

การวิเคราะห์และออกแบบการบริการและการจัดการโครงสร้างพื้นฐานระบบกฎหมายสาธารณะ  
สำหรับหน่วยงานราชการขนาดใหญ่

นายสมคิด ลัฐิถาวณิชย์



วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2545

ISBN 974-17-1524-2

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

ANALYSIS AND DESIGN OF SERVICE AND MANAGEMENT OF PUBLIC KEY INFRASTRUCTURE  
FOR LARGE GOVERNMENT AGENCIES

Mr.Somkid Latthithawanich

A Thesis Submitted in Partial Fulfillment of the Requirements  
for the Degree of Master of Science in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2002

ISBN 974-17-1524-2


หัวข้อวิทยานิพนธ์      การวิเคราะห์และออกแบบการบริการและการจัดการโครงสร้างพื้นฐาน  
ระบบกฎแฉสารสนเทศสำหรับหน่วยงานราชการขนาดใหญ่  
โดย                              นายสมคิด ลัฐิถาวณิชย์  
สาขาวิชา                      วิทยาศาสตร์คอมพิวเตอร์  
อาจารย์ที่ปรึกษา              อาจารย์ ดร.ยรรยง เต็งอำนาจ

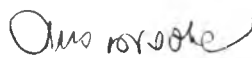
---

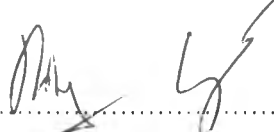
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้หัวข้อวิทยานิพนธ์ฉบับนี้  
เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต


  
..... คณบดีคณะวิศวกรรมศาสตร์  
(ศาสตราจารย์ ดร.สมศักดิ์ ปัญญาแก้ว)

คณะกรรมการสอบวิทยานิพนธ์

  
..... ประธานกรรมการสอบ  
(อาจารย์ จารุมาต ปันทอง)

  
..... อาจารย์ที่ปรึกษา  
(อาจารย์ ดร.ยรรยง เต็งอำนาจ)

  
..... กรรมการ  
(อาจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์)

  
..... กรรมการ  
(ดร.พีระพงศ์ ศิริเกษม)

สมคิด ลัฐิถาวณิษฐ์ : การวิเคราะห์และออกแบบการบริการและการจัดการโครงสร้างพื้นฐานระบบกุญแจสาธารณะสำหรับหน่วยงานราชการขนาดใหญ่. (ANALYSIS AND DESIGN OF SERVICE AND MANAGEMENT OF PUBLIC KEY INFRASTRUCTURE FOR LARGE GOVERNMENT AGENCIES). อ.ที่ปรึกษา : อ.ดร.ยรรยง เต็งอำนวย 60 หน้า. ISBN 974-17-1524-2.

ระบบรักษาความมั่นคงปลอดภัยโดยอาศัยเทคโนโลยีการเข้ารหัสแบบกุญแจสาธารณะ ทำให้การดำเนินงานบนระบบเครือข่ายเปิดอย่างระบบเครือข่ายอินเทอร์เน็ตเป็นสิ่งที่ทำได้สะดวกกว่าในอดีตมาก อย่างไรก็ตามการก่อสร้างระบบรักษาความมั่นคงปลอดภัยที่ดีต้องอาศัยปัจจัยหลายด้าน ทั้งด้านเทคโนโลยี นโยบายขององค์กร รวมถึงการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของสมาชิกภายในองค์กร

วิทยานิพนธ์ฉบับนี้กล่าวถึงการวิเคราะห์และออกแบบโครงสร้างพื้นฐานระบบกุญแจสาธารณะสำหรับหน่วยงานราชการขนาดใหญ่ โดยมุ่งเน้นการวิเคราะห์และออกแบบสถาปัตยกรรมโครงสร้างพื้นฐานระบบกุญแจสาธารณะ เพื่อจัดเป็นโครงสร้างพื้นฐานสำหรับองค์กร โดยมีกรุงเทพมหานครเป็นกรณีศึกษา รวมถึงการชี้แนะแนวทางด้านนโยบายและด้านการบริหารจัดการ และแผนงานการจัดสร้างโครงสร้างพื้นฐานระบบกุญแจสาธารณะของกรุงเทพมหานคร ทั้งนี้ขอบเขตของวิทยานิพนธ์ไม่ครอบคลุมการนำโครงสร้างพื้นฐานระบบกุญแจสาธารณะไปใช้ในโปรแกรมระบบงาน เพียงยกตัวอย่างเพื่อประกอบคำอธิบายให้เข้าใจในหลักการเท่านั้น

ภาควิชาวิศวกรรมคอมพิวเตอร์  
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์  
ปีการศึกษา 2545

ลายมือชื่อผู้คิด..... สมคิด ลัฐิถาวณิษฐ์  
ลายมือชื่ออาจารย์ที่ปรึกษา..... On route  
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม.....



# # 4271484021 : MAJOR COMPUTER SCIENCE

KEY WORD: SECURITY / PUBLIC KEY INFRASTRUCTURE / PKI / PUBLIC KEY CERTIFICATE /  
ELECTRONIC SIGNATURE / BANGKOK METROPOLITAN ADMINISTRATION / BMA  
SOMKID LATTHITHAWANICH : ANALYSIS AND DESIGN OF SERVICE AND  
MANAGEMENT OF PUBLIC KEY INFRASTRUCTURE FOR LARGE GOVERNMENT  
AGENCIES. THESIS ADVISOR : DR.YUNYONG TENG-AMNUAY. 60 pp.  
ISBN 974-17-1524-2.

The emerging technology of public key encryption makes the security on open network, such as the Internet, much easier than in the past. However, strengthening security system needs various factors such as technology, organization policy, as well as the cooperation of members in the organization.

This thesis focuses on analysis and design of service and management of public key infrastructure as a basic infrastructure for large government agencies, using Bangkok Metropolitan Administration (BMA) as a case study. The thesis discusses about analysis and design of public key infrastructure, and also recommends policies, management and administration, and planning for building BMA's public key infrastructure. However, the study does not include deployment of public key infrastructure with other applications.

Department of Computer Engineering  
Field of study Computer Science  
Academic year 2002

Student's signature.....  
Advisor's signature.....  
Co-advisor's signature.....



## กิตติกรรมประกาศ

ในการจัดทำวิทยานิพนธ์นี้ ข้าพเจ้าใคร่ขอกราบขอบพระคุณท่านอาจารย์ ดร.ยรรยง เต็งอำนวยการ อาจารย์ที่ปรึกษา ซึ่งให้ความกรุณาชี้แนะแนวทางในการศึกษาค้นคว้า และเสียสละเวลาอ่านและแก้ไขบทวิทยานิพนธ์ให้ข้าพเจ้าจนเสร็จสมบูรณ์ และขอขอบพระคุณ ดร.พีระพงศ์ ศิริเกษม กองควบคุมระบบคอมพิวเตอร์ สำนักนโยบายและแผนกรุงเทพมหานคร ที่กรุณารับเป็นกรรมการในการสอบวิทยานิพนธ์ รวมถึงให้ข้อเสนอแนะซึ่งมีประโยชน์ในการศึกษา และวิเคราะห์เป็นอันมาก

สุดท้ายนี้ ข้าพเจ้าขอขอบพระคุณ ดร.ปรัชญา เปี่ยมสมบูรณ์ และเจ้าหน้าที่ของ บริษัท ซิม ซิสเต็ม (ประเทศไทย) จำกัด ทุกท่าน ที่ได้ช่วยเหลือด้านการหาข้อมูล จัดทำเอกสารและให้กำลังใจให้ข้าพเจ้าจัดทำวิทยานิพนธ์สำเร็จลุล่วงไปได้ด้วยดี หากวิทยานิพนธ์นี้มีข้อผิดพลาดหรือบกพร่องประการใด ข้าพเจ้าขอน้อมรับไว้แต่เพียงผู้เดียว

# สารบัญ

	หน้า
บทคัดย่อภาษาไทย .....	ง
บทคัดย่อภาษาอังกฤษ .....	จ
กิตติกรรมประกาศ.....	ฉ
สารบัญ .....	ช
สารบัญภาพ .....	ญ
สารบัญตาราง.....	ฎ
บทที่	หน้า
1. บทนำ .....	1
1.1. วัตถุประสงค์ .....	2
1.2. ขอบเขตการวิจัย .....	2
1.3. ขั้นตอนการดำเนินการวิจัย .....	2
1.4. ประโยชน์ที่คาดว่าจะได้รับ .....	3
2. แนวคิดและทฤษฎีที่เกี่ยวข้อง .....	4
2.1. วิทยาการเข้ารหัสลับ (Cryptography) .....	4
2.1.1. การเข้ารหัสแบบกุญแจลับ (Secret Key Cryptography) .....	4
2.1.2. การเข้ารหัสแบบกุญแจสาธารณะ (Public Key Cryptography) .....	5
2.1.3. ฟังก์ชันแฮช (Hash Function) .....	6
2.1.4. ลายมือชื่อดิจิตอล (Digital Signature).....	7
2.2. โครงสร้างพื้นฐานระบบกุญแจสาธารณะ .....	7
2.2.1. องค์ประกอบของโครงสร้างพื้นฐานระบบกุญแจสาธารณะ.....	8
2.2.2. สถาปัตยกรรมของหน่วยออกใบรับรอง.....	9
3. การวิเคราะห์และออกแบบ .....	12
3.1. เกณฑ์การออกแบบ .....	12
3.2. การเลือกกรณีศึกษา .....	12
3.3. โครงสร้างการบริหารราชการ .....	13
3.3.1. โครงสร้างองค์กร.....	13
3.3.2. โครงสร้างหน่วยงานด้านเทคโนโลยีสารสนเทศ.....	15

## สารบัญ (ต่อ)

บทที่	หน้า
3.4. โครงสร้างระบบเครือข่ายของกรุงเทพมหานคร.....	19
3.5. สถาปัตยกรรมภายในกรุงเทพมหานคร.....	21
3.6. การจัดวางระบบเข้ากับโครงสร้างระบบเครือข่ายของกรุงเทพมหานคร .....	23
3.6.1. การจัดวางหน่วยออกใบรับรอง.....	23
3.6.2. การจัดวางหน่วยรับรองบุคคล.....	24
3.7. สถาปัตยกรรมเชื่อมโยงกับหน่วยงานภายนอก.....	26
4. นโยบายและการบริหารจัดการ .....	28
4.1. แนวทางนโยบายด้านโครงสร้างพื้นฐานระบบกฎหมายสาธารณะ.....	28
4.1.1. การจัดตั้งตำแหน่งผู้บริหารระดับสูงฝ่ายความมั่นคงด้านสารสนเทศ (CSO – Chief Security Officer).....	28
4.1.2. การจัดตั้งคณะกรรมการกำหนดนโยบายด้านความมั่นคงปลอดภัย.....	29
4.1.3. การจัดตั้งคณะกรรมการกำหนดนโยบายด้านใบรับรองกฎหมายสาธารณะ.....	29
4.2. แนวทางการบริหารจัดการ.....	29
4.2.1. การกำกับการพัฒนาระบบงานสารสนเทศ.....	29
4.2.2. การจัดการระบบโครงสร้างพื้นฐานระบบกฎหมายสาธารณะให้ครบวงจร.....	31
4.2.3. การบริหารให้เกิดความเชื่อมั่นใน CA.....	31
4.3. ตัวอย่างการประยุกต์ใช้คุณสมบัติของโครงสร้างพื้นฐานระบบกฎหมายสาธารณะใน โครงการของกรุงเทพมหานคร.....	32
4.4. ตัวอย่างโครงสร้างเนื้อหา Certificate Policy และ Certificate Practices Statement.....	35
5. แผนงานการจัดสร้าง.....	36
5.1. รายละเอียดโครงการ.....	36
5.1.1. โครงการจัดสร้างโครงสร้างพื้นฐาน.....	36
5.1.2. โครงการพัฒนานโยบายด้านความมั่นคงปลอดภัย.....	38
5.1.3. โครงการสนับสนุนงานพัฒนาระบบสารสนเทศ.....	40
5.2. สรุปแผนการจัดสร้าง.....	41



สารบัญ (ต่อ)

บทที่	หน้า
6. บทสรุป.....	43
6.1. สรุปผลการวิจัย.....	43
6.2. ข้อเสนอแนะ.....	43
รายการอ้างอิง.....	44
ภาคผนวก.....	46
ภาคผนวก ก.....	47
ภาคผนวก ข.....	51
ภาคผนวก ค.....	58
ประวัติผู้เขียนวิทยานิพนธ์.....	60

## สารบัญภาพ

ภาพประกอบ	หน้า
2.1 การเข้ารหัสและถอดรหัสแบบกุญแจลับ .....	4
2.2 การเข้ารหัสและถอดรหัสแบบกุญแจสาธารณะ .....	5
2.3 การลงลายมือชื่อและการทวนสอบ .....	6
2.4 ขั้นตอนการตรวจสอบลายมือชื่อดิจิตอล .....	7
2.5 โครงสร้างพื้นฐานระบบกุญแจสาธารณะ .....	8
2.6 สถาปัตยกรรมแบบหน่วยออกใบรับรองเดี่ยว .....	9
2.7 สถาปัตยกรรมแบบจัดลำดับชั้น .....	10
2.8 สถาปัตยกรรมแบบตาข่าย .....	11
2.9 สถาปัตยกรรมแบบ Bridge .....	11
3.1 ผังโครงสร้างองค์กร .....	14
3.2 ผังโครงสร้างหน่วยงานด้านเทคโนโลยีสารสนเทศ .....	16
3.3 Logical Diagram ของระบบเครือข่ายของกรุงเทพมหานคร .....	20
3.4 Logical Diagram ของระบบเครือข่ายของกรุงเทพมหานคร(Equipment Viewpoint) .....	20
3.5 โครงสร้างหน่วยออกใบรับรองของกรุงเทพมหานคร (BMA Logical CA Architecture) .....	22
3.6 ผังแสดงการวางระบบเข้ากับระบบเครือข่ายของกรุงเทพมหานคร .....	25
3.7 การปรับสถาปัตยกรรมเป็นส่วนหนึ่งของสถาปัตยกรรมแบบจัดลำดับชั้น ระดับประเทศ .....	26
3.8 การปรับสถาปัตยกรรมเป็นส่วนหนึ่งของสถาปัตยกรรมแบบ Bridge .....	27
4.1 องค์ประกอบของระบบสารสนเทศที่เป็น PKI-Enabled Application .....	30
4.2 เทคโนโลยี Air Gap .....	32

## สารบัญตาราง

ตาราง	หน้า
3.1	หน้าที่ความรับผิดชอบของหน่วยงานกลางด้านเทคโนโลยีสารสนเทศ ..... 17
4.1	ตัวอย่างการประยุกต์ใช้คุณสมบัติของโครงสร้างพื้นฐานระบบกฎหมายสาธารณะ ในโครงการของกรุงเทพมหานคร ..... 33
4.2	จำนวนโครงการ แบ่งตามประเภทของบริการชั้นพื้นฐาน ..... 33
4.3	ตัวอย่างระบบงานและรายละเอียดการประยุกต์ใช้งาน ..... 34
5.1	แผนการจัดสร้างโครงสร้างพื้นฐานระบบกฎหมายสาธารณะของกรุงเทพมหานคร โดยยึดตามแผนแม่บทเทคโนโลยีสารสนเทศของกรุงเทพมหานคร (พ.ศ.2544-2549) 42