การออกแบบกระบวนการลงลายมือชื่อดิจิทัลตามตำแหน่งงานสำหรับหน่วยงานภาครัฐ

THE DESIGN OF THE POSITION BASED DIGITAL SIGNATURE PROCESSES FOR THE GOVERNMENT ORGANIZATIONS

***สุปราณี ลี้เจริญ*[1*], *สมชาย นำประเสริฐชัย*[2]**

***Supranee Leecharoen*[1*], *Somchai Numprasertchai*[2]**

[1]*สาขาเทคโนโลยีสารสนเทศ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์*

[1]*Science in Information Technology Program, Department of Computer Engineering, Faculty of Engineering, Kasetsart University.*

[2]*ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์*

[2]*Department of Computer Engineering, Faculty of Engineering, Kasetsart University.*

***Corresponding author, E-mail:** supranee.l@ku.ac.th*

บทคัดย่อ

ระบบเอกสารอิเล็กทรอนิกส์ (e-Document) เป็นระบบสารสนเทศหลักที่ช่วยเพิ่มความคล่องตัวในการปฏิบัติงานขององค์กร การลงลายมือชื่อดิจิทัลเป็นส่วนสำคัญในการจัดส่งเอกสารอิเล็กทรอนิกส์สำหรับตรวจสอบและยืนยันตัวบุคคลที่จัดส่งเอกสารและเป็นบุคคลที่มีอำนาจในการลงนามเอกสารได้ งานวิจัยนี้เป็นการนำเสนอแนวคิดการออกแบบกระบวนการนำการลงลายมือชื่อดิจิทัลมาใช้ในการประทับตราตามตำแหน่งงานและกรอบแนวคิดระบบบริหารจัดการใบรับรองอิเล็กทรอนิกส์ตามตำแหน่งงานสำหรับใช้ในการพัฒนาระบบเอกสารอิเล็กทรอนิกส์ภายในหน่วยงาน โดยใช้ระบบกุญแจสาธารณะ (Public Key Infrastructure) ที่มีการเข้ารหัสแบบอสมมาตร (Asymmetric Key Cryptography)

ผลการประเมินพบว่าการใช้กุญแจหลัก (Personal Master Key) มีความเหมาะสมกับการรับรองลายมือชื่ออิเล็กทรอนิกส์แบบอิงตำแหน่งงานที่สุด เนื่องจากวิธีการลงทะเบียน การลงลายมือชื่อไม่ซับซ้อน และการตรวจสอบความถูกต้องของเอกสารเป็นที่ยอมรับ

คำสำคัญ: การลงลายมือชื่อดิจิทัล เอกสารอิเล็กทรอนิกส์ ตราประทับเวลาอิเล็กทรอนิกส์

Abstract

e-Document is one of the most important information system (IS) which increase the flexibility of working processes. The digital signature is a vital part in the e-Documents mechanism for identifying user and verifying the user's authority to sign the document. This paper presents the concept of designing the position based digital signature process and certificate management framework for implementing internal e-Document system which increases using Public Key Infrastructure (PKI) with Asymmetric Key Cryptography.

The results presented that the Personal Master Key is suitable for position-based digital signature. Based on the easy registration, simple sign process and acceptable document verification.

Keywords: Digital Signature, Electronics Document, Electronics Timestamp

บทนำ

หน่วยงานภาครัฐมีการพัฒนาระบบงานสารสนเทศเพื่อการบริหารจัดการ เพิ่มประสิทธิภาพการดำเนินการและอำนวยความสะดวกแก่บุคลากร ระบบเอกสารอิเล็กทรอนิกส์เป็นระบบสารสนเทศหนึ่งที่มีความสำคัญสำหรับทุกองค์กรที่ช่วยเพิ่มความคล่องตัวในการปฏิบัติงานและลดปัญหางานเอกสาร การลงลายมือชื่อดิจิทัล (Digital Signature) เป็นส่วนสำคัญในการสร้างความเชื่อมั่นในการยืนยันตัวตนของบุคคลที่จัดส่งและมีอำนาจในการลงนามเอกสารอิเล็กทรอนิกส์ได้ นอกจากนี้ระบบเอกสารอิเล็กทรอนิกส์ยังมีกระบวนการตรวจสอบว่าเอกสารที่จัดส่งนั้นไม่มีการแก้ไขเปลี่ยนแปลงข้อมูลระหว่างการส่งโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certificate Authority)

หน่วยงานของรัฐมีการบริหารงานแบบลำดับชั้นต้องการนำระบบการลงลายมือชื่อดิจิทัลมาใช้ทดแทนการลงนามเอกสารแบบเดิม จำเป็นต้องคำนึงถึงระดับชั้นตามความสำคัญของตำแหน่งงาน ช่วงเวลาการดำรงตำแหน่งหรือการปฏิบัติหน้าที่แทนบุคลากรหนึ่งคนสามารถดำรงตำแหน่งได้หลายตำแหน่งในคราวเดียวกัน ดังนั้นการออกแบบและสร้างใบรับรองอิเล็กทรอนิกส์ที่เป็นส่วนตัวของผู้ใช้งาน และใบรับรองอิเล็กทรอนิกส์ที่ใช้แทนตราประทับประจำตำแหน่งจึงมีความสำคัญเป็นอย่างยิ่ง ระบบที่ออกแบบต้องสามารถป้องกันการปลอมแปลงข้อมูลตำแหน่งงาน และสามารถเปลี่ยนแปลงตำแหน่งงานให้เป็นไปตามกฎระเบียบของหน่วยงานเช่น การแต่งตั้ง การเพิกถอน และการมอบหมายรักษาการแทน เป็นต้น

ดังนั้นบทความนี้จึงเสนอแนวคิดการออกแบบกระบวนการนำการลงลายมือชื่อดิจิทัลมาใช้ในการประทับตราตำแหน่งงาน รวมทั้งกรอบแนวคิดของระบบบริหารจัดการใบรับรองอิเล็กทรอนิกส์ตามตำแหน่งงานเพื่อสร้างความน่าเชื่อถือของเอกสารอิเล็กทรอนิกส์ที่ลงนาม สำหรับใช้เป็นแนวทางในการพัฒนาระบบเอกสารอิเล็กทรอนิกส์ที่เหมาะสมสำหรับหน่วยงานของรัฐต่อไป โดยอาศัยเทคโนโลยีดังต่อไปนี้

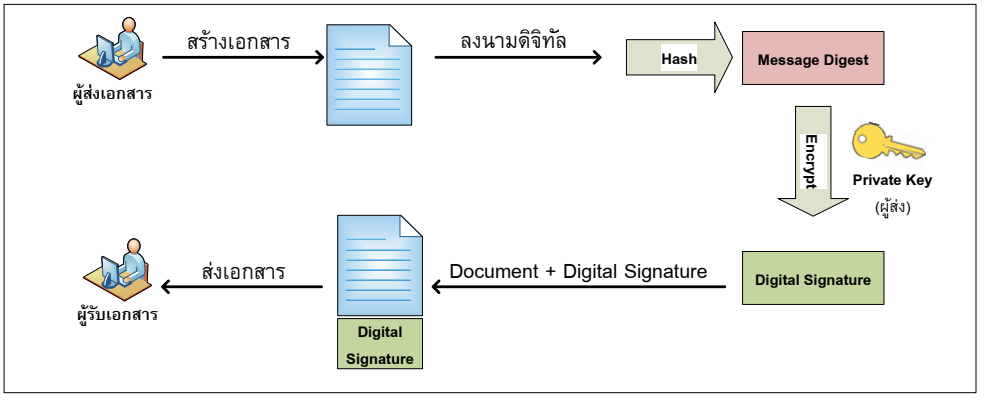
ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) หมายถึง ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ [1] ซึ่งออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority : CA) ที่มีความน่าเชื่อถือ แบ่งเป็น 3 ประเภท คือ ใบรับรองตัวบุคคล (Personal Certificate) ใบรับรองสำหรับนิติบุคคล องค์กรหรือหน่วยงาน (Enterprise Certificate) และใบรับรองเครื่องให้บริการเว็บ (SSL Certificate) [2-3] ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แต่ละรายจะสร้างใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน (Public Key Cryptography Standards: PKCS) [4] ซึ่งเป็นมาตรฐานการเข้ารหัสข้อความ ตัวอย่างเช่น PKCS#11 เป็นใบรับรองอิเล็กทรอนิกส์ที่อยู่ในรูปแบบ Token Interface ซึ่งอาจจะเป็นอุปกรณ์ที่เชื่อมต่อผ่าน API ของซอฟต์แวร์คอมพิวเตอร์ PKCS #12 เป็นการจัดเก็บ private key พร้อม Public key ในรูปแบบไฟล์โดยป้องกันด้วยรหัสผ่านที่แบบสมมาตร (Symmetric key) เป็นต้น

ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) เป็น อักษร อักขระ ตัวเลข เสียง หรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้นและเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความ

ในข้อมูลอิเล็กทรอนิกส์นั้น [1] ในขณะที่ลายมือชื่อดิจิทัล (Digital Signature) เป็นลายมือชื่ออิเล็กทรอนิกส์อย่างหนึ่ง ซึ่งเป็น อักษร อักขระ หรือสัญลักษณ์ที่สร้างขึ้นโดยโปรแกรมคอมพิวเตอร์ โดยอาศัยเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI) หรืออาจใช้วิธีการจัดการกุญแจแบบ PGP (Pretty Good Privacy) โดยที่ทั้งสองวิธีการนั้นพัฒนาขึ้นจากการเข้ารหัสลับ (Cryptography) จึงทำให้มีคุณสมบัติในการสร้างและตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ได้เป็นที่ยอมรับ [5]

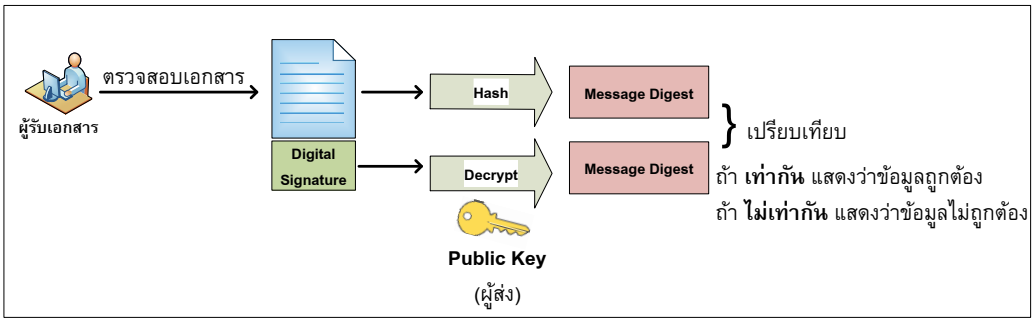
ระบบงานเอกสารอิเล็กทรอนิกส์จำนวนมากมีการลงลายมือชื่อดิจิทัล เช่น ระบบงานสารบรรณอิเล็กทรอนิกส์ของจุฬาลงกรณ์มหาวิทยาลัย [6] ใช้ใบรับรองอิเล็กทรอนิกส์บุคคลในการลงนามดิจิทัลโดยไม่มีระบบตราประทับเวลาอิเล็กทรอนิกส์แสดงวันและเวลา สำหรับระบบสารบรรณอิเล็กทรอนิกส์ทั่วไปที่ดำเนินการโดยบริษัทเอกชนไม่พบว่ามีการออกแบบให้รองรับการลงนามอิเล็กทรอนิกส์ตามตำแหน่งงานและไม่มีการใช้ระบบตราประทับเวลา เช่น ระบบ ThSaraban [7]

การรักษาความปลอดภัยเอกสารอิเล็กทรอนิกส์ทั่วไปใช้ระบบกุญแจสาธารณะ (Public Key Infrastructure : PKI) [8] ประกอบด้วยกุญแจ 2 ชนิดที่มีความสัมพันธ์กันคือ กุญแจส่วนตัว (Private Key) ที่จะถูกเก็บไว้กับเจ้าของกุญแจสำหรับการยืนยันตัวตน และกุญแจสาธารณะ (Public Key) ที่ถูกเผยแพร่ให้บุคคลอื่นสามารถติดต่อสื่อสารกับเจ้าของกุญแจได้ ซึ่งเป็นวิธีการที่ได้รับการยอมรับและใช้งานทั่วโลก โดยมีขั้นตอนการลงลายมือชื่อดิจิทัลดังภาพที่ 1 เริ่มจากผู้ส่งเอกสารสร้างเอกสารอิเล็กทรอนิกส์จากนั้นทำการลงนามดิจิทัล ในขั้นตอนนี้ระบบจะนำเอกสารมาผ่านฟังก์ชันทางคณิตศาสตร์ที่เรียกว่า แฮชฟังก์ชัน (Hash Functions) เพื่อให้ได้รหัสจำเพาะของเอกสารฉบับนั้นๆ เรียกว่า เมสเซสไดเจสต์ (Message Digest) จากนั้นนำรหัสจำเพาะของเอกสารที่ได้เข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่งเอกสารตามกระบวนการเข้ารหัสแบบอสมมาตร (Asymmetric Key Cryptography) ได้ลายมือชื่อดิจิทัล เพื่อนำมาประกอบกับเอกสารต้นฉบับส่งให้ผู้รับต่อไป



ภาพที่ 1 ขั้นตอนการลงลายมือชื่อดิจิทัล

สำหรับการตรวจสอบความถูกต้องของเอกสารที่ผ่านการลงลายมือชื่อดิจิทัลนั้น ผู้รับเอกสารจะทำการตรวจสอบด้วยกุญแจสาธารณะของผู้ส่งดังภาพที่ 2 โดยระบบจะนำส่วนที่เป็นเนื้อหาเอกสารมาผ่านแฮชฟังก์ชันได้เมสเซสไดเจสต์แรก เพื่อนำมาเปรียบเทียบกับเมสเซสไดเจสต์ที่สองที่ได้จากการนำส่วนลายมือชื่อดิจิทัลมาถอดรหัสด้วยกุญแจสาธารณะของผู้ส่งตามกระบวนการถอดรหัสรูปแบบอสมมาตร หากเปรียบเทียบเมสเซสไดเจสต์แล้วเท่ากันแสดงว่าเอกสารที่ได้รับถูกต้องไม่มีการแก้ไขระหว่างทาง



ภาพที่ 2 วิธีการตรวจสอบการลงลายมือชื่อดิจิทัล

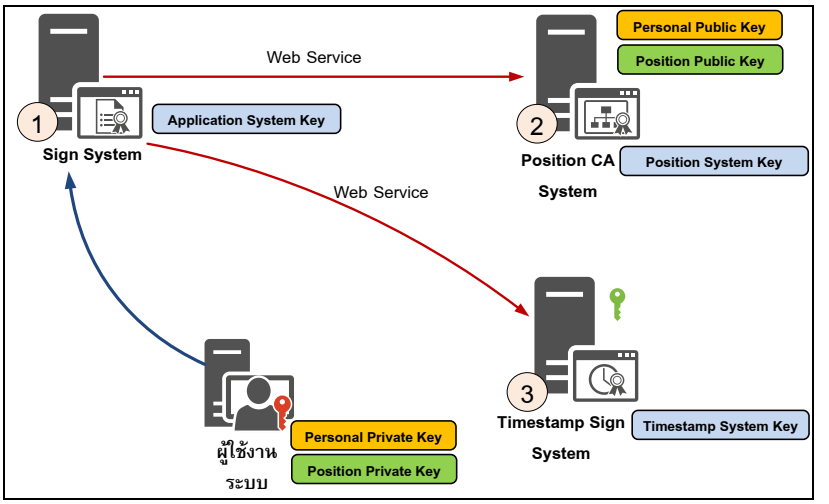
การประทับเวลาอิเล็กทรอนิกส์ (Timestamp) ได้มีนำการประทับเวลาอิเล็กทรอนิกส์มาเป็นส่วนในการพิจารณาการรับรองเอกสารอิเล็กทรอนิกส์เพื่อเป็นการยืนยันความถูกต้องของวันและเวลาในการลงนามเอกสาร ตราประทับเวลาและขั้นตอนการตรวจสอบตราประทับเวลาสามารถใช้เป็นหลักฐานและใช้สำหรับพิสูจน์หลักฐานดิจิทัลได้ [9] นอกจากนี้ยังมีตราประทับเวลาอิเล็กทรอนิกส์แบบออฟไลน์ที่ใช้ชิพ TPM สำหรับประมวลผลเพื่อเข้ารหัสข้อมูลด้วยการเชื่อมต่อผ่าน Library ที่พัฒนาบนภาษา JAVA TPM เพื่อตราประทับเวลาตามมาตรฐาน RFC3161 [10] ทั้งนี้การเพิ่มความน่าเชื่อถือของเอกสารอิเล็กทรอนิกส์โดยการใช้ตราประทับเวลาจากเซิร์ฟเวอร์กลางสามารถลดความแตกต่างของเวลาลงนามในเอกสารอิเล็กทรอนิกส์อันเนื่องมาจากขั้นตอนการประกอบเอกสารเข้ากับลายมือชื่อดิจิทัล [11] การนำตราประทับเวลาอิเล็กทรอนิกส์มาใช้งานมีส่วนช่วยในการตรวจสอบวันและเวลาที่ลงนามดิจิทัลช่วยให้แก้ปัญหาด้านเวลาเหลื่อม (Time Zone) ได้ และสามารถตรวจสอบวันและเวลาของเอกสารทุกฉบับของหน่วยงานที่ใช้ระบบประทับตรากลาง อย่างไรก็ตามการนำตราประทับเวลามาใช้ในการให้บริการพาณิชย์อิเล็กทรอนิกส์ในประเทศไทยยังไม่มีมาตรฐาน และกฎหมายรองรับ [12]

วัตถุประสงค์ของการวิจัย

1. เพื่อออกแบบกระบวนการลงลายมือชื่อดิจิทัลตามตำแหน่งงานในหน่วยงานภาครัฐ
2. เพื่อออกแบบวิธีการตรวจสอบและยืนยันตัวตนของผู้มีสิทธิ์ลงลายมือชื่อดิจิทัลตามตำแหน่งงานที่เหมาะสมสำหรับหน่วยงานภาครัฐ

วิธีดำเนินการวิจัย

บทความนี้เป็นการนำเสนอการออกแบบกระบวนการลงลายมือชื่อดิจิทัลสำหรับการลงลายมือชื่อดิจิทัลตามตำแหน่งงานสำหรับระบบเอกสารอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ ก่อนที่จะนำไปพัฒนาระบบเอกสารอิเล็กทรอนิกส์ต้นแบบเพื่อพิสูจน์ประสิทธิภาพและยืนยันความเหมาะสมของกระบวนการอีกครั้งหนึ่ง



ภาพที่ 3 แนวคิดการออกแบบกระบวนการลงลายมือชื่อดิจิทัลตามตำแหน่งงานในหน่วยงานภาครัฐ

แนวคิดในการออกแบบกระบวนการแบ่งระบบออกเป็น 3 ส่วนดังภาพที่ 3 คือ 1) ระบบบริหารจัดการการลงนามดิจิทัล (Sign System) สำหรับควบคุมขั้นตอนการลงนามเอกสารอิเล็กทรอนิกส์และมีส่วนสำหรับให้ผู้ใช้งานตรวจสอบความถูกต้องของการลงนามเอกสาร 2) ระบบบริหารจัดการสิทธิ์ตามตำแหน่งงาน (Position based CA System) ทำหน้าที่จัดเก็บความสัมพันธ์ระหว่างบุคคล หน่วยงาน ตำแหน่งงาน ช่วงเวลาที่ปฏิบัติงาน และกุญแจสาธารณะของบุคคล เพื่อให้รองรับการตรวจสอบสิทธิ์ในการลงนามเอกสารตามตำแหน่งงานได้อย่างถูกต้องและน่าเชื่อถือและสามารถจัดเก็บข้อมูลการลงนามในกรณีปฏิบัติหน้าที่แทนได้ และ 3) ระบบประทับเวลาอิเล็กทรอนิกส์ (Timestamp Sign System) สำหรับรับรองวันและเวลาในการลงนามดิจิทัลเพื่อให้เป็นมาตรฐานเวลาเดียวกันทั้งระบบงาน ในการเข้าถึงระบบงานแบ่งได้เป็น 2 ส่วน ส่วนแรกคือการเข้าถึงระบบงานจากผู้ลงนามเอกสาร โดยสามารถเรียกใช้งานได้เฉพาะระบบบริหารจัดการการลงนามดิจิทัลเท่านั้น ส่วนที่สองคือการเข้าถึงระบบงานผ่านการเชื่อมต่อเว็บเซอร์วิสโดยระบบบริหารจัดการสิทธิ์ตามตำแหน่งงานและระบบประทับเวลาอิเล็กทรอนิกส์จะอนุญาตให้เฉพาะระบบบริหารจัดการการลงนามดิจิทัลเชื่อมต่อเท่านั้น

ทั้งนี้ การออกแบบกระบวนการข้างต้นเป็นการแบ่งระบบเพื่อความชัดเจนในการบริหารจัดการและการรักษาความปลอดภัยข้อมูลของเอกสารที่ลงนาม นอกจากนี้มีส่วนงานที่เป็นหัวใจสำคัญของการออกแบบเพื่อความสมบูรณ์ของระบบคือ ส่วนของการลงลายมือชื่อดิจิทัลโดยการนำกุญแจสาธารณะมาใช้ประโยชน์ เพื่อให้ระบบมีความน่าเชื่อถือ เป็นที่ยอมรับ และสามารถตรวจสอบการลงลายมือชื่อดิจิทัลตามตำแหน่งงานได้อย่างครอบคลุม

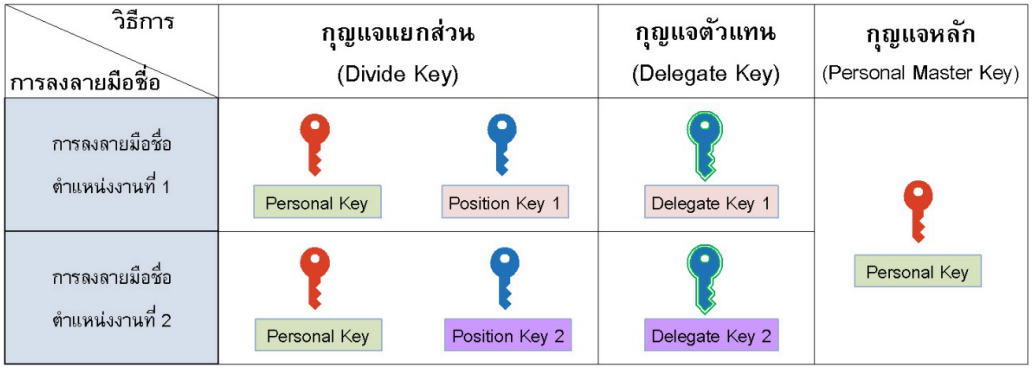
เพื่อให้ได้วิธีการใช้งานกุญแจสาธารณะที่เหมาะสมจะนำมาใช้งานในหน่วยงานมากที่สุดนั้น ได้มีการประเมินความเหมาะสมของการออกแบบวิธีการใช้งานกุญแจสาธารณะนี้แบ่งออกเป็น 2 ส่วน คือ การเปรียบเทียบข้อเด่นและด้อยคุณสมบัติของวิธีการทั้ง 3 รูปแบบ และการประเมินจากผู้เชี่ยวชาญ จำนวน 3 คนที่เป็นผู้บริหารองค์กรระดับผู้อำนวยการและรองผู้อำนวยการที่เกี่ยวข้องกับระบบเอกสารอิเล็กทรอนิกส์และมีความรู้ความเข้าใจด้าน ICT

ผลการวิจัย

ผลการดำเนินการสามารถแบ่งออกเป็น 2 ส่วนคือ 1) การออกแบบกระบวนการลงลายมือชื่อดิจิทัลตามตำแหน่งงาน และ 2) ผลการประเมินกระบวนการลงลายมือชื่อดิจิทัลตามตำแหน่งงานและความคิดเห็นจากจากผู้เชี่ยวชาญและผู้ใช้งานที่เกี่ยวข้องกับระบบเอกสารอิเล็กทรอนิกส์

การออกแบบกระบวนการลงลายมือชื่อดิจิทัลตามตำแหน่งงาน

การออกแบบกระบวนการลงลายมือชื่อดิจิทัลตามตำแหน่งงานนี้ได้พิจารณาออกแบบเป็น 3 วิธีการ/รูปแบบ คือ วิธีการที่ 1: กุญแจแยกส่วน (Divide Key) วิธีการที่ 2: กุญแจตัวแทน (Delegate Key) และวิธีการที่ 3: กุญแจหลัก (Personal Master Key) ดังภาพที่ 4 โดยทั้ง 3 วิธีจำเป็นต้องมีกุญแจที่ได้รับการรับรองจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certificate Authority) ที่น่าเชื่อถือและได้รับการยอมรับเพื่อใช้ในการยืนยันตัวบุคคลหรือหน่วยงาน



ภาพที่ 4 การใช้กุญแจแต่ละประเภทในการลงลายมือชื่อดิจิทัลตามตำแหน่งงานของแต่ละวิธีการ

ในการออกแบบแต่ละวิธีมีรายละเอียดดังนี้

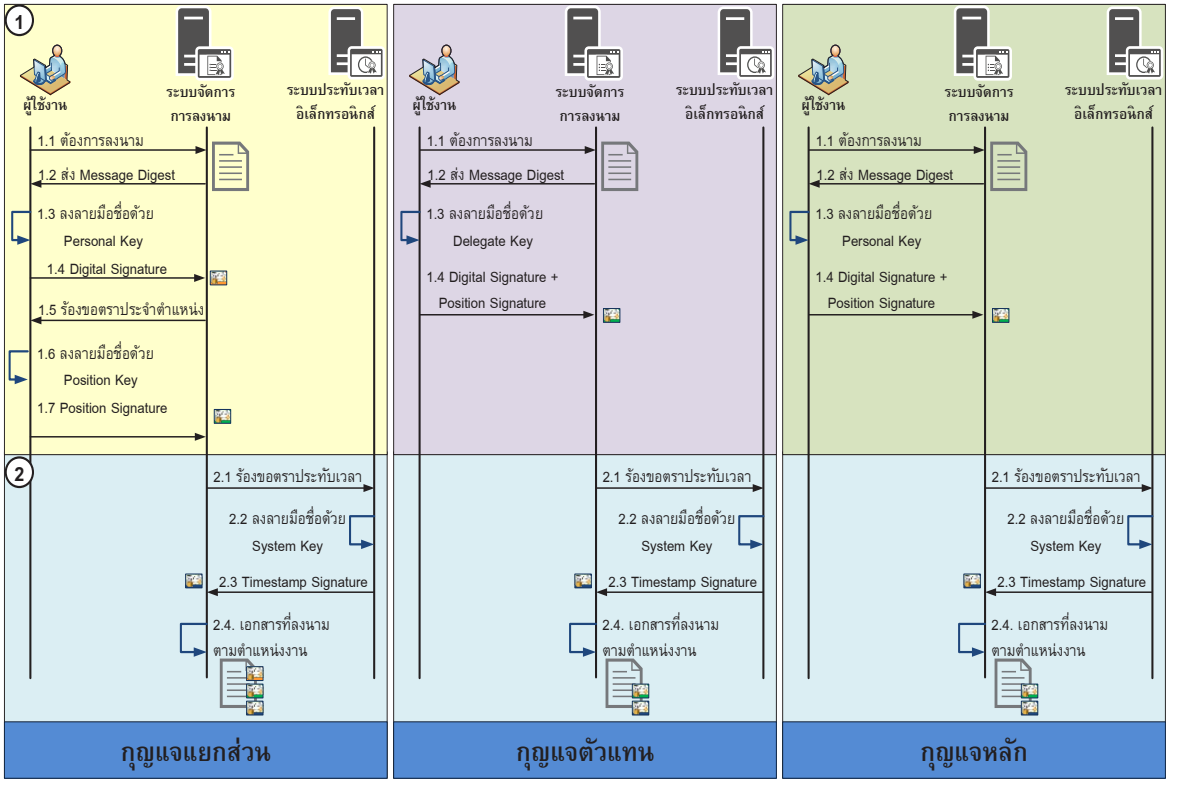
วิธีการที่ 1 **กุญแจแยกส่วน (Divide Key)** ผู้ใช้งานต้องมีกุญแจจำนวน 2 ดอก ในการลงลายมือชื่อตามตำแหน่งงาน กุญแจดอกแรกคือ กุญแจส่วนบุคคล (Personal Key) ออกในนามบุคคลธรรมดาโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือและได้รับการยอมรับเพื่อใช้ในการยืนยันตัวบุคคล ส่วนกุญแจดอกที่สอง ออกในนามหน่วยงานโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือและได้รับการยอมรับเพื่อใช้ในการยืนยันหน่วยงาน โดยเรียกว่า กุญแจตามตำแหน่งงาน (Position Key) ทั้งนี้การลงทะเบียนใช้งานในระบบบริหารจัดการสิทธิ์ในการลงนามตามตำแหน่งงาน (Position based CA System) ระบบจะมีการผูกความสัมพันธ์ของข้อมูลของกุญแจประจำตำแหน่งงานทั้ง 2 ดอก เข้ากับตำแหน่งงานที่ร้องขอ ดังนั้น วิธีการนี้ จำนวนกุญแจแยกส่วนจะมีเท่ากับกุญแจส่วนบุคคลรวมกับจำนวนตำแหน่งงานที่ดำรงหรือรักษาการแทนของผู้ใช้งาน เมื่อต้องการลงลายมือชื่อดิจิทัลตามตำแหน่งงานใดให้นำกุญแจส่วนบุคคล พร้อมทั้งกุญแจประจำตำแหน่งนั้นลงนามควบคู่กันทุกครั้ง

วิธีการที่ 2 **กุญแจตัวแทน (Delegate Key)** ผู้ใช้งานต้องมีกุญแจอย่างน้อย 1 ดอก ขึ้นอยู่กับตำแหน่งที่รับผิดชอบ โดยหน่วยงานจัดซื้อใบรับรองอิเล็กทรอนิกส์ที่ออกในนามหน่วยงานจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือและได้รับการยอมรับ ผู้ใช้งานต้องลงทะเบียนใช้งานในระบบบริหารจัดการสิทธิ์ในการลงนามตามตำแหน่ง

งาน (Position based CA System) เพื่อเชื่อมโยงความสัมพันธ์ระหว่างบุคคลและตำแหน่งงาน กุญแจ 1 ดอก ต่อการดำรงตำแหน่งงาน 1 ตำแหน่ง เพื่อใช้ลงลายมือชื่อดิจิทัลตามตำแหน่งงานที่รับผิดชอบในเอกสารอิเล็กทรอนิกส์

วิธีการที่ 3 **กุญแจหลัก (Personal Master Key)** ผู้ใช้งานจะใช้กุญแจเพียงดอกเดียวเท่านั้นในการลงลายมือชื่อตามตำแหน่งงานใดๆ โดยผู้ใช้งานนำกุญแจสาธารณะส่วนบุคคล (Public Key) มาลงทะเบียนในระบบบริหารจัดการสิทธิ์ในการลงนามตามตำแหน่งงาน (Position based CA System) และจัดเก็บเป็นกุญแจส่วนบุคคล (Personal Key) ที่มีการบันทึกความสัมพันธ์ระหว่างบุคคลและตำแหน่งงาน เมื่อมีการปรับเปลี่ยนตำแหน่งงานทุกครั้งให้ผู้ใช้งานทำการลงทะเบียนกุญแจตำแหน่งงานทุกครั้ง ดังนั้นการลงลายมือชื่อดิจิทัลจะใช้เพียงกุญแจส่วนบุคคลในการลงนามเท่านั้น

จากแนวคิดข้างต้น ได้มีการออกแบบกระบวนการลงลายมือชื่อดิจิทัลตามตำแหน่งงานของแต่ละวิธีการออกเป็น 2 ส่วน คือ ส่วนที่ 1 การลงนามเพื่อรับรองตำแหน่งงาน ส่วนที่ 2 การลงนามเพื่อรับรองวันและเวลาลงนาม ดังภาพที่ 5 ส่วนการลงนามเพื่อรับรองตำแหน่งงานมีขั้นตอนการดำเนินการที่แตกต่างกันในส่วนของการเลือกใช้กุญแจของแต่ละรูปแบบ ส่วนการลงนามเพื่อรับรองวันและเวลาในการลงนามของทั้ง 3 วิธีการจะมีขั้นตอนการดำเนินการที่เหมือนกัน ดังนี้



ภาพที่ 5 เปรียบเทียบขั้นตอนการลงลายมือชื่อดิจิทัลตามตำแหน่งงานของแต่ละวิธีการ

ส่วนที่ 1 ส่วนการลงนามเพื่อรับรองตำแหน่งงานด้วยวิธีการแบบกุญแจแยกส่วนจะใช้กุญแจจำนวน 2 ดอก ในการลงนามโดยดอกแรกคือกุญแจส่วนบุคคล ดอกที่สองคือกุญแจตามตำแหน่งงานที่ออกในนามหน่วยงาน ทำให้ผู้ที่ได้รับเอกสารที่ทำการลงนามสามารถตรวจสอบยืนยันตัวบุคคลและหน่วยงานที่ลงนามได้ทันที แต่ทั้งนี้การตรวจสอบวาระในการดำรงตำแหน่งต้องตรวจสอบผ่านระบบของหน่วยงานที่ออกเอกสาร โดยขั้นตอนการลงนามเริ่มจากผู้ใช้งานสร้างเอกสารที่ต้องการลงลายมือชื่อดิจิทัล จากนั้นส่งการร้องขอลงนามผ่านระบบบริหารจัดการการลงนามดิจิทัล (Sign System)(1.1) ระบบบริหารจัดการการลงนามดิจิทัลนำเอกสารที่ได้รับมาผ่านฟังก์ชันทางคณิตศาสตร์ที่เรียกว่า แฮชฟังก์ชัน (Hash Functions) เพื่อให้ได้รหัสจำเพาะของข้อความตั้งต้นเรียกว่า เมสเซสไดเจสต์ (Message Digest) ส่งกลับให้ผู้ใช้งาน พร้อมร้องขอลายมือชื่อดิจิทัล (1.2) จากนั้นเป็นขั้นตอนการเลือกกุญแจส่วนบุคคลเพื่อลงลายมือชื่อดิจิทัลยืนยันตัวบุคคล (1.3) เมื่อระบบบริหารจัดการการลงนามดิจิทัลได้รับเอกสารตัวแทนที่ผ่านการลงลายมือชื่อดิจิทัลของบุคคล (1.4) จะทำการร้องขอการลงลายมือชื่อตามตำแหน่งงานเป็นลำดับถัดไป (1.5) ผู้ใช้งานทำการเลือกกุญแจประจำตำแหน่งงานที่ต้องการลงนาม (1.6) ระบบบริหารจัดการการลงนามดิจิทัลได้รับเอกสารตัวแทนที่ผ่านการลงลายมือชื่อดิจิทัลตามตำแหน่งงานของบุคคล (1.7) เป็นอันสิ้นสุดขั้นตอนในส่วนที่หนึ่งของวิธีการกุญแจแยกส่วน สำหรับวิธีการกุญแจตัวแทนนั้นจะมีความแตกต่างจากกุญแจแยกส่วนคือการเลือกกุญแจสำหรับใช้งานจะดำเนินการเพียงครั้งเดียวเท่านั้น โดยการใช้กุญแจที่ออกในนามหน่วยงานและมีการผูกความสัมพันธ์ตามตำแหน่งงานกับผู้ใช้งานไว้เรียบร้อยแล้วในการลงนาม ทำให้ลดขั้นตอนในการลงนาม แต่ยังคงมีความยุ่งยากในการเลือกหยิบกุญแจให้ถูกต้องตามตำแหน่งงานที่ต้องการและในส่วนของการตรวจสอบเอกสารโดยผู้รับสามารถตรวจสอบความถูกต้องของหน่วยงานที่ออกเอกสารได้ในทันที แต่ยังไม่สามารถยืนยันตัวตนบุคคลที่ลงนามและวาระในการดำรงตำแหน่งของบุคคลได้ต้องส่งเอกสารที่ได้รับไปตรวจสอบกับระบบตรวจสอบเอกสารของหน่วยงานที่ออกเอกสารเพื่อยืนยันความถูกต้อง ส่วนวิธีการกุญแจหลักจะมีการใช้กุญแจเพียงดอกเดียวคือกุญแจส่วนบุคคลในการลงนามสำหรับทุกตำแหน่งงานทำให้ลดขั้นตอนในการลงนาม พร้อมทั้งลดข้อผิดพลาดจากการหยิบกุญแจผิดดอกมาใช้งานและเอกสารที่ลงนามสามารถยืนยันตัวตนของบุคคลที่ลงนามได้ในทันที แต่ทั้งนี้การตรวจสอบวาระในการดำรงตำแหน่งและหน่วยงานที่ออกเอกสารต้องตรวจสอบผ่านระบบของหน่วยงานที่ออกเอกสาร

ส่วนที่ 2 ส่วนการลงนามเพื่อรับรองวันและเวลาในการลงนาม ทั้ง 3 วิธีการจะมีขั้นตอนการดำเนินการเหมือนกันเนื่องจากเป็นขั้นตอนการขอให้รับรองวันและเวลาจากระบบตราประทับเวลากลางที่จัดตั้งขึ้นเพื่อลดข้อผิดพลาดทางด้านเวลาที่ไม่ตรงกัน โดยการร้องขอเริ่มจากระบบบริหารจัดการการลงนามดิจิทัลทำการร้องขอตราประทับเวลาเพื่อขอรับรองวันและเวลาในการลงลายมือชื่อไปที่ระบบประทับเวลาอิเล็กทรอนิกส์ (Timestamp Sign System)(2.1) จากนั้นระบบประทับเวลาอิเล็กทรอนิกส์ทำการลงลายมือชื่อด้วยกุญแจส่วนตัวของระบบตราประทับเวลา (Timestamp Private Key)(2.2) เมื่อระบบบริหารจัดการการลงนามดิจิทัลได้รับเอกสารตัวแทนที่ผ่านการลงตราประทับเวลา (2.3) จะทำการประกอบเอกสารที่ผ่านการลงลายมือชื่อดิจิทัลตามตำแหน่งงาน (2.4) เป็นอันเสร็จสิ้นกระบวนการ

จากการออกแบบกระบวนการลงลายมือชื่อดิจิทัลทั้ง 3 รูปแบบสามารถเปรียบเทียบการออกแบบกระบวนการทั้ง 3 รูปแบบในประเด็นหลักๆ – ประเด็นคือ 1) ขั้นตอนการลงทะเบียน 2) การลงลายมือตามตำแหน่งงาน และ 3) การตรวจสอบการลงลายมือชื่อตามตำแหน่งงาน ได้ดังตารางที่ 1

ตารางที่ 1 การเปรียบเทียบการใช้กุญแจลงลายมือชื่อดิจิทัลตามตำแหน่งงานของแต่ละวิธีการ

วิธีการ / ประเด็นพิจารณา	**กุญแจแยกส่วน** (Divide Key)	**กุญแจตัวแทน** (Delegate Key)	**กุญแจหลัก** (Personal Key)
ขั้นตอนการลงทะเบียน			
จำนวนกุญแจอิเล็กทรอนิกส์	ต้องมีกุญแจอย่างน้อย 2 ดอก ขึ้นกับตำแหน่งงานที่รับผิดชอบ	ต้องมีกุญแจอย่างน้อย 1 ดอก ขึ้นกับตำแหน่งงานที่รับผิดชอบ	กุญแจ 1 ดอกสำหรับใช้ในการลงนามทุกตำแหน่งงาน
การรับมอบกุญแจประจำตำแหน่ง	**ยุ่งยาก** ต้องทำการรับมอบกุญแจประจำตำแหน่งเท่ากับตำแหน่งที่ได้รับทุกครั้ง	**ยุ่งยาก** ต้องทำการรับมอบกุญแจประจำตำแหน่งเท่ากับตำแหน่งที่ได้รับทุกครั้ง	**สะดวก** ใช้กุญแจส่วนบุคคลเพื่อรับมอบตำแหน่งเพียงครั้งเดียว ส่วนตำแหน่งอื่นสามารถดำเนินการทางออนไลน์ได้
การลงลายมือชื่อตามตำแหน่งงาน			
ขั้นตอนการลงนาม	**3 ขั้นตอน :** ขั้นตอนที่ 1 ต้องเลือกกุญแจที่ถูกต้องสำหรับแต่ละขั้นตอน ขั้นตอนที่ 2 ลงนามด้วยกุญแจส่วนบุคคล ขั้นตอนที่ 3 ลงนามด้วยกุญแจประจำตำแหน่งที่ต้องการ	**2 ขั้นตอน :** ขั้นตอนที่ 1 ต้องเลือกกุญแจประจำตำแหน่ง ขั้นตอนที่ 2 ลงนามด้วยกุญแจประจำตำแหน่งที่ต้องการ	**1 ขั้นตอน :** ลงนามด้วยกุญแจส่วนบุคคล
ความผิดพลาดที่เกิดจากการลงนามโดยผู้ใช้งาน	**มีโอกาสเกิดขึ้นสูง** เนื่องจากผู้ใช้งานต้องนำกุญแจส่วนบุคคลและกุญแจประจำตำแหน่งมาใช้งานให้ตรงกับเอกสารที่จะลงลายมือชื่อ	**มีโอกาสเกิดขึ้นปานกลาง** เนื่องจากผู้ใช้งานต้องนำกุญแจประจำตำแหน่งมาใช้งานให้ตรงกับเอกสารที่จะลงลายมือชื่อ	**โอกาสผิดพลาดต่ำ** เนื่องจากลงนามด้วยกุญแจส่วนบุคคล
ความน่าเชื่อถือของกุญแจที่ใช้ในการลงนาม	**มีความน่าเชื่อถือสูง** เนื่องจากออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือและได้รับการยอมรับ	**มีความน่าเชื่อถือสูง** เนื่องจากออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือและได้รับการยอมรับ	**มีความน่าเชื่อถือสูง** เนื่องจากออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือและได้รับการยอมรับ
การตรวจสอบการลงลายมือชื่อตามตำแหน่งงาน			
การตรวจสอบความน่าเชื่อถือของเอกสารด้วยใบรับรองอิเล็กทรอนิกส์	**น่าเชื่อถือสูง** เนื่องจากมีการใช้กุญแจที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certificate Authority) ที่น่าเชื่อถือจำนวน 2 ดอก ในการตรวจสอบเอกสาร ทำให้สามารถยืนยันตัวบุคคล และหน่วยงานที่ลงนามได้ทันที	**น่าเชื่อถือปานกลาง** เนื่องจากมีการใช้กุญแจที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certificate Authority) ที่น่าเชื่อถือจำนวน 1 ดอก ในการตรวจสอบเอกสาร ทำให้สามารถยืนยันหน่วยงานที่ลงนามได้	**น่าเชื่อถือต่ำ** เนื่องจากมีการใช้กุญแจที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certificate Authority) ที่น่าเชื่อถือจำนวน 1 ดอก ในการตรวจสอบเอกสาร ทำให้สามารถยืนยันตัวบุคคลได้เท่านั้น
การใช้ระบบตรวจสอบความถูกต้องของเอกสาร (Backend)	**จำเป็น** เนื่องจากต้องตรวจสอบวาระในการดำรงตำแหน่งว่าถูกต้องหรือไม่	**จำเป็น** เนื่องจากต้องตรวจสอบบุคคลและวาระในการดำรงตำแหน่งว่าถูกต้องหรือไม่	**จำเป็น** เนื่องจากต้องตรวจสอบหน่วยงาน และวาระในการดำรงตำแหน่งว่าถูกต้องหรือไม่

การออกแบบทั้ง 3 วิธีการ มีข้อดีและข้อเสียที่แตกต่างกันโดย 1) วิธีการกุญแจแยกส่วนขั้นตอนในการลงนามจะมีโอกาสเกิดความผิดพลาดในการนำกุญแจมาใช้งานได้สูงหากบุคคลดำรงหลายตำแหน่งงานในช่วงเวลาเดียวกัน แต่ทั้งนี้ในการตรวจสอบความถูกต้องของเอกสารจากบุคคลที่ได้รับเอกสารสามารถตรวจสอบตัวตนผู้ลงนามและหน่วยงานที่ลงนามในเอกสารได้ชัดเจนมากที่สุด 2) วิธีการกุญแจตัวแทนจะมีข้อดีที่ผู้รับเอกสารสามารถตรวจสอบรายละเอียดหน่วยงานที่ออก

เอกสารได้ทันที แต่จะมีปัญหาในส่วนการเลือกใช้งานกุญแจประจำตำแหน่งงานซึ่งจะมีจำนวนดอกเท่ากับจำนวนตำแหน่งงานของบุคคล และ 3) วิธีการกุญแจหลักมีการใช้กุญแจส่วนบุคคลเพียงดอกเดียวในการลงนามเอกสารในทุกตำแหน่งงานของบุคคลช่วยอำนวยความสะดวกให้กับผู้ใช้งาน สามารถลดข้อผิดพลาดที่เกิดจากการใช้กุญแจผิดดอกในการลงนามจะสามารถยืนยันได้ว่าบุคคลใดที่ลงนามในเอกสารแต่จะไม่ทราบหน่วยงาน ทั้ง 3 วิธีการหากต้องการตรวจสอบความถูกต้องของเอกสารที่ลงนามตามตำแหน่งงานจำเป็นต้องส่งเอกสารกลับมาตรวจสอบที่ระบบตรวจสอบความถูกต้องของหน่วยงานทั้งสิ้น เนื่องจากการตรวจสอบเบื้องต้นจะไม่ทราบถึงวาระในการครองตำแหน่งงานของแต่ละบุคคล ดังนั้น วิธีที่ 3 ที่ใช้กุญแจหลักจึงเป็นวิธีการที่เหมาะสมที่สุดใน 3 วิธี เนื่องจากสามารถลดข้อผิดพลาดในการใช้งานได้ดีที่สุด

การออกแบบขั้นตอนการตรวจสอบการลงลายมือชื่อดิจิทัลตามตำแหน่งงานนี้ ได้นำขั้นตอนกระบวนการต่างๆ ไปนำเสนอเพื่อทดสอบที่หน่วยงานภาครัฐแห่งหนึ่ง โดยให้บุคลากรที่เกี่ยวข้องกับระบบเอกสารอิเล็กทรอนิกส์เป็นผู้ประเมิน พบว่ากระบวนการที่ออกแบบนั้นมีความเหมาะสมและสะดวกในการใช้งาน โดยเฉพาะอย่างยิ่งวิธีที่ 3 การใช้กุญแจหลัก (Personal Master Key) มีความเหมาะสมที่สุด สามารถนำมาพัฒนาเพื่อจัดทำระบบต้นแบบได้ดี เนื่องจากวิธีการไม่ซับซ้อนยุ่งยาก เหมาะกับผู้ใช้งาน อย่างไรก็ตามในเชิงปฏิบัติสำหรับการนำไปใช้จริงนั้นอาจต้องมีการพิจารณาในประเด็นของกฎ ระเบียบที่ต้องพิจารณาการรับรองลายมือชื่ออิเล็กทรอนิกส์แบบอิงตำแหน่งงานต่อไป

นอกจากนี้ยังได้นำไปให้ผู้เชี่ยวชาญด้านระบบสารสนเทศของหน่วยงานภาครัฐจำนวน 3 คนให้ความเป็นและช่วยพิจารณาเลือกวิธีการที่เหมาะสมสำหรับนำไปพัฒนาระบบ โดยควรคำนึงถึงความน่าเชื่อถือของเอกสารที่ลงนามความสะดวกและง่ายต่อการนำไปใช้งาน โดยนำตารางเปรียบเทียบการใช้กุญแจลงลายมือชื่อดิจิทัลตามตำแหน่งงานของแต่ละวิธีการ (ตารางที่ 1) มาพิจารณาเลือกวิธีการที่เหมาะสมดังตารางที่ 2 โดยแต่ละประเด็นที่พิจารณาจะมีการกำหนดคะแนน 1 – 10 คะแนน โดยกำหนดเป็น 3 ช่วงคะแนน ช่วงที่ 1) คะแนน 1-3 คะแนน เป็นช่วงคะแนนสำหรับผลประเมินที่เป็นลบ ไม่เป็นที่ยอมรับ หรือควรปรับปรุง ช่วงที่ 2) คะแนนระหว่าง 4-7 คะแนน เป็นช่วงคะแนนสำหรับผลประเมินอยู่ในระดับปานกลาง ยอมรับได้ และช่วงที่ 3) คะแนนระหว่าง 8-10 คะแนน เป็นช่วงคะแนนสำหรับผลประเมินที่เป็นบวก หรืออยู่ในเกณฑ์ที่ดีมาก

นอกจากนี้ยังมีการให้น้ำหนักในแต่ละหัวข้อหลักของประเด็นที่ไม่เท่ากันพิจารณาจากความสำคัญและการนำไปใช้งานได้จริง การวิจัยนี้ได้ให้น้ำหนักในขั้นตอนการลงลายมือชื่อและการตรวจสอบการลงลายมือชื่อตามตำแหน่งงานมีน้ำหนักมาก เนื่องจากเกี่ยวข้องกับความน่าเชื่อถือของเอกสารตามที่ได้รับคำแนะนำของผู้เชี่ยวชาญ โดยกำหนดให้ขั้นตอนการลงทะเบียนร้อยละ 20 เนื่องจากจะดำเนินการเมื่อเริ่มต้นใช้งานระบบเท่านั้นหลังจากนั้นจะมีการดำเนินการก็ต่อเมื่อมีการเลื่อนระดับ หรือรับมอบหมายตำแหน่งงาน ส่วนการลงลายมือชื่อตามตำแหน่งงานให้ร้อยละ 40 โดยน้ำหนักของขั้นตอนการลงนามมีน้ำหนักเป็น 2 เท่าของประเด็นอื่นๆ และส่วนการตรวจสอบการลงลายมือชื่อตามตำแหน่งงานร้อยละ 40 มีน้ำหนักที่เท่ากันในแต่ละประเด็น

เมื่อนำคะแนนจากผู้เชี่ยวชาญในแต่ละประเด็นมาคิดคะแนนรวมแต่ละหัวข้อพิจารณาตามน้ำหนักที่ระบุได้ผลลัพธ์ดังตารางที่ 2

ตารางที่ 2 ตารางแสดงผลการเปรียบเทียบการลงลายมือชื่อดิจิทัลตามตำแหน่งงานของแต่ละวิธีการโดยการให้น้ำหนักในแต่ละประเด็น

ประเด็นพิจารณาในแต่ละขั้นตอน / วิธีการ		กุญแจแยกส่วน (Divide Key)			กุญแจตัวแทน (Delegate Key)			กุญแจหลัก (Personal Key)		
		ผู้ทำแบบประเมิน			ผู้ทำแบบประเมิน			ผู้ทำแบบประเมิน		
		1	2	3	1	2	3	1	2	3
ขั้นตอนการลงทะเบียน		**น้ำหนักในการพิจารณา 20**								
1	จำนวนกุญแจอิเล็กทรอนิกส์ (1)	3	3	3	7	3	3	10	8	10
2	การรับมอบกุญแจประจำตำแหน่ง (1)	5	3	1	7	3	1	10	8	10
คะแนนเฉลี่ยที่ได้เมื่อเทียบจากน้ำหนักในการพิจารณา		**6.00**			**8.00**			**18.67**		
การลงลายมือชื่อตามตำแหน่งงาน		**น้ำหนักในการพิจารณา 40**								
3	ขั้นตอนการลงนาม (2)	3	3	3	8	5	3	10	8	10
4	ความผิดพลาดที่เกิดจากการลงนามโดยผู้ใช้งาน (1)	6	3	3	8	5	3	10	8	10
5	ความน่าเชื่อถือของกุญแจที่ใช้ในการลงนาม (1)	10	8	8	9	8	7	8	8	6
คะแนนเฉลี่ยที่ได้เมื่อเทียบจากน้ำหนักในการพิจารณา		**18.67**			**24.00**			**35.33**		
การตรวจสอบการลงลายมือชื่อตามตำแหน่งงาน		**น้ำหนักในการพิจารณา 40**								
6	การตรวจสอบความน่าเชื่อถือของเอกสารด้วยใบรับรองอิเล็กทรอนิกส์ (2)	10	8	8	9	5	7	8	3	6
7	การใช้ระบบ (Backend) ตรวจสอบความถูกต้องของเอกสาร (2)	8	8	8	7	5	8	7	3	8
คะแนนเฉลี่ยที่ได้เมื่อเทียบจากน้ำหนักในการพิจารณา		**33.33**			**27.33**			**23.33**		
คะแนนเฉลี่ยที่ได้จากเต็มหนึ่งร้อย		**58.00**			**59.33**			**77.33**		

จากตารางที่ 2 แสดงให้เห็นว่าผู้เชี่ยวชาญทั้ง 3 ให้คะแนนโดยรวมมีความสอดคล้องกัน ถึงแม้บางประเด็นจะมีข้อคิดเห็นที่ไม่ไปในทางเดียวกัน เช่น ในประเด็นพิจารณาที่ 2 ผู้เชี่ยวชาญจำนวน 1 ท่าน ให้คะแนนผลประเมินกุญแจแยกส่วนและกุญแจตัวแทนเพียง 1 คะแนน เนื่องจากผู้เชี่ยวชาญเกี่ยวข้องกับการนำระบบไปใช้งานที่พิจารณาในมิติของผู้ใช้งานเป็นหลัก จึงมีความคิดเห็นว่ามีความเป็นไปได้สูงที่ผู้ใช้งานที่มีการถือกุญแจมากกว่า 1 ดอก จะเกิดการผิดพลาดของการเลือกใช้งานกุญแจผิดดอก จึงให้คะแนนในแง่ลบ อย่างไรก็ตามเมื่อมีการอภิปรายเพิ่มเติมหลังจากการแสดงความคิดเห็นก็เข้าใจและยอมรับแนวทางดังกล่าว ส่วนในประเด็นพิจารณาที่ 6 และ 7 มีผู้เชี่ยวชาญ 1 ท่าน ให้คะแนนผลประเมินกุญแจหลักเป็นลบ เนื่องจากคิดเห็นว่าหากใช้กุญแจส่วนบุคคลเพียงดอกเดียวในการดำเนินการจะสามารถตรวจสอบเพื่อยืนยันตัวบุคคลได้เท่านั้น ไม่สามารถตรวจสอบเบื้องต้นถึงหน่วยงานที่ออกเอกสารได้ในทันที แต่ผู้เชี่ยวชาญอีก 2 ท่าน มีความคิดเห็นว่าการจะเลือกวิธีการกุญแจรูปแบบใดก็ตาม จำเป็นต้องมีการส่งเอกสารเพื่อตรวจสอบผ่านระบบตรวจสอบความถูกต้องของเอกสาร (Backend) ตามระเบียบที่ต้องปฏิบัติของหน่วยงาน เพื่อยืนยันว่าเอกสารออกจากหน่วยงานนั้นๆ และวาระในการดำรงตำแหน่งของผู้ออกเอกสารถูกต้องจริงทำให้คะแนนที่ได้เป็นแง่บวก

จากคะแนนในประเด็นต่างๆ รวมทั้งคะแนนรวมทำได้สามารถสรุปในเบื้องต้นได้ว่า

วิธีการที่ 3 กุญแจหลัก (Personal Key) ซึ่งได้รับคะแนนร้อยละ 77.33 ซึ่งสูงกว่าวิธีการอื่นๆ มีความเหมาะสมที่จะนำไปใช้ในการพัฒนาต้นแบบระบบเอกสารอิเล็กทรอนิกส์ขององค์กรภาครัฐต่อไปสำหรับการลงนามตามตำแหน่งงานของหน่วยงานภาครัฐซึ่งมีการดำรงตำแหน่งงานมากว่าหนึ่งตำแหน่งงานต่อบุคคล นอกจากนี้ผู้เชี่ยวชาญยังให้ข้อเสนอเพิ่มเติมถึงการนำวิธีการกุญแจแยกส่วนนำไปใช้งานกับหน่วยงานที่มีบุคคลดำรงตำแหน่งงานเพียง 1 ตำแหน่ง เนื่องจากผู้รับเอกสารสามารถตรวจสอบผู้ลงนามเอกสารและหน่วยงานได้ทันที แต่ทั้งนี้ต้องพิจารณาถึงงบประมาณที่ใช้ในการดำเนินการประกอบด้วย

สรุปและอภิปรายผล

การวิจัยพบว่าการบริหารจัดการการลงลายมือชื่อตามตำแหน่งงานของประเทศไทยมีปัจจัยที่ต้องพิจารณาหลายประการทั้งในด้านเทคโนโลยีพื้นฐานกุญแจสาธารณะ (PKI) ซึ่งมีวิธีการจัดเก็บกุญแจส่วนตัวที่เรียกว่า Public Key Cryptography Standards (PKCS) 15 รูปแบบการเลือกมาใช้งานต้องพิจารณาถึงความน่าเชื่อถือความปลอดภัย ความสะดวกของผู้ใช้งาน และการรองรับการเชื่อมต่อกับแอพพลิเคชั่นหรือระบบที่จะนำไปใช้งานประกอบกัน นอกจากนี้ในทางปฏิบัติจะมีประเด็นเรื่องการมอบหมายอำนาจในการลงนามตามตำแหน่งงานซึ่งบุคคลหนึ่งๆ อาจมีได้หลายบทบาท เนื่องจากสามารถปฏิบัติหน้าที่ได้มากกว่าหนึ่งตำแหน่งงาน ณ เวลาเดียวกัน มีวาระการครองตำแหน่งงานที่ไม่เท่ากันในแต่ละตำแหน่งงาน สามารถมีการแต่งตั้งเพื่อปฏิบัติหน้าที่แทนหรือรักษาการแทนได้ การเพิกถอนออกจากตำแหน่งก่อนหมดวาระตามตำแหน่งงาน รวมทั้งการลงนามต้องกระทำในวันและเวลาราชการเท่านั้น

กระบวนการกุญแจหลักที่ออกแบบมีระบบบริหารจัดการใบรับรองอิเล็กทรอนิกส์ตามตำแหน่งงานในลักษณะรวมศูนย์เพื่อควบคุมสิทธิ์การลงนามตามตำแหน่งงาน สามารถตรวจสอบข้อมูลการลงนามได้อย่างครอบคลุม และมีระบบตราประทับเวลาอิเล็กทรอนิกส์เป็นระบบจัดเก็บข้อมูลวันและเวลา เพื่อรักษาความถูกต้องและเป็นมาตรฐานเวลาในการอ้างอิงเดียวกันทั้งระบบงาน นอกจากนี้ การใช้กุญแจส่วนบุคคลเพียงดอกเดียวในการลงนามเอกสารทำให้สะดวกและรวดเร็วต่อการใช้งานของผู้ปฏิบัติงาน สามารถยืนยันตัวตนบุคคลที่ลงนามในเอกสาร โดยที่บุคคลนั้นไม่สามารถปฏิเสธความรับผิดชอบต่อการลงนามได้ ตามพระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ จึงสามารถนำไปประยุกต์ใช้งานกับระบบเอกสารอิเล็กทรอนิกส์แบบไร้กระดาษได้

เอกสารอ้างอิง

[1] ราชกิจจานุเบกษา. (2544, 4 ธันวาคม). พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔. เล่ม 118 ตอนที่ 112 ก, หน้า 27.

[2] ประเภทบริการ CAT CA. (2559). สืบค้นจาก http://www.thaipki.com/service.html

[3] ประเภทการให้บริการของ TOT CA. (2559). สืบค้นจาก http://www.ca.tot.co.th/Default.aspx?tabid=7810

[4] Public Key Cryptography Standards. (2016). Retrieved from https://en.wikipedia.org/wiki/PKCS

[5] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2559). กฎหมายธุรกรรมทางอิเล็กทรอนิกส์. สืบค้นจาก http://www.mict.go.th/view/1/%E0%B8%82%E0%B9%88%E0%B8%B2%E0%B8%A7%E0%B8%81%E0%B8%A3%E0%B8%B0%E0%B8%97%E0%B8%A3%E0%B8%A7%E0%B8%87%E0%B8%AF/102

[6] มานพ วงศ์สายสุวรรณ; และ แก้ว ปุณฑริกโกทก. (2558). ระบบสารบรรณอิเล็กทรอนิกส์ LessPaper จุฬาลงกรณ์มหาวิทยาลัย. สืบค้นจาก http://www.cca.chula.ac.th/edocuments/manual.html

[7] บริษัท อีออฟฟิศออนไลน์ จำกัด. (2559). ระบบสารบรรณอิเล็กทรอนิกส์. สืบค้นจาก http://www.thsaraban.com

[8] Public Key Infrastructure. (2016). Retrieved from https://en.wikipedia.org/wiki/Public_key_infrastructure

[9] Ćosić, J. and Bača, M. (2010). (im)proving chain of custody and digital evidence integrity with time stamp. Proceedings of the 33rd International Convention MIPRO, Opatija, Croatia, pp. 1226-1230.

[10] Kakei, S., Mohri, M., Shiraishi, Y. and Noguchi, R. (2012). Offline time-stamping using TPM and its Java library. In 2012 International Symposium on Computer Applications and Industrial Electronics (ISCAIE), IEEE. pp. 64-69.

[11] Goswami, S., Misra, S. and Mukesh, M. (2014). A PKI based timestamped secure signing tool for e-documents. In High Performance Computing and Applications (ICHPCA), 2014 International Conference on, IEEE, pp. 1-6.

[12] พรชัย นพประโคน. (2555). การประทับตราเวลา: ความจำเป็นในการให้บริการ พาณิชย์อิเล็กทรอนิกส์และพระราชบัญญัติว่าด้วย ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔. *Thai Journal of Science and Technology*. (1): 1-12.