Available online at www.sciencedirect.com

ScienceDirect

Electronic Commerce Research and Applications 7 (2008) 214–231

Electronic Commerce Research and Applications

www.elsevier.com/locate/ecra

Utilizing national public-key infrastructure in mobile payment systems

Marko Hassinen [a,*], Konstantin Hyppönen [a], Elena Trichina [b]

[a] *University of Kuopio, Department of Computer Science, P.O.B. 1627, FI-70211, Kuopio, Finland*
[b] *Spansion International Inc., Willi-Brandt-Allee 4, 81829 Munich, Germany*

Received 18 September 2006; received in revised form 27 March 2007; accepted 28 March 2007
Available online 20 April 2007

Abstract

Payments are the locomotive behind any business domain. It has been predicted that mobile payments will become one of the most successful mobile services, and the security of payments is an important requirement. However, it is difficult to strongly authenticate mobile users remotely and provide an adequate level of non-repudiation of transactions. In this article, we argue that a nationwide public-key infrastructure supported by governmental bodies can be used in a mobile payment system. Not only does it provide strong security, but it also makes the system open to any mobile user, merchant, or financial service provider. Two payment protocols are described: one for virtual point-of-sale payments, and one for vending machine payments. We argue that such a system can be implemented using open development platforms, and its performance is adequate for enabling swift transactions. A prototype of a system which accepts virtual point-of-sale payments is implemented, and its performance and usability are evaluated.

Keywords: Mobile payments; Wireless applications; PKI; Mobile ID

1. Introduction

With the flourishing of electronic commerce and widespread use of mobile devices, a new type of service is emerging that extends e-business using wireless technology by enabling e-commerce services on mobile devices. The pervasiveness of wireless networks and deployment of packet-switching technology create new opportunities for innovative mobile services such as dynamic location-based information (e.g., news, road conditions), entertainment (e.g., m-games, playback of video clips) and communication (e.g., mobile advertising, promotions). Great expectations are also being placed on mobile transaction services such as m-payments, m-banking, and m-auctions. The vision that mobile devices can be used as enablers for contactless proximity-based payments in traditional face-to-face commerce and peer-to-peer transactions is taking hold too.

The reasons for such high expectations are many. For users, mobile phones offer convenience, immediacy and personalization for consumer transactions. From the merchants' point of view, m-commerce allows enterprises to expand their market reach and reduce cost. From the mobile network operator's perspective, m-commerce has considerable potential in maintaining and increasing average revenue per user. Financial service providers (FSP) such as banks and credit card companies are seeing opportunities in using mobile phones as a personal (secure) payment terminal [1] as well as addressing a new customer base that traditionally operated in the sachet[1] economy [2].

It has been predicted that mobile payments have the potential to become one of the most important services in future mobile networks [3–5]. It is clear, however, that many issues have to be resolved before mass adoption

[*] Corresponding author. Tel.: +358 17 162559; fax: +358 17 162595.
E-mail addresses: Marko.Hassinen@uku.fi (M. Hassinen), Konstantin.Hypponen@uku.fi (K. Hyppönen), Elena.Trichina@spansion.com (E. Trichina).

[1] An economy where populace can only afford buying in small quantities and relies on cash for such transactions. While usually being outside of a banking system due to low income, the same group is known to be avid users of mobile phones with pre-paid top-up accounts.

1567-4223/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.elerap.2007.03.006

can occur; among them, security has a prominent role [6,7]. Indeed, influential industrial consortia such as Mobey Forum consider security to be a fundamental requirement for mobile payments and financial services to be valid and adopted by all stakeholders [1]. For customer acceptance, both technical and perceived levels of security should be high, so that customers do not suffer financial losses and their privacy is not compromised [8]. For businesses, effective customer authentication is cited as the most important element in facilitating mobile payments [9]. Transaction-level security must be end-to-end, with message integrity, confidentiality and non-repudiation guaranteed [10]. Non-repudiation (ensuring that a purchase contract cannot later be denied by any of the parties involved) is especially important in mobile payments. If non-repudiation is not ensured, users can potentially claim that the messages related to a transaction were generated by a rogue insider of the mobile network operator.

While architectural decisions concerning the level of security are left to service providers, strong authentication and non-repudiation based on wireless public-key infrastructure (WPKI) and digital certificates are required in macro-payments (i.e., payments higher than 10€) and in all mobile banking services [1,11].

This paper concentrates on the topic of secure mobile payments. Specifically, we describe an open PKI-based platform that facilitates the development of a wide range of secure mobile payment applications. It provides an open technological solution to secure mobile payment transactions that can be freely utilized by financial institutions, mobile network operators or independent third parties. Moreover, in line with the requirements of time to market, our solution relies on today's handset technology and is based on existing standards, such as SIM Application Toolkit (SAT) [12], and open certificate status protocol (OCSP) [13]. The proof-of-concept implementation is done entirely on open development tools and platforms such as Java 2 Micro Edition and Web Services technology [14].

The proposed solution allows us to provide strong customer authentication and non-repudiation by employing public-key cryptography for customer certificates and digital signatures. Confidentiality and message integrity are provided by encrypting messages that constitute mobile payment transactions. What sets our system apart is that it utilizes the existing national public-key infrastructure, which is independent of financial institutions, network operators and mobile payment intermediaries but can be used by all of them. Nowadays, such public-key infrastructure (PKI) is available in Finland, but in the near future it will become available within the whole of the EU [15] and in some countries of the Asia-Pacific region, as amply described in the "One card, one Asia" slogan, see http://www.asiaiccardforum.org. The use of a national PKI solves the basic problem of any system based on asymmetric cryptography, namely, who signs the root certificate and maintains the required infrastructure.

The rest of the paper is organized as follows. Before proceeding with a detailed description of our mobile payment platform, in the following section we review the context and concepts of mobile payment procedures as defined in various academic surveys [5,16–19] and white papers of industrial consortia [1,2,20]. We discuss payment risks, and then formulate the requirements of mobile payment transaction security and present different ways these requirements can be enabled using mobile phones. In Section 3 we give a short overview of the Finnish national public-key infrastructure, namely, FINEID. Next, we provide a specification of mobile payment protocols that guarantee strong authentication and non-repudiation. Section 4 describes protocols for two scenarios; one is for virtual point-of-sale (POS) payments and one is for contactless proximity-based payments at vending machines or physical POS. In Section 5 we give an example of a system that implements our virtual POS payment protocol. The proof-of-concept implementation is an application for buying train tickets using a mobile phone. The application architecture, technical details of the implementation, and test results are provided. We conclude the paper by discussing advantages and limitations of the proposed solution and possibilities of using the platform in other countries.

2. Mobile payment procedures and their security

Following [18], we define mobile payments as wireless transactions of monetary value from one party to another where a mobile device (e.g., mobile phone, PDA, smartphone or any mobile payment terminal) is used in order to initialize, activate and/or confirm the payment.

Mobile payments may be categorized into various types depending on a large number of parameters, such as the transaction settlement method (pre-paid, post-paid, or pay-now), purchase type (digital or real goods) and value (pico-, micro-, and macro-payments). Mobile payment environments can be divided into remote (mobilization of traditional e-commerce by enabling access to WAP shops, or virtual POS), local (by facilitating payment services at physical POS) and proximity (contactless variants of face-to-face commerce) payments. Various enabling (SIM, WIM, dual slot, external card reader) and interactive (voice, Short Message Service (SMS) or Unstructured Supplementary Service Data (USSD), WAP, RFID, Bluetooth) technologies are competing to become established standards for physical and virtual mobile payments. An encompassing summary of various mobile payment procedures and systems is given in [17,18,16] suggests an interesting basis for their systematic comparison in the form of a morphological box of mobile payment characteristics and instances.

2.1. Mobile payment framework

To introduce the mobile payment context, its players and their roles we use as a reference the enhanced variant