

Universiti Teknologi MARA

**The Usability of Online Certificate
Injection System (OCIS) at
Digicert Sdn.Bhd**

Wan Razinah Wan Zakaria

Thesis submitted in fulfilment of the requirements for
Bachelor of Science (Hons) Business Computing
Faculty of Information Technology and
Quantitative Science

November 2006

DECLARATION

I certify that this thesis and the research to which it refers are the product of my own work and that any ideas or quotation from the work of other people, published or otherwise are fully acknowledged in accordance with the standard referring practices of the discipline

NOVEMBER 30,2006

WAN RAZINAH WAN ZAKARIA

2004658965

TABLE OF CONTENTS

CONTENT	PAGE
ACKNOWLEDGEMENT	i
TABLE OF CONTENTS	ii
LIST OF TABLES	iii
LIST OF FIGURES	iv
LIST OF ABBREVIATIONS	v
ABSTRACT	vi

CHAPTER ONE: INTRODUCTION

1.0	Introduction	1
1.1	Project background	1
1.2	Problem Statement	5
1.3	Research Questions	5
1.4	Objectives	5
1.5	Scope	5
1.6	Significances	6

CHAPTER TWO: LITERATURE REVIEW/THEORY

2.0	Introduction	7
2.1	Organization background	7

2.2	Public Key Infrastructure (PKI) and Digital Certificates	15
2.3	Utilization of PKI in the government sector	33
2.4	System Acceptance	36

CHAPTER THREE: RESEARCH METHODOLOGY

3.0	Introduction	44
3.1	Research Model	44
3.2	Research Methodology	48
3.3	Definition Process	49
3.4	Gathering and analyzing process	49
3.5	Presentation process	50
3.6	Sampling	50

CHAPTER FOUR: RESULT AND FINDINGS

4.0	Introduction	53
4.1	Survey return rate	53
4.2	Usability	54
4.3	Usefulness and ease of use	67
4.4	Heuristics	70
4.5	Satisfaction	73
4.6	Summarize result	75
4.7	Research Hypotheses	76

ABSTRACT

Identity is our most valuable commodity on the Internet or online transaction. It defines who we are and is essential in doing business and carrying personal information over the net. Unfortunately on the Internet, identity can be ambiguous. The online users can now protect themselves with the use of Digital Certificate which is using a cryptographic system. A cryptographic system that uses two keys- a public key is known to everyone and private or secret key only known to the recipient of the message. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key. OCIS was developed to request the certificate from CCM server and then inject the certificate into the smart card. The smart card contains two certificate, Digital Signature certificate and Non repudiation certificate and can be used to make a secured online transaction. There is a need to understand the users' perspective and their acceptance of OCIS System. Technology acceptance model (TAM) was used as a theoretical basis to understand individual acceptance of users. In this study, five individual and system components are used to explore individual user acceptance of an OCIS system. Antecedents such as search function, screen design, navigation and system reliability have significant effects on perceived ease-of-use and perceived usefulness which in turn have a significant effect on individual user acceptance.