Electronic Payment Scheme Using Identity-Based Cryptography

Son Thanh Nguyen and Chunming Rong

Department of Electrical Engineering and Computer Science, University of Stavanger, Norway
{son.t.nguyen,chunming.rong}@uis.no

Abstract. Online electronic wallet with decentralized credential keepers is an architecture allowing users to leave most of the content of his electronic wallet at the security of his residential electronic keeper, while traveling with his mobile phone. This paper proposed a new security scheme for mobile payment using such architecture. The approach differs from the previous work in that it uses identity-based encryption for securing payment between the payer and payee, which takes full advantage of public-key cryptography while simplifies the authenticity requirements of the public keys.

Keywords: Identity-based cryptography, electronic wallet.

1 Introduction

The global mobile market has increased dramatically in recent years thanks to the technology development, network infrastructure availability and good tariff policy. According to OECD [14], the ratio of mobile phones per individual is close to one hundred percent in many European countries.

Mobile phones become indispensable devices with many people since they play as communication, entertainment and even business-assistant devices. The service providers, in the meantime, offer more value added services. For example, GSM service providers have launched a pilot program to enable global money transfer using mobile phones [7]. The program can even support transactions for people not having bank accounts. The near future use of one's mobile phone as a special wallet to pay bills at the restaurant, to buy tickets at the train station, or to do shopping is possible.

In [12], the authors proposed an electronic wallet architecture (e-wallet) using mobile phones as payment devices, which enables users using their mobile phones to access different kinds of credentials required for specific tasks (payment information, authentication information etc).

Our paper revisits the security issues in [12] by using identity-based encryption for securing the wireless transmission between the user's mobile phone and the merchant.

The rest of the paper is organized as follow. Section 2 reviews previous works, including the proposed architecture for online e-wallet system with decentralized

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 330–337, 2007.

credential keepers. The previous related works about identity-based encryption is also presented here. Section 3 is our solution using identity-based encryption for securing the mobile payment. Finally, section 4 draws conclusions.

2 Previous Works

2.1 Existing Proposals for E-Wallet

The electronic wallet concept was introduced in Chaum-Pedersen's work [3] and subsequently was revisited in the CAFE project [1], which developed the concept and prototype for electronic payments via short-range radio links or over the Internet. However, the payment concept in the project did not integrate with mobile communication technology. In addition, the project, and other proposals alike, faced with a problem of multi-issuers [12] in which, smart cards from different service providers are not compatible and their information cannot be shared with one another.

To ease the burden of bringing multiple smart cards and remembering multiple credentials, authors in [12] proposed a model in which all the credentials are kept away from the card's owner and can be securely accessed with using his mobile phone through GPRS links.

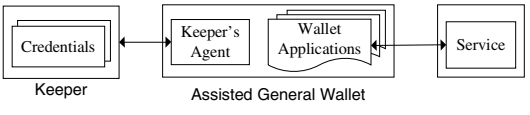

Fig. 1. The online wallet general architecture [12]

Fig.1 represents the general architecture for online electronic wallet. In this model, the keeper is a place where the owner keeps his electronics credentials. This is normally one or more servers with attached card readers and is located in a safe place.

The assisted general wallet is the personal device (e.g. mobile phone) with internet connection (GPRS) plus additional software to enable credential retrieval. When a person needs to do a transaction, (e.g. with a merchant, here denoted by "Service"), he will contact his keeper via network to obtain his credentials (e.g. credit cards information). Having contacted with and authenticated by the keeper, the appropriate credentials are securely sent to his mobile phone through internet connection.

Fig.2 shows an example of a payment system using online wallet derived from [12]. In this figure, the buyer is denoted *b* and is represented by a mobile phone *p*. His counterparts are the merchant *m*, which he will pay for goods, and the trusted server *s*, which he will contact for his appropriate credentials. The buyer *b* owns a mobile phone *p* with a private key SK_p. He also holds the trusted server's public key PK_s. Similarly, the trusted server *s* has its own private key SK_s as well as the mobile's public key PK_p. In addition, the trusted server connects to a database of the buyer's credentials. Since the buyer *b* uses the mobile *p* to do shopping and payment, we use terms mobile phone *p* and buyer *b* interchangeably.