

**AUTHENTICATED ELECTRONIC DOCUMENTS  
USING DIGITAL SIGNATURE**

**LYE SHI TYNG**

This report is submitted in partial fulfillment of the requirements for the  
Bachelor of Information and Communication Technology (Computer Network)


**FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY  
NATIONAL TECHNICAL UNIVERSITY COLLEGE OF MALAYSIA  
2004**

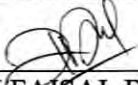
**ADMISSION**

I admitted that this project title name of

**AUTHENTICATED ELECTRONIC DOCUMENTS USING DIGITAL  
SIGNATURE**

is written by me and is my own effort and that no part has been plagiarized without  
citations.

STUDENT :  Date : 20/10/2024  
( LYE SHI TYNG )

SUPERVISOR :  Date : 20/10/2024  
( EN. SHEKH FAISAL B. ABDUL LATIP )

## **DEDICATION**

To my Mom and Dad,  
whose boundless love and support replenishes and enriches my soul  
during the long hours of writing.

## ACKNOWLEDGEMENT

One of the greatest pleasures is acknowledging the efforts of many people whose names may not appear on the cover, but whose hard work, cooperation, friendship, and understanding were crucial throughout the process of this thesis.

First and foremost, I would like to thank my project supervisor, En. Shekh Faisal Abd. Latip, for teaching, guiding and advising me on matters related to the project. Thanks for being so supportive, cooperative and leading the way throughout the whole course of the project. Also, I would like to express my sincere thanks for all PSM committees. The project would not have been completed without the guidance from them.

It is with utmost pleasure also that I would like to thank En. Ahmad Fadzli Nizam, the administrative officer of Faculty Information and Communication Technology, for spending his precious time to accept my interview. The facts collected are significant and valuable for entire system construction.

I would like to thank my parent and siblings, for their undying support, thoughts and encouragement during study in Kolej Universiti Teknikal Kebangsaan Malaysia (KUTKM). Last but not least, I want to show my heartiest gratitude to all my friends and all those who helped me in one way or another towards the success of this project.

## ABSTRACT

The title of this thesis is “Authenticated Electronic Documents using Digital Signature (AED)”. The main purpose of AED system is to transmit form electronically in a secure method within a sender (applicant) and receiver (approver) using digital signature infrastructure. Digital signatures let the recipient of information verify the authenticity of the information’s origin, and also verify that the information was not altered while in transit. Staffs in Faculty of Information and Communication Technology have to hand in their form application manually in existing form transmission system. This process is awkward and time-consuming for both the staffs and the faculty. The technology to submit assessments electronically is available. However, there do exist certain requirements from the involved entities that they want to be sure that their application are submitted confidentially and that the authenticity of an application preserved. In addition they want a confirmation of receipt. The faculty needs to be certain about the originator of a form and that staffs cannot falsely claim not having sent an assessment. This thesis addresses these issues of authenticity, integrity and non-repudiation when using AED system for the submission of form application electronically. It introduces several ways to achieve the desired services and demonstrates how to methodically proceed from the initial problem up to a later implementation of the solution, people feel confident that their form is not going to be altered by a determined and highly resourceful attacker during the form transmission process.

## ABSTRAK

Tesis yang bertajuk “Authenticated Electronic Documents using Digital Signature (AED)” ini bertujuan untuk memastikan proses penghantaran borang secara elektronik berlaku dalam satu prosedur yang selamat dan tidak diancam di antara penerima dan pengirim dengan menggunakan senibina *digital signature*. Senibina *digital signatures* membolehkan penerima membuat pengesahan terhadap keaslian informasi yang diterima di samping memastikannya tidak diminda atau diubah semasa proses penghantaran. Kumpulan pekerja di Fakulti Teknologi Maklumat dan Komunikasi perlu menghantar borang permohonan mereka secara sendiri dalam sistem penghantaran borang yang sedia ada. Proses ini adalah ketinggalan dan membuang masa bagi kedua-dua pihak pekerja dan fakulti. Proses penghantaran secara elektronik sedia digunakan tetapi masih wujud keperluan dikalangan pengguna dimana mereka perlu memastikan borang permohonan dikirim dalam satu keadaan yang rahsia dan pengesahan dipentingkan. Di samping itu, kumpulan pekerja memerlukan pemastian tentang status penerimaan borang dan pihak fakulti perlu memastikan tentang identiti pemilik asal bagi borang tersebut. Tesis ini menyelesaikan masalah ini dari segi ketulenan, ketulusan dan ketidakkwaan dengan menggunakan sistem AED untuk menguruskan proses penghantaran borang permohonan. Pelbagai cara digunakan untuk memenuhi perkhidmatan idaman. Pekerja akan berasa yakin bahawa data tidak diubah oleh penceroboh rangkaian semasa proses penghantaran borang.



## TABLE OF CONTENTS

<b>PROJECT TITLE</b>	i
<b>ADMISSION</b>	ii
<b>DEDICATION</b>	iii
<b>ACKNOWLEDGEMENT</b>	iv
<b>ABSTRACT</b>	v
<b>ABSTRAK</b>	vi
<b>TABLE OF CONTENTS</b>	vii
<b>LIST OF TABLES</b>	x
<b>LIST OF FIGURES</b>	xii
<b>LIST OF ABBREVIATION</b>	xiii
<b>LIST OF APPENDIXS</b>	xiv
<b>INTRODUCTION</b>	
1.1 Introduction	1
1.2 Problem Statements	2
1.3 Goal of Project	3
1.4 Objectives	3
1.5 Scopes	5
1.6 Significances	6
1.7 Propose solutions	7
1.8 Organization of project report	8
<b>LITERATURE REVIEW</b>	
2.1 Introduction	9
2.2 Fact and Finding	9
2.2.1 Theory and Concept	10
2.2.1.1 Authentication	10
2.2.1.2 The ISO /OSI basic reference model	11
2.2.1.3 Asymmetric Cryptography	12
2.2.1.4 RSA Public Key Cryptosystem	14
2.2.1.5 Hash Function (SHA-1)	15
2.2.1.6 Digital Signatures	16
2.2.1.7 Public key Encryption for Digital Signatures	18
2.2.1.8 Digital Certificates	20
2.2.2 Case study	20
2.2.2.1 Privacy enhanced mail(PEM)	21
2.2.2.2 Secure MIME (S/MIME)	22
2.2.2.3 Pretty Good Privacy (PGP)	22
2.2.2.4 Comparison between PGP, PEM, S/MIME	24

2.3	Conclusion	25
<b>PROJECT PLANNING AND METHODOLOGY</b>		
3.1	Introduction	28
3.2	High-Level Project Requirements	28
	3.2.1 Project Facilities Requirements	29
	3.2.2 Software Requirement	29
	3.2.3 Hardware Requirement	32
3.3	System Development Approach	33
3.4	Project Schedules and Milestone	36
3.5	Conclusion	37
<b>ANALYSIS</b>		
4.1	Introduction	38
4.2	Analysis of Current System	38
	4.2.1 Business Process	39
	4.2.2 Problem Analysis	40
	4.2.2.1 Overview	40
	4.2.2.2 Description of current situation	40
	4.2.3 Problem Statements	42
4.3	Analysis of To Be System	44
	4.3.1 Functional Requirements	44
	4.3.2 Technical Requirements	47
	4.3.2.1 Software Requirement	48
	4.3.2.2 Hardware/Firmware Requirement	49
	4.3.2.3 Implementation/ Development Requirement	49
4.4	Conclusion	50
<b>DESIGN</b>		
5.1	Introduction	51
5.2	Preliminary/High Level Design	52
	5.2.1 Raw input/data	52
	5.2.2 System architecture	52
	5.2.3 User Interface Design	54
	5.2.3.1 Navigation Design	54
	5.2.3.2 Input Design	55
	5.2.3.3 Output Design	55
	5.2.4 Database Design	56
	5.2.4.1 Logical Database Design	56
5.3	Detailed Design	59
	5.3.1 Software Specification	59
	5.3.1.1 Data Flow Diagram (DFD) Level 0 – Context Diagram	60
	5.3.1.2 Data Flow Diagram Level 1	61
	5.3.1.3 Data Flow Diagram (DFD) Level 2	62
	5.3.2 Physical Database Design	70
5.4	Conclusion	71
<b>IMPLEMENTATION</b>		
6.1	Introduction	72



6.2	Software Development Environment setup	73
6.2.1	Network Configuration	73
6.2.2	Database Configuration	74
6.3	Implementation Status	76
6.4	Conclusion	78
<b>TESTING</b>		
7.1	Introduction	79
7.2	Test Plan	80
7.2.1	Test Organization	80
7.2.2	Test Environment	81
7.2.3	Test Schedule	82
7.3	Test Strategy	83
7.3.1	Classes of tests	84
7.4	Test Design	85
7.4.1	Test Description	85
7.4.2	Test Data	86
7.5	Test Case Results	92
7.6	Conclusion	92
<b>PROJECT CONCLUSION</b>		
8.1	Observation on Weaknesses and Strengths	93
8.2	Propositions for Improvement	94
8.3	Conclusion	94
<b>BIBLIOGRAPHY</b>		95
<b>ATTACHMENTS</b>		99
<b>APPENDIX A - TABLES</b>		100
<b>APPENDIX B - GANTT CHART</b>		107
<b>APPENDIX C - ORGANIZATION CHART</b>		109
<b>APPENDIX D - USER INTERFACE DESIGN</b>		111
<b>APPENDIX E - INTERVIEW CONTENTS</b>		130
<b>APPENDIX F - TESTING</b>		134
<b>APPENDIX G – USER MANUAL</b>		146

## LIST OF TABLES

<b>No.</b>	<b>Title</b>	<b>Page</b>
2.1	ISO/OSI Security Services	11
2.2	ISO/OSI Security Services and Layers	12
2.3	RSA encryption algorithm	15
2.4	Summary of PGP	23
2.5	PGP, PEM and S/MIME	24
2.6	Comparison between RSA and DSA.	27
3.1	Project facilities requirements for AED system	29
3.2	Comparison between Visual Basic. NET and Visual Basic 6	30
3.3	Comparison between SQL server and Microsoft Access	31
3.4	Hardware requirement for AED application	32
3.5	Objective of Project Planning Type	34
A.1	Project schedule of AED system	101
4.1	Specification Login Requirement	45
4.2	Specification Form Submission Requirement	46
4.3	Specification Form Status Requirement	46
4.4	Specification Public Key Checking Requirement	47
4.5	Specification Administrative Requirement	47
4.6	Software Requirements for AED system	48
4.7	Hardware Requirements for AED system	49
4.8	Implementation Requirements for AED system	50
5.1	Raw Data of Leave form, Vehicle Services form and Room/Hall booking form	52
A.2	Input Design	102
A.3	Output Design	103
A.4	Data Dictionary for all the tables in AED database	105
6.1	Network configurations of AED system	74
6.2	Database configuration of AED system	75
6.3	Implementation status	76
7.1	AED Test Environment	81
7.2	AED Test Schedule	82
7.3	Categories of Test Case Design Techniques	83
F.1	Output Correctness Testing for AED system	135
F.2	Test Description for User Login Module testing.	137
F.3	Test Description for Leave form Module Testing.	138

F.4	Test Description for Vehicle Services Form Module testing.	139
F.5	Test Description for Room/Hall Booking Form Module testing.	140
F.6	Test Description for Public Key Checking Module Testing.	141
F.7	Test Description for Administration Module Testing.	142
7.4	Test Data for User Login Module	86
7.5	Test Data for Leave Form Module	86
7.6	Test Data for Leave Form - Verify Module	87
7.7	Test Data for Leave Form – Signing Module	87
7.8	Test Data for Vehicle Services Form Module	88
7.9	Test Data for Vehicle Services Form -Verify Module	88
7.10	Test Data for Vehicle Services Form - Signing Module	89
7.11	Test Data for Room/Hall Booking Module	89
7.12	Test Data for Room/Hall Booking Form -Verify Module	90
7.13	Test Data for Vehicle Services Form - Signing Module	90
7.14	Public Key Checking Module	91
7.15	Admin Module	91
F.8	Test Case Results for AED System	144

## LIST OF FIGURES

<b>No.</b>	<b>Title</b>	<b>Page</b>
1.1	Organization of project report	8
2.1	Asymmetric Key Encryption	13
2.2	Public Key Encryption for Digital Signature	18
2.3	Overall view of a typical digital signature scheme	19
3.1	Waterfall Model	33
4.1	Entire form transmission process	42
4.2	Sentinel Complaints by Calendar Year	43
4.3	DFD Level 1- AED System	45
5.1	System Architecture of AED system	53
5.2	Navigation design of AED system	54
5.3	Entities Relationship Diagram (ERD) in AED system.	56
5.4	Relationship between table tblLeaveForm and tblStaffProfile	57
5.5	Relationship between table tblRHBookForm and tblStaffProfile	58
5.6	Relationship between table tblVehicleForm and tblStaffProfile	59
5.7	Context Diagram of AED system	60
5.8	DFD Level 1- AED System	61
5.9	DFD Level 2- Process Login	62
5.10	DFD Level 2- Process Send Forms	64
5.11	DFD Level 2- Process Reply Form Status	67
5.12	DFD Level 2- Process Public Key Checking	68
5.13	Process Maintain User Profiles	69
6.1	Overview of software development environment	73



## LIST OF ABBREVIATION

<b>Abbreviation</b>	<b>Definition</b>
AED	Authenticated Electronic Documents using Digital Signature
DES	Data Encryption Standard
DFD	Data Flow Diagram
DSA	Digital Signature Algorithm
ERD	Entity Relationship Diagram
E-SIGN	Electronic Signatures in Global and National Commerce
FTMK	Fakulti Teknologi Maklumat dan Komunikasi
GUI	Graphical User Interface
HTTP	Hyper Text Transport Protocol
ICT	Information and Communication Technology
IDEA	International Data Encryption Algorithm
ISO	International Organization for Standardization
IT	Information Technology
KUTKM	Kolej Universiti Teknikal Kebangsaan Malaysia
LAN	Local Area Network
MD4	Message Digest Algorithm version 4
MD5	Message Digest Algorithm version 5
NIST	National Institute of Standard and Technology
OSI	Open System Interconnect
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PSM	<i>Projek Sarjana Muda</i> (Project of Bachelor Degree)
RSA	Rivest, Shamir and Adleman
S/MIME	Secure/ Multipurpose Internet Mail Extension
SHA-1	Secure Hash Algorithm
SHS	Secure Hash Standard
SMTP	Simple Mail Transport Protocol
SQL	Structure Query Language
UML	Unified Modeling Language
VB	Visual Basic
WBS	Work Breakdown Structure

**LIST OF APPENDIX**

<b>Appendix</b>	<b>Title</b>	<b>Page</b>
A	Tables	100
B	Gantt Chart	107
C	FTMK Organization Chart	109
D	User interface Design	111
E	Interview Content	130
F	Testing	134
G	User Manual	146



## CHAPTER I

### INTRODUCTION

#### 1.1 Introduction

As global networks expand the interconnection of the world, the smooth operation of communication and computing systems becomes vital. However, recurring events such as criminal and worm attacks illustrate the weaknesses in current information technologies and the need for heightened security of this system. Increasingly, people need a way to ensure that the transmission process of information are kept confidential and is not altered in transit (message integrity). Certificates and associated keys can be used to encrypt and digitally sign messages.

The “Authenticated Electronic Documents using Digital Signature (AED)” system is an integrated application that developed to transmitting electronic documents electronically in a secure method within a sender (applicant) and receiver (approver) using digital signature infrastructure. An authentication service makes sure that a communication is authentic and the message is from the source that it claims to be from. The main purpose of the project is to enforce the security method from the moment the application form leaves the sender until it arrives at the receiver. It also resolves the problems or errors that appear in the manual form transmitting system.

## 1.2 Problem Statements

FTMK (Faculty Information and Communication Technology) staffs are required to fill in the forms which deal with certain tasks such as applying for a leave, hall booking or applying for transport services. After filling the form, the staffs will hand in the form to the Administration Officer. Then, the Administration Officer will make a consideration about the application based on the reason that is related before making a decision whether to approve or reject the application. The staff has to wait until the leave application is approved or vice versa. There are a lot of problems in the existing form transmitting system which need to be resolved and ameliorated. The problem is as follows:

### a) **Unprotected form transmitting process**

Existing systems implemented in an unprotected method, it is possible that the message contents have been modified during transmission either accidentally or deliberately by a third party. There is no guarantee that the form has come from the person whose name is on the form.

### b) **Time consuming**

Current systems operated in a non-convenient way and take an extended time in handling a simple task. It is a very complicated process where the staffs need to manually perform the tasks such as filling and sending the form. Applicants need to remain checking and verifying for the status of the form's application. Time is wasted during the time of obtaining forms, filling forms and waiting for the consequence of approval. Lecturers, tutors and other staffs are busy with their tasks; it is not a practical method to spend an amount of time to apply the form.

c) **Disorganized form system**

System is not systematic and methodical enough. There are various type of form in Faculty and is arranged in an unformatted method where staffs need to stumble on searching their form from the rack and sometime they need to reprint the form if the form is out of stock. In addition, tedious manual input system is easy prompt for errors.

d) **Paper-based process**

Another issue is that the current mainly paper-based process is not suitable for an immediate digital storage. Amount of paper wasted by using the manual form transmitting system. It is a large expenditure on the paper raw material, furthermore, it is not a good recycle consciousness too in material handing system.

### **1.3 Goal of Project**

The goal of this project is to develop a secure integrated application in form transmission between staff members and administration officer using digital signature infrastructure. The application provides the ability to determine the identity of a party to an interaction and to ensure that a form came from who it claims to have come from using a public key infrastructure.

### **1.4 Objective**

The objective of “Authenticated Electronic Document Using Digital Signature (AED)” system is to develop an integrated application for the staff from Faculty of Information and Communication Technology (FTMK) in handing form



transmission. Staffs should be able to access the form from the application, fill up the form application specified and then send it to the administration officer. The objectives of the system are as below:

- a) To present a secure method of transmitting information electronically - providing data authentication and integrity that ensures the connection is not interfered with a third party during the data transmission.
- b) To offer a public key infrastructure environment where user know who sent the message, the message content has not been altered in any way between sending and receiving and finally only the person the message is directed to can open it.
- c) To provide a variety of application forms to staffs in a single user interface which will make the form appliance process more easily and effectively. User can access the form with only one single click. All the form is arranged in an order form.
- d) To reduce the time spend in handing the form appliance process in which all process will be implementing through network in a secure and safety background.
- e) To eliminate tedious manual input process that prompts for error. User sometime might be input the data and information wrongly, and the more serious events occurs if they key in some important info such as employee ID. A variety of window controls like drop down menu and combo box will minimize the inaccuracy.
- f) To reduce the superabundance waste in paper material for a good recycles consciousness in material handing method.

## 1.5 Scopes

The set tasks of this system is to deliver a system to fulfill general requirements in submit and receive form electronically in a prescribed format where the form should be authenticated and the receiver should have assurance that the files were submitted by the specified person. System will focus on submission process only in entire form transmission system. The submission process including the process of form filling, form submission and form approval. Three type of forms included only in system, there are room/hall booking form, leave apply form and transport service apply form.

In key pair management method, a database will develop to store the public keys for all staffs in faculty while the private key will kept by the staffs. The project is not concern on the database security management's policy and private key management tasks, staffs need to keep the private key in a secure method. Besides, the project will focus on security services in authentication area only and not cover up the confidentiality services of data.

The users of this application are consisting of the staffs in Faculty of Information and Communication and Technology (FTMK) from KUTKM. User can access all the available form, fill in the form and send the form. Each user has one employee ID and password to log in the application. User is able to view their own status of application whether it is approved or not. This system is build for FTMK staff at this beginning phase, so the system will store information of FTMK staffs only.

## 1.6 Significances

Security threats in fabrication which represent when an unauthorized party inserts counterfeit objects into the system can be eliminated through the system. There are various hacking tools available that can quite easily intercept online messages, who's content, unless encrypted, will be fully available to the attacker.

There are a lot of tools that let people send "spoofed" messages. These are messages that appear to have come from someone that user know, when in reality they were sent by the attacker trying to social engineer his way into the system. If all conversations with the people that user know and trust are digitally signed, user will easily identify that the message did not come from a true people.

It is more efficient and makes the process of application become easier because once the staff apply, it will send the form directly to administration officer. After that, the form will be sent to the staff and the staff can know the status of the application whether is approved or not. The staff does not do anything such as ask administration to know the status of application but just wait until he receives the status of application.

Staffs can apply for leave no matter anywhere as long as they have computer and have connected their computer to Intranet. Staff doesn't need to go to faculty to take application form. Staff can apply for leave directly from home or work place. Besides that, form application is used in a paperless environment. It means we do not need to use any paper for application. It will reduce the usage of papers.

The interface design of the system is in a systematic and attractive view. It has various windows control such as combo box or drop-down menu, tedious manual input which prompts for error will be minimized.



## 1.7 Proposed solution

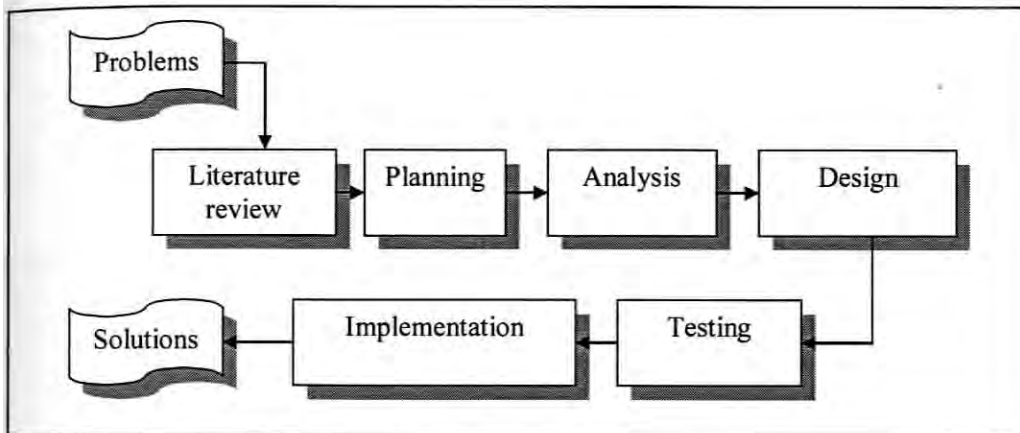
In order to fulfill the objective of project that mention before, a proposed solution planned to meets user requirement and adapt to the environment use of the users. The proposed solutions are as following:

Every staff in Faculty Information and Communication Technology are given one user ID and password to log in to the system. After that, the staffs are able to select a list of form and fill it in. A private key are required to digitally sign the form, the system will then generate a “signature” from the content of form application. All data will then store in a Microsoft SQL server database.

Administrative officer will log in to the system and check for the database for approve. Different table will list out different form application that staff applies to. Administrative officer need to insert the specified staff's public key to verify the signature. A status (approve or reject) will be given to the form, the administrative officer will “sign ” the form again using private key before sending the form to database. Staffs will check for the form's status after administrative officer send the status. Public key needed to verify the authenticity of form status.

## 1.8 Organization of project report

The method that is going to follow in order to systematically approach the problem resembles the main stages of a standard development process. (Figure 1.1)



**Figure 1.1: Organization of project report**

Researcher will make acquainted with the basic concepts and technologies used in the project in literature review (Chapter 2). Then it will progress to the planning phase (Chapter 3). In the planning phase, researcher will understand *why* the system should be built and determining *how* to build it. The analysis phase (Chapter 4) will aim at answers the questions of *who* will use the system, *what* the system will do, and *where* and *when* it will be used. In the design phase (Chapter 5); researcher will decide *how* the system will operate, in term of the user interface, forms, databases that will be needed. The following phase, implementation phase (Chapter 6) phase focus on the construction and implementation process to deliver the final system into operation. After that, testing process (Chapter 7) determine whether the system matches its specification and executes in its intended environment. Finally, observation, propositions for improvement and conclusion will be made towards the project.

## **CHAPTER II**

### **LITERATURE REVIEW**

#### **Introduction**

Literature Review in Chapter II provide the examples, case studies and other relevant work that has been done in the past, it gives the chance to investigate areas that user may not have thought about before, and to read around the subject. The literature review focuses on the various theory and basic network knowledge used in the “Authenticated Electronic Document using Digital Signature”(AED) project.

A key issue of authentication is described in section 2.2.1.1. In section 2.2.1.2-2.2.1.5 of the literature review will show that this objective can be achieved using cryptographic techniques. The section 2.2.1.6-2.2.1.9 will deal with further technique prerequisites that need to know about in order to understand later design solution. Finally, section 2.2.2 will focus on research on existing case that similar to the project.

#### **2.2 Fact and finding**

There are a lot of technique used to collect information that related to the project such as project problem, opportunities, solution requirements and priorities. These initial



documents will provide direction for the modeling techniques to analyze the requirements to determine what the correct requirements for the project are.

## **2.2.1 Theory and Concept**

In order to fully understand the process role and algorithm applied in the thesis, the following basic concepts and theory are required be identified to enable an effective and practical system development process:

### **2.2.1.1 Authentication**

Authentication services are concerned with ensuring that a communication is authentic. In the case of single message, such as a warning or alarm signal, the function of the authentication services is to assure the recipient that the documents or form is from the source that it claims to be from.

“All authentication schemes are based on the possession of some secret information known only to the user and possibly (but not necessarily) to the authentication system itself.” (Borman, 1993). Interactions with other parties use this secret in a way that allows the recipient to verify that the user possesses the secret, but that does not divulge the secret itself. This means that the secret itself cannot be shared, since to do so would allow the recipient to impersonate the user on subsequent interactions with other parties.

Using ISO terminology, it is a distinction between peer entity authentication and data origin authentication services (David Well, 1989). The first shall confirm the identities of one or more of the entities connected to one or more of the other entities. Peer entity authentication is used when establishing a data transfer or at the time of the