SIM-enabled Open Mobile Payment System Based on Nation-wide PKI

Elena Trichina¹ · Konstantin Hyppönen² · Marko Hassinen²

¹Spansion International Inc., Willi-Brandt-Allee 4
D-81829 Munich, Germany
Elena.Trichina@spansion.com

²University of Kuopio, Department of Computer Science, P.O.B. 1627
FI-70211 Kuopio, Finland
{Konstantin.Hypponen | Marko.Hassien}@uku.fi

Abstract

Many current mobile payment systems rely on mobile network operators for authentication, and lack adequate non-repudiation. In this work we describe a mobile payment system that uses a governmentally administered public-key infrastructure, namely, the Finnish Electronic Identity. FINEID cards store user credentials and private keys for authentication and digital signature, and upon user request can be issued as an application on a PKI-enabled SIM card which is used as a trusted module in our application. Using FINEID, our system authenticates persons, not customers of a certain bank, mobile network operator, or payment service provider. It also ensures non-repudiation, integrity and confidentiality of the messages related to the payment transactions. As the administration of the PKI system is the responsibility of the government, the system is very economical for both the service providers and the users. The proof-of-concept implementation, a system for purchasing train tickets, is done using freely available development tools and platforms. Implementing an open payment system based on a nation-wide PKI has proven to be feasible.

1 Introduction

Mobile payments are defined as wireless transactions of a monetary value from one party to another where a mobile device (e.g., a mobile phone, PDA, smartphone, etc.) is used in order to initialize, activate and/or confirm the payment [OnPi05, Karn04]. Mobile payments cannot be seen only as a “mobilization” of e-payments by providing a mobile interface to existing Internet payment procedures because the context (business models, players’ relationships and roles) and capabilities (e.g., end device and communication technologies) are different. The obvious difference between mobile and other types of digital payments is that the customer and possibly the merchant use mobile devices in order to realize the transaction. This brings a new party, namely a mobile network operator (MNO) into the picture.

Traditionally payment service providers are financial institutions, such as banks and card issuers. They have experience in financial transactions and risk management and have established infrastructure and customer base. In a mobile payment context, mobile network operators are also natural candidates to offer payment services. They have customer base and some financial relationships with their customers via bills. Although a mobile device is only a medium by which payments may be carried out, its technical capabilities and security features may be of crucial importance, therefore device manufacturers also
have a role to play. Other players are newcomers and intermediaries, who can be competitors as well as enablers.

![Building blocks for mobile payments](image)

**Platforms:** SAT, Browser (WML), Java

**Enabling technologies:** SIM, WPKI/WIM, phone with external card reader interface, dual slot phone, ...

**Interface technologies:** Voice, SMS/USSD, WAP

**Transport:** PLMN(GSM), GPRS, 3G, ...

Figure 1 summarizes main building blocks of the mobile payment systems, and helps a reader to navigate among multiple communication, enabling and interface technologies and development platforms. For more details we refer to [KrPT02, Karn04, NLTL04, HaHT07].

Many issues have to be resolved before expecting mass adoption; such as standards, branding, legislation, finding profitable business models... Among issues to be resolved, security has a prominent role. Industrial consortia [MFS03] consider security as the basic requirement for mobile payments and financial services to be valid and adopted by all stakeholders. For customer proposition, both, technical and perceived levels of security should be high, so that customers do not suffer financial losses and that their privacy is protected (i.e., personal details are not disclosed to an unauthorized party). For business priorities, effective customer authentication (establishing customer’s credentials) is cited as the most important element. It is mandated that in macro-payments (i.e., payments in excess of 10 euro) and in all mobile banking services strong authentication based on wireless public key infrastructure [WPKI01] and non-repudiation (i.e., binding parties to the transaction so that none of the involved parties can later deny the transaction details) based on digital certificates is necessary. It is also mandatory that transaction level security should be end-to-end, with message integrity (ensuring that payment data are not altered), confidentiality (protecting sensitive data from non-authorized parties), and authentication guaranteed.

Does the security level of existing mobile payment systems satisfy these requirements? A systematic summary of existing mobile payment solutions with respect to security functions can be found in [HaHT07]; papers [SaWi04, NLTL04] concentrate on security analysis of wireless communication, interface, and enabling technologies while [MaTu05] and [LiPW07] consider security issues from the merchants and customers point of view, respectively.

In almost all existing mobile payment procedures (for an encompassing survey see [Karn04]), the customer authentication is based on her mobile phone ID. A mobile device is considered as being highly personal, belonging to and being managed by the owner; and security of the transactions often relies