มสพร./DD
มกราคม ๒๕๖๕

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัลอยู่ระหว่างการจัดทำ
ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน
มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัลฉบับสมบูรณ์จะมีประกาศโดย
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ร่าง

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล
DGA Community Standard

ว่าด้วยแนวปฏิบัติการลงลายมืออิเล็กทรอนิกส์ สำหรับเจ้าหน้าที่ของรัฐ

GUIDELINE ON E-SIGNATURE FOR GOVERNMENT OFFICIAL

สำหรับคณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ชั้น ๑๗ อาคารบางกอกไทยทาวเวอร์ ๑๐๘ ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ ๑๐๔๐๐
หมายเลขโทรศัพท์: ๐ ๒๖๑๒ ๖๐๐๐ โทรสาร: ๐ ๒๖๑๒ ๖๐๑๑ ๐ ๒๖๑๒ ๖๐๑๒

สารบัญ

สารบัญตาราง

สารบัญภาพ

คำนำ

ในปัจจุบันการปฏิบัติหน้าที่ในหน่วยงานภาครัฐเพื่อการบริหารราชการแผ่นดินและการให้บริการประชาชน มีความจำเป็นต้องอาศัยกระบวนการหรือการดำเนินงานทางดิจิทัลที่มีประสิทธิภาพ จึงมีความต้องการแนวปฏิบัติพื้นฐานเกี่ยวกับการลงลายมือชื่ออิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัยและน่าเชื่อถือ สามารถใช้เป็นหลักฐานที่สามารถระบุตัวเจ้าของลายมือชื่อ และแสดงเจตนาของเจ้าของลายมือชื่อที่เกี่ยวข้องกับข้อความที่ได้ลงลายมือชื่อ ซึ่งเป็นไปตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

มาตรฐานสำนักงานรัฐบาลดิจิทัล (มสพร.) ว่าด้วยแนวปฏิบัติการลงลายมืออิเล็กทรอนิกส์ สำหรับเจ้าหน้าที่ของรัฐฉบับนี้ ครอบคลุมเนื้อหาเกี่ยวกับกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้องกับการลงลายมือชื่ออิเล็กทรอนิกส์ของเจ้าหน้าที่ภาครัฐ แนวทางการพิจารณาเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ และปัจจัยที่ต้องพิจารณาในการลงลายมือชื่ออิเล็กทรอนิกส์ ประกอบกับรายละเอียดแนวทางการพัฒนาและบริหารจัดการระบบการลงลายมือชื่ออิเล็กทรอนิกส์โดยสังเขป โดยอ้างอิงกรณีศึกษาการใช้ลายมือชื่ออิเล็กทรอนิกส์ในประเทศไทย ๒ กรณีศึกษา ได้แก่ ระบบสารบรรณอิเล็กทรอนิกส์ และระบบออกใบรับรองผลการศึกษา รวมทั้งกรณีศึกษาจากต่างประเทศ ได้แก่ ประเทศเอสโตเนีย ประเทศแคนาดา และประเทศออสเตรเลีย

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล
ว่าด้วยแนวปฏิบัติการลงลายมืออิเล็กทรอนิกส์ สำหรับเจ้าหน้าที่ของรัฐ

๑. ขอบข่าย

มาตรฐานสำนักงานรัฐบาลดิจิทัล (มสพร.) ฉบับนี้นำเสนอเนื้อหาในภาพรวมของการลงลายมือชื่ออิเล็กทรอนิกส์ สำหรับเจ้าหน้าที่ของรัฐ รวมทั้งนำแสนอแนวทางการนำไปปฏิบัติใช้ ซึ่งได้อ้างอิงมาตรฐาน แนวปฏิบัติ และข้อเสนอแนะที่เกี่ยวข้อง ดังนี้

(๑) มาตรฐาน Nist Special Publication 800-57 Part 1 Revision 5 – Recommendation For Key Management: Part 1 – General [๑]

(๒) แนวปฏิบัติ Enisa Security Guidelines On The Appropriate Use Of Qualified Electronic Signatures – Guidance For Users [๒]

(๓) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ขมธอ.) ๒๓-๒๕๖๓ ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ เวอร์ชัน ๑.๐ [๓]

โดยในเอกสารฉบับนี้ฉบับนี้มีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหา เชิงบรรทัดฐาน (Normative) และเนื้อหาเชิงให้ข้อมูล (Informative) มีดังนี้

- “ต้อง” (Shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (Requirement) ที่ต้องปฏิบัติตาม
- “ควร” (Should) ใช้ระบุสิ่งที่เป็นข้อแนะนำ (Recommendation)
- “อาจ” (May) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (Permission)

ทั้งนี้เอกสารฉบับนี้เป็นคำแนะนำโดยทั่วไปซึ่งไม่สามารถครอบคลุมประเด็นทางกฎหมายทั้งหมดที่อาจเกิดขึ้นได้ ดังนั้น ควรมีการปรึกษากับผู้เชี่ยวชาญทางกฎหมายก่อนดำเนินการ

๒. บทนิยาม

ความหมายของนิยามที่ใช้ในมาตรฐานสำนักงานรัฐบาลดิจิทัลฉบับนี้ มีดังนี้

(๑) ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature หรือ E-Signature) หมายถึง อักษร อักขระ ตัวเลข เสียง หรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้นและเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น [๓].

(๒) ลายมือชื่อดิจิทัล (Digital Signature) หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่ถูกสร้างด้วยกุญแจส่วนตัว ในระบบรหัสแบบอสมมาตร (Asymmetric Cryptography) ทำให้สามารถยืนยันความเป็นเจ้าของลายมือชื่อ รวมทั้งตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ รวมถึงทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ [๓]

(๓) กุญแจส่วนตัว (Private Key) หมายถึง กุญแจที่ใช้สร้างลายมือชื่อดิจิทัล ในระบบรหัสแบบอสมมาตร [๔]

(๔) กุญแจสาธารณะ (Public Key) หมายถึง กุญแจที่ใช้ตรวจสอบลายมือชื่อดิจิทัลและเอกสารอิเล็กทรอนิกส์ที่ถูกลงลายมือชื่อ ในระบบรหัสแบบอสมมาตร [๔]

(๕) ใบรับรอง (Certificate) หมายถึง ข้อมูลอิเล็กทรอนิกส์ ซึ่งใช้ยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อเข้ากับกุญแจสาธารณะ รวมถึงข้อมูลอื่น ๆ ที่เกี่ยวข้อง [๔]

(๖) ผู้ให้บริการออกใบรับรอง (Certification Authority: CA) หมายถึง บุคคล หน่วยงาน หรือเครื่องให้บริการ (Server) ที่ให้บริการรับรองกุญแจสาธารณะให้กับผู้ใช้บริการโดยการออกใบรับรองให้กับผู้ใช้บริการ และยังมีหน้าที่บริหารจัดการใบรับรองของผู้ใช้บริการ เช่น เผยแพร่ใบรับรอง เพิกถอนใบรับรอง และเผยแพร่ข้อมูลสำหรับตรวจสอบสถานะใบรับรอง [๔]

(๗) โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) หมายถึง โครงสร้างพื้นฐานที่รับรองกุญแจสาธารณะว่าเป็นของบุคคล หน่วยงาน หรืออุปกรณ์ที่กล่าวอ้างถึงจริง ด้วยการออกใบรับรอง รวมถึงจัดเก็บ เผยแพร่ และเพิกถอนกุญแจสาธารณะที่รับรอง [๕]

(๘) ผู้ลงนาม (Signer) หรือ เจ้าของลายมือชื่อ หมายถึง ผู้ซึ่งถือข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์และสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นในนามตนเองหรือแทนบุคคลอื่น [๓]

(๙) เอกสารอิเล็กทรอนิกส์ (Electronic Document) หมายถึง เอกสารในรูปแบบอิเล็กทรอนิกส์ที่ได้สร้าง ส่ง รับ เก็บรักษา หรือ ประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ [๓]

๓. กฎหมายที่เกี่ยวข้อง

ปัจจุบันประเทศไทยมีกฎหมายที่รับรองลายมือชื่ออิเล็กทรอนิกส์ให้มีผลบังคับใช้ทางกฎหมายเช่นเดียวกันกับลายมือชื่อบนเอกสารที่อยู่ในรูปแบบกระดาษ รวมถึงกฎหมายสำหรับการประยุกต์ใช้งานเทคโนโลยีดิจิทัลเพื่อการปฏิบัติงานของเจ้าหน้าที่รัฐที่เป็นประโยชน์ต่อการบริหารงาน และการให้บริการประชาชน

๓.๑ กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์

รายละเอียดเกี่ยวกับองค์ประกอบและประเภทของลายมือชื่ออิเล็กทรอนิกส์ ได้มีการกำหนดไว้ภายใต้พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม ซึ่งเป็นกฎหมายกลางที่รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ ให้มีผลผูกพันและใช้บังคับได้ตามกฎหมาย โดยมีหลักเกณฑ์พื้นฐานสำคัญ ๓ ข้อ ได้แก่ (๑) หลักความเท่าเทียมกัน (Functional Equivalence) ระหว่าง “กระดาษ” และ “ข้อมูลอิเล็กทรอนิกส์” เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ มีผลทางกฎหมายเทียบเท่าการใช้กระดาษ (๒) หลักความเป็นกลางทางเทคโนโลยี (Technological Neutrality) ที่ไม่ระบุเฉพาะเจาะจงเทคโนโลยีใดเทคโนโลยีหนึ่ง แต่รองรับพัฒนาการของเทคโนโลยีที่จะเกิดขึ้นในอนาคต และ (๓) หลักเสรีภาพการแสดงเจตนา (Party Autonomy) ของคู่สัญญา [๖]

มาตรา ๙ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ที่แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒ ระบุว่าธุรกรรมหรือนิติกรรมใด ๆ มีการลงลายมือชื่อแล้ว หากมีองค์ประกอบ ๓ ข้อ ได้แก่ สามารถระบุตัวผู้เป็นเจ้าของลายมือชื่อได้ สามารถแสดงเจตนาของเจ้าของลายมือชื่อเกี่ยวกับข้อความในข้อมูลอิเล็กทรอนิกส์ และใช้วิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของธุรกรรม ทั้งนี้ วิธีการที่เชื่อถือได้ให้คำนึงถึง (๑) ความมั่นคงและรัดกุมของวิธีการที่ใช้ (๒) ลักษณะ ประเภท ของธุรกรรมที่ทำ และ (๓) ความรัดกุมของระบบติดต่อสื่อสาร

นอกจากลายมือชื่ออิเล็กทรอนิกส์ทั่วไป ตาม**มาตรา ๒๖** ระบุถึงลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ ซึ่งเป็นลายมือชื่อที่สร้างจากกระบวนการทางเทคโนโลยีและมีคุณสมบัติเพิ่มเติม ได้แก่

(๑) ข้อมูลสำหรับสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นเชื่อมโยงไปยังเจ้าของลายมือชื่อได้

(๒) ข้อมูลสำหรับสร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อขณะสร้างลายมือชื่อ

(๓) ต้องสามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่อหรือข้อความในเอกสาร นับแต่เวลาที่สร้างขึ้น

ทั้งนี้สามารถเปรียบเทียบลายมือชื่ออิเล็กทรอนิกส์ประเภททั่วไปตามมาตรา ๙ และประเภทที่เชื่อถือได้ตามมาตรา ๒๖ ในแง่มุมของภาระการพิสูจน์ความน่าเชื่อถือ สรุปตารางที่ ๑ โดยภาระในการพิสูจน์ถึงความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์ประเภททั่วไปนั้นอยู่ที่ผู้ที่กล่าวอ้างว่าลายมือชื่อนั้นน่าเชื่อถือ ในขณะที่ภาระในการพิสูจน์ถึงความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์ประเภทเชื่อถือได้นั้นอยู่ที่ผู้ที่โต้แย้งหรือคัดค้านว่าลายมือชื่อนั้นไม่น่าเชื่อถือ

ตารางที่ ๑ การกล่าวอ้างและภาระการพิสูจน์ของลายมือชื่ออิเล็กทรอนิกส์

ประเภทลายมือชื่ออิเล็กทรอนิกส์	การกล่าวอ้างและภาระการพิสูจน์ของลายมือชื่ออิเล็กทรอนิกส์	
	ผู้ที่กล่าวอ้างว่าลายมือชื่อนั้นน่าเชื่อถือ	**ผู้ที่โต้แย้งหรือคัดค้านว่าลายมือชื่อนั้นไม่น่าเชื่อถือ**
ทั่วไป (มาตรา ๙)	ผู้ที่กล่าวอ้างมีภาระการพิสูจน์ถึงความน่าเชื่อถือนั้น	ผู้ที่โต้แย้งหรือคัดค้านมิได้มีภาระการพิสูจน์ถึงความไม่น่าเชื่อถือนั้น
ที่เชื่อถือได้ (มาตรา ๒๖)	ผู้ที่กล่าวอ้างพิสูจน์เพียงว่าตนได้ปฏิบัติตามเงื่อนไขแห่งมาตรา ๒๖ แล้วผู้ที่กล่าวอ้างจะได้รับประโยชน์จากข้อสันนิษฐานความน่าเชื่อถือนั้น นั้นคือผู้กล่าวอ้างไม่มีภาระพิสูจน์	ผู้ที่โต้แย้งหรือคัดค้านมีภาระการพิสูจน์ถึงความไม่น่าเชื่อถือนั้น

๓.๒ กฎหมายเกี่ยวกับการลงลายมือชื่อของเจ้าหน้าที่ภาครัฐ

ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ เป็นกฎหมายที่เกี่ยวกับการบริหารเอกสารของส่วนราชการ ซึ่งกำหนดชนิดของหนังสือราชการ แบบฟอร์มของหนังสือแต่ละชนิด การลงชื่อและตำแหน่งของผู้มีอำนาจลงนาม และการดำเนินการต่าง ๆ ตั้งแต่การจัดทำ รับส่ง เก็บรักษา ยืมและทำลาย โดยระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ ๒) พ.ศ. ๒๕๔๘ ได้เพิ่มเติมนิยามของระบบสารบรรณอิเล็กทรอนิกส์ และรับรองให้มีการติดต่อราชการด้วยระบบสารบรรณอิเล็กทรอนิกส์ได้เพิ่มเติมจากการดำเนินการโดยหนังสือในรูปแบบกระดาษ

จากนั้นระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ ๔) พ.ศ. ๒๕๖๔ ได้กำหนดหลักการในการรับส่งข้อมูลข่าวสารและหนังสือราชการด้วยระบบสารบรรณอิเล็กทรอนิกส์ และไปรษณีย์

อิเล็กทรอนิกส์ หรืออีเมล เพื่อให้เกิดแนวปฏิบัติที่ชัดเจนในการรับส่งเอกสารในรูปแบบอิเล็กทรอนิกส์ของเจ้าหน้าที่ภาครัฐ โดยส่วนราชการต้องมีอีเมลกลางซึ่งใช้ชื่อโดเมน (Domain Name) ของส่วนราชการ และอาจจัดให้มีลายมือชื่ออิเล็กทรอนิกส์เพื่อรับรองความถูกต้อง

๓.๓ กฎหมายเกี่ยวกับการให้บริการภาครัฐผ่านระบบดิจิทัล

การประยุกต์ใช้งานเทคโนโลยีดิจิทัลเพื่อการปฏิบัติงานของเจ้าหน้าที่ภาครัฐ ซึ่งรวมถึงกฎหมายเกี่ยวกับการลงลายมือชื่ออิเล็กทรอนิกส์และเอกสารอิเล็กทรอนิกส์สำหรับภาครัฐ ได้มีการกำหนดไว้ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ โดยกำหนดให้สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) มีอำนาจในการวางกรอบการบริหารจัดการข้อมูลของหน่วยงานภาครัฐ เพื่อให้ภาครัฐสามารถจัดการกับข้อมูลและจัดเก็บได้ในรูปแบบของดิจิทัล แทนที่จะเป็นรูปแบบกระดาษ และนำข้อมูลที่อยู่ในรูปแบบดิจิทัลมาใช้ประโยชน์ให้สูงสุด รวมถึงลดต้นทุนของกระบวนการทำงานเดิมที่ข้อมูลอยู่ในรูปแบบของกระดาษ

๓.๔ กฎหมายเกี่ยวกับเอกสารอิเล็กทรอนิกส์

มาตรา ๘ วรรคแรก แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ที่แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒ ได้ให้การรับรองข้อมูลในรูปแบบอิเล็กทรอนิกส์ โดยกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือหรือมีเอกสารมาแสดง หรือกำหนดผลทางกฎหมายกรณีไม่ทำเป็นหนังสือ ไม่มีหลักฐานเป็นหนังสือหรือไม่มีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือหรือมีเอกสารมาแสดงตามที่กฎหมายกำหนด

ดังนั้น กฎหมายของประเทศไทยรับรองให้เอกสารอิเล็กทรอนิกส์มีสถานะเป็นหนังสือที่มีผลทางกฎหมาย หากเข้าองค์ประกอบสามประการ คือ

(๑) ข้อมูลต้องสามารถเข้าถึงได้

(๒) ข้อมูลต้องนำกลับมาใช้ใหม่ได้

(๓) ข้อมูลต้องมีความหมายที่ไม่เปลี่ยนแปลง

นอกจากนี้มาตรา ๑๐ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ ยังให้การรองรับในเรื่องของเอกสารต้นฉบับ หากเป็นกรณีที่กฎหมายกำหนดให้ต้องมีการนำเสนอหรือเก็บรักษาเอกสารแบบต้นฉบับ ให้ถือว่าเอกสารอิเล็กทรอนิกส์สามารถใช้แทนการกระทำดังกล่าวได้เช่นต้นฉบับ

เมื่อพิจารณาถึงพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม จะเห็นได้ว่ามีบทบัญญัติซึ่งรับรองผลทางกฎหมายของเอกสารที่ได้มีการจัดทำให้อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์มาตั้งแต่ต้น เช่น การลงลายมือชื่ออิเล็กทรอนิกส์ การรับรองตราประทับบนเอกสารอิเล็กทรอนิกส์ การยอมรับสิ่งพิมพ์ออกของเอกสารอิเล็กทรอนิกส์ที่ได้นำเสนอหรือเก็บรักษาตามหลักเกณฑ์ที่กำหนด ทำให้การแปลงข้อมูลในรูปแบบกระดาษให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ในภายหลังมีฐานะเป็นเพียงสำเนาเท่านั้น

๔. ภาพรวมของลายมือชื่ออิเล็กทรอนิกส์

๔.๑ ลายมือชื่ออิเล็กทรอนิกส์

แนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับเจ้าหน้าที่ของรัฐ สามารถอ้างอิงถึงข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ (ขมธอ.๒๓-๒๕๖๓) [๓] โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ซึ่งได้นิยามลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) ว่าประกอบไปด้วย ๓ องค์ประกอบหลัก ได้แก่

(๑) การพิสูจน์และยืนยันตัวตน: ลายมือชื่ออิเล็กทรอนิกส์นำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์สามารถระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่อที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น

(๒) เจตนาในการลงลายมือชื่อ: ลายมือชื่ออิเล็กทรอนิกส์ต้องสามารถแสดงเจตนาของเจ้าของลายมือชื่อเกี่ยวกับข้อความที่ตนเองลงลายมือชื่อได้

(๓) การรักษาความครบถ้วนของข้อมูล: ข้อมูลที่ลงลายมือชื่อ ลายมือชื่ออิเล็กทรอนิกส์ และข้อมูลอื่น ๆ ที่เกี่ยวข้องจะต้องมีการเก็บรักษา ข้อมูลให้มีความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อมูลตลอดระยะเวลาทั้งหมดของการเก็บรักษา

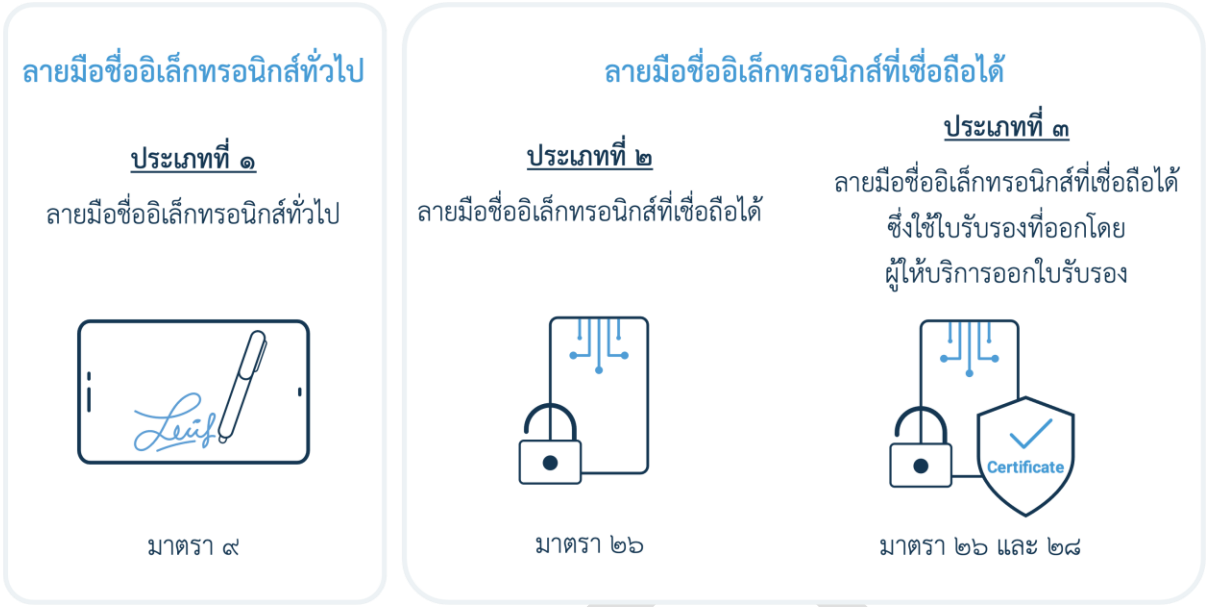
๔.๑.๑ ประเภทลายมือชื่ออิเล็กทรอนิกส์

ประเภทลายมือชื่ออิเล็กทรอนิกส์ตาม ขมธอ.๒๓-๒๕๖๓ ได้แบ่งลายมือชื่ออิเล็กทรอนิกส์ออกเป็น ๓ ประเภท [๓] ได้แก่

- **ประเภทที่ ๑**: ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป เป็นลายมือชื่ออิเล็กทรอนิกส์ในรูปแบบใด ๆ ที่มีคุณลักษณะ ตามที่กำหนดในมาตรา ๙ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

- **ประเภทที่ ๒**: ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีคุณลักษณะตามที่กำหนดในมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

- **ประเภทที่ ๓**: ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีคุณลักษณะตามที่กำหนดในมาตรา ๒๖ และอาศัยใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ตามที่กำหนดในมาตรา ๒๘ แห่ง พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งกำหนดให้ผู้ให้บริการต้องจัดให้มีวิธีการที่เหมาะสม เพื่อให้บุคคลภายนอกเข้าถึงและตรวจสอบข้อมูลใบรับรองที่แสดงข้อมูลเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์



รูปที่ ๑ ประเภทและคุณสมบัติของลายมือชื่ออิเล็กทรอนิกส์ (ขมธอ.๒๓-๒๕๖๓)

๔.๑.๒ ตัวอย่างการเลือกใช้และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๑ สามารถจัดทำขึ้นได้ในหลากหลายรูปแบบ [๓] ซึ่งส่งผลให้วิธีการตรวจสอบความถูกต้องครบถ้วนของลายมือชื่ออิเล็กทรอนิกส์ มีแนวทางที่แตกต่างกันออกไป

- การพิมพ์ชื่อไว้ที่ท้ายเนื้อหาของอีเมล ผู้ตรวจสอบสามารถตรวจสอบข้อมูลที่ลงลายมือชื่อ ชื่อที่พิมพ์ไว้ท้ายเนื้อหาของอีเมล ประกอบกับวันเวลาที่ลงลายมือชื่อ หรือวันเวลาที่ส่งอีเมล เพื่อตรวจสอบเจตนาและความถูกต้องของข้อมูล รวมถึงหลักฐานอื่นที่เกี่ยวข้อง เช่น ตรวจสอบที่อยู่ของอีเมลว่ามาจากชื่อโดเมน (Domain Name) ของส่วนราชการ ซึ่งแสดงถึงการพิสูจน์และยืนยันตัวตนที่น่าเชื่อถือของเจ้าหน้าที่ผู้ลงนาม
- การสแกนภาพของลายมือชื่อที่เขียนด้วยมือและแนบไปกับเอกสาร หรือการใช้สไตลัสเขียนลายมือชื่อด้วยมือลงบนหน้าจอและบันทึกไว้ ผู้ตรวจสอบสามารถตรวจสอบข้อมูลที่ลงลายมือชื่อภาพของลายมือชื่อ ประกอบกับวันเวลาที่ลงลายมือชื่อ เพื่อตรวจสอบเจตนาและความถูกต้องของข้อมูล นอกจากนี้ อาจมีหลักฐานอื่นซึ่งแสดงถึงบริบทที่สำคัญเกี่ยวกับการลงลายมือชื่อ เช่น บุคคลที่สาม
- การใช้ระบบงานอัตโนมัติที่มีการยืนยันตัวผู้ใช้งานมาประกอบกับรูปแบบของลายมือชื่อประเภทที่ ๑ ผู้ตรวจสอบสามารถตรวจสอบข้อมูลที่ลงลายมือชื่อ และลายมือชื่ออิเล็กทรอนิกส์ ซึ่งอาจไม่ได้อยู่ในรูปแบบของชื่อ หรือลายมือชื่อ แต่เป็นลักษณะของข้อมูลที่แสดงว่าผู้ลงนามมีเจตนาในการลงลายมือชื่อและยอมรับความถูกต้องของข้อมูล เช่น บันทึกเหตุการณ์ (Log) ของการยืนยันตัวผู้ใช้งานและการแสดงเจตนาจากการกดยอมรับในระบบงาน

ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๒ และ ๓ อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) ในการสร้างและตรวจสอบ โดยลายมือชื่อดิจิทัลอาจไม่แสดงผลในรูปแบบของรูปภาพลายมือชื่อเหมือนการลงลายมือชื่อบนกระดาษ หรือลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๑ บางรูปแบบ แต่จะเป็นชุดข้อมูลที่ต้องอาศัยซอฟต์แวร์ในการประมวลผล ผู้ตรวจสอบ

สามารถใช้บริการตรวจสอบผ่านเว็บไซต์หรือแอปพลิเคชั่น หรือผ่านการใช้งานโปรแกรมสำหรับการเปิดเอกสารอิเล็กทรอนิกส์ซึ่งรองรับการตรวจสอบลายมือชื่อดิจิทัล โดยจะมีข้อความหรือสัญลักษณ์ที่ระบุว่าลายมือชื่อดิจิทัลมีความสมบูรณ์ และน่าเชื่อถือ เช่น Signature Is Valid นอกจากนี้ผู้ตรวจสอบสามารถพิจารณาข้อมูลใบรับรองเพื่อสนับสนุนการตรวจสอบลายมือชื่อดิจิทัล เช่น ข้อมูลของผู้ลงนาม วันหมดอายุของใบรับรอง รายละเอียดกรณีถูกพักใช้ หรือเพิกถอน ชื่อผู้ให้บริการออกใบรับรอง

ในกรณีลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ ใบรับรองสำหรับการตรวจสอบลายมือชื่อดิจิทัล ต้องเป็นใบรับรองที่มาจากผู้ให้บริการออกใบรับรองที่ดำเนินการตามมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ เช่น องค์กรที่ได้รับการรับรองจากผู้ให้บริการออกใบรับรองแห่งชาติ (Thailand National Root Certification Authority: NRCA)

๔.๒ ลายมือชื่อดิจิทัล

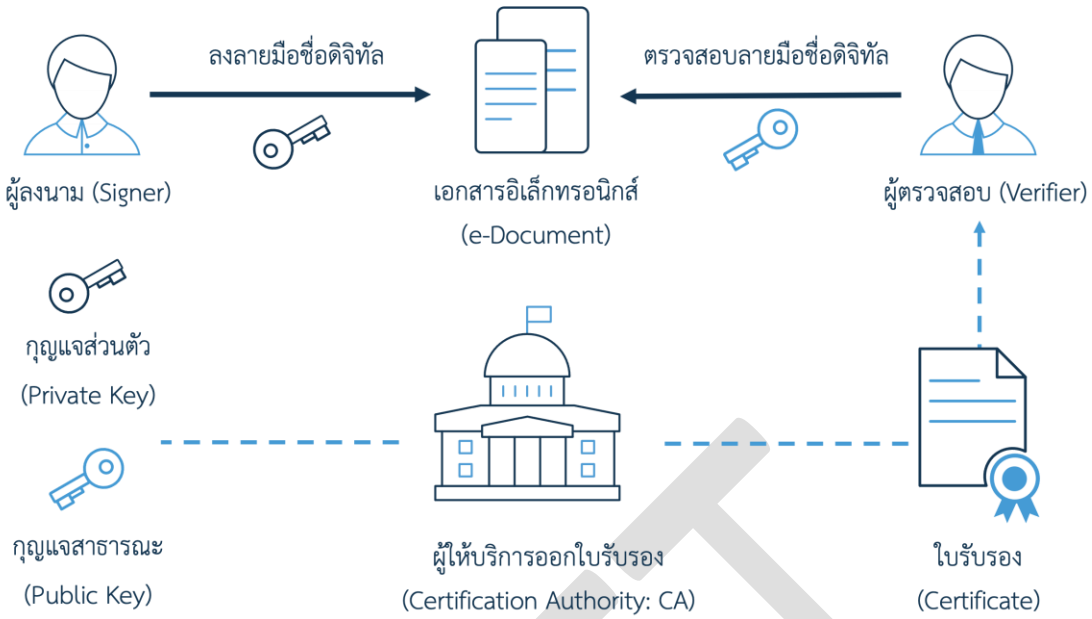
ลายมือชื่อดิจิทัล (Digital Signature) คือ ลายมือชื่ออิเล็กทรอนิกส์รูปแบบหนึ่ง ซึ่งสามารถจัดได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ (ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๒ และ ๓) ตามที่กำหนดในมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ โดยลายมือชื่อดิจิทัลถูกสร้างขึ้นด้วยระบบรหัสแบบ อสมมาตร (Asymmetric Cryptography) ซึ่งมีคุณสมบัติด้านความมั่นคงปลอดภัย ดังนี้

(๑) สามารถยืนยันตัวเจ้าของลายมือชื่อได้ (Authentication)

(๒) สามารถตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ (Data Integrity)

(๓) ทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเอง ลงลายมือชื่อได้ (Non-Repudiation)

ในกระบวนการลายมือชื่อดิจิทัล ผู้ลงนาม (Signer) ดำเนินการลงลายมือชื่อดิจิทัลบนเอกสารอิเล็กทรอนิกส์ด้วยกุญแจส่วนตัว (Private Key) และเผยแพร่กุญแจสาธารณะ (Public Key) ไปยังผู้ตรวจสอบ (Verifier) เพื่อใช้ในกระบวนการตรวจสอบลายมือชื่อ ซึ่งแนวทางการเผยแพร่ข้อมูลกุญแจสาธารณะไปยังผู้ตรวจสอบนั้น สามารถใช้บริการจากผู้ให้บริการออกใบรับรอง (Certification Authority: CA) ให้ออกใบรับรอง (Certificate) ซึ่งเป็นเอกสารระบุข้อมูลกุญแจสาธารณะของผู้ลงนาม



รูปที่ ๒ การสร้างและการตรวจสอบลายมือชื่อดิจิทัล

๔.๓ ผู้ให้บริการออกใบรับรอง

ผู้ให้บริการออกใบรับรอง (Certification Authority: CA) คือ ผู้ที่ทำหน้าที่สร้างและออกใบรับรอง (Certificate) ให้แก่ผู้ใช้บริการออกใบรับรองหรือผู้ลงนาม โดยใบรับรองทำหน้าที่ยืนยันความเชื่อมโยงระหว่างผู้ลงนามและข้อมูลที่ใช้ในการสร้างลายมือชื่อดิจิทัล การออกใบรับรองต้องผ่านการตรวจสอบและพิสูจน์ตัวตนผู้ลงนามด้วยวิธีการที่น่าเชื่อถือ ทำให้ใบรับรองเป็นองค์ประกอบสำคัญที่ทำให้ขั้นตอนการตรวจสอบลายมือชื่อดิจิทัลมีความสะดวกและน่าเชื่อถือ ทั้งนี้ ผู้ให้บริการออกใบรับรองต้องเป็นบุคคลที่เป็นที่ยอมรับและน่าเชื่อถือแก่บุคคลที่เกี่ยวข้องกับการใช้งานใบรับรอง ได้แก่ ผู้ใช้บริการ ผู้ตรวจสอบ และบุคคลอื่นซึ่งกระทำหรือยกเว้นการกระทำใด ๆ เพราะเชื่อถือข้อมูลในใบรับรอง

๔.๓.๑ ใบรับรอง

ใบรับรองทำหน้าที่รับรองกุญแจสาธารณะให้กับผู้ลงนาม ประกอบไปด้วยข้อมูลของเจ้าของใบรับรอง ข้อมูลของผู้ออกใบรับรอง กุญแจสาธารณะของผู้เป็นเจ้าของใบรับรอง ช่วงเวลาที่ใบรับรองสามารถใช้งานได้ และลายมือชื่อดิจิทัลที่สร้างขึ้นโดยผู้ให้บริการออกใบรับรองเพื่อรับรองความถูกต้องของข้อมูลในใบรับรอง เป็นต้น [๔]

- ใบรับรองสำหรับการลงลายมือชื่อ สามารถแบ่งออกได้เป็น ๓ ประเภทหลัก ซึ่งมีค่าใช้จ่ายในการใช้บริการออกใบรับรองและเอกสารเพื่อเป็นหลักฐานประกอบการใช้บริการแตกต่างกัน ดังนี้
- ใบรับรองบุคคลธรรมดา (Personal Certificate) สำหรับประชาชนทั่วไป ผู้ซึ่งต้องการใช้ใบรับรองในการลงลายมือชื่อดิจิทัลเพื่อทำธุรกรรมทางอิเล็กทรอนิกส์
- ใบรับรองเจ้าหน้าที่นิติบุคคล (Enterprise User Certificate) สำหรับเจ้าหน้าที่ขององค์กรหรือหน่วยงาน ซึ่งหลักฐานในการสมัครขอใช้บริการจะต้องมีเอกสารสำคัญขององค์กรหรือหน่วยงานประกอบกันกับเอกสารข้อมูลของเจ้าหน้าที่
- ใบรับรองนิติบุคคล (Enterprise Certificate) สำหรับองค์กรหรือหน่วยงาน โดยใช้เอกสารสำคัญขององค์กรหรือหน่วยงานในการสมัครขอใช้บริการ

นอกจากนี้ ยังมีใบรับรองประเภทอื่น ๆ ซึ่งไม่เกี่ยวข้องกับการลงลายมือชื่อโดยบุคคล เช่น ใบรับรองเว็บไซต์ (Ssl Certificate) สำหรับใช้ยืนยันตัวตนของ Web Server และใบรับรองคอมพิวเตอร์หรืออุปกรณ์ (Computer/Equipment Certificate) เพื่อยืนยันความปลอดภัยในการใช้งานหรือติดต่อสื่อสารผ่านอุปกรณ์

๔.๓.๒ รายการเพิกถอนใบรับรอง

ผู้ใช้บริการออกใบรับรองสามารถแจ้งขอยกเลิกใบรับรองได้หากผู้ใช้บริการต้องการยุติการใช้งานใบรับรอง หรือเมื่อเกิดเหตุจำเป็น เช่น กุญแจส่วนตัวสูญหาย กุญแจส่วนตัวถูกเข้าถึงโดยผู้ไม่ได้รับอนุญาต หรือ ข้อมูลในใบรับรองมีการเปลี่ยนแปลง โดยผู้ให้บริการออกใบรับรองจะต้องรับแจ้งการเพิกถอนใบรับรอง จากนั้นบันทึกและเผยแพร่รายการเพิกถอนใบรับรอง (Certificate Revocation List)

โดยรายการเพิกถอนใบรับรองประกอบไปด้วยข้อมูลของผู้ออกรายการเพิกถอนใบรับรอง วันที่ออกรายการเพิกถอนใบรับรองนี้ วันที่จะออกรายการเพิกถอนใบรับรองครั้งต่อไป รายการใบรับรองที่ถูกเพิกถอน และลายมือชื่อดิจิทัลที่สร้างขึ้นโดยผู้ให้บริการออกใบรับรองเพื่อรับรองความถูกต้องของข้อมูลในรายการเพิกถอนใบรับรอง เป็นต้น [๔]

๔.๓.๓ ผู้ให้บริการออกใบรับรองในประเทศไทย

ผู้ให้บริการออกใบรับรองแห่งชาติ (Thailand National Root Certification Authority: NRCA) มีสถานะเป็นผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด (Root CA) จัดตั้งขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ในปี พ.ศ. ๒๕๕๔ มีวัตถุประสงค์เพื่อส่งเสริมให้ประเทศไทยมีโครงสร้างพื้นฐานที่สำคัญในการขับเคลื่อนการดำเนินงานผ่านระบบดิจิทัลและการทำธุรกรรมทางอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัยและสอดคล้องกับมาตรฐานสากล

ผู้ที่ต้องการขอใช้บริการออกใบรับรองเพื่อรับรองข้อมูลส่วนตัว หรือผู้ใช้บริการ (Subscriber) สามารถขอรับบริการได้ที่หน่วยงานที่ได้รับการรับรองจาก NRCA ในฐานะผู้ให้บริการออกใบรับรองในลำดับชั้นถัดลงมา (Subordinate CA)

เพื่อให้การให้บริการของผู้ให้บริการออกใบรับรองมีความน่าเชื่อถือและเป็นไปในทิศทางเดียวกัน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) ได้ออกประกาศเรื่อง แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) พ.ศ. ๒๕๕๒ โดยวางแนวทาง เช่น หัวข้อที่ต้องกำหนดไว้ในนโยบายและแนวปฏิบัติ รวมถึงสาระสำคัญของเนื้อหาในแต่ละหัวข้อ

ในการให้บริการ ผู้ให้บริการออกใบรับรองควรจัดทำใบรับรองและรายการเพิกถอนใบรับรองให้อยู่ในรูปแบบที่สอดคล้องกัน โดยสามารถอ้างอิงจากข้อกำหนดต่าง ๆ ในข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการกำหนดข้อมูลในใบรับรอง และรายการเพิกถอนใบรับรอง (ขมธอ. ๑๕-๒๕๖๐) [๔] ที่ระบุถึงแนวทางการกำหนดข้อมูลที่เหมาะสมสำหรับใบรับรองแต่ละประเภท

๔.๓.๔ การใช้งานและตรวจสอบใบรับรองจากต่างประเทศ

NRCA เป็นศูนย์กลางในการสร้างความน่าเชื่อถือ หรือที่เรียกว่า Trust Anchor เพื่อให้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองในลำดับชั้นถัดลงมามีความน่าเชื่อถือและได้รับการยอมรับ ทั้งระดับภายในประเทศและระดับนานาชาติ โดยมีการผลักดันให้เกิดการทำงานร่วมกัน และสามารถตรวจสอบใบรับรองอิเล็กทรอนิกส์ระหว่างกันได้ โดย NRCA ได้เข้าไปอยู่ในรายชื่อผู้ให้บริการออกใบรับรองขององค์กรระดับสากล ยกตัวอย่างเช่น Adobe Approved Trust List และ Microsoft Trusted Root Program

Adobe Approved Trust List (Aatl) เป็นโครงการที่จัดทำขึ้นโดยบริษัท Adobe เพื่อเผยแพร่รายชื่อผู้ให้บริการออกใบรับรองจากทั่วโลกที่ดำเนินการตามระดับความน่าเชื่อถือ (Assurance Level) ที่กำหนดไว้ในข้อกำหนดทางเทคนิค (Aatl Technical Requirements) ทำให้เอกสารที่มีการลงลายมือชื่อดิจิทัลด้วยใบรับรองที่ออกโดยสมาชิกของ Aatl ได้รับการรับรองว่ามีความน่าเชื่อถือโดยอัตโนมัติ หากเปิดใช้งานด้วยโปรแกรม Adobe Acrobat หรือ Adobe Reader โดยโปรแกรมจะมีการเชื่อมต่อกับรายชื่อที่เผยแพร่อย่างสม่ำเสมอ เพื่อให้ข้อมูลมีความทันสมัย ซึ่ง NRCA เป็นหนึ่งในสมาชิกของ Aatl ส่งผลให้เอกสารที่มีการลงลายมือชื่อดิจิทัลด้วยใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองในลำดับชั้นถัดลงมาต่าง ๆ ของ NRCA มีความน่าเชื่อถือและสามารถนำไปใช้งานในต่างประเทศได้

Microsoft Trusted Root Program คือ โครงการที่มีลักษณะเดียวกันกับ Aatl เพื่อให้การเปิดใช้งานเอกสารด้วยผลิตภัณฑ์และบริการในเครือ Microsoft ได้รับการรับรองความน่าเชื่อถือโดยอัตโนมัติ หากเป็นเอกสารที่มีการใช้งานใบรับรองจากผู้ให้บริการออกใบรับรองในโครงการ ในการนี้ NRCA ได้ผ่านการตรวจสอบข้อกำหนดด้านต่าง ๆ และได้รับการรับรองให้อยู่ใน Microsoft Trusted Root Program พร้อมทั้งมีการรักษาข้อมูลให้มีความทันสมัยตามข้อกำหนดของระบบฐานข้อมูล

นอกจากนี้ Microsoft เป็นสมาชิกของ Common Certificate Authority Database (Ccadb) ซึ่งเป็นระบบฐานข้อมูลผู้ให้บริการออกใบรับรองที่จัดทำขึ้นโดยบริษัท Mozilla ผ่านความร่วมมือกับผู้ให้บริการเว็ปเบราว์เซอร์ หรือผู้พัฒนาซอฟต์แวร์ที่มีการจัดทำข้อมูลรายชื่อผู้ให้บริการออกใบรับรองที่น่าชื่อถือของตนเอง หรือที่ Ccadb เรียกว่า Root Store Operator เพื่อยกระดับให้ฐานข้อมูลมีความครอบคลุม รวมถึงทันสมัย เนื่องจากมีระบบแจ้งเตือนให้ผู้ให้บริการออกใบรับรองที่อยู่ในฐานข้อมูลมีการปรับปรุงข้อมูลที่มีความล้าหลังเป็นประจำ เช่น รายการตรวจสอบ (Audit Statement) ที่ใกล้หมดอายุ โดยผู้ที่เป็นสมาชิกของ Ccadb สามารถเข้าถึงข้อมูลดังกล่าวและใช้ประโยชน์ในการนำไปพัฒนาข้อมูล (Root Store) สำหรับผลิตภัณฑ์และบริการของตนเองได้ ซึ่งผู้ให้บริการรายใหญ่อย่าง Microsoft และ Google ต่างก็เป็นหนึ่งในสมาชิกของ Ccadb กล่าวได้อีกนัยคือ ผู้ให้บริการออกใบรับรองจะต้องมีการให้ข้อมูลและผ่านการตรวจสอบตามข้อกำหนดเบื้องต้นของ Ccadb เพื่อให้มีรายชื่ออยู่ในฐานข้อมูล โดย Root Store Operator อาจมีเกณฑ์การตรวจสอบเพิ่มเติมก่อนที่จะรับรองและนำรายชื่อผู้ให้บริการออกใบรับรองเข้าสู่ Root Store ของตนเอง

๔.๔ มาตรฐานเอกสารอิเล็กทรอนิกส์

เอกสารอิเล็กทรอนิกส์ คือ เอกสารที่จัดทำในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นอีกรูปแบบหนึ่งในการบริหารจัดการเอกสารที่แตกต่างจากการดำเนินการในรูปแบบกระดาษ โดยมีข้อดีด้านการลดการใช้งานทรัพยากรกระดาษ และสามารถรักษาสภาพคงทนได้ตามความก้าวหน้าทางเทคโนโลยี

ในปัจจุบัน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ได้กำหนดมาตรฐานเกี่ยวกับเอกสารอิเล็กทรอนิกส์ รวมถึงเอกสารในรูปแบบ Portable Data Format (Pdf) ใน ขมธอ. ๑๑-๒๕๖๐ [๕] และ รูปแบบ Extensible Markup Language (Xml) ใน ขมธอ. ๑๔-๒๕๖๐ [๗] สำหรับการใช้งานประเภทต่าง ๆ รวมถึง การจัดทำหนังสือรับรอง การออกใบประมวลผลการศึกษา การออกใบเสร็จรับเงินภาครัฐ และ การควบคุมวัตถุอันตราย เป็นต้น นอกจากนี้มีการกำหนดโครงสร้างข้อมูล (Data Structure) สำหรับเอกสารรับรอง (Verifiable Credential: Vc) และ เอกสารสำแดง (Verifiable Presentation: Vp) ในขมธอ. ๒๔-๒๕๖๓ [๘] สำหรับการใช้งานเพื่อพิสูจน์และยืนยันตัวตน การให้ความยินยอม การมอบอำนาจ หรือ การแสดงข้อมูลที่ถูกรับรองแก่ผู้อื่น ในรูปแบบอิเล็กทรอนิกส์ เป็นต้น

การลงลายมือชื่อในเอกสารอิเล็กทรอนิกส์ควรอ้างอิงแนวทางจากมาตรฐานสากล เช่น มาตรฐานลายมือชื่ออิเล็กทรอนิกส์ขั้นสูง (Advanced Electronic Signature: ADES) จากสถาบัน European Telecommunications Standards Institute (ETSI) ซึ่งในปัจจุบันได้กำหนดมาตรฐานสำหรับเอกสารทั้งหมด ๕ ประเภท [๙] ได้แก่

(๑) Cms Advanced Electronic Signatures (CADES) สำหรับเอกสารอิเล็กทรอนิกส์ในรูปแบบ Cryptographic Message Syntax (Cms)

(๒) Xml Advanced Electronic Signatures (XADES) สำหรับเอกสารอิเล็กทรอนิกส์ในรูปแบบ Extensible Markup Language (Xml)

(๓) Pdf Advanced Electronic Signatures (PADES) สำหรับเอกสารอิเล็กทรอนิกส์ในรูปแบบ Portable Data Format (Pdf)

(๔) Json Advanced Electronic Signatures (JADES) สำหรับเอกสารอิเล็กทรอนิกส์ในรูปแบบ Javascript Object Notation (Json)

(๕) Associated Signature Containers (ASiC) สำหรับการรวมเอกสารอิเล็กทรอนิกส์มากกว่าหนึ่งฉบับมาลงลายมือชื่อและประทับรับรองเวลาร่วมกัน

๔.๕ การลงลายมือชื่ออิเล็กทรอนิกส์เพื่อการตรวจสอบในระยะยาว

โดยทั่วไป ลายมือชื่อประเภทดิจิทัลที่ถูกสร้างขึ้นด้วยใบรับรองหนึ่ง ๆ จะสามารถถูกตรวจสอบได้นับจากขณะเวลาที่ถูกสร้างขึ้น ไปจนถึงเวลาที่ใบรับรองนั้นหมดอายุหรือถูกเพิกถอน

ดังนั้น หากลายมือชื่อในเอกสารอิเล็กทรอนิกส์ใด ๆ มีความจำเป็นต้องถูกตรวจสอบในระยะยาว หน่วยงานที่เกี่ยวข้องควรกำหนดมาตรการการลงลายมือชื่อและการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ในระยะยาว โดยสามารถอ้างอิงแนวทางจากมาตรฐานลายมือชื่ออิเล็กทรอนิกส์ขั้นสูง (Advanced Electronic Signature: ADES) จากสถาบัน European Telecommunications Standards Institute

(ETSI) [๙] โดยเจ้าหน้าที่ของรัฐจากหน่วยงานที่เกี่ยวข้องควรทำการประทับรับรองเวลา (Time Stamping) บนเอกสารอิเล็กทรอนิกส์ที่ถูกลงมือชื่อ โดยใช้บริการจากผู้ให้บริการประทับรับรอง (Time Stamping Authority) ที่น่าเชื่อถือ ก่อนที่ใบรับรองนั้นจะหมดอายุหรือถูกเพิกถอน ทั้งนี้ เจ้าหน้าที่ของรัฐผู้ดำเนินการขอใช้บริการประทับรับรองเวลา จะเป็นบุคคลเดียวกันกับเจ้าของลายมือชื่อหรือไม่ก็ได้

การประทับรับรองเวลาจะให้การรับรองว่าเอกสารอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์นั้นถูกสร้างขึ้นโดยผู้ที่กล่าวอ้างจริง อีกทั้งไม่ถูกปลอมแปลงแก้ไขนับจากเวลาที่ถูกประทับรับรองเวลา ทำให้สามารถตรวจสอบได้ภายหลังจากที่ใบรับรองหมดอายุหรือถูกเพิกถอนไปแล้ว

๕. แนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์

แนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์ สำหรับเจ้าหน้าที่ของรัฐ มีจุดมุ่งหมายเพื่อจัดทำข้อเสนอแนะในการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทต่าง ๆ ให้เหมาะสมกับชนิดของเอกสาร ซึ่งครอบคลุมเอกสารราชการที่เจ้าหน้าที่ของรัฐในทุกระดับจัดทำขึ้นเพื่อการปฏิบัติหน้าที่ รวมถึงแนวทางการดำเนินการในกรณีที่ส่วนราชการไม่สามารถปฏิบัติตามได้ด้วยข้อยกเว้น และข้อจำกัดต่าง ๆ

๕.๑ กรอบแนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์

อ้างอิงจากเอกสาร Security Guidelines On The Appropriate Use Of Qualified Electronic Signatures [๒] โดย European Union Agency For Network And Information Security (Enisa) ได้มีคำแนะนำการประเมินลักษณะของธุรกรรม โดยแบ่งตามระดับตามความวิกฤต (Criticality Levels) ได้แก่

(๑) ระดับธรรมดา (Standard) หมายถึง ธุรกรรมทั่วไป กล่าวคือ การแลกเปลี่ยนหรือเข้าถึงข้อมูลอย่างจำกัดที่มีผลกระทบในระดับต่ำต่อองค์กร ซึ่งอาจรวมถึงการแลกเปลี่ยนข้อมูลภายในองค์กรที่อยู่ในลำดับชั้นข้อมูลที่ต่ำ เช่น ทั่วไป (Official) หรือเผยแพร่ได้ (Publish)

(๒) ระดับขั้นสูง (Advanced) หมายถึง ธุรกรรมที่ต้องมีการพิจารณาอย่างรอบคอบถึงเงื่อนไขหรือข้อควรระวังเบื้องต้น อาจมีความเกี่ยวข้องกับความเสี่ยงทางด้านการเงินในระดับจำกัด หรืออาจมีการแลกเปลี่ยนข้อมูลในลำดับชั้นของข้อมูลที่สูงขึ้น เช่น ข้อมูลที่เป็นความลับ (Confidential) หรือใช้ภายใน (Internal Use)

(๓) ระดับอ่อนไหว (Sensitive) หมายถึง ธุรกรรมที่เกี่ยวข้องกับข้อมูลที่มีความละเอียดอ่อน อาจมีความเสี่ยงทางด้านการเงินโดยตรง เช่น ธุรกรรมที่เกี่ยวข้องกับข้อมูลที่เป็นความลับขององค์กร (Secret หรือ Top Secret) รวมถึงธุรกรรมที่ก่อให้เกิดผลกระทบในวงกว้าง

ทั้งนี้ นอกเหนือจากการประเมินลักษณะของธุรกรรมจากด้านความเสี่ยงทางการเงินและลำดับชั้นของข้อมูล Enisa แนะนำให้พิจารณาถึงปัจจัยอื่น ซึ่งมีส่วนเกี่ยวข้องต่อการดำเนินงานขององค์กร โดยอาจมีปัจจัยเฉพาะสำหรับแต่ละธุรกิจ หรืออุตสาหกรรมที่ควรคำนึงถึงแตกต่างกันไป ซึ่งจากระดับของลักษณะธุรกรรมดังกล่าว นำมาประยุกต์ใช้เป็นแนวทางในการจัดทำข้อเสนอแนะในการเลือกใช้ประเภทของลายมือชื่ออิเล็กทรอนิกส์ โดยสรุปในตารางที่ ๒ ดังนี้

(๑) ข้อเสนอแนะระดับทั่วไป (Basic) สำหรับธุรกรรมในระดับธรรมดา ควรเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ที่ได้รับการยอมรับเทียบเท่ากับการลงลายมือชื่อบนกระดาษ โดยแนะนำให้ใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๑

(๒) ข้อเสนอแนะระดับแนะนำ (Recommended) สำหรับธุรกรรมขั้นสูง ควรเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ที่มีคุณสมบัติเพิ่มเติมด้านการตรวจพบการเปลี่ยนแปลงของข้อมูล และการคงสภาพในระยะยาว เพื่อการตรวจสอบความถูกต้องของข้อมูลระยะยาว (Long-Term Validation) โดยแนะนำให้ใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๒

(๓) ข้อเสนอแนะในการยกระดับ (Enhanced) สำหรับธุรกรรมอ่อนไหว นอกเหนือจากการใช้ลายมือชื่ออิเล็กทรอนิกส์ที่ได้รับการยอมรับเทียบเท่าการลงลายมือชื่อบนกระดาษ และมีการตรวจสอบความถูกต้องของข้อมูลระยะยาว ควรเลือกใช้บริการที่ได้รับการรับรองคุณภาพ โดยแนะนำให้ใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓

ตารางที่ ๒ ระดับความเสี่ยงของธุรกรรมและประเภทลายมือชื่ออิเล็กทรอนิกส์ที่แนะนำ

ระดับความเสี่ยงของธุรกรรม	แนวทางการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ของกลุ่มสหภาพยุโรป	แนวทางการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ในประเทศไทย
ธรรมดา (Standard)	Basic	ประเภทที่ ๑
ขั้นสูง (Advanced)	Recommended	ประเภทที่ ๒
อ่อนไหว (Sensitive)	Enhanced	ประเภทที่ ๓

๕.๒ การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์สำหรับหนังสือราชการ

ในการดำเนินงานด้านเอกสาร เจ้าหน้าที่ของรัฐต้องมีการพิจารณาเลือกใช้งานประเภทของเอกสารให้ตรงตามระเบียบที่กำหนดไว้ ซึ่งเอกสารแต่ละประเภทถูกกำหนดให้มีองค์ประกอบ รูปแบบ วัตถุประสงค์ในการจัดทำและผู้ลงนามที่แตกต่างกัน ในการนี้ การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์จำเป็นต้องมีการพิจารณาถึงประเด็นดังกล่าว เพื่อประเมินระดับความเสี่ยงของธุรกรรมและประเภทของลายมือชื่ออิเล็กทรอนิกส์ที่เหมาะสม

๕.๒.๑ ประเภทหนังสือราชการ

หนังสือราชการ คือ เอกสารที่เป็นหลักฐานในราชการ มี ๖ ชนิด ตามข้อ ๑๐ แห่งระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ ได้แก่

(๑) หนังสือภายนอก คือ หนังสือติดต่อราชการที่เป็นแบบพิธีโดยใช้กระดาษตราครุฑ เป็นหนังสือติดต่อระหว่างส่วนราชการ หรือส่วนราชการมีถึงหน่วยงานอื่นใดซึ่งมิใช่ส่วนราชการ หรือที่มีถึงบุคคลภายนอก เช่น การติดต่อระหว่างกระทรวง การติดต่อระหว่างส่วนราชการกับภายนอกส่วนราชการ

(๒) หนังสือภายใน คือ หนังสือติดต่อราชการที่เป็นแบบพิธีน้อยกว่าหนังสือภายนอก เป็นหนังสือติดต่อภายในกระทรวง ทบวง กรม หรือจังหวัดเดียวกัน เช่น การติดต่อระหว่างกรม หรือหน่วยงานที่เทียบเท่ากรมภายในสังกัดกระทรวงเดียวกัน

(๓) หนังสือประทับตรา คือ หนังสือที่ใช้การประทับตราแทนการลงชื่อหัวหน้าส่วนราชการระดับกรมขึ้นไป โดยให้หัวหน้าส่วนราชการระดับกองหรือผู้ที่ได้รับมอบหมายจากหัวหน้าส่วนราชการระดับกรมขึ้นไป เป็นผู้รับผิดชอบลงชื่อย่อกำกับตรา ใช้เฉพาะกรณีไม่ใช่เรื่องสำคัญ เช่น การขอรายละเอียดเพิ่มเติม การส่งสำเนาหนังสือ สิ่งของ เอกสาร หรือบรรณสาร การตอบรับทราบที่ไม่เกี่ยวกับราชการสำคัญ หรือการเงิน การแจ้งผลงานที่ได้ดำเนินการไปแล้วให้ส่วนราชการที่เกี่ยวข้องทราบ การเตือนเรื่องที่ค้าง

(๔) หนังสือสั่งการ ได้แก่ คำสั่ง ระเบียบ และข้อบังคับ

(๕) หนังสือประชาสัมพันธ์ ได้แก่ ประกาศ แถลงการณ์ และข่าว

(๖) หนังสือที่เจ้าหน้าที่จัดทำขึ้นหรือรับไว้เป็นหลักฐานในราชการ ได้แก่ หนังสือรับรอง รายงานการประชุม บันทึก และหนังสืออื่น

๕.๒.๒ ประเภทของผู้ลงนาม

เจ้าหน้าที่ของรัฐที่มีอำนาจในการลงนาม สามารถแบ่งออกได้ดังนี้

- ผู้ลงนามในนามส่วนราชการ หมายถึง หัวหน้าส่วนราชการที่มีสถานะเป็นนิติบุคคล ทั้งนี้ ให้รวมถึงคณะกรรมการด้วย ดังนั้น หนังสือที่จัดทำขึ้นเพื่อก่อให้เกิดธุรกรรมซึ่งผูกพันส่วนราชการจะเป็นการลงนามโดยหัวหน้าส่วนราชการ ระดับกระทรวง ทบวง กรม สำนักงาน สถาบันการศึกษา จังหวัดหรือส่วนราชการอื่น นอกจากนี้ อาจมีกรณีซึ่งหัวหน้าส่วนราชการมอบอำนาจให้ผู้บริหารหรือเจ้าหน้าที่เป็นผู้ลงนามแทน
- ผู้บริหาร หมายถึง ผู้ดำรงตำแหน่งในสายงานบริหาร เช่น หัวหน้าส่วนราชการและรองหัวหน้าส่วนราชการระดับกรมขึ้นไป หัวหน้าส่วนราชการระดับต่ำกว่ากรม หัวหน้าคณะทำงาน หรือประธานคณะกรรมการซึ่งจัดตั้งขึ้นเพื่อวัตถุประสงค์เฉพาะ มีอำนาจโดยการรับมอบอำนาจหรือได้รับอำนาจตามกฎหมายให้เป็นผู้ลงนามในเรื่องที่เกี่ยวกับขอบเขตการปฏิบัติงานของผู้ดำรงตำแหน่งนั้น ๆ
- เจ้าหน้าที่ผู้ได้รับมอบหมาย หรือเจ้าหน้าที่ผู้ได้รับมอบอำนาจ เป็นผู้ที่ได้รับมอบอำนาจจากหัวหน้าส่วนราชการให้เป็นผู้มีอำนาจลงนามเฉพาะเรื่องที่ได้รับมอบหมาย
- เจ้าหน้าที่ทั่วไป ซึ่งรวมถึงเจ้าหน้าที่ธุรการ เป็นผู้ลงนามในนามบุคคล ซึ่งสามารถลงนามในหนังสือที่ได้จัดทำขึ้นเพื่อการปฏิบัติหน้าที่โดยทั่วไปตามตำแหน่ง

๕.๒.๓ ประเภทลายมือชื่อที่แนะนำ

เพื่อเป็นแนวทางในการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์สำหรับเจ้าหน้าที่ของรัฐ ตารางที่ ๓ สรุปข้อเสนอแนะของประเภทลายมือชื่ออิเล็กทรอนิกส์ขั้นต่ำที่แนะนำ ดังนี้

- **หนังสือภายนอก หนังสือภายใน และหนังสือประทับตรา** เป็นหนังสือแบบพิธีการเพื่อการติดต่อระหว่างส่วนราชการ หรือบุคคลภายนอกส่วนราชการ โดยมีแนวทางการใช้งานตามลำดับความสำคัญของหัวข้อเรื่อง ซึ่งเป็นการกระทำในนามส่วนราชการที่มีการลงนามโดยหัวหน้าส่วน

ราชการ หรือผู้ที่ได้รับมอบหมาย และมีผลผูกพันส่วนราชการ ควรใช้งานลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ เพื่อความน่าเชื่อถือของข้อมูลผู้ลงนามแทนส่วนราชการ

- **หนังสือสั่งการ** ซึ่งอาจเป็นการสั่งการในนามผู้บริหาร หรือในนามส่วนราชการ หากเป็นการออกหนังสือไปยังเจ้าหน้าที่ภายใต้บังคับบัญชา หรือภายในส่วนราชการเดียวกัน ควรใช้งานลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๒ โดยทั่วไปจะมีการยืนยันตัวตนในเบื้องต้นก่อนการลงลายมือชื่อ ส่วนการออกหนังสือไปยังภายนอกส่วนราชการที่มีผลกระทบในวงกว้างควรใช้งานลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ เพื่อความน่าเชื่อถือ และบุคคลภายนอกสามารถตรวจสอบใบรับรองได้อย่างสะดวก
- **หนังสือประชาสัมพันธ์** เป็นหนังสือที่มีการเผยแพร่สู่สาธารณชน ควรใช้งานลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ เพื่อให้บุคคลภายนอกสามารถตรวจสอบได้ว่าเป็นการเผยแพร่โดยหน่วยงานภาครัฐ
- **หนังสือที่มีการจัดทำขึ้น หรือรับไว้เป็นหลักฐานราชการ** สามารถเลือกใช้งานตามลำดับความเสี่ยงของธุรกรรม สำหรับเจ้าหน้าที่ธุรการอาจใช้งานลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๑ ในการรับแบบคำร้อง หรือคำขอต่าง ๆ เพื่อนำเข้าทะเบียนรับหนังสือของราชการ ซึ่งพิจารณารวมถึงความคล่องตัวในการใช้งานจริง สำหรับบันทึกเพื่อการติดต่อประสานงานเป็นการภายในและรายงานการประชุม ควรใช้งานลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๒ ในขณะที่หนังสือรับรองซึ่งลงลายมือชื่อโดยหัวหน้าส่วนราชการหรือผู้ที่ได้รับมอบหมาย เช่น นายทะเบียน ควรใช้งานลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ ซึ่งมีใบรับรองในฐานะเจ้าหน้าที่ของส่วนราชการ นอกจากนี้ หนังสือที่จัดทำขึ้นระหว่างองค์กรที่หัวหน้าของหน่วยงานภาครัฐจะเป็นผู้ลงนาม หรือมอบอำนาจให้แก่ผู้ดำรงตำแหน่งรองลงไปดำเนินการแทนตามระเบียบต่าง ๆ ที่เกี่ยวข้อง ซึ่งจะต้องมีพยานร่วมลงนาม ควรใช้งานลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ เช่นเดียวกันทั้งเอกสาร เช่น สัญญาจัดซื้อจัดจ้าง บันทึกความร่วมมือ

ทั้งนี้ ข้อเสนอแนะประเภทลายมือชื่ออิเล็กทรอนิกส์ขั้นต่ำเป็นเพียงข้อเสนอแนะเบื้องต้น โดยเจ้าหน้าที่ของรัฐอาจเลือกใช้ประเภทลายมือชื่ออิเล็กทรอนิกส์ที่สูงหรือต่ำกว่าประเภทที่แนะนำตามความเหมาะสมกับธุรกรรมที่ทำ

ตารางที่ ๓ แนวทางการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ตามชนิดของหนังสือราชการ

รูปแบบการลงลายมือชื่ออิเล็กทรอนิกส์	ประเภทของผู้ลงนาม	ประเภทลายมือชื่อที่แนะนำ
๑) หนังสือภายนอก	ในนามส่วนราชการ โดยหัวหน้าส่วนราชการระดับกระทรวง ทบวง กรม หรือผู้บริหารตามที่ได้รับมอบหมาย	ประเภทที่ ๓
๒) หนังสือภายใน	ในนามส่วนราชการ โดยหัวหน้าส่วนราชการระดับกระทรวง ทบวง กรม หรือผู้บริหารตามที่ได้รับมอบหมาย	ประเภทที่ ๓

รูปแบบการลงลายมือชื่ออิเล็กทรอนิกส์	ประเภทของผู้ลงนาม	ประเภทลายมือชื่อที่แนะนำ
๓) หนังสือประทับตรา	ในนามส่วนราชการ โดยหัวหน้าส่วนราชการระดับกองหรือเจ้าหน้าที่ผู้ได้รับมอบหมาย	ประเภทที่ ๓
๔) หนังสือสั่งการ		
๔.๑) มีผลบังคับใช้ภายในส่วนราชการ	ผู้บริหารหรือในนามส่วนราชการ	ประเภทที่ ๒
๔.๒) มีผลบังคับใช้ในวงกว้าง	ผู้บริหารหรือในนามส่วนราชการ	ประเภทที่ ๓
๕) หนังสือประชาสัมพันธ์	ในนามส่วนราชการ	ประเภทที่ ๓
๖) หนังสือที่เจ้าหน้าที่จัดทำขึ้น หรือรับไว้เป็นหลักฐานราชการ		
๖.๑) หนังสือที่ใช้ในการปฏิบัติงานในลักษณะเป็นประจำทั่วไป	เจ้าหน้าที่ธุรการหรือระบบอัตโนมัติ	ประเภทที่ ๑
๖.๒) บันทึกเพื่อการติดต่อภายในส่วนราชการระดับต่ำกว่ากรม บันทึกข้อความ เสนอและสั่งการ รายงานการประชุม	ผู้บริหารหรือเจ้าหน้าที่ทั่วไป	ประเภทที่ ๒
๖.๓) หนังสือรับรอง	ในนามส่วนราชการ โดยหัวหน้าส่วนราชการระดับกระทรวง ทบวง กรมหรือเจ้าหน้าที่ผู้ได้รับมอบหมาย	ประเภทที่ ๓
๖.๔) หนังสือที่มีพยานร่วมลงนาม	*ผู้ลงนาม*: ในนามส่วนราชการโดยผู้มีอำนาจลงนาม *พยาน*: เจ้าหน้าที่ผู้ได้รับมอบหมาย	ประเภทที่ ๓

๕.๓ การลงลายมือชื่อโดยบุคคลเดียวและหลายบุคคล

เอกสารอิเล็กทรอนิกส์หนึ่ง ๆ อาจมีความจำเป็นต้องลงลายมือชื่อโดยบุคคลเดียวหรือหลายบุคคล ขึ้นกับประเภทและระดับความเสี่ยงของธุรกรรม โดยมีแนวปฏิบัติเบื้องต้น ดังนี้

(๑) การลงลายมือชื่อโดยบุคคลเดียว (Single Signing) สำหรับเอกสารที่ต้องการการลงลายมือชื่อเพียงครั้งเดียวตามอำนาจหน้าที่ที่ได้กำหนดไว้ ตัวอย่างเช่น การลงลายมือชื่อในนามหัวหน้าส่วนราชการ หรือในนามนิติบุคคลโดยหัวหน้าส่วนราชการ ซึ่งเป็นผู้มีอำนาจตามที่ได้กำหนดไว้ในระเบียบ การลงลายมือชื่อโดยผู้รับมอบหมาย หรือมอบอำนาจ สำหรับการปฏิบัติภารกิจที่ได้รับมอบหมายหรือมอบอำนาจ การลงลายมือชื่อในนามบุคคลธรรมดา สำหรับจัดทำบันทึกข้อความของเจ้าหน้าที่โดยทั่วไป

(๒) การลงลายมือชื่อหลายบุคคล (Multiple Signing) ในกรณีที่มีการจัดตั้งคณะกรรมการ หรือคณะบุคคล เพื่อการปฏิบัติหน้าที่เฉพาะกิจ กรณีการลงนามตามสายบังคับบัญชา และกรณีการจัดทำสัญญาหลายฝ่าย เช่น สัญญาจัดซื้อจัดจ้าง บันทึกความร่วมมือระหว่างองค์กร โดยในกรณีนี้ จะมีพยานร่วมลงนามในเอกสาร ซึ่ง**ผู้ลงนามทุกคน<u>ควร</u>ใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทเดียวกัน**ใน

การลงลายมือชื่อบนเอกสารเดียวกัน เพื่อให้แนวทางการบริหารจัดการที่เกี่ยวข้องกับข้อมูลการลงลายมือชื่อและการตรวจสอบเป็นไปในทิศทางเดียวกัน

๕.๔ การใช้งานลายมือชื่ออิเล็กทรอนิกส์หลายประเภท

การประยุกต์ใช้งานลายมือชื่ออิเล็กทรอนิกส์ สามารถเลือกใช้งานประเภทของลายมือชื่ออิเล็กทรอนิกส์ให้สอดคล้องกับแนวทางการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ตามชนิดของหนังสือราชการ อย่างไรก็ดี บางตำแหน่งงาน ได้แก่ หัวหน้าส่วนราชการ อธิการบดี ผู้บริหาร และผู้มีอำนาจในการปฏิบัติหน้าที่เฉพาะ เช่น นายทะเบียน อาจใช้งานลายมือชื่ออิเล็กทรอนิกส์มากกว่าหนึ่งประเภท เพื่อแยกวัตถุประสงค์ในการใช้งานสำหรับการดำเนินการเอกสารต่างประเภท ซึ่งมีความเหมาะสมในการใช้ลายมือชื่ออิเล็กทรอนิกส์ในประเภทที่แตกต่างกันไป ตัวอย่างเช่น นายทะเบียนซึ่งได้รับมอบหมายให้ลงลายมือชื่อประเภทที่ ๓ สำหรับเอกสารรับรองหรือเอกสารสำคัญที่ออกให้แก่บุคคลภายนอก ในขณะที่การจัดทำบันทึกเพื่อติดต่อสื่อสารภายในส่วนราชการ สามารถใช้งานลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๒ ในฐานะเจ้าหน้าที่ทั่วไปได้ ดังนั้น ควรแยกดำเนินการตามแนวทางที่เหมาะสมสำหรับลายมือชื่อแต่ละประเภท

๕.๕ แนวทางการลงลายมือชื่อระหว่างสถานการณ์ฉุกเฉิน

การดำเนินการด้านเอกสารในรูปแบบอิเล็กทรอนิกส์มีส่วนสำคัญต่อการปฏิบัติงานของเจ้าหน้าที่ภาครัฐอย่างมีประสิทธิภาพ การหยุดชะงักของระบบอิเล็กทรอนิกส์สำหรับการจัดทำเอกสารและการลงลายมือชื่อในสถานการณ์ฉุกเฉิน อาจส่งผลต่อการปฏิบัติหน้าที่ ทำให้เกิดความล่าช้าหรืออาจไม่สามารถปฏิบัติหน้าที่ได้เลย ดังนั้น ส่วนราชการจึงควรจัดทำมาตรการและแผนรับมือต่อสถานการณ์ดังกล่าว เพื่อบรรเทาผลกระทบที่อาจเกิดขึ้น

๕.๕.๑ การเตรียมการก่อนสถานการณ์ฉุกเฉินและแนวทางการดำเนินการระหว่างสถานการณ์ฉุกเฉิน

ส่วนราชการ หรือหน่วยงานควรมีการจัดทำแผนการดำเนินการเพื่อให้เกิดความต่อเนื่องในการปฏิบัติงาน สำหรับรองรับสถานการณ์ฉุกเฉิน หรือสภาวะวิกฤติที่อาจเกิดขึ้นในพื้นที่ปฏิบัติงานและทำให้กระบวนการทำงานหยุดชะงัก ไม่ว่าจะเป็นภัยพิบัติทางธรรมชาติ เช่น อุทกภัย อัคคีภัย หรือเหตุชั่วคราวทางด้านโครงสร้างพื้นฐานที่อาจส่งผลให้เกิดข้อขัดข้องทางด้านเทคโนโลยีสารสนเทศและระบบไฟฟ้า ซึ่งสามารถประยุกต์ใช้แนวทางภายใต้คู่มือการบริหารความพร้อมต่อสภาวะวิกฤต [๑๐] โดยสำนักงานคณะกรรมการพัฒนาระบบราชการ (สำนักงาน ก.พ.ร.)

โดยแนวทางในเบื้องต้นสำหรับดำเนินการเกี่ยวกับงานสารบรรณและงานธุรการทั่วไป เมื่อเกิดสถานการณ์ฉุกเฉิน ควรมีการรายงานไปยังส่วนราชการ หรือผู้ที่เกี่ยวข้องเพื่อให้รับทราบสถานการณ์ รวมถึงรายละเอียดสำคัญ เช่น ผู้ประสานงานหลัก การดำเนินงานที่ได้รับผลกระทบ ทางเลือกที่เป็นไปได้สำหรับการดำเนินงานที่ได้รับผลกระทบ ซึ่งส่วนราชการควรใช้วิธีการทำงานที่ไม่ต้องพึ่งพาระบบ (Manual Work) คือ การลงลายมือชื่อบนเอกสารในรูปแบบกระดาษ

๕.๕.๒ แนวทางการบริหารจัดการหลังจากสถานการณ์ฉุกเฉินจบลง

หลังจากสถานการณ์กลับสู่ภาวะปกติ ควรมีการสร้างข้อมูลอิเล็กทรอนิกส์กลับขึ้นมาใหม่เพื่อการเก็บรักษา โดยสามารถอ้างอิงตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ โดยใช้ความระมัดระวังไม่ให้เกิดการทำซ้ำ หรือขาดตกบกพร่อง

ในการแปลงเอกสารให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้น ควรคำนึงถึงความละเอียดของภาพและสีที่กำหนดไว้เป็นขั้นต่ำ และต้องมีมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นวิธีการที่เชื่อถือได้ เพื่อให้สามารถยืนยันได้ว่า ข้อมูลอิเล็กทรอนิกส์ที่ได้จัดทำขึ้นนั้นดำเนินการโดยผู้มีสิทธิหรือผู้รับผิดชอบเท่านั้น โดยอย่างน้อยต้องครอบคลุมหัวข้อต่อไปนี้

- การระบุตัวตน (Identification)
- การยืนยันตัวตน (Authentication)
- การอนุญาตเฉพาะผู้มีสิทธิ์เข้าถึง (Authorization)
- ความรับผิดชอบต่อผลของการกระทำ (Accountability)

องค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์ครอบคลุมหลักเกณฑ์ดังกล่าว นั้นคือ มีการพิสูจน์และยืนยันตัวตนก่อนการลงลายมือชื่อ รวมถึงสามารถแสดงเจตนาการลงลายมือชื่อ ทำให้ลายมือชื่ออิเล็กทรอนิกส์มีความเหมาะสมในการใช้งานร่วมกับการแปลงเอกสารให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

ทั้งนี้ เอกสารและข้อความในรูปแบบกระดาษซึ่งถูกจัดทำขึ้นระหว่างสถานการณ์ฉุกเฉินจะมีฐานะเป็นต้นฉบับ ในขณะที่เอกสาร หรือข้อมูลอิเล็กทรอนิกส์ที่จัดทำขึ้นภายหลังนั้น จะมีฐานะเป็นเพียงสำเนาของเอกสารต้นฉบับ ซึ่งเจ้าหน้าที่ของรัฐสามารถทำการลงลายมือชื่ออิเล็กทรอนิกส์เพิ่มเติมเพื่อรับรองสำเนาดังกล่าวให้สอดคล้องกับหลักเกณฑ์ที่กำหนดไว้ โดยผู้จัดทำเอกสารต้นฉบับและผู้รับรองสำเนาจะเป็นบุคคลเดียวกันหรือไม่ก็ได้

๕.๖ แนวทางการลงลายมือชื่อสำหรับส่วนราชการที่ไม่มีความพร้อม

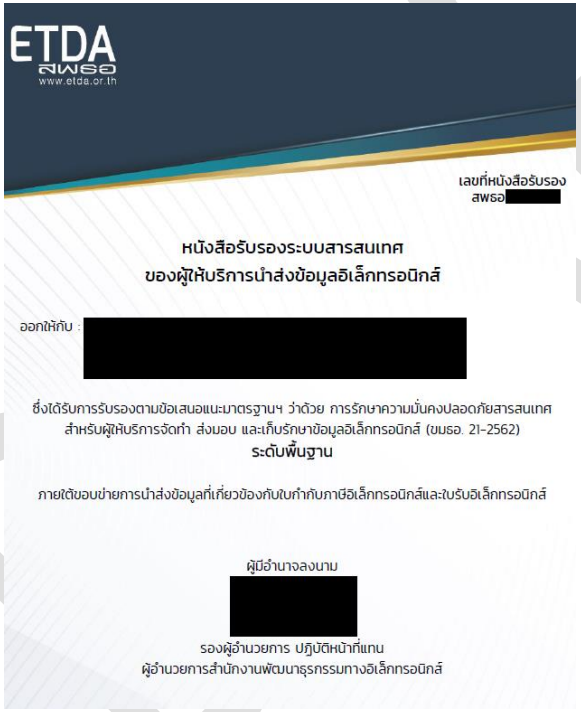
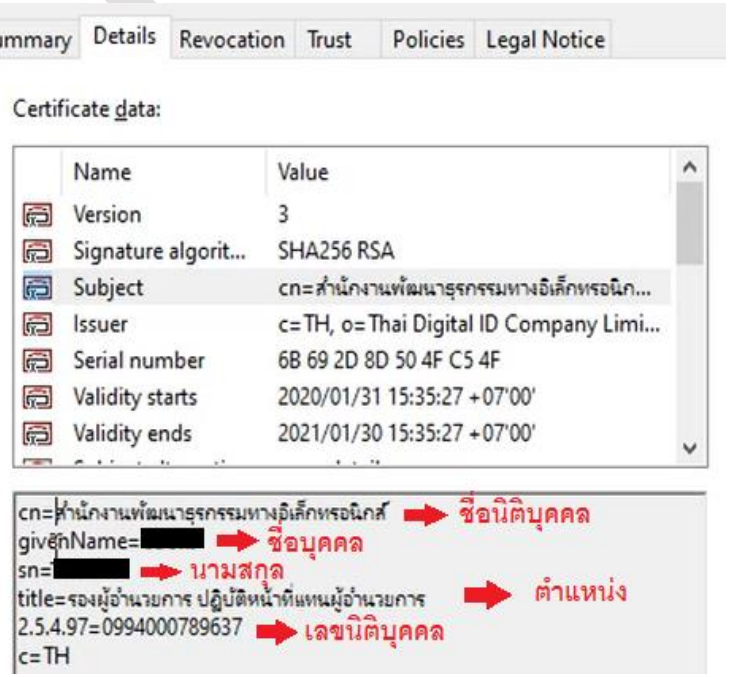
กรณีส่วนราชการมีเหตุจำเป็นซึ่งไม่สามารถดำเนินการทางเอกสารผ่านระบบอิเล็กทรอนิกส์ได้ เช่น ส่วนราชการที่ไม่สามารถเข้าถึงเครือข่ายอินเทอร์เน็ต ระบบอินเทอร์เน็ตขาดเสถียรภาพ หรือไม่มีระบบเทคโนโลยีสารสนเทศที่มีประสิทธิภาพเพียงพอ เนื่องจากอยู่ในพื้นที่ห่างไกล เจ้าหน้าที่ของรัฐสามารถอ้างอิงแนวปฏิบัติในการรับ-ส่งหนังสือราชการทางอิเล็กทรอนิกส์ระหว่างส่วนราชการที่เป็นนิติบุคคลโดยสำนักงานคณะกรรมการพัฒนาระบบราชการ (สำนักงาน ก.พ.ร.) [๑๑] โดยส่วนราชการที่ไม่มีความพร้อมอาจแจ้งส่วนราชการผู้จัดส่งเอกสารเพื่อขอรับหนังสือในรูปแบบกระดาษ หรือเจ้าหน้าที่ผู้รับผิดชอบในการรับหนังสือราชการอิเล็กทรอนิกส์ อาจพิมพ์ออกและลงลายมือชื่อด้วยหมึกเพื่อรับรองเอกสาร ก่อนที่จะส่งต่อไปยังส่วนราชการที่ไม่มีความพร้อมเพื่อให้สามารถดำเนินการต่อในรูปแบบกระดาษได้

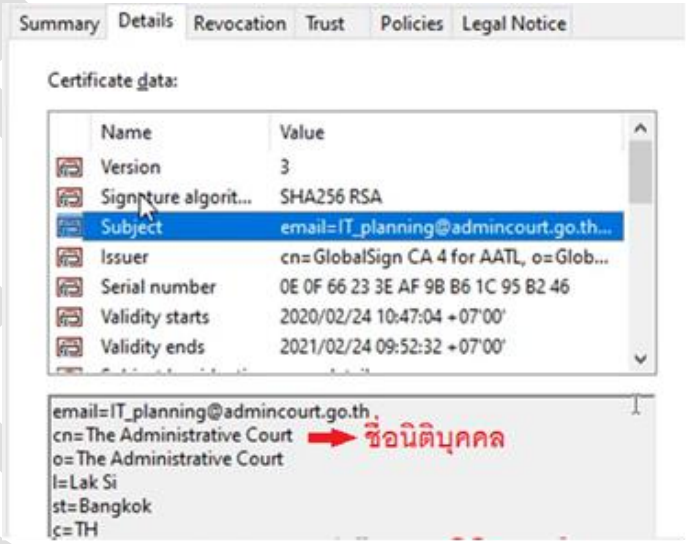
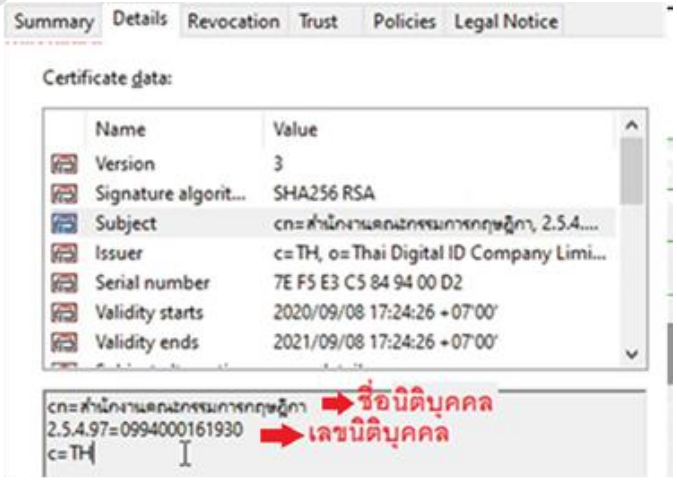
หากเป็นหนังสือที่ส่วนราชการซึ่งไม่มีความพร้อมจัดทำเพื่อส่งออกไปยังภายนอก ซึ่งเป็นธุรกรรมที่มีความสำคัญ และส่วนราชการปลายทางมีการรับเอกสารผ่านระบบสารบรรณอิเล็กทรอนิกส์หรืออีเมลเท่านั้น ต้นสังกัดของส่วนราชการที่ไม่มีความพร้อมควรจัดให้มีอุปกรณ์พร้อมระบบเทคโนโลยีสารสนเทศ ณ สำนักงานในเขตพื้นที่ เช่น ศาลากลางจังหวัด สำนักงานประจำจังหวัดหรือภาค เพื่อให้ส่วนราชการที่ไม่มีความพร้อมดังกล่าว สามารถยืมใช้งานอุปกรณ์ในการจัดทำเอกสารอิเล็กทรอนิกส์และลงลายมือชื่ออิเล็กทรอนิกส์

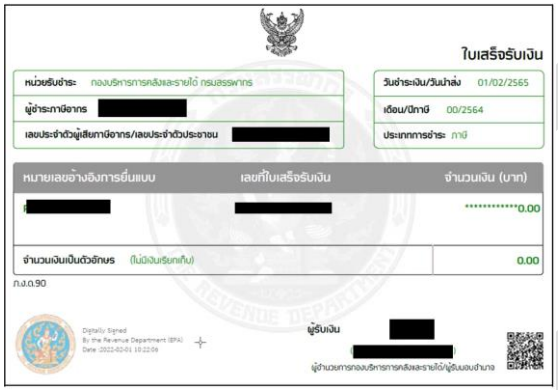
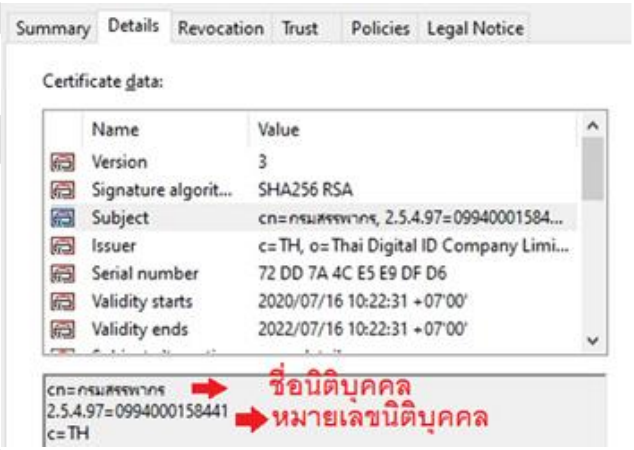
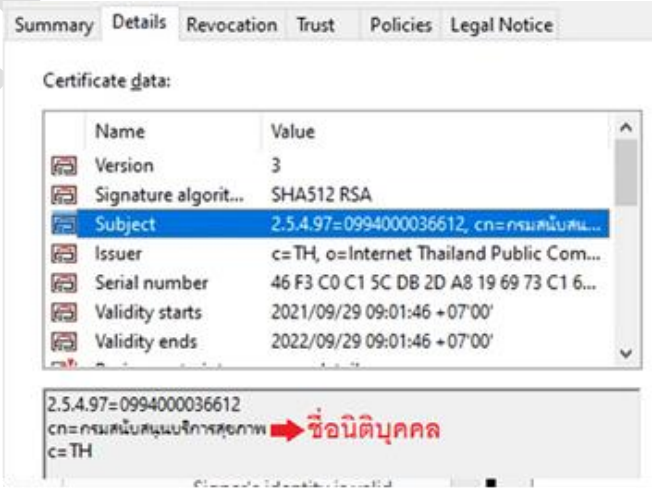
๕.๗ ตัวอย่างการใช้ลายมือชื่ออิเล็กทรอนิกส์ในเอกสารราชการ

การใช้ลายมือชื่ออิเล็กทรอนิกส์ในเอกสารราชการที่มีการใช้งานลายมือชื่อต่างกันในแต่ละประเภทของเอกสารซึ่งได้รวบรวมและแสดงได้ดังตารางที่ ๔ (ใส่ Comment ว่ามาจากมติ Tc1 1/2565 วาระพิจารณา)

ตารางที่ ๔ ตัวอย่างการใช้ลายมือชื่ออิเล็กทรอนิกส์ในเอกสารราชการ

เอกสาร	ภาพตัวอย่างเอกสารรูปแบบ PDF และข้อมูลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ (CA)	
๑. หนังสือรับรองระบบสารสนเทศของผู้ให้บริการนำส่งข้อมูลทางอิเล็กทรอนิกส์ ของ สพธอ. แนวทางการใช้งานเอกสารต้นฉบับและการลงลายมือชื่อเป็นอิเล็กทรอนิกส์ตั้งแต่ต้น ซึ่งมีการลงลายมือชื่ออิเล็กทรอนิกส์โดยใช้ใบรับรองอิเล็กทรอนิกส์ของบุคคล (โดยระบุชื่อ นามสกุล หน่วยงานที่สังกัด ตำแหน่งหน้าที่ชัดเจน)		

เอกสาร	ภาพตัวอย่างเอกสารรูปแบบ PDF และข้อมูลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ (CA)	
๒.เอกสารการขอคัดคำพิพากษาจากเว็บไซต์ของศาลปกครอง มีการลงลายมือชื่อบนกระดาษและสแกนเอกสารเป็นไฟล์อิเล็กทรอนิกส์ โดยมีการลงลายมือชื่ออิเล็กทรอนิกส์ทับลงไปในเอกสาร เพื่อไม่ให้เกิดการแก้ไขเปลี่ยนแปลงได้ในภายหลัง โดยเป็นใบรับรองอิเล็กทรอนิกส์ที่ออกให้หน่วยงาน หรือองค์กร (นิติบุคคล)		
๓.หนังสือเชิญประชุมจากสำนักงานกฤษฎีกา มีการลงลายมือชื่อบนกระดาษและสแกนเอกสารเป็นไฟล์อิเล็กทรอนิกส์ โดยมีการลงลายมือชื่ออิเล็กทรอนิกส์ทับลงไปในเอกสาร เพื่อไม่ให้เกิดการแก้ไขเปลี่ยนแปลงได้ในภายหลัง โดยเป็นใบรับรองอิเล็กทรอนิกส์ที่ออกให้องค์กร (ใบรับรองนิติบุคคล โดยมีเลขนิติบุคคลขององค์กรแสดง)		

เอกสาร	ภาพตัวอย่างเอกสารรูปแบบ PDF และข้อมูลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ (CA)	
๔. ใบเสร็จรับเงินอิเล็กทรอนิกส์โดยกรมสรรพากร มีการนำลายมือชื่อที่เป็นภาพมาการนำลายมือชื่อที่เป็นภาพมาวาง ก่อนมีการลงลายมือชื่ออิเล็กทรอนิกส์โดยใบรับรองอิเล็กทรอนิกส์ขององค์กร		
๕. เอกสารใบอนุญาตโดยผู้มีอำนาจลงนาม ๒ ท่าน ขึ้นไป เอกสารนี้เป็นลักษณะของเอกสารที่ผู้มีอำนาจหลายคนลงนามบนเอกสารเดียวกันมีการนำลายมือชื่อที่เป็นภาพมาวาง ก่อนมีการลงลายมือชื่ออิเล็กทรอนิกส์โดยใบรับรองอิเล็กทรอนิกส์ขององค์กร (ใบรับรองนิติบุคคล) เพื่อไม่ให้เกิดการแก้ไขเปลี่ยนแปลงได้ในภายหลัง		

หมายเหตุ *ตัวอย่างกรณีศึกษาเป็นเอกสารจากหน่วยงานภาครัฐ นำเสนอในการประชุมคณะทำงานเทคนิคด้านความปลอดภัยภาครัฐครั้งที่ ๑/๒๕๖๕*

จากกรณีตัวอย่าง (ตารางที่ ๔) เป็นแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ของบุคคล สามารถใช้งานลายมือชื่อประเภทที่ ๓ โดยใช้ใบรับรอง (CA) ที่ออกให้เฉพาะบุคคล เช่น นายทะเบียน ผู้มีอำนาจออกใบอนุญาต หรือใบรับรอง ซึ่งเป็นของเจ้าหน้าที่ผู้ใดผู้หนึ่งในหน่วยงาน เช่น กรณีตัวอย่างที่ ๑

หมายเหตุ

กรณีที่หน่วยงานมีการโยกย้าย ปรับเปลี่ยนตำแหน่ง หรือลาออกของบุคลากร และจำเป็นต้องใช้งานใบรับรองจำนวนมากอาจมีผลกระทบต่อค่าใช้จ่ายในการดำเนินงาน อาจพิจารณาใช้งานลายมือชื่อประเภทที่ ๑ ของบุคคล ร่วมกับลายมือชื่อประเภทที่ ๓ ที่ใช้ใบรับรองของนิติบุคคล ซึ่งสามารถดำเนินการตามตัวอย่างกรณีที่ ๒-๕ โดยเอกสารที่ลงนามจะสามารถระบุผู้ลงนาม แสดงเจตนา และมีช่องทางที่ปลอดภัยอย่างครบถ้วน

๖. แนวทางการพัฒนาระบบลงลายมือชื่ออิเล็กทรอนิกส์

๖.๑ องค์ประกอบระบบลงลายมือชื่ออิเล็กทรอนิกส์ที่แนะนำ

การพัฒนาระบบลงลายมือชื่ออิเล็กทรอนิกส์ให้มีคุณสมบัติสอดคล้องตามมาตรา ๙ หรือมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ มีความจำเป็นต้องอาศัยโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศที่มีความน่าเชื่อถือ เป็นไปตามมาตฐานสากล อีกทั้งมีความมั่นคงปลอดภัยและบริหารจัดการข้อมูลส่วนบุคคลของผู้ใช้งานอย่างเหมาะสม สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ตามลำดับ โดยระบบลงลายมือชื่ออิเล็กทรอนิกส์ ควรให้บริการ ๕ ส่วนดังนี้ [๙]

(๑) อุปกรณ์จัดเก็บกุญแจ (Key Storage) คือ ฮาร์ดแวร์ หรือ ซอฟต์แวร์ ที่อยู่ภายใต้การควบคุมของผู้ลงนาม มีหน้าที่หลักในการใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ รวมถึงการบริหารจัดการและใช้งานกุญแจส่วนตัวในกรณีของลายมือชื่อดิจิทัล

(๒) โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) คือ นโยบาย มาตรการ และระบบเทคโนโลยีสารสนเทศ สำหรับการสร้าง และบริหารจัดการใบรับรอง ทั้งใบรับรองส่วนบุคคลและนิติบุคคล รวมทั้งการกำหนดความเชื่อมโยงระหว่างกุญแจสาธารณะและผู้ลงนาม โดยองค์ประกอบนี้อาจถูกละเว้นหากไม่ได้ใช้งานลายมือชื่อดิจิทัล

(๓) บริการเอกสารอิเล็กทรอนิกส์ (E-Document Service) คือ ระบบเทคโนโลยีสารสนเทศที่ทำหน้าที่บริหารจัดการเอกสารอิเล็กทรอนิกส์ตลอดวงจรชีวิตการใช้งาน โดยอาจรวมถึงการบริหารจัดการกระบวนการดำเนินงานด้านเอกสาร (Workflow)

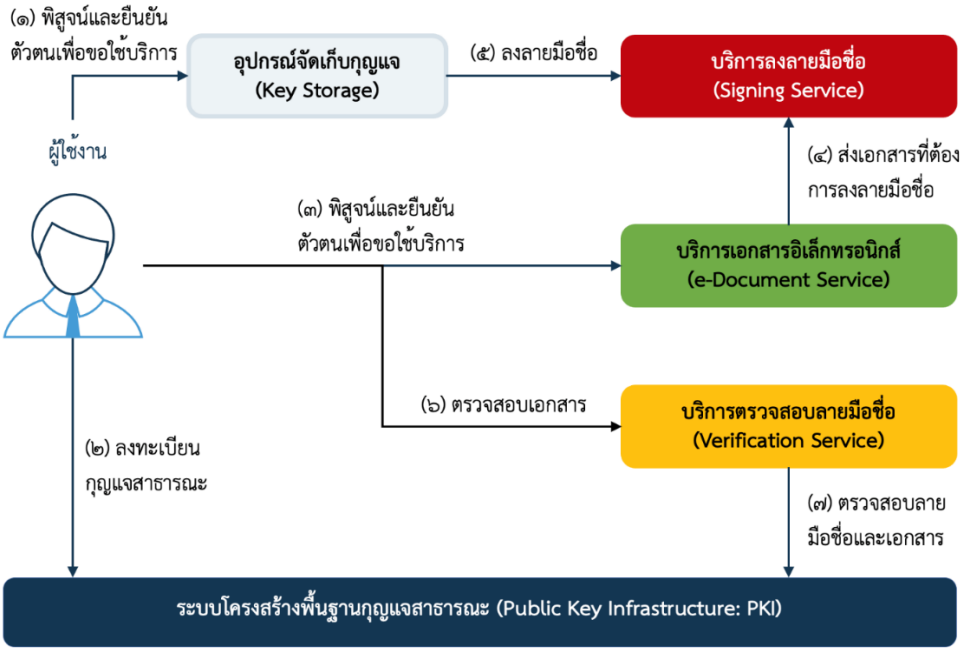
(๔) บริการลงลายมือชื่อ (Signing Service) คือ ระบบเทคโนโลยีสารสนเทศให้บริการลงลายมือชื่ออิเล็กทรอนิกส์ โดยอาศัยข้อมูลจากอุปกรณ์จัดเก็บกุญแจ และเอกสารจากบริการเอกสารอิเล็กทรอนิกส์

(๕) บริการตรวจสอบลายมือชื่อ (Verification Service) คือ ระบบเทคโนโลยีสารสนเทศที่ทำหน้าที่ตรวจสอบลายมือชื่ออิเล็กทรอนิกส์และเอกสารอิเล็กทรอนิกส์ที่ถูกลงลายมือชื่อ โดยอาศัยข้อมูลกุญแจสาธารณะที่ได้รับการรับรองการโครงสร้างพื้นฐานกุญแจสาธารณะ

การแบ่งองค์ประกอบการทำงานของระบบลงลายมือชื่ออิเล็กทรอนิกส์โดยสังเขปเพื่อเป็นแนวทางเบื้องต้นให้กับหน่วยงานของรัฐ โดยสามารถประยุกต์แนวทางการพัฒนาระบบได้หลากหลายรูปแบบ ซึ่งมีข้อแนะนำเบื้องต้นดังนี้

- อาจควบรวมองค์ประกอบให้ทำงานร่วมกัน หรือใช้บริการบางองค์ประกอบจากผู้ให้บริการภายนอกองค์กร เช่น ในกรณีของการลงลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๑ ไม่จำเป็นต้องมีอุปกรณ์จัดเก็บกุญแจและโครงสร้างพื้นฐานกุญแจสาธารณะ
- ควรมีการจัดเก็บข้อมูลเพื่อเป็นพยานหลักฐานที่จำเป็นตามลักษณะของธุรกรรม
- ควรมีการกำหนดนโยบายการใช้งานลายมือชื่อ (Signature Policy) ซึ่งรวมถึง นโยบายการสร้างลายมือชื่อ (Signature Creation Policy) นโยบายการตรวจสอบลายมือชื่อ (Signature Validation Policy) และนโยบายการเสริมการทำงานของลายมือชื่อ (Signature Augmentation Policy) เช่น การเพิ่มข้อมูลเพื่อการตรวจสอบลายมือชื่อในระยะยาว (Long-Term Validation) [๙]

๖.๑.๑ แนวทางการดำเนินงานของระบบลงลายมือชื่ออิเล็กทรอนิกส์ที่แนะนำ



รูปที่ ๓ องค์ประกอบและหลักการทำงานเบื้องต้นของระบบลงลายมือชื่ออิเล็กทรอนิกส์

กระบวนการทำงานของระบบลงลายมือชื่ออิเล็กทรอนิกส์ ควรมีขั้นตอนพื้นฐานดังภาพที่ ๓ ซึ่งมีขั้นตอนดังนี้

(๑) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนก่อนเริ่มการใช้งานระบบ และต้องทำการยืนยันตัวตนก่อนการใช้งานกุญแจ (Key Storage) ทั้งการสร้างคู่กุญแจส่วนตัวและกุญแจสาธารณะ หรือเข้าถึงเพื่อใช้งานหรือบริหารจัดการในภายหลัง

(๒) ผู้ใช้งานต้องลงทะเบียนกุญแจสาธารณะกับโครงสร้างพื้นฐานกุญแจสาธารณะเพื่อขอใบรับรองในกรณีใช้งานลายมือชื่อดิจิทัล (PKI)

(๓) ผู้ใช้งานบริหารจัดการเอกสารอิเล็กทรอนิกส์ผ่านบริการเอกสารอิเล็กทรอนิกส์ โดยบริการเอกสารอิเล็กทรอนิกส์ควรกำหนดให้ผู้ใช้งานทำการพิสูจน์ตัวตนก่อนเริ่มการใช้งาน และทำการยืนยันตัวตนก่อนการใช้งานแต่ละครั้ง

(๔) ผู้ใช้งานร้องขอการลงลายมือชื่อจากบริการเอกสารอิเล็กทรอนิกส์โดยอาจเชื่อมต่อไปยังบริการลงลายมือชื่อ

(๕) บริการลงลายมือชื่อขอข้อมูลจากอุปกรณ์จัดเก็บกุญแจเพื่อสร้างลายมือชื่อบนเอกสารอิเล็กทรอนิกส์ ซึ่งควรมีการยืนยันตัวตนก่อนทุกครั้ง

(๖) ผู้ใช้งานควรจะสามารถตรวจสอบลายมือชื่อและเอกสารอิเล็กทรอนิกส์ที่ถูกลงลายมือชื่อ ผ่านบริการตรวจสอบลายมือชื่อได้

(๗) ในกรณีของลายมือชื่อดิจิทัล บริการตรวจควรจะสามารถสอบลายมือชื่อทำการตรวจสอบลายมือชื่อและเอกสารอิเล็กทรอนิกส์ที่ถูกลงลายมือชื่อ โดยเชื่อมต่อกับโครงสร้างพื้นฐานกุญแจสาธารณะ

๖.๑.๒ อุปกรณ์จัดเก็บกุญแจ

อุปกรณ์จัดเก็บกุญแจ (Key Storage) ทำหน้าที่สร้างลายมือชื่ออิเล็กทรอนิกส์จากคำสั่งของผู้ลงนามและบริหารจัดการข้อมูลที่เกี่ยวข้อง ผู้ใช้งานต้องทำการพิสูจน์ตัวตนก่อนเริ่มการใช้งานระบบและต้องทำการยืนยันตัวตนก่อนการใช้งานกุญแจ โดยอาจบันทึกข้อมูลเอกสารอิเล็กทรอนิกส์และข้อมูลพยานหลักฐานประกอบการลงลายมือชื่ออิเล็กทรอนิกส์ รวมทั้งทำหน้าที่ในการเชื่อมต่อและแลกเปลี่ยนข้อมูลกับระบบอื่น

อุปกรณ์จัดเก็บกุญแจต้องทำหน้าที่บริหารจัดการกุญแจส่วนตัวให้มีความมั่นคงปลอดภัย เพื่อป้องกันไม่ให้ผู้อื่นซึ่งไม่ได้รับการอนุญาตลงลายมือชื่อแทน โดยอาจเลือกลักษณะการจัดเก็บกุญแจส่วนตัวรูปแบบใดรูปแบบหนึ่งตามความเหมาะสมจาก ๒ ประเภท [๑๒] ได้แก่

(๑) การจัดเก็บกุญแจส่วนตัวไว้ภายในอุปกรณ์ในครอบครองของผู้ใช้งาน (Edge Computing) เช่น คอมพิวเตอร์ส่วนบุคคล แท็บเล็ต หรือ โทรศัพท์สมาร์ตโฟน โดยมี**ข้อดี**คือกุญแจส่วนตัวอยู่ภายใต้การควบคุมดูแลของผู้ใช้งานโดยแท้จริง อีกทั้งมีความเสี่ยงต่ำจากการถูกโจมตีทางไซเบอร์ (Cyber Attack) แต่มี**ข้อเสีย**คือผู้ใช้งานมีภาระในการจัดเก็บและสำรองข้อมูล (Backup) กุญแจส่วนตัวด้วยตนเอง ซึ่งกุญแจส่วนตัวมีโอกาสสูญหายได้หากผู้ใช้งานขาดไม่ระมัดระวัง

(๒) การจัดเก็บกุญแจส่วนตัวไว้บนคลาวด์คอมพิวเตอร์ (Cloud Computing) ซึ่งไม่อยู่ในครอบครองของผู้ใช้งาน โดยผู้ใช้งานสามารถเข้าถึงกุญแจส่วนตัวผ่านระบบของผู้ให้บริการดูแลกุญแจส่วนตัว (Custodian) โดยมี**ข้อดี**คือผู้ใช้งานไม่มีภาระในการบริหารจัดการกุญแจส่วนตัวโดยตรง อีกทั้งระบบคลาวด์คอมพิวเตอร์มีการสำรองข้อมูลโดยอัตโนมัติ แต่มี**ข้อเสีย**คือข้อมูลกุญแจส่วนตัวอยู่ภายใต้การควบคุมดูแลของผู้ให้บริการ ซึ่งมีโอกาสถูกโจมตีทางไซเบอร์ (Cyber Attack) ทำให้ความมั่นคงปลอดภัยของกุญแจส่วนตัวนั้น ขึ้นอยู่กับความน่าเชื่อถือของผู้ให้บริการ

๖.๑.๓ บริการเอกสารอิเล็กทรอนิกส์

บริการเอกสารอิเล็กทรอนิกส์ (E-Document Service) ทำหน้าที่บริหารจัดการเอกสารอิเล็กทรอนิกส์ตลอดวงจรชีวิตของเอกสาร ตาม ขมธอ. ๑๑-๒๕๖๐ [๕] และเชื่อมต่อกับบริการอื่น ๆ เพื่ออำนวยให้เกิดการลงลายมือชื่ออิเล็กทรอนิกส์ รวมถึงการบริหารจัดการกระแสงาน (Workflow) เพื่อจัดลำดับในการดำเนินงานเอกสารและลำดับในการลงลายมือชื่อ ในกรณีที่เอกสารต้องการการลงลายมือชื่อหลายบุคคล โดยมีข้อแนะนำเบื้องต้นดังนี้

- ระบบควรมีการพิสูจน์และยืนยันตัวตนผู้ใช้งานเพื่อตรวจสอบอำนาจในการลงลายมือชื่อในเอกสารตามกฎหมาย ระเบียบ หรือข้อบังคับที่ส่วนราชการได้จัดทำไว้ รวมทั้งระบบควรทำการบันทึกพยานหลักฐานที่เหมาะสมกับประเภทของลายมือชื่ออิเล็กทรอนิกส์ ตาม ขมธอ. ๒๓–๒๕๖๓ [๓]
- บริการเอกสารอิเล็กทรอนิกส์อาจเชื่อมต่อเข้ากับบริการประเภทอื่น ๆ นอกเหนือไปจากการลงลายมือชื่ออิเล็กทรอนิกส์ เช่น บริการประทับรับรองเวลาอิเล็กทรอนิกส์ (E-Timestamping Service) และบริการอากรแสตมป์ (E-Stamp Duty Service)

๖.๑.๔ บริการลงลายมือชื่อ

บริการลงลายมือชื่อ (Signing Service) ทำหน้าที่อำนวยการลงลายมือชื่ออิเล็กทรอนิกส์บนเอกสารอิเล็กทรอนิกส์โดยเชื่อมต่อกับอุปกรณ์จัดเก็บกุญแจและบริการเอกสารอิเล็กทรอนิกส์ เพื่อรับเอกสารที่ต้องการลงลายมือชื่อและสร้างลายมือชื่ออิเล็กทรอนิกส์ผ่านกุญแจส่วนตัว จากนั้น จึงส่งเอกสารอิเล็กทรอนิกส์ที่ลงลายมือชื่อเรียบร้อยแล้วกลับไปยังบริการเอกสารอิเล็กทรอนิกส์ โดยมีข้อแนะนำเบื้องต้นดังนี้

- การสร้างลายมือชื่ออิเล็กทรอนิกส์ควรเกิดขึ้นภายในอุปกรณ์จัดเก็บกุญแจ โดยที่บริการลงลายมือชื่อไม่ควรได้รับข้อมูลกุญแจส่วนตัวของผู้ใช้งานโดยตรง
- บริการลงลายมือชื่อควรดำเนินการลบข้อมูลเอกสารหรือข้อมูลส่วนบุคคลใด ๆ ภายหลังการลงลายมือชื่อ หากไม่มีเหตุจำเป็นต้องจัดเก็บข้อมูลดังกล่าว เพื่อบรรเทาความเสี่ยงจากภัยคุกคามทางไซเบอร์และการรั่วไหลของข้อมูลส่วนบุคคล

๖.๑.๕ บริการตรวจสอบลายมือชื่อ

บริการตรวจสอบลายมือชื่อ (Verification Service) ทำหน้าที่เชื่อมต่อกับระบบโครงสร้างพื้นฐานกุญแจสาธารณะเพื่อตรวจสอบลายมือชื่อและเอกสาร เพื่อยืนยันว่าไม่มีการปลอมแปลง หรือแก้ไขข้อมูล รวมทั้งระบุตัวตนของผู้ลงนาม และเจตนาในการลงลายมือชื่อ รวมทั้งตรวจสอบรายการเพิกถอนใบรับรองเพื่อตรวจสอบว่าลายมือชื่อนั้นไม่ถูกสร้างขึ้นจากใบรับรองถูกยกเลิกไปแล้ว

- ผู้ใช้งานควรจะสามารถตรวจสอบลายมือชื่อและเอกสารอิเล็กทรอนิกส์ที่ถูกลงลายมือชื่อ ผ่านบริการตรวจสอบลายมือชื่อได้
- ในกรณีของลายมือชื่อดิจิทัล บริการตรวจควรจะสามารถตรวจสอบลายมือชื่อโดยเชื่อมต่อกับโครงสร้างพื้นฐานกุญแจสาธารณะ
- บริการตรวจสอบลายมือชื่อควรดำเนินการลบข้อมูลเอกสารหรือข้อมูลส่วนบุคคลใด ๆ ภายหลังการลงลายมือชื่อ หากไม่มีเหตุจำเป็นต้องจัดเก็บข้อมูลดังกล่าว เพื่อบรรเทาความเสี่ยงจากภัยคุกคามทางไซเบอร์และการรั่วไหลของข้อมูลส่วนบุคคล

๖.๒ แนวทางการบริหารจัดการกุญแจส่วนตัวสำหรับบุคคล

- อุปกรณ์จัดเก็บกุญแจซึ่งบริหารจัดการกุญแจส่วนตัวสำหรับบุคคลและเจ้าหน้าที่นิติบุคคล ต้องมีความมั่นคงปลอดภัย สามารถรับประกันว่าผู้ใช้งานซึ่งเป็นเจ้าของกุญแจส่วนตัว เป็นเพียงบุคคลเดียวที่สามารถลงลายมือชื่อได้ด้วยกุญแจส่วนตัวนั้น ๆ โดยกำหนดแนวทางเบื้องต้นสำหรับการบริหารจัดการกุญแจส่วนตัว ดังนี้
- ควรใช้กุญแจประเภท Rsa ขนาด 2048 Bits หรือ Ecdsa ขนาด 256 Bits เป็นอย่างน้อย หรือกุญแจประเภทอื่น ๆ ที่มีความปลอดภัยเทียบเท่า ตามมาตรฐานสากล เช่น Nist Sp 800-57 Part 3 [๑๓]
- ต้องทำการยืนยันตัวตนผู้ใช้งานเพื่อเข้าถึงกุญแจส่วนตัว ก่อนการลงลายมือชื่อทุกครั้ง โดยเลือกใช้สิ่งที่ใช้ยืนยันตัวตน (Authenticators) ตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level: Aal) ที่เหมาะสมกับประเภทของธุรกรรม [๑๔][๑๕]
- ต้องจัดเก็บกุญแจส่วนตัวให้มีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ โดยใช้มาตรฐานการจัดเก็บกุญแจที่น่าเชื่อถือ เช่น เข้ารหัสกุญแจส่วนตัวตามมาตรฐาน Pkcs #12 [๑๖] หรือจัดเก็บภายในอุปกรณ์ที่น่าเชื่อถือ เช่น อุปกรณ์ Secure Enclave ตามมาตรฐานสากล เช่น Fips 140-3 Security Level 1 เป็นอย่างน้อย [๑๗]
- ควรจัดทำแนวทางและมาตรการการเพิกถอน (Revocation) และ/หรือการกู้คืนข้อมูล (Recovery) กุญแจส่วนตัว
- ควรบริการจัดการกุญแจส่วนตัวตลอดวงจรชีวิต ตามมาตรฐานสากล เช่น Nist Sp 800-57 Part 1 [๑]
- ควรบันทึกประวัติการใช้งานกุญแจส่วนตัว เพื่อเป็นพยานหลักฐานประกอบการลงลายมือชื่อ
- ต้องมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้งานไม่ให้รั่วไหลหรือถูกนำไปใช้โดยไม่ได้รับอนุญาต

๖.๓ แนวทางการบริหารจัดการกุญแจส่วนตัวสำหรับนิติบุคคล

กุญแจส่วนบุคคลสำหรับนิติบุคคลอาจมีเจ้าหน้าที่มากกว่า ๑ คนที่มีสิทธิ์เข้าถึงกุญแจส่วนตัว เช่น ผู้บริหารระดับสูงและเจ้าหน้าที่ผู้ได้รับมอบอำนาจให้ลงลายมือชื่อแทนหัวหน้าส่วนราชการ ดังนั้น แนวทางการบริหารจัดการกุญแจส่วนตัวสำหรับนิติบุคคลจึงมีข้อกำหนดเพิ่มเติม ดังนี้

- ต้องกำหนดนโยบายและมาตรการบริหารจัดการการเข้าถึงข้อมูลกุญแจส่วนตัว ของผู้ใช้งานที่มีสิทธิ์หรือได้รับมอบอำนาจ
- ต้องกำหนดนโยบายและมาตรการบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามมาตรฐาน เช่น Iso/Iec 27001 [๑๘]
- ควรจัดทำบันทึกการตรวจสอบ (Audit Trail) เพื่อบันทึกการใช้งานกุญแจส่วนตัวของผู้ใช้งานทั้งหมด
- ควรใช้อุปกรณ์ที่น่าเชื่อถือในการจัดเก็บกุญแจส่วนตัว ตามมาตรฐานสากล เช่น Nist Fips 140-3 Security Level 2 เป็นอย่างน้อย [๑๗]

๖.๔ แนวทางการกำหนดวงจรชีวิตกุญแจส่วนตัว

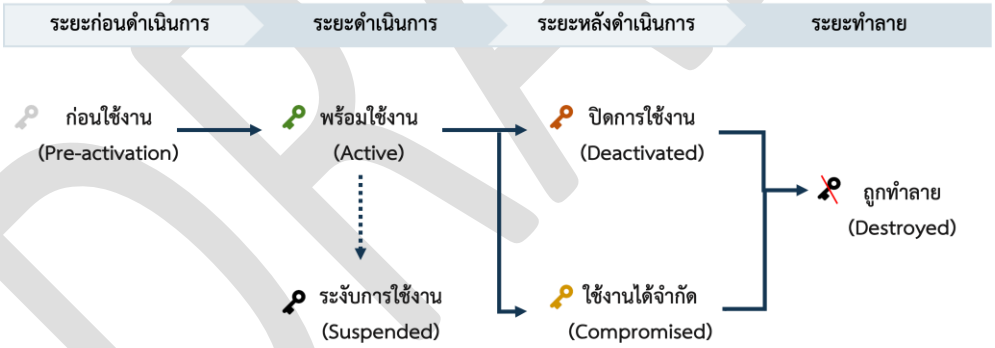
อุปกรณ์จัดเก็บกุญแจมีหน้าที่ในการบริการจัดการกุญแจส่วนตัวตลอดวงจรชีวิต ตั้งแต่การสร้างกุญแจไปจนถึงการทำลายกุญแจ ให้มีความมั่นคงปลอดภัยและเป็นไปตามมาตรฐาน โดยระบบอาจมีการแบ่งระยะการใช้งานกุญแจส่วนตัวออกเป็น ๔ ระยะ ดังนี้ [๑]

(๑) ระยะก่อนดำเนินการ กุญแจถูกสร้างขึ้นและอยู่ในสถานะก่อนใช้งาน (Pre-Activation) โดยถูกด้วยขึ้นด้วยอัลกอริทึมที่มีความมั่นคงปลอดภัยและเป็นไปตามมาตรฐาน

(๒) ระยะดำเนินการ เมื่อผู้ใช้งานทำการพิสูจน์ยืนยันสิทธิในการเข้าถึงและใช้งาน กุญแจจะเปลี่ยนเป็นสถานะพร้อมใช้งาน (Active) โดยระหว่างการใช้งานเมื่อมีเหตุที่ผู้ใช้งานไม่สามารถเข้าถึงกุญแจได้หรือคาดว่ากุญแจอาจถูกเข้าถึงโดยผู้ไม่ได้รับอนุญาต ผู้ใช้งานสามารถเปลี่ยนกุญแจให้เป็นสถานะถูกระงับการใช้งาน (Suspended) และสามารถเปลี่ยนกลับเป็นสถานะพร้อมใช้งานได้ในภายหลัง

(๓) ระยะหลังดำเนินการ กุญแจจะไม่สามารถถูกใช้งานได้เมื่อกุญแจมีอายุการใช้งานครบตามที่กำหนด (Cryptoperiod) โดยผู้ใช้งานสามารถเปลี่ยนกุญแจให้เป็นสถานะถูกปิดการใช้งาน (Deactivated) หรือถูกจำกัดการใช้งาน (Compromised) ก่อนครบกำหนดอายุการใช้งาน ในกรณีที่ผู้ใช้งานต้องการเปลี่ยนกุญแจ กุญแจเกิดการสูญหาย หรือกุญแจถูกเข้าถึงได้โดยผู้ที่ไม่ได้รับอนุญาต

(๔) ระยะการทำลาย กุญแจส่วนตัวและข้อมูลสำรองที่เกี่ยวข้องต้องถูกทำลาย (Destroyed) ทำให้ไม่สามารถเข้าถึงหรือใช้งานได้อีกต่อไป โดยข้อมูล Metadata ของกุญแจอาจไม่จำเป็นต้องถูกทำลายไปพร้อมกับกุญแจ



รูปที่ ๔ แผนภาพแสดงวงจรชีวิตกุญแจส่วนตัว

๖.๕ แนวทางการกู้คืนและเพิกถอนกุญแจ

ผู้ลงนามด้วยลายมือชื่อดิจิทัลมีความเสี่ยงที่จะสูญเสียการเข้าถึงกุญแจส่วนบุคคล ทำให้ไม่สามารถลงลายมือชื่อได้ด้วยกุญแจส่วนบุคคลดังกล่าวอีกต่อไป ดังนั้นอุปกรณ์จัดเก็บกุญแจจึงควรกำหนดมาตรการในการบริหารจัดการความเสี่ยง ทั้งจากกรณีที่อุปกรณ์จัดเก็บกุญแจส่วนตัวเกิดการสูญหายหรือเสียหาย (Data Corruption) และการกรณีที่เกิดภัยคุกคามทางไซเบอร์ โดยอาจจะกำหนดนโยบายและมาตรการสำรอง (Backup) และกู้คืน (Recovery) ข้อมูลกุญแจส่วนตัว ได้ทั้งหมด ๓ รูปแบบ ได้แก่

(๑) การกู้คืนข้อมูลแบบออฟไลน์ (Offline Recovery หรือ Cold Storage) สำรองข้อมูลกุญแจส่วนตัวภายในอุปกรณ์ซึ่งไม่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต โดยอุปกรณ์ที่ใช้สำรองข้อมูลควรมีอายุการใช้งานยาวนานเพียงพอต่ออายุการใช้งานของกุญแจ (Cryptoperiod)

(๒) การกู้คืนข้อมูลแบบออนไลน์ (Online Recovery หรือ Hot Storage) สำรองข้อมูลกุญแจส่วนตัวบนระบบคลาวด์คอมพิวเตอร์ โดยควรเลือกใช้บริการจากผู้ให้บริการคลาวด์คอมพิวเตอร์ที่น่าเชื่อถือ และควรจัดเก็บกุญแจส่วนตัวที่ถูกเข้ารหัสแล้วด้วยกุญแจส่วนตัวอื่นหรือใช้รหัสผ่าน ตามมาตรฐานสากล เช่น Pkcs #12 [๑๖]

(๓) การกู้คืนข้อมูลแบบสังคม (Social Recovery) สำรองกุญแจจากกับบุคคลหรือองค์กรอื่นที่ผู้ใช้งานเชื่อถือ (Trustees) เช่น การใช้กระบวนการ Key Sharding เพื่อแบ่งข้อมูลกุญแจส่วนตัวออกเป็นหลายส่วน และให้ Trustees เป็นผู้จัดเก็บ

นอกจากนี้ ควรกำหนดมาตรฐานการเพิกถอน (rEvocation) กุญแจส่วนตัว ในกรณีที่กุญแจส่วนตัวถูกเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต หรือสูญหายโดยไม่สามารถกู้คืนได้ โดยผู้ใช้งานหรือระบบอัตโนมัติสามารถแจ้งคำร้องสำหรับการเพิกถอนกุญแจไปยังโครงสร้างพื้นฐานกุญแจสาธารณะ

๖.๖ โครงสร้างพื้นฐานกุญแจสาธารณะ

โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) เป็นระบบสำหรับให้บริการออกใบรับรอง (Certificate) เพื่อสนับสนุนลายมือชื่อดิจิทัล โดยการรับรองว่ากุญแจสาธารณะมีความน่าเชื่อถือและอยู่ภายใต้การควบคุมของผู้ลงนามตามที่กล่าวอ้างจริง สามารถนำไปใช้ตรวจสอบลายมือชื่อและเอกสารที่ถูกลงลายมือชื่อว่าไม่มีการเปลี่ยนแปลง รวมทั้งบันทึกรายการเพิกถอนกุญแจสาธารณะหรือใบรับรอง (Revocation List) โดยโครงสร้างพื้นฐานกุญแจสาธารณะสามารถถูกแบ่งออกเป็น ๒ ประเภท ตามเทคโนโลยีที่ใช้ในการพัฒนา ได้แก่

(๑) โครงสร้างพื้นฐานกุญแจสาธารณะแบบรวมศูนย์ (Centralized Public Key Infrastructure) มีผู้ให้บริการออกใบรับรอง (Certification Authority: CA) เป็นตัวกลางในการรับรองความน่าเชื่อถือและตรวจสอบความถูกต้องของลายมือชื่อ รวมทั้งทำหน้าที่เป็นรากฐานความน่าเชื่อถือ (Root Of Trust) ของระบบโดยผู้ให้บริการออกใบรับรองแบ่งออกเป็น ๒ ประเภทย่อย ได้แก่

- ผู้ให้บริการออกใบรับรองสาธารณะ (Public CA) ซึ่งให้บริการต่อสาธารณะ
- ผู้ให้บริการออกใบรับรองส่วนตัว (Private CA) ซึ่งให้บริการภายในองค์กร

(๒) โครงสร้างพื้นฐานกุญแจสาธารณะแบบกระจายศูนย์ (Decentralized Public Key Infrastructure) ใช้เทคโนโลยีแบบกระจายศูนย์ โดยไม่มีตัวกลางเป็นบุคคลหรือองค์กรใด ๆ โดยใช้ระบบอัตโนมัติทำหน้าที่เป็นรากฐานความน่าเชื่อถือ (Root Of Trust) เพื่อรับรองความถูกต้องของกุญแจสาธารณะลายมือชื่อ

โดยการเลือกรูปแบบโครงสร้างพื้นฐานกุญแจสาธารณะอาจพิจารณาความเหมาะสมตามตารางที่ ๔ ระหว่างโครงสร้างพื้นฐานกุญแจสาธารณะแบบรวมศูนย์ และแบบกระจายศูนย์ และตารางที่ ๕ ระหว่าง

การใช้ผู้ให้บริการออกใบรับรองสาธารณะ ผู้ให้บริการออกใบรับรองส่วนตัว และการใช้โครงสร้างพื้นฐานกุญแจสาธารณะแบบกระจายศูนย์

ตารางที่ ๔ เกณฑ์การพิจารณาเบื้องต้นในการเลือกรูปแบบโครงสร้างพื้นฐานกุญแจสาธารณะ

เกณฑ์การพิจารณา	แบบรวมศูนย์	แบบกระจายศูนย์
ขนาดและรูปแบบ	ขนาดใหญ่	ใช้ได้วงจำกัดเน้นเสถียรภาพ
การคงทนต่อความเสียหาย (Fault Tolerance)	ต่ำ	สูง
ความซับซ้อนของการสื่อสาร(Messaging Complexity)	ต่ำ	สูง
ข้อมูลส่วนเกิน (Messaging Overhead)	ต่ำ	สูง

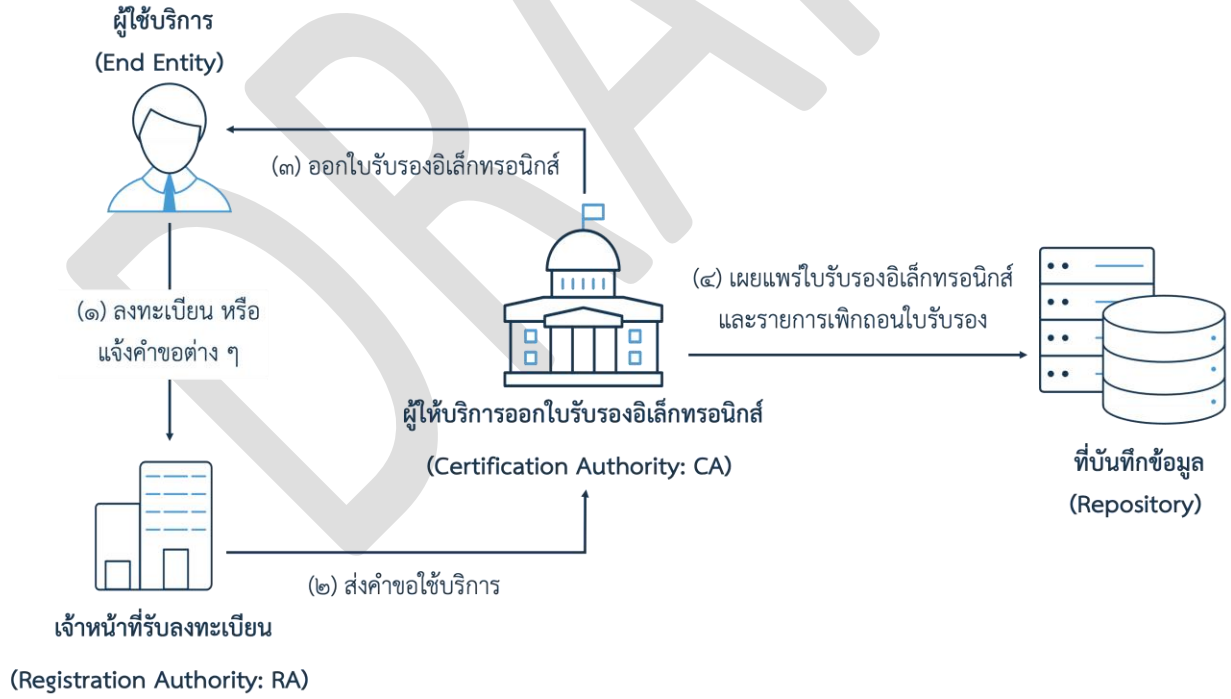
ตารางที่ ๕ เปรียบเทียบโครงสร้างพื้นฐานกุญแจสาธารณะประเภทต่าง ๆ

ประเภทโครงสร้างพื้นฐานกุญแจสาธารณะ	ข้อดี	ข้อเสีย	ประเภทธุรกรรมที่เหมาะสม
ผู้ให้บริการออกใบรับรองสาธารณะ (Public CA)	- รับรองลายมือชื่อประเภทที่ ๓ - หน่วยงานไม่จำเป็นต้องติดตั้งและดูแลระบบ PKI ด้วยตนเอง - หน่วยงานไม่จำเป็นต้องพัฒนาบริการตรวจสอบลายมือชื่อ	- ใบรับรองมีราคาแพง หากมีความต้องการใช้งานกุญแจเป็นจำนวนมาก - การออกใบรับรองใหม่เพื่อรับรองกุญแจใหม่มีราคาแพง	- การลงลายมือชื่อในเอกสารที่ต้องใช้ตรวจสอบจากภายนอกองค์กร - การลงลายมือชื่อในนามส่วนราชการหรือผู้บริหารระดับสูง
ผู้ให้บริการออกใบรับรองส่วนตัว (Private CA)	- รับรองลายมือชื่อประเภทที่ ๒ - องค์กรสามารถออกใบรับรองให้บุคลากรของตนได้อย่างอิสระ	- การจัดตั้งและดูแลระบบมีราคาแพง - องค์กรต้องจัดทำนโยบายและมาตรการบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์	- การลงลายมือชื่อในเอกสารที่ใช้ภายในองค์กร โดยบุคลากรเป็นจำนวนมาก
โครงสร้างพื้นฐานกุญแจสาธารณะแบบกระจายศูนย์ (Decentralized PKI)	- รับรองลายมือชื่อประเภทที่ ๒ - องค์กรสามารถออกใบรับรองให้บุคลากรของตนได้อย่างอิสระ - การจัดตั้งและดูแลระบบมีราคาถูก	- เป็นเทคโนโลยีใหม่ที่ยังไม่มีการใช้งานอย่างแพร่หลาย - มีมาตรฐานและกรณีศึกษาสำหรับการอ้างอิงเป็นจำนวนน้อย	- การลงลายมือชื่อในเอกสารที่ใช้ภายในองค์กร โดยบุคลากรเป็นจำนวนมาก - การทำธุรกรรมภายในภาคีความร่วมมือ (Consortium) ระหว่างองค์กร

๖.๖.๑ ข้อแนะนำเกี่ยวกับโครงสร้างพื้นฐานกุญแจสาธารณะแบบรวมศูนย์

โครงสร้างพื้นฐานกุญแจสาธารณะแบบรวมศูนย์ ควรมีมาตรฐานสากลสำหรับการออกใบรับรอง (Certificate) และรายการเพิกถอนใบรับรอง (Certificate Revocation List: Crl) เป็นไปตามตามมาตรฐาน X.509 [๑๙] และขมธอ. ๑๕-๒๕๖๓ ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) [๔] โดยมีผู้ให้บริการออกใบรับรองเป็นตัวกลางในการรับรองความน่าเชื่อถือและตรวจสอบความถูกต้องของลายมือชื่อ และโดยทั่วไปควรมีโครงสร้างประกอบด้วย ๔ องค์ประกอบหลัก ดังนี้

(๑) ผู้ใช้บริการ (End Entity) เป็นผู้ซึ่งประสงค์จะขอใช้บริการออกใบรับรอง
(๒) เจ้าหน้าที่รับลงทะเบียน (Registration Authority: Ra) มีหน้าที่รับลงทะเบียน แจ้งเพิกถอนหรือต่ออายุใบรับรอง รวมทั้งตรวจสอบและยืนยันความถูกต้องของข้อมูลที่ผู้ใช้บริการ
(๓) ผู้ให้บริการออกใบรับรอง (Certification Authority: CA) ซึ่งมีบทบาทในการให้บริการเกี่ยวกับการออกใบรับรอง
(๔) ที่บันทึกข้อมูล (Repository) เป็นระบบคอมพิวเตอร์สำหรับสืบค้นใบรับรองและรายการเพิกถอนใบรับรองของผู้ใช้บริการ ซึ่งบุคคลทั่วไปสามารถเข้าถึงได้



รูปที่ ๕ องค์ประกอบของโครงสร้างพื้นฐานกุญแจสาธารณะแบบรวมศูนย์

๖.๖.๒ ข้อแนะนำการเกี่ยวกับบริการผู้ให้บริการออกใบรับรองสาธารณะ

ผู้ให้บริการออกใบรับรองสาธารณะ คือ ผู้ให้บริการออกใบรับรองที่ให้บริการต่อสาธารณะ รวมถึงประชาชนทั่วไป บริษัทเอกชน และหน่วยงานของรัฐ โดยลายมือชื่อดิจิทัลที่มีใบรับรองจากผู้ให้บริการออกใบรับรองสาธารณะ ซึ่งจัดเป็นลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓

ผู้ให้บริการออกใบรับรองสาธารณะในประเทศไทยควรอยู่ภายใต้การกำกับดูแลโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) โดยมีผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (Thailand National Root Certification Authority: NRCA) เป็นผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด (Root CA) ซึ่งรับรองผู้ให้บริการออกใบรับรองในลำดับชั้นถัดลงมา (Subordinate CA)

๖.๖.๓ ข้อแนะนำสำหรับผู้ให้บริการออกใบรับรองส่วนตัว

ผู้ให้บริการออกใบรับรองส่วนตัว คือ ผู้ให้บริการออกใบรับรองที่ให้บริการภายในองค์กรหรือหน่วยงาน ซึ่งลายมือชื่อดิจิทัลที่มีใบรับรองจากผู้ให้บริการออกใบรับรองส่วนตัว จัดเป็นลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๒

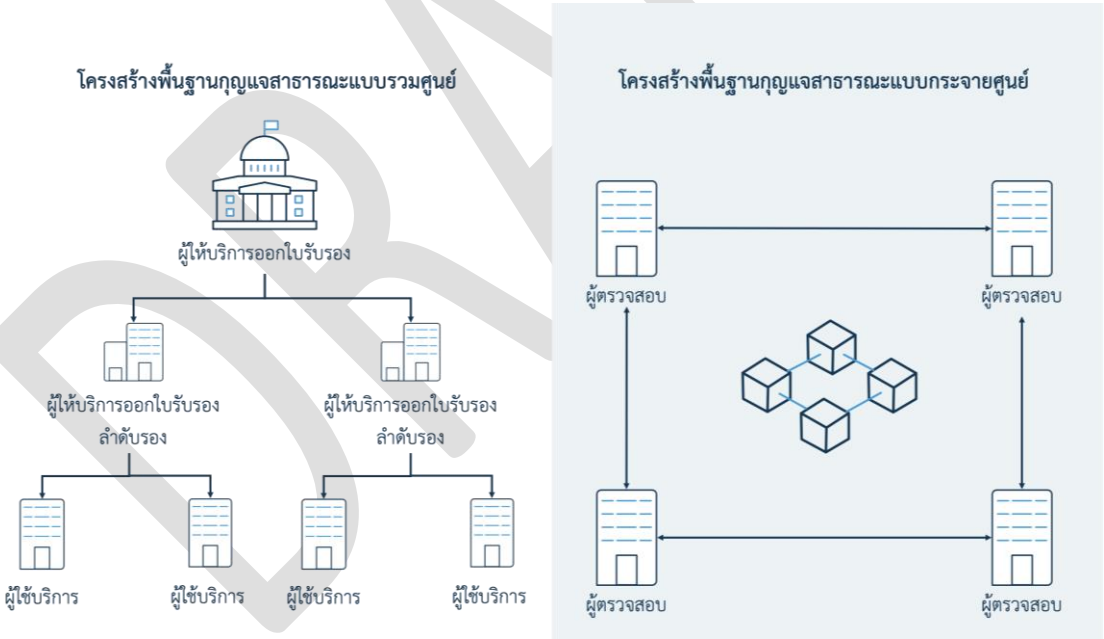
หากหน่วยงานภาครัฐมีความประสงค์ที่จะพัฒนาระบบผู้ให้บริการออกใบรับรองประเภทส่วนตัว หน่วยงานสามารถปฏิบัติตามแนวทางเบื้องต้น ดังนี้

- ควรออกใบรับรองและรายการเพิกถอนใบรับรองที่สอดคล้องกับมาตรฐานที่มีการใช้อ้างอิงกันอย่างแพร่หลาย เช่น มาตรฐาน X.509 [๑๙] และ ขมธอ. ๑๕-๒๕๖๐ [๔] เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการออกใบรับรองที่ไม่เหมาะสม
- ต้องทำการพิสูจน์และยืนยันตัวตนผู้ใช้งานเพื่อเข้าถึงกุญแจส่วนตัวสำหรับการออกรับรองที่เหมาะสมกับประเภทของธุรกรรม [๑๔][๑๕]
- ต้องจัดเก็บกุญแจส่วนตัวให้มีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ โดยใช้อุปกรณ์ที่น่าเชื่อถือ ตามมาตรฐานสากล เช่น FIPS 140-3 Security Level 2 เป็นอย่างน้อย [๑๗]
- ควรบริหารจัดการกุญแจส่วนตัวสำหรับการออกใบรับรองตลอดวงจรชีวิตกุญแจ ตามมาตรฐาน เช่น ใช้กุญแจประเภท RSA ขนาด 2048 Bits หรือ ECDSA ขนาด 256 Bits เป็นอย่างน้อย [๑] [๑๓] [๒๐]
- ควรกำหนดนโยบายและมาตรการบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามมาตรฐานสากล เช่น ISO/IEC 27001 [๑๘]
- ต้องมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้งานไม่ให้รั่วไหลหรือถูกนำไปใช้โดยไม่ได้รับอนุญาต
- ควรจัดทำบันทึกการตรวจสอบ (Audit Trail) เพื่อบันทึกการใช้งานของระบบทั้งหมด
- อาจใช้โปรโตคอลตรวจสอบสถานะของใบรับรอง (Online Certificate Status Protocol: OCSP) เพื่อให้ผู้ใช้บริการสามารถตรวจสอบสถานะของใบรับรองว่าใบรับรองถูกเพิกถอนหรือไม่ ตามมาตรฐาน RFC 6960 [๒๑]
- ควรกำหนดให้ผู้ใช้งานภายในองค์กรเป็นผู้สร้างและถือครองกุญแจส่วนตัวด้วยตนเอง โดยส่งคำร้องขอใบรับรอง (Certificate Signing Request) มายังระบบออกใบรับรอง ตามมาตรฐาน เช่น PKCS #10 [๒๒]

๖.๖.๔ ข้อแนะนำเกี่ยวกับโครงสร้างพื้นฐานกุญแจสาธารณะแบบกระจายศูนย์

โครงสร้างพื้นฐานกุญแจสาธารณะแบบกระจายศูนย์ (Decentralized Public Key Infrastructure: DPKI) ใช้เทคโนโลยีแบบกระจายศูนย์ เช่น เทคโนโลยีบล็อกเชน (Blockchain) [๒๓] มาประยุกต์ใช้งานเพื่อรับรองความน่าเชื่อถือของกุญแจสาธารณะและลายมือชื่อดิจิทัล โดยไม่มีตัวกลางเป็นบุคคลหรือองค์กร โครงสร้างพื้นฐานกุญแจสาธารณะแบบกระจายศูนย์ใช้มาตรฐาน เช่น ตัวระบุแบบกระจายศูนย์ (Decentralized Identifier: Did) และใบรับรองตัวระบุแบบกระจายศูนย์ (Did Document) [๒๓][๒๔] ทดแทนการออกใบรับรองและรายการเพิกถอนใบรับรองตามมาตรฐาน X.509

รูปที่ ๖ เปรียบเทียบความแตกต่างของโครงสร้างพื้นฐานกุญแจสาธารณะแบบรวมศูนย์และกระจายศูนย์ โดยโครงสร้างพื้นฐานกุญแจสาธารณะแบบรวมศูนย์มีผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด (Root CA) เป็นเป็นรากฐานความน่าเชื่อถือ (Root Of Trust) ซึ่งมีผู้ให้บริการออกใบรับรองในลำดับชั้นถัดลงมา (Subordinate CA) ให้บริการออกใบรับรองแก่ผู้ใช้บริการ ในขณะที่โครงสร้างพื้นฐานกุญแจสาธารณะแบบกระจายศูนย์ซึ่งใช้เทคโนโลยีบล็อกเชน มีระบบอัตโนมัติซึ่งประกอบไปด้วยเครือข่ายของผู้ตรวจสอบ (Validators) เป็นรากฐานความน่าเชื่อถือ (Root Of Trust) โดยมีข้อแนะนำการใช้โครงสร้างพื้นฐานกุญแจสาธารณะแบบกระจายศูนย์ดังนี้



รูปที่ ๖ เปรียบเทียบโครงสร้างพื้นฐานกุญแจสาธารณะแบบรวมศูนย์และกระจายศูนย์

- การเพิกถอน (Revocation) ต้องมีกลไกการเพิกถอนใบรับรอง (Certificates) เนื่องจากการเพิกถอนใบรับรองเป็นกลไกที่สำคัญในระบบโครงสร้างพื้นฐานกุญแจสาธารณะ
- การเลือกชนิดของบ็อลกเชน (Blockchain Type) ควรเลือกรูปแบบที่ใช้อย่างกว้างขวางและมีการศึกษา และสนับสนุนมาอย่างต่อเนื่อง

- การเลือกรูปแบบของใบรับรอง (Certificate Format) ควรเลือกใช้รูปแบบใบรับรองที่เป็นมาตรฐาน (Standardized Certificate Format) โดยมีการปรับส่วนขยายเพียงเล็กน้อย เช่น X509 SPKI หรือ Openpgp Certificates.
- ชนิดของโครงสร้างกุญแจสาธารณะ (PKI Type) ควรใช้ชนิดของ PKI ที่มีรูปแบบเป็น Web Of Trust (Wot) มากกว่ารูปแบบ Domain-Specific.
- การเก็บข้อมูล (Storage) ควรพิจารณาเก็บข้อมูลเท่าที่จำเป็นในบล็อกเชนเนื่องจากกระทบค่าใช้จ่ายและประสิทธิภาพ.
- ผลตอบแทน (Incentives) ควรพิจารณาผลตอบแทนผู้มีส่วนร่วมในโครงสร้างบล็อกเชน ให้มีความเหมาะสมเพื่อสเถียรภาพของโครงสร้างพื้นฐาน

๗. กรณีศึกษาแนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์

แนวปฏิบัติแนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์ สำหรับเจ้าหน้าที่ของรัฐ ถูกจัดทำขึ้นโดยมีจุดมุ่งหมายให้ครอบคลุมการดำเนินงานทางด้านเอกสารราชการทุกชนิด ทำให้เจ้าหน้าที่ของรัฐสามารถนำไปประยุกต์ใช้ได้จริงในการปฏิบัติหน้าที่ อีกทั้งมีความสอดคล้องกับแนวปฏิบัติและมาตรฐานสากล ดังนั้น การจัดทำร่างแนวปฏิบัติฯ จึงทำการรวบรวม ศึกษาและวิเคราะห์ข้อมูล จากกรณีศึกษาในประเทศไทย ๒ กรณีศึกษา ได้แก่ ระบบสารบรรณอิเล็กทรอนิกส์ (E-Saraban) และระบบออกใบรับรองผลการศึกษา (Digital Transcript) อีกทั้งศึกษากฎหมาย แนวทาง แนวปฏิบัติ วิธีการที่เกี่ยวข้องกับการลงลายมือชื่ออิเล็กทรอนิกส์ จากแนวทางของต่างประเทศอย่างน้อย ๓ ประเทศ ได้แก่ ประเทศเอสโตเนีย ประเทศแคนาดา และประเทศออสเตรเลีย

๗.๑ กรณีศึกษาระบบสารบรรณอิเล็กทรอนิกส์

ระบบสารบรรณอิเล็กทรอนิกส์ (E-Saraban) เป็นระบบที่ให้บริการบริหารจัดการเอกสารทางราชการอิเล็กทรอนิกส์แบบครบวงจร โดยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ได้จัดทำระบบสนับสนุนการแลกเปลี่ยนข้อมูลระหว่างระบบสารบรรณอิเล็กทรอนิกส์ (Electronic Correspondence Management Services: E-Cms) เพื่อให้บริการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างระบบสารบรรณอิเล็กทรอนิกส์ของแต่ละหน่วยงาน บนระบบคลาวด์ภาครัฐ (Government Cloud: G-Cloud)

การดำเนินงานของระบบสารบรรณอิเล็กทรอนิกส์ นั้นเป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม โดยล่าสุดมีประกาศระเบียบสารบรรณอิเล็กทรอนิกส์ พ.ศ. 2564 ซึ่งเป็นระเบียบหลักที่ใช้เป็นแนวทางในการดำเนินงานด้านเอกสารของทางราชการ นอกจากนี้ภาครัฐได้จัดทำมาตรฐานและกรอบแนวทางที่เกี่ยวข้อง ดังนี้

- กรอบแนวทางการเชื่อมโยงรัฐบาลอิเล็กทรอนิกส์แห่งชาติ (Thailand E-Government Interoperability Framework: Th E-Gif) [๒๕]
- มาตรฐานการแลกเปลี่ยนข้อมูลระหว่างระบบสารบรรณอิเล็กทรอนิกส์ (E-Correspondence System Interoperability Standard) [๒๖]

๗.๑.๑ ประเภทผู้ลงนามในระบบสารบรรณอิเล็กทรอนิกส์

ระบบสารบรรณอิเล็กทรอนิกส์ซึ่งเกี่ยวข้องกับการดำเนินงานด้านเอกสารของทางราชการสามารถแบ่งประเภทของผู้ลงลายมือชื่อในหนังสือราชการ โดยอ้างอิงจากภาคผนวก ๓ แห่งระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ กำหนดให้หัวหน้าส่วนราชการระดับกรมขึ้นไปเป็นผู้ลงนามในหนังสือทุกกรณี เว้นแต่จะมีการมอบอำนาจหรือกฎหมายได้ให้อำนาจผู้ดำรงตำแหน่งใดไว้โดยเฉพาะ ซึ่งสามารถสรุปได้ได้ดังนี้

(๑) หัวหน้าส่วนราชการ มีอำนาจลงลายมือชื่อในหนังสือราชการทุกประเภท

(๒) ผู้บริหาร มีอำนาจในการลงลายมือชื่อตามที่ได้รับมอบหมายแทนหัวหน้าส่วนราชการ หรือได้รับอำนาจโดยตำแหน่งให้สามารถดำเนินการภายในขอบเขตหน้าที่และความรับผิดชอบ

(๓) เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดำเนินการแทน โดยได้รับมอบอำนาจจากหัวหน้าส่วนราชการให้ลงลายมือชื่อในหนังสือราชการ ตามวัตถุประสงค์และความสำคัญของหัวข้อเรื่อง

(๔) เจ้าหน้าที่ทั่วไป มีอำนาจลงลายมือชื่อในเอกสารทั่วไป หรือบันทึกเพื่อใช้ภายในส่วนราชการ รวมถึงเอกสารที่จัดทำขึ้นหรือรับไว้เป็นหลักฐานราชการที่อยู่ภายใต้การปฏิบัติหน้าที่ตามปกติ

๗.๑.๒ แนวทางการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับระบบสารบรรณอิเล็กทรอนิกส์

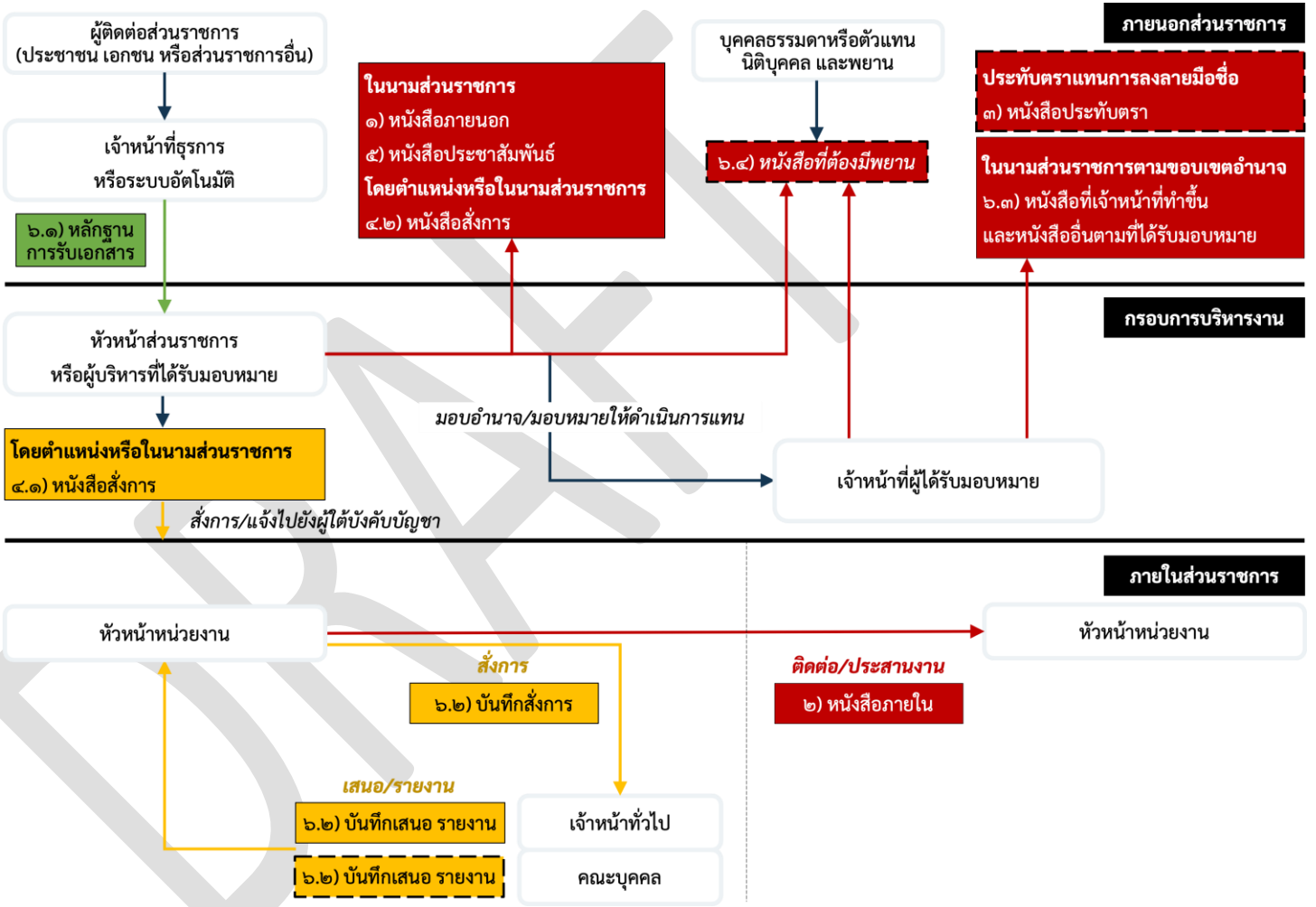
เจ้าหน้าที่ภาครัฐสามารถเลือกใช้ประเภทของลายมือชื่ออิเล็กทรอนิกส์โดยคำนึงถึงประเภทของผู้ลงลายมือชื่อ เจ้าหน้าที่ทั่วไปอาจใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๑ และ ๒ สำหรับหนังสือที่เจ้าหน้าที่จัดทำขึ้นหรือรับไว้เป็นหลักฐานราชการโดยพิจารณาตามความเสี่ยงของธุรกรรม ซึ่งการปฏิบัติหน้าที่ในลักษณะที่เป็นประจำ และยังไม่มีความเกี่ยวข้องกับการพิจารณาถึงการดำเนินการในลำดับถัดไป เช่น เจ้าหน้าที่ธุรการ อาจใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๑ ได้ตามระดับความเสี่ยง ส่วนเจ้าหน้าที่ที่ปฏิบัติงานทั่วไป ซึ่งมีการจัดทำหนังสือที่มีสาระสำคัญเกี่ยวข้องกับการปฏิบัติหน้าที่ภายในส่วนราชการ ควรใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๒

หัวหน้าส่วนราชการควรใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๒ สำหรับธุรกรรมที่เกิดขึ้นภายในส่วนราชการเดียวกัน เช่น คำสั่งภายใน รวมถึงเรื่องที่มีการใช้บันทึกข้อความเพื่อการติดต่อ ซึ่งเป็นชนิดของหนังสือราชการที่ใช้ภายในกรมเดียวกัน และควรใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ สำหรับธุรกรรมเกี่ยวข้องกับบุคคลภายนอกส่วนราชการ รวมถึงเรื่องที่ใช้หนังสือภายในเพื่อการติดต่อซึ่งเป็นชนิดของหนังสือราชการที่ใช้ระหว่างหน่วยงานภายในกระทรวงเดียวกัน ส่วนเจ้าหน้าที่ผู้ได้รับมอบหมายให้ดำเนินการแทนควรใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ เช่นเดียวกัน

โดยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับระบบสารบรรณอิเล็กทรอนิกส์สามารถสรุปได้ดังที่แสดงในรูปที่ ๗ โดยอ้างอิงตัวเลขระบุประเภทหนังสือราชการอ้างอิงจากตารางที่ ๓ อีกทั้งใช้สีในการระบุประเภทลายมือชื่ออิเล็กทรอนิกส์ที่แนะนำ ได้แก่ สีเขียวสำหรับประเภทที่ ๑ สีเหลืองสำหรับประเภทที่ ๒ และสีแดงสำหรับประเภทที่ ๓

คำอธิบายแผนภาพ

แผนภาพแบ่งออกเป็น 3 ส่วนหลัก ได้แก่
(๑) ภายนอกส่วนราชการ หมายถึงบุคคลภายนอก หน่วยงานอื่นใดซึ่งมิใช่ส่วนราชการและส่วนราชการอื่น ที่มีหนังสือมายังส่วนราชการและที่ส่วนราชการออกหนังสือไปถึง
(๒) กรอบการบริหารงาน หมายถึง กระบวนการพิจารณาถึงการดำเนินงานที่เกี่ยวข้องกับหนังสือที่ได้รับ
(๓) ภายในส่วนราชการ หมายถึงเจ้าหน้าที่ภายในส่วนราชการเดียวกัน



ประเภทลายมือชื่ออิเล็กทรอนิกส์ที่แนะนำ

- ธุรกรรมธรรมดา (ประเภทที่ ๑)
- ธุรกรรมขั้นสูง (ประเภทที่ ๒)
- ธุรกรรมอ่อนไหว (ประเภทที่ ๓)

ลักษณะการลงนาม

- ลงนามบุคคลเดียว
- ลงนามหลายบุคคล

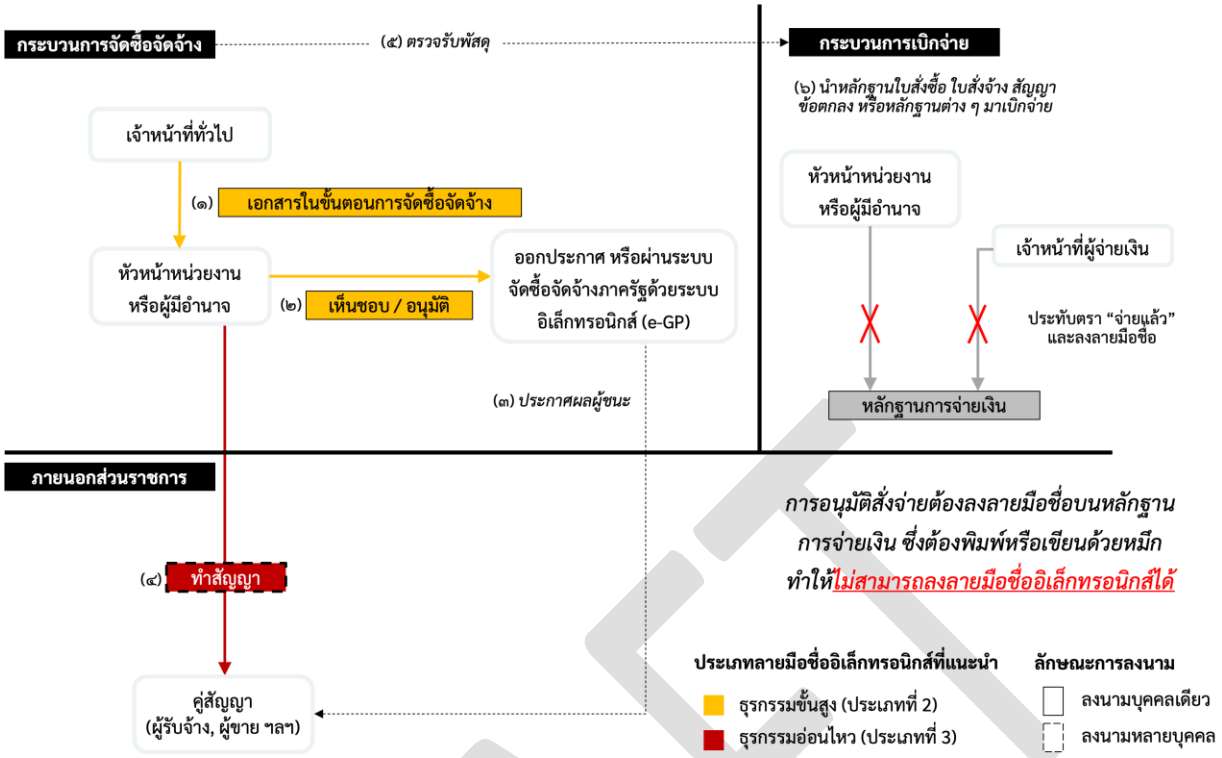
รูปที่ ๗ แผนภาพการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์สำหรับงานสารบรรณ

๗.๑.๓ แนวทางและข้อจำกัดในการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับเอกสารทางด้านการเงิน

เอกสารทางด้านการเงินเป็นเอกสารประเภทที่ความอ่อนไหวสูง อีกทั้งมีกฎระเบียบเฉพาะที่แตกต่างจากเอกสารราชการประเภทอื่นที่มีการใช้งานภายในระบบสารบรรณอิเล็กทรอนิกส์ โดยสามารถสรุปแนวทางและข้อจำกัดในการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับเอกสารทางด้านการเงินใน Error! Reference source not found.

ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ กำหนดให้ผู้มีอำนาจในการสั่งซื้อ หรือสั่งจ้างเป็นหัวหน้าหน่วยงานของรัฐ หรือมอบอำนาจแก่ผู้ดำรงตำแหน่งใดในสังกัดเดียวกัน ซึ่งในขั้นตอนการจัดทำขอบเขตของงานหรือรายละเอียดคุณลักษณะของพัสดุ การเชิญชวนและการยื่นข้อเสนอ การพิจารณาผล การเสนอขออนุมัติสั่งซื้อหรือสั่งจ้าง การทำนิติกรรมสัญญา ไปจนถึงการตรวจรับพัสดุสามารถดำเนินการในรูปแบบอิเล็กทรอนิกส์ได้ตามหนังสือด่วนที่สุด ที่ กค (กวจ) ๐๔๐๕.๒/ว๓๔๘ ลงวันที่ ๑๔ มิถุนายน ๒๕๖๔ โดยคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กรมบัญชีกลาง เรื่อง การใช้ลายมือชื่ออิเล็กทรอนิกส์ในการจัดซื้อจัดจ้าง

อย่างไรก็ดี ตามระเบียบกระทรวงการคลัง ว่าด้วยการเบิกเงินจากคลัง การรับเงิน การจ่ายเงิน การเก็บรักษาเงินและการนำเงินส่งคลัง พ.ศ. ๒๕๖๒ ให้เป็นอำนาจของหัวหน้าส่วนราชการระดับกรม หรือผู้ที่หัวหน้าส่วนราชการระดับกรมมอบหมายซึ่งดำรงตำแหน่งในระดับที่กำหนดไว้ หรือหัวหน้าส่วนราชการในภูมิภาคสำหรับส่วนราชการในราชการบริหารส่วนภูมิภาคในการอนุมัติจ่ายเงิน พร้อมลงลายมือชื่อในหลักฐานการจ่ายเงิน และให้เจ้าหน้าที่ผู้จ่ายเงินประทับตรา “จ่ายแล้ว” พร้อมลงลายมือชื่อรับรองการจ่ายและลงรายละเอียดตามที่กำหนดในระเบียบกำกับไว้ในหลักฐานการจ่ายเงิน ซึ่งหลักฐานการจ่ายเงินต้องอยู่ในรูปแบบของเอกสารพิมพ์ออก หรือเขียนด้วยหมึก ทำให้การอนุมัติจ่ายเงินมีข้อจำกัดที่ไม่สามารถดำเนินการในรูปแบบลายมือชื่ออิเล็กทรอนิกส์ได้ หากหน่วยงานไม่ปฏิบัติตามระเบียบที่ได้กำหนดไว้ จะส่งผลกระทบต่อกรอบการดำเนินงานของสำนักงานการตรวจเงินแผ่นดิน ซึ่งมีอำนาจรวมถึงการตรวจสอบหลักฐานการใช้จ่ายด้วย



รูปที่ ๘ แผนภาพแสดงข้อจำกัดของการใช้ลายมือชื่ออิเล็กทรอนิกส์สำหรับเอกสารทางการเงิน

๗.๒ กรณีศึกษาระบบออกผลใบประมวลผลการศึกษา

บริการระบบออกใบรับรองผลการศึกษา (Digital Transcript) คือใบรับรองผลการศึกษาที่อยู่ในรูปแบบอิเล็กทรอนิกส์ เช่น ไฟล์ Pdf โดยมีการลงลายมือชื่ออิเล็กทรอนิกส์ในรูปแบบลายมือชื่อดิจิทัล อีกทั้งมีการแนบใบรับรองเพื่อป้องกันการแก้ไขเปลี่ยนแปลงเอกสาร

โดยนิสิตและนักศึกษาสามารถส่งไฟล์เอกสารใบรับรองผลการศึกษา ให้บริษัทที่สมัครงานหรือหน่วยงานที่ร้องขอได้โดยไม่ต้องพิมพ์เป็นกระดาษ และเจ้าหน้าที่ของหน่วยงานที่ได้รับไฟล์ใบรับรองผลการศึกษา สามารถตรวจสอบลายมือชื่อดิจิทัลได้ด้วยซอฟต์แวร์พื้นฐาน เช่น Adobe Acrobat Reader โดยไม่จำเป็นต้องส่งหนังสือกับไปตรวจสอบที่มหาวิทยาลัยต้นสังกัด และสามารถเก็บเป็นหลักฐานเพื่ออ้างอิงในอนาคตได้

เอกสารใบรับรองผลการศึกษาจะถูกดำเนินการโดยระบบอัตโนมัติที่มีการเชื่อมต่อกับระบบฐานข้อมูลนักศึกษา (Student Information System: Sis) ซึ่งเอกสารจะถูกจัดเก็บในรูปแบบ Pdf/A3 ประกอบกับเอกสารแนบ Xml โดยมีการลงลายมือชื่อในนามมหาวิทยาลัยด้วยใบรับรองประเภทนิติบุคคลบนเอกสาร Xml ก่อนที่จะนำมาแนบไว้กับเอกสาร Pdf และลงลายมือชื่อทับบนเอกสาร Pdf อีกครั้งหนึ่ง เพื่อให้ตรวจสอบได้หากมีการเปลี่ยนแปลงข้อมูลในเอกสารทั้ง ๒ ส่วน

๗.๒.๑ ประเภทผู้ลงนามในระบบออกผลใบประมวลผลการศึกษา

อ้างอิงจากข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อความอิเล็กทรอนิกส์สำหรับใบประมวลผลการศึกษา (ขมธอ.๒๕-๒๕๖๓) [๒๗] ผู้ออกใบประมวลผลการศึกษา หมายถึง สถาบันการศึกษาที่จัดทำใบประมวลผลการศึกษา

สำหรับสถาบันระดับอุดมศึกษา อธิการบดีเป็นผู้บังคับบัญชาสูงสุดและรับผิดชอบการบริหารงานของมหาวิทยาลัยตามกฎหมายว่าด้วยการจัดตั้งสถานศึกษานั้น ๆ โดยมีการออกคำสั่งแต่งตั้งนายทะเบียนเพื่อปฏิบัติหน้าที่ และรับผิดชอบเกี่ยวกับการออกเอกสารสำคัญ หรือหลักฐานทางการศึกษา

๗.๒.๒ แนวทางการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับระบบออกผลใบประมวลผลการศึกษา

แนวทางการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับระบบออกผลใบประมวลผลการศึกษา สามารถสรุปในตารางที่ ๔ และรูปที่ ๙ ดังนี้

เจ้าหน้าที่ธุรการซึ่งทำหน้าที่รับแบบคำร้อง หรือคำขอเกี่ยวกับเอกสารสำคัญ หรือหลักฐานทางการศึกษาอาจใช้งานลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๑ เพื่อความสะดวก และเหมาะสมกับการทำธุรกรรมที่มีความเสี่ยงระดับธรรมดา

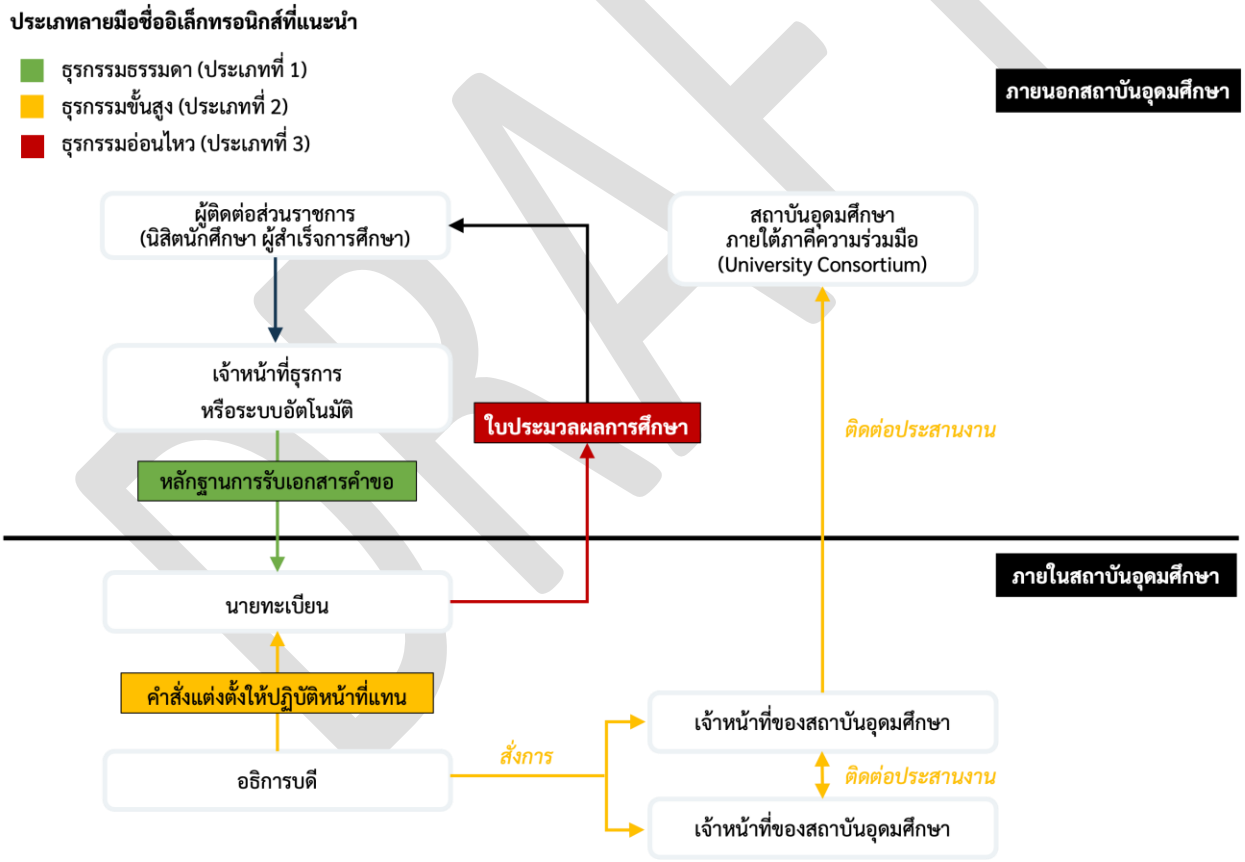
อธิการบดี ควรใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๒ สำหรับการแต่งตั้งนายทะเบียน เพื่อการปฏิบัติหน้าที่แทน หรือการสั่งการอื่น ๆ ซึ่งเป็นธุรกรรมภายในหน่วยงาน

นายทะเบียน ซึ่งโดยทั่วไปจะมีการแต่งตั้งผู้อำนวยการสำนักทะเบียนและวัดผล หรือส่วนงานอื่นที่เทียบเท่าเป็นผู้ดำเนินการออกเอกสารสำคัญทางการศึกษา ควรใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ ซึ่งมีใบรับรองที่ระบุรายละเอียดสำคัญเกี่ยวกับการปฏิบัติหน้าที่ในนามสถาบันการศึกษา ในการลงลายมือชื่อเอกสารสำคัญทางการศึกษา

ในกรณีที่มีการจัดตั้งภาคีความร่วมมือ อาทิ Thailand University Consortium ซึ่งมหาวิทยาลัยแต่ละแห่งสามารถดำเนินการออกใบรับรองให้แก่บุคลากรภายในของตนเองได้ ทำให้หนังสือที่มีไปมาระหว่างสถาบันการศึกษาที่อยู่ภายใต้ภาคีความร่วมมือเดียวกัน สามารถใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๒ ได้

ตารางที่ ๔ แนวทางการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์สำหรับเอกสารของสถาบันการศึกษา

รูปแบบการลงลายมือชื่ออิเล็กทรอนิกส์	ประเภทของผู้ลงนาม	ประเภทลายมือชื่อที่แนะนำ
๑) เอกสารสำคัญทางการศึกษา เช่น ใบประมวลผลการศึกษา	ในนามสถาบันการศึกษา โดยเจ้าหน้าที่ผู้ได้รับมอบหมาย	ประเภทที่ ๓
๒) หนังสือคำสั่ง	ในนามสถาบันการศึกษา โดยอธิการบดี	ประเภทที่ ๒
๓) หนังสือที่เจ้าหน้าที่จัดทำขึ้น หรือรับไว้เป็นหลักฐานในการปฏิบัติหน้าที่ เช่น แบบคำขอ	เจ้าหน้าที่ธุรการ หรือระบบอัตโนมัติ	ประเภทที่ ๑
๔) หนังสือที่มีไปมาระหว่างสถาบันการศึกษาที่อยู่ภายใต้ภาคีความร่วมมือ	ในนามสถาบันการศึกษา หรือในนามบุคคล	ประเภทที่ ๒



รูปที่ ๙ แผนภาพตัวอย่างการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์สำหรับเอกสารของสถาบันการศึกษา

๗.๓ กรณีศึกษาประเทศเอสโตเนีย

เอสโตเนียได้ริเริ่มการออกบัตรประชาชนอิเล็กทรอนิกส์ครั้งแรกในปี ค.ศ. ๒๐๐๒ และตั้งแต่นั้นมาได้มีการใช้เทคโนโลยีการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity) อย่างเป็นทางการทั่วประเทศ ซึ่งในที่สุดทำให้เกิดการพัฒนาระบบการลงลายมือชื่ออิเล็กทรอนิกส์โดยภาครัฐ ซึ่งเป็นระบบกลางให้ประชาชนทุกคนได้ใช้บริการเพื่อการลงลายมือชื่ออิเล็กทรอนิกส์

๗.๓.๑ กฎหมาย

เอสโตเนีย ซึ่งเป็นหนึ่งในประเทศสมาชิกสหภาพยุโรป ได้มีการถอดแบบกฎหมายสหภาพยุโรป ที่มีชื่อว่า Regulation (Eu) No. 910/2014 Of The European Parliament And Of The Council Of 23 June 2014 On Electronic Identification And Trust Services For Electronic Transactions In The Internal Market And Repealing Directive 1999/93/Ec ที่เรียกโดยย่อว่า Eidas Regulation เพื่อออกเป็นกฎหมายที่มีการบังคับใช้ในระดับประเทศที่มีชื่อว่า Electronic Identification And Trust Services For Electronic Transactions Act รัฐบัญญัติฉบับนี้เป็นกฎหมายหลักที่กำกับดูแลเบ็ดเสร็จในเรื่องทั้งหมดที่เกี่ยวข้องกับดิจิทัลไอดี อาทิ ดิจิทัลไอดี การพิสูจน์และยืนยันตัวตน การลงลายมือชื่ออิเล็กทรอนิกส์ การตรวจประเมินบริการให้ได้มาตรฐาน และการรับประกันความปลอดภัยของระบบ

หน่วยงานที่กำกับดูแลการให้บริการลายมือชื่ออิเล็กทรอนิกส์ คือ Information System Authority หรือเรียกโดยย่อว่า Ria ในภาษาเอสโตเนีย หน่วยงานดังกล่าวได้รับอำนาจหน้าที่โดยตรงจากมาตรา ๒ แห่ง Electronic Identification And Trust Services For Electronic Transactions Act ซึ่งกำหนดให้ Ria เป็น Supervisory Body ตามมาตราที่ ๑๙ แห่ง Eidas Regulation

ในส่วนของการรับรองให้มีผลทางกฎหมาย ลายมือชื่ออิเล็กทรอนิกส์ที่ถูกต้องตามกฎหมายและเทียบเท่ากับลายมือชื่อแบบเขียน (Handwritten Signature) คือลายมือชื่อดิจิทัลเท่านั้น ซึ่งในกฎหมายเอสโตเนีย ลายมือชื่อดิจิทัลหมายความถึงเฉพาะลายมือชื่ออิเล็กทรอนิกส์ระดับสูงสุดที่ระบุไว้ใน Eidas Regulation ที่เรียกว่า Qualified Electronic Signature (Qes) ส่วนลายมือชื่ออิเล็กทรอนิกส์ระดับอื่น ๆ ยังคงมีข้อจำกัดเรื่องผลทางกฎหมาย

๗.๓.๒ แนวทางและแนวปฏิบัติ

ซอฟต์แวร์กลางที่ Ria จัดทำขึ้นเพื่อให้บริการประชาชนมีชื่อว่า Digidoc ซึ่งสามารถใช้งานได้ผ่านคอมพิวเตอร์และสมาร์ตโฟน โดยบริษัทเอกชนซึ่งเป็นผู้ผลิตและพัฒนาซอฟต์แวร์ดังกล่าวร่วมกับภาครัฐได้อยู่ในรายชื่อผู้ให้บริการที่น่าเชื่อถือของสหภาพยุโรป หรือที่เรียกว่า Eidas Trusted List (Lotl) ซอฟต์แวร์นี้เชื่อมต่อกับระบบดิจิทัลไอดีของประเทศ และใช้เพื่อจุดประสงค์หลักสองอย่าง คือ การลงลายมือชื่อในเอกสาร และการตรวจสอบความถูกต้องของเอกสารที่ลงลายมือชื่อแล้ว เอกสารที่ลงลายมือชื่อดิจิทัลไม่ตรงตามข้อกำหนด จะขึ้นข้อความเตือนบนซอฟต์แวร์ในลักษณะดังนี้

(๑) ลายมือชื่อดิจิทัลถูกต้อง และมีผลเทียบเท่ากับลายมือชื่อแบบเขียนทุกประการ กรณีนี้ขึ้นข้อความเตือนด้วยสีเขียวประกอบ

(๒) ลายมือชื่ออิเล็กทรอนิกส์ถูกต้อง แต่ไม่มีผลเทียบเท่ากับลายมือชื่อแบบเขียน เนื่องจากเป็นเพียงลายมือชื่ออิเล็กทรอนิกส์ระดับที่ ๒ (ระดับรองลงมาจากระดับสูงสุด) กรณีนี้ขึ้นข้อความเตือนด้วยสีเขียวและสีเหลืองประกอบ

(๓) ลายมือชื่ออิเล็กทรอนิกส์ถูกต้อง แต่ไม่มีผลเทียบเท่ากับลายมือชื่อแบบเขียน เนื่องจากโปรแกรมตรวจสอบแล้วพบว่าลายมือชื่ออิเล็กทรอนิกส์มีลักษณะบางอย่างที่ยังไม่สมบูรณ์ กรณีนี้ขึ้นข้อความเตือนด้วยสีเขียวและสีเหลืองประกอบ

(๔) ลายมือชื่ออิเล็กทรอนิกส์ไม่สามารถตรวจสอบความถูกต้องได้ กรณีนี้ขึ้นข้อความสีแดงประกอบ

(๕) ลายมือชื่ออิเล็กทรอนิกส์ไม่ถูกต้อง กรณีนี้ขึ้นข้อความสีแดงประกอบเช่นเดียวกัน

(๖) ผู้ใช้งานสามารถคลิกที่ผลการตรวจสอบ เพื่อดูรายละเอียดของลายมือชื่อได้ อาทิ ใบรับรองของผู้ลงลายมือชื่อ, ใบประทับรับรองเวลา (Timestamp) ของลายมือชื่อ และใบรับรองของผู้ลงประทับรับรองเวลา

๗.๔ กรณีศึกษาประเทศออสเตรเลีย

ออสเตรเลียไม่มีระบบลงลายมือชื่ออิเล็กทรอนิกส์กลางโดยภาครัฐ กล่าวคือ เอกสารของภาครัฐสามารถลงลายมือชื่อผ่านระบบของแต่ละหน่วยงาน ในขณะที่เอกสารทั่วไปที่มีการใช้งานในภาคประชาชนและภาคธุรกิจสามารถลงลายมือชื่อผ่านบริการของภาคเอกชน โดยมีหน่วยงานที่กำกับดูแลการลงลายมือชื่ออิเล็กทรอนิกส์คือ Digital Transformation Agency (Dta)

๗.๔.๑ กฎหมาย

ออสเตรเลียได้มีกฎหมายระดับประเทศเกี่ยวกับการลงลายมือชื่ออิเล็กทรอนิกส์ คือ Electronic Transactions Act 1999 และแต่ละรัฐได้มีการออกกฎหมายเพื่อบังคับใช้ในระดับรัฐ (State) หรือเขตการปกครองภายใน (Internal Territory) ซึ่งมีความสอดคล้องกับกฎหมายหลักของประเทศ

มาตรา ๑๐ แห่ง Electronic Transactions Act 1999 รับรองให้การลงลายมือชื่ออิเล็กทรอนิกส์มีผลทางกฎหมายเท่ากับการลงลายมือชื่อแบบเขียน ตราบใดที่

- วิธีการที่ใช้ระบุตัวตนเป็นวิธีการที่กำหนดโดยกฎหมายว่าสามารถใช้ได้
- วิธีการได้มาซึ่งลายมือชื่ออิเล็กทรอนิกส์มีความน่าเชื่อถือ (Reliable)
- พิสูจน์ได้ว่าผู้ลงลายมือชื่อให้ความยินยอม

อย่างไรก็ดี ได้มีข้อยกเว้นใน Schedule 1 ของกฎหมาย Electronic Transactions Regulations 2020 ว่าการลงลายมือชื่อสำหรับธุรกรรมบางประเภทให้ดำเนินการบนกระดาษได้เท่านั้น ดังนั้น ข้อกำหนดเหล่านี้จึงบ่งชี้ว่า (๑) ลายมือชื่ออิเล็กทรอนิกส์ในออสเตรเลีย ยังไม่สามารถแทนที่ลายมือชื่อแบบเขียนได้ในทุกกรณีและ (๒) คุณสมบัติของลายมือชื่ออิเล็กทรอนิกส์ มีเพียงข้อกำหนดไว้กว้าง ๆ โดยไม่ระบุถึงประเภทเทคโนโลยีที่ใช้และไม่มีการแบ่งประเภทย่อยตามระดับความน่าเชื่อถือ

๗.๔.๒ แนวทางและแนวปฏิบัติ

ออสเตรเลียไม่มีบัตรประชาชน ทำให้การพิสูจน์ตัวตนจะอาศัยเอกสารระบุตัวตนอื่น ๆ ซึ่งเป็นที่ยอมรับโดยทั่วไป เช่น หนังสือเดินทาง ใบขับขี่ และสูติบัตร ส่วนการพิสูจน์และยืนยันตัวตนทางดิจิทัลนั้น มีผู้ให้บริการในปัจจุบัน ได้แก่ Digital Id โดย Australia Post และ Mygovid โดย Dta ภายใต้กรอบการทำงาน Trusted Digital Identity Framework (Tdif) ที่ Dta เป็นผู้กำกับดูแล นอกจากนี้ ยังมีการใช้งานดิจิทัลไอดีภายใต้กรอบการทำงานอื่น สำหรับบางสาขาอาชีพ หรือสาขาธุรกิจโดยเฉพาะ

บริการการพิสูจน์และยืนยันตัวตนทางดิจิทัลเหล่านี้ คือสิ่งที่จะใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับเอกสารภาครัฐบนระบบหรือ Portal ของหน่วยงานรัฐ ตัวอย่างเช่น การลงลายมือชื่อในเอกสารอิเล็กทรอนิกส์เกี่ยวกับภาษีอากร สามารถทำได้ด้วย Mygovid ผ่านระบบของ Australia Tax Office แต่ไม่สามารถนำมาใช้ลงลายมือชื่อในเอกสารอิเล็กทรอนิกส์โดยทั่วไปนอกระบบของหน่วยงานรัฐได้

การลงลายมือชื่ออิเล็กทรอนิกส์ในเอกสารโดยทั่วไป สามารถทำได้ผ่านบริการของภาคเอกชนเท่านั้น ซึ่งแพลตฟอร์มของภาคเอกชนไม่มีการเชื่อมโยงกับผู้ให้บริการไอเดนทิตีโดยภาครัฐ ดังนั้น ผู้ให้บริการแต่ละรายต้องมีการพิสูจน์และยืนยันตัวตนผู้ใช้งานเอง จากนั้นเมื่อผนวกเข้ากับการตรวจสอบที่น่าเชื่อถือ (Audit Trail) และการใช้เทคโนโลยีการเข้ารหัสในการจัดการเอกสาร จะทำให้ลายมือชื่ออิเล็กทรอนิกส์มีผลผูกพันตามกฎหมายและใช้เป็นหลักฐานในชั้นศาลตามเกณฑ์ของ Electronic Transactions Act 1999 ได้

อีกบริการหนึ่งที่น่าสนใจ คือบริการ My Equals (มีที่มาจากคำว่า My Electronic Qualifications) ที่สถาบันอุดมศึกษาทั้งของรัฐและเอกชนใช้ในการจัดการและออกเอกสารสำคัญทางการศึกษา อาทิ ใบประมวลผลการศึกษาและปริญญาบัตร โดยนักศึกษาสามารถนำลิงก์จาก My Equals เพื่อส่งต่อให้กับผู้ตรวจสอบ เช่น นายจ้าง หรือสถาบันการศึกษาอื่นได้โดยตรง หรือดาวน์โหลดไฟล์อิเล็กทรอนิกส์ประเภท Pdf ที่มีการลงลายมือชื่ออิเล็กทรอนิกส์จากสถาบันการศึกษาแล้วไปใช้งาน

๗.๕ กรณีศึกษาประเทศแคนาดา

การลงลายมือชื่ออิเล็กทรอนิกส์ในแคนาดามีลักษณะที่คล้ายกันกับกรณีศึกษาประเทศออสเตรเลีย กล่าวคือ เอกสารของภาครัฐสามารถลงลายมือชื่อผ่านระบบของแต่ละหน่วยงาน ในขณะที่เอกสารทั่วไปสามารถใช้บริการของภาคเอกชนในการลงลายมือชื่อ

๗.๕.๑ กฎหมาย

กฎหมายกลางของแคนาดาที่เกี่ยวกับการลงลายมือชื่ออิเล็กทรอนิกส์ ได้แก่ Personal Information Protection And Electronic Documents Act (PIPEDA) และ Secure Electronic Signature Regulations PIPEDA กำหนดไว้เพียงว่าลายมือชื่ออิเล็กทรอนิกส์คือ ลายมือชื่อที่ประกอบด้วยตัวอักษร อักขระ ตัวเลข หรือสัญลักษณ์อื่นใด จำนวน ๑ ตัวหรือมากกว่า ที่อยู่ในรูปแบบดิจิทัล โดยควบรวม แนบ หรือประกอบอยู่ในเอกสารอิเล็กทรอนิกส์ ซึ่งเป็นบทบัญญัติโดยทั่วไป และไม่ได้เฉพาะเจาะจงถึงวิธีการสร้างลายมือชื่อ อย่างไรก็ดี สำหรับเอกสารที่มีความสำคัญมากขึ้น หน่วยงานรัฐสามารถยกระดับการลงลายมือชื่อเป็นลายมือชื่อประเภท Secure Electronic Signature (SES) ได้ ซึ่งมีการกำหนดคุณสมบัติของเทคโนโลยีที่ใช้และกระบวนการได้มาซึ่งลายมือชื่อดังต่อไปนี้

- Uniqueness: ลายมือชื่อต้องพิสูจน์ได้ว่าเชื่อมโยงกับผู้ลงนามเพียงคนเดียวเท่านั้น อาทิ ผ่านการยืนยันตัวตนโดยอาศัย “สิ่งที่รู้”, การยืนยันตัวตนโดยบริการไอเดนทิตีของบุคคลที่สาม, รหัสผ่านแบบใช้ครั้งเดียว, การสำแดงสำเนาใบขับขี่, การใช้ใบรับรอง
- Sole Control: ลายมือชื่อต้องพิสูจน์ได้ว่าอยู่ภายใต้การควบคุมของผู้ลงนามเพียงคนเดียวเท่านั้น
- Identifiability: ลายมือชื่อต้องระบุได้ว่าเป็นของผู้ลงนามคนใด

- Tamper-Evidence: ลายมือชื่อต้องเชื่อมโยงกับเอกสารในลักษณะที่สามารถบอกได้ว่าเอกสารมีการแก้ไขหลังลงนามหรือไม่

หลังจากนั้น ได้มีข้อกำหนดเพิ่มเติมภายใต้ Secure Electronic Signature Regulations โดยระบุเฉพาะเจาะจงถึงเทคโนโลยีที่ใช้และกระบวนการได้มาซึ่งลายมือชื่อ และผู้ให้บริการออกใบรับรองบนโครงสร้างพื้นฐานกุญแจสาธารณะ ต้องได้รับการรับรองจาก President Of The Treasury Board และประกาศไว้บนเว็บไซต์ของ Treasury Board Secretariat เป็นการสาธารณะ

นอกจากนั้นแล้ว PIPEDA ยังกำหนดประเภทของเอกสารที่ต้องลงนามด้วย SES เท่านั้น ได้แก่

- เอกสารที่ใช้เป็นหลักฐานหรือข้อพิสูจน์ ที่ลงนามโดยรัฐมนตรีและบุคลากรของหน่วยงานรัฐ (มาตรา ๓๖)
- ตราประทับ เฉพาะประเภทที่กำหนดในภาคผนวก ๒ และ ๓ (มาตรา ๓๙)
- เอกสารที่ใช้ลายมือชื่ออิเล็กทรอนิกส์ในการบ่งชี้ว่าเป็นเอกสารต้นฉบับ (มาตรา ๔๒)
- เอกสารประกอบคำให้การที่มีคำสาบานประกอบ (มาตรา ๔๔)
- เอกสารที่ใช้เป็นหลักฐานแสดงว่าข้อมูลที่บอกไว้ในเอกสารเป็นความจริง ถูกต้องแม่นยำ หรือมีความสมบูรณ์ครบถ้วน (มาตรา ๔๕)
- เอกสารที่มีพยานลงลายมือชื่อประกอบด้วย โดยต้องเป็น Ses ทั้งของลายมือชื่อหลัก และลายมือชื่อพยาน (มาตรา ๔๖)

๗.๕.๒ แนวทางและแนวปฏิบัติ

การพิสูจน์ตัวตนในแคนาดาจะอาศัยใบขับขี่เป็นหลัก ซึ่งออกโดยหน่วยงานกำกับดูแลของแต่ละรัฐเอง แต่หากบุคคลผู้นั้นไม่สามารถขับขี่ยานพาหนะทางบกได้ หลายรัฐจะมีการออกบัตรประชาชนให้ใช้แทน นอกจากนั้น ในส่วนของดิจิทัลไอดี จะเป็นการให้บริการโดย Shared Services Canada ชื่อว่า Gckey โดยอยู่ในลักษณะของ Username และ Password ที่ผู้ใช้งานสามารถนำไปเข้าสู่ระบบบริการของหน่วยงานรัฐต่าง ๆ ได้ ทั้งนี้ ต้องเป็นกลุ่มบริการที่สามารถใช้งานได้ ซึ่งเรียกว่า Enabled Service เท่านั้น ลักษณะพิเศษที่น่าสนใจ ๒ ประการของ Gckey คือ (๑) ผู้ใช้งานสามารถตั้ง Username ได้เอง และรัฐบาลแนะนำว่าไม่ควรประกอบด้วยชื่อจริงหรือข้อมูลส่วนตัวใด ๆ เช่น ที่อยู่อีเมล หมายเลขประกันสังคม และ (๒) ประชาชนสามารถมี Gckey ได้หลายบัญชี ลักษณะพิเศษทั้ง ๒ อย่างนี้ เป็นไปเพื่อรักษาความเป็นส่วนตัวของผู้ใช้งาน

Gckey คือ ดิจิทัลไอดีที่ประชาชนจะต้องใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับเอกสารภาครัฐบนระบบหรือ Portal ของหน่วยงานรัฐ ส่วนการลงลายมือชื่ออิเล็กทรอนิกส์ในเอกสารโดยทั่วไป สามารถดำเนินการได้ผ่านบริการของภาคเอกชนเท่านั้น เนื่องจากแพลตฟอร์มของภาคเอกชนไม่ได้มีการเชื่อมโยงกับ Gckey ดังนั้น ผู้ให้บริการแต่ละรายต้องมีการพิสูจน์และยืนยันตัวตนผู้ใช้งานเอง หากเทคโนโลยีและกระบวนการสร้างลายมือชื่ออิเล็กทรอนิกส์เป็นไปตามข้อกำหนดจะทำให้ลายมือชื่ออิเล็กทรอนิกส์มีผลผูกพันตามกฎหมาย

บรรณานุกรม

[๑] National Institute Of Standards And Technology. (2020). *Nist Special Publication 800-57 Part 1 Revision 5 – Recommendation For Key Management: Part 1 – General*. Us Department Of Commerce.

[๒] European Union Agency For Network And Information Security. (2016). *Security Guidelines On The Appropriate Use Of Qualified Electronic Signatures – Guidance For Users*. European Union.

[๓] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๖๓). *ขมธอ. ๒๓-๒๕๖๓ ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ เวอร์ชัน ๑.๐.* กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

[๔] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๖๐). *ขมธอ. ๑๕-๒๕๖๐ ว่าด้วยการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง เวอร์ชัน ๑.๐.* กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

[๕] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๖๐). *ขมธอ. ๑๑-๒๕๖๐ ว่าด้วยการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ เวอร์ชัน ๑.๐.* กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

[๖] สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (๒๕๖๓). *Digital Law – พ.ร.บ.ธุรกรรมฯ เดอะซีรีส์*. สำนักนายกรัฐมนตรี.

[๗] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๖๐). *ขมธอ. ๑๔-๒๕๖๐ ว่าด้วยการใช้ข้อความ Xml สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน เวอร์ชัน ๑.๐.* กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

[๘] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๖๓). *ขมธอ. ๒๔-๒๕๖๓* ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง *เวอร์ชัน ๑.๐.* กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

[๙] European Telecommunications Standards Institute. (2021). *ETSI En 319 102-1 V1.3.1 (2021-11) Electronic Signatures And Infrastructures (Esi); Procedures For Creation And Validation Of ADES Digital Signatures; Part 1: Creation And Validation*.

[๑๐] สำนักงานคณะกรรมการพัฒนาระบบราชการ. (๒๕๖๓) *คู่มือการบริหารความพร้อมต่อสภาวะวิกฤต (Business Continuity Management: Bcm).* สำนักนายกรัฐมนตรี

[๑๑] สำนักงานคณะกรรมการพัฒนาระบบราชการ. (๒๕๖๓) *แนวปฏิบัติในการรับ-ส่งหนังสือราชการทางอิเล็กทรอนิกส์ระหว่างส่วนราชการที่เป็นนิติบุคคล.* สำนักนายกรัฐมนตรี

[๑๒] Alex Preukschat And Drummond Reed. (2021). *Self-Sovereign Identity*. Manning Publications.

[๑๓] National Institute Of Standards And Technology. (2015). *Nist Special Publication 800-57 Part 3 Revision 1 – Recommendation For Key Management: Part 3 – Application-Specific Key Management Guidance.* Us Department Of Commerce.

[๑๔] สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (๒๕๖๔). *มรด. ๑ - ๑ : ๒๕๖๔ ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม เวอร์ชัน ๑.๐*. สำนักนายกรัฐมนตรี.

[๑๕] สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (๒๕๖๔). *มรด. ๑ - ๒ : ๒๕๖๔ ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย เวอร์ชัน ๑.๐*. สำนักนายกรัฐมนตรี.

[๑๖] Internet Engineering Task Force. (2014). Rfc 7292 – Pkcs #12: Personal Information Exchange Syntax V1.1.

[๑๗] National Institute Of Standards And Technology. (2019). *Nist Federal Information Processing Standards Publication 140-3 – Security Requirements For Cryptographic Modules.* Us Department Of Commerce.

[๑๘] International Standard Organization. (2013). *Iso/Iec 27001 Information Security Management System*.

[๑๙] Telecommunication Standardization Sector Of Itu. (2016). *X.509 Information Technology – Open Systems Interconnection – The Directory: Public-Key And Attribute Certificate Frameworks*. International Telecommunication Union.

[๒๐] National Institute Of Standards And Technology. (2019). *Nist Special Publication 800-57 Part 2 Revision 1 – Recommendation For Key Management: Part 2 – Best Practices For Key Management Organizations.* Us Department Of Commerce.

[๒๑] Internet Engineering Task Force. (2014). Rfc 6960 – Internet Public Key Infrastructure Online Certificate Status Protocol - Ocsp.

[๒๒] Internet Engineering Task Force. (2014). Rfc 2986 – Pkcs #10: Certification Request Syntax Specification Version 1.7

[๒๓] Telecommunication Standardization Sector Of Itu. (2020). *X.1403 Security Guidelines For Using Distributed Ledger Technology For Decentralized Identity Management*. International Telecommunication Union.

[๒๔] W3c Proposed Recommendation. (2021). Decentralized Identifiers (Dids) V1.0 – Core Architecture, Data Model, And Representations. World Wide Web Consortium (W3c).

[๒๕] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. *กรอบแนวทางเชื่อมโยง รัฐบาลอิเล็กทรอนิกส์แห่งงชาติ เวอร์ชัน ๒.๐*.

[๒๖] สำนักงานพัฒนารัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๕๘). *มาตรฐานการแลกเปลี่ยนข้อมูลระหว่างระบบสารบรรณอิเล็กทรอนิกส์ เวอร์ชัน ๑.๐*. สำนักนายกรัฐมนตรี.

[๒๗] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๖๓). *ขมธอ. ๒๕-๒๕๖๓* ข้อความอิเล็กทรอนิกส์สำหรับใบประมวลผลการศึกษา *เวอร์ชัน ๑.๐*. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.