

ขั้นตอนการปฏิบัติงานที่เชื่อถือได้เพื่อการได้มา และการใช้งานระยะเวลาของกฎแฉรหัสส่วนตัว



นายชนะ ปรีชามานิตกุล

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2548

ISBN 974-53-2651-8

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

23 ๒๕.๕. 2551

TRUSTWORTHY OPERATIONAL PROCEDURE FOR OBTAINING AND LONG-TERMED  
USING OF PRIVATE KEY

Mr. Chana Prechamanitkul

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

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2005

ISBN 974-53-2651-8

หัวข้อวิทยานิพนธ์

ขั้นตอนการปฏิบัติงานที่เชื่อถือได้เพื่อการได้มา และการใช้งานระยะยาวของกุญแจรหัสส่วนตัว

โดย

นายชนะ ปรีชามานิตกุล


สาขาวิชา

วิทยาศาสตร์คอมพิวเตอร์


อาจารย์ที่ปรึกษา


อาจารย์ ดร. ยรรยง เต็งอำนวยการ

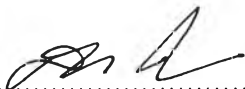
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้รับวิทยานิพนธ์ฉบับนี้  
เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาโทบัณฑิต

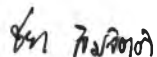
  
..... คณบดีคณะวิศวกรรมศาสตร์  
(ศาสตราจารย์ ดร. ดิเรก ลาวัณย์ศิริ)

คณะกรรมการสอบวิทยานิพนธ์

  
..... ประธานกรรมการ  
(อาจารย์ จารุมาต ปันทอง)

  
..... อาจารย์ที่ปรึกษา  
(อาจารย์ ดร. ยรรยง เต็งอำนวยการ)

  
..... กรรมการ  
(อาจารย์ รงชัย โรจน์กังสดาล)

  
..... กรรมการ  
(นาย ชยา ลิ้มจิตติ)

ชนะ ปริษามานิตกุล : ขั้นตอนการปฏิบัติงานที่เชื่อถือได้เพื่อการได้มา และการใช้งาน  
 ระยะเวลาของกุญแจรหัสส่วนตัว (TRUSTWORTHY OPERATIONAL PROCEDURE FOR  
 OBTAINING AND LONG-TERMED USING OF PRIVATE KEY) อ.ที่ปรึกษา : อ.ดร.ยรรยง  
 เต็งอำนาจ, 92 หน้า. ISBN 974-53-2651-8

กุญแจรหัสส่วนตัวของเทคโนโลยีกุญแจคู่สาธารณะเป็นวิธีการหนึ่งที่ได้รับการยอมรับว่ามีความปลอดภัยสูงในการนำไปใช้ในการรักษาความลับและกระบวนการของการพิสูจน์ตัวตน ในปัจจุบันมีการประยุกต์ใช้งานในรูปแบบของลายมืออิเล็กทรอนิกส์ เพื่อใช้ในการทำธุรกรรมทางอิเล็กทรอนิกส์ต่างๆ เปรียบเทียบเท่ากับลายมือชื่อหรือลายเซ็นโดยทั่วไป อันต้องมีผลบังคับทางด้านกฎหมายด้วย ดังนั้นขั้นตอนหรือกระบวนการในการได้มา การดูแลรักษา ของกุญแจรหัสส่วนตัวต้องมีความน่าเชื่อถือว่ามีความปลอดภัยเพียงพอในการนำไปใช้เนื่องจากผู้ใช้ต้องรับผิดชอบต่อการทำธุรกรรมที่มีมูลค่ามหาศาลนั้นๆ

งานวิจัยนี้มีจุดประสงค์หลักคือการสร้างแนวทางที่เป็นขั้นตอนในการปฏิบัติงานเพื่อความปลอดภัยในการได้มาและใช้งานของกุญแจรหัสส่วนตัวที่เชื่อถือได้ รวมถึงข้อควรระวังในการนำไปใช้งานตลอดจนการดูแลรักษากุญแจรหัสส่วนตัว การวิจัยใช้วิธีการศึกษาและอ้างอิงโดยเปรียบเทียบจากมาตรฐานด้านความปลอดภัยที่ยอมรับในระดับสากลซึ่งมีการนำไปใช้งานอย่างแพร่หลายเช่น ISO, COBIT, ITIL และ HIPAA และยังศึกษาถึงกระบวนการยอมรับของผู้บริหารเพื่อให้นำเสนอต่อผู้บริหารขององค์กรซึ่งในงานวิจัยนี้เลือกสภาพแวดล้อมจุฬาลงกรณ์มหาวิทยาลัยเป็นกรณีศึกษาถึงการนำกระบวนการดังกล่าวไปใช้งาน

ผลที่ได้จากการศึกษาพบว่าขั้นตอนต่างๆที่ครอบคลุมตั้งแต่ นโยบาย การเตรียมความพร้อมพื้นฐานต่างๆเพื่อความปลอดภัย และขั้นตอนการสร้างกุญแจรหัสนั้น สามารถทำได้โดยนำจุดเด่นของแต่ละมาตรฐานมาประยุกต์ใช้ พร้อมแจกแจงรายละเอียดการปฏิบัติงานซึ่งบางมาตรฐานไม่ได้กล่าวไว้มาสรุปเป็นขั้นตอนการปฏิบัติงาน โดยสามารถแยกเป็น 2 แนวทางด้วยกันคือ ขั้นตอนการปฏิบัติสำหรับเจ้าหน้าที่ผู้ปฏิบัติงานทั่วไป และสำหรับการใช้งานในระดับผู้บริหารเพื่อใช้ในงานด้านความปลอดภัยของหน่วยงานหรือองค์กรต่อไป

ภาควิชา...วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต..... ๑๕๖..... ปริษามานิตกุล  
 สาขาวิชา...วิทยาศาสตร์คอมพิวเตอร์..... ลายมือชื่ออาจารย์ที่ปรึกษา.....  
 ปีการศึกษา. 2548.....

# # 4671406521 : MAJOR COMPUTER SCIENCE

KEY WORD: LONG-TERMED KEY USAGE/TRUSTWORTHY/STEALING KEY/HUMAN  
FACTOR/PROTECTION KEY/DIGITAL SIGNATURE

CHANA PRECHAMANITKUL: TRUSTWORTHY OPERATIONAL PROCEDURE  
FOR OBTAINING AND LONG-TERMED USING OF PRIVATE KEY. THESIS  
ADVISOR: YUNYONG TENG-AMNUAY, Ph.D., 92 pp. ISBN 974-53-2651-8

Private key of Public key infrastructure is a well accepted mean of high security in upholding confidentiality and verifying personal authentication. Presently, the implementation of digital signature for worldwide electronic transactions is be coming comparable to general hand writing or personal signature and also must be authorized legally. As a result, the procedure of obtaining and maintaining a long-termed private key should be convincingly trustworthy to the user who has to be responsible to those valuable transactions.

This research has the main objective to provide a framework for creating the trustworthy and secure operational procedure for obtaining and using long-termed private keys. The research employs the method of analysis and reference in many presently well-known and worldwide recognized standards, such as ISO, COBIT, ITIL and HIPPPAA. It also presents the procedure for executive. Chulalongkorn University is the environment selected as case study.

The result of this study found that the whole process, covering policy, security infrastructure preparation, and the private key generation procedure, is trustworthy by applying the strength of each standard accompanied by the detail deliberation of the work instructions that few standards have not been proposed. The procedures are divided into two parts: one for general administrators and an other for managerial level to use in the security task within the division or organization.

Department... Computer Engineering..... Student's signature..... *Chana P*  
Field of study.. Computer Science..... Advisor's signature..... *Yu Yong Teng*  
Academic year.. 2005.....

## กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้ด้วยความกรุณาเป็นอย่างยิ่งของ อาจารย์ ดร. ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษา ที่เมตตาชี้แนะแนวทางในการแก้ปัญหาต่างๆ ตลอดระยะเวลาในการทำวิทยานิพนธ์ ท่านได้เสียสละเวลาอันมีค่าของท่านในการให้คำปรึกษาแม้ว่าจะนัดท่านในเวลานอกราชการ รวมทั้งกรุณาช่วยตรวจทาน แก้ไขเนื้อหาวิทยานิพนธ์ ผู้เขียนรู้สึกซาบซึ้งในความเมตตาของท่านเป็นอย่างยิ่ง จึงขอกราบขอบพระคุณอาจารย์ ดร.ยรรยง ไว้เป็นอย่างสูง ณ โอกาสนี้

ผู้เขียนขอกราบขอบพระคุณ อาจารย์ จารุมาตร ปิ่นทอง ที่เมตตารับเป็นประธานกรรมการสอบวิทยานิพนธ์ อาจารย์ ธงชัย โรจน์กั้งสตาล กรรมการสอบวิทยานิพนธ์ผู้เป็นอาจารย์ที่สอนวิชาด้านความปลอดภัยให้กับผู้เขียน อีกทั้งยังแนะนำความรู้และแนวคิดด้านต่างๆ ให้ผู้เขียนได้คบคิดอยู่เสมอ คุณชยา ลิมจิตติ ท่านได้กรุณาสละเวลา ซึ่งท่านมีภารกิจมากมายรับเป็นกรรมการสอบวิทยานิพนธ์ ผู้เขียนขอกราบขอบพระคุณอาจารย์ทุกๆ ท่านในสาขาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย ที่สอนวิชาต่างๆ ในหลักสูตรให้กับผู้เขียน นอกจากนี้ขอขอบคุณหทัย คุณเดี่ยว คุณลักษณะ คุณกอล์ฟ จุ่ม ตลอดจนเพื่อนๆ ร่วมรุ่นทุกคน ที่ได้ร่วมทุกข์ร่วมสุข และโดยเฉพาะอย่างยิ่ง คุณไกรสิทธิ์ อัญชนานนท์ ซึ่งเป็นผู้ที่ให้กำลังใจคำแนะนำ คอยกระตุ้นเตือนให้กำลังใจอยู่เสมอ

ผู้เขียนขอกราบขอบพระคุณ คุณขวัญตา คุณขวัญจิตร และคุณขวัญภา บริษามานิตกุล ที่เป็นพี่และน้องที่แสนดียิ่งเป็นผู้ที่ได้มอบความรักความเสียสละ และมอบโอกาสทางการศึกษาแก่ผู้เขียนมาตลอดชีวิต ขอขอบคุณ คุณเฉลิมพร สิริวิชัย ที่เป็นกำลังใจทำให้ผู้เขียนได้สอบเข้ามาศึกษาจนจบ และอยู่เคียงข้างช่วยเหลือจนกระทั่ง วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี และขอกราบขอบพระคุณ คุณ สุมาลัย ศรีกำไลทอง ที่เมตตาอนุญาติให้ผู้เขียนสามารถลางานบางส่วนเพื่อการศึกษาได้

ท้ายนี้ หากวิทยานิพนธ์ฉบับนี้มีคุณค่าและประโยชน์ประการใดแล้ว ผู้เขียนขอกราบเป็นกตเวทิตาคุณแก่บิดามารดา คณาจารย์ และผู้มีพระคุณทุกท่านของผู้เขียน แต่หากวิทยานิพนธ์ฉบับนี้มีความบกพร่องประการใดก็แล้วแต่ ผู้เขียนขอน้อมรับไว้เพียงผู้เดียว

# สารบัญ

	หน้า
บทคัดย่อภาษาไทย .....	ง
บทคัดย่อภาษาอังกฤษ .....	จ
กิตติกรรมประกาศ .....	ฉ
สารบัญ .....	ช
บทที่	
1 บทนำ .....	1
1.1 ความเป็นมาและความสำคัญของปัญหา .....	1
1.2 วัตถุประสงค์ของการวิจัย .....	3
1.3 ขอบเขตของการวิจัย .....	3
1.4 ขั้นตอนการวิจัย .....	3
1.5 ประโยชน์ที่คาดว่าจะได้รับ .....	4
1.6 โครงสร้างวิทยานิพนธ์.....	4
2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง .....	5
2.1 บทนำ.....	6
2.2 งานวิจัยที่เกี่ยวข้อง .....	6
2.2.1 มาตรฐานความปลอดภัย.....	6
2.2.2 งานวิจัยลายมือชื่อและใบรับรอง.....	8
2.2.3 การพิสูจน์ตัวตน.....	29
2.2.4 รูปแบบการรับรองระหว่างหน่วยงาน .....	15
2.3 ทฤษฎีการยอมรับและกระบวนการยอมรับ.....	18
3 ขั้นตอนการได้มาของกุญแจรหัสส่วนตัว .....	23
3.1 นโยบายด้านความปลอดภัย .....	29
3.2 การเตรียมการด้านความปลอดภัย.....	31
3.3 รูปแบบของใบรับรองอิเล็กทรอนิกส์และกุญแจรหัสส่วนตัว .....	37
3.4 แนวทางการป้องกันกุญแจรหัสส่วนตัว .....	42
3.5 การตรวจสอบและประเมินความเสี่ยงด้านการใช้งาน .....	47
3.6 มาตรฐานที่จำเป็นพื้นฐาน .....	49
3.7 แนวทางในการเสนอเพื่อให้ผู้บริหารยอมรับเพื่อการนำไปใช้งาน .....	55
4 ผลการวิจัย .....	58

บทที่	หน้า
4.1 ขั้นตอนการปฏิบัติงานสำหรับเจ้าหน้าที่ทั่วไป .....	59
4.2 ขั้นตอนการปฏิบัติงานสำหรับผู้บริหาร .....	68
5 สรุปผลการวิจัยและข้อเสนอแนะ .....	71
5.1 สรุปผลการวิจัย .....	71
5.2 ปัญหาและอุปสรรคในการทำวิจัย .....	71
5.3 ข้อเสนอแนะ .....	72
5.4 ข้อเสนอแนะงานวิจัย .....	72
5.3 งานวิจัยในอนาคต .....	72
รายการอ้างอิง .....	73
ภาคผนวก	
ภาคผนวก ก มาตรฐานความปลอดภัยที่ใช้ในการอ้างอิง .....	76
ภาคผนวก ข ตัวอย่างแบบสำรวจข้อมูล .....	80
ประวัติผู้เขียนวิทยานิพนธ์ .....	84