International Journal of Communication Networks and Security

Volume 1 | Issue 4 Article 2

April 2012

A MOBILE PAYMENT SYSTEM THROUGH INDEPENDENT M-SIGNATURE SERVICE

P. VAISHNAVI
1,2Department Of Computer Applications, Anna University of Technology - Tiruchirappalli,
vaishmk@gmail.com

M. IBRAHIM
Department Of Computer Applications, Anna University of Technology - Tiruchirappalli,
ibrahim.aut@gmail.com

A MOBILE PAYMENT SYSTEM THROUGH INDEPENDENT M-SIGNATURE SERVICE

P.VAISHNAVI[1] & M. IBRAHIM[2]

[1,2]Department Of Computer Applications, Anna University of Technology - Tiruchirappalli
E-mail : vaishmk@gmail.com, ibrahim.aut@gmail.com

Abstract - Nowadays a great number of applications require the use of Electronic Signature (e-signature) and non-repudiation services such as certified e-mail, contract signing, electronic payment system and etc... The authenticity and integrity generated by e-signature in electronic document is like a handwritten signature in the paper document. The mobile user would be able to use any application that requires an e-signature is called as Mobile Signature (m-signature). M-signature can be created by different ways, such as Server-based signatures, Mobile Signature Service (MSS), Mobile Signature Application Unit (MSAU). But those have several limitations. In this work, we present the implementation of mobile payment system using m- signature service to an insurance company and for a mobile shop.

Keywords **-** *Electronic signature , Mobile signature, MSAP, iMSSP.*

I. INTRODUCTION

Electronic signature (e-signature) provides interesting features such as integrity, authentication and non- repudiation. Different applications use the e-signature for non-repudiation services such as (mobile) electronic payment systems, certified e-mail, contract signing protocols, e-auctions, long-term preservation of documents, e-procurement, e-invoices, etc. The e-signature provide guarantee of authenticity and integrity for electronic documents like a paper documents. (Ruiz et al., 2007)

In developed countries almost everybody has a mobile handset (mobile phones, personal digital assistants, etc.) and almost everybody has it on them all the time. The e-signature based mobile applications could be developed for mobile devices. Any user would be able to use any application that requires an e-signature. This kind of signature is named mobile signature (m-signature)

It's proposed as a solution that can be used in any application. Furthermore, thanks to the fact that the signature is generated in a mobile device, it may be used everywhere, every time. Finally, the mobile signature is designed so that application providers do not have to develop multiple solutions for the wide range of mobile handsets, mobile operating systems and e-signature technologies that exist for mobile devices. m-signature can be used to provide another security services such as mobile authentication, service identity signing, etc.M-signature can be created by different ways, such as Server-based signatures, Mobile Signature Service (MSS), Mobile Signature Application Unit (MSAU). But those have several limitations, the server-based signatures cannot be considered legally equivalent to the handwritten signatures, The MSS proposal would require that every Mobile Network Operator supported it in order to provide a universal solution, The MSAU, it does not define an standardized interface for the invocation. But we propose an implementation for the payment system for an insurance company and for a mobile shop. The important features are being implanted are avoid intervention of MNO, the user has more control on the signature process, here all the information is exchanged in a secure way.

II. RELATED WORKS

"Electronic signature(e-signature)is fundamental in fields such as electronic commerce and government since it provides some interesting features such as integrity, authentication and non-repudiation". (Ford and Baum, 1997; Sherif, 2000). "The purpose of the e-signature is to guarantee the authenticity and integrity of electronic documents in a way equivalent to the handwritten signature in paper documents". (Rossnagel, 2004; Ruiz-Martıoinez et al.,2007). "This process MSS_Registration) is carried out by means of a MASP such as the RA. In some cases the user has to provide some information that completes registration process such as a PIN, a certificate, etc". (European Telecommunications Standards Institute (ETSI), 2003a). "The roles are similar to the ones proposed by the ETSI, namely, Mobile Network Operators, Certification Authority, Registration Authority, Mobile Signature Service Provider and the Mobile User". (European Telecommunications Standards Institute (ETSI), 2003a)

III. PROPOSED SYSTEM

In this paper we propose a new Mobile Signature Service architecture that is MNO-independent and is not linked to any mobile handset-based specific technology to generate the electronic signature in the mobile handset.

We have improved the functionality of the MSSP and reduced its overhead because in our model the MSSP, which is named MNO-independent MSSP (iMSSP), is not responsible for checking whether the mobile handset is available to perform an m-signature.

In our proposal the mobile user, when available and able to perform signature processes, checks by means of a Web service in the iMSSP whether there are m-signature requests to be signed. Currently, it is feasible to invoke Web services from mobile devices thanks to the development of the Extensible Markup Language (XML) and Web services (WS) Application Programming Interfaces (APIs) and libraries for mobile handsets

A Web service interface to be developed by the MSSPs for mobile clients, we promote the development of our m-signature solution for a mobile handset since the m-signature application developed could be used with different MSSPs.

IV. SYSTEM PROCESS FOR MPLEMENTATION OF MOBILE PAYMENT SYSTEM

The purpose of this section is to provide an overview of the different processes that will take place in our mobile signature system. The purpose of obtaining a certificate the mobile user performs a certification process with a Public Key Infrastructure (PKI) (step 0). Once the mobile user owns a certificate he performs an enrollment process (step 1) with an iMSSP. Through this process the mobile user obtains an identifier that will be used to receive mobile signature requests and a mobile signature application, if needed, to sign them. When the mobile user wants to use an m-signature-based services/application of a MASP, he has to provide her identifier to the MASP(step2).In our case of use, let us suppose that insurance application or for the mobile shop, the user chooses the options he wants to enrol in from the list of the fills in a form with his personal data. The mobile user has to sign the form to confirm his/her enrolment. For this purpose, he provides his identifier to initiate the process that will allow the application to obtain the signature of the data introduced in the form. From the identifier, the insurance/mobile application locates the WS of the iMSSP and sends an m-signature request (step 3). The iMSSP stores all the requests received from different MASPs (insurance/mobile shop) and when the mobile user is available to make m-signatures, she connects to the iMSSP to obtain m-signature requests and signs them if he agrees with them(step4).In our case of use, the mobile user, sometimes after having provided his identifier to the application, will use his m-signature application to connect to the iMSSP and receive as m-signature request the information related to the course in order to sign it. Once them-signature has been performed, the MASP can obtain it, validate it(step5)and then, the application or the service confirms the finalization of the process and performs its task or provides the information needed(step6). In our case of use, the MASP would validate the signature and would provide a receipt to his enrolment in the selected course to the mobile user.

COMPONENTS:

This system consists of the following components (shown in Figure 1):-

Mobile User:

Here the user can use m-signature based applications through network connected mobile.

iMSSP: (independent mobile signature services provider)

It is service, for creating signature for the users. The personal details of the user are gathering from applications and stored on here one database. The signatures are created by users given details based example name, organization and etc. The PKI(Public Key Infrastructure) is creates one certificate and one key for each users, that certificate is act as a m-signature. Both the key and certificate are saved on imssp database.

MASP: (Mobile Service/ Application Provider)

It's are mobile payment system based applications. Here we use two different applications though are

1. Online Mobile Shop
2. Online Insurance payment system.

These two applications have some common modules,

- **Login Form** for existing users. Here the user can give their username and password for login to their account.
- **Registration Form** for new users. Here the new user enters their personal details for creating a new signature. It is stored on imssp database.
- **Details Form** for show/explain details about the mobile phones/insurances plans.
- **Payment Form** here we choose and pay money for our favorite mobile phone/insurance plan.
- **Report Form** after pay the money some details about products and thank you messages have been display on this form.
- **Logout Form** its final form for end the process.

Bank Service:

It is any one general bank system used for pay the money for users from their account, because who have account on bank he/she only eligible for creating the signature on imssp. Its have three modules,

- **Deposit Form** here the account holders deposit money to their account.
- **Withdrawal Form** here the user withdraw money for their use, in directly or through

ATM or through our mobile payment system based.

- **Display Form** here the user seen their personal details about their account.

V. DEVELOPMENT ENVIRONMENT

We have developed based on Java language, which is based on object oriented programming concept. The IDE supports the SOAP messages and WSDL libraries for the development of two services. Those web service for the insurance service and for the mobile shop are been provided through Apache Tomcat server.

Fig 2 (a) Home Page for Insurance plan

Fig 2 (b) Home Page for Mobile shop

Fig 2 a and b shows the home page for Mobile shop and Insurance company.

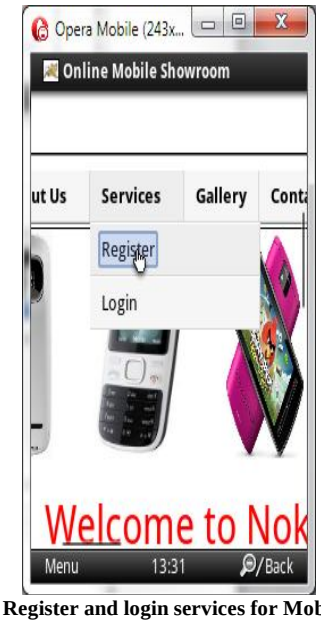

Fig 3 Register and login services for Mobile shop

Fig 3 The mobile shop have basic two forms. One is for exiting user login form and another for new user registration form. In the time of registration one key and one certificate are been created by PKI and it stored on iMSSP database.

Fig 4 Login form form mobile customers

Fig 4 This is the login form for the existing users. The mobile user can enter the user name and password on here.

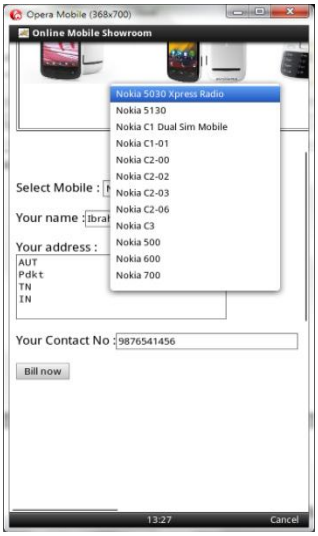

Fig 5 Mobile choosing form on Mobile shop

Fig 5 This form is used to select the mobile for purchase and display information about the login user details.

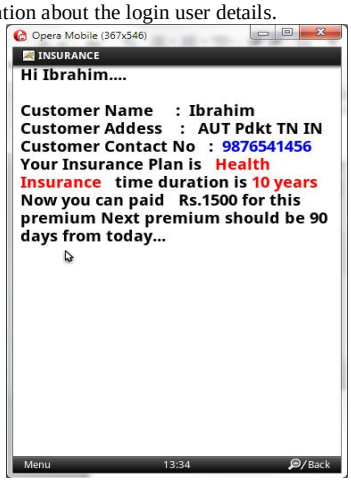

Fig 6 Final report details form for Insurance plan

Fig 6 This form is used for display the final report of the service for mobile shop or insurance plan. Thank you message is display on is form.

VI. CONCLUSIONS

In the implementation of the mobile payment system the low cost, secure, ubiquitously accessible, auto-configurable, remotely controlled solution for automation of mobile payment system are been implemented and tested for the insurance company and the mobile shop. This process adopts the m-signature process through the web service as iMSSP. The approach discussed in the system is novel implementation for the Mobile payment system through m- signature service. The basic level of network control and remote monitoring has been implemented. In future the system will be provided with more secured features to implement m- signature for the independent mobile payment system.

REFERENCES

[1] European Telecommunications Standards Institute (ETSI). Mobile Commerce (M-COMM); mobile signatures; business and functional requirements. Technical report 102 203, May 2003a.

[2] European Telecommunications Standards Institute (ETSI). Mobile Commerce (M-COMM); mobile signatures; Web service interface. Technical report 102 204, August 2003b.

[3] Ruiz-Martinez A, Sanchez-Martinez D, Martinez-Montesinos M, Gomez-Skarmeta AF. A s urvey of electronic signature solutions in mobile devices. Journal of The oritical and Applied Electronic Commerce Research 2007.

[4] Hassinen M, Hypp¨onen K, Haataja K. An open, PKI-based mobile payment system. In: Proceedings of the emerging trends in information and communication security, 2006.p.86–100.

[5] Rossnagel H. Mobile qualified electronic signatures and certification on demand. In: Proceedings of first European PKI workshop: research and applications, EuroPKI 2004, 2004. p. 274–286.

[6] Overview of Electronic Signatures and Records Act (ESRA) Alan S. Kowlowitz Strategic Policies, Acquisitions and e-Commerce NYS Office for Technology ppt.