The Smart University experience: A NFC-based ubiquitous environment

Departamento de Tecnologías de la Información y las Comunicaciones
Universidad Politécnica de Cartagena
Cartagena, Spain
{mvictoria.bueno, pablo.pavon}@upct.es

Abstract—EHEA guidelines are promoting the modernization of the universities all over Europe, focusing on the implementation of new technologies to get services offered by universities closer to society. With this idea in mind, the Technical University of Cartagena is deeply involved in the development and implementation of the so-called Smart University model: a ubiquitous computing platform based on NFC, where NFC devices and applications interact with each other to provide an intelligent environment. Before dealing with this ambitious project, a study to know the impact of the NFC technology in the university society was carried out. Positive results encouraged the idea of the Smart University, and two innovative NFC projects have been addressed: a NFC-attendance-registering-system and a NFC-administrative-fees-payment-system.

Keywords—EHEA, Smart University, RFID, NFC

I. INTRODUCTION

The European universities are involved in significant changes to adapt themselves to the current European directives in educational matters, the European Higher Education Area (EHEA) [1]. The goal is to create more comparable, compatible and coherent systems of higher education in Europe. Besides the curricula adaptations and changes in the teaching model, the EHEA guidelines imply the modernization of the University through the full implementation of new technologies in all university areas. The goal is to create a technological environment where students, teachers, university facilities and resources, etc., interact in a “natural” way under a ubiquitous computing environment, the so-called Smart University.

Near Field Communication (NFC) is an emerging technology which is becoming a possible candidate to fit the requirements of the implementation of the future Smart University [2]. This technology combines a wireless proximity communication technology with mobile phones and allows the simple, easy and almost unaware user interaction with the smart computing elements of the environment by simply “touching” them, thereby adding new value to mobile phone users.

The Technical University of Cartagena (UPCT) has promoted an ambitious project to create the UPCT Smart University, developing and implementing different NFC applications with two goals: First, to create a ubiquitous computing system where relationships between people, practice and technology happen as a part of a natural “touching” interaction paradigm; and the interaction in the environment is realized by bringing the mobile device into contact or very close to smart objects [3]; Second, to provide University with revolutionary applications that replace some of those rudimentary tasks that cause teachers, students and personal staff to spend time daily.

In this paper we present some of the innovative NFC projects in which we are working on: a NFC-attendance-registering-system to control the attendance in practice and theory lessons at University and a NFC-payment-system, to speed up administrative fees at University. These applications are being developed, implemented and tested in the facilities of the Telecommunications Faculty at UPCT. In this work, we also summarize a preliminary research we addressed to study the impact of NFC technology in a university environment. This research was aimed at finding out the degree of penetration and acceptance by users of mobile communications, hardware and software requirements, concerns about security and privacy, etc.

The paper is organized as follows: section 2 overviews the NFC technology. Section 3 summarizes the results of the study we carried out to know the impact of NFC technology in the university society. Section 4 describes the current NFC pilot projects in which we are working on. Finally, section 5 concludes.

II. THE NFC TECHNOLOGY

Near Field Communication (NFC) is an emerging technology based on Radio Frequency Identification (RFID) [4] that combines wireless proximity communication with mobile devices. NFC users interact with the smart computing elements of their surroundings by simply “touching” them with their NFC-enabled devices, like mobile phones, proximity cards, etc. On the proximity, NFC devices set up a P2P connection and exchange configuration and authentication data. The devices could engage in transactions using any of the compatible protocols or set up
a connection using faster and longer range protocols like Bluetooth, IrDA or Wi-Fi. Thereby, NFC turns mobile devices into more valuable tools by providing them with additional applications.

NFC operates in the 13.56 MHz frequency band, allowing data communication over a distance up to 20 cm and data rates up to 424 kbps. NFC is compatible with current standards for contactless communication and supports two communication protocols: NFC Interface and Protocol NFCIP-1 [5] and NFCIP-2 [6]. A built-in NFC chip can operate both as a contactless card and as a contactless reader, making the standard very suitable for device identification and communication initialization. Because the transmission range is quite short, NFC-enabled transactions are inherently secure. Also, physical proximity of the device to the reader gives users the reassurance of being in control of the process.

Depending on the final application, NFC makes use of different devices: mobile phones to enable payments, digital cameras to send their photos to other device like a TV with just a touch, etc.

The huge incorporation of NFC technology on mobile phones and the availability of them to final users is a matter of a short time, as Fig. 1 predicts. This is the reason why in recent years several pilot projects using NFC mobile phones are being conducted for very different proposals [7-10].

### III. THE IMPACT OF NFC TECHNOLOGY ON THE UNIVERSITY SOCIETY

The project of a Smart University cannot be addressed if the acceptance of university society is not sufficient. Hence, the first step is to know the impact of the use of NFC technology in a university environment. Under this idea, a deep study was carried out, finding out the impact of NFC technology in the university society (teachers, students and personal staff); the degree of penetration and acceptance by users of mobile communications; the hardware and software requirements; the concerns about security and privacy; and the technological impact.

The study was carried out with an opinion poll. Twenty five questions were designed to know, from demographic data and general questions about the knowledge of NFC, to more specific questions focused on the usability of NFC applications in different university facilities, or secure payments with NFC. From the UPCT, two hundred and fifty people were polled, the 3.5 % of the total population. In this work we only overview some of the most significant questions and their results. Questions are summarized in Table I and results in Fig. 2.

Results in questions 3 and 4 show the 70% of the university population has one last generation mobile, but almost the same percentage does not know anything about NFC. Results in question capture the acceptance in the use of one of NFC applications projected to be implemented in the UPCT, with more than 90% population that agrees with the idea of using a NFC attendance registering system. Questions 23 and 24 wants show if the university society is confident with the use of NFC for payments, and its security, thinking in the idea of implementing a NFC-administrative fees payment system at UPCT. Results show that around 70% of the population is confident. The result is as we expected, because society is still afraid of the security issues in payments with mobile communications. Lastly, results in question 25 show the good acceptance of NFC in the university society, if this technology is adopted in the UPCT.

From the whole results we extracted as a conclusions that, although in general university society does not know NFC, there is a positive interest in the implementation of NFC applications in the University. In fact, if NFC is consolidated as a stable technology, even people would be willing to update their mobile phones with the aim of using NFC. However, even though results are quite positive, a 79% of the polled people are afraid of security and possible bank commissions in the NFC bank payments. Results felt us confident to address the project of the UPCT Smart University.

![Figure 1. Evolution of NFC enabled phones in million units, by HIS](image)

<table>
<thead>
<tr>
<th>Question number</th>
<th>Question description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Do you have a 3G or 3.5G mobile phone?</td>
</tr>
<tr>
<td>4</td>
<td>Do you know about NFC technology?</td>
</tr>
<tr>
<td>11</td>
<td>Imagine you can control the attendance register (teacher) or confirm your attendance (student) in a lab/room automatically, only by touching your mobile phone with a reader, placed in the PC of the room. Is it easier and more comfortable for you?</td>
</tr>
<tr>
<td>23</td>
<td>If you have a NFC mobile phone, Are you confident to use it for payments?</td>
</tr>
<tr>
<td>24</td>
<td>Do you think that NFC is, in general, a secure technology?</td>
</tr>
<tr>
<td>25</td>
<td>Do you think NFC technology could be quickly extended if people know it?</td>
</tr>
</tbody>
</table>

Table I Some questions of the poll designed to collect the opinio about the use of NFC in a university environment
IV. THE UPCT SMART UNIVERSITY

Different NFC projects are being carried out at UPCT to create the Smart University. All projects are executed under the same hardware and software. The hardware components of the Smart University system architecture are:

- **NFC-enabled active devices**, which run the client software applications and store user information. Two different models are used: Nokia 6212 NFC Classic and Samsung Nexus S.

- **NFC-enabled passive devices**, which only keep specific info (a URL, vCard, text, jpeg image, etc.) Three different tags are used: Topaz, Touchatag and Nokia.

- **NFC readers: hardware devices** which allows the communication between NFC users and the UPCT servers. The reader is the mediator which allows the NFC users to interact with the system, that is, this device acts as a middleware of the system. This device is in direct connection with the NFC server host. The ACS-ACR-122U NFC readers are used.

- **NFC server hosts**, which are attached to the university network and handle the communication link with the NFC readers. These hosts execute the server software applications and provide access to the readers. The applications receive and execute users’ commands. Some applications will open connections to the DBMS (Data Base Management System) and LDAP (Lightweight Directory Access Server) university servers.

The adopted strategy for the software development has been to use open-source tools, meeting this way the non-functional requirement of minimizing economic costs. The use of Agile Methodologies [11] perfectly fits to these projects due to several factors: i) the novelty of the NFC technology usage and the new programming issues related to mobile phones, ii) the presence of unstable software requirements, iii) the reduced development staff and iv) the tight delivery deadline. The most popular methodology nowadays within this group is Extreme Programming (XP) [12], which constitutes an agile methodology focused on promoting interpersonal relations as the key to success in software development. XP is especially aimed at those projects with small development teams, with short deadlines, volatile requirements, and/or based on new technologies.

Under the same development methodology, we have developed the projects under the two most extended O.S. in the mobile phone market: Windows Mobile and Android. Under these O.S. we developed the applications using the software programming languages Java (J2ME and J2SE), and Android.

In the following subsections we review some of the projects which are being developed and implemented in the UPCT facilities.

A. NFC-attendance-registering-system

In the UPCT, the attendance in practice lessons labs is obligatory, and sometimes in some theory lessons. Practice lessons take place in labs, most of them with a computer for every two students. Theory lessons take place in rooms with a single computer in the teacher’s table. The current system to register the student attendance is as follows: some teachers do it manually, writing the attendance in a piece of paper, a computer or PDA. It forces teacher to ask, one by one, all students in the room, spending a lot of time when the number of students per room/lab is high. In other cases, teacher put a piece of paper in the room, and students write their attendance directly, provoking some students can trick the system, writing the name of other students that could not attend. In those labs with computers, a web system is used. Students register themselves, accessing to a webpage where they have to log, using the login and password that the University gives to every student. In this case, students can also impersonate other students.

The goal of the NFC-attendance-registering project is to create an innovate NFC system to change the way the students register their attendance, making faster the registration and being sure that students will not trick the system. The infrastructure of the proposal is shown in Fig. 3. In every room/lab, there is a NFC-reader connected to a PC, which is connected to the UPCT network. In this network there is a LDAP and DBMS server. The former stores in a database the credentials (login and password) of UPCT users (teachers, students and personal staff), The DBMS server stores the practices and theory database scheme at the UPCT.
Teachers and students are actors of this system through their NFC mobile phones. They access to the NFC system through their NFC phone application, previously installed for that purpose. The applications can be downloaded from the faculty web page, requiring authentication by UPCT LDAP.

Students have a different version from teachers, as can be seen in Fig. 4 and 5. In the former, students can configure their personal data and language. The last option is only selected when the registration takes place, where the students introduce their login and password. Note that these data are not stored in the phone memory to keep the student data security. In the teachers’ version, there are two new options: to activate a group and to list the attendees. In the former, the teacher has to log, indicating which group wants to activate. Note that in UPCT every theory and practice group is registered in the DBMS server with a code, which is known by teachers. The last option permits teachers to list the students in a group that were registered successfully.

The way the NFC system works in a typical registering attendance is as follows:

- First, the teacher enters in a lab/room, put the mobile phone in the NFC reader proximity, the NFC teacher application is automatically run. In a few seconds, the teacher can activate the corresponding group, filling the gaps in the applet. When the teacher pushes enter, the NFC reader receives data, and sends them to the LDAP server, to check the teacher’s login and password. If the authentication is right, the NFC reader sends the activating group order to the DBMS server, which sends the confirmation back to the NFC reader, and it sends it to the teachers’ mobile phone.

- When students enter the room, the group must be activated by the teacher. Students put their mobile phones in the NFC reader proximity, and the NFC student’s application run automatically. The students select the register option, fill their login and password, and keep waiting the successful registration. As in the teachers application, the data travels through the NFC reader to the LDAP server to confirm the students authentication, and then to the DBMS to register the attendance of the activated group. Note that students does not know the name of the group, this information is stored in the NFC reader in the moment a group is activated, and it is sent, together the student’s info, to the DBMS, to confirm the registration.

The pilot testing experiences saw that the gain in terms of saving time in lessons and the technology performance were satisfactory. Besides, students were not able to trick the system because the system was designed to avoid a single mobile can register twice in the same group session. On the other hand, we are really convinced that those students that do not attend lessons do not give their mobile phone to other students to trick the system, because students are not confident with the idea of giving their mobile, with personal and private data, to others.

B. NFC administrative fees payment system

The current payment of administrative fees at UPCT (such as matriculation charges, transcripts of records issuing, certified documents, or extra-curricular activities, etc.) involves the following steps:

- A student goes to the secretariat of the faculty to query about the payment. The secretariat staff checks the student data, and print three copies of the administrative fees to pay. Then the student must go to the bank that maintains an agreement with the UPCT to pay the fees.

- Once the student pays the fees, the bank stamps the three copies: one of them is required by the bank, the other one is required by the university, and the third one is for the student. After that, the student must go back to the secretariat to deliver one of the copies.

- The student arrives again to the secretariat, delivers the copy, and the secretariat staff proceed to finish the fees payment.
As can be seen, this rudimentary payment system could be improved using NFC, providing an online payment process in secretariat. This will save time to students, banks and university staff. Hence, the purpose of the NFC system suggested is to allow students to perform administrative payments immediately, just by touching with their mobile phones a NFC reader placed in the secretariat concerned (see Fig. 6). The infrastructure of this system requires a NFC reader connected to the secretariat PC, which is also connected to the secretariat server, where the secretariat NFC application is stored. The UPCT network must be connected to the Internet (by wired or wireless connection), to communicate with the bank server. The NFC system also communicates with the LDAP server, because it stores the students’ bank data: credit card and bank account numbers.

People paying fees in secretariat are the actors of this system through their NFC mobile phones. They access to the NFC system through their NFC phone application, previously installed for that purpose. This application can be downloaded through a smart-poster, placed in the main door of the secretariat. The smart poster has a NFC tag that stores a URL where the application is available.

A successful administrative fees payment with NFC is as follows (see Fig. 7):
- A student that needs to pay any fees goes to the secretariat and the secretariat staff serves the request in a PC with a NFC server.
- Once the secretariat staff configures the payment, the student put the mobile phone in the NFC reader proximity, and the application is automatically run, requiring the student’s login and password.
- Student enters the required data and they travel through the NFC reader to the UPCT LDAP server to confirm the student authentication.
- If the authentication is successful, the application shows two options: Confirm payment and Settings
d. Pressing the former, the secretariat server sends, by the NFC reader to the student’s mobile, the payment concept and the total amount to pay.

Note that, the student data security is kept since the login, password and secret numbers are neither stored in the phone memory nor in the secretariat server.

Data sent between NFC mobile phone and NFC reader are always encrypted, as well as data sent between secretariat server and bank server. Java language provides digital certificates and signature management as well as the following cryptographic operations: Hash functions such as MD2, MD5 and SHA-1; and asymmetric encryption RSA, symmetric DES, triple DES, AES, etc [13]. In this project SHA-1 and AES is used.

We would like to remark that in this work only the successful payment is described, but the application has been designed to face different problems and cancelations, both in the student and bank side: maximum number of attempts of secret number, user cancelation in any step of the process, invalid credit card, blocked credit card, etc.

A first version of the application is already in testing process, but only the bank account transaction is available. Payments with credit cards are pending due to the agreements between the UPCT, the bank and the credit cards companies. The UPCT only has agreements with two Spanish banks and it can order bank account transactions without problems. However, the communication protocol designed in this project emulates a user paying fees with a credit card, being the UPCT the entity that orders the charge to the bank. This mechanism is bit more complex, and requires new agreements between the bank and the credit card companies.

---

1 The first time the student uses the application the “Confirm payment” option is not available, and the user is forced to press “Setting” option to fill the required data for transactions: credit card number, CVV, bank account number, language, type of notification after a transaction (by SMS sent by the bank, monthly in a bank statement, etc.). This info is encrypted and sent from the user mobile to the LDAP server, via NFC reader and Secretariat server. This info only travels through the University network.
C. Other NFC developments in working process

Other ambitious projects are being studied and developed to be implemented in a near future in the UPCT facilities:

- **NFC-access control system.** This system will allow the university staff to open the doors of the dependencies to which they have granted access, by simply touching with their mobile phones an NFC reader on the door. The reader, connected to the university network, will handle the queries to the LDAP database that contains all the information about users, dependencies and permissions granted. The authorization will be obtained when the mobile user has access to that dependency. If so, the door will open using a relay circuit.

- **NFC library at UPCT.** This system will allow all the university members to perform the loan of didactic resources (books, software, and magazines) in two simple steps: i) the user, touching an NFC tag placed on a book, captures the book data, and then ii) the user touches an NFC reader of the library as a final step to perform the loan. The reader will be connected to the UPCT library database, that stores all the information about loans, users, and expiration dates of loans.

V. CONCLUSIONS

The modernization of Universities through the new technologies is one of the EHEA guidelines. The UPCT is intensively working on it with the aim of creating a technological environment where students, teachers, university facilities and resources, etc., interact in a natural way under the ubiquitous computing environment using NFC technology. This ambitious project, called UPCT Smart University, involves the development of several NFC applications. Two of them are overviewed in this work: a NFC-attendance-registering-system to control the students’ attendance in practice and theory lessons and a NFC-payment-system, to speed up administrative fees at the University. A preliminary study that authors carried out to know the impact of the massive use of NFC in a university environment is also summarized. The results of this research showed a positive interest in the implementation of NFC applications in the University. And the first testing experiences of the applications presented in this work encourage the success of the UPCT Smart University project we are carrying out.

ACKNOWLEDGMENTS

This work has been partially supported by the MICINN/FEDER project grant TEC2010-21405-C02-02/TCM(CALM) and the framework of the project from Fundación Séneca “Programa de Ayudas a Grupos de Excelencia de la Región de Murcia”, Plan Regional de Ciencia y Tecnología 2007/2010.

REFERENCES


