An Improved Approach for Secured Mobile Payment System Based on Public-Key Cryptography

By

Ehab Moufeed Alkhateeb

Supervisor
Dr. Mohammad Ahmad Alia

Co-Supervisor
Dr. Adnan Ahmad Hnaif

Abstract

In this study, we investigate different mobile payment systems in the scope of cryptography. The study also explores different methods, cryptographic protocols used and the technologies that are being adopted.

It is found that, the study indicates a lack in the performance of the existing systems in term of security level and execution time. It was also noted that attacks (e.g. Man-in-Middle attacks) could be developed due to the technologies that were being used. The study proposes an improved approach to ensure the security and efficiency of a mobile payment system based on Elliptic Curve Cryptography (ECC).

It is concluded that using Elliptic Curve Integrated Encryption Scheme ECIES encryption and Elliptic Curve Digital Signature Algorithm ECDSA authentication algorithms enhances the efficiency and security of the mobile payment system. The improvements through the proposed secured mobile payment system (SMPS) are to propose an efficient approach to End-to-End encryption (E2EE) between merchant and

bank relying on ECC. Since the proposed system SMPS provides higher security levels with smaller key size (224-bit) comparing to RSA based mobile payment which is used (2048-bit). Thus, the proposed SMPS improved the computation time and the performance speed. Adopting Unstructured Supplementary Service Data (USSD) technology for a PIN (Personal Identification Number) authentication, which increased the authentication level by preventing Man-in-Middle attacks, and preventing the possibility of fraud. The Bank-centric mobile payment system is established where the bank is the central node of the mobile payment system, thus, managing the payment, and improving security as no bank card details are either entered or stored on the merchant, IT system. The SMPS is simple, and lack the need of extra hardware or software requirements.