ESPOO 2007 VTT RESEARCH NOTES 2400

Heikki Ailisto, Tapio Matinmikko, Juha Häikiö,
Arto Ylisaukko-oja, Esko Strömmer,
Mika Hillukkala, Arto Wallin, Erkki Siira,
Aki Pöyry, Vili Törmänen, Tua Huomo,
Tuomo Tuikka, Sonja Leskinen & Jarno Salonen

Physical browsing with NFC technology

VTT TIEDOTTEITA – RESEARCH NOTES 2400

Physical browsing with NFC technology

Heikki Ailisto, Tapio Matinmikko, Juha Häikiö, Arto Ylisaukko-oja,
Esko Strömmer, Mika Hillukkala, Arto Wallin, Erkki Siira,
Aki Pöyry, Vili Törmänen, Tua Huomo, Tuomo Tuikka,
Sonja Leskinen & Jarno Salonen

ISBN 978-951-38-6946-5 (soft back ed.)
ISSN 1235-0605 (soft back ed.)

ISBN 978-951-38-6947-2 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)

JULKAISIJA – UTGIVARE – PUBLISHER

VTT, Vuorimiehentie 3, PL 1000, 02044 VTT
puh. vaihde 020 722 111, faksi 020 722 4374

VTT, Bergsmansvägen 3, PB 1000, 02044 VTT
tel. växel 020 722 111, fax 020 722 4374

VTT Technical Research Centre of Finland, Vuorimiehentie 3, P.O. Box 1000, FI-02044 VTT, Finland
phone internat. +358 20 722 111, fax +358 20 722 4374

VTT, Kaitoväylä 1, PL 1100, 90571 OULU
puh. vaihde 020 722 111, faksi 020 722 2320

VTT, Kaitoväylä 1, PB 1100, 90571 ULEÅBORG
tel. växel 020 722 111, fax 020 722 2320

VTT Technical Research Centre of Finland, Kaitoväylä 1, P.O. Box 1100, FI-90571 OULU, Finland
phone internat. +358 20 722 111, fax +358 20 722 2320

Technical editing Maini Manninen

Edita Prima Oy, Helsinki 2007

Ailisto, Heikki, Matinmikko, Tapio, Häikiö, Juha, Ylisaukko-oja, Arto, Strömmer, Esko, Hillukkala, Mika, Wallin, Arto, Siira, Erkki, Pöyry, Aki, Törmänen, Vili, Huomo, Tua, Tuikka, Tuomo, Leskinen, Sonja & Salonen, Jarno. Physical browsing with NFC technology. Espoo 2007. VTT Tiedotteita – Research Notes 2400. 70 p.

Keywords RFID, Radio Frequency Identification, Physical browsing, Human Computer Interaction, HCI, CHI, contactless, payment and ticketing, NFC, Near Field Communication, peer to peer, ISO 14443

Abstract

Physical browsing is a new intuitive human computer interfacing paradigm for mobile users. Services, such as information retrieval, peer to peer communication, payment or ticketing, and professional applications can be initiated by simply touching an object with a user's personal device. This paradigm can be implemented with RFID technology. A number of major companies in the fields of mobile communications, electronics and financing have joined forces in an effort to commercialise this human computer interaction paradigm with the brand name Near Field Communication (NFC). NFC is based on existing technology using 13.56 MHz RFIDs and international standards. NFC forum is creating standards and recommendations for the upper level protocols and application models. VTT is leading a European-wide project which develops and pilots NFC technology. This report describes the findings and results of the first project year. The report outlines the concept of Physical browsing, NFC technology, its main applications, and describes a pilot case with a meal service for elderly citizens. An NFC Bluetooth gateway prototype has been designed and the first experiments are briefly described. Security and privacy issues relevant to NFC are described. The main business models, namely those driven by financial institutions, mobile operators or other parties, are discussed. A look at major trials and roll-outs of contactless payment is given. Some solutions to the dilemma of scarce NFC services and low penetration of NFC phones are suggested.

Preface

This report has been written as a result of the first project year in the Smarttouch project. The project is a European ITEA2 project with about 30 members in Finland, Spain, France, Belgium, Germany and Israel. The Finnish consortium consists of VTT, the City of Oulu and six companies. The report describes the state of the art in a new user interface paradigm, Physical Browsing, and its commercial implementation, Near Field Communication technology. It also describes the results of VTT in this project during the first project year.

Oulu, May 2007

Heikki Ailisto and the project team

Contents

List of symbols and acronyms

B2B	Business-to-Business
B2C	Business-to-Consumer
B2E	Business-to-Employee
EEPROM	Electrically Erasable Programmable Read-Only Memory
EIA	Electronic Industries Association
EMV	Set of specifications for smart cards by EMVCo
GPIO	General Purpose Input/Output
HCI	Human-to-Computer Interface
ISO 14443	International standard
IO	Input/Output
IR	Infrared
IrDA	Infrared Data Association
JTAG	Joint Test Action Group
LED	Light Emitting Diode
Li-Ion	Lithium-Ion
MNO	Mobile network operator
NFC	Near Field Communication
PDA	Personal Digital Assistant
POS	Point of Sale
QR	Quick Response code

RAM	Random Access Memory
RFCOMM	Radio Frequency Communication
RFID	Radio Frequency Identification
RS-232	Serial communications standard defined by EIA
SPI	Serial Peripheral Interface
SWP	Single Wire Protocol
UART	Universal Asynchronous Receiver Transmitter
UI	User Interface
USB	Universal Serial Bus
WLAN	Wireless Local Area Network

1. Introduction

The vision of ubiquitous computing and communication, first outlined by Vannevar Bush in 1945 (Bush 1945) and then refined and coined by Mark Weiser (Weiser 1991), is becoming technically feasible. One of the building blocks for this ubicom vision is easy and natural interaction between humans and technology. One way to provide this natural interaction is the concept of physical browsing, i.e. to implement interaction methods by which the user can achieve her or his goals, such as acquiring information, transferring data, performing financial transactions or initiating actions, just by pointing or touching. This document reports results of research and experimentation in this field.

Several methods for implementing the concept of physical browsing can be used (Ailisto 2003). From the user perspective, these can be divided into "point me", "touch me" and "scan me" paradigms. The point me paradigm is most naturally implemented with optical means, since the direction of optical pointing, either an active "ray" or a passive camera, can be directed easier and more intuitively than radio frequency (RF) or magnetic techniques, which lend themselves more naturally to touch me and scan me paradigms. VTT has implemented all of these methods in earlier projects with infrared (IrDA), laser pointing, camera and RFID technologies (Ailisto 2006). One of the camera-based methods has led to commercial activity (Bäckström 2006).

The mobile phone as the pervasive personal digital device for implementing physical browsing was recognised by VTT (Ailisto 2003, Keränen 2005, Ailisto 2006). VTT also built a software framework for mobile phones to be used for hosting physical browsing applications (Keränen 2005). Naturally, the same line of thought was pursued by some major handset manufacturers, especially Nokia. Japanese operators also saw the possibilities of the physical browsing concept early on and implemented a visual matrix code and camera phone-based Quick Response (QR) code. RFID-based implementations are also used in Japan for contactless payments with mobile phones.

A number of major companies, including Nokia, Philips and Sony, formed an alliance in 2004 to advance the use of RFID technology in consumer applications. The alliance, the Near Field Communication forum (NFC), was later joined by others such as Visa, Mastercard, Samsung, Microsoft and Motorola. The applications targeted are contactless payment, ticketing, easy information access, and peer-to-peer communication. The NFC concept is based on integrating existing RFID technology, especially ISO 14443-based Mifare (Philips) and Felica (Sony), to portable consumer devices, such as mobile phones. Due to the strong support it receives from companies, the NFC concept was forecasted[1] to achieve 60% penetration in mobile phones, excluding the ultra-low-cost models, in 2010, i.e. 500 million NFC compatible mobile phones sold that year. Since

[1] ABI Research reports 2005 and 2006.

this prediction in May 2006 the forecasts have become more cautious, but forecasting still predicts 450 million units sold in 2011.

The work reported in this document is done within an ITEA 2 / EUREKA project, Smarttouch. The project aims at developing, experimenting and analysing the technology and applications of a user interface paradigm where the services are activated by the touch of a mobile device. The project relies on NFC/RFID technology and the *touch me* paradigm. The project is a large multinational effort with participants from Finland (VTT, Buscom, Idesco, Nokia, Nordea, City of Oulu, TeliaSonera and TopTunniste), France, Belgium, Spain, the Netherlands, Israel, Germany, and the United Kingdom. The work done within this project at VTT is based on VTT's earlier self financed project Physical browsing for ambient intelligence (PB-AMI) and other projects.

This report is organised as follows. The concept of physical browsing and its implementation is described in Section 2. Technical results are described in Section 3 while user experiences in early pilot cases are discussed in Section 4. Security and privacy issues as well as the business viewpoint are described in Sections 5 and 6, respectively. Discussion is in Section 7 while Section 8 holds the conclusion.

2. Physical browsing with RFID technology

The concept of physical browsing is first discussed at a general level and a short description of the state of the art in research is given with some links to commercial applications. The NFC technology is described in sub-section 2.2 and specific requirements and definitions for NFC implementations in the cases of Payment and Ticketing, Smartposter and peer-to-peer communications are given in the following Sub-Sections 2.3 to 2.5.

2.1 Physical browsing concept

The concept of using intuitive means of touching or pointing as a way of interfacing between a human and digital resources has been present in research at least since the 1990s (Ullmer 1998, Want 1998). Using RFID-based badges for granting physical access is one of the earliest applications, it being around for more than two decades. There are some major differences between this early application and the concept of physical browsing as discussed here: the RFID access badge is a dedicated device for one purpose only; it does not contain independent means for user interface, communication or memory, except in the dedicated and fixed sense. *In the physical browsing concept as defined here the personal device or ensemble*[2] *of personal devices used for interacting with the environment through physical browsing has capabilities for user interfacing, such as display, sound and keypad; read and write memory; processing power and communication capabilities other than those needed for physical browsing.* An example of such a personal device is a mobile phone or a Personal Digital Assistant (PDA) with the ability to read matrix codes with a built-in camera or RFID tags with an incorporated RFID reader.

2.1.1 Related work

The vision of ambient intelligence involve the idea of accessing services and devices embedded in our everyday environment in a natural way (Aarts 2003). The idea of relying on resources embedded ubiquitously in the environment, for example using local displays, pads and boards, and input devices (such as whiteboards) has been suggested and demonstrated (Streitz 2001). In this vision, the technology is embedded in the environment, not so much carried by the user. However, the proliferation of portable devices with increasing capabilities has evoked the question of their potential, especially when combined with the concept of a "tagged environment" (Rekimoto 2000).

[2] This ensemble of personal devices might include, for example, a gateway enabled to read RFID tags and communicate with a mobile phone via a local communication method, such as Bluetooth.

Related work in the field of pervasive or ubiquitous computing has been reported for example in studies by Ullmer and Kindberg (Ullmer 1998, Kindberg 2000). Proposals on graspable UIs, mediaBlocks and Phicons involve an idea of physical icons for containment, transport and manipulation of information in an office environment (Ullmer 1998). The HP Cooltown project presented the idea of infrastructure to support "web presence" in the real world (Kindberg 2000). The main idea is connecting physical objects with corresponding web sites. Infrared (IR) beacons, electronic tags or barcodes are suggested for creating the connection. Ljungstrand and Holmqvist (Ljungstrand 1999) suggest using barcoded WebStickers attached to physical objects as bookmarks to the web. The domain discussed is desktop computing. Rekimoto and Ayatsuka have proposed augmenting the environment with two-dimensional matrix code, the CyberCode (Rekimoto 2000). Since more and more portable devices are equipped with digital cameras, they see potential for applications utilising camera-readable visual codes. These include physically embedded links to digital information, navigational aids and physical drag-and-drop of information content. SpotCode is a visual code which enables a camera phone to be used as an innovative user interface (Toye 2004). The Quick Response code is a commercial implementation of similar technology with widespread use in Japan.

The question of easily opening inter-device communication in an environment with a large number of networked devices is addressed in a paper by Rekimoto and co-workers (Rekimoto 2003). They suggest using either RFID tags or infrared technology for opening the connection between two devices.

Siegemund and Flörkemeier studied using active Bluetooth-based tags and passive RFID tags in the context of pervasive computing (Siegemund 2003). They have analysed interaction in pervasive computing and divided it into interaction initiated by users and interaction initiated by smart objects. Closely related to the initiation is association between a user and a smart object – close to our *selection* of a physical object. Siegemund and Flörkemeier classify association to explicit, implicit and predefined associations. They note that these association methods may not be adequate in their pure form in a pervasive computing setting with a massive amount of smart objects, but that a hybrid form is needed. Therefore they introduce invisible pre-selection, in which only probable candidates for interaction are presented to the user for explicit selection. We argue that in many cases physical selection can be used as "visible pre-selection", i.e. the user himself can process from the environment the object he wants to interact with, and associate himself with it by pointing at it or touching it.

2.2 NFC technology

In March 2004, a new interconnection technology, Near Field Communication (NFC), 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. In co-operation with Ecma, the NFC Forum will promote the implementation and standardisation of NFC technology to ensure interoperability between devices and services. As of the end of 2006, about 100 members have joined the NFC Forum.

Near field communication (NFC) is a very short-range (max. 20 cm), wireless point-to-point interconnection technology, evolved from a combination of earlier RFID contactless identification and interconnection technologies (ISO14443A/MIFARE/FeliCa). It enables users of handheld electronic devices to access content and services in an intuitive way by simply "touching" smart objects (e.g. sensors, RFID tags, other handheld devices), in other words, connecting devices just by holding them next to each other. The communication is based on inductive coupling. The 13.56 MHz carrier frequency is used and the available data rates are 106, 212 and 424 kbps. The related standards are shown in Figure. 1.

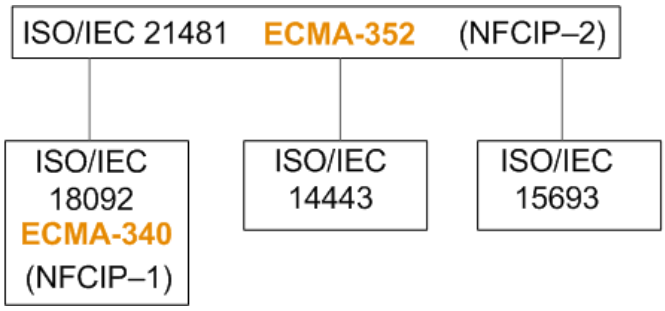

Figure 1. NFC-related standards. The upper layer defines the mechanism of selecting the communication mode on the lower layer.

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.

In addition to the reader/writer and card emulation modes, there is an NFC-specific NFCIP-1 mode ("peer-to-peer mode"), defined in the ECMA-340 standard. This mode

is intended for peer-to-peer data communication between devices. 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. 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.

NFCIP-2 (specified in ECMA-352) defines how to automatically select the correct operation mode when starting communications.

In peer-to-peer mode, the participant that starts the communication is called the initiator and the other participant the target. The peer-to-peer mode is divided into two variants: active mode and passive mode. In active mode, both participants generate their own carrier while transmitting data. In passive mode, only the initiator generates a carrier during communications, and the target device uses load modulation when communicating back to the initiator, in a way similar to passive RFID tag behaviour (ECMA 2004). This makes it possible to save power in the target device, which is a useful feature if the target device has a very restricted energy source, such as a small battery. Fundamentally, it is possible to make a target device – such as a battery assisted (semipassive) sensor readable over NFC – last for several years, even if operated from a small lithium coin-cell battery. Batteryless (passive) sensors that are powered by the RF field of an active NFC device are also feasible.

In peer-to-peer mode, NFC communication offers the following advantages over Bluetooth:

- NFC enables easy-to-use touch-based communication and interaction between two devices. For example, the communication can be executed or initiated by touching a fitted or portable NFC-enabled device by a hand-held NFC-enabled device.
- Communication set-up latency with NFC is typically some hundreds of milliseconds, whereas with Bluetooth it is typically several seconds.
- NFC enables longer lifetime of the battery, since the power consumption of an NFC node in passive mode can be negligible and the passive NFC node can be activated by an active NFC device (e.g. a mobile phone).
- Pure NFC communication enables lower pricing, since NFC is technically less complex than Bluetooth.
- Due to its shorter range and near field coupling, NFC is more immune to eavesdropping as well as intentional or unintentional interferences.

The main limitation of NFC compared to Bluetooth is the very short communication range, which, depending on the application, can include the following disadvantages:

- NFC is not suitable for portable devices that require online connectivity to another portable device or to a fixed access point.
- A lower bit rate together with the short communication range can make the touch-based transfer of longer data blocks unpleasant.
- The placement of the antenna is more critical. The place of the antenna has to be indicated to the user.

These disadvantages can be partly overcome by combining NFC with Bluetooth or WLAN, which on the other hand will mean that some of the advantages, such as the lower price, of pure NFC implementation are lost.

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. According to the downgraded forecast of the NFC-enabled mobile handsets by ABI Research in September 2006, the number of shipped NFC-enabled handsets in 2011 will be 450 million units, or 30 per cent of all handsets.

2.3 Payment & ticketing

Mobile payment as a concept is defined as the use of a mobile device (e.g. a mobile phone) to perform a payment transaction in which money or funds are transferred from one party (payer) to another party (receiver) via an intermediary, such as a financial institution, or directly without an intermediary. (Mallat 2005)

Near Field Communication (NFC) brings a new twist to mobile payment, as it can embed the functions that users have become used to with different contactless cards like credit cards, public transportation tickets and the like. The combination of mobile devices and NFC opens up new possibilities for mobile payment, which as a whole has encountered different problems and its volume has been small.

As a new technology that needs an infrastructure to work, the process of adaptation has been slow when compared to other technologies integrated to mobile devices, for example the camera. There has been non-standard payment and ticketing schemes in

public use in Asia, but in North America and Europe the services have more or less only been used in different piloting schemes.

2.3.1 Technology

Secure payment and ticketing functions need a different kind of architecture than straight NFC-function with reader and tag. Some kind of secure chip must be included into the architecture for a secure place for persistent data. There are two different solutions for this secure chip implementation. In the current Nokia solution there is a separate chip for this. It is a semi-open, device-specific chip that is controlled by the device manufacturer. Another solution is to use a SIM-card as a secure chip. It seems convenient that a SIM-card is used, because it is already in use. The use of SIM-cards would make operators a major part of the NFC-scheme. The nature of NFC excludes the operators from gaining profit from the use itself (compared to fees for network traffic), but as the operators control the SIM-cards they can control the business done with it. To date, the interface between NFC and SIM-cards has not been standardised, but some non-standard implementations have been done. The non-standardised interface is shown in Figure 2 Single Wire Protocol (SWP) has been suggested as a standard interface between NFC and SIM.

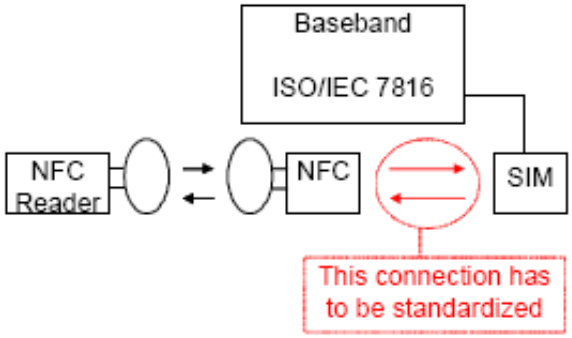

Figure 2. Interface standardisation for SIM-key exchange. (Noll 2005). Note that Single Wire Protocol has been suggested as a standard interface between NFC and SIM.

Nokia has implemented four basic communication modes for its payment and ticketing architecture (Figure 3). Only one mode can be selected at any time. It is simple mode architecture and might be the architecture for the future implementations also. The architecture consists of three different parts: MIDlet, secure chip and a part that includes external reader, card or tag. MIDlet and secure chip is located in an NFC-enabled device such as a mobile phone.

1. *Secure chip internal*: In this mode all data that is sent by the MIDlet is routed to the secure chip and the secure chip is not visible to external devices. This mode

is maintained only as long the MIDlet is connected to the chip. After disconnecting the mode is switched to what it was before *secure chip internal* – mode. In this mode, the chip responses as a target with ISO 14443-3 and Mifare Classic 1k capabilities were in the RF field.

2. *Secure chip only*: The secure chip communicates directly and independently to an external device via NFC. External readers see the chip as an ISO 14443-4 and a Mifare Classic 1k tag. The NFC and RFID features, like reading of or writing into tags, and sending to or receiving data from another NFC devices, are not enabled in the secure chip only -mode.

3. *Secure chip off*: Secure chip functionality is disabled and direct connection between MIDlet and a NFC device or an RFID tag is possible. This is a normal NFC-functionality without any payment and ticketing abilities.

4. *Secure chip on*: A combination of the modes *secure chip off* and *secure chip only*. That is, the MIDlet can communicate with external targets and external readers can communicate with secure chip and the MIDlet by using NFC P2P.

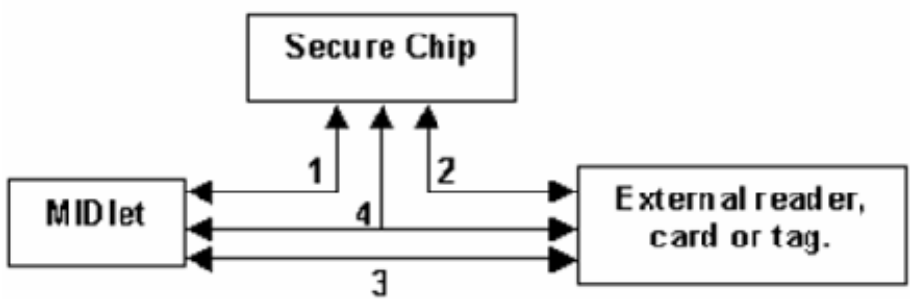

Figure 3. Secure chip communication modes and the relationship with software and peripherals. (Nokia 2005)

The mode change can be put behind a PIN-query, because enabling and disabling the payment and ticketing functionality is a powerful security feature.

2.3.2 Smartcard

Contactless payment systems are catching up to the contactless ticketing systems in popularity. The reason for this surge of contactless payment is the standardised Radio Frequency Identifier (RFID) chip ISO/IEC 14443. Big credit card companies like Visa, MasterCard and American Express are issuing their contactless payment cards for consumers and that market push is answered by merchants by upgrading their payment terminals to handle RFID-based transactions. North America, with their credit card

culture, has been more eager to take contactless payment into use than Europe. In contrast, in Europe the contactless ticketing has been a success, because of its public transportation industry. (Calvet 2005)

One of the main advantages of an NFC is that the device can be a reader but also it can simulate a smart card. The NFC recommendation[3] is built so that it is backward compatible with the contactless card standards. The smart card infrastructure is already installed and the ability to tap into this existing infrastructure is an important feature for NFC. The contactless payment standard is fully compatible with NFC. (Calvet 2005)

Unlike the communication with tags or other NFC-devices, the communication between an NFC-device and smartcard is done through APDUs (Application Protocol Data Units) which can be handled and executed in the processor of a proximity card. APDUs conform to the ISO/IEC 7816-3 and 7816-4 standards. (Ortiz 2003)

Nokia, for one, has used a secure Java smart card chip as the smartcard chip in the NFC payment and ticketing architecture. The communication with java chip is done by a message-passing model. The applet in the Java chip receives a *command APDU* and then returns a *response APDU*. Both have an optional body, but *command APDU* has a mandatory header part and *response APDU* has a mandatory trailer part. (Ortiz 2003)

2.3.3 Security and Privacy

Ticketing and especially payment are very secure-based functions and problems in either of them results in severe consequences and financial losses. Users are concerned about privacy of information and when NFC-devices hold that sensitive information such as credit card numbers, the fear of unauthorised reading and copying of the information exists. This might be the greatest barrier for adoption of NFC-based payments. (Calvet 2005)

NFC-based payment devices are significantly more secure than traditional payment cards. The ISO 14443 standard allows the account information to be encrypted while giving each issuer the possibility to use different encryption method and keys. The very short range (0–4 cm) of communication makes the unauthorised eavesdropping difficult and that enhances the security. (Calvet 2005) NFC is a wireless technology and thus the possibility of eavesdropping cannot be avoided. (Haselsteiner 2006) Another non-trivial security feature is that the user will not be required to surrender their credit card to the salesperson, but has control over his or her NFC-device during the transaction.

[3] Since Near Field Communication forum is not a standardisation body, we call the documents issued by NFC forum as “recommendations”.

2.4 Smart Poster

This chapter presents the Smart Poster concept. At first the Smart Poster concept is being presented at a general level. After that an example of a fictitious movie poster example that uses the Smart Poster Technical Concept is revealed and explained. In the last section, the Smart Poster Technical Concept is explained at a technical level.

The Smart Poster Technical Concept has been developed by NFC Forum. It defines how a phone number, SMS or URL can be stored in an NFC tag or transport them between devices. This way information and actions can be attached in a Smart Poster. Basically this allows transforming any physical object to a smart object by attaching a NFC tag in it. This means that the object can store additional information about itself. (NFCForum 2006a)

The Smart Poster makes it possible to initiate a phone call, send an SMS or go to a URL by reading an NFC tag with an NFC phone. The Smart Poster can contain actions that trigger an application in the NFC phone. The technical solution also makes it possible to edit or save the information (phone number, SMS, URL) read from the NFC tag. (NFCForum 2006a)

2.4.1 Movie poster example

This section demonstrates a movie poster which has several NFC tags with the Smart Poster functionality. The movie poster features the Finnish parody movie StarWreck, running in a new theatre located in Oulu, see Figure 4.

First functionality for a smart movie poster would be buying tickets. Touching the “buy tickets” tag would open a Web browser and the URL in the tag leads the user to reserve and purchase the seats for the movie. When the transaction is completed, the back-end system sends the tickets as an SMS to the phone.

The user might want to get more information about the movie before buying the ticket. When the “more info” tag is touched, a few things could occur, depending on what functionality is programmed into the tag. First, a mini-trailer could be loaded from the tag and shown. The trailer could also be downloaded via a URL. The information in the tag can lead to the film’s homepage or even its entry in the Internet Movie Database (www.imdb.com). However, only one action per tag is allowed.

The “Download soundtrack” tag has a URL which leads to an online music store.

The movie poster could have an ad for a nearby restaurant offering a discount. Touching the ad would save the discount offer as an SMS message in the phone’s message inbox.

A second tag in the ad could be used to reserve a table at the restaurant. Touching the tag would open an SMS with some predefined text and the user could type her name and desired time and then send the message to complete the reservation.

The movie poster could also have a tag which opens a Web page that has directions to the movie theatre.

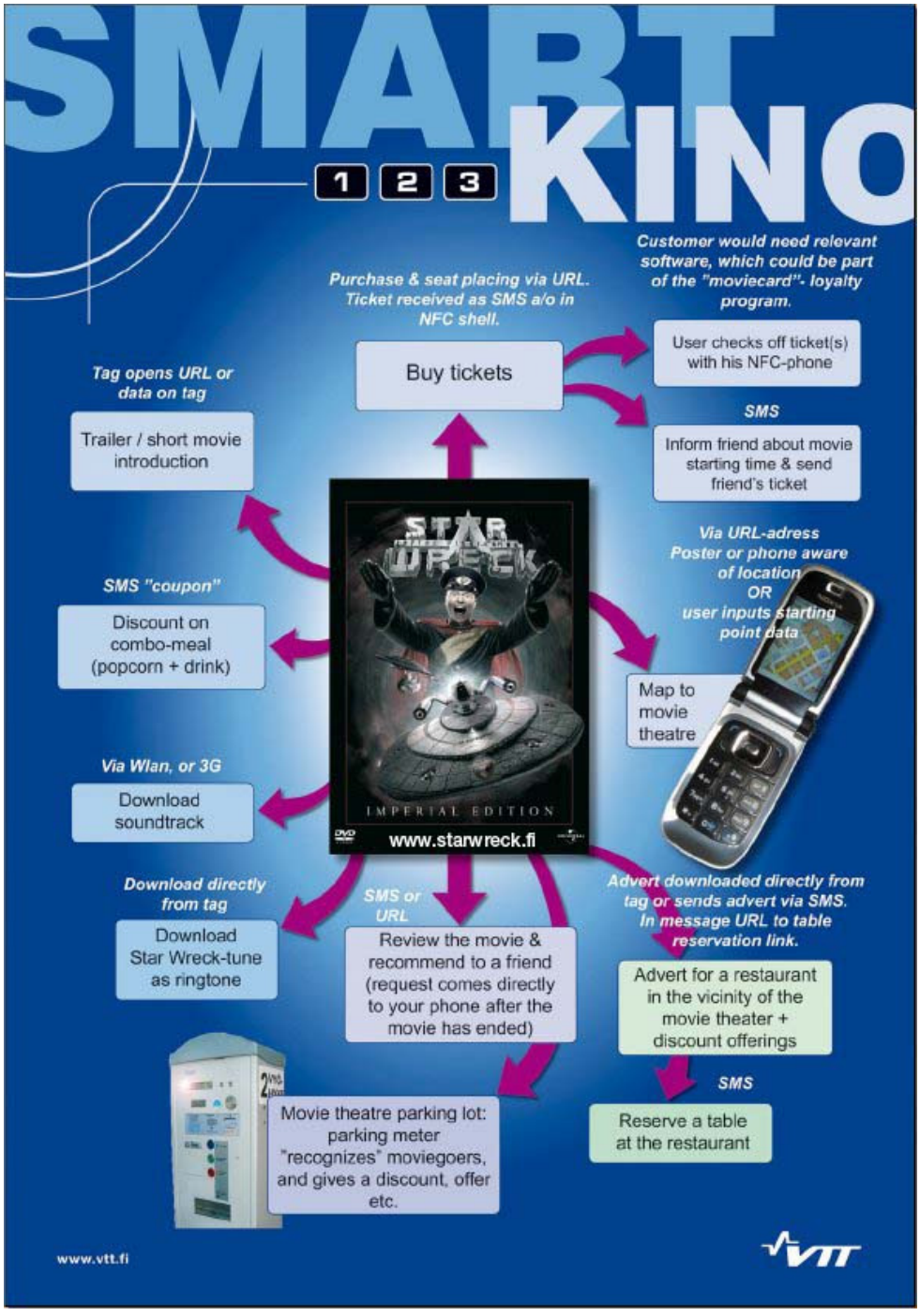

Figure 4. Smart Movie Poster Example.

2.4.2 Smart poster technical specification

NFC Forum has developed and released the Smart Poster RTD (Table 1). The concept is built around Uniform Resource Identifiers (URI). The Smart Poster RTD defines a superstructure that associates a URI with various types of metadata. The messaging sequence is not specific because the information is read and then acted according to its type and content. Reply to the message is not assumed. (NFCForum 2006a)

The message in the Smart Poster is an NDEF message and the contents of the message are several NDEF records. Zero, one or more of the following components can be found in the Smart Poster.

Table 1. Smart Poster NDEF (NFCForum 2006a).

Record Name	**Content**
Title	Title for the service (there can be many of these in different languages, but a language MUST NOT be repeated). This record is optional.
URI	This is the core of the Smart Poster, and all other records are just metadata about this record. There MUST be one URI record and there MUST NOT be more than one.
Action	This record describes how the service should be treated. For example, the action may indicate that the device should save the URI as a bookmark or open a browser. The Action record is optional. If it does not exist, the device may decide what to do with the service. If the action record exists, it should be treated as a strong suggestion; the UI designer may ignore it, but doing so will induce a different user experience from device to device.
Icon	A Smart Poster may include an icon by including one or many MIME-typed image records within the Smart Poster. If the device supports images, it SHOULD select and display one of these, depending on the device capabilities. The device SHOULD display only one. The Icon record is optional.
Size	If the URI references an external entity (e.g., by URL), the Size record may be used to tell how large the object is. This is useful if the reader device needs to decide in advance whether it has the capability to process the referenced object. The Size record is optional.
Type	If the URI references an external entity (e.g. via a URL), the Type record may be used to declare the MIME type of the entity. This can be used to tell the mobile device what kind of an object it can expect before it opens the connection. The Type record is optional.
Other	There MAY be other records, which can be treated in an application-specific manner. For example, some applications might include a vCard contact card using the proper MIME type. Applications MAY ignore any extra records inside the Smart Poster.

The contents of the record could resemble the contents of the Table 2 (total length 23 bytes).

Table 2. Example for a Simple URI (NFCForum 2006a).

Offset	Content	Length	Explanation
0	0xD1	1	NDEF header. TNF = 0x01 (Well Known Type). SR=1, MB=1, ME=1
1	0x02	1	Record name length (2 bytes)
2	0x12	1	Length of the Smart Poster data (18 bytes)
3	“Sp”	2	The record name
5	0xD1	1	NDEF header. TNF = 0x01, SR=1, MB=1, ME=1
6	0x01	1	Record name length (1 byte)
7	0x0E	1	The length of the URI payload (14 bytes)
8	“U”	1	Record type: “U”
9	0x01	1	Abbreviation: “http://www.”
10	“nfc-forum.org”	13	The URI itself.

3. Technical results

3.1 Implementation of pilot cases with early NFC phones

3.1.1 Meals on wheels

The NFC-based catering service trial was one of the pilot tests of the SmartTouch project. The pilot was conducted during autumn 2006 in Oulu, Finland. The service was implemented in collaboration with VTT Technical Research Centre of Finland and ToP Tunniste.

The process diagram is shown in Figure 5. A meal producer prepares meals and gives them to a logistics service for distribution. A logistics employee reports with his NFC-enabled mobile phone that the meals on his route are now on their way. This creates a timestamp. When the logistics employee arrives at the meal recipient's home, he reports that the meal has been delivered by touching a tag in the client's home. If the client is not at home he can report the absence of the client. The timestamp is now affiliated to the meal order. Timestamps are important to prove how long it took to deliver a specific meal. When the logistics employee returns to the food service facilities, he will report that his route is now complete. The whole delivery process now creates logs that can be used for billing, route planning and optimisation.

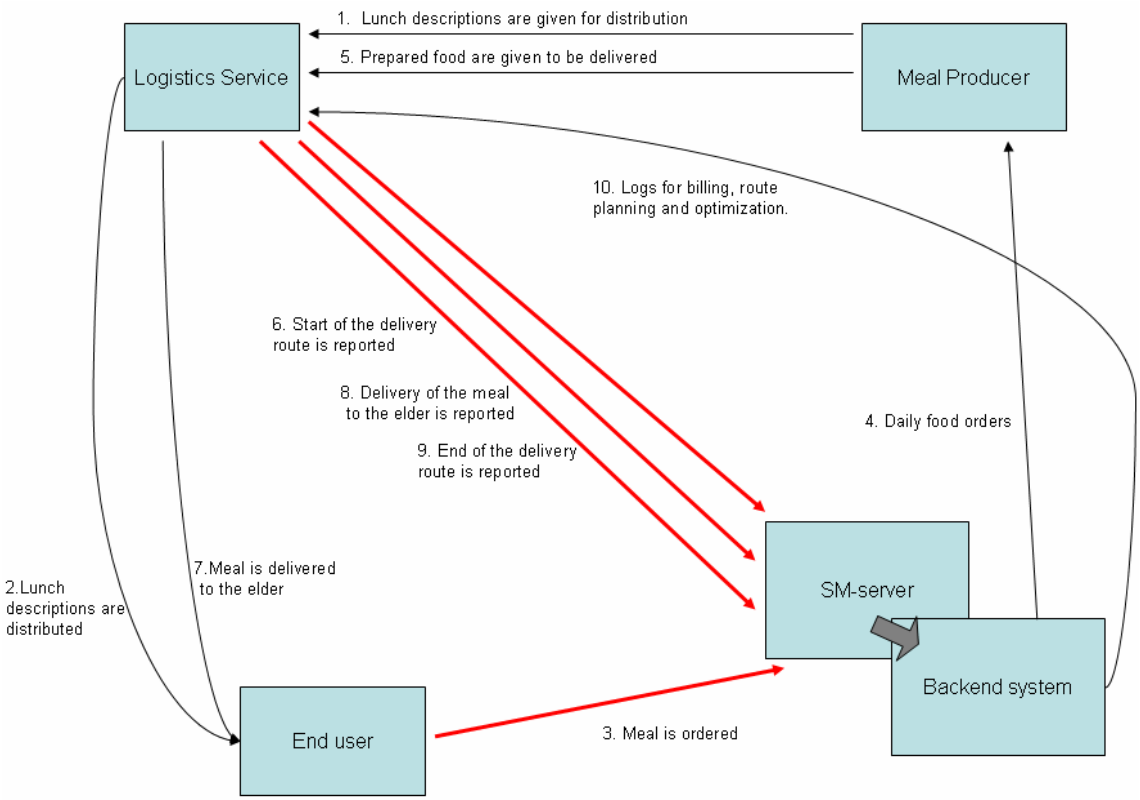

Figure 5. The overall view of the pilot. Red arrows indicate phases done with NFC.

In the pilot there were nine elderly people and five drivers who used NFC-devices. Two different JavaME applications were written for the devices. Elderly people had one application designed for them and logistics workers had another. Both applications were designed based on the feedback of users and their representatives. The feedback was mainly for user interface decisions. The goal was to make applications as simple as possible by minimising button presses and tag touches. For the meal recipients, the interface was highly specialised to overcome the challenges they face with their motor skills and eyesight.

The application made for the logistics employees was constructed on a framework which is provided by Nokia to generalise NFC-based applications. GUI for the application revolves around the Nokia Field Force paradigm which is deeply interwoven in the architecture of a Nokia SM-server. The logistics application starts by touching a tag. This touch will not read the content of the tag touched. After start-up, the application demands a login. The login is done by touching the ID-tag and then the application contacts the SM-server through a GPRS-network.

After login the application is ready to use. It accepts three different tag-based actions which are “start route”, “end route” and “meal is delivered”. The data in the tag should be in CSV-structure. If network coverage is not available or a suitable login is not done when reporting, the application will store the information until it finds the network and then sends all the stored information in a burst. This feature means that the time for the timestamp is taken from the mobile device. If the meal recipient is not home, the user can ask the back-end system to return the names of the recipients in his route. Then he can choose from a list which recipient was not home and report that to the back-end system.

At first, the application for the meal recipients was also based on the general NFC framework. After evaluating the first prototypes the user interface seemed to be too difficult for the meal recipients to use, so use of the framework was given up in this application. The Nokia SM-server still needs the login information to work, but the login process was considered to be a hindrance in the meal ordering and thus needlessly complicated the process. The problem was solved by storing the login information in the application and then sending it automatically when the application was started. The application had the possibility to change the login data by touching the ID-tag, but this was not taught to the meal recipients.

Figure 6. The plastic stand for the menu with NFC tags. Behind the coloured stickers are pre-programmed tags.

The application started up from a tag and remembered the content of the touched tag. The functionality was made to be as easy as possible and this feature provided the possibility to meal recipients to merely touch a tag on the meal stand (seen in Figure 6) and the rest was done automatically. The application started, logged on to the SM-server, sent the selected tag's information to the back-end system and then closed itself after enough time had passed. Users were informed during the automatic ordering process what was happening. No actual surveillance from the user was needed, but it helped to reduce misunderstandings or incorrect touches, as it told which meal was ordered. If the order was wrong or a meal recipient changed his or her opinion about food to order, order tags could be just touched again and in the back-end system only the last choice would matter.

A separate backend system was constructed for the pilot because existing back-end systems the city of Oulu had could not be used for the pilot. A third party server (a Nokia SM-server) was used as a connector between applications and the back-end system. The connection from the SM-server to the back-end system follows the standard method defined for the SM-server. Data is stored in a SOAP-XML -package which is extracted in the back-end system servlets and put into a MySQL-database run with an Apache Tomcat server. The meal producer employees use the HTML pages generated by a Java servlet from the data in the database.

Webpages were behind a username/password -based recognition that no outsider could access the data which could be considered very personal, such as allergies, addresses and meal ordering history. For the meal producer as well as social and health care organizations there was one collective information page and for logistics there was another because they were interested in different types of information. The former webpage listed current meal orders, orders for a specific date or all orders. The orders were mapped with the time information when the meal was reported to have been sent from the kitchen and when it was actually delivered to its recipient. The delivery time was calculated as it is required by law for meals to be delivered within a certain time limit.

The logistics webpage showed the data from a different angle. They were interested in how the delivery route went, how long it took to get from client to client, what was the total time of the delivery route, as it could be a basis for billing. This data could be checked from a driver-specific view, a date-specific view or as a global look at the whole process.

Logistics employees used Nokia 5140i mobile phones with an NFC-shell accessory. The phone was chosen because it was more suitable for work environments than the other possible option, a Nokia 3220 mobile phone with an NFC-shell. The meal recipients used a Nokia 3220 with an NFC-shell as their device. Tags used in the pilot were MiFare 1k compatible tags.

Combined, the nine meal recipients made 230 individual food orders, with the most being 39 orders from a single recipient, and the least being 14 orders. The median for orders was 24. Altogether, drivers made 214 reported food deliveries. These include some deliveries that were not ordered, but the nature of the pilot was that the recipients still get their food if they forgot to order their meal.

Reliability of the pilot was quite high. The difference between the orders and deliveries are mostly due to the instability of the third party server that was used to communicate between NFC-devices and the back-end system. It caused a situation in which, for a few days, deliveries and orders could not be reported. Food orders were made throughout the day and downtimes in the third party server did not cause many problems in that respect. In the end, about 7% of orders were never reported as delivered.

3.1.2 Physical access

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. A block diagram is shown in Figure 7.

A scenario:

Mr. Smith has an NFC phone containing the Buscom card application (applet). The card applet consists of a valid product, i.e. an electronic ticket/passport that entitles Mr. Smith to access the sports hall. The ticket has been admitted by the City of Oulu according to a payment (sports hall fee) by Mr. Smith's employee.

The electronic lock use scenario is based on a smart card solution. The NFC phone contains a secure Buscom public transport card application (applet) and a BuscomNFC Midlet which provides the user with an interface to the card application.

The pilot makes use of the current season ticket product based on the Buscom Palette product family of travel card systems. The back-end system tools provide the user with an interface to configure profiles for end users.

An example:

Mr. Smith is allowed to access the sports hall only on Monday afternoons between 3 PM and 5 PM.

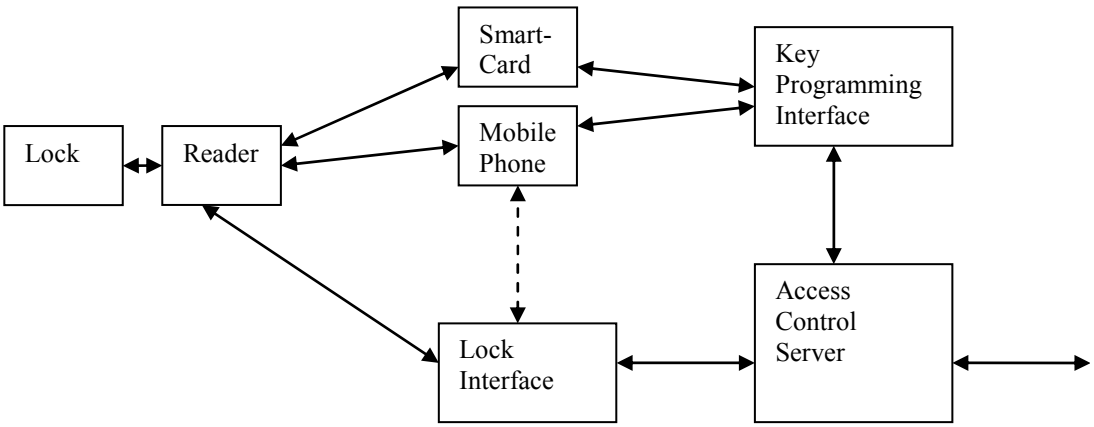

Figure 7. A general view of the parts of an electronic access control system.

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.

3.2 Smart NFC Interface

Smart NFC Interface is a multi-purpose platform by VTT, intended for developing and demonstrating different applications of physical browsing. Here the focus is on the touch-based paradigm (*TouchMe*), or bringing two devices close to each other. Support for the touch-based user paradigm is an inherent feature of NFC technology. In addition, the same platform can provide support for other physical browsing paradigms such as *PointMe* or *ScanMe.* The former means selecting an object by pointing at it with a visible or invisible beam whereas the latter means, for example, that a list of surrounding objects or services is provided to the user based on a limited communication range of a short-range radio.

Smart NFC Interface is a light, matchbox-sized device with a microcontroller, rechargeable Li-Ion battery with charging electronics, data logging memory, RS-232 serial port and other wired communications, as well as NFC, IrDA and Bluetooth wireless communications. The structure is modular to facilitate modifiability for different applications. There are connectors for extensions such as sensors. A temperature sensor is readily included, and the design supports ultra-low-power operating modes. The microcontroller is programmable by C. A photograph of the device electronics is shown in Figure 8.

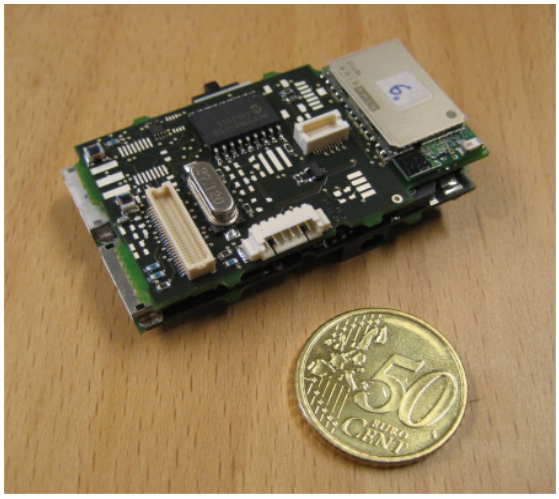

Figure 8. Device electronics (NFC antenna not installed). Communication Board is shown on top.

The purpose of the platform is to

- serve as a research and development tool of physical browsing technologies
- enable rapid prototyping and demonstrating of product ideas
- serve as a basis for product development (technology transfer to products).

In the following chapters, the electronics and software as well as applications are described further.

3.2.1 Electronics

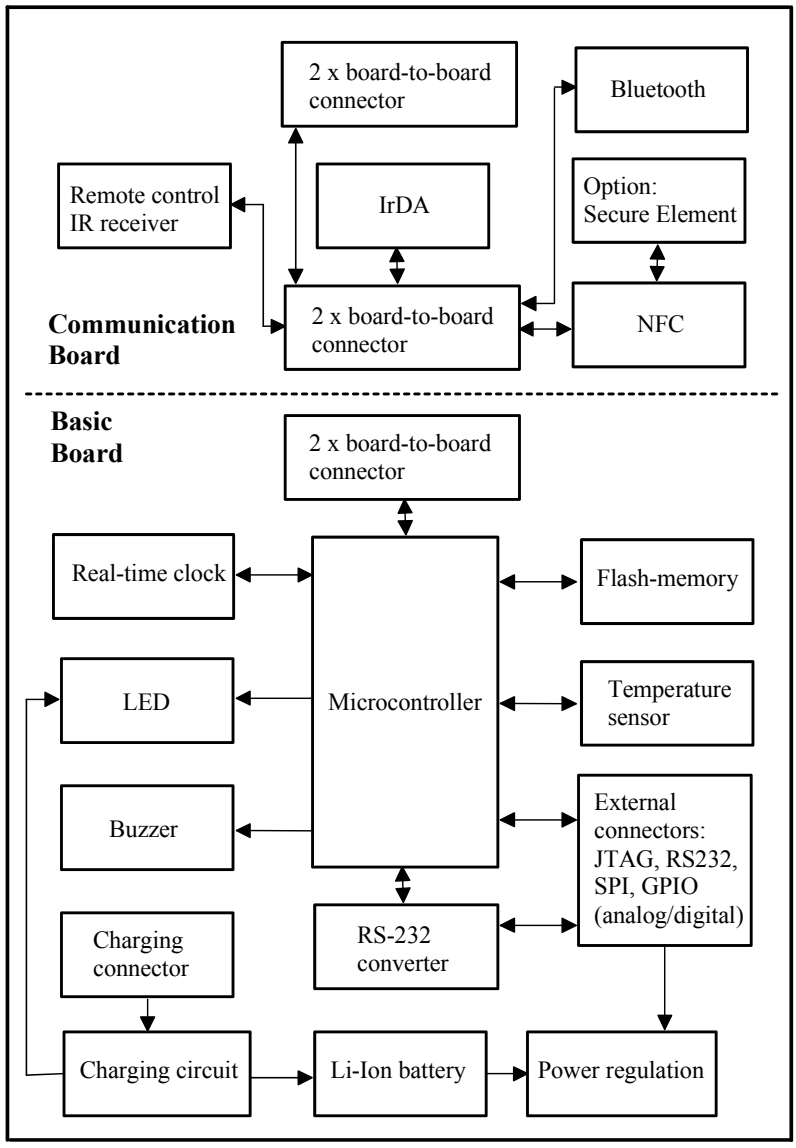

Figure 9. Block diagram of the electronics.

The block diagram of Smart NFC Interface electronics is shown in Figure 9. In its basic form, the device contains two boards: 1) Basic Board, and 2) Communication Board. However, more boards can be installed on top of the Communication Board if needed. For example, VTT has a compatible sensor board with 3-axis acceleration sensors, 2-axis magnetic (compass) sensor, a visible light sensor and an IR-based proximity sensor.

The dimensions of both boards are 56 x 31 mm. Overall thickness of the device including the default battery is 16 mm without encapsulation (boards attached one on top of another).

The device has a single 8-bit microcontroller (Atmel AVR series ATmega128L) which is equipped with 128 kilobytes of flash program memory, enabling easy reprogramming and debugging via JTAG interface. There are 4 kilobytes of internal RAM and 4 kilobytes of EEPROM in the microcontroller. There is also external 8 Mbit flash memory, connected to SPI bus of the microcontroller. This can be used for data logging purposes, for example.

The circuit is equipped with Philips PCF8563T real-time clock circuit, whose main purposes are 1) enabling recording of timestamps for events (data logging applications, for example) and 2) serving as a wakeup timer, facilitating ultra-low power modes.

A versatile power supply circuitry is used, enabling power to be taken not only from the internal battery, but also from RS-232 serial port or other external supplies. The power supply automatically adjusts to a wide range of input voltages. The battery charging connector and circuit is compatible with Nokia mobile phone chargers (specified to be compatible with Nokia ACP-12E charger). The charging circuit is connected to the LED, which indicates the charging status. While not charging, the LED is also software controlled by the microcontroller. Another supported UI feature is the buzzer.

Many anticipated applications are related to sensors. These can be connected to the external connector or to board-to-board connectors. A temperature sensor is integrated to the Basic Board.

On the Communication Board, the NFC is based on NXP Semiconductor PN531 circuit, which is connected to the microcontroller via SPI bus. A Smart MX secure chip can optionally be installed. Bluetooth (Class 2 Bluetooth radio) is based on Bluegiga WT12-A-AI module, which contains Bluetooth protocol layers up to RFCOMM and profiles, and is connected to the microcontroller by UART. IrDA support currently exists only in HW, based on Microchip MCP2150-I/SO IrDA controller and Zilog ZHX1403 IrDA transceiver. The same is true for the remote control infrared (IR) receiver.

The general purpose IO (GPIO) on the external connector also includes analogue input. This can be used to connect analogue sensors, for example. On the other hand, digital interfaces such as RS-232/UART and SPI can often be used. RS-232 levels are converted to logic level UART and vice versa by Maxim MAX3222CAP IC.

3.2.2 Basic scenarios as an NFC server

The main idea of the Smart NFC Interface is to enable a user's interaction with various objects by mobile device and local communication. Existing devices can be amended

into NFC-enabled smart devices by connecting or embedding the NFC platform into them. Especially the former method enables rapid prototyping or demonstrating of product ideas. In this case, the Smart NFC Interface works as an *NFC Server (*a.k.a. *Ambient Server)*. This principle is illustrated in Figure 10.

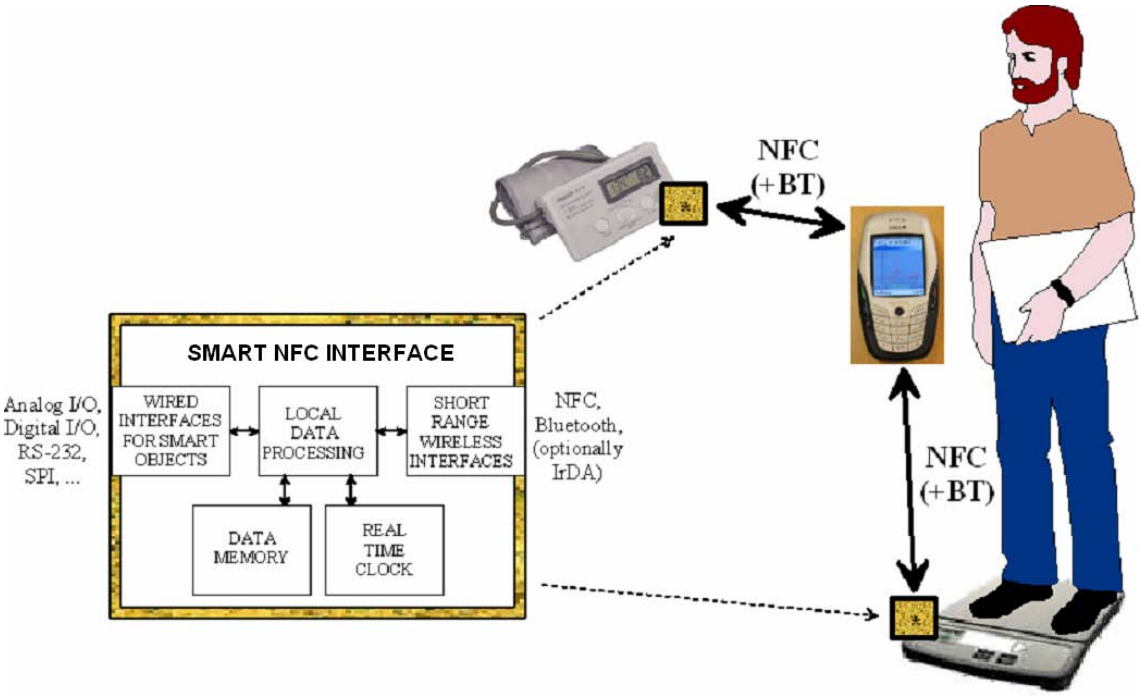

Figure 10. Smart NFC Interface as an NFC Server, amending existing devices (here a blood pressure meter and a scale) into NFC-enabled devices. User communication is enabled by the NFC phone.

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 (NFCIP-1) of NFC is suitable for these kind 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 11. NFC server technology enables using a mobile phone as the user interface for non-UI devices.

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 (value to be shown on screen). 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 again (see Figure 11). Here again, peer-to-peer communication mode is the most natural choice, the phone taking the role of the initiator.

In this kind of 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 more 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.

3.2.3 Basic scenarios as an NFC-Bluetooth Gateway

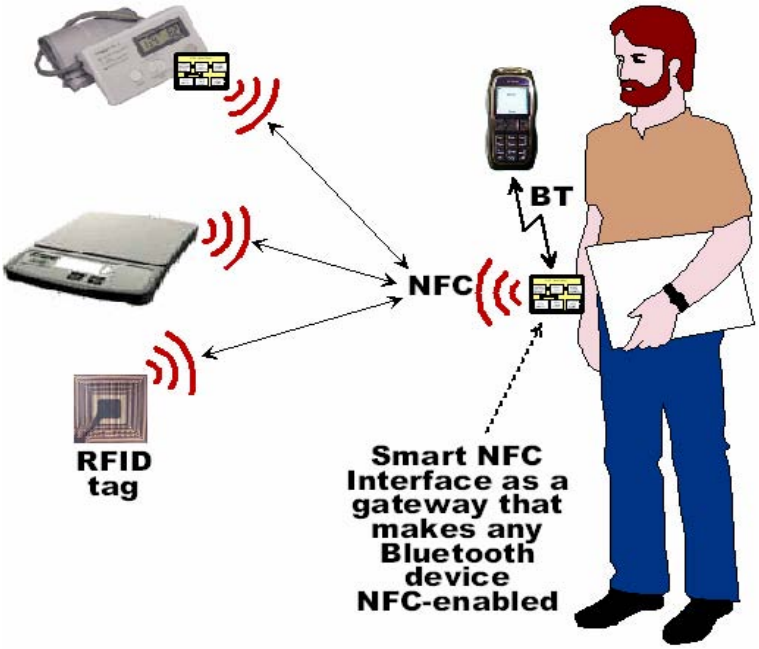

Figure 12. The Gateway can add NFC connectivity to a mobile phone or other device otherwise lacking NFC support.

An important application for the Smart NFC Interface is an NFC-Bluetooth Gateway. This enables adding NFC capability to mobile phones, laptops or other devices currently lacking NFC support but supporting Bluetooth. This principle is illustrated in Figure 12, illustrating also the different roles of NFC Server (attached to a blood pressure meter in the top left corner) and Gateway concepts. Now the Gateway is used to touch tags or NFC devices instead of the phone, but the data is communicated to and from the phone by Bluetooth. In practice, the Gateway can be, e.g. a wrist unit or a pendant, or can be fitted or even mechanically integrated into the phone.

There is a clear need for this type of gateway solution due to current poor availability of NFC phones. For example, there are no smartphones available at the moment that would have NFC support. However, many potential applications work best if implemented on a smartphone platform. In some applications, a robust device is required to survive in the working conditions. A gateway can be a solution for these cases: the phone can reside safe in a pocket or briefcase, but the gateway is encapsulated in a robust casing.

If laptops or desktop PCs are considered, they are bigger and heavier than phones, thus not being suitable for touching objects that cannot be easily brought close to the laptop. This is the case when communicating with fixed NFC installations, for example. Here the gateway type of solution could hold potential also as a product, or as an alternative to an integrated NFC or a USB-NFC dongle.

The Gateway can be used to read or write to NFC compatible tags (the currently supported and tested type is Mifare 1K), or to communicate with peer-to-peer (NFCIP-1) NFC devices. There is currently no support for tag emulation or secure communications, but a Smart MX IC can be installed if tag emulation is to be supported. However, this will require additional SW development work as well. A smartphone, Gateway and a tag are shown in Figure 13.

Figure 13. A smartphone with Bluetooth is connected to VTT's Gateway (GW) via Bluetooth. This enables reading (or writing) of data from VTT's NFC/Ambient Server (AS) or from NFC tags to the phone.

3.2.4 Other possibilities

NFC can be used to initiate connections between devices using other communication technologies such as Bluetooth or WLAN. In that case, NFC is a tool to configure the connection easily and explicitly with a simple touch, instead of configuring the connection by performing device searches or setting of configuration parameters by browsing menus and using keypads. Compared to pure NFC, the user does not need to keep the devices close to each other after the connection has been initiated, and Bluetooth and especially WLAN offer higher data rates in addition to the longer communication range. NFC can be used to create long- term device pairs (such as Bluetooth trusted pair) as well as to initiate new connections in an ad-hoc manner.

Based on Smart NFC interface, it is also possible to implement tag reading devices without a Bluetooth connection. This reading device can be a fixed installation, for example. Access control is one example of a typical application.

4. User experience

User experiences from pilot tests with NFC-enabled phones are described in this section. Section 4.1 describes the catering service for the elderly pilot (Meals on wheels) and section 4.2 describes the access control system pilot.

4.1 Catering service for the elderly pilot

This section describes user experiences of the elderly clients when they were using the new NFC-based meal service. The field study settings and data gathering methods are described in sub-section 4.1.1. Sub-section 4.1.2 represents the results and findings the study has achieved and the sub-section 4.1.3 represents the conclusions based on the pilot test.

Recent studies have shown that touch-based user interfaces have been found to be easy to learn and intuitive to use (e.g. (Rukzio 2006) and (Välkkynen 2006)). Therefore, the hypothesis of the study was that a touch-based user interface could be suitable for elderly users who are not fluent technology users, and who are challenged by current prevailing user interface paradigms and technologies.

4.1.1 Field study

A field study was arranged so that the technology and the application were used on a trial basis in a real usage environment with all actors of the service chain from the kitchen to the home of the elderly. The elderly users taking part in the study were volunteer customers of a meal delivery service provided by the city of Oulu, located in Finland. A total of 11 elderly users volunteered, from which nine users were able to finish the study. All users had somehow weakened cognitive capabilities (such as memory), and some had limited physical capabilities (such as controlling hand movement) or mental problems. They were eligible for the city-supported meal service as their functional capabilities were low (measured with the RAVA index (Rajala 2001). The youngest user was just under sixty and the oldest one was 88 years old. The average age of the users was 76.6 years. All users were able to live at home alone, but because of cognitive or physical restrictions, were unable to cook or go grocery shopping by themselves. However, the trial users represented the ones with good cognitive, mental and physical condition among home care clients. With large-scale use, the average user would have more problems with all these skills. The total study period was approximately eight weeks. The time of active usage varied between individual users from three weeks to eight weeks.

The participants of the pilot test received the following items for making meal orders:

1) An NFC tag stand (shown in Figure 14)
   a) meal tag A
   b) meal tag B
   c) no meal tag C
   d) paper menu (illustrated in Figure 15)

2) A Nokia 3220 mobile phone equipped with an NFC-reader shell.

Figure 14. The plastic stand for the menu with NCF tags.

Week 43 23.10.2006-27.10.2006	A	B	C
MONDAY	Broilersauce	Mushoon soup	No meal
TUESDAY	Bolognese	Beef in peppercorn sauce	No meal
WEDNESDAY	Meat soup	Vegetable loaf	No meal
THURSDAY	Beef and potato bake	Salmon bake	No meal
FRIDAY	Game temptation with bacon	Ham-vegetable soup	No meal

Figure 15. An example of the paper menu.

The total amount of required steps for placing a meal order decreased notably during the development of a UI. In the pilot, test users' had to touch a tag once with a mobile phone to order a meal. Before the touching a tag, the user had to check the menu and

choose between three options. These options are meal options A and B and no meal option C. After a user has touched a tag, the user receives feedback from a mobile phone and when the order is ready the application in the mobile phone closes automatically. After this, the mobile phone is ready to be used for a new meal selection. Required steps when a user is ordering meal A are presented in the Table 3.

Table 3. The meal order based on one touch with a mobile phone.

User	Phone	NFC tag
Takes the phone →		
	Touches meal tag A →	
←	'Opening the application'	
←	'WAIT'	
←	'MEAL A ORDERED'	
←	'Closing the application'	

Data gathering methods for investigating the user experience were selected based on the evaluated skills of the participants and earlier studies. Initial information about the participants was received by interviewing home care employee. According to home care employees, novel technological solutions were not too familiar for the participants. In addition, all the participants were experiencing a decline in some of their skills. These facts were considered when it was time to select appropriate data gathering methods. Naturally, the aim was to choose data gathering methods which would not interrupt or disturb the use of the new catering service. The methods chosen were three traditional methods: interview, observation and pen-and-paper based diary.

The diary was not a successful method of gathering data. The participants were asked to report their feelings about the use of the meal service. Only one participant completed the diary as it was meant to be completed. In addition to evaluation of the use, he also often evaluated the quality of the meals. In fact, the participants often evaluated the quality of meals among. Four of the participants evaluated only the quality of meals and four participants did not complete the diary at all. One of the participants evaluated the meals directly on the paper menu. It seemed that evaluating the feelings created by use of the system was very difficult for the participants.

Every participant was interviewed twice at their homes. Initial interviews were conducted before training sessions in the beginning phase of the test. Semi-structured interviews were conducted at homes of the participants. In the initial interview 11 elderly clients of the catering service were interviewed. In these interviews the main focus was on the background of the participants and their relationship with the new

technologies. In the final interviews the aim was to gather data about user experiences and attitudes concerning the new catering service and the related interaction technique. Interviews provided the possibility to open some of the questions for the participants when it seemed to be too hard to understand the question. Interviews succeeded well and all the participants were eager to answer the questions. Each question and answer from the recorded interviews was recorded in an Excel sheet, which made it possible to examine the answers of the different participants side by side.

Use of the user interface was also observed in the training session, in support visits and in the end phase of the test period. The aim of the observation was to gather data about the use of the user interface on a detailed level. Observing and making notes was demanding during a training session. It would have been easier if one person could have concentrated solely on taking notes with a pen and paper and another person could have concentrated on communication with the participant. However, observations gave valuable data about the use.

4.1.2 Results and findings

Out of eleven voluntary users, nine started to use the application after the pre-interview and training. The two users who decided not to adopt the application made this decision when the researcher responsible for the training and pre-interview introduced them to the application and related physical devices. These users had volunteered for the trial, but during the introduction they decided not to even try. Neither of the users physically used the application; they made the decision to drop out of the trial purely on the basis of the visual encounter and the information they got by following and listening to the researcher who showed them how the application works. One user referred to the non-aesthetically pleasing looks of the plastic stand and menu. Out of the nine users who were willing to adopt the application, none dropped out during the trial, even though most required encouragement and support, especially in the beginning, as they doubted their ability to adopt the new technology.

All users were able to place meal orders without difficulties. Thus, we conclude that the touch-based user interface was very intuitive, and easy to learn and use. Even the users with restrictions in the physical movement of their hands, and who had problems with hand-and-eye coordination, did not have problems in using the interface. Some system failures occurred during trial use. As the user interface was very simple, the end users could not get information about failures, and were unable to correct them. Therefore, our researchers monitored the meal orders placed, and checked manually if they suspected something was wrong. For example, if a meal order was not placed in time, the researcher would call the elderly user in question to ask if everything was well.

All but one of the trial users had been satisfied with the meals and the service they had received prior to trial. After the trial, about half of the users (five) preferred the new service over the old one, as it provided them added value by allowing them to choose their meals. However, approximately another half (four users) stated that they did not really need options for their meals and were quite happy with the meals they received automatically. On the contrary, they expressed that the application caused them stress and worries, as they had to remember to place orders in time. Even though the willingness to adopt the system strongly correlated with the fact that the user previously owned a mobile phone, we saw no difference in how the non-mobile phone users and mobile phone users used the touch-based user interface. Both learned to use it quickly and managed to use it with similar fluency.

4.1.3 Conclusions

As our experiences show, the touch-based user interface is very appropriate and suitable for applications that are used in the everyday routines of elderly users. Our trial users were able to use it fluently after a short hands-on training. However, constant involvement in the form of phone support and system status monitoring was required to ensure the correct operation in case of technical problems.

Taking into account different shortages in the UI which emerged in the pilot test, it would be possible to improve its usability. For example, adding the reminder property to the order application for reducing the demands of remembering could help users with a memory difficulties. Also, by changing the feedback of a mobile phone in a way that it gives auditory, tactile and visual feedback immediately after a successful reading could possibly improve the usability of the solution. However, it would be unlikely that acceptance of the catering service would change substantially, because all participants did not see the basic idea about meal selection as necessary for themselves. In other words, if the service is not experienced as useful, then the value of the UI and related technology is not very essential. One conclusion based on this study is that when we are designing services for the elderly, who are inexperienced with the technology, we should focus on the wider entity, which consists of several factors. This way, the new technology-based services could have wider acceptability among the elderly.

4.2 Access control system pilot

This section describes user experiences from the access control system pilot. The pilot was divided into two parts: electronic lock and usage monitoring of the facilities. NFC-based mobile phones were used to provide access to the sport facilities of a school. In

addition, users sent number of players to a background system by using NFC-based application. This provided the possibility to monitor the utilisation rate of sport facilities easily from the Webpage.

The objective of the pilot was to investigate how an NFC-based system is suited for access control system. Sub-section 4.2.1 describes the field study, sub-section 4.2.2 represents the results and findings the study has achieved, and sub-section 4.2.3 represents the conclusions based on the pilot test.

4.2.1 Field study

An access control trial was conducted from October 2006 to February 2007. The first part (Electronic lock) started in October and the usage monitoring started in December. The aim of the pilot was to investigate how well the NFC-based access control system works in a real use environment. There were nine participants in a trial. Four of them were in the role of an employee (three teachers and a janitor) and five pilot users were members of hobby groups. Evening and weekend users used both the electronic lock system and the usage monitoring application. Employees of the school used only the electronic lock system.

The research problem of the study was how suitable the NFC-based access control system and usage monitoring application are for the access control and usage monitoring of the facilities in a real use environment.

Users touched an NFC reader with an NFC-enabled Nokia 3220 mobile phone to open the door (Figure 16 and 17). After the touch, the system checked the access rights of the user, which were defined in a mobile phone. If the access rights were valid, the lock of the door was opened.

Figure 16. NFC reader.

Figure 17. Touch with an NFC-enabled mobile phone to a reader.

After touching the reader, the user received visual feedback from the reader. The text "Wait…" and "Welcome" were displayed on a reader screen. In addition, a green light indicated that access rights were valid and the lock was opened.

In addition to the use of the electronic lock, evening and weekend users also fed information to the background system by using the NFC-enabled usage monitoring application. Users touched the tag attached to a piece of paper, which was on a wall of the sports hall (Figure 18). After the touch, the mobile application was opened and a user could feed the amount of the participants and possible additional information to the text fields. After this, the user sent information to the back-end system by selecting OK from the mobile phone. This information provided possibility for monitoring the utilization degrees of the sport facilities for the sport and education department of the city of Oulu.

Figure 18. NFC-based usage monitoring application.

Data was collected by using questionnaires with open-ended and structured questions. The questionnaire was sent to all the participants by e-mail. Seven of nine trial participants answered the questionnaire. All of them were men and their average age

was approximately 44 years. Five of the respondents were weekend and evening users and two of the respondents used the electronic lock as employees of the school.

4.2.2 Results and findings

Table 4 represents users and their experience from the use of access control system and usage monitoring application. The rightmost column displays preferences for the new and old practice. Four of the participants expressed that their experience from the use was positive, two experienced that the use was neutral and one user's experience from the use was rather negative. One of the participants saw that the new solution was worse and one saw it as much worse than the earlier practice. Four of the participants expressed that the new solution was better than the earlier practice. One respondent's opinion was that the new system was much better compared to the earlier practice.

Table 4. Experiences from the use and preferences for the practices.

User	Age	Gender	Use	Experience	Preference (New vs. old practice)
K1	28	Male	Evening use	Neutral	New better
K2	69	Male	Evening use	Positive	New better
K3	53	Male	Work	Positive	New better
K4	40	Male	Evening use	Neutral	New worse
K5	49	Male	Evening use	Positive	New much better
K6	38	Male	Work	Positive	New better
K7	31	Male	Evening use	Rather Negative	New much worse

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 respondent's experience about the effectiveness of the application. It was also the feature which emerged in almost every participant's answers.

Five of the respondents saw the system as useful whereas two of the users expressed that the system was relatively useless for them. One teacher expressed that he did not benefit much from the system in his work, but saw that evening users could benefit from the solution. Many users saw that the idea behind the solution is good, but the system should be developed to be more reliable.

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.

4.2.3 Conclusions

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.

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.

5. Security issues of RFID-based near field communication

This section describes some security and privacy issues of NFC (near field communication). We begin by describing the importance of security in a mobile context, defining terms such as security and privacy and describing the methodology for determining the security issues. In the third chapter we introduce the methodology before describing some challenges related to the current NFC implementations. Finally, we conclude the section with a short discussion.

5.1 Importance of security-based issues

As different electronic devices nowadays handle an increasing amount of information, the implementation of security-based solutions and applications has become vital before taking new technology into wider use, but also within the developed services that are using the technology. In addition, when determining the security of personal devices such as mobile phones or PDAs, privacy can also be highlighted, since the devices contain a lot of personal information that can be used for tracing the user's true identity.

The possibility of using Radio Frequency Identification (RFID) for tracing purposes has already resulted in protests and legal initiatives made by consumer organisations. Two recent technology trials by Benetton Group in Italy and Metro Extra Future Store in Germany have been cancelled after activists protested against their RFID roll-out plans. In 2006 in the United States the Governor of California vetoed a proposed bill that would have regulated the use of government-issued RFID cards and their information content. Last year, the EU carried out a study with an objective to reassure the public about the positive aspects of the technology.

As the previous measures were mainly based on RFID technology implementations in smart cards and tags, what will future solutions entail? Mobile devices are ideal targets of application for RFID technology, i.e. near field communication (NFC). However, in the future security measures play an increasing role as the devices contain an increasing amount of personal information such as email and SMS messages, pictures, passwords and/or other important notes. By neglecting the assessment of security issues, we might inhibit the potential consumer interest in RFID technology in the mobile environment and slow the development of future services.

5.2 Definition of mobile RFID security and privacy

In this chapter, we define terms such as information security, communication security and mobile RFID security as well as privacy that constitute the framework of the security analysis performed in the Smarttouch project.

The term *security* has many meanings depending on the method of interpretation. In this paper, we focus mainly on information and communication technology perspectives, but also take into account the business perspective.

The U.S. Office of Personnel Management handbook defines Information Security (IS) work as *"Security work that involves ensuring the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information systems security programs, policies, procedures, and tools."* (USOPM 2001). Krause and Tipton point out that *"communications security involves ensuring the integrity and confidentiality of information transmitted via telecommunications media as well as ensuring the availability of the telecommunications media itself"* (Krause 1998). They also divide communications security into three categories: (1) telecommunications security objectives, threats, and countermeasures; (2) network security; and (3) Internet security. (Krause 1998). In this context, we are dealing to some extent also with physical security when discussing physical tampering or destroying NFC tags, but the main focus is still on the three previously mentioned categories.

A way of categorising the security of mobile RFID is presented by Konidala and Kwangjo who divide the application layer into three different zones; The "Location-based Services (LBS) Zone" consists of public services targeted to the consumers. The "Enterprise Zone" assists company personnel while they are on the move. Finally, the "Private Zone" assists consumers in their private space: home, garden or garage. The three zones represent different security needs and therefore also security levels that have to be taken into account when designing the required security measures for a single service/application. (Konidala 2006)

In addition to the previous definitions, we determine also the term "privacy" due to the personality of mobile devices that was explained in chapter 5.1. Andersson defines privacy as *"the ability and/or right to protect your personal secrets; it extends to the ability and/or right to prevent invasions of your personal space"*. He also highlights that privacy can extend to families, but not to legal persons (i.e. companies). (Anderson 2001)

5.3 Methodology

In this chapter, we present the structure (methods) of the security analysis that will be performed for selected use cases within the Smarttouch project. Since the security analysis is currently at section one, the later sections (2–4) are in a draft stage and therefore subject to change before and during their completion.

The security analysis consists of the following four parts:

1. Security design
2. Vulnerability and risk analysis
3. Risk mitigation and security policies
4. Security deployment and monitoring.

We begin the security design section by determining the basic information for the security analysis. The basic information consists of the necessary descriptions concerning the organisation and other background from the use case. After that we describe the scope of the analysis by defining the target functionalities, components, architecture, life cycle and by determining the security objectives. Finally we define the assets and security requirements that are partially derived from the previously described sections.

The second section of the analysis consists of risk and vulnerability analysis. We perform the analysis by evaluating the potential risks (threats) and vulnerabilities using the following questions:

- **Who** is going to conduct the attack and/or benefit from it?
- **What** are the objectives of the attack/attacker?
- **When** will the attack happen?
- **Where** will the attack take place?
- **How** will the attack happen?

In addition to the previous questions, the attack potential is measured in a three-point scale that is included in a table consisting of the different threat elements and affected security criteria. After that we define the scale of vulnerabilities for each threat using a five-point scale in order to formalise several key threats that will be selected for later assessment.

The third section of the analysis deals with risk mitigation (i.e. management). In practice we determine the real risks affecting the target system, which is performed by comparing the threats with the security needs and estimating the impact for the

organisation. Based on the mitigation, a security policy is proposed for the target environment in order to counter some of the retained threats.

The final section of the security analysis concentrates on the deployment and monitoring of security-based issues. In other words, we set a target in order to encounter the remaining threats. Finally, we finalise the analysis by providing an expression of assurance requirements according to the strength level of the security objectives defined in the risk mitigation paragraph. The security objectives form the grounds for confidence that a target system is protected by mechanisms resistant enough against the noticed threats.

5.4 Security challenges

In this chapter, we present some security challenges related to several case-examples within the SmartTouch project utilising NFC technology. The security challenges form the basis for the initial security design part of the analysis and therefore also provide an overview of the document formalisation process.

5.4.1 Electronic lock and mobile ticketing

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 Larsen who describes the use of a secure solution using digital keys and certificates over a Bluetooth connection (Beaufour 2003). Even though the Bluetooth solution is an economically more 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 more 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. The current mobile devices provide this kind of functionality for money transactions in a specific electronic purse application, but it can also be developed by a third (external) party. All-in-all, mobile ticketing provides the required motivation in order to attract consumers into using NFC technology and together with the two following case-examples, it may well build up into a complete service chain that starts from home, makes use of public transportation and provides the customer with a positive mobile service experience without any security hazards nor usability deficiencies.

5.4.2 Mobile payment

As already described in chapter 2.3, mobile devices and NFC have opened up new possibilities for the mobile payment market. Especially within the proximity (local) payment technologies such as public transportation, NFC gains advantage against traditional mobile phone based payment as it provides the same transaction speed and therefore usability as contactless cards, but at the same time enables charging the electronic purse over the wireless channel instead of going to a kiosk or a ticketing machine.

Even though NFC improves the traditional mobile payment technology, the security and privacy issues have also increased. This is mainly due to the two-way communication (long-range communication is used for charging the purse and short range communication for paying), i.e. the new solution contains the security threats of both the previous solutions. In addition, as the mobile device is also used for other purposes, the threat of financial losses or even losing the whole device frightens the users and might affect their behaviour when adopting NFC payment technology. In addition, since a dead battery also affects the paying capabilities of the device, this might also be a barrier to the users, at least before technologies that enable contactless payment also in this case, have been taken into use. In case the focus of NFC technology remains on micro-payments in the future, this might alleviate the fears that any users might have and result in an increase in the adoption of this new technology.

5.4.3 Smart poster

Smart Posters, as already introduced in chapter 2.4, can be used as advertising elements such as signs or billboards that incorporate a passive NFC tag containing information. The data can be extracted by touching the tag with a NFC-enabled handset that initiates data exchange between the tag and the device. The tag can initiate a phone call, send an SMS message or open an application that provides a graphical user interface to the tag information content. And in case the required application does not exist in the phone, the tag can even direct the phone browser to a download page where the user can acquire the necessary software. A smart poster can be located for example in a public transport station (bus, railway, etc.) where it can be used for downloading timetables and other information or buying a ticket using a ticketing application provided by the transportation company that can be downloaded to the phone from the Internet. In this case the smart poster provides added usability to the system as the users touches the tag that provides information or redirects the user to a Web site instead of the users reading and typing the URL to the browser themselves.

The smart poster case-example introduces completely new security challenges due to the added usability of the solution. For example, in the previous public transportation case-example, the location of the smart poster is public, which can result in physical tampering or even changing the tag. A malicious tag might redirect the user to a forged Web page that allows the user to buy the ticket, but sends it to another device instead of the rightful owner. In the worst case, the tag might contain a virus that spreads and/or makes phone calls to expensive service numbers or even another country. These security issues can be prevented by either installing the smart poster behind plexiglas or by implementing digital signing of the NDEF (NFCForum 2006b) data in order to verify the authenticity of the smart poster tag automatically by the phone. In case the physical tampering and tag changing could be prevented, the tag could still be destroyed by e.g. drilling a hole through it or someone could create smart posters that look like the original, but do not contain any tags. These cases would result in a Denial of Service (DoS) attack that might decrease the motivation of users to later touch smart posters with their NFC-capable mobile devices, thus affecting negatively the future of smart posters.

5.5 Discussion

The security analysis provides vital information about the security issues and processes that the NFC technology and service providers will most likely have to cope with in order to develop successful services to the consumer market. Based on the recent discussion on RFID privacy, also those issues should be thoroughly examined.

As an emerging technology, NFC has to overcome the prejudice of consumers and build a positive image among them. By providing enough information on the potential threats and risk mitigation, the technology will gain ground among the already existing competing technologies and may well end up being a dominant design in the coming decade.

6. Business models and challenges

6.1 Mobile payment and ticketing schemes

There are numerous ways to categorise mobile payment and ticketing solutions. Categorisations can be made based on some special characteristic, for example, timing of payment (real-time, prepaid, or post-paid), payment height (pico, micro or macro) or medium of payment (bank account, credit card or phone bill). The general way is to make the division based on the technology used for mobile payment. Figure 19 depicts some technologies that are used in different mobile payment and ticketing systems. (Kreyer 2002, Choi 2006)

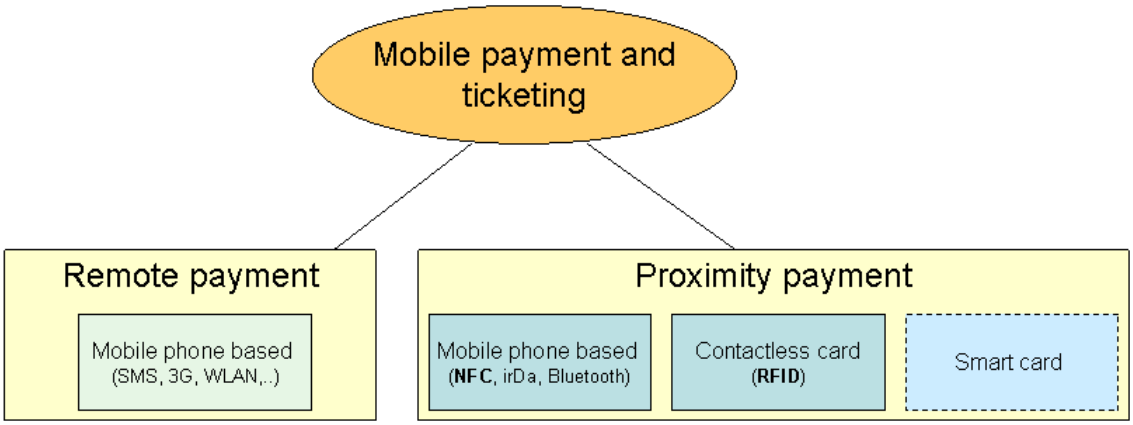

Figure 19. Mobile payment and ticketing technologies.

A rough division of technologies can be made between remote payment and proximity payment, which is also referred to as local payment. Remote transactions are carried out over communication networks such as GSM, 3G or WLAN. Several remote mobile payment systems have been developed since the mid 1990s, but those have not achieved notable customer volumes and most of the expectations about the success of remote mobile payment systems have been postponed to the future.

Proximity payments take place when a payment device or a card communicates with a nearby machine or device. A transaction takes place in a similar situation where one might normally use a contact card that has to be inserted into reader, such as purchases in stores, public transportation or when using a vending machine. Smart cards are considered as a pre-stage to mobile payment systems. Instead of mobile payment, electronic payment is a more appropriate term for payment schemes that use smart cards such as Proton or Moneo. Contactless smart cards that use RFID technology are more advanced means of payment. Contactless payment is often seen as a transitional stage to mobile phone based proximity payments. Proximity payment using NFC-enabled

mobile phone and contactless smart cards are nowadays considered as the most promising technologies in the area of mobile payments and those are the most relevant technologies from the viewpoint of this report. (Choi 2006)

There are several differences in proximity payment between mobile phones and contactless smart cards. Some pros and cons of the mobile payment using a NFC-enabled handset compared to contactless payment are introduced in Table 5.

Table 5. Pros and cons of the mobile phone based proximity payment compared to contactless payment.

+/-	Effect	Stakeholder
+	Reduced card issuing costs	Bank
+	Less to carry, because there is no need for both contactless cards and mobile phone. Mobile device can include several accounts.	Consumers
+	Possibility to view account information from a phone's display.	Consumers
+	Improved privacy in a situation where a PIN code has to be entered compared to entering a PIN-code to a POS-terminal.	Consumers
+	Increased data transmission because of over-the-air downloads	MNO
+	Revenues from managing applications at payment platform.	MNO / bank / ?
-	Brand visibility may be reduced in mobile phones.	Card association
-	Fears about security and privacy issues	Consumers
-	More costs to consumers because a new NFC-enabled handset is required for the mobile payment services	Consumers

Mobile payment systems can be further classified according to the actor who is responsible of the payment platform where the customer data is located. Mobile network operators are very interested in getting their share of the mobile payment business. The best way to get that share is by having payment applications loaded into a SIM-card, which is managed by the operator. The major problem is that financial institutions would also like to manage the payment platform and thus manage customer information held in those. In addition, there are numerous payment systems where customer information is stored and managed by some other actor. For example, several public transport ticketing systems that use contactless payment work independently of financial institutions and MNOs. The following three sub-sections concentrate on these three payment schemes one by one and finally in section 6.1.4 co-operation between different stakeholders is discussed.

6.1.1 Contactless payment schemes driven by financial institutions

International credit card associations have been very active in promoting contactless payment to consumers, especially in North America. Major financial institutions have

foreseen the transformation of the payment markets and in order to make sure that after the revolution they still hold strong positions in the market, they have made great investments in the new technology. Because of the significant push from the global credit card associations, contactless payment and ticketing seems to be the main driver to the acceptance of NFC/RFID-related solutions.

The main reason why consumers and merchants are moving towards this new form of payment is the speed and convenience of payment process. Payment is very handy for small transactions referred to as micro payments (usually under $10), because consumers can just tap their contactless payment device on a reader and go. There is no need for a signature or a PIN code. On the other hand, merchants obtain benefits from improved operational efficiencies and decreased cost of handling cash.

But what is the motivator for the financial sector? Two main motivating reasons can be seen. Firstly, the fear that MNOs are taking control of an area that has traditionally been in the hands of the financial sector is keeping financial institutions on their toes. 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. MasterCard has already succeeded in gaining a customer base and market awareness with its Paypass contactless smart card and it remains to be seen how much help that provides to competition in continually more competitive mobile payment markets.

Although 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. 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.

6.1.2 Mobile phone based payment schemes operated by MNO's

GSM association is one of the most enthusiastic spokesmen on behalf of mobile phone based mobile payment. According to their initiative called "the Pay-Buy Mobile", the best way to advance mobile technology would be to store payment applications on the SIM-card. This would enable a viable business model for mobile operators, since they could charge banks and credit card companies fees from downloading card issuers' payment applications on the SIM. According to operators, financial institutions would be willing to pay because they would save money on card issuing costs and would generate more transactions. (Card 2007a)

However, financial institutions are not as sure about the fair division economical benefits in this solution. Another problem is that there are not currently any commercially available NFC-enabled mobile phones where payment applications would reside in the SIM-card. Therefore, if a SIM-card based solution is to be used, new mobile phone models have to arrive before NFC can really hit consumer markets.

6.1.3 Independent payment schemes

Independent payment schemes consist of all the solutions that are not directly controlled by MNOs or financial institutions. This scheme requires quite a large customer base to be viable and therefore most popular initiatives come from the public transport sector where transport operators can have a significant installed customer base (Ondrus 2006). In addition, introduction of contactless/mobile payment scheme to public transport customers seem to be reasonably easy, since the scheme provides clear benefits to customers with shorter queues and waiting times.

Many well-known public transport ticketing systems are controlled by local public transport operators or other actors outside financial or mobile network business. For example, the contactless card system Octopus in Hong Kong is jointly controlled by Hong Kong's major transport operators (Octopus 2007). One of the main reasons that transit operators trust independent payment schemes might be that they do not want to pay transaction fees to financial institutions if they can avoid it (Ondrus 2006).

6.1.4 Competition or co-operation between stakeholders

Competition between financial institutions and MNOs may cause disagreement to the question about the party who should be controlling the payment platform and issuing the mobile payment element where actual payment application resides. However, both financial institutions and mobile operators need each other in order for mobile payment using NFC-enabled handsets to take off. Without the interest of the operator, there will not be many NFC-enabled mobile phones on the market since in most countries MNOs are key players in deciding which mobile phones will be pushed to the market. On the other hand MNOs need to co-operate with the financial sector, which has a long tradition and knowledge of payment issues, good connections to retailers and a large installed base of paying customers.

One solution to this problem might be that some neutral third party would take the role of platform manager. There are several possible candidates for this position, but secure element (SE) vendors are probably best positioned in terms of business relations and technical expertise, because the same SE vendors supply IC chips for smart cards to banks and SIM cards to operators. In addition, the number of SE vendors is relatively small also internationally, which makes the business model simpler on an international scope. (Risikko 2006)

In Europe a company named Venyon, which is a joint venture between Giesecke&Devrient and Nokia, is an example of a neutral third party between the financial sector and MNOs. Its main purpose is to supply secure chip management services for NFC ecosystems and contacts with both parties. There is also a trusted third party in the Japanese NFC ecosystem, where a company named Felica Networks already acts as a centralised platform manager. In Japanese markets, mobile operators issue chips for end users' mobile devices.

For the global breakthrough of NFC-based mobile payment, it would be extremely important that both financial institutions and network operators could find viable business models that work together. Otherwise, NFC-based mobile payment is in danger to end up as just another failed mobile payment scheme.

6.1.5 EMV restrictions to the development of mobile payment systems

EMV (Europay, MasterCard and Visa) is a set of specifications for smart cards to ensure worldwide interoperability and acceptance between IC cards and terminals. The standard is managed, maintained and enhanced by EMVCo, which is jointly owned by MasterCard, JCB and Visa (EMVCo 2007).

One reason why acceptance of mobile payment has been so slow in Europe may be that European banks have just recently invested heavily in replacing old magnetic stripe cards with EMV cards. Merchants have also made modifications to the payment systems and are not willing to make big investments to new contactless technology for a while, unless they can see clear cost savings resulting from the migration to new system.

EMVCo is currently developing a new EMV contactless specification which is expected to be released in the second quarter of 2007 (EMVCo 2007). Leading card associations have not had the patience to wait for the specification and they have developed their own EMV contactless specifications. Giesecke & Devrient was first to introduce dual interface a contactless EMV card in Europe and terminal manufacturers have also come up with point-of-sale machines compatible with contactless EMV specifications developed by card associations. Dual interface cards, which include both contactless and traditional EMV smart card functionality, may lighten the deployment of the mobile payment systems in Europe. (Smart 2006)

6.2 NFC trials and roll-outs

In 2006 there were approximately 30 NFC trials running globally and several commercial rollouts were taking place in various locations around the world. The commercial success of NFC compatible mobile phone solutions has been most considerable in the Asia-Pacific region. In the United States, contactless payment with smart cards has shown significant success and development is rapidly proceeding towards contactless payment with mobile phones. Europe is also on the cutting edge of NFC development, but the majority of implementations are still at the piloting stage. In addition to these three most important regions of NFC development, also other countries all around the world (e.g. Lebanon, South Africa, Guatemala and Mexico) have recently piloted some NFC-related solutions.

Contactless payment and public transport/event ticketing pilots and roll-outs have attracted most consumer and media attention. In addition to those, several pilots have included service discovery applications, for example SmartPosters, but the consumer acceptance for the services provided has been only moderate. Connectivity applications to link two NFC-enabled devices easily together have been developed, but commercially available solutions are still waiting to be announced.

The year 2007 looks very promising from the viewpoint of NFC technology. Contactless infrastructure either exists or is developing in all regions. Since previous contactless payment and ticketing trials have provided promising feedback, numerous new trials are planned to be implemented and several new commercial roll-outs are

expected to take place. New NFC-enabled mobile phone models are expected to be released by several mobile phone manufacturers in 2007 and market penetration of NFC mobile phones is expected to speed up in next three years.

6.2.1 Asia-Pacific

Some of the countries in the Asia-Pacific region have been intensively driving NFC related FeliCa technology for several years. The first and one of the most well-known FeliCa applications is the Octopus card that has been used in Hong Kong as a public transportation payment card since 1997. Suica contactless payment system in Japan is another example of the widespread contactless infrastructure in the area. Both of these systems currently have millions of users and services have expanded to various other areas, such as retail stores, vending machines and access control.

Japan has also led the way in contactless payment with mobile phones. Japanese operators with NTT DoCoMo in the forefront have sold nearly 30 million mobile phones with contactless capabilities since 2004 and paying with those has gained wide acceptance. Millions of passengers and retail store customers are using their mobile phones for public transport ticketing and to pay small purchases. However, the fact that contactless payment applications in Japan use non-standardised FeliCa technology causes challenges to the use of contactless payment. A customer making contactless payment cannot be sure that the brand of his contactless payment instrument is accepted at that certain point-of-sale terminal. Agreements on interoperability between different payment schemes have been made, but there is still long way to go for total interoperability. Despite the difficulties, FeliCa is nowadays a basic functionality in new mobile phones by major mobile network operators. In Japan the penetration rate of mobile phones with the FeliCa chip reached 27% in November 2006. This wide penetration of mobile wallet phones enables a large customer base for payment and ticketing services. (Card 2007b)

There are also many other countries in Asia-Pacific region that have implemented NFC compatible applications. For example, China, South-Korea, Malaysia, Singapore, Taiwan and Thailand have either been piloting NFC/FeliCa applications or taken those into commercial use. However, the differences in technological development inside countries or between countries of the region are significant and where some country may be adopting a state-of-the-art technology, the other may completely lack the infrastructure needed for the services.

Public transport ticketing has been a main driver in adoption of FeliCa/NFC applications in Asia-Pacific region. Strong contactless infrastructure combined with

widely used wireless technology has smoothed the way to the adoption of mobile phone-based contactless payment systems. Another important factor in the deployment has been mobile phone operators' strong influence and huge investments in the contactless technology. Japan's biggest network operator NTT DoCoMo has pushed their mobile wallet services to customers with success and a recently formed consortium together with some competing payment platforms provide for an even more promising future for NFC related services.

6.2.2 North-America

Contactless payment has been the main driver of NFC/RFID development in North American consumer markets. Currently, there are several contactless payment programs in the United States with different companies. For example, three major credit card companies have their own programs: America Express (ExpressPay), MasterCard (PayPass), and Visa (Visa Contactless). All three products are based on the same ISO/IEC 14443 standard, which is also NFC compatible.

Contactless payment is already quite well spread in the United States By the end of 2006 there were over 18 million contactless chip cards in the market. In addition to card issuers, many national and regional retailers are advancing the use of contactless payment technology. For example, 7-Eleven and McDonald's have decided to start accepting contactless payments at all of their store locations in the United States.

There have been some trials (e.g. Philips Arena in Atlanta, New York Mobile Trial and two trials in Dallas) where contactless payment is handled with mobile phone (Nokia 3220). However, except for these trials contactless payment is not yet widely used via mobile phones. Instead, contactless credit and debit cards are gaining widespread acceptance and contactless payment tags that fit on key chains are also becoming more popular, especially in public transport systems.

6.2.3 Europe

In most European trials the main NFC application is either public transport ticketing or event ticketing; mobile payment and content downloading from SmartPosters are part of some trials, but those are not the main issue in most of the recently finished or currently ongoing trials.

Public transport ticketing trials or roll-outs have been conducted or are about to begin at least in the Czech Republic, Finland, France, Germany, the Netherlands, Norway,

Poland, Spain, and Great Britain. Public transport ticketing is now shifting from trials to commercial programs. Payment terminal infrastructure has developed notably in the last few years, which will make it easier to introduce contactless ticketing with mobile phones in the future. Ticketing using NFC-enabled mobile phones may also smooth the path of commercialisation of mobile phone based contactless payment in Europe.

Despite the fact that NFC-related public transport ticketing systems have already spread to a large group of cities, a contactless payment scheme has not yet gained popularity in Europe. The first European commercial roll-out aiming for large-scale contactless payment markets started recently in Turkey. Technology of this roll-out is based on MasterCard's PayPass. MasterCard and Visa have plans to soon introduce their contactless payment programs in other European countries, especially if final reports of contactless payment trials turn out to be as positive as they look at first sight. However, contactless is not currently a priority in Europe because of the market preoccupation with EMV implementation. Europe may have to wait for a while until countries are nearing the end of their EMV migration and are ready to start examining contactless opportunities (MPW 2006).

6.3 Industry perspective to NFC business models in the future

This section is based on interviews done on 10 and 15 October 2006, with different players in the NFC market. The interviewees represented different branches of the NFC industry, namely a hardware supplier, a technology manufacturer and an application user.

So far, RFID technology has been used primarily in Business-to-Consumer (B2C) for public transportation ticketing and in mobile payment and in Business-to-Business (B2B) to aid the mobile workforce. Especially in the latter, the use of NFC-compliant mobile phones has been eminent. It is hard to predict how RFID and NFC technology will be used in the future and how to get it to be a mass product. The people interviewed could not say with certainty how RFID will break through. In addition, their views on how NFC will become a commodity were opposed. On the one hand, it was believed that RFID and NFC will develop a bit in the same way as mobile phones did, i.e. first the professionals will start to use it and thereafter also the general public. In short, B2B products will bring the technology to the general public's knowledge, from which point it will be easier to break through to the B2C and other markets. On the other hand, it was also believed that in the future large user-volumes for RFID and NFC products will come from consumer products. Therefore at first, products will be developed for consumers, as it to some extent already has, and first then through B2C product success, business clients, i.e. professionals, will get interested in the product. In the end, it is

however believed that the significant financial profits will be gained from B2B and or B2E (Business-to-Employee) products.

At the moment the second hypothesis seems to hold ground. The present RFID- and NFC-based trials have concentrated on B2C applications. Despite this fact, the interviewees believe that in the future the demand for B2B products will increase. According to them the best economical benefits will be gained from B2B applications that concentrate on the mobile workforce, such as security, home care and maintenance. In these branches RFID applications can help with more accurate, real-time information and monitoring. So far the largest difference between B2C and B2B RFID and NFC products are that applications designed for consumers work so that the consumer has a smart card with an NFC tag or a mobile phone that has an NFC tag. In contrast to the consumer products, the applications for B2B usage usually work so that the mobile phone acts as an NFC or RFID tag reader. The interviewees believe that in the future this pattern might change, but in the near future it is very unlikely that mobile phones would have both NFC reader and tag capability. To gain both consumer and professional users, it is imperative that all the large mobile phone manufacturers put out mobile phone models with NFC capability, either tag and/or reader. The natural development would be that at some point there is no more need for smart cards, but mobile phones will take over their functionality and NFC will become one of the everyday user interfaces.

It is important that not all products have to be NFC compliant, as one of the interviewees pointed out. In some products it is even better that they are not built in accordance to the NFC regulations and standards, such as some medical applications. In some situations it is important that only authorised people are allowed to make changes to a tag's information, or even to read the tag. In a hospital environment this will minimise the risk of wrong information and breaches of the patient's medical confidentiality.

7. Discussion

Physical browsing is seen as a very significant user interface paradigm in the mobile domain. The paradigm can be divided into three sub-cases: Point me, Touch me and Scan me. RFID technology best serves the Touch me paradigm, where the action, such as information retrieval or payment, is initiated by touching a tag (or some other artefact) with the user's personal device. NFC technology embedded in mobile phones is by far the most promising implementation of the Touch me concept.

The NFC-based Touch me paradigm can find usage in many domains. Payment and ticketing applications are driving the development in the consumer market. Other applications, such as easy information retrieval, peer-to-peer communication, either using NFC or initiated by NFC as well as NFC-based sensors are expected to become popular after the consumer market adopts NFC technology first for payment and ticketing. Contactless payment has been a success in the United States and in parts of Asia. The contactless payment has most often been implemented with contactless smart cards, but it has also been integrated into mobile phones using NFC technology. In Japan contactless ticketing in mass transit has been widely adopted with the brand names FeliCa and Suica. The technology has also been integrated to mobile phones, although it is not fully NFC compatible.

Europe has been lagging behind in contactless payment in general, partly due to EMV specification and its implementation, which restricts the non-PIN code use of contactless payment. In some countries, like Finland, the ongoing introduction of smart cards and corresponding Point-of-Sale (POS) terminals will block introduction of new payment methods for some time, since retailers and consumers are reluctant to make new investments or to learn new ways. The adoption of NFC as a new payment method requires a business model which is acceptable for all relevant players: the retailers, restaurants and other service providers, financial institutions, mobile operators and consumers.

Perhaps the applications of NFC technology with the most potential in Europe in the short term can be found in mass transit companies and authorities, who have substantial experience of contactless tickets (smart cards) and who can push the technology to the customers if they see it in their interest. In this respect ticketing differs from payment, since ticketing is often a closed vertical case where as payment is more open and involves various stake holders with different interests.

The professional market differs from consumer markets in two ways: the market for a certain application is usually rather small compared to the consumer market and the use of a certain technology, such as NFC, can be mandated by the employer who sets up the

necessary infrastructure and supplies the users with the NFC compatible terminals. For this reason the first trials of NFC technology in Europe have been professional applications. So-called field-force solutions, used by security guards, janitors or cleaning personnel, have been pioneering in this respect.

Abi research, a market research company following the NFC market, projected in their 2004/2005 report that 50% of the mobile phones sold in 2009 would have NFC capability. The challenges encountered during 2006 caused Abi research to scale down their forecast to 30% of mobile phones having NFC in 2011. The main reasons for this development are the difficulties in finding a workable business model for NFC-based payments and the chicken-and-egg problem of NFC phones and NFC services, which has manifested itself in the delayed launches of NFC phones. At the time of writing (May 2007) Nokia had two models, 5140 and 6131, of which 6131 is not yet commercially available. Other manufacturers like Sagem and Samsung have NFC phone models with limited availability. However, in the Japanese market NFC-like phones are already popular.

Although the proliferation of NFC technology will come slower than was initially expected, this does not mean that it will not have a deep penetration in the market in the longer term. This can be compared to Bluetooth, which took severalyears (1998 – ca. 2005) to win acceptance, first from the manufacturers of digital devices and later from the users.

A window of opportunity for NFC Bluetooth gateways may exist during next couple of years, while NFC infrastructure is emerging, first in niche markets, and most mobile devices do not yet support NFC. VTT has developed a prototype of a gateway accessory which can act as a bridge between NFC-based infrastructure, such as tags, sensors, smart posters, and Bluetooth-enabled mobile devices.

8. Conclusions

We have discussed the concept of Physical Browsing, which aims at developing a new intuitive user interface paradigm especially for mobile users. When successful, this new paradigm could bring about a change in mobile Human-to-Computer Interface (HCI) similar to the one the graphical Web browser caused in the use of Internet, changing the restricted world of the Internet into the World Wide Web. The report focuses on the NFC technology, which is the most potential implementation of the physical browsing concept.

The NFC technology is based on existing RFID technology and standards. The relationship between the NFC to the underlying ISO/IEC and ECMA standards was discussed. The main applications of NFC can be divided into payment and ticketing, information retrieval, e.g. with the Smart Poster concept, and peer-to-peer applications, where NFC serves as an easy to use way of opening a communication channel between devices that are physically close.

The report discussed a pilot case, where the meal service for elderly people is made more efficient by the use of NFC technology. Further, the experiences of the users were analysed. The results of this pilot case were positive: the feasibility of ordering meals with a simple touch-based user interface was shown, and the non-technologically oriented users, i.e. elderly people, could use the solution successfully. This shows that NFC technology, when properly applied, can be used to decrease the Digital divide problem.

We also present a multi-functional platform, which can be used as gateway between NFC devices and Bluetooth-equipped mobile devices or as an NFC interface for non-NFC devices, such as sensors or medical measurement appliances.

The security and privacy aspects of all RFID-related technologies are very important if the trust of the users is to be won. The security of NFC technology is discussed in this report and some solutions are suggested.

The business interest in NFC technology stems from three major sources: payment, ticketing and professional applications. We deliberately distinguish between payment, which is a more open multi-player field, and ticketing, which is closed Business-to-Customer cases. Contactless payment (not necessarily using NFC but more often contactless smart cards) is gaining ground in the United States and many Asian countries, while Europe is lagging behind. We have identified three main business models depending on the key player: financial institutions, mobile network operators or other players, such as mass transit authorities, in the key role. Professional applications,

such as field-force solutions, are often justified by process improvements, e.g. real-time monitoring of work progress.

The forecasts for NFC proliferation, which were published in 2005, have been proven to be too optimistic. The growth of NFC usage has been hindered by the familiar chicken-and-egg problem: since there are no NFC-based services, consumers do not demand NFC-equipped phones and the manufacturers do not offer them and thus there is no incentive for infrastructure providers to use NFC. This vicious circle can be broken in closed business cases, such as mass transit ticketing or by the joint launch of NFC-based payment service by major financial institutions and retailers, restaurants, etc. Here we come to the critical question of business model: in the open multi-player case, all partners must have some interest (or necessity) in adopting the new technology before it can become established. In this sense the NFC adoption is more a business model question than it is a technical, user acceptance or security issue.

Acknowledgements

The financial support of Tekes (Finnish Funding Agency of Technology and Innovation) for the SmartTouch project is gratefully acknowledged. The support of ITEA2 organisation for the SmartTouch (ITEA No 05024) project is acknowledged. The authors wish to thank the other partners in the Smarttouch consortium, both Finnish and those from other European countries.

References

(Aarts 2003) Aarts, E. and Marazano, S. (eds.) The New Everyday: Visions of Ambient Intelligence. 010 Publishing, Rotterdam, The Netherlands, 2003.

(Ailisto 2003) Ailisto, H., Plomp, J., Pohjanheimo, L. and Strömmer, E. Physical selection paradigm for ubiquitous computing. In: E. Aarts et al. (eds.): EUSAI 2003. Lecture Notes in Computer Science, Vol. 2875. Springer-Verlag. Berlin, 2003.

(Ailisto 2006) Ailisto, H., Pohjanheimo, L., Välkkynen, P., Strömmer, E., Tuomisto, T. and Korhonen, I. Bridging the physical and virtual worlds by local connectivity-based physical selection. Personal and Ubiquitous Computing 10, 2006, pp. 333–344.

(Anderson 2001) Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2001.

(Bäckström 2006) Bäckström, C., Södergård, C. and Udd, S. A video processing method for convenientmobile reading of printed barcodes with camera phones. Multimedia Content Analysis, Management, and Retrieval 2006. Proceedings of SPIE. Vol. 6073. 2006.

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

(Bush 1945) Bush, V. As we may think. Athlantic Monthly, July 1945.

(Calvet 2005) Calvet, J. C. L. The Role of RFID in Mobile Phone. Telektronikk 3/4 2005, Telenor, 2005, pp. 131–142.

(Card 2007a) Card Technology. (14.2.2007) Mobile Operators Announce Payment Initiative (2007 Mar. 13), Available at HTTP: http://www.cardtechnology.com.

(Card 2007b) Card Technology. (13.4.2007) Japan's Mobile Wallets Fail to Inspire – Yet. (2007 April 16), Available at HTTP: http://www.cardtechnology.com.

(Choi 2006) Choi, Y. B., Crowgey, R. L., Price, J. M. and VanPelt, J. S. The state-of-the-art of mobile payment architecture and emerging issues. International Journal of Electronic Finance, Vol. 1, No. 1, 2006, pp. 94–103.

(EMVCo 2007) EMVCo. (2007 Mar. 13) Available at HTTP: http://www.emvco.com/.

(Haselsteiner 2006) Haselsteiner, E. and Breitfuss, K. Security in Near Field Communication. Workshop on RFID Security 2006, Graz, Austria, 2006.

(Keränen 2005) Keränen, H., Pohjanheimo, L. and Ailisto, H. (2005) Tag Manager: a Mobile Phone Platform for Physical Selection Services in International conference on Pervasive Services (ICPS 2005). Santorini, Greece. Pp. 405–412.

(Kindberg 2000) Kindberg, T. et al. People, Places, Things: Web Presence for Real World. In: IEEE Workshop on Mobile Computing Systems and Applications WMCSA'00, IEEE Press, 2000.

(Konidala 2006) Konidala, D. and Kwangjo, K. Mobile RFID Security Issues. In: The 2006 Symposium on Cryptography and Information Security (SCIS 2006). The Institute of Electronics, Information and Communication Engineers. Hiroshima, Japan, 2006.

(Krause 1998) Krause, M. and Tipton, H. Handbook of Information Security Management. Auerbach publications, 1998.

(Kreyer 2002) Kreyer, N., Pousttchi, K. and Turowski, K. Characteristics of Mobile Payment Procedures. In: Proceedings of the ISMIS 2002 Workshop on M-Services, Lyon, 2002.

(Ljungstrand 1999) Ljungstrand, P. and Holmqvist, L. WebStickers: Using Physical Objects as WWW Bookmarks. In: Extended Abstracts of CHI '99, ACM Press, 1999.

(Mallat 2005) Mallat, N. Mobility in Mobile Consumer Services. IRIS28, Kristianstad, Norway, 2003.

(MPW 2006) Mobile Payment World. 2006: the Year of Contactless. Q1, 2006.

(NFCForum 2006a) NFC Forum™, Smart Poster Record Type Definition. (Online technical specification), (2006 July), (2007 January 15), Available at HTTP: http://www.nfc-forum.org/specs/.

(NFCForum 2006b) NFC Forum™, NFC Forum Data Exchange Format Specification. (Online technical specification), (2006 July), (2007 April 4), Available at HTTP: http://www.nfc-forum.org/specs/.

(Nokia 2005) Nokia Corp. Nokia Secure Chip SDK 1.0 Programmer’s Guide rev. 1.0, 2005.

(Noll 2005) Noll, J. and Calvet J. C. L. SIM-card Enabled Access in Mobile and Broadband Access Networks. Wireless World Research Forum 15. Paris, France, 2005.

(Octopus 2007) Octopus (2007 Feb. 14) Available at HTTP: http://www.octopuscards.com/.

(Ondrus 2006) Ondrus, J. and Pigneur, Y. Towards A Holistic Analysis of Mobile Payments: A Multiple Perspectives Approach. Electronic Commerce Research and Applications. Vol. 5, Iss. 3, pp. 246–257.

(Ortiz 2003) Ortiz, C. E. An Introduction to Java Card Technology – Part 1. Sun Microsystems Inc., 2003.

(Rajala 2001) Rajala, T., Lahtinen, Y. and Paunio, P. Suurten kaupunkien 2. RAVA-tutkimus. Vanhuksien toimintakyky ja avun tarve. Suomen Kuntaliitto, 2001. (in Finnish)

(Rekimoto 2000) Rekimoto, J. and Ayatsuka, Y. CyberCode: Designing Augmented Reality Environments with Visual Tags. Proc. Designing Augmented Reality Environments (DARE 2000), ACM Press, 2000. Pp. 1–10.

(Rekimoto 2003) Rekimoto, J., Ayatsuka, Y., Kohno, M. and Oba, H. Proximal Interactions: A Direct Manipulation Technique for Wireless Networking, INTERACT 2003.

(Risikko 2006) Risikko, J. and Choudhary, B. Mobile Financial Services – Business Ecosystem Scenarios & Consequences. Mobey Forum. 2006.

(Rukzio 2006) Rukzio, E., Leichtenstern, K., Callaghan, V., Schmidt A., Holleis, P. and Chin, J. An experimental comparison of physical mobile interaction techniques: Touching, pointing and scanning. Proc. of Ubicomp, 2006.

(Siegemund 2003) Siegemund, F. and Flörkemeier, C. Interaction in Pervasive Computing Settings Using Bluethooth-enabled Active Tags and Passive RFID Technology Together with Mobile Phones. 2003. Proceedings of the First IEEE International Conference on Pervasive Computing and Communications.

(Smart 2006) Smart Card Alliance. Giesecke & Devrient Provides for the First Contactless EMV Card in Europe. (2007 Feb. 14) Available at HTTP: http://www.smartcardalliance.org/articles/2006/10/05/giesecke-devrient-provides-cards-for-the-first-contactless-emv-card-in-europe.

(Streitz 2001) Streitz, N., Tandler, P., Müller-Tomfelde, C. and Konomi, S. Roomware: Towards the Next Generation of Human-Computer Interaction based on an Integrated Design of Real and Virtual Worlds. In: J. Carroll (ed.): Human-Computer Interaction in the New Millennium, Addison-Wesley, 2001.

(Toye 2004) Toye, E. et al. Using camera-phones to interact with context-aware mobile servces. In: UCAM-CL-TR-609. University of Cambridge: Cambridge Press, 2004.

(Ullmer 1998) Ullmer, B., Ishii, H. and Glas, D. mediaBlocks: Physical Containers, Transports, and Controls for Online Media. In: Proceedings of SIGGRAPH '98, ACM Press, 1998.

(USOPM 2006) Handbook of Occupational Groups and Families. United States Office of Personnel Management, (2001 August), (2007 April 4) Available at HTTP: http://www.opm.gov/fedclass/text/GS-2200.htm.

(Want 1998) Want, R., Weiser, M. and Mynatt, E. Activating everyday objects. In: Darpa/NIST Smart Spaces Workshop, USC Information Sciences Institute, 1998.

(Weiser 1991) Weiser, M. The Computer of the 21st Century, Scientific American, September 1991.

(Välkkynen 2006) Välkkynen, P., Niemelä, M. and Tuomisto, T. Evaluating touching and pointing with a mobile terminal for physical browsing. Proc. of the NordiCHI, 2006. Pp. 28–37.

Published by

Series title, number and report code of publication

VTT Research Notes 2400
VTT–TIED–2400

Author(s)
Ailisto, Heikki, Matinmikko, Tapio, Häikiö, Juha, Ylisaukko-oja, Arto, Strömmer, Esko, Hillukkala, Mika, Wallin, Arto, Siira, Erkki, Pöyry, Aki, Törmänen, Vili, Huomo, Tua & Tuikka, Tuomo

Title

Physical browsing with NFC technology

Abstract

Physical browsing is a new intuitive human-computer interfacing paradigm for mobile users. Services, such as information retrieval, peer-to-peer communication, payment or ticketing, and professional applications can be initiated by simply touching an object with a user's personal device. This paradigm can be implemented with RFID technology. A number of major companies in the fields of mobile communications, electronics and financing have joined forces in an effort to commercialise this human-computer interaction paradigm with the brand name Near Field Communication (NFC). NFC is based on existing technology using 13.56 MHz RFIDs and international standards. The NFC forum is creating standards and recommendations for the upper level protocols and application models. VTT is leading a Europe-wide project which develops and pilots NFC technology. This report describes the findings and results of the first project year. The report outlines the concept of Physical browsing, NFC technology, its main applications, and describes a pilot case with a meal service for elderly people. An NFC Bluetooth gateway prototype has been designed and the first experiments are briefly described. Security and privacy issues relevant to NFC are described. The main business models, namely those driven by financial institutions, mobile operators or other parties are discussed. A look at major trials and roll-outs of contactless payment is given. Some solutions to the dilemma of scarce NFC services and low penetration of NFC phones are suggested.

ISBN
978-951-38-6946-5 (soft back ed.)
978-951-38-6947-2 (URL: http://www.vtt.fi/publications/index.jsp)

Series title and ISSN	Project number
VTT Tiedotteita – Research Notes 1235-0605 (soft back ed.) 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)	5197

Date	Language	Pages
August 2007	English	70 p.

Name of project	Commissioned by
Smarttouch	

Keywords	Sold by
RFID, Radio Frequency Identification, Physical browsing, Human Computer Interaction, HCI, CHI, contactless, payment and ticketing, NFC, Near Field Communication, peer to peer, ISO 14443	VTT Technical Research Centre of Finland P.O. Box 1000, FI-02044 VTT, Finland Phone internat. +358 20 722 4404 Fax +358 20 722 4374

Physical browsing is a new intuitive human computer interfacing paradigm for mobile users. Services, such as information retrieval, peer to peer communication, payment or ticketing, and professional applications can be initiated by simply touching an object with a user's personal device. This paradigm can be implemented with RFID technology, for example using so called Near Field Communication (NFC) technology supported by an industrial consortium. NFC is based on existing technology using 13.56 MHz RFIDs and international standards.

This report describes the findings and results of the first project year in a VTT led European research project on the subject. The report outlines the concept of Physical browsing, NFC technology, its main applications, and describes a pilot case with a meal service for elderly citizens. An NFC Bluetooth gateway prototype has been designed and the first experiments are briefly described. Security and privacy issues relevant to NFC are described. The main business models, namely those driven by financial institutions, mobile operators or other parties, are discussed. A look at major trials and roll-outs of contactless payment is given. Some solutions to the dilemma of scarce NFC services and low penetration of NFC phones are suggested.

Julkaisu on saatavana
VTT
PL 1000
02044 VTT
Puh. 020 722 4404
Faksi 020 722 4374

Publikationen distribueras av
VTT
PB 1000
02044 VTT
Tel. 020 722 4404
Fax 020 722 4374

This publication is available from
VTT
P.O. Box 1000
FI-02044 VTT, Finland
Phone internat. + 358 20 722 4404
Fax + 358 20 722 4374

ISBN 978-951-38-6946-5 (soft back ed.)
ISSN 1235-0605 (soft back ed.)
ISBN 978-951-38-6947-2 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)