Chapter 10
A Secure and Optimized Proximity Mobile Payment Framework With Formal Verification

Shaik Shakeel Ahamad
KL University, India

V.N. Sastry
Institute for Development and Research in Banking Technology (IDRBT), India

Siba K. Udgata
University of Hyderabad, India

ABSTRACT

In this paper the authors propose a Secure and Optimized Proximity Mobile Payment (SOPMP) Framework using NFC (Near Field Communication) technology, WPKI (Wireless Public Key Infrastructure), UICC (Universal Integrated Circuit Card). The novelty of this proposed mobile payment framework is messages are exchanged in the form of Digital Signature with Message Recovery (DSMR) and merchant sends Invoice in the form of Digital Invoice Certificate (DIC) (which is digitally signed by the merchant). The communication link between mobile phone and merchant POS (Point Of Sale) is NFC. Digital Signature with Message Recovery based on ECDSA eliminates the need of adopting PKI cryptosystems thereby reducing the consumption of resources i.e. it consumes less computational and communication cost. DSMR eliminates the need of certificates validation and removes the hurdle of PKI thereby reducing storage space, communication cost and computational cost. The authors proposed protocol ensures Authentication, Integrity, Confidentiality and Non Repudiation, achieves Identity protection from merchant and Eavesdropper, achieves Transaction privacy from Eavesdropper and Payment Gateway, achieves Payment Secrecy, Order Secrecy, forward secrecy, and prevents Double Spending, Overspending and Money laundering. In addition to these our proposed protocol withstands Replay, Man in the Middle and Impersonation attacks. The security properties of the proposed protocol have been verified using AVISPA and Scyther Tools and presented with results.

DOI: 10.4018/978-1-5225-2599-8.ch010

1. INTRODUCTION

Near field communication (NFC) is a short-range wireless technology which is the advanced development of RFID technology. NFC's fundamental advantages compared to other wireless technologies like Bluetooth is the availability of the data storage facility known as the NFC tag. NFC is not just a replacement data cable as Bluetooth, but also as a means of store of data. Referring to the NFC Forum, NFC technology is currently used in three areas, namely sharing, pairing, and transaction. NFC operates between two devices over a very short communication range. NFC communication uses the 13.56 MHz spectrum as in RFID. Currently data transfer speed options are 106, 212, and 424 kbps. NFC technology operates in different operating modes; reader/writer, peer-to peer, and card emulation where communication occurs between an NFC mobile on one side, and a passive RFID tag (NFC tag), an NFC mobile or an NFC reader on the other side. Michahelles et al. (2007) and Ondrus, J. and Pigneur, Y. (2009) gives a good overview of NFC, Context and Foundations of RFID and NFC.

NFC is a bidirectional and short range wireless communication technology. The communication occurs between two NFC compliant devices within a few centimeters. A 13.56 MHz signal with a bandwidth not more than 424 kbps is used. NFC technology operates in different operating modes; reader/writer, peer-to-peer, and card emulation where communication occurs between an NFC mobile on one side, and a passive RFID tag (NFC tag), an NFC mobile or an NFC reader on the other side, respectively (Vedat Coskun et al., 2012). Cho, J. Kim, J. and Kim, S. (2009) and Mair, R. G. (2010) gives a good description of NFC Infrastructure (i.e. about Tags, Antennas, Readers and NFC chip). Miraz, G. M. Ruiz, et al. (2009) gives good overview of Card Emulation Mode Applications in NFC such as payment, mobile coupons, ticketing, and electronic key. The NFC interface is composed of an analog/digital front-end called an NFC Contactless Front-end (NFC CLF), an NFC antenna and an NFC controller to enable NFC communication. The NFC controller enables NFC communication of the mobile phone with the external NFC device. An NFC enabled mobile phone requires an SE for performing secure transactions with the external NFC devices. The SE provides a secure environment for related programs and data. It enables storage of sensitive data of the user. It also enables secure storage and execution of NFC enabled services such as contactless payments.

Various standards have already been defined for NFC communication between two NFC enabled devices, and data transfer within the NFC mobile phone such as Single Wire Protocol (SWP) or the NFC Wired Interface (NFC-WI) (Vedat Coskun et al., 2012). There are various SE alternatives but the most popular ones are a) Embedded hardware; b) Secure Memory Card (SMC); and c) Universal Integrated Circuit Card (UICC) (Vedat Coskun et al., 2012). Mobile commerce literature reviews are also good

Table 1. Comparison of NFC with other wireless technologies Chang, Y. et al. (2010)

Wireless Technologies / Parameter	RFID	Bluetooth	ZigBee	NFC
Security	High	Low	Low	High
Personalization	High	Medium	Low	High
Flexibility	Low	High	High	High
Power Consumption	No	High	Medium	Low