Data Management
การประยุกต์ใช้งานลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) ในภาครัฐ

ที่มา : วารสารมหาวิทยาลัยศรีนครินทรวิโรฒ (สาขาวิทยาศาสตร์และเทคโนโลยี)
ปีที่ 9 ฉบับที่ 17 มกราคม - มิถุนายน 2560

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

หน่วยงานของรัฐมีการบริหารงานแบบลำดับชั้นต้องการนำระบบการ ลงลายมือชื่อดิจิทัลมาใช้ทดแทนการลงนามเอกสารแบบเดิมจำเป็นต้องคำนึงถึงระดับชั้นตามความสำคัญของตำแหน่งงาน ช่วงเวลาการดำรงตำแหน่งหรือการปฏิบัติหน้าที่แทนบุคลากรหนึ่งคนสามารถดำรงตำแหน่งได้หลายตำแหน่งในคราวเดียวกัน ดังนั้นการออกแบบและสร้างใบรับรองอิเล็กทรอนิกส์ที่เป็นส่วนตัวของผู้ใช้งาน และใบรับรองอิเล็กทรอนิกส์ที่ใช้แทนตราประทับประจำตำแหน่งจึงมีความสำคัญเป็นอย่างยิ่ง ระบบที่ออกแบบต้องสามารถป้องกันการปลอมแปลงข้อมูลตำแหน่งงาน และสามารถเปลี่ยนแปลงตำแหน่งงานให้เป็นไปตามกฎระเบียบของหน่วยงาน เช่น การแต่งตั้งการเพิกถอน และการมอบหมายรักษาการแทน เป็นต้น

ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) หมายถึง ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใดซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ ซึ่งออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority : CA) ที่มีความน่าเชื่อถือ แบ่งเป็น 3 ประเภท คือ

- ใบรับรองตัวบุคคล (Personal Certificate)
- ใบรับรองสำหรับนิติบุคคล องค์กรหรือหน่วยงาน (Enterprise Certificate)
- ใบรับรองเครื่องให้บริการเว็บ (SSL Certificate)

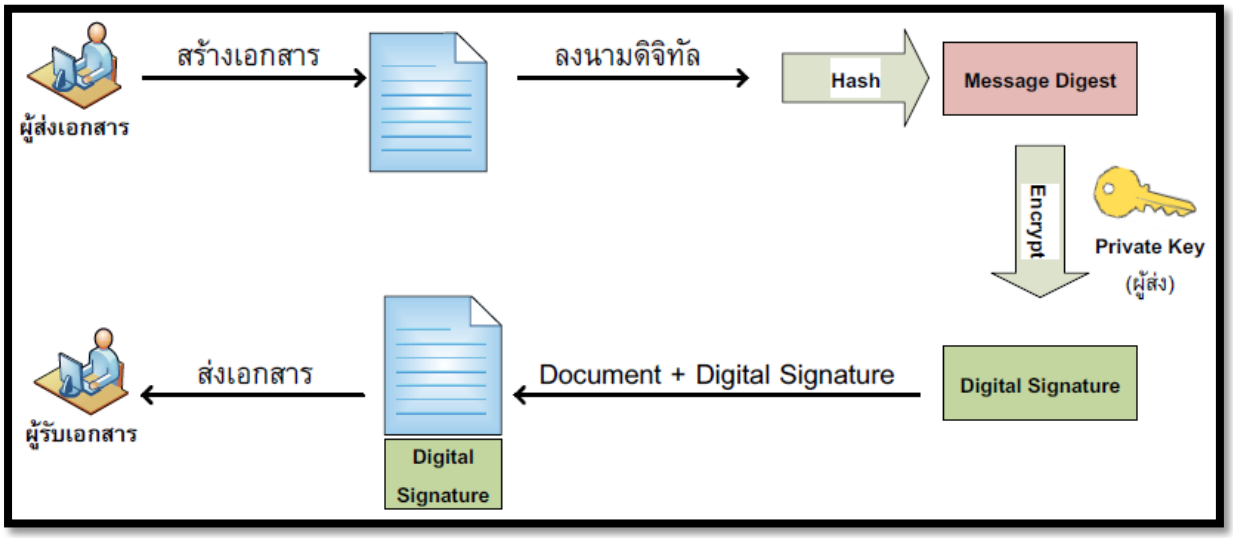
หมายเหตุ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แต่ละรายจะสร้างใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน (Public Key Cryptography Standards: PKCS) ซึ่งเป็นมาตรฐานการเข้ารหัสข้อความ เป็นใบรับรองอิเล็กทรอนิกส์ที่อยู่ในรูปแบบ Token Interface ซึ่งอาจจะเป็นอุปกรณ์ที่เชื่อมต่อผ่าน API ของซอฟต์แวร์คอมพิวเตอร์ เป็นการจัดเก็บ private key พร้อมPublic key ในรูปแบบไฟล์โดยป้องกันด้วยรหัสผ่านที่แบบสมมาตร (Symmetric key) เป็นต้น

ลายมือชื่อดิจิทัล (Digital Signature) เป็นลายมือชื่ออิเล็กทรอนิกส์อย่างหนึ่ง ซึ่งเป็น อักษร อักขระหรือสัญลักษณ์ที่สร้างขึ้นโดยโปรแกรมคอมพิวเตอร์โดยอาศัยเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI) หรือ อาจใช้วิธีการจัดการกุญแจแบบ PGP (Pretty Good Privacy) โดยที่ทั้งสองวิธีการนั้นพัฒนาขึ้นจากการเข้ารหัสลับ (Cryptography) จึงทำให้มีคุณสมบัติในการสร้างและตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ได้เป็นที่ยอมรับ ประกอบด้วย

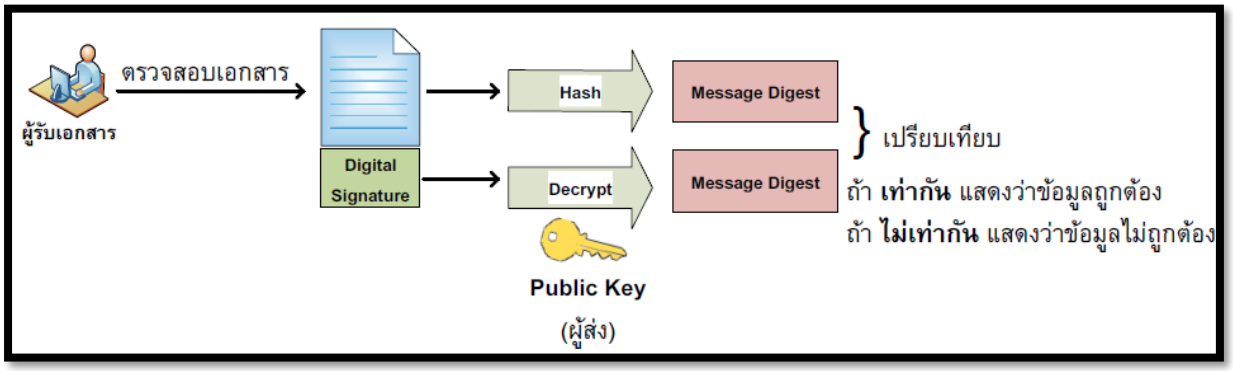
- **Signer Authentication** เป็นความสามารถในการพิสูจน์ว่าใครเป็นคนเซ็นเอกสาร ตัวลายเซ็นจะสามารถใช้ในการเชื่อมโยงไปยังบุคคลที่เซ็นเอกสารได้
- **Data Integrity** เป็นความสามารถในการตรวจสอบ หรือพิสูจน์ได้ว่ามีการแก้ไขเอกสารหลังจากที่ได้มีการเซ็นไปแล้วหรือไม่

- **Non-repudiation** การไม่สามารถปฏิเสธความรับผิดชอบได้ เนื่องจากลายเซ็นที่สร้างขึ้นมีเอกลักษณ์สามารถพิสูจน์ในชั้นศาลได้ว่าใครเป็นผู้เซ็นเอกสาร

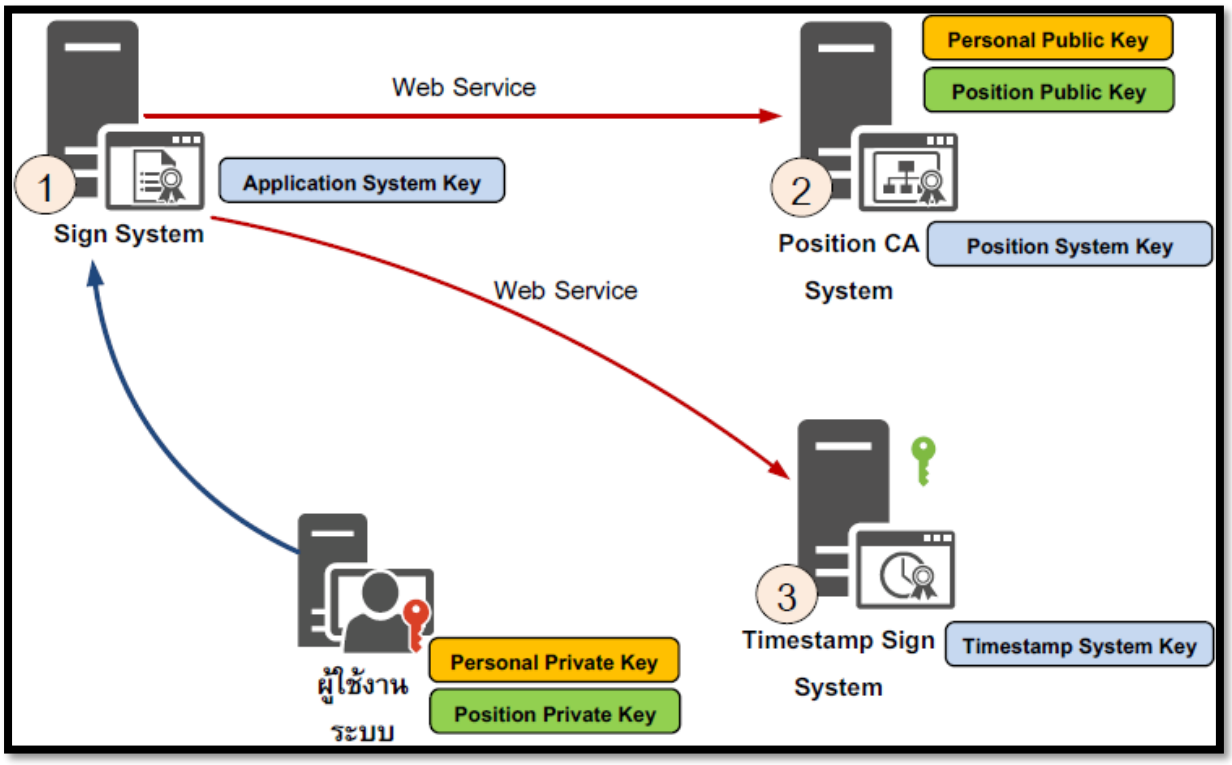
ขั้นตอนการลงลายมือชื่อดิจิทัล



การตรวจสอบการลงลายมือชื่อดิจิทัล



กระบวนการลงลายมือชื่อดิจิทัลตามตำแหน่งงาน



กระบวนการลงลายมือชื่อดิจิทัลตามตำแหน่งงาน

1. **ระบบบริหารจัดการการลงนามดิจิทัล (Sign System)** สำหรับควบคุมขั้นตอนการลงนามเอกสารอิเล็กทรอนิกส์และตรวจสอบความถูกต้องของการลงนามเอกสาร
2. **ระบบบริหารจัดการสิทธิ์ตามตำแหน่งงาน (Position based CA System)** ทำหน้าที่จัดเก็บความสัมพันธ์ระหว่างบุคคล หน่วยงาน ตำแหน่งงาน ช่วงเวลาที่ปฏิบัติงาน และกุญแจสาธารณะของบุคคล เพื่อให้รองรับการตรวจสอบสิทธิ์ในการลงนามเอกสารตามตำแหน่งงานได้อย่างถูกต้องและน่าเชื่อถือและสามารถจัดเก็บข้อมูลการลงนามในกรณีปฏิบัติหน้าที่แทนได้
3. **ระบบประทับเวลาอิเล็กทรอนิกส์ (Timestamp Sign System)** สำหรับรองรับวันและเวลาในการลงนามดิจิทัลเพื่อให้เป็นมาตรฐานเวลาเดียวกันทั้งระบบงาน

กฎหมายที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์

ที่มา : สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
https://www.etcommission.go.th

1. **ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) พ.ศ. 2552**

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และ
แนวปฏิบัติ (Certification Practice Statement)
ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority)
พ.ศ. ๒๕๕๒

เพื่อให้การให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์มีความน่าเชื่อถือ คลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงเห็นควรกำหนดแนวทางในการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority)

อาศัยอำนาจตามความในมาตรา ๒๘ (๖) มาตรา ๒๖ (๗) และมาตรา ๓๗ (๔) แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) จัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ตามแนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) ท้ายประกาศนี้

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๙ ตุลาคม พ.ศ. ๒๕๕๒
ร้อยตรีหญิง ระนองรักษ์ สุวรรณฉวี
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

2. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551

พระราชบัญญัติ

ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒)

พ.ศ. ๒๕๕๑

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๖ กุมภาพันธ์ พ.ศ. ๒๕๕๑

เป็นปีที่ ๖๓ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้เพิ่มความต่อไปนี้เป็นวรรคสองของมาตรา ๔ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

3. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

มาตรา ๙ ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

(๑) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(๒) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

วิธีการที่เชื่อถือได้ตาม (๒) ให้คำนึงถึง

ก. ความมั่นคงและรัดกุมของการใช้วิธีการหรืออุปกรณ์ในการระบุตัวบุคคล สภาพพร้อมใช้งานของทางเลือกในการระบุตัวบุคคล กฎเกณฑ์เกี่ยวกับลายมือชื่อที่กำหนดไว้ในกฎหมายระดับความมั่นคงปลอดภัยของการใช้ลายมือชื่ออิเล็กทรอนิกส์ การปฏิบัติตามกระบวนการในการระบุตัวบุคคลผู้เป็นสื่อกลาง ระดับของการยอมรับหรือไม่ยอมรับ วิธีการที่ใช้ในการระบุตัวบุคคลในการทำธุรกรรม วิธีการระบุตัวบุคคล ณ ช่วงเวลาที่มีการทำธุรกรรมและติดต่อสื่อสาร

ข. ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ จำนวนครั้งหรือความสม่ำเสมอในการทำธุรกรรม ประเพณีทางการค้าหรือทางปฏิบัติ ความสำคัญ มูลค่าของธุรกรรมที่ทำ หรือ

ค. ความรัดกุมของระบบการติดต่อสื่อสาร[๗]

ให้นำความในวรรคหนึ่งมาใช้บังคับกับการประทับตราของนิติบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์ ด้วยโดยอนุโลม[๘]