Android application for mobile e-commerce with eSignus card

Francisco M. Santana Verona, Fernando de la Puente Arrate

***Abstract*—Nowadays, the use of mobile phones is becoming more common. However, users are generally not aware of their insecurities: third party applications, web browsers exploits, etc. Furthermore, firewalls and antivirus are not usually installed, increasing security risks. On these devices, smart cards technology offers one of the most reliable ways in terms of security. One of the latest applications is its use for payments, either using it as a credit card or as a POS terminal. The IUMA has develop an electronic signer with smart card form called eSignus [1] to allow users sign data. Combining mobile applications and eSignus technology, we developed an application for Android to realize bank transfers and payments signing operations data with eSignus.**

***Index Terms*—android, bluetooth low energy, esignus, smart card**

I. Introduction

WHEN we are making online transactions, companies, banks and users should ensure that these movements are taking place in a a secure environment. In recent years we are seeing a lot of techniques and technologies to ensure that users can remotely access and interact safely with their money.

The smart card technology provide a very secure way to improve authentication and communication methods, allowing the user to sign data using digital certificates. These certificates uniquely identifies the person, entity or corporation, avoiding attacks in communications as man-in-the-middle. In the e-commerce field, this factor is critical because users are not physically in the shop, so no one can ensure that the amount transferred is correct. Furthermore, we need to avoid modifications just before arrive to bank computer system to avoid frauds.

With this in mind, the eSignus card [1] can help us to improve the security of these transactions. This technology consist in an smart card which incorporates digital certificates to sign data. To make it easier, the eSignus card has an embed display and a keyboard, so the user is able to see which data is going to be signed in the card itself.

This new generation of smart cards could be combined with mobile phones to provide secure e-commerce anywhere. Their uses could be as POS terminal (to do payments in a shop) or to transfer money between bank accounts from mobile phone. The basics of its operation will be:

1) The card ask for user PIN (4 digits). Then it waits for data reception to sign. If it does not receive any data, the card automatically turned off.
2) The mobile phone application creates the data which is going to be transfered to eSignus card in order to be signed.
3) Then, the application creates the connection with the card and send the data created on step 2 to it using Bluetooth Low Energy protocol.
4) The card show the data in its display and waits for user confirmation (press OK on embed card keyboard) to start the sign process.
5) If the user accepts, the card start to sign data; this may take 2 or 3 seconds.
6) When it finish, the card return the signature to the application.
7) Now, the application just need to send this signature to bank in order to verify and complete the transaction.

Thus, the user can verify that the data has not been modified by any external device in the sending process, such as computers, ATMs, etc. In this sense the card can be very useful because it is not reprogrammable so the signed data must be what the user wants.

Las Palmas, Spain, e-mail: franverona@gmail.com.
Institute of Applied Microelectronics, University of Las Palmas de Gran Canaria, Las Palmas, Spain, e-mail: fpuente@iuma.ulpgc.es.

II. Mobile application

Using the application, the users are able to perform both bank transfers and payments by signing data using eSignus card. Therefore, we have divided the application focusing on two possible uses: bank transfers and mobile payments using the phone as POS terminal.

A. Bank transfer

The Figure 1 show us a general work flow of a bank transfer using eSignus card and the application.

The user must choose an origin account from where he wants to transfer money. In this work we did not develop bank connectivity (it was simulated), so we allow to add accounts on-the-fly. The next step is to choose a destination account and enter the amount that is going to be transfer. Now, the application build the data packet in eSignus format and send it to the card using Bluetooth Low Energy protocol (1). When the user decide to accept the sign process, eSignus card returns the signed data to the application after a few seconds (2). In the last steps, the signature is sent to bank (3) in order to validate the sign to complete the transaction.

B. Mobile as a POS Terminal

In the Figure 2 we can see the steps of the application used as a virtual POS terminal.

The user enters the amount of the payment and press the confirmation button. Then, data is sent to the card (1). If the

Figure 1. Steps for transference.

Figure 2. Steps for POS terminal.

user is satisfied, the card sign the data and the result will returned to the phone (2). Finally, the application will make the appropriate operations to complete the payment (3).

III. Results

Actually, there are not a very extensive list of smartphones over Android that incorporate Bluetooth Low Energy devices [2], so official Android SDK does not bring support yet. The unofficial alternatives to use Bluetooth Low Energy in Android are currently two: Open Bluetooth Low Energy SDK for Android[3] and Motorola's API [4]. For this work, we have chosen Motorola's API since in our opinion it has a better deployment and is easier to use. But our actual problem is that neither Motorola's API nor Open Bluetooth Low Energy SDK for Android allow us to negotiate connection parameters between eSignus card and the mobile phone.

These connection parameters are often used when we are searching for communication efficiency allowing us to configure the connectivity between devices (latency, timeouts), so we can obtain higher speeds than the protocol offers us by default.

The connection and data sending from phone to card is done in approximately two seconds. The problem comes when we are receiving the signature from eSignus card. Although the signature size is about 2kb, it can take up to 14 or 15 seconds to be received and if we try to modify eSignus firmware, the signature was received partially. Anyways, Bluetooth Low Energy is a very young technology and when Android will support the protocol the general performance might be better.

IV. Conclusions

In this work we saw that Bluetooth Low Energy and Android can be combined perfectly to achieve a better security framework into mobile applications field using eSignus card as an external signer device. The general communications performance was not so good as we expected in the beginning due to the unofficial support for Bluetooth Low Energy on Android. Motorola's API for Bluetooth Low Energy did not allow us to negotiate connection parameters, so as a solution, we can solve it in two different ways: improving Motorola's API or developing a Bluetooth Low Energy API by ourselves. We are not unable to improve Motorola's API because the source code is private, and we cannot decompile it. The best could be to develop a new API to work with Bluetooth Low Energy, so we are going to let this as a future work for next iterations. We expected that the next mobile generations incorporate Bluetooth Low Energy chips and Google adds support for this technology into their SDK.

The integration of mobile e-commerce is a complex process that both financial institutions and manufacturers devices must agree. It is not simply to provide a new payment mechanism; it should be safe and the user should feel comfortable with it. We have seen some security issues that may arise in today's technology, as the man-in-the-middle attacks, eavesdropping passive or spoofing by poor implementation of authentication mechanisms. Currently there are some several alternatives (NFC for mobile phone and POS terminal simulators) and even we have proposed the symbiosis between eSignus card and Android, but there is no effective way to know which one will dominate the coming years. We only have to wait and see how financial institutions and manufacturers adapt to these technological changes in the field of electronic commerce from the mobile phones.

References

[1] P. P. B. C. J. M. G. Fernando de la Puente Arrate, Juan Domingo Sandoval Gonzalez, "External signature device with wireless communication capacity," Spain Patent 0 287 376, Nov. 11, 2010.

[2] Bluetooth. (2012, Jun.) Bluetooth smart ready products. [Online]. Available: http://www.bluetooth.com/Pages/Bluetooth-Smart-Devices.aspx

[3] A. Eisenbach. (2012, May) Open bluetooth low energy sdk for android. [Online]. Available: http://code.google.com/p/broadcom-ble/

[4] Motorola. (2011, Nov.) Motorola bluetooth low energy api. [Online]. Available: http://developer.motorola.com/docs/bluetooth-low-energy-api/