

**E-COMMERCE SOLUTION FOR ELECTRONIC TENDERING
SYSTEM USING SECURE ELECTRONIC TRANSACTION**

MAZLINA ABDUL MAJID

**FACULTY OF COMPUTER SCIENCE & INFORMATION
TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR**

2004

**E-COMMERCE SOLUTION FOR ELECTRONIC TENDERING
SYSTEM USING SECURE ELECTRONIC TRANSACTION**

MAZLINA ABDUL MAJID

**THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER**

**FACULTY OF COMPUTER SCIENCE & INFORMATION
TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR**

2004

ACKNOWLEDGEMENT

Grateful to Allah SWT, I have completed this thesis and dissertation. Therefore, in this opportunity, I would like to express my deepest gratitude to my Master Project Coordinator, Puan Norazlina Binti Khamis for all her advices and opinions. She has guided and monitored my progress until the end. Thank you so much to Puan and I really appreciate your kindness.

Not forgotten also, to all lecturers who have taught me during my master program. I have applied and practiced all the subjects content in this project.

Millions of thanks to Telekom Malaysia Berhad, Kuala Lumpur which has allowed me to use their website as my reference and provided data for my research analysis. In this opportunity also, I would like to express sincere gratitude to KUKTEM and all suppliers that were involved in my project testing.

Last but not least, to my family and friends who have always been there by giving the motivation to finish the project. All the opinions and support will remain forever in my heart.

ABSTRACT

The remarkable growth of companies from day to day is making the business opportunity as a big challenge. To obtain the profit from a business, they have to compete with each other in the fairest way. Tendering process gives companies the same time limit to respond, the same objectives to overcome and with no preferential treatment. In order to provide the reliable, efficient and secure tendering process, this project has been developed with one e-commerce solution called as The Electronic Tendering System (ETS) for Malaysia companies. The system will focus on the website security in terms of secure electronic payment and secure file transfer. The web security protocol that will be implemented is the Secure Electronic Transaction or known as SET. It has been designed to protect credit card transaction on the Internet. Meanwhile for the secure file transfer, the approach that will be used is based on the existing software called as Microsoft Outlook Express. The Outlook has been chosen because it provides the encryption and decryption method to support secure file transfer. ETS provides a secure online infrastructure for front end user to register, read notification of tenders, downloading tender documents, receiving and responding to enquiries, submission of tender proposal and to buy tender document using credit card payment via Internet. Meanwhile for back-end user, ETS can be used to update supplier information, administrator information, update tender notice, awarded tender and read and reply supplier feedbacks. ETS has been developed using Macromedia Dreamweaver MX with support of Microsoft Access 2000 as the database. With the help of ETS, problems with the current tendering process can be overcome.

TABLE OF CONTENTS

Acknowledgement	i
Abstract	ii
Table of Contents	iii
List of Figures	ix
List of Table	xi
List of Symbols And Abbreviations	xi
CHAPTER 1 : INTRODUCTION	1
1.1 Overview	1
1.2 Project Objective	3
1.3 Scope of Study	3
1.4 Problem Analysis	4
1.4.1 Type of Tenders	4
1.4.2 The Current Tendering Process	5
1.4.2.1 Tender Notice	5
1.4.2.2 Getting Tender Document	6
1.4.2.3 Tender Submission	6
1.4.2.4 Tender Proposal Evaluation	6

1.4.3	Current Tendering Process Problem	7
1.4.3.1	Time Consuming	7
1.4.3.2	Cost Increasing	8
1.4.3.3	Payment and Submission Difficulty	8
1.4.4	E-commerce Solution	8
1.4.5	ETS Element Framework	9
CHAPTER 2 : LITERATURE REVIEW		11
2.1	Introduction	11
2.2	Electronic Commerce	15
2.3	Electronic Payment System	16
2.4	Credit card purchases	18
2.5	Credit Card-Based System	19
2.5.1	Secure Socket Layer (SSL)	19
2.5.1.1	What is Secure Socket Layer?	20
2.5.1.2	How Does Secure Socket Layer Work?	21
2.5.2	CyberCash	24
2.5.2.1	CyberCash's Secure Internet Payment Service	24
2.5.2.2	The CyberCash Credit Card Purchasing/Payment System	25
2.5.2.3	The Purchasing/Payment Process	26
2.5.2.4	The Pros and Cons	29

2.5.3	I-Key Protocol (IKP)	30
2.5.3.1	What is IKP (i-Key Protocol)	30
2.5.3.2	iKP Payment Model	33
2.5.4	Secure Electronic Transaction (SET)	36
2.5.4.1	Introduction	37
2.5.4.2	The SET Scene	37
2.5.4.3	SET Participants	39
2.5.4.4	SET in Action	42
2.5.4.5	Dual Signature	44
2.5.4.6	Payment Processing	47
2.5.4.7	SET in Practice	59
2.6	The Chosen Protocol	59
2.6.1	Why SET?	60
2.6.2	SET Requirement	66
2.7	Ms Outlook Express	68
2.7.1	Introduction	68
2.7.2	Why Ms Outlook Express	68
CHAPTER 3 : METHODOLOGY		70
3.1	Introduction	70
3.2	Research Methodology	71
3.2.1	Project Initiating and Planning	71

3.2.1.1	Preliminary investigation	71
3.2.1.2	Data Sources and Instrumentation	74
3.2.2	Analysis	74
3.2.2.1	The Unified Approach	75
3.2.2.1.1	Object-oriented Analysis Process	78
3.2.2.1.2	Design	108
3.2.2.1.3	Implementation and Testing	110
3.3	System Development Requirement	110
3.3.1	Hardware Specification	111
3.3.2	Software Specification	112
CHAPTER 4: SYSTEM FUNCTIONALITY		113
4.1	Introduction	113
4.2	System Workflow	114
4.2.1	Front-End Interface Workflow	114
4.2.2	Back -End Interface Workflow	116
4.3	The ETS Scenarios	116
4.3.1	Front-End Process	117
4.3.2	Back-End User	119

CHAPTER 5 : IMPLEMENTATION AND TESTING	121
5.1 Introduction	121
5.2 System Testing	122
5.2.1 Choose Testing Strategy	122
5.2.2 Prepare test specifications and create test data	123
5.2.3 Performing System Tests	125
5.3 System Installation	126
5.4 User Satisfaction Test	128
CHAPTER 6 : RESULT AND DISCUSSION	129
6.1 Introduction	129
6.2 Test Result	128
6.3 Disadvantages of ETS	132
6.4 Assumption and Further Research	133
CHAPTER 7 : CONCLUSION	137
REFERENCES	139

APPENDIX A	Gantt Chart
APPENDIX B	Example of Tender Document
APPENDIX C	Example of Tender Proposal 1(Technical Specifications)
APPENDIX D	Example of Tender Proposal 2(Technical Specifications)
APPENDIX E	Example of Vendor Registration Form (Government Sector)
APPENDIX F	User Satisfaction Test
APPENDIX G	User Manual

LIST OF FIGURES

Figure 1.1	The Current Tendering System	7
Figure 1.2	ETS Element Framework Process	10
Figure 2.1	Proposed Technology For Internet Payment	17
Figure 2.2	Netscape's Secure Sockets Layer	21
Figure 2.3	CyberCash Purchasing Process	26
Figure 2.4	Generic Model of Payment System	34
Figure 2.5	ZiP Implementation Architecture	36
Figure 2.6	Secure Electronic Commerce Components	41
Figure 2.7	Construction of Dual Signature	44
Figure 2.8	Purchase Request	49
Figure 2.9	Cardholder Sends Purchase Request.	51
Figure 2.10	Merchant Verifies Customer Purchase Request	54
Figure 2.11	SET Certificates hierarchy of trust	65
Figure 3.1	The Model of Electronic Tendering System	73
Figure 3.2	The Processes and Components of The Unified Approach	77
Figure 3.3	Business Process Model For Electronic Tendering System	81
Figure 3.4	Business Process Model for Download Tender Document using SET Payment Processing Protocol	84
Figure 3.5	Business Process Model for Tender Proposal Sending	85
Figure 3.6	Customer Use-Case	87
Figure 3.7	Merchant/Administrator Use-Case	90

Figure 3.8	Administrator Use-Case	91
Figure 3.9	Issuer Use Case	93
Figure 3.10	Certification Authority Use-Case	94
Figure 3.11	Payment Gateway Use-Case	95
Figure 3.12	Acquirer Use-Case	96
Figure 3.13	New Customer Login Collaboration Diagram	98
Figure 3.14	New Administrator Collaboration Diagram	99
Figure 3.15	Registered Customer Login Collaboration Diagram	100
Figure 3.16	Invalid Customer Login Collaboration Diagram	100
Figure 3.17	Administrator Valid Login Collaboration Diagram	101
Figure 3.18	Administrator Invalid Login Collaboration Diagram	101
Figure 3.19	Download Tender Document Collaboration Diagram	102
Figure 3.20	Send Tender Proposal Collaboration Diagram	103
Figure 3.21	Awarded Tender Collaboration Diagram	104
Figure 3.22	Feedback Process Collaboration Diagram	105
Figure 3.23	Customer Profile Update Process Collaboration Diagram	106
Figure 3.24	Class Diagram for SET Process	107
Figure 4.1	Interface Flow For Registered Supplier	114
Figure 4.2	Interface Flow For Unregistered Supplier	115
Figure 4.3.	Back-End Interface Flow	116
Figure 6.1	Bar Chart On User Satisfaction Test Based On CUPRIMDA Categories	130
Figure 6.2	SupplyPoint Functional Structure	135

Figure 6.3	SupplyPoint Architecture	136
------------	--------------------------	-----

LIST OF TABLE

Table 2.1	SET Transaction Types	48
Table 3.1	Lists of Actors	79
Table 5.1	Test Specification for Login Interface in ETS	124
Table 5.2	Test Data Sets To Verify The Login Interface In ETS	125
Table 6.1	Total of User Satisfaction Test Based On CUPRIMDA Categories	130

LIST OF SYMBOLS AND ABBREVIATIONS

ETS	Electronic Tendering System
SET	Secure Electronic Transaction
SSL	Secure Socket Layer
HTTP	Hyper Text Transfer Protocol
FTP	File Transfer Protocol
VAN	Value Added Networks
ISP	Internet Service Provider
MAC	Message Authentication Code
DES	Data Encryption System
PKI	Public Key Infrastructure
IKI	I Key Protocol
CA	Certification Authority

OOSD Object Oriented Software Development

UML Unified Modeling Language

UA Unified Approach

University of Malaya

CHAPTER 1

INTRODUCTION

1.1.1 Overview

The advances in the globalization of business have made the competition between companies become challenging from time to time since the introduction of tendering process. Tendering gives companies the same time limits to respond, the same objectives to overcome and with no preferential treatment. Tendering is the fairest way for buyers to ensure they have received the best offer from the market.

The principles of tendering process are: -

- To ensure that funds are spent effectively and economically (*value for money*) while at the same time taking into account costs other than the quoted price (such as after-sales service).
- To encourage open and effective competition, while at the same time recognizing that, in exceptional circumstances, it may be necessary to limit the number of those quoting or tendering to a small selection whose track record and current financial position make them potentially rewarding partners in terms of cost, quality, delivery and service.
- To meet public accountability requirements.
- To maintain a reputation for fair dealing by employing open communication with potential suppliers at all times [1].

Therefore, the purpose of this research is to build one e-commerce solution for online tendering system called as Electronic Tendering System (ETS). The system will focus on the electronic payment protocol in terms of secure electronic payment and secure file transfer. The system provides secure online infrastructure for supplier registration, notification of tenders, downloading tender documents, receiving and responding to enquiries, submission of tender offers and support credit card payment via Internet.

Because it is Web-based, there are no restrictions of geographical location or time zone. As a result, the system tenders will be accessible on a 24x7 basis, making it far easier for suppliers or contractors around Malaysia to take part in the procurement process. In addition, subscribers will save time receiving and submitting tender documents and minimize costs, for postage and packing. The whole process cuts down on paperwork and increases efficiency.

This chapter will elaborate about introduction of ETS, Chapter Two will elaborate on the literature review, Chapter Three will elaborate about methodology that is used to show the research process and ETS process, Chapter Four is about the functionality of ETS, Chapter Five will elaborate about the system implementation and testing, Chapter Six will elaborate about the result and discussion and Chapter Seven is about conclusion.

1.2 Project Objective

The objective of the project is to develop one system called Electronic Tendering System or ETS, which can be implemented in any Malaysia organization in term to support their tendering process. ETS emphasizes on:

1. The integrated management as the new technology approach in the Malaysia tendering environment through the combination of multiple tendering process in one application.
2. The efficient way to save the process time, cost and easy access for supplier and administration because it supports payment via Internet using credit card transaction and secure file transfer using Ms Outlook Express.
3. The security and the integrity of the tendering process through the implementation of Secure Electronic Transaction (SET) protocol.

1.3 Scope of Study

The study scope is to implement the electronic payment protocol. The electronic payment protocol that will be implemented is Secure Electronic Transaction or known as SET. It has been designed to protect credit card transaction on the Internet. Since SET concept is so wide, therefore this project will only focus until the bank verifies the customer credit card. Meanwhile for the secure file transfer, the approach that will be used is based on the existing software called as Microsoft Outlook Express. The Outlook has been chosen because it provides the encryption and decryption method in regards to support secure file transfer. Furthermore, the target user for the system is the organization in Malaysia that involved in tendering process.

1.4 Problem Analysis

In order to develop the ETS, reviewing the existing tendering system in the Malaysia company must be done in regards to retrieve and understand the tendering process.

Therefore, by understanding the tendering process, the problems in the existing system can be analyzed and research can be done to increase the quality and the efficiency of the system.

1.4.1 Types of Tenders

Different company may have different types of tenders. Tenders in Malaysia company may be invited in the following ways.

1.4.1.1 Open Tender

Tender invitations are published in the merchants website and local newspaper. All interested contractors or suppliers have the freedom to submit their tenders.

1.4.1.2 Invited Tender

Only those contractors or suppliers invited by the contracting authority may submit tenders. Tender invitations are sent by letter to all contractors/suppliers on the relevant approved lists of qualified contractors/suppliers. Tenders received

from contractors or suppliers who have not been listed on the approved lists should also be considered, provided that there is sufficient time to complete the qualification procedure.

1.4.1.3 Close Tender

Tender invitations are sent by letter to only one or a number of contractors or suppliers approved by the company, upon the originating department's recommendation.

1.4.2 The Current Tendering Process

Companies in Malaysia are mostly based on the similar concept of the tendering process. The tendering process involves manual procedure in getting and paying the document tender and also submitting the proposal. Information about the tender notice is advertised in the merchants website and newspaper. Figure 1.1 shows the current tendering process. Details about the tendering process are as bellow: -

1.4.2.1 Tender Notice

The information about the tenders are advertised in the company website. For other companies, tender notice can be found in newspaper or through their company website.

The information includes the tender title, tender reference number, document fee, closing date and time, type of payment that can be made, company address and tender submission information.

1.4.2.2 Getting Tender Document

The website only provides the information about the tender notice. Therefore customers have to go to the merchants office where the address is stated in the website. For the new customers, they have to register as a new client for the company by filling up the customer registration form. Next, the customer has to make payment for the document tender in the form of Cashier's Cheque/Bank Draft/Banker's Cheque/Cash/Postal Order/Money Order payable to the merchant's office. The payment made is not refundable. Tender document can be collected by presenting the receipt of payment, which is issued by merchants accounts department.

1.4.2.3 Tender Submission

The completed Tender Proposals must be handed in sealed packages to the merchant's office.

1.4.2.4 Tender Proposal Evaluation

Tender proposal will be evaluated after the deadline. Late proposals will be returned unopened. Customer has to wait at least three months to know the awarded tender. No notice about the awarded tender will be displayed. Company staff will only contact the customer who won the tender.

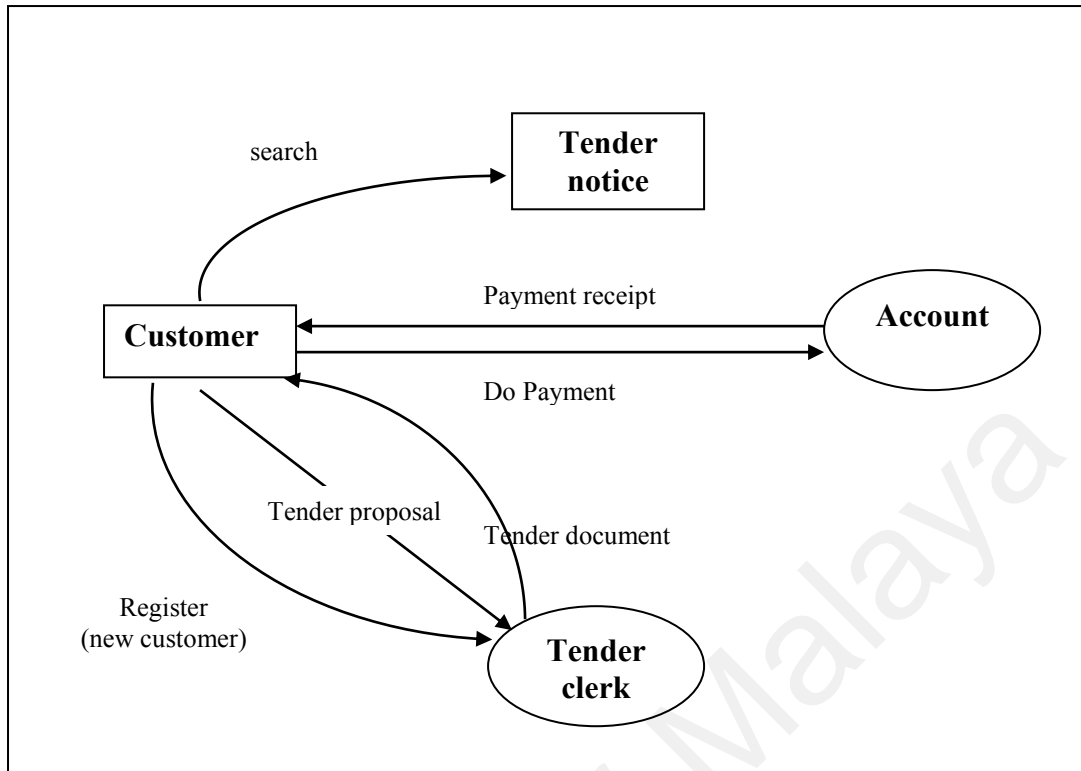


Figure 1.1

The Current Tendering System

1.4.3 Current Tendering Process Problem

1.4.3.1 Time Consuming

The current tendering process is time consuming in terms of getting tender document and submitting tender proposal. This will cause difficulty especially for customers who are not in the same area or state with the merchants office. Moreover, parking problem is always an issue due to lack of parking space nearby the merchants office. These problems will lead to a lot of time consumption.

1.4.3.2 Cost Increasing

The tender proposal has to be submitted in printing, binding and sealed package format whereby this leads to the packing cost. Since the proposal has to be submitted by hand, therefore this will cause the traveling expenses such as toll, parking ticket and fuel.

1.4.3.3 Payment and Submission Difficulty

Difficulty of getting and making the payment for the tender document causes the current tendering process to be less efficient. In fact, the same problem also occurs when submitting the tender proposal. The problems due to only merchant's office manage the payment and tender submission, and this will cause difficulty to their customers who are not in the same state where the tender office is located. Nevertheless, this problem can be solved if the customer can download the tender document or submit the tender proposal via Internet.

1.4.4 E-commerce Solution

Due to a lot of difficulties brought up by the existing tendering process, therefore this research suggested a new solution using E-commerce concept by developing the Electronic Tendering System or known as ETS.

ETS is web based where the entire customer around the Malaysia can access the website and retrieve the information easily via Internet. It has been developed for front end user (supplier) and back end user (administrator). Front end user means the customer of the systems where the front end system supports function such as downloading the tender document, submitting tender proposal, supplier registration,

standard terms of tender, tender notice, tender awarded and also support payment via Internet. Meanwhile the back end-user means the administrator of the merchant company where they have to monitor and manage the front-end process. Therefore the back end system support functions such as updating supplier information, updating administrator information, updating tender notice, update awarded tender and read and reply supplier feedback.

To develop ETS, one secure electronic payment protocol has been implemented known as Secure Electronic Transaction (SET). SET is used to protect the credit card transaction; meanwhile to protect file transfer in the tendering system, the Microsoft Outlook Express will be used. These approaches made ETS more reliable, efficient and secure. In fact, by applying ETS, all the problems that have been discussed above can be overcome.

1.4.5 ETS Element Framework

The operational framework is designed to display the relationship between the system elements in the Electronic Tendering System. The system elements can be referred as shown in figure 1.2.

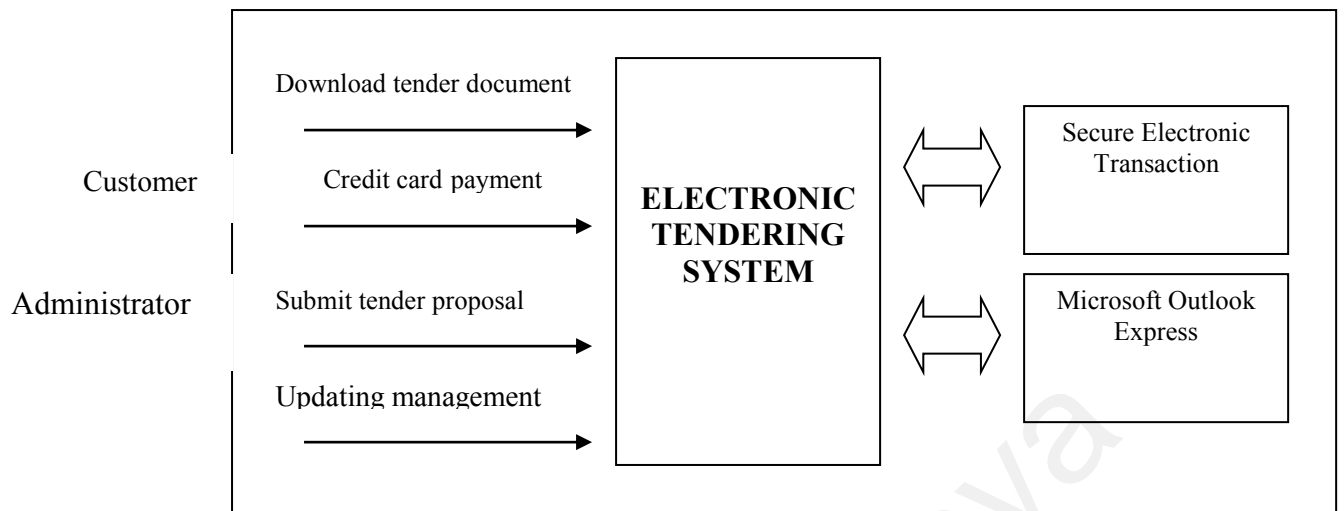


Figure 1.2

ETS Element Framework Process

University of Malaya

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The explosive development of electronic commerce in recent years makes the issue of paying over open networks very important. Electronic payment systems are required to bring the necessary infrastructure to facilitate payment over the Internet. They are becoming an essential part of, and are greatly necessary for further development of electronic commerce and electronic business.

An electronic payment system refers to a complete system designed to enable and execute payment transactions among parties. Electronic payment systems can be classified as offline and online systems. Electronic cash or token-based systems are categorized under offline systems, while credit-debit or account-based systems are categorized under online systems [2]. Purchasing using a credit card over open networks is categorized under credit-debit based systems.

In this research review, electronic payment systems based on the credit card system will be focused. Nowadays, there are a large number of systems developed involving credit transactions. Examples of electronic payment systems based on credit cards are Jaybis E-com [3], WMC-Procurement [12], ETS Hong Kong Government [11] and others.

However, in Malaysia, there is one electronic payment system that is currently being used among the government companies called as Electronic Procurement System or E-Perolehan [45]. Every access to the system will require the user to use their ePerolehan Smart Card for identification, authentication and verification by the system. The smart card will be storing user profile for each appointed and authorized user. Nevertheless, the Smart Card concept is not secure as the credit card concept and this shows that the ePerolehan is less satisfies by the credit card owner [15]. The Smart Card concept is based on the off-line system and credit card concept is based on the on-line system[15]. The off-line and on-line system will be discussed in next section.

At this moment, there are many different companies trying to position their products as the dominant way to transfer money across the Internet [4,5,6]. At the same time, these companies do not realize the problem that they are facing at present. Is it the transaction over open network is the conventional ways of paying for goods and services since it do not work suitably over the Internet. Existing payment systems for the real world, such as credit cards are widely accepted as means of payment on the Internet, however their use encounters difficulties among users who do not see in them enough trust and security [7].

Therefore, this research is done to analyze the existing payment protocol, implement the protocol process and capture the benefit by develops one system called as Electronic Tendering System.

Payment protocol refers to a collection of messages, used to carry electronic payment related information and instructions among the parties involved, and the flow or sequence of those messages [1]. Examples of electronic payment protocol are First Virtual, Secure Socket Layer (SSL) and Secure Electronic Transaction (SET).

First Virtual System is one of the earliest credit card-based payment protocol systems launched for the Internet was the product of a company called First Virtual Holdings, Inc. based at San Diego [3]. Since it the earliest credit card-based payment protocol, is still covered with disadvantages such as when consumers and vendors establish an account with First Virtual, there have to fax or telephone their credit card numbers to it. This shows that the payment protocol was less efficient [8].

In the early '90s, Secure Socket Layer (SSL) was first introduced by Netscape as a security protocol. SSL allowed users to send and receive information to companies on the World Wide Web in an encrypted manner [9]. SSL based protocol provides privacy, integrity and authentication of merchant to consumer. However, it does not guarantee the authentication of consumer to merchant and consumer non-repudiation. The consumer may deny making the payment and the merchant may not be able to prove the fact even if the transaction was legitimate. This causes a “charge-back” cost for honest merchants due to dishonest consumers. The SSL based methods may also work for dishonest merchants to make illegal money [8].

On February 1, 1996, SET was developed by VISA and MasterCard, with participation from leading technology companies, including Microsoft, IBM, Netscape,

SAIC, GTE, RSA, Terisa Systems and VeriSign. SET is a standard for safeguarding credit card purchases made over open networks [9] [10].

The first live SET transaction was performed in Denmark on the last day of 1996 in an IBM pilot scheme. The first application based on SET was appeared at the end of 1998. It is expected that this protocol will supplant otherschemes, and become a standard for all network transactions involving credit cards in the near future [3].

Examples of system that has been developed based on SET protocol are OpenMarket (Transact 4.0), Brokat (X-PAY Server), Maithean (NetPay Merchant™),Maithean (NetPay Merchant™),Maithean (NetPay Merchant™), VeriFone (VeriFone vPOS™),GlobeSET (GlobeSET POS™), and Terisa (SecureWeb Payments™) [11].

The SET protocol provides three main advantages, that put together make it safer then other payment methods. These advantages are [11]: -

- *Privacy*, via cryptography that renders intercepted messages unreadable.
- *Integrity*, via hashing and signing assures that messages sent are received without alteration.
- *Authentication*, via digital certificates which assures that the parties involved in the transaction are who they claim to be, and prevents them from denying that they sent a message (example. non-repudiation).

SET is still new to the web market. Therefore, the use of SET protocol in the electronic tendering systems, is still not available in the e-commerce. Most of the existing electronic tendering systems are based on the SSL protocol since this protocol is one of the pioneers to the security protocol [5]. However, the use of SSL protocol did not provide 100% security [8]. Example of electronic tendering systems, which is based on the SSL protocol, is WMC-Procurement [12].

Although there are lots of tendering systems over Internet but most of them do not support the payment transaction. Example of the tendering systems are Bid Express, Citadon MarketNet, MERX, BIDDs, DCIS System, TED and many more [13].

2.2 Electronic Commerce

E-commerce refers to any sort of commercial transaction that takes place electronically. The transaction might be between two businesses over Value Added Networks (VAN) s, which are specialized firms, in order to provide support for these transactions. Also transaction might be between a business and a consumer, over the Internet [14]. It incorporates support for interpersonal communication, online payment transaction and sharing common database among others.

2.3 Electronic Payment System

Online payment transaction is a part of the electronic commerce. To support online payment transaction, an electronic payment system is needed. Figure 2.1 shows the proposed technology for Internet payment. Electronic payment system can be divided into two models: on-line and off-line systems. The on-line property means that the coins are being verified during transaction. This means that the merchant has to have a connection to the bank, in order to check that every coin spent is valid. This is a strict requirement for the bank, since it has to have very efficient computers to make it possible to check every on-line transaction, in real-time. The off-line property means that the bank is not there to verify every single coin spent during the transaction, at least not in small payment [15].

Online Payment Systems	Offline Payment Systems
<p>Credit-card Payment Systems:</p> <p>Proposal using no Cryptography: <i>First Virtual</i></p> <p>Proposal using Cryptography: <i>CyberCash and iKP</i></p> <p>Proposed Standard : <i>SET</i></p>	<p>Electronic purses, using smart cards:</p> <p>Shared Key: <i>Danmont, Proton</i></p> <p>Public Key: <i>Express</i></p> <p>Not known publicly: <i>Mondex</i></p> <p>Standardizations: <i>CEN Intersector Electronic Purse, EMV Electronic Purse.</i></p>

Figure 2.1

Proposed Technologies For Internet Payment

The electronic payment systems can also be divided according to their anonymity property. There are two levels of anonymity: untraceability and unlinkability.

Untraceability means that the merchant cannot determine the identity of the customer during a transaction, example. it is impossible to trace the coins to a customer.

Nevertheless, if a coin is spent twice, the system guarantees that the identity of the double spender is revealed. Unlinkability is a stronger form of untraceability. It means that two different coins from the same account cannot be linked. The division can also be made into five models based on how the payments are carried out. These five models can be put into two categories: payment through accounts and payment per transaction. Payment

through accounts means that the customer and the merchant have set up an account on beforehand, which the merchant can charge. The three methods of this category are subscriptions, purchase orders and Internet accounts (not necessarily issued by an ISP) [15].

Payment per transaction means that, user do not arrange anything with the merchant in advance, but when user find something user "must" have, arrange the payment on the spot. The method of payment per transaction is credit card purchases.

Credit card purchases will be further discussed in the next subchapter since this project will focus to the credit card transaction via Internet.

2.4 Credit card purchases

This is the most common model, since credit cards have been around for decades and are familiar to everyone. Credit cards are available to almost all adults, and can therefore also prove that the customer is at least example 18 of age, since credit cards are not available to children. The credit card number is sent encrypted (example using SSL), and is verified by the merchant within a reasonable timeframe (example 30 seconds). The encrypted connection between the merchant and the customer protects both parties from malicious third parties [15].

Credit card purchase is depended on credit card-based system. Example of credit card-based systems are Secure Socket Layer (SSL),CyberCash, I-Key Protocol (IKP) and

Secure Electronic Transaction (SET). Secure Electronic Transaction is a new standard for the secure credit card purchase over the Internet. SET will be introduced as a payment protocol for this research.

2.5 Credit Card-Based System Protocol

Credit Card-Based System Protocol is also known as electronic payment protocol. There are many well-known protocols and existing electronic payment system implemented by commercial company working in the Internet. Payment protocol refers to a collection of messages, used to carry electronic payment related information and instructions among the parties involved, and the flow or sequence of those messages. Below are the well-known protocols of electronic payment that will be discussed in this research.

2.5.1 Secure Socket Layer (SSL)

Secure Socket Layer (SSL) is the first protocol that will be discussed in this section.

2.5.1.1 What is Secure Socket Layer?

Secure Socket Layer is a security protocol that was first introduced by Netscape in the early '90s. SSL will allow users to send and receive information to companies on the World Wide Web in an encrypted manner. This means that any information such as, text, pictures, forms that are transmitted through the Web browsers will be completely encrypted. When information has to get from one point to another, it travels throughout several computers. The data that is sent through the Internet may travel across 25 or 35 networks. When this data is in transit, any one of these computer systems represents an intermediary with the potential to access the flow of information between the user's computer and a trusted server. The Internet does not provide built-in security. However, SSL will encrypt the data in a manner that will prohibit interlopers from reading data that the user is sending or receiving. SSL provides privacy, authentication and message integrity. [17]

The Secure Socket Layer is a security protocol that resides at the transport layer, see Figure 2.2. The advantage of residing at the transport layer is that it does not make SSL application dependent. The SSL protocol is application independent, allowing protocols such as HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), and Telnet to be layered on top of it transparently [17].

HTTP	Telnet	NNTP	FTP	SMTP	SHTTP	Etc...
SSL						
TCP/IP						

Figure 2.2
Netscape's Secure Sockets Layer

2.5.1.2 How Does Secure Socket Layer Work?

Upon the initial connection, SSL does a security handshake, which is used to start the TCP/IP connection. SSL uses encryption and authentication technology developed by RSA. RSA is a public key cryptography for both encryption and authentication. RSA is part of many official standards worldwide. Data that is encrypted with the *public key*, can only be decrypted with a *private key*, and vice versa. Authentication is the process of verifying that the user is actually who he or she claims to be [16].

During a secure transmission, the client and the server use what are called keys. As mentioned earlier, there are two keys, a public key and a private key. The public key is available to everyone, however, the private key is only available to the user. For example, suppose Zam wanted to send Ina a message. Zam can use Ina's public key to encrypt the message and then send it to her. Once Ina receives the message, she can decrypt it by using her private key. Ina can be assured that she was the only one to read the message, because only her private key can decrypt the data that was encrypted using the public key [16].

In order to make the message even harder to decrypt, a technique known as **digital signature** is used. A digital signature is a code that can be attached to the message that is being sent, that uniquely identifies the sender. The purpose of the digital signature is to guarantee that the user sending the message is actually who he or she claims to be. However, there is still a problem with this. By having only a public-private key and a digital signature, any user can still fake who he or she is. To solve this problem, another attachment is made to the message. A **digital certificate** performs connection verifications between server's public key and server's identification. These certificates are issued by third parties called **Certificate Authorities (CAs)**. A Certification Authority is a trusted authority responsible for issuing certificates used to identify a community of individuals, systems or other entities, which make use of a computer network. A certificate has the following content [17]: -

- The certificate issuer's name.
- The entity for whom the certificate is being issued, also known as the subject.
- The public key of the subject.
- Some time stamps.

A user that wishes to send an encrypted message applies for a digital certificate through a CA. The CA issues an encrypted digital certificate containing the user's public key and a variety of other identification information that was mentioned above. The CA uses its private key to encrypt the digital signature, so it cannot be forged.

By using the methods of encryption described so far, no hacker will be able to read messages that do not belong to them. However, there is still a chance that the hacker that

stands between two users can damage the messages that are sent, although he cannot read them. The hacker can just replace the message with garbled information. The reason is because he knows what protocol the users are utilizing. In order to prevent this, a new technique has been introduced called Message Authentication Code (MAC), which can be used in the protocol. A MAC uses an algorithm that computes a secret piece of data that is then added to the message. The values of a MAC can be 40 or 128 bits, which would make it impossible to try to figure out what the right MAC is. The odds of guessing are 2 to the power of 128 [17].

There are two ways to find out whether a document comes from a secure server. One way is to look at the URL. If the URL begins with **https://** as opposed to **http://**, then the document comes from a secure server. Another way to verify the security of a document in a Netscape browser is by looking at the golden key in the lower left corner of the screen. If the key displayed is broken with a gray background that means that the document is insecure. However, if the key is not broken and a blue background is displayed, then the document comes from a secure server.

2.5.2 CyberCash

The second payment protocol that will be discussed is CyberCash.

2.5.2.1 CyberCash's Secure Internet Payment Service

CyberCash, Inc. was founded in August 1994 .In February, 1996, it became a publicly traded company .The company is focused on providing Secure Financial Transactions Services over the Internet, including secure credit card transactions, electronic checks and micro transactions . Some features of the company are[18]: -

- Secure Internet credit card (macro-level) transactions since April 1995.
- Thousands of transactions processed daily.
- Over 500,000 CyberCash Customer-Wallets in the distribution channel, including CyberCash, Checkfree, and Compuserve wallets.
- Connected to 80% of the banks in the U.S.
- New and upcoming CyberCash Payment Services[18].
- Electronic Coin: The micropayment product for purchases of \$0.25 - \$10.
- Cash/Check product due 4th Quarter, 1996.

2.5.2.2 The CyberCash Credit Card Purchasing/Payment System

The CyberCash credit card payment system consists of three parts [18]: --

- The CyberCash Wallet-software distributed free to consumers (Windows or Mac-based).
- The Secure Merchant Payment System (SMPS) for the seller's web-server. It communicates with the customer and the Wallet-software.
- CyberCash Gateway Servers for banks. It links the seller's server to existing financial networks of the bank in a safe manner for the bank and acts as a firewall.

As a variation to this, at least QuakeNet services can configure the seller's SMPS server to accept credit card payment via an SSL compatible browser. This is known as a merchant generated transaction. When a user enters a credit card directly into the secure form, the amount to be charged and the credit card number is directly passed to the CyberCash payment server for processing [18].

2.5.2.3 The Purchasing/Payment Process

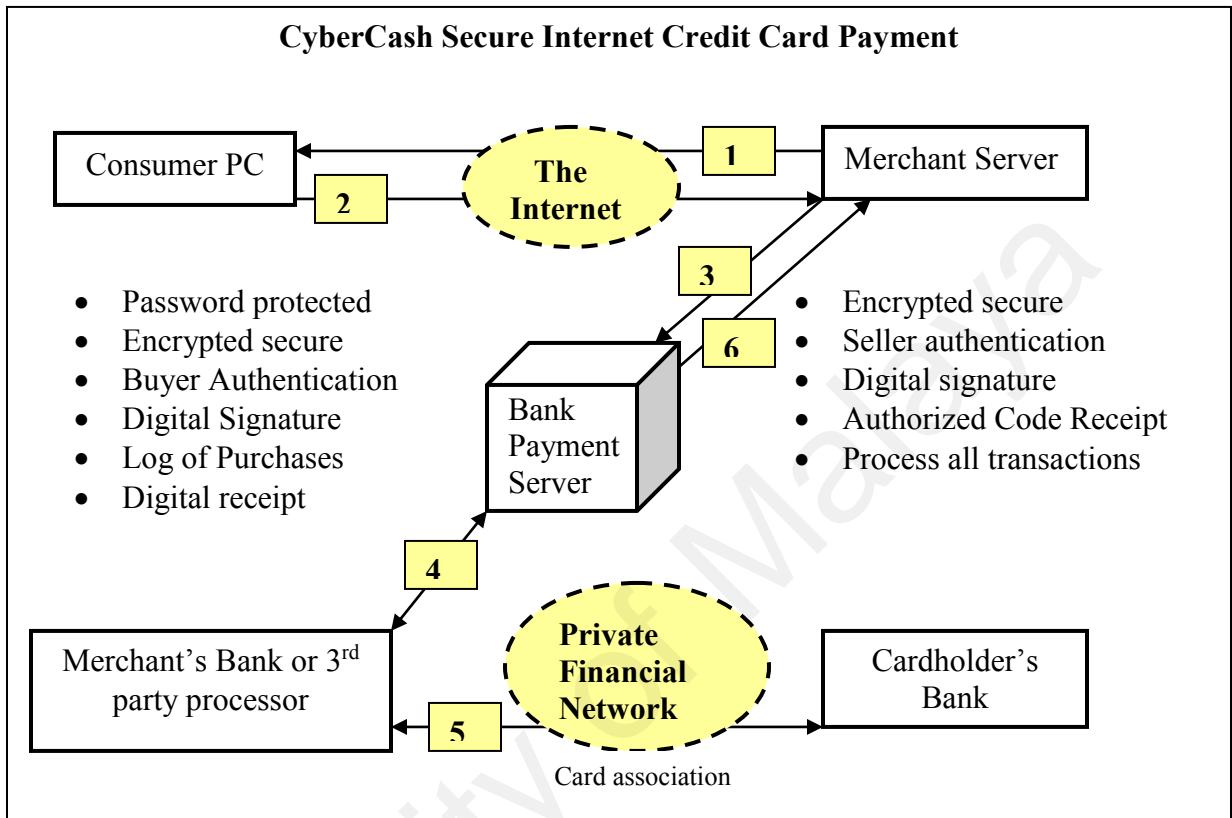


Figure 2.3

CyberCash Purchasing Process

- i. The Customer has decided what it is he or she wishes to purchase, where he or she wants it shipped. The seller's server returns a summary of the item, price, transaction ID, to consumer.
- ii. If everything is OK, the customer clicks on the "Pay" Button which launches the CyberCash, Checkfree or Compuserve Wallet. The customer chooses the

credit card from their "wallet" with which he/she wishes to pay with and clicks OK to forward the order and encrypted payment information to the seller [18].

- iii. The seller's server receives the packet, strips off the order and forwards the still encrypted payment information digitally signed with the seller's private key to the bank's CyberCash gateway-server. The merchant cannot see the consumer's credit card information, since it is encrypted with a key that only the bank's CyberCash gateway can decrypt [18].
- iv. CyberCash gateway-server receives the packet, takes the transaction behind its firewall and off the Internet, unwraps the data, reformats the transaction (the payer's identity, amount to pay and the seller's identity) and forwards it to the seller's bank over dedicated financial networks [18].
- v. The seller's bank then forwards the authorization request to the issuing (customer's) bank via the card associations or directly to American Express or Discover in those cases (this is applicable only to the USA). The approval or denial code then is sent back to CyberCash gateway-server [18].
- vi. CyberCash gateway-server then returns the approval or denial code to the seller who then passes it on to the customer [18].

To complete the transaction, the seller's server sends the customer a digital receipt. A transaction can be captured and posted to the seller's account while the customer is still on-line, or later if seller cannot ship the purchased product immediately [18].

From Step one to Step four takes approximately 15-20 seconds. All encryption is at the message level and is therefore independent of the browser technology used.2.4.2.3 Security and Encryption [18].

CyberCash transactions are protected by encryption, combining DES private-key and 768-bit RSA public-key encryption technologies (soon or already 1024-bit) [18].

Messages between the Wallet (the customer), the seller, and the CyberCash Gateway Server are encrypted by "industry-standard" 56-bit DES technology that uses a key unique to that one transaction. The DES key itself is encrypted by a 768-bit RSA key and appended to the DES-encrypted message to be delivered [18].

Considering that all DES-keys are unique to one transaction, the 56-bit key is strong enough as is the 1024-bit RSA encryption used to protect the DES-key.

The CyberCash system also uses digital RSA signatures to verify the senders of messages to support the authentication process and well as non-repudiation of charges [18]. This method seems to be reliable and strong enough.

To truly ensure security, the user must also be certain he/she is using a true copy of the CyberCash-software code. For this a third party verification service will be available which provides certificates which convey the correct hash code for the software. The hash algorithm is MD5. Routines, which check the hash code, will be available from a variety of sources and will be well documented [18].

2.5.2.4 The Pros and Cons

- The benefits of CyberCash-technology are as follows [18]: -
- CyberCash is the only company with worldwide export license of 1024-bit RSA encryption algorithm.
- The CyberCash wallet is browser-independent. The CyberCash wallet can be used with user favorite browser.
- CyberCash offers real-time transactions and secure credit card authentication based on digital signatures and RSA-encryption.
- From the bank's point of view, the gateway server converts the payments into such form that they look like ordinary credit card payments. This creates only minimal needs to change the existing systems.

The drawbacks are hard to assess due to the embryonic stage of the business. One major drawback of CyberCash, that is common to all electronic payment services today, is that it is not yet commercially important or highly visible in the Internet [18].

2.5.3 I-Key Protocol (IKP)

I-Key Protocol (IKP) is the third protocol that will be discussed in this section.

2.5.3.1 What is IKP (i-Key Protocol)

IKP or I-key protocol ($i = 1; 2; 3$) are under one family of secure electronic payment protocols. These protocols are compatible with the existing card-based business models and payment system infrastructures. They involve three parties: the buyer (who makes the actual payment), the merchant (who will receive the payment) and the acquirer gateway (who acts as an intermediary between the electronic payment world and the existing payment infrastructure, and authorizes transactions by using the latter)[19].

All iKP protocols are based on public-key cryptography, but they vary in the number of parties (out of the three involved) that possess individual public key-pairs and can thus generate digital signatures. This number is reflected in the name of the individual protocols: 1KP, 2KP, and 3KP. The iKP protocols offer increasing levels of security and sophistication as the number of parties who possess own public key-pairs increases [19].

The simplest protocol, 1KP, requires only the acquirer to possess a public key-pair. Buyers and merchants only need to have authentic copies of the acquirer's public key, reflected in a public key certificate. This involves a minimal public key infrastructure (PKI) to provide certificates for a small number of entities, namely, the

acquirers. A large credit card company can operate this type of a PKI, for example. In the 1KP setting, buyers are authenticated on the basis of their credit card numbers and optional secret PINs. Payments are authenticated by communicating the credit card number and optional PIN appropriately encrypted under the acquirer's public key, and cryptographically bound to relevant transaction information (purchase amount, identities, and others.). This prevents fraudulent merchants from collecting credit card numbers and creating fraudulent payments. 1KP does not offer non-repudiation for messages sent by buyers and merchants. This means that disputes about the authenticity of payment orders are not unambiguously resolvable within the digital system. 2KP demands that merchants, in addition to acquirers, hold public key-pairs and public key certificates. The protocol can thereby provide non-repudiation for messages originated by merchants. Additionally, 2KP enables buyers to verify that they are dealing with *bona fide* merchants by checking their certificates, without any on-line contact with a third party. As in 1KP, payment orders are authenticated via the buyer's credit card number and PIN, encrypted before transmission [19].

3KP further assumes that buyers have their own public key-pairs and public key certificates, thus achieving non-repudiation for all messages of all parties involved. The combination of credit card number, optional PIN and a digital signature of the buyer authenticate payment orders. This makes the forging of payment orders computationally infeasible. Additionally, 3KP enables merchants to authenticate buyers on-line. This requires a full public key infrastructure covering all parties involved.

The main reason for designing these three variants was to enable gradual deployment: 1KP requires only a minimal PKI and would have been suitable for immediate deployment at the time it was proposed in early 1995. 2KP requires a PKI covering all merchants, 3KP one covering all merchants and all cardholders. Looking back at what actually transpired with the deployment of iKP and its descendant, SET, there was actually no need for a 1KP-like protocol. All iKP protocols can be implemented in either software or hardware. In fact, in 1KP and 2KP, the buyer does not even need a personalized payment device: only credit card data and PIN (if present) must be entered to complete a payment. However, for the sake of increased security, it is obviously desirable to use a tamper-resistant device to protect the PIN and {in case of 3KP {the secret key of the buyer) [19].

We emphasize that the goal of iKP is to enable payments. It is not concerned with any aspect of the determination of the order; it assumes that the order, including price, have already been decided on between buyer and merchant. It does, however, provide secure and unambiguous linking of order information with the payment to enable effective dispute handling.

iKP protocols do not provide secrecy (encryption) of the order information. Such protection is assumed to be provided by other mechanisms, example, SSL [3] or IPSec [4]. This decoupling of order encryption from the electronic payment protocol is an important design principle of iKP, which supports compatibility with different underlying browsing and privacy-protecting mechanisms. It also contributes to the overall simplicity, modularity, and ease of analysis of the protocols. An additional advantage is freeing iKP

from US export restrictions related to the use of bulk encryption. Thus, if desired, the iKP family (especially, 2KP and 3KP) can be easily extended to generate shared keys between buyer and merchant for protection of browsing and order information.

2.5.3.2 iKP Payment Model

All iKP protocols are based on the existing credit-card payment system. The parties in the payment system are shown in Figure 2.3. The iKP protocols deal with the payment transaction only (example: the solid lines in Figure 2.3), and therefore involve only three parties, called B { Buyer, S { Seller, and A { Acquirer (gateway). Recall that A is not the acquirer in the financial sense, but a gateway to the existing credit card clearing/authorization network. In other words, the function of A is to serve as a front-end to the current infrastructure that remains unchanged.

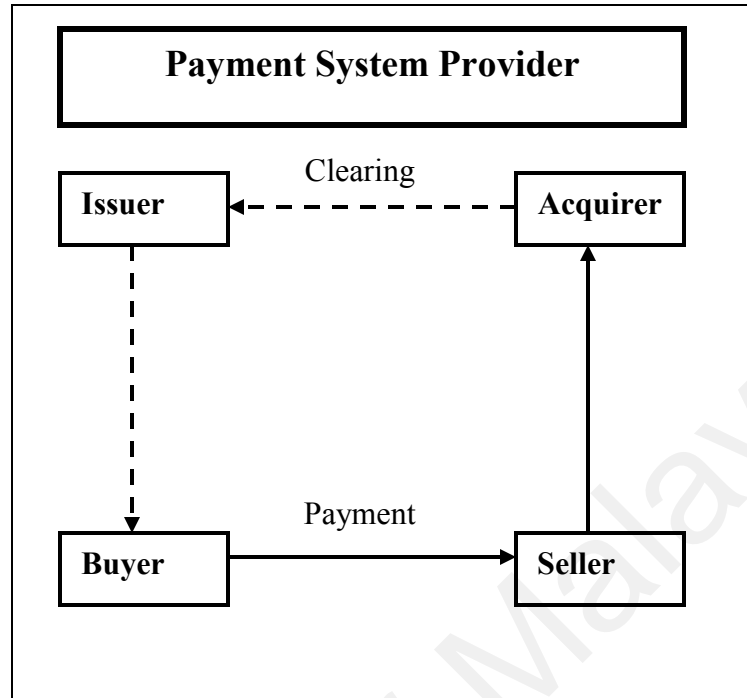


Figure 2.4

Generic Model of Payment System

A payment system provider who maintains a fixed business relationship with a number of banks operates the payment system. Banks act as credit card (account) issuers to buyers, and/or as acquirers of payment records from merchants (sellers). Each issuer has a Bank Identification Number (BIN) assigned when an issuer signs up with a payment system provider. A BIN is embossed on each credit card included as part of the credit card number [19].

BIN also identifies the payment system provider. We assume that each buyer receives its credit card from an issuer, and is somehow assigned (or selects) an optional

PIN as is common in current credit card systems. In 1KP and 2KP, payments are authenticated only by means of the credit card number and the optional PIN (both suitably encrypted), while, in 3KP, a digital signature is used, in addition to the above. It is also assumed (as is natural in the context of electronic payments) that the buyer is using a computer to execute the payment protocol. Since this computer must receive the buyer's PIN and/or secret signature key, it must be a trustworthy device. We caution that even a buyer owned computer is vulnerable: it may be used by several people and may contain a Trojan horse or a virus that could steal PINs and secret keys [18].

The best payment device would be a secure isolated and strictly personal device, example, a tamper-resistant smart card, connected to the computer used for shopping via a buyer-owned smart card reader with its own keyboard and display. (This is often referred to as an electronic wallet.) Technically, 1KP and 2KP can be used with any kind of payment device, while for 3KP the buyers need secure personal devices to store their secret signature keys and certificates. A seller signs up with the payment system provider and with a specific bank, called an acquirer, to accept deposits. Like a buyer, a seller needs a secure device that stores the seller's secret keys and performs the payment protocol. Clearing between acquirers and issuers is done using the existing financial networks [19]. Figure 2.5 shows the example prototype of 2KP and 3KP, called as The Zurich iKP Prototype (ZiP).

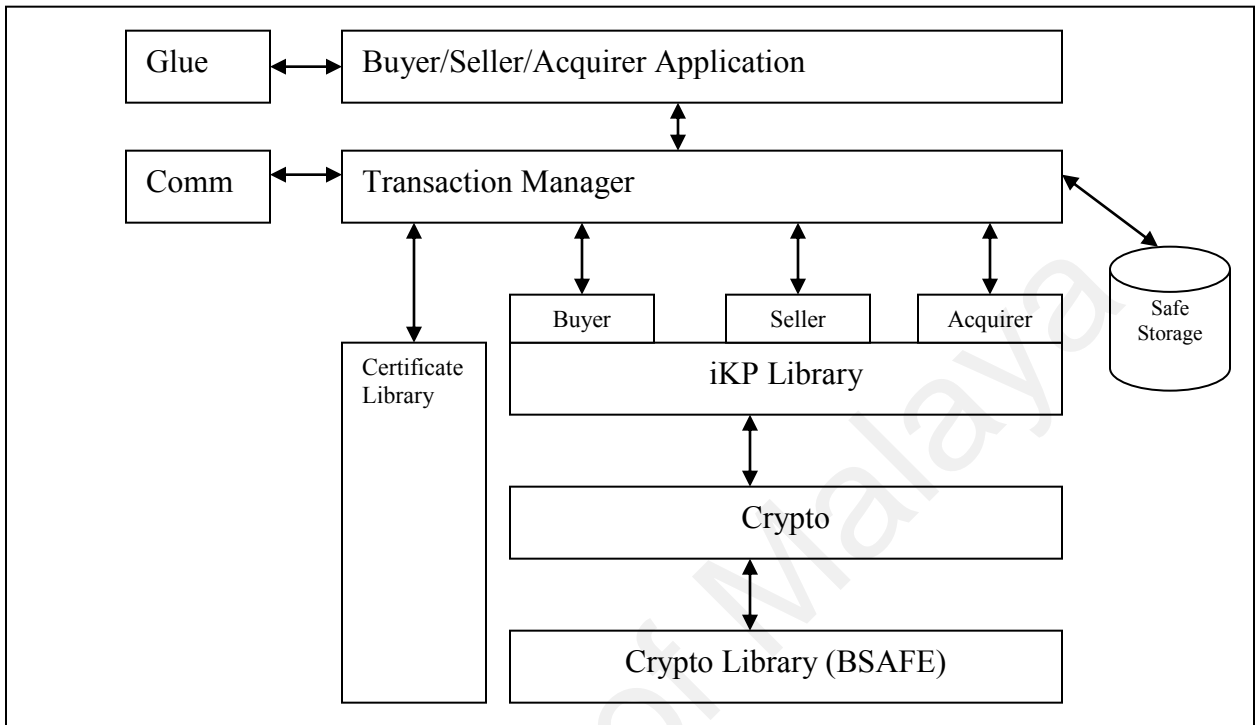


Figure 2.5

ZiP Implementation Architecture

2.5.4 Secure Electronic Transaction

Secure Electronic Transaction is the final protocol that will be discussed in this section. This protocol will be implemented in ETS to support payment via Internet using card credit transaction.

2.5.4.1 Introduction

Secure Electronic Transaction (SET) is an open encryption and security protocol designed to protect credit card transactions on the Internet. The SET emerged from a call for security standards by MasterCard and Visa in February 1996. A wide range of companies were involved in developing the initial protocol, including IBM, Microsoft, Netscape, RSA, Terisa, and Verisign. Since 1996 there have been numerous tests of the concept; by 1998, the first wave of SET-compliant products was available [20].

SET is not itself a payment system. It's a set of security protocols and formats enabling users to employ the existing credit card payment infrastructure on an open network, such as the Internet, in a secure fashion. SET consists of three services: -

- Providing a secure communications channel among all parties involved in a transaction.
- Providing trust by the use of X.509v3 digital certificates.
- Ensuring privacy because the information is only available to parties in a transaction when and where necessary.

2.5.4.2 The SET Scene

SET involves interaction among credit card holders, merchants, issuing banks, payment processing organizations, and public-key certificate authorities. SET is a complex protocol defined in three "books" issued in May 1997, and running to nearly

1,000 pages. SET provides important features needed for secure credit-card transactions over the Internet: -

i. **Confidentiality of information**

Cardholder account and payment information is secured as it travels across the network. An interesting and important feature of SET is that it prevents the merchant from learning the cardholder's credit card number; this is provided only to the issuing bank. Conventional encryption by DES is used to provide confidentiality.

ii. **Integrity of data**

Payment information sent from cardholders to merchants includes order information, personal data, and payment instructions. SET guarantees that these message contents are not altered in transit. RSA digital signatures, using SHA-1 hash codes, provide message integrity. Certain messages are also protected by the message authentication code HMAC, using SHA-1.

iii. **Cardholder account authentication**

SET enables merchants to verify that a cardholder is a legitimate user of a valid card account number. For this purpose SET uses X.509v3 digital certificates with RSA signatures.

iv. **Merchant authentication**

SET enables cardholders to verify that a merchant has a relationship with a financial institution allowing it to accept payment cards. For this purpose also, SET uses X.509v3 digital certificates with RSA signatures.

2.5.4.3 SET Participants

Figure 2.6 shows the participants in the SET protocol: -

i. **Cardholder**

In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over the Internet. A cardholder is an authorized holder of a payment card (MasterCard or Visa) that has been issued by an issuer.

ii. **Merchant**

A merchant is a person or organization with goods or services to sell to the cardholder. These goods or services are offered via a web site or by electronic mail. A merchant that accepts payment cards must open an account with an acquirer.

iii. **Issuer**

This is a financial institution, such as a bank, that provides the cardholder with the payment card. Accounts are applied for and opened by mail or in person. The issuer is responsible for the payment of the debt of the cardholder.

iv. **Acquirer**

This is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. Merchants will usually accept more than one credit card brand but don't want to deal with multiple bankcard associations or with multiple individual issuers. The acquirer provides authorization to the merchant that a given card account is active and that the proposed purchase does not exceed the credit limit. The acquirer also provides electronic transfer of payments to the merchant's account. The acquirer is reimbursed by the issuer over payment network for electronic funds transfer.

v. **Payment Gateway**

This is a function operated by the acquirer or a designated third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for authorization and payment functions. The merchant exchanges SET messages with the payment gateway over the Internet, while the payment gateway has some direct or network connection to the acquirer's financial processing system.

vi. **Certification Authority (CA)**

This is an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose. A hierarchy of CAs is used, in order for participants need not be directly certified by a root authority.

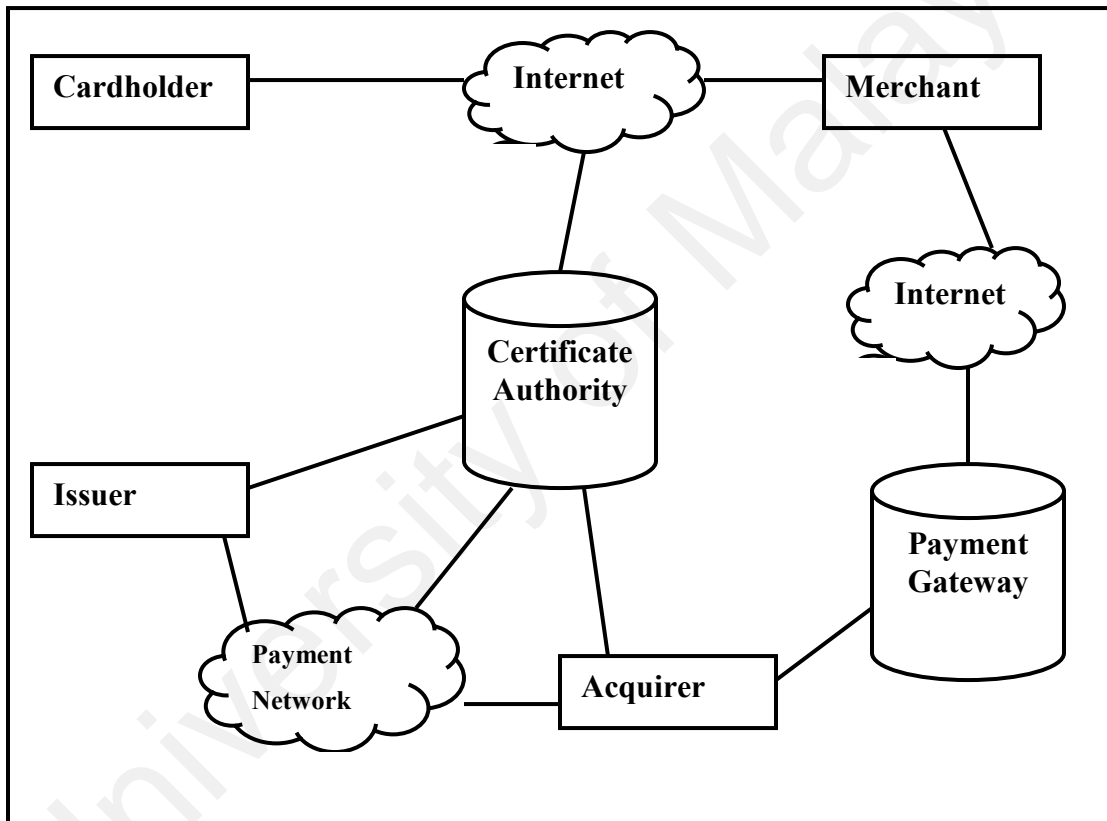


Figure 2.6

Secure Electronic Transaction Components

2.5.4.4 SET in Action

SET is a dynamic, automated protocol that allows a customer with a credit card to order items over the Internet from merchants, in a secure process. Processes in SET are as follows: -

i. **The customer opens an account.**

The customer obtains a credit card account, such as MasterCard or Visa, with a bank that supports electronic payment and SET.

ii. **The customer receives a certificate.**

After suitable verification of identity, the customer receives an X.509v3 digital certificate, which is signed by the bank. The certificate verifies the customer's RSA public key and its expiration date. It also establishes a relationship, guaranteed by the bank, between the customer's key pair and his or her credit card.

-Merchants Have Their Own Certificates

A merchant who accepts a certain brand of card must be in possession of two certificates for two public keys owned by the merchant: one for signing messages, and one for key exchange. The merchant also needs a copy of the payment gateway's public-key certificate.

iii. **The customer places an order.**

This is a process that may involve the customer first browsing through the merchant's web site to select items and determine the price.

iv. **The merchant is verified.**

In addition to the order form, the merchant sends a copy of its certificate, so that the customer can verify that he or she is dealing with a valid store.

v. **The order and payment are sent.**

The customer sends both order and payment information to the merchant, along with the customer's certificate. The order confirms the purchase of the items in the order form. The payment contains credit card details. The payment information is encrypted in such a way that it cannot be read by the merchant. The customer's certificate enables the merchant to verify the customer.

vi. **The merchant requests payment authorization.**

The merchant sends the payment information to the payment gateway, requesting authorization that the customer's available credit is sufficient for this purchase.

vii. **The merchant confirms the order.**

The merchant sends confirmation of the order to the customer.

viii. **The merchant provides the goods or service.**

The merchant ships the goods or provides the service to the customer.

ix. **The merchant requests payment.**

This request is sent to the payment gateway, which handles all of the payment processing.

2.5.4.5 Dual Signature

Before looking at the details of the SET protocol, let's discuss an important innovation introduced in SET: the dual signature. The purpose of the dual signature is to link two messages that are intended for two different recipients. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant doesn't need to know the customer's credit card number, and the bank doesn't need to know the details of the customer's order. The customer is afforded extra protection in terms of privacy by keeping these two items separate. However, the two items must be linked in a way that can be used to resolve disputes if necessary. The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods or services [20].

To see the need for the link, suppose that the customer sends the merchant two messages: a signed OI and a signed PI, and the merchant passes the PI to the bank. If the merchant can capture another OI from this customer, the merchant could claim that this

OI goes with the PI, rather than the original OI. The linkage prevents this. Figure 2.7 shows the use of a dual signature to meet this requirement.

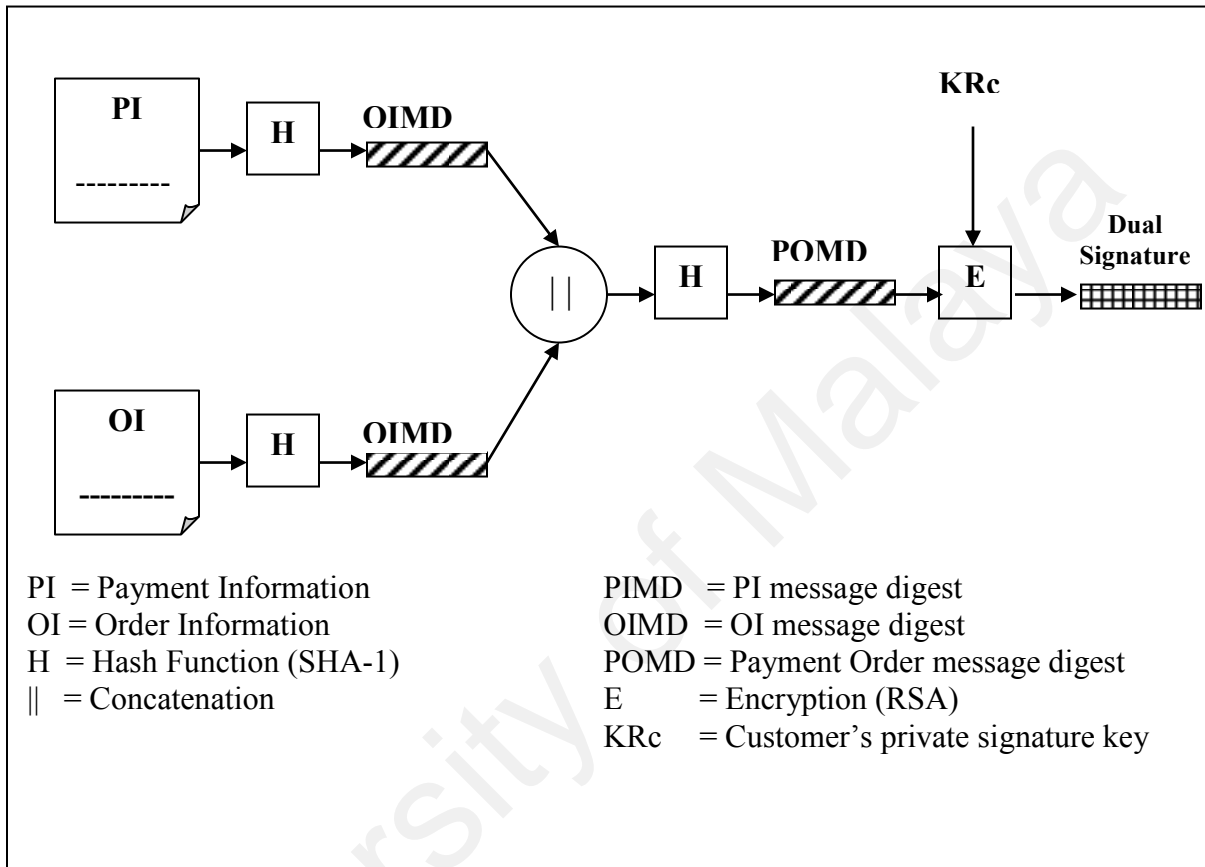


Figure 2.7

Construction of Dual Signature

The customer takes the hash (using SHA-1) of the PI and the hash of the OI. These two hashes are then concatenated and the hash of the result is taken. Finally, the customer encrypts the final hash with his or her private signature key, creating the dual signature. The operation can be summarized as follows, where KRc is the customer's private signature key: -

$$DS = E_{K_{Rc}} [H (H (PI) || H (OI))]$$

Now suppose that the merchant is in possession of the dual signature (DS), the OI, and the message digest for the PI (PIMD). The merchant also has the public key of the customer, taken from the customer's certificate. Then the merchant can compute the following two quantities, where K_{Uc} is the customer's public signature key: -

$$H (PIMD || H (OI) \text{ and } D_{K_{Uc}} [DS])$$

If these two quantities are equal, the merchant has verified the signature. Similarly, if the bank is in possession of DS, PI, the message digest for OI (OIMD), and the customer's public key, the bank can compute the following: -

$$H (H (PI) || OIMD) \text{ and } D_{K_{Uc}} [DS]$$

Again, if these two quantities are equal, the bank has verified the signature. In summary,

- i. The merchant has received OI and verified the signature.
- ii. The bank has received PI and verified the signature.
- iii. The customer has linked the OI and PI and can prove the linkage.

For example, suppose the merchant wants to substitute another OI in this transaction, to its advantage. It would then have to find another OI whose hash matches the existing OIMD. With SHA-1, this is deemed not to be feasible. Thus, the merchant cannot link another OI with this PI [20].

2.5.4.6 Payment Processing

SET defines a variety of transaction protocols that use the cryptographic concepts to securely conduct electronic commerce. There are several transaction types. Table 2.1 lists the transaction types supported by SET [21].

University of Malaya

SET TRANSACTION TYPES	
Certificate inquiry and status	If the CA is unable to complete the processing of a certificate request quickly, it will send a reply to the cardholder or merchant indicating that the requester should check back later. The cardholder or merchant sends the <i>Certificate Inquiry</i> message to determine the status of the certificate request and to receive the certificate if the request has been approved.
Purchase inquiry	Allows the cardholder to check the status of the processing of an order after the purchase response has been received. Note that this message does not include information such as the status of authorization capture and credit processing.
Authorization reversal	Allows a merchant to correct previous authorization requests. If the order will be not completed, the merchant reverses the entire authorization. If part of the order will not be completed (such as when goods are back ordered), the merchant reverses part of the amount of the authorization.
Capture reversal	Allows a merchant to correct errors in capture requests such as transaction amounts that were entered incorrectly by a clerk.
Credit	Allows a merchant to issue a credit to a cardholder's account such as when goods are returned or were damaged during shipping. Note that the SET <i>Credit</i> message is always initiated by the merchant, not the cardholder. All communication between the cardholder and the merchant that result in a credit being processed happens outside of SET.
Credit reversal	Allows a merchant to correct a previously request credit.
Payment gateway certificate request	Allows a merchant to query the Payment Gateway and receive a copy of the gateway's current key-exchange and signature certificates.
Batch Administration	Allows a merchant to communicate information to the Payment Gateway regarding merchant batches.
Error message	Indicates that a responder rejects a message because it fails format or content verification tests.

Table 2.1

SET Transaction Types

The process in payment processing included: -

- i. Purchase request.
- ii. Payment authorization.
- iii. Payment capture.

I. Purchase request

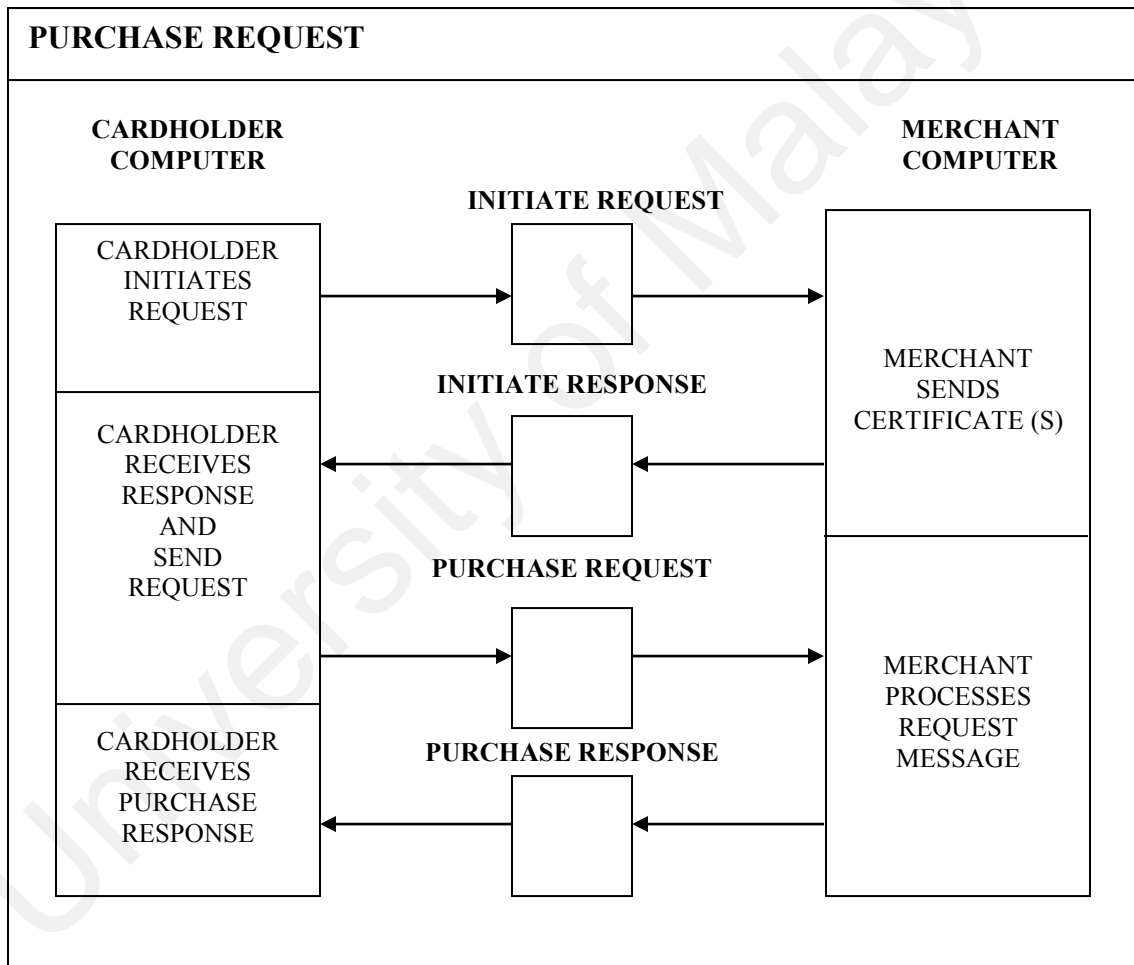


Figure 2.8

Purchase Request

Before the purchase request exchange begins, the cardholder has completed browsing, selecting, and ordering. The end of this preliminary phase occurs when the merchant sends a completed order form to the customer. All of the preceding occurs without the use of SET.

The purchase request exchange consists of four messages [22]: -

- Initiate Request.
- Initiate Response.
- Purchase Request.
- Purchase Response.

To send SET messages to the merchant, the cardholder must have a copy of the certificates of the merchant and the payment gateway. The customer requests the certificates in the Initiate Request message, sent to the merchant. This message includes the brand of the credit card that the customer is using. The message also includes an ID assigned to this request/response pair by the customer.

The merchant generates a response and signs it with its private key. The response includes a transaction ID for this purchase transaction. In addition to the signed response, the Initiate Response message includes the merchant's certificate and the payment gateway's certificate.

The cardholder verifies the merchant and gateway certificates by means of their respective CA signatures and then creates the order information (OI) and payment information (PI). The transaction ID assigned by the merchant is placed in both the OI

and PI. The OI doesn't contain explicit order data such as the number and price of items. Rather, it contains an order reference generated in the exchange between merchant and customer during the shopping phase before the first SET message [22].

Next, the cardholder prepares the Purchase Request message (see Figure 2.9).

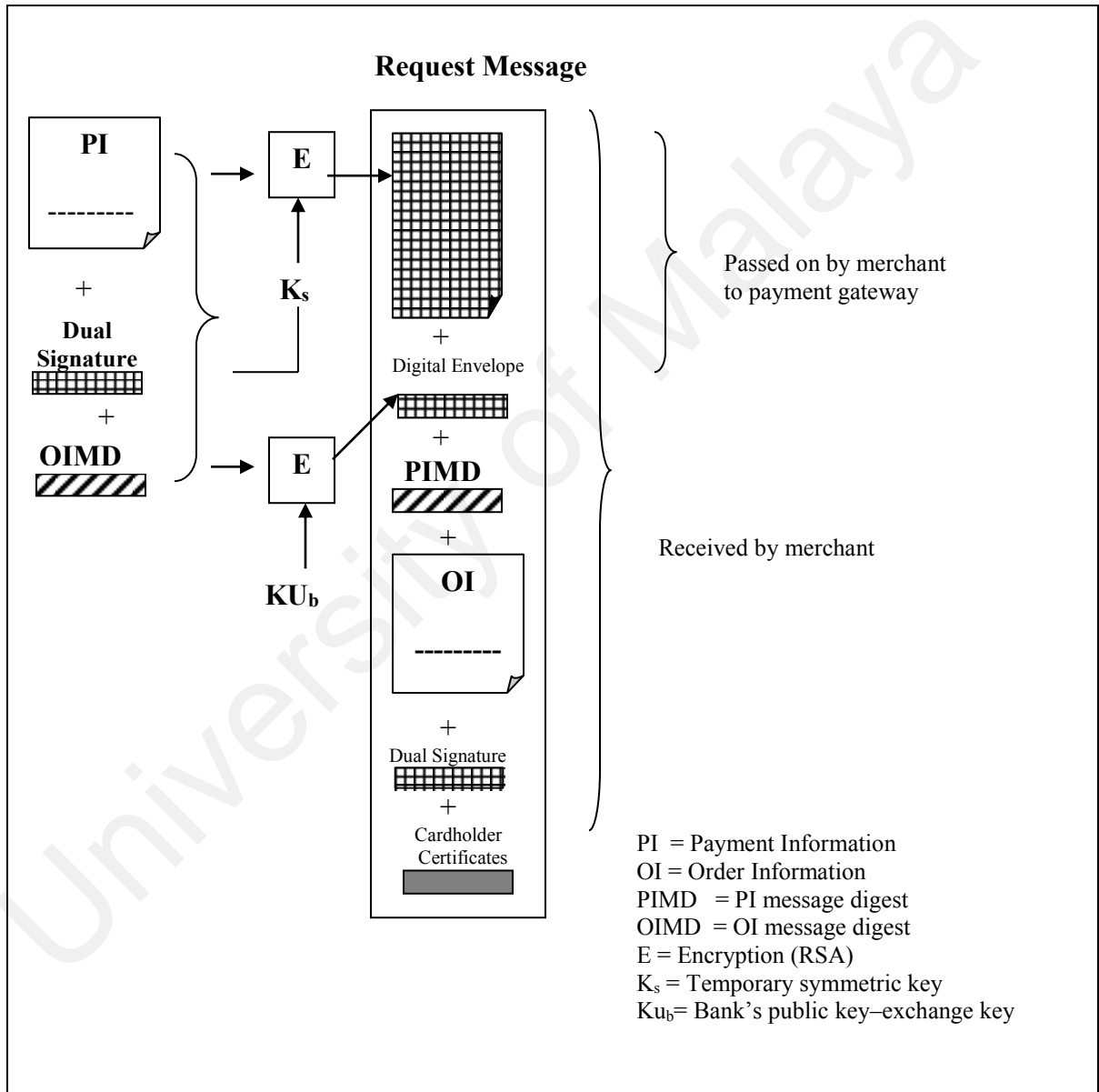


Figure 2.9

Cardholder Sends Purchase Request

For this purpose, the cardholder generates a one-time DES encryption key, known as a *session key*. The message includes as follows [22]: -

- **Purchase-related information.**

This information will be forwarded to the payment gateway by the merchant and consists of the PI and a dual signature. The dual signature is a signature that covers both the PI and the OI. It's constructed in such a way that both the merchant and the payment gateway can verify the signature, even though the merchant only sees the OI and the payment gateway only sees the PI. Both the PI and the dual signature are encrypted using the one-time session key. Finally, the session key is encrypted with the public key of the payment gateway and added to the message; only the payment gateway will be able to decrypt and read the session key and therefore only the payment gateway will be able to recover the PI.

- **Order-related information.**

This information is needed by the merchant and consists of the OI and the dual signature. The merchant uses the dual signature to verify that the OI is valid.

- **Cardholder certificate.**

This contains the cardholder's public key. It's needed by both the merchant and the payment gateway.

When the merchant receives the Purchase Request message, it performs the following actions (Figure 2.10)[23]: -

- i. Verifies the cardholder certificates by means of its CA signatures.
- ii. Verifies the dual signature using the customer's public signature key. This ensures that the order has not been tampered with in transit and that it was signed using the cardholder's private signature key.
- iii. Processes the order and forwards the payment information to the payment gateway for authorization.
- iv. Sends a purchase response to the cardholder.

The **Purchase Response** message includes a response block that acknowledges the order and references the corresponding transaction number. This block is signed by the merchant using its private signature key. The block and its signature are sent to the customer, along with the merchant's signature certificate.

When the cardholder software receives the Purchase Response message, it verifies the merchant's certificate and then verifies the signature on the response block. Finally, it takes some action based on the response, such as displaying a message to the user or updating a database with the status of the order.

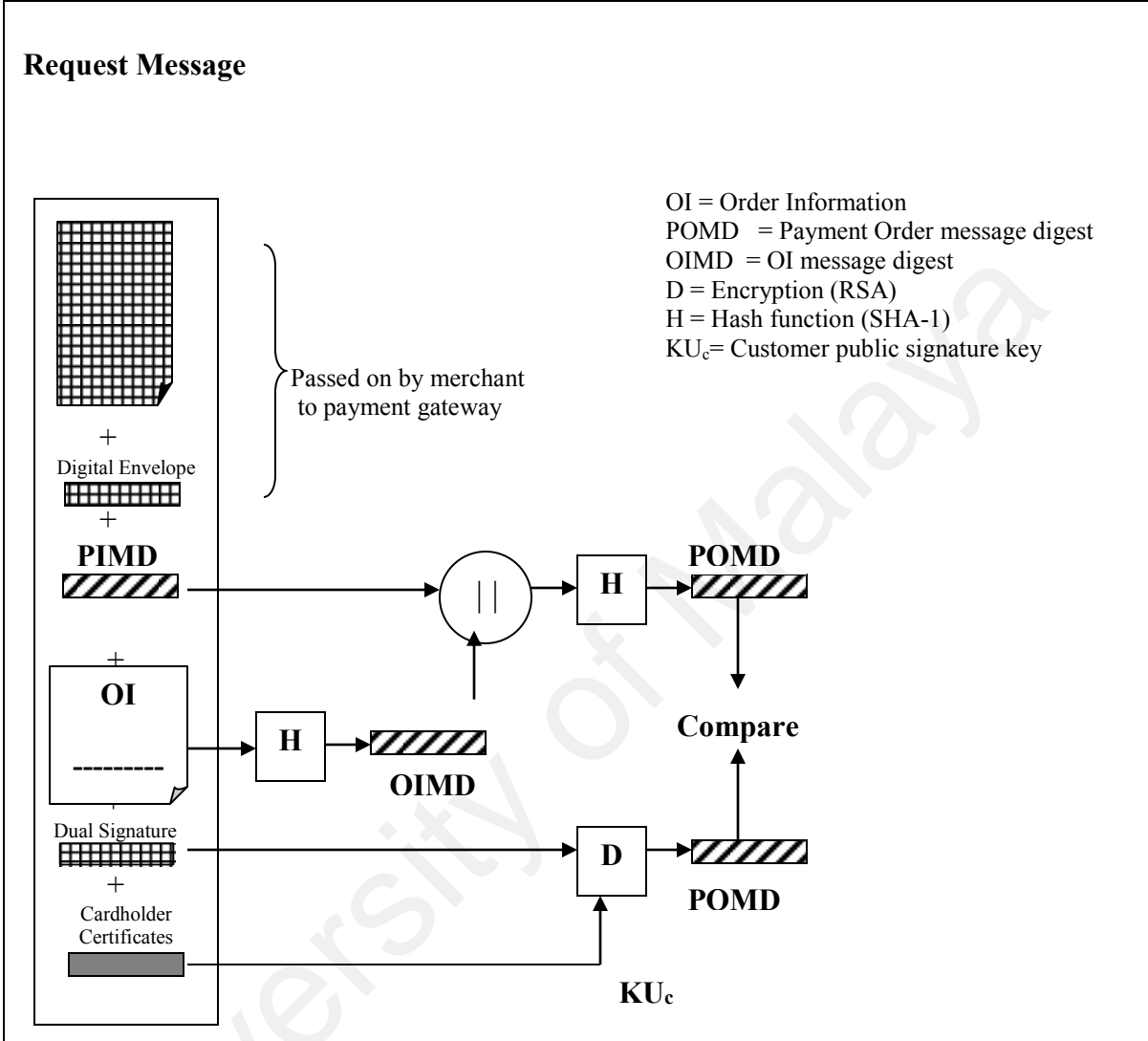


Figure 2.10
Merchant Verifies Customer Purchase Request

II. Payment Authorization

During the processing of an order from the cardholders, the merchant authorizes the transaction with the payment gateway. The payment authorization ensures that the issuer approved the transaction. This authorization grantee that the merchant will receive payment and allow the merchant to provide the services or goods to the customer.

The payment authorization exchange consists of two messages: -

- Authorization Request
- Authorization Response.

The merchant sends an Authorization Request message to the payment gateway consisting of the following: -

i. Purchase-related information.

This information was obtained from the customer and consists of

- The PI.
- The dual signature, calculated over the PI and OI, signed with the customer's private signature key.
- The OI message digest (OIMD).
- The digital envelope.

ii. Authorization-related information

This information is generated by the merchant and consists of

- An authorization block that includes the transaction ID signed with the merchant's private signature key and encrypted with a one-time symmetric key generated by the merchant.
- A digital envelope. This is formed by encrypting the one-time key with the payment gateway's public key-exchange key.

ii. Certificates.

The merchant includes the cardholder's signature key certificate (used to verify the dual signature), the merchant's signature key certificate (used to verify the merchant's signature), and the merchant's key-exchange certificate (needed in the payment gateway's response).

The payment gateway performs the following tasks: -

- Verifies all certificates.
- Decrypts the digital envelope of the authorization block to obtain the symmetric key and then decrypts the authorization block.
- Verifies the merchant's signature on the authorization block.
- Decrypts the digital envelope of the payment block to obtain the symmetric key and then decrypts the payment block
- Verifies the dual signature on the payment block.

- Verifies that the transaction ID received from the merchant matches that in the PI received (indirectly) from the customer.
- Request and receives an authorization from the issuer.

Having obtained authorization from the issuer, the payment gateway returns an **Authorization Response** message to the merchant. It includes the following elements: -

i. Authorization-related information

Includes an authorization block, signed with the gateway's private signature key and encrypted with a one-time symmetric key generated by the gateway. Also includes a digital envelope that contains the one-time key encrypted with the merchant's public key exchange key.

ii. Capture token information

This information will be used to effect payment later. This block is of the same form as (1) namely, a signed, encrypted capture token together with a digital envelope. This token is not processed by the merchant. Rather it must be returned, as is, with a payment request.

iii. Certificate

The gateway's signature key certificate. With the authorization from the gateway, the merchant can provide the goods or service to the customer.

III. Payment Capture

To obtain payment, the merchant engages the payment gateway in a payment capture transaction, consisting of a Capture Request and a Capture Response message.

For the **Capture Request** message, the merchant generates, signs and encrypts a capture request block, which includes the payment amount and the transaction ID. The message also includes the encrypted capture token received earlier (in the Authorization Response) for this transaction, as well as the merchant's signature key and key exchange key certificates [21].

When the payment gateway receives the capture request message, it decrypts and verifies the capture request block and decrypts and verifies the capture block. It then checks for consistency between the capture request and capture token. It then creates a clearing request that is sent to the issuer over the private payment network. This request causes funds to be transferred to the merchant's account.

The gateway then notifies the merchant of payment in a **Capture Response** message. The message includes a capture response block that the gateway signs and encrypts. The message also includes the gateway's signature key certificate. The merchant software stores the capture response to be used for reconciliation with payment receives from the acquirer [23].

2.5.4.7 SET in Practice

Purchase by credit card over the Internet involves many functions and actions, of which only a few are implemented in SET. SET provides a payment protocol that defines the communication among cardholder, merchant, and payment gateway for purchases and refunds. It also provides a key exchange protocol, by which the various parties exchange public-key certificates. A number of activities for this scope are required. Both cardholders and merchants must obtain certificates that verify their public keys. The process of browsing and selecting goods for purchase is also outside the scope of SET.

On the cardholder side, the cardholder must obtain and install the SET software and arrange a credit card account that supports SET and provides the needed certificate. The merchant must install the merchant-side SET software and integrate this with a web-based product or service ordering system. The merchant's software requirements are more complex, because communication is required both with the cardholder and the payment gateway.

Thus, for SET to work, the supporting software and certification functions must be in place. But, with the backing of the two largest credit-card organizations, Visa and MasterCard, SET is poised to become the standard means for credit card transactions via the Internet.

2.6 The Chosen Protocol

In this research, the SET payment protocol is been chosen to be implemented in the project during the card credit transaction.

2.6.1 Why SET?

The protocol is been chosen because SET provides three services which different from others payment protocol: -

i. Privacy via cryptography

The SET protocol uses two forms of cryptography to ensure the confidentiality of the transactions. First, an asymmetric form known as RSA is used for signatures and public-key encryption of symmetric encryption keys and bank card numbers, and then a symmetric form called DES takes care of the encryption of the data that is to be transmitted during the transaction. It might be of interest to take a closer look at these two forms of cryptation, so lets start with RSA.

- **RSA**

RSA is form of cryptography developed at MIT by Ron Rivest, Adi Shamir, and Leonard Adleman back in 1977. RSA builds on the concept of asymmetric or *public-key cryptography* that was introduced in 1976 by Whitfield Diffie and Martin Hellman [24] in order to solve the key management problem.. It uses pairs

of so called *private* and *public* keys, that are mathematically related to each other. The public keys are shared over any network (including the Internet) and used to encrypt messages to the owners of them. The owner then decrypts the message using his/her private key. This way anyone can send an encrypted message, using only the public keys, but only someone in possession of the matching private key can decrypt the message. The need for exchanging the encryption keys over safe communication channels is thus eliminated, as user can make their public key openly available over the Internet without danger [25].

- ***DES***

DES (Data Encryption Standard) is an encryption block cipher defined and endorsed by the U.S. government in 1977 as an official standard. It was originally developed at IBM, and is the most well-known and widely used cryptographic system in the world. It is a symmetric cryptosystem, which means that both the sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message. DES can also be used for single-user encryption, such as to store files on a hard disk in encrypted form. In a multi-user environment, secure key distribution may be difficult, as it requires access to completely safe communication channels. This is also its major disadvantage compared to asymmetric public-key cryptography, which provides an ideal solution to this problem. Why is then DES used in the SET protocol? It's used because it's much faster than RSA, generally at least 100 times as fast [26].

So how does the SET protocol combine the best of the two encryption methods? It does so by encrypting the message data using a randomly generated symmetric DES encryption key. This key is, in turn, encrypted using the message recipient's RSA public key. This second encryption is referred to as the "digital envelope" of the message and is sent to the recipient along with the encrypted message itself. After receiving the digital envelope, the recipient decrypts it using his or her private key and obtains the randomly generated symmetric key and then uses the symmetric key to unlock the original message [27].

In other words, SET protects the cardholder's privacy to a certain extent by making sure that each of the involved parties knows only as much as is needed to perform the credit card payment and its validation correctly. Most credit card payments in the Internet are usually carried out using a server-side authenticated and secure connection based on the secure sockets layer (SSL)-protocol. This protects the details of the cardholder's credit card (example the credit card number) from malicious third parties, but the merchant still learns the credit card number. If we compare SET to credit card payments as they are performed today in the Internet, then SET adds the following to protect the cardholder's privacy [11]: -

- i. The merchant never learns details about the cardholder's credit card (example the credit card number). This reduces the risk of fraud by the merchant.

- ii. The payment gateway (which is usually the same instance as the acquirer) does not learn the details of the cardholder's order.

- ***How safe is SET?***

SET is designed to be used with 1,024-bit cipher keys, making it one of the strongest encryption applications in public use. The time it would take to break the encryption described here, especially with all the various level of encryption that are occurring, is upwards to 2,800,000,000,000 years using 100 computers each able to process 10,000,000 instructions per second. Even then, only a single message could be broken and with the next message, the entire process would need to start over. While it may seem like overkill, the protocol is quite attractive to all those wanting to conduct widespread business over the Internet, especially the card issuers who have the most to lose from fraud. SET has been approved for export from the US, provided that it's only used in financial transactions, and not as a mechanism to pass secret or sensitive information to those outside the US [28].

To summarize, SET enhances the privacy of the cardholder by making sure that none of the involved parties learns everything about a whole transaction. This is not the case in today's Internet, where the merchant learns everything. SET guarantees this by splitting the knowledge between the merchant and the payment gateway. If these two parties collude, then they know exactly as much as the merchant does in today's Internet.

ii. Integrity via hashing and digital signing

The SET protocol ensures data integrity by using one-way cryptographic hashing algorithms and digital signatures to make sure that the messages transmitted have not been modified in transit. A hashing algorithm is a function used to calculate a unique integrity value, called the hash value or message digest, from the original data (the message). But the hash function by itself does not guarantee absolute data integrity. For this it needs to be combined with a secret encryption key. Here is where digital signing comes into the picture. A digital signature is simply a hash value that has been encrypted using the sender's private key before being appended to the rest of the message. The recipient decrypts the hash value using the sender's (mathematically matching) public key and checks the resulting value. This procedure ensures the integrity of the data, since no one can encrypt a new and false message without the right private key [29].

However, anyone can generate a private/public key pair and impersonate someone else, so it's essential to have some mechanism that binds the public key to the sender in a trustworthy way. This is where the digital certificates come into the picture.

iii. Authentication via digital certificates

Authentication deals with assuring that the message was in fact sent by the party who claims to have sent it. As mentioned above, each party in a SET transaction is authenticated by the use of digital certificates. These certificates are issued by a trusted third party known as a Certification Authority (CA), which vouches for the identity of the

certificate holder. Each digital certificate contains both owner identification information, and a copy of one of the owner's public keys. Furthermore each certificate is digitally signed by the Certificate Authority to ensure its validity. To administrate the validity of all certificates an hierarchy of trust has been constructed (see figure 2.11 below).

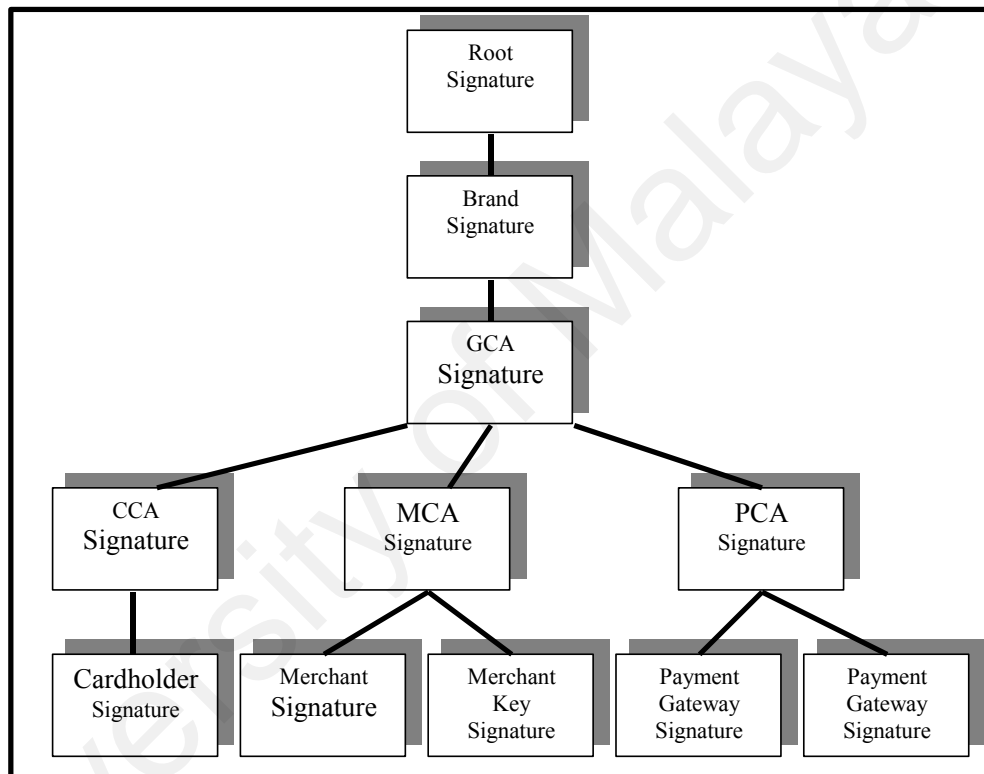


Figure 2.11

SET Certificates hierarchy of trust.

As illustrated in figure 2.11 there are a number of different digital certificates specified by the SET protocol. As mentioned earlier every party involved must have the appropriate certificates, so obviously both the cardholder, the merchant and the acquirer must have theirs. But this is not enough. The different Certificate Authorities (example:

the cardholder, merchant, acquirer, brand and root Certificate Authorities) must also have theirs, and they are arranged in a tree of trust with the one unique Root CA as the base and origin of all the others .SET certificates are thus verified through this hierarchy of trust. Each certificate is linked to the signature certificate of the entity that digitally signed it. By following the trust tree to a known trusted party, one can be assured that the certificate is valid. For example, a cardholder certificate is linked to the certificate of the Issuer (or the Brand on behalf of the Issuer). The Issuer's certificate is linked back to a root key through the Brand's certificate. The public signature key of the root is known to all SET software and may be used to verify each of the certificates in turn [30].

2.6.2 SET Requirement

The SET specification states the following requirements for secure credit card payments over the Internet: -

- **Confidentiality**

The consumers want to be sure that their payment and personal information is safe and only available to the intended party. Encryption is used in order to achieve confidentiality.

- **Integrity**

The information sent during the SET session must under no circumstances be tampered by malicious third parties. Digital signatures are used to verify the integrity of the transmitted data.

- **Mutual authentication**

The merchants want to be sure that the customer is a legitimate user of a credit card. This is done by a mechanism that links a cardholder to a specific account number, which reduces both the risk of fraud and the costs of the payment processing. The customer again wants to be sure the merchant can accept credit card transactions through its relationship with a financial institution. This means that the cardholders must be able to identify a merchant they can conduct secure transactions with. For these both types of authentication digital signatures and certificates are used [30].

- **Good design and high security**

SET must be well designed and implement the best security methods in order to protect all the participating parties in a transaction. The specification is well tested and only highly secure cryptographic algorithms are used.

- **Independent of other security mechanisms:**

SET is not depending on any transport security protocol, but does not either prevent usage of any. IPSec and SSL or TLS can be safely used in SET.

- **Platform independence:**

SET is not depending on any specific hardware platform or operating system, and can therefore be used on almost any system.

2.7 Ms Outlook Express

2.7.1 Introduction

Microsoft includes a basic e-mail client with the Internet Explorer 4.0 distribution, called Outlook Express. This client software will probably be more than sufficient for most individuals' needs relating to e-mail as well as for Internet news groups, access to on-line directories, and support for personal address management. Also incorporated into the Outlook Express client is support for SI MIME e-mail security through message encryption and decryption as well as digital signature signing and certifying.

2.7.2 Why Ms Outlook Express?

Following Netscape's lead, Microsoft began incorporating S/MIME e-mail support in its Internet web and e-mail clients (Internet Explorer, Outlook, and Outlook Express) by the fall of 1997.[45] With support from these two massively dominant vendors in the browser market, S/MIME stands a very good chance of becoming a de

facto standard for casual e-mail security no matter what security standard the IETF ultimately selects for secure e-mail. As implemented currently, S /MIME has a number of advantages over the other secure e-mail approaches such as [45]: -

- User do not need to be using the same e-mail client as they correspondent; as long as they both have S /MIME compliant clients, they should be able to exchange encrypted and signed messages interoperable.
- It currently can be exported from the United States, so it can (at least in theory) be used to sign and encrypt messages both by U.S. users and by international users.
- S/MIME requires the use of triple DES, which is considered secure for most purposes.
- S/MIME-enabled clients are widely and freely available, and include the most popular Internet clients from Netscape and Microsoft.
- S/MIME clients can exchange both e-mail messages and e-mail attachments that have been digitally signed and or encrypted, eliminating concerns about the authentication or integrity of a message connected with an encrypted or signed enclosure.
- Certificates and public keys use standard formats, and most CA providers' certificates will be able to be used interchangeably under S /MIME; there is no requirement for clients to support any proprietary certificate file formats in order to interoperate.

CHAPTER 3

METHODOLOGY

3.1 Introduction

Nowadays, there are a vast number of tools and methodologies available for system development. System development is dynamic and always undergoing major change. It refers to all activities that go into producing an information system solution. One of the most common system developments is system development life cycle or SDLC. It is a traditional methodology consists of activities such as initiating and planning, analyzing, designing, implementing, testing and maintaining [46].

A software development methodology is a series of process that if followed can lead to the development of an application [31]. In this project, the flow of research methodology is based on the common activities in the SDLC phases which called as Waterfall Method[46]. Meanwhile, the flow of the system development is based on the object oriented software development (OOSD) using Unified Approach (UA) where this methodology is being adopted in the research analysis phase to structure and organize the system requirement in forms of model and diagram.

3.2 Research Methodology

The systems development life cycle (SDLC) is a common methodology for system development in many organizations, featuring several phases that mark the progress of the system analysis and design effort [31]. Therefore, this common life cycle will be adopted into this project research methodology phases. Research methodology shows how the research is done from the starting point until the end. Phases include in the research methodology are project initiating and planning, analyzing, designing, implementing, testing and result and discussion.

3.2.1 Project Initiating and Planning

The first phase in the research methodology is called project initiating and planning. The two major activities in this phase are the preliminary investigation and data sources and instrumentation.

3.2.1.1 Preliminary investigation

The purpose of this activity is to identify why the research is done, why system should be developed and to capture the idea of how to construct ETS model. To gain this purpose, literature review from the past journals and article is being done to derive the project objective, scope, problem statement and the construction of ETS model [20].

Refer Chapter One for the detail explanation on the project objective, scope and problem

statement. Meanwhile for ETS model, refer Figure 3.1. ETS model shows how the element inside it interacts with each other in one organization.

The model is important as the basic model for Electronic Tendering System. It is designed based on SET protocol [20] that is already discussed in Chapter 2. Nevertheless, the model is slightly different with the original SET protocol because it has been designed in order to suit and fulfill the objective and the scope of ETS. There are eight elements that must have in ETS and without them ETS cannot be implemented. The ETS elements are Cardholder, ETS Website, Merchant, Acquirer, Microsoft Outlook, Certificate Authority, Payment Gateway and Issuer. The connection flow between the elements in ETS is shown by the connection arrow.

Furthermore, the position of the elements in ETS model is as in Figure 3.1 because it represents the step-by-step process happened in ETS. Generally, the tendering process in ETS starts when cardholder logs in to ETS website whether to send tender proposal (using Microsoft Outlook) or download the tender document. The term of cardholder is used in the model instead of customer because the user of the system must be the credit card owner. The ETS website must belong to one organization and the merchant term is used to represent the owner of the website. The merchant has to open an account with the acquirer who is a financial institution that processes payments between the bank issuer and merchant. Nevertheless, the acquirer function is not further described because ETS does not cover the payment processing.

When the cardholder chooses to download the tender document, the certificate authority starts to issue public-key certificates for customer, merchants, and payment gateways. Then the merchant will verify the cardholder credit card by sending the

authorization message to payment gateway where the payment gateway is a function operated by the acquirer or a designated third party that processes merchant payment messages. Next, the authorization message will be sent to the issuer of the credit card. After verification, the message will be returned to payment gateway. Here, the payment gateway will pass the message response to merchant. The response message will allow the merchant to give the permission to the cardholder to download the tender document. The detail explanation on this model and its elements is discussed in the analysis phase.

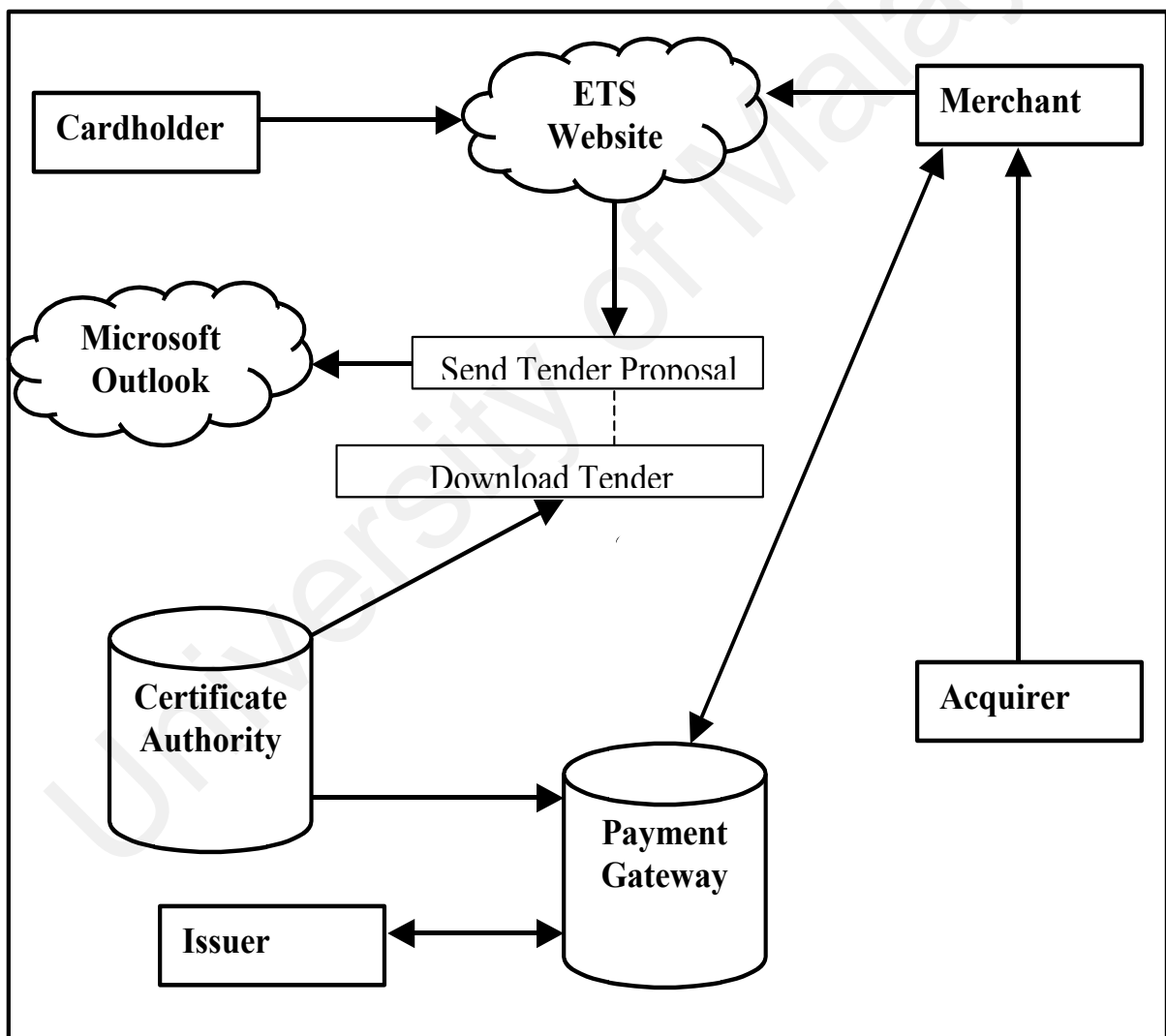


Figure 3.1

The Model of Electronic Tendering System

3.2.1.2 Data Sources and Instrumentation

The purpose of this activity is to do the data collection and to identify the user/system requirement. During this research, there are two types of data are gathered:

i. Primary data

Primary data is a collection of data that is gathered from interviews, surveys, experiment or questionnaires. Therefore, in this research, results from the questionnaires and interviews of the staff in the selected company have been collected. The questionnaires and interviews are based on the tendering process in their company.

ii. Secondary data

Secondary data is a collection of data that is gathered in form of hardcopy.

Sources for the secondary data that have been collected for the research are:

- Books related with the electronic commerce and SET.
- Journals that consist the approaches to the secure credit card transaction using SET.
- Articles from the Internet on the tendering process and SET.

3.2.2 Analysis

The second phase in the research methodology is called as analysis. The purpose of analysis is to structure and organize the system requirement in forms of diagrams and

description (models) that can be analyzed to show deficiencies of the system elements. Since there are a lot of diagrams that will be designed, therefore, object oriented software development or known, as OOSD based on Unified Approach is adopted into the research analysis.

3.2.2.1 The Unified Approach

The object-oriented methodology based on the Unified Approach is used as the software development methodology for this project development. The Unified Approach (UA) is the combination of the best practices, processes, methodologies and guidelines along with UML notation and diagrams for better understanding object-oriented concept and software development [31]. The functionality of the Electronic Tendering System (ETS) system based on the Unified Approach methodology is discussed in details in Chapter Four.

Figure 3.1 shows the processes and components of the Unified Approach.

The processes in the Unified Approach are:

- Use-case development
- Object-oriented analysis
- Object-oriented design
- Incremental development and Prototyping
- Continuous testing

The methods and technology that are employed include:

- Unified modeling language used for modeling
 1. Class diagram
 2. Use case diagram
 3. Behavior diagram
 - 3.1 Interaction diagram
 - 3.1.1 Sequence diagram
 - 3.1.2 Collaboration diagram
 - 3.2 Statechart diagram
 - 3.3 Activity diagram
 4. Implementation diagram
 - 4.1 Component diagram
 - 4.2 Deployment diagram

The major benefits of Unified Approach are:-

- It allows iterative development by allowing us to go back and forth between the design and modeling or analysis phases, which allows no form of backtracking.
- The components can be easily replaced, modified and reused.
- Provide faster development, reusability, increased quality and easier maintenance

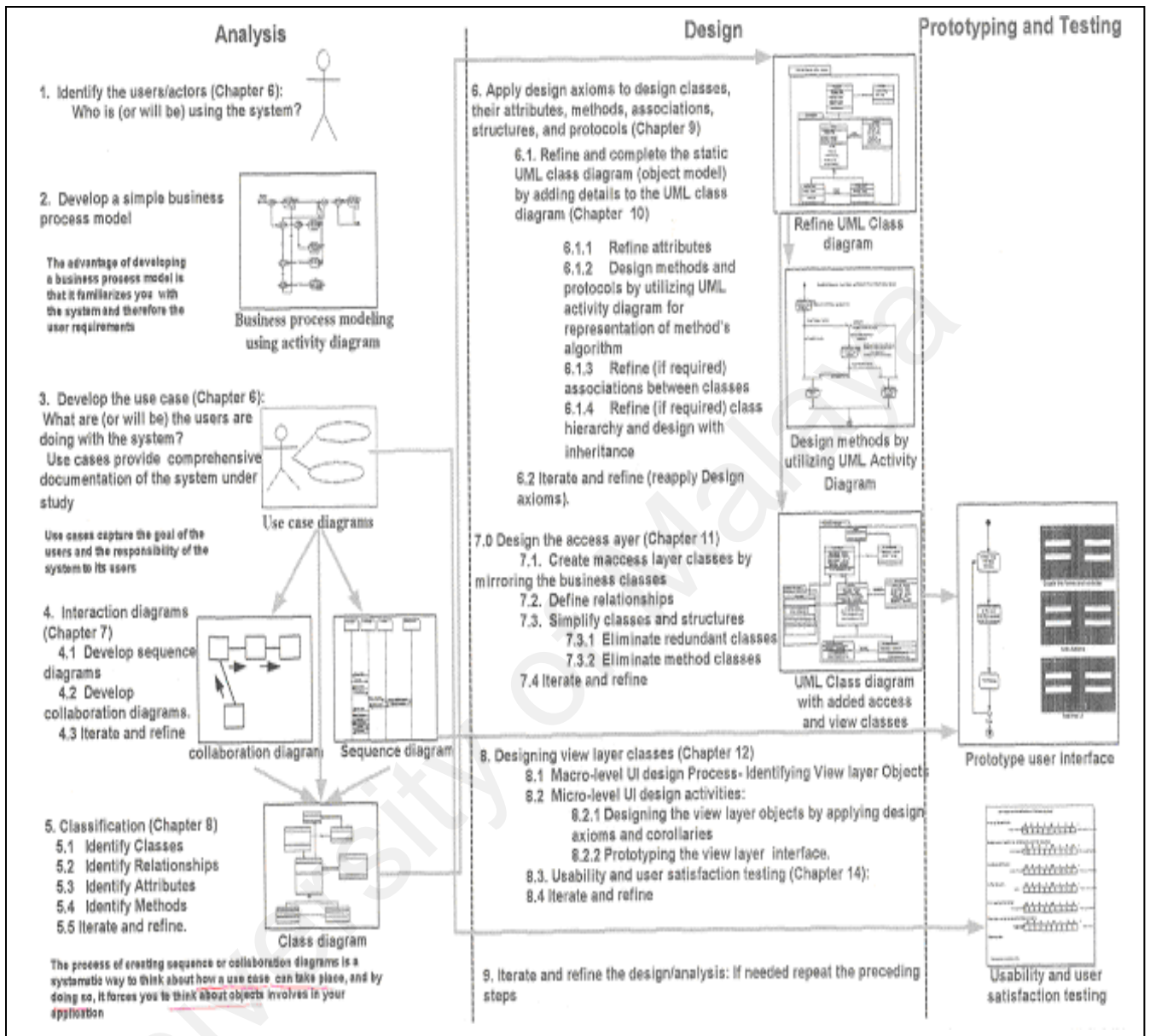


Figure 3.2

The Processes and Components of The Unified Approach.

3.2.2.1.1 Object-oriented Analysis Process

The object-oriented analysis (OOA) phase of the unified approach uses actors and use cases to describe the system from the user's perspective. The actors are external factors that interact with the system meanwhile use cases are scenarios that describe how actors use the system. The OOA process consists of the following steps:

1. Identify the actors.
2. Develop a simple business process model using UML activity diagram.
3. Develop use case.
4. Prepare interaction diagram.
5. Classification –develop a static UML class diagram.
6. Iterate and refine. (If needed)

3.2.2.1.1.1 Identifying the actors

The term actor represents the role of user plays with respect to the system. Furthermore, an actor should represent a single user. Table 3.1 shows the actors that have been identified in this project. The actors, are identified based on the following questions [31]:

- i. Who is using the system?
- ii. Who affects the system?
- iii. Which external hardware or other systems use the system to perform tasks?
- iv. What problems does this application solve? (For whom)

The actors below refer to the elements or participants in ETS. The operation of ETS is depended on these elements, therefore all of the participants must exist in one organization.

ACTORS	FUNCTIONS
1. Customer	Interact with the merchant over the internet to deal about tender .For example, to download tender document, to send tender proposal or others.
2. Merchant	Organization with goods or services to sell to the customer.
3. Administration	Person in charge in merchant.
4. Issuer	A financial institution, such as a bank, that provides the customer with the payment card.
5. Certification Authority (CA)	An entity that is trusted to issue public-key certificates for customer, merchants, and payment gateways.
6. Payment Gateway	A function operated by the acquirer or a designated third party that processes merchant payment messages.
7.Acquirer	A financial institution that establishes an account with a merchant and processes payment card authorizations and payments.

Table 3.1
Lists of Actors

3.2.2.1.1.2 Business Process Modeling

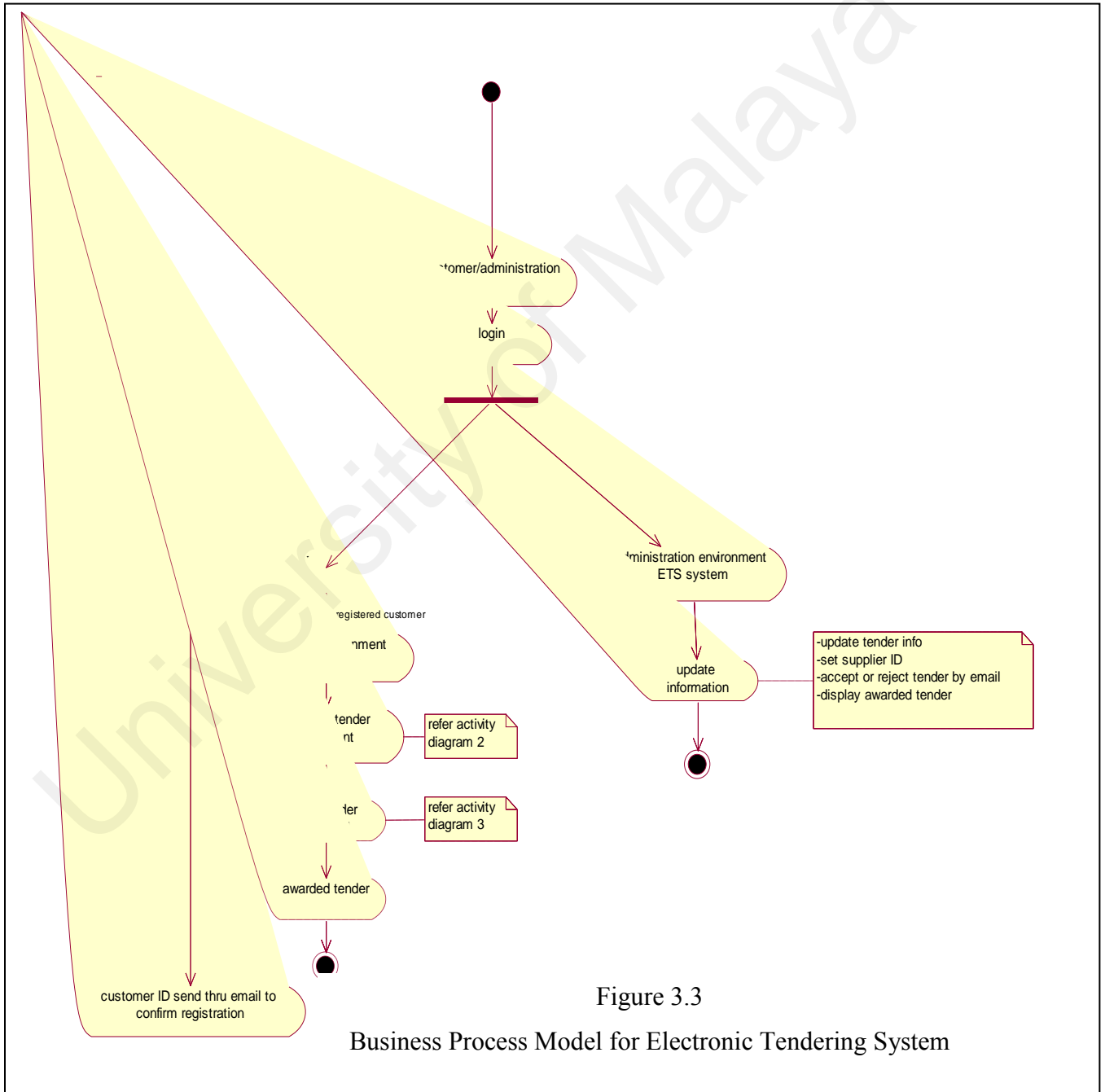
After identifying the actors, the next step is to develop one simple business process model using UML activity diagram. The development of this business process model is based on ETS model (Figure 3.1). The main idea behind the business process is to get a basic model without spending too much time on the process because it can be very time consuming. The advantage of developing a business process model is to become more familiar with the system, understanding the user requirement and helping in developing use cases. Figure 3.3 shows the business process modeling for the develop system.

I. Activity Diagram 1

When the customer or administrator browse to Electronic Tendering System website, the first page that will be appear is the login page. For the new customer, they have to register as members by filling up the registration form. They cannot directly use the system after registration. This is because, the administrators need to verify their company information and profile. As the confirmation of registration, administrator will send to them their customer password and ID through email.

Meanwhile, for the registered customer, after login, they will access to the Customer ETS Environment. Here, they can access all the menus in the system such as downloading the tender document, sending the tender proposal, viewing the awarded tender and others. Refer activity diagram Figure 3.4 and 3.5 to know the detail process of downloading the tender document and sending the tender proposal.

For the administrator, after registration, they will access to the Admin ETS Environment. Here, they may access all the menus in the system such as update new tender, update awarded tender, accept or reject customer and others. Meanwhile, for new administrator, they have to fill up their information and set up their id and password before using the system.



The activity diagram describes the process of downloading of the tender document using SET Payment Processing Protocol. This is the major activity in ETS because it involves a lot of processes. Refer Figure 3.4.

Every customer who wants to use ETS must open an account with the issuer where the issuer will provide credit card to the customer. The merchant is also facing the same process where it has to register and open an account with acquirer.

Before the SET protocol begins, it's expected that the cardholder has browsed the merchants Website and has selected the tender document. To send SET messages to the merchant, the customer must have a copy of the certificates of the merchant and the payment gateway. The customer requests the certificates in the Initiate Request message, sent to the merchant. This message includes the brand of the credit card that the customer is using. The message also includes an ID assigned to this request/response pair by the customer.

The merchant generates a response and signs it with its private key. The response includes a transaction ID for this purchase transaction. In addition to the signed response, the Initiate Response message includes the merchant's certificate and the payment gateway's certificate.

The customer verifies the merchant and gateway certificates by means of their respective CA signatures and then creates the order information (OI) and payment information (PI). The transaction ID assigned by the merchant is placed in both the OI and PI. The OI doesn't contain explicit order data such as the number and price of items. Rather, it contains an order reference generated in the exchange between merchant and customer during the shopping phase before the first SET message.

Next, the customer prepares the Purchase Request message. For this purpose, the customer generates a one-time DES encryption key, known as a *session key*. The message includes Purchase-related information, Order-related information and customer certificate.

The customer sends the Purchase Request message to the merchant. Merchant then receives the Purchase Request message. During the processing of an order from the customer, the merchant authorizes the transaction with the payment gateway. The merchant sends an Authorization Request message to the payment gateway consisting of Purchase-related information, Authorization-related information and Certificates. Payment Gateway receives the message and requests the authorization from the card issuer.

After receiving the request authorization message, issuer will verify and validate the card and send back the verification message to the payment gateway. Next, Payment Gateway will return the authorization response to the merchant. The message consists of Authorization-related information, Capture token information and Certificate. Then merchant will allow customer to download the tender document by sending the purchase request message. Customer will receive the message and start to download the document.

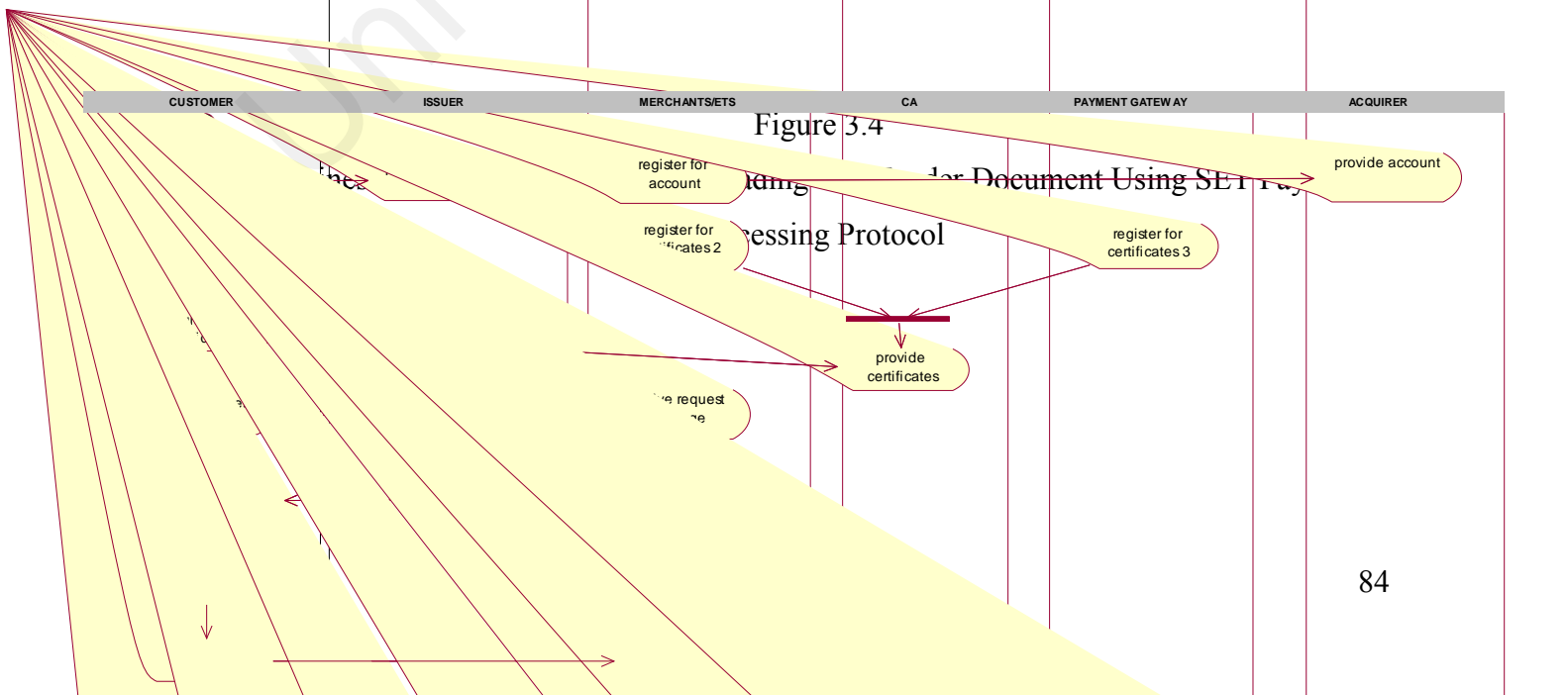
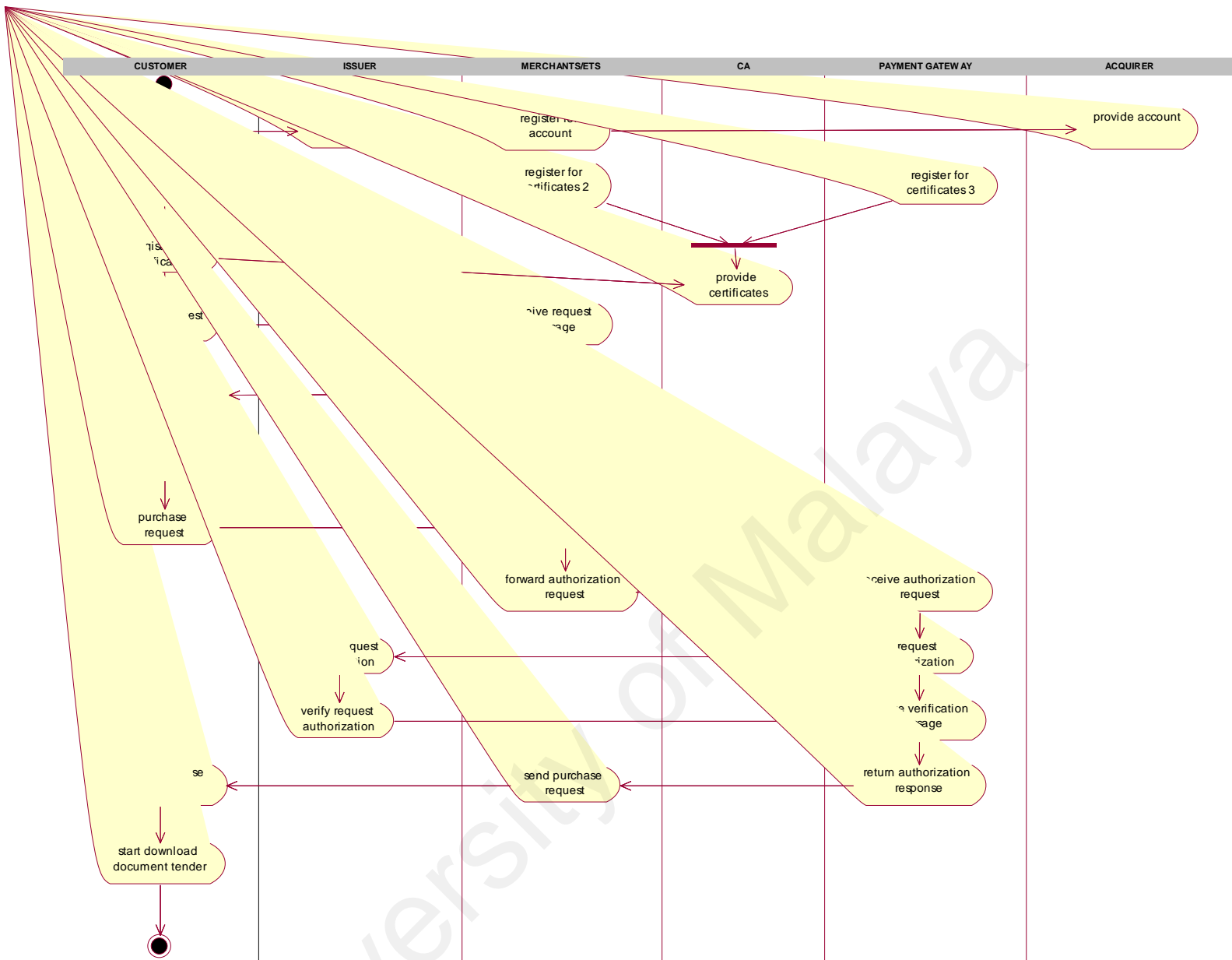


Figure 3.4

Using the Issuer for Document Using SET Protocol

Processing Protocol

III. Activity Diagram 3

This activity generally describes the process to send the tender proposal by customer to the merchant using ETS. Figure 3.5 shows the business process model for tender proposal sending.

The Ms Outlook Express is used in ETS as the middleware to send the tender proposal to the merchant. ETS is automatically designed to show only the tender, which does not exceed the due date. After customer has selected the sending option, the merchant will receive the proposal attachment. Merchant will then verify the proposal. The purpose is to make sure if the tender is already submitted by the same customer. If customer sends the proposal twice, then the second proposal will be rejected. If the proposal fulfills all the merchant requirement, then it will be accepted.

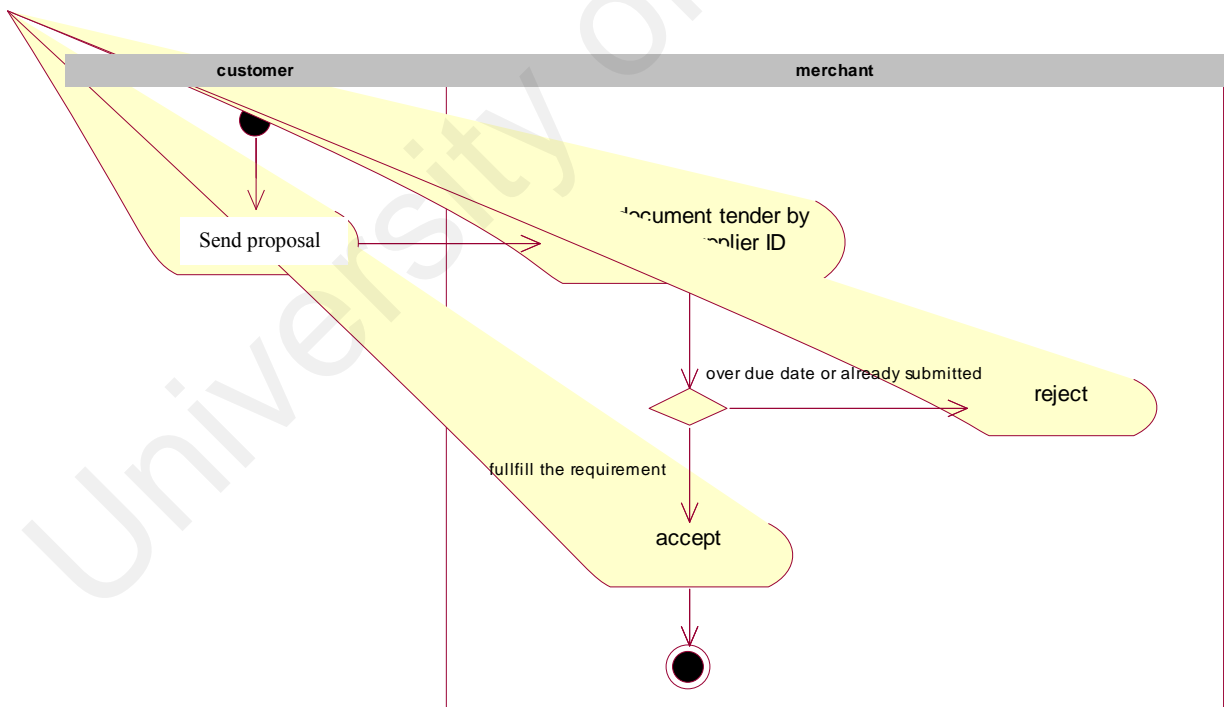


Figure 3.5
Business Process Model for Tender Proposal Sending

3.2.2.1.1.3 Use-Case Model

Use cases are scenarios for understanding system requirements. A use-case model can be instrumental in project development, planning and documentation of systems requirements.[12] A use case is an interaction between users and a system, it captures the goal of the users and the responsibility of the system to its users. The use-case model describes the use of the system and shows the courses of event that can be performed. The interaction between the actors and the use case for the system is described as below:-

I. Customer Use Case

Customer is the main actor in ETS. They interact with a lot of process in the system such as user login, registration, downloading document tender, sending tender proposal, searching tender, user feedback and payment processing.

Figure 3.6 shows the Customer Use-case. The use-case shows the interaction between the customers with ETS system. The interaction process includes user login, user registration, downloading tender document, tender proposal submission, tender searching (awarded and current tender), sending feedback and payment processing.

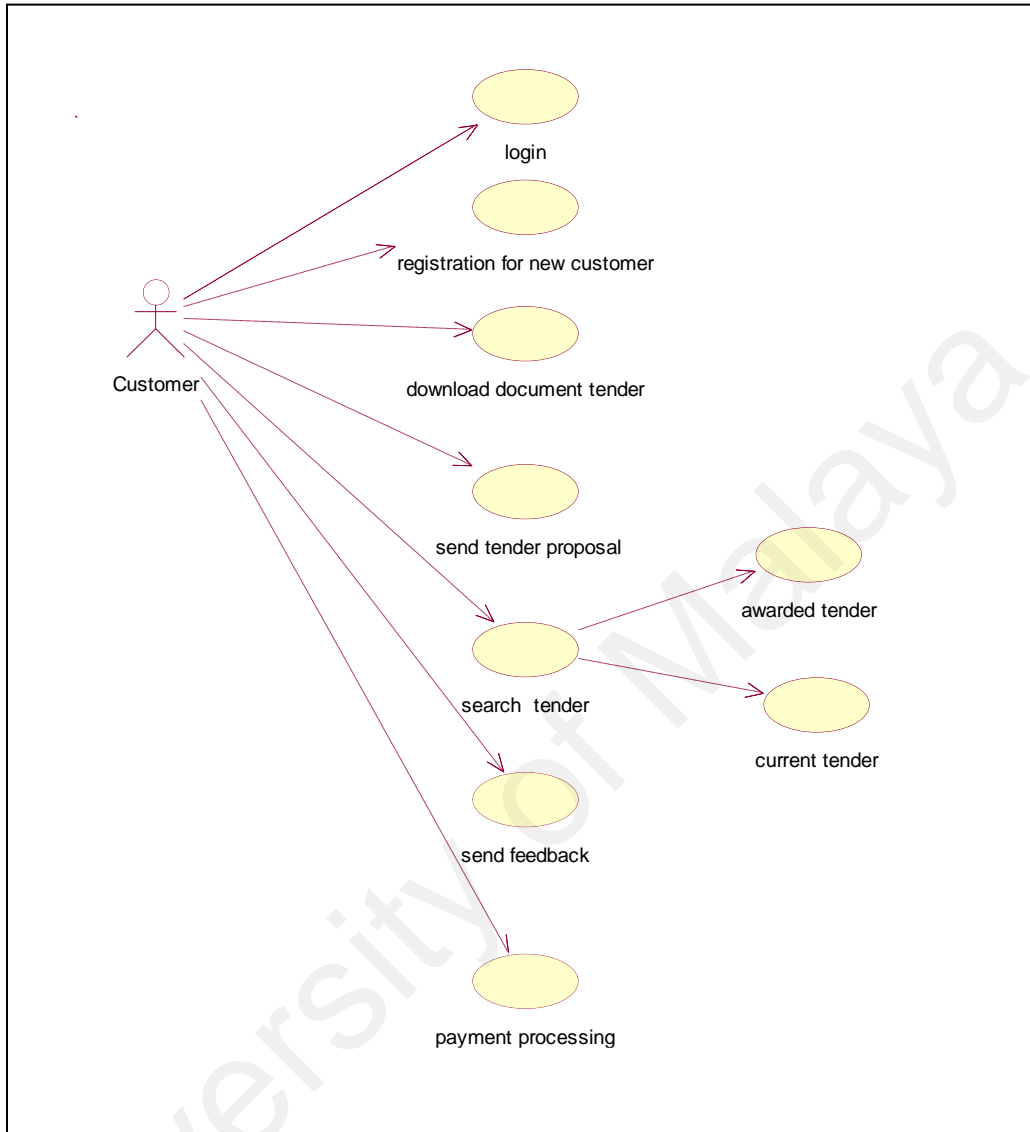


Figure 3.6
Customer Use-Case

The function of Customer Use-Case is described as follows:-

1. Login Use-Case

The login use-case functions as the authentication process. It allows only the authorized person to use the system.

2. Registration New Customer Use-Case

Every new customer has to fill up the registration form. The complete form will be sent to the merchant to verify their company profile. They can only access ETS after the verification process.

3. Download Tender Document Use-Case

The use-case describes the downloading process of tender document from ETS to the customer.

4. Send Tender Proposal Use-Case

The use-case describes the submission process of tender proposal process from the customer to the merchant.

5. Search Tender Use-Case

The searching process of awarded and current tender is described in this use-case.

6. Awarded Tender Use-Case

The use-case displays all awarded tender by month.

7. Current Tender Use-Case

The use-case displays all the available tender and its detail.

8. Send Feedback Use-Case

Through this use-case, enquiry from customer is recorded using feedback form.

9. Payment Processing Use-Case

The use-case includes the payment process until the bank verifies the customer credit card.

II. Merchant

Merchant is an organization with goods or services to sell to the customer. Since the merchant website support the online payment, therefore, merchant has to open an account with the acquirer and register for certificates with Certification Authority (CA). Figure 3.7 shows the Merchant Use-Case.

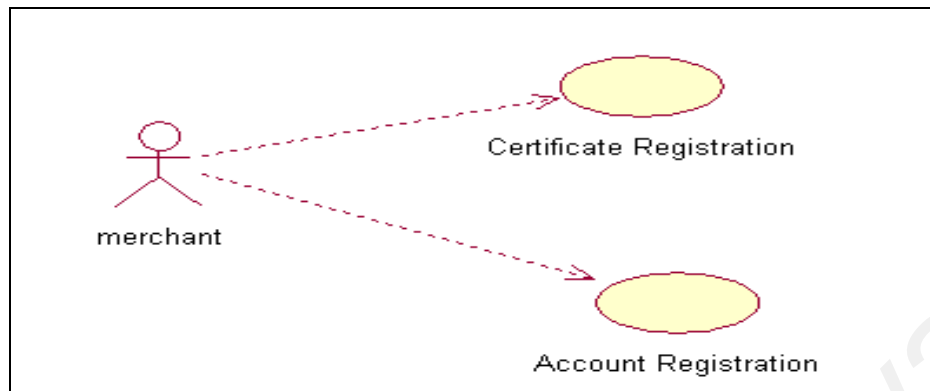


Figure 3.7
Merchant Use-Case

The function of Merchant Use-Case is described as follows:-

1. Certificate Registration Use-Case

The use-case describes the certificate registration process between Merchant and Certification Authority (CA). Merchant will register the certificate with CA and CA will provide public key certificate for merchant. The certificate is used as the authentication when dealing with credit card transaction from customer to merchant and from merchant to acquirer.

2. Account Registration Use-Case

The use-case describes the account registration between merchant and acquirer. Acquirer is a financial institution. Merchant has to open an account with the acquirer.

III. Administrator

Administrator is the person in charge in merchant office to organize the tendering process. Activities involved by administrator are processing the tender proposal, updating information on tender, confirming the customer registration, updating awarded tender information and replying feedback. Figure 3.8 shows the Administrator Use-Case.

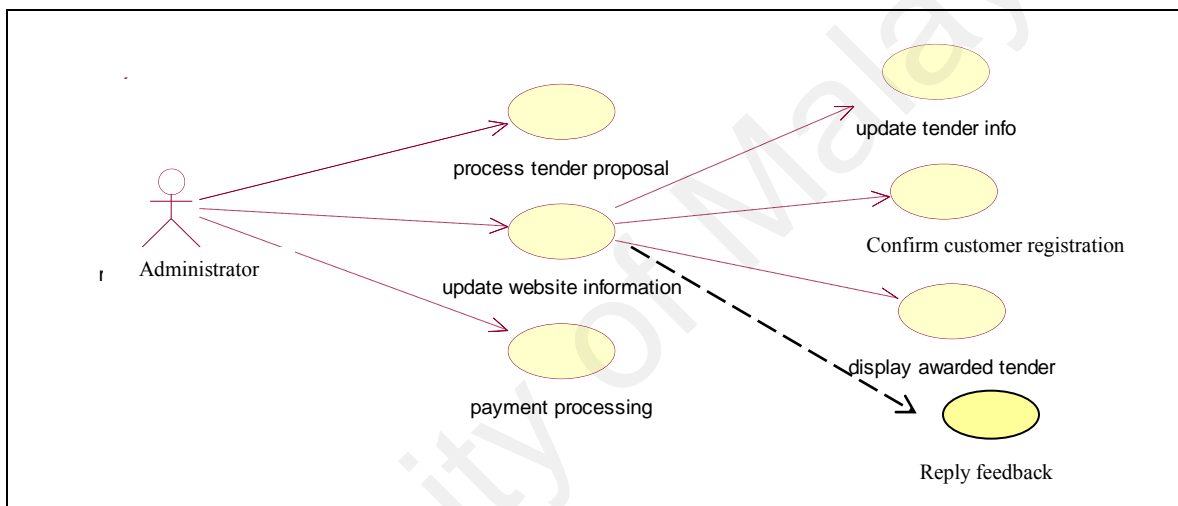


Figure 3.8
Administrator Use-Case

The function of Administrator Use-Case is described as follows:-

1. Process Tender Proposal Use-Case

The use-case describes the submission process of tender proposal by customer.

The administrator will analyze the tender proposal whether to be

accepted or rejected.

2. Update Website Information Use-Case

The administrator will update all the new information from time to time regarding tender information, setting the customer ID or information on awarded tender.

3. Update Tender Info Use-Case

The process involved in this use case will add new tender or delete expire tender.

4. Confirm Customer Registration Use-Case

The use-case involves the confirmation process of registration from new customer by verifying their company profile.

5. Display Awarded Tender Use-Case

The process includes updating awarded tender menu by adding new-awarded tender or deleting old awarded tender.

6. Reply feedback Use-Case

The administrator will reply the customer enquires in this use-case process.

IV. Issuer

Issuer is a financial institution, such as a bank, that provides the customer with the payment card. Issuer is involved in the SET during the payment processing. The activities include provide account, receive request authentication and verify request authentication. Figure 3.9 shows the Administrator Use-Case.

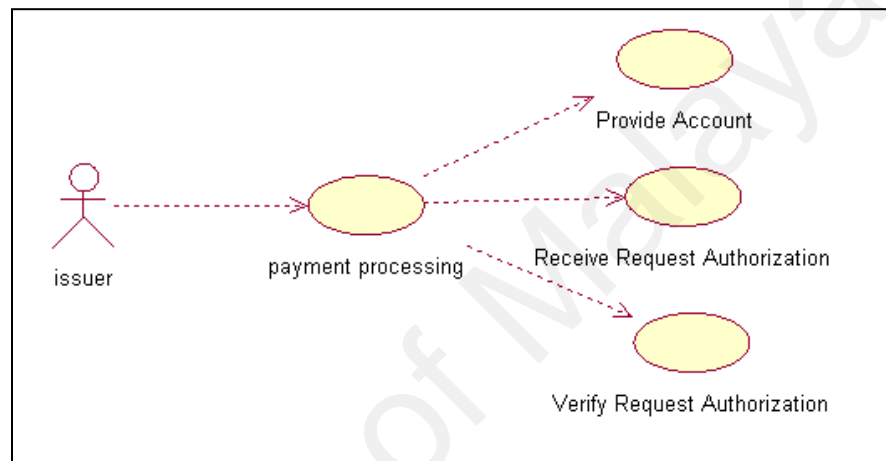


Figure 3.9

Issuer Use Case

The function of Issuer Use-Case is described as follows: -

1. Payment Processing Use-Case

The process describes the issuer involvement in SET payment processing through the activities such as provides account, receive request authorization and verify request authorization.

2. Provide Account Use-Case

The use-case is about the issuer provides account to the customer who wants to have credit card.

3. Receive Request Authorization Use-Case

Issuer receives request authorization from the payment gateway to confirm customer credit card validation.

4. Verify Request Authorization Use-Case

Issuer will send the verify request authorization message to the payment gateway to confirm customer credit card validation.

V. Certification Authority (CA)

Certification Authority (CA) is an entity that is trusted to issue public-key certificates for customer, merchants, and payment gateways. Figure 3.10 shows the certification Authority Use-Case.



Figure 3.10

Certification Authority Use-Case

The function of Certification Authority Use-Case is described as follows:

1. Provide Certificates

The use-case describes the process of CA provides the public key certificates to customer, merchant and payment gateway.

VI. Payment Gateway

Payment gateway is a function operated by the acquirer or a designated third party that processes merchant payment messages. It operates in the SET payment processing in the authorization request activity, verification request activity and authorization response activity. Figure 3.11 shows the certification Authority Use-Case.

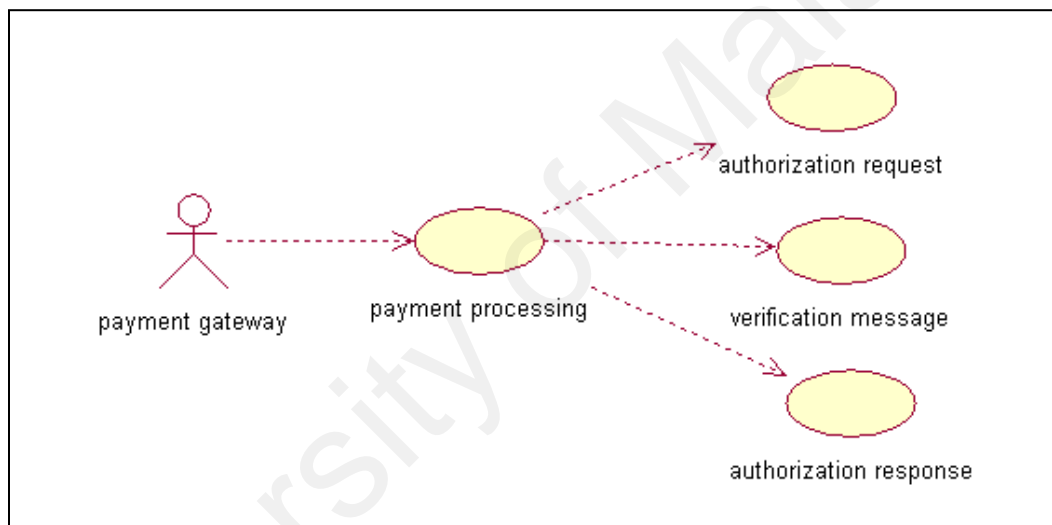


Figure 3.11
Payment Gateway Use-Case

The function of Payment Gateway Use-Case is described as follows: -

1. Payment Processing Use-Case

Payment Gateway involves in payment processing through authorization request, verification request and authorization response activities.

2. Authorization request Use-Case

Payment Gateway receives request authorization from merchant and forward to issuer to verify the customer credit card .

3. Verification message Use-Case

Payment Gateway receives verification message from the issuer as to confirm customer credit card validation.

4. Authorization response Use-Case

Payment Gateway sends the authorization response to merchant as to confirm customer credit card validation. The response will allow customer to download the tender document

VII. Acquirer

Acquirer is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. Figure 3.12 shows the certification authority use-case.

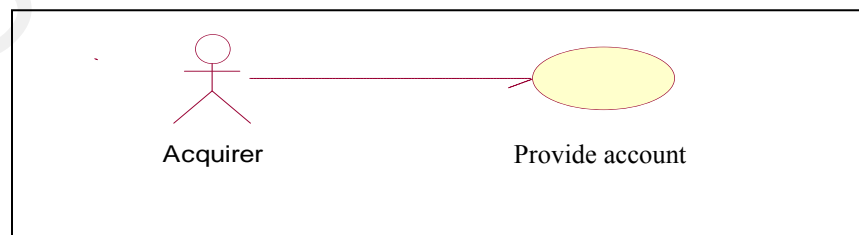


Figure 3.12
Acquirer Use-Case

The function of Acquirer Use-Case is described as follows:

1. Provide account Use-Case

The use-case describes the Acquirer that provides an account with the merchant to allow SET payment processing.

3.2.2.1.1.4 Interaction Diagrams

UML Interaction Diagrams that is used to represent ETS element is called as Collaboration Diagram. A collaboration diagram represents a set of objects related in a particular context and the exchange of their messages to achieve a desired outcome.

Below is the detail description about ETS module represent in the collaboration diagram.

I. Login and Registration Process

Login process in collaboration is more detail compare to login process in business activity diagram. This is because, this diagram represent object in numbering sequence. Therefore the login process will be easier to understand based on its sequence flow.

There are two types of customer in ETS. New customer is the person who has not register to the merchant website meanwhile registered customer is the person who is already a member to ETS. For new customers, they have to register their company profile to the merchant through ETS. They have to fill up the registration form in the customer

registration menu to set their password and ID. The data will be saved in ETS database. Administrator will retrieve the new registration through Admin ETS Environment and then verify the registration if the information given by customer is valid. Customer cannot use ETS before they receive the confirmation email from the administrator. The confirmation email consists of customer password and ID. Figure 3.13 shows the new customer login collaboration diagram.

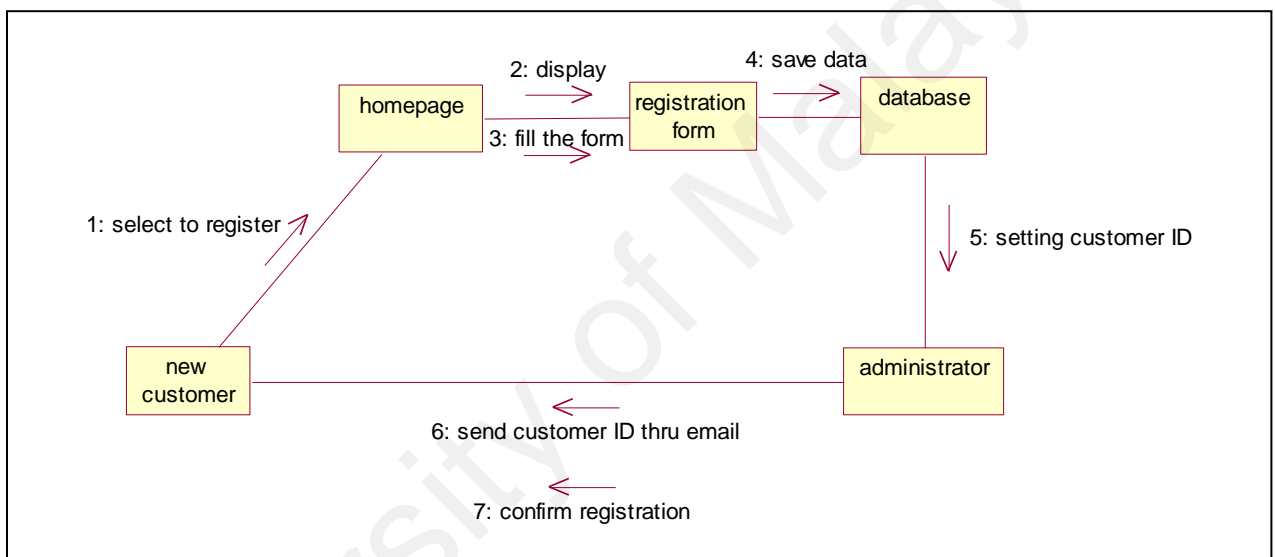


Figure 3.13
New Customer Login Collaboration Diagram

In addition, for unregistered or new administrator, they have to register by filling up the administrator registration form to set their password and ID. After registering, they are allowed to use the Admin ETS directly. Figure 3.14 shows the new administrator collaboration diagram.

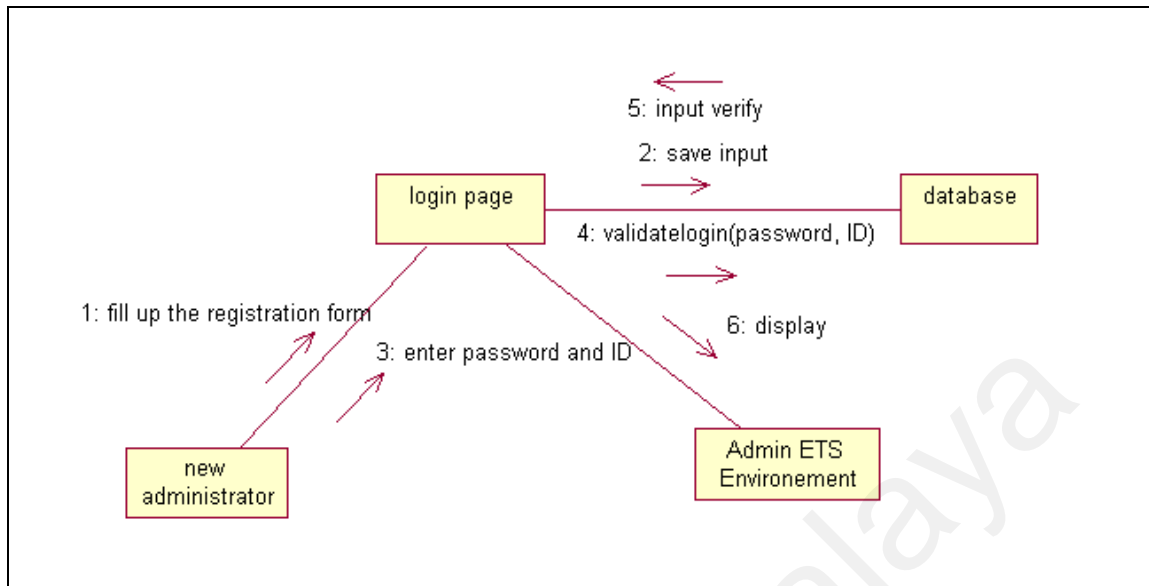


Figure 3.14
New Administrator Collaboration Diagram

Meanwhile for the registered customer and administrator, they need to enter their password and ID to allow them to use ETS. The login will be validated based on ETS database. If the login is verified, then ETS customer homepage or ETS admin homepage will be displayed. Otherwise, if the login is invalid, then they have to reenter their password and ID and the system will validate again their login. Figure 3.15 shows the registered customer login collaboration diagram, Figure 3.16 shows the invalid customer login collaboration diagram, Figure 3.17 shows the administrator valid login collaboration diagram and Figure 3.18 shows the invalid administrator login collaboration diagram.

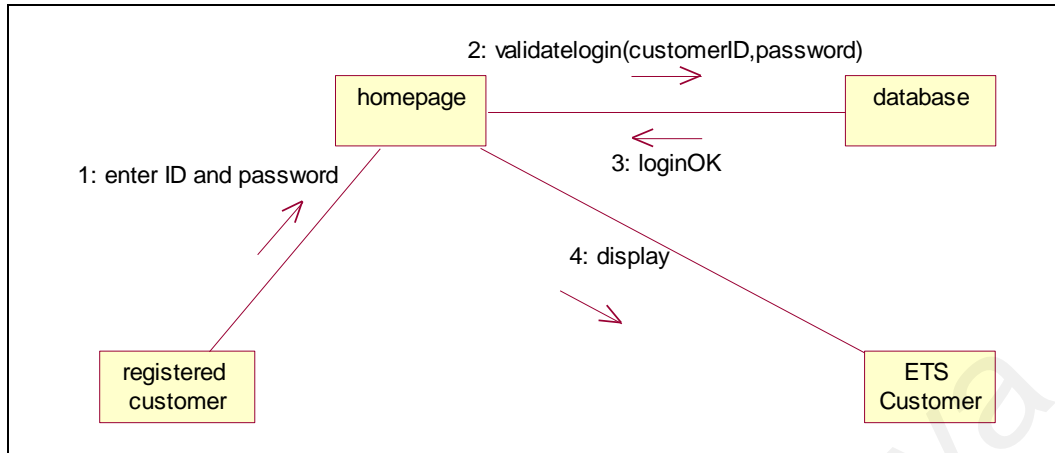


Figure 3.15
Registered Customer Login Collaboration Diagram

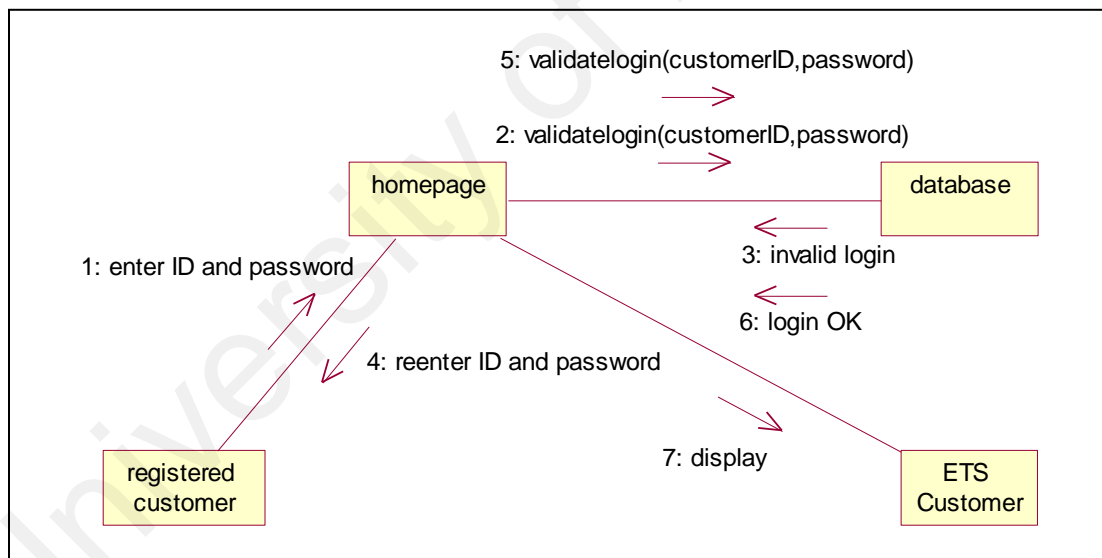


Figure 3.16
Invalid Customer Login Collaboration Diagram

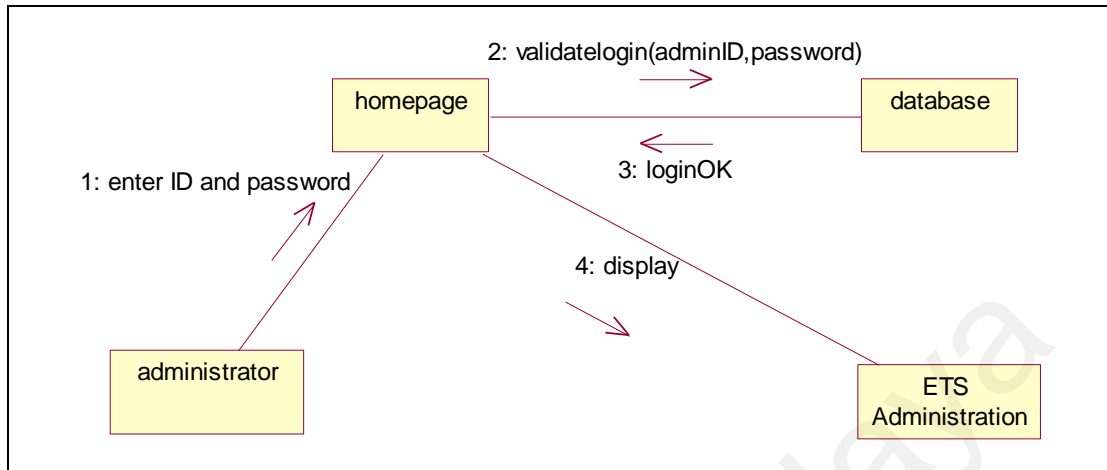


Figure 3.17
Administrator Valid Login Collaboration Diagram

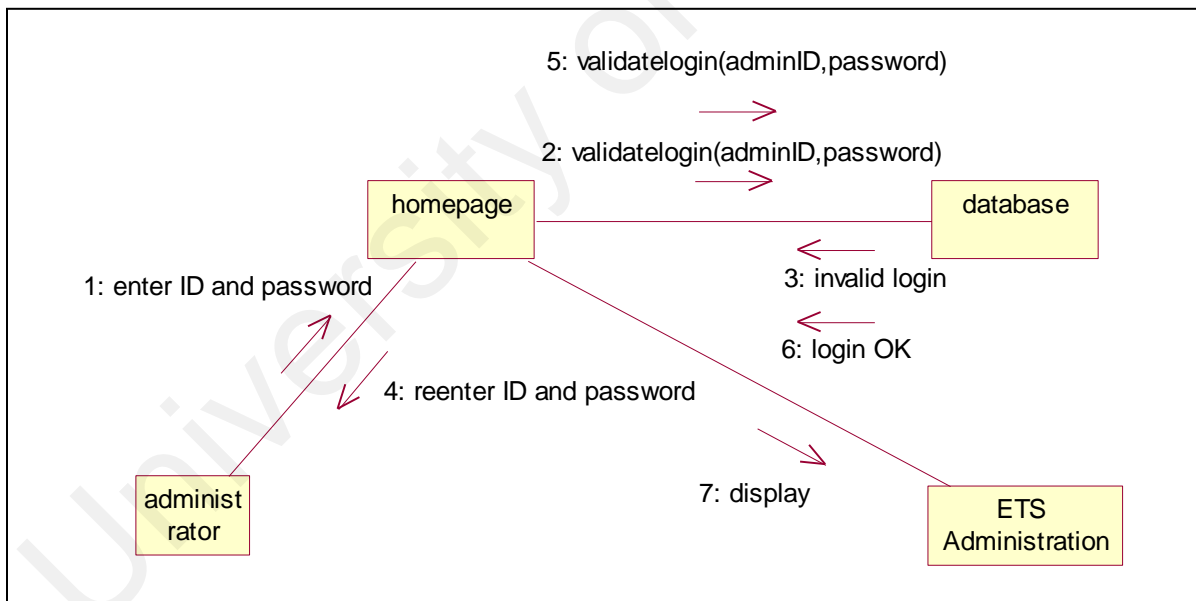


Figure 3.18
Administrator Invalid Login Collaboration Diagram

2. Download Tender Document Process

Figure 3.19 shows the collaboration diagram for the process of SET in ETS. The explanation of this process is the same as the business process model in Figure 3.3.

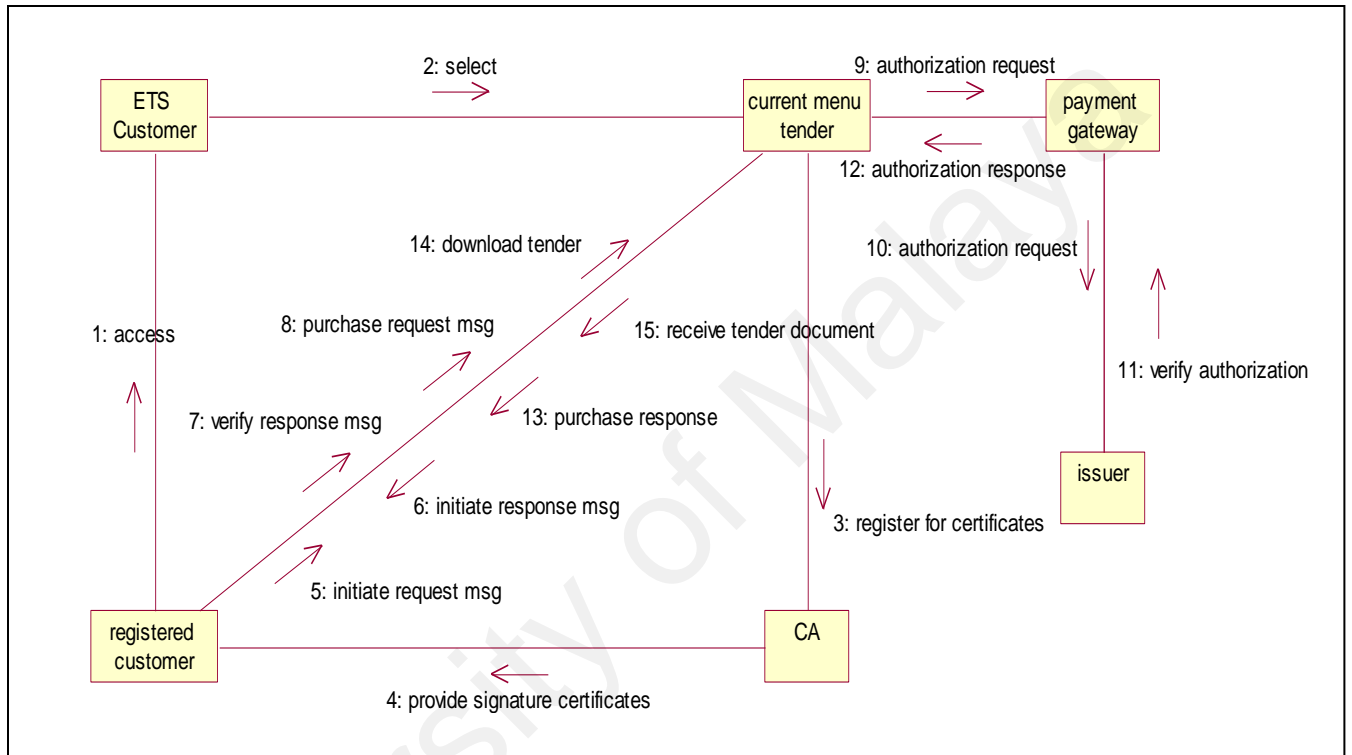


Figure 3.19

Download Tender Document Collaboration Diagram

3. Send tender proposal process

Send tender proposal process is a process where customers want to send their tender proposal to the merchant through ETS. The process begins when customers select the sending option in the Tender Proposal Menu. The proposal attachment will be sent to the administrator email using Ms Outlook Express. The administrator will verify the email

based on the customer password and ID. The verification is important to make sure the received proposal came from the registered customer. Otherwise, the proposal will automatically reject. After verifying the customer password and ID, the administrator will check the proposal to make sure it fulfills the requirement. If qualified, then it will be accepted otherwise if the proposal has already been submitted before this, then it will be rejected. Refer Figure 3.20.

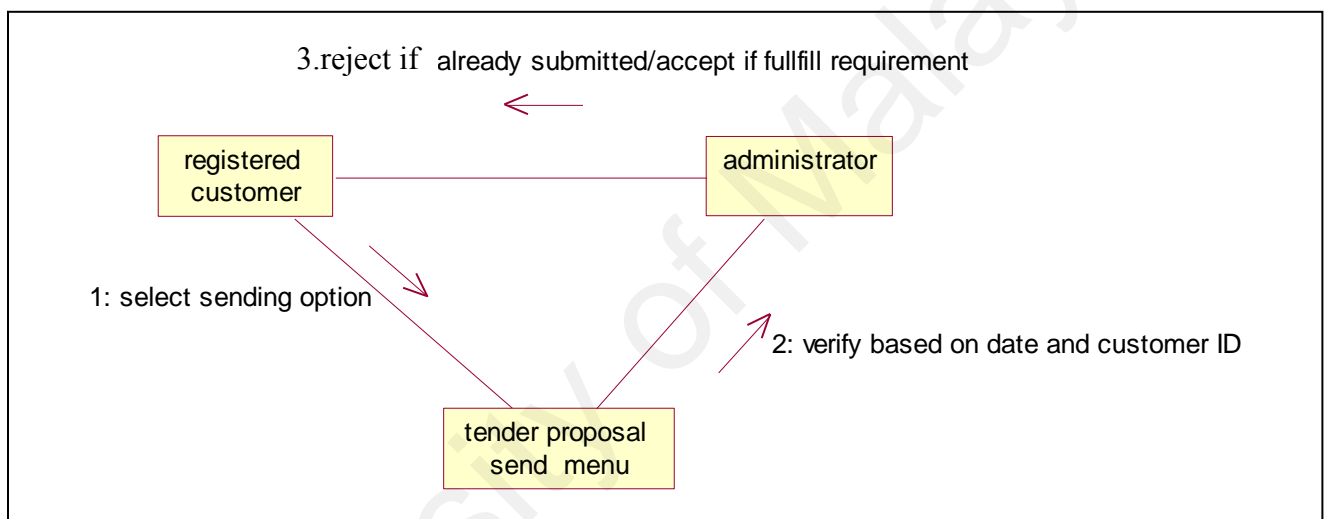


Figure 3.20
Send Tender Proposal Collaboration Diagram

4. Awarded Tender Process

The awarded tender process allows supplier to view information regarding the tender that has been awarded. It contains information such as tender reference number, title of tenders, suppliers who win the tender, total quantity or item win, price amount of tender and date awarded. To access the awarded tender, customer must select the awarded tender menu from the Customer ETS. Then customer has to search the tender by

month. If the information is in the database, the awarded tender will be displayed. Figure 3.21 shows the awarded tender collaboration diagram.

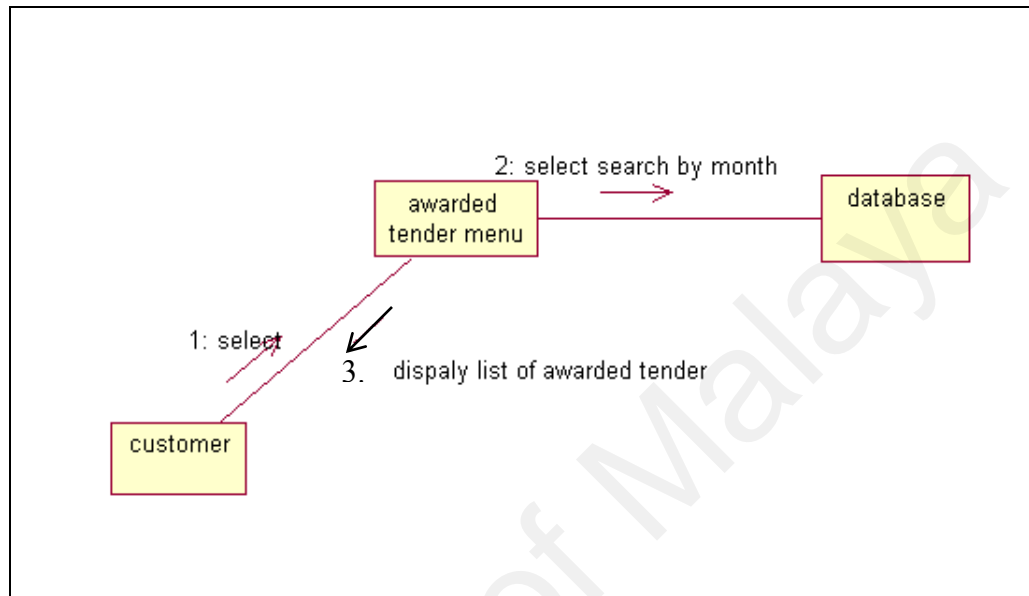


Figure 3.21

Awarded Tender Collaboration Diagram

5. Feedback Process

Customer is allowed to give their feedback in order to enquire about their interested tender or other related field. Customer can write their feedback in the feedback form and select sending option. Administrator will read the feedback and reply the feedback through email to customer. Refer Figure 3.22.

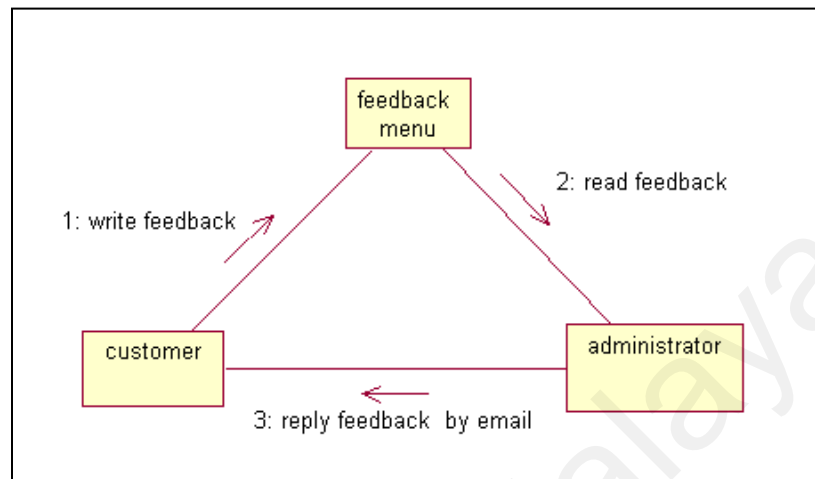


Figure 3.22
Feedback Process Collaboration Diagram

6. Customer Profile Update Process

The customer profile update process is a process that allows customer to update their company information. Customer is allowed to edit all the information including their username and password. This will prevent unauthorized user using their login data. The system will save the new data into ETS database and automatically the data will be updated. Figure 3.23 shows the customer profile update process collaboration diagram.

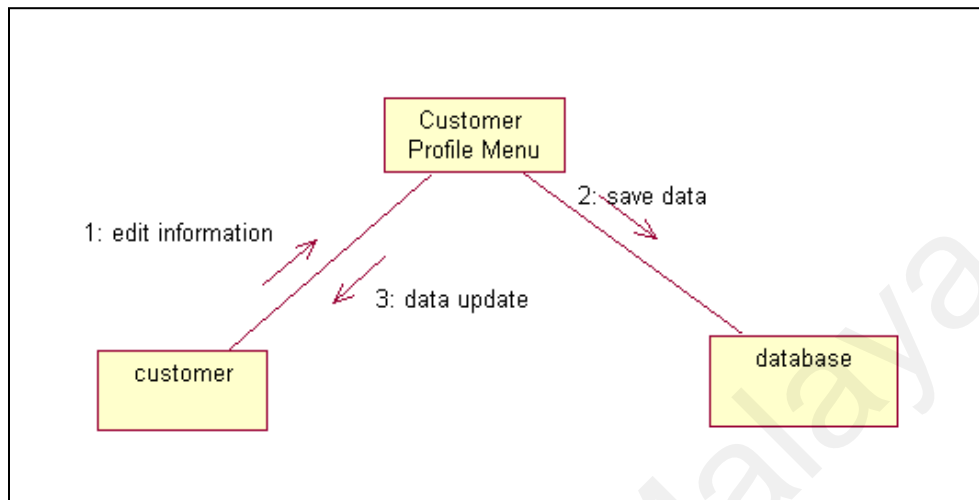


Figure 3.23

Customer Profile Update Process Collaboration Diagram

3.2.2.1.1.5 Classification

Classification is the process of checking to see if an object belongs to a category or a class and it is regarded as a basic attribute of human nature. A class is a specification of structure, behaviour and the description of an object. Classification is more concerned with identifying the individual objects in a system.

The class diagram in Figure 3.24 shows the class diagram for the process of SET in ETS. The explanation of this process is the same as the business process model in Figure 3.3.

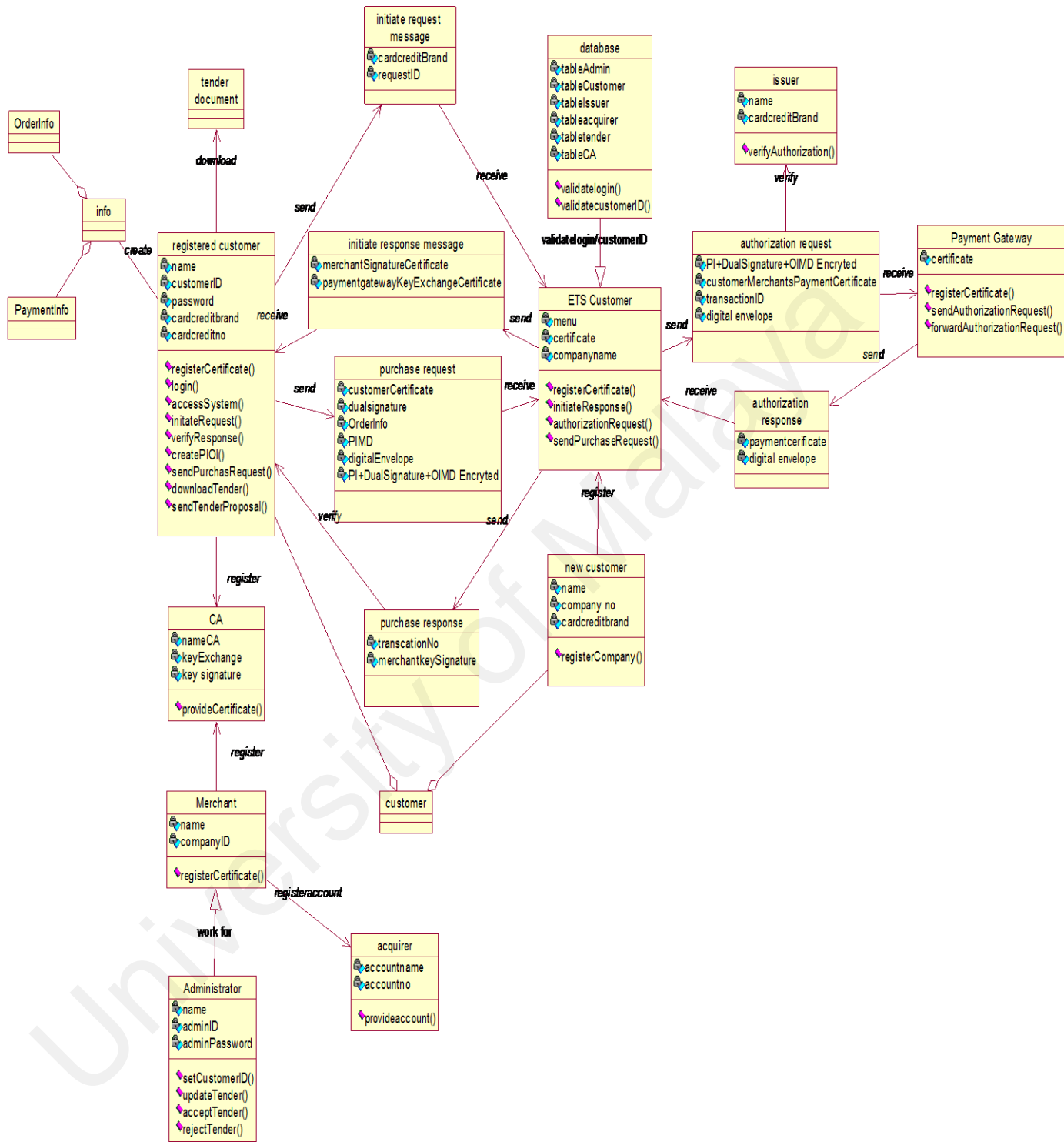


Figure 3.24
Class Diagram for SET Process

3.2.2.1.2 Design

Design is a process to implement the structure and diagrams of the system requirement that has been identified during analysis phase. Activities includes in design phase are:

i. Design database

The database is designed based on the objects that identified using UML diagrams. Ms Access 2000 is been chosen as the database for ETS project.

- Why MS Access?

MS Access is a Windows based database system. Developing or modifying code is much easier and faster, hence cheaper, than doing the same thing in DOS, mini-computers or mainframes. Reports can be also being quickly added, modified, or new ones created based on already existing reports.[32]

Moreover, another advantage of MS Access is, it comes with MS Office suit whereby all the companies in the world are using this suit for their office management work. Therefore, this will save their cost in order to avoid buying any new software and license.

i. Build prototype

Prototype is a program that reads a text file and produces the look and feel of an application [33]. The purpose of the prototype is to allow user to react with

the design and suggest changes (if needed) to the design. It is the main technique to support the iterative refinement.

In this project, one web-based prototype is being developed using Macromedia Dreamweaver MX.

iii. Program coding

The main programming language that is used in ETS project is Active Server Page (ASP) meanwhile Java Script is used for animation.

- Why choose ASP?

ASP is a great tool for creating dynamics web pages. The power of ASP lies in two facts: first, the HTML is not created until the user wants to see the web page, and second, it doesn't care what web browser is being used. ASP isn't the first technology to offer these features, but it's undoubtedly one of the most powerful and widely used in industry; and crucially, it's one of the fastest. Active Server Pages is different from many Microsoft technologies in the following respect: while ASP must be executed on a computer that supports it, can view ASP-driven web pages from *any* computer, and with *any* modern browser. This has enabled developers to enhance their web pages with interactive features, and even to solve common business problems - to such an extent that pages with the .asp suffix are fast becoming as common as those with the .htm suffix.[34]

3.2.2.1.3 Implementation and Testing

Implementation and testing are the last phase in this research methodology.

The purpose of this phase is to install the prototype that is been developed during design phase in one organization and evaluating the system based on the user satisfaction test.

Activities includes in the implementation and testing in ETS project are:

- System Testing
- System Installation
- User Satisfaction Test

Details elaboration on this section will be described in the Chapter Five.

3.3 System Development Requirement

In the system development, software and hardware requirement is important to support the faster and easier development. Follows are the details regarding software and hardware that are used as the project requirement.

3.3.1 Hardware Specification

Hardware that is required for this project is as follows: -

- i. Personal Computer /Laptop
 - The computer is installed with operating system Windows XP Professional.
This OS is used because it includes together with Microsoft Internet Information Services that will be used as the web server.
 - Processor with capacity of Intel Pentium® III 400Mhz and above.
- ii. Memory 64 megabytes (MB)
- iii. Hard Disk -4.3 gigabyte (GB) with at least 1 gigabyte (GB) available space
- iv. Modem - At least 33.6 kbps
- v. Display - Super VGA (800 x 600)
- vi. Monitor
- vii. Keyboard
- viii. Mouse
- ix. Scanner
- x. Printer

3.3.2 Software Specification

Software that is required for this project is as follows: -

i. Macromedia Dreamweaver MX

Macromedia Dreamweaver MX software is used to design the user interface for ETS meanwhile Active Server Page (ASP) and Java Script is used as the programming language.

ii. Microsoft Access 2000

Microsoft Access 2000 software is used as the database for ETS.

iii. Internet Information Server (IIS 5.0)

IIS 5.0 is a web server that supports Active Server Pages. The purpose of the web server is to publish ETS system over Internet.

CHAPTER 4

SYSTEM FUNCTIONALITY

4.1 Introduction

As mentioned earlier in Chapter One, the purpose of this research is to build one e-commerce solution for online tendering system called as Electronic Tendering System (ETS). ETS can be accessed by front end and back end user with different URL address.

Front end user means the customer of the systems where the front end system support functions such as downloading the tender document, submitting tender proposal, supplier registration, standard terms of tender, tender notice, tender awarded and also support payment via Internet. Meanwhile for the back end-user means the administrator of the merchant company where their tasks are to monitor and manage the front-end process. Therefore the back end system support functions such as updating supplier information, administrator information, tender notice, awarded tender and read and reply supplier feedback. This chapter will elaborate more on the process and the functionality in ETS.

4.2 System Workflow

The process flow in one system will be easier if it is represented in interface framework. Therefore, figure 4.1, 4.2 and 4.3 will show the relationship among user interfaces in the Electronic Tendering System (ETS).

4.2.1 Front-End Interface Workflow

i. Interface View For The Registered Supplier

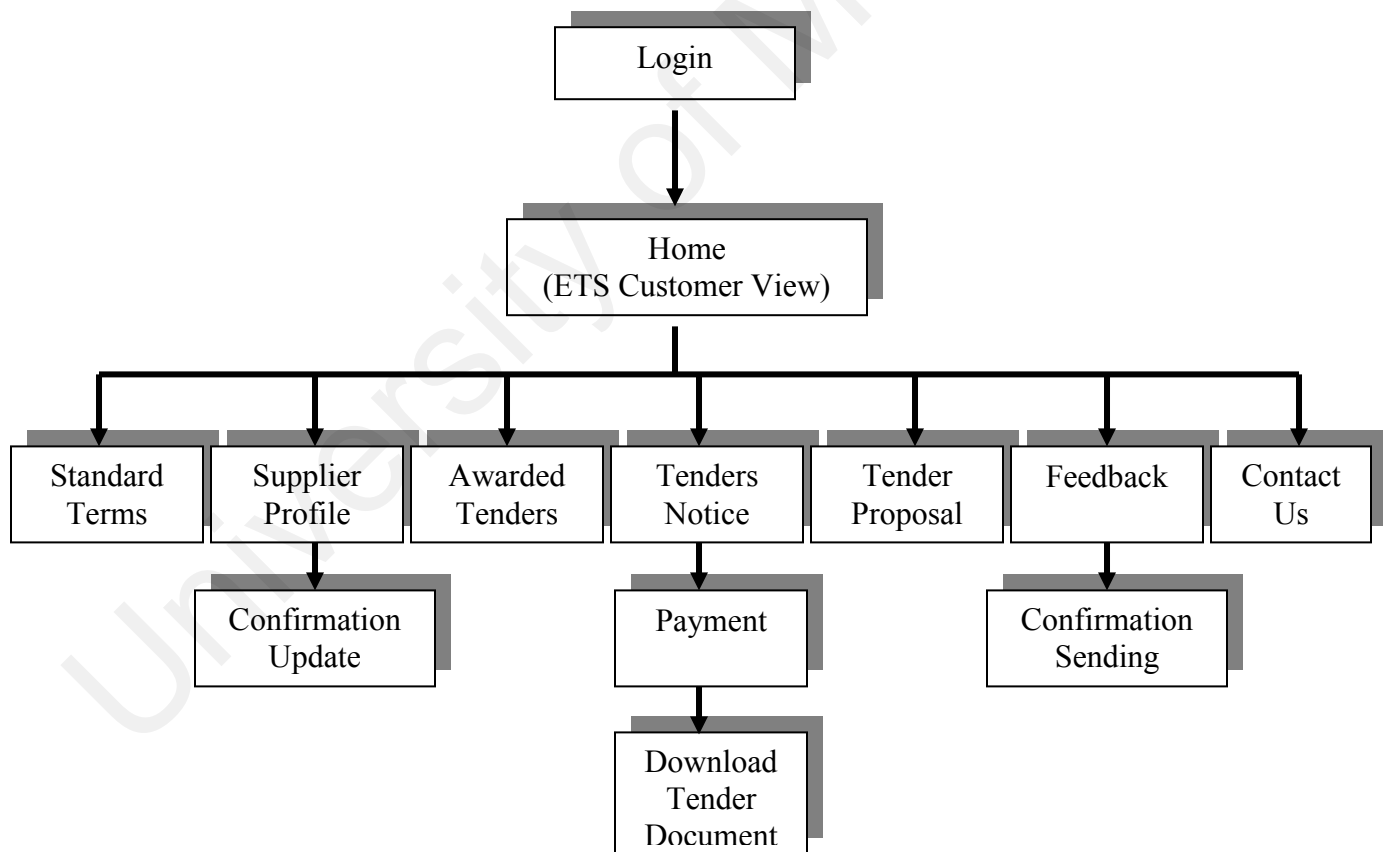


Figure 4.1
Interface Flow For The Registered Supplier

ii. Interface View For The Unregistered Supplier

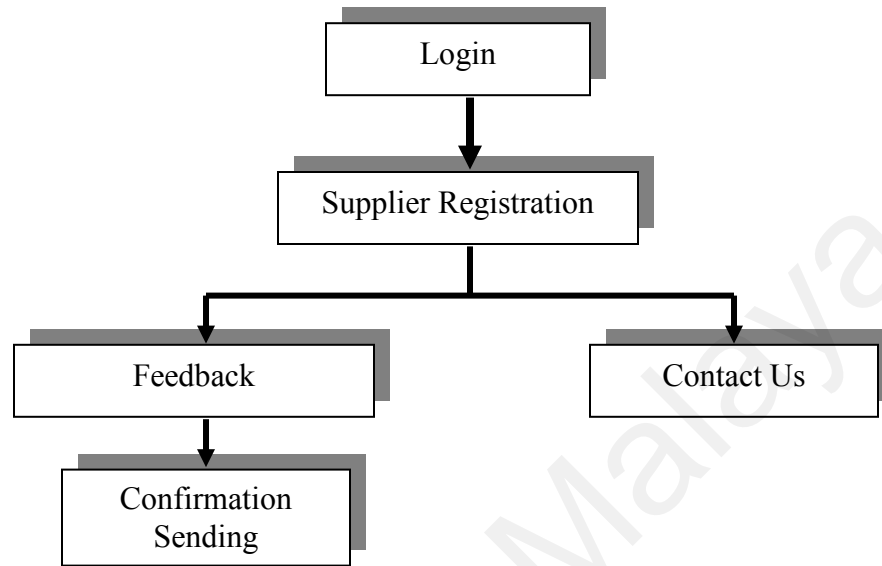


Figure 4.2

Interface Flow For The Unregistered Supplier

4.2.2 Back -End Interface Workflow

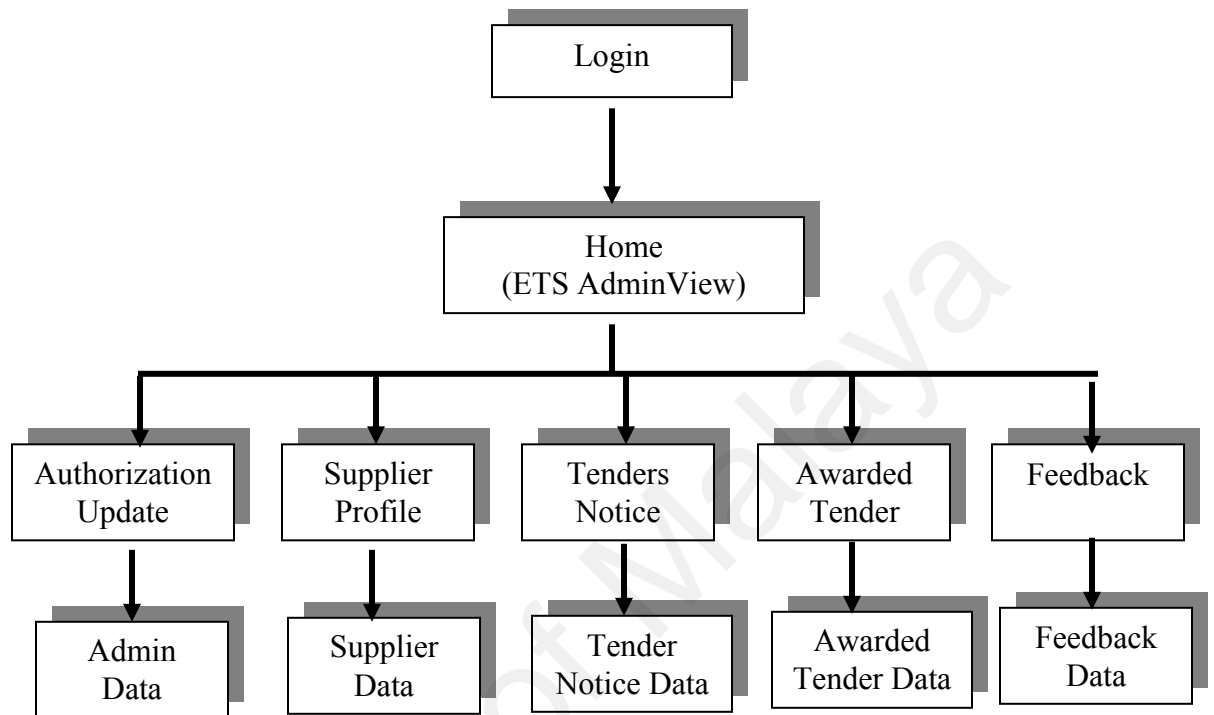


Figure 4.3
Back-End Interface Flow

4.3 ETS Scenarios

ETS scenarios are divided into two processes:

- Front-end process
- Back-end process

4.3.1 Front-End Process

The main functions or operations emphasize in ETS are: -

1. Downloading tender document

This function allows customer to download tender document via the merchant website. Before merchant can retrieve this function, they must have MasterCard or Visa credit card only. These two types of credit card are used because the MasterCard and Visa Company developed SET protocol [20]. To download the document, customer will browse and select the interested tender in the Tender Notice Menu. Next, they have to make online payment transaction by entering their credit card number. Verification and validation of authorization from the issuer will lead the customer to download the document tender. The implementation of ETS is based on the SET protocol and process. SET is used to support payment transaction.

2. Submitting tender proposal

Tender proposal is very confidential and only authorized person can read the content. Therefore, the submitting process must be done in secure transaction. Customer will access Tender Proposal menu and to submit the proposal. Next, the process continues with the help from Microsoft Outlook Explorer. Tender proposal will be evaluated after the deadline. Late proposals will be rejected by the system.

Other support functions in ETS are: -

1. Standard terms of tender

This function is basically about the rules provide by merchants that contain information about the interpretation word used in tender, contract, payment to customer, risk, and etc. It is important for customer to review this part so that they will know the merchants rule.

2. Tender notice

The information about the merchant's tenders is advertised in this function. The tender notice includes information such as the tender title, tender reference number, document fee, closing date and time, type of payment that can be made, company address and tender submission information. The downloading of tender document starts from this menu where customer can select only one tender at one time by clicking the "download" button.

3. Supplier registration

This is the submenu in the login process. Customer must have customer ID to use ETS. Therefore, they have to register to get the ID and to be the authorized customer to use the system. The unregistered customer must select the register option during the login time. Next, they have to fill in the registration form and submit to the

administrator. If the customers fulfill all the requirements needed by the merchant, their username and password will be sent to them through email.

4. Awarded Tender

This function will display the awarded tender to the qualified customer. The administrator will take a few months (based on the company) from the dateline to display the awarded tender. Customer must access the Awarded Tender Menu to see whether they have been awarded or not for the related tender.

5. Feedback

This function allows customer to send any feedback to the merchant either it regards to their interested tender or other enquiries.

4.3.2 Back-End User

1. Updating Supplier Information

The function allows administrator to update information related to supplier such as delete, search and view supplier. Administrator will verify new supplier by checking their company profile. If the information regarding their company profile is valid, then, in order to confirm the registration, administrator will send the username and password to them by email.

2. Updating administrator information

The function allows administrator to update information related to their authorization to login the system. Administrator can add new authorized person to do the management process. Moreover, they are allowed also to delete, search or view authorize person.

3. Updating Tender Notice

The function allows administrator to update information related to tender such as add new, delete, search and view tenders.

4. Update Awarded Tender

The function allows administrator to update information related to award tender such as add new, delete, search and view awarded tenders.

5. Read And Reply Supplier Feedback.

Administrator can read and view feedback from supplier in this menu.

They also can reply the supplier feedback using their email through Microsoft Outlook Express.

CHAPTER 5

IMPLEMENTATION AND TESTING

5.1 Introduction

The implementation phase of the systems development life cycle is the most expensive and time-consuming phase of the entire life cycle. Implementation is expensive because so many people are involved in the process; it is time consuming because of all the work that has to be completed during implementation [35]. Physical design specifications must be turned into working computer code, the code must be tested until most of errors have been detected and corrected, the system must be installed, user sites must be prepared for the new system, and users must come to rely on new system rather than the existing one to get their work done.

Implementation phase involves testing and installation for this project system and it has been done at Kolej Universiti Kejuruteraan dan Teknologi Malaysia (KUKTEM), Kuantan, Pahang. The college has been chosen because it is a new college and involves with a lot of development, renovation and installation. These made them need a lot of contractors or suppliers. Therefore, tendering process with online payment is one of the new alternative solutions for them.

The phases included in this project implementation are: -

- System testing
- System installation
- User Satisfaction Test

5.2 System Testing

System testing is a process to test the developed system in the real world-working environment. The purpose of system testing is to ensure that all the system components work well together.

The steps involved in testing are [36]: -

- i. Choose a testing strategy
- ii. Prepare test specifications and create test data
- iii. Perform system test.

5.2.1 Choose Testing Strategy

Two fundamental testing strategies are [36]:

- i. The Black-Box Strategy

As its name implies, the black-box testing strategy treats the system as a box where the contents cannot be discerned. This strategy assumes that if, given certain inputs, the "box" (example: the system) generates the correct outputs, and then the contents of the box (example: the system's programs, data structures, interfaces and others) must be correct.

ii. The Glass-Box Strategy

This strategy is also called as *white-box* or *program-based testing*. The glass-box testing strategy looks "inside the box" to verify system components and functions by examining each line of code and each data structure. The glass-box strategy verifies program code and data structures, therefore it is best use in order to verify individual program modules or system components and to test custom-developed software.

Although there are two testing strategy, but only one strategy has been done for this project system. The black-box strategy has been chosen, because it is more appropriate to verify system functions and programs by generating correct output, thus, it is best use in order to verify the system as a whole or to test purchased software.

5.2.2 Prepare test specifications and create test data

A test specification outlines the procedures for testing the system; it serves both to plan and to document the results of unit and system tests [36].

At KUKTEM, the test will be done in the finance department because this department deals with the tender processing. Therefore test specification team consists of:

- One accountant
- Two suppliers
- One developer (system owner)

The accountant and the two suppliers will be the users and they function as the prime candidates to help prepare the test specifications because they are familiar with procedures and the kind of errors that a user is likely to make. Meanwhile, the developer is also involved in preparing the test specifications because she is familiar with the error-trapping procedures built into the system. The result of test specification will be discussed in Chapter Six. Refer Table 5.1 for the example of test specification that has been prepared by test specification team in KUKTEM.

Test Specification for : <u>Electronic Tendering System</u>				Page: 1
Designed by: Mazlina		Module or Screen: Customer and Admin Login		
Test Data Source: Data sets 1-2		Objectives: To verify the accuracy of login screen		
Test Condition	Description of Condition	Test Steps	Expected Results	Executed by
1	Incorrect format for password	Enter "12-0378"	System recognizes format error and display error message	Mohd Syarul bin Hassan
2	Id and Password did not match	Enter "Fatimah" and "120378"	System recognizes error and display " Re-enter Id and Password" error message	Mohd Syarul bin Hassan

Table 5.1
Test Specification for Login Interface in ETS

To determine whether the system is performing its input data verification, data retrieval, and report generation functions correctly, appropriate test conditions must be run against a set of valid stored data called test data [36]. The collection of test data is created by the users (accountant and suppliers). The test data contains only valid data. Table 5.2 shows the example of test data for login interface in ETS.

Test Data Set 1		Test Data Set 2	
Data: Administrator Login		Data: Customer Login	
ID	Password	ID	Password
Mazlina	120378	IKCM	KC145
Syahizam	140876	CleanCare	7878TR
RoslanAli	RA121	Fikiran Arif	FA445

Table 5.2
Test Data Sets To Verify The Login Interface In ETS

5.2.3 Performing System Tests

The system test simulates the production environment as closely as possible to verify that all components are integrated effectively and that the system performs its function accurately, reliably, and efficiently [36]. The steps to perform system test in KUKTEM are as follows: -

- i. First, the test procedures outlined in the *test specification* are run using small test data sets.

- ii. The results of each test are documented in the "Executed by/Results" column of the test specification form. If the system fails a test, the failure is noted on the form, indicates how the actual result differed from the expected result.
- iii. After completion of the system test, developer reviews each discrepancy, tracing its cause and prescribing a solution.
- iv. Then users (accountant and supplier) and developer meet to prioritize errors for correction. Critical errors must be repaired and the system test repeated.

5.3 System Installation

After the system has been verified to operate correctly, then the system is ready to be installed in KUKTEM. Before installing the system, the installation strategy must be identified. An *installation strategy* defines a process for converting from the old production system to the new. Four installation strategies are direct cutover, pilot installation, phased installation and parallel operation.

In this project, parallel installation has been chosen as the installation strategy. The strategy allows both, the old tendering process and the new system operates concurrently until the finance department has assured the new system's accuracy and reliability. This strategy is chosen because ETS is a web-based system. This strategy still gives the opportunity to the KUKTEM customers who do not realized about the existing of ETS. Nevertheless, as the first choice, customer will be advised to use the system rather than the old process. This is important to make sure a variety of customers, test the ETS functions to assure its accuracy and reliability.

Firstly, the ETS system will be installed in KUKTEM server for six months. During the installation period, developer will monitor ETS from time to time to avoid any unexpected error especially in the online payment section. This part is important because it deals with customer's credit card. After six months, the users from test specification team (accountant and suppliers) will finalize the system. If the system is successful then it will be accepted otherwise if the systems is still not functioning well, then, it has to iterate all the SDLC processes to detect and to overcome the errors that occur during execution.

The advantages of parallel installation are:

- It provides safety because if the new system fails, the old system is a ready fallback.
- It provides opportunity to verify the new system by validating its output against those of the old system.

The used of parallel installation still has the disadvantages such as increased workload, duplicated paperwork, and stressed users. Although, parallel installation has some disadvantages, but it is a good choice and perhaps the only choice for systems whose failure would cripple the organization.

5.4 User Satisfaction Test

User satisfaction test is a test to assure the new system fulfills the company requirement. In this project, the satisfaction test, which has been done, is called as system evaluation test.

The test is done to evaluate the CUPRIMDA [37] categories in the system. CUPRIMDA stand for capability, usability, performance, reliability, installability, maintainability, documentation/information and availability. It is done based on the five-point satisfaction scale (very satisfied, satisfied, neutral, not satisfied and very dissatisfied). The method of question used is email questionnaires. 15 questions have been created by the system developer. Then, the questions will be emailed to every internal users who are involved with the system operation through KUKTEM E-Community Website. For KUKTEM external users, they will receive the test through their company email.

The users of the satisfaction test are as follows: -

- i. Head of Finance and their accountant (5 person)
 - ii. Lab Instructors (5 person)
 - iii. Finance clerks (2 person)
 - iv. KUKTEM Customers (18 person)
- } Internal Users
- } External Users

The result of the user satisfaction test will be discussed in the Chapter Six. Refer Appendix F for the example of user satisfaction test.

CHAPTER 6

RESULT AND DISCUSSION

6.1 Introduction

During the implementation and testing phase, ETS has gone through testing process and user satisfaction test. To see how efficient and reliability of ETS, this chapter will analyze and reveal the result of all tests. The test result is important to see the areas of strength and weakness of the ETS for improvement.

6.2 Test Result

Result for ETS will be discussed based on the System Evaluation Test (User Satisfaction Test) where the test has been done during testing phase. There are 30 users involved in this test. The result of this test is analyzed based on the user satisfaction for CUPRIMDA categories in the system. Table 6.1 shows the total of user satisfaction and Figure 6.1 shows the bar chart result of the test.

Category	Very Satisfied	Satisfied	Neutral	Not Satisfied	Very Dissatisfied	Total
capability	3	10	17	0	0	30
usability	10	14	6	0	0	30
performance	0	18	10	2	0	30
reliability	7	13	7	3	0	30
installability	15	10	5	0	0	30
maintainability	4	11	14	1	0	30
documentation/information	22	8	0	0	0	30
availability	9	17	4	0	0	30
Total Scale	70	101	63	6	0	240
Percentage	29%	42%	26%	3%	0%	100%

Table 6.1
Total of User Satisfaction Test Based On CUPRIMDA Categories

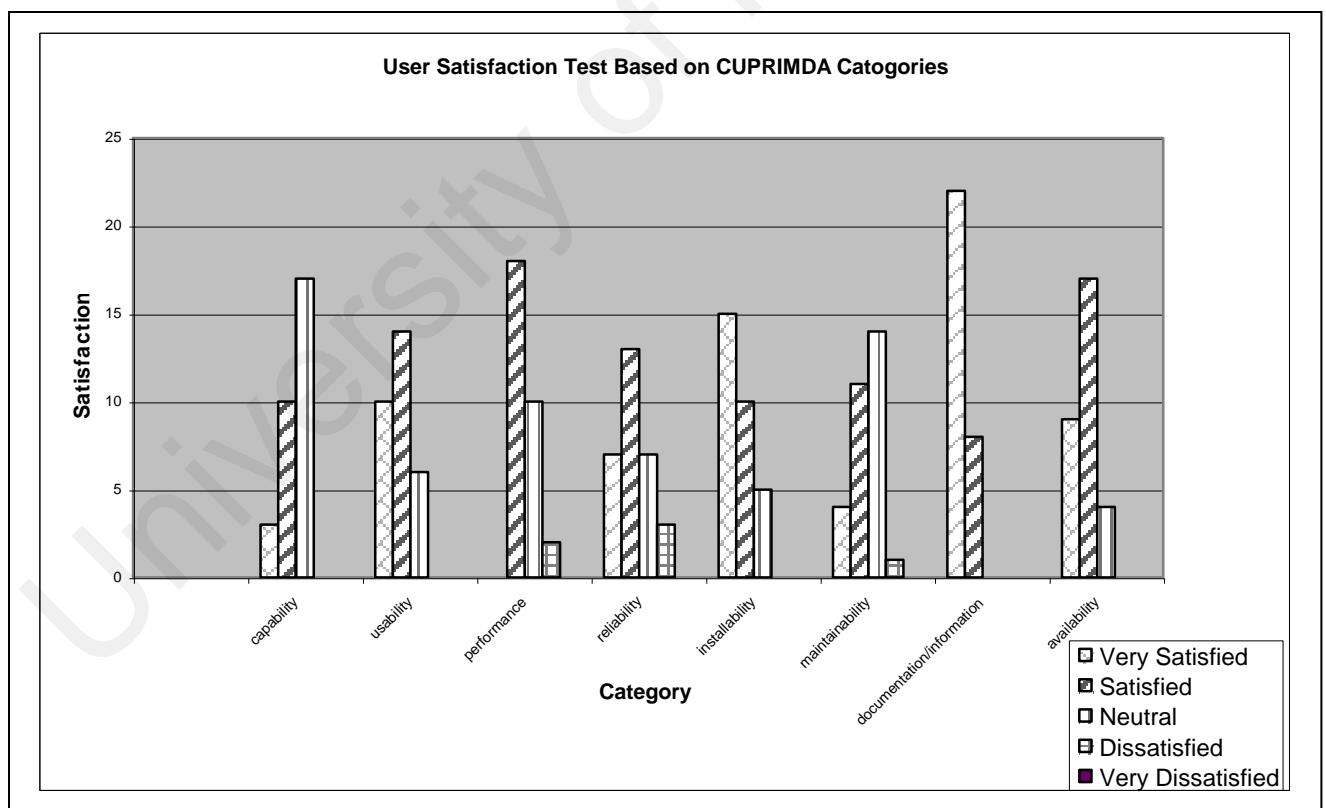


Figure 6.1
Bar Chart On User Satisfaction Test Based On CUPRIMDA Categories

As to conclude from the bar chart result, *very satisfied* scale shows 29%, *satisfied* scale shows 42%, *neutral* scale shows 26%, *not satisfied* scale shows 3% and *very dissatisfied* scale shows 0%.

Users are satisfied most in the documentation and information, where from the bar chart shows more than half users are *very satisfied* with this category. This is due to the documentation given is clear and easy for users to understand and retrieve the user manual from the file library menu in the KUKTEM E-community. Moreover, users also are also very satisfied with the installability and usability category because the system does not have difficulty during installation and it meets most of the usability criteria such as minimize user memory load, speak the user language, consistency, and others.

In the *satisfied* scale, users choose the performance and availability categories. This is due to the smooth of system performance during verifying and validating the customer credit card and downloading the tender document. In the availability category, users are satisfied because the system is easy to access since it has been programmed using ASP and Java Script where those languages are very compatible with any web server.

On the other hand, capability and maintainability categories are the user's choice for the neutral scale. The capability category is a neutral scale because the system is not fully capable in processing the online payment where the system only functions until the bank verifies the customer credit card and KUKTEM has to deal manually with the credit card issuer to capture the payment. Furthermore, maintainability is neutral scale because the tendering process in ETS is depends on the updating work, which is done by the

administrator in the Finance Department. If the administrators delay their works, at the same time, the tendering process will be delayed too.

Not satisfied and very dissatisfied scale shows that less than 3% users are not satisfied with ETS. Meanwhile, almost 71% of users are satisfied with ETS. This describes that users give good feedback to ETS and satisfied with ETS process. Therefore, to make ETS fully accepted by their user, all the strengths and weaknesses identified in this test will be improved from time to time to achieve the excellent result.

6.3 Disadvantages of ETS

Based on the test result as described in the above section, survey on Electronic Tendering System not only shows the advantages of the system but the disadvantages as well. Following are the disadvantages of the ETS, captured during system testing: -

i. Capture Payment

In the payment processing section, the system only includes until the bank verifies the customer credit card. However, the process of capture payment between merchant and the issuer is not included. Therefore the merchant has to deal manually with credit card issuer to capture the payment.

ii. Administrator Task

Most of the updating process in ETS depends on the administrator. If the administrator delay their work, at the same time, the tendering process will

be delayed too. The processes that really depends on the administrator are verifying the customer profile, sending confirmation of registration and updating tender proposal.

As to conclude, ETS still cannot overcome some problems in term of time-consuming and management because some parts in the ETS still needs manual process from the organization.

6.4 Assumption and Further Research

The Electronic Tendering System or ETS with the implementation of Secure Electronic Transaction or SET can be brought to the better performance for tendering process in term of time consuming, reduce cost, secure online payment and submission. In fact, by applying this approach, most of the problems in current tendering process can be overcome. Moreover, the tendering system provides systematic, effective, efficient and high quality of tender process. This assumption will lead to the good relationship between the suppliers and the merchants because both of them can gain some benefits and profits from ETS.

Nevertheless, ETS will be more complete and effective if overall process of tendering can be applied. To enhance the function of ETS, SupplyPoint will be the solution [13]. SupplyPoint is a collaborative research and technology development project. It comes as

an attempt to support the whole tendering or bidding process and also provides services for forming virtual consortia that bids for construction projects.

The concept of the system's functionality is as follows: Assume that company A wishes to search for tenders and connects to the system through the Internet. This will make company A browse for ETS. Search results for tenders are stored in the databases of SupplyPoint. Company A can now search using SupplyPoint, for partners (Company B), and establish communication with them, resulting in the function of a virtual consortium. Companies A and B use the electronic space provided to them by SupplyPoint and prepare the bid to the selected tender. In this context, they locate Company C that will provide them with the necessary material, and invitations to bid and requests for quotations are made. Figure 6.2 shows the supplypoint functional structure and figure 6.3 shows the supplypoint architecture.

The SupplyPoint system consists of nine concrete subsystems[13].

- the document management subsystem, which provides a flexible environment for creation, editing, exchanging and deleting of documents.
- the workflow management subsystem, supporting the automation of workflows for the formation of the virtual consortium and the preparation of the bid.
- the subsystem for the management of the electronic payments of the users' fees.
- the subsystem for the management of searches, including the criteria-based search for tenders as well as the search for potential partners using the profiles of the companies registered to SupplyPoint.

- the administration subsystem, which gives users the possibility to add other users and change the company's working and interest profile.
- the graphical user interface (GUI) that connects the user to the system.
- the help subsystem, providing technical and functional help to the users.

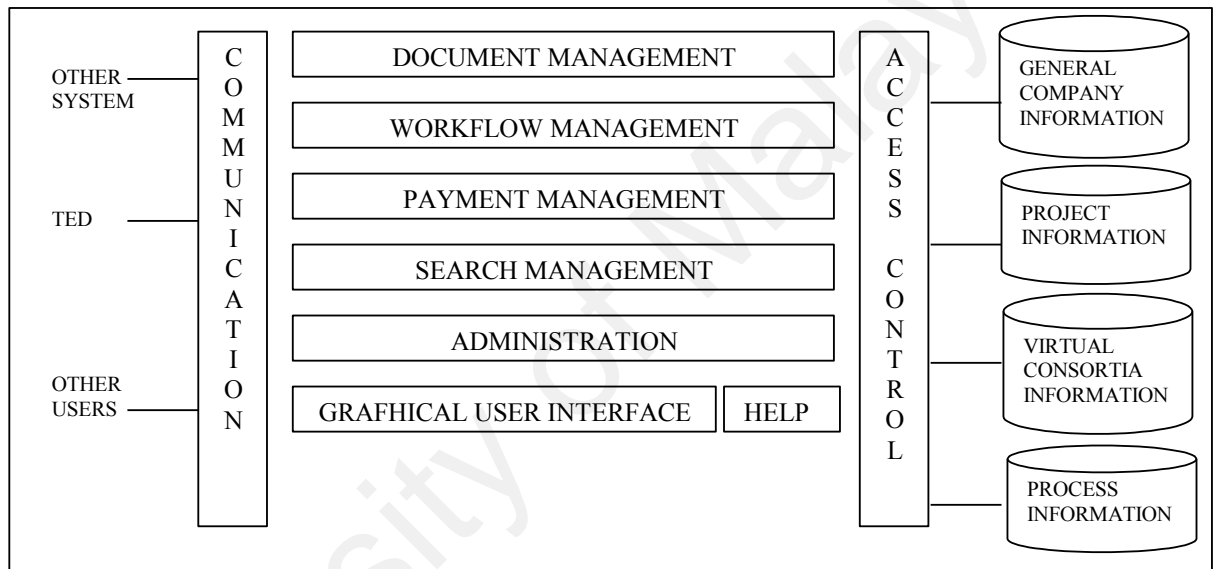


Figure 6.1
SupplyPoint Functional Structure

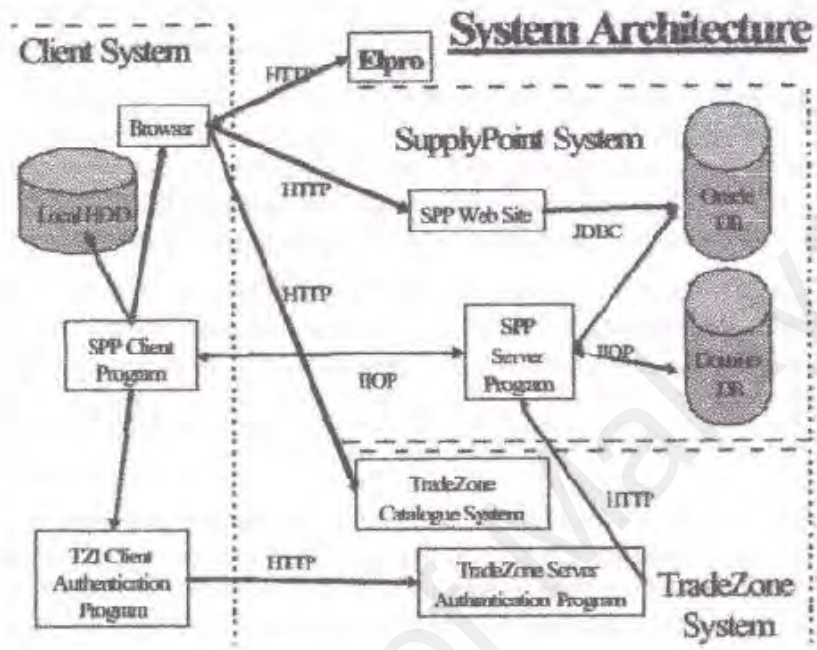


Figure 6.2

SupplyPoint Architecture

CHAPTER 7

CONCLUSION

The Electronic Tendering System or ETS has been developed as a solution in e-commerce for tendering process. The current tendering process in most company produces a lot of difficulties in terms of payment and submission difficulty, time consuming and cost. Therefore ETS has been built to overcome these problems.

In building ETS, one standard protocol has been used which is called as Secure Electronic Transaction or SET. SET is one medium that protects online card credit transaction. SET supports safety communication between the customer, merchant and bank. The types of credit card that are supported by SET are only VISA and MasterCard.

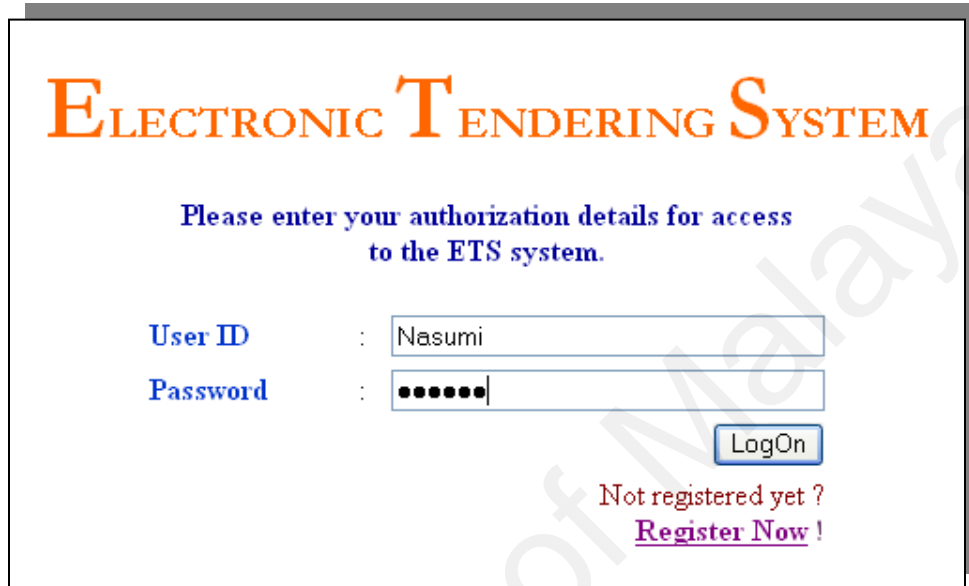
ETS has been developed for front end user (supplier) and back end user (administrator). Front end user support functions such as downloading the tender document, submitting tender proposal, supplier registration, standard terms of tender, tender notice, tender awarded and also support payment via Internet. Meanwhile for the back end-user, they have to monitor and manage the front-end process. Back end system support functions such as updating all the tender information and verify supplier company data.

Based on the testing result, it shows that, ETS can be accepted by the users and most of them are satisfied with its function and process. Therefore, with ETS, the whole process of tendering will cut down on paperwork and increase efficiency in merchant administration as well as provides the new approach in the e-commerce tendering process.

University of Malaya

Front-End Prototype

1. Login Interface



ELECTRONIC TENDERING SYSTEM

Please enter your authorization details for access to the ETS system.

User ID :

Password :

Not registered yet ?
[Register Now !](#)

Figure 1

Login Interface

This is the authorization process. Only the authorized supplier can use the Electronic Tendering System. To be the authorized supplier, they must register their company information. After register, supplier has to wait within 3 days for the company administration to verify their data. Their user id and password will be email to them by administrator. After receiving the user id and password, they may start to use the ETS.

2. Home Interface



Figure 2

Home Interface

The interface shows the ETS Supplier Environment. The difference between the ETS Administration and ETS Supplier is on the menu function. In this interface, it displays a menu on standard terms, supplier profile, awarded tenders, tender notice, tender proposal, feedback and contact us. It also shows a notice about the latest news in tender at the right hand side of the interface.

3. Standard Terms Interface

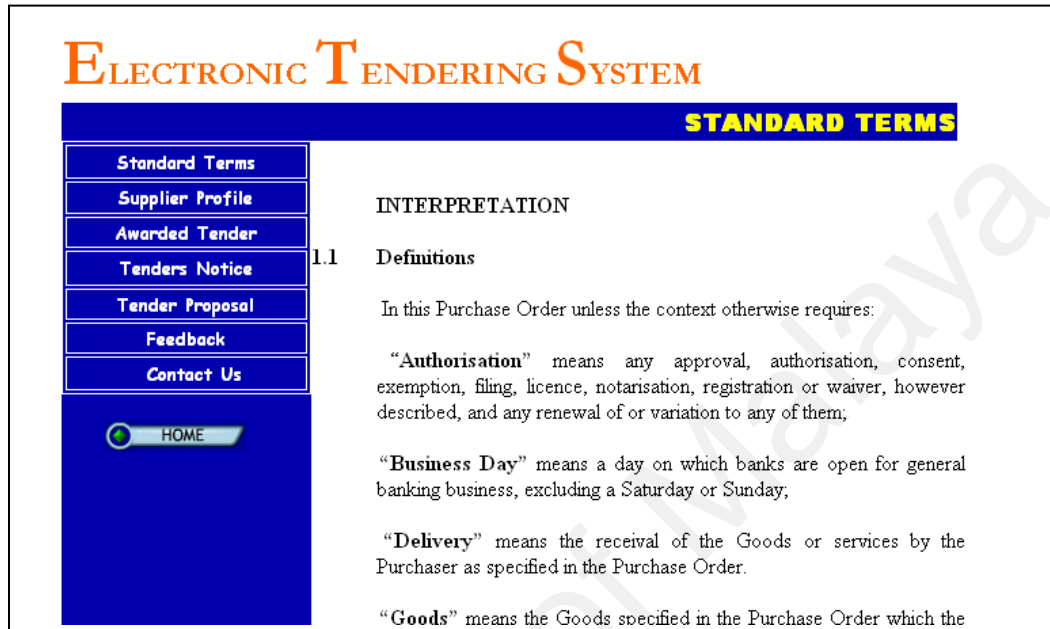


Figure 3

Standard Terms Interface

Standard Terms interface is about the terms that is used by the company with regards to the tendering process. The standard terms included information about the interpretation word used in tender, contract, payment to customer, risk, and etc. Therefore, supplier is advice to read this layout before start to download the tender document.

4. Supplier Profile Interface

The screenshot displays the 'SUPPLIER PROFILE' interface. On the left is a navigation menu with links: Standard Terms, Supplier Profile, Awarded Tender, Tenders Notice, Tender Proposal, Feedback, and Contact Us. Below the menu is a 'HOME' button. The main content area features a search bar for 'Registration No.' with the value '351404 U' and a 'Search' button. Below the search bar is a message: 'This form should be completed in FULL.To view all data,clik VIEW DATA.' The form contains the following fields:

Registration No :	351404 U	Search
Company Name :	Senario Jaya Sdn Bhd	
Office Address:	9128A Jalan Bandar 4, Taman Melawati, 53100 Kuala Lumpur	
Tel No:	03-61896299	
Fax No:	03-61896290	
Email:	general@spantel.com.i	
Supplier URL:	www.spantel.com.my	
User Name:	Spantel	
Password:	••••••	
Comfirm Password:	••••••	
	Update	

Figure 4

Supplier Profile Interface

This interface allowed supplier to update their company information. Supplier must fill their company registration number and press the search button. Next, all the detail about their company that entered during the registration will be display. Supplier is allowed to edit all the information including their username and password. This will prevent unauthorized user using their login data.

5. Awarded Tender Interface

ELECTRONIC TENDERING SYSTEM

Standard Terms
 Supplier Profile
 Awarded Tender
 Tenders Notice
 Tender Proposal
 Feedback
 Contact Us

HOME

Tender Awarded : January 2003 Search

No	Reference No	Title	Supplier	Item/Quantity	Amount
1	A2514542001	Supply of major pumps and hydraulic platforms to the Fire Services Department	Spantel Sdn Bhd, KL	2	RM 200 0
2	A3714202001	Supply, delivery, installation, commissioning, maintenance of hardware and software and the provision of related implementation services for the server upgrade of communal information system	Amfa Enterprise, Ktn	1	RM 50 00
3	A4111722002	Supply of tacrolimus preparations to the Hospital Authority and the Department of Health	TNB KL	3	RM 100 0
4	A6610922002	Supply and installation of high throughput DNA sequencer and accessories	Hitech Padu KL	-	RM 50 00
5	A4810952002	Supply of screw pump gearboxes to Kivun Tong Preliminary Treatment Works	Pernee KL	-	RM 70 00
6	A8710712002	socket layer Supply and installation of electro-mechanically cooled high purity germanium detector	Nasumi Engineering KL	-	RM4000.1
7	A7710672002	Supply of trunked radio equipment and accessories	Senario Jaya KL	2	RM 50 00

Figure 5

Awarded Tender Interface

The awarded tender interface allowed supplier to view information regarding the tender that has been awarded. This interface contains information such as tender reference number, title of tenders, suppliers who win the tender, total quantity or item win, price amount of tender and date awarded. Company administrator will take about 3 months from the closing date to display in the system. The supplier who wins the tender will also be notifying by email.

6. Tender Notice Interface

ELECTRONIC TENDERING SYSTEM

TENDERS NO

Click download to access the tender document. Payment are made only by using credit card VISA OR MASTERCARD.

NO	TITLE	REFERENCE NO	DOCUMENT FEE	CLOSING DATE	CLOSING TIME	CONTACT PERSON	DOWNLO
1	Supply of major pumps and hydraulic platforms to the Fire Services Department	A2514542001	RM 100 000.00	04/04/2004	12 PM	En Amri Abdul Majid	Download
2	Supply of tacrolimus preparations to the Hospital Authority and the Department of Health	A3714202001	RM 500 000.00	20/03/2004	12 PM	En Adam Aiman	Download
3	Supply of trunked radio equipment and accessories	A4111722002	RM 200 000.00	10/03/2004	12 PM	Puan Sara Sufea Saidin	Download
4	Supply and installation of electro-mechanically cooled high purity germanium detector	A6610922002	RM 100 000.00	04/02/2004	12 PM	Puan Fatimah Charu	Download

Figure 6

Tender Notice Interface

The information about the company's tenders was advertised in this tender notice interface. The tender notice included information such as the tender title, tender reference number, document fee and closing date and time. To download the tender document of the interested tender, supplier must click the download option at the right hand side. The next process will lead supplier to the payment authentication for verify and validate supplier card credit.

7. Payment Processing Interface

ELECTRONIC TENDERING SYSTEM

PAYMENT PROCESSING

Standard Terms
Supplier Profile
Awarded Tender
Tenders Notice
Tender Proposal
Feedback
Contact Us
HOME

Fill the information below to verify your card credit.

Tender Reference No :A3714202001

1. Company Registration No:

3. MasterCard Number : *xxxx xxxx xxxx

Figure 7

Payment Processing Interface

After supplier selects their interested tender, secure electronic transaction start to execute. Supplier has to enter their company registration number and MasterCard number. The data will be retrieved from the card credit issuer database. If the data are match , then the card will be verify by the system and next, the card will be validate by the issuer to make sure the card is valid or not for payment. If valid, then, authorization message will appear to allow the supplier download the tender document, as shown in figure 8 and 9.

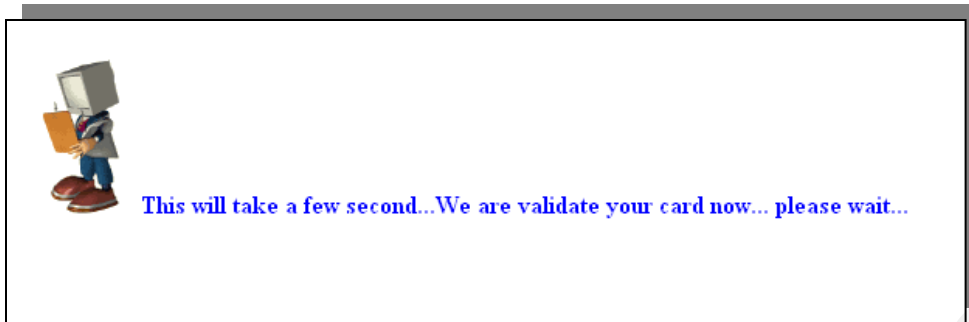


Figure 8
Card Validation Interface

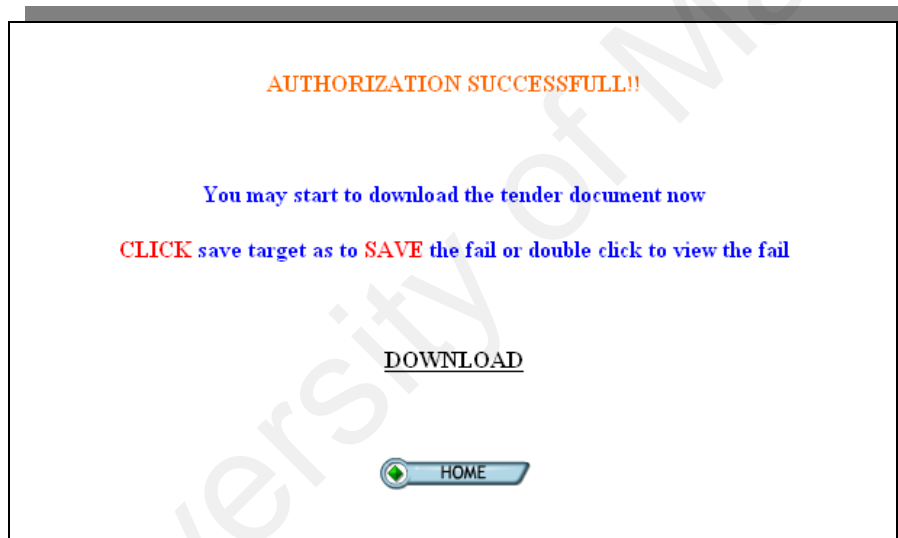


Figure 9
Authorization To Download Tender Document

8. Tender Proposal Interface

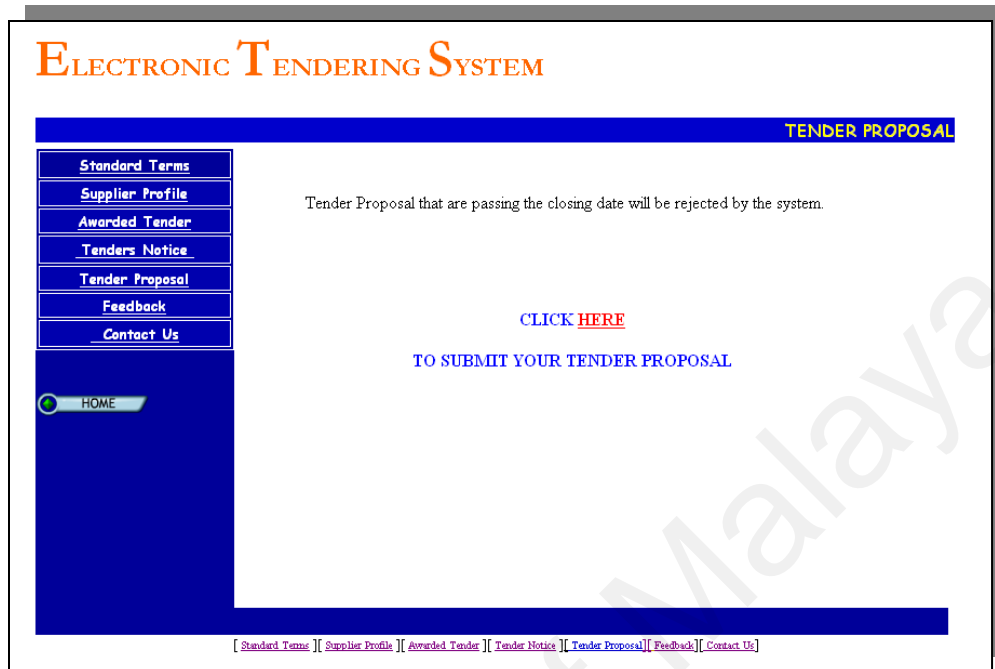


Figure 10

Tender Proposal Interface

This interface provides online tender proposal submission. The submission process will be done by the help from Microsoft Outlook Express. The Outlook has been chose because it provide the encrypt and decrypt method in regards to support secure file transfer. Nevertheless, tender proposal that are passing the closing date will be rejected by the system.

9. Feedback Interface

ELECTRONIC TENDERING SYSTEM

FEEDBACK

Thank you for visiting [OUR ELECTRONIC TENDERING SYSTEM](#) . We hope you had and enjoyable and useful visit. If you have an enquiry about any of the information presented here, please fill out the following form.

Name:

Position:

Company:

Address:

Telephone:

Fax:

Email: *example (ina@yahoo.com)

Enquiry:

HOME

Figure 11

Feedback Interface

Supplier is allowed to give their feedback in order to enquiry about their interested tender or other related field. The confirmation sending message will appear after supplier submit the feedback, refer figure 12. Administrator will reply the supplier's feedback within 2 days by email.



Figure 12

Confirmation Sending Interface

10.Contact Us Interface

The screenshot shows the 'ELECTRONIC TENDERING SYSTEM' logo at the top left. A blue navigation bar on the left contains the following menu items: Standard Terms, Supplier Profile, Awarded Tender, Tenders Notice, Tender Proposal, Feedback, and Contact Us. Below the navigation bar is a 'HOME' button. The main content area is titled 'CONTACT US' and lists contact information for five different roles:

- General Manager Supply, Mr Gavan Wright**
Phone (03) 9685 6045 Fax (03) 9685 6087 Mobile 0417 542 864
email Gavan.Wright@wmc.com
- Group Manager, e-Supply, Mr John Jeffreys**
Phone (03) 9685 6113 Fax (03) 9685 6087
email john.jeffreys@wmc.com
- Group Manager, Business Processes & Support, Mr Jerome Curwood**
Phone (03) 9685 6451 Fax (03) 9685 6414 Mobile 0407 990 402
email jerome.curwood@wmc.com
- Group Manager, Purchasing, Mrs Bronwyn McMillan**
Phone (03) 9685 6195 Fax (03) 9685 6411 Mobile 0419 772 624
email bronwyn.mcmillan@wmc.com
- Group Manager, Supply Operations (East), Mr Garry Wyatt**
Phone (03) 9685 6198 Fax (03) 9685 6087
email garry.wyatt@wmc.com

At the bottom, there is a line for **Group Manager, Transport and Logistics, Mr John Oliver**.

Figure 13

Contact Us Interface

Contact us interface contains information on the person in charge to the tenders. If the supplier urgently wants to respond on their enquiry about the related tenders, they may contact the person in charge by telephone. Other information in this interface are company address, telephone number and email of person in charge.

11. Supplier Registration Interface

SUPPLIER REGISTRATION

[Feedback](#)
[Contact Us](#)

[HOME](#)

Complete this form to register as a supplier for the our company. Registered suppliers have access to the latest tender information and documents published on this system. All information is kept confidential.

You are allowed to used this system after we confirm your registration by email to you ,Your UserName and Password . If these are not received within 3 days ,please contact the System Administrator in "Contact Us".

This form should be completed in FULL, and fields marked with "*" are MANDATORY.

PART I - DETAILS OF THE COMPANY

1. Registration No : *

2. Name of Company : *

3. Office Address : *

4. Tel No : *

5. Fax No : *

6. Email : *

7. Customer URL : *

The username and password you enter will be used to subsequently access this website.

Your password must be same as your confirm password

Username: *

Password: *

Confirm Password: *

PART III - REGISTRATION DOCUMENT

Documents required upon registration

1. Ministry of Finance Certificate(2 copy)
2. Contractor Service Center Certificate(2 copy)
3. Form 9,24,44,49(1copy)

The interfaces only for those suppliers who are not register yet to this company. Therefore they have to fill all their company information and set their username and password. The unregistered supplier can only access feedback and contact us menu.

Supplier must send by post all their company certificate as stated in the continues interface shown in figure 14(b). These certificate will next be analyze and verify by the administrator. If valid, admin confirm the registration by sending the supplier username and password as authorized to access the ETS.

The screenshot displays a web interface titled "PART III - REGISTRATION DOCUMENT". On the left, there is a large blue vertical bar. The main content area has a yellow background and lists the following documents required upon registration:

1. Ministry of Finance Certificate(2 copy)
2. Contractor Service Center Certificate(2 copy)
3. Form 9,24,44,49(1 copy)
4. Company Registration Form(1 copy)
5. Company Profile(1 copy)

Below the list, it states: "These documents should be send by post to:" followed by the contact information for Telekom Malaysia Berhad:

Telekom Malaysia Berhad
PO BOX 234
68000
Kuala Lumpur

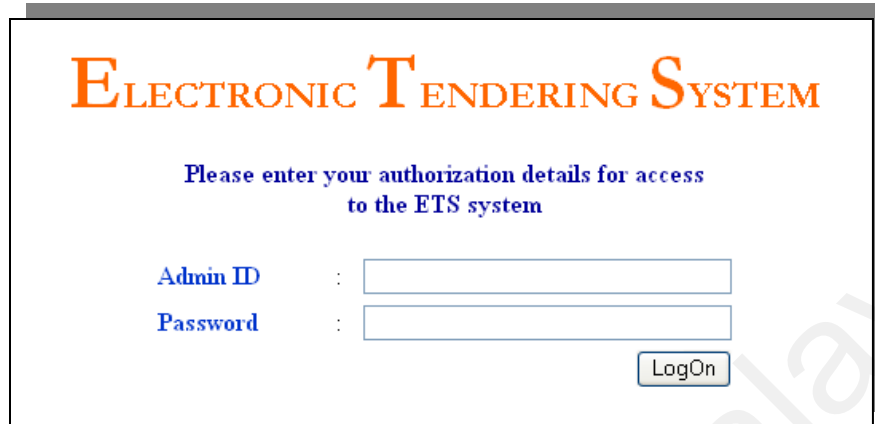
At the bottom, it says: "If you have any enquiry please do not hesitate to contact us."

Figure 14(b)

Supplier Registration Interface (Continue)

Back-End Prototype

1. Login Interface



The screenshot displays the login interface for the Electronic Tendering System. At the top, the title "ELECTRONIC TENDERING SYSTEM" is written in a large, orange, serif font. Below the title, a blue instruction reads: "Please enter your authorization details for access to the ETS system". There are two input fields: "Admin ID" and "Password", each followed by a colon and a text box. A "LogOn" button is positioned to the right of the password field.

Figure 15

Admin Login Interface

Basically, the admin login function same as supplier login. The different is, only authorize person can add new authorize user. This is important to make sure only the right person using the ETS since this system is too confidential. Therefore, admin are required to change their password regularly to avoid eavesdropper among company staff.

2. Home Interface

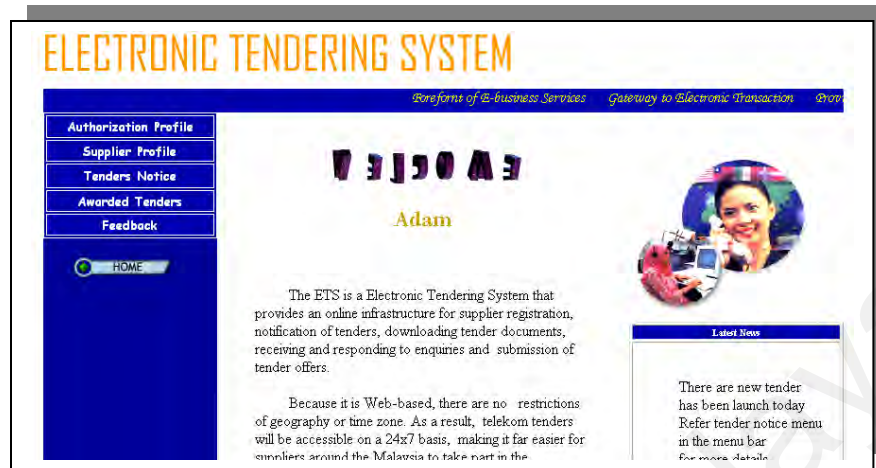


Figure 16

Home Interface

The home interface for the admin system basically same as supplier system but the different is on the menu function where only five types of menu available for admin usage. There are authorization profile, supplier profile, tenders notice, awarded tender and feedback menu

3.Authorization Profile Interface

The screenshot shows the 'ELECTRONIC TENDERING SYSTEM' logo at the top left. A blue header bar contains the text 'AUTHORIZATION PROFILE' in yellow. Below the header, a navigation menu on the left lists 'Authorization Profile', 'Supplier Profile', 'Tenders Notice', 'Awarded Tenders', and 'Feedback'. A 'HOME' button is also visible. The main content area features a search bar for 'IC No.' with the value '630108075673' and a 'Search' button. Below this, a form displays the following fields: 'Name' (Adam Aiman Zulkornain), 'Position' (Application Engineer), 'User Name' (Adam), 'Password' (masked with four dots), and 'Confirm Password' (masked with four dots). At the bottom of the form are buttons for 'Add', 'Save', and 'Delete'. A note above the form states: 'This form should be completed in FULL.To view all data,click VIEW DATA.'

Figure 17

Authorization Profile Interface

The Authorization Profile Interface will allow administrator to update information related to their authorization to login the system. Administrator can add new authorize person to do the management process. They are allow also deleting, search or view authorize person. Furthermore, this interface allows admin to view all the data directly from the database. See figure 18.

ADMINISTRATOR DATA

No	IC No	Name	Position	UserName	Password	Confirm Password
1	0045	Alia Sabrina Zulkornain	Clerk	Alia	alia	alia
2	0046	Aira Safiya Zulkornain	Engineer	Aira	AIRA	AI
3	0047	fatimah	sada	adsd	timah	timah
4	0067	Adam Aiman Zulkornain	Application Engineer	Adam	adam	adam
5	630108075673	Adam Aiman Zulkornain	Application Engineer	Adam	adam	adam
6	700414055532	Alia Sabrina Zulkornain	Clerk	Alia	alia	alia
7	78031206558	MAZLINA BT ABDUL MAJID	ACCOUNTANT	INA	INA	INA

Figure 18

Authorization Data Interface

4. Supplier Profile Interface

SUPPLIER PROFILE

This form should be completed in FULL.To view all data,click VIEW DATA.

Registration No :

Company Name :

Office Address:

Tel No:

Fax No:

Email:

Supplier URL:

User Name:

Password:

Confirm Password:

Status :

[View Data](#)

Figure 19

Supplier Profile Interface

The menu will allow administrator to update information related to supplier information such as delete, search and view supplier. Administrator will verify new supplier by checking their company profile. If their company profile is valid then to confirm the registration, admin will select the status confirm. Then administrator will send the username and password to them by email. This interface also provides link to view all data directly from the database. See figure 20.

SUPPLIER DATA										
No	Registration No	Company Name	Office Address	Tel No	Fax No	Email	Supplier URL	UserName	Password	Confir Password
1	11	kakani	kuktem	09-5141704	55555	hhhh	ddd	ani	ani	ani
2	12	mazkck	xxdes	55	55	55	fgdg	baby	ina	ina
3	13	df	filfil	dsf	sdf	s	flsf	dfis	44	44
4	14	wedesdf	dsfs	234	3424	dsf	df	dfsdf	dff	ff
5	15	sds	dsada	5646	346	fdsf	dfsdf	dsf	dsc	sds
6	16	dfs	dfs	dsf	dfil	dfs	d	dsf	ere	
7	17	mazlina	108 jln lengkok taman tanah putih baru 25150 ktn	09-5141704	09-5141704	inaomel@yahoo.com	http://telekom.com.my	dxcsd	sdf	ddd
8	18	rflg	dsfsdgd	54534	5434	fdfdg	fcfgg	flg	gflg	fgg
9	19	hsdag	sdsflsdf	435646	546456	vxcv	cvxcv	fsdf	444	444
10	20	weer	dzsd	52345	3455	dsfs	sdfsdf	ggg	22	
11	21	nasumi	czxc	eee	eee	CCKC	cxc	nasumi	nasumi	nasumi
12	22	rrr	rr	rr	rr	rr	rrr	rr	44	
13	23	test	eee	eee	ee	22	sas	rr	rr	
14	24	ina	rerewrwersdsfsdfsdfsdfsdfsdf	444	444	rrr	fff	rrr	rr	rr

Figure 20

Supplier Data Interface

5. Tender Notice Interface

ELECTRONIC TENDERING SYSTEM

TENDER NOTICE

This form should be completed in FULL. To view all data, click VIEW DATA.

Reference No :

Title:

Document Fee:

Closing Date:

Closing Time :

Contact Person:

Tender File:

[View Data](#)

Figure 21

Tender Notice Interface

The Tender Notice Interface allow administrator to update information related to tender such as add new, delete, search and view tenders. See figure 22.

TENDER NOTICE DATA

No	Reference No	Title	Document Fee	Closing Date	Closing Time	Contact Person	Tender File
1	A2514542001	Supply of major pumps and hydraulic platforms to the Fire Services Department	RM 100 000.00	04/04/2004	12 PM	En Amri Abdul Majid	A28.pdf
2	A3714202001	Supply of tacrolimus preparations to the Hospital Authority and the Department of Health	RM 500 000.00	20/03/2004	12 PM	En Adam Aiman	A27.pdf
3	A4111722002	Supply of trunked radio equipment and accessories	RM 200 000.00	10/03/2004	12 PM	Puan Sara Sufea Saidin	A26pdf
4	A6610922002	Supply and installation of electro-mechanically cooled high purity germanium detector	RM 100 000.00	04/02/2004	12 PM	Puan Fatimah Ghani	A25.pdf

Figure 22

Tender Notice Data

6. Awarded Tender Interface

ELECTRONIC TENDERING SYSTEM

AWARDED TENDERS

This form should be completed in FULL. To view all data, click VIEW DATA.

Reference No:

Title:

Supplier:

Item/Quantity:

Amount:

Date Awarded:

[View Data](#)

Figure 23

Awarded Tender Interface

The menu will allow administrator to update information related to award tender such as add new, delete, search and view awarded tenders. See figure 24.

No	Reference No	Title	Supplier	Item/Quantity	Amount	Date Awarded
1	A2514542001	Supply of major pumps and hydraulic platforms to the Fire Services Departmen	Spantel Sdn Bhd, KL	2	RM 200 000.00	1/3/2003
2	A3714202001	Supply, delivery, installation, commissioning, maintenance of hardware and software and the provision of related implementation services for the server upgrade of communal information system	Amfa Enterprise, Ktn	1	RM 50 000.00	1/10/2003

Awarded Tender Data

7.Feedback Interface

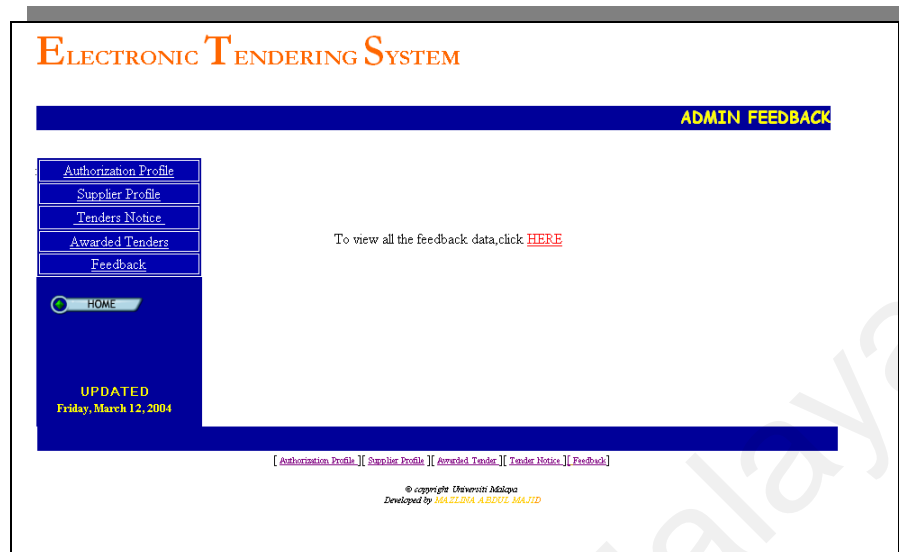


Figure 25

Feedback Interface

Administrator can read and view feedback from supplier in the Feedback Interface To view all feedback from supplier, admin must click the provided link. After read the supplier feedback; admin can directly reply by selects their email. Next the link will brought automatically to Microsoft Outlook Express. For the enquiry that has been reply, admin must select “reply” to show current status of enquiry. Otherwise the admin will leave blank See figure 26.

FEEDBACK DATA

No	Date	Name	Position	Company	Address	Telephone	Fax	Email	Enquiry	Status
1	3/8/2004 4:41:58 PM	sac	azxc	zxcz	c2xc	zxc0	zxc0	xzc	xzc	REPLY ▾
2	3/8/2004 4:43:01 PM	df	df	vcx	vcvxc	vcv	vcv	cv	cv	REPLY ▾
3	3/9/2004 12:12:14 AM	Syahnizam Abdullah Sani	Engineer	Spantel Sdn Bhd	PO BOX 68000,Kuala Lumpu	09- 6831200	09- 6831200	syah@spantel.com	please inform me about the lastest tender.	REPLY ▾
4	3/3/2004 9:06:47 AM	MAZLINA BT ABDUL MAJID	LECTURER	KUKTEM	BDR MEC KTN	019- 9310429	019- 9310429	MAZLINA@KUKTEM.EDU.MY	please inform me about new tender.tq	▾
5	3/3/2004 9:06:47 AM	AMRI MOHD HALIM	ENGINEER	AMFA ENTERPRISE	BLOK B,LORONG 3,JALAN WONG AH JANG KTN	09- 5178996	09- 5178996	Amri@amfa.com	when will tender be awarded	▾
6	3/7/2004 9:06:47 AM	fff	fff	fff	fffj	fff	fff	fff	fff	▾
7	3/7/2004 10:41:20 AM	Damia	Clerk	Nasumi	ghDzf	dfdf	dfdf	damia@nasumi.com.my	dfsfsdf	▾
8	3/7/2004	ghg	gfh	gfh	hg	hg	h	h	hj	▾

Figure 26

Feedback Data Interface

REFERENCES

- [1] Universiti of Sydney, *Purchasing Policy : Guidelines and Procedures*, Revised December 1999, page 3
- [2] Alireza Bahreman and Rajkuman Narayanaswamy, *Payment Method Negotiation Service: Framework and Programming Specification*, Oakland, California, November 1996
- [3] Thomi Pilioura , *Electronic Payment Systems on Open Computer Networks: A Survey*.
- [4] N.Asokan, Phillippe A. Janson, Michael Steiner and Michael Wainder, “The State of the Art in Electronic Payment Systems”.
- [5] Special Issue on Electronic Money, IEEE Spectrum, February 1997
- [6] Donal O’Mahony, Michael Peirce and Hitesh Tewari, “Electronic Payment Systems”, Artech House, 1997
- [7] Description on the **Cybercash** at <http://www.cybercash.com/cybercash/wp/>.
- [8] Lynch, D.C. and Lundquist, L.: *Digital Money: The New Era Of Internet Commerce*. Chichester: Wiley (1996)

- [9] Description the **Visa** at <http://www.visa.com/cgi-bin/vee/nt/ecommerce/set/main.html>
- [10] Description on the MasterCard at <http://www.mastercard.com/set/set.html>
- [11] Description on the <http://www.wolrath.com/set.html>
- [12] Description on the website WMC-Procurement at <http://www.wmc-procurement.com>.
- [13] Christos HALARIS, Georgia Bafoutsou, George Papavassiliou, Gregoris Mentzas, *A System For Virtual Tendering And Bidding*, Department of Electrical and Computer Engineering, University of Athens, Greece
- [14] Siddharth Nartiyal, *E-Commerce Support :A Report*, January 12, 1999, page 5
- [15] Peik Niemi, *Electronic Payment System*, November 12, 2000, page 2,3,6,7
- [16] <http://developer.netscape.com/tech/security/ssl/howitworks.html>
- [17] Eugenio S.Passalacqua, *Secure Socket Layer*, May 9, 1997
- [18] http://www.tml.hut.fi/Studies/Tik-110.350/1997/Ecommerce/sips_4.html

- [19] Mihir Bellare, Juan A. Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Els Van Herreweghen, Michael Waidner, ***Design, Implementation and Deployment of the iKP Secure Electronic Payment System***, IEEE Journal of Selected Areas in Communications, VOL 18, NO. 4, April 2000
- [20] William Stallings, ***Introduction to Secure Electronic Transaction (SET)***, May 17, 2002.
- [21] Mastercard and Visa, ***External Interface Guide, Secure Electronic Transaction***, September 24, 1997
- [22] ***SET Secure Electronic Transaction Specification, Book 2: Programmer's Guide***, Version 1.0, May 31, 1997
- [23] William Stallings, ***Network Security Essentials: Application and Standards***, Prentice Hall, United State of America, 2000
- [24] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22: 644-654, 1976.
- [25] For more details about RSA go to: <http://www.rsa.com/rsalabs/newfaq/>
- [26] For more details about DES see: <http://www.rsa.com/rsalabs/newfaq/q64.html> , <http://www.rsa.com/rsalabs/newfaq/q9.html>
- [27] For an in-depth description of the crypto in SET see: [SET Specification, Book 1: Business Description \(1997\), p. 14-24](#)
- [28] Source about RSA at: <http://www.rsa.com/set/html/howstrong.html>

- [29] SET Specification Book 2: Programmer's Guide (1997), page 43. Downloadable at http://www.setco.org/set_specifications.html
- [30] SET Specification Book 1: Business Description (1997), page 27. Downloadable at http://www.setco.org/set_specifications.html
- [31] Ali Bahrami, *Object Oriented Systems Development*, International Edition, Irwin McGraw-Hill, Singapore, 1999, page 59,79.
- [32] <http://www.granite.ab.ca/access/advantages.htm/>
- [33] Description on the Prototype at <http://www.pierlou.com/prototype/>
- [34] David Buser, *Beginning Active Server Pages 3.0*, Wrox Press ,United States,UK, 2002.
- [35] Jeffrey A.Hoffer,Modern Systems Analysis and Design, Third Edition, Prentice Hall,USA, 2002.
- [36] Sandra Donaldson Dewitz, System Analysis and Design and the Transition to Objects, Mc-GrawHill,Singapore, 1996.
- [37] Lecture Note, Software Metric.2002
- [38] George Apostolopoulos, Vinod Peris,Debanjan Saha,*Transport Layer Security:How much it really cost?* IBM TJ Watson Research Center, New York.
- [39] Description on the oversea tenders at [https:// tenders.nsw.gov.au](https://tenders.nsw.gov.au).

- [40] Link to UK ETS at <https://ets.leeds.gov.uk>
- [41] Link to bipcontracts at <http://www.bipcontracts/delta.html>.
- [42] Christos HALARIS, Georgia Bafoutsou, George Papavassiliou, Gregoris Mentzas, *A System For Virtual Tendering And Bidding*, Department of Electrical and Computer Engineering, University of Athens, Greece
- [43] Dennis Abrazhevich, *Classifications and Characteristics of Electronic Payment System*, IPO Center of User System Interaction, Technical University of Eindhoven (TUE), Eindhoven, The Netherlands.
- [44] Pete Loshin, *Personal Encrytion*, Academic Press, London, 1998
- [45] E-perolehan -the electronic procurement system of the government of Malaysia, 2004.
<http://home.eperolehan.com.my/en/default.aspx>
- [46] **Software Development LifeCycle (SDLC)**, Version 1.0d 4, 2004.
www.elucidata.com/refs/sdlc.pdf