. Unreliability of the electronic lock was the one factor, which negatively affected one respondents experience about the effectiveness of the application. It was also the feature which emerged in almost every participant answers. (VTT 2007, 43.)

In addition to reliability issues, some problems emerged during the adoption of the usage monitoring application. Installation of the Service discovery application was not clear for most of the users. Users had installation instructions in a written form and they also had a telephone number for support. Despite this, many users did not succeed in installing the application. This clearly hindered the adoption of the usage monitoring application. Reliability of the system played a central role in the pilot test. Reliability of a lock with a traditional key is nearly 100%. This sets high requirements to the reliability of the electronic lock. A lock which does not open reliably may cause a lot of frustration in people. In order for users to really trust the electronic lock, its reliability should be improved. (VTT 2007, 43.)

Requirements concerning installation of the Service discovery application in the adoption phase of the usage monitoring application caused problems for many users. In the future it should be taken into account that installation of mobile applications could be too troublesome for some users. All the applications should be installed to the mobile phone before it is given to the user. The adoption phase of the application should be as easy as possible for the user.

Most users saw the idea behind the solution as useful. When the reliability and adoption challenges described above have been solved, NFC technology can be seen as a potential technology to be applied in the access control and usage monitoring of the facilities. (VTT 2007, 44)

5.3 Critical issues of NFC technology

Problems in developing standards are quite normal but they can become fatal if solving them takes too long and other technologies gain market share in applications critical to successful diffusion. In the case of NFC, other wireless technologies may become widely adopted before the problems with them standard are overcome, which can considerably threaten the diffusion and adoption of NFC. Wireless local area networks are already being implemented in many places and usage situations.

While NFC technology is still under construction, this other – already several times faster – techniques are gaining positions in the marketplace. Once consumers have invested and adopted fast and reliable connections, it is not easy to see that they would switch to possibly slower and still evolving NFC technology. Keeping this in mind it could be even speculated that NFC might be fighting a loosing battle in some application visions.

The success is also threatened if the high expectations of the market cannot be fulfilled in due time, because the expectations toward NFC may start declining. This peak of inflated expectations may even be very close, as the promises of the mobile future have already been in the open for quite a while. There is also a danger that people will expect too much of NFC as of mobile commerce in general, before the multiple technologies have been fully refined and they thus become disappointed. This concerns the interoperability of the devices as well. It is planned to be the bearing strength of the technology and if it fails it may threaten the whole success. It is important to have some proof of the capabilities of the technology and its upcoming features in the near future, because otherwise people may loose their faith in NFC.

The application visions of NFC should be carefully examined both on the technical and business side. There are many visions that can be executed easily and even cheaper or conveniently with existing technologies, and therefore the use of NFC needs to be well justified in each situation.

From marketing point of view, it is crucial to examine whether there exists a need for the envisioned services and products. True customer needs relating to the usage visions have not most likely been investigated yet, and it is likely that the investigation is not even possible before some concrete applications can be introduced.

Telecommunications and computing industries have been, in general, quite technology-push-oriented, which is bound to change in the future. It would be better to anticipate the change to market-pull orientation and focus on application visions having real potential in the marketplace at security sector.

The main concerns that came up in the discussions have to do with the building of and the complexity of the standards; its substitutes and the assurance of the quality of service after the applications are introduced. In history, dominant standards have been built within specific segments, and after one segment has adopted the technology it has expanded to other segments and slowly grown to a general standard. NFC, on the contrary, has no killer application yet and it is seen rather as a universal solution to way of identification.

5.4 Current and future solutions

Near Field Communication is opening up whole new services and business opportunities. The technology impresses by its simplicity and speed of use, the high level of security and convenience it offers for users, whose mobile phones can be automatically supplied with up-to-the-minute data. NFC's greatest potential lies in payment and security applications, although the new radio technology is also ideally suited to customer loyalty schemes. The mobile phone would be a really easy way of collecting reward points in these schemes. And in future, RFID labels attached to goods or labels can forward information to users from security point of view.

The NFC Mobile Ecosystem is an expansion of the current contactless ecosystem, mainly targeting contactless card businesses. To be attractive and successful, it must create value, and to achieve that goal, it requires the addition of new functionality on top of the current card business. On the other hand, depending on the marketplace, the NFC Mobile Ecosystem must be open enough to support the variety of existing and future models. To be successful it must support a win-win relationship among all the ecosystem players. This section considers the key factors for building a successful NFC Mobile Ecosystem from the viewpoint of the potential players, especially targeted to the new functionalities.

5.5 Economic aspects and investment to NFC technology

NFC's staggering global growth, combined with the development of a technology standard has occurred thanks to the work of the NFC Forum, a non-profit organization set up by Philips, Nokia, and Sony in 2004. Its membership reads like a Who's Who of international enterprise – starting with technology giants like IBM, Intel, Hewlett Packard and Microsoft, through financial organizations such as MasterCard, Visa and Deutsche Postbank, to mobile phone companies like Telefonica and Vodafone. They receive support from the GSM Association, which is just as committed to the spread of NFC.

NFC forum too has become actively involved in the standardization aspect and is playing a leading role in driving the development and spread of NFC technology, for example by collaborating with industry to develop solutions for the security architecture of a mobile phone, while through Venyon it is enabling applications to be downloaded securely. This background work is putting the foundations in place to make it possible to develop a successful NFC ecosystem.

Major mobile phone manufacturers have developed handsets that work with the new technology. For example, Nokia has already brought out two mobile phones which support the new technology. Meanwhile Samsung and Sagem have both introduced their own NFC-enabled handsets. According to research and consultancy firm Abi Research, 20% of all mobile phones will be NFC-compatible by 2012. Semiconductor manufacturer Inside Contactless is developing NFC architectures in collaboration with Infineon.

NXP is also investing in the new technology, while companies like UK-based wireless designer CSR is taking a great interest in NFC and sees great future potential here. A mere five years since the NFC standard first got under way, the main foundations for building NFC infrastructures have already been laid: first NFC mobile phones, soon standardized NFC-compatible SIM cards and platforms for flexible management of NFC applications. The pilot projects that have now been running worldwide for more than a year are giving out positive signals, while new business fields are waiting to be discovered by enterprises of all sectors.

5.6 Business models at NFC access control solutions

In the mobile NFC ecosystem the two major actors are the service providers and the mobile network operator. Among the service providers it is important to single out the card companies, who are representing a very concentrated power with a service that has great application potential in the NFC environment.

These two actors are representing diverse business and marketing interest which up to this point could not be bridged. The MNOs have the benefit that they control the only generally available download facility. What is more, they also have the space on their SIM cards which could also be utilized for storing third party secure applications. Controlling the download and hosting the applications as well, two services that can be charged for, would provide great benefits for the operators.

Apart from the financial results, positioning themselves in the key points of the value chain would provide control for the MNOs not only over the service provisioning but to a certain extent also over the customers using the various services. This disintermediation of the customer from the financial service providers is something that these entities cannot tolerate. The service providers – actually at this point we should not generalize too much, as we are talking about a very diverse group – would prefer a solution where they can independently arrange for the application download, and where the application would be hosted in a neutral space in the handset, in a second chip, which is either embedded in the device or is an SD card that can be used in various devices.

The evolution of a mobile phone into an NFC Mobile Phone will provide mobile network operators with opportunities to develop new business areas. NFC mobile services will increase the opportunity for mobile usage in many new situations, as explained in the use cases. To achieve this, it is not sufficient to offer the contactless card functionalities separately from those of a mobile phone. It is vital to create and offer new value by combining the functionalities of both mobile phones and contactless cards.

When an NFC Mobile Phone supports the multi-application capability, it will not only boost convenience for users by allowing them to use many applications in one device, but will also stimulate the NFC market by increasing the number of users of NFC

mobile services. Smooth introduction of the multiple-application capability is one of the key success factors. A second essential factor is to guarantee to users and service providers a trusted end-to-end system for their applications and data.

5.7 Scenario analysis to NFC access control solutions

Scenario analysis offers one way to deal with complexity and uncertainty, and it involves the development of a set of scenarios that describe what the future environment will contain. (Aaker 1988, 121; Sikiö 2001, 60) Scenarios are alternatives to the future. It recognizes different possibilities what ways environmental development might happening and it is systematical way help management to do their decisions. It helps strategic planning predict future short term or long term actions.

In practice, scenarios are various ways, and there is no one right procedure for carrying out multiple scenario analysis.

Linneman & Klein (1979, 84; Sikiö 2001, 60) used the following generally agreed classification of the basic steps:

- Isolating assumptions about the future, which are sure to occur within the planning time frame
- Identifying key impact variables
- Specifying other environmental variables that may affect the behavior of the impact variables
- Constructing at least two descriptions of possible futures – scenarios – which depict a range of behavior of the impact variables
- Developing strategies which are responsive to one or more of the scenarios

The factors affecting the enterprise and decisions taken within it can be developed in various ways – for example from business and government literature, case histories, experts and the provider's own history. An example is a division into five principal categories that can be: political, economic, social, technological and environmental factors. Zentner & Gelb consider three as the ideal number of scenarios in many cases, because with just two scenarios it is tempting to consider one a "worst case" and the other one a "best case", and with more, scenarios will be hard to keep in mind and construct. (Zentner & Gelb 1991, 213 ; Sikiö 2001, 61.)

I am presenting in this study discussions of NFC effects on the future value network of the security access control sector. There is a very little reliable information what values and which scenarios are beneficial in security industry and operators. There will be presented guidelines what directs to best practices and not only single procedure. NFC brings various opportunities for current services and when increasing value chain and networks. In these scenarios NFC is either product feature or service what is part of product offerings giving an operator competence and value add when provided to customer.

These scenarios are showing simply way of thinking and development ideas, how re-thinking can proceed. There might be cases, where all these scenarios are involve and controlled by different industry players or business segments.

Scenario: ‘Products from market leaders’

In this scenario market leader use their position as controlling value network to gain best possible earnings and customer feedback. They are negotiating directly to their customers and co-operating their network companies as leading them as subcontractors. Features like NFC are integrated their service portfolio and part of their sales activities to customer, it has minor role from all customer offerings. It is service which way operative action improves and customer positive reaction can be seen as improved operative quality.

Scenario: ‘Customized products – specialized operators’

The second scenario presents situation where NFC are utilizing possibilities but market is very small. The product complexity to integrate to current system requires specialized customization. These services might to be provided by cloud based internet services and real time. Currently there is limitations especially NFC devices, because feature is included only a few mobile phones and devices. This causes challenges to integrate to current solutions and IT environment.

System integrators to be successors in the future, these companies are able to built customized systems, admin and develop those directly with customers when selling value added security services. Several niche concepts are applicable even specialized requirements included or segmented user group to be utilize system point of view.

These service can included web services through internet or locally specified services which are not provided through internet especially some legal reasons or information security point of view.

Scenario: ‘Products to the mass market’

In this third scenario the market for NFC products and services is wide and big, normally global scaling possible. Service providers seen that product demand is increasing and they can offer it through customers, build similar kind of services to different industries. They can scale product offer and in some cases customize it if necessary for special environment or needs. Scaling is possible globally and some of the products are directly planned to global markets.

6 DISCUSSIONS

In the previous chapters this thesis studied different aspects of NFC technology, benefits from the use of the technology in access control solutions. In this chapter this data is analyzed and compared with the collected data.

In addition to the interview outline, some additional questions were prepared to this thesis. The interview guide is presented in Appendix A and time was maximum 1 hour. The interview guide part took from 45 minutes to one hour. The remaining time was reserved for questions related to this thesis and additional conversation. All the interviews were held within this time limit.

The interviews were conducted with security management personnel in order to get an accurate and reliable picture of NFC economic aspects in access control solutions. For the study, it was important that the people interviewed had knowledge that was tangential with either IS or areas where NFC had or could be used. Some of them had also been involved in NFC application pilots, and therefore knew how NFC technology was perceived by workmen, company management and other parties involved. The results of the interviews are presented in a general manner in the following chapters

6.1 The value of NFC in security access control solutions

The analysis of and conclusions on the user group's interviews, observations and authors own interpretations are discussed in the following chapters. The frame of the analysis is organized in accordance with Patton's (2002) recommendations. There were rather similar views on the value of using NFC applications. The group was, however, rather unanimous in their opinion that the right type of NFC could generate value once the basic processes worked properly and it will replace passive detection technologies in the long term if availability about NFC devices are guaranteed. NFC is increasingly open to 3rd partner solutions and this way application development easier and possibilities customize personnel business opportunities. Operational cost is rather low, that will help usability to replace old technologies at access control solutions.

In Finland, small markets and shortage of cooperation models, particularly economic one between different operators slow down the commercial deployment of NFC technology. The development of commercial services would be faster if the NFC

operating environment was as open as possible since this is increasing the creation and deployment of NFC services.

Information technology has been a major driver of change in value creation and there is no reason to believe that it would not continue to be so in the future. Therefore, the impact it has previously had on the value network was considered a proper basis for predicting the future value network. The complexity of the environment and the uncertainty of the future were dealt with the means of scenario approach. This approach was used as it allowed presenting simplified alternative models for the future value network. Scenario analysis was not executed in full-scale.

The original value chain theory of Porter (1985) provides a valuable basis for studying value creation but it is insufficient in several ways for responding to the market requirements today. Creating value often requires bringing together previously unrelated technologies and combining competencies that one company may not have. (Aldrich 1998, 281) Value network structure allows cooperation of several companies and enables serving customers flexibly and cost-competitively. (Moore 2000, 10)

Cooperation is often required across industry boundaries when developing products and services in ICT industry as the applications are often very complex by nature. (Ali-Yrkkö.2000, 22) Developing NFC applications does not make any exception in the trend as applications are developed in many different industries. NFC may even bring new sectors together as increasingly innovative applications are likely to be demanded in the future.

Value networks are increasingly flexible than value chains, but they may fall short in competition over the quality of integration of products and services. (Moore 2000, 12) However, the integrity may be enhanced if the network is guided by a large core firm that acts as a strategic center of the network. (Pfohl & Buse 2000, 395) Previous studies have shown that networks with strategic centers have proved to be fruitful in developing skills and integrated products. (Lorenzoni & Baden-Fuller 1995, 34)

6.2 Challenges for NFC usability in security access control solutions

The obstacles were considered to be related to the mobile devices, not the application themselves. At the moment situation is that availability of NFC support devices is bad. There is really small amount of NFC supported devices on the market. All the interviewees do not believe that the present obstacles will be overcome. The basic reason is that Bluetooth technology can be used in similar applications and it is even better because detection distance can be even 1000 meter which will be maximum 10cm at NFC. These two things will affect how NFC applications as business purpose to be segmented and used.

However, legislative obstacles or the lack of necessary frequencies do no hinder the development of NFC technology. This gives good ground utilize and development new applications to security sector. The common belief was that NFC functionality has much potential and use of it will increase in the security industry. The overall opinion was that NFC applications could generate benefits when used in recurring daily routines, but they would not provide strategic solutions for the core business. Many believed that once the next generations of workers, who are increasingly accustomed to computers, enter the workforce complex devices and applications can be handled.

Once IS solutions usability is common within the security industry, more attention to be paid for the NFC using through mobile devices overall functionality. At this point PDAs could come into the picture once again, unless increasingly sophisticated mobile phones have replaced them on the market. These new technologies can bring benefits to processes and a range of uses that have not been possible or even noted before. The interviewees' common belief was that the logical and practical development and use of these technologies will increase the significance of NFC solutions in the security industry. There was, however, still debate on when these technologies can be effectively used. There are limitations related to NFC and other common technologies with similar functionalities.

Using the mobile phone as a device for access control is considered to be one of the future killer applications within the mobile technology area. Access control functionality has already been implemented in mobile phones, for example by using a GSM-based approach (opening the door by making a phone call), using SMS messaging or via a wireless (Bluetooth, e.g.) connection. An example of the latter is given by

Beaufour (2003, 4) who describes the use of a secure solution using digital keys and certificates over a Bluetooth connection. (Beaufour 2003, 3) Even though the Bluetooth solution is reasonable solution compared to the GSM-based solution that requires a GSM modem in the back-end system, it is not equivalent to an RFID-based access control solution that can be considered as secure, because of the short reading range between the reader (door) and the device containing the key. This way, the user can visually verify the integrity of the reader and/or door before using the key to access it.

In the electronic lock case-example, the biggest security challenges are located in the security of the back-end system and in the key distribution process. For example the information between the reader (door) and the back-end system verifying the digital key used to open the door can be monitored in order to capture the key or the open door command. On the other hand, a key distribution process performed via SMS, Bluetooth or some other communication method relies on the security of the communications channel used.

In some cases, the increased usability in the distribution channel or the process may result in weaker security against malicious attackers or even the exposure of the key recipient identity. The latter privacy issue becomes especially crucial when the electronic lock is located in a public place such as a movie theatre or other service providing access via electronic ticketing. When a mobile device is used for accessing different doors (business, leisure, etc.), the separation of different keys (i.e. differentiation of device roles) within the device also has to be taken into account in order to prevent the exposure of the other keys to a single access control system or outsider.

6.3 Analysis and results from interview data

To a large degree, this is due to the fact that the values a NFC application have not been measured, and there are no appropriate methods or tools with which to do this yet. (Pöyhönen 2010) Furthermore, since NFC applications are only supporting the core business, it has not been considered necessary to try to measure the benefits they create. The intangible benefits have been noted, but there is insufficient data to measure the possible tangible benefits.

The technology suppliers have the knowledge of what is possible within NFC technology, but they are still often unsure about what the security industry exactly desires. (Junnonaho, 2010) Two questions were often asked in the interviews: What are the benefits for this company? Why would we use this system if we cannot economic benefit from it? Security industry companies need to evolve from this type of questioning and see the larger picture so that NFC applications can be part of the security industry. Companies should not disregard a new system just because they are not the initial obvious benefactors of it. One must remember that benefits can also be received later in the process, and be of a qualitative nature. Even though the common belief was that mobile solutions would be used in the future, the benefits were perceived to come from areas other than access control solution process. (Junnonaho 2010)

It is evident that the introduction of NFC functionality together with mobile phones into the security industry will bring new players into the field, and some of the old players will need to adapt to the new system. Multiple versatile functions, such as NFC, RFID, camera and telecommunications, are combined into a high degree of utilization in a mobile phone, at a reasonable price. Therefore, the use of mobile phone together with NFC technology in business will increase and expand in the future. It is important that the security industry notices the benefits that NFC technology can bring and that it sees the use of NFC together with mobile technology as necessary. This can be achieved once there are demonstrable mobile phone technology success stories with tangible economic benefits for the security industry.

As new technologies require innovative business models they also force companies to look for new opportunities as their old businesses may be under a threat of becoming commodities. New technologies also enable the provision of new value propositions, which may mean re-aggregation of current proposals and a change in the set of actors participating in value creation. (Tapscott 1999, 14.) NFC may have this kind of effects on the security value network as it offers a new operations channel.

To date, the NFC solutions for the security industry have primarily been used on replacing passive detection technologies with active technology by NFC. The possible tangible benefits can be achieved when there will be done integration and applications especially with wireless devices. This requires device availability at markets and especially mobile phones which includes NFC possibility.

When thinking about positive drivers, the following benefits from the security industry can be achieved:

- Improved time efficiency during safety monitoring rounds; accurate time and place information supported by photographic evidence if necessary; less paperwork; speedy acknowledgement and resolution of problems; increased transparency and increasingly accurate monitoring.
- Improved time efficiency because of site preparedness; accurate, real time information throughout the process; less paperwork; speedy rectifications of false or faulty material; easy, accurate and speedily done status reports and identification of arriving material; better transparency in the supply chain and enhanced B2B relationship.

In addition to the above, it was hoped that future NFC solutions would also have some of the following benefits: easier monitoring of personnel, licenses, permits, equipment and materials. One of future possibilities is positioning and sharing guiding information.

Many ICT companies that are offering new technology features in their products and services could be thought to have also a good knowledge about the benefit side. And when technology is developing so fast like in wireless technologies, these companies have, or already had, a window of opportunity to gain competitive advantage by being among the first also as a user. However, there is no strong proof about that based on research. More or less it seems that these companies in many cases would need some outsider to say how they could utilize new technologies in their own operations.

One good example about the dilemma of an information technology investment could be how to evaluate the benefits of wireless instant messaging solution, which is already available in the market. This application can easily be rejected as an investment based on increasing network traffic. On the benefit side there could be faster communication inside community, increased virtual awareness about other members and thus the deeper integration of whole working group.

The way of work of the working group could change radically. It is clear that these kinds of benefits are impossible to put in figures such as the costs of the increased traffic inside the company network. However, it is also easy to hide behind the statement that the role of information technology is to act as an enabler. There are also many cases where it should be possible to calculate costs and to estimate benefits. (Korppas 2002, 66)

7 CONCLUSIONS

This final chapter summarizes the research frame and presents the major findings of the study. The purpose of this study was to research the future effects of one potentially discontinuous innovation, namely NFC in access control solutions point of view, and to find out how it may change the value network of the operators. The main purpose was to answer the question: “How NFC may be able to create possibilities?” The study was meant to clarify the value added by NFC to security access control solutions and operators of the value network, the effects of NFC on the structure of the value network as well as the opportunities and threats it may pose to the operators of the security sector. Some suggestions for further research are presented at the end of the study.

Answers to the research questions were searched with qualitative methods and the study had features of futures research as explorative methods were employed. The problem was approached by researching the theory of technological change and the nature of technological innovations as well as by researching how the value network has previously transformed. Therefore, the future value network of the ICT sector is seen to be a strategic network, in which a leader controls the development and may considerably affect its direction. The empirical part of this study also favored strategic network model as it was seen necessary to have some actor to control the activities of the network and to ensure the benefit of customers.

However, it is also unwise to underestimate the importance of tacit knowledge, when estimating the benefits of a new application. However, a start situation can be modeled in many cases, environment where an application is in use is changing all the time, especially in an area where technology is developing still quite rapidly and started to spread. Also a well-known statement is that almost all benefits concerning the investments in information technology tend to flow for the end users like employees and for customers.

According to the findings the company itself as an investor does not receive any lasting competitive edge. However, these investments are necessary to keep it on competition. If a company has a power in its value chain, it can try to push its suppliers to acquire the latest technology and thus to attain indirect benefits for itself. A good question is if a

company is not that kind of a lead company is it then wise at all to be among the first as a user of the latest information technology like NFC technology.

In the discussions with the industry representatives it became obvious that what ever the model of the future value network will be, it is likely that there is a need for some kind of an operator or coordinator. Due to the open nature of NFC, the quality of service may be lost if no party is ensuring it. It may be even important for the benefit of users to have some customer-ship operator with whom customers establish relationships. A model where all content providers push their own content to all the user terminals within the band range would most likely be too chaotic as users would need to establish relationships with all of them. Along with the services managed by larger coordinators it is likely that there will also be room for some niche services that may be provided by small, independent players.

For further research interesting areas could be found in researching the effects NFC may have on different industry sectors, as it might shake up traditional way of doing business. The differences in the impact of NFC on the ICT value network between different parts of international markets could also be interesting to study, because the markets are lead by different types of actors and the behavior of customers differs from one culture to another. Since the development in this area is so fast and unpredictable, a new study on this topic within a couple of years as there is already some experience from NFC applications might give new insights into the future value network.

NFC usability of security solutions is ongoing and spreading. Technology is ready for wider usage, but the diffusion has slowed its pace during the last year because of small amount of availability for wireless NFC devices. This means that from the point of user it is a revolution and from the point of technology it is an evolution, which goes on but it takes increasingly time than it was thought initially. NFC mobile services are an important emerging area for NFC technology, with great potential for growth. This combination is accelerating the growth of this business area includes recognizing and describing what is needed to realize successful NFC mobile access control solutions to future. This is essential for successful NFC mobile ecosystems.

Throughout this research it has been evident that NFC tied with mobile technology can be used in security industry benefit ways. The applications should be customized and developed by security operators. These companies can see best economic possibilities

where old technology can be replaced by NFC and economic value-adding is achieved when at the same time operational processes were utilized. Through these thesis final outcomes is to give ideas to future planning the NFC technology capabilities in security industry and I hope, this helps readers to create developing their businesses around NFC.

REFERENCES

Printed

Aaker, D. 1988. Strategic Market Management. John Wiley & Sons. Second edition. New York.

Ailisto, H. & Matinmikko, T. & Häikiö, J. & Ylisaukko-oja, A. & Strömmer, E. & Hillukkala, M. & Wallin, A. & Siira, E. & Pöyry, A. & Törmänen, V. & Huomo, T. & Tuikka, T. & Leskinen, S. & Salonen, J. 2010. Physical browsing with NFC technology. VTT Research Notes. Edita Prima. Vantaa.

Aldrich, D. 1998. The new value chain, Information week. Issue 700. 278- 281.

Ali-Yrkkö, J. & Paija, L. & Reilly, C. & Ylä-Anttila, P. 2000. NOKIA – A Big Company in a Small Country. ETLA – The Research Institute of the Finnish Economy. Vantaa.

Beaufour Larsen, A. 2003. Secure Access Control Using Mobile Bluetooth Devices. M.Sc. Thesis. University of Copenhagen.

Cartwright, S.. & Oliver, R. 2000. Untangling the value web. The Journal of Business Strategy. Volume 21. Issue 1. 22-27.

Christensen, Clayton M. 1998. Why great companies lose their way. Across the Board. Volume 35. Issue 9. 16-22.

Christensen, C. 2000. The Innovator´s Dilemma. HarperBusiness. Harvard Business School Press. Boston.

Copacino, W. 1999. The emergence of “value networks”. Logistics Management and Distribution Report. Volume 38. Issue 8. 38.

Cross, G. 2000. How e-business is transforming supply chain management, The Journal of Business Strategy, Vol. 21, Issue 2. 36-39.

Grassie, K. 2010. Easy handling and security make NFC a success.G&D.

De Rose, L. 1994. The value network: integrating the five critical processes that create customer satisfaction. AMACOM. New York.

Hirsjärvi, S. & Hurme H. 2001. Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki. Yliopistopaino.

Kahn, H. & Wiener, A. 1967. The Year 2000: a Framework for Speculation on the Next Thirty-three Years. Macmillan. London.

Korppas, J. 2002. Wireless E-Business Applications in ICT Industry. Master’s Thesis. Lappeenranta University of Technology.

Kotler, P. 1994. Marketing Management – Analysis, Planning,

Implementation, and Control. Prentice Hall International. Eight Edition. USA.

Lorenzoni, G. & Baden-Fuller C. 1995. Creating a Strategic Center to Manage a Web of Partners. California Management Review. Volume 37. No. 3.

Moore, G. 2000. Living on the fault line. HarperBusiness. New York.

Ovum. 2000. Mobile E-commerce: Market Strategies. Parts D-E. Study of Ovum.

Patton, M. 2002. Qualitative research and evaluation methods. 3rd edition. Thousand Oaks. USA. Sage Publications.

Pfohl, H-C. & Buse, H. 2000. Inter-organizational logistics systems in flexible production networks. International Journal of Physical Distribution & Logistics Management. Volume 30, No. 5. 388-408.

Porter, M. 1985. Competitive advantage – Creating and sustaining superior performance. The Free Press. New York.

Ramirez, R. 1999. Value co-production: intellectual origins and implications for practice and research. Strategic Management Journal. Volume 20. Issue1. 49-65.

Sikiö, T. 2001. The role of Bluetooth technology in transforming the value network of ICT industry. Lappeenranta University of Technology.

Tapscott, D. 1999. Creating value in the network economy. Harvard Business Review.

Vilmos A.. 2004. The need for business and operating standards in the mobile NFC ecosystem. Budapest. Hungary

Zentner, R. & Gelb, B. 1991. Scenarios: A planning tool for health care organizations. Hospital & Health Services Administration. Volume 36, Issue 2. 211-222.

Özdenizci, B. & Aydin, M. & Coskun, V. & Ok, K. 2010. NFC Research Framework: A literature Review And Future Research Directions. Information Technologies Department. ISIK University. Istanbul. Turkey.

Non-printed

Interview Junnonaho, Seppo. 2010. Product Manager – International. Schneider Electric Buildings Finland 5.5.2010

Interview Pöyhönen, Arto 2010. Product Manager – Domestic, Schneider Electric Buildings Finland 5.5.2010

Huomo, T. 2008. Near Field Communication in the public transport industry. Ministry of Transport and Communications. Near Field Communications. NFC-working group final report 31.12.2010. http://www.lvm.fi/c/document_library/get_file?folderId=1551284&name=DLFE-11779.pdf&title=Julkaisuja 4-2011

Naumanen, M & Rouhiainen V. 2006. Security-tutkimuksen roadmap. Research notes VTT 2327.

www.vtt.fi/inf/pdf/tiedotteet/2006/T2327.pdf

NFC Forum. 2011. About Us.

http://www.nfc-forum.org/aboutus/

APPENDICES

Appendix 1: Interview framework 1, Arto Pöyhönen

1. What kind of NFC applications could be of use in the future for access control solutions?
    a. NFC information based security applications to be future are possible, because operators are changing detection technology from passive to active like NFC
    b. Applications are detection manufacturer based solutions where NFC most likely will be one of their future options
    c. Placement applications - it is hard to say at the moment what detection technologies coming to be popular in the future where competitor technology Bluetooth is one of the possibilities
2. What is the present of NFC in your company or business segment?
    a. There is not exact for NFC projects in applications for access control security segment at the moment, technology is different at this business segment
3. What benefits/values/profits does a NFC application might generate?
    a. This depends from NFC devices how those can be used in the future, if possible to use mobile phone – this generates new opportunities
    b. There is no operational costs for the technology, so this is based on application related costs and pricing from operators
4. What you can see, are the problems with NFC applications?
    a. Limitations of the readability which in NFC is max 20 centimeters for example in Bluetooth that is several meters
    b. This technology can read only one data per time, which creates limitations for usability
5. What, at present, are the obstacles in using and increasing the usage of NFC applications?
    a. Technology limitations like readability and how popular NFC devices are coming in the future
6. What would increase mobile usability as NFC security solutions?
    a. This would utilize NFC related security solutions because there would be availability of devices in the field which decreases operational costs

7. How do you see the future of NFC functionality in your company products?

    a. There might be applications relating guardian related services where guard is doing guardian round – there is tags around different places and information that where guard has been visited at real-time

8. How do you see the future of NFC functionality for security access control solutions business segments?

    a. Current web features and usability are in that level that there is not clear direction to develop NFC functionality

9. What kind of security companies are starting to use NFC technology and especially using it through wireless devices in their service portfolio?

    a. There is not because security solutions based on NFC, because all applications are based on Bluetooth at moment because almost all mobile phones include Bluetooth capability. NFC capability from mobile phones are missing currently, it can not be only smartphone feature if NFC might be future technology

Appendix 2: Interview framework 1, Seppo Junnonaho

1. What kind of NFC applications could be of use in the future for access control solutions?

    a. Security applications what are based small amount of data information and in these cases NFC is possible to use

2. What is the present of NFC in your company or business segment?

    a. There are no actions ongoing with development

3. What benefits/values/profits does a NFC application might generate?

    a. Do not see operational values and benefits, where NFC generates benefits

4. What you can see, are the problems with NFC applications?

    a. Availability of the NFC devices, it has to be in mobile phone that services are possible to use

    b. Technology itself does not utilize more possibilities comparing current detection technologies

5. What, at present, are the obstacles in using and increasing the usage of NFC applications?

    a. Amount of technology devices and when needs to transfer big amount of data, for example pictures – NFC is not best technology for this. Problems are also technology as usability related

6. What would increase mobile usability as NFC security solutions?

    a. Not see development possibilities because technology related problems for data transfer

7. How do you see the future of NFC functionality in your company products?

    a. Not see many applications for NFC functionality because there is always security aspect and it has to be taken into account, functionality is more relating usability as guidance point of view at the premises when temporary access

8. How do you see the future of NFC functionality for security access control solutions business segments?

    a. There needs to be NFC in general availability that can use features with cost effective way to users

9. What kind of security companies are starting to use NFC technology and especially using it through wireless devices in their service portfolio?

a. There would not be much security companies which are developing NFC technology applications to markets because limitations can be see from device availability point of view and patents which are released and ongoing not supporting spreading more wider use from global point of view