***The Generalised Secured Mobile Payment System Based on ECIES and ECDSA***

# Ehab M. Alkhateeb

Faculty of Science and Information Technology: Al Zaytoonah University of Jordan

Amman, Jordan ehabalkh@gmail.com

# Mohammad A. Alia

Faculty of Science and Information Technology: Al Zaytoonah University of Jordan

Amman, Jordan dr.m.alia@zuj.edu.jo

# Adnan A. Hnaif

Faculty of Science and Information Technology: Al Zaytoonah University of Jordan

Amman, Jordan dr.adnan\_hnaif@zuj.edu.jo

***Abstract*— Mobile payment system is defined as an electronic payment method, also it is defined as mobile money transfer and mobile wallet. Since mobile payment has been generated to be an attractive alternative for the traditional payments systems such as credit cards. In this paper Elliptic curve cryptography is used to mobile payment system. Meanwhile, the proposed mobile payment system includes three main processes: Authentication process, Member recognition process, and Payment process. Moreover, Elliptic Curve Integrated Encryption Scheme ECIES and Elliptic Curve Digital Signature Algorithm ECDSA cryptographic protocols have been applied to enhance the security of the proposed mobile payment system. However, the proposed system is secure, easy and straightforward payment process. As well as, USSD technology is used in this system for PIN authentication process with high security performance.**

***Keywords— ECC, ECIES, ECDSA, Mobile Payment System, and Cryptography.***

##  I. INTRODUCTION

 Mobile payment is defined as payment for products or services between two parties for which a mobile device, such as a mobile phone, plays a key role in the realization of the payment [1]. Nowadays mobile phones are spreading widely through social communities, and becoming a replacement for laptops and desktop PCs. The user demands for convenient and intelligent ways in which to make payments for goods and services using a mobile phone is creating exciting opportunities for those organizations that are part of the mobile payment ecosystem [2]. However, Mobile payments facing critical security issues with the rise of identity fraud, and illegal access to confidential data, such as credit card details. Furthermore, the cryptanalysis and attacking, protocols speed, and performance evaluation are the core elements in building a secure mobile payment system. Therefore, this paper focuses its attention on these concerns by presenting a mobile payment which is based on public key cryptography. The assessment of security for the proposed mobile system is based on the strength of proposed cryptographic algorithm, the selected key size, the performance and the speed of the proposed system. This approach is rather a replacement or a merge for classical way to pay using credit card and the current mobile payment methods.

##  II. RELATED WORKS

### A. Cryptography

Cryptography is a cornerstone of the modern electronic security technologies used today to protect valuable information resources on intranets, extranets, and the Internet. Cryptography is the science of providing security for information [3]. Cryptography have many algorithms that can be categorized into two main types based on the nature of key, namely secret and public keys. The secret key or non-public key cryptosystem only need one key(secret key) to encrypt and decrypt the data between the sender and the recipient, while public-key cryptosystems comes in more difficult approach, it consists of two keys, the public key which is used to encrypt the data and private key for decryption . Public key based on key exchange protocol rises above the difficulties faces by the secret key cryptosystem. This is because key management is much easier with the help of a key exchange protocol such as Diffe-Hellman [4].

Point of Sale (POS),