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

กุญแจรหัสส่วนตัวของเทคโนโลยีกุญแจคู่สาธารณะเป็นวิธีการหนึ่งที่ได้รับการยอมรับว่ามีความปลอดภัยสูงในการนำไปใช้ในด้านการรักษาความลับและกระบวนการของการพิสูจน์ตัวตน ในปัจจุบันมีการประยุกต์ใช้งานในรูปแบบของลายมืออิเล็กทรอนิกส์ เพื่อใช้ในการทำธุรกรรมทางอิเล็กทรอนิกส์ต่างๆ เปรียบเทียบเท่ากับลายมือชื่อหรือลายเซ็นโดยทั่วไป อันต้องมีผลบังคับทางด้านกฎหมายด้วย ดังนั้นขั้นตอนหรือกระบวนการในการได้มา การดูแลรักษา ของกุญแจรหัสส่วนตัวต้องมีความน่าเชื่อถือว่ามีความปลอดภัยเพียงพอในการนำไปใช้เนื่องจากผู้ใช้ต้องรับผิดชอบต่อการทำธุรกรรมที่มีมูลค่ามหาศาลนั้นๆ

งานวิจัยนี้มีจุดประสงค์หลักคือการสร้างแนวทางที่เป็นขั้นตอนในการปฏิบัติงานเพื่อความปลอดภัยในการได้มาและใช้งานของกุญแจรหัสส่วนตัวที่เชื่อถือได้ รวมถึงข้อควรระวังในการนำไปใช้งานตลอดจนการดูแลรักษากุญแจรหัสส่วนตัว การวิจัยใช้วิธีการศึกษาและอ้างอิงโดยเปรียบเทียบจากมาตรฐานด้านความปลอดภัยที่ยอมรับในระดับสากลซึ่งมีการนำไปใช้งานอย่างแพร่หลายเช่น ISO, COBIT, ITIL และ HIPPAA และยังศึกษาถึงกระบวนการยอมรับของผู้บริหารเพื่อใช้นำเสนอต่อผู้บริหารขององค์กรซึ่งในงานวิจัยนี้เลือกสภาพแวดล้อมจุฬาลงกรณ์มหาวิทยาลัยเป็นกรณีศึกษาถึงการนำกระบวนการดังกล่าวไปใช้งาน

ผลที่ได้จากการศึกษาพบว่าขั้นตอนต่างๆที่ครอบคลุมตั้งแต่ นโยบาย การเตรียมความพร้อมพื้นฐานต่างๆเพื่อความปลอดภัย และขั้นตอนการสร้างกุญแจรหัสนั้น สามารถทำได้โดยนำจุดเด่นของแต่ละมาตรฐานมาประยุกต์ใช้ พร้อมแจกแจงรายละเอียดการปฏิบัติงานซึ่งบางมาตรฐานไม่ได้กล่าวไว้มาสรุปเป็นขั้นตอนการปฏิบัติงาน โดยสามารถแยกเป็น 2 แนวทางด้วยกันคือ ขั้นตอนการปฏิบัติสำหรับเจ้าหน้าที่ผู้ปฏิบัติงานทั่วไป และสำหรับการใช้งานในระดับผู้บริหารเพื่อใช้ในงานด้านความปลอดภัยของหน่วยงานหรือองค์กรต่อไป

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 HIPPAA. 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.