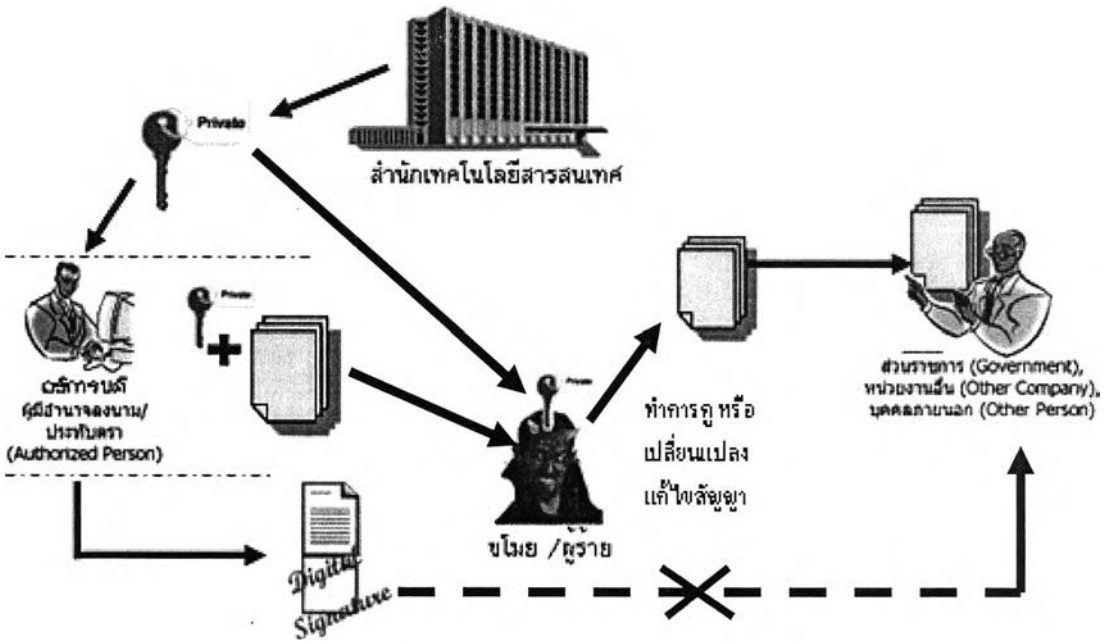
บทที่ 1

บทนำ

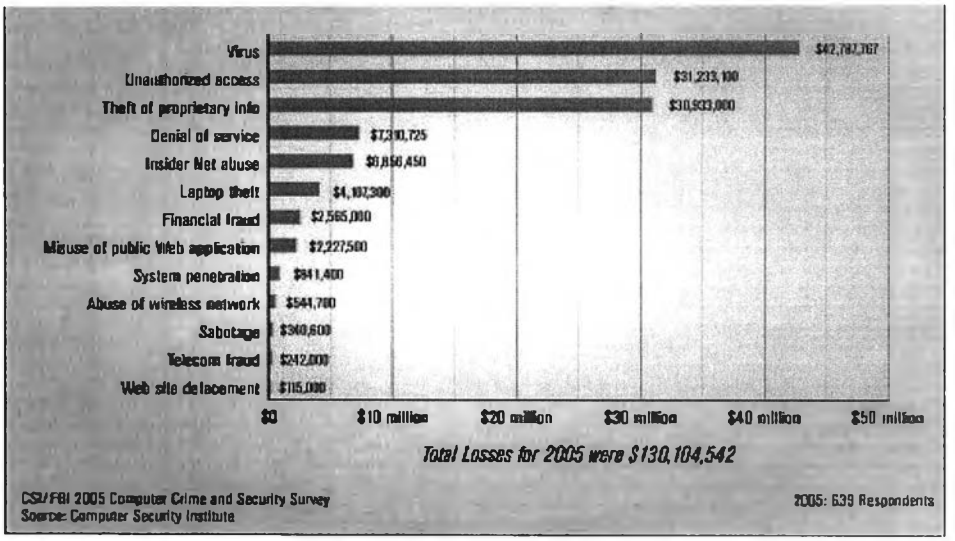
1.1 ความเป็นมาและความสำคัญของปัญหา

การนำเทคโนโลยีของกุญแจรหัสส่วนตัวของกุญแจคู่สาธารณะไปประยุกต์ใช้งานในรูปของลายมือชื่ออิเล็กทรอนิกส์ นั้นในปัจจุบันมีการนำไปใช้งานอย่างกว้างขวางในด้านของธุรกรรมและพาณิชย์อิเล็กทรอนิกส์ ซึ่งกฎหมายรับรองว่ามีค่าเทียบเท่ากับการเซ็นด้วยลายมือชื่อทางกายภาพบนกระดาษและมีผลผูกพันตามกฎหมายแต่ ในการทำธุรกรรมที่มีมูลค่ามหาศาลผลภาระของความรับผิดชอบและผูกพันโดยเฉพาะผู้บริหารระดับสูงๆ เช่น อธิการบดี เป็นต้น



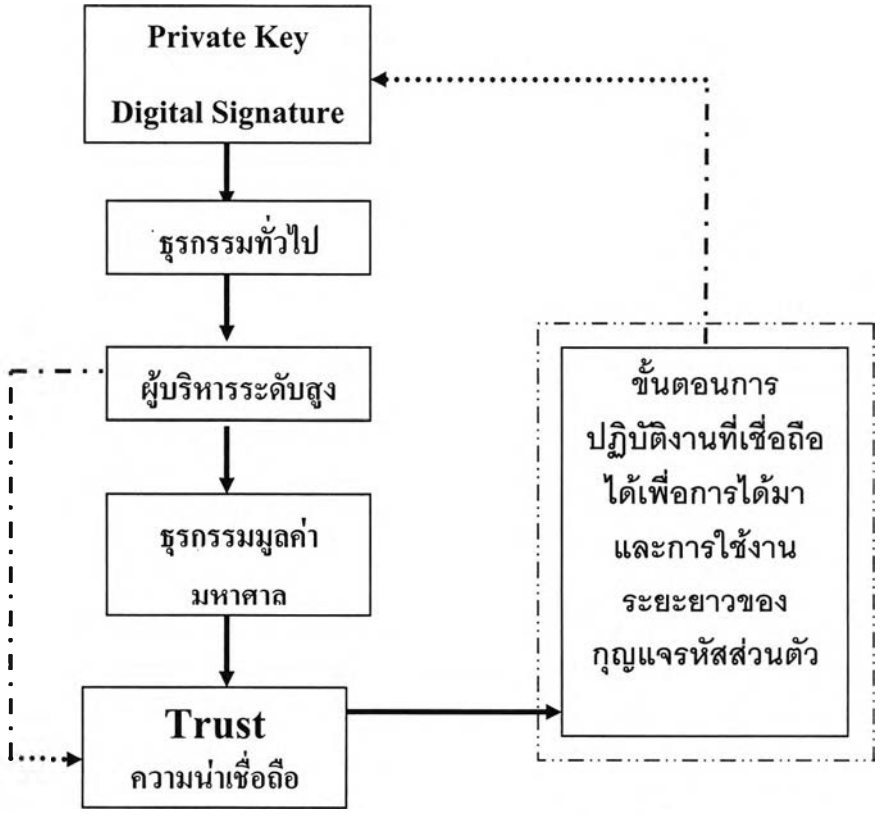
รูปที่ 1.1 ความเสี่ยงในการใช้งานกุญแจรหัสส่วนตัว

จากรูปที่ 1.1 จะเห็นว่ามีความเสี่ยงในการที่ผู้ไม่ประสงค์ดีจะทำการขโมยรหัสกุญแจส่วนตัวแล้วทำการแก้ไขหรือเปิดเผยสัญญาที่เป็นความลับก่อนที่จะส่งถึงผู้รับทำให้เกิดความเสียหายและส่งผลทำให้ไม่เกิดความน่าเชื่อถือต่อการนำกุญแจรหัสส่วนตัวไปใช้งาน สถิติของสถาบันการรักษาความปลอดภัยทางคอมพิวเตอร์ (Computer Security Institute) [4] ปี 2005 แสดงไว้ดังรูปที่ 1.2 ในอันดับที่ 2 และ 3 แสดงให้เห็นมูลค่าความเสียหายในรูปแบบการโจมตีของการเข้าถึงข้อมูลโดยมิได้รับอนุญาตและการโจรกรรมข้อมูลที่มีค่าในหน่วยงาน



รูปที่ 1.2 **ความสูญเสียจากการโจมตีแบบต่าง ๆ**[4]

ดังนั้นการใช้งานจึงควรมีวิธีการหรือขั้นตอนที่จะสร้างความปลอดภัยและน่าเชื่อถือให้แก่ผู้ใช้งานในการนำกุญแจรหัสส่วนตัวไปใช้งานในรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ เพื่อทำสัญญาหรือเซ็นรับรองเอกสารอิเล็กทรอนิกส์ต่างๆ งานวิจัยนี้จึงนำเสนอขั้นตอนการปฏิบัติงานที่น่าเชื่อถือได้เพื่อการได้มาและการใช้งานของกุญแจรหัสส่วนตัวให้มีความปลอดภัยและน่าเชื่อถือ ดังแสดงภาพรวมของลำดับการนำขั้นตอนการปฏิบัติในงานวิจัยไปใช้งานในรูปที่ 1.1



รูปที่ 1.3 **ภาพรวมของการการสร้างขั้นตอนการปฏิบัติงาน**

1.2 วัตถุประสงค์ของการวิจัย

1. สร้างแนวทางที่เป็นขั้นตอนในการปฏิบัติงานเพื่อความปลอดภัยในการได้มาและใช้งานของกุญแจรหัสส่วนตัวที่เชื่อถือได้ รวมถึงข้อควรระวังในการนำไปใช้งานตลอดจนการดูแลรักษากุญแจรหัสส่วนตัว
2. เสนอแนวทางหรือวิธีการสร้างการยอมรับในการนำขั้นตอนปฏิบัติการของงานวิจัยนี้เสนอผู้บริหารเพื่อการนำไปใช้งานจริง
3. เสนอความปลอดภัยด้านกายภาพในขั้นตอนต่างๆเพื่อเสริมในส่วนที่ยังมีจุดอ่อนในการสร้างและดูแลรักษากุญแจรหัสส่วนตัว

1.3 ขอบเขตของการวิจัย

1. ใช้สภาพแวดล้อมของ จุฬาลงกรณ์มหาวิทยาลัย เป็นกรณีศึกษา
2. ใช้อุปกรณ์และกรรมวิธีที่สามารถจัดหาได้โดยไม่คิดมูลค่าหรือในราคาที่เหมาะสม
3. สร้างความน่าเชื่อถือเชื่อมั่นของขั้นตอนการใช้งานกุญแจรหัสส่วนตัว ให้เป็นที่ยอมรับของผู้บริหาร เช่น รองอธิการหรือคณบดีขึ้นไป
4. จุดอ่อนบางอย่างในกระบวนการไม่สามารถแก้ไขได้โดยง่ายแต่จะแจกแจงประเด็นให้เห็นรวมถึงแนวทางที่จะช่วยผ่อนคลายสถานการณ์

1.4 ขั้นตอนการวิจัย

1. ศึกษาข้อมูลเกี่ยวกับมาตรฐานการรักษาความปลอดภัยต่างที่นิยมนำมาใช้งานและดำเนินการเปรียบเทียบมาตรฐานต่างๆ
2. ศึกษา การรับรองลายมือชื่ออิเล็กทรอนิกส์ ในด้านกฎหมาย พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์,RFCที่เกี่ยวข้องกับความปลอดภัยของกุญแจส่วนตัว
3. ศึกษาการวิธีการสร้าง กุญแจส่วนตัว ที่ ครบวงจร และรวบรวมวิธีที่ป้องกันและบริหาร key จากแหล่ง ข้อมูลต่างๆ รวบรวมวิธีที่ผู้ถือรหัสลับควรที่จะป้องกันการถูกขโมยกุญแจรหัสส่วนตัว และการดูแลและบริหาร กุญแจรหัสส่วนตัว พิจารณาถึงข้อแนะนำต่างๆที่ควรป้องกันจากเอกสารและรายงานการประชุมต่างๆ
4. นำขั้นตอนและวิธีการบริหารจัดการคีย์ จากแหล่งต่างๆ นำมารวบรวมและสรุปเป็นขั้นตอนที่ควรจะมีในการบริหารดูแลรักษากุญแจรหัสส่วนตัว ทำการศึกษา

พิจารณาถึงปัจจัยและผลกระทบต่างๆในการที่ผู้บริหารระดับสูงจะพิจารณาการใช้งานกุญแจรหัสส่วนตัว

5. สืบค้นวิธีการ ขั้นตอน เพื่อให้ผู้บริหารยอมรับในการที่จะทดลองหรือนำนวัตกรรมใหม่ไปใช้งานด้วยความเชื่อมั่น
6. ศึกษาถึงวิธีการส่งมอบรหัสลับและการจัดตั้งหน่วยงานกลางขึ้นมารองรับ และการออกใบรับรองรหัส
7. พิจารณาขั้นตอนแนวทางการปฏิบัติงานที่สำคัญสำหรับบุคคลากรที่เกี่ยวข้องในการบริหารจัดการกุญแจส่วนตัว
8. รวบรวมการป้องกันทางกายภาพด้านต่างๆที่อาจมีบุคคลเข้าไปเกี่ยวข้องเพื่อสรุปเป็นขั้นตอนทางการป้องกันทางกายภาพจากเอกสารอ้างอิงต่างๆ
9. ศึกษามาตรฐาน ต่างๆ เช่น RFC3126 – Electronic Signature Formats for long term electronic signatures และ case study ต่างๆ เพื่อเป็นแนวทางอ้างอิง
10. สรุปเป็นขั้นตอนต่างๆเป็นแนวทางในการการบริหารจัดการ กุญแจรหัสส่วนตัว

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ผู้บริหารและดูแลระบบไม่ต้องรับผิดชอบในเรื่องของ กุญแจรหัสส่วนตัว
2. ไม่จำเป็นต้องมีผู้เชี่ยวชาญพิเศษที่มีความชำนาญเมื่อปฏิบัติตามขั้นตอนตามงานวิจัยนี้
3. ลดความตึงเครียดในการทำงานของผู้ดูแลระบบ
4. สร้างความเชื่อมั่นให้แก่ผู้บริหารระดับสูงขององค์กรในการใช้งาน กุญแจรหัสส่วนตัว เป็นระบบที่สามารถสร้างขึ้นได้โดยสามารถจัดหาหรือจัดซื้อได้โดยทั่วไป

1.6 โครงสร้างวิทยานิพนธ์

ในบทที่ 2 จะกล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง บทที่ 3 จะทำการเปรียบเทียบขั้นตอนการปฏิบัติจากมาตรฐานด้านความปลอดภัยที่ยอมรับในระดับสากลซึ่งมีการนำไปใช้งานอย่างแพร่หลายเช่น ISO, COBIT, ITIL และ HIPPAA เพื่อนำมาอ้างอิงในการสร้างขั้นตอนในการปฏิบัติงานเพื่อความปลอดภัยในการได้มาและใช้งานของกุญแจรหัสส่วนตัวรวมไปถึงการป้องกันทางกายภาพเพื่อเสริมเข้าไปในขั้นตอนที่ควรจะมี และนำเสนอถึงข้อควรระวังในการนำไปใช้งานตลอดจนการดูแลรักษากุญแจรหัสส่วนตัว บทนี้ยังเสนอกระบวนการเพื่อการยอมรับเพื่อใช้นำเสนอต่อผู้บริหาร โดยใช้สภาพแวดล้อมจุฬาลงกรณ์มหาวิทยาลัยเป็นกรณีศึกษา บทที่ 4 จะ

เป็นผลการวิจัยโดยสรุปขั้นตอนจากบทที่3 ได้แนวทางในการนำไปใช้งานอยู่ 2 แนวทางคือ ขั้นตอนการปฏิบัติงานสำหรับผู้บริหาร ขั้นตอนการปฏิบัติงานสำหรับเจ้าหน้าที่ทั่วไปและแนวทางขั้นต่ำที่ควรมีในการปฏิบัติงานเพื่อความปลอดภัยขององค์กร และบทที่ 5 จะทำการสรุปผลที่ได้ ปัญหาและอุปสรรครวมถึงข้อเสนอแนะต่างๆไว้ในบทนี้