

ETDA
สำนักงาน
www.eta.or.th



กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

ลายมือชื่อ อิเล็กทรอนิกส์ Electronic Signature

ข้อเสนอแนะมาตรฐานฯ ว่าด้วย
แนวทางการลงลายมือชื่ออิเล็กทรอนิกส์
(Electronic Signature Guideline)
เลขที่ ขมร. 23-2563

ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature)

ตาม พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ที่แก้ไขเพิ่มเติม (ฉบับที่ 3) พ.ศ. 2562

หมายถึง อักษร อักษรระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

แบ่งได้เป็น 2 ประเภท

★ ลายมือชื่อตามมาตรา 9

1

ระบุตัว
ผู้เป็นเจ้าของ
ลายมือชื่อได้

2

แสดงเจตนาของ
เจ้าของลายมือชื่อ
กับข้อความที่
ลงลายมือชื่อได้

3

ใช้วิธีการที่เชื่อถือได้ *
โดยคำนึงถึง

ความมั่นคงและรัดกุม
ของวิธีการที่ใช้

ลักษณะ ประเภท หรือ
ขนาดของธุรกรรมที่ทำ ฯลฯ

ความรัดกุมของระบบ
ติดต่อสื่อสาร

★ ลายมือชื่อตามมาตรา 26

กฎหมายให้ถือว่าเป็นลายมือชื่อที่เชื่อถือได้

1

ข้อมูลที่ใช้สร้าง
ลายมือชื่อ
เชื่อมโยง
ไปยังเจ้าของ
ลายมือชื่อได้

2

ข้อมูลที่ใช้สร้าง
ลายมือชื่อ
อยู่ภายใต้
การควบคุมของ
เจ้าของลายมือชื่อ

3

สามารถตรวจพบ
การเปลี่ยนแปลง
ของลายมือชื่อ /
ข้อความ ได้



* นอกจากจะใช้วิธีการที่เชื่อถือได้ในการลงลายมือชื่อแล้ว สามารถเลือกวิธีการอื่นใดหรือพยานหลักฐานอื่นประกอบ เพื่อระบุตัวเจ้าของลายมือชื่อ และการแสดงเจตนาของเจ้าของลายมือชื่อได้ด้วย

ข้อเสนอแนะมาตรฐานฯ (ETDA Recommendation) ว่าด้วย

แนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature Guideline)

ขอบข่าย

อธิบายภาพรวมและข้อกำหนดที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ เพื่อให้ผู้ใช้งานที่ต้องการใช้ลายมือชื่ออิเล็กทรอนิกส์มีแนวทางในการลงลายมือชื่ออิเล็กทรอนิกส์ และสามารถเลือกใช้วิธีการลงลายมือชื่ออิเล็กทรอนิกส์ที่เหมาะสมกับการทำธุรกรรมทางอิเล็กทรอนิกส์



อย่างไรก็ตาม ข้อเสนอแนะมาตรฐานฉบับนี้เป็นคำแนะนำเกี่ยวกับการปฏิบัติตามข้อกำหนดตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งอาจยังมีข้อกำหนดเกี่ยวกับการลงลายมือชื่ออิเล็กทรอนิกส์ตามกฎหมายอื่นที่กำหนดไว้เป็นการเฉพาะ ดังนั้น ผู้ใช้งานควรมีการศึกษาข้อกำหนดอื่น ๆ ที่เกี่ยวข้องประกอบด้วย

ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ เป็นอย่างไร

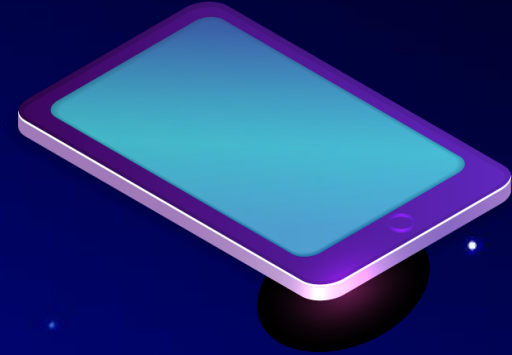
หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่
กำหนดใน**มาตรา 26** แห่งกฎหมายว่าด้วยธุรกรรมทาง
อิเล็กทรอนิกส์

ลายมือชื่อดิจิทัล (Digital Signature)

หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการ
เข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งช่วยให้สามารถ
ยืนยันตัวเจ้าของลายมือชื่อและตรวจพบการเปลี่ยนแปลง
ของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ รวมถึง
การทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดชอบ
จากข้อความที่ตนเองลงลายมือชื่อได้



ตัวอย่างรูปแบบของลายมือชื่ออิเล็กทรอนิกส์



- การพิมพ์ชื่อไว้ท้ายเนื้อหาของอีเมล
- การสแกนภาพของลายมือชื่อที่เขียนด้วยมือและแนบไปกับเอกสาร
- การใช้สไตลัส (stylus) เขียนลายมือชื่อด้วยมือลงบนหน้าจอและบันทึกไว้
- การคลิกปุ่มแสดงการยอมรับหรือตกลง
- การทำเครื่องหมายในช่องแสดงการยอมรับ
- การใช้ลายมือชื่อดิจิทัล

รูปแบบของลายมือชื่ออิเล็กทรอนิกส์สามารถนำมาใช้ใน**ระบบงานอัตโนมัติ (automated workflow system)** ซึ่งจะมีการควบคุมการเข้าถึง การยืนยันตัวตน และการตรวจสอบสิทธิของผู้ใช้งาน ก่อนอนุญาตให้ผู้ใช้งานดำเนินการลงลายมือชื่อ ตัวอย่างเช่น ระบบอีเมลที่มีการยืนยันความถูกต้องของผู้ส่งอีเมลและการส่งอีเมล

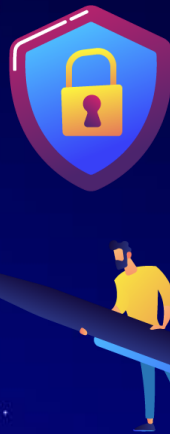
ประเภทของลายมือชื่ออิเล็กทรอนิกส์

ประเภทที่ 1 ลายมือชื่อ อิเล็กทรอนิกส์ ทั่วไป



เป็นลายมือชื่ออิเล็กทรอนิกส์ในรูปแบบใด ๆ (เป็นอักษร อักษรตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์) ที่มีลักษณะตามที่กำหนดใน**มาตรา 9** แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ประเภทที่ 2 ลายมือชื่อ อิเล็กทรอนิกส์ ที่เชื่อถือได้



เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดใน**มาตรา 26** แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

เช่น ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐาน
กุญแจสาธารณะ (Public Key Infrastructure:
PKI)

ประเภทที่ 3 ลายมือชื่อ อิเล็กทรอนิกส์ ที่เชื่อถือได้

ซึ่งใช้ในรับรองที่ออกโดย
ผู้ให้บริการออก
ใบรับรอง

เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดใน**มาตรา 26** และอาศัยใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ตามที่กำหนดใน**มาตรา 28** แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

เช่น ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) และใช้ในรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง

ประเภทของลายมือชื่ออิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป

ประเภทที่ 1
ลายมือชื่อ
อิเล็กทรอนิกส์
ทั่วไป

เป็นลายมือชื่ออิเล็กทรอนิกส์ในรูปแบบใด ๆ (เป็นอักษร อักษรตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์) ที่มีลักษณะตามที่กำหนดใน**มาตรา 9** แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

ประเภทที่ 2
ลายมือชื่อ
อิเล็กทรอนิกส์
ที่เชื่อถือได้

เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดใน**มาตรา 26** แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

เช่น ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐาน
กุญแจสาธารณะ: (Public Key Infrastructure:
PKI)

ประเภทที่ 3
ลายมือชื่อ
อิเล็กทรอนิกส์
ที่เชื่อถือได้

ซึ่งใช้ในรับรองที่ออกโดย
ผู้ให้บริการออก
ใบรับรอง

เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดใน**มาตรา 26** และอาศัยใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ตามที่กำหนดใน**มาตรา 28** แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

เช่น ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ:
(PKI) และใช้ในรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง

องค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์

	การพิสูจน์และยืนยันตัวตน ¹	เจตนาในการลงลายมือชื่อ	การรักษาความครบถ้วนของข้อมูล
ประเภทที่ 1 ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป	มีการพิสูจน์และยืนยันตัวตนที่น่าเชื่อถือและเหมาะสมกับความเสี่ยงของธุรกรรม	มีกระบวนการหรือหลักฐานที่แสดงได้ว่าบุคคลได้ยอมรับการลงลายมือชื่อที่ตนได้ลงลายมือชื่ออย่างชัดเจน	ใช้หลักฐานหรือบุคคลที่สามที่น่าเชื่อถือได้ เพื่อแสดงว่าไม่มีการเปลี่ยนแปลงความหมายของข้อความที่ลงลายมือชื่อ และรับรองความครบถ้วนของข้อมูล
ประเภทที่ 2 ลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือ	<ul style="list-style-type: none"> มีการพิสูจน์ตัวตนที่น่าเชื่อถือและเหมาะสมกับความเสี่ยงของธุรกรรมหรือที่ระดับ IAL2 ขึ้นไป ² มีการยืนยันตัวตนที่ระดับ AAL2 ขึ้นไป ³ 	ใช้ลายมือชื่อดิจิทัลในการลงลายมือชื่อต่อข้อความที่ตนแสดงเจตนา	ใช้ลายมือชื่อดิจิทัลในการลงลายมือชื่อต่อข้อความ
ประเภทที่ 3 ลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง	<ul style="list-style-type: none"> มีการพิสูจน์ตัวตนที่น่าเชื่อถือและเหมาะสมกับความเสี่ยงของธุรกรรมหรือที่ระดับ IAL2 ขึ้นไป มีการยืนยันตัวตนที่ระดับ AAL2 ขึ้นไป 	ใช้ลายมือชื่อดิจิทัลซึ่งใช้ใบรับรองที่ออกโดย CA ในการลงลายมือชื่อต่อข้อความที่ตนแสดงเจตนา	ใช้ลายมือชื่อดิจิทัลซึ่งใช้ใบรับรองที่ออกโดย CA ในการลงลายมือชื่อต่อข้อความ

¹ ข้อเสนอนโยบายมาตรฐาน 4 แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ เลขที่ ขมรจ. 18-2561, เวอร์ชัน 1.0.

² ข้อเสนอนโยบายมาตรฐาน 4 แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน เลขที่ ขมรจ. 19-2561, เวอร์ชัน 1.0.

³ ข้อเสนอนโยบายมาตรฐาน 4 แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน เลขที่ ขมรจ. 20-2561, เวอร์ชัน 1.0.

การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์

การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ที่มีความน่าเชื่อถือและความเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ จะช่วยจัดการความเสี่ยงหรือผลกระทบที่เป็นไปได้จาก**ภัยคุกคามหรือเหตุการณ์ที่ลายมือชื่ออิเล็กทรอนิกส์จะไม่ใช่ที่ยอมรับ** ดังตัวอย่างเช่น

- **การปลอมตัวเป็นผู้อื่น (impersonation)**
เช่น ผู้ลงลายมือชื่อไม่ใช่เจ้าของลายมือชื่อ
- **การปฏิเสธความรับผิดชอบ (repudiation)**
เช่น ผู้ลงลายมือชื่อพยายามปฏิเสธว่าตนเองไม่ได้ลงลายมือชื่อ
- **ข้อมูลไม่มีความครบถ้วน (loss of data integrity)**
เช่น ข้อมูลมีการเปลี่ยนแปลงหลังจากที่ลงลายมือชื่อ
- **การไม่มีอำนาจลงนาม (exceeding authority)**
เช่น ผู้ลงลายมือชื่อไม่ได้รับอนุญาตให้ลงลายมือชื่อกับข้อมูลอิเล็กทรอนิกส์



ในการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ ผู้ใช้งานควรพิจารณาถึงปัจจัยเสี่ยงเพื่อนำไปวิเคราะห์ความเสี่ยงและวิธีการบรรเทาความเสี่ยงจากเหตุการณ์ที่ลายมือชื่ออิเล็กทรอนิกส์จะไม่ใช่ที่ยอมรับได้อย่างเหมาะสม

การบรรเทาความเสี่ยงและหลักฐานของลายมือชื่ออิเล็กทรอนิกส์

ประเภทที่ 1 ลายมือชื่อ อิเล็กทรอนิกส์ ทั่วไป

ตัวอย่างของรูปแบบของลายมือชื่ออิเล็กทรอนิกส์	ตัวอย่างของการบรรเทาความเสี่ยง	ตัวอย่างของพยานหลักฐาน
<ul style="list-style-type: none"> - การพิมพ์ชื่อไว้ท้ายเนื้อหาของอีเมล 	<ul style="list-style-type: none"> - ตรวจสอบการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของอีเมล - บันทึกข้อมูลการตัดสินใจทางอีเมลไว้ในระบบการจัดการเอกสารที่เหมาะสม 	<ul style="list-style-type: none"> - ข้อมูลที่ลงลายมือชื่อ - ชื่อที่พิมพ์ไว้ท้ายเนื้อหาของอีเมล - วันที่เวลาที่ลงลายมือชื่อ หรือวันที่เวลาที่ส่งอีเมล - อัตลักษณ์ (identity) ของผู้ลงลายมือชื่อ - วิธีการที่ใช้ยืนยันตัวตน
<ul style="list-style-type: none"> - การสแกนภาพของลายมือชื่อที่เขียนด้วยมือและแนบไปกับเอกสาร - การใช้สไตลัส (stylus) เขียนลายมือชื่อด้วยมือลงบนหน้าจอและบันทึกไว้ 	<ul style="list-style-type: none"> - เชื่อมโยงวิธีการที่บุคคลใช้แสดงเจตนากับข้อมูลบริบทที่สำคัญเกี่ยวกับผู้ลงลายมือชื่อ รูปแบบของลายมือชื่อ กระบวนการลงลายมือชื่อ และวันที่เวลาที่ลงลายมือชื่อ - เชื่อมโยงวิธีการที่บุคคลใช้แสดงเจตนากับข้อความที่ลงลายมือชื่ออย่างชัดเจน - ดำเนินการตรวจสอบกระบวนการลงลายมือชื่ออย่างสม่ำเสมอเพื่อแสดงให้เห็นถึงการใช้งานที่สอดคล้องกัน 	<ul style="list-style-type: none"> - ข้อมูลที่ลงลายมือชื่อ - ภาพของลายมือชื่อที่เขียนด้วยมือ - วันที่เวลาที่ลงลายมือชื่อ - อัตลักษณ์ (identity) ของผู้ลงลายมือชื่อ - วิธีการที่ใช้ยืนยันตัวตน
<ul style="list-style-type: none"> - การใช้ระบบงานอัตโนมัติที่มีการยืนยันตัวผู้ใช้งานมาประกอบกับรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 1 	<ul style="list-style-type: none"> - ดำเนินการตรวจสอบระบบงานและฟังก์ชันการทำงานอย่างสม่ำเสมอ - บันทึกข้อมูลบริบทที่จำเป็นโดยอัตโนมัติหากเป็นไปได้ - มีกระบวนการที่เหมาะสมในการพิสูจน์และยืนยันตัวตนของบุคคลและการควบคุมการเข้าถึงข้อมูล - ตั้งค่าหรือควบคุมเอกสารและเนื้อหาไม่ให้มีการแก้ไขเปลี่ยนแปลงได้หลังจากลงลายมือชื่อแล้ว - มีบันทึกธุรกรรม (transaction record) ส่งให้ผู้ที่เกี่ยวข้องเพื่อเก็บรักษาเป็นหลักฐานของการทำธุรกรรม 	<ul style="list-style-type: none"> - ข้อมูลที่ลงลายมือชื่อ - ลายมือชื่ออิเล็กทรอนิกส์ - บันทึกเหตุการณ์ (log) ของการยืนยันตัวผู้ใช้งาน - บันทึกเหตุการณ์ (log) ของการแสดงเจตนาในการลงลายมือชื่อ (เช่น การคลิกปุ่มหรือการกำเครื่องหมายในช่องแสดงการยอมรับ) - อัตลักษณ์ (identity) ของผู้ลงลายมือชื่อ - วิธีการที่ใช้ยืนยันตัวตน

การบรรเทาความเสี่ยงและหลักฐานของลายมือชื่ออิเล็กทรอนิกส์

ประเภทที่ 2 ลายมือชื่อ อิเล็กทรอนิกส์ ที่เชื่อถือได้

ตัวอย่างของรูปแบบของลายมือชื่ออิเล็กทรอนิกส์	ตัวอย่างของการบรรเทาความเสี่ยง	ตัวอย่างของพยานหลักฐาน
<ul style="list-style-type: none"> ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) 	<ul style="list-style-type: none"> มีการบริหารจัดการคู่กุญแจและข้อมูลใบรับรองใน PKI อย่างเหมาะสม เพื่อให้มั่นใจได้ว่า ลายมือชื่อดิจิทัลสามารถยืนยันตัวเจ้าของลายมือชื่อและตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ 	<ul style="list-style-type: none"> ข้อมูลที่ลงลายมือชื่อ ลายมือชื่อดิจิทัล วันเวลาที่ลงลายมือชื่อ ใบรับรอง ซึ่งใช้สนับสนุนการตรวจสอบลายมือชื่อดิจิทัล ข้อมูลสำหรับตรวจสอบความสมบูรณ์ของใบรับรองการพิกใช้ หรือการเพิกถอนใบรับรอง
<ul style="list-style-type: none"> ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) และใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง 	<ul style="list-style-type: none"> มีการบริหารจัดการคู่กุญแจและข้อมูลใบรับรองใน PKI อย่างเหมาะสม เพื่อให้มั่นใจได้ว่า ลายมือชื่อดิจิทัลสามารถยืนยันตัวเจ้าของลายมือชื่อและตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ 	<ul style="list-style-type: none"> ข้อมูลที่ลงลายมือชื่อ ลายมือชื่อดิจิทัล วันเวลาที่ลงลายมือชื่อ ใบรับรอง ซึ่งใช้สนับสนุนการตรวจสอบลายมือชื่อดิจิทัล ข้อมูลสำหรับตรวจสอบความสมบูรณ์ของใบรับรองการพิกใช้ หรือการเพิกถอนใบรับรอง

ประเภทที่ 3 ลายมือชื่อ อิเล็กทรอนิกส์ ที่เชื่อถือได้ ซึ่งใช้ใบรับรองที่ ออกโดยผู้ให้บริการ ออกใบรับรอง



ETDA
เอสพีเอส
www.eta.or.th



กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม