Reducing the Computational Cost of Certification Path Validation in Mobile Payment

Cristina Satizábal[1,2], Rafael Martínez-Peláez[1], Jordi Forné[1], and Francisco Rico-Novella[1]

[1] Telematics Engineering Department. Technical University of Catalonia
C/Jordi Girona 1-3, C3, 08034 - Barcelona (Spain)
{isabelcs,rafaelm,jforne,f.rico}@entel.upc.edu
[2] Engineering and Architecture Department. Pamplona University
Km 1 via a Bucaramanga, Pamplona (Colombia)

Abstract. PKI can improve security of mobile payments but its complexity has made difficult its use in such environment. Certificate path validation is complex in PKI. This demands some storage and processing capacities to the verifier that can exceed the capabilities of mobile devices. In this paper, we propose TRUTHC to reduce computational cost of mobile payment authentication. TRUTHC replaces verification operations with hash operations. Results show a better reduction of the cost with ECDSA than with RSA.

Keywords: Public Key Infrastructure (PKI), mobile payment, certification path validation, hash chains.

1 Introduction

The m-payment is defined as the process of exchange money using a mobile device to obtain a product or service [1]. Since the process of payment is achieved without any physical contact between the customer and merchant, and payment information is sent through an open communication, participants can be victims of fraud. Due to these drawbacks, m-payment scheme must offer a high level of security.

The m-payment must consider the following security requirements in order to reduce or avoid frauds: authentication, authorization, confidentiality, integrity and non-repudiation. Different studies about m-payment are centred on the vulnerabilities of its authentication mechanisms and the repudiation problem that affects merchants and financial entities.

Certificates and PKI can be used to provide a good authentication mechanism in m-payment. The use of certificates allows establishing a secure channel for the payment, avoids the repudiation of a transaction and guarantees the integrity and origin of data through digital signature [1].

In spite of the advantages that certificates and PKI offer to m-payment mechanisms, their use is not common, because of the limited resources of mobile devices (processing power, storage capacity and power consumption) and the bandwidth of existing wireless technologies [2]. Additionally, the security infrastructure used for

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 280–296, 2007.

m-payment must support efficiently certificate management (distribution, revocation, and path validation) [3].

Certification path validation is one of the most complex processes of PKI, because it involves: discovering the certification path, retrieving the certificates in the path, verifying the signature of each certificate, and checking the expiration and revocation state of the certificates. This process becomes more complex when the infrastructure grows and also the length of the certification paths, what supposes more work for the verifier and an increase in its storage and processing capacities. Therefore, constrained devices, such as mobile telephones and smart cards, can not always support these requirements.

In this paper, we describe a mechanism to establish an alternative trust relationship between the different entities of a hierarchical PKI using hash chains, what we have called TRUTHC (Trust Relationship Using Two Hash Chains). This contributes to reduce the number of signature verification operations of a path validation process and therefore decreases the verifier's computational cost. This mechanism can be used in some mobile payment scenarios. Section 2 describes the most common mobile payment scenarios, the certification path validation process and the hierarchical architecture. In addition, it defines the hash chains. In section 3, we present some proposals that use certificates for authentication in mobile payment environments. Section 4 shows the operation of TRUTHC. In section 5, we evaluate and compare the computational cost of cryptographic operations in a P2P mobile payment scenario. Finally, section 6 concludes.

2 Background

2.1 Mobile Payment Scenarios

There are different scenarios of mobile payment that can be classified as follows [4]:

- *Real POS (Point Of Sale):* The customers purchase a product on a vending machine using their mobile device. There are two types: in the first type, the customer establishes a communication with the vending machine through a short wireless technology (e.g. Bluetooth or infrared) and all the business transaction is achieved without the participation of the merchant; in the second type, the customer and merchant establish a communication through their mobile device to carry out the payment.
- *Virtual POS:* The merchant gives the option to pay for products using mobile devices. In this scenario participate the following entities: banks (issuer and acquirer), customer, merchant and SP (Service Provider). The customer can pay using a bank account or via phone bill. The payment information is send through UMTS (Universal Mobile Telecommunications System) by a SMS (Short Message Service) or WAP (Wireless Application Protocol).
- *Internet:* The customer makes all the purchase process with his/her mobile device using Internet. The participants are the same like in the virtual POS. The authentication of the merchant before the customer and bank uses digital certificates. The payment information is send through the SP network using WAP.