

**ONLINE CERTIFICATE INJECTION SYSTEM (OCIS)**

**MOHD NOR HAIZAM BIN SAMSUN BAHARUN**

**UNIVERSITI TEKNOLOGI MALAYSIA**



## UNIVERSITI TEKNOLOGI MALAYSIA

### BORANG PENGESAHAN STATUS TESIS<sup>♦</sup>

JUDUL : ONLINE CERTIFICATE INJECTION SYSTEM (OCIS)

SESI PENGAJIAN: 2005/2006

Saya MOHD NOR HAIZAM BIN SAMSUN BAHARUN  
(HURUF BESAR)

mengaku membenarkan tesis (~~PSM/Sarjana/Doktor Falsafah~~)\* ini di simpan di Perpustakaan Universiti Teknologi Malaysia dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hak milik Universiti Teknologi Malaysia.
2. Perpustakaan Universiti Teknologi Malaysia dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. \*\*Sila tandakan ( ✓ )

SULIT

(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

TERHAD

(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

TIDAK TERHAD



(TANDATANGAN PENULIS)

Disahkan oleh



(TANDATANGAN PENYELIA)

Alamat Tetap:  
NO 23 JALAN CEMPAKA,  
KAMPUNG SRI MAKMUR,  
26030 KUANTAN.

MR MOHD OTHMAN BIN YUSOP  
(Nama Penyelia)


Tarikh: 14 OKTOBER 2005


Tarikh: 14 OKTOBER 2005

♦ Tesis dimaksudkan sebagai tesis bagi Ijazah Doktor Falsafah dan Sarjana secara penyelidikan, atau disertasi bagi pengajian secara kerja kursus dan penyelidikan, atau Laporan Projek Sarjana (PSM).

## SUPERVISOR DECLARATION

“I/~~We~~ hereby declare that I/~~We~~ have read this thesis and in my/our opinion this thesis is sufficient in terms of scope and quality for the award of the degree of Masters of Science (Computer Science – Real Time System Software Engineering)”

Signature :   
Academic Supervisor : MR. OTHMAN BIN YUSOP  
Date : 14<sup>TH</sup> OCTOBER 2005

Signature :   
Academic Supervisor : MR. LESTER SOO NGAI KWONG  
Date : 14<sup>TH</sup> OCTOBER 2005

ONLINE CERTIFICATE INJECTION SYSTEM

MOHD NOR HAIZAM BIN SAMSUN BAHARUN

A dissertation submitted in partial fulfillment  
of the requirements for the award of the degree of  
Master of Science (Computer Science - Real Time Software Engineering)

Centre for Advanced Software Engineering  
Universiti Teknologi Malaysia

OCTOBER, 2005

## DECLARATION

I declare that this dissertation entitled “Online Certificate Injection System (OCIS)” is the result of my own research except as cited in the references. The dissertation has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature

:



Name

:

MOHD NOR HAIZAM BIN SAMSUN BAHARUN

Date

:

14<sup>TH</sup> OCTOBER 2005

*To my father, Samsun Baharun and my mother, Norihan  
Thanks for being wonderful parents.*

*To my beloved fiancé, Sophia and my family  
Thanks for your fully support.*

## ACKNOWLEDGEMENT

Praise to Allah the Almighty; for His will that I manage to complete this technical report. The accomplishment of this technical report numerously depend on the assistance of the people below for them have given me their precious advice and help.

First of all, I thankfully acknowledge the contribution of my Academic Mentor En Othman Bin Yusop for his supervision, teaching and time as well as to my industrial mentor Mr. Lester Soo Ngai Kwong for his endless support and supervision.

Secondly, I would like to express my gratitude to my fellow friends for their support and idea throughout the whole project.

Lastly, I extend my appreciation to my family for all they have done for me. Thank you very much.



## ABSTRACT

Identity is your most valuable commodity on the Internet or online transaction. It defines who you 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 a *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 .i.e. Digital Signature Certificate and Non-Repudiation Certificate and can be used to make a secured online transaction.

## ABSTRAK

Pengenalan diri adalah perkara yang sangat penting di dalam penggunaan Internet atau transaksi atas talian. Dengan pengenalan diri kita boleh membuktikan diri kita sebenar yang melakukan transaksi atau urusan. Namun begitu pengenalan diri di dalam penggunaan Internet adalah pelbagai. Pada masa ini para pengguna Internet boleh menggunakan Sijil Digital untuk melindungi diri mereka sendiri yang mana sijil tersebut menggunakan sistem kriptografi. Sistem Kriptografi menggunakan dua kekunci yang dipanggil kekunci umum (public key) yang diketahui umum dan kekunci persendirian (private key) yang hanya diketahui oleh penerima pesanan. Perkara penting kepada sistem kekunci umum (public key) ialah kekunci umum dan kekunci persendirian tersebut saling berkaitan dan hanya mesej yang di'encrypt'kan dengan menggunakan kekunci umum boleh di'decrypt'kan semula menggunakan kekunci persendirian. Tambahan pula untuk mengetahui kekunci persendirian dari kekunci umum adalah mustahil bagi manusia biasa kerana memerlukan pengiraan yang begitu rumit. Untuk merialisasikan tujuan ini, OCIS telah dibangunkan untuk membolehkan permintaan sijil baru dari server CCM dilakukan di atas talian kemudian memasukkan sijil tersebut ke dalam 'smart card'. 'Smart Card' tersebut mengandungi dua sijil iaitu 'Digital Certificate' dan 'Non-Repudiation Certificate' yang boleh digunakan untuk membuat transaksi atas talian dengan selamat.

## TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	<b>DECLARATION</b>	<b>ii</b>
	<b>ACKNOWLEDGEMENT</b>	<b>iv</b>
	<b>ABSTRACT</b>	<b>v</b>
	<b>ABSTRAK</b>	<b>vi</b>
	<b>TABLE OF CONTENTS</b>	<b>vii</b>
	<b>LIST OF TABLES</b>	<b>xi</b>
	<b>LIST OF FIGURES</b>	<b>xi</b>
	<b>LIST OF ACRONYMS</b>	<b>xii</b>
	<b>LIST OF APPENDICES</b>	<b>xiii</b>
<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
	1.0 Introduction	1
	1.1 Project Background	1
	1.2 Organization Background	5
	1.3 Project Objectives	6
	1.4 Project Scopes	6
	1.5 Project Deliverable	7
	1.6 Project Plan	7
<b>2</b>	<b>LITERATURE STUDY</b>	<b>8</b>
	2.0 Introduction	8
	2.1 Comparison between RUP and XP	8
	2.1.1 Rational Unified Process (RUP)	9
	2.1.1.1 RUP Characteristic	9
	2.1.1.2 RUP Phases – The Time Dimension	10

	2.1.1.3 RUP Workflows	13
	2.1.1.4 RUP Best Practices	15
	2.1.2 Extreme Programming	16
	2.1.2.1 XP Rules and Phases	18
	2.1.2.2 XP Best Practices	21
	2.1.3 The Advantages and Disadvantages RUP over XP and Vise Versa	24
	2.1.4 The Reasons Why Choose XP	26
2.2	Public Key Infrastructure (PKI) and Digital Certificates	26
	2.2.1 Cryptography and Encryption	27
	2.2.1.1 Symmetric Key Encryption (Secret Key)	28
	2.2.1.2 Asymmetric Key Encryption (Public Key)	28
	2.2.2 Introduction to PKI	30
	2.2.3 Utilization of PKI in the Government Sector	34
	2.2.3.1 Online Tax Submission	34
	2.2.3.2 Electronic Procurement (EP)	35
	2.2.3.3 Government Office Environment (GOE)	35
	2.2.3.4 Human Resources Management System (HRMS)	36
	2.2.3.5 Telemedicine	36
	2.2.3.6 Smart Schools	38
<b>3</b>	<b>PROJECT METHODOLOGY</b>	<b>39</b>
	3.0 Introduction	39
	3.1 Software Development Methodology	39
	3.2 Tools	41
	3.2.1 Visual Basic 6.0	42
	3.2.2 Microsoft SQL Server 2000	43
	3.2.3 ASP	44
<b>4</b>	<b>PROJECT DISCUSSION</b>	<b>45</b>
	4.0 Introduction	45
	4.1 Advantages and Disadvantages	45
	4.2 Deliverable	46
	4.3 Project Constraint and Solution	46

4.4	Recommendation	48
4.5	Personal Experience	48
<b>5</b>	<b>CONCLUSION</b>	<b>50</b>
	<b>REFERENCES</b>	<b>52</b>

**LIST OF TABLES**

<b>TABLE NO.</b>	<b>TITLE</b>	<b>PAGE</b>
2.1	RUP Main Characteristics	10
2.2	Brief Description of RUP Phases	12
2.3	The Focus of RUP Process Workflows	14
2.4	RUP Best Practices	15

**LIST OF FIGURES**

<b>FIGURE NO.</b>	<b>TITLE</b>	<b>PAGE</b>
2.1	OCIS Modules	5
2.2	Two Dimensional RUP Framework Architecture	11
2.3	XP Project's Phases	19
2.4	Example of Encryption	27
2.5	Public Key Message Encryption	30
2.6	Message Encryption with Digital Signature	32

**LIST OF ACRONYMS**

3-DES	Triple DES
CA	Certification Authority
CCM	Certificate Center Management
CDC	Commerce Dot Com
DES	Data Encryption Standard
EP	Electronic Procurement
GOE	Government Office Environment
HRMS	Human Resources Management System
IDEA	International Data Encryption Algorithm
KGS	Key Generation System
LCM-API	Local Certificate Management API
MSC	Multimedia Super Corridor
OCIS	Online Certificate Injection System
PKCS	Public Key Cryptographic Services
PKI	Public Key Infrastructure
PUK	PIN Unblocking Code
RC4	Rivest Cipher 4
SSL	Secure Socket Layer
STD	Software Test Document
STR	Software Test Result
XP	Extreme Programming



**LIST OF APPENDICES**

<b>APPENDIX</b>	<b>TITLE</b>
A	OCIS Gantt Chart
B	Software Test Report (STR)

## **CHAPTER 1**

### **INTRODUCTION**

#### **1.0 Introduction**

This chapter focuses on the introduction of the project. The first section describes on the project background while the organization background is elaborate in the second section. Third and fourth section outlines the writer's project objectives and the scope of the project. Following the section is the project deliverables and project plan which states the writer's task schedule that fit the project overall timeframe.

#### **1.1 Project Background**

Online Certificate Injection System (OCIS) is an online Registration Authority. This system was developed for Digicert Sdn Bhd's regular customer Commerce Dot Com. Commerce Dot Com will use this system for e-Perolehan application named ePShoppe for issuing smart card that contain two certificates i.e. Digital Signature Certificate and Non-Repudiation Certificate to a registered organization.

OCIS will simplify the issuance process by enable the issuance at customer site. This practice eliminated the old process that the issuances of the smart cards with certificate need to be done at Digicert Sdn Bhd site. The customer can issue

the smart card with certificates at their premise. The process of the issuance will take about less than five minutes.

OCIS is not stand alone system. This system actually depends on to another server application called LCM-API Server. This server act as a bridge between OCIS and the Certificate Authority Engine called Certificate Center Management Server (CCM Server). CCM Server is a certificates factory where all certificates request will be processed. OCIS will send the PKCS#10 with subject DN to the LCM-API Server and than the LCM-API Server will make a request with the given information to the CCM Server. CCM Server will process the request and generate a certificate with PKCS#7 format. The certificate then sent to the OCIS to inject to smart card. The process runs twice because it involves the request of two certificates.

Authenticity and integrity is an important aspect in this kind of transaction. The communication from customer to the web server is through SSL connection using 443 port which is required a valid certificate. Only authorized officer with a valid certificate can do the transaction.

OCIS is developed using tailored extreme programming which will be discussed in detailed at Chapter 2.

OCIS contain modules as diagramed in Figure 2.1. The breakdown structure of the modules is based on functionality. All the same color modules are within the OCIS system whereas the dark blue color is external entity to complete the system. The writer has the responsibility to complete all these modules within the timeline. OCIS consists of six (6) modules:

- (i) Login Module
- (ii) Signing Module
- (iii) Requesting Certificate Module
- (iv) Injecting Certificate Module

- (v) Administration Module
- (vi) LCM-API Server Module

The followings are the brief description for each module provided in OCIS system:

**(i) Login Module**

The Login Module has the capability to end user provide the valid certificate with correct token password. The system then checks with the database by comparing the certificate serial number and also checks the issuer of that certificate.

**(ii) Signing Module**

The Signing Module has the capability to get the information from the end user. That information named subject DN. Signing is the process of encryption the Subject DN using relevant private key of user certificate and then the encrypted Subject DN will be decrypted back using relevant public key of the same certificate. If the Subject DN can be decrypted, it means the certificate is valid with match private and public key.

**(iii) Requesting Certificate Module**

The Requesting Certificate Module has the capability to create PKCS#10 at client site. The successful generated PKCS#10 with Subject DN will be sent to the LCM-API Server for certificate request.

**(iv) Injecting Certificate Module**

The Injecting Certificate Module has the capability to get the certificate that was returned by LCM-API Server. Both certificates i.e. Digital Signature Certificate and Non-Repudiation Certificate which are in PKCS#7 formats then will be injected to the smart card.

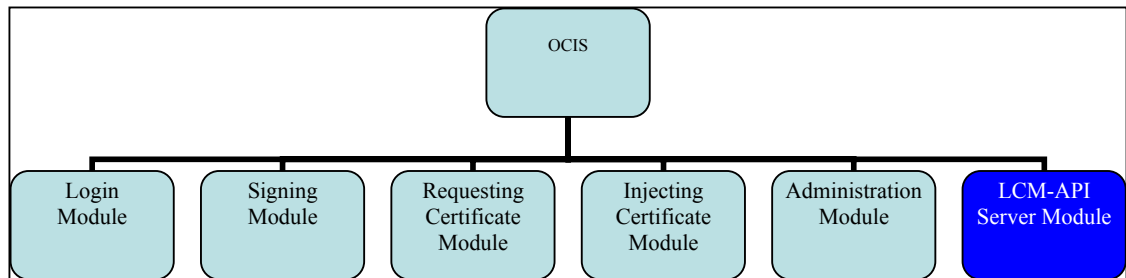
**(v) Administration Module**

The Administration Module has the capability to allow Digicert System Administrator to generate preset card serial number and PIN unblocking code (PUK) in the database. The serial number is preset by sequence number whereas the PUK is generated randomly.

**(vi) LCM-API Server Module**

The LCM-API Server Module has been developed to act as a server. This server will open the connection at port number 20248 to communicate with the web server. All the information like PKCS#10 and subject DN will be received using that port number then the information will be sent to CCM Server through port number 5055.

The number of modules is shown in figure 2.1 below.



**Figure 2.1: OCIS Modules**

## 1.2 Organization Background

Digicert Sdn Bhd is a company offering trusted certifications services for the Internet to enable trusted commerce and communication.

The company is the first certification authority in Malaysia offering digital certificate for secure web server, browser and e-mail packages with a range of assurance level.

The scope of the company's usefulness extends equally appropriate into the public as well as the private sectors in the domestic and international markets.

Digicert Sdn Bhd is determined to carry out its functions as a trusted third party in the most efficient and secure manner. Certificate issuance, maintenance, and revocation will be done by our highly trained staffs.

With strong group of technical specialists coupled with a competent management team, we are determined to provide a solution for your security worries.

Digicert Sdn Bhd uses a Public Key Infrastructure (PKI) solution that meets the requirements of the Malaysian Digital Signature Act 1997. The PKI solution will use public key digital technology to ensure authenticity and integrity of information in electronic transaction, and to enforce non-repudiation in personal and private sector.

### **1.3 Project Objectives**

The main objective of this project is to provide the availability of online certificate issuance. Hence, the project aims to fulfill the following objectives:

- (i) To make the process of issuance and injection of the digital certificate into the smart card can be made at customer's side by secure online transaction.
- (ii) To increased services and capability to Registration Authority as well as making the system administrators tasks more efficient.

### **1.4 Project Scopes**

The scopes of the OCIS pertaining to the objectives which are listed in Section 1.3 are limited to:

- (i) Study the principles of PKI and the usage of digital certificates.
- (ii) Study the business flow of OCIS base on CDC requirement.
- (iii) Developing the Online Certificate Injection module.
- (iv) Writing the Software Test Document (STD) for OCIS module.

## **1.5 Project Deliverable**

Software Test Document (STD) for this system will be produced after the completion of development. The writer will follow the company standard to produce the document.

## **1.6 Project Plan**

This project was completed within the time line specified. The development started from 17th of February 2005 until 13th of July 2005. The Gant Chart for this project provided at Appendix A.



## REFERENCES

- Abraham, P., Salo, O., Ronkainen, J., and Warsta, J. (2002). *Agile Software Development Methods – Review and Analysis*. Finland: VTT Publications 478.
- Andersen, N. E., Kensing, F., Lundin, J., Mathiassen, L., Munk-Madsen, A., Rasbech, M., and Sorgaard, P. (1990). *Professional Systems Development: Experience, Ideas and Action*. United Kingdom: Prentice Hall.
- Bennett, S., Farmer, R., and McRobb, S. (2002). *Object-Oriented System Analysis and Design Using UML*. 2<sup>nd</sup> edition. United Kingdom: McGraw Hill.
- Boogs, M., and Boggs, W. (2002). *Mastering UML with Rational Rose 2002*. United State: Sybex.
- Booch, G., Martin, R.C., and Newkirk, J. (1998). *Object Oriented Analysis and Design with Applications*. 2<sup>nd</sup> edition. Addison Wesley, Longman Inc.
- Booch, G., Jacobson, I., and Rumbaugh, J. (1999). *The Unified Modeling Language User Guide*. India: Pearson Education Asia.
- Dijkstra, D. H. (1972) *Structured Programming*. Academic Press.
- Ferraby, L. (1990). *Change Control During Computer System Development*. United Kingdom: Prentice Hall.
- Fowler, M., and Scott, K. (1997). *UML Distilled: Applying The Standard Object Modeling Language*. Canada: Addison Wesley Longman Inc.
- Hagelstein, J., Macdonald, I. G., Olle, T. W., Rolland, C., Sol, H. G., Van Assche, F. J.M., and Verrijn-Stuart, A. A. (1991). *Information System Methodologies: A Framework for Understanding*. 2<sup>nd</sup> edition. Singapore: Addison Wesley.
- Kotonya, G., and Sommerville, I. (1998). *Requirements Engineering: Process and Techniques*. England: Wiley.
- Icarus. (2002a). The Art of Software Development (part 1): Understanding Need. *Melonfire*: Article.
- Icarus. (2002b). The Art of Software Development (part 4): Delivering Quality. *Melonfire*: Article.

- Martin, C. F. (1988). *User-Centered Requirements Analysis*. United State: Prentice Hall.
- Riehle, D. (2000). A Comparison of the Value Systems of Adaptive Software Development and Extreme Programming: How Methodologies May Learn from Each Other. *SKYVA International*: Article.
- Rational Software, (2001). *Rational Unified Process Fundamentals*. Cupertino, USA: Rational University : Student Manual Version 2002.05.00.
- RJW Consulting (1999). Software Engineering Process. Available at <http://www.rjw-consulting.com>
- Rothi, J., and Yen, D. (1989). *System Analysis and Design in End User Developed Applications*. Journal of Information Systems Education.
- Steward, D. V. (1987). *Software Engineering with Systems Analysis and Design*. Brooks/Cole Publishing. California: Monterey.
- Vaswani, V. (2002a). The Art of Software Development (part 2): Designing for Simplicity. *Melonfire*: Article.
- Vaswani, V. (2002b). The Art of Software Development (part 3): Coding to a Plan. *Melonfire*: Article.
- Vaswani, V. (2002c). The Art of Software Development (part 5): Adding Value. *Melonfire*: Article.