

# NFC-BASED MOBILE MIDDLEWARE FOR INTUITIVE USER INTERACTION WITH SECURITY IN SMART HOMES

Zoe Antoniou and Dimitris N. Kalofonos  
Nokia Research Center Cambridge  
3 Cambridge Center  
Cambridge, MA, 02142, U.S.A.  
{zoe.antoniou, dimitris.kalofonos}@nokia.com

## ABSTRACT

Home networks and networked consumer electronic devices are increasingly becoming a part of our everyday lives. One of the challenges in designing smart home technology is making these systems secure and, at the same time, easy-to-use for non-expert consumers. We believe that mobile devices equipped with a “touch” network interface and corresponding middleware are ideal for enabling users to intuitively setup and manage the security of their smart homes. In this paper, we propose such a middleware for mobile phones based on Near Field Communication (NFC) technology. We propose a mobile middleware architecture based on a higher-level User-Interaction with Security (UI-SEC) middleware, called IntuiSec, and a lower-level NFC middleware, called *iTouch*. We present the proposed overall architecture, with particular emphasis on the integration modules, as well as, the detailed design of the necessary NFC records that are exchanged over RF. Finally, we present our experience with an initial implementation of parts of the proposed middleware using actual NFC hardware and Symbian-based mobile phones.

## KEY WORDS

Intelligent interfaces, intelligent ambience, intuitive user interaction, NFC, UI-SEC

## 1. Introduction

The wide availability of affordable wireless and wireline networking equipment has recently led to the rapid proliferation of home networks. Although their current usage is mainly limited to traditional computer applications (e.g. web browsing, printing, data backups), a number of standards and industry efforts [1], [2] are maturing that will enable networked home-entertainment applications, a step towards making “smart homes” a reality. Mobile phones have a central role in the user interaction with these environments because they are ubiquitous and personal, they have significant storage and computational capabilities, and they feature a multitude of connectivity options. Among their emerging network

interfaces, of particular interest is Near Field Communication (NFC) [3], because it adds an intuitive “touch”-based modality of user interaction. NFC is essentially based on Radio Frequency Identification (RFID) technology. NFC interfaces have a short operating range of a few centimetres and enable devices to exchange information over the RF medium. NFC-compatible tags have a modifiable state and can support capacities of several kilobytes.

As smart homes and networked applications increasingly become part of our everyday life, so do the network security threats and their potential impact. One of the main challenges in home network security is that its users are non-expert consumers, who have no background nor interest in understanding the relevant technologies. This leads to a growing problem whereby, no matter how sophisticated are the underlying security algorithms and protocols, home networks remain vulnerable because users either misconfigure or even do not use the security infrastructure at all [4]. Clearly, there is a need for solutions that enable an intuitive user interaction with security in smart homes.

In this paper, we propose an NFC-based middleware architecture for mobile devices, which enables them to be used by non-expert users to interact intuitively with security in their smart homes. The proposed architecture integrates *iTouch* [5], our NFC middleware for mobile phones, with IntuiSec [6], [7] our framework for intuitive user interaction with security (UI-SEC) in smart homes. We show through selected use cases how mobile devices implementing the proposed architecture can simplify the management of access control at the network and application level. We present in detail the middleware design and give our experience with a preliminary implementation on mobile phones.

The rest of this paper is organized as follows: in Section 2 we present references to related work; in Section 3 we describe in detail the proposed overall architecture and the design of the most important modules; in Section 4 we present the current status of the system implementation; finally, in Section 5 we present our conclusions.

## 2. Related work

There is growing recognition that there is a need to make security in pervasive computing environments easier to use [8]. In particular, although there are many proposals for smart home security (e.g. [9], [10]), the issue of usability can be very challenging for non-expert consumers. This has led to research to make existing home security mechanisms easier to use for non-experts (e.g. [6], [7], [11]), and standardization efforts, such as the work of Wi-Fi Alliance Easy Setup WG [12].

One of the most intuitive modalities to interact with smart devices and objects is through the use of “touch” interfaces (also known as Location Limited Channels LLC, e.g. infrared, RFID and NFC), e.g. as proposed in [5], [13], [14], [15]. LLCs are both intuitive and inherently secure channels and usage of infrared-based LLCs have been proposed to facilitate the user interaction with security [6], [7], [16], [17]. Use cases for NFC-based security initializations using mobile devices are considered in the NFC forum [3], but there are no proposals for NFC-based mobile middleware for security interaction with smart home security.

## 3. Middleware Architecture and Design

This section presents the middleware architecture and design. It focuses on the main features and key functionality exposed through the APIs.

### 3.1 Background

The NFC layer of the proposed architecture is based on iTouch [5]. iTouch is an NFC-enhanced middleware architecture for mobile devices that enables intuitive user interaction in smart spaces, easy service discovery and face-to-face sharing. It provides a layer of indirection between (a) a variety of proximity connectivity technologies (RFID, Infrared, Camera, Laser etc), and (b) user-domain applications and service discovery engines. Communication between the different layers is realized through APIs. In this paper, the only proximity technology used is NFC and data is formatted as NFC packets, also referred to as records. iTouch consists of one core module, Link Management layer, and multiple specialized modules. The Link Management layer provides the basic read/write, send/receive functionality, as well as, composition and parsing of the NFC records. Specialized modules can be added to perform dedicated tasks and add value to the middleware. In the proposed design there are three specialised modules: ‘out-of-band connectivity’, ‘iTouch service discovery’ and ‘iTouch security’.

The user interaction with the security layer of the proposed architecture is based on IntuiSec [6], [7].

IntuiSec is a framework that enables non-expert users to easily create secure home networks and interact with smart home security. IntuiSec provides a level of indirection between the concepts that users understand intuitively and the underlying security system settings through a middleware layer and user-level tools. The IntuiSec architecture provides the following functionality:

- *Easy Setup* – a process to take ownership of new devices and add them securely to the home network.
- *Build Trust* – a process by which users can intuitively establish trusted relationships between devices. This enables the user to securely authenticate and reliably verify the identity of a remote device.
- *Grant Access* – a process by which users can easily grant access to both home occupants and visitors to use devices that they own.
- *Security Visualization* – a set of API’s exposed by the framework to enable other applications to display security-related parameters using visualizations meaningful to non-expert users.

### 3.2 Architecture

The proposed middleware architecture is depicted in Figure 1.

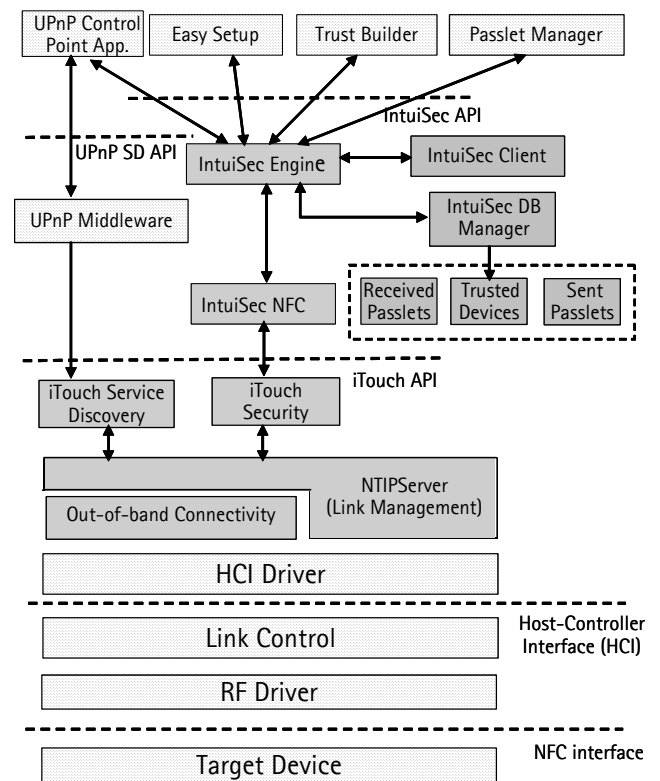


Figure 1 – Proposed middleware architecture.

Starting from the lower layers, a *Host Controller Interface (HCI)* driver resides on the mobile device and

communicates with an NFC transceiver unit over a USB interface. The Link Control layer on the transceiver performs the RF communication. The transceiver is controlled by the host via commands sent through the HCI driver. The design allows for the transceiver to be “armed” at the press of a button on the host, activating the RF layer. At all other times, the RF unit is in idle mode, thus conserving power. Data is exchanged in the form of NFC packets which are communicated over the air interface to target devices (send/receive) or tags (read/write). Target devices are enhanced with the same set of middleware tools.

The HCI driver interacts with the Link Management layer. In this layer, a variable length packet format is defined for the frames communicated over RF. This format is based on *NDEF* guidelines (*NFC Data Exchange Format, formerly called NTIP, NFC Transfer Interchange Packet*) as defined by the NFC Forum<sup>1</sup> [3]. The heart of the Link Management layer is the *NtipServer*. The *NtipServer* can manage multiple clients on the host device. It operates in the asynchronous mode, collecting requests from all clients. It uses a unique type string that binds each request to the client. Both applications and specialized middleware modules can act as clients, by registering with the *NtipServer* to receive specific record types. This allows clients to maintain a level of privacy and have complete control of the interpretation of the data. Record types are mapped to clients in an internal registration database.

Incoming NFC packets are received by the *NtipServer*. These packets can contain one or more records. The *NtipServer* parses them and extracts the NFC record(s). Next, it determines the destination of these records based on the registration database. In the reverse direction, client applications can use public functions exposed through the *iTouch* API to write to tags or send messages through the NFC interface. In this case, the *NtipServer* receives a set of data parameters through the API and composes an NFC record in the appropriate format before sending it over the air interface.

In the proposed architecture there is a specialized security module, named *iTouch Security*. This module provides an integration point with the *IntuiSec* security framework that utilizes proximity wireless technologies such as NFC to perform secure network setup and device discovery. This module is described in more detail in Section 3.4. Examples of other specialized *iTouch* modules are:

- *Out-of-band Connectivity module*: this module is designed to setup out-of-band network connections, such as WLAN or Bluetooth. It can declare its own record type(s). When such a record type is extracted

from an NFC packet in the Link Management layer, it is passed to this module where it is parsed, processed and the necessary steps are taken to establish the connection. In [5] the design and implementation for the WLAN case is presented.

- *Service Discovery module*: this module is designed to perform service discovery. Similar to the Out-of-band Connectivity module, it can, declare its own record type(s) that contain service discovery descriptions. In [5] the design and implementation of the SD module for UPnP service discovery is presented.

The bulk of the *IntuiSec* framework is implemented by the *IntuiSec Engine*. The function calls of the *IntuiSec API* that require sending and receiving information over the proximity wireless interface are asynchronous and constitute the TAPing protocol. It is a set of commands used by the *IntuiSec* tools to perform Easy Setup, build Trust and manage Passlets. All devices have a TAP server running on them that listens for incoming TAPs. The TAPing protocol is part of the *IntuiSec NFC* module and it is described in more detail in Section 3.3.

### 3.3 *IntuiSec NFC Module*

The *IntuiSec NFC* module is responsible for issuing outgoing commands and validating/consuming incoming commands and data. *IntuiSec* middleware and tools are agnostic to the specifics of the NFC communication and the tag record format. The *IntuiSec NFC* module uses a set of methods provided by the *iTouch Security* module to send and receive *IntuiSec* specific data (e.g. home IDs) and commands to the *iTouch Security* module. *iTouch* middleware performs all the NFC-related formatting and processing.

The *IntuiSec NFC* module implements the TAPing protocol. The first step in any and all TAPing transactions is for the devices to exchange and authenticate their respective HomeIDs. If the HomeIDs do not match, the transaction enters “unprivileged mode”, where certain requests are not honored (e.g. GET\_CONNECTIVITY\_INFO). If they match then the devices proceed with the requested transaction(s). The following TAPing commands are defined:

- HOME\_ID <homeID>: Sends the home ID to the TAPed device.
- GET\_CONNECTIVITY\_INFO: If the device making the request is authorized after exchanging the HomeID, the receiver of the request transfers a file containing 100 link keys to the requestor.
- CONNECTIVITY\_INFO: Sends the connectivity information as a response to the GET\_CONNECTIVITY\_INFO command.

---

<sup>1</sup> The names NDEF and NTIP are used interchangeably. NFC standardization is ongoing, hence naming conventions and record formats are still evolving.

- GET\_DEVICE\_INFO: Gets information of all UPnP devices residing on the physical device: DeviceID, OwnerID, HomeID, DeviceName, DeviceType.
- DEVICE\_INFO: Sends the device information as a response to the GET\_DEVICE\_INFO command.
- PASSLET <passlet>: Sends a passlet to the TAPed device. Currently passlets are sent in plain text and consist of: UserID, DeviceID, DeviceName, ExpiryTime, PermissionLevel, and DeviceType.
- The remaining commands are OK, ERROR, UNAUTHORISED, DONE and CLOSE

Based on an incoming command, this module invokes the appropriate actions in the IntuiSec Engine.

### 3.4 iTouch Security Module

The iTouch Security module implements the following public functions available through the API:

- SetCommand(TUint8 aCommand): this method passes a command from the IntuiSec NFC module to iTouch in order to be sent.
- SetPasslet(TIntuiSecPasslet aPasslet): this method passes a passlet from the IntuiSec NFC module to iTouch in order to be sent.
- SetHomeID(TIntuiSecHomeID aHomeID): this method passes the HomeID from the IntuiSec NFC to iTouch in order to be sent.

This module defines its own record type ‘IntuiSec’ or ‘IS’. Incoming ‘IS’ records are received from the Link Management layer and are parsed to extract the IntuiSec commands and data. These are then passed to the IntuiSec NFC module. Likewise, it packages outgoing commands and data into an ‘IS’ record and transmits it over the RF interface.

### 3.5 IntuiSec NFC Record Definition

The proposed NFC tag record design is a flexible and extensible structure that can be used to exchange the IntuiSec commands and data in a variety of use cases (Figure 2). The information exchanged is the Payload. The Payload contains a Header and a record list with one or more records. The Header contains the length of the Payload and it is used to determine how much data must be read from a tag. Each record is a sequence of three elements, a triplet of (*Type*, *Content-Length*, *Content*). The record *Type* identifies the structure and semantics of the record by providing the *Type* name. The *Content-Length* identifies the length of the record *Content*. The record *Content* contains the actual data.

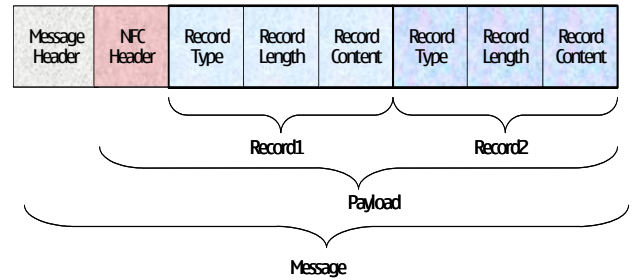


Figure 2: The basic tag structure.

An IntuiSec record type is defined as ‘IS’. For each ‘IS’ record, there is a sub-record containing one of the TAPing commands. Further data sub-records are defined to convey parameters relevant to each command (e.g. “psl” for passlet data or “hid” for the homeID). These data sub-records can follow the same triplet structure: (Type, Length, Content). The command sub-record can either follow the triplet structure or it can be defined as the first byte to follow the “IS” type declaration (this is the format assumed in this section). The tag record format for all the current IntuiSec transactions is listed in Table 1.

Record type	Sub-record type	Data sub-records [type, length, content]
IS	HomeID	[hid, hidLength, <homeID>]
IS	GetConnectivityInfo	
IS	GetDeviceInfo	
IS	ConnectivityInfo	[dn, dnLength, <DeviceName>] [mac, macLength, MACaddress>] [ct, ctLength, ConnectivityType>] [lk, lkLength, <LinkKeys>]
IS	DeviceInfo	[did, didLength, <DeviceID>] [dn, dnLength, <DeviceName>] [hid, hidLength, <homeID>] [oid, oidLength, <ownerID>] [dt, dtLength, <DeviceType>]
IS	Passlet	[uid, uidLength, <UserID>] [un, unLength, <UserName>] [did, didLength, <DeviceID>] [dn, dnLength, <DeviceName>] [et, etLength, <ExpiryTime>] [per, perLength, <Permissions>] [dt, dtLength, <DeviceType>] [pid, pidLength, <PassletID>]
IS	Ok	
IS	Done	
IS	Error	
IS	Unauthorised	
IS	Close	

Table 1: Tag formats for IntuiSec commands.

## 4. Prototype implementation

The implementation results presented in this section are work-in-progress and include a subset of the proposed architecture described in Section 3. The implementation of the system builds on prototypes we have developed in

projects iTouch [5], IntuiSec [6], [7], and Smart Sleeve [18]. Software components were developed for Symbian-based Nokia mobile phones, such as the Nokia 9500 Communicator and the Nokia 6620 Smartphone. The hardware support for the NFC interface is provided by a smart sleeve with an NFC add-on module [18]. A demonstration of the experimental setup of the system is depicted in Figure 3.



Figure 3 – A demonstration of the experimental setup.

Part of the demonstration tools is an application, called iTouchConfig, which provides basic functions such as starting and stopping the NtipServer, reading from and writing to an RFID tag, sending to and receiving from another NFC-enabled device. In addition, an RFID hot-button has been implemented to arm the RFID reader before each reading action.

One of the scenarios possible with the current implementation is setting up a new mobile device to become part of the home network. This is part of the Easy Setup process described in [6]. In Step 3 of this process, the user “touches” with the NFC interface of his mobile phone that of the Network Access Point (NAP) and establishes permanent connectivity for the phone to the home network. This one-touch action from the user triggers a series of steps in the middleware. Once the user TAPs the NAP, the IntuiSec NFC module issues the following outgoing request command ‘GET\_CONNECTIVITY\_INFO’. This is passed to the iTouch Security module through the SetCommand(GET\_CONNECTIVITY\_INFO) method of the iTouch API. iTouch Security module packages it in the following record: [IS][GET\_CONNECTIVITY\_INFO] and passes it to the Link Management layer where it is further formatted with the necessary headers. Then it is sent through the HCI to the RF interface. The NFC packet is received by the NAP and forwarded through the middleware in the reverse order where it is finally received by the NAP IntuiSec NFC module. Provided that HomeID authentication

succeeds, it issues a ‘CONNECTIVITY\_INFO’ reply command with the appropriate data parameters. The command and data are formatted into an NFC reply packet in the same fashion as the request packet and sent back to the mobile device. An example demonstration of this step for a WLAN NAP with SSID = ‘LitePad’ is shown in Figure 4. Once the NAP connectivity information is received by the mobile device, an information box pops up announcing the new WLAN network and ‘LitePad’ is added to the list of available wireless networks on the device.

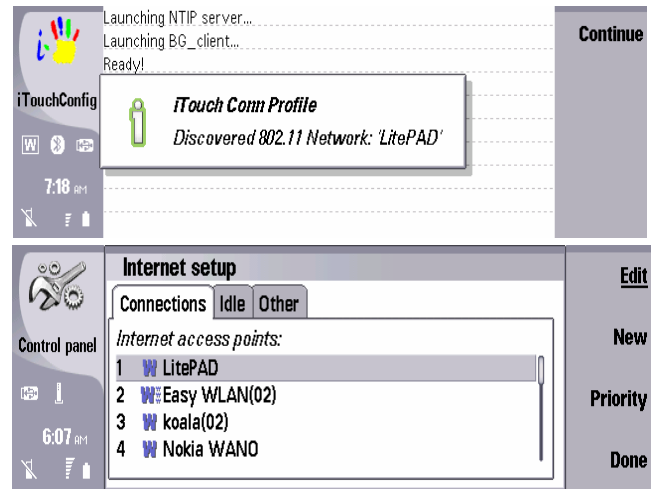


Figure 4 – Using NFC to establish connectivity to the home network.

Another example of what is possible with the proposed architecture is the use of NFC-based touch to grant access to a visitor to services provided by one of the home devices, e.g. a printer. The user interaction in this case is depicted in Figure 5 where a snapshot of the GUI of the “Passlet Manager” user-level tool is also shown.

The user launches the “Passlet Manager” tool and creates the passlet he/she wants to grant to the guest. The tool then prompts the user to TAP the guest device. At this point, the following takes place. The IntuiSec NFC module issues an outgoing command ‘PASSLET’. It uses the SetCommand(PASSLET) and SetPasslet (<passlet\_data>) methods of the iTouch API to pass the command and passlet\_data to the iTouch Security module. Command and passlet\_data are then packaged in the following record [IS][PASSLET][<passlet\_data>] with the passlet parameters as listed in Table 1. The record is passed to the Link Management layer where it is further formatted with the necessary headers before it is sent through the HCI to the RF interface. The NFC packet is received by the guest device and forwarded through the middleware in the reverse order. The command and data are received by the IntuiSec NFC module and added to the ‘Received Passlets’ database. An information box pops up announcing the new passlet to the guest.

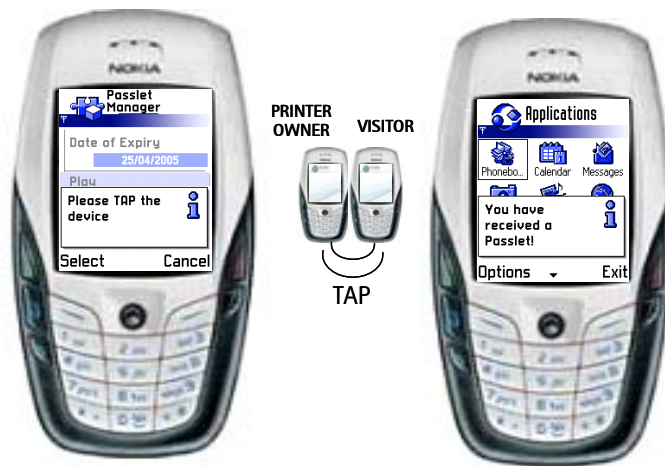


Figure 5 – User interaction for granting access to a visitor to print.

## 5. Conclusions

In this paper we presented a middleware architecture which enables mobile devices to leverage the inherent properties of NFC and allow consumers to intuitively interact with security in smart homes. Our middleware architecture is implementable using today's smartphones and NFC hardware. We believe usage of mobile phones with NFC interfaces can contribute significantly in improving smart home security usability. However, this would require other players in the industry, such as computer, network equipment, and consumer electronics manufacturers to also widely adopt NFC and work together towards standardizing a common middleware framework for interoperability.

## Acknowledgements

Special thanks to Srikant Varadan, Saad Shakhshir and Marios Michalakis for their contributions to the iTouch, IntuiSec, and Smart Sleeve projects respectively during their internships at Nokia Research Center.

## References

- [1] Universal Plug-and-Play (UPnP) Forum, *UPnP Device Architecture 1.0.1*, December 2003.
- [2] Digital Living Network Alliance (DLNA), *Digital Living Network Alliance Home Networked Device Interoperability Guidelines Expanded*, March 2006.
- [3] NFC Forum, [www.nfc-forum.com](http://www.nfc-forum.com)
- [4] Chris Hurley, Michael Puchol (Editor), Russ Rogers, Frank Thornton, *WarDriving: Drive, detect, defend, a guide to wireless security* (Syngress, 1st edition, 2004).
- [5] Z. Antoniou and S. Varadan, iTouch: RFID middleware for boosting connectivity and intuitive user

interaction in smart spaces, *Nokia Research Center Technical Report (NRC-TR-2006-002)*, May 2006. <http://research.nokia.com/tr/NRC-TR-2006-002.pdf>

[6] D. Kalofonos, IntuiWare security functional specification, *Nokia Research Center Technical Report (internal)*, April 2004.

[7] S. Shakhshir and D. Kalofonos, IntuiSec: a framework for intuitive user interaction with smart home security, *Nokia Research Center Technical Report (NRC-TR-2006-003)*, April 2006.

<http://research.nokia.com/tr/NRC-TR-2006-003.pdf>

[8] P. Dourish, R. Grinter, J. Delgado de la Flor, and M. Joseph, Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6), 2004, 391-401.

[9] C. Ellison, Home network security, *Intel Technology Journal*, 6(4), 2002, 37-48.

[10] H. Nakakita, K. Yamaguchi, M. Hashimoto, T. Saito, and M. Sakurai, A study on secure wireless networks consisting of home appliances, *IEEE Trans. on Consumer Electronics*, 49(2), 2003, 375-381.

[11] S. Shakhshir and D. Kalofonos, Usable Security in Smart Homes, *Proc. of the 8th Inter. Wireless Personal Multimedia Comm. Symp. (WPMC'05)*, Aalborg, Denmark, 2005.

[12] Wi-Fi Alliance (WFA), [www.wi-fi.org](http://www.wi-fi.org)

[13] Z. Antoniou, G. Krishnamurthi and F. Reynolds, Intuitive service discovery in RFID-enhanced networks, *Proc. of IEEE COMSWARE Conference*, India, 2006.

[14] J. Riekkki, T. Salminen and I. Alakarppa, Requesting Pervasive Services by Touching RFID Tags, *Pervasive Computing Magazine*, 5(1), 2006, 40-46.

[15] T. Pering, R. Ballagas and R. Want, Spontaneous Marriages of Mobile Devices and Interactive Spaces, *Communications of the ACM*, 48(9), 2005, 53-59.

[16] D. Balfanz, G. Durfee, R. Grinter, D. Smetters, and P. Stewart, Network-in-a-Box: how to set up a secure wireless network in under a minute. *Proc. of 13th USENIX Security Symposium*; San Diego, CA, 2004, 207-222.

[17] D. Balfanz, D. Smetters, P. Stewart, H. Chi Wong, Talking to strangers: authentication in ad-hoc wireless networks. *Proc. of the Network and Distributed Systems Security Symp. (NDSS'02)*, San Diego, CA, 2002.

[18] M. Michalakis, D. Kalofonos, Shafai B., An experimental hardware extension platform for mobile devices in smart spaces, *Proc. International Conference on Pervasive Systems and Computing (PSC'06)*, Las Vegas, NV, 2006.