

## Abstract

---

E-Commerce takes the advantage of the Internet to eliminate physical boundaries and to reach out the global market. Today, online shopping plays an important role in our life. More and more people are changing their shopping behavior to buy online. Electronic Payment System (EPS) is essential for online shopping. A successful EPS supports the transfer of electronic money or sensitive information with security, accuracy, and integrity between the seller and the buyer over the telecommunication network. SET, CyberCash, Paypal and iKP are the most popular Credit Card-Based EPSs (CCBEPS) or protocols. Some of the existing CCBEPSs only use SSL to provide a secure communication channel. Hence they prevent only the "Man in the Middle" fraud but they do not protect sensitive cardholder information such as credit card number to be passed to the merchant, who may be unscrupulous. Many existing CCBEPSs use complex mechanisms such as cryptography, certificate authorities, etc. to fulfill the security schemes but factors such as ease of use for the cardholder and the implementation cost for each party are not considered. For example, some CCBEPSs require certificate authorities to authenticate each participant's certificate but it is inefficient to have certificate revocation control. In this thesis, we propose a new payment system based on ANSI X9.59-2006 with extra features added on top of this standard.

An Efficient and Secure Card-based Payment System (ESCPS), which is based on X9.59-2006, is proposed in this thesis. The X9.59 is an Account Based Digital Signature (ABDS) and consumer-oriented payment system. It utilizes the existing financial network and financial messages to complete the payment process. However,

there are two main limitations in this standard. This thesis provides a solution to solve the X9.59 limitations by adding the merchant authentication feature during payment cycle but without any addenda records to be added in the existing financial messages. In addition, ESCPS provides other functions which are not present in the X9.59 standard. We conducted a performance testing on the proposed system by a comparison of SET and X9.59 in simulation. Three simulation models have been built for SET, X9.59 and the proposed system to analyze their performance and their levels of security.