ทำให้บทนิยามนี้รองรับเทคโนโลยีใหม่ที่จะเกิดขึ้นในอนาคตได้เป็นอย่างดี) เมื่อพิเคราะห์บทนิยามนี้แล้ว กฎหมายแม่แบบนี้ใช้บังคับกับการทำการค้าโดยใช้ข้อมูลอิเล็กทรอนิกส์ทุกประเภท

แม้กฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์ทางอิเล็กทรอนิกส์จะมุ่งใช้บังคับกับความสัมพันธ์เชิงพาณิชย์ แต่ก็เปิดโอกาสให้ประเทศต่าง ๆ ขยายขอบเขตการใช้บังคับของกฎหมายนี้เพื่อให้ใช้บังคับกับความสัมพันธ์ที่มิใช่เชิงพาณิชย์ได้ บางประเทศจึงรับเอาหลักเกณฑ์ที่กำหนดไว้ในกฎหมายแม่แบบนี้ไปใช้เป็นการทั่วไป โดยไม่คำนึงว่าจะเป็นกิจกรรมเชิงพาณิชย์หรือไม่ เช่น ประเทศสิงคโปร์หรือมลรัฐอิลลินอยส์ได้นำหลักเกณฑ์เหล่านั้นไปใช้กับการติดต่อกับราชการ หรือกับคำสั่งทางปกครองด้วย เช่น การออกใบอนุญาตตามกฎหมายต่าง ๆ แต่หน่วยงานภาครัฐบางหน่วยงานอาจจะไม่พร้อมหรือมีเหตุผลที่ยังไม่สามารถให้สิทธิเอกชนทำการติดต่อกับราชการโดยใช้ข้อมูลอิเล็กทรอนิกส์ได้ จึงกำหนดไว้ในกฎหมายว่าการติดต่อกับหน่วยงานของรัฐโดยใช้ข้อมูลอิเล็กทรอนิกส์แทนเอกสารธรรมดาต้องได้รับความยินยอมจากหน่วยงานของรัฐที่รับผิดชอบด้วย กล่าวคือ มิใช่เป็นสิทธิเด็ดขาดของเอกชน (not as of right) ที่จะเลือกใช้ข้อมูลอิเล็กทรอนิกส์ในการติดต่อกับทางราชการ แต่เป็นสิทธิของทางราชการในการให้เอกชนทำการเช่นว่านั้นได้[3] กฎหมายของประเทศที่ไม่จำกัดการบังคับใช้ของกฎหมายเกี่ยวกับการยอมรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้บังคับใช้กับความสัมพันธ์เชิงพาณิชย์เท่านั้นมักจะมีชื่อกฎหมายของตนว่า " กฎหมายธุรกรรมทางอิเล็กทรอนิกส์" (Electronic Transactions Law)

1.2 บทบัญญัติทั่วไปที่รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์

กฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์ยอมรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ในหลายเรื่องดังได้กล่าวมาบ้างแล้วในตอนต้น แต่บทบัญญัติทั่ว

---

[3] ดู Electronic Transactions Act 1998 ของประเทศสิงคโปร์ ซึ่งบัญญัติไว้ใน Part XI Government Use of Electronic Records and Signatures โดย Article 47 บัญญัติดังนี้

"(1) Any Department or ministry of the Government, organ of State or statutory corporation that, pursuant to any written law –

a. accepts the filing of documents, or requires that documents be created or retained;

b. issues any permit, licence or approval; or

c. provides for the method and manner of payment,

may, notwithstanding anything to the contrary in such written law –

i. accept the filing of such documents, or the creation or retention of such documents in the form of electronic records;

ii. issue such permit, licence or approval in the form of electronic records; or

iii. make such payment in electronic form.

(2) ... ...

(3) Nothing in this Act shall by itself compel any department or ministry of the Government, organ of State or statutory corporation to accept or issue any document in the form of electronic records."

ไปปรากฏอยู่ใน Article 5: Legal recognition of data messages ซึ่งบัญญัติว่า "ข้อมูลจะไม่ถูกปฏิเสธผลทางกฎหมาย หรือปฏิเสธความสมบูรณ์หรือการมีผลบังคับทางกฎหมายเพียงเพราะเหตุที่ว่าเป็นข้อมูลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์"[4] บทบัญญัตินี้นับเป็นหัวใจของกฎหมายแม่แบบฉบับนี้ นอกจากบทบัญญัติมาตรานี้แล้ว ผู้ร่างกฎหมายแม่แบบได้ตระหนักว่าประเด็นทางกฎหมายเกี่ยวกับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์มักจะเป็นประเด็นที่เกี่ยวข้องกับการทำสัญญาระหว่างกัน จึงได้มีบทบัญญัติบางประการที่กล่าวย้ำถึงการรับรองผลทางกฎหมายของคำเสนอ คำสนอง และการแสดงเจตนาอีก ดังจะได้อธิบายต่อไป[5]

1.3 หลักเกณฑ์เกี่ยวกับ "หนังสือ"

ดังได้กล่าวแล้ว ข้อขัดข้องทางกฎหมายประการหนึ่งที่เกิดในแทบทุกประเทศคือข้อกำหนดเกี่ยวกับ "หนังสือ" (Writing) กฎหมายของประเทศต่าง ๆ มักกำหนดให้สัญญาบางประเภทหรือการบางอย่างต้องทำเป็นหนังสือ หรือมีหลักฐานเป็นหนังสือ จึงจะใช้บังคับได้ กฎหมายแม่แบบจึงกำหนดให้การใช้ข้อมูลอิเล็กทรอนิกส์ในการนั้นๆ ถือว่าเป็นการทำเป็นหนังสือหรือมีหลักฐานเป็นหนังสือแล้วหากข้อมูลอิเล็กทรอนิกส์นั้นอยู่ในสภาพที่สามารถเข้าถึงได้และนำกลับมาใช้ในภายหลังได้ (accessible so as to be usable for subsequent reference) ทั้งนี้ คำอธิบายประกอบกฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์ (Guide to Enactment)[6] ได้อธิบายว่าสภาพที่สามารถเข้าถึงข้อมูลอิเล็กทรอนิกส์นั้นหมายถึงสภาพที่ข้อมูลอิเล็กทรอนิกส์นั้นสามารถอ่านได้และแปลความหมายได้ (readable and interpretable)[7] ดังนั้น หากมีการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลนั้นไว้ ข้อมูลนั้นก็ต้องอยู่ในสภาพที่พร้อมที่จะถอดรหัสเพื่อให้เข้าใจได้ด้วย ส่วนการนำกลับมาใช้ในภายหลังนั้นมิได้จำกัดอยู่เพียงการใช้โดยมนุษย์เท่านั้น แต่ยังรวมไปถึงการใช้โดยเครื่องคอมพิวเตอร์อีกด้วย[8] (เช่นในระบบ EDI ที่มีการตั้งโปรแกรมให้คอมพิวเตอร์

---

[4] **Article 5.** Legal recognition of data messages

"Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message."

[5] ดูหัวข้อ 1.8 ต่อไป

[6] Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce เป็นคำอธิบายประกอบตัวบทในกฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์ คำอธิบายประกอบนี้จัดทำขึ้นเพื่ออธิบายความหมายของบทบัญญัติต่างๆ เพื่อความเข้าใจร่วมกันของประเทศต่างๆ โดยได้เขียนขึ้นจากบรรดาข้อเท็จจริงและเอกสารที่เกิดขึ้นหรือที่จัดทำขึ้นในชั้นที่ได้ยกร่างกฎหมายนี้ (traveaux préparatoires)

[7] ดู paragraph 50 ของ Guide to Enactment

[8] *Ibid.*

สามารถประมวลผลข้อมูลอิเล็กทรอนิกส์ที่ได้รับ และหลังจากที่ได้รับและประมวลผลแล้ว เครื่องคอมพิวเตอร์ก็อาจส่งคำตอบรับต่างๆ ไปยังเครื่องคอมพิวเตอร์ของอีกฝ่ายหนึ่งได้ทันที)[9]

แม้ว่ากฎหมายจะให้การยอมรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์เสมอกับเอกสารธรรมดาในแง่ของการทำเป็นหนังสือหรือการมีหลักฐานเป็นหนังสือ แต่ก็ต้องตระหนักว่าในบางกรณีอาจมีความจำเป็นต้องกำหนดข้อยกเว้นมิให้ใช้ข้อมูลอิเล็กทรอนิกส์แทนข้อความธรรมดา เช่น ในกรณีที่กฎหมายกำหนดให้ผู้ประกอบการค้าเขียนข้อความในลักษณะเตือนให้ผู้บริโภคทราบถึงอันตรายของสินค้าหรือบริการบางประเภท ในกรณีเช่นว่านี้ไม่สมควรที่ให้ผู้ประกอบการค้าแจ้งคำเตือนภัยโดยใช้ข้อมูลอิเล็กทรอนิกส์ เป็นต้น หรือในกรณีที่เกี่ยวกับเช็คซึ่งประเทศต่างๆ ยอมรับกันว่าไม่สมควรที่จะให้มีการใช้ข้อมูลอิเล็กทรอนิกส์แทนตราสารในขณะนี้[10]

1.4 หลักเกณฑ์เกี่ยวกับ "ลายมือชื่อ"

หลักเกณฑ์เกี่ยวกับลายมือชื่อเป็นเรื่องใหญ่ที่มีความสำคัญมาก หลายประเทศได้มีการตรากฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signatures) หรือลายมือชื่อดิจิทัล (Digital Signatures) โดยเฉพาะ บทความนี้จะอธิบายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ (รวมถึงลายมือชื่อดิจิทัล) ไว้ในส่วนที่ 2 จึงไม่ขอกล่าวถึงรายละเอียดในที่นี้ แต่จะกล่าวเพียงบทบัญญัติของกฎหมายแม่แบบของ UNCITRAL เกี่ยวกับเรื่องนี้เท่านั้น เพื่อเป็นข้อมูลเบื้องต้นที่จะช่วยให้เข้าใจส่วนที่ 2 ของบทความนี้ได้ดียิ่งขึ้น

ในขณะที่บุคคลลงลายมือชื่อธรรมดาลงในเอกสารเพื่อแสดงว่าตนเห็นชอบ รับรู้หรือรับรองเนื้อหาสาระของเอกสารนั้น การใช้ลายมือชื่ออิเล็กทรอนิกส์ก็มีวัตถุประสงค์เช่นเดียวกัน กล่าวคือ บุคคลจะใช้ลายมือชื่ออิเล็กทรอนิกส์กำกับข้อความอิเล็กทรอนิกส์เพื่อแสดงว่าตนเป็นเจ้าของลายมือชื่อนั้นและเห็นชอบกับข้อความอิเล็กทรอนิกส์นั้น วัตถุประสงค์ดังกล่าวเป็นการตรวจสอบความถูกต้อง (Authentication) นั่นเอง Article 7 ของกฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์จึงกำหนดหลักเกณฑ์พื้นฐานของลายมือชื่ออิเล็กทรอนิกส์ว่าต้องสร้างขึ้นโดยกระบวนการที่สามารถระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่อและสามารถบ่งบอกได้ว่าบุคคลนั้นเห็นชอบกับข้อความอิเล็กทรอนิกส์ที่มีลายมือชื่อนั้นกำกับ กฎหมายแม่แบบยังกำหนดด้วยว่าวิธีการที่นำมาใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นต้องมีความน่าเชื่อถือ โดยต้องเป็นวิธีการที่เหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ ส่วนความน่าเชื่อถือและเหมาะสมในนัยดังกล่าวนั้นเป็นเรื่องที่ต้องพิเคราะห์พฤติการณ์ทั้งปวงประกอบ ทั้งนี้ คำอธิบายประกอบกฎหมายแม่แบบ (Guide to Enactment) ได้ให้ตัวอย่างของพฤติการณ์ดังกล่าวไว้อย่างกว้างขวาง ซึ่งรวมถึงพฤติ

[9] ดูเชิงอรรถที่ 27

[10] ดู paragraph 51 ของ Guide to Enactment

การณ์ดังต่อไปนี้ คือ ความพร้อม คุณสมบัติหรือประสิทธิภาพของเครื่องมือที่คู่กรณีนำมาใช้ ความสามารถของระบบสื่อสาร ลักษณะของกิจกรรมทางการค้านั้นๆ ความบ่อยครั้งที่คู่กรณีทำธุรกรรมระหว่างกัน ประเภทและขนาดของธุรกรรมที่ทำระหว่างกัน ความสำคัญและมูลค่าของข้อมูลอิเล็กทรอนิกส์ที่สื่อสารกัน ทางปฏิบัติทางการค้า เป็นต้น[11]

1.5 หลักเกณฑ์เกี่ยวกับ "ต้นฉบับ"

ในบางกรณีกฎหมายกำหนดให้ต้องแสดงหรือเก็บรักษาเอกสาร**ต้นฉบับ** ผู้ที่ใช้ข้อมูลอิเล็กทรอนิกส์อาจประสงค์จะแสดงหรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์แทนการนำเอกสารมาแสดงหรือแทนการเก็บรักษาเอกสาร แต่ข้อมูลอิเล็กทรอนิกส์ไม่มีคุณสมบัติของความเป็น**ต้นฉบับ**ในความหมายที่ใช้กับเอกสารทั่วไปเพราะผู้ที่รับข้อมูลอิเล็กทรอนิกส์ล้วนแล้วแต่รับสำเนาของสื่อที่ทำขึ้นทั้งสิ้น กฎหมายแม่แบบของ UNCITRAL จึงมีบทบัญญัติที่ว่าหากมีการแสดงหรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์โดยวิธีการที่น่าเชื่อถือได้ซึ่งสามารถรักษาความถูกต้องของข้อมูลอิเล็กทรอนิกส์ตั้งแต่ที่แรกสร้างข้อมูลนั้นขึ้นเป็นข้อมูลรูปแบบสุดท้าย (final form) ก็ให้ถือว่าเป็นการแสดงหรือเก็บรักษาเอกสารต้นฉบับตามกฎหมายนั้นแล้ว[12] การรักษาความถูกต้องของข้อมูลอิเล็กทรอนิกส์ต้องพิเคราะห์ว่าข้อมูลอิเล็กทรอนิกส์ยังอยู่ในสภาพที่สมบูรณ์โดยปราศจากการเปลี่ยนแปลงแก้ไข (complete and unaltered) หรือไม่ ส่วนการพิเคราะห์ว่าวิธีการรักษาความถูกต้องของข้อมูลอิเล็กทรอนิกส์เป็นวิธีการที่น่าเชื่อถือได้หรือไม่ก็เป็นเรื่องที่ต้องพิจารณาจากพฤติการณ์ที่เกี่ยวข้องทั้งปวง นอกจากนี้ หากเป็นกรณีที่กฎหมายกำหนดให้แสดงเอกสารต้นฉบับ ถ้าบุคคลเลือกที่จะนำ

---

[11] ดู paragraph 58 ของ Guide to Enactment

[12] **Article 8. Original**

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

... ...

(3) For the purposes of subparagraph (a) of paragraph (1):

(a) the criteria for assessing integrity shall be whether the inofrmation has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

ข้อมูลอิเล็กทรอนิกส์ที่ไม่มีการเปลี่ยนแปลงแก้ไขมาแสดงแทนการแสดงเอกสารต้นฉบับ ข้อมูลอิเล็กทรอนิกส์นั้นต้องอยู่ในสภาพที่สามารถทำให้ปรากฏแก่บุคคลที่จะเป็นผู้รับข้อมูลนั้นด้วย[13]

ในการรับส่งข้อมูลอิเล็กทรอนิกส์โดยทางคอมพิวเตอร์หรือโดยระบบเครือข่ายมักมีการตั้งโปรแกรมให้ระบบคอมพิวเตอร์หรือระบบเครือข่ายบันทึกข้อความที่จำเป็นเพิ่มเติมเข้าไปในตอนต้นหรือตอนท้ายของข้อความเดิม เช่น การบันทึกเครือข่ายต้นทางของข้อมูลอิเล็กทรอนิกส์ เป็นต้น การเพิ่มข้อความในลักษณะนี้ไม่ถือว่าเป็นการเปลี่ยนแปลงแก้ไขความเดิมของข้อมูลอิเล็กทรอนิกส์ ดังนั้น หากความอื่นของข้อมูลอิเล็กทรอนิกส์ยังอยู่ในสภาพที่สมบูรณ์โดยปราศจากการเปลี่ยนแปลงแก้ไขก็ยังถือว่าข้อมูลอิเล็กทรอนิกส์นั้นยังอยู่ในสภาพต้นฉบับอยู่[14]

1.6 การรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน

เมื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์โดยให้มีผลทางกฎหมายเช่นเดียวกับเอกสารธรรมดาก็จำเป็นต้องให้บุคคลสามารถนำข้อมูลอิเล็กทรอนิกส์มาเป็นพยานหลักฐานได้ กฎหมายแม่แบบของ UNCITRAL จึงมีบทบัญญัติเกี่ยวกับการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานไว้ด้วย[15] ส่วนการชั่งน้ำหนักพยานหลักฐานนั้นเป็นเรื่องที่ต้องพิจารณาถึงพฤติการณ์ทั้งปวง โดยคำนึงถึงวิธีการสร้าง เก็บ รับ และส่งข้อมูลอิเล็กทรอนิกส์นั้น และวิธีการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์นั้นด้วย[16]

1.7 หลักเกณฑ์เกี่ยวกับการเก็บรักษาข้อมูลหรือเอกสาร

---

[13] ดู Article 8 (1) (b).

[14] ดู Article 8 (3) (a) and Guide to Enactment, paragraph 67.

[15] **Article 9. Admissibility and evidential weight of data messages**

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

[16] ดู Article 9 (2)

กฎหมายของประเทศต่าง ๆ มักกำหนดให้บุคคลเก็บรักษาข้อมูลหรือเอกสารไว้เพื่อประโยชน์ตามที่กฎหมายนั้น ๆ กำหนด เช่น การเก็บรักษาสมุดบัญชี เป็นต้น หากต้องเก็บรักษาข้อมูลเหล่านี้ในรูปของเอกสารธรรมดาเสมอไปก็อาจจะเกิดความไม่สะดวกและทำให้สิ้นเปลืองเนื้อที่จัดเก็บเอกสารเป็นอย่างมาก กฎหมายแม่แบบของ UNCITRAL จึงมีบทบัญญัติให้เก็บรักษาข้อมูลในรูปของข้อมูลอิเล็กทรอนิกส์ได้โดยให้มีผลทางกฎหมายเช่นเดียวกับการเก็บรักษาข้อมูลในรูปของเอกสารธรรมดา[17] กฎหมายแม่แบบกำหนดหลักเกณฑ์สำคัญเกี่ยวกับเรื่องนี้ไว้ ประการแรก การเก็บรักษาข้อมูลอิเล็กทรอนิกส์ที่มีผลเช่นเดียวกับการเก็บรักษาข้อมูลในรูปเอกสารธรรมดาจะต้องปรากฏว่าข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงและนำมาใช้ในภายหลังได้ (accessible so as to be usable for subsequent reference) หลักเกณฑ์นี้เป็นหลักเกณฑ์เดียวกับที่กำหนดไว้ในบทบัญญัติเกี่ยวกับ "หนังสือ" (Writing) นั่นเอง[18] ประการต่อไป การเก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นต้องกระทำในรูปแบบที่สามารถแสดงว่าข้อมูลอิเล็กทรอนิกส์ที่เก็บรักษานั้นมีเนื้อหาตรงกันกับข้อมูลหรือเอกสารที่ต้องเก็บรักษา ตามคำอธิบายประกอบกฎหมายแม่แบบ ข้อกำหนดที่ว่าข้อมูลอิเล็กทรอนิกส์ที่เก็บรักษานั้นต้องมีเนื้อหาตรงกัน (represent accurately) กับข้อมูลหรือเอกสารที่ต้องเก็บรักษานั้นมิได้หมายความว่าข้อมูลอิเล็กทรอนิกส์นั้นต้องไม่มีการเปลี่ยนแปลงจากรูปเดิม ทั้งนี้เพราะการเก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นมักมีการเข้ารหัสข้อมูล การบีบข้อมูล (Compression) หรือการเปลี่ยนรูปข้อมูล (Conversion) อยู่เป็นปกติ[19]

1.8 การแสดงเจตนาโดยใช้ข้อมูลอิเล็กทรอนิกส์

บทบัญญัติทั่วไปใน Article 5 ของกฎหมายแม่แบบของ UNCITRAL ที่รับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ (โดยห้ามปฏิเสธผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์เพียงเพราะเหตุที่ว่าข้อมูลนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์) ก็อาจมีความหมายครอบคลุมถึงการยอมรับให้มีการทำคำเสนอ คำสนอง หรือการแสดงเจตนาโดยใช้ข้อมูลอิเล็กทรอนิกส์ได้ อย่างไรก็

---

[17] **Article 10.** Retention of data messages

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

... ...

[18] ดู 1.3 ข้างต้น

[19] ดู Guide to Enactment, paragraph 73.

ตาม กฎหมายแม่แบบได้มีบทบัญญัติต่างหากที่กล่าวถึงการทำคำเสนอ คำสนอง หรือแสดงเจตนาโดยใช้ข้อมูลอิเล็กทรอนิกส์ ทั้งนี้ โดยบัญญัติว่าคำเสนอ คำสนองอาจแสดงโดยใช้ข้อมูลอิเล็กทรอนิกส์ได้และห้ามปฏิเสธความสมบูรณ์หรือการมีผลบังคับของสัญญาโดยยกเหตุผลเพียงว่าเป็นสัญญาที่คู่กรณีได้ทำคำเสนอหรือคำสนองโดยใช้ข้อมูลอิเล็กทรอนิกส์[20] นอกจากนี้ บทบัญญัติอีกมาตราหนึ่งยังบัญญัติต่อไปด้วยว่าคู่กรณีอาจแสดงเจตนาหรือให้คำบอกกล่าวอย่างอื่นโดยใช้ข้อมูลอิเล็กทรอนิกส์ได้โดยห้ามปฏิเสธความสมบูรณ์หรือการมีผลบังคับของการแสดงเจตนาหรือการให้คำบอกกล่าวนั้นโดยเพียงเหตุที่ว่าเป็นการแสดงเจตนาหรือการให้คำบอกกล่าวที่กระทำในรูปของข้อมูลอิเล็กทรอนิกส์[21] เหตุที่ต้องมีบทบัญญัติทั้งสองเป็นพิเศษอีกเป็นเพราะเกรงกันว่าระบบกฎหมายในบางประเทศยังไม่ยอมรับให้สัญญา "เกิด" (formed) โดยวิธีการทางอิเล็กทรอนิกส์ที่อาจไม่ต้องอาศัยการกระทำของมนุษย์ในการทำคำเสนอและคำสนองโดยตรง[22] (เช่น ในระบบ EDI เครื่องคอมพิวเตอร์จะทำคำเสนอ คำสนอง และรับหรือส่งคำเสนอ คำสนองไปยังเครื่องคอมพิวเตอร์ของอีกฝ่ายหนึ่งโดยอัตโนมัติ) ส่วนบทบัญญัติเกี่ยวกับการแสดงเจตนาโดยใช้ข้อมูลอิเล็กทรอนิกส์นั้นได้บัญญัติเพิ่มเข้ามาในภายหลังเพราะเห็นกันว่าเป็นเรื่องที่มิได้มุ่งหมายโดยตรงต่อการเกิดของสัญญา หากแต่มีความเกี่ยวข้องกับการปฏิบัติการชำระหนี้ตามสัญญา เช่น การแจ้งให้ทราบถึงความชำรุดบกพร่องของสินค้า การบอกกล่าวรับสภาพหนี้ เป็นต้น[23]

1.9 ความเป็นเจ้าของข้อมูลอิเล็กทรอนิกส์และเวลา
และสถานที่ที่ถือว่าได้ส่งและได้รับข้อมูล

การส่งและการรับข้อมูลอิเล็กทรอนิกส์มีเรื่องทางเทคนิคเข้ามาเกี่ยวข้องอย่างมาก เนื่องจากเป็นการส่งทางเครือข่าย (Network) กันเป็นส่วนใหญ่โดยผู้ส่งและผู้รับอาจมิได้ส่งและรับข้อมูลอิเล็กทรอนิกส์กันโดยตรง แต่อาจใช้บริการเครือข่ายของผู้ให้บริการเครือข่าย (เช่น Internet Service

---

[20] **Article 11. Formation and validity of contracts**

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

... ...

[21] **Article 12. Recognition by parties of data messages**

(1)As between the originator and the addressee of data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

... ...

[22] ดู Guide to Enactment, paragraph 76 - 77.

[23] ดู Guide to Enactment, paragraph 81.

Provider หรือ ISP) ซึ่งผู้ให้บริการเครือข่ายดังกล่าวก็อาจใช้บริการเครือข่ายของผู้ให้บริการเครือข่ายรายอื่นอีกต่อหนึ่ง จึงมีลักษณะเป็นเครือข่ายหลายเครือข่ายที่พ่วงกันเป็นทอดๆ ดังนั้น ข้อมูลอิเล็กทรอนิกส์ที่ส่งไปจึงมักผ่านเครือข่ายหลายทอด แต่ละทอดก็อยู่ในความดูแลของบุคคลต่างบุคคลกัน การส่งข้อมูลก็อาจกระทำโดยบุคคลอื่นที่มีรหัสผ่านของเจ้าของรหัส จึงมีปัญหาว่าจะใช้เกณฑ์ใดพิจารณาเกี่ยวกับความเป็นเจ้าของข้อมูลอิเล็กทรอนิกส์นั้นๆ (กล่าวคือ บุคคลที่ปรากฏชื่อว่าเป็นผู้ส่งข้อมูลอิเล็กทรอนิกส์เป็นผู้ส่งที่แท้จริงหรือไม่) และจะให้คู่กรณีรับเอาความเสี่ยงในความผิดพลาดของเนื้อหาของข้อมูลซึ่งอาจเกิดจากระบบคอมพิวเตอร์หรือไม่ นอกจากนี้ จะใช้หลักเกณฑ์ใดพิจารณาเวลาและสถานที่ที่ถือว่าการส่งและการรับข้อมูลอิเล็กทรอนิกส์นั้นมีผล ประเด็นเกี่ยวกับเวลาที่การส่งและการรับข้อมูลอิเล็กทรอนิกส์มีผลตามกฎหมายนั้นเป็นประเด็นที่มีความเกี่ยวข้องกับประเด็นการเกิดขึ้นของสัญญาและกฎหมายที่จะใช้บังคับกับสัญญาอีกด้วย

1.9.1 ข้อสันนิษฐานเกี่ยวกับตัวผู้ส่งข้อมูลอิเล็กทรอนิกส์

ในการส่งและรับข้อมูลอิเล็กทรอนิกส์ กฎหมายแม่แบบของ UNCITRAL กำหนดข้อสันนิษฐานบางประการเกี่ยวกับตัวผู้ส่งและผู้รับข้อมูลอิเล็กทรอนิกส์ **ประการแรก** หากผู้ส่งได้ส่งข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง กฎหมายถือว่าผู้ส่งเป็นผู้ส่งข้อมูลอิเล็กทรอนิกส์นั้น จะปฏิเสธว่าตนมิได้ส่งไม่ได้[24] **ประการที่สอง** ในระหว่างผู้ส่งและผู้รับข้อมูลอิเล็กทรอนิกส์ ถ้าข้อมูลอิเล็กทรอนิกส์ใดส่งโดยผู้มีอำนาจกระทำแทนผู้ส่งเกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้น กฎหมายก็ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นของผู้ส่งเช่นเดียวกัน[25] **ประการที่สาม** ในกรณีที่ข้อมูลอิเล็กทรอนิกส์นั้นได้ส่งไปโดยระบบคอมพิวเตอร์หรือระบบเครือข่ายเองโดยตั้งโปรแกรมให้ดำเนินการรับส่งและประมวลผลข้อมูลโดยอัตโนมัติ กฎหมายก็ถือว่าข้อมูลอิเล็กทรอนิกส์ที่ได้มีการส่งออกไปทางระบบที่ทำงานโดยอัตโนมัติดังกล่าวเป็นข้อมูลของผู้ที่ปรากฏชื่อว่าเป็นผู้ส่ง[26] ข้อสันนิษฐานในกรณีนี้มุ่งหมายจะใช้กับการติดต่อสื่อสารในระบบการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์ด้วยกันโดยใช้มาตรฐานที่ตกลงกันไว้ล่วงหน้า หรือ EDI เป็นสำคัญ ข้อสันนิษฐานในกรณีดังที่กล่าวมานี้ล้วนเป็นข้อสันนิษฐานที่เด็ดขาด[27]

---

[24] Article 13 (1)

[25] Article 13 (2) (a)

[26] Article 13 (2) (b)

[27] ในปัจจุบัน ผู้ประกอบการค้าใช้ระบบ EDI กันอย่างกว้างขวาง ในระบบนี้ คู่กรณีต้องมีระบบคอมพิวเตอร์แลกเปลี่ยนข้อมูลกัน โดยใช้ระบบการรับ ส่ง และประมวลผลข้อมูลระบบเดียวกัน เพื่อให้คอมพิวเตอร์ของทั้งสองฝ่ายสามารถติดต่อสื่อสารกันได้เองโดยอัตโนมัติโดยคู่กรณีไม่ต้องดำเนินการเอง เช่น ในกิจการห้างสรรพสินค้าซึ่งห้างสรรพสินค้าต้องสั่งซื้อสินค้าจากผู้ผลิตหรือผู้จำหน่ายอยู่ตลอดเวลานั้น พนักงานของห้างสรรพสินค้าไม่จำเป็นต้องทำคำสั่งซื้อส่งไปยังผู้จำหน่ายด้วยตนเอง แต่อาจตกลงร่วมกัน

ประการต่อมาเป็นข้อสันนิษฐานในกรณีคู่กรณีได้ตกลงกันเกี่ยวกับวิธีการในการพิสูจน์ตัวบุคคล สำหรับข้อสันนิษฐานข้อนี้ เมื่อมีการส่งข้อมูลอิเล็กทรอนิกส์ไปยังอีกฝ่ายหนึ่ง ถ้าผู้รับข้อมูลได้ใช้วิธีการตรวจสอบตัวบุคคลตามวิธีการที่ตกลงกันไว้ก่อนแล้วและผลการตรวจสอบปรากฏว่าบุคคลใดเป็นผู้ส่งข้อมูลอิเล็กทรอนิกส์ กฎหมายกำหนดข้อสันนิษฐานเป็นคุณแก่ผู้รับข้อมูลว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับนั้นเป็นข้อมูลที่ส่งโดยบุคคลนั้น ผู้ที่ระบบการตรวจสอบระบุว่าเป็นผู้ส่งข้อมูลจะอ้างว่าตนมิได้เป็นผู้ส่งข้อมูลไม่ได้[28] เหตุที่กฎหมายสันนิษฐานเป็นคุณแก่ผู้รับข้อมูลก็เป็นเพราะผู้ส่งข้อมูลได้ตกลงให้ผู้รับข้อมูลใช้ระบบการตรวจสอบเช่นนั้นเองจึงต้องผูกพันโดยระบบการตรวจสอบที่ตนได้ตกลงไว้ก่อนแล้ว คำว่า "ตกลงไว้ก่อนแล้ว" ในที่นี้ อันที่จริงแล้วกฎหมายแม่แบบของ UNCITRAL มิได้มุ่งหมายถึงกรณีที่ผู้รับและผู้ส่งได้ตกลงกันก่อนเท่านั้น แต่ยังมีเจตนารมณ์ให้หมายรวมไปถึงกรณีที่ผู้ส่งได้ตกลงไว้กับผู้อื่นซึ่งให้บริการเครือข่ายด้วย (third-party service provider)[29] อย่างไรก็ตาม แม้กฎหมายจะสันนิษฐานเป็นคุณแก่ผู้รับข้อมูล แต่กฎหมายก็เปิดโอกาสให้ผู้ที่ถูกสันนิษฐานว่าเป็นผู้ส่งข้อมูลอิเล็กทรอนิกส์นั้นบอกกล่าวให้ผู้รับข้อมูลทราบว่าตนมิได้เป็นผู้ส่งข้อมูลดังกล่าว นับตั้งแต่เวลาที่ได้รับคำบอกกล่าวดังกล่าว ผู้รับข้อมูลไม่อาจที่จะดำเนินการใดภายใต้ข้อสันนิษฐานว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นของผู้บอกกล่าวอีกต่อไป หากดำเนินการใดไปเช่นนั้นภายหลังจากที่ได้รับคำบอกกล่าว ก็จะเรียกร้องเอาจากผู้บอกกล่าวไม่ได้ แต่

กับบริษัทผู้ผลิตหรือผู้จำหน่ายสินค้านั้นเพื่อติดตั้งระบบคอมพิวเตอร์เชื่อมโยงกันเพื่อให้คอมพิวเตอร์ของทั้งสองฝ่ายสามารถตรวจสอบสินค้าคงเหลือและจัดทำ ส่งหรือรับคำสั่งซื้อหรือคำตอบรับการสั่งซื้อได้เลย ทั้งนี้ เมื่อลูกค้าของห้างฯ ซื้อสินค้าแต่ละชิ้น คอมพิวเตอร์ ณ จุดแคชเชียร์ของห้างฯ ซึ่งเชื่อมโยงกับระบบคอมพิวเตอร์หลักก็จะบันทึกข้อมูลนั้นส่งไปยังระบบคอมพิวเตอร์หลักของห้างฯเพื่อให้ระบบคอมพิวเตอร์หลักประมวลผลว่ายังคงมีสินค้าชนิดนั้นคงคลังอยู่เท่าไร และเมื่อปรากฏผลจากการประมวลผลดังกล่าวว่ามีสินค้านั้นคงคลังอยู่น้อย คอมพิวเตอร์ของห้างฯก็จะจัดทำคำสั่งซื้อและส่งคำสั่งซื้อไปยังระบบคอมพิวเตอร์ของผู้จำหน่ายโดยอัตโนมัติ ซึ่งระบบคอมพิวเตอร์ของผู้จำหน่ายได้เชื่อมโยงกับระบบคอมพิวเตอร์ของห้างฯ เมื่อได้รับคำสั่งซื้อจากคอมพิวเตอร์ของห้างฯ แล้ว คอมพิวเตอร์ของผู้จำหน่ายก็จะประมวลผลและหากมีสินค้าเพียงพอที่จะจัดส่งให้ห้างฯตามคำสั่งซื้อก็จะจัดทำและส่งคำตอบรับการสั่งซื้อไปยังผู้สั่งซื้อโดยอัตโนมัติเช่นเดียวกัน สัญญาจึงเกิดขึ้นโดยอัตโนมัติโดยผ่านระบบคอมพิวเตอร์โดยคู่สัญญาแต่ละฝ่ายไม่จำเป็นต้องติดต่อกันเองโดยตรง

[28] Article 13 (3): "As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if: (a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; ... "

[29] ดู Guide to Enactment, paragraph 86.

แม้จะได้รับคำบอกกล่าว ถ้าผู้รับข้อมูลไม่มีเวลาพอที่จะดำเนินแก้ไขความเสียหายที่ตนจะได้รับ ผู้รับข้อมูลก็ชอบที่จะกระทำการใดต่อไปโดยถือว่าข้อมูลอิเล็กทรอนิกส์ส่งโดยผู้บอกกล่าวจนกว่าจะมีเวลาพอที่จะดำเนินการแก้ไข ส่วนการดำเนินการใดไปก่อนที่ได้รับคำบอกกล่าวโดยเชื่อว่าข้อมูลนั้นได้ส่งโดยบุคคลซึ่งให้คำบอกกล่าวก็มีผลผูกพันบุคคลนั้นโดยถือว่าเป็นผู้ส่งข้อมูลอิเล็กทรอนิกส์แม้ว่าตนจะมิได้ส่งข้อมูลนั้นก็ตาม[30] อย่างไรก็ตาม ในกรณีที่ผู้รับข้อมูลอิเล็กทรอนิกส์ได้ทราบหรือมีเหตุควรได้ทราบว่าข้อมูลอิเล็กทรอนิกส์ที่ตนได้รับนั้นมิได้เป็นของบุคคลที่กฎหมายสันนิษฐานว่าเป็นเจ้าของข้อมูล โดยที่บุคคลผู้ถูกสันนิษฐานดังกล่าวมิได้เป็นผู้บอกกล่าวมายังผู้รับข้อมูล ในกรณีเช่นว่านี้ผู้รับข้อมูลก็ยังคงชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นของบุคคลที่ถูกสันนิษฐาน เหตุที่กฎหมายถือเช่นนี้ก็เป็นเพราะต้องการให้ความสำคัญต่อวิธีการตรวจสอบตัวบุคคลที่ได้ตกลงไว้นั่นเอง[31] แต่แม้กฎหมายแม่แบบจะยอมรับเช่นนั้นก็ยังมีข้อสงสัยว่าการให้ผู้รับข้อมูลอิเล็กทรอนิกส์ซึ่งได้ทราบความจริงแล้วยังคงถือว่าข้อมูลนั้นเป็นของบุคคลที่ถูกระบุว่าเป็นผู้ส่งจะเป็นการขัดต่อหลักสุจริตหรือไม่

ข้อสันนิษฐาน**ประการสุดท้าย**เกี่ยวกับการเป็นเจ้าของข้อมูลอิเล็กทรอนิกส์เป็นกรณีที่การส่งข้อมูลอิเล็กทรอนิกส์นั้นเกิดจากการกระทำของผู้ที่มีความสัมพันธ์กับบุคคลหนึ่งอยู่โดยที่เป็นความสัมพันธ์ถึงขนาดที่สามารถเข้าถึง (access) และนำวิธีการทางเทคนิคของบุคคลนั้นไปใช้ในการส่งข้อมูลอิเล็กทรอนิกส์ไปให้ผู้รับ ในกรณีเช่นว่านี้กฎหมายสันนิษฐานว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นเป็นของบุคคลดังกล่าวแม้ว่าตนจะมิได้เป็นผู้ส่งข้อมูลนั้นก็ตาม[32] เหตุที่กฎหมายสันนิษฐานเช่นนี้ก็เป็นเพราะประสงค์ให้บุคคลใช้ความระมัดระวังวิธีการรักษาความปลอดภัยของตนเอง เช่น ระมัดระวังรหัสส่วนตัวของตนเอง หากตกไปอยู่ในความครอบครองของผู้อื่นที่มีความสัมพันธ์กับตนอย่างใกล้ชิดเช่นนั้น ก็ต้องรับผิดชอบในข้อมูลอิเล็กทรอนิกส์ที่ถูกส่งออกไปแม้ว่าตนจะมิได้อนุญาตให้บุคคลอื่นนั้นนำรหัสส่วนตัวของตนไปใช้ก็ตาม[33] แต่ถ้าผู้รับข้อ

---

[30] Article 13 (4): "Paragraph (3) does not apply: (a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or ... " และดู Guide to Enactment, paragraph 85 ประกอบด้วย

[31] ดู Guide to Enactment, paragraph 89.

[32] Article 13 (3) (b): "As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if: (a) ... (b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own."

มูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับนั้นมิใช่เป็นของผู้ที่ถูกระบุว่าเป็นผู้ส่งหากได้ใช้ความระมัดระวังอันสมควร ผู้รับข้อมูลก็ไม่อาจถือได้ว่าข้อมูลนั้นเป็นของผู้ที่ถูกระบุว่าเป็นผู้ส่ง

1.9.2 เวลาที่ถือว่าได้ส่งและได้รับข้อมูล

ดังได้กล่าวแล้ว การส่งข้อมูลอิเล็กทรอนิกส์มักเป็นการส่งผ่านเครือข่ายที่เชื่อมต่อกันเป็นทอดๆ แต่ละทอดอาจอยู่ในความดูแลของบุคคลต่างบุคคลกัน จึงต้องมีหลักเกณฑ์ในการพิจารณาว่าการส่งและการรับข้อมูลอิเล็กทรอนิกส์มีผลในเวลาใด สำหรับเวลาที่ถือว่าการส่งข้อมูลอิเล็กทรอนิกส์มีผลนั้น กฎหมายแม่แบบของ UNCITRAL กำหนดให้มีผลเมื่อข้อมูลนั้นเข้าสู่ระบบข้อมูลที่อยู่นอกเหนือการควบคุมของผู้ส่งหรือของตัวแทนของผู้ส่ง (enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator) คำว่า "ระบบข้อมูล" หมายถึงระบบที่ใช้ในการสร้าง ส่ง รับ เก็บรักษา และประมวลผลข้อมูลอิเล็กทรอนิกส์ กล่าวคือ เป็นระบบคอมพิวเตอร์ที่คู่กรณีใช้นั่นเอง เช่น ระบบเครือข่ายอินเทอร์เน็ต หรือระบบการแลกเปลี่ยนข้อมูลระหว่างเครื่องคอมพิวเตอร์ที่ใช้มาตรฐานร่วมกัน (EDI) ระบบข้อมูลที่ข้อมูลที่ส่งไปจะ "เข้าสู่" นั้นอาจไม่จำเป็นต้องเป็นระบบข้อมูลของผู้รับโดยตรง แต่อาจเป็นระบบข้อมูลของผู้เป็นสื่อกลางหรือให้บริการเครือข่ายก็ได้และโดยเหตุที่เครือข่ายมักมีการเชื่อมโยงกันหลายทอด กฎหมายจึงให้การส่งข้อมูลมีผลเมื่อข้อมูลเข้าสู่เครือข่ายของบุคคลใดที่อยู่นอกเหนือการควบคุมของผู้ส่งหรือของตัวแทนของผู้ส่ง (outside the control of the originator or of the person who sent the data message on behalf of the originator) ส่วนสภาพที่ข้อมูลอิเล็กทรอนิกส์ "เข้าสู่" (enter) ระบบดังกล่าวก็คือสภาพที่ระบบดังกล่าวอยู่ในสภาพที่พร้อมที่จะประมวลผลข้อมูลนั้นนั่นเอง ดังนั้น การที่ระบบข้อมูลมีเหตุขัดข้องไม่สามารถประมวลผลข้อมูลได้ แม้ข้อมูลอิเล็กทรอนิกส์นั้นจะเข้าสู่ระบบข้อมูลนั้นแล้วก็ไม่ถือว่าได้ "เข้าสู่" จึงมีผลต่อไปว่าการส่งข้อมูลไม่เกิดขึ้นในสายตาของกฎหมาย อนึ่ง เมื่อข้อมูลอิเล็กทรอนิกส์นั้นได้ไปถึงระบบข้อมูลที่อยู่นอกเหนือการควบคุมของผู้ส่งหรือตัวแทนโดยที่ระบบข้อมูลนั้นพร้อมที่จะประมวลผลแล้ว การส่งก็มีผลโดยที่ไม่จำเป็นที่ข้อมูลนั้นต้องอยู่ในสภาพที่อ่านออกหรือไม่เพราะในความเป็นจริงอาจมีการส่งข้อมูลที่เข้ารหัสกันไว้ด้วย[34]

ส่วนเวลาที่กฎหมายถือว่าการรับข้อมูลอิเล็กทรอนิกส์นั้นมีผลนั้น ก็ใช้หลักเกณฑ์เดียวกัน กล่าวคือ หลักเกณฑ์ที่ว่าข้อมูลอิเล็กทรอนิกส์ "เข้าสู่ระบบข้อมูล" ในกรณีของการรับนั้น กฎหมายกำหนดว่าถ้าผู้รับได้กำหนดระบบข้อมูลที่ใช้รับข้อมูลไว้โดยเฉพาะ การรับข้อมูลจะมีผลเมื่อข้อมูลได้เข้าสู่ระบบข้อมูลที่กำหนดไว้ แต่หากได้ส่งข้อมูลไปยังระบบข้อมูลอื่นซึ่งมิใช่ระบบ

---

[33] ดู Guide to Enactment, paragraph 87.

[34] ดู Guide to Enactment, paras 100 - 104.

ข้อมูลที่ผู้รับข้อมูลกำหนดไว้ กฎหมายก็จะถือว่าการรับข้อมูลมีผลเมื่อผู้รับได้เรียกข้อมูลนั้นขึ้นมาให้ปรากฏแก่ผู้รับด้วย (retrieved by the addressee) แต่หากมิได้มีการกำหนดระบบข้อมูลใดไว้โดยเฉพาะ การรับข้อมูลจะมีผลตั้งแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นเข้าสู่ระบบข้อมูลของฝ่ายผู้รับข้อมูลนั้น[35]

1.9.3 สถานที่ที่ถือว่าได้ส่งและรับข้อมูลอิเล็กทรอนิกส์

การส่งและการรับข้อมูลอิเล็กทรอนิกส์มักทำกันผ่านเครือข่ายและคู่กรณีก็อาจอยู่ห่างไกลกันคนละประเทศ และระบบข้อมูลที่คู่กรณีกำหนดกันไว้เพื่อประโยชน์ในการรับส่งข้อมูลนั้นก็อาจจะมิได้อยู่ในประเทศเดียวกันกับประเทศที่คู่กรณีอยู่ จึงมีปัญหาเกี่ยวกับสถานที่ที่จะถือว่าการส่งและการรับข้อมูลอิเล็กทรอนิกส์มีผล กฎหมายแม่แบบของ UNCITRAL จึงกำหนดหลักเกณฑ์เกี่ยวกับสถานที่ที่ถือว่าการส่งและการรับข้อมูลอิเล็กทรอนิกส์มีผล ทั้งนี้ โดยถือว่าข้อมูลอิเล็กทรอนิกส์ได้ส่ง ณ สถานที่ที่ผู้ส่งข้อมูลอิเล็กทรอนิกส์ประกอบธุรกิจ และได้รับ ณ สถานที่ที่ผู้รับประกอบธุรกิจ หากคู่กรณีมีสถานที่ประกอบธุรกิจหลายแห่งก็ให้ยึดถือเอาสถานที่ที่มีความสัมพันธ์ใกล้ชิดกับธุรกรรมนั้นมากที่สุด หรือหากไม่อาจชี้ได้ว่าสถานที่ใดมีความสัมพันธ์ใกล้ชิดกับธุรกรรมนั้นมากที่สุด ก็ให้ยึดเอาสถานที่ทำการแห่งใหญ่ หากไม่มีสถานที่ทำการแห่งใหญ่ก็ให้ถือเอาถิ่นที่อยู่ปกติของคู่กรณีเป็นสำคัญ[36] ดังนั้น ในกรณีที่ผู้ประกอบการค้าในประเทศไทยซึ่งมีสถานที่ประกอบธุรกิจในเมืองไทยมีระบบ EDI กับผู้ค้าในประเทศอังกฤษซึ่งมีสถานที่ประกอบธุรกิจในนครลอนดอน การที่คอมพิวเตอร์ของผู้ประกอบการค้าในเมืองไทยส่งคำสั่งซื้อไปยัง

---

[35] Article 15 (2): "Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determinable as follows:

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

(i) at the time when the data message enters the designated information system; or

(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;

(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee."

[36] Article 15 (4): "Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;

(b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence."

คอมพิวเตอร์ของผู้ประกอบการค้าประเทศอังกฤษ ถือว่าการส่งคำสั่งซื้อมีผลในขณะที่ข้อมูลได้เข้าสู่ระบบคอมพิวเตอร์ที่อยู่นอกเหนือการควบคุมของผู้สั่งซื้อ (ในกรณีนี้คือเวลาที่คำสั่งซื้อได้เข้าสู่ระบบคอมพิวเตอร์ของฝ่ายผู้ขายในประเทศอังกฤษ) แต่ในตัวอย่างดังกล่าวนี้ ต้องถือว่าคำสั่งซื้อได้ส่งในเมืองไทยและได้รับในลอนดอน ซึ่งเป็นสถานที่ที่ผู้ส่งข้อมูลและผู้รับข้อมูลมีสถานที่ประกอบธุรกิจ หรือในกรณีที่นักธุรกิจชาวไทยส่งไปรษณีย์อิเล็กทรอนิกส์โดยใช้เครื่องคอมพิวเตอร์กระเป๋าหิ้วของตนในขณะที่พักอยู่ที่โรงแรมกลางนครเบอร์ลินระหว่างที่เดินทางไปเจรจาธุรกิจที่ประเทศเยอรมันก็ถือว่าไปรษณีย์อิเล็กทรอนิกส์นั้นได้ส่งในประเทศไทยซึ่งบุคคลดังกล่าวมีสถานประกอบธุรกิจ เป็นต้น

หลักเกณฑ์ที่ให้ถือว่าการส่งข้อมูลอิเล็กทรอนิกส์เกิดขึ้น ณ สถานที่ประกอบธุรกิจของผู้ส่งข้อมูลและการรับข้อมูลอิเล็กทรอนิกส์เกิดขึ้น ณ สถานประกอบธุรกิจของผู้รับข้อมูลนั้นก็เป็นเพราะเห็นได้ชัดว่าการส่งและการรับข้อมูลในยุคเทคโนโลยีสารสนเทศในปัจจุบันนั้นมักจะกระทำผ่านเครือข่ายซึ่งแม้ผู้ส่งและผู้รับข้อมูลจะเดินทางไปยังประเทศอื่นก็ยังสามารถเชื่อมต่อมายังเครือข่ายของตนหรือเครือข่ายของผู้ให้บริการเครือข่าย (network provider) ที่ตนใช้บริการอยู่ได้อย่างสะดวกเสมือนกับได้ส่งหรือรับข้อมูลอิเล็กทรอนิกส์ในประเทศอันเป็นที่ตั้งของสถานประกอบธุรกิจของตนเอง กฎหมายจึงมีบทบัญญัติที่ให้ถือว่าการส่งข้อมูลอิเล็กทรอนิกส์เกิดขึ้น ณ สถานประกอบธุรกิจของผู้ส่งข้อมูลและถือว่าการรับข้อมูลเกิดขึ้น ณ สถานประกอบธุรกิจของผู้รับข้อมูล โดยไม่คำนึงถึงสถานที่ที่ข้อมูลอิเล็กทรอนิกส์ได้ส่งหรือรับกันจริง ๆ อย่างไรก็ตาม หากเป็นการส่งข้อมูลโดยใช้วิธีการสื่อสารประเภทที่มิได้มีการทำงานโดยใช้ระบบคอมพิวเตอร์ (non-computerised transmission) เช่น การสื่อสารโดยทางโทรเลข หรือเทเล็กซ์ ย่อมเห็นได้ชัดว่าการส่งหรือการรับนั้นเกิดขึ้น ณ สถานที่ที่แน่นอน กล่าวคือ สถานที่ที่เครื่องส่งโทรเลขหรือเครื่องเทเล็กซ์ตั้งอยู่นั่นเอง บทบัญญัติที่ให้ถือว่าการส่งข้อมูลอิเล็กทรอนิกส์เกิดขึ้น ณ สถานที่ประกอบธุรกิจของผู้ส่งข้อมูลหรือของผู้รับข้อมูลจึงไม่ใช้กับกรณีดังกล่าว[37]

1.9.4 ความผิดพลาดและความซ้ำซ้อนของข้อมูลอิเล็กทรอนิกส์

ข้อสันนิษฐานเกี่ยวกับความเป็นเจ้าของข้อมูลนั้นมีความหมายด้วยว่านอกจากผู้รับข้อมูลมีสิทธิที่จะถือว่าบุคคลที่ถูกระบุว่าเป็นผู้ส่งข้อมูลอิเล็กทรอนิกส์นั้นเป็นผู้ส่งข้อมูล ผู้รับข้อมูลยังมีสิทธิที่จะถือว่าบุคคลนั้นได้ส่งข้อมูลดังกล่าวโดยมีเนื้อหาสาระตามที่ปรากฏ (as received) กล่าวคือ ข้อมูลนั้นไม่มีข้อผิดพลาด กล่าวอีกนัยหนึ่ง แม้ข้อมูลที่ส่งหรือถือว่าได้ส่งนั้นมีเนื้อหาที่

---

[37] ดู Guide to Enactment, para 107: "However, it was felt during the preparation of the Model Law that introducing a deemed place of receipt, as distinct from the place actually reached by that data message at the time of its receipt, would be inappropritae outside the context of computerized transmissions of data messages."

ผิดพลาด ผู้ส่งหรือผู้ถูกสันนิษฐานว่าเป็นผู้ส่งจะปฏิเสธความรับผิดโดยอ้างว่าได้มีข้อผิดพลาดในเนื้อหาของข้อมูลนั้นไม่ได้ เว้นแต่ผู้รับได้รู้ถึงความผิดพลาดนั้นหรือควรจะได้รู้ในความผิดพลาดนั้นหากได้ใช้ความระมัดระวังอันสมควร[38] นอกจากนี้ กฎหมายก็ยังให้สิทธิแก่ผู้รับข้อมูลที่จะถือว่าข้อมูลที่ได้รับแต่ละครั้งนั้นเป็นข้อมูลที่ต่างหากจากกันโดยที่ผู้ส่งมิได้ส่งซ้ำกันโดยไม่เจตนา ดังนั้น ในกรณีที่มีการกรอกใบฟอร์มในเว็บไซท์เพื่อสั่งซื้อสินค้าที่ประกาศขายทางเว็บไซท์นั้นจำนวน 10 ชิ้น หากผู้สั่งซื้อกรอกแบบฟอร์มในเว็บไซท์ดังกล่าวและได้กดคีย์หรือเมาส์เพื่อส่งคำสั่งไปยังระบบคอมพิวเตอร์ของผู้ขายแล้ว แต่ก็ยังกดคีย์หรือเมาส์เพื่อส่งคำสั่งดังกล่าวเป็นครั้งที่สองอีกเพราะเกรงว่าการส่งคำสั่งครั้งแรกอาจมีปัญหาทางเทคนิคที่ทำให้ผู้ขายไม่ได้รับข้อมูลที่ส่งไป ในกรณีเช่นว่านี้ผู้ขายก็มีสิทธิที่จะถือว่าผู้สั่งซื้อได้สั่งซื้อสินค้าจำนวน 20 ชิ้น อย่างไรก็ตาม กฎหมายกำหนดว่าหากผู้รับข้อมูลได้รู้หรือควรจะได้รู้ (หากได้ใช้ความระมัดระวังตามสมควร) ว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับเป็นข้อมูลซ้ำซ้อนที่ผู้ส่งได้ส่งออกไปโดยไม่ตั้งใจ ผู้รับข้อมูลก็ไม่อาจให้ผู้ส่งข้อมูลต้องผูกพันในข้อมูลที่ส่งซ้ำนั้น[39]

๒.๑๐ การตอบรับว่าได้รับข้อมูลอิเล็กทรอนิกส์

กฎหมายแม่แบบของ UNCITRAL ยังมีบทบัญญัติเกี่ยวกับการตอบรับว่าได้รับข้อมูลอิเล็กทรอนิกส์ (Acknowledgement of receipt of data messages) ซึ่งเป็นบทบัญญัติที่ให้สิทธิผู้ส่งข้อมูลในการกำหนดให้ผู้รับข้อมูลตอบรับ (acknowledge) ว่าได้รับข้อมูลอิเล็กทรอนิกส์ที่ผู้ส่งข้อมูลได้ส่งไปหรือไม่ ทำนองเดียวกับการที่ผู้ส่งเอกสารทางไปรษณีย์ตอบรับต้องการใบตอบรับจากพนักงานไปรษณีย์ว่าผู้รับได้รับเอกสารที่ส่งไปแล้ว การตอบรับในที่นี้มิใช่การทำคำสนอง แต่พฤติการณ์การตอบรับของผู้รับข้อมูลจะถึงขั้นที่ถือได้ว่าเป็นคำสนองหรือไม่นั้นเป็นประเด็นต่างหาก

ในบางกรณีผู้ส่งข้อมูลอาจกำหนดเป็นเงื่อนไขว่าการส่งข้อมูลอิเล็กทรอนิกส์ของตนจะมีผลก็ต่อเมื่อมีการตอบรับการได้รับข้อมูลจากผู้รับข้อมูล ในกรณีเช่นว่านี้แม้จะมีการส่งข้อมูล

---

[38] ดู Article 13 (5): "Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received."

[39] ดู Article 13 (6): "The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate."

อิเล็กทรอนิกส์ไปแล้ว แต่กฎหมายก็ถือว่าข้อมูลอิเล็กทรอนิกส์ไม่มีการส่งเลยจนกว่าผู้ส่งข้อมูลจะได้รับการตอบรับจากผู้รับข้อมูล[40] อย่างไรก็ตาม ส่วนใหญ่แล้วแม้ผู้ส่งข้อมูลกำหนดให้ผู้รับข้อมูลตอบรับการได้รับข้อมูล แต่ผู้ส่งข้อมูลก็มิได้กำหนดเงื่อนไขไว้ด้วยว่าการส่งข้อมูลอิเล็กทรอนิกส์ของตนจะมีผลก็ต่อเมื่อตนได้รับการตอบรับจากผู้รับข้อมูลเสียก่อน ในกรณีเช่นว่านี้ เมื่อผู้ส่งข้อมูลมิได้รับการตอบรับจากผู้รับข้อมูลภายในระยะเวลาที่กำหนดหรือภายในระยะเวลาอันสมควร ผู้ส่งข้อมูลอาจบอกกล่าวไปยังผู้รับข้อมูลพร้อมทั้งกำหนดเวลาให้ผู้รับข้อมูลตอบรับ หากล่วงพ้นระยะเวลาดังกล่าวไปแล้วผู้ส่งข้อมูลยังมิได้รับการตอบรับจากผู้รับข้อมูลอยู่อีก กฎหมายก็จะให้ประโยชน์แก่ผู้ส่งข้อมูลโดยให้สิทธิผู้ส่งข้อมูลที่จะถือว่าข้อมูลที่ตนได้ส่งไปแล้วนั้นไม่เคยมีการส่งไปเลย ซึ่งก็เป็นการให้สิทธิแก่ผู้ส่งข้อมูลในการปลดเปลื้องตนเองจากความผูกพันที่เกิดขึ้นจากข้อมูลที่ตนได้ส่งไปแล้วนั่นเอง โดยจะหลุดพ้นจากความผูกพันตามข้อมูลอิเล็กทรอนิกส์ที่ตนส่งไปนับแต่ระยะเวลาที่ตนได้กำหนดไว้ในคำบอกกล่าวนั้นสิ้นสุดลงและผู้ส่งข้อมูลได้แจ้งให้ผู้รับข้อมูลทราบถึงการหลุดพ้นจากความผูกพันดังกล่าว[41] จะเห็นว่าทันทีที่ผู้ส่งข้อมูลได้หลุดพ้นจากความผูกพันตามข้อมูลอิเล็กทรอนิกส์ที่ส่งไปยังผู้รับข้อมูลแล้ว ผู้ส่งข้อมูลก็สามารถที่จะทำคำเสนอไปยังบุคคลอื่นได้ จริงอยู่ว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้ส่งข้อมูลส่งไปอาจจะมิใช่เป็นคำเสนอทุกกรณีไป แต่โดยมากแล้วข้อมูลอิเล็กทรอนิกส์ที่ส่งโดยผู้ส่งข้อมูลซึ่งกำหนดให้ผู้รับต้องตอบรับการได้รับข้อมูลนั้นมักจะถึงขั้นเป็นคำเสนอแล้ว มิฉะนั้นแล้วผู้ส่งข้อมูลก็ไม่มีความจำเป็นต้องกำหนดให้มีการตอบรับเพื่อจะทราบเวลาที่แน่นอนที่ตนจะหลุดพ้นจากความผูกพันตามข้อมูลที่ส่งไป[42]

---

[40] Article 14 (3): "Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received."

[41] Article 14 (4): "Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have."

[42] ใน paragraph 96 ของ Guide to Enactment ยกตัวอย่างดังนี้ "An example of a factual situation where a provision along the lines of paragraph (4) would be particularly useful would be that the originator of an offer to contract who has not received the requested acknowledgement from the addressee of the offer may need to know the point in time after which it is free to transfer the offer to another party."

II. ลายมือชื่ออิเล็กทรอนิกส์

2.1 ลักษณะของลายมือชื่ออิเล็กทรอนิกส์

ความก้าวหน้าทางเทคโนโลยีสารสนเทศทำให้มีการใช้ลายมือชื่ออิเล็กทรอนิกส์กันมากขึ้น แม้กฎหมายจะรับรองให้ข้อมูลอิเล็กทรอนิกส์มีผลทางกฎหมายเสมอกับเอกสารธรรมดา (โดยต้องพิสูจน์ความน่าเชื่อถือของข้อมูลอิเล็กทรอนิกส์กัน ซึ่งศาลจะชั่งน้ำหนักพยานหลักฐานตามพฤติการณ์แห่งกรณี ดังได้กล่าวมาแล้วในส่วนแรกของบทความนี้) แต่ผู้ที่ทำการติดต่อสื่อสารโดยใช้ข้อมูลอิเล็กทรอนิกส์อาจใช้ลายมือชื่ออิเล็กทรอนิกส์กำกับข้อมูลอิเล็กทรอนิกส์นั้นอีกด้วยเพื่อให้ข้อมูลอิเล็กทรอนิกส์ที่ส่งกันนั้นมีความปลอดภัยยิ่งขึ้น โดยจะเป็นหลักประกันว่าบุคคลที่ใช้ลายมือชื่ออิเล็กทรอนิกส์นั้นเป็นเจ้าของลายมือชื่อนั้นและเห็นชอบกับเนื้อหาสาระของข้อมูลอิเล็กทรอนิกส์ที่มีลายมือนั้นกำกับ ลักษณะหน้าที่ดังกล่าวนี้ของลายมืออิเล็กทรอนิกส์เป็นสาระสำคัญที่กฎหมายแม่แบบกำหนดไว้ใน Article 7 นั่นเอง[43] กฎหมายของประเทศต่าง ๆ จึงมักกำหนดบทนิยามของ "ลายมือชื่ออิเล็กทรอนิกส์" ให้สอดคล้องกับสาระสำคัญของ Article 7 ของกฎหมายแม่แบบ เช่น Electronic Transactions Act 1998 ของประเทศสิงคโปร์ได้นิยามลายมือชื่ออิเล็กทรอนิกส์ว่าหมายถึง "อักษร อักขระ ตัวเลข หรือสัญลักษณ์อื่นที่อยู่ในรูปดิจิทัล ซึ่งนำมาประกอบกับหรือนำมาใช้ให้มีความสัมพันธ์เชิงตรรกะกับข้อมูลอิเล็กทรอนิกส์ และสร้างขึ้นหรือรับมาใช้เพื่อพิสูจน์ความถูกต้องแท้จริงของข้อมูลอิเล็กทรอนิกส์และความเห็นชอบกับข้อมูลอิเล็กทรอนิกส์"[44]

2.2 ลายมือชื่อดิจิทัลและเทคโนโลยีที่ใช้กุญแจสาธารณะพิสูจน์ความถูกต้อง (PKI Infrastructure)

วิธีการในการสร้างลายมืออิเล็กทรอนิกส์นั้นมีหลายวิธี ซึ่งแต่ละวิธีต้องสามารถระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่อนั้นได้และต้องประกันได้ว่าผู้เป็นเจ้าของลายมือชื่อได้เห็นชอบกับเนื้อหาของข้อมูลอิเล็กทรอนิกส์ที่ได้ใช้ลายมือชื่ออิเล็กทรอนิกส์กำกับ ตัวอย่างของวิธีการที่อาจนำมาใช้ เช่น การใช้รหัสประจำตัว (PIN) การใช้ลายพิมพ์นิ้วมือแบบดิจิทัล การสแกนม่านตาของบุคคล หรือการแปลงสัญญาณเสียงพูดเป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งคอมพิวเตอร์จะนำเอาสิ่งเหล่านั้นมาประกอบกับข้อมูลอิเล็กทรอนิกส์ที่ประสงค์จะส่งไปยังคู่กรณีอีกฝ่ายหนึ่ง ขณะนี้หลายประเทศได้มีกฎหมายว่าด้วยลายมือชื่ออิเล็กทรอนิกส์เพื่อเสริม Article 7 ของกฎหมายแม่แบบของ UNCITRAL

---

[43] ดู 1.4 ข้างต้น

[44] Article 2: "In this Act, unless the context otherwise requires –
"electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record."

บางประเทศก็ได้ออกเป็นกฎหมายฉบับเดียวกับกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions) โดยมีหมวดที่ว่าด้วยลายมือชื่ออิเล็กทรอนิกส์เป็นการเฉพาะ บางประเทศก็แยกบัญญัติเกี่ยวกับลายมืออิเล็กทรอนิกส์เป็นกฎหมายอีกฉบับหนึ่งต่างหากจากกันแต่มีความสัมพันธ์กัน และในการบัญญัติรับรองผลทางกฎหมายของลายมืออิเล็กทรอนิกส์นั้นบางบางประเทศบัญญัติรับรองเฉพาะลายมือชื่อดิจิทัลเท่านั้น[45] จึงต้องพิเคราะห์กันว่าลายมือชื่อดิจิทัลมีลักษณะอย่างไรและแตกต่างกับลายมือชื่ออิเล็กทรอนิกส์ทั่วไปหรือไม่

คำว่า "ลายมือชื่ออิเล็กทรอนิกส์" นั้นเป็นคำที่มีความหมายกว้าง ซึ่งครอบคลุมถึงลายมือชื่อที่สร้างโดยวิธีการทางอิเล็กทรอนิกส์ทุกประเภท (การสแกนม่านตา การใช้รหัสประจำตัว การแปลงสัญญาณเสียงพูดเป็นข้อมูลอิเล็กทรอนิกส์ ฯลฯ) ส่วนคำว่า "ลายมือชื่อดิจิทัล" มีความหมายอย่างแคบ ซึ่งหมายถึงลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นโดยใช้เทคโนโยลีกุญแจคู่เท่านั้น ทั้งนี้โดยอาศัยระบบการเข้ารหัสแบบอสมมาตร (asymmetric cryptosystem หรือ asymmetric cryptography) ซึ่งจะได้กล่าวต่อไป

การใช้เทคโนโลยีกุญแจคู่นั้นมีการสร้างกุญแจคู่หนึ่ง (Key Pair) ซึ่งประกอบด้วยกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) ซึ่งสร้างขึ้นโดยใช้ระบบคอมพิวเตอร์เพื่อให้กุญแจทั้งสองมีความสัมพันธ์เชิงคณิตศาสตร์ (Algorithm) ซึ่งกันและกัน การที่ต้องให้ระบบคอมพิวเตอร์สร้างกุญแจที่มีความสัมพันธ์เชิงคณิตศาสตร์ซึ่งกันและกันก็เพื่อให้ผู้ที่ประสงค์จะสร้างลายมือชื่ออิเล็กทรอนิกส์สามารถใช้กุญแจส่วนตัว***ในการสร้าง***ลายมือชื่ออิเล็กทรอนิกส์และให้บุคคลทั่วไปสามารถใช้กุญแจสาธารณะ***ในการตรวจพิสูจน์***ว่าลายมืออิเล็กทรอนิกส์ที่สร้างขึ้นนั้นเป็นลายมือชื่อที่แท้จริงหรือไม่และข้อมูลอิเล็กทรอนิกส์ที่มีการใช้ลายมืออิเล็กทรอนิกส์กำกับนั้นเป็นข้อมูลที่ถูกเปลี่ยนแปลงแก้ไขหลังจากที่มีการสร้างลายมือชื่อหรือไม่ การที่สามารถตรวจพิสูจน์เช่นว่านั้นได้ก็เป็นเพราะความสัมพันธ์เชิงคณิตศาสตร์ระหว่างกุญแจทั้งสองนั่นเอง ผู้ที่จะสร้างลายมือชื่ออิเล็กทรอนิกส์เพื่อกำกับข้อมูลอิเล็กทรอนิกส์ใดก็จะนำเอาข้อมูลอิเล็กทรอนิกส์นั้นมาเข้ารหัส (encryption) โดยใช้กุญแจส่วนตัวซึ่งไม่มีผู้ใดทราบนอกจากผู้เป็นเจ้าของกุญแจส่วนตัวเอง[46] ข้อ

---

[45] เช่น The Digital Signature Act ของมลรัฐยูท่าห์ ประเทศสหรัฐอเมริกา; The Digital Signatures Act ของประเทศเกาหลีใต้; The Digital Signatures Act 1997 ของประเทศมาเลเซีย; The Digital Signature Act ของประเทศเยอรมัน (ซึ่งปรากฏเป็น Article 3 (อันประกอบด้วยบทบัญญัติ 16 มาตรา) ของ Information and Communication Services Act 1997)

[46] อันที่จริงแล้ว ก่อนที่จะนำข้อมูลอิเล็กทรอนิกส์นั้นมาเข้ารหัสด้วยกุญแจส่วนตัวก็อาจมีการนำข้อมูลนั้นมาผ่านกระบวนการย่อยข้อมูลอีกด้วย ซึ่งมักจะทำให้ข้อมูลนั้นมีขนาดเล็กลง กระบวนการนี้เรียกว่าHash Function กฎหมายของบางประเทศกำหนดให้มีการใช้ Hash Function อีกด้วย เช่น Electronic

มูลอิเล็กทรอนิกส์ที่เข้าถูกเข้ารหัสแล้วจะเรียกว่า ciphertext ส่วนนี้เองที่เป็นลายมือชื่ออิเล็กทรอนิกส์และเป็นส่วนที่นำไปใช้กำกับกับข้อมูลอิเล็กทรอนิกส์เดิม[47] เมื่อมีการส่งข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่ออิเล็กทรอนิกส์นั้นกำกับอยู่ไปยังผู้รับ ผู้รับก็สามารถใช้กุญแจสาธารณะที่เจ้าของลายมือชื่อเผยแพร่ให้บุคคลทั่วไปทราบนั้นมาตรวจสอบลายมือชื่อดังกล่าว กุญแจสาธารณะจะถอดรหัส (decryption) ของข้อมูลที่ได้เข้ารหัสไว้ด้วยกุญแจส่วนตัว เนื่องจากกุญแจสาธารณะมีความสัมพันธ์ทางคณิตศาสตร์กับกุญแจส่วนตัว ดังนั้น ข้อมูลอิเล็กทรอนิกส์ที่ได้รับหลังจากการถอดรหัสด้วยกุญแจสาธารณะจึงต้องตรงกัน และดังที่ได้กล่าวมาแล้ว ข้อมูลอิเล็กทรอนิกส์ที่นำมาเข้ารหัสด้วยกุญแจส่วนตัวเพื่อเป็นลายมือชื่ออิเล็กทรอนิกส์นั้นก็คือข้อมูลเดิมที่ประสงค์จะนำลายมือชื่ออิเล็กทรอนิกส์นั้นไปกำกับอยู่นั่นเอง ด้วยเหตุนี้ หากมีการเปลี่ยนแปลงเนื้อหาสาระของข้อมูลอิเล็กทรอนิกส์นี้หลังจากที่ได้ส่งข้อมูลนี้ไปแล้ว เมื่อนำกุญแจสาธารณะมาถอดรหัสกลับเป็นข้อมูลหรือข้อความเดิม ก็จะได้ข้อมูลหรือข้อความที่ไม่เหมือนกัน จึงสามารถทราบได้ว่าข้อมูลอิเล็กทรอนิกส์มีการเปลี่ยนแปลงแก้ไขจากเดิม เทคโนโลยีที่มีการใช้กุญแจสาธารณะตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ที่สร้างโดยอาศัยการนำกุญแจส่วนตัวมาเข้ารหัสนั้นเรียกว่า "เทคโนโลยีกุญแจสาธารณะ" หรือ Public Key Infrastructure หรือเรียกย่อว่า เทคโนโลยี PKI (บางครั้งก็เรียกกันว่า Public Key Cryptography หรือ PKC) และลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นโดยเทคโนโลยีนี้จะเรียกกันว่า **"ลายมือชื่อดิจิทัล"** [48]

2.3 การรับรองลายมือชื่อดิจิทัล

การใช้กุญแจสาธารณะเพื่อตรวจสอบความถูกต้องแท้จริงของลายมือชื่อดิจิทัลจะไม่เป็นที่น่าเชื่อถือแก่บุคคลทั่วไปถ้าหากไม่มีการรับรองโดยบุคคลที่สามที่น่าเชื่อถือได้ (Trusted Third Party) ทั้งนี้

Transactions Act 1998 ของประเทศสิงคโปร์ และ Digital Signature Act 1997 ของประเทศมาเลเซีย

[47] ลายมือชื่ออิเล็กทรอนิกส์มีลักษณะดังตัวอย่างข้างล่างนี้

82:03:9f:35:5a:f6:d5:d6:70:04:74:55:22:f5:d2:42:6f:7e:87:b9:3b:
59:33:68:19:21:85:ab:cb:a2:77:8e:97:f0:2e:52:28:8a:ed:fe:30:91:
52:11:9f:4b:1e:10:d5:96:2e:9f:17:48:3b:62:6b:b6:53:31:3b:a1:e6:
f5:a3:fa:80:bf:01:5c:42:4a:de:bf:b3:12:2f:8b:c0:63:80:13:89:54:
ae:52:b8:0b:f4:86:5d:09:43:bd:39:35:63:60:35:7e:c3:83:20:26:1e:
ac:af:6c:da:98:69:13:31:ba:7b:01:f9:59:57:71:27:1b:59:8a:16:1c:
09:24

(ที่มา: หนังสือเผยแพร่ร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. .... ของสำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ศูนย์เทคโนโลยี อิเล็กทรอนิกส์ และคอมพิวเตอร์แห่งชาติ, 2543)

[48] ดูภาพประกอบที่ 1 และ 2 ในภาคผนวก

ถ้าไม่มีบุคคลที่สามเป็นผู้รับรองความถูกต้องของกระบวนการสร้างกุญแจคู่แล้ว ก็เท่ากับว่าผู้ที่ประสงค์จะใช้ลายมือชื่อดิจิทัลเป็นผู้รับรองตนเอง บุคคลที่สามที่น่าเชื่อถือได้ที่ทำหน้าที่ในการรับรองเกี่ยวกับลายมือชื่อดิจิทัลนั้นจะเรียกกันว่า Certification Authority หรือ CA (ซึ่งในที่นี้จะเรียกว่า "ผู้ประกอบการรับรอง") ในการรับรอง ผู้ประกอบการรับรองจะออกใบรับรองให้ผู้ขอ

ในหลายประเทศกำหนดให้ผู้ประกอบการรับรองต้องได้รับอนุญาตให้ประกอบการ โดยหน่วยงานของรัฐจะเป็นผู้ออกใบอนุญาต ซึ่งโดยปกติแล้วผู้ประกอบการรับรองจะต้องอยู่ภายใต้การกำกับดูแลของรัฐ โดยรัฐอาจกำหนดหลักเกณฑ์ต่างๆ ให้ผู้ประกอบการรับรองปฏิบัติ เช่นหลักเกณฑ์เกี่ยวกับวิธีการที่นำมาใช้สร้างกุญแจส่วนตัวและกุญแจสาธารณะ โดยต้องเป็นวิธีการที่มีความปลอดภัยเหมาะสมกับความก้าวหน้าทางเทคโนโลยีและสภาพทางธุรกิจ หรือหลักเกณฑ์ว่าด้วยการจัดทำข้อปฏิบัติเกี่ยวกับการประกอบการรับรอง (ที่เรียกกันว่า Certification Practice Statements หรือ CPS) ในขณะที่บางประเทศก็มิได้ควบคุมการประกอบการรับรองเกี่ยวกับลายมือชื่อดิจิทัลและถือว่าเป็นเรื่องที่ต้องปล่อยให้เป็นไปตามกลไกของตลาด

สิ่งสำคัญประการแรกที่ผู้ประกอบการรับรองต้องกระทำเพื่อให้ลายมือชื่อดิจิทัลของผู้ขอใบรับรองมีความน่าเชื่อถือก็คือการพิสูจน์ตัวบุคคลของผู้ขอใบรับรอง (ซึ่งมักเรียกกันว่า Subscriber) ในการนี้ ผู้ประกอบการรับรองต้องตรวจสอบให้เป็นที่แน่ชัดว่าบุคคลนั้นมีตัวตนจริงและไม่ได้นำชื่อของบุคคลอื่นไปแอบอ้างใช้โดยไม่ได้รับอนุญาต เมื่อตรวจสอบตัวบุคคลแล้วก็ต้องตรวจสอบความปลอดภัยและความถูกต้องของกุญแจส่วนตัวและกุญแจสาธารณะ ทั้งนี้ ต้องแน่ใจว่าผู้ที่จะได้รับใบรับรองต้องใช้วิธีการที่น่าเชื่อถือได้ในการสร้างกุญแจคู่ ผู้ประกอบการรับรองบางรายก็กำหนดให้ต้องใช้โปรแกรมคอมพิวเตอร์ของผู้ประกอบการรับรองในการสร้างกุญแจคู่และในการเข้ารหัสข้อมูล แต่ผู้ประกอบการรับรองบางรายก็อาจเปิดโอกาสให้ผู้ขอใบรับรองใช้โปรแกรมของผู้ขอใบรับรองได้ โดยอาจวางข้อกำหนดว่าโปรแกรมนั้นต้องมีลักษณะทางเทคนิคบางประการ (กฎหมายของบางประเทศอาจกำหนดให้ต้องใช้วิธีการหรือเทคโนโลยีที่รัฐกำหนดโดยอาจออกข้อบังคับหรือกฎหมายลำดับรองมากำหนดรายละเอียดอีกทีหนึ่ง) เมื่อออกใบรับรองให้แก่ผู้ขอใบรับรอง ผู้ประกอบการรับรองจะระบุรายละเอียดดังต่อไปนี้ไว้ในใบรับรอง กล่าวคือ ข้อเท็จจริงเกี่ยวกับตัวบุคคลของผู้ได้รับการรับรอง วิธีการทางเทคนิคที่ใช้ในการสร้างกุญแจคู่หรือมาตรฐานที่นำมาใช้ในการเข้ารหัส และกุญแจสาธารณะของผู้ถือใบรับรอง นอกจากข้อเท็จจริงเกี่ยวกับผู้ถือใบรับรองแล้ว ใบรับรองยังระบุรายละเอียดเกี่ยวกับผู้ประกอบการรับรองอีกด้วย ซึ่งนอกจากระบุชื่อและสถานที่ทำการของผู้ประกอบการรับรองแล้วยังต้องระบุกุญแจสาธารณะและลายมือชื่อดิจิทัลของ

ตนเองอีกด้วย เพราะผู้ประกอบการรับรองต้องลงลายมือชื่อดิจิทัลในใบรับรองที่ออกให้แก่ผู้ขอใบรับรองจากตนด้วย[49]

2.4 ผลของการใช้ลายมือชื่ออิเล็กทรอนิกส์และลายมือชื่อดิจิทัล

การใช้ลายมือชื่ออิเล็กทรอนิกส์ทั่วๆ ไป (กล่าวคือ ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นโดยใช้วิธีการที่สามารถระบุตัวบุคคลผู้สร้างลายมือชื่อได้และสามารถแสดงได้ว่าบุคคลนั้นเห็นชอบกับเนื้อหาสาระของข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อนั้นกำกับอยู่นั้น) ก็ได้รับการรับรองให้มีผลทางกฎหมายเช่นเดียวกับลายมือชื่อธรรมดาที่ลงกันในเอกสารอยู่แล้ว ส่วนความถูกต้องแท้จริงกันนั้นเป็นเรื่องที่ต้องพิสูจน์กันในภายหลัง ซึ่งจะต้องมีการสืบพยานและศาลจะเป็นผู้ชั่งน้ำหนักพยานเอง อย่างไรก็ตาม ถ้าหากได้มีการใช้ลายมือชื่ออิเล็กทรอนิกส์ที่อยู่ในรูปของ**ลายมือชื่อดิจิทัล** กฎหมายของหลายประเทศมักจะรับรองผลมากกว่าลายมือชื่ออิเล็กทรอนิกส์ทั่วๆไป โดยจะถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัย ซึ่งจะได้รับประโยชน์ในแง่ข้อสันนิษฐานทางกฎหมาย ดังจะกล่าวต่อไป

ในกฎหมายต่างประเทศนั้น คำว่า **"ลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัย"** (Secure electronic signature) จะหมายถึงลายมือชื่อที่สร้างขึ้นโดยวิธีการที่มีลักษณะเฉพาะตัวของบุคคลผู้สร้างลายมือชื่อ (unique to that person) และวิธีการดังกล่าวจะอยู่ภายใต้การควบคุมของบุคคลนั้นโดยเฉพาะ (under the sole control of that person)[50] เมื่อวิธีการที่นำมาใช้นั้นมีลักษณะเฉพาะของบุคคลที่ประสงค์จะสร้างลายมือชื่อและเป็นวิธีการที่ไม่มีผู้ใดนอกจากบุคคลนั้นเองควบคุมการสร้างลายมือชื่อนั้นก็ย่อมเป็นที่แน่ชัดว่าลายมือชื่อนั้นเป็นของบุคคลนั้น กฎหมายจึงสร้าง**ข้อสันนิษฐาน**ว่าลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัยเป็นของบุคคลนั้นและข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อแบบปลอดภัยดังกล่าวกำกับอยู่นั้นได้รับความเห็นชอบโดยบุคคลนั้น (กล่าวคือ มิได้มีการเปลี่ยนแปลงแก้ไขเลย)[51] ผลของข้อสันนิษฐานดังกล่าวทำให้ผู้ที่ยืนยันในความถูกต้องแท้จริงของลายมือชื่อนั้นและของข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อนั้นกำกับอยู่ไม่ต้องมีหน้าที่พิสูจน์ แต่บุคคลที่จะโต้แย้งว่าลายมือชื่อหรือข้อมูลนั้นไม่ถูกต้องมีหน้าที่ต้องพิสูจน์ ซึ่งกรณีที่มีการโต้แย้งนั้นอาจมีทั้งกรณีที่

---

[49] ตัวอย่างของใบรับรอง ดูภาคผนวก

[50] ดู Section 17 ของ Electronic Transactions Act 1998 ของประเทศสิงคโปร์ และ Section 10-110 ของ Electronic Commerce Security Act 1999 ของมลรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา เป็นต้น

[51] ดู Section 18 (2) ของ Electronic Transactions Act 1998 ของประเทศสิงคโปร์ และ Section 10-120 ของ Electronic Commerce Security Act 1999 ของมลรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา เป็นต้น

บุคคลที่ถูกสันนิษฐานว่าเป็นเจ้าของลายมือชื่อโต้แย้งว่าตนมิได้สร้างลายมือชื่อนั้นหรือโต้แย้งว่าข้อมูลอิเล็กทรอนิกส์ที่ตนใช้ลายมือชื่อกำกับนั้นถูกเปลี่ยนแปลงแก้ไข และกรณีที่บุคคลอื่นซึ่งไม่ประสงค์จะถูกผูกพันโดยนิติกรรมโต้แย้งเพื่อให้หลุดพ้นจากความรับผิดที่มิฉะนั้นแล้วตนจะมีต่อผู้ที่ได้รับการสันนิษฐานว่าเป็นเจ้าของลายมือชื่อทั้งหมดหรือบางส่วน ในการกำหนดข้อสันนิษฐานเกี่ยวกับลายมือชื่ออิเล็กเล็กทรอนิกส์แบบปลอดภัยนั้น กฎหมายแต่ละประเทศอาจวางข้อกำหนดไว้ต่างกันบ้าง ซึ่งก็เป็นข้อกำหนดเกี่ยวกับวิธีการเพื่อความปลอดภัย (Security Procedure) ที่นำมาใช้ บางประเทศกำหนดว่าวิธีการเพื่อความปลอดภัยจะต้องเป็นวิธีการที่กฎหมายกำหนดหรือที่มีความเหมาะสมในทางธุรกิจตามที่คู่กรณีตกลงกัน[52] (ซึ่งอาจกำหนดหลักเกณฑ์ในการพิเคราะห์ความเหมาะสมในทางธุรกิจไว้ด้วยว่าให้คำนึงถึงวัตถุประสงค์ของวิธีการรักษาความปลอดภัยที่นำมาใช้ ตลอดจนพฤติการณ์ทางธุรกิจ ซึ่งรวมถึง พฤติการณ์ดังต่อไปนี้ คือ ลักษณะของธุรกรรม ลักษณะและสภาพของคู่กรณี จำนวนของธุรกรรมทำนองเดียวกัน วิธีการอื่นที่ใช้รักษาความปลอดภัยมีอยู่หรือไม่ และจำนวนค่าใช้จ่ายหากนำวิธีการอื่นมาใช้ ตลอดจนวิธีการรักษาความปลอดภัยที่ใช้ในธุรกรรมทำนองเดียวกัน)[53] บางประเทศก็กำหนดถึงขนาดที่ว่าวิธีการรักษาความปลอดภัยต้องเป็นวิธีการที่ได้รับการรับรองจากเจ้าหน้าที่หรือองค์กรของรัฐเท่านั้น[54]

สำหรับลายมือชื่อดิจิทัลนั้น โดยเหตุที่ลายมือชื่อดิจิทัลเป็นลายมือชื่อที่สร้างขึ้นโดยใช้เทคโนโลยีแบบ PKI ซึ่งได้รับการยอมรับกันเป็นการสากลว่าเป็นเทคโนโลยีที่มีความปลอดภัยสูง *ดังนั้น กฎหมายจึงถือว่าลายมือชื่อดิจิทัลเป็นลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัย ซึ่งเมื่อถือว่าเป็นลายมือชื่อิเล็กทรอนิกส์แบบปลอดภัยแล้วก็จะทำให้ข้อสันนิษฐานเกี่ยวกับความถูกต้องแท้จริงใช้บังคับทันที* อย่างไรก็ตาม โดยทั่วไปแล้ว กฎหมายของประเทศต่างๆได้กำหนดให้ลายมือชื่อดิจิทัลได้รับประโยชน์จากข้อสันนิษฐานเช่นว่านั้นก็เฉพาะเมื่อได้รับการรับรองโดยผู้ประกอบการรับรองเท่านั้น ซึ่งส่วนใหญ่จะกำหนดด้วยว่าต้องได้รับการรับรองโดยผู้ประกอบการรับรองที่ได้รับอนุญาตเท่านั้น (Licensed certification authority)[55] และกฎหมายอาจให้อำนาจรัฐมนตรีออกระเบียบกำหนดหลักเกณฑ์เพิ่มเติมด้วยว่าลายมือชื่อดิจิทัลที่จะถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัยต้องมีลักษณะใดบ้าง[56]

2.5 ความเชื่อถือในลายมือชื่อดิจิทัลและหน้าที่และความรับผิดของบุคคลที่เกี่ยวข้อง

2.5.1 เหตุแห่งความเชื่อถือ

---

[52] ดู Section 17 ของ Electronic Transactions Act 1998 ของประเทศสิงคโปร์ เป็นต้น

[53] ดู Section 16 (2) ของ Electronic Transactions Act 1998 ของประเทศสิงคโปร์ เป็นต้น

[54] ดู Electronic Commerce Security Act 1999 ของมลรัฐอิลลินอย์ ประเทศสหรัฐอเมริกา เป็นต้น

[55] ดู Section 20 ของ Electronic Transactions Act 1998 ของประเทศสิงคโปร์ เป็นต้น

[56] ดู Section 42 ของ Electronic Transactions Act 1998 ของประเทศสิงคโปร์ เป็นต้น

การสร้างระบบการรับรอง (Certification) เกี่ยวกับลายมือชื่อดิจิทัลก็เพื่อให้ผู้ที่ทำการติดต่อกับผู้ที่ได้รับการระบุชื่อในใบรับรองว่าเป็นเจ้าของลายมือชื่อนั้นมีความมั่นใจในความถูกต้องแท้จริงของลายมือชื่อนั้นและของข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อนั้นกำกับ การที่จะเชื่อถือในความถูกต้องแท้จริงของสิ่งดังกล่าวได้ บุคคลที่เข้าติดต่อก็ต้องเชื่อถือในรายการต่างๆ ที่ระบุไว้ในใบรับรอง โดยจะเชื่อถือว่าผู้ประกอบการรับรองได้ตรวจสอบรายการเหล่านั้นมาอย่างถูกต้องแล้ว โดยเฉพาะอย่างยิ่ง การตรวจสอบตัวบุคคลและกุญแจคู่ของผู้ถือใบรับรอง

2.5.2 หน้าที่ของผู้ประกอบการรับรองและผู้ขอหรือผู้ถือใบรับรอง

เพื่อเป็นหลักประกันว่าข้อมูลที่ระบุในใบรับรองจะเป็นข้อมูลที่ถูกต้อง กฎหมายว่าด้วยลายมือชื่อดิจิทัลของประเทศต่างๆ จึงมักกำหนดหน้าที่สำคัญๆ ของผู้ประกอบการรับรองและของผู้ขอหรือผู้ถือใบรับรองไว้ โดยในส่วนของผู้ประกอบการรับรองนั้น กฎหมายกำหนดให้ใช้ระบบที่น่าเชื่อถือได้ (Trustworthy system) ในการประกอบการรับรองและตรวจสอบข้อเท็จจริงเกี่ยวกับผู้ขอใบรับรอง (ทั้งข้อเท็จจริงเกี่ยวกับตัวบุคคลของผู้ขอใบรับรอง ข้อเท็จจริงเกี่ยวกับกุญแจของผู้ขอใบรับรอง และข้อเท็จจริงอื่นๆ) นอกจากนี้ ในกรณีที่มีการระงับหรือเพิกถอนใบรับรองที่ผู้ประกอบการรับรองออกให้แก่บุคคลใดไปแล้วนั้นหรือมีข้อเท็จจริงอันเป็นสาระสำคัญที่มีผลกระทบต่อความน่าเชื่อถือของใบรับรอง (เช่น มีการปลอมแปลงกุญแจส่วนตัว หรือมีการเปลี่ยนแปลงรายการในใบรับรองโดยไม่ได้รับอนุญาตจากผู้ประกอบการรับรอง) ผู้ประกอบการรับรองก็ต้องแจ้งให้สาธารณชนทราบด้วย โดยต้องมีระบบการแจ้ง (repository) ที่มีประสิทธิภาพและทันกาล นอกจากนั้น หากตนทราบว่าเหตุเช่นว่านั้นจะมีผลกระทบต่อบุคคลใดเป็นการเฉพาะก็ต้องแจ้งให้บุคคลนั้นทราบด้วย[57] ซึ่งโดยปกติแล้วผู้ประกอบการรับรองมักจะมีข้อปฏิบัติในการประกอบการรับรอง (CPS) เกี่ยวกับเรื่องเหล่านี้อยู่แล้ว ส่วนผู้ขอหรือผู้ถือใบรับรองนั้น นอกจากต้องใช้วิธีการที่น่าเชื่อถือในการสร้างกุญแจส่วนตัว (ดังกล่าวใน 2.3) กฎหมายยังกำหนดให้ต้องใช้ความระมัดระวังในการรักษากุญแจส่วนตัวและไม่เปิดเผยกุญแจส่วนตัวให้ผู้ซึ่งมิได้รับอนุญาตทราบ[58] ตลอดจนหน้าที่ที่จะต้องแจ้งให้ผู้ที่เกี่ยวข้องหรือผู้ที่อาจได้รับความเสียหายทราบในกรณีรู้หรือสงสัยว่ามีการปลอมแปลงเกิดขึ้น

2.5.3 คำรับรองตามกฎหมาย (Representations)

นอกจากกฎหมายจะกำหนดหน้าที่ที่ผู้ประกอบการรับรองและผู้ขอหรือผู้ถือใบรับรองต้องปฏิบัติแล้ว กฎหมายมักจะมีระบบ "คำรับรอง" (Representations) ทั้งในส่วนของผู้ประกอบ

---

[57] ดู Section 27; Section 28 (2) และ Section 29 (2) ของ Electronic Transactions Act 1998 ของประเทศสิงคโปร์ เป็นต้น

[58] ดู Section 36 และ Section 39 ของ Electronic Transactions Act 1998 ของประเทศสิงคโปร์ เป็นต้น

การรับรองและผู้ขอหรือผู้ถือใบรับรอง การให้คำรับรองข้อเท็จจริงต่างๆ ทำให้บุคคลทั่วไปเชื่อถือในความถูกต้องแท้จริงของลายมือชื่อดิจิทัลและของข้อมูลอิเล็กทรอนิกส์ที่มีการใช้ลายมือชื่อดิจิทัลกำกับ สำหรับผู้ประกอบการรับรองนั้นกฎหมายมักกำหนดว่าการที่ผู้ประกอบการรับรองออกใบรับรองให้ผู้ใดถือว่าผู้ประกอบการรับรองได้ให้คำรับรองว่าผู้นั้นได้ยอมรับ (accept) ใบรับรองแล้วและได้ถือกุญแจส่วนตัวโดยชอบซึ่งสามารถใช้กุญแจสาธารณะตรวจสอบความถูกต้องแท้จริงของลายมือชื่อดิจิทัลและของข้อมูลอิเล็กทรอนิกส์ได้ นอกจากนี้ กฎหมายยังถือว่าผู้ประกอบการรับรองได้รับรองว่าข้อมูลที่ระบุในใบรับรองเป็นข้อมูลที่ถูกต้องโดยผู้ประกอบการรับรองมิได้รู้ถึงข้อเท็จจริงอันเป็นสาระสำคัญซึ่งอาจมีผลกระทบต่อความน่าเชื่อถือของใบรับรอง[59] ในด้านผู้ขอหรือผู้ถือใบรับรองนั้น กฎหมายถือว่าผู้ขอหรือผู้ถือใบรับรองได้รับรองว่าข้อมูลอันเป็นสาระสำคัญที่ได้ให้ไว้แก่ผู้ประกอบการรับรองเป็นจริงและตนเป็นผู้ถือกุญแจส่วนตัวโดยชอบ[60]

2.5.4 ความสมเหตุสมผลของการเชื่อถือในความถูกต้องแท้จริง

แม้กฎหมายจะกำหนดหน้าที่ให้ทั้งผู้ประกอบการรับรองและผู้ขอหรือผู้ถือใบรับรองปฏิบัติเพื่อให้ใบรับรองมีความน่าเชื่อถือและเพื่อให้บุคคลทั่วไปเชื่อมั่นว่าข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อดิจิทัลกำกับนั้นเป็นข้อมูลอิเล็กทรอนิกส์ที่ถูกต้อง แต่กฎหมายก็ไม่ประสงค์ให้ผู้ที่เชื่อถือในความถูกต้องแท้จริงนั้นเชื่อถือโดยปราศจากเหตุผลอันสมควร ดังนั้น หากมีพฤติการณ์ที่เห็นได้ว่าบุคคลไม่ควรเชื่อถือว่าใบรับรองหรือข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อดิจิทัลกำกับนั้นถูกต้องแท้จริง บุคคลที่ดำเนินการใดไปโดยเชื่อถือในใบรับรองหรือในข้อมูลอิเล็กทรอนิกส์นั้นก็ไม่อาจเรียกร้องค่าเสียหายอันเกิดจากความเชื่อถืออันไม่สมเหตุสมผลนั้น พฤติการณ์ที่แสดงว่าบุคคลไม่ควรจะเชื่อถือในความถูกต้องแท้จริงนั้นต้องพิเคราะห์กันเป็นกรณีๆ ไป โดยปกติแล้วต้องคำนึงถึงสิ่งดังต่อไปนี้ด้วย คือ ต้องพิเคราะห์ว่าบุคคลที่เชื่อถือในใบรับรองหรือในข้อมูลอิเล็กทรอนิกส์ได้รู้ถึงข้อเท็จจริงในใบรับรองหรือไม่ มูลค่าหรือความสำคัญของข้อมูลอิเล็กทรอนิกส์ที่มีการใช้ลายมือชื่อดิจิทัล ทางปฏิบัติระหว่างคู่กรณีและทางปฏิบัติทางการค้า เป็นต้น[61]

2.5.5 ความรับผิดของผู้ประกอบการรับรองและของผู้ขอหรือผู้ถือลายมือชื่อ

การที่กฎหมายกำหนดหน้าที่ของผู้ประกอบการรับรองและของผู้ขอหรือผู้ถือใบรับรองมีผลให้บุคคลดังกล่าวต้องรับผิดต่อผู้ที่ได้รับความเสียหายจากการกระทำผิดหน้าที่ที่กฎหมายกำหนดนั่นเอง เช่น ในกรณีที่ผู้ขอใบรับรองใช้ชื่อปลอมในการขอใบรับรองและผู้

---

[59] ดู Section 30 ของ Electronic Transactions Act 1998 ของประเทศสิงคโปร์ เป็นต้น

[60] ดู Section 37 และ Section 38 ของ Electronic Transactions Act 1998 ของประเทศสิงคโปร์ เป็นต้น

[61] ดู Section 22 ของ Electronic Transactions Act 1998 ของประเทศสิงคโปร์ เป็นต้น

ประกอบการรับรองมิได้ใช้ความระมัดระวังอันสมควรในการตรวจสอบตัวบุคคล (Identity) ของผู้ขอใบรับรองจึงออกใบรับรองให้แก่ผู้ขอใบรับรองที่ใช้ชื่อปลอมนั้น ในกรณีดังว่านี้ผู้ประกอบการรับรองจะต้องรับผิดต่อผู้ที่เชื่อถือในใบรับรองนั้น (เว้นแต่จะมีพฤติการณ์ที่แสดงว่าไม่สมควรจะเชื่อถือ ดังกล่าวข้างต้น) ในทำนองเดียวกัน การที่กฎหมายกำหนดคำรับรอง (Representations) ของผู้ประกอบการรับรองและของผู้ถือใบรับรองไว้ก็มีผลให้บุคคลดังกล่าวต้องรับผิดต่อผู้ที่ได้รับความเสียหายจากการที่ข้อเท็จจริงที่ได้ให้คำรับรองนั้นเป็นเท็จ อย่างไรก็ตาม บางประเทศยอมให้ผู้ประกอบการรับรองจำกัดความรับผิดได้ โดยต้องระบุระดับของความรับผิดไว้ในใบรับรอง ซึ่งเมื่อบุคคลทั่วไปได้เห็นระดับของความรับผิดที่ระบุไว้ในใบรับรองแล้วก็จะสามารถตัดสินใจได้ว่าตนควรจะให้ความเชื่อถือในใบรับรองหรือในข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อดิจิทัลกำกับมากเพียงไร

2.6 ร่างกฎหมายแม่แบบของ UNCITRAL

หลังจากที่ UNCITRAL ได้ตรากฎหมายแม่แบบว่าด้วยพาณิชย์อิเล็กทรอนิกส์แล้ว ก็ยังพยายามที่จะตรากฎหมายลักษณะเดียวกันว่าด้วยลายมือชื่ออิเล็กทรอนิกส์อีกด้วย โดยได้ยกร่างขึ้นเป็น Draft Model Law on Electronic Signatures ซึ่งมุ่งหมายให้เป็นกฎหมายที่เสริมและขยายความ Article 7 ของกฎหมายแม่แบบว่าด้วยพาณิชย์อิเล็กทรอนิกส์ ในการนี้ UNCITRAL ได้แต่งตั้งคณะทำงาน (Working Group) เพื่อดำเนินการในเรื่องนี้ นับจนถึงขณะนี้ (พฤศจิกายน 2543) คณะทำงานได้จัดประชุมเพื่อพิจารณาร่างกฎหมายนี้ไปแล้ว 6 ครั้ง ที่นครเวียนนาและนครนิวยอร์ค ร่างกฎหมายแม่แบบดังกล่าวมุ่งหมายใช้บังคับกับลายมือชื่ออิเล็กทรอนิกส์ทุกประเภทโดยมิได้จำกัดอยู่เพียงลายมือดิจิทัลเท่านั้น ในระยะแรก ร่างกฎหมายนี้มีชื่อเรียกว่า Draft Uniform Rules on Electronic Signatures แต่ในการประชุมของคณะทำงานครั้งที่ 6 ที่นครเวียนนาในระหว่างวันที่ 18 - 29 กันยายน 2543 ที่ผ่านมา คณะทำงานได้พิจารณาข้อความ (Text) ของบทบัญญัติมาตราต่าง ๆ จนเสร็จสิ้น (Final) และได้มีการเปลี่ยนชื่อร่างกฎหมายนี้จาก Draft Uniform Rules เป็น Draft Model Law คณะทำงานกำหนดจัดให้มีประชุมอีกครั้งในเดือนกุมภาพันธ์ 2544เพื่อพิจารณาคำอธิบายประกอบร่างกฎหมายแม่แบบนี้ (Guide to Enactment) ***โดยจะไม่มีการทบทวนข้อความในบทบัญญัติต่างๆ อีกแล้ว***[62]

ในการร่างกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์**ในระยะแรกๆ** บทบัญญัติหลายมาตราก็ได้ยกร่างขึ้นโดยมุ่งเน้นที่ลายมือชื่อประเภทที่สร้างขึ้นโดยใช้วิธีการที่มีความเชื่อมโยงกับบุคคลเป็นการเฉพาะ ซึ่งก็มีความหมายทำนองเดียวกับลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัย (Secure electronic signatures) ดังที่ปรากฏในกฎหมายของหลายประเทศนั่นเอง แต่ร่างกฎหมายแม่

[62] สำหรับข้อความ (Text) ของบทบัญญัติของ UNCITRAL Draft Model Law on Electronic Commerce ดูเอกสาร A/CN.9/483, 6 October 2000 ของ UNCITRAL)

แบบของ UNCITRAL จะใช้คำว่า enhanced electronic signatures[63] (ซึ่งลายมือชื่อดิจิทัลที่สร้างโดยใช้เทคโนโลยีแบบ PKI ก็จัดได้ว่าเป็น enhanced electronic signature) ทั้งนี้ ร่างกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ของ UNCITRAL ได้บัญญัติเกี่ยวกับหน้าที่ของเจ้าของลายมือชื่อ หน้าที่ของผู้ประกอบการรับรอง การเชื่อถือในลายมือชื่ออิเล็กทรอนิกส์ การเชื่อถือในใบรับรอง ฯลฯ ด้วย ประเทศส่วนใหญ่เห็นว่าบทบัญญัติที่เกี่ยวข้องกับการรับรองน่าจะใช้กับลายมือชื่อประเภทที่เป็น enhanced electronic signatures เท่านั้น อันที่จริงแล้ว แม้ว่า enhanced electronic signatures จะไม่จำกัดอยู่เพียงลายมือชื่อดิจิทัลเท่านั้นแต่ก็ดูเหมือนว่าในทางปฏิบัติแล้วบุคคลทั่วไปยังใช้ลายมือชื่อดิจิทัลกันเป็นส่วนใหญ่ จึงมีผลว่ากฎหมายลายมือชื่ออิเล็กทรอนิกส์ยังจำกัดอยู่เพียงลายมือชื่อดิจิทัลเท่านั้น

อย่างไรก็ตาม หลังจากการประชุมของคณะทำงานครั้งที่ 5 ที่นครนิวยอร์คในเดือนกุมภาพันธ์ 2543 เป็นต้นมา ได้มีความพยายามที่จะยกร่างใหม่โดยไม่มีการกล่าวถึง Enhanced electronic signature อีกเลย คงมีแต่การกล่าวถึง electronic signatures เป็นการทั่วไปเท่านั้น โดยบัญญัติให้ลายมือชื่ออิเล็กทรอนิกส์มีผลทางกฎหมายหาก*เชื่อถือได้ตามที่เหมาะสมกับวัตถุประสงค์ที่สร้างข้อมูลอิเล็กทรอนิกส์ขึ้น*[64] (ซึ่งก็เป็นการกล่าวซ้ำถึงข้อกำหนดใน Article 7 ของกฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์นั่นเอง) มีข้อสังเกตว่าแม้ร่างใหม่ได้ตัดคำว่า Enhanced electronic signature ออกไปแล้ว แต่ความจริงแล้วแนวความคิดเกี่ยวกับ Enhanced

---

[63] ตามบทนิยามใน Article 2 ของร่างกฎหมายแม่บทฉบับที่ยกร่างหลังจากการประชุมที่นครเวียนนาในเดือนกันยายน 1999 เพื่อใช้ในการประชุมที่นครนิวยอร์คในเดือนกุมภาพันธ์ 2000 คำว่า "Enhanced electronic signature" หมายความว่า "an electronic signature in respect of which it can be shown, through the use of a [security procedure] [method], that the signature:

(i) is unique to the signature device holder [for the purpose for] [within the context in] which it is used;

(ii) was created and affixed to the data message by the signature device holder or using a means under the sole control of the signature device holder [and not by any other person];

(iii) [(iii) was created and is linked to the data message to which it relates in a manner which provides reliable assurance as to the integrity of the message";] (ดูเอกสาร A/CN.9/WG.IV/WP.84, 8 December 1999 ของ UNCITRAL)

[64] **Article 6 Compliance with a requirement for a signature**

"(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement." : ดูเอกสาร A/C.9/467, April 2000 และเอกสาร A/CN.9/483, October 2000 ของ UNCITRAL)

electronic signature ก็แฝงอยู่ในบทบัญญัติของร่างใหม่นี้อยู่เหมือนเดิม ทั้งนี้ ใน Article 6 (3) ของร่างดังกล่าวได้บัญญัติว่าลายมือชื่อที่มีลักษณะตามที่กล่าวใน (a) ถึง (d) ของ Article 6 (3)[65] จะเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ ซึ่งเมื่อพิเคราะห์สาระสำคัญของ (a) ถึง (d) ดังกล่าวจะเห็นว่าเป็นลักษณะของ Enhanced electronic signature ตามบทนิยามของร่างเดิมก่อนเสร็จสิ้นการประชุมที่นครนิวยอร์คในเดือนกุมภาพันธ์ 2543 นั่นเอง นอกจากนี้ Article 6 (4) บัญญัติว่าไม่ว่ากรณีจะเป็นอย่างไรก็ตาม บุคคลใดอาจพิสูจน์ความน่าเชื่อหรือความไม่น่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์ได้ ซึ่งก็มีความหมายสำคัญอย่างน้อย 2 ประการ คือ (1) ในกรณีที่เป็นลายมือชื่ออิเล็กทรอนิกส์ที่ไม่มีลักษณะตาม Article 6 (3) (a) - (d) (Enhanced electronic signature) ก็เป็นเรื่องที่จะต้องสืบความน่าเชื่อถือกันเอง และ (2) แม้จะเป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตาม Article 6 (3) (a) -(d) (Enhanced electronic signature) ซึ่งกฎหมายถือว่า (หรือสันนิษฐานว่า) เป็นลายมือชื่อที่มีความถูกต้องแท้จริง คู่กรณีที่โต้แย้งความถูกต้องแท้จริงอาจจะสืบให้เห็นเป็นอย่างอื่นได้เสมอ[66]

ในการประชุมคณะทำงานซึ่งยกร่างกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ระหว่างวันที่ 19 - 29 กันยายน 2543 ที่ผ่านมา ณ นครเวียนนา เพื่อพิจารณาร่างกฎหมายนี้ คณะกรรมาธิการกฎหมายการค้าระหว่างประเทศ (UNICITRAL) ประสงค์จะให้เป็นการประชุมของคณะทำงานครั้งสุดท้าย ซึ่งตามระเบียบวาระการประชุมชั่วคราว[67] นอกจากจะมีการพิจารณาประเด็นทางกฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์แล้ว จะมีการพิจารณาร่างคำอธิบายประกอบตัวบทกฎหมายอีกด้วย (Draft Guide to Enactment)[68] อย่างไรก็ตาม ในการประชุมครั้งนั้น (ซึ่งผู้เขียนได้เข้าร่วมประชุมและทำหน้าที่ Rapporteur ด้วย) ปรากฏว่ามีการทบทวนประเด็นต่างๆ มากมาย รวมทั้งประเด็นที่ต้องอภิปรายเพิ่มเติม

---

[65] ความของ Article 6 (3) มีดังนี้

"An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if:

(a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.": ดูเอกสาร A/CN.9/483, October 2000 ของ UNCITRAL, หน้า 39 - 43)

[66] ดูเอกสาร A/C.9/467, April 2000 ของ UNCITRAL)

[67] ดูเอกสาร A/CN.9/WGIV/WP.85, 11 July 2000 ของ UNCITRAL)

[68] สำหรับ Draft Guide to Enactment ดูเอกสาร A/CN.9/WGIV/WP.86 and Add. 1. ของ UNCITRAL

อันเนื่องมาจากการตัดแนวความคิดเรื่อง Enhanced electronic signature ออกไปจากร่างเดิม คณะทำงานได้นำร่างเดิมตามที่ปรากฏในเอกสารฉบับที่จัดทำสำหรับการประชุมที่นิวยอร์คในเดือนกุมภาพันธ์ 2543[69] มาประกอบการพิจารณาด้วย ในที่สุด คณะทำงานก็ไม่มีเวลาเพียงพอที่จะพิจารณาร่างคำอธิบายประกอบตัวบทกฎหมาย จึงได้กำหนดพิจารณาเอกสารดังกล่าวในการประชุมครั้งต่อไปซึ่งจะจัดให้มีขึ้นที่นครนิวยอร์คในเดือนกุมภาพันธ์ 2544[70]

III. ความพยายามในการยกร่างกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และกฎหมายว่าด้วยลายมือชื่ออิเล็กทรอนิกส์

1. การยกร่างโดยหน่วยงานต้นสังกัด

รัฐบาลไทยได้ให้เล็งเห็นความสำคัญของการตรากฎหมายรองรับความก้าวหน้าของเทคโนโลยีสารสนเทศ จึงได้มีการดำเนินการยกร่างกฎหมายเกี่ยวกับเทคโนโลยีสารสนเทศหลายฉบับ ซึ่งรวมทั้งร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... และร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. ... ด้วย คณะรัฐมนตรีได้มีมติรับหลักการของร่างพระราชบัญญัติทั้งสองนี้ในวันที่ 14 มีนาคม 2543 ร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์เสนอโดยกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม (โดยศูนย์เทคโนโลยี อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ หรือ NECTEC) และโดยกระทรวงยุติธรรม ในขณะที่ร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์เสนอโดยกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม ร่างพระราชบัญญัติฉบับแรกได้ยกร่างขึ้นตามกฎหมายแม่แบบของ UNCITRAL โดยยึดถือถ้อยคำที่ปรากฏในกฎหมายแม่แบบของ UNCITRAL ค่อนข้างจะเคร่งครัด ส่วนร่างพระราชบัญญัติฉบับหลังได้รับรองผลทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์ ไม่ว่าจะเป็นลายมือชื่ออิเล็กทรอนิกส์แบบใด แต่บทบัญญัติส่วนใหญ่ของร่างพระราชบัญญัตินี้ยังมุ่งเน้นที่ลายมือชื่อดิจิทัล ทั้งนี้ ร่างกฎหมายนี้ได้กำหนดให้มีผู้ประกอบการรับรองโดยต้องขออนุญาตจากรัฐและรัฐกำกับดูแลการประกอบการของผู้ประกอบการรับรอง ลายมือชื่อดิจิทัลที่ได้มีการออกใบรับรองโดยผู้ประกอบการรับรองที่ได้รับอนุญาตจะได้รับการถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัย (Secure electronic signature) ซึ่งจะได้รับประโยชน์จากข้อสันนิษฐานทางกฎหมาย กล่าวคือ กฎหมายจะสันนิษฐานว่าข้อมูลอิเล็กทรอนิกส์ที่มีการใช้ลายมือชื่อดังกล่าวกำกับนั้นเป็นข้อมูลอิเล็กทรอนิกส์ที่ไม่มีการเปลี่ยน

---

[69] ดูเอกสาร A/CN.9/WGIV/WP.84 ของ UNCITRAL)

[70] สำหรับรายงานการประชุมครั้งล่าสุดของคณะทำงานฯ (18 - 29 กันยายน 2543) ดูเอกสาร A/CN.9/483, October 2000 ของ UNCITRAL

แปลงแก้ไขนับแต่เวลาที่มีการสร้างลายมือชื่อนั้นและลายมือชื่อนั้นเป็นของบุคคลที่ปรากฏชื่อว่าเป็นผู้ถือใบรับรอง จะเห็นว่าแนวความคิดดังกล่าวเป็นแนวความคิดที่ปรากฏในกฎหมายต่างประเทศนั่นเอง ทั้งนี้ คณะอนุกรรมการยกร่างกฎหมายได้พยายามศึกษาข้อดีข้อเสียของกฎหมายต่างประเทศเพื่อนำมาใช้เป็นแนวทางในการยกร่างกฎหมายไทย

2. ผลการตรวจพิจารณาร่างกฎหมายของสำนักงานคณะกรรมการกฤษฎีกา

ในชั้นการตรวจพิจารณาโดยสำนักงานคณะกรรมการกฤษฎีกา ในส่วนของร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ คณะกรรมการกฤษฎีกาได้แก้ไขในเรื่องของการใช้สำนวนกฎหมายและในเรื่องของความสอดคล้องกับกฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์มากยิ่งขึ้น เช่น ในบทบัญญัติที่เกี่ยวกับการเก็บรักษาเอกสารหรือข้อความในรูปของข้อมูลอิเล็กทรอนิกส์ ร่างฯเดิม (มาตรา 11) ได้กำหนดให้ "เอกสารหรือข้อความนั้นสามารถเข้าถึงได้ด้วยการอ่านและแปลงเป็นข้อความที่นำมาใช้ในการอ้างอิงในภายหลังได้" อันที่จริงแล้ว เมื่อมีการเก็บรักษาเอกสารหรือข้อความในรูปของข้อมูลอิเล็กทรอนิกส์ สิ่งที่ต้องสามารถเข้าถึงได้ด้วยการอ่านและแปลงเป็นข้อความนั้นก็คือข้อมูลอิเล็กทรอนิกส์ มิใช่เอกสารหรือข้อความอีก คณะกรรมการกฤษฎีกาจึงได้แก้ถ้อยคำส่วนดังกล่าวเป็น "ข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงได้ด้วยการอ่านและแปลงเป็นข้อความที่นำมาใช้ในการอ้างอิงในภายหลังได้" เป็นต้น

ส่วนร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. .... นั้น สำนักงานคณะกรรมการกฤษฎีกามีข้อสังเกตว่ามีเนื้อหาสาระเกี่ยวข้องกับร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ... อย่างใกล้ชิด เพราะ (1) เป็นการรับรองผลทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์ และ (2) เป็นการกำหนดวิธีการเกี่ยวกับการรับรองในเรื่องลายมือชื่ออิเล็กทรอนิกส์เพื่อให้ธุรกรรมทางอิเล็กทรอนิกส์มีความน่าเชื่อถือ เมื่อพิจารณาร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. .... แล้ว ปรากฏว่าผู้ร่างได้นำรายละเอียดทางเทคนิคเกี่ยวกับวิธีการรับรองในเรื่องลายมือชื่ออิเล็กทรอนิกส์มาบัญญัติไว้อย่างละเอียด ซึ่งบทบัญญัติมาตรา 8 ถึงมาตรา 69 (ในขณะที่ร่างกฎหมายนี้ประกอบด้วย 70 มาตรา) ได้บัญญัติเกี่ยวกับลายมือชื่อดิจิทัลและการกำกับการประกอบการรับรองเกี่ยวกับลายมือชื่อดิจิทัล ตลอดจนบทกำหนดโทษเกี่ยวกับลายมือชื่อดิจิทัลทั้งสิ้น อันที่จริงแล้วรายละเอียดทางเทคนิคในเรื่องเหล่านี้สมควรแยกไปบัญญัติเป็นพระราชกฤษฎีกา (ซึ่งเป็นกฎหมายลำดับรอง) จะมีความเหมาะสมกว่าเพราะจะทำให้สามารถปรับเปลี่ยนรายละเอียดทางเทคนิคได้ทันเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็วตลอดเวลา สำนักงานคณะกรรมการกฤษฎีกาจึงเห็นว่าเมื่อแยกรายละเอียดทางเทคนิคเหล่านั้นไปกำหนดเป็นพระราชกฤษฎีกาแล้ว บทบัญญัติที่จะคงเหลืออยู่ในร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. .... จะมีเพียงเล็กน้อยเท่านั้น ซึ่งสามารถนำไปบัญญัติรวมไว้เป็นส่วนหนึ่งของร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... ได้

ด้วยเหตุนี้ สำนักงานคณะกรรมการกฤษฎีกาจึงได้จัดทำร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... ฉบับที่รวมร่างกฎหมายทั้งสองฉบับเป็นฉบับเดียวกัน โดยนอกจากมีบทบัญญัติที่รองรับบทบัญญัติของกฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์แล้ว ยังมีบทบัญญัติหลักที่ให้อำนาจในการออกพระราชกฤษฎีกาเพื่อกำหนดวิธีการต่างๆ เกี่ยวกับความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์และการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างอื่นด้วย (เช่น ความน่าเชื่อถือของการเก็บรักษาต้นฉบับเอกสาร เป็นต้น) การปรับปรุงหลักการให้มีขอบเขตกว้างขึ้นในเรื่องของวิธีการต่างๆ เกี่ยวกับความน่าเชื่อถือ โดยไม่จำกัดอยู่เพียงวิธีการรับรองเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์หรือลายมือชื่อดิจิทัล (ดังในร่างฯ เดิมของกระทรวงวิทยาศาสตร์) นั้นก็เป็นเพราะการบัญญัติเพียงการประกอบการรับรองในเรื่องลายมือชื่ออิเล็กทรอนิกส์ไว้เท่านั้นทำให้กฎหมายมีข้อจำกัดบังคับได้เฉพาะกรณีดังกล่าว และลายมือชื่ออิเล็กทรอนิกส์ก็เป็นเพียงเรื่องการรับรองผลในด้านเทคนิคด้านหนึ่งเท่านั้น ซึ่งในการทำธุรกรรมอาจมีการประกอบการอย่างอื่นที่ต้องการความน่าเชื่อถือเช่นเดียวกันด้วย ถ้าหากกฎหมายจำกัดเพียงเทคนิคบางด้าน ทำให้ไม่อาจปรับใช้กับกิจการที่ดำเนินการในวัตถุประสงค์เดียวกันได้ ฉะนั้น บทบัญญัติในส่วนนี้จึงควรจะบัญญัติไว้ในลักษณะที่สามารถนำไปปรับใช้กับกิจการทุกประเภทที่จำเป็นได้โดยครบถ้วน ส่วนรายละเอียดในด้านเทคนิคแต่ละเรื่องควรแยกไปออกเป็นพระราชกฤษฎีกาเฉพาะในแต่ละกิจการต่อไป

ในการประชุมคณะรัฐมนตรีในวันที่ 25 กรกฎาคม 2543 คณะรัฐมนตรีเห็นชอบตามร่างฉบับที่สำนักงานคณะกรรมการกฤษฎีกาเสนอให้รวมร่างกฎหมายทั้งสองฉบับเป็นฉบับเดียวกัน ร่างพระราชบัญญัติฉบับนี้ประกอบด้วย 4 หมวด โดยหมวด 1 เป็นหมวดว่าด้วย**ธุรกรรมทางอิเล็กทรอนิกส์** ซึ่งมีบทบัญญัติที่รองรับเรื่องต่างๆ ที่กำหนดไว้ในกฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์ แต่ในหมวดนี้ได้เพิ่มบทบัญญัติที่กำหนดให้มีการตราพระราชกฤษฎีกากำหนดวิธีการในการลงลายมือชื่อ การเก็บรักษาต้นฉบับ หรือการกระทำใดในการทำธุรกรรมทางอิเล็กทรอนิกส์ที่จะได้รับประโยชน์จากข้อสันนิษฐานให้เป็นกรณีที่เชื่อถือได้และมีผลตามกฎหมาย ทั้งนี้ เพื่อที่จะสามารถกำหนดรายละเอียดเกี่ยวกับวิธีการทางเทคนิคที่จะยอมรับความถูกต้องของวิธีการที่กระทำได้ (มาตรา 24)[71] นอกจากนี้ได้เพิ่มหมวด 2 **การประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์** โดยกำหนดในลักษณะเป็นบทบัญญัติกลางที่สามารถนำไปปรับใช้กับการประกอบธุรกิจต่าง ๆ ที่มีการดำเนินการเกี่ยวกับความน่าเชื่อถือของธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งจะมีความหมายรวมถึงการรับรองลายมือชื่ออิเล็กทรอนิกส์อยู่ด้วย ทั้งนี้ โดยให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เป็นผู้พิจารณาเสนอความเห็นในการตราพระราชกฤษฎีกาว่า การใดมีความจำเป็นต้องควบคุมดูแล

---

[71] **มาตรา 24** การลงลายมือชื่อ การเก็บรักษาต้นฉบับ หรือการกระทำใดในการทำธุรกรรมทางอิเล็กทรอนิกส์ ถ้าได้กระทำตามวิธีการที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็นกรณีที่เชื่อถือได้และมีผลตามกฎหมาย

การประกอบธุรกิจ รวมทั้งพิจารณาระดับการควบคุมดูแลว่าควรจะเป็นการแจ้งให้ทราบหรือการอนุญาต ซึ่งจะแตกต่างกันไปตามลักษณะการประกอบธุรกิจ (มาตรา 25)[72]

ในกรณีที่มีพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์กรณีใดเป็นกิจการที่ต้องแจ้งให้ทราบ ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวต้องแจ้งให้พนักงานเจ้าหน้าที่ทราบก่อนเริ่มประกอบธุรกิจนั้น และต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกาและตามที่คณะกรรมการกำหนดในการประกอบธุรกิจ (ร่างมาตรา 26) ส่วนในกรณีที่มีพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์กรณีใดเป็นกิจการที่ต้องได้รับใบอนุญาต ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวต้องยื่นคำขอรับใบอนุญาตต่อพนักงานเจ้าหน้าที่ ส่วนคุณสมบัติของผู้ขอใบอนุญาต ตลอดจนหลักเกณฑ์และวิธีการที่เกี่ยวข้องให้เป็นไปตามที่กำหนดในพระราชกฤษฎีกาและตามประกาศหรือเงื่อนไขที่คณะกรรมการกำหนด (ร่างมาตรา 27) นอกจากนั้น ยังมีบทบัญญัติกำหนดโทษปรับทางปกครองสำหรับผู้ซึ่งไม่แก้ไขการแจ้งให้ถูกต้องหรือครบถ้วนตามคำสั่งของพนักงานเจ้าหน้าที่และสำหรับผู้ได้รับใบอนุญาตที่ฝ่าฝืนหรือปฏิบัติไม่ถูกต้องตามหลักเกณฑ์การประกอบธุรกิจที่กฎหมายกำหนด (ร่างมาตรา 26 วรรคสี่และวรรคห้า และร่างมาตรา 27 วรรคสี่) ซึ่งหากผู้กระทำความผิดที่มีโทษปรับทางปกครองกระทำความผิดดังกล่าวซ้ำอีก คณะกรรมการมีอำนาจออกคำสั่งห้ามประกอบธุรกิจหรือเพิกถอนใบอนุญาตอีกด้วย (ร่างมาตรา 26 วรรคหก และร่างมาตรา 27 วรรคห้า) ส่วนบทกำหนดโทษทางอาญานั้นมีเฉพาะกรณีที่ประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่แจ้งหรือไม่ได้รับใบอนุญาตตามที่กฎหมายกำหนดและกรณีที่ฝ่าฝืนคำสั่งห้ามการประกอบธุรกิจของคณะกรรมการ (ร่างมาตรา 36 และร่างมาตรา 37)

ส่วนองค์กรในการบริหารกฎหมาย ได้กำหนดให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เป็นผู้พิจารณาให้มีการพัฒนาด้านธุรกรรมทางอิเล็กทรอนิกส์และกำกับการประกอบธุรกิจเกี่ยวกับธุร

---

[72] **มาตรา 25** ในกรณีจำเป็นเพื่อรักษาความมั่นคงทางการเงินและการพาณิชย์หรือการเสริมสร้างความเชื่อถือและยอมรับในระบบข้อมูลอิเล็กทรอนิกส์ หรือเพื่อป้องกันความเสียหายต่อสาธารณชน คณะกรรมการอาจเสนอให้ตราพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์กรณีใดเป็นกิจการที่ต้องแจ้งให้ทราบหรือต้องได้รับใบอนุญาตก่อนก็ได้

ในการกำหนดให้กรณีใดต้องแจ้งให้ทราบหรือกรณีใดต้องได้รับใบอนุญาตตามวรรคหนึ่ง ให้กำหนดโดยพิจารณาจากความเหมาะสมในการป้องกันความเสียหายตามระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจากการประกอบธุรกิจนั้น

ในการนี้จะกำหนดให้หน่วยงานของรัฐแห่งหนึ่งแห่งใดเป็นผู้รับผิดชอบในการควบคุมดูแลในพระราชกฤษฎีกาดังกล่าวก็ได้

กรรมทางอิเล็กทรอนิกส์ โดยมีศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติเป็นหน่วยงานธุรการ (มาตรา 28 ถึงมาตรา 35)[73]

อันที่จริงแล้ว แนวทางการบัญญัติกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์โดยกำหนดเพียงหลักการกว้างๆ ไว้ แล้วให้อำนาจไปออกรายละเอียดต่างๆ ในรูปของกฎหมายลำดับรองก็ปรากฏอยู่ในกฎหมายของบางประเทศเช่นกัน เช่น Electronic Communications Act 2000 ของประเทศสหราชอาณาจักร ซึ่งบทบัญญัติส่วนแรกของกฎหมายนี้ได้บัญญัติเกี่ยวกับการควบคุมผู้ประกอบบริการการเข้ารหัส (Cryptography Service Providers) และในส่วนที่ 2 ได้บัญญัติเกี่ยวกับการส่งเสริมพาณิชย์อิเล็กทรอนิกส์ การเก็บรักษาข้อมูลและการอื่นๆ ที่เกี่ยวข้อง (Facilitation of Electronic Commerce, Data Storage, Etc.) ซึ่ง Section 8 ของกฎหมายนี้เป็นบทบัญญัติสำคัญที่ให้อำนาจรัฐมนตรีที่เกี่ยวข้องออกกฎหมายลำดับรอง (ในรูป Statutory Instrument) เพื่อกำหนดหลักเกณฑ์เกี่ยวกับการติดต่อสื่อสารทางอิเล็กทรอนิกส์และการเก็บรักษาข้อมูลทางอิเล็กทรอนิกส์ หากพิเคราะห์แล้วจะเห็นว่า Electronic Communications Act 2000 มิได้ยกร่างขึ้นโดยลอกเลียนถ้อยคำในกฎหมายแม่แบบของ UNCITRAL เลย แต่ได้บัญญัติให้ออก Statutory Instrument เพื่อรองรับหลักการต่างๆ ในกฎหมายแม่แบบและในร่างกฎหมายเอกรูปของ UNCITRAL ได้อย่างครบถ้วนและรองรับเทคโนโลยีที่เปลี่ยนแปลงไปอยู่เสมอ[74]

---

[73] รายละเอียดของร่างกฎหมายฉบับนี้ ดูเรื่องเสร็จที่ 353/2543 ของสำนักงานคณะกรรมการกฤษฎีกา

[74] **Section 8.** "(1) Subject to subsection (3), the appropriate Minister may by order made by statutory instrument modify the provisions of-

(a) any enactment or subordinate legislation, or

(b) any scheme, licence, authorisation or approval issued, granted or given by or under any enactment or subordinate legislation,

in such manner as he may think fit for the purpose of authorising or facilitatin the use of electronic communications or electronic storage (instead of other forms of communication or storage) for any purpose mentioned in subsection (2).

(2) Those purposes are-

(a) the doing of anything which under any such provisions is required to be or may be done or evidenced in writing or otherwise using a document, notice or instrument;

(b) the doing of anything which under any such provisions is required to be or may be done by post or other specified means of delivery;

(c) the doing of anything which under any such provisions is required to be or may be authorised by a person's signature or seal, or is required to be delivered as a deed or witnessed;

(d) the making of any statement or declaration which under any such provisions is required to be made under oath or to be contained in a statutory declaration;

(e) the keeping, maintenance or preservation, for the purposes or in pursuance of any such provisions, of any account, record, notice, instrument or other document;

(f) the provision, production or publication under any such provisions of any information or other matter;

3. การพิจารณาโดยสภาผู้แทนราษฎร

หลังจากที่คณะรัฐมนตรีมีมติเห็นชอบตามร่างฉบับที่สำนักงานคณะกรรมการกฤษฎีกาเสนอ ร่างกฎหมายดังกล่าวได้ผ่านการพิจารณาของคณะกรรมการประสานงานสภาผู้แทนราษฎรเมื่อวันที่ 26 กรกฎาคม 2543 และได้ส่งให้สภาผู้แทนราษฎรพิจารณา ในการพิจารณาของสภาผู้แทนราษฎรในชั้นกรรมาธิการฯ ได้มีการแก้ไขบทบัญญัติบางมาตราและได้มีการเพิ่มบทบัญญัติว่าด้วยลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัย (Secure electronic signatures) นอกจากนี้ ได้มีการเปลี่ยน "คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์" เป็น "คณะกรรมการลายมือชื่ออิเล็กทรอนิกส์" และจะมีการควบคุมเฉพาะผู้ประกอบการรับรองเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์*แบบปลอดภัย*เท่านั้น แม้ว่าการแก้ไขบางประการได้ก่อให้เกิดผลดี แต่ดังที่ได้กล่าวแล้วในบทนำ *การแก้ไขในหลายมาตรา (โดยสมาชิกสภาผู้แทนราษฎรท่านหนึ่งซึ่งผู้เขียนไม่ประสงค์จะระบุนาม ณ ที่นี้)* ***ได้กระทำในลักษณะที่ผิดไปจากหลักสากลในสาระสำคัญ นอกจากนั้น ยังปรากฏด้วยว่าบางมาตราก็ขัดแย้งกันเอง*** *ซึ่งแสดงให้เห็นว่าผู้เสนอแก้ไขมิได้มีความรู้ความเข้าใจกฎหมายพาณิชย์อิเล็กทรอนิกส์อย่างเพียงพอ ร่างกฎหมายดังกล่าวได้รับความเห็นชอบโดยสภาผู้แทนราษฎรแล้วในวันที่ 27 กันยายน 2543 ที่ผ่านมาและจะเข้าสู่การพิจารณาโดยวุฒิสภาต่อไป เมื่อมีความผิดพลาดเกิดขึ้นในชั้นสภาผู้แทนราษฎร* ***จึงจำเป็นอย่างยิ่งที่วุฒิสภาต้องแก้ไขความผิดพลาดที่ปรากฏในร่างกฎหมายฉบับนี้ มิฉะนั้นแล้ว ภาพลักษณ์ของความพร้อมด้านกฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์ของประเทศไทยในประชาคมโลกก็คงเป็นภาพลักษณ์ในทางที่ "น่าเป็นห่วงเป็นอย่างยิ่ง"***

ตัวอย่างของบทบัญญัติที่ผิดพลาดในสาระสำคัญ เช่น มาตรา 33 (2) ซึ่งบัญญัติเกี่ยวกับลักษณะของ "ลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัย" โดยบัญญัติว่า *"****ในกรณีที่ผู้ส่งข้อมูลและผู้รับข้อมูลได้ตกลงกันไว้ว่าลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นโดยอยู่ในความควบคุมของผู้ส่งข้อมูลคนใดในขณะที่สร้าง*** *และวิธีการที่ใช้ในการสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นสามารถเชื่อมโยงบุคคลดังกล่าวกับลายมือชื่ออิเล็กทรอนิกส์นั้นเป็นการเฉพาะ"* แนวความคิดที่ปรากฏอยู่ในมาตรา 33 (2) ดังกล่าวผิดพลาดเพราะจะมีผลว่าลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะ ๒ ประการ (สร้างขึ้นโดยวิธีการที่อยู่ในความควบคุมของบุคคลใดโดยเฉพาะในขณะที่สร้างและวิธีการที่ใช้ในการสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นสามารถเชื่อมโยงบุคคลดังกล่าวกับลายมือชื่ออิเล็กทรอนิกส์นั้นเป็นการเฉพาะ) จะเป็นลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัยได้**ก็ต่อเมื่อคู่กรณีตกลงกันเท่านั้น** ซึ่งความจริงแล้วลักษณะ ๒ ประการดังกล่าวเป็นลักษณะสากลของลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัยหรือลาย

(g) the making of any payment that is required to be or may be made under any such provisions.

... ..."

มือชื่อที่ถือว่าเชื่อถือได้ โดยไม่ต้องอาศัยความตกลงระหว่างคู่กรณี[75] ซึ่งใน Article 6 (3) ของ Draft Model Law on Electronic Signatures ก็บัญญัติให้มีผลเช่นนั้น มาตรา 33 (2) จึงต้องแก้ไขให้ถูกต้อง [76]

บทสรุป:

เทคโนโลยีที่ก้าวหน้าอย่างรวดเร็วทำให้ต้องมีกฎหมายรองรับปรากฏการณ์ใหม่ๆ ที่เกิดขึ้น นับเป็นที่น่ายินดีที่ประเทศไทยจะมีกฎหมายรองรับพาณิชย์อิเล็กทรอนิกส์หรือธุรกรรมทางอิเล็กทรอนิกส์ในอนาคตอันใกล้นี้ ซึ่งจะเอื้อต่อการค้าทั้งในประเทศและระหว่างประเทศ ตลอดจนการติดต่อกับทางราชการ อย่างไรก็ตาม กฎหมายเป็นสถาปัตยกรรมทางสังคมที่ต้องมีความเป็นพลวัตร (Dynamic) เท่าทันกับความเปลี่ยนแปลงของเทคโนโลยีอยู่เสมอ จึงต้องคอยติดตามกันต่อไปว่าแนวความคิดทางกฎหมายที่พยายามบรรจุเข้าไปเป็นเนื้อหาสาระของกฎหมายของเรานั้นมีความเหมาะสมกับเทคโนโลยีที่จะเกิดขึ้นใหม่ในอนาคตหรือไม่ นอกจากนี้ ประสบการณ์ที่ผ่านมาแสดงให้เห็นด้วยว่าบุคคลหลายฝ่าย รวมทั้งผู้ตรากฎหมายและผู้ปรับใช้กฎหมายยังขาดความรู้ความเข้าใจในเรื่องนี้ จึงควรต้องเร่งสร้างความรู้ความเข้าใจด้วย อันที่จริงแล้ว นอกจากร่างกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ซึ่งมีเรื่องลายมือชื่ออิเล็กทรอนิกส์รวมอยู่ด้วยนั้น) ยังจะมีร่างกฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ (Electronic Fund Transfer) ร่างกฎหมายเกี่ยวกับการคุ้มครองข้อมูล (Data Protection) และร่างกฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์ (Computer Crime) ในอนาคตอันใกล้นี้อีกด้วย การดำเนินการยกร่างกฎหมายเหล่านั้นจึงต้องกระทำด้วยความรอบคอบและชาญฉลาดเช่นกัน

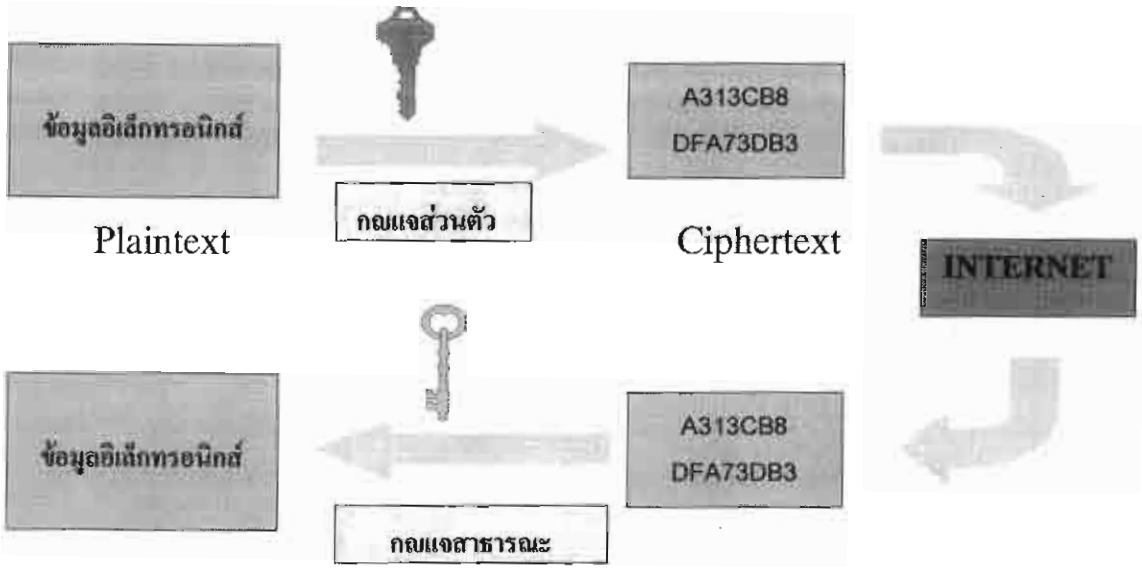
---

[75] ในกรณีที่คู่กรณีตกลงกันให้ใช้ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นด้วยวิธีการใด (ไม่ว่าจะมีลักษณะ ๒ ประการดังกล่าวหรือไม่) ลายมือชื่ออิเล็กทรอนิกส์นั้นจะถือว่าถูกต้องแท้จริงและข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อนั้นกำกับก็จะถือว่าไม่มีการเปลี่ยนแปลงแก้ไขนับแต่ขณะที่สร้างเสมอ

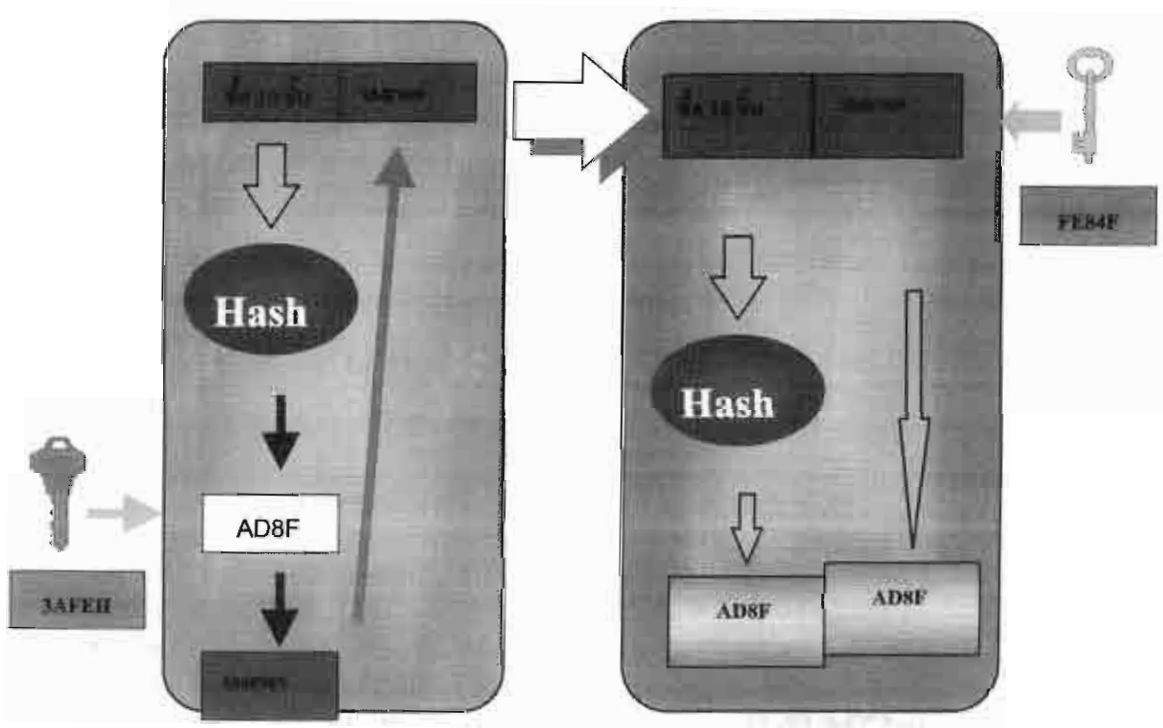
[76] อย่างไรก็ตาม มีข้อสังเกตว่า Article 6 (3) (a) ของ UNCITRAL Draft Model Law on Electronic Signatures ใช้คำว่า "the signature creation data are, within the context in which they are used, linked to the signatory and to no other person" ตาม Draft Model Law ดังกล่าว ความเชื่อมโยงจึงเป็นความเชื่อมโยงระหว่าง**วิธีการที่ใช้ในการสร้างลายมือชื่ออิเล็กทรอนิกส์และเจ้าของลายมือชื่อ** ดังนั้น ความในมาตรา 33 (2) จึงควรแก้เป็น ***"ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นโดยอยู่ในความควบคุมของบุคคลใดในขณะที่สร้างและวิธีการที่ใช้ในการสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นเชื่อมโยงกับบุคคลดังกล่าวเป็นการเฉพาะ"***

ภาคผนวก

ภาพแสดงการใช้ระบบรหัสแบบอสมมาตรในการสร้างลายมือชื่อดิจิทัล



ภาพแสดงตัวอย่างการสร้างและตรวจสอบลายมือชื่อดิจิทัล



ที่มา: หนังสือเผยแพร่ร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. .... ของสำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ศูนย์เทคโนโลยี อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2543