บทที่ 2
ความปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์

2.1 ความไว้วางใจและความเชื่อมั่นในเครือข่ายอิเล็กทรอนิกส์

ปัจจุบันความก้าวหน้าของเทคโนโลยีสารสนเทศ* ได้ก่อให้เกิดมิติใหม่ของการสื่อสาร การสื่อสารข้อมูลต่างๆ เป็นไปอย่างรวดเร็ว และมีประสิทธิภาพ ข่าวสารของซีกโลกหนึ่งจะถูกถ่ายทอดสู่ซีกโลกอื่นได้ภายในระยะเวลาไม่ถึงนาที การสื่อสารข้อมูลทางอิเล็กทรอนิกส์ เป็นรูปแบบของการสื่อสารข้อมูลที่ได้มีการพัฒนาอย่างต่อเนื่องมาจากเทคโนโลยีคอมพิวเตอร์ ซึ่งปัจจุบันมีบทบาทอย่างสูงในการปฏิบัติงานโดยทั่วไป เทคโนโลยีสารสนเทศได้ทำลายอุปสรรคของการสื่อสารไม่ว่าจะเป็นในเรื่องของเวลา, สถานที่ หรือแม้กระทั่งในเรื่องของพรมแดนระหว่างประเทศ จนกล่าวได้ว่าเป็นโลกยุคไร้พรมแดน (Globalization) ซึ่งส่งผลต่อการพัฒนาในรูปแบบต่างๆ โดยเฉพาะอย่างยิ่งการพัฒนารูปแบบการค้าใหม่ที่เรียกว่า "การพาณิชย์อิเล็กทรอนิกส์" (Electronic Commerce : E-Commerce) จนอาจกล่าวเปรียบเทียบได้ว่าเป็นยุคของการปฏิวัติทางธุรกิจเช่นเดียวกับที่เคยมียุคปฏิวัติทางอุตสาหกรรมเลยทีเดียว

ปรากฏการณ์ดังกล่าวข้างต้นเป็นปรากฏการณ์ที่รู้จักกันภายใต้ชื่อว่า "พาณิชย์อิเล็กทรอนิกส์" หากจะพิเคราะห์กันตามตัวอักษรแล้วก็คือการค้าโดยใช้สื่ออิเล็กทรอนิกส์นั่นเอง อันที่จริงแล้วสื่ออิเล็กทรอนิกส์มิได้จำกัดอยู่ที่ระบบเครือข่ายอินเทอร์เน็ตเท่านั้น แต่ยังรวมไปถึงสื่อทุกชนิดที่ใช้วิธีการทางอิเล็กทรอนิกส์ ดังนั้นการใช้เทเล็กซ์ โทรเลข โทรสาร หรือระบบการแลกเปลี่ยนข้อมูลกันโดยใช้มาตรฐานที่คู่กรณีกำหนดกันไว้ล่วงหน้า (ที่เรียกกันว่า Electronic data

---

* เทคโนโลยีสารสนเทศหรือไอที (Information Technology : IT) คือเทคโนโลยีที่ใช้เพื่อการจัดการ จัดหา ประมวล จัดเก็บ เรียกใช้ แลกเปลี่ยน หรือเผยแพร่สารสนเทศด้วยเทคโนโลยีอิเล็กทรอนิกส์ หรือการนำข้อมูลสารสนเทศไปปฏิบัติตามเนื้อหาของข้อมูลนั้นๆ เพื่อบรรลุเป้าหมายของผู้ใช้ ดังนั้น เทคโนโลยีสารสนเทศจึงประกอบด้วยเทคโนโลยีใหม่ๆ หลายด้าน เช่น เทคโนโลยีด้านคอมพิวเตอร์ ซึ่งรวมถึง ฮาร์ดแวร์ ซอฟต์แวร์ และฐานข้อมูลเทคโนโลยีคมนาคม ซึ่งรวมถึงเทคโนโลยีระบบสื่อสารทั้งแบบมีสายและไร้สาย ตลอดจนการสื่อสารในระบบ multi-media and interactive system เทคโนโลยีด้านอิเล็กทรอนิกส์ต่างๆ ซึ่งรวมถึงสารกึ่งตัวนำ เส้นใยแก้วนำแสง โทรทัศน์ความคมชัดสูง (HDTV) ปัญญาประดิษฐ์ (AI) CAD/CAM และ Office Automation เป็นต้น (สำนักงานเลขานุการส่งเสริมการพัฒนาเทคโนโลยีสารสนเทศแห่งชาติ, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC), แนวทางการพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศแห่งประเทศไทย. กรกฎาคม 2537, หน้า 8)

interchange หรือ EDI) ก็ล้วนแล้วแต่อยู่ในขอบเขตของคำว่า "พาณิชย์อิเล็กทรอนิกส์" ทั้งสิ้น แต่ที่มักจะใช้คำนี้ในบริบทของการติดต่อผ่านเครือข่ายอินเทอร์เน็ตก็เป็นเพราะระบบเครือข่ายอินเทอร์เน็ตเป็นระบบที่ใช้กันแพร่หลายมากที่สุดในปัจจุบันนั่นเอง [1]

ในส่วนของคำจำกัดความของการพาณิชย์อิเล็กทรอนิกส์นี้ ได้มีผู้ทรงคุณวุฒิหลายท่านได้ให้คำจำกัดความไว้ ดังนี้

"ในความหมายกว้างที่สุดแล้ว การพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce หรือ EC) หมายถึง การดำเนินการทางเศรษฐกิจใดๆ ที่กระทำบนเครือข่ายสื่ออิเล็กทรอนิกส์ ทั้งนี้การดำเนินการทางเศรษฐกิจดังกล่าวอาจรวมถึง การออกแบบ การผลิต การโฆษณาสินค้า การค้าทั้งปลีกและส่ง และการทำธุรกรรม ตลอดจนการชำระเงิน ส่วนเครือข่ายสื่ออิเล็กทรอนิกส์อาจรวมถึง เครือข่ายคอมพิวเตอร์ ทั้งเครือข่ายภายในองค์กร เครือข่ายเอกชน เครือข่ายระหว่างองค์กร หรือเครือข่ายสาธารณะ เช่นเครือข่ายอินเตอร์เน็ต หรือเครือข่ายสื่ออิเล็กทรอนิกส์อื่นๆ เช่นเครือข่ายโทรทัศน์ และเครือข่ายโทรศัพท์ เป็นต้น" [2]

"E-Commerce หมายถึง การทำกิจกรรมทางการค้า การซื้อขายสินค้าและบริการ โดยการใช้สื่อกลางอิเล็กทรอนิกส์เป็นตัวกลางในการส่งผ่านข้อมูลต่างๆ ทดแทนการใช้เอกสารในรูปแบบของกระดาษ ทำให้เกิดความสะดวก รวดเร็ว และครอบคลุมพื้นที่ในการทำธุรกิจการค้าได้มากขึ้น โดยจะดำเนินการผ่านระบบเครือข่ายอินเตอร์เน็ต" [3]

"องค์การการค้าโลก (World Trade Organization – WTO) ได้ให้ความหมายของคำว่า "การพาณิชย์อิเล็กทรอนิกส์" ว่า การผลิต การจัดจำหน่าย การตลาด การซื้อขายหรือส่งมอบสินค้าและบริการ โดยวิธีการทางอิเล็กทรอนิกส์" [4]

---

[1] พินัย ณ นคร, "กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์", ใน บทบัณฑิต. เล่ม 56. ตอน 2 (กรุงเทพมหานคร:, 2543), หน้า 2

[2] สมเกียรติ ตั้งกิจวานิชย์, การพาณิชย์อิเล็กทรอนิกส์. โครงการแผนแม่บทกระทรวงพาณิชย์ พ.ศ.2540-2549, ฝ่ายการวิจัยเศรษฐกิจรายสาขา สถาบันวิจัยเพื่อการพัฒนาประเทศไทย, พฤศจิกายน 2541, หน้า 1

[3] สมัชชา โยชน์ชัยสาร, "E-Commerce...การค้ายุคใหม่", ใน วิชาการปริทัศน์. ปีที่ 7 ฉบับที่ 2 (กุมภาพันธ์ 2542), หน้า 8

[4] WTO Committee on Trade and Development, paper on "Development Implications of Electronic Commerce", (WT/COMTD/W/51, 23 November 1998) อ้างถึงใน วิลาวรรณ มังคละธนะกุล, "Electronic Commerce", เอกสารในการสัมมนาเรื่อง "กฎหมายการค้าระหว่าง

การพาณิชย์อิเล็กทรอนิกส์นั้นเกิดขึ้นมาตั้งแต่ปี ค.ศ.1960 โดยเริ่มจากบริษัทในสหรัฐอเมริกาได้นำการส่งเอกสารอิเล็กทรอนิกส์ที่เรียกว่าระบบ EDI มาช่วยในการซื้อขายสินค้าระหว่างบริษัท นอกจากนั้นในสถาบันการเงินและธนาคารต่างๆ ได้มีการสร้างเครือข่ายทางคอมพิวเตอร์ที่เรียกว่า Electronic Fund Transfer (EFT) ซึ่งถูกออกแบบมาเพื่อใช้ส่งผ่านรายการโอนเงินในเครือข่ายคอมพิวเตอร์ของสถาบันการเงินได้อย่างมีประสิทธิภาพมาหลายสิบปีแล้ว ในช่วงเวลาดังกล่าว การติดตั้ง EDI ของบริษัทจะต้องสร้างเครือข่ายสื่อสารส่วนตัวขึ้นมาเองซึ่งลงทุนสูงและมีราคาแพง การใช้งานของ EDI จึงจำกัดอยู่ที่บริษัทขนาดใหญ่และสถาบันการเงินที่มีทุนทรัพย์เท่านั้น แต่ในปัจจุบันนี้ความแพร่หลายของอินเตอร์เน็ตทำให้โลกการพาณิชย์อิเล็กทรอนิกส์เปลี่ยนแปลงไป อินเตอร์เน็ตได้กลายเป็นช่องทางสื่อสารรูปแบบใหม่ที่มีการนำไปใช้งานอย่างกว้างขวางและขยายความสำคัญอย่างรวดเร็วสู่ธุรกิจทุกระดับชั้น จนทำให้ระบบการพาณิชย์อิเล็กทรอนิกส์ในปัจจุบันไม่ได้จำกัดอยู่แค่สถาบันการเงินหรือบริษัทขนาดใหญ่เท่านั้น

2.1.1 แนวความคิดพื้นฐานของความไว้วางใจและความเชื่อมั่นในเครือข่ายอิเล็กทรอนิกส์

จากที่การพาณิชย์อิเล็กทรอนิกส์นั้นผู้ขายและผู้ซื้ออาจจะไม่เคยรู้จักกันเลยมาก่อนและตลอดการติดต่อกันก็ไม่เคยพบหน้ากันเลย ทำให้เกิดความไม่แน่ใจระหว่างผู้ขายและผู้ซื้อ ทั้งการติดต่อกันโดยผ่านเครือข่ายอิเล็กทรอนิกส์โดยเฉพาะอินเตอร์เน็ตนั้น ยังสามารถถูกผู้ไม่ประสงค์ดี (Imposter) เข้าคุกคามเพื่อก่อความเสียหาย ตารางต่อไปนี้จะเป็นตัวอย่างของความเสียหายที่เกิดขึ้นพร้อมทั้งการแก้ไขหรือวิธีที่ใช้ป้องกันการบุกรุก

ประเทศกับประเทศไทย" จัดขึ้น ณ กระทรวงการต่างประเทศ วันที่ 8 กุมภาพันธ์ 2543, หน้า 1 (เอกสารไม่ตีพิมพ์เผยแพร่)

วิธีการบุกรุก	การแก้ไขปัญหา	การทำงาน	เทคโนโลยีที่ใช้
ลักลอบเข้ามาขโมยและแก้ไขข้อมูลในระบบ	เก็บข้อมูลโดยใช้การเข้ารหัส (Encryption)	เข้ารหัสของข้อมูลเพื่อป้องกันการลักลอบดูข้อมูล	วิธีการเข้ารหัสแบบสมมาตร (Symmetric Encryption) และแบบไม่สมมาตร (Asymmetric Encryption)
ปลอมตัวเข้ามาใช้ระบบและทำรายการปลอม	ระบบตรวจสอบว่าเป็นบุคคลที่มีสิทธิจริง (Authentication)	ตรวจสอบข้อมูลหลักฐานของทั้งทางผู้รับและผู้ส่งข้อมูล	ลายเซ็นดิจิตอล (Digital Signature)
ใช้ระบบโดยไม่มีสิทธิและใช้ระบบนี้ในการเข้าสู่ระบบอื่น	Firewall	ทำการตรวจสอบและกรองข้อมูลของการติดต่อจากเครือข่ายคอมพิวเตอร์หรือจากเครื่องเซิร์ฟเวอร์ของระบบ	Firewall และการวางเครือข่ายเสมือน (Virtual Private Network – VPN) ของตนเองซ้อนอีกชั้นหนึ่งในอินเตอร์เน็ต

แผนภูมิ 2-1[5] : ตัวอย่างของการบุกรุกเข้าสู่ระบบและการแก้ไข

ดังนั้นในการประกอบการพาณิชย์อิเล็กทรอนิกส์หรือทำการติดต่อระหว่างกันโดยผ่านทางเครือข่ายอิเล็กทรอนิกส์นั้น ผู้ประกอบการหรือผู้ทำการติดต่อย่อมต้องการความปลอดภัย ความเชื่อถือหรือความไว้วางใจในการประกอบธุรกรรมโดยผ่านเครือข่ายอิเล็กทรอนิกส์ ซึ่ง The Commission of the European Communities ได้กล่าวถึงเรื่องนี้ไว้ว่า

> "วัตถุประสงค์แรกคือการสร้างความไว้วางใจและความเชื่อมั่น การพาณิชย์อิเล็กทรอนิกส์จะขยายตัวมากขึ้น ถ้าผู้บริโภคและธุรกิจมีความมั่นใจว่าธุรกรรมอิเล็กทรอนิกส์ของตนจะไม่ถูกขัดขวางหรือถูกแก้ไข ผู้ซื้อหรือผู้ขายคือบุคคลที่อ้างว่าเป็นผู้ซื้อหรือผู้ขายจริง และกลไกในการทำธุรกรรมดังกล่าวใช้ได้ เป็นไปตามกฎหมายและปลอดภัย การสร้างความไว้วางใจและความเชื่อมั่นคือเงื่อนไขเบื้องต้นของการประสบความสำเร็จในการประกอบการพาณิชย์อิเล็กทรอนิกส์" *

---

[5] ที่มา : ฉันทวุฒิ พืชผล, ผู้แปล, เปิดโลกการพาณิชย์อิเล็กทรอนิกส์, พิมพ์ครั้งที่ 1 (กรุงเทพมหานคร : โปรวิชั่น), 2541, หน้า 74

* The Commission of the European Communities, A European Initiative in Electronic Commerce, (COM(97)157 final, Apr. 16,1997). http://www.cordis.lu/esprit/src/ecomcom.htm

"The first objective is to build trust and confidence. For e-commerce to develop, both consumer and business must confident that their transaction will not be intercepted or modified ,

ความไว้วางใจและความเชื่อมั่นเป็นหัวใจสำคัญของการทำธุรกรรมทุกประเภท ไม่ว่าจะเป็นธุรกรรมที่กระทำลงบนกระดาษหรือที่ได้กระทำโดยผ่ายทางเครือข่ายอิเล็กทรอนิกส์ ซึ่งแนวความคิดพื้นฐานที่ทำให้เกิดความไว้วางใจและความเชื่อมั่นมีดังนี้

2.1.1.1 การตรวจสอบความถูกต้องแท้จริงของบุคคลผู้ใช้ระบบ (Authentication of Users)

ในระบบการสื่อสารทุกระบบ เป็นเรื่องสำคัญที่จะต้องระบุถึงตัวบุคคลผู้ทำการสื่อสารได้อย่างชัดเจนและไม่มีข้อสงสัย และยังเป็นความต้องการพื้นฐานของการตรวจสอบอำนาจในการเข้าถึงระบบ (Authorized access to use a system) โดยสามารถที่จะอ่าน, เขียน, แก้ไข, หรือทำลายข้อมูลที่อยู่ในระบบ เพราะมิใช่ผู้ใช้ระบบทุกคนที่จะได้รับสิทธิให้ใช้ข้อมูลทุกชนิดที่มีอยู่ในระบบ คำว่าระบบในที่นี้มิได้หมายถึงเฉพาะระบบคอมพิวเตอร์ แต่หมายความรวมถึงระบบอื่นๆ อีกด้วย เช่น ระบบการเงิน ระบบข้อมูลต่างๆ เป็นต้น ซึ่งในปัจจุบันส่วนใหญ่จะออกแบบหรือจัดเก็บในรูปของระบบคอมพิวเตอร์

ปัจจุบันโลกกำลังเข้าสู่ยุคของระบบเศรษฐกิจอิเล็กทรอนิกส์ (Electronic Economy) ที่ใช้ระบบการติดต่อสื่อสารผ่านระบบเครือข่ายทางอิเล็กทรอนิกส์ขนาดใหญ่ การพัฒนาระบบการตรวจสอบบุคคลผู้ใช้ระบบที่แข็งแกร่งจึงเป็นสิ่งที่มีความสำคัญมากขึ้น เนื่องมาจากประกอบการพาณิชย์บนเครือข่ายอิเล็กทรอนิกส์ เป็นการขจัดไปซึ่งระบบการติดต่อในรูปแบบเดิมที่เน้นการพบปะในทางกายภาพของผู้ซื้อและผู้ขาย ซึ่งมีผลทำให้แนวโน้มการฉ้อโกงเพิ่มมากขึ้น เช่น ในระบบการพาณิชย์แบบเดิม เมื่อผู้ซื้อยื่นบัตรเครดิตของตนเพื่อชำระราคาสินค้าให้แก่ผู้ขาย ผู้ขายสามารถที่จะตรวจสอบความถูกต้องด้วยการ ตรวจสอบลายมือชื่อ (Hand-written Signature) ของผู้ซื้อ ว่าตรงกับลายมือชื่อที่อยู่บนบัตรเครดิตหรือไม่ เป็นต้น ซึ่งแตกต่างจากการติดต่อกันทางเครือข่ายอิเล็กทรอนิกส์ ถ้าผู้ซื้อทำการชำระราคาสินค้าด้วยวิธีการกรอกหมายเลขบัตรเครดิต ผู้ขายจะไม่มีทางที่จะตรวจสอบลายมือชื่อของผู้ซื้อได้เลย เพราะมิได้เห็นลายมือชื่อของผู้ซื้อ รวมทั้งยังไม่เห็นตัวอย่างลายมือชื่อในบัตรเครดิตที่จะนำมาเป็นตัวอย่างลายมือชื่อเพื่อนำมาตรวจสอบอีกด้วย

เมื่อบุคคลทำการติดต่อทำธุรกรรมทางเครือข่ายอิเล็กทรอนิกส์ บุคคลนั้นก็ย่อมที่จะต้องการที่จะทราบและทำการตรวจสอบถึงแหล่งที่มาของข้อความหรือข้อมูลที่ได้รับเพื่อที่จะแน่ใจได้ว่า ข้อความหรือข้อมูลที่ได้รับนั้นมาจากผู้ที่อ้างว่าเป็นผู้ส่งจริง การตรวจสอบดังกล่าวรู้

---

that the seller and the buyer are who they say they are, and that transaction mechanisms are available, legal, and secure. Building such trust and confidence is the prerequisite to win over business and consumers to e-commerce."

จักกันในบริบทที่ว่า "การตรวจสอบความถูกต้องแท้จริงของบุคคลผู้ใช้ระบบ" (Authentication of Users) หรือในบางครั้งเรียกว่า "การระบุตัวบุคคลผู้ใช้"

การตรวจสอบความถูกต้องแท้จริงของบุคคลผู้ใช้ระบบจึงเป็นเรื่องที่เกี่ยวข้องกับแหล่งที่มาหรือจุดกำเนิดของการสื่อสาร ใครคือผู้ส่งข้อความ? และข้อความดังกล่าวเป็นของจริงหรือถูกปลอมแปลง? [6]

การตรวจสอบความถูกต้องแท้จริงของบุคคลผู้ใช้ระบบ คือ ความสามารถที่จะระบุได้ว่าบุคคลที่ติดต่อด้วยนั้น เป็นบุคคลตามที่กล่าวอ้างหรือมีอำนาจหน้าที่ตามที่กล่าวอ้างจริง [7]

ตัวอย่างของการตรวจสอบความถูกต้องแท้จริงของบุคคลผู้ใช้ระบบที่เห็นได้ชัดเจนในปัจจุบัน ก็คือ ในกรณีที่มีคำสั่งแจ้งมายังธนาคารให้โอนเงินให้แก่บุคคลใดบุคคลหนึ่งโดยลูกค้าของธนาคารทางโทรศัพท์ ธนาคารก็จะต้องทำการตรวจสอบว่าคำสั่งโอนเงินดังกล่าวมาจากลูกค้าของตนจริง และต้องทำให้แน่ใจว่าคำสั่งโอนเงินดังกล่าวมิได้มาจากผู้ประสงค์ร้าย ซึ่งการตรวจสอบดังกล่าวของธนาคารก็อาจจะให้บุคคลที่มีคำสั่งให้โอนเงินดังกล่าวกระทำการกดหมายเลขประจำตัวบุคคล (PINs หรือ Personal Identify Numbers) หรือกดรหัสผ่าน (Password) ถ้าถูกต้องทางธนาคารก็จะกระทำการตามคำสั่งดังกล่าว ถ้าไม่ถูกต้องธนาคารก็จะปฏิเสธที่จะกระทำการตามคำสั่งโอนเงินดังกล่าว

วิธีการตรวจสอบความถูกต้องแท้จริงของบุคคลผู้ใช้ระบบนี้ สามารถแบ่งได้ตามลักษณะของสิ่งที่ถูกนำมาใช้ในการระบุตัวบุคคลดังต่อไปนี้ [8]

2.1.1.1.1 "สิ่งที่คุณรู้" (Something you know)*

ตัวอย่างที่เป็นที่รู้จักกันอยู่ทั่วไปในปัจจุบันคือ การใช้รหัสผ่าน (Password) หรือหมายเลขประจำตัวบุคคล (PINs or Personal Identify Numbers) ในการผ่าน

---

[6] Thomas J. Smedinghoff and Ruth Hill Bro, "Moving with Change: Electronic Signature Legislation as A Vehicle for Advancing E-COMMERCE", John Marshall Journal of Computer and Information Law, Vol. XVII, No.3 Spring 1999, p. 743

[7] สมเกียรติ ตั้งกิจวานิชย์, รายงานการวิจัยเรื่อง ลายมือชื่ออิเล็กทรอนิกส์และองค์กรออกใบรับรอง, สถาบันวิจัยเพื่อการพัฒนาประเทศไทย, พฤศจิกายน 2542, หน้า 4

[8] กฤษณะ ช่างกล่อม, (ร่าง) รายงานการศึกษาวิจัยเรื่องกฎหมายลายมือชื่อดิจิตอล ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ, หน้า 28-29

* "รู้" ในที่นี้หมายถึงจำได้ เช่นการจำรหัสบัตรเอทีเอ็ม เป็นต้น

เข้าสู่ระบบคอมพิวเตอร์ ระบบคอมพิวเตอร์ส่วนใหญ่จะมีรหัสผ่านก่อนที่จะสามารถผ่านเข้าไปใช้ระบบอยู่แล้ว หรือเครื่อง ATM ที่กำหนดให้ผู้ใช้ต้องมีหมายเลขประจำตัว (PINs) ก่อนเข้าใช้บริการทางการเงินของธนาคาร การระบุตัวบุคคลแบบนี้บางที่ใช้ข้อมูลส่วนบุคคลที่รู้เฉพาะบุคคลเป็นเครื่องพิสูจน์ยืนยันความถูกต้อง เช่น ในบางประเทศธนาคารบางแห่งจะถามผู้ใช้บริการให้ใช้ชื่อหรือนามสกุลก่อนแต่งงานของมารดาของตนเองเป็นรหัสเมื่อตอนขอเปิดบัญชี ในขณะที่การระบุตัวบุคคลในรูปแบบนี้เป็นที่นิยม แต่อย่างไรก็ตามก็มีข้อเสียอยู่หลายประการ เช่น ประการแรก รหัสลับดังกล่าวมีรหัสเดียวแต่มีผู้รู้อย่างน้อยสองคน คือ เจ้าของรหัสและผู้ให้บริการ (ซึ่งในที่นี้คือธนาคาร เป็นต้น) ข้อเสียประการที่สอง เนื่องจากการกำหนดรหัสลับมักจะใช้ข้อมูลที่เกี่ยวกับบุคคลเจ้าของรหัส เช่น วันเดือนปีเกิด หรือชื่อมารดาของเจ้าของรหัส ดังนั้นจึงเป็นสาเหตุที่ทำให้บุคคลที่ไม่สุจริตสามารถแกะรหัสดังกล่าวได้ไม่ยากนัก

2.1.1.1.2 "สิ่งที่คุณเป็น" (Something you are)*

ซึ่งมักจะเรียกว่า "ชีวมิติ" (Biometrics) วิธีนี้จะใช้ลักษณะทางชีววิทยาของบุคคลเป็นเครื่องมือตรวจสอบความถูกต้องแท้จริง ตัวอย่างเช่น ลายพิมพ์นิ้วมือ การพิมพ์เส้นเลือดของจอรับภาพนัยน์ตา (Retina Scan) หรือม่านตา (Irises) เสียง (Voice Print) หรือลายมือชื่อ (Hand Written signature) เป็นต้น หรือใช้ลักษณะนิสัยหรือความเคยชินส่วนตัวของแต่ละบุคคล ซึ่งสิ่งต่างๆ ที่กล่าวมานี้ในแต่ละบุคคลจะไม่เหมือนหรือซ้ำกันจึงถือว่าเป็นวิธีการระบุตัวบุคคลที่ดีมาก และยากหรือไม่สามารถที่จะลอกเลียนแบบได้ แต่ข้อเสียของการระบุตัวบุคคลในรูปแบบนี้คือต้องใช้เครื่องไม้เครื่องมือที่ซับซ้อนและมีราคาค่อนข้างสูง ในบางกรณีการที่จะตรวจสอบลักษณะประจำตัวบุคคลอย่างเช่น จอรับภาพนัยน์ตาต้องใช้แสงอินฟราเรดส่องผ่าน ทำให้หลายคนไม่ค่อยชอบใช้เครื่องมือดังกล่าว เนื่องจากเกรงว่าจะมีผลต่อสายตาได้ ซึ่งถือเป็นอุปสรรคในการใช้เครื่องมือและวิธีการดังกล่าวอย่างหนึ่ง นอกจากนั้นข้อมูลที่ได้รับจากการระบุตัวบุคคลแบบนี้ อาจเป็นการเปิดเผยความลับในเรื่องของสุขภาพที่เจ้าของอาจไม่ต้องการเปิดเผยต่อสาธารณชนก็ได้** อย่างไรก็ดีในทางปฏิบัติก็มีผู้นิยมใช้การระบุตัวบุคคลแบบชีวมิติ (Biometrics) ไม่น้อยเช่นกัน อย่างเช่นหน่วยงานที่เกี่ยวกับการตรวจคนเข้าเมืองซึ่งจะใช้เทคโนโลยีการตรวจสอบลายมือ (Hand-print Technology) ในการตรวจสอบหนังสือเดินทางเพื่อให้เกิดความรวดเร็วในการตรวจ

---

* "เป็น" ในที่นี้หมายถึง ลักษณะเฉพาะของแต่ละบุคคล อย่างเช่น ลายนิ้วมือ หรือเลนซ์แก้วตา (Irises) หรือเยื่อบุแก้วตา (Retinas) เป็นต้น

** ตัวอย่างเช่น สุขภาพบางอย่างของบุคคลสามารถวิเคราะห์ได้จากความบกพร่องของม่านตา ในขณะการส่องฉาย (Scan) ซึ่งอาจไม่มีผลต่อสายตาก็จริง แต่มีผลต่อความเป็นส่วนตัว (Privacy) ซึ่งบางทีเจ้าของข้อมูลส่วนตัวดังกล่าวไม่อยากบอกใคร

สอบ หรือบริษัทประกันภัยมักจะใช้เทคโนโลยีทางด้านชีวมิติของลายมือชื่อ(Signature Biometrics) ในการตรวจสอบว่ากรมธรรม์นั้นเป็นของบุคคลผู้นั้นจริง

2.1.1.1.3 "สิ่งที่คุณมี" (Something you have)*

ซึ่งถือเป็นการระบุตัวบุคคลทางอิเล็กทรอนิกส์ที่ได้รับความนิยมอยู่ในขณะนี้ โดยที่คำว่า "สิ่งที่คุณมี" นั่นควรเป็นสิ่งที่จับต้องได้ หรือเป็นข้อมูล อย่างเช่นกุญแจการเข้ารหัส (Encryption Key) เป็นต้น ตัวอย่างรูปแบบการระบุตัวบุคคลในรูปแบบนี้คือ ลายมือชื่อดิจิตอล ที่ผู้ใช้ "มี" กุญแจรหัสส่วนตัวหรือกุญแจรหัสลับ (Private Key) ที่มีความสอดคล้องกับกุญแจรหัสสาธารณะ โดยกุญแจรหัสลับใช้สำหรับลงลายมือชื่อและกุญแจรหัสสาธารณะใช้สำหรับตรวจสอบว่าเป็นลายมือชื่อดิจิตอลที่ถูกต้องแท้จริงหรือไม่ รายละเอียดของลายมือชื่อดิจิตอลจะได้อธิบายต่อไปในหัวข้อ 2.3

2.1.1.2 การรักษาความถูกต้องสมบูรณ์ของข้อมูล (Integrity)

ในระบบการสื่อสารผ่านทางเครือข่ายอิเล็กทรอนิกส์ มีอยู่สองสาเหตุที่จะทำให้ของมูลที่ได้รับหรือที่เก็บอยู่ในหน่วยความจำของระบบแตกต่างจากข้อมูลที่ได้ส่งมาหรือที่ได้เก็บรักษาไว้ เหตุผลประการแรก คือ เกิดความผิดพลาดในทางเทคนิคของตัวเครื่องมือในระบบเครือข่ายอิเล็กทรอนิกส์ และเหตุผลประการที่สอง คือ มีบุคคลอื่นไปแก้ไขข้อมูลดังกล่าว ซึ่งการแก้ไขข้อมูลอิเล็กทรอนิกส์สามารถที่จะกระทำได้โดยไม่หลงเหลือไว้ซึ่งร่องรอยการการแก้ไขอยู่เลย เพราะฉะนั้นระบบการตรวจสอบความถูกต้องสมบูรณ์ของข้อมูล (Integrity checks) จึงถูกสร้างขึ้นเพื่อทำการตรวจสอบความถูกต้องและความสมบูรณ์ของข้อมูลที่ได้รับว่าเหมือนกันกับข้อมูลที่ถูกส่งมาหรือเก็บรักษาไว้หรือไม่ และถ้าไม่เหมือนส่วนไหนของข้อมูลที่แตกต่างหรือถูกแก้ไข ไม่ว่าความแตกต่างของข้อมูลที่เกิดขึ้นนั้นจะเกิดขึ้นจากสาเหตุประการแรกหรือประการที่สองก็ตาม

การรักษาความถูกต้องสมบูรณ์ของข้อมูลจึงเป็นเรื่องที่เกี่ยวข้องกับความถูกต้องและความสมบูรณ์ของการติดต่อสื่อสาร ข้อความที่ผู้รับได้รับเหมือนกันกับข้อความที่ผู้ส่งได้ส่งหรือไม่? ข้อความดังกล่าวสมบูรณ์หรือไม่? ข้อความนั้นได้ถูกแก้ไขเปลี่ยนแปลงในระหว่างการส่งหรือการเก็บรักษาหรือไม่? [9]

---

* "มี" ในที่นี้หมายถึง การที่คุณมีหรืออยู่ในความครอบครองซึ่งสิ่งของหรือรหัส ซึ่งสามารถใช้ยืนยันถึงตัวคุณได้ เช่นการมีกุญแจรหัสส่วนตัวหรือกุญแจรหัสลับที่ใช้ในการเข้ารหัส ซึ่งจะมีคุณคนเดียวที่มีกุญแจรหัสส่วนตัวหรือกุญแจรหัสลับดังกล่าว

[9] Thomas J. Smedinghoff and Ruth Hill Bro, "Moving with Change: Electronic Signature Legislation as A Vehicle for Advancing E-COMMERCE", Id., p. 744

การรักษาความถูกต้องสมบูรณ์ของข้อมูล คือ การทำให้แน่ใจถึงความสม่ำเสมอของข้อมูล ป้องกันการสร้างข้อมูล เปลี่ยนแปลงข้อมูล หรือทำลายข้อมูลโดยไม่มีอำนาจ[10]

ผู้รับข้อมูลหรือข้อความอิเล็กทรอนิกส์จะต้องมั่นใจในความสามารถรักษาความถูกต้องสมบูรณ์ของข้อมูลหรือข้อความที่ตนได้รับในระบบการสื่อสาร ก่อนที่จะเข้าเกี่ยวข้องหรือปฏิบัติตามข้อมูลหรือข้อความดังกล่าว การรักษาความถูกต้องสมบูรณ์ของข้อมูลหรือข้อความนี้จึงเป็นเรื่องสำคัญในการติดต่อผ่านทางเครือข่ายอิเล็กทรอนิกส์ เมื่อมีความจำเป็นที่จะต้องทำการเจรจาต่อรองหรือกระทำนิติกรรมสัญญาทางเครือข่ายอิเล็กทรอนิกส์ ให้ใบอนุญาตในเรื่องที่เกี่ยวข้องกับระบบดิจิตอล กระทำการชำระเงินทางเครือข่าย หรือแม้กระทั่งเมื่อต้องทำการพิสูจน์ถึงความมีอยู่ของธุรกรรมโดยใช้ข้อมูลที่บันทึกไว้ในรูปแบบอิเล็กทรอนิกส์ (Electronic record)

2.1.1.3 การห้ามปฏิเสธความรับผิด (Non-repudiation)

ถ้าในขณะที่เรากำลังติดต่อสื่อสารในเครือข่ายอิเล็กทรอนิกส์อยู่นั้น เราได้ทำการตรวจสอบจนมั่นใจแล้วว่ากำลังติดต่ออยู่กับบุคคลที่เขาอ้างว่าเป็นจริง และข้อมูล*ที่ได้รับในระหว่างทำการติดต่อกันก็ตรวจสอบแล้วว่าถูกต้องตรงตามเจตนาของผู้ส่งจริง แต่ถ้าในเวลาต่อมาผู้ที่เราทำการติดต่อดังกล่าวปฏิเสธว่าไม่ได้เป็นผู้ทำการติดต่อ หรือปฏิเสธว่าข้อความที่ได้รับไม่ถูกต้องตรงกันกับข้อความที่ส่งมา จะทำอย่างไรที่จะสามารถป้องกันการปฏิเสธความรับผิดชอบของผู้ที่ทำการติดต่อในเครือข่ายอิเล็กทรอนิกส์ได้

ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ การห้ามปฏิเสธความรับผิดจากฝ่ายต่างๆ ที่เกี่ยวข้องในการสื่อสารว่าไม่ได้เป็นผู้ติดต่อ หรือไม่ได้มีการส่งหรือรับข้อมูล ก็คือการมีหลักฐานอันเพียงพอที่จะระบุถึงตัวบุคคลผู้ที่ทำการติดต่อ ผู้ที่ทำการรับหรือส่งข้อมูล และพิสูจน์ได้ว่าข้อมูลที่ได้รับในการติดต่อสื่อสารนั้นถูกต้องตรงกันกับข้อมูลที่ส่งมา เพื่อที่จะป้องกันมิให้ปฏิเสธถึงความเป็นผู้ส่งข้อมูล ปฏิเสธว่าข้อมูลไม่ได้ถูกจัดส่ง ปฏิเสธว่าไม่ได้รับข้อมูล หรือปฏิเสธว่าข้อมูลที่ได้รับไม่ถูกต้องตรงกับที่จัดส่งมา หรือกล่าวได้อีกอย่างหนึ่งว่า การห้ามปฏิเสธความรับผิด ก็คือความสามารถที่จะป้องกันผู้ที่ทำการติดต่อสื่อสารปฏิเสธว่าไม่มีการสื่อสารเกิดขึ้น หรือข้อมูลที่ทำการติดต่อสื่อสารนั้นไม่ถูกต้อง[11] หลักฐานที่จะนำมาใช้เพื่อพิสูจน์ในการห้ามปฏิเสธความ

---

[10] Warwick Ford and Michael S. Baum, Secure Electronic Commerce. (New Jerseyy : Prentice-Hall, Inc., 1997), p.. 94

* คำว่า "ข้อมูล" ในที่นี้ หมายถึง ข้อมูล ข้อความ ข่าวสารหรือสิ่งอื่นใดที่ส่งไปมาระหว่างผู้ที่ทำการติดต่อสื่อสารกัน

[11] Warwick Ford and Michael S. Baum, Id., p. 315

รับผิด ก็จะได้มาจากการการตรวจสอบความถูกต้องแท้จริงของบุคคลผู้ใช้ระบบและการรักษาความถูกต้องของข้อมูลนั่นเอง

ในการติดต่อสื่อสารไม่ว่าจะเป็นการสื่อสารสองฝ่ายหรือหลายฝ่ายก็ตาม จะสามารถแบ่งได้เป็นสองฝ่ายก็คือ ผู้ส่งข้อมูล (Originators) และผู้รับส่งข้อมูล (Recipients) เพราะฉะนั้นการห้ามปฏิเสธความรับผิดก็จะแบ่งได้เป็น 2 ประเภทก็คือ การห้ามปฏิเสธความรับผิดของผู้ส่ง กับการห้ามปฏิเสธความรับผิดของผู้รับ นอกจากนี้แล้วยังมีการห้ามปฏิเสธความรับผิดว่าไม่ได้จัดส่ง[12] ซึ่งแต่ละประเภทมีรายละเอียดดังนี้

2.1.1.3.1 การห้ามปฏิเสธความรับผิดว่าไม่ได้เป็นผู้ส่ง (Non-repudiation of Origin)

การห้ามปฏิเสธความรับผิดว่าไม่ได้เป็นผู้ส่งจะช่วยป้องกันหรือขจัดข้อถกเถียงในเรื่องของการเป็นผู้ส่งข้อมูล* ความถูกต้องของข้อมูล และเวลาในการส่งข้อมูลในการติดต่อสื่อสาร โดยมุ่งปกป้อง "ผู้รับข้อมูล" (recipients) ด้วยการจัดหาพยานหลักฐานที่เพียงพอที่จะใช้พิสูจน์ในกรณีที่เกิดประเด็นข้อถกเถียงขึ้น ซึ่งข้อถกเถียงจะเกิดขึ้นเมื่อ 1) ผู้รับอ้างว่าได้รับข้อมูล แต่ผู้ที่ถูกระบุว่าเป็นผู้ส่งอ้างว่าไม่ได้ส่งข้อมูล 2) ผู้รับอ้างว่าได้รับข้อมูลที่แตกต่างจากข้อมูลที่ผู้ส่งอ้างว่าได้จัดส่ง และ 3) ผู้รับอ้างว่าได้รับข้อมูลที่ส่งในเวลาใดเวลาหนึ่งโดยเฉพาะแต่ผู้ที่ถูกระบุว่าเป็นผู้ส่งอ้างว่าไม่ได้จัดส่งข้อมูลในเวลาดังกล่าว

ประเด็นข้อถกเถียงเหล่านี้จะเกิดขึ้นจากสาเหตุใดสาเหตุหนึ่งดังต่อไปนี้ 1) ผู้ส่งโกหก 2) ผู้รับโกหก 3) เครื่องคอมพิวเตอร์หรือเครื่องมือในการสื่อสารเกิดความผิดพลาด หรือ 4) ผู้ไม่หวังดีบุคคลอื่นสร้างขึ้น เพื่อเป็นการป้องกันการปฏิเสธความรับผิดชอบของผู้ส่งในข้อถกเถียงเหล่านี้ ผู้รับจึงต้องจัดหาพยานหลักฐานที่เพียงพอและเชื่อถือได้ที่สามารถ 1) ระบุตัวผู้ส่ง 2) แสดงถึงเนื้อหาหรือความถูกต้องของข้อมูล 3) แสดงถึงวันและเวลาที่ข้อมูลถูกส่ง 4) แสดงถึงตัวผู้รับที่ผู้ส่งต้องการส่งให้ (Intended recipient) และ 5) หลักฐานที่สามารถแสดงถึงบุคคลที่เป็นกลางและไว้วางใจได้ (trusted third party) ที่เกี่ยวข้องในการจัดหาพยานหลักฐาน

---

[12] Ibid., p. 321

* ในกรณีที่เป็นการจัดเก็บข้อมูล ฝ่ายที่เป็นผู้จัดเก็บข้อมูลจะเสมือนเป็นผู้ส่ง และฝ่ายที่รับข้อมูลเข้าหน่วยความจำของระบบ (retrieving the data item) จะเสมือนเป็นผู้รับข้อมูล

2.1.1.3.2 การห้ามปฏิเสธความรับผิดว่าไม่ได้เป็นผู้รับ (Non-repudiation of Delivery)

การห้ามปฏิเสธความรับผิดว่าไม่ได้เป็นผู้รับจะช่วยป้องกันหรือขจัดข้อถกเถียงในเรื่องของการเป็นผู้รับข้อมูล ความถูกต้องของข้อมูล และเวลาที่การรับข้อมูลเกิดขึ้นในการติดต่อสื่อสาร โดยมุ่งปกป้อง "ผู้ส่งข้อมูล" (senders) ด้วยการจัดหาพยานหลักฐานที่เพียงพอที่จะใช้พิสูจน์ในกรณีที่เกิดประเด็นข้อถกเถียงเหล่านี้ขึ้น คือ 1) ผู้ส่งอ้างว่าได้ส่งข้อมูล แต่ผู้ที่ถูกระบุว่าเป็นผู้รับอ้างว่าไม่ได้รับข้อมูล 2) ผู้ส่งอ้างว่าได้ส่งข้อมูลที่แตกต่างจากข้อมูลที่ผู้รับอ้างว่าได้รับ และ 3) ผู้ส่งอ้างว่าได้ส่งข้อมูลในเวลาใดเวลาหนึ่งโดยเฉพาะ แต่ผู้ที่ถูกระบุว่าเป็นผู้รับอ้างว่าได้รับข้อมูลในเวลาที่ไม่มีความสัมพันธ์กับเวลาที่ผู้ส่งอ้างดังกล่าว

เพื่อป้องกันการปฏิเสธความรับผิดของผู้รับในข้อถกเถียงเหล่านี้ ผู้ส่งต้องมีพยานหลักฐานที่เพียงพอและเชื่อถือได้ที่สามารถ 1) ระบุตัวผู้รับ 2) แสดงถึงเนื้อหาหรือความถูกต้องของข้อมูล 3) แสดงถึงวันและเวลาที่ได้รับข้อมูล 4) แสดงถึงตัวผู้ส่ง และ 5) หลักฐานที่สามารถแสดงถึงบุคคลที่เป็นกลางและไว้วางใจได้ (trusted third party) ที่เกี่ยวข้องในการจัดหาพยานหลักฐาน

2.1.1.3.3 การห้ามปฏิเสธความรับผิดว่าไม่ได้จัดส่ง (Non-repudiation of Submission)

ในบางกรณีการห้ามปฏิเสธความรับผิดว่าไม่ได้จัดส่งนั้นถูกพิจารณาว่ามีความแตกต่างจากการห้ามปฏิเสธความรับผิดว่าไม่ได้เป็นผู้ส่งและการห้ามปฏิเสธความรับผิดว่าไม่ได้เป็นผู้รับ จึงถูกจัดให้เป็นรูปแบบที่สามของการห้ามปฏิเสธความรับผิด การห้ามปฏิเสธความรับผิดว่าไม่ได้จัดส่งจะช่วยป้องกันหรือขจัดข้อถกเถียงในเรื่องของการจัดส่งข้อมูล ความถูกต้องของข้อมูลที่จัดส่ง และเวลาที่เกิดการส่งข้อมูลในการติดต่อสื่อสาร โดยมุ่งปกป้อง "ผู้ส่งข้อมูล" (senders) ด้วยการจัดหาพยานหลักฐานที่เพียงพอที่จะใช้พิสูจน์ในกรณีที่เกิดประเด็นข้อถกเถียงขึ้นในกรณีดังนี้ 1) ผู้ส่งอ้างว่าได้ส่งข้อมูล แต่ผู้รับที่ผู้ส่งต้องการส่งให้ (intended recipient) อ้างว่านอกจากจะไม่ได้รับข้อมูลแล้ว ผู้ส่งยังไม่ได้ส่งข้อมูลอีกด้วย และ 2) ผู้ส่งอ้างว่าได้ส่งข้อมูลในเวลาใดเวลาหนึ่งโดยเฉพาะ แต่ผู้รับที่ผู้ส่งต้องการส่งให้ (intended recipient) อ้างว่าผู้ส่งไม่ได้ส่งข้อมูลในเวลาที่ผู้ส่งอ้างถึงดังกล่าว

การห้ามปฏิเสธความรับผิดว่าไม่ได้จัดส่งจะมีประโยชน์อย่างมากในกรณีที่เวลาในการจัดส่งข้อมูลเป็นปัจจัยสำคัญต่อผลทางกฎหมายของการติดต่อนั้นๆ เช่นในเรื่องของการทำคำสนองตอบคำเสนอที่มีกำหนดเวลา หรือในเรื่องของการส่งคำบอกยกเลิกคำเสนอของตน เป็นต้น

ในบางกรณีการห้ามปฏิเสธความรับผิดว่าไม่ได้จัดส่ง (Non-repudiation of Submission) ถูกพิจารณาว่าเหมือนกับการห้ามปฏิเสธความรับผิดว่าไม่ได้เป็นผู้รับ (Non-repudiation of Delivery) เพราะต่างก็มุ่งปกป้อง "ผู้ส่ง" ทั้ง 2 ประเภท และวิธีการในจากจัดหาพยานหลักฐานก็เหมือนกันทั้งสองกรณี การปฏิเสธความรับผิดชอบว่าไม่ได้จัดส่ง (Non-repudiation of Submission) จึงถูกพิจารณาว่าเป็นส่วนหนึ่งของ การห้ามปฏิเสธความรับผิดว่าไม่ได้เป็นผู้รับ (Non-repudiation of Delivery)

ในการติดต่อทางเครือข่ายอิเล็กทรอนิกส์ในปัจจุบัน มีวิธีการที่จะใช้จัดหาพยานหลักฐานเพื่อจุดประสงค์ในการห้ามปฏิเสธความรับผิด (Non-repudiation) อยู่ 5 ขั้นตอนด้วยกัน คือ ขั้นตอนแรกคือผู้ส่งหรือผู้รับจะต้องทำการร้องขอบริการ ในการจัดหาหลักฐานเพื่อการห้ามปฏิเสธความรับผิด ซึ่งมีผู้เปิดให้บริการอยู่ในเครือข่ายอิเล็กทรอนิกส์ ขั้นตอนต่อมาก็คือการจัดหาพยานหลักฐานที่มั่นคงและเชื่อถือได้ตามที่ร้องขอ เพื่อใช้พิสูจน์ในเวลาที่มีข้อถกเถียงเกิดขึ้น ขั้นที่สามก็คือการจัดส่งพยานหลักฐานที่หามาได้ให้แก่ผู้ส่งหรือผู้รับที่ทำการร้องขอบริการ ต่อมาก็ทำการตรวจสอบพยานหลักฐานดังกล่าว ว่าเพียงพอที่จะใช้พิสูจน์ในเวลาที่มีข้อถกเถียงหรือไม่ ขั้นตอนสุดท้ายคือการจัดเก็บพยานหลักฐานดังกล่าวไว้ใช้ในเวลาที่เกิดข้อถกเถียงขึ้น[13] ขั้นตอนดังกล่าวนี้เป็นไปตาม ISO/IEC 10181-4 : Information Technology - Security Frameworks in Open system – Non-repudiation Framework แต่ใน ISO/IEC 10181-4 ได้จัดให้การระงับข้อพิพาท (dispute resolution) เป็นขั้นตอนสุดท้ายของการห้ามปฏิเสธความรับผิด (Non-repudiation) เพราะว่า หนึ่งในจุดประสงค์ของการห้ามปฏิเสธความรับผิด ก็คือผลในการระงับข้อพิพาท แต่การหลีกเลี่ยงข้อพิพาทก็เป็นหนึ่งในจุดมุ่งหมายของการห้ามปฏิเสธความรับผิด ในที่นี้จึงจัดให้การระงับข้อพิพาทเป็นประเด็นหนึ่งแต่ก็เป็นวิธีการที่แยกต่างหากออกไป ในมุมมองนี้การห้ามปฏิเสธความรับผิดจึงเป็นเครื่องมือที่ช่วยในการระงับข้อพิพาท ซึ่งแตกต่างจากการที่การระงับข้อพิพาทเป็นขั้นตอนหนึ่งในการการห้ามปฏิเสธความรับผิด (Non-repudiation) [14]

วิธีการจัดหาพยานหลักฐานและขั้นตอนต่างๆ เหล่านี้มีวิธีการและรายละเอียดที่น่าสนใจอีกมาก แต่เนื้อหาดังกล่าวอยู่นอกขอบเขตของวิทยานิพนธ์ฉบับนี้ จึงขอข้ามรายละเอียดในส่วนนี้ไป ผู้สนใจรายละเอียดเพิ่มเติมโปรดหาอ่านได้ในหนังสือ "Secure Electronic Commerce" ของ Warwick Ford and Michael S. Baum

---

[13] Warwick Ford and Michael S. Baum, Id., p. 348

[14] Ibid., pp.351-352

2.1.1.4 การปกป้องความลับในการทำธุรกรรม (Preservation of Confidentiality)

ในระบบการติดต่อสื่อสารนั้นทุกๆ ระบบจะต้องมีการออกแบบวิธีการในการปกป้องความลับในการติดต่อสื่อสาร โดยไม่ให้ผู้ที่ไม่เกี่ยวข้องกับการสื่อสาร หรือผู้ประสงค์ร้ายสามารถที่จะทราบถึงข้อมูลในการสื่อสารได้ ในทางปรกติมี 3 วิธีการที่จะสามารถรักษาความลับในการทำธุรกรรมอิเล็กทรอนิกส์ได้ นั่นคือ การรักษาความปลอดภัยทางกายภาพ การทำให้คลุมเครือสับสน และการเข้ารหัส

การรักษาความปลอดภัยทางกายภาพนั้น ผู้ทำการติดต่อตระหนักดีถึงความยากในการบุกรุกเข้าถึงสื่อที่ใช้ในการสื่อสารหรือเครื่องมือที่ใช้สื่อสารในทางทางกายภาพ เช่น การใช้เส้นใยแก้วนำแสง (Optical fiber) ซึ่งเป็นตัวกลางที่ใช้ในการสื่อสารที่ทำการดักฟังยากมาก เป็นต้น

ในเรื่องของการทำให้คลุมเครือสับสน ผู้ทำการติดต่อสื่อสารควรจะทราบว่าเป็นการดีที่จะทำการซ่อนข้อมูลที่ทำการสื่อสารไว้ในอะไรบางอย่างได้ เช่น สามารถที่จะซ่อนข้อมูลที่จะทำการสื่อสารไว้ในรูปภาพ ซึ่งขนาดของรูปภาพอาจจะใหญ่ขึ้นบ้าง แต่คงไม่มีใครทราบนอกจากผู้สร้าง เป็นต้น

ในส่วนสุดท้ายการเข้ารหัส ผู้ทำการติดต่อสื่อสารฝ่ายหนึ่งอาจจะใช้วิธีการเข้ารหัสแบบที่ตกลงกันไว้ทำการเข้ารหัสข้อมูลที่ต้องการติดต่อสื่อสาร แล้วจึงค่อยส่งให้ผู้ติดต่อสื่อสารอีกฝ่ายหนึ่ง ซึ่งเป็นการยากที่ผู้อื่นหรือผู้ประสงค์ร้ายจะสามารถแกะข้อมูลที่เข้ารหัสดังกล่าว ถึงแม้จะได้ข้อมูลที่ทำการเข้ารหัสนั้นไปก็ตาม

การที่จะให้ระบบการสื่อสารสามารถรักษาความลับได้ ก็จะต้องสามารถระบุตัวผู้ใช้ได้ การตรวจสอบความถูกต้องแท้จริงของบุคคลผู้ใช้ระบบ (Authentication of Users) ก็เป็นส่วนหนึ่งที่สำคัญ ที่ทำให้ระบบการสื่อสารสามารถที่จะรักษาความลับในการติดต่อสื่อสารกันได้

2.2 เทคโนโลยีการเข้ารหัส

ปัจจุบันความสามารถของ Personal Computer (PC) และการศึกษาวิธีการคำนวณเกี่ยวกับการแปลงรหัสข้อมูล (Cryptosystem) ได้พัฒนาไปจนสามารถนำมาประยุกต์ใช้เพื่อทำการตรวจสอบหลักฐานว่าเป็นจริงหรือเท็จ และใช้เพื่อป้องกันความปลอดภัยของระบบที่ใช้ในการทำรายการอิเล็กทรอนิกส์ได้อย่างดีและมีประสิทธิภาพ คำว่าการเข้ารหัสนี้คือการนำข้อความที่เราไม่อยากให้ผู้อื่นทราบมาทำการเข้ารหัส (Encryption) สับเปลี่ยนจนทำให้ผู้อื่นไม่สามารถเข้าใจและใช้ประโยชน์จากข้อมูลนั้นได้ และการเข้ารหัสดังกล่าวยังมีประโยชน์มากไปกว่านั้น คือ สามารถนำมาประยุกต์ใช้ตรวจสอบว่าผู้ที่กำลังใช้เครือข่ายคอมพิวเตอร์หรือทำรายการบนเว็บเพจเป็นผู้ที่เราต้องการติดต่อ

จริง ไม่ใช่ผู้อื่นที่แอบอ้างตัวเข้ามาใช้ระบบ นอกจากนี้ยังสามารถประยุกต์ไปใช้เป็นลายมือชื่อดิจิตอลในการระบุหรือยืนยันว่าอีเมล์หรือแฟ้มข้อมูลที่ส่งไปให้ผู้อื่นนั้นมาจากผู้ส่งที่อ้างถึงจริงๆ

การเข้ารหัสคือกระบวนการดัดแปลงหรือกลบเกลื่อนข้อมูล (Data) หรือข้อความ (Message) ซึ่งมนุษย์สามารถอ่านเข้าใจได้ (Plaintext) ให้กลายเป็นข้อมูลหรือข้อความที่มนุษย์ไม่สามารถอ่านเข้าใจได้ (Ciphertext)* ส่วนการถอดรหัส (Decryption) คือกระบวนการในการเปลี่ยนข้อมูลหรือข้อความที่ได้ทำการเข้ารหัส กลับไปสู่ข้อมูลหรือข้อความก่อนที่จะทำการเข้ารหัส ซึ่งมนุษย์สามารถอ่านเข้าใจได้**

2.2.1 ประวัติของการเข้ารหัส

ประวัติของการเข้ารหัสเพื่อใช้ในการติดต่อสื่อสารเพื่อป้องกันจากผู้ที่ไม่พึงประสงค์เริ่มมีมาตั้งแต่สมัยโรมันในยุคของจูเลียส ซีซาร์ (Julius Caesar) โดยทั้งผู้ส่งและผู้รับจะสื่อสารกันได้ก็ต่อเมื่อทั้งสองฝ่ายทราบกฎเกณฑ์เดียวกันในการเข้ารหัส ซึ่งกฎดังกล่าวจะใช้การเปลี่ยนข้อความต้นฉบับ (Plain Text) ให้กลายเป็นข้อความที่เข้ารหัส (Cipher Text) ซึ่งผู้อื่นอ่านไม่รู้เรื่อง ตัวอย่างของการเข้ารหัสแบบง่ายๆ เช่นการใช้กฎการเพิ่มค่า 13 เข้าไปตรงตำแหน่งแต่ละตำแหน่งของอักขระในข้อความ*** โดยอักษร A จะมีค่าตำแหน่งเป็น 1 และอักษร Z จะมีค่าตำแหน่งเป็น 26 ดังนั้นอักษร "A" ในข้อความต้นฉบับจะถูกเข้ารหัสเป็นอักษร "N"† เมื่อผู้ได้รับข้อความที่เข้ารหัส ผู้รับก็เพียงแต่ทราบว่ามีกฎเกณฑ์อย่างไรในการเข้ารหัส แล้วจึง "ถอดรหัส" (Decryption) นั้นโดยทำการกลับกัน ซึ่งในที่นี้ก็คือการลบค่าตำแหน่งออก 13 ตำแหน่งจากข้อความที่เข้ารหัส ก็จะได้ผลลัพธ์ออกมาเป็นข้อความเดิมที่ใช้สื่อสารกันได้ [15]

---

* Warwick Ford and Michael S. Baum, Secure Electronic Commerce, Id., p. 101

"Encryption is a process which is applied to data, knows as **plaintext**, that directly represents information such as the word or numbers constituting a message. Encryption transforms the plaintext data in to intelligible data call **ciphertext.**"

** Warwick Ford and Michael S. Baum, Secure Electronic Commerce, Id., p. 101

"A Decryption transformation, applied to ciphertext data, results in the regeneration of the the original plaintext data."

*** วิธีการนี้เป็นวิธีการเข้ารหัสของ Caesar หรือที่เรียกว่า "Caesar Cipher" ตัวอย่างเช่น ถ้าใช้ Caesar Cipher โดยการเพิ่มค่าอักขระไปอีก 13 ตำแหน่ง (A = ตำแหน่งที่ 1 ; Z = ตำแหน่งที่ 26) ในชื่อ David จะได้รหัสออกมาเป็น Qnivq (ถ้าพบตัวอักษร Z ให้เริ่มนับวนมาที่ A ใหม่)

† "A" + 13 = "N" คือตัวอักษรที่ 14

[15] ฉันทวุฒิ พืชผล, เรื่องเดิม, หน้า 76

2.2.2 ระบบพื้นฐานในการเข้ารหัส

การเข้ารหัสประกอบด้วยสองส่วนสำคัญ คือ 1) ขั้นตอนหรือวิธีการคำนวณในการเข้ารหัส (Algorithm) และ 2) กุญแจรหัส (Key) ที่จะใช้ในการเข้าหรือถอดรหัส โดยขั้นตอนการเข้ารหัสจะเป็นการใช้ชุดฟังก์ชั่นการคำนวณทางคณิตศาสตร์ ส่วนกุญแจจะเป็นชุดตัวเลขหรืออักขระที่นำมาใช้แทนค่าในชุดฟังก์ชั่นการคำนวณทางคณิตศาสตร์เพื่อทำการเข้ารหัสข้อมูลต่อไป

ถึงแม้ว่าจะมีวิธีการเข้ารหัสบางประเภทที่ไม่จำเป็นต้องใช้กุญแจในการเข้ารหัส* อย่างไรก็ดีการมีกุญแจสำหรับใช้ในการเข้ารหัสนั้นก็มีความสำคัญอย่างยิ่งสองประการ คือ (1) ขั้นตอนการเข้ารหัสนั้นซับซ้อนและคิดค้นขึ้นมาได้ยาก การใช้กุญแจในการเข้ารหัสจึงทำให้สามารถใช้ขั้นตอนการเข้ารหัสเดิมโดยไม่ต้องคิดค้นขั้นตอนหรือวิธีการเข้ารหัสขึ้นมาใหม่ทุกครั้ง เพียงแค่เปลี่ยนกุญแจในการเข้ารหัสเอกสารแต่ละชุดเท่านั้น (2) ในกรณีที่มีผู้อื่นทราบรหัสผ่านหรือกุญแจที่ใช้ในการถอดรหัสข้อความ ก็สามารถเปลี่ยนกุญแจและนำข้อความนั้นมาเข้ารหัสใหม่อีกครั้งโดยที่ไม่ต้องเสียเวลาเข้าไปเปลี่ยนแปลงขั้นตอนการเข้ารหัสใหม่ทั้งหมด ยกเว้นแต่ในกรณีที่ตรวจพบว่าขั้นตอนการเข้ารหัสมีข้อบกพร่อง หรือช่องโหว่ที่ทำให้ผู้อื่นสามารถถอดรหัสได้[16]

จำนวนกุญแจที่สามารถสร้างขึ้นเพื่อใช้ในการเข้ารหัสได้นั้น ขึ้นอยู่กับจำนวนบิตของกุญแจที่ใช้ เช่น ถ้ากุญแจที่ใช้มีขนาดความยาว 8 บิต (1 ไบต์) จะมีกุญแจที่สามารถสร้างได้ 256 กุญแจ** ยิ่งจำนวนบิตที่ใช้ยิ่งมากเท่าไรหรือกุญแจยิ่งยาวเท่าไร การคาดเดาหรือแกะรหัสก็จะทำได้ยากยิ่งขึ้น เช่น ถ้าใช้กุญแจขนาด 8 บิต ในการเข้ารหัส ก็จะสามารถมีกุญแจที่เป็นไปได้ทั้งหมด 256 กุญแจที่แตกต่างกัน ถ้าใช้คอมพิวเตอร์ในการคาดเดากุญแจนี้คอมพิวเตอร์อาจใช้เวลาไม่ถึงหนึ่งส่วนพันวินาทีในการสุ่มหากุญแจที่ถูกต้องจาก 256 กุญแจที่เป็นไปได้เพื่อการถอดรหัส*** แต่ถ้าใช้กุญแจที่มีความยาว 100 บิต ก็จะมีกุญแจที่สามารถสร้างได้ทั้งหมดถึง 2^{100} กุญแจ สมมติว่าคอมพิวเตอร์มีความสามารถในการถอดรหัสด้วยความเร็วหนึ่งล้านกุญแจต่อวินาที ในการสุ่มหากุญแจที่ถูกต้องของกุญแจยาว 100 บิต จะต้องใช้เวลาเป็นปีๆ ถึงจะหากุญแจที่ถูกต้องพบ

---

* เช่น วิธีการเข้ารหัสแบบแฮชฟังก์ชั่น (Hash Function)

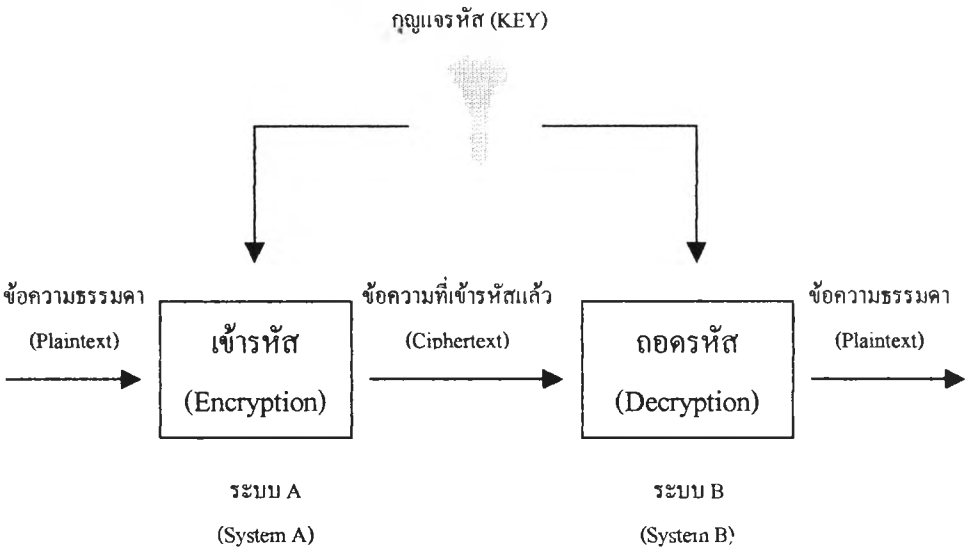
[16] ฉันทวุฒิ พืชผล, เรื่องเดิม, หน้า 76

** คำนวณจาก $2^8 = 256$ เนื่องมาจาก 1 บิต จะใช้ตัวเลขในระบบเลขฐาน 2 ซึ่งจะประกอบไปด้วยตัวเลข 2 ตัว คือ 0 กับ 1 เช่น 0000 0000 หรือ 0000 0001 เป็นต้น

*** การลองสุ่มใช้กุญแจไปเรื่อยๆ จนหากุญแจที่ถูกต้องพอ เรียกวิธีการนี้ว่าBrute-force Method

2.2.2.1 การเข้ารหัสแบบสมมาตร (Symmetric Cryptography)

ระบบการเข้ารหัสแบบสมมาตร (Symmetric Cryptosystem) หรือ การเข้ารหัสแบบกุญแจรหัสส่วนตัว (Secret-key, Private-key Cryptography) จัดเป็นระบบการเข้ารหัสโดยใช้กุญแจรหัสที่เก่าแก่ที่สุดในปัจจุบัน วิธีนี้ทั้งผู้รับและผู้ส่งข้อความจะต้องทราบกุญแจรหัสที่เหมือนกันทั้งสองฝ่ายในการรับหรือส่งข้อความ[17] ซึ่งก็คือต้องใช้กุญแจรหัสเดียวกันในการเข้ารหัสและถอดรหัส ความปลอดภัยของการเข้ารหัสแบบนี้ขึ้นอยู่กับกุญแจรหัส ผู้ที่ทราบกุญแจรหัสก็จะสามารถถอดรหัสข้อความได้ ดังนั้นถ้ากุญแจรหัสถูกเปิดเผย หรือถูกล่วงรู้โดยผู้อื่นก็จะทำให้ระบบการเข้ารหัสแบบนี้สูญเสียความปลอดภัยไป



แผนภูมิ 2-2 [18] : ระบบการเข้ารหัสแบบสมมาตร (Symmetric Cryptosystem)

วิธีการเข้ารหัสแบบนี้ผู้ส่ง (System A) จะนำข้อความธรรมดา (plaintext) มาทำการเข้ารหัส (Encryption) โดยใช้กุญแจรหัสที่ต้องเก็บไว้เป็นความลับ (โปรดดูแผนภูมิ 2-2 ประกอบ) เมื่อทำการเข้ารหัสแล้วจะได้ข้อความที่มนุษย์ไม่สามารถอ่านรู้เรื่องได้ (ciphertext) แล้วจึงทำการจัดส่งให้แก่ผู้รับ (System B) ผู้รับก็จะนำข้อความที่ได้รับมาทำการถอดรหัส (Decryption) โดยใช้กุญแจรหัสเดียวกันกับการเข้ารหัส ผู้รับก็จะได้รับข้อความธรรมดาที่สามารถอ่านรู้เรื่องได้ออกมา การเข้ารหัสแบบนี้ที่ดีนั้น ถ้าใส่กุญแจรหัสที่ไม่ถูกต้องทุกบิต (Bit) จะต้องไม่ได้รับข้อมูลหรือข้อความธรรมดา (plaintext) แม้แต่ส่วนใดส่วนหนึ่งจากกระบวนการถอดรหัส

---

[17] Warwick Ford and Michael S. Baum, Id., p. 102

[18] ที่มา : Warwick Ford and Michael S. Baum, Id., p. 102

ระบบการเข้ารหัสแบบนี้ นิยมใช้มาตรฐาน DES (Data Encryption Standard) ซึ่งคิดค้นโดยบริษัท IBM ในปี 1974 และเป็นมาตรฐานของ U.S. Federal Information System Processing ในปี 1977[19] และได้รับการยอมรับเป็นมาตรฐานของ American National Standard Institute สำหรับบริการทางการเงินในปี 1981[20] แม้ว่ามาตรฐาน DES จะได้รับการพิสูจน์ว่าเป็นระบบการเข้ารหัสที่ดี แต่ก็มักถูกวิพากษ์วิจารณ์ว่ามีจุดอ่อนมากมาย หนึ่งในจุดอ่อนที่สำคัญก็คือ ในการติดต่อกันเป็นครั้งแรก ผู้ใช้จะแจ้งให้บุคคลที่ตนต้องการติดต่อทราบได้อย่างไรว่า ข้อความที่ส่งไปถูกเข้ารหัสด้วยกุญแจรหัสใด ถ้าแจ้งกุญแจให้ผู้ที่ต้องการติดต่อรู้ผ่านทางเครือข่ายโดยไม่ต้องเข้ารหัสข้อมูล (เพราะอีกฝ่ายไม่ทราบกุญแจรหัสที่ใช้ในการเข้ารหัส) จะแน่ใจได้อย่างไรว่าจะไม่ถูกผู้ไม่ประสงค์ดีดักฟังข้อความที่ส่งไปหรือไม่มีผู้อื่นที่เข้ามาแอบเห็นข้อความดังกล่าว และปัญหาที่สำคัญอีกประการหนึ่งก็คือ ถ้าผู้ใช้มีบุคคลที่ต้องการจะติดต่อ n คน ก็จำเป็นที่จะต้องมีกุญแจรหัสทั้งหมด n กุญแจรหัส ทั้งจะต้องคอยจำว่ากุญแจรหัสใดใช้กับใคร หรือถ้าผู้ใช้ใช้กุญแจรหัสเดียวกันทั้งหมดในการติดต่อ ก็จะทำให้บุคคลเหล่านั้นสามารถอ่านข้อความที่ส่งให้บุคคล n คนได้ทั้งหมด

2.2.2.2 การเข้ารหัสแบบอสมมาตร (Asymmetric Cryptography)

ระบบการเข้ารหัสแบบอสมมาตร (Asymmetric Cryptosystem) หรือระบบการเข้ารหัสแบบกุญแจรหัสสาธารณะ (Public-key Cryptosystem) ระบบการเข้ารหัสแบบนี้ถูกเผยแพร่ในปี ค.ศ. 1976 โดย Whitifield Diffie และ Mattin E. Hellman ของมหาวิทยาลัย Standford การเข้ารหัสแบบนี้ใช้แนวความคิดของการมีคู่กุญแจรหัสที่สามารถเข้าและถอดรหัสของกันและกันได้เท่านั้น โดยเมื่อใช้กุญแจรหัสหนึ่งในการเข้ารหัสแล้ว จะต้องใช้กุญแจรหัสที่เหลือในการถอดรหัสเท่านั้น[21] จะไม่สามารถใช้กุญแจรหัสที่ใช้ในการเข้ารหัสมาทำการถอดรหัสข้อมูลได้ ในทางปฏิบัติจะเก็บกุญแจรหัสหนึ่งกุญแจไว้ที่เจ้าของคู่กุญแจเท่านั้น ซึ่งจะต้องเก็บไว้เป็นความลับเฉพาะตัว เรียกกุญแจนี้ว่า "กุญแจรหัสส่วนตัว" (Private key) และกุญแจรหัสที่เหลือสามารถเปิดเผยให้บุคคลอื่นหรือสาธารณะชนทราบได้ ซึ่งเรียกกุญแจรหัสนี้ว่า "กุญแจรหัสสาธารณะ" (Public

---

[19] David L. Gripman, "Electronic Document Certificate : A Primer on The Technology Behind Digital Signature", in John Mashall Journal of Computer & Information Law, Vol.XVII, 1999, p.775

[20] กฤษณะ ช่างกล่อม, (ร่าง) รายงานการศึกษาวิจัยเรื่องกฎหมายพาณิชย์อิเล็กทรอนิกส์, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ, หน้า 24

[21] David L. Gripman, Id., p.776

key)[22] ทั้งนี้จะไม่สามารถนำกุญแจรหัสหนึ่งกุญแจมาทำการคำนวณเพื่อหาคู่กุญแจรหัสที่เหลือได้* ระบบการเข้ารหัสแบบอสมมาตรนี้ สามารถนำมาประยุกต์ใช้ได้ในสองลักษณะดังต่อไปนี้

2.2.2.2.1 เพื่อการรักษาความลับของข้อความ[23]

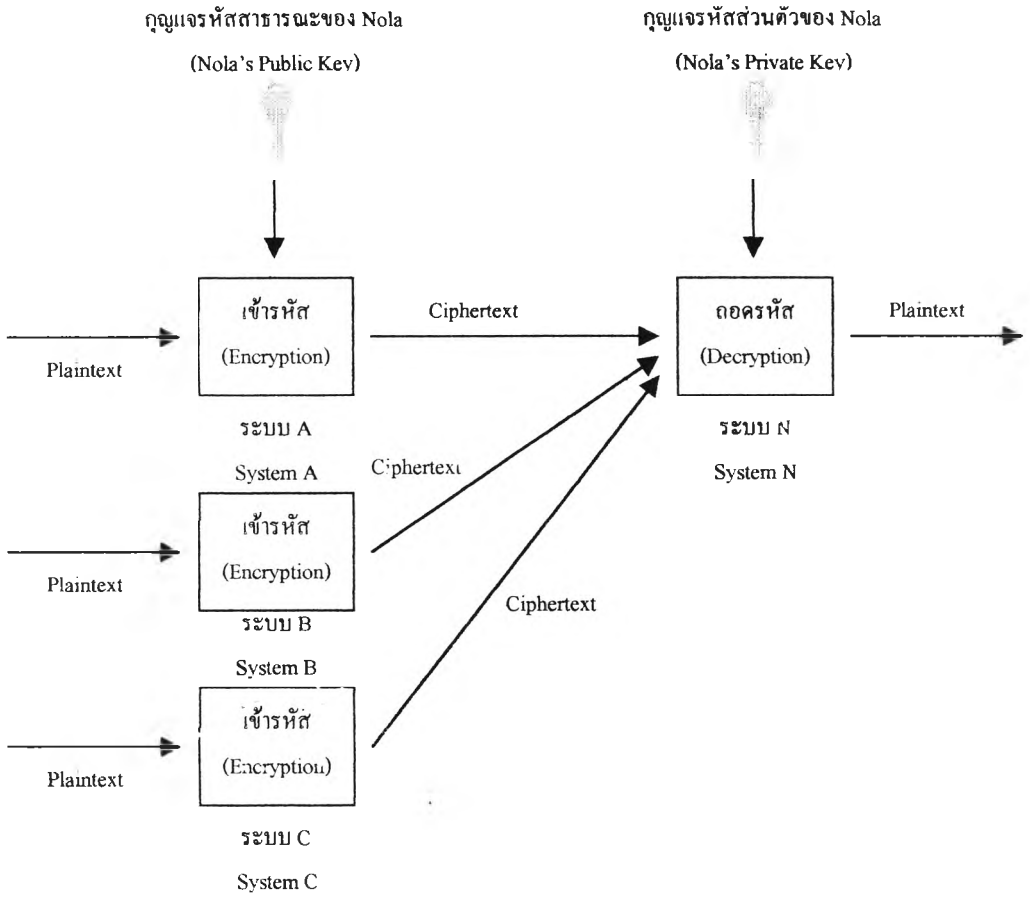
การเข้ารหัสเพื่อรักษาความลับของข้อความนี้ เช่น ถ้าผู้ส่งต้องการส่งข้อความที่เป็นความลับให้แก่ Nola ผู้ส่ง (ไม่ว่าจะเป็นผู้ส่งจากระบบ A ระบบ B หรือ ระบบ C ก็ตาม) จะนำข้อความธรรมดา (plaintext) นำมาเข้ารหัสโดยใช้กุญแจรหัสสาธารณะ (Nola's Public key) ของ Nola (โปรดดูแผนภูมิ 2-3 ประกอบ) แล้วจะทำการส่งข้อความที่ได้รับการเข้ารหัสแล้ว (ciphertext) ไปให้แก่ Nola เมื่อ Nola ได้รับข้อความก็จะนำกุญแจรหัสส่วนตัวของตน (Nola's Private key) มาทำการถอดรหัสข้อความที่ได้รับ ก็จะได้ข้อความธรรมดา (plaintext) และมีเพียง Nola ผู้เดียวเท่านั้นที่สามารถถอดรหัสข้อความที่ส่งมา เพราะ Nola เป็นเพียงผู้เดียวที่มีกุญแจรหัสส่วนตัวของตน จึงมั่นใจได้ว่าข้อความที่ส่งมาจะถูกเก็บรักษาไว้เป็นความลับจากผู้อื่น

---

[22] Warwick Ford and Michael S. Baum, Id., p. 107

* อย่างไรก็ตาม การที่ไม่สามารถนำกุญแจรหัสหนึ่งกุญแจรหัสมาทำการคำนวณเพื่อหาคู่กุญแจรหัสที่เหลือได้ก็เป็นเพียงช่วงระยะเวลาหนึ่งเท่านั้น เช่น 1ปี หรือ 6 เดือน เป็นต้น เพราะฉะนั้นคู่กุญแจรหัสหนึ่งๆ จึงมีระยะเวลาในการใช้ โดยขึ้นอยู่กับระยะเวลาที่จะสามารถนำกุญแจรหัสหนึ่งกุญแจรหัสมาคำนวณเพื่อหาคู่กุญแจรหัสที่เหลือได้ ซึ่งหลังจากนั้นก็จะต้องมีการสร้างคู่กุญแจรหัสขึ้นมาใช้ใหม่ เพื่อประกันความปลอดภัยของการเข้ารหัสในระบบนี้

[23] Warwick Ford and Michael S. Baum, Id., p. 107



แผนภูมิ 2-3 [24] : การเข้ารหัสแบบอสมมาตร (Asymmetric Cryptosystem)
(ในกรณีที่ต้องการรักษาความลับของข้อความ)

2.2.2.2.2 เพื่อการพิสูจน์ความถูกต้องแท้จริงของผู้ส่งข้อความ[25]

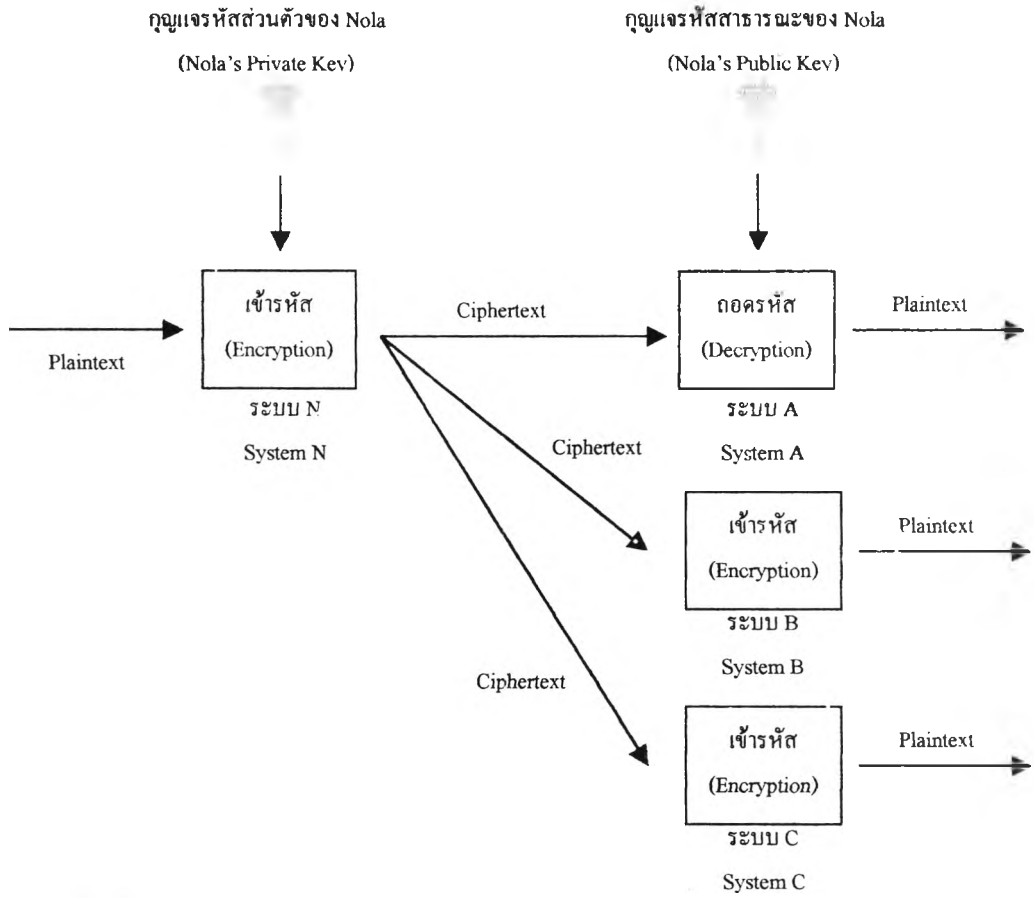
การเข้ารหัสเพื่อพิสูจน์ความถูกต้องแท้จริง (Authentication) ของผู้ส่งข้อความนี้ เช่น ถ้าผู้รับ (ไม่ว่าจะเป็นผู้รับในระบบ A ระบบ B หรือระบบ C ก็ตาม) ต้องการพิสูจน์ว่าข้อความที่ตนได้รับส่งมาจาก Nola จริง วิธีการก็จะเริ่มจากการที่ Nola จะนำข้อความธรรมดา (plaintext) มาทำการเข้ารหัสโดยใช้กุญแจรหัสส่วนตัวของตน (Nola's Private key) ก็จะได้ข้อความที่เข้ารหัสแล้ว (Ciphertext) จากนั้นทำการส่งข้อความที่เข้ารหัสแล้วนี้ให้แก่ผู้รับในระบบต่างๆ เมื่อผู้รับได้รับข้อความจาก Nola แล้ว ก็จะนำกุญแจรหัสสาธารณะ (Nola's Public key) ของ Nola มาทำการถอดรหัส (โปรดดูแผนภูมิ 2-4 ประกอบ) ถ้าทำการถอดรหัสได้ก็แสดงว่าข้อความนั้นส่งมาจาก Nola จริง เพราะมีเพียงกุญแจรหัสสาธารณะของ Nola เท่านั้นที่จะถอดรหัสข้อ

---

[24] ที่มา : Warwick Ford and Michael S. Baum, Id., p. 107

[25] Warwick Ford and Michael S. Baum, Id., p. 108

ความที่เข้ารหัสโดยกุญแจรหัสส่วนตัวของ Nola และมีเพียง Nola คนเดียวที่มีกุญแจรหัสส่วนตัวของตน



แผนภูมิ 2-4 [26] : การเข้ารหัสแบบอสมมาตร (Asymmetric Cryptosystem)
(ในกรณีที่ต้องการพิสูจน์ความถูกต้องแท้จริงของผู้ส่งข้อความ)

ระบบการเข้ารหัสแบบอสมมาตรที่สามารถทำงานได้ทั้งการรักษาความลับและพิสูจน์ความถูกต้องแท้จริงของผู้ส่งข้อความเรียกว่า "Reversible public-key cryptosystem" ส่วนการเข้ารหัสแบบอสมมาตรที่สามารถทำงานได้แต่การพิสูจน์ความถูกต้องแท้จริงเท่านั้นเรียกว่า "irreversible public-key cryptosystem" [27]

อาจจะเห็นว่าการเข้ารหัสแบบอสมมาตรนี้แตกต่างจากการเข้ารหัสแบบสมมาตรเพียงเล็กน้อย แต่จริงๆ แล้วระบบกุญแจรหัสสาธารณะนี้มีข้อดีกว่าระบบกุญแจรหัสส่วนตัวหลายประการ ประการแรกคือสามารถแจกจ่ายกุญแจรหัสสาธารณะได้ทันที (อาจเป็นบนเครื่อง

---

[26] ที่มา : Warwick Ford and Michael S. Baum, Id., p. 108

[27] Warwick Ford and Michael S. Baum, Id., p. 109

เซิร์ฟเวอร์หรือบนอินเตอร์เน็ตก็ได้) โดยไม่ต้องกังวลว่าผู้อื่นจะสามารถทราบถึงกุญแจรหัสส่วนตัวได้ในช่วงระยะเวลาหนึ่ง (Cryptoperiod) นอกจากนี้ยังไม่จำเป็นต้องส่งกุญแจรหัสสาธารณะของตัวเองไปให้ผู้อื่นที่เราต้องการติดต่อด้วยทุกคน เนื่องจากผู้ที่ต้องการติดต่อกับเราสามารถไปหากุญแจรหัสสาธารณะของเราได้จากผู้ให้บริการระบบกุญแจรหัส ผู้ประกอบการรับรอง (Certificate Authority) ซึ่งเป็นผู้ออกใบรับรองว่ากุญแจรหัสสาธารณะที่แจกจ่ายนั้นเป็นกุญแจรหัสที่คู่กับกุญแจรหัสส่วนตัวของผู้ใช้จริง หรือเซิร์ฟเวอร์ของบริษัทซึ่งทำหน้าที่เก็บกุญแจรหัสสาธารณะของพนักงานทุกคนไว้

ตัวอย่าง Algorithm ที่ใช้ในการเข้ารหัสแบบกุญแจรหัสสาธารณะที่เป็นที่นิยมใช้และรู้จักกันมากได้แก่ RSA Algorithm ซึ่งเป็นการเข้ารหัสข้อมูลแบบ reversible public-key cryptosystem ซึ่งคิดค้นโดย Ron Riverst, AdiShamir และ Len Adleman ของ Massachusetts Institute of Technology (MIT) ในปี ค.ศ. 1978 โปรดดูรายละเอียดเพิ่มเติมเกี่ยวกับ RSA Algorithm ได้ใน Warwick Ford and Michael S. Baum หน้า 109-110 หรือหนังสือเกี่ยวกับการเข้ารหัสเล่มอื่นๆ

จากการที่สามารถนำระบบการเข้ารหัสแบบอสมมาตรนี้มาใช้เพื่อพิสูจน์ความถูกต้องแท้จริงของผู้ส่งนี้เอง เทคโนโลยีการเข้ารหัสแบบนี้จึงถูกนำมาประยุกต์ใช้เป็นลายมือชื่อดิจิตอล (Digital Signature) ซึ่งมีความสำคัญทั้งในแง่ความปลอดภัยของการส่งข้อมูล สิทธิส่วนตัว (Private Right) ความไว้วางใจ (trust)ในการติดต่อหรือการพาณิชย์ในเครือข่ายอิเล็กทรอนิกส์ รวมทั้งความผูกพันหรือนิติสัมพันธ์ในมุมมองของกฎหมาย

2.2.3 การบริหารคู่กุญแจรหัส (Public-Private Key pair Management)[28]

การใช้งานเทคโนโลยีการเข้ารหัสแบบอสมมาตร (Asymmetric Cryptosystem) หรือเรียกอีกอย่างหนึ่งว่า การเข้ารหัสแบบกุญแจรหัสสาธารณะนี้อยู่บนพื้นฐานของความปลอดภัยของกุญแจรหัสลับหรือกุญแจรหัสส่วนตัว (Private key) หากกุญแจรหัสลับถูกเปิดเผยต่อบุคคลภายนอกหรือบุคคลที่ไม่มีอำนาจที่จะใช้ ก็จะไม่มีความปลอดภัยและความไว้วางใจในการใช้เหลืออยู่เลย ดังนั้นการบริหารคู่กุญแจรหัสที่ดี คือการรักษาคู่กุญแจรหัสให้ปลอดภัยอยู่เสมอ ซึ่งจะช่วยให้ระบบการเข้ารหัสแบบนี้สามารถใช้งานได้เป็นอย่างดีทั้งในการเข้ารหัสและการใช้เป็นลายมือชื่อดิจิตอลต่อไป

---

[28] Ibid., p. 201

2.2.3.1 การสร้างคู่กุญแจ (Key-pair Generation)[29]

เมื่อมีการสร้างคู่กุญแจรหัสขึ้นมาใหม่ ก็มีความจำเป็นที่จะต้องรักษาความปลอดภัยในการส่งคู่กุญแจรหัส โดยกุญแจรหัสส่วนตัวก็จะต้องถูกส่งไปยังระบบของผู้ถือกุญแจรหัสส่วนตัวและระบบสำรองคู่กุญแจรหัสในกรณีที่มีความจำเป็น และกุญแจรหัสสาธารณะก็จะต้องถูกส่งไปยังผู้ประกอบการรับรอง เพื่อทำการออกใบรับรองต่อไป

วิธีการสร้างคู่กุญแจรหัสมีสองแบบดังนี้

ก. ระบบผู้ถือคู่กุญแจรหัส (Key-pair holder system) คู่กุญแจรหัสจะถูกสร้างขึ้นโดยระบบที่เป็นที่เก็บรักษาและใช้งานกุญแจรหัสส่วนตัว วิธีการนี้เป็นที่นิยมทำการในกรณีที่คู่กุญแจรหัสถูกสร้างขึ้นเพื่อใช้งานเป็นลายมือชื่อดิจิตอล (Digital Signature) เพราะกุญแจรหัสส่วนตัวจะไม่เคยออกจากระบบของผู้ถือกุญแจรหัสเลย จึงมั่นใจในความปลอดภัยของกุญแจรหัส (วิธีการนี้เป็นไปตามมาตราฐาน ANSI X9.57)

ข. ระบบกลาง (Central system) คู่กุญแจรหัสจะถูกสร้างโดยระบบกลาง ซึ่งอาจเป็นระบบของผู้ประกอบการรับรอง กุญแจรหัสส่วนตัวจะถูกส่งอย่างเป็นความลับไปสู่ผู้ใช้กุญแจรหัสส่วนตัว การสร้างแบบนี้สามารถสร้างคู่กุญแจรหัสที่มีคุณภาพสูงกว่าวิธีการแรก (คุณภาพสูงกว่าในที่นี่หมายถึงมีความเป็นไปได้ในการคาดเดาคู่กุญแจรหัสน้อยกว่า) เพราะที่ระบบกลางมีทรัพยากรและวิธีการควบคุมที่แข็งแกร่ง และถ้าในกรณีที่มีความจำเป็นจะต้องทำการสำรองกุญแจรหัสไว้ที่ระบบกลาง วิธีการนี้จะอำนวยความสะดวกได้อย่างมาก

อย่างไรก็ตามในทางปฏิบัติการที่จะเลือกวิธีการสร้างคู่กุญแจรหัสแบบใดขึ้นอยู่กับวัตถุประสงค์ในการสร้างคู่กุญแจรหัส และปัจจัยอื่นๆ เช่น ในเรื่องของตัวบทกฎหมาย ข้อบังคับขององค์กร หรือประเด็นในเรื่องของความเสี่ยง เป็นต้น

2.2.3.2 การป้องกันกุญแจรหัสลับหรือกุญแจรหัสส่วนตัว (Private-key Protection)[30]

เนื่องจากการใช้เทคโนโลยีการเข้ารหัสแบบกุญแจรหัสสาธารณะนี้ ขึ้นอยู่กับความปลอดภัยของกุญแจรหัสส่วนตัวหรือกุญแจรหัสลับ (Private key) ที่ต้องมีเพียงผู้ถือกุญแจ

---

[29] Ibid., p. 202

[30] Ibid., p. 203

รหัสส่วนตัวคนเดียวเท่านั้นที่มีกุญแจรหัสดังกล่าว เนื่องจากผู้ที่มีกุญแจรหัสส่วนตัวจะถูกระบุในใบรับรองว่าเป็นผู้ถือกุญแจรหัสส่วนตัวที่เป็นคู่กุญแจรหัส (Key-pair) กับกุญแจรหัสสาธารณะ (Public key) ที่ได้ระบุในใบรับรอง เพราะฉะนั้นการป้องกันกุญแจรหัสส่วนตัวจากการเข้าถึงโดยไม่มีอำนาจจึงเป็นเรื่องที่มีความสำคัญอย่างมากในการใช้เทคโนโลยีการเข้ารหัสแบบกุญแจรหัสสาธารณะนี้

กุญแจรหัสส่วนตัวจะได้รับการปกป้องด้วยวิธีการดังนี้

ก. เก็บในอุปกรณ์ฮาร์ดแวร์หรือ token ที่สามารถป้องกันการแทรกแซง เช่น smart card หรือ PCMCIA card เป็นต้น หรือ

ข. เก็บในรูปแบบที่ได้เข้ารหัสไว้ในระบบคอมพิวเตอร์ หรือสื่อที่ใช้ในการเก็บข้อมูลทั่วไป เช่น diskette เป็นต้น

ไม่ว่าจะใช้วิธีการปกป้องอย่างไรก็ตาม การที่จะสามารถเข้าถึงกุญแจรหัสได้จะต้องมีการพิสูจน์ความถูกต้องแท้จริงของผู้ใช้อย่างน้อยหนึ่งวิธีการหรือมากกว่า โดยทั่วไปจะเป็นการใช้ Password หรือ PIN เพื่อทำการระบุตัวบุคคลผู้ใช้ จะใช้ในกรณี ข. เช่น เข้ารหัสกุญแจรหัสส่วนตัวด้วยวิธีการเข้ารหัสแบบสมมาตร (Symmetric Cryptosystem) โดยใช้กุญแจที่ได้มาจากการคำนวณ Password หรือ PIN ของเจ้าของกุญแจ ซึ่งจะมีเพียงเจ้าของกุญแจเพียงคนเดียวเช่นกันที่รู้ Password หรือ PIN ดังกล่าว เป็นต้น ส่วนการพิสูจน์ความถูกต้องแท้จริงของผู้ใช้ในกรณี ก. นั้นนิยมวิธีการตรวจสอบทางกายภาพ (Biometrics check) มากกว่า

โดยทั่วไปวิธีการ ก. จะให้ความปลอดภัยมากกว่าวิธีการ ข. แต่ก็มีค่าใช้จ่ายที่แพงกว่ามาก ส่วนวิธีการ ข. สามารถที่จะป้องกันกุญแจรหัสส่วนตัวจำนวนมากหรือข้อมูลที่มีความสำคัญได้ในโครงสร้างข้อมูลที่เรียกว่า "Digital wallet"

2.2.3.3 การปรับปรุงคู่กุญแจรหัส (Key-pair Update)[31]

ในการบริหารคู่กุญแจรหัสที่ดี จะต้องมีการ Update คู่กุญแจรหัสอยู่เสมอ โดยขึ้นอยู่กับข้อกำหนดการใช้ ช่วงเวลาที่เหมาะสม และในเงื่อนไขหรือกรณีบางอย่าง เช่น สงสัยว่ามีการรั่วไหลของกุญแจรหัสส่วนตัว (suspected compromise of a private key) เป็นต้น ทั้งในส่วนของคู่กุญแจรหัสเองการที่บุคคลอื่นไม่สามารถทราบกุญแจรหัสส่วนตัวจากการคำนวณหาจากกุญแจรหัสสาธารณะนั่น ก็เป็นเพียงชั่วระยะเวลาหนึ่งเท่านั้น เช่น 6 เดือนหรือหนึ่งปี เป็นต้น เมื่อครบกำหนดเวลาดังกล่าวก็มีความจำเป็นที่จะต้อง Update หรือทำการสร้างคู่กุญแจรหัสขึ้นใหม่

---

[31] Ibid., p. 203

2.2.3.4 การจัดการคู่กุญแจรหัสที่ต่างประเภทกัน (Management Requirements for Different Key-pair Types)[32]

โดยทั่วไป ผู้ใช้มักจะมีคู่กุญแจรหัสมากกว่าหนึ่งคู่กุญแจรหัสเสมอและยอมหมายถึงใบรับรองที่มากกว่าหนึ่งใบ ในทางเทคนิคกุญแจรหัสและใบรับรองสามารถที่จะนำมาใช้ใน Application เดียวกันได้ อย่างไรก็ตามแต่ละคู่กุญแจรหัสมีความต้องการทางด้านธุรกิจและนโยบายที่แตกต่างกันในการใช้คู่กุญแจรหัสเป็นลายมือชื่อดิจิตอลหรือใช้ในการเข้ารหัสข้อมูล

มักมีการนำการเข้ารหัสแบบกุญแจรหัสสาธารณะนี้มาใช้อย่างผิดหลักการเสมอ ถึงแม้ในทางทฤษฎีและทางปฏิบัติจะสามารถนำคู่กุญแจรหัสเดียวกันมาใช้ทั้งเป็นลายมือชื่อดิจิตอลและใช้ในการเข้ารหัสข้อมูล เมื่อพิจารณาในส่วนของการจัดการคู่กุญแจรหัสแล้ว การใช้ประโยชน์ทั้งสองด้านจากคู่กุญแจรหัสเดียวจะไม่เป็นการเหมาะสมนัก

ข้อจำกัดในการจัดการกับคู่กุญแจรหัสทั้งสองประเภท ประการแรกข้อจำกัดสำหรับการจัดการกับคู่กุญแจรหัสที่ใช้ในการลงลายมือชื่อดิจิตอล มีดังนี้

ก. กุญแจรหัสส่วนตัวที่ใช้ในการลงลายมือชื่อดิจิตอลนั้น จะต้องถูกเก็บรักษาอย่างดีตลอดอายุการใช้งาน เพื่อให้เป็นไปตามข้อสันนิษฐานเบื้องต้นของการลงลายมือชื่อดิจิตอล กุญแจรหัสส่วนตัวจะต้องถูกสร้าง ใช้ และทำลายในระบบความปลอดภัยเดียวกัน

ข. กุญแจรหัสส่วนตัวสำหรับลายมือชื่อดิจิตอลไม่มีความจำเป็นที่จะต้องทำการสำรองกุญแจไว้ในกรณีที่กุญแจรหัสส่วนตัวเกิดสูญหาย เพราะคู่กุญแจรหัสใหม่สามารถสร้างขึ้นอย่างง่ายดาย ทั้งการสำรองกุญแจยังไม่เป็นไปตามข้อ ก. อีกด้วย

ค. การเก็บกุญแจรหัสส่วนตัวภายหลังหมดอายุการใช้งานแล้วไม่มีความจำเป็นสำหรับในกรณีเพื่อลายมือชื่อดิจิตอล เพราะกุญแจรหัสส่วนตัวควรจะถูกทำลายอย่างสิ้นเชิงเมื่อหมดอายุการใช้งาน เพื่อป้องกันมิให้สามารถนำไปใช้เพื่อทำการหลอกลวงผู้อื่นในขณะที่อายุการใช้งานของกุญแจเพิ่งสิ้นสุดลงไม่นาน (การประทับเวลาในขณะลงลายมือชื่อจะเป็นวิธีการหนึ่งที่ช่วยลดความเสี่ยงในกรณีนี้ได้)

ง. ในส่วนกุญแจรหัสสาธารณะสำหรับการตรวจสอบลายมือชื่อดิจิตอลและใบรับรองมีความจำเป็นที่จะต้องทำการเก็บรักษาไว้ถึงแม้คู่กุญแจรหัสจะหมดอายุการใช้งานแล้วก็ตาม เพื่อทำการตรวจสอบ

---

[32] Ibid., p. 204

ลายมือชื่อดิจิตอลเก่าที่ได้ทำไว้ในกรณีจำเป็นภายหลัง เช่น เมื่อมีการฟ้องร้องคดีต่อศาล เป็นต้น

ในส่วนที่สอง ข้อจำกัดของคู่กุญแจรหัสที่ใช้เพื่อการเข้ารหัส มีดังนี้

จ. กุญแจรหัสส่วนตัวสำหรับการเข้ารหัสมีความจำเป็นที่จะต้องทำการสำรองหรือทำการเก็บรักษาไว้ เพราะเป็นวิธีการเดียวที่จะเข้าถึงข้อมูลที่ได้ทำการเข้ารหัสไว้ ในกรณีที่อุปกรณ์ที่ใช้เก็บกุญแจรหัสส่วนตัวสูญหายหรือลืม password ที่ใช้ในการเข้าถึงกุญแจรหัสสาธารณะจะเป็นความเสียหายอย่างมากที่จะสูญเสียข้อมูลที่ทำการเข้ารหัสไว้ด้วย หรือในกรณีที่ต้องการเข้าถึงข้อมูลที่ได้ทำการเข้ารหัสในภายหลัง

ฉ. เมื่อหมดอายุการใช้งานแล้ว กุญแจรหัสส่วนตัวที่ใช้สำหรับการเข้ารหัส ไม่มีความจำเป็นที่จะต้องทำลายทิ้งทั้งหมด ทั้งในกรณีตามข้อ จ. กุญแจรหัสส่วนตัวจำเป็นที่จะต้องเก็บรักษาไว้

ช. เมื่อพิจารณาตามวิธีการของการเข้ารหัส (Algorithm) กุญแจรหัสสาธารณะไม่มีความจำเป็นที่จะต้องทำการสำรองหรือเก็บรักษาไว้ เพราะในกรณีที่กุญแจรหัสสาธารณะสูญหายไป การสร้างคู่กุญแจใหม่จะเป็นวิธีการที่ดีและง่ายกว่า

จากข้อจำกัดดังกล่าวข้างต้น จะเห็นได้ว่ามีส่วนที่ขัดแย้งกันอย่างมาก ดังนั้นจึงไม่สามารถที่จะใช้คู่กุญแจรหัสเดียวกันทั้งในการลงลายมือชื่อดิจิตอลและการเข้ารหัส ทั้งยังมีเหตุผลอื่นๆ ที่สนับสนุนไม่ให้มีการใช้คู่กุญแจรหัสเดียวกันทั้งสองด้านดังนี้

1. การใช้คู่กุญแจรหัสเพื่อการเข้ารหัส จะมีข้อจำกัดเพื่อการควบคุมการใช้ที่เข้มงวดกว่าการใช้เพื่อลายมือชื่อดิจิตอล เช่น ความยาวของคู่กุญแจรหัสที่ใช้ในการเข้ารหัสข้อมูลจะถูกจำกัดความยาวให้สั้นกว่าที่อนุญาตให้ใช้กับลายมือชื่อดิจิตอล ตามแต่นโยบายในเรื่องการเข้ารหัสของประเทศนั้นๆ ดังนั้นการใช้คู่กุญแจรหัสเดียวกันทั้งสองส่วนจะเป็นการจำกัดความยาวของคู่กุญแจรหัส ซึ่งส่งผลให้เป็นการลดความแข็งแกร่งของกระบวนการลายมือชื่อดิจิตอลไปด้วย
2. คู่กุญแจรหัสทั้งสองอาจจำเป็นต้องมีช่วงอายุการใช้งานที่แตกต่างกัน การใช้คู่กุญแจรหัสเดียวกันทำให้ทำให้ต้อง Update คู่กุญแจรหัลบ่อยเพราะอายุการใช้งานของคู่กุญแจรหัสในการเข้ารหัสมีช่วงเวลาที่สั้นกว่า (เนื่องมาจากถูกจำกัดในเรื่องความยาวของกุญแจรหัส)

และยังต้องมีการสำรองและเก็บรักษาคู่กุญแจรหัสทั้งสองกุญแจรหัสตามเหตุผลที่ได้กล่าวข้างต้น ทำให้มีความยุ่งยากมากขึ้น

3. ในการเข้ารหัสข้อมูล รัฐมักจะมีการกำหนดให้มีการทำระบบ Key Escrow หรือ Key Recovery เพื่อเอาไว้ใช้ในการถอดรหัสของผู้ต้องสงสัยหรืออาชญกรในกรณีของความมั่นคงของประเทศ แต่เมื่อใช้คู่กุญแจรหัสเดียวกันในการลงลายมือชื่อดิจิตอลด้วย จะมีผลทำให้รัฐสามารถที่จะปลอมแปลงลายมือชื่อของประชาชนได้ด้วยเช่นกัน กุญแจรหัสส่วนตัวที่ใช้ในการลงลายมือชื่อดิจิตอลจึงไม่ควรได้รับการเปิดเผยต่อรัฐ

จากเหตุผลดังกล่าวข้างต้น จึงไม่ควรที่จะนำคู่กุญแจรหัสเดียวกันมาใช้ทั้งการลงลายมือชื่อดิจิตอลและการเข้ารหัส อย่างไรก็ตามเหตุผลเหล่านี้ได้ถูกมองข้ามไปในการออกแบบระบบของการ PEM และ PGP ซึ่งเป็นระบบการส่งข้อความอิเล็กทรอนิกส์ที่ได้รับความนิยมอย่างสูงในปัจจุบัน

2.2.4 ระบบการฝากกุญแจรหัส (Key Escrow) และระบบการกู้กุญแจรหัส (Key Recovery)

ระบบการฝากกุญแจรหัส (Key Escrow) และระบบการกู้กุญแจรหัส (Key Recovery) คือระบบการเข้ารหัสที่มีความสามารถในการทำการถอดรหัสสำรองที่จะอนุญาตให้บุคคลที่มีอำนาจหรือขบวนการที่เรียกว่าการเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย (ไม่ว่าจะเป็นผู้ใช้ เจ้าหน้าที่ในหน่วยงาน หรือเจ้าพนักงานของรัฐ) ในเงื่อนไขที่กำหนดไว้เฉพาะ ซึ่งจะสามารถถอดรหัส Ciphertext โดยความช่วยเหลือของข้อมูลที่ได้จากบุคคลที่สามารถที่ไว้วางใจได้ที่มีวิธีการกู้ข้อมูลพิเศษ

การเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยใช้ระบบการเก็บกุญแจรหัส (Key Archiving) หมายถึง การที่ผู้ใช้เทคโนโลยีเข้ารหัสดำเนินการทำสำเนากุญแจรหัสส่วนตัวหรือกุญแจรหัสลับของตนแล้วจัดเก็บไว้ที่ใดที่หนึ่ง ไม่ว่าเพราะการถูกกฎหมายกำหนดหรือด้วยความต้องการของตนเอง ตัวอย่างของระบบการเก็บกุญแจรหัสก็คือระบบฝากกุญแจรหัส (Key Escrow) ซึ่งจะกำหนดให้เจ้าหน้าที่ของรัฐหรือบุคคลที่รัฐแต่งตั้ง เช่น ผู้ประกอบการรับรองของผู้ใช้กุญแจรหัสทำการเก็บสำเนากุญแจรหัสส่วนตัวไว้ เพื่อใช้ในการถอดรหัสในกรณีที่รับต้องการตรวจสอบหรือเจ้าของกุญแจต้องการ

ส่วนการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยใช้ระบบการกู้กุญแจ (Key Recovery) เป็นวิธีการที่ใช้กุญแจรหัสสาธารณะของหน่วยงานกู้กุญแจเข้ารหัสกุญแจรหัสลับของผู้ใช้แล้วผู้ใช้ทำการผนวกกุญแจรหัสส่วนตัวที่ทำการเข้ารหัสดังกล่าวลงไปในข้อมูลที่ตนทำการเข้า

รหัสด้วย เมื่อรัฐต้องการตรวจสอบหรือผู้ใช้ (ที่เป็นเจ้าของกุญแจรหัสส่วนตัว) ต้องการถอดรหัสข้อมูลดังกล่าว เนื่องจากได้ทำกุญแจรหัสส่วนตัวของตนสูญหาย ก็จะสามารถใช้กุญแจรหัสส่วนตัวของหน่วยงานกู้กุญแจทำการถอดรหัสกุญแจรหัสส่วนตัวที่ได้ผนวกกับข้อมูลไว้ แล้วใช้กุญแจรหัสส่วนตัวที่ได้มาทำการถอดรหัสข้อมูลอีกที่หนึ่ง

เมื่อข้อมูลต่างๆ ถูกเก็บอยู่ในรูปของการเข้ารหัส และกุญแจรหัสที่ต้องใช้ในการถอดรหัสเกิดสูญหายไป ย่อมหมายความว่าจะสูญเสียข้อมูลที่อยู่ในรูปของการเข้ารหัสนั้นไปด้วย ระบบฝากกุญแจรหัสหรือการกู้กุญแจรหัสพิเศษนี้จึงมีความจำเป็นใน 3 กรณีดังนี้

1. เมื่อกุญแจรหัส (Key) เกิดสูญหายไปจากผู้ถือกุญแจโดยอุบัติเหตุ หรือในกรณีที่ผู้ถือกุญแจรหัสเสียชีวิต เช่น แผ่นบันทึกข้อมูลที่ทำการบันทึกกุญแจรหัสไว้เกิดสูญหาย จากการที่ผู้ถือกุญแจรหัสหลงลืม หรือตัวแผ่นบันทึกได้รับความเสียหายจากกรณีใดๆ ที่ทำให้ไม่สามารถใช้งานได้อีก ในกรณีนี้ผู้ถือกุญแจรหัสย่อมต้องการที่กุญแจรหัสกู้ข้อมูลพิเศษนี้ เพื่อให้สามารถเข้าไปใช้ข้อมูลที่ทำการเข้ารหัสไว้โดยกุญแจที่สูญหายไปได้ หรือในกรณีผู้ถือกุญแจรหัสเสียชีวิต ทายาทหรือผู้จัดการมรดกย่อมต้องการระบบกุญแจกู้ข้อมูลพิเศษนี้เพื่อทำการเข้าถึงข้อมูลของผู้ตาย เป็นต้น
2. ในกรณีของลูกจ้างขององค์กรหรือบริษัทต่างๆ เมื่อลูกจ้างคนดังกล่าวได้ลาออกไปจากบริษัทและไม่ได้ส่งคืนกุญแจรหัสที่ใช้เข้ารหัสข้อมูลต่างๆ ของบริษัท หรือลูกจ้างคนดังกล่าวเสียชีวิต องค์กรหรือบริษัทย่อมมีความจำเป็นที่จะต้องใช้ระบบกุญแจกู้ข้อมูลพิเศษนี้ เพื่อเข้าถึงข้อมูลขององค์กรหรือบริษัทดังกล่าว
3. ในกรณีที่มีกฎหมายบังคับ เช่นในกรณีของการสืบสวนสอบสวนหน่วยงานที่เกี่ยวข้องย่อมต้องการระบบฝากกุญแจหรือการกู้กุญแจรหัสพิเศษนี้เพื่อประโยชน์ในการสืบสวนสอบสวน ใช้ตรวจสอบข้อมูลของผู้ที่ตกเป็นผู้ต้องสงสัย หรือของจำเลยในชั้นศาล หรือในกรณีเพื่อความมั่นคงของประเทศ เป็นต้น

2.3 ลายมือชื่อดิจิตอล (Digital Signature) และโครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะ

ลายมือชื่อดิจิตอลคือเทคนิคในทางอิเล็กทรอนิกส์ที่นำเอาเทคโนโลยีในการเข้ารหัสแบบอสมมาตรมาประยุกต์ใช้แทนการลงลายมือชื่อในกระดาษ ซึ่งลายมือชื่อดิจิตอลถือเป็นลายมือชื่ออิเล็กทรอนิกส์ชนิดหนึ่ง ซึ่งการใช้ลายมือชื่อดิจิตอลจำเป็นที่จะต้องมีการว่างโครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะ เพื่อให้ลายมือชื่อดิจิตอลมีความน่าเชื่อถือและสามารถไว้วางใจได้

2.3.1 ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature)

ลายมือชื่ออิเล็กทรอนิกส์เป็นผลของการพัฒนาเทคโนโลยีเพื่อหาวิธีการที่จะนำมาใช้ในการแสดงความเป็นเจ้าของหรือระบุตัวบุคคล รวมทั้งแสดงความเห็นชอบของผู้ลงลายมือชื่อต่อข้อความที่ทำการติดต่อสื่อสารกันแทนการลงลายมือชื่อในการติดต่อสื่อสารที่ใช้กระดาษเป็นพื้นฐาน เช่น การลงท้ายเอกสารต่างๆ การลงนามท้ายจดหมาย หรือการลงนามในหนังสือสัญญาหรือธุรกรรมต่างๆ เป็นต้น

เทคโนโลยีลายมือชื่ออิเล็กทรอนิกส์แต่ละประเภทมีความแตกต่างกันในเรื่องของทางเทคนิคและวิธีการในการใช้หรือประยุกต์ใช้ แต่มีจุดมุ่งหมายเดียวกัน คือ ใช้เป็นสัญลักษณ์ที่สร้างขึ้นโดยผู้ลงลายมือชื่อและแสดงถึงผู้ที่เป็นทำการลงลายมือชื่ออิเล็กทรอนิกส์นั้น การลงลายมือชื่อทั่วไป (Hand-written Signature) ใช้กระดาษกับปากกา หรือใช้หัวแม่มือกับหมึกประทับลงบนกระดาษ[33] แต่ลายมือชื่ออิเล็กทรอนิกส์ใช้วิธีการทางเทคโนโลยี เพื่อให้ใช้งานได้ง่าย เหมาะสมกับสื่ออิเล็กทรอนิกส์ และสามารถทำการตรวจสอบถึงบุคคลผู้ทำการลงลายมือชื่ออิเล็กทรอนิกส์ได้

ลายมือชื่ออิเล็กทรอนิกส์เป็นลายมือชื่อที่ได้สร้างขึ้นมาด้วยวิธีการทางอิเล็กทรอนิกส์ ซึ่งอาจจะใช้เทคโนโลยีชีวมิติ (Biometrics) ต่างๆ การใช้รหัสผ่าน (Password) หมายเลขประจำตัวบุคคล (PIN) หรือการนำเทคโนโลยีการเข้ารหัสมาประยุกต์ใช้เป็นลายมือชื่อดิจิตอล เพื่อใช้เป็นข้อมูลหรือกลุ่มข้อมูลที่นำไปใช้ในการตรวจสอบความถูกต้องแท้จริงในการติดต่อสื่อสารที่ใช้สื่ออิเล็กทรอนิกส์เป็นพื้นฐาน

2.3.2 ลายมือชื่อดิจิตอล (Digital Signature)

ลายมือชื่ออิเล็กทรอนิกส์เป็นคำที่มีความหมายกว้าง ครอบคลุมถึงวิธีการต่างๆ ทางอิเล็กทรอนิกส์ที่นำมาใช้แทนการลงลายมือชื่อ (Hand-written Signature) ในกระดาษเพื่อระบุตัวบุคคลผู้ลงลายมือชื่อหรือตัวบุคคลผู้ทำธุรกรรมอิเล็กทรอนิกส์ ส่วนลายมือชื่อดิจิตอล คือ ลายมือชื่ออิเล็กทรอนิกส์ชนิดหนึ่ง ที่ถูกสร้างขึ้นเพื่อใช้ตรวจสอบผู้จัดทำข้อมูลและความสมบูรณ์ของข้อมูลที่ถูกส่งผ่านทางเครือข่ายอิเล็กทรอนิกส์ กระบวนการที่ทำให้เกิดความเชื่อมั่นในแหล่งกำเนิดและความสมบูรณ์ของข้อมูลดังกล่าวนี้เรียกว่า “การพิสูจน์ความถูกต้องแท้จริง” (Authentication) ซึ่งสามารถแยกได้เป็นการตรวจสอบความถูกต้องแท้จริงของบุคคลผู้ใช้ระบบ (Authentication of Users) และการรักษาความถูกต้องของข้อมูล (Integrity) ดูรายละเอียดได้ในหัวข้อ 2.1.1.1 และหัวข้อ 2.1.1.2

---

[33] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 9

ลายมือชื่อดิจิตอล (Digital Signature) คือ กลุ่ม (Set) ของตัวเลข (Alphanumeric Characters) ที่เกิดจากการเข้ารหัสทางคณิตศาสตร์ในข้อมูลอิเล็กทรอนิกส์โดยคอมพิวเตอร์ [34]

ลายมือชื่อดิจิตอล หมายถึง ค่าทางคณิตศาสตร์ (Numerical Value) ที่ประทับอยู่ท้ายข้อมูล โดยใช้วิธีการทางคณิตศาสตร์นำข้อมูลมาทำการเข้ารหัส (Encrypt) ด้วยกุญแจรหัสส่วนตัว (Private Key) ที่เป็นความลับและรู้เฉพาะผู้ที่เป็นเจ้าของกุญแจรหัสส่วนตัว โดยที่กุญแจรหัสส่วนตัวดังกล่าวมีความเชื่อมโยงทางคณิตศาสตร์กับกุญแจรหัสสาธารณะ (Public Key) ซึ่งเป็นกุญแจที่สามารถทำการถอดรหัส (Decrypt) และใช้ยืนยันว่าลายมือชื่อดังกล่าวเป็นของบุคคลที่อ้างถึงจริง ทั้งนี้ผู้ที่ถือกุญแจรหัสสาธารณะจะไม่สามารถสืบค้นในทางตรรกถึงกุญแจรหัสส่วนตัวได้ หรือต้องใช้เวลาในการค้นหาที่นานจนไม่เกิดประโยชน์ที่จะทำการค้นหา

<Signed SigID=1>

Promissory Note

I, Mary Smith, promise to pay to the order of First Western Bank five thousand dollars and no cents ($5,000) on or before June 10, 1998, with interest at the rate of fifteen per cent (15%) per annum.

Mary Smith, Maker

</Signed>

<Signature SigID=1 PsnID=smith082>

2AB3764578CC18946A29870F40198B240CD2302B2349802DE002342B

212990BA5330249C1D20774C1622D39</Signature>

แผนภูมิ 2-5[35] : ตัวอย่างของเอกสารอิเล็กทรอนิกส์ที่ได้มีการลงลายมือชื่อดิจิตอล

---

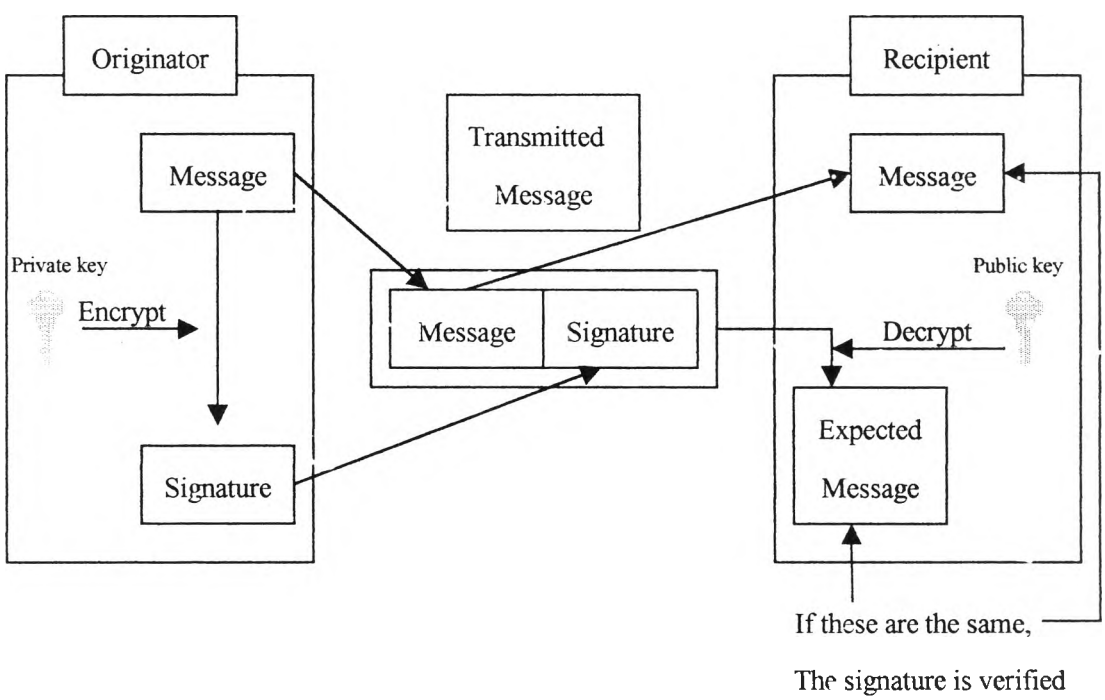
[34] B. Schneier, Applied Cryptography, (USA : John Wiley & Sons Inc., 1994) อ้างถึงใน ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, เอกสารประกอบการสัมมนาหัวข้อปัญหาข้อกฎหมายที่เกี่ยวกับการพาณิชย์อิเล็กทรอนิกส์ในสังคมยุคเทคโนโลยีสารสนเทศ, หน้า 37

[35] ที่มา : Information Security Committee, Electronic Commerce Division, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, www.abanet.org/scitech/ec/isc.dsgfree.html, (A.B.A. SEC. SCI. & TECH :1996), p.14

ลายมือชื่อดิจิตอลถูกคิดค้นขึ้นเพื่อทำหน้าที่เหมือนกับการลงลายมือชื่อในเอกสารที่เป็นกระดาษต่างๆ[36] แต่ไม่ใช่การนำรูปภาพของลายมือชื่อ (Hand-written Signature) ไปแปะหรือวางไว้บนเอกสารอิเล็กทรอนิกส์ แต่เป็นการนำเอาระบบการเข้ารหัสแบบอสมมาตร (Asymmetric Cryptosystem) มาประยุกต์ใช้ โดยนำเอาวิธีการเข้ารหัสแบบอสมมาตรเพื่อการพิสูจน์ความถูกต้องแท้จริง (Authentication) มาใช้ดังนี้

2.3.2.1 RSA Digital Signature

เป็นการนำการเข้ารหัสแบบอสมมาตร RSA Algorithm มาใช้ในการเข้ารหัสหรือถอดรหัส เพื่อทำการลงลายมือชื่อดิจิตอล โดยผู้ส่งจะนำกุญแจรหัสส่วนตัวของตน (Originator's Private key) มาใช้เข้ารหัสข้อความ (plaintext message) ที่จะส่ง จากนั้นจะส่งข้อความต้นฉบับ (plaintext message) ไปพร้อมกับข้อความที่ถูกเข้ารหัส (ciphertext message) ผู้รับ (Recipient) ก็จะนำกุญแจรหัสสาธารณะของผู้ส่ง (Originator's Public key) มาทำการถอดรหัส ciphertext message ที่ส่งมาด้วยแล้วนำมาเปรียบเทียบกับข้อความที่ส่งมา ถ้าเหมือนกันผู้รับก็จะมั่นใจได้ว่า ข้อความดังกล่าวส่งมาจากผู้ส่งที่แท้จริง และข้อความก็ไม่ถูกเปลี่ยนแปลงระหว่างทางที่ส่งมา



แผนภูมิ 2-6[37] : โครงสร้างของ RSA Digital Signature

---

[36] David L. Gripman, Id., p.777

[37] ที่มา : Warwick Ford and Michael S. Baum, Id., p. 113

การเข้ารหัสข้อมูลทั้งหมดที่จะส่งไปหรือข้อมูลยาวๆ นั้นค่อนข้างจะเสียเวลามาก เนื่องมาจากขั้นตอนการเข้ารหัสต้องใช้การคำนวณที่ยุ่งยากซับซ้อน จึงมีการสร้างขั้นตอนที่สามารถคำนวณได้อย่างรวดเร็ว เพื่อเปลี่ยนข้อความทั้งหมดให้เหลือเพียงข้อความสั้นๆ ที่เป็นเอกลักษณ์เฉพาะเพื่อเป็นตัวแทนของข้อความทั้งหมด (หรือที่เรียกว่า "Fingerprint" ของข้อมูลหรือข้อความทั้งหมด)[38] โดยนำข้อความหรือข้อมูลที่จะส่งมาทำการย่อย (digest) แล้วจึงนำผลที่ได้มาทำการลงลายมือชื่อ (ขั้นตอนในการย่อยข้อมูลดังกล่าวเรียกว่า Hash Function) ซึ่งมีขั้นตอนในการลงลายมือชื่อดิจิตอลดังนี้

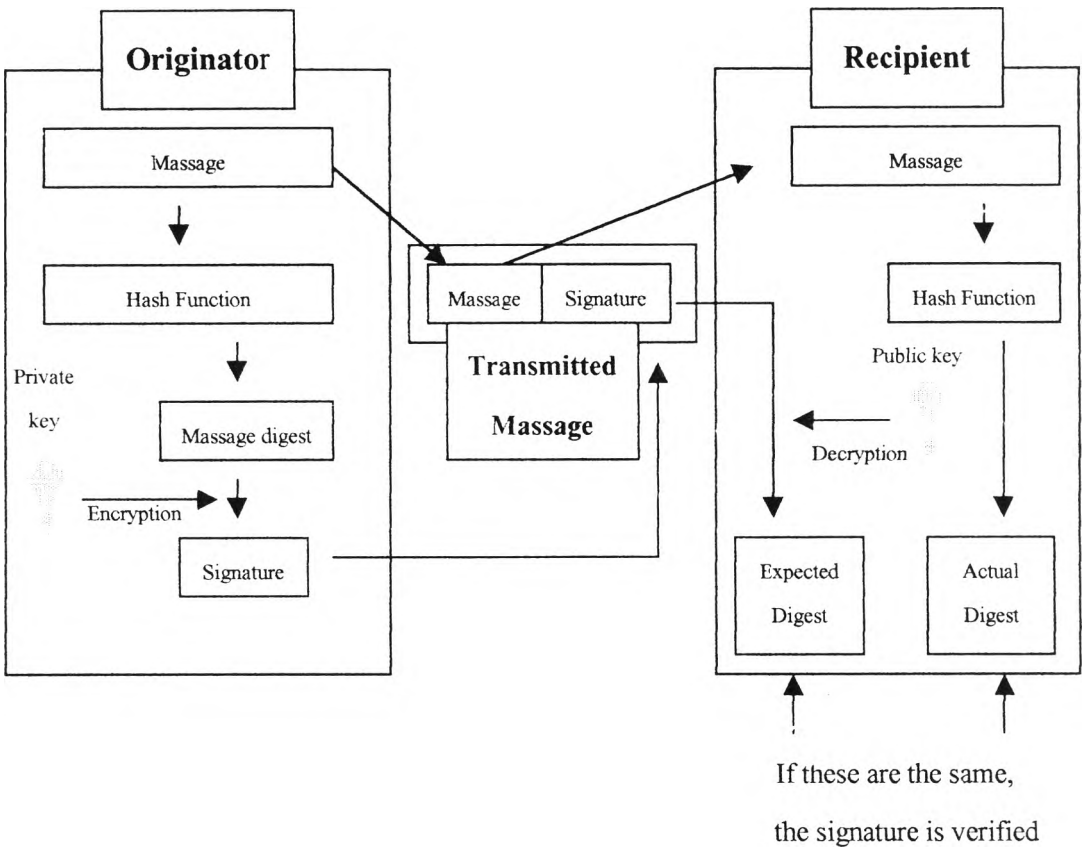
1. ผู้ส่ง (Originator) สร้างหรือได้รับคู่กุญแจ ซึ่งประกอบด้วยกุญแจรหัสส่วนตัว (private key or secret key) ที่เกี่ยวเนื่องทางตรรกะกับกุญแจรหัสสาธารณะ (public key) ของตน
2. ผู้ส่งตระเตรียมข้อมูลที่จะส่งทางเครือข่ายอิเล็กทรอนิกส์ (โปรดดูแผนภูมิ 2-7 ประกอบ)
3. ผู้ส่งทำการย่อยข้อมูล (Message digest) โดยใช้สูตรทางคณิตศาสตร์ (Hash Function) จะได้ผลลัพธ์เป็น Hash Value
4. ผู้ส่งจะทำการเข้ารหัส (Encryption) ข้อมูลที่ได้ทำการย่อย (digest) แล้ว โดยใช้กุญแจรหัสส่วนตัว (private key) ซึ่งกุญแจรหัสส่วนตัวดังกล่าวจะได้รับการผนวกเข้ากับข้อมูลที่ได้ย่อยแล้วโดยใช้สูตรทางคณิตศาสตร์ (Mathematical Algorithm) ได้เป็นกลุ่มของตัวเลขและตัวอักษรของมากลุ่มหนึ่ง ซึ่งถือว่าเป็นลายมือชื่อดิจิตอล
5. ผู้ส่งทำการผนึกหรือแนบลายมือชื่อดิจิตอลเข้ากับข้อความที่จะทำการส่ง
6. ผู้ส่งทำการส่งข้อความพร้อมลายมือชื่อดิจิตอล (โดยที่ข้อความพร้อมลายมือชื่อดิจิตอลจะได้รับการเข้ารหัสอีกครั้งเพื่อรักษาความลับหรือไม่ก็ตาม) ไปยังผู้รับโดยทางเครือข่ายอิเล็กทรอนิกส์ที่ต้องการ
7. เมื่อผู้รับได้รับข้อความที่ส่งมา ก็จะนำกุญแจรหัสสาธารณะ (public key) ของผู้ส่งมาทำการถอดรหัส (Decryption) ลายมือชื่อดิจิตอลของผู้ส่งที่ได้แนบมาพร้อมกับข้อความ ถ้าถอดรหัสได้ก็สรุปได้ว่าส่งมาจากผู้ส่ง (Originator) ที่อ้างถึงจริง เพราะเมื่อใช้กุญแจรหัสสาธารณะของผู้ส่งทำการถอดรหัสแล้วสามารถถอดรหัสได้ ก็เนื่องจากข้อ

---

[38] กฤษณะ ช่างกล่อม, (ร่าง) รายงานการศึกษาวิจัยเรื่องกฎหมายพาณิชย์อิเล็กทรอนิกส์, หน้า 31

ความนั้นถูกเข้ารหัสมาด้วยกุญแจรหัสส่วนตัวของผู้ส่งที่เป็นคู่กุญแจรหัสกันเท่านั้น ถ้าไม่สามารถถอดรหัสได้ก็สรุปได้ว่ามีผู้อื่นแอบอ้างชื่อผู้ส่งส่งข้อความมา

8. ผู้รับทำการย่อยข้อมูลโดยใช้สูตรทางคณิตศาสตร์ (Hash Function Algorithm) สูตรเดียวกันกับของผู้ส่ง
9. ผู้รับทำการเปรียบเทียบข้อมูลที่ได้รับการย่อยในข้อ 8. กับผลที่ได้จากการถอดรหัสในข้อ 7. (ในกรณีที่ถอดรหัสได้) ซึ่งก็คือการเปรียบเทียบ hash value ทั้งสองค่า ถ้าเหมือนกันก็แสดงว่าข้อความที่ส่งมาไม่ได้ถูกเปลี่ยนแปลงแก้ไขภายหลังการลงนาม เพราะข้อความเดียวกันเมื่อนำมาทำการย่อยข้อมูลโดยใช้สูตรทางคณิตศาสตร์ (Hash Function) เดียวกัน ย่อมได้รับผลรับที่เหมือนกัน ถ้าหากข้อความที่ส่งมาถูกแก้ไขแค่เพียงหนึ่งบิต (bit) เมื่อทำการย่อยข้อมูลก็จะได้รับผลจากการย่อยข้อมูลที่แตกต่างจากผลที่ได้รับจากข้อ 7. อย่างชัดเจน
10. ผู้รับสามารถจะร้องขอใบรับรอง (certificate) จากผู้ประกอบการรับรอง (Certification Authority) ซึ่งใบรับรองดังกล่าวจะมีข้อมูลที่ต่างๆ ที่จำเป็นในการยืนยันว่าลายมือชื่อดิจิตอลที่ส่งแนบมากับข้อมูลนั้น เป็นของผู้ที่ลงนามจริง



แผนภูมิ 2-7 [39] : โครงสร้างของ RSA Digital Signature แบบที่ใช้ Hash Function

วิธีการในการลงลายมือชื่อดิจิตอลแบบนี้ เป็นวิธีการมาตรฐานในการลงลายมือชื่อดิจิตอลที่ใช้อยู่ในปัจจุบัน

2.3.2.2 Hash Function

Hash Function คือ วิธีการคำนวณในทางคณิตศาสตร์ที่สร้างตัวแทนดิจิตอล (Digital representation) หรือ "Fingerprint" ในรูปของค่า Hash Value หรือ Hash Result ของข้อมูล ที่มีขนาดความยาวตามที่กำหนดไว้ ซึ่งจะสั้นกว่าข้อมูลเดิมแต่มีเอกลักษณ์เฉพาะตัว ถ้าข้อมูลเดิมถูกเปลี่ยนแปลงแม้เพียงเล็กน้อย (แม้เพียง bit เดียว) เมื่อนำมาทำการ Hash Function ด้วยวิธีการเดิมก็จะได้ค่า Hash Value หรือ Hash Result ที่แตกต่างจากเดิม Hash Function ที่มีความปลอดภัยสูงเรียกกันว่า "one-way hash function" ซึ่งเป็นฟังก์ชั่นแบบทางเดียว (one-way function) โดยมีแนวความคิดที่ว่า เป็นการง่ายที่จะนำข้อมูลมาประมวลโดยสูตรทางคณิตศาสตร์เพื่อหาค่า Hash Value หรือ Hash Result ของข้อมูล แต่ไม่สามารถนำค่า Hash Value หรือ Hash Result มา

---

[39] ที่มา : Warwick Ford and Michael S. Baum, Id., p. 114

ประมวลผลกลับเพื่อหาข้อมูลเดิมได้ โดยใช้แนวความคิดของสมการทางคณิตศาสตร์ที่ว่า $y = f(x)$ นั้นเป็นการง่ายที่จะหาค่า y เมื่อให้ค่า x มา แต่เป็นการยากที่จะหาค่า x เมื่อให้ค่า y มา[40]

Hash Function ที่ใช้ใน Digital Signature เป็นฟังก์ชั่นแบบทางเดียว (one-way hash function) คือ Hash Function ที่ไม่สามารถเป็นไปได้ในทางการคำนวณ (Computationally Infeasible) ที่จะได้รับข้อมูลต้นฉบับจากการนำค่า Hash Value หรือ Hash Result มาคำนวณ ซึ่ง one-way hash function จะต้องมีคุณสมบัติดังนี้

1. จะต้องเป็นฟังก์ชั่นแบบทางเดียวจริงๆ คือไม่สามารถแปลง Hash Value หรือ Hash Result ที่เกิดจาก Hash Function กลับไปเป็นข้อมูลที่ใส่เข้าไป (input message, original message) ได้
2. ต้องไม่สามารถได้ผลลัพธ์ (hash value) 2 ผลลัพธ์ จากข้อมูลเดียวกันที่ใส่เข้าไป (input message) ได้
3. ต้องไม่สามารถได้ผลลัพธ์เดียวกันจากข้อมูลที่ต่างกันที่ถูกป้อนเข้าไปใน Hash Function เดียวกัน

ข้อบกพร่องของ Hash Function ในคุณสมบัติเหล่านี้จะส่งผลกลายเป็นจุดอ่อนในการใช้ลายมือชื่อดิจิตอล เพราะถ้าผู้ไม่ประสงค์ดี (Imposter) สามารถที่จะทำให้ข้อความที่ถูกแก้ไขมีค่า hash value ค่าเดียวกันกับข้อมูลเดิมที่ไม่ได้ถูกแก้ไข จะส่งผลให้ไม่สามารถทำการตรวจพบการแก้ไขดังกล่าวได้เลย เพราะฉะนั้นการใช้ Hash Function ที่ดีจึงเป็นเรื่องที่มีความสำคัญอย่างมากในการใช้ลายมือชื่อดิจิตอล

2.3.2.3 มาตรฐาน Digital Signature Algorithm ของสหรัฐอเมริกา

ในเดือนสิงหาคม ค.ศ.1991 สถาบันมาตรฐานและเทคโนโลยีของสหรัฐอเมริกา (U.S. National Institute of Standard and Technology, NIST) ได้ออกประกาศเพื่อเสนอมาตรฐานของลายมือชื่อดิจิตอล (Digital Signature Standard, DSS) ที่เรียกว่า Digital Signature Algorithm (DSA) ซึ่งต่อมาได้ถูกแก้ไขตามความเห็นของสาธารณชน แล้วถูกตีพิมพ์เผยแพร่ในรูปของ Federal Information Processing Standard (FIPS) ในปี ค.ศ.1994

โครงสร้างของ DSA นี้แตกต่างจาก RSA เพียงเล็กน้อยเท่านั้น โดยกระบวนการจะสร้างข้อมูลที่ถูกย่อย (digest) ซึ่งเกิดมาจาก Hash Function แบบเดียวกับ RSA แล้วนำผลลัพธ์มาทำการเข้ารหัสแบบ DSA จะได้ลายมือชื่อดิจิตอลที่มีขนาด 160 บิต (bit) จากนั้นแนบส่งไปกับข้อความที่ต้องการส่ง ผู้รับจะนำข้อความที่ได้มาทำการย่อย แล้วนำ Message digest ที่ได้

---

[40] Warwick Ford and Michael S. Baum, Id., p.115

กับลายมือชื่อดิจิตอลที่ส่งมาและกุญแจรหัสสาธารณะของผู้ส่ง มาเข้ากระบวนการตรวจสอบของ DSA ซึ่งขบวนการนี้จะให้ผลลัพธ์มาทันทีว่าเป็นลายมือชื่อที่ถูกต้องหรือไม่

ข้อแตกต่างที่น่าสนใจก็คือ DSA นี้ถูกสร้างขึ้นเพื่อลายมือชื่อดิจิตอลเท่านั้น ไม่สามารถนำไปเข้ารหัสข้อมูลในแบบในต้องการรักษาความลับของข้อความ ซึ่งส่งผลให้ DSA มีข้อได้เปรียบ RSA ในเรื่องเกี่ยวกับการส่งออก เนื่องมาจากเทคโนโลยีการเข้ารหัสเป็นเทคโนโลยีที่ถูกจำกัดการส่งออกในประเทศสหรัฐอเมริกา

2.3.2.4 Elliptic Curve Digital Signature Systems*

เทคโนโลยีใหม่ที่เรียกว่า 'Elliptic curve cryptosystems" ได้กลายเป็นเทคโนโลยีที่ได้รับการยอมรับมากขึ้นสำหรับระบบลายมือชื่อดิจิตอล โดยพื้นฐานจะเหมือนกันกับ RSA และ DSA แต่การใช้งาน Elliptic curve cryptosystems จะสามารถสร้างระบบการเข้ารหัสที่แข็งแกร่งขึ้นได้ โดยใช้ความยาวของกุญแจ (ชุดตัวเลขหรืออักขระ) ที่สั้นกว่า RSA และ DSA รวมทั้งส่วนระบบสนับสนุนของ Elliptic curve cryptosystems ก็มีประสิทธิภาพมากกว่า ดังนั้นการใช้ elliptic curve cryptosystems จะทำให้การใช้ลายมือชื่อดิจิตอลสามารถสร้างและตรวจสอบลายมือชื่อได้รวดเร็วกว่าทั้ง RSA และ DSA ทั้งยังสามารถใช้งานได้ดีกับระบบประมวลที่มีคุณภาพไม่สูงมากนัก เช่น บัตรอัจฉริยะ (smart card) เป็นต้น[41]

2.3.2.5 การตรวจสอบลายมือชื่อดิจิตอล (Verify Digital Signature)

การตรวจสอบลายมือชื่อดิจิตอลคือ ขบวนการในการตรวจสอบว่าลายมือชื่อดิจิตอลที่ปรากฏอยู่ในข้อมูลหรือข้อความที่ได้รับในการสื่อสารนั้นถูกต้องหรือไม่ ขบวนการในการตรวจสอบจะใช้ข้อความ (plaintext) ที่ถูกส่งมาในขั้นตอนการสื่อสารและกุญแจรหัสสาธารณะของบุคคลที่เป็นผู้ส่ง โดยมีแนวความคิดเบื้องหลังการตรวจสอบคือ "ลายมือชื่อดิจิตอลที่ถูกต้องแท้จริงจะต้องสร้างขึ้นโดยนำข้อความต้นฉบับ (Original Message) ไม่ว่าจะนำมาทำการหาค่า Hash result จากการทำ Hash Function ข้อความต้นฉบับก่อนหรือไม่ก็ตาม มาเข้ารหัสโดยกุญแจรหัสส่วนตัวที่มีความเกี่ยวพันกับคู่กุญแจรหัสสาธารณะ ซึ่งผลลัพธ์ที่ได้จากขั้นตอนดังกล่าวคือลายมือชื่อดิจิตอล"

---

* โปรดดูรายละเอียดเพิ่มเติมเกี่ยวกับ elliptic curve cryptosystems ใน D. Stinson, Cryptography: Theory and Practice. และ A.Menezes, Elliptic Curve Public Key Cryptosystems (Boston: MA: Kluwer Academic Publisher, 1993)

[41] Ibid., p.117

ผลของการตรวจสอบจะแสดงว่าเป็นลายมือชื่อดิจิตอลที่แท้จริงของเจ้าของลายมือชื่อก็ต่อเมื่อ (1) สามารถใช้กุญแจรหัสสาธารณะของเจ้าของลายมือชื่อทำการถอดรหัสลายมือชื่อดิจิตอลได้ เพราะมีเพียงการเข้ารหัสโดยคู่กุญแจรหัสที่เรียกว่ากุญแจรหัสส่วนตัวที่จะสามารถใช้กุญแจรหัสสาธารณะถอดรหัสได้ และมีเพียงเจ้าของลายมือชื่อเท่านั้นที่จะมีกุญแจรหัสส่วนตัวที่เป็นคู่กุญแจกับกุญแจรหัสสาธารณะที่ใช้ตรวจสอบ และ (2) ข้อความที่ได้รับจากการติดต่อสื่อสารมิได้ถูกเปลี่ยนแปลงแก้ไขภายหลังที่ได้มีการลงลายมือชื่อดิจิตอล ซึ่งสามารถตรวจสอบได้โดยการเปรียบเทียบค่า Hash result ที่ได้จากการทำ Hash Function ข้อความที่ได้รับ แล้วนำมาเปรียบเทียบกับค่า Hash result ที่ได้จากการถอดรหัสในข้อ (1) ซึ่งค่า Hash result ทั้งสองจะต้องเป็นค่าเดียวกัน

2.3.3 ใบรับรองลายมือชื่อดิจิตอล (Certification of the Digital Signature)

ในระบบการเข้ารหัสแบบอสมมาตรที่นำมาประยุกต์ใช้เป็นลายมือชื่อดิจิตอลนั้น จะต้องมีการสร้างกุญแจรหัสสาธารณะและกุญแจรหัสส่วนตัว ซึ่งการสร้างคู่กุญแจรหัสดังกล่าวสามารถกระทำได้โดยโปรแกรมที่ใช้ติดต่อกันในโลกของเครือข่ายอิเล็กทรอนิกส์ เช่น โปรแกรมเว็บบราวเซอร์ (Web Browser) หรือโปรแกรมที่ใช้ในการติดต่อกันทางจดหมายอิเล็กทรอนิกส์ เป็นต้น หลังจากที่สร้างคู่กุญแจรหัสเรียบร้อยแล้ว ผู้ใช้จะต้องเก็บรักษากุญแจรหัสส่วนตัวไว้เป็นความลับ อย่าให้ผู้อื่นรู้หรือสามารถนำไปใช้ได้ เพราะพื้นฐานของความมั่นคงและความน่าเชื่อถือของระบบลายมือชื่อดิจิตอลอยู่บนข้อสันนิษฐานที่ว่า ผู้ใช้เป็นผู้เดียวที่มีกุญแจรหัสส่วนตัว ซึ่งกุญแจรหัสส่วนตัวหรือกุญแจรหัสลับดังกล่าวมีความสัมพันธ์ทางคณิตศาสตร์กับกุญแจรหัสสาธารณะที่คู่กัน จากนั้นก็จะเป็นการแจกจ่ายกุญแจรหัสสาธารณะไปสู่ผู้อื่นด้วยวิธีการใดๆ เช่น อาจแจกกุญแจรหัสสาธารณะโดยการส่งไปกับจดหมายอิเล็กทรอนิกส์ไปให้ผู้ที่ต้องการติดต่อด้วย ซึ่งวิธีการนี้อาจจะทำให้ไม่สามารถส่งกุญแจรหัสสาธารณะไปให้ครบทุกคน และยังต้องเป็นภาระเมื่อต้องการจะติดต่อกับบุคคลที่ไม่เคยติดต่อกันมาก่อน นอกจากนี้ผู้รับก็ไม่สามารถมั่นใจได้ว่ากุญแจรหัสสาธารณะที่ส่งมานั้นเป็นของบุคคลที่อ้างถึงจริง เนื่องจากอาจมีผู้ไม่ประสงค์ดีแอบสร้างคู่กุญแจรหัสขึ้นโดยใช้ชื่อผู้อื่น และแอบส่งกุญแจรหัสสาธารณะที่สร้างขึ้นเพื่อให้เข้าใจว่ากุญแจรหัสสาธารณะนั้นเป็นของบุคคลที่อ้างถึงก็ได้ เช่น นายดำสร้างคู่กุญแจรหัสขึ้น แล้วนำกุญแจรหัสสาธารณะมาแจกจ่ายโดยอ้างว่าเป็นของนายขาว ต่อมานายดำนำกุญแจรหัสส่วนตัวมาทำการลงลายมือชื่อในจดหมายอิเล็กทรอนิกส์ เพื่ออ้างว่าเป็นจดหมายของนายขาวแล้วส่งให้นายแดง เมื่อนายแดงนำกุญแจรหัสสาธารณะที่นายดำเผยแพร่ว่าเป็นของนายขาวมาใช้ในการตรวจสอบลายมือชื่อดิจิตอลที่ปรากฏในจดหมาย ระบบการตรวจสอบก็จะยืนยันว่าถูกต้อง ซึ่งจะทำให้นายแดงเข้าใจว่าเป็นจดหมายของนายขาวจริง ซึ่งจะสร้างความเสียหายให้แก่นายขาวและนายแดงได้ เป็นต้น

วิธีการที่ดีกว่าในการแจกจ่ายกุญแจรหัสสาธารณะก็คือ การแจกจ่ายกุญแจรหัสสาธารณะโดยบุคคลที่เป็นกลางและไว้วางใจได้ (Trusted Third Party)[42] ซึ่งเรียกว่า ผู้ประกอบการรับรองดิจิตอล (Digital Certification Authority) โดยผู้ประกอบการรับรองนี้จะทำการตรวจสอบกุญแจรหัสสาธารณะที่ตนทำการเผยแพร่ พร้อมทั้งออกใบรับรองว่ากุญแจรหัสสาธารณะนั้นเป็นของบุคคลที่ถูกระบุในใบรับรองจริง

2.3.3.1 ใบรับรอง

ใบรับรองดิจิตอลจะประกอบด้วยข้อมูลหลักๆ ดังนี้ ชื่อของผู้ถือใบรับรอง (ในภาษาอังกฤษเรียกผู้มีชื่อในใบรับรองหรือผู้ถือใบรับรองว่า "Subscriber") ชื่อของผู้ประกอบการรับรอง กุญแจรหัสสาธารณะของผู้ถือใบรับรอง วันออกและวันหมดอายุของใบรับรอง (โดยทั่วไปใบรับรองจะมีอายุประมาณ 6 เดือนถึงหนึ่งปี) ระดับชั้นของใบรับรอง เลขหมายของใบรับรอง และลายมือชื่อดิจิตอลของผู้ประกอบการรับรอง

ข้อมูลแสดงตัวของผู้ถือใบรับรอง ชื่อ ชื่อบริษัท ที่อยู่
ชื่อผู้ประกอบการรับรอง
กุญแจรหัสสาธารณะของผู้ถือใบรับรอง
วันออกและวันหมดอายุของใบรับรอง
ระดับชั้นของใบรับรอง
เลขที่ของใบรับรอง
ลายมือชื่อดิจิตอลของผู้ประกอบการรับรอง

แผนภูมิ 2-8 : แสดงรายละเอียดข้อมูลที่จำเป็นในใบรับรองดิจิตอลทั่วไป

ใบรับรองดิจิตอลแบ่งออกได้เป็นสี่ระดับชั้น ตามระดับการตรวจสอบข้อมูลของเจ้าของใบรับรอง ระดับชั้นที่หนึ่งเป็นชั้นที่ออกใบรับรองได้ง่ายที่สุดและปลอดภัยน้อยที่สุด เนื่องมาจากมีการตรวจสอบน้อยที่สุด โดยจะตรวจสอบแค่ชื่อผู้ถือใบรับรอง และที่อยู่ตามจดหมายอิเล็กทรอนิกส์เท่านั้น (E-Mail Address) ว่าถูกต้องหรือไม่เท่านั้น ในใบรับรองชั้นที่สองจะตรวจสอบถึงเลขบัตรประจำตัวประชาชน เลขสวัสดิการสังคมหรือประกันสังคม (social security number) และวันเดือนปีเกิด ในชั้นที่สามจะมีการตรวจสอบเพิ่มเติมเกี่ยวกับประวัติการใช้เครดิต

---

[42] กฤษณะ ช่างกล่อม, (ร่าง) รายงานการศึกษาวิจัยเรื่องกฎหมายพาณิชย์อิเล็กทรอนิกส์, หน้า 20

และการชำระเงิน สำหรับใบรับรองในชั้นที่สี่นั้นยังไม่มีการออกมาเป็นมาตรฐานอย่างแน่ชัด แต่จะเป็นการตรวจสอบข้อมูลเพิ่มเติมเกี่ยวกับตำแหน่งหน้าที่ในองค์กรด้วย ในการขอใบรับรองดิจิตอลนั้น ผู้ขอจะเสียค่าธรรมเนียมให้แก่หน่วยงานที่ออกใบรับรอง เพื่อให้เป็นค่าใช้จ่ายในการตรวจสอบประวัติของผู้ขอใบรับรอง ค่าธรรมเนียมนี้จะขึ้นอยู่กับระดับชั้นของใบรับรองที่ขอ เนื่องจากผู้ประกอบการรับรองจะต้องเสียค่าใช้จ่ายมากขึ้นในการตรวจสอบข้อมูลของผู้ขอมากขึ้น ระดับชั้นของใบรับรองยิ่งสูงยิ่งทำให้แน่ใจได้ว่าใบรับรองนั้นแสดงถึงบุคคลที่อ้างถึงในใบรับรองจริง[43]

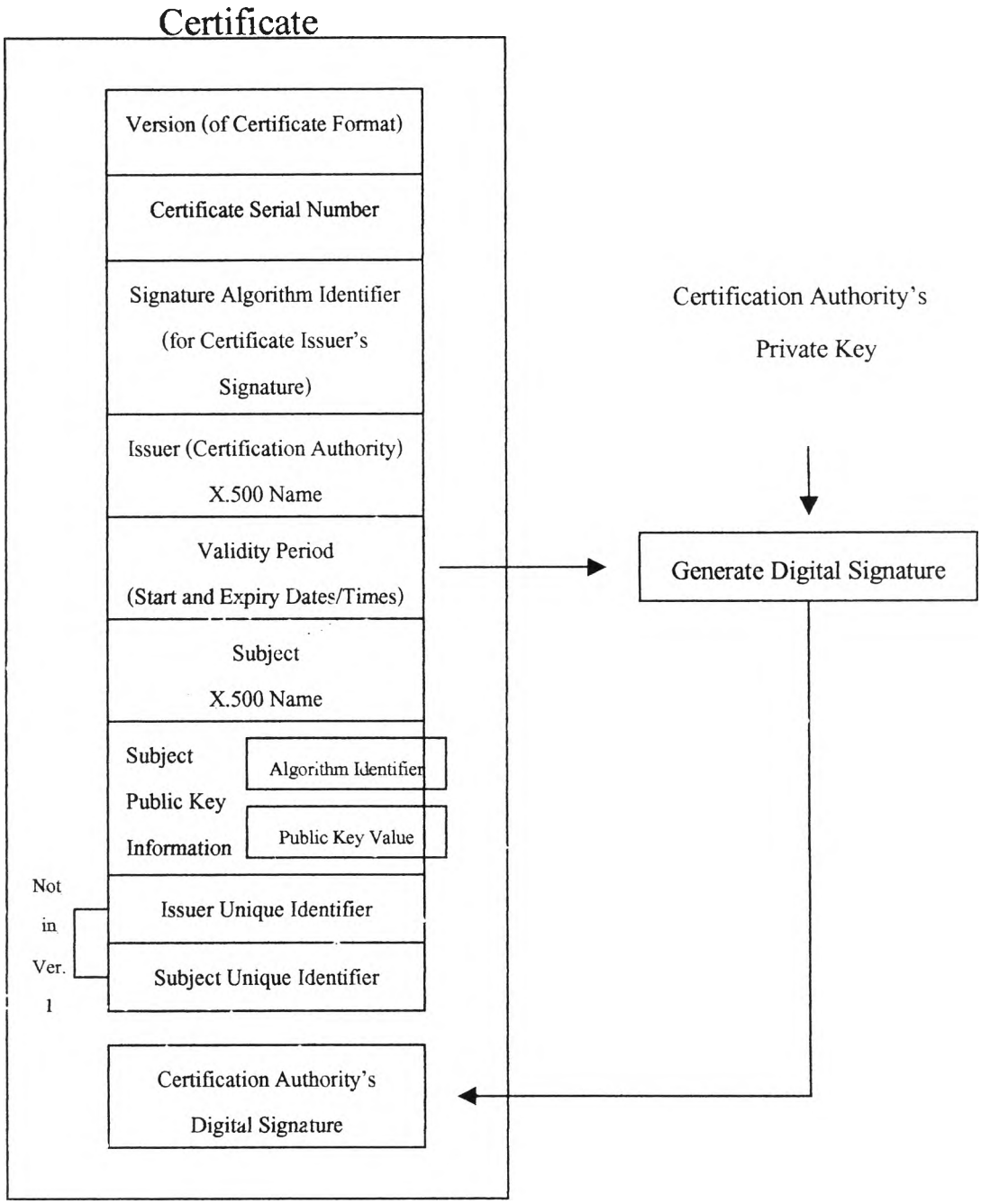
2.3.3.2 แบบของใบรับรอง

แบบของใบรับรองที่ใช้ในการตรวจสอบลายมือชื่อดิจิตอลที่เป็นที่รู้จักและนิยมในขณะนี้คือแบบที่เรียกว่า ISO/IEC/ITU X.509 standard* ซึ่ง version 1 ได้ประกาศใช้มาตั้งแต่ปี ค.ศ.1988 version 2 ใช้ในปี ค.ศ.1993 และ version 3 ใช้ในปี 1996

---

[43] ฉันทวุฒิ พืชผล, เรื่องเดิม. หน้า 86

* ISO คือ องค์กรมาตรฐานระหว่างประเทศ (International Standard Organization) และ ITU คือ สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union)



แผนภูมิ 2-9[44] : รูปแบบของใบรับรอง X.509 Version 1 และ Version 2

---

[44] ที่มา : Warwick Ford and Michael S. Baum, Id., p. 215

โดยในใบรับรองจะมีรายละเอียดดังนี้

(a) Version: ตัวชี้บอกถึง Version ของใบรับรอง และเพื่อเปิดโอกาสให้ Version ใหม่ๆ ของใบรับรองในอนาคต

(b) Serial number: ตัวเลขประจำตัวของใบรับรองที่ระบุโดยผู้ประกอบการรับรอง ที่ใช้เพื่อทำการอ้างระบุลำดับที่ของใบรับรอง

(c) Signature: ระบุวิธีการคำนวณในการเข้ารหัส (Algorithm) ที่ผู้ประกอบการรับรองใช้ในการลงลายมือชื่อดิจิตอลในใบรับรอง

(d) Issuer: ชื่อของผู้ประกอบการรับรอง ระบุชื่อโดยวิธีการ X.500 name (โปรดดูเกี่ยวกับ X.500 Names เพิ่มเติม)

(e) Validity: วันเวลาเริ่มต้นและสิ้นสุดความมีผลสมบูรณ์ของใบรับรอง

(f) Subject: ชื่อของผู้ถือกุญแจรหัสส่วนตัวที่มีความเกี่ยวข้องกับกุญแจรหัสสาธารณะที่ถูกรับรองในใบรับรอง ระบุชื่อโดยวิธีการ X.500 name (โปรดดูเกี่ยวกับ X.500 Names เพิ่มเติม)

(g) Subject public-key information: ค่าของกุญแจรหัสสาธารณะและวิธีการคำนวณในการเข้ารหัส (Algorithm) ที่กุญแจดังกล่าวจะถูกนำไปใช้

(h) Issuer unique identifier: ส่วนเพิ่มเติมของข้อมูลที่ช่วยทำให้ชื่อของผู้ประกอบการรับรองเกิดความชัดเจน ในกรณีที่มีผู้ประกอบการรับรองชื่อเดียวกัน (โปรดดูเกี่ยวกับ X.500 Names เพิ่มเติม)

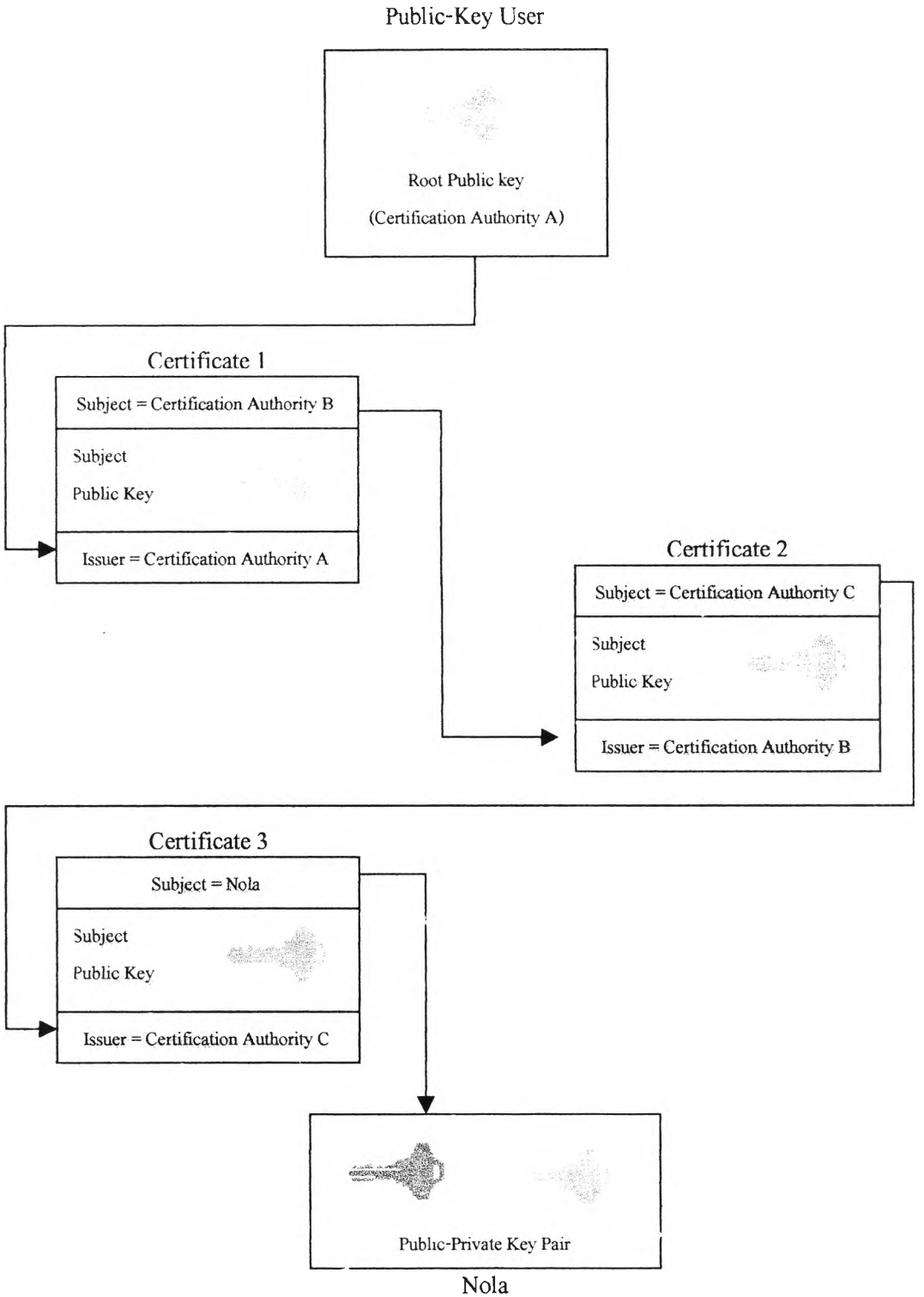
(i) Subject unique identifier: ส่วนเพิ่มเติมของข้อมูลที่ทำให้ชื่อของบุคคลที่เป็นผู้ถือใบรับรองเกิดความชัดเจน ในกรณีที่มีผู้ถือใบรับรองที่มีชื่อเดียวกัน (โปรดดูเกี่ยวกับ X.500 Names เพิ่มเติม)

รายละเอียดเพิ่มเติมเกี่ยวกับมาตรฐานของใบรับรอง โปรดดูในหนังสือ Secure Electronic Commerce ของ Warwick Ford and Michael S. Baum รายละเอียดของหนังสือเล่มนี้โปรดดูในรายการอ้างอิง

2.3.3.3 เส้นทางของใบรับรอง (Certification Path)

ในการติดต่อสื่อสารหรือการประกอบพาณิชย์อิเล็กทรอนิกส์ที่มีขอบข่ายทั่วโลก คงเป็นไปได้ยากที่จะมีผู้ประกอบการรับรอง (Certification Authority) รายเดียวที่ใช้ร่วมกันทั่วโลก ในแต่ละประเทศก็จะต้องมีผู้ประกอบการรับรองที่ผู้ใช้มีความไว้วางใจของแต่ละประเทศหรือแต่ละกลุ่ม ดังนั้นจึงมีความจำเป็นที่จะต้องยอมรับว่าในเบื้องต้นว่า จะต้องมีผู้ประกอบการรับรองที่หลากหลาย

ในการที่จะได้มาซึ่งกุญแจรหัสสาธารณะจากบุคคลที่ไม่รู้จักที่อยู่ตามมุมโลกต่างๆและสามารถไว้วางใจได้ว่ากุญสาธารณะดังกล่าวเป็นของบุคคลที่อ้างถึงจริง มีความจำเป็นที่จะต้องผ่านผู้ประกอบการรับรองมากมาย ซึ่งจะก่อให้เกิดคำที่เรียกว่า "เส้นทางของใบรับรอง" (Certification Chain or Certification Path) ซึ่งจะประกอบด้วย ผู้ประกอบการรับรองหลายแห่งที่เชื่อมโยงกันอย่างเป็นระบบ โดยผู้ใช้กุญแจรหัสสาธารณะจะต้องเริ่มจากการได้มาซึ่งกุญแจรหัสสาธารณะของผู้ประกอบการรับรองหนึ่งแห่งที่เรียกว่า "ผู้ประกอบการรับรองรากฐาน" (Root Certification Authority) จากนั้นผู้ใช้กุญแจรหัสสาธารณะสามารถที่จะได้รับและใช้กุญแจรหัสสาธารณะของเจ้าของลายมือชื่ออื่นอย่างไว้วางใจได้ โดยผ่ายเครือข่ายของผู้ประกอบการรับรอง ตัวอย่างเช่น ถ้าต้องกุญแจรหัสสาธารณะของบุคคลที่ชื่อว่า Nola โดยมีผู้ประกอบการรับรอง C เป็นผู้รับรองว่ากุญแจรหัสสาธารณะดังกล่าวเป็นของ Nola จริง และผู้ใช้กุญแจรหัสสาธารณะมีความไว้วางใจผู้ประกอบการรับรอง A เส้นทางของใบรับรองก็จะเป็นดังนี้ (ในที่นี้ไม่ได้คำนึงถึงเรื่องข้อจำกัดในความสัมพันธ์ระหว่างผู้ประกอบการรับรอง ซึ่งโครงสร้างความสัมพันธ์ระหว่างผู้ประกอบการรับรองหรือการรับรองซึ่งกันและกันระหว่างผู้ประกอบการรับรองจะได้กล่าวถึงต่อไปในหัวข้อ 2.3.6 โครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะ)



แผนภูมิ 2-10[45] : เส้นทางของใบรับรอง (Certification Path)

---

[45] ที่มา : Warwick Ford and Michael S. Baum, Id., p. 198

2.3.3.4 สภาพแวดล้อมในการออกใบรับรองดิจิตอล[46]

สภาพแวดล้อมในการออกใบรับรองสามารถแบ่งออกได้เป็น 2 ประเภท คือ สภาพแวดล้อมแบบเปิด สภาพแวดล้อมแบบปิด ในสภาพแวดล้อมแบบเปิดซึ่งพบมากในการค้าปลีกผ่านเครือข่ายอินเตอร์เน็ตหรือการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจกับผู้บริโภค (Business to Consumer หรือ B to C) ฝ่ายต่างๆ ที่เกี่ยวข้องมักไม่รู้จักกันมาก่อนและไม่มีบทบาทสัมพันธ์ในเชิงสัญญา (Contractual relationship) กันล่วงหน้า ในสภาพแวดล้อมแบบเปิดนี้บทบาทของผู้ประกอบการรับรองคือ การออกใบรับรองตัวบุคคล (identity certificate) เพื่อให้ทั้งสองฝ่ายสามารถระบุตัวบุคคลคู่สัญญาอีกฝ่ายหนึ่งได้

ส่วนในสภาพแวดล้อมแบบปิด ฝ่ายต่างๆ ที่เกี่ยวข้องจะรู้จักกันและมักมีความสัมพันธ์ในเชิงสัญญากันอยู่แล้ว ซึ่งพบบ่อยในการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจกับธุรกิจ (Business to Business หรือ B to B) เช่นการซื้อขายสินค้าผ่านเครือข่ายเอ็กซ์ทราเน็ต (extranet) หรือเครือข่ายการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI) การติดต่อระหว่างบุคคลฝ่ายต่างๆ ในองค์กรเดียวกันผ่านเครือข่ายอินทราเน็ต (intranet) หรือแม้กระทั่งการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจกับผู้บริโภคในบางรูปแบบ เช่น การทำธุรกรรมด้านการเงินระหว่างธนาคารกับลูกค้าของตน เป็นต้น ในบางกรณีบุคคลที่สองและบุคคลที่สามอาจเป็นบุคคลเดียวกัน ทำให้เหลือเพียงฝ่ายต่างๆ ที่เกี่ยวข้องเพียงสองฝ่าย (two-party model) เช่น ธนาคารเป็นผู้ออกใบรับรองให้แก่ลูกค้าและใช้ใบรับรองนั้นในการระบุตัวลูกค้าของตนในการทำธุรกรรม หรือบริษัทเป็นผู้ออกใบรับรองให้แก่พนักงานและใช้ใบรับรองนั้นในการกำหนดสิทธิในการใช้เครื่องคอมพิวเตอร์ ในสภาพแวดล้อมแบบปิดนี้บทบาทของผู้ประกอบการรับรองอาจเปลี่ยนจากการออกใบรับรองตัวบุคคลไปสู่การออกใบรับรองสิทธิหรืออำนาจหน้าที่ (Authority certificate) แทน เช่นการออกใบรับรองว่าผู้สั่งซื้อสินค้าเป็นเจ้าหน้าที่ซึ่งมีอำนาจในการสั่งซื้อจริง เป็นต้น

รูปแบบเฉพาะของสภาพแวดล้อมในการออกใบรับรองนี้ มีผลต่อการวางระบบพื้นฐานของกุญแจรหัสสาธารณะ (Public Key Infrastructure) รวมทั้งการกำหนดนโยบายและออกกฎหมายที่เกี่ยวข้องกับลายมือชื่อดิจิตอลอีกด้วย

2.3.3.5 ระยะเวลาการใช้ใบรับรองและการเพิกถอนใบรับรอง (Operation period of certificate and Revocation a certificate)

ในการใช้ใบรับรองเพื่อทำการตรวจสอบยืนยันความถูกต้องของลายมือชื่อดิจิตอลนั้น ระยะเวลาที่ใบรับรองมีผลบังคับใช้เป็นเรื่องที่ต้องให้ความสำคัญ เพราะคู่กุญแจรหัส

---

[46] สมเกียรติ ตั้งกิจวานิชย์, รายงานการวิจัยเรื่อง ลายมือชื่ออิเล็กทรอนิกส์และองค์กรออกใบรับรอง, สถาบันวิจัยเพื่อการพัฒนาประเทศไทย, หน้า 8

ที่ใช้ในการสร้างและตรวจสอบลายมือชื่อนั้นก็ไม่สามารถใช้ได้ตลอดไป มีความจำเป็นที่จะต้องทำการเปลี่ยนหรือปรับปรุงคู่กุญแจรหัสใหม่ตามที่ได้อธิบายไปในหัวข้อ 2.2.3.3 ในทางเทคนิคคู่กุญแจรหัสคู่หนึ่งจะมีระยะเวลาการใช้ที่จำกัดเพื่อควบคุมโอกาศของความเป็นไปได้ที่จะสามารถวิเคราะห์วิธีการเข้ารหัสจากการทราบกุญแจรหัสสาธารณะและเพื่อป้องกันระยะเวลาที่เป็นไปได้ที่กุญแจรหัสส่วนตัวจะเกิดการรั่วไหลขึ้นได้ (Compromise) เพราะฉะนั้นใบรับรองก็จะมีกำหนดเวลาที่ใบรับรองมีผลบังคับใช้เช่นกัน โดยจะทำการระบุถึงวันเวลาที่ใบรับรองเริ่มมีผลบังคับใช้และวันเวลาที่ใบรับรองสิ้นผลบังคับใช้ (Operation period) ภายหลังที่ใบรับรองสิ้นผลบังคับ การรับรองถึงความสัมพันธ์ระหว่างกุญแจรหัสสาธารณะที่ระบุในใบรับรองกับการรับรองที่ปรากฏในใบรับรอง รวมถึงคำรับรองถึงข้อมูลต่างๆ ที่ปรากฏในใบรับรองดังกล่าวก็จะสิ้นผลลงเช่นกัน รวมทั้งใบรับรองจะไม่เป็นที่น่าเชื่อถืออีกต่อไป เว้นแต่จะใช้ใบรับรองดังกล่าวเพื่อทำการตรวจสอบยืนยันลายมือชื่อดิจิตอลในเอกสารเก่า ที่ได้ทำการลงลายมือชื่อดิจิตอลในเวลาที่ใบรับรองมีผลบังคับใช้เท่านั้น[47]

ในกรณีที่เกิดการรั่วไหลหรือสูญหายของกุญแจรหัสส่วนตัวก็สามารถที่จะป้องกันการใช้กุญแจรหัสสาธารณะที่เกี่ยวข้องซึ่งปรากฏในใบรับรองก่อนเวลาที่ใบรับรองจะสิ้นความสมบูรณ์ โดยการทำการระงับการใช้ใบรับรองชั่วคราวหรือทำการเพิกถอนใบรับรอง ซึ่งจะทำให้ใบรับรองหยุดระยะเวลาที่มีผลบังคับใช้ลงชั่วคราวชั่วระยะเวลาหนึ่งหรือทำให้ใบรับรองสิ้นความสมบูรณ์ลงแล้วแต่กรณี และไม่สามารถใช้เพื่อทำการตรวจสอบยืนยันลายมือชื่อดิจิตอลได้ รายละเอียดในเรื่องของการระงับการใช้ใบรับรองชั่วคราวหรือการเพิกถอนใบรับรองจะได้อธิบายในบทที่ 4 ต่อไป

2.3.4 ผู้ประกอบการรับรอง (Certification Authority)

2.3.4.1 แนวความคิด

ผู้ประกอบการรับรอง (Certification Authority) เป็นบุคคลหรือองค์กรที่ได้รับความไว้วางใจในการจัดทำระบบการออกใบรับรองของลายมือชื่อดิจิตอล (Digital Signature) ที่มีความปลอดภัยและน่าเชื่อถือไว้วางใจ โดยอาศัยแนวความคิดในเรื่องของ "บุคคลที่สามที่เป็นกลางและไว้วางใจได้" (Trusted Third Party) โดยแนวความคิดดังกล่าวนี้คือ การให้บุคคลที่ไม่มีส่วนได้ส่วนเสียหรือที่เรียกกันว่าบุคคลที่สามซึ่งเป็นผู้ประกอบวิชาชีพ ซึ่งบุคคลเหล่านี้จะมีข้อบังคับและจรรยาบรรณของผู้ประกอบวิชาชีพเป็นเครื่องยืนยันถึงความน่าเชื่อถือเป็นผู้ให้การรับรองเรื่องใดเรื่องหนึ่งโดยเฉพาะ ซึ่งเป็นแนวความคิดเดียวกันกับโนตารีพับลิก (Notary Public) ที่ให้การ

---

[47] Warwick Ford and Michael S. Baum, Id., p. 199

รับรองลายมือชื่อ (Hand-written Signature) ในเอกสารที่เป็นกระดาษต่างๆ ว่าเป็นลายมือชื่อที่แท้จริง โนตารีพับลิกเป็นที่รู้จักแพร่หลายในทุกๆ ประเทศทั่วโลกและมีเชื่อเสียงในเรื่องของความน่าเชื่อถือ ผู้ประกอบการรับรองจึงทำหน้าที่คล้ายกับโนตารีพับลิก คือ เป็นบุคคลที่สามที่น่าเชื่อถือในการตรวจสอบความถูกต้องของข้อมูลต่างๆ ที่เกี่ยวข้องกับผู้ที่ยื่นคำขอใบรับรองจากตน เมื่อผู้ประกอบการรับรองทำการตรวจสอบความถูกต้องของข้อมูลต่างๆ แล้ว ก็จะดำเนินการจัดทำใบรับรองและทำการเผยแพร่หรือจัดส่งใบรับรองดังกล่าวไปยังบุคคลหรือหน่วยงานที่ต้องการใช้ใบรับรองดังกล่าวในการตรวจสอบลายมือชื่อดิจิตอล

2.3.4.2 นิยาม

ในเรื่องของนิยามหรือคำจำกัดความของผู้ประกอบการรับรองนี้ ในแต่ละประเทศหรือแต่ละองค์กรระหว่างประเทศก็จะได้ให้นิยามหรือคำจำกัดความที่แตกต่างกันออกไปตามแต่วัตถุประสงค์ แต่อย่างไรก็ตามก็ได้ยืนอยู่บนพื้นฐานเดียวกัน คือ หน่วยงานที่ได้รับความไว้วางใจให้เป็นผู้ที่ทำการออกใบรับรอง ในระบบการใช้ลายมือชื่อดิจิตอล ซึ่งพอที่จะยกตัวอย่างได้ดังนี้

ISO 9594-8-The Directory-Authentication Framework ได้กำหนดคำนิยามของผู้ประกอบการรับรอง (Certification Authority) ไว้ว่า "หน่วยงานที่ได้รับความไว้วางใจโดยผู้ใช้รายหนึ่ง หรือหลายรายให้จัดทำและส่งใบรับรอง ในบางกรณีผู้ประกอบการรับรองอาจช่วยสร้างกุญแจให้กับผู้ใช้ได้" [48]

ผู้ประกอบการรับรอง คือ ฝ่ายที่สามที่เป็นอิสระที่เป็นผู้ทำการผูกพันกุญแจรหัสสาธารณะกับบุคคลผู้ที่เป็นเจ้าของกุญแจรหัส[49]

ในส่วนของกฎหมายแม่แบบของคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ (United Nations Commission on International Trade Law (UNICITRAL) Working Group on Electronic Commerce) ได้ให้คำนิยามไว้ในกฎหมายแม่แบบในเรื่องลายมือชื่ออิเล็กทรอนิกส์ (Draft Uniform Rules on Electronic Signature) พร้อมทั้งคำแนะนำในการออกกฎหมายล่าสุดคือเอกสารเลขที่ A/CN.9/WG.IV/WP.88 ไว้ในมาตรา 2 ว่า "ผู้ให้บริการออกใบรับรอง คือ บุคคลผู้ทำการออกใบรับรองและให้บริการอย่าง

---

[48] กฤษณะ ช่างกล่อม, (ร่าง) รายงานการศึกษาวิจัยเรื่องกฎหมายพาณิชย์อิเล็กทรอนิกส์, หน้า 20

[49] Michael J. Osty and Michael J. Pulcanio, "The Liability of Certification Authorities to Relying Third Parties", in John Mashall Journal of Computer & Information Law, Vol.XVII, 1999, p.775

อื่นที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์"* สาเหตุที่ UNCITRAL ใช้คำว่า "Certification service provider" แทนคำว่า "Certification Authority" เพราะ UNCITRAL ได้ใช้แนวทางในการร่างกฎหมายโดยใช้รูปแบบที่รักษาความเป็นกลางทางเทคโนโลยี ซึ่งจะได้อธิบายต่อไปในบทที่ 3 หัวข้อ 3.2.2.1.1 ต่อไป

ในส่วนของประเทศไทยได้ให้คำนิยามไว้ใน "ร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. ..." ซึ่งได้ให้ไว้ในมาตรา 4 ดังนี้ "ผู้ประกอบการรับรอง" หมายความว่า ผู้ประกอบการเกี่ยวกับการรับรองกุญแจคู่หรือกุญแจสาธารณะซึ่งสัมพันธ์กับตัวบุคคลผู้เป็นเจ้าของลายมือชื่อดิจิทัล และการดำเนินการใดๆ ที่เกี่ยวข้องตามพระราชบัญญัตินี้** และตาม "ร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ..." ได้ให้คำนิยามไว้ว่า "ผู้ประกอบการรับรอง" หมายความว่า บุคคลซึ่งประกอบกิจการรับรองเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัยตามพระราชบัญญัตินี้***

2.3.4.3 บทบาทของผู้ประกอบการรับรอง

เนื่องจากคุณสมบัติสำคัญของผู้ประกอบการรับรองจะต้องเป็นบุคคลที่เป็นกลางและไว้วางใจได้ (Trusted Third Party) ในการระบบการใช้ลายมือชื่อดิจิตอล ผู้ประกอบการรับรองจึงเป็นบุคคลที่มีหน้าที่ดังนี้

2.3.4.3.1 บริการด้านการเข้ารหัสและถอดรหัส

การบริการด้านการเข้ารหัสและถอดรหัสนี้ เป็นบริการที่เกี่ยวกับคู่กุญแจรหัสและขั้นตอนในการลงลายมือชื่อและการตรวจสอบลายมือชื่อ ซึ่งประกอบไปด้วย

---

* United Nations, "Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signature", (A/CN.9/WG.IV/WP.88), 30 January 2001, www.un.or.at/uncitral (visited Feb, 2 2001) ,p. 5

"**Article 2 Definitions**

For the purpose of this law:

.....

(e) "Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;

....."

** โปรดดู **ภาคผนวก ก.**

*** โปรดดู **ภาคผนวก ค.**

การผลิตกุญแจรหัสลับ (Generation of confidential key) การส่งมอบกุญแจรหัสลับ (Distribution of confidential key) ในส่วนของการเข้าและถอดรหัส และการผลิตกุญแจรหัสส่วนตัวและกุญแจรหัสสาธารณะ (Generation of Private/Public key) การสร้างลายมือชื่อดิจิตอล (Generation of digital signature) และการรับรองลายมือชื่อดิจิตอล (Validation of digital signature) ในส่วนของขั้นตอนในการลงลายมือชื่อและการตรวจสอบลายมือชื่อ

2.3.4.3.2 บริการด้านบริหารการรับรอง

การบริการด้านการบริหารใบรับรองนี้เป็นการบริการเกี่ยวกับใบรับรองที่ออกโดยผู้ประกอบการรับรอง ซึ่งประกอบด้วย การออกใบรับรอง (Certificate issuance) การระงับใช้ใบรับรองชั่วคราวและการเพิกถอนใบรับรอง (Certificate suspension or revocation) ในกรณีที่ผู้ถือใบรับรองถูกขโมยกุญแจรหัสส่วนตัว การเผยแพร่ใบรับรองแก่บุคคลทั่วไป (Certificate publishing) การเก็บต้นฉบับใบรับรอง (Certificate achieving) ในกรณีที่ต้องใช้ตรวจสอบข้อมูลต่างๆ ในใบรับรองที่ได้สิ้นความสมบูรณ์ (Expired certificate) แล้ว รวมทั้งการใช้ใบรับรองเพื่อการตรวจสอบยืนยันลายมือชื่อดิจิตอลในข้อมูลเก่า เมื่อเวลาที่ใบรับรองได้สิ้นความสมบูรณ์ลง รวมทั้งการกำหนดนโยบายการออกและอนุมัติใบรับรอง (Policy creation/approval) ที่เรียกว่าการจัดทำถ้อยแถลงแนวทางปฏิบัติในการออกใบรับรอง (Certification Practice Statement หรือ CPS)

2.3.4.3.3 บริการเสริม (Ancillary Services)

บริการเสริมเป็นบริการอื่นๆ ที่มิได้เป็นการบริการหลักของผู้ประกอบการรับรอง เป็นแต่เพียงส่วนเสริมเพื่อให้บริการหลักมีความสมบูรณ์เท่านั้น เช่น บริการจัดเก็บเอกสาร (Archival Service) คือบริการจัดเก็บบันทึกข้อมูล (record) เกี่ยวกับใบรับรอง ผู้ประกอบการรับรองหรือการพาณิชย์อิเล็กทรอนิกส์ สำหรับจุดประสงค์ในการเก็บรักษาเอกสารทางการค้าต่างๆ บริการฝากกุญแจรหัส (Key Escrow) และกู้กุญแจรหัส (Key Recovery) สำหรับในกรณีที่มีความจำเป็นที่จะต้องมีการฝากกุญแจรหัสส่วนตัวสำรองไว้ หรือต้องการใช้ระบบการกู้กุญแจรหัสทั้งในเพื่อการพาณิชย์หรือในกรณีที่กำหนดในกฎหมาย บริการจัดทำทะเบียนข้อมูล (Directory service) เป็นบริการจัดทำข้อมูลเกี่ยวกับบุคคลที่เกี่ยวในการพาณิชย์อิเล็กทรอนิกส์หรือบุคคลต่างๆ ที่ทำการติดต่อสื่อสารทางเครือข่ายอิเล็กทรอนิกส์ บริการตรวจสอบทางเทคนิคที่เกี่ยวข้อง (Technical due diligence service) หรือบริการการลงประทับเวลา (Time-stamping service) ในการทำธุรกรรมหรือการติดต่อสื่อสารต่างๆ เป็นต้น

2.3.5 การประทับเวลา (Time-Stamping)

การประทับเวลาคือการรับรองถึงตัวบงชี้ในเรื่องของวันและเวลาที่ถูกต้อง ในการกระทำทางอิเล็กทรอนิกส์ เช่นการส่งข้อมูล การเริ่มติดต่อสื่อสาร การลงลายมือชื่ออิเล็กทรอนิกส์หรือลายมือชื่อดิจิตอล เป็นต้น เนื่องมาจากเวลาที่กระทำการดังกล่าวเป็นส่วนสำคัญที่จะทำให้การกระทำเหล่านั้นเป็นผลหรือไม่เป็นผล เช่น ถ้าได้มีบุคคลหนึ่งได้ลงลายมือชื่อดิจิตอลในเวลาก่อนที่ผู้ประกอบการรับรองหนึ่งจะได้ออกใบรับรองในแก่บุคคลผู้นั้น หรือได้ลงลายมือชื่อในช่วงเวลาที่ใบรับรองถูกระงับใช้ หรือภายหลังจากที่ใบรับรองถูกยกเลิกไปแล้ว ลายมือชื่อดิจิตอลดังกล่าวไม่อาจถือได้ว่าเป็นลายมือชื่อดิจิตอลของบุคคลผู้นั้น เป็นต้น

การประทับเวลา คือการให้ผู้ประกอบการรับรองหรือบุคคลที่เป็นกลางและไว้วางใจได้ (Trusted Third Party) ทำการลงเวลาในการกระทำทางอิเล็กทรอนิกส์ที่เกิดขึ้น เพื่อรับรองว่าการกระทำดังกล่าวได้กระทำหรือเกิดขึ้นหรือสิ้นผลลงในเวลานั้นจริง เวลาที่ทำการประทับจะใช้เวลาที่เป็นมาตรฐานสากล เพื่อให้เกิดความแน่นอนและลดข้อถกเถียงที่จะเกิดขึ้นได้

การประทับเวลาก็เป็นบริการหนึ่งที่ผู้ประกอบการรับรองสามารถให้บริการได้

2.3.6 โครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะ (Public Key Infrastructure)

โครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะ (Public Key Infrastructure, PKI) คือ องค์ประกอบพื้นฐานที่สนับสนุนการใช้เทคโนโลยีการเข้ารหัสที่อยู่บนพื้นฐานของระบบกุญแจรหัสสาธารณะในวงกว้างหรือระหว่างประเทศ อย่างไรก็ตามเมื่อพยายามทำการวางโครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะก็จะพบถึงความหลากหลายของโครงสร้างทางสังคมในแต่ละประเทศ ความต่างของระดับเทคโนโลยีและระบบกฎหมาย ซึ่งทั้งสองส่วนเป็นสิ่งสำคัญที่จะทำให้สามารถใช้ศักยภาพของระบบกุญแจรหัสสาธารณะได้อย่างเต็มที่ โครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะจึงมีความสำคัญอย่างมากที่จะทำให้การใช้ลายมือชื่อดิจิตอลที่ใช้เทคโนโลยีของการเข้ารหัสแบบอสมมาตร (Asymmetric Encryption) หรือระบบกุญแจรหัสสาธารณะเป็นพื้นฐาน จะสามารถดำรงอยู่และแพร่หลายมากขึ้นในระบบการสื่อสารอิเล็กทรอนิกส์ ที่ทำให้เกิดระบบการสื่อสารแบบโลกไร้พรมแดน ผู้ประกอบการรับรอง (Certification Authority) และการบริหารใบรับรองคือส่วนสำคัญของโครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะ โครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะจะเป็นการจัดหาบริการที่เกี่ยวข้องกับการใช้ลายมือชื่อดิจิตอล ดังนี้[50]

(1) การบริหารกุญแจที่ใช้สำหรับการเข้ารหัสที่ใช้ในการลงลายมือชื่อและตรวจสอบลายมือชื่อ

---

[50] United Nations, "Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signature", (A/CN.9/WG.IV/WP.88), p. 21

(2) ให้การรับรองว่ากุญแจรหัสสาธารณะกับกุญแจรหัสส่วนตัวของผู้ใช้มีความเกี่ยวพันกันจริง

(3) จัดหาคู่กุญแจรหัสให้แก่ผู้ใช้

(4) ทำการตัดสินใจว่าผู้ใช้คนใดจะมีเอกสิทธิ์ใดในระบบ

(5) ทำการเผยแพร่ทะเบียนข้อมูลกุญแจรหัสสาธารณะและใบรับรองอย่างปลอดภัย

(6) บริหารสื่อที่ใช้เก็บข้อมูล (personal tokens e.g., smart card) ที่สามารถทำการระบุตัวผู้ใช้โดยใช้ข้อมูลที่มีลักษณะเฉพาะตัวของผู้ใช้หรือสามารถสร้างหรือเก็บกุญแจรหัสส่วนตัวได้

(7) ทำการตรวจสอบการระบุตัวบุคคลผู้ใช้และให้บริการแก่คนเหล่านั้น

(8) ให้บริการเกี่ยวกับการป้องกันการปฏิเสธความรับผิด (non-repudiation)

(9) ให้บริการการลงประทับเวลา

(10) ทำการบริการคู่กุญแจรหัส เพื่อการใช้ในการเข้ารหัสเพื่อรักษาความลับ ในกรณีที่ได้รับอนุญาต

นอกจากนี้โครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะยังเป็นเรื่องที่มีพื้นฐานเกี่ยวกับลำดับชั้นขององค์กร รูปแบบของของการจัดลำดับชั้นขององค์กรในประเทศส่วนใหญ่จะมีการจัดลำดับชั้นขององค์กรดังนี้ (1) ผู้ประกอบการรับรองรากฐาน (Root Certification Authority) ที่ทำหน้าที่ในการรับรองเทคโนโลยีและการปฏิบัติของทุกฝ่ายที่ได้รับอนุญาตให้ออกกุญแจรหัสที่ใช้ในการเข้ารหัส หรือใบรับรองที่รับรองความสัมพันธ์ระหว่างการใช้ของแต่ละคู่กุญแจรหัส และทำการขึ้นทะเบียนผู้ประกอบการรับรองที่อยู่ในลำดับที่ต่ำกว่า (2) ผู้ประกอบการรับรองอื่นๆ ที่อยู่ในลำดับที่ต่ำกว่าผู้ประกอบการรับรองรากฐาน ซึ่งเป็นผู้ออกใบรับรองถึงความเกี่ยวพันระหว่างกุญแจรหัสสาธารณะและกุญแจรหัสส่วนตัวของผู้ใช้แต่ละคน และ (3) องค์กรท้องถิ่นที่ได้รับการขึ้นทะเบียน ที่อยู่ในลำดับที่ต่ำกว่าผู้ประกอบการรับรองเป็นรู้รับการร้องขอต่างๆ จากผู้ใช้ในเรื่องของกุญแจรหัสที่ใช้ในการเข้ารหัสและใบรับรอง ซึ่งองค์กรท้องถิ่นดังกล่าวต้องทำการระบุและตรวจสอบการระบุตัวผู้ใช้ ในบางประเทศได้กำหนดให้โนตารี พับลิค (Notary Public) ทำหน้าที่เป็นเป็นองค์กรท้องถิ่นตามข้อนี้

เนื่องมาจากในแต่ละประเทศก็มีผู้ประกอบการรับรอง (Certification Authority) ของตนเอง และในแต่ละประเทศก็มิได้มีผู้ประกอบการรับรองเพียงองค์กรเดียว ทั้งผู้ประกอบการรับรองแต่ละองค์กรก็ออกใบรับรองเพื่อตอบสนองวัตถุประสงค์ที่แตกต่างกัน เช่น ผู้ประกอบการรับรองที่ดำเนินงานเพื่อออกใบรับรองให้กับกิจกรรมทางพาณิชย์ หรือผู้ประกอบการรับรองที่ออกใบรับรองเพื่อกิจการทางการเงินเท่านั้น เป็นต้น เพราะฉะนั้นจึงต้องมีการวางโครงสร้างถึงความสัมพันธ์ที่เป็นลำดับชั้นระหว่างผู้ประกอบการรับรองด้วยกันเอง ซึ่งโครงสร้างดังกล่าวนี้ในบางครั้ง

เรียกว่า "trust models" เพื่อสร้างความไว้วางใจ (trust) ให้เกิดขึ้นแก่ผู้ประกอบการรับรอง ซึ่งทำหน้าที่เป็นบุคคลที่เป็นกลางและไว้วางใจได้ (Trusted Third Party) ในเครือข่ายอิเล็กทรอนิกส์

อย่างไรก็ตามมิได้เป็นการง่ายที่จะทำให้ PKI สามารถประสานกลมกลืนกันในระดับระหว่างประเทศ จากการที่ PKI เป็นเรื่องที่เกี่ยวกับเทคโนโลยีที่หลากหลายพอๆ กับความหลากหลายของนโยบายสาธารณะของแต่ละประเทศ ในแต่ละประเทศจึงมีประเด็นที่จะต้องตัดสินใจเมื่อจะทำการสร้าง PKI ดังนี้ (1) รูปแบบและจำนวนของลำดับชั้นของผู้ประกอบการรับรองที่ควรมีใน PKI (2) กุญแจรหัสควรกำหนดให้สามารถออกได้เฉพาะผู้ประกอบการรับรองที่ได้รับอนุญาตหรือให้ผู้ใช้ทำการสร้างกุญแจรหัสของตนเอง (3) ผู้ที่ทำหน้าที่เป็นผู้ประกอบการรับรองคู่กุญแจรหัสควรที่จะเป็นหน่วยงานของรัฐหรือหน่วยงานของเอกชน (4) ควรที่จะควบคุมองค์กรผู้ทำหน้าที่เป็นผู้ประกอบการรับรองด้วยระบบใบอนุญาตหรือระบบอื่นใดที่สามารถควบคุมคุณภาพขององค์ผู้ออกใบรับรองได้ในกรณีที่ไม่ได้ใช้ระบบการให้ใบอนุญาต (5) ขอบเขตของการใช้เทคโนโลยีการเข้ารหัสเพื่อรักษาความลับ (for confidential purpose) (6) หน่วยงานของรัฐควรหรือไม่ที่จะสามารถเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย ด้วยการกำหนดให้ใช้ระบบการฝากกุญแจ (Key Escrow) หรือระบบการกู้กุญแจ (Key Recovery) หรือระบบอื่นที่มีลักษณะใกล้เคียงกันในหัวข้อนี้จะได้กล่าวถึงโครงสร้างความสัมพันธ์ที่เป็นลำดับชั้นระหว่างผู้ประกอบการรับรอง เพื่อทำการศึกษาถึงรูปแบบการวางโครงสร้างดังกล่าว ในประเด็นอื่นๆ ที่เกี่ยวข้องกับเรื่องของโครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะจะได้กล่าวถึงในบทต่อไป

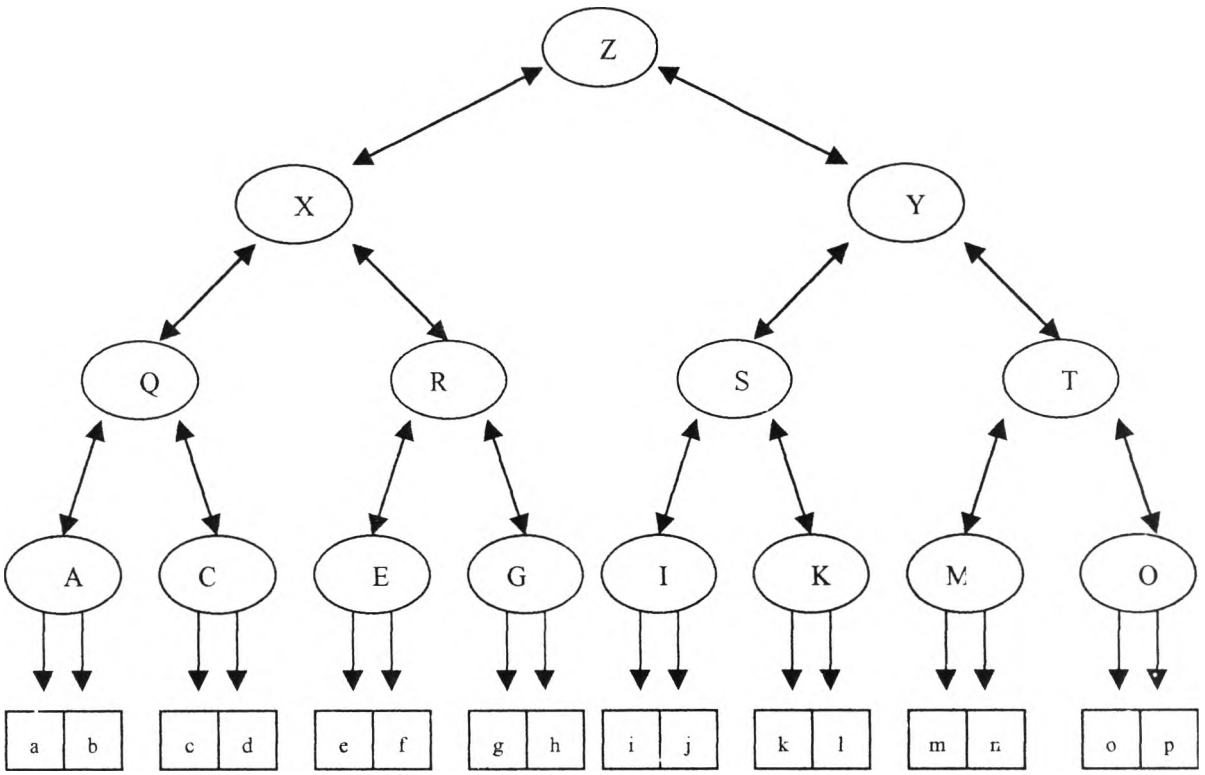
โครงสร้างความสัมพันธ์ที่เป็นลำดับชั้นระหว่างผู้ประกอบการรับรองได้มีการออกแบบโครงสร้างไว้ดังนี้[51]

2.3.6.1 โครงสร้างแบบการจัดลำดับทั่วไป (General Hierarchical Structure)

เพื่อลดปัญหาเกี่ยวกับความไว้วางใจในผู้ประกอบการรับรอง จึงต้องมีการสร้างระบบเพื่อกำหนดความสัมพันธ์ระหว่างผู้ประกอบการรับรอง โดยการใช้แนวความคิดในเรื่องของ "กราฟ" ในทางคณิตศาสตร์ ออกแบบเป็นโครงสร้างแบบต้นไม้ซึ่งในภาษาอังกฤษเรียกว่า Tree-structures หรือ Hierarchies เพื่อให้เป็นระบบและตอบสนองต่อปัญหาในเรื่องความไว้วางใจ

---

[51] Warwick Ford and Michael S. Baum, Id., pp. 265-275



แผนภูมิ 2-11 [52] : โครงสร้างแบบการจัดลำดับทั่วไป (General Hierarchical Structure)

จากแผนภูมิ 2-11 วงรี หมายถึง ผู้ประกอบการรับรอง (Certification Authority) เช่น Z, X และ Y เป็นต้น และสี่เหลี่ยม หมายถึง ผู้ขอใบรับรอง (Subscribers) เช่น a, b และ c เป็นต้น เส้นตรงที่มีสัญลักษณ์ลูกศรด้านเดียว หมายถึง ผู้ประกอบการรับรองออกใบรับรองให้กับผู้ขอใบรับรอง และเส้นตรงที่มีสัญลักษณ์ลูกศรสองด้าน หมายถึง ผู้ประกอบการรับรองที่ออกใบรับรองให้แก่กัน

ในโครงสร้างนี้ เป็นการง่ายที่จะสร้างเส้นทางในการออกใบรับรองในกรณีที่ผู้ขอใบรับรองติดต่อกัน โดยอยู่บนข้อสันนิษฐานที่ว่า ผู้ขอใบรับรองได้ให้ความไว้วางใจผู้ประกอบการรับรองหนึ่งและยอมรับผู้ประกอบการรับรองดังกล่าวเป็นผู้ประกอบการรับรองรากฐาน (Root Certification Authority) ของตน เช่น a มีความไว้วางใจ ผู้ประกอบการรับรอง A และยอมรับกุญแจรหัสสาธารณะของผู้ประกอบการรับรอง A เป็นกุญแจรหัสสาธารณะรากฐาน (Root Public Key) ในกรณีนี้ a จะสามารถได้รับสำเนากุญแจรหัสสาธารณะของทุกๆ คนหรือองค์กรในโครงสร้างนี้อย่างเป็นระบบ เนื่องจากมีเส้นทางของใบรับรองเชื่อมต่อทุกคนหรือองค์กรในโครงสร้าง ซึ่งโครงสร้างแบบนี้สามารถที่จะรองรับการสื่อสารขนาดใหญ่ได้เป็นอย่างดี

---

[52] ที่มา : Warwick Ford and Michael S. Baum, Id., p. 266

ตัวอย่างเช่นในกรณีที่ a ต้องการที่จะได้สำเนากุญแจรหัสสาธารณะของ c เส้นทางการได้มาของใบรับรองของ a จะต้องมีใบรับรอง สามใบดังต่อไปนี้ (โปรดดูแผนภูมิ 2-11 ประกอบ)

- ใบรับรองสำหรับผู้ประกอบการรับรอง Q ที่ออกโดยผู้ประกอบการรับรอง A (เนื่องจาก a ไว้วางใจ กุญแจรหัสสาธารณะของผู้ประกอบการรับรอง A)
- ใบรับรองของผู้ประกอบการรับรอง C ที่ออกให้โดยผู้ประกอบการรับรอง Q
- ใบรับรองของ c ที่ออกให้โดยผู้ประกอบการรับรอง C

หาก a ต้องการสำเนากุญแจรหัสสาธารณะของ g จะต้องมีการออกใบรับรองห้าใบ หรือหาก a ต้องการสำเนากุญแจรหัสสาธารณะของ m จะต้องมีการออกใบรับรองเจ็ดใบ เป็นต้น

ปัญหาประการหนึ่งของโครงสร้างแบบนี้คือ เส้นทางของใบรับรอง (Certification path) จะต้องผ่านผู้ประกอบการรับรองที่มีลำดับศักดิ์เหนือกว่าโดยเฉพาะส่วนที่อยู่บนสุดของโครงสร้าง เช่น ผู้ประกอบการรับรอง Z เป็นต้น ซึ่งทุกคนในโครงสร้างจะต้องให้ความไว้วางใจแก่ผู้ประกอบการรับรอง Z ถ้าผู้ประสงค์ร้ายสามารถที่จะขโมย ทำสำเนา หรือทำปลอมกุญแจรหัสส่วนตัวหรือกุญแจรหัสลับ (Private Key) ของผู้ประกอบการรับรอง Z ได้ ก็จะทำให้โครงสร้างดังกล่าวนี้ขาดความน่าเชื่อถือลงทันที ตัวอย่างเช่น ผู้ประกอบการรับรอง Z เป็นผู้ประกอบการรับรองระหว่างประเทศ และผู้ประกอบการรับรอง X และ Y เป็นผู้ประกอบการรับรองระดับประเทศ เช่น เป็นผู้ประกอบการรับรองของประเทศสหรัฐอเมริกา และประเทศอังกฤษ เป็นต้น ส่วนผู้ประกอบการรับรองระดับต่ำสุดเป็นผู้ประกอบการรับรองของแต่ละท้องถิ่นในแต่ละประเทศ ในกรณีที่ผู้ประสงค์ร้ายสามารถขโมยกุญแจรหัสส่วนตัวของผู้ประกอบการรับรองระดับประเทศ เช่น ผู้ประกอบการรับรองระดับประเทศของสหรัฐอเมริกาไปได้ ผู้ประสงค์ร้ายดังกล่าวก็จะสามารถ

- ปลอมแปลงลายมือชื่อดิจิตอลของบุคคลหรือองค์กรใดก็ได้ในประเทศสหรัฐอเมริกา แล้วนำไปหลอกลวงบุคคลอื่นๆ ที่อยู่ในโครงสร้างในต่างประเทศ ว่าลายมือชื่อดิจิตอลดังกล่าวถูกต้อง
- ปลอมแปลงลายมือชื่อดิจิตอลของบุคคลที่ไม่ได้อยู่ในประเทศสหรัฐอเมริกา แล้วนำไปหลอกบุคคลที่อยู่ในประเทศสหรัฐอเมริกาว่าลายมือชื่อดิจิตอลดังกล่าวถูกต้อง

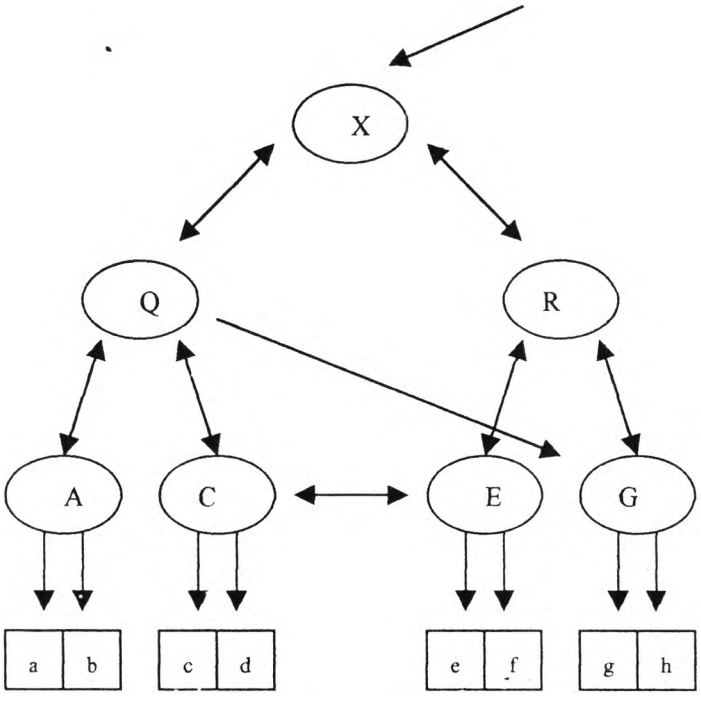
จากปัญหาดังกล่าวทำให้โครงสร้างแบบนี้ไม่เป็นที่ยอมรับในกลุ่มอุตสาหกรรมบางกลุ่มและในระบบการสื่อสารแบบปิดอื่นๆ

2.3.6.2 โครงสร้างแบบการจัดลำดับทั่วไปพร้อมส่วนเชื่อมต่อเพิ่มเติม (General Hierarchical Structure with Additional Links)

โครงสร้างแบบการจัดลำดับทั่วไปนั้นมีความเหมาะสมกับโครงสร้างของระบบการสื่อสารขนาดใหญ่มาก แต่ก็จะส่งผลให้ต้องใช้เวลาและกระบวนการที่ยาวนานมากในเรื่องของเส้นทางของใบรับรอง

จากโครงสร้างแบบการจัดลำดับทั่วไปมีความเป็นไปได้ที่จะเพิ่มจุดเชื่อมโยงโดยตรงระหว่างผู้ประกอบการรับรองภายในโครงสร้างแบบเดิมเพื่อที่จะได้เป็นการลดเส้นทางของใบรับรองลง เพื่อเป็นการประหยัดเวลา ตามแผนภูมิ 2-12 แสดงให้เห็นถึงส่วนหนึ่งของแผนภูมิ 2-11 แต่ได้เพิ่มเติมการเชื่อมโยงผู้ประกอบการรับรอง C และ E โดยทั้งคู่ได้เลือกที่จะมีการรับรองซึ่งกันและกัน ซึ่งส่งผลให้ผู้ถือใบรับรองที่ออกโดยผู้ประกอบการรับรอง C และ E สามารถใช้กุญแจรหัสสาธารณะของกันและกันได้สะดวกมากยิ่งขึ้น (โปรดดูแผนภูมิที่ 2-12 ประกอบ)

การเชื่อมโยงแบบนี้บางทีเรียกว่า "การรับรองข้ามระบบ" (cross-certificates) การรับรองระหว่างผู้ประกอบการรับรอง C และ E หมายความว่าจะมีใบรับรองเพียงแค่สองใบสำหรับผู้ถือใบรับรองที่ออกโดยผู้ประกอบการรับรอง C และ E ซึ่งแต่ต่างจากโครงสร้างแบบการจัดลำดับทั่วไปในข้อ 2.3.6.1 ซึ่งต้องมีใบรับรองถึง 5 ใบ เช่นเดียวกันกับผู้ประกอบการรับรอง Q ที่ได้ออกใบรับรองให้แก่ผู้ประกอบการรับรอง G ส่งผลให้ a และ c สามารถใช้กุญแจรหัสสาธารณะของ g หรือ h โดยมีเส้นทางของใบรับรองเพียงสามใบ แทนที่จะเป็นห้าใบในโครงสร้างการจัดลำดับแบบทั่วไป การรับรองข้ามระบบนี้สามารถทำได้สองอย่าง คือ แบบทวิภาคี (Bilateral) เช่นกรณีของผู้ประกอบการรับรอง C และ E เป็นต้น และการรับรองฝ่ายเดียว (Unilateral) อย่างเช่นผู้ประกอบการรับรอง Q และ G ซึ่งทางเลือกว่าจะรับรองข้ามระบบแบบใด ขึ้นอยู่กับความไว้วางใจและข้อกำหนดในการดำเนินงานของแต่ละผู้ประกอบการรับรอง



แผนภูมิ 2-12 [53] : โครงสร้างแบบการจัดลำดับทั่วไปพร้อมส่วนเชื่อมต่อเพิ่มเติม (General Hierarchical Structure with Additional Links)

2.3.6.3 โครงสร้างแบบการจัดลำดับจากบนลงล่าง (Top-down Hierarchical Structure)

โครงในรูปแบบนี้พัฒนาขึ้นโดยกระทรวงกลาโหมของสหรัฐอเมริกา เพื่อให้เป็นโครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะ ที่มีความปลอดภัยสำหรับการส่งข้อมูลทางการทหาร โปรดดูแผนภูมิที่ 2-13

โครงสร้างนี้มีความแตกต่างจากโครงสร้างแบบการจัดลำดับทั่วไปตรงที่เส้นทางของใบรับรองทั้งหมดจะต้องเริ่มจากผู้ประกอบการรับรองระดับสูงเท่านั้น (Top-level certification Authority) นั่นคือ ผู้ประกอบการรับรองไม่ต้องออกใบรับรองให้ผู้ประกอบการรับรองระดับที่สูงกว่า ผู้ใช้ใบรับรองทั้งหมดจะมีหน่วยงานระดับสูง (Top-level) เป็นผู้ประกอบการรับรองรากฐานของตน หรือกล่าวได้อีกอย่างหนึ่งว่าผู้ใช้ใบรับรองจะต้องมีสำเนาของกุญแจรหัสสาธารณะของผู้ประกอบการรับรองระดับสูงที่ถูกต้องอยู่

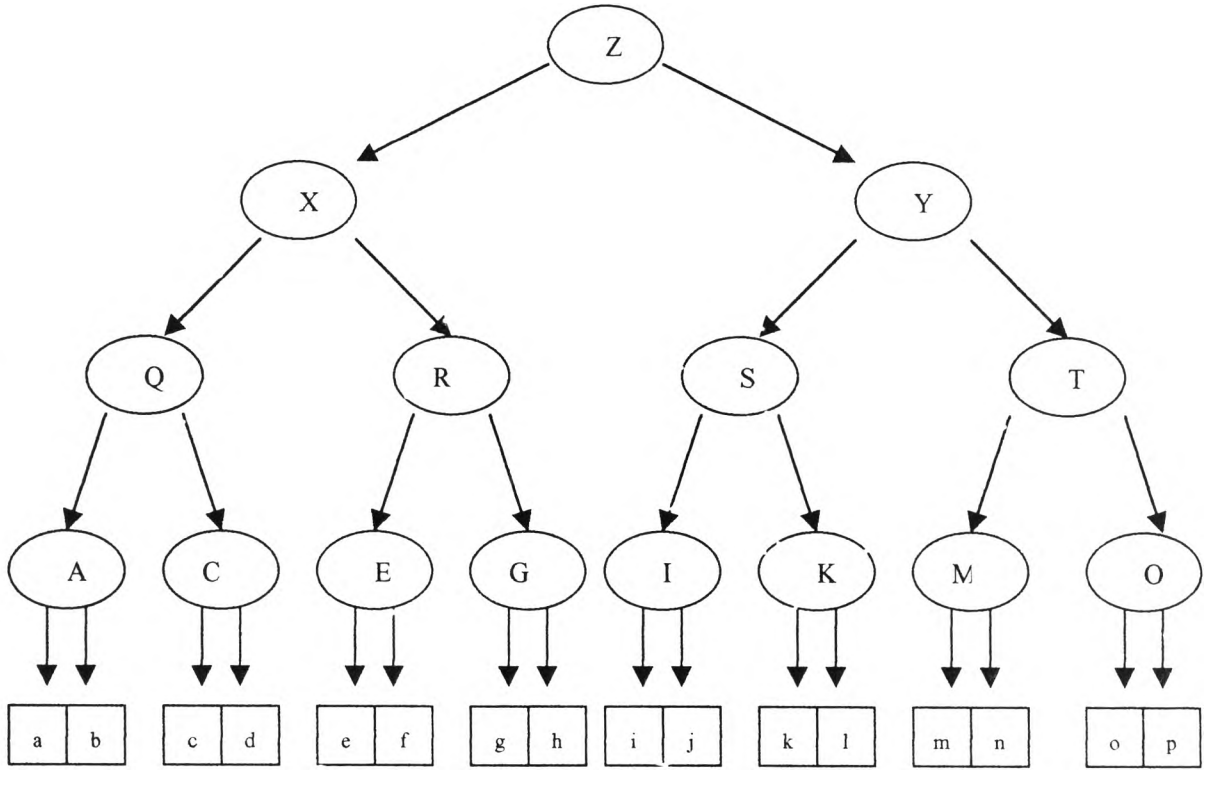
โครงสร้างแบบนี้มีข้อดีอยู่หลายประการ คือ

---

[53] ที่มา : Warwick Ford and Michael S. Baum, Id., p. 269

- จะมีเส้นทางของใบรับรองเพียงเส้นทางเดียวสำหรับผู้ใช้ใบรับรองปลายทางทุกคน เช่น a สามารถหาเส้นทางของใบรับรองของผู้ที่ติดต่อด้วยจนถึงผู้ประกอบการรับรอง Z เพียงเส้นทางเดียวก็เพียงพอ
- เมื่อนำโครงสร้างแบบนี้ไปใช้กับหน่วยงานที่มีลำดับการบังคับบัญชาอยู่แล้ว ก็จะเป็นการง่ายที่จะปฏิบัติและสามารถที่จะตรวจสอบความน่าเชื่อถือได้อย่างสะดวก

อย่างไรก็ตาม โครงสร้างแบบนี้ก็มีข้อเสียที่สำคัญที่เหมือนกันกับโครงสร้างการจัดลำดับแบบทั่วไปอยู่ก็คือ ความน่าเชื่อถือของผู้ประกอบการรับรองระดับสูง ถ้าผู้ประกอบการรับรองระดับสูงไม่ใช่หน่วยงานของทางราชการที่มีความน่าเชื่อถือสูง เช่น กระทรวงกลาโหม เป็นต้น ความน่าเชื่อถือของผู้ประกอบการรับรองระดับสูงก็จะเป็นประเด็นที่จะต้องพิจารณาอย่างมาก และมีความเสี่ยงสูงในประเด็นเรื่องความน่าเชื่อถือดังกล่าว



แผนภูมิ 2-13 [54] : โครงสร้างแบบการจัดลำดับจากบนลงล่าง

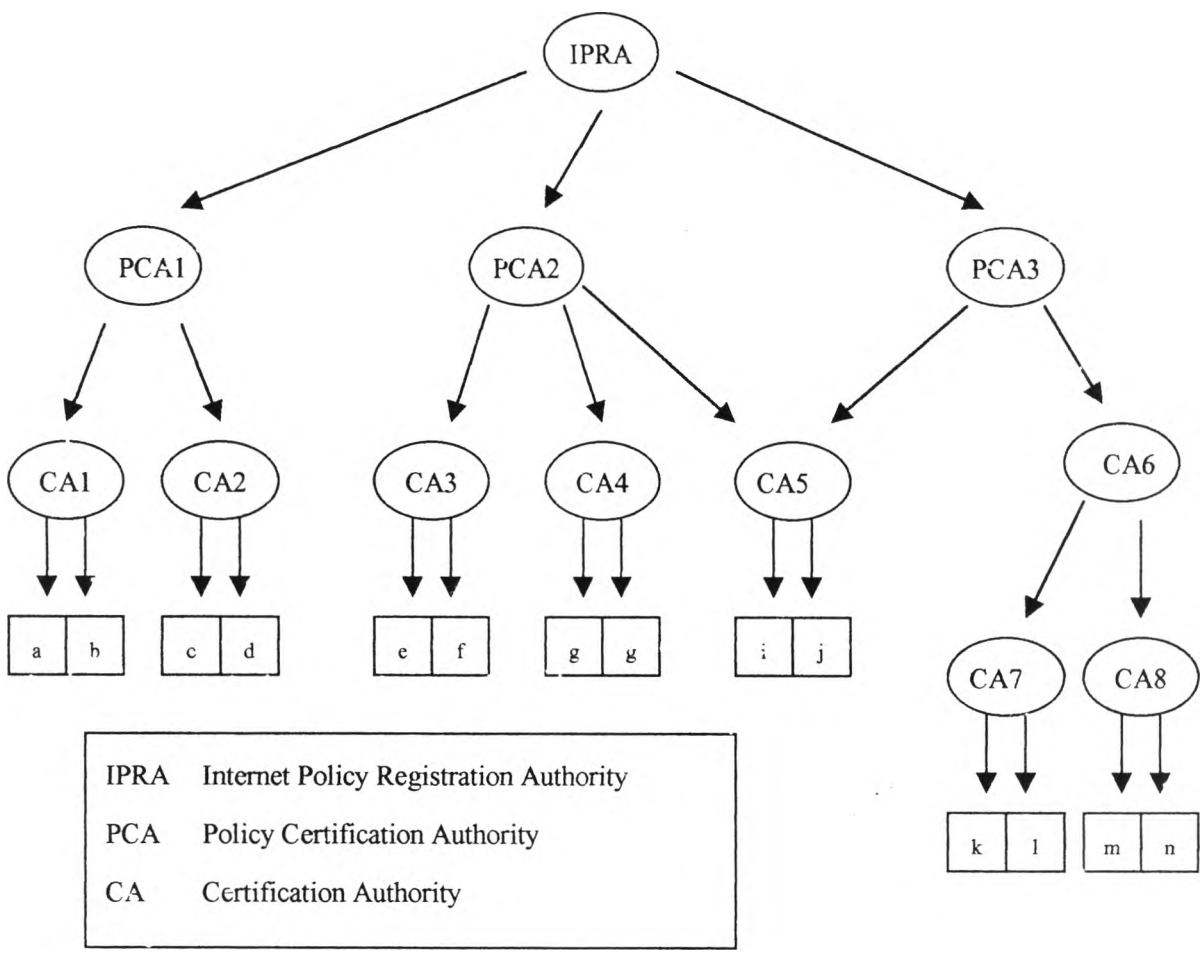
(Top-down Hierarchical Structure)

---

[54] ที่มา : Warwick Ford and Michael S. Baum, Id., p. 270

2.3.6.4 โครงสร้างพื้นฐานการส่งไปรษณีย์ที่คุ้มครองความเป็นส่วนตัว (Privacy Enhanced Mail Infrastructure)

ในปี 1993 ประชาคมอินเตอร์เน็ต (Internet Community) ได้พัฒนามาตรฐานของ โครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะ ที่เรียกว่าโครงสร้างพื้นฐานการส่งไปรษณีย์ที่คุ้มครองความเป็นส่วนตัว {Privacy Enhanced Mail (PEM) Infrastructure} ซึ่งในโครงสร้างดังกล่าวนี้ใช้โครงสร้างแบบจัดลำดับบนลงล่าง เป็นต้นแบบ



แผนภูมิ 2-14 [55] : โครงสร้างพื้นฐานการส่งไปรษณีย์ที่คุ้มครองความเป็นส่วนตัว {Privacy Enhanced Mail (PEM) Infrastructure}

---

[55] ที่มา : Warwick Ford and Michael S. Baum, Id., p. 270

ในโครงสร้างแบบนี้จะมีผู้ประกอบการรับรองอยู่สามประเภทดังต่อไปนี้

1. Internet Policy Registration Authority (IPRA) ซึ่งถือเป็นผู้ประกอบการรับรองในระดับสูงสุด ซึ่งดำเนินการโดยสถาบันเทคโนโลยีแห่งแมสซาชูเซ็ท (Massachusetts Institute of Technology : MIT) ภายใต้อุปถัมภ์ ของ Internet Society ซึ่งเป็นองค์กรระหว่างประเทศที่มิได้ค้ากำไร โดยทำหน้าที่แจกจ่ายกุญแจรหัสสาธารณะรากฐาน (Root Public Key) เพื่อการใช้โดยทั่วไปและจะทำหน้าที่รับรองนโยบายของผู้ประกอบการรับรองต่างๆ
2. Policy Certification Authority (PCA) จะเป็นหน่วยงานที่อยู่ในลำดับที่สองและถือเป็นผู้ประกอบการรับรองที่ได้รับการรับรองโดย IPRA เท่านั้น PCA จะต้องจดทะเบียนกับ IPRA และจะต้องตีพิมพ์นโยบายในการรับรองผู้ใช้และผู้ประกอบการรับรองลำดับรองลงมา (Certification Practice Statement) ทั้งนี้นโยบายที่แตกต่างกันก็เพื่อที่จะตอบสนองต่อกลุ่มกิจการที่แตกต่างกัน ตัวอย่างเช่น การให้ความมั่นใจในระดับสูงเพื่อกิจกรรมทางด้านการเงิน เป็นต้น
3. Lower-level Certification Authority (CAs) เป็นผู้ประกอบการรับรองที่เป็นตัวแทนขององค์กรหรือกลุ่มภูมิภาค

อย่างไรก็ตามโครงสร้างแบบนี้มีข้อแตกต่างจากโครงสร้างแบบจัดลำดับจากบนลงล่างอยู่ก็คือ Lower-level Certification Authority สามารถได้รับการรับรองจาก Policy Certification Authority ได้มากกว่าหนึ่งองค์กร (โปรดดูแผนภูมิที่ 2-14 ประกอบ) เช่น CA5 ได้รับการรับรองจากทั้ง PCA2 และ PCA3 เป็นต้น เพื่อสามารถให้เส้นทางของใบรับรองได้หลายทางโดยมีต่างนโยบายที่แตกต่างกันได้

PEM ได้กำหนดนโยบายของ Lower-level Certification Authority ไว้สามประเภทด้วยกัน (ซึ่งนโยบายดังกล่าวนี้จะมีผลต่อ PCA policy statement) ดังนี้[56]

1) An organizational คือ ผู้ประกอบการรับรองที่ออกใบรับรองให้แก่บุคคลที่เป็นสมาชิกบริษัท หน่วยงานรัฐบาล และสถาบันการศึกษา เป็นต้น เช่น ข้าราชการในหน่วยงานรัฐบาล นิสิตนักศึกษาในมหาวิทยาลัย เป็นต้น

---

[56] Warwick Ford and Michael S. Baum, Id., p. 273

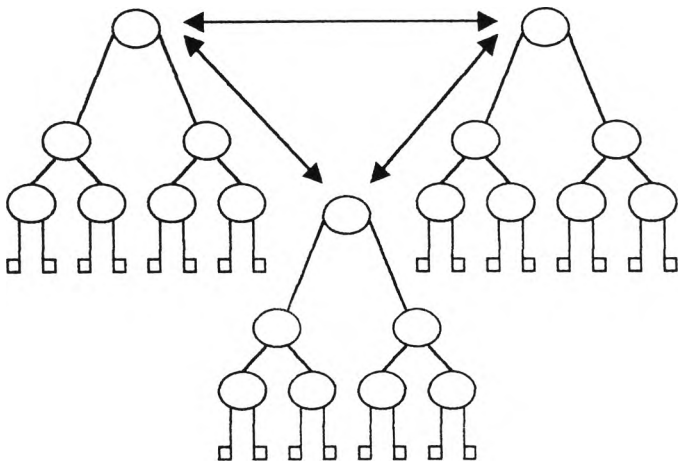
2) A Residential คือ ผู้ประกอบการรับรองให้แก่ผู้ร้องขอใบรับรองตามสถานที่อยู่ในทางภูมิศาสตร์ ซึ่งถูกคาดหวังว่าต่อไปหน่วยงานทางมหาดไทยจะเป็นดูแลในส่วนนี้

3) A PERSONA คือ ผู้ประกอบการรับรองในกรณีพิเศษ ซึ่งออกแบบมาเพื่อที่จะให้บริการออกใบรับรองกับบุคคลที่ไม่ต้องการเปิดเผยชื่อที่แท้จริงของตนเพื่อความเป็นส่วนตัว เมื่อใช้บริการปกป้องข้อมูลของ PEM (PEM data protection service)

2.3.6.5 ระบบป่าของโครงสร้างความสัมพันธ์ (Forest of Hierarchies)

ปัญหาหลักของโครงสร้างแบบการจัดลำดับนั้น เป็นการยากที่จะให้ทุกบุคคลหรือทุกองค์กรในโครงสร้างมีความไว้วางใจองค์กรที่จะทำหน้าที่เป็นผู้ประกอบการรับรองระดับสูง (Top-level Certification Authority) อย่างเช่น ในระดับประเทศ ถ้าจะให้ผู้ประกอบการรับรองของทุกประเทศมีผู้ประกอบการรับรองระดับสูงเป็นองค์กรเดียวกัน โดยองค์กรดังกล่าวเป็นองค์กรระหว่างประเทศ ในทางทฤษฎีถือเป็นเรื่องที่ดีมาก เนื่องจากผู้ประกอบการรับรองของทุกๆ ประเทศจะได้มีความมั่นใจในเรื่องนโยบายและมาตรฐานของผู้ประกอบการรับรองของประเทศอื่นเพราะมีผู้ประกอบการรับรองระดับสูงองค์กรเดียวกัน แต่ในทางปฏิบัติการกระทำดังกล่าวเป็นเรื่องของความสัมพันธ์ระหว่างประเทศ รวมทั้งเรื่องอำนาจอธิปไตยของแต่ละประเทศ (National Sovereignty) ซึ่งเป็นเรื่องที่มีความอ่อนไหวอย่างมาก จึงเป็นไปได้ยากหรือเป็นไปไม่ได้เลยในทางปฏิบัติ

ปัญหาเดียวกันนี้ก็เกิดในภาคธุรกิจ เพราะแต่ละธุรกิจก็มีความไว้วางใจในองค์กรแต่ละองค์กรไม่เหมือนกัน จึงเกิดเป็นแนวความคิดให้มีการนำเอาโครงสร้างความสัมพันธ์ระหว่างผู้ประกอบการรับรองต่างๆ ที่มีอยู่มาสร้างจุดเชื่อมโยงเฉพาะในระดับผู้ประกอบการรับรองระดับสูง



แผนภูมิ 2-15 [57] : โครงสร้างแบบป่า (Forest of Hierarchies)

โครงสร้างแบบนี้จะมีความสำคัญเป็นอย่างมาก เนื่องจากสามารถทำให้โครงสร้างความสัมพันธ์ระหว่างผู้ประกอบการรับรองที่มีอยู่อย่างกระจัดกระจายสามารถเชื่อมต่อเป็นระบบเดียวกัน ในขณะที่แต่ละโครงสร้างก็ยังสามารถมีลักษณะเฉพาะของตนเองได้

---

[57] ที่มา : Warwick Ford and Michael S. Baum, Id., p. 275