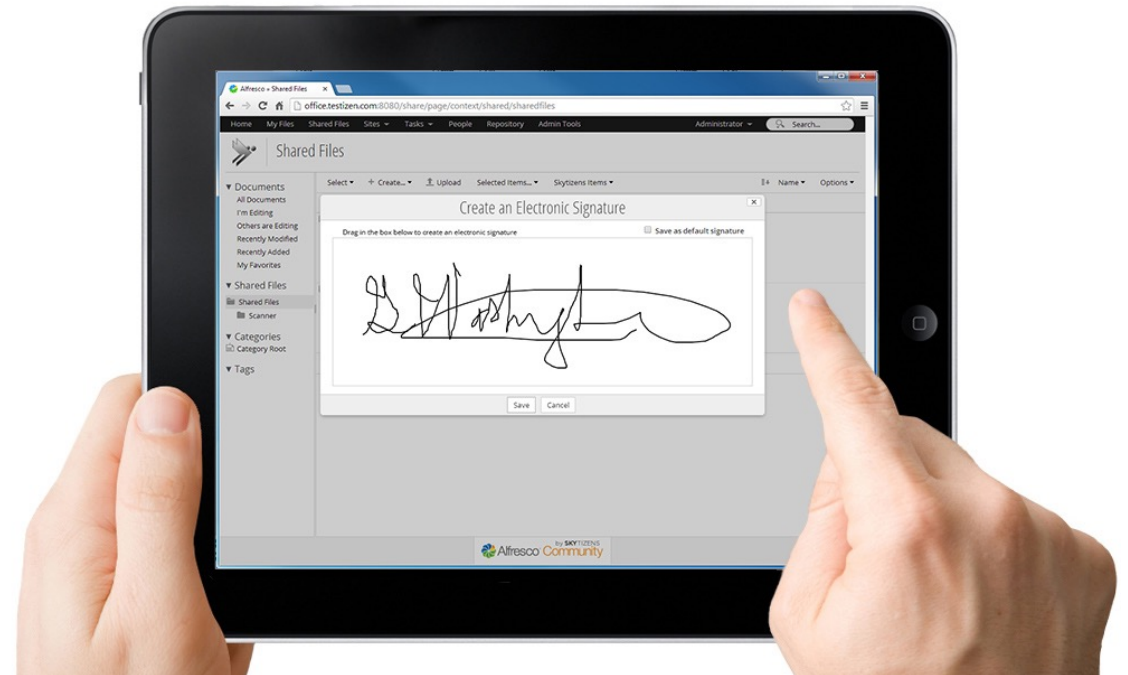


กฎหมายเทคโนโลยีสารสนเทศ :
กฎหมายลายมือชื่ออิเล็กทรอนิกส์

Unit 4

กฎหมายลายมือชื่ออิเล็กทรอนิกส์

- ลายมือชื่ออิเล็กทรอนิกส์กลายเป็นกฎหมายธุรกรรมทางอิเล็กทรอนิกส์ เป็นการระบุการใช้ลายมือดิจิทัล (digital signature) เพื่อระบุหรือยืนยันต่อบุคคลให้เท่าเทียมกับการลงลายมือชื่อทั่วไป โดยคำนึงถึงความเป็นกลางและความน่าเชื่อถือของเทคโนโลยี รวมทั้งคุ้มครองสิทธิของคู่กรณี กฎหมายคุ้มครองให้ลายมือดิจิทัลใช้รับรองลายมือชื่อแบบเดิม (Hand Written) ได้ทุกประการ
- แต่มีข้อแตกต่างที่การลงลายมือดิจิทัลไม่สามารถแยกจากเนื้อหาที่ลงลายมือชื่อได้ จึงส่งผลให้การแก้ไขตัดแปรงได้เล็กน้อยจึงจะสามารถทราบได้ทันที
- กฎหมายที่กำกับดูแล ได้แก่ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔



ประเภทของลายมือชื่ออิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์แบ่งประเภทได้ 2 แบบ

ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป คือ ลายมือชื่อที่เป็นไปตามมาตรา 9 ของพระราชบัญญัติ

- ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน
- วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

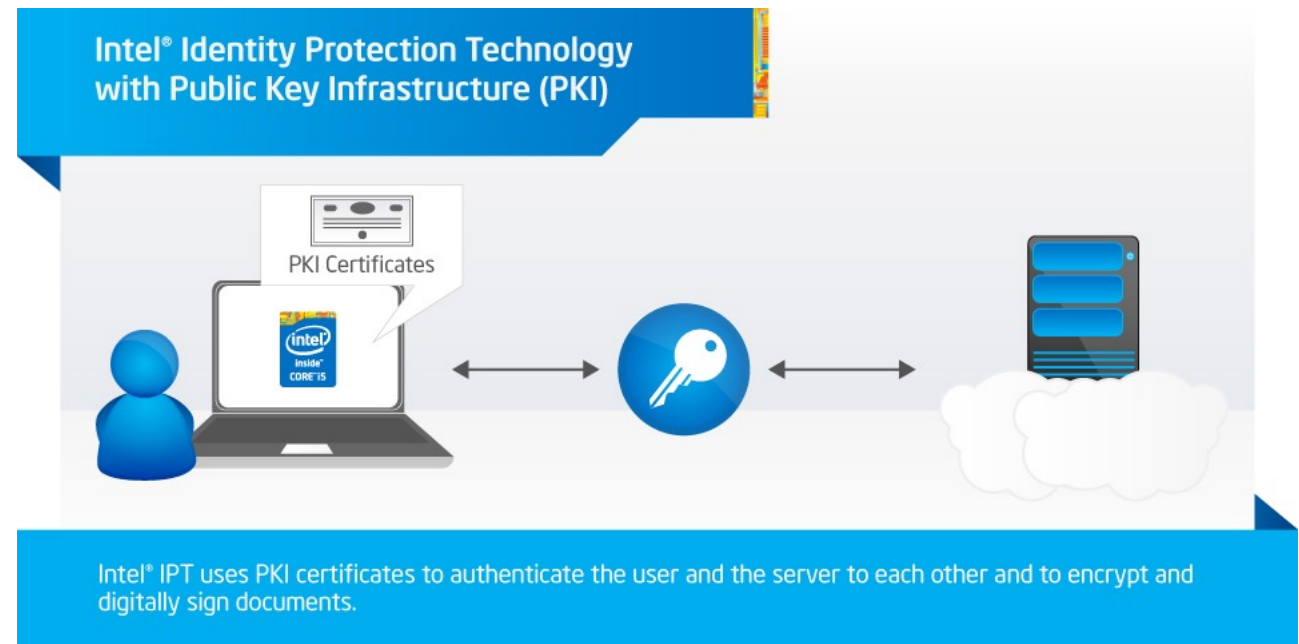
ประเภทของลายมือชื่ออิเล็กทรอนิกส์ [ต่อ]

ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ ในมาตรา 26 ตามพระราชบัญญัติฯ ได้บัญญัติเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือ และลักษณะหรือคุณสมบัติในการพิจารณาว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ ให้พิจารณาจากหลักเกณฑ์ ดังต่อไปนี้

- ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ได้เชื่อมโยงไปยังเจ้าของลายมือชื่อ โดยไม่เชื่อมโยงไปยังบุคคลอื่น ภายใต้อุปกรณ์ที่นำมาใช้
- การเปลี่ยนแปลงใดๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้
- ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปเพื่อรองรับความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์
- ในขณะที่สร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

ลายมือชื่อดิจิทัลและเทคโนโลยี PKI (Public Key Infrastructure)

- การใช้ “กุญแจส่วนตัว” ในการเข้ารหัสจะเป็นส่วนสำคัญในการสร้างลายมือชื่ออิเล็กทรอนิกส์ทั่วไปเรียกว่า “ลายมือชื่อ-ดิจิทัล (Digital Signature)” เพื่อยืนยันตัวบุคคล
- และใช้กุญแจอีกข้างหนึ่ง ที่เรียกว่า “กุญแจสาธารณะ” ในการถอดรหัสซึ่งทำหน้าที่สำคัญ ในการตรวจสอบตัวบุคคล จนกลายเป็นที่มาของการเรียกเทคโนโลยีนี้ว่า “เทคโนโลยี PKI”



การสร้างลายมือชื่อดิจิทัล

1) การสร้างกุญแจคู่ (Key Pairs)

- ก่อนการสร้างลายมือชื่อดิจิทัลต้องมีการสร้างกุญแจคู่ขึ้นมาก่อนด้วยกระบวนการทางคณิตศาสตร์
- โดยเจ้าของกุญแจคู่จะต้องเก็บกุญแจแรกที่เราเรียกว่า “**กุญแจส่วนตัว**” ไว้เป็นความลับ เก็บรักษา “กุญแจส่วนตัว” จะบันทึกและเก็บไว้ในสมาร์ตการ์ด
- ส่วน “**กุญแจสาธารณะ**” ก็จะเปิดเผยไว้ในระบบฐานข้อมูลของผู้ประกอบการรับรอง (Certificaton Authority) เพื่อให้สามารถตรวจสอบตัวบุคคลได้โดยง่าย



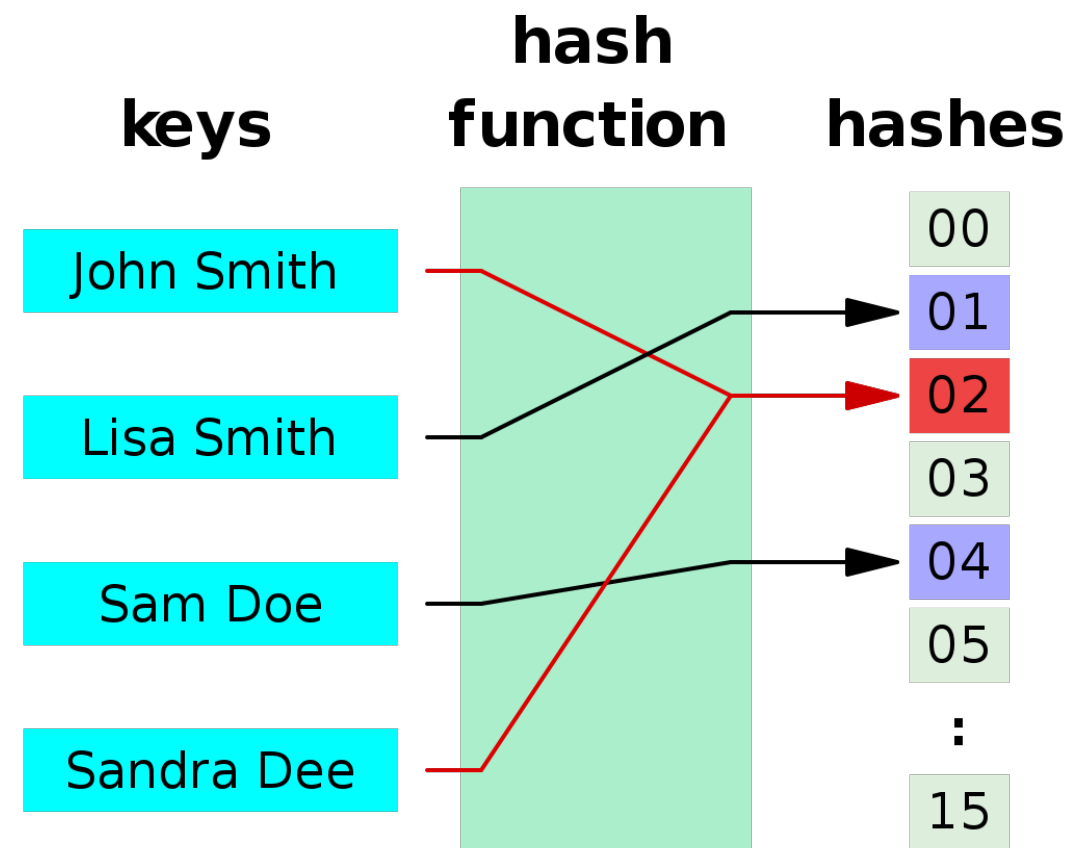
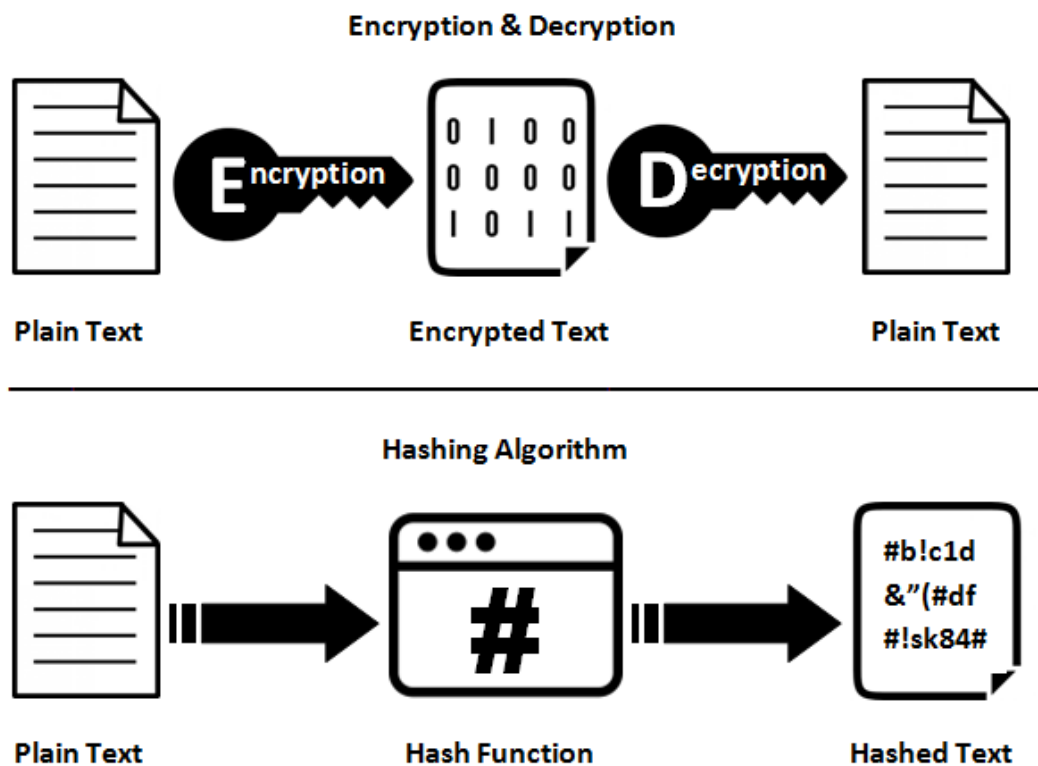
การสร้างลายมือชื่อดิจิทัล [ต่อ]

2) ขั้นตอนการแฮชหรือย่อ (Hash Function)

- ก่อนสร้างลายมือชื่อดิจิทัลมีขั้นตอนสำคัญในการนำข้อมูลอิเล็กทรอนิกส์ที่ผู้ส่งข้อมูลประสงค์จะส่งให้แก่ผู้รับข้อมูล นำมาคำนวณด้วยกระบวนการทางคณิตศาสตร์ (Algorithm) ที่เรียกว่า “ขั้นตอนการแฮช (Hash Function) หรือ One-way cryptography หรือ One-way hash function¹¹
- เพื่อย่อหรือทำให้ข้อมูลอิเล็กทรอนิกส์มีขนาดเล็กลงอันจะทำให้ง่ายต่อการคำนวณทางคณิตศาสตร์และการจัดส่งให้ผู้รับข้อมูล

การสร้างลายมือชื่อดิจิทัล [ต่อ]

ขั้นตอนการแฮชหรือย่อ (Hash Function)



การสร้างลายมือชื่อดิจิทัล [ต่อ]

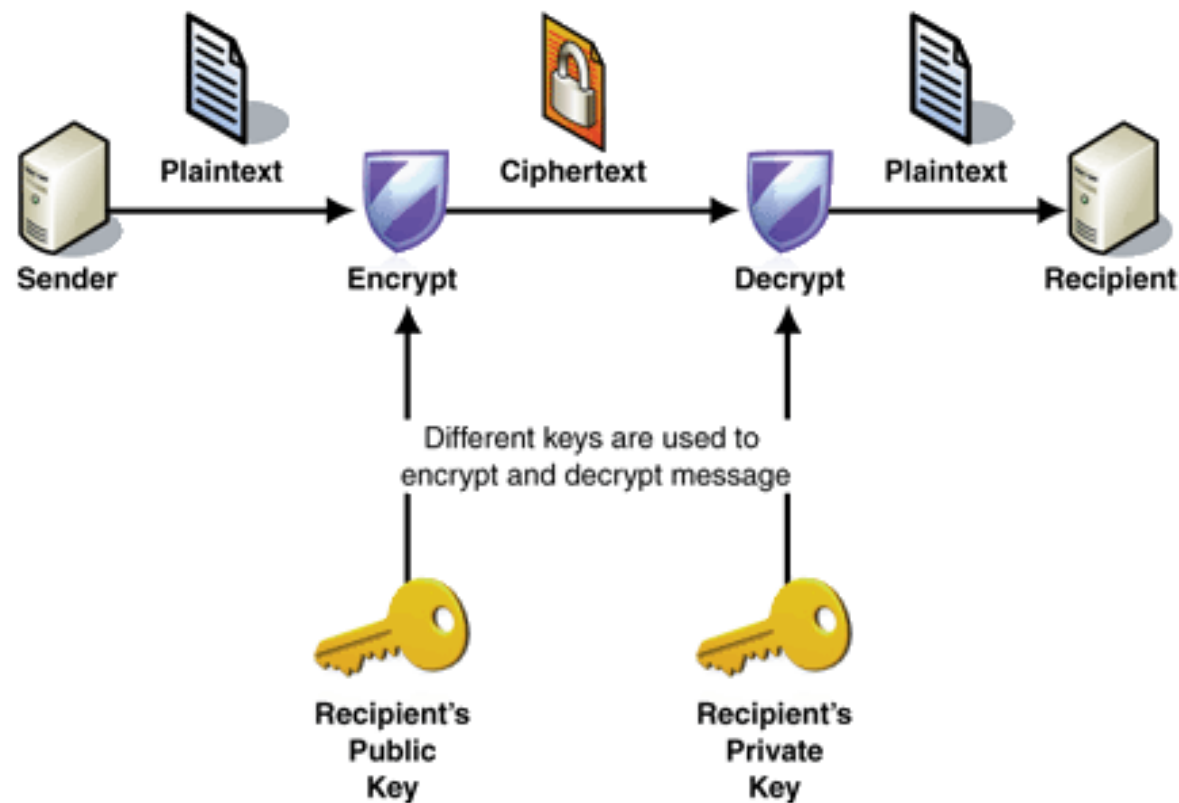
3) การสร้างลายมือชื่อดิจิทัล

- นำกุญแจส่วนตัวมาทำการเข้ารหัสกับข้อมูลที่แฮช ซอฟต์แวร์ก็จะทำการแปลงข้อมูลอิเล็กทรอนิกส์ให้เป็นลายมือชื่อดิจิทัล (Digital Signature)
- จะมีลักษณะเฉพาะที่สัมพันธ์กับข้อมูลแฮช และกุญแจส่วนตัว ทุกครั้งที่ข้อมูลแฮชหรือกุญแจส่วนตัวเปลี่ยนแปลงไปจากเดิม ลายมือชื่อ ดิจิทัลที่ได้ก็จะเปลี่ยนแปลงตามไปด้วย
- ลายมือชื่อดิจิทัลจึงไม่มีโอกาสซ้ำกัน หลังจากสร้างลายมือชื่อดิจิทัลแล้ว ซอฟต์แวร์ก็จะทำการนำลายมือชื่อดิจิทัลที่ได้ไปแนบไว้ท้ายข้อความที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์เพื่อใช้ส่งให้กับผู้รับข้อมูล

การสร้างลายมือชื่อดิจิทัล [ต่อ]

ดังนั้น การส่งข้อมูลอิเล็กทรอนิกส์โดยแนบลายมือชื่อดิจิทัลไปด้วย ประกอบด้วยข้อมูลอิเล็กทรอนิกส์ 3 ส่วน ได้แก่

- **ส่วนแรก** คือข้อมูลอิเล็กทรอนิกส์ที่มีข้อความเดิมซึ่งใช้ในการติดต่อสื่อสารระหว่างบุคคลอันเป็นข้อความที่อ่านออกและเข้าใจได้
- **ส่วนที่สอง** เป็นลายมือชื่อดิจิทัล
- **ส่วนสุดท้าย** จะเป็นกุญแจสาธารณะพร้อมกับใบรับรองกุญแจสาธารณะของผู้ลงลายมือชื่อดิจิทัล



การรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์

ส่วนสำคัญอย่างยิ่งต่อการพัฒนาเทคโนโลยีในการระบุตัวบุคคล การรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์แบ่งออกได้เป็น 5 ประการ ดังนี้

- **การระบุตัวบุคคล (Authentication)** เพื่อยืนยันตัวบุคคลผู้ส่งหรือผู้สร้างข้อมูลอิเล็กทรอนิกส์
- **การควบคุมการเข้าถึง** (ในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ **Access Control**) ซึ่งอนุญาตให้เฉพาะบุคคลซึ่งมีสิทธิหรือได้รับอนุญาตเท่านั้นละป้องกันมิให้บุคคลซึ่งไม่มีสิทธิหรือไม่ได้รับอนุญาตเข้าถึงข้อมูลอิเล็กทรอนิกส์
- **การรักษาความลับ (Confidentiality)** เพื่อป้องกันมิให้บุคคลซึ่งไม่ได้รับอนุญาตหรือไม่มีสิทธิอ่านข้อมูลอิเล็กทรอนิกส์ได้
- **ความถูกต้องครบถ้วนของข้อมูลอิเล็กทรอนิกส์ (Integrity)** เพื่อป้องกันมิให้มีการเปลี่ยนแปลง แก้ไข ทำลายหรือสร้างข้อมูลอิเล็กทรอนิกส์ขึ้นโดยไม่ได้รับอนุญาต
- **การป้องกันการปฏิเสธความรับผิดชอบ (Non-repudiation)** เพื่อป้องกันมิให้ผู้ส่งข้อมูลหรือผู้รับข้อมูลปฏิเสธว่าตนไม่ได้ส่งหรือ ไม่ได้รับข้อมูลอิเล็กทรอนิกส์

พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ.2551

กฎหมายลายมือชื่ออิเล็กทรอนิกส์อยู่ใน พรบ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ.2551 ในหมวด 2
ลายมือชื่ออิเล็กทรอนิกส์ (มาตรา 26 -31)

- **มาตรา 26** เป็นการกำหนดคุณลักษณะการเป็นลายมือชื่ออิเล็กทรอนิกส์ ประกอบด้วย
 - (1) ต้องสามารถเชื่อมโยงไปยังเจ้าของลายมือชื่อได้
 - (2) การสร้างลายมือชื่ออิเล็กทรอนิกส์ต้องไม่มีการควบคุมของบุคคลอื่น
 - (3) การเปลี่ยนแปลงใด ๆ สามารถตรวจพบได้
 - (4) การลงลายมือชื่อ (การนำไปใช้) เมื่อมีการเปลี่ยนแปลงสามารถตรวจพบนับตั้งแต่การลงลายมือชื่ออิเล็กทรอนิกส์

พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ.2551 [ต่อ]

- มาตรา 27 กำหนดเพื่อเป็นแนวทางในการสร้างลายมือชื่ออิเล็กทรอนิกส์
 - (1) ระมัดระวังในการใช้ข้อมูลสำหรับการสร้างลายมือชื่ออิเล็กทรอนิกส์
 - (2) การแจ้งเตือนหากข้อมูลถูกละเมิด ไม่ว่าจะเป็น การถูกทำลาย ถูกแก้ไข ถูกเปิดเผย หรือ ถูกล่วงรู้
 - (3) ในกรณีการออกใบรับรองสนับสนุนการใช้ลายมือชื่ออิเล็กทรอนิกส์ จะต้องระมัดระวัง
- มาตรา 28 ใบรับรองที่สนับสนุนลายมือชื่ออิเล็กทรอนิกส์ให้มีผลทางกฎหมายเสมือนลงลายมือชื่อ
- มาตรา 29 การพิจารณาความเชื่อถือได้ของระบบ วิธีการ และบุคคลากรตามมาตรา 28
- มาตรา 30 คู่กรณีที่เกี่ยวข้องต้องดำเนินการ
 - (1) ดำเนินการตามสมควรในการตรวจสอบ
 - (2) ในกรณีลายมือชื่ออิเล็กทรอนิกส์มีใบรับรอง ต้องมีการตรวจสอบ

พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ.2551 [ต่อ]

- มาตรา 31 ใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ให้ถือว่ามียุทธทางกฎหมายโดยไม่ต้องคำนึงถึง
 - (1) สถานที่ออกใบรับรองหรือสถานที่สร้างหรือใช้ลายมือชื่ออิเล็กทรอนิกส์
 - (2) สถานที่ทำการทำงานของผู้ออกใบรับรองหรือเจ้าของลายมือชื่ออิเล็กทรอนิกส์

