รายงานวิจัยฉบับสมบูรณ์

ลายมือชื่ออิเล็กทรอนิกส์และองค์กรออกใบรับรอง

(โครงการผลกระทบทางเศรษฐกิจส่วนรวมของ
การพาณิชย์อิเล็กทรอนิกส์ต่อประเทศไทย)

โดย สมเกียรติ ตั้งกิจวานิชย์
สถาบันวิจัยเพื่อการพัฒนาประเทศไทย

สนับสนุนโดย
สำนักงานกองทุนสนับสนุนการวิจัย (สกว.)

พฤศจิกายน 2542

สัญญาเลขที่ RDG01/0009/2542

รายงานวิจัยฉบับสมบูรณ์

ลายมือชื่ออิเล็กทรอนิกส์และองค์กรออกใบรับรอง

(โครงการผลกระทบทางเศรษฐกิจส่วนรวมของ
การพาณิชย์อิเล็กทรอนิกส์ต่อประเทศไทย)

ผู้วิจัย สมเกียรติ ตั้งกิจวานิชย์
สถาบันวิจัยเพื่อการพัฒนาประเทศไทย

สนับสนุนโดยสำนักงานกองทุนสนับสนุนการวิจัย (สกว.)

พฤศจิกายน 2542

กิตติกรรมประกาศ

การวิจัยนี้จะไม่สามารถสำเร็จลงได้หากไม่ได้รับความสนับสนุนจากหน่วยงานและบุคคลจำนวนมาก ก่อนอื่นผู้วิจัยขอขอบคุณสำนักงานกองทุนสนับสนุนการวิจัย (สกว.) ที่ให้ความสนับสนุนในการวิจัย

ผู้วิจัยยังได้ประโยชน์เป็นอย่างยิ่งจากการแลกเปลี่ยนความคิดเห็นกับคุณชัยชนะ มิตรพันธุ์ และได้เริ่มคิดประเด็นกฎหมายลายมือชื่ออิเล็กทรอนิกส์จากการระดมสมองกับคณะผู้แทนไทยที่เข้าร่วมในการประชุมเพื่อร่างข้อกำหนดมาตรฐานว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ของคณะกรรมาธิการด้านกฎหมายของสหประชาชาติ (UNCITRAL Uniform Rules on Electronic Signatures)

ผู้เชี่ยวชาญต่างชาติอีกหลายท่านยังมีส่วนช่วยให้ผู้วิจัยเข้าใจประเด็นต่าง ๆ ในรายงานฉบับนี้ได้ดีขึ้น ผู้เชี่ยวชาญเหล่านี้รวมถึง Dr. Gerold Herrman และ Mr. Renaud Soriel จาก UNCITRAL, Mr. Takeshi Shinohara จาก Nomura Research Institute, Mr. Tomoyuki Suga และ Mr. Hiroyuki Kato จาก Electronic Commerce Promotion Council of Japan (ECOM), Dr. Imho Kang จาก Korea Information Society Development Institute (KISDI), Mr. Steven Harrison จาก Government of Canada Public Key Infrastructure Project, Mr. Prabir Neogi จาก Task Force on Electronic Commerce, Industry Canada, Ms. K. Sue Bryant จาก Interdepartment PKI Task Force, Treasury Board of Canada และ Mr. Clement Leopng Ying Siong และคณะจาก National Computer Board, Singapore

ผู้วิจัยขอขอบคุณนักข่าวในสังกัดชมรมนักข่าวเทคโนโลยีสารสนเทศ (ITPC) โดยเฉพาะคุณกาญจนา กาญจนทวีที่ให้ความสนับสนุนในการประชาสัมพันธ์การนำเสนอผลการวิจัยนี้ ท้ายที่สุดนี้งานวิจัยนี้คงไม่สามารถสำเร็จลงได้หากปราศจากความช่วยเหลือของคุณเสาวลักษณ์ ชีวสิทธิยานนท์และคุณมาเรียม ชอลิฮี ซึ่งช่วยเตรียมการสัมมนา

บทสรุปสำหรับผู้บริหาร

ความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์เป็นสิ่งสำคัญที่จะสร้างความเชื่อมั่นให้เกิดขึ้นกับการพาณิชย์อิเล็กทรอนิกส์ ระบบอิเล็กทรอนิกส์ที่มีความปลอดภัยอย่างแท้จริงจะต้องมีความสามารถใน 4 ด้านคือ การระบุตัวบุคคลที่เกี่ยวข้อง (authenticity) การรักษาความลับของข้อมูล (confidentiality) การรักษาความถูกต้องของข้อมูล (integrity) และการป้องกันการปฏิเสธความรับผิดชอบ (non-repudiation) เทคโนโลยีที่เกี่ยวข้องกับการรักษาความปลอดภัยดังกล่าวคือลายมือชื่อหรือใบรับรองอิเล็กทรอนิกส์ ซึ่งใช้เทคโนโลยีเข้ารหัส (encryption technology)

ในรายงานฉบับนี้ผู้วิจัยได้ศึกษาเพื่อหาแนวทางที่เหมาะสมในการกำหนดนโยบายด้านความปลอดภัยในการดำเนินธุรกิจการพาณิชย์อิเล็กทรอนิกส์ ซึ่งรวมถึงการส่งเสริมให้เกิดองค์กรออกใบรับรองอิเล็กทรอนิกส์ (certification authority) การออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์ และการกำหนดนโยบายที่เกี่ยวข้องกับเทคโนโลยีการเข้ารหัส

การส่งเสริมให้เกิดองค์กรออกใบรับรองอิเล็กทรอนิกส์

ที่ผ่านมาการจัดตั้งองค์กรออกใบรับรองในประเทศไทยเป็นเรื่องที่ได้รับการกล่าวถึงมาก โดยมักมีข้อเสนอให้รัฐเป็นผู้จัดตั้งและให้บริการออกใบรับรองอิเล็กทรอนิกส์เอง อย่างไรก็ตาม ผู้วิจัยพบว่า ยังไม่มีหลักฐานว่ากลไกตลาดมีความล้มเหลวจนรัฐจำเป็นต้องเป็นผู้ให้บริการเอง

อย่างไรก็ตามรัฐอาจจำเป็นต้องเป็นผู้ให้บริการเองในการใช้งานในภาครัฐที่ต้องการความปลอดภัยสูง ด้วยเหตุผลด้านความมั่นคง นอกจากนี้รัฐยังสามารถมีบทบาทในการสนับสนุนผู้ประกอบธุรกิจออกใบรับรองได้ในกิจกรรมต่างๆ เช่นการวิจัยและพัฒนาตลอดจนการพัฒนาทรัพยากรมนุษย์ที่เกี่ยวข้องเป็นต้น

การออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์

ในประเด็นการออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์ ผู้วิจัยมีข้อเสนอแนะ 4 ประการ คือ ประการที่หนึ่ง ควรร่างกฎหมายให้มีความเป็นกลางทางเทคโนโลยี (technology neutrality) กล่าวคือ กฎหมายไม่ควรที่จะมุ่งใช้เฉพาะเทคโนโลยีใดเทคโนโลยีหนึ่ง เนื่องจากการออกกฎหมายที่มุ่งเน้นเฉพาะเทคโนโลยีจะบิดเบือนกลไกตลาดและจะทำให้กฎหมายล้าสมัยได้ง่ายเมื่อเกิดเทคโนโลยีใหม่

ประการที่สอง ธุรกิจการออกใบรับรองอาจเป็นธุรกิจที่อยู่ในข่ายที่ต้องกำกับดูแล อย่างไรก็ตามระบบใบอนุญาตไม่ได้เป็นเงื่อนไขที่จำเป็นในการกำกับดูแล ในกรณีที่รัฐต้องการนำระบบใบอนุญาตมาใช้ควบคู่กับการกำกับดูแล ระบบใบอนุญาตนั้นควรเป็นระบบใบอนุญาตแบบสมัครใจ (voluntary licensing) เพื่อป้องกันมิให้กฎหมายสร้างต้นทุนที่สูงขึ้นโดยไม่จำเป็นแก่องค์กรออกใบรับรองโดยเฉพาะในการออกใบรับรองที่ฝ่ายต่าง ๆ ที่เกี่ยวข้องมีความสัมพันธ์กันโดยสัญญาล่วงหน้า ทำให้มีความจำเป็นน้อยในการคุ้มครองจากความเสียหายจากการออกใบรับรองที่ผิดพลาด

ประการที่สาม กฎหมายลายมือชื่ออิเล็กทรอนิกส์ควรกำหนดหน้าที่ของฝ่ายต่าง ๆ ที่เกี่ยวข้องกับการใช้ลายมือชื่ออิเล็กทรอนิกส์คือผู้ลงลายมือชื่อ (signature holder) ผู้ใช้ลายมือชื่อ (relying party) และองค์กรออกใบรับรอง (certification authority) เพื่อให้การใช้ลายมือชื่ออิเล็กทรอนิกส์นั้นเป็นไปอย่างระมัดระวังไม่ก่อให้เกิดความเสียหายโดยไม่สมควรจากความประมาทหรือการกระทำที่เสี่ยงภัยเกินเหตุ นอกจากนี้กฎหมายลายมือชื่ออิเล็กทรอนิกส์อาจอนุญาตให้องค์กรออกใบรับรองสามารถกำหนดขอบเขตของความรับผิดชอบสูงสุดของตนได้ เพื่อส่งเสริมให้เกิดการให้บริการออกใบรับรองในประเทศไทย

ประการที่สี่ ผู้วิจัยเสนอว่ากฎหมายลายมือชื่ออิเล็กทรอนิกส์ของไทยควรยอมรับหลักการปฏิบัติเยี่ยงคนชาติ ซึ่งหมายถึงการยอมรับใบรับรองที่ออกโดยผู้ประกอบการต่างชาติ หากใบรับรองนั้นออกโดยมีมาตรฐานที่ไม่ต่ำกว่ามาตรฐานของประเทศไทย อย่างไรก็ตามรัฐบาลไทยจะต้องป้องกันไม่ให้เกิดการกีดกันจากต่างประเทศต่อใบรับรองที่ออกโดยผู้ประกอบการไทย โดยเสนอให้มีการกำหนดมาตรฐานขั้นต่ำซึ่งมีความโปร่งใส ซึ่งทุกประเทศที่ทำความตกลงร่วมกันจะต้องยอมรับใบรับรองที่ผ่านมาตรฐานดังกล่าว

นโยบายที่เกี่ยวข้องกับเทคโนโลยีเข้ารหัส

ในการกำหนดนโยบายเทคโนโลยีเข้ารหัส รัฐควรมุ่งรักษาสมดุลระหว่างการส่งเสริมการพาณิชย์อิเล็กทรอนิกส์และการคุ้มครองเสรีภาพในการสื่อสารของประชาชนกับการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยรัฐด้วยเหตุผลด้านความมั่นคง ผู้วิจัยเสนอว่าตัวอย่างการกำหนดนโยบายในลักษณะดังกล่าวที่ประเทศไทยสามารถอ้างอิงเป็นต้นแบบได้คือแนวทางการใช้เทคโนโลยีเข้ารหัสขององค์กรความร่วมมือด้านเศรษฐกิจและการพัฒนา (OECD)

รัฐควรเปิดกว้างให้ประชาชนและธุรกิจสามารถเลือกใช้เทคโนโลยีได้ตามความต้องการของตนเองโดยไม่มีข้อจำกัดเรื่องการนำเข้าและการใช้ ซึ่งจะเอื้ออำนวยให้เกิดการรับนวัตกรรมทางเทคโนโลยีใหม่ๆ จากต่างประเทศและส่งเสริมการใช้เทคโนโลยีดังกล่าวในการพาณิชย์

อิเล็กทรอนิกส์ อย่างไรก็ตามในอนาคตหน่วยงานด้านความมั่นคงและหน่วยงานที่บังคับใช้กฎหมายต่าง ๆ อาจเห็นความจำเป็นในการควบคุมเทคโนโลยีเข้ารหัส โดยเฉพาะการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยหน่วยงานรัฐเพื่อป้องกันการก่อการร้าย การก่ออาชญากรรม และการฟอกเงิน

ในกรณีดังกล่าวควรกำหนดขอบเขตการแทรกแซงของรัฐเฉพาะในกรณีการใช้เทคโนโลยีเข้ารหัสในการรักษาความลับของข้อมูลเท่านั้น โดยไม่ให้แทรกแซงการใช้เทคโนโลยีดังกล่าวในการระบุตัวบุคคล หรือรักษาความถูกต้องของข้อมูล และควรกำหนดหลักเกณฑ์ที่ชัดเจนในการอนุญาตให้รัฐเข้าถึงข้อมูลโดยชอบด้วยกฎหมายเช่น ให้ทำได้ต่อเมื่อได้รับคำสั่งหรือหมายศาลเท่านั้น

บทคัดย่อ

ในการทำธุรกรรมผ่านเครือข่ายอินเทอร์เน็ต การลงลายมือชื่อตามปรกติเป็นสิ่งที่ไม่สามารถทำได้และจำเป็นต้องอาศัยการใช้ "ลายมือชื่ออิเล็กทรอนิกส์" (electronic signature) ซึ่งได้รับการรับรองความถูกต้องจากองค์กรออกใบรับรอง (certification authority) อย่างไรก็ตามในปัจจุบันประเทศไทยยังไม่มีหน่วยงานดังกล่าว

ผู้วิจัยเสนอให้ภาคเอกชนเป็นผู้ดำเนินการให้บริการในการออกใบรับรอง และให้รัฐเป็นผู้กำกับดูแลการให้บริการดังกล่าวและเสนอแนวคิดในการออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์เพื่อรองรับการใช้เทคโนโลยีลายมือชื่ออิเล็กทรอนิกส์ใน 4 ประเด็นคือ ให้ออกกฎหมายที่มีความเป็นกลางทางเทคโนโลยี (technology neutral) ซึ่งเปิดให้กลไกตลาดสามารถเลือกเทคโนโลยีที่เหมาะสม ให้ระบบการขออนุญาตจัดตั้งหน่วยงานออกใบรับรองเป็นระบบใบอนุญาตแบบอัตโนมัติ ซึ่งผู้ประกอบการที่มีคุณสมบัติสอดคล้องกับเงื่อนไขที่กำหนดสามารถขอประกอบการได้ทันที ให้รับรองลายมือชื่ออิเล็กทรอนิกส์ที่ออกในต่างประเทศเหมือนลายมือชื่อที่ออกในประเทศไทย และให้มีการกำหนดความรับผิดชอบ (liability) สูงสุดของหน่วยงานออกใบรับรองเพื่อส่งเสริมธุรกิจดังกล่าวในระยะเริ่มต้น

ต่อประเด็นนโยบายเทคโนโลยีการเข้ารหัสเพื่อรักษาความลับของข้อมูล (encryption policy) ผู้วิจัยเสนอให้ออกกฎหมายให้รัฐสามารถใช้สิทธิในการถอดรหัสข้อมูลดังกล่าวได้ในกรณีที่การใช้ข้อมูลนั้นอาจมีผลต่อความมั่นคงของชาติ อย่างไรก็ตามการใช้อำนาจดังกล่าวจะต้องมีกลไกถ่วงดุลไว้เช่น ให้ทำได้โดยอาศัยอำนาจของศาลเท่านั้น เป็นต้น

Abstract

Electronic signature is necessary for identity authentication in online transactions. To ensure a secure signature system, a trusted third party is required. Such entity is called a "certification authority" (CA). Currently, there is no CA operating in Thailand. While it is often argued that the government should play a leading role in setting up a CA, we found no market failure and proposed that the private sector, not the government, should operate a CA. The government should play only a regulatory role if the industry is in need of regulation.

We also lay down a guideline for drafting an electronic signature law, which includes four important principles. Firstly, the law should be technological neutral in order to avoid distorting market decisions. Secondly, the licensing scheme, if required by the law, should be an automatic one. Thirdly, the law should recognize signatures issued by foreign CAs. Finally, liabilities of licensed CAs may be capped to promote the industry in its infancy.

Concerning encryption policy, we argued that no import nor export control of encryption technology is necessary. However, security needs may provide a rationale for state control of the technology. In that case, a balance should be strike between security and civic liberty. State access to secret signature keys should be allowed on a condition that such action is warranted by court order.

สารบัญ

บทที่ 1	ลายมือชื่อและใบรับรองดิจิตัล	1
บทที่ 2	ธุรกิจออกใบรับรอง	8
บทที่ 3	นโยบายควบคุมเทคโนโลยีเข้ารหัส	22
บทที่ 4	แนวทางในการออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์ในประเทศไทย	30
ภาคผนวก 1	ขั้นตอนในการขอใบรับรองดิจิตัล	38
ภาคผนวก 2	ตัวอย่างขั้นตอนการรับรองซึ่งกันและกัน	41

บทที่ 1 ลายมือชื่อและใบรับรองดิจิตัล

ความปลอดภัยในการทำธุรกรรมเป็นหัวใจของการพาณิชย์อิเล็กทรอนิกส์ ในบทนี้ผู้วิจัยจะกล่าวถึงการรักษาความปลอดภัยในการพาณิชย์อิเล็กทรอนิกส์ เทคโนโลยีและโครงสร้างพื้นฐานที่เกี่ยวข้องกับการรักษาความปลอดภัยดังกล่าว

1.1 ความปลอดภัยในการพาณิชย์อิเล็กทรอนิกส์และเทคโนโลยีที่เกี่ยวข้อง

ความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์เป็นสิ่งสำคัญที่จะสร้างความเชื่อมั่นให้เกิดขึ้นกับการพาณิชย์อิเล็กทรอนิกส์ทั้งการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและผู้บริโภค (B-to-C E-Commerce) และการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและธุรกิจ (B-to-B E-Commerce) ธุรกรรมอิเล็กทรอนิกส์ที่มีความปลอดภัยอย่างแท้จริงจะต้องเกิดขึ้นในระบบที่มีความสามารถใน 4 ด้านคือการระบุตัวบุคคล (authenticity) การรักษาความลับ (confidentiality) การรักษาความถูกต้อง (integrity) และการป้องกันการปฏิเสธความรับผิดชอบ (non-repudiation) ดังตารางที่ 1.1

ตารางที่ 1.1 ความสามารถของระบบการพาณิชย์อิเล็กทรอนิกส์ที่ปลอดภัย

ความสามารถ	ความหมาย
การระบุตัวบุคคล (authenticity)	สามารถระบุได้ว่าบุคคลที่ติดต่อด้วยนั้นเป็นบุคคลตามที่กล่าวอ้างหรือมีอำนาจหน้าที่ตามที่กล่าวอ้างจริง
การรักษาความลับ (confidentiality)	สามารถรักษาความลับมิให้มีผู้อื่นแอบดูข้อมูลที่เก็บไว้หรือข้อมูลส่งผ่านไปทางเครือข่าย
การรักษาความถูกต้อง (integrity)	สามารถรักษาความถูกต้องของข้อมูลมิให้มีการแก้ไขโดยไม่ปรากฏร่องรอย
การป้องกันการปฏิเสธความรับผิดชอบ (non-repudiation)	สามารถป้องกันการปฏิเสธความรับผิดชอบ จากฝ่ายต่าง ๆ ที่เกี่ยวข้องว่าไม่ได้มีการส่งหรือรับข้อมูล

ตัวอย่างของเทคโนโลยีที่ช่วยในการรักษาความปลอดภัยในการพาณิชย์อิเล็กทรอนิกส์ที่มีความสามารถครบทั้ง 4 ประการดังที่กล่าวมาข้างต้นคือ เทคโนโลยีการเข้ารหัสที่ใช้กุญแจลับ (secret key) คู่กับกุญแจสาธารณะ (public key) หรือที่จะเรียกสั้น ๆ ว่า "เทคโนโลยีการเข้ารหัสด้วยกุญแจสาธารณะ" ซึ่งเป็นเทคโนโลยีที่ใช้กุญแจดอกหนึ่งในการเข้ารหัสและใช้อีกดอกหนึ่งในการถอดรหัส

นอกจากเทคโนโลยีการเข้ารหัสด้วยกุญแจสาธารณะแล้ว เทคโนโลยีอื่น ๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยในการพาณิชย์อิเล็กทรอนิกส์ได้แก่ เทคโนโลยีการเข้ารหัสด้วยกุญแจลับเพียงดอกเดียว ซึ่งมีความสามารถครบทั้ง 4 ประการแต่ไม่สะดวกที่จะใช้ในสภาพแวดล้อมแบบเปิดเช่นเครือข่ายอินเทอร์เน็ต ส่วนเทคโนโลยีอื่น ๆ เช่นการใช้รหัสผ่าน (password) และการใช้หมายเลขประจำตัวบุคคล (PINS) จะมีความสามารถในการระบุตัวบุคคลแต่ไม่มีความสามารถอื่น ๆ ที่เหลือ ในขณะที่การใช้ลักษณะทางชีวภาพ (biometrics) เช่นลายนิ้วมือหรือเสียงจะสามารถระบุตัวบุคคลและการป้องกันการปฏิเสธความรับผิดชอบได้เท่านั้น แต่ไม่มีความสามารถอื่น ๆ

1.2 ลายมือชื่อและใบรับรองอิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์เป็นการประยุกต์ใช้เทคโนโลยีต่าง ๆ ดังกล่าวข้างต้นในการระบุตัวบุคคล ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างจากเทคโนโลยีเข้ารหัสด้วยกุญแจสาธารณะเรียกว่า "ลายมือชื่อดิจิตัล" (digital signature) ในการลงลายมือชื่อดิจิตัลกำกับข้อความที่ต้องการส่งผ่านทางเครือข่าย ผู้ส่งข้อความจะใช้กุญแจลับของตนในการลงลายมือชื่อโดยผ่านกระบวนการคำนวณทางคณิตศาสตร์ ผู้รับจะสามารถตรวจสอบความถูกต้องของลายมือชื่อดังกล่าวได้โดยใช้กุญแจสาธารณะของผู้ส่งที่แสดงอยู่ใน "ใบรับรองดิจิตัล" (digital certificate) ซึ่งมักจัดเก็บโดยบุคคลหรือองค์กรซึ่งเป็นผู้ออกใบรับรองนั้น นอกจากช่วยในการระบุตัวผู้ส่งข้อมูลแล้วการลงลายมือชื่อดิจิตัลยังป้องกันข้อมูลให้มีความถูกต้องไม่ถูกแก้ไขโดยไม่ทิ้งร่องรอยไว้ได้อีกด้วย

นอกเหนือไปจากกุญแจสาธารณะแล้ว ใบรับรองดิจิตัลยังแสดงข้อมูลอื่น ๆ อีกหลายอย่างเช่นใบรับรองดิจิตัลที่ออกตามมาตรฐาน X.509 v3 ซึ่งเป็นมาตรฐานที่แพร่หลายที่สุดจะมีข้อมูลดังต่อไปนี้

- หมายเลขของใบรับรอง (serial number)
- วิธีการที่ใช้ในการเข้ารหัสข้อมูล (algorithm)
- หน่วยงานที่ออก (issuer)
- เวลาที่ใบรับรองเริ่มใช้ได้ (starting time)
- เวลาที่ใบรับรองหมดอายุ (expiring time)
- ผู้ได้รับการรับรอง (subject)
- กุญแจสาธารณะของผู้ได้รับการรับรอง (subject's public key)
- ลายมือชื่อดิจิตัลของหน่วยงานที่ออกใบรับรอง (CA signature)

ใบรับรองดิจิตัลสามารถแบ่งตามลักษณะการใช้งานออกเป็นกลุ่ม ๆ ได้ดังนี้คือ

- ใบรับรองเครื่องแม่ข่าย (server certificate) เช่นใบรับรองเครื่องแม่ข่าย SSL ที่ใช้ทั่วไปในการพาณิชย์อิเล็กทรอนิกส์ ซึ่งจะมีชื่อของบริษัทที่เกี่ยวข้อง ชื่อโดเมนของเครื่อง กุญแจสาธารณะของเครื่อง เป็นต้น
- ใบรับรองบุคคล (personal certificate) หรือใบรับรองเครื่องลูกข่าย (client certificate) ซึ่งจะระบุชื่อบุคคลนั้นและข้อมูลอื่น ๆ เช่นรหัสไปรษณีย์อิเล็กทรอนิกส์หรือที่อยู่
- ใบรับรององค์กรออกใบรับรอง (certification authority certificate) ซึ่งจะมีชื่อองค์กรออกใบรับรองที่ได้รับการรับรอง และกุญแจสาธารณะขององค์กรนั้น และลายมือชื่อดิจิตัลขององค์กรออกใบรับรองที่ให้การรับรอง ซึ่งอาจเป็นการรับรองตนเอง (self-certified) ก็ได้ในกรณีที่องค์กรออกใบรับรองทั้งสองเป็นหน่วยงานเดียวกัน

ภาคผนวกที่ 1 แสดงขั้นตอนการขอใบรับรองดิจิตัลสำหรับเครื่องแม่ข่ายแบบ SSL ซึ่งนิยมใช้ในการพาณิชย์อิเล็กทรอนิกส์และการขอใบรับรองดิจิตัลสำหรับเครื่องลูกข่าย

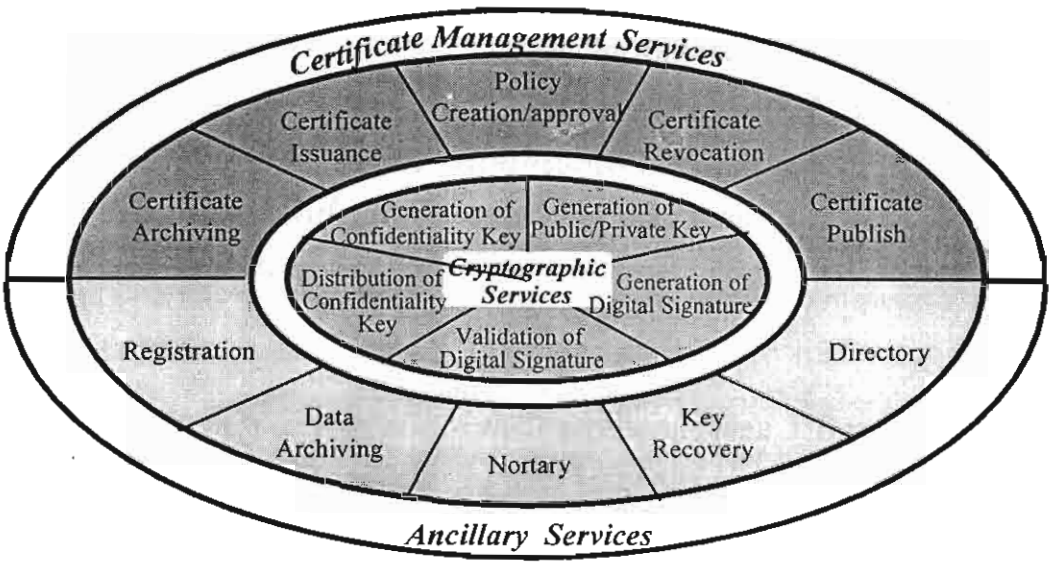
1.3 องค์กรออกใบรับรอง

การระบุตัวบุคคลโดยใช้ใบรับรองดิจิตัลอาจทำได้โดยการออกใบรับรองให้แก่บุคคลอื่นซึ่งรู้จักกันในลักษณะการแนะนำกันต่อเป็นทอด ๆ ในลักษณะของ "สายใยแห่งความเชื่อถือ" (web of trust) อย่างไรก็ตามการตรวจสอบการระบุตัวบุคคลในลักษณะดังกล่าวเป็นสิ่งที่มีความยุ่งยากมากและมีความน่าเชื่อถือต่ำ เนื่องจากเป็นการรับรองกันเป็นทอด ๆ โดยผู้รับรองแต่ละคนมีมาตรฐานในการรับรองที่แตกต่างกัน

โครงสร้างพื้นฐานซึ่งจะช่วยให้สามารถระบุตัวบุคคลได้อย่างสะดวกและมีความน่าเชื่อถือสูงคือหน่วยงานที่เรียกว่า "องค์กรออกใบรับรอง" (Certification Authority หรือ CA) หรือที่เรียกกันว่า "โครงสร้างพื้นฐานของระบบกุญแจสาธารณะ" (Public Key Infrastructure หรือ PKI) ซึ่งจะเป็นตัวกลางในการตรวจสอบและออกใบรับรองให้แก่ผู้อื่น ตามแนวทางนี้จะมีบุคคลต่าง ๆ ที่เกี่ยวข้องกัน 3 ฝ่าย (three-party model) คือ ผู้ถือใบรับรอง (certificate holder) ซึ่งเราอาจเรียกว่าเป็นบุคคลที่หนึ่ง ผู้ใช้ใบรับรองในการระบุตัวผู้ถือใบรับรอง (relying party) ซึ่งอาจเรียกว่าเป็นบุคคลที่สอง และองค์กรออกใบรับรองซึ่งอาจเรียกว่าบุคคลที่สาม หรือที่นิยมเรียกกันว่า "บุคคลที่สามที่เชื่อถือได้" (trusted third party)

องค์กรออกใบรับรองโดยทั่วไปจะมีบทบาทในการให้บริการใน 3 ด้านใหญ่ๆ คือ การให้บริการเทคโนโลยีเข้ารหัส (cryptographic service) บริการที่เกี่ยวข้องกับการออกใบรับรอง (certification management service) และบริการเสริม (ancillary service) ต่างๆ ดังมีรายละเอียดดังต่อไปนี้ (ดูภาพที่ 1.1)[1]

ภาพที่ 1.1 บริการต่าง ๆ ขององค์กรออกใบรับรอง



ที่มา: Certification Authority Working Group, ECOM

1. บริการเทคโนโลยีเข้ารหัสซึ่งจะประกอบไปด้วยการผลิตกุญแจลับ (generation of private key) การส่งมอบกุญแจลับ (distribution of private key) การผลิตกุญแจสาธารณะและกุญแจลับ (generation of public/private key) การผลิตลายมือชื่อดิจิตัล (generation of digital signature) และการรับรองลายมือชื่อดิจิตัล (validation of digital signature)
2. บริการที่เกี่ยวข้องกับการออกใบรับรองซึ่งประกอบไปด้วยการออกใบรับรอง (certificate issuance) การยกเลิกใบรับรอง (certificate revocation) การตีพิมพ์ใบรับรองเผยแพร่แก่บุคคลทั่วไป (certificate publishing) การเก็บต้นฉบับใบรับรอง (certificate archiving) และการกำหนดนโยบายการออกและอนุมัติใบรับรอง (policy creation/approval) เช่นขั้นตอนในการปฏิบัติงานในการออกใบรับรอง

[1] ผู้สนใจกรุณาดูรายละเอียดเพิ่มเติมใน Certification Authority Working Group, "*Certification Authority Guidelines (Alpha version)*", ECOM, http://www.ecom.or.jp/

3. บริการเสริมซึ่งได้แก่การบันทึก (registration) ข้อมูลต่างๆ ที่จำเป็นต้องใช้ในการออกหรือยกเลิกใบรับรอง การเก็บต้นฉบับข้อมูล (data achiving) เพื่อการตรวจสอบในระยะยาว การตรวจสอบสัญญาต่างๆ (notarial authentiation) การกู้กุญแจ (key recovery) ในกรณีที่ผู้ใช้ทำกุญแจของตนหาย การทำทะเบียน (directory) ข้อมูลต่างๆ ที่เกี่ยวข้องกับผู้ใช้บริการ เช่นที่อยู่ หมายเลขโทรศัพท์

1.4 สภาพแวดล้อมแบบเปิดและสภาพแวดล้อมแบบปิด

เราอาจแบ่งสภาพแวดล้อมในการออกใบรับรองออกเป็นสภาพแวดล้อมแบบเปิด (open PKI) และสภาพแวดล้อมแบบปิด (closed PKI) ในสภาพแวดล้อมแบบเปิดซึ่งพบมากในการค้าปลีกผ่านเครือข่ายอินเทอร์เน็ตและการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและผู้บริโภคอื่น ๆ ฝ่ายต่าง ๆ ที่เกี่ยวข้องมักไม่รู้จักกันมาก่อนและไม่มีความสัมพันธ์ในเชิงสัญญา (contractual relationship) กันล่วงหน้า ในสภาพแวดล้อมนี้บทบาทขององค์กรออกใบรับรองคือ การออกใบรับรองตัวบุคคล (identity certificate) เพื่อให้ทั้งสองฝ่ายสามารถระบุตัวบุคคลอีกฝ่ายหนึ่งได้

ส่วนในสภาพแวดล้อมแบบปิด ฝ่ายต่าง ๆ ที่เกี่ยวข้องจะรู้จักกันและมักมีความสัมพันธ์ในเชิงสัญญากันอยู่แล้ว ซึ่งพบบ่อยในการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจ-ธุรกิจเช่นการซื้อขายสินค้าผ่านเครือข่ายเอ็กซ์ทราเน็ต (extranet) หรือเครือข่ายอีดีไอ (EDI) การติดต่อระหว่างบุคคลต่าง ๆ ในองค์กรเดียวกันผ่านเครือข่ายอินทราเน็ต (intranet) หรือแม้กระทั่งการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและผู้บริโภคในบางรูปแบบเช่นการทำธุรกรรมด้านการเงินระหว่างธนาคารและลูกค้าของธนาคาร เป็นต้น ในบางกรณีบุคคลที่สองและบุคคลที่สามอาจเป็นบุคคลเดียวกัน ทำให้เหลือเพียงฝ่ายต่าง ๆ ที่เกี่ยวข้องเพียงสองฝ่าย (two-party model) เช่นธนาคารเป็นผู้ออกใบรับรองให้แก่ลูกค้าและใช้ใบรับรองนั้นในการระบุตัวลูกค้าของตนในการทำธุรกรรม หรือบริษัทเป็นผู้ออกใบรับรองให้แก่พนักงานและใช้ใบรับรองนั้นในการกำหนดสิทธิในการใช้เครื่องคอมพิวเตอร์ ในสภาพแวดล้อมนี้บทบาทขององค์กรออกใบรับรองอาจเปลี่ยนจากการออกใบรับรองตัวบุคคลไปสู่การออกใบรับรองสิทธิหรืออำนาจหน้าที่ (authority certificate) แทน เช่นการออกใบรับรองว่าผู้สั่งซื้อสินค้าเป็นเจ้าหน้าที่ซึ่งมีอำนาจในการสั่งซื้อจริง

ลักษณะเฉพาะของการออกใบรับรองในสภาพแวดล้อมทั้งสองแบบนี้เป็นประเด็นที่มีความสำคัญในการกำหนดนโยบายและออกกฎหมายที่เกี่ยวข้องดังที่จะกล่าวถึงในบทที่ 4

1.5 ข้อจำกัดในการระบุตัวบุคคลด้วยใบรับรองดิจิตัล

แม้ว่าการใช้ใบรับรองดิจิตัลจะช่วยแก้ปัญหาความปลอดภัยในการทำธุรกรรมทางการพาณิชย์อิเล็กทรอนิกส์ได้ในระดับหนึ่งจากการช่วยให้ฝ่ายต่าง ๆ สามารถระบุตัวบุคคลอื่นที่ติดต่อด้วยได้ก็ตาม วิธีการตรวจสอบและออกใบรับรองในปัจจุบันยังมีข้อจำกัดที่สำคัญหลายประการคือ

- การระบุตัวบุคคลด้วยใบรับรองดิจิตัลยึดหลักในการระบุตัวบุคคลด้วยกุญแจลับซึ่งเป็นสิ่งที่บุคคลนั้นมีในครอบครอง ในทางปฏิบัติผู้ครอบครองกุญแจลับอาจไม่ใช่เจ้าของใบรับรองนั้นก็ได้ซึ่งแตกต่างจากการระบุตัวบุคคลด้วยลักษณะทางชีวภาพ (biometrics)
- ใบรับรองตามมาตรฐาน X. 509 v3 ซึ่งเป็นมาตรฐานหลักไม่มีข้อมูลที่เพียงพอในการระบุตัวบุคคลในบางสถานการณ์เช่น ไม่ระบุอายุหรือเพศของผู้ถือใบรับรอง ซึ่งอาจจำเป็นต้องใช้ในเว็บไซต์บางแห่งเช่นเว็บไซต์ที่ให้บริการเฉพาะผู้ที่มีอายุเกิน 20 ปีขึ้นไป หรือเว็บไซต์ที่ให้บริการเฉพาะผู้หญิง
- ในการใช้ใบรับรองตามมาตรฐาน X. 509 v3 ผู้ถือใบรับรองไม่สามารถเลือกเปิดเผยข้อมูลบางส่วนในใบรับรองได้แต่ต้องเปิดเผยทั้งหมด ทั้งที่ในบางสถานการณ์ข้อมูลอื่นในใบรับรองอาจไม่เกี่ยวข้องในการใช้เลยก็ตามเช่นในการใช้เว็บไซต์ที่จำกัดเพียงอายุของผู้ใช้ ผู้ใช้อาจไม่ต้องการเปิดเผยชื่อและที่อยู่
- การตรวจสอบหลักฐานว่าบุคคลนั้นเป็นบุคคลตามที่กล่าวอ้างหรือไม่นั้นมักใช้วิธีง่าย ๆ เพื่อประหยัดต้นทุนในการตรวจสอบ ทำให้ผู้ใช้ใบรับรองในการระบุตัวผู้อื่นไม่มีความมั่นใจอย่างเต็มที่[2]
- การออกใบรับรองตัวบุคคลในการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจกับผู้บริโภคส่วนใหญ่ยังเป็นการออกใบรับรองให้แก่เฉพาะธุรกิจ หรือการรับรองเครื่องแม่ข่ายแบบ SSL ซึ่งทำให้ผู้บริโภคสามารถระบุตัวผู้ขายได้ แต่ผู้ขายยังไม่สามารถระบุตัวผู้ซื้อได้ ทั้งนี้เนื่องจากผู้ซื้อยังไม่มีแรงจูงใจในการขอใบรับรองดังกล่าว

[2] ตัวอย่างเช่นการตรวจสอบตัวบุคคลที่ขอใบรับรองชั้นที่ 1 (Class I) ของบริษัท Verisign ซึ่งเป็นบริษัทออกใบรับรองรายใหญ่ทำโดยการส่งไปรษณีย์อิเล็กทรอนิกส์ไปหาบุคคลผู้นั้นเท่านั้น ส่วนการตรวจสอบตัวบุคคลในการออกใบรับรองชั้นที่ 2 (Class II) ของบริษัทดังกล่าว ทำโดยใช้ข้อมูลทุติยภูมิ (secondary data) เช่นตรวจสอบกับฐานข้อมูลของหน่วยงานให้สินเชื่อแก่ผู้บริโภคแทนการตรวจสอบด้วยตนเอง

จะเห็นได้ว่าข้อจำกัดเหล่านี้บางข้อเป็นเพียงข้อจำกัดที่เกิดจากมาตรฐานหรือวิธีการในการออกใบรับรองในปัจจุบัน ในขณะที่บางข้อเป็นข้อจำกัดที่แท้จริงของเทคโนโลยีใบรับรองดิจิตัล เทคโนโลยีและวิธีการในการระบุตัวบุคคลที่ใช้ในการพาณิชย์อิเล็กทรอนิกส์ในอนาคตจึงอาจแตกต่างจากเทคโนโลยีและวิธีการที่ใช้ในปัจจุบันเป็นอย่างมาก ซึ่งผู้กำหนดนโยบายหรือผู้ยกร่างกฎหมายที่เกี่ยวข้องจะต้องพิจารณาถึงพัฒนาการดังกล่าวด้วย

บทที่ 2 ธุรกิจออกใบรับรอง

ในบทนี้ผู้วิจัยจะวิเคราะห์ถึงธุรกิจออกใบรับรองในด้านขอบเขตของสินค้าและบริการ โมเดลในการทำธุรกิจ โครงสร้างต้นทุน รายได้ บุคลากรและระดับการใช้เทคโนโลยีเพื่อเป็นข้อมูลพื้นฐานแก่ผู้สนใจ เนื่องจากธุรกิจดังกล่าวเป็นธุรกิจใหม่ซึ่งยังไม่มีในประเทศไทย โดยจะใช้กรณีศึกษาของบริษัทผู้ประกอบการรายใหญ่ 2 แห่งคือบริษัท Verisign ของในสหรัฐและบริษัท Entrust ของแคนาดาเป็นหลัก[1] นอกจากนี้ผู้วิจัยจะกล่าวถึงความเคลื่อนไหวของการยอมรับใบรับรองซึ่งกันและกัน (cross-certification) ซึ่งจะช่วยให้ใบรับรองที่ออกโดยองค์กรออกใบรับรองแห่งหนึ่งสามารถใช้กับออกใบรับรองแห่งอื่นได้

2.1 สินค้าและบริการ

Verisign เป็นบริษัทที่แยกตัวมาจากบริษัท RSA Security Inc ซึ่งเป็นเจ้าของเทคโนโลยีกุญแจสาธารณะ RSA ซึ่งเป็นที่รู้จักทั่วไปเมื่อปี 1995 ส่วนบริษัท Entrust เป็นบริษัทที่แยกตัวมาจากบริษัท Nortel Network Corp. เมื่อปี 1998 บริษัททั้งสองเป็นธุรกิจสร้างความเชื่อถือในการสื่อสารในเครือข่ายอินเทอร์เน็ต (Internet-based trust service) หรือการเป็นองค์กรออกใบรับรองให้แก่ธุรกิจและบุคคลทั่วไป บริษัททั้งสองแห่งมีสินค้าและบริการที่แตกต่างกันพอสมควรกล่าวคือบริษัท Verisign จะเน้นหนักในการออกใบรับรองให้แก่ลูกค้า ในขณะที่บริษัท Entrust จะเน้นหนักในการขายซอฟต์แวร์และเทคโนโลยีในการรักษาความปลอดภัยของตน

บริการของบริษัท Verisign ได้แก่

- การออกใบรับรองดิจิตัลแก่เว็บไซต์ของธุรกิจซึ่งส่วนใหญ่เป็นการรับรองเครื่องแม่ข่ายแบบ SSL ที่นิยมใช้ในการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจกับผู้บริโภค (B-to-C E-Commerce)
- การออกใบรับรองดิจิตัลแก่เครื่องแม่ข่ายแบบ SSL ในเครือข่ายอินทราเน็ต (intranet) และเครือข่ายเอ็กซ์ทราเน็ต (extranet) ของบริษัทขนาดใหญ่เช่น

[1] สาเหตุที่ผู้วิจัยใช้ตัวอย่างทั้งสองเนื่องจากเหตุผล 2 ประการคือ ประการแรกบริษัททั้งสองมีความก้าวหน้าในการให้บริการออกใบรับรองมากที่สุดและมีการลงทุนในประเทศต่าง ๆ ทั่วโลกเช่น บริษัท Verisign มีการลงทุนในประเทศญี่ปุ่นตลอดจนประเทศอื่น ๆ ในเอเชีย และอาจให้บริการแก่ผู้ใช้กลุ่มต่าง ๆ ในประเทศไทยในอนาคต ประการที่สองบริษัททั้งสองเป็นธุรกิจที่จดทะเบียนในตลาดหลักทรัพย์สหรัฐซึ่งจะต้องรายงานผลการดำเนินการแก่คณะกรรมการกำกับดูแลตลาดหลักทรัพย์ (US Stock Exchange Commission) อย่างละเอียดสม่ำเสมอ ทำให้สามารถใช้เป็นแหล่งข้อมูลในการวิจัย

บริษัทข้ามชาติและสถาบันการเงินต่าง ๆ ในการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจกับธุรกิจ (B-to-B E-Commerce)

- การออกใบรับรองดิจิตัลในนามหน่วยงานอื่นโดยบริการที่เรียกว่า Affiliate Certificate Service โดยหน่วยงานอื่นนั้นอาจเป็นเว็บไซต์ที่เป็นพอร์ตอล (portal) หรือชุมชนอิเล็กทรอนิกส์ (community) ซึ่งต้องการให้สมาชิกของตนสามารถระบุตัวกันได้
- การออกใบรับรองดิจิตัลแก่บุคคลทั่วไปหรือที่เรียกว่าใบรับรองเครื่องลูกข่าย (client certificate)
- การให้บริการเสริมต่าง ๆ เช่นการทำเช่าพื้นที่ของเว็บไซต์ (Web hosting) การออกใบแจ้งหนี้ (billing) การจัดทำรายงานการใช้บริการ (report generation) ในลักษณะเดียวกับการให้บริการระบบ (system integration) ในธุรกิจคอมพิวเตอร์โดยทั่วไป

ส่วนสินค้าและบริการของบริษัท Entrust ได้แก่

- ผลิตภัณฑ์ที่ใช้ในการบริหารองค์กรออกใบรับรอง (Authority and Administration Solution) โดยให้ลูกค้าเป็นผู้ติดตั้ง (install) และใช้ (maintain) ผลิตภัณฑ์เหล่านั้นเอง
- การออกใบรับรองต่าง ๆ เช่นใบรับรองเครื่องแม่ข่ายและเครื่องลูกข่าย และบริการประทับเวลาอิเล็กทรอนิกส์ (timestamp)
- ผลิตภัณฑ์ที่ช่วยรักษาความปลอดภัยให้แก่โปรแกรมประยุกต์ต่าง ๆ เช่น โปรแกรมไปรษณีย์อิเล็กทรอนิกส์

ตารางที่ 2.1 และ 2.2 แสดงอัตราค่าบริการในการออกใบรับรองของ Verisign และ Entrust ตามลำดับ

จากรายงานประจำปีต่อคณะกรรมการกำกับดูแลตลาดหลักทรัพย์สหรัฐ จนถึงเมื่อต้นปี 1999 บริษัท Versign ได้ออกใบรับรองให้แก่เว็บไซต์ไปแล้วประมาณ 1 แสนแห่งและแก่ผู้ใช้ทั่วไปอีกประมาณ 3 ล้านคน ในขณะที่บริษัท Entrust ได้ให้สิทธิในการใช้ซอฟต์แวร์ด้านความปลอดภัย (software licensing) แก่หน่วยงานต่าง ๆ ไปแล้วกว่า 500 แห่ง

ตารางที่ 2.1 ค่าบริการในการออกใบรับรองประเภทต่าง ๆ ของบริษัท Verisign

ชื่อของใบรับรอง	ชนิดของใบรับรอง	แนวทางการตรวจสอบในการออกใบรับรอง	ค่าบริการ	ความรับผิดชอบสูงสุด
Class 1	บุคคล	ตรวจสอบเลขที่ไปรษณีย์อิเล็กทรอนิกส์ (E-mail address) ของผู้ขอใบรับรองนั้น	$ 9.95 ต่อปี	$ 100
Class 2	บุคคล	ตรวจสอบผู้ขอใบรับรองโดยสืบค้นเทียบกับข้อมูลในฐานข้อมูลผู้บริโภคเช่นฐานข้อมูลของ Equifax	$ 19.95 ต่อปี	$ 5,000
Class 3	บุคคล	ตรวจสอบผู้ขอใบรับรองโดยตรวจสอบภูมิหลัง (background check) และการสืบสวน (investigative service)	ปีแรก $ 290 ต่ออายุ $ 75	$ 100,000
Secure Server	แม่ข่าย	ตรวจสอบผู้ขอใบรับรองโดยตรวจสอบภูมิหลัง (background check) และการสืบสวน (investigative service)	ปีแรก $ 290 ต่ออายุ $ 75	$ 100,000

ที่มา: Versign

ตารางที่ 2.2 ราคาของผลิตภัณฑ์และบริการของบริษัท Entrust

ผลิตภัณฑ์หรือบริการ	ราคา
ผลิตภัณฑ์ในการบริหารออกใบรับรอง (Entrust Authority and Admin)	$ 25,000 ต่อเครื่องแม่ข่าย
ผลิตภัณฑ์ด้านไดเร็กทอรี่ (Directory)	$ 3,000 ในกรณีที่ผู้ใช้น้อยกว่า 1,000 คน $ 3,000 และค่าบริการต่อหัวผู้ใช้ในกรณีที่ผู้ใช้มากกว่า 1,000 คน
บริการให้การรับรองแก่องค์กร	$ 159 ต่อจำนวนผู้ใช้ (เครื่องแม่ข่าย/ลูกข่าย) 1 ราย

ที่มา: Entrust

2.2 รายได้และต้นทุนในการประกอบการ

ตารางที่ 2.3 แสดงผลการประกอบการของบริษัททั้งสองในปี 1996-1998 จากตารางจะเห็นว่าบริษัททั้งสองยังคงขาดทุนอยู่อย่างต่อเนื่อง เนื่องจากมีค่าใช้จ่ายสูงกว่ารายได้[3]

ภาพที่ 2.1 แสดงตัวอย่างของโครงสร้างของค่าใช้จ่ายของทั้งสองบริษัทในปี 1998 จากภาพจะเห็นว่าบริษัททั้งสองแห่งมีต้นทุนในการประกอบการในรูปของต้นทุนทางตรงในการสร้างรายได้ (cost of revenue) จากการการออกใบรับรองไม่สูงนักคือเพียงประมาณร้อยละ 12.7 ในกรณีของ Entrust ซึ่งมีรายได้ส่วนใหญ่จากการจำหน่ายซอฟต์แวร์ และประมาณร้อยละ 31.3 ในกรณีของ Verisign ซึ่งมีรายได้ส่วนใหญ่จากการออกใบรับรอง[4] ต้นทุนส่วนอื่น ๆ ที่เหลือส่วนใหญ่เป็นต้นทุนในการดำเนินงาน (operating cost) เช่น การขายและการตลาด การวิจัยและพัฒนาตลอดจนต้นทุนอื่น ๆ เช่นค่าใช้จ่ายพิเศษ (special charge) ในการซื้อกิจการอื่น ๆ ซึ่งมีเทคโนโลยีในการรักษาความปลอดภัยของข้อมูล

ในไตรมาสแรกแรกของปี 1999 บริษัท Entrust เริ่มมีกำไรจากการประกอบการ ในขณะที่บริษัท Verisign ยังคงขาดทุนอย่างต่อเนื่องอยู่ อย่างไรก็ตามนักวิเคราะห์ส่วนใหญ่มีความเห็นว่า Verisign มีโมเดลในการดำเนินธุรกิจที่ดีกว่า Entrust กล่าวคือ Verisign มีรายได้ส่วนสำคัญมาจากการรับบริการการรักษาความปลอดภัยให้แก่บริษัทลูกค้าซึ่งทำให้บริษัทมีรายได้จากค่าสมาชิกอย่างสม่ำเสมอ ในขณะที่ Entrust มีรายได้ส่วนใหญ่จากการจำหน่ายซอฟต์แวร์ในการรักษาความปลอดภัยของเว็บไซต์ให้แก่ลูกค้าซึ่งเป็นรายได้ครั้งเดียว[5]

---

[3] ข้อสรุปในทำนองเดียวกันยังใช้ได้กับธุรกิจรับรองความถูกต้องในประเทศอื่นเช่น Netrust ในสิงคโปร์ซึ่งจากการสัมภาษณ์พบว่า*ยังคงขาดทุนอยู่อย่างต่อเนื่องเช่นเดียวกัน*

[4] ต้นทุนทางตรงในการสร้างรายได้ (cost of revenue) ในการออกใบรับรองรวมถึงต้นทุนทางด้านสถานที่และเครื่องคอมพิวเตอร์ในการออกใบรับรอง การให้การสนับสนุนผู้ใช้ (customer support) การฝึกอบรมและให้คำปรึกษาผู้ใช้ ตลอดจนค่าประกันภัยต่าง ๆ

[5] Dow Jones Business News, Investors See Differences in Tow Leading Web Security Companies, September 1, 1999

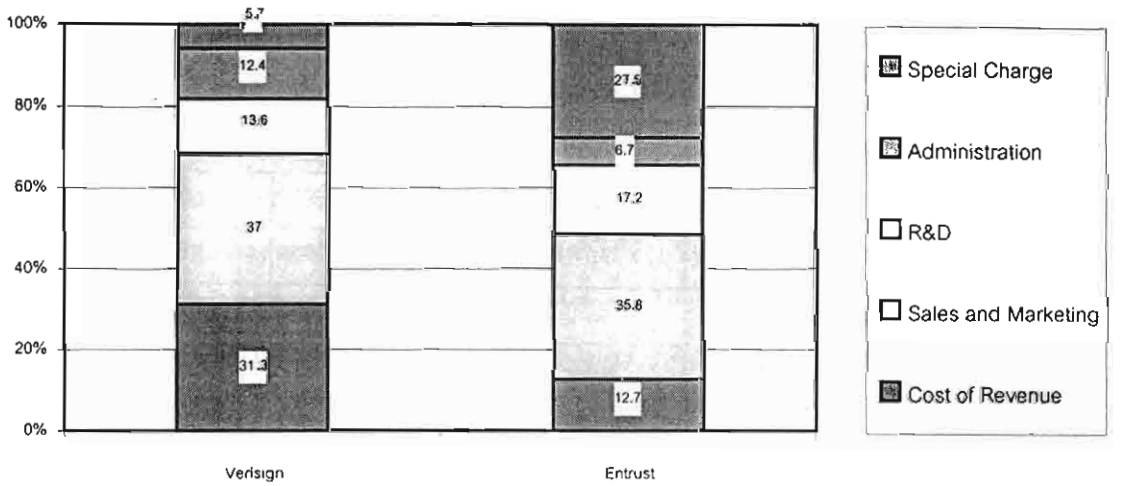
ตารางที่ 2.3 ผลการประกอบการของ Verisign และ Entrust ในระหว่างปี 1996-1998

(หน่วย: พันดอลลาร์สหรัฐ)

	Verisign			Entrust		
	1996	1997	1998	1996	1997	1998
1. รายได้รวม	1,356	13,356	38,930	12,802	25,006	48,988
2. รวมค่าใช้จ่ายโดยตรง	2,791	9,689	19,454	3,550	4,916	9,531
3. ค่าใช้จ่ายในด้านการตลาด	4,885	11,826	22,943	3,858	11,193	26,802
4. ค่าวิจัยและพัฒนา	2,058	5,303	8,435	2,874	5,692	12,840
5. ค่าบริหาร	2,681	5,039	7,688	2,464	3,695	5,046
6. ค่าใช้จ่ายอื่น ๆ	-	2,800	3,555	-	-	20,564
7. รวมค่าใช้จ่ายในการดำเนินงาน	12,415	34,657	62,075	9,196	20,580	65,252
8. รายได้จากการดำเนินงาน	(11,059)	(21,301)	(23,145)	56	(490)	(25,795)
9. รายได้อื่น ๆ	(67)	1,174	2,120	-	723	1,807
10. รายได้ก่อนหักประโยชน์จากภาษี	(11,126)	(20,127)	(21,025)	56	233	(23,988)
11. ประโยชน์จากภาษีรายได้	838	1,538	1,282	331	281	160
12. รายได้สุทธิ	(10,288)	(18,589)	(19,743)	387	514	(23,828)

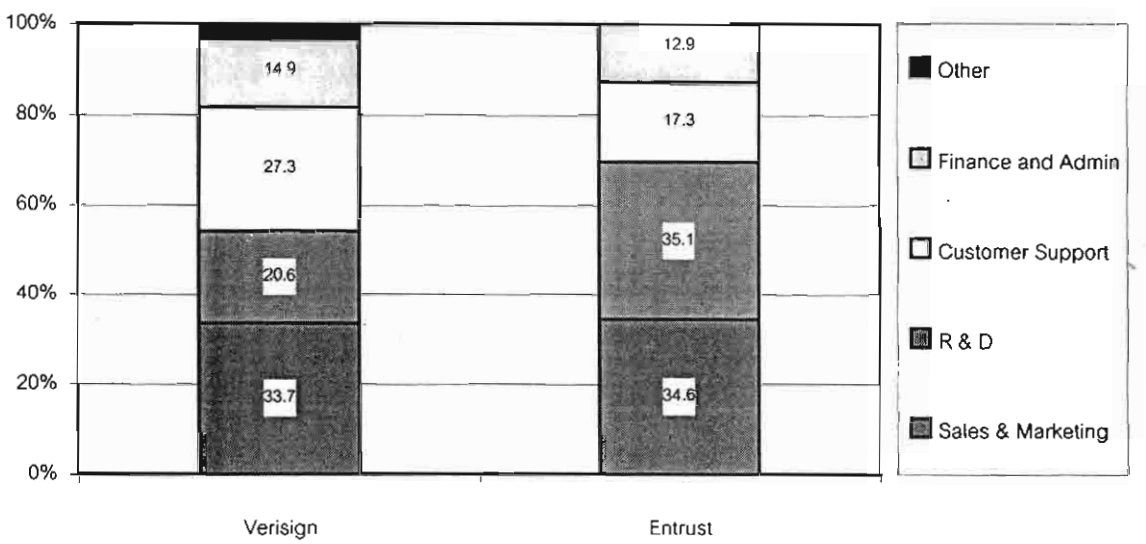
ที่มา: คณะกรรมการกำกับดูแลตลาดหลักทรัพย์สหรัฐ (Security Exchange Commission)

ภาพที่ 2.1 โครงสร้างต้นทุนของธุรกิจออกใบรับรอง



ที่มา: สถาบันวิจัยเพื่อการพัฒนาประเทศไทย จากเอกสารรายงานคณะกรรมการกำกับดูแลตลาดหลักทรัพย์สหรัฐ (Security Exchange Commission)

ภาพที่ 2.2 โครงสร้างบุคลากรของธุรกิจออกใบรับรอง



ที่มา: สถาบันวิจัยเพื่อการพัฒนาประเทศไทย จากเอกสารรายงานคณะกรรมการกำกับดูแลตลาดหลักทรัพย์สหรัฐ (Security Exchange Commission)

2.3 บุคลากรและระดับเทคโนโลยี

ภาพที่ 2.2 แสดงตัวอย่างของโครงสร้างบุคลากรปลายปี 1998 ของ Verisign และ Entrust ซึ่งมีพนักงานทั้งสิ้น 315 และ 456 คนตามลำดับ จากภาพจะเห็นว่าองค์กรออกใบรับรองทั้งสองแห่งมีพนักงานด้านขายและการตลาด (sales & marketing) ประมาณ 1 ใน 3 ของพนักงานทั้งหมดและเป็นกลุ่มที่ใหญ่ที่สุด รองลงมาคือพนักงานฝ่ายวิจัยและพัฒนา (R&D) หรือพนักงานที่ทำหน้าที่ให้ความช่วยเหลือลูกค้า (customer support) ซึ่งต้องมีความสามารถด้านเทคนิครวมกันอีกประมาณร้อยละ 50 ที่เหลือเป็นพนักงานด้านการเงินและธุรกิจ (finance & administration) และพนักงานอื่น ๆ

ภาพที่ 2.3 เปรียบเทียบระดับการใช้เทคโนโลยีของบริษัททั้งสองกับบริษัทในธุรกิจการพาณิชย์อิเล็กทรอนิกส์อื่น ๆ คือบริษัท Excite และ Infoseek ซึ่งอยู่ในธุรกิจพอร์ตอลบริษัท Geocities ซึ่งอยู่ในธุรกิจชุมชนอิเล็กทรอนิกส์ และบริษัท CD-Now ซึ่งอยู่ในธุรกิจค้าเพลงผ่านอินเทอร์เน็ตโดยใช้ดัชนี 2 ตัวคือ สัดส่วนของพนักงานด้านวิจัยและพัฒนาต่อจำนวนพนักงานทั้งหมดและจำนวนสิทธิบัตรที่ยื่นจดและได้รับในสหรัฐ โดยเชื่อว่าธุรกิจที่ใช้เทคโนโลยีระดับสูงจะมีค่าดัชนีทั้งสองอยู่ในระดับที่สูง[6]

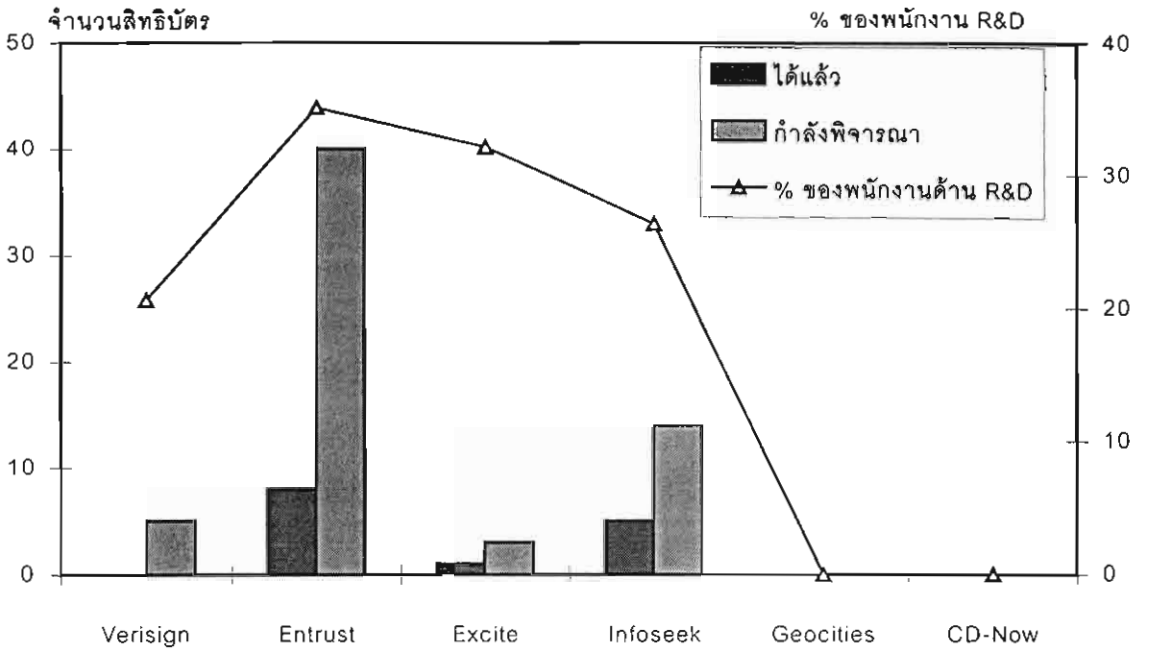
เมื่อพิจารณาจากสัดส่วนของพนักงานด้านวิจัยและพัฒนาต่อหนักงานทั้งหมด ธุรกิจออกใบรับรองไม่แตกต่างจากของบริษัทในธุรกิจพอร์ตอลมากนัก กล่าวคือสัดส่วนดังกล่าวจะอยู่ระหว่างร้อยละ 20 ถึงร้อยละ 35 โดยบริษัท Entrust มีสัดส่วนดังกล่าวสูงกว่าบริษัท Verisign อย่างไรก็ตามสัดส่วนดังกล่าวของบริษัทในธุรกิจออกใบรับรองทั้งสองอยู่ในระดับที่สูงกว่าของบริษัท Geocities และบริษัท CD-Now ซึ่งไม่มีพนักงานด้านวิจัยและพัฒนาอย่างเห็นได้ชัด

เมื่อพิจารณาจากจำนวนสิทธิบัตรที่ได้รับ (granted patent) และสิทธิบัตรที่อยู่ในระหว่างการตรวจสอบ (pending patent) ของบริษัทต่าง ๆ จะพบว่าธุรกิจออกใบรับรองมีระดับของเทคโนโลยีที่สูงกว่าธุรกิจอื่น ๆ อย่างเห็นได้ชัด นอกจากนี้บริษัท Entrust ยังมีจำนวนสิทธิบัตรมากกว่าบริษัท Verisign อีกด้วย ทั้งนี้เนื่องจากบริษัท Entrust มีธุรกิจหลักในการจำหน่ายซอฟต์แวร์และเทคโนโลยี ในขณะที่บริษัท Verisign มีธุรกิจหลักในการให้บริการ

---

[6] นอกจากใช้สิทธิบัตรแล้ว บริษัทในธุรกิจรับรองความถูกต้องยังคุ้มครองทรัพย์สินทางปัญญาของตนด้วยลิขสิทธิ เครื่องหมายการค้า และความลับทางการค้า อย่างไรก็ตามในธุรกิจดังกล่าวสิทธิบัตรเป็นสิ่งที่มีความสำคัญมากที่สุด

ภาพที่ 2.3 ระดับการใช้เทคโนโลยีของบริษัทในธุรกิจออกใบรับรอง
เปรียบเทียบกับบริษัทในธุรกิจพาณิชย์อิเล็กทรอนิกส์อื่น ๆ



ที่มา: สถาบันวิจัยเพื่อการพัฒนาประเทศไทยจากเอกสารรายงานคณะกรรมการกำกับดูแลตลาดหลักทรัพย์สหรัฐ (Security Exchange Commission)

2.4 ธุรกิจออกใบรับรองในประเทศอื่น ๆ

จากการสำรวจขององค์กรความร่วมมือด้านเศรษฐกิจและการพัฒนา (OECD) ซึ่งเป็นหน่วยงานความร่วมมือด้านวิชาการของประเทศพัฒนาแล้ว พบว่าในบรรดาประเทศสมาชิกขององค์กรดังกล่าวส่วนใหญ่ได้มีการจัดตั้งองค์กรออกใบรับรองและใช้ลายมือชื่ออิเล็กทรอนิกส์แล้ว กล่าวคือในบรรดาประเทศในการสำรวจ 17 ประเทศ มีถึง 14 ประเทศที่มีองค์กรออกใบรับรองที่ดำเนินการโดยรัฐหรือเอกชนเปิดให้บริการแล้ว โดยในจำนวนนี้มีถึง 11 ประเทศที่มีการใช้ลายมือชื่ออิเล็กทรอนิกส์ในกิจการที่เกี่ยวกับรัฐ ดังปรากฏในตารางที่ 2.4

ในกลุ่มประเทศในเอเชีย มีหลายประเทศที่มีองค์กรออกใบรับรองแล้วเช่น ญี่ปุ่น สิงคโปร์ เกาหลีใต้ มาเลเซีย เป็นต้น โดยในญี่ปุ่นมีองค์กรออกใบรับรองที่ดำเนินการในเชิงพาณิชย์แล้วอย่างน้อย 3 แห่งคือ Verisign Japan ซึ่งก่อตั้งในปี 1996 CyberTrust Japan ซึ่งก่อตั้งเมื่อปี 1997 และ Japan Certificate ซึ่งก่อตั้งเมื่อปี 1997[7] ส่วนสิงคโปร์มีองค์กรออกใบรับรองที่ดำเนินการในเชิงพาณิชย์แล้ว 2 แห่งคือ Netrust และอีกแห่งหนึ่งซึ่งเพิ่งได้รับการก่อตั้งขึ้นในปี 1999 โดยบริษัททั้งสองต่างเป็นบริษัทที่เกี่ยวข้องกับรัฐ (state-linked company)[8]

ส่วนในเกาหลีใต้ ในปัจจุบันมีองค์กรออกใบรับรองอย่างน้อย 2 แห่งคือ CrossCert ซึ่งก่อตั้งโดยบุคคลในวงการโทรคมนาคม และบริษัท SoftForum ซึ่งเป็นบริษัทลูกของบริษัทผู้ผลิตเครื่องมือทดสอบสารกึ่งตัวนำ บริษัททั้งสองแห่งเพิ่งได้รับการจัดตั้งขึ้นในปี 1999 ในอนาคตมีความเป็นไปได้ว่าจะมีผู้ประกอบการรายใหม่หลายรายโดยเฉพาะบริษัทด้าน SI ในกลุ่มของบริษัทขนาดใหญ่ (chaebol) ธนาคารหรือหน่วยงานที่ให้บริการด้านเครือข่ายการค้าหลักทรัพย์และเครือข่ายการชำระเงิน ตลอดจนหน่วยงานของรัฐที่ให้บริการด้านไปรษณีย์เข้าสู่ตลาด[9]

---

[7] จากการสัมภาษณ์ผู้บริหารบริษัท Japan Certificate เมื่อเดือนมกราคม 1999

[8] บริษัทที่เกี่ยวข้องกับรัฐบาลในสิงคโปร์หมายถึง บริษัทที่มีรัฐบาลสิงคโปร์เป็นผู้ถือหุ้น แต่สัดส่วนการถือหุ้นต่ำกว่าร้อยละ 50 ทำให้บริษัทดังกล่าวไม่มีฐานะเป็นรัฐวิสาหกิจ ในทางปฏิบัติบริษัทดังกล่าวมักจะบริหารงานค่อนข้างอิสระ โดยรัฐบาลไม่เข้าแทรกแซงมากนัก

[9] จากการสัมภาษณ์เจ้าหน้าที่ของ Korea Information Society Development Institute (KISDI) ซึ่งเป็นหน่วยงานด้านนโยบายด้านการพาณิชย์อิเล็กทรอนิกส์ของเกาหลีใต้ เมื่อเดือนมีนาคม 1999

ตารางที่ 2.4 องค์กรออกใบรับรองและ
การใช้ลายมือชื่ออิเล็กทรอนิกส์ในกลุ่มประเทศ OECD

ประเทศ	เอกชนเปิดให้บริการองค์กรออกใบรับรองแล้ว	ใช้ลายมือชื่ออิเล็กทรอนิกส์ในกิจการที่เกี่ยวกับรัฐ
ออสเตรเลีย	√	√
ออสเตรีย	X	X
เบลเยี่ยม	√	√
สาธารณรัฐเช็ค	√	√
ฟินแลนด์	√	X
เยอรมัน	√	√
กรีซ	X	X
ญี่ปุ่น	√	X
เม็กซิโก	√	√
เนเธอร์แลนด์	√	√
นิวซีแลนด์	X	√
นอร์เวย์	√	√
โปแลนด์	√	X
สวีเดน	√	√
ตุรกี	√	X
สหราชอาณาจักร	√	√
สหรัฐอเมริกา	√	√

ที่มา: OECD, *Inventory of Approaches to Authentication and Certification in a Global Networked Society*, 1999

2.5 แนวโน้มของธุรกิจออกใบรับรอง

ในปัจจุบันบริษัทที่ให้บริการออกใบรับรองส่วนใหญ่ยังยังไม่สามารถสร้างรายได้จนถึงจุดคุ้มทุนได้ ในความคิดเห็นของผู้วิจัยปัญหาดังกล่าวน่าจะเกิดจากการที่การใช้ใบรับรองยังไม่แพร่หลายมากพอเนื่องจากการออกใบรับรองในปัจจุบันส่วนใหญ่เป็นการออกใบรับรองให้แก่เครื่องแม่ข่าย (server certificate) โดยเฉพาะเครื่องแม่ข่ายที่ใช้โปรโตคอลรักษาความปลอดภัยแบบ SSL โดยมีการออกใบรับรองให้แก่โปรแกรมประยุกต์ในเครื่องลูกข่าย (client certificate) น้อยมาก ทั้งนี้เนื่องจากกระบวนการในการขอใบรับรองยังคงยุ่งยากและผู้บริโภคส่วนใหญ่ยังไม่เห็นความจำเป็นในการต้องมีใบรับรองเพราะเป็นการเพิ่มต้นทุนในการซื้อสินค้าผ่านการพาณิชย์อิเล็กทรอนิกส์โดยไม่เห็นผลตอบแทนที่ชัดเจน นอกจากนี้ร้านค้าส่วนใหญ่ก็ยังไม่กล้าจำกัดการประกอบธุรกิจกับผู้บริโภคที่มีใบรับรองเท่านั้น เพราะจะทำให้ฐานลูกค้าของตนเล็กลง แม้ว่าการใช้ใบรับรองในลักษณะดังกล่าวจะก่อให้เกิดความเสี่ยงในการประกอบธุรกรรมก็ตาม จนถึงปัจจุบันยังไม่ปรากฏว่ามีผู้ประกอบการรายใดได้รับความเสียหายขนานใหญ่จากการไม่สามารถระบุตัวผู้บริโภคได้

อย่างไรก็ตามในอนาคตมีความเป็นไปได้มากว่า การใช้ใบรับรองจะแพร่หลายมากขึ้นจากพัฒนาการในด้านต่าง ๆ ต่อไปนี้

- การทำธุรกรรมทางการเงิน (financial transaction) เช่นการโอนเงินหรือการซื้อขายหลักทรัพย์ผ่านเครือข่ายอินเทอร์เน็ตที่แพร่หลายมากขึ้นและมีมูลค่าของทำธุรกรรมมูลค่าสูงจะทำให้เกิดความจำเป็นในการใช้เทคโนโลยีใบรับรองเพิ่มขึ้น
- การที่หน่วยงานรัฐหรือธนาคารพาณิชย์รายใหญ่เข้าร่วมในการออกใบรับรองจะช่วยให้เกิดความเชื่อมั่นต่อข้อมูลในใบรับรองซึ่งจะทำให้การใช้เทคโนโลยีดังกล่าวแพร่หลายมากขึ้น เนื่องจากรัฐและธนาคารพาณิชย์เป็นสถาบันที่สามารถตรวจสอบข้อมูลต่าง ๆ ที่มีความสำคัญสูงเช่น ข้อมูลทะเบียนราษฎร์ ทะเบียนนิติบุคคล ตลอดจนข้อมูลสถานะทางการเงินต่าง ๆ เช่นรายได้ของผู้ขอใบรับรองเป็นต้น
- การผนวกใบรับรองอิเล็กทรอนิกส์เข้าเป็นส่วนหนึ่งของโปรแกรมประยุกต์เช่นบราวเซอร์หรือโปรแกรมไปรษณีย์อิเล็กทรอนิกส์โดยให้ผู้ใช้สามารถขอใบรับรองได้ในขณะติดตั้งโปรแกรมประยุกต์นั้น จะช่วยลดความยุ่งยากในการขอใบรับรองและจะทำให้การใช้ใบรับรองมีความแพร่หลายมากขึ้น[๑๐]

[๑๐] ในช่วงต้นปี 1999 เริ่มมีแนวโน้มในทิศทางดังกล่าวจากการที่บริษัท Netscape ได้ทำความตกลงกับบริษัท Verisign ที่จะผนวกใบรับรองของบริษัท Verisign เข้าในบราวเซอร์ Netscape Navigator ในอนาคต

- ความแพร่หลายของการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและธุรกิจ (B-to-B E-Commerce) ผ่านเครือข่ายเอ็กซ์ทราเน็ต ตลอดจนการที่องค์กรต่าง ๆ เริ่มอนุญาตให้พนักงานของตนสามารถใช้งานเครื่องคอมพิวเตอร์จากนอกสำนักงาน (remote login) จะทำให้เกิดความจำเป็นในการใช้เทคโนโลยีใบรับรองเพื่อรักษาความปลอดภัยมากขึ้น

2.6 แนวโน้มในการรับรองซึ่งกันและกัน

ในอนาคตคงเป็นไปได้ยากที่จะมีองค์กรออกใบรับรองเหลือเพียงแห่งเดียว ปัญหาที่เกิดขึ้นจากการมีองค์กรออกใบรับรองหลายแห่งก็คือ องค์กรออกใบรับรองแต่ละแห่งอาจไม่ยอมรับใบรับรองที่ออกโดยองค์กรออกใบรับรองอื่นก็ได้ ทำให้ผู้ใช้ต้องขอรับใบรองหลายใบซึ่งเป็นการสร้างภาระที่ไม่จำเป็น การรับรองซึ่งกันและกัน (cross-certification) ขององค์กรออกใบรับรองคือกระบวนการที่จะทำให้ใบรับรองขององค์กรออกใบรับรองแห่งหนึ่งสามารถใช้ได้กับแห่งอื่นได้ด้วยหรือมีความสามารถในการใช้งานร่วมกันได้ (inter-operablity) นั่นเอง

ในทางปฏิบัติการรับรองซึ่งกันและกันสามารถทำได้โดยองค์กรออกใบรับรองที่ต้องการรับรองซึ่งกันและกันต่างดำเนินการตรวจสอบและเปรียบเทียบแนวทางในการออกใบรับรองของอีกฝ่ายหนึ่ง ทั้งการเปรียบเทียบนโยบายในการออกใบรับรอง การตรวจสอบสถานที่ และสำรวจระบบที่เกี่ยวข้องเพื่อให้แน่ใจว่ามีมาตรฐานในการรักษาความปลอดภัยที่ใกล้เคียงกัน หลังจากนั้นก็จะตกลงกันในประเด็นทางกฎหมายในการแบ่งรับหน้าที่และความรับผิดชอบ และการแบ่งผลประโยชน์กัน (ดูรายละเอียดในภาคผนวกที่ 2)

อย่างไรก็ตามมีข้อสังเกตว่าในปัจจุบันยังมีการรับรองซึ่งกันและกันระหว่างองค์กรออกใบรับรองต่าง ๆ น้อยมาก[11] ทั้งนี้อาจเนื่องมาจากเหตุผลต่าง ๆ หลายประการคือ

- ธุรกิจออกใบรับรองยังอยู่ขั้นเริ่มต้นและการใช้ใบรับรองยังไม่แพร่หลายนัก ความต้องการของตลาดที่จะให้ใบรับรองที่ออกโดยองค์กรออกใบรับรองแห่งหนึ่งสามารถใช้ได้กับองค์กรออกใบรับรองแห่งอื่นจึงยังไม่เกิดขึ้นมากนัก

---

[11] ที่ผ่านมามีข่าวว่ามีองค์กรออกใบรับรองของรัฐบาลแคนาดาและบริษัท Netrust ของสิงคโปร์ได้ตกลงยอมรับใบรับรองของกันและกัน อย่างไรก็ตามในความเป็นจริงแล้ว ความเคลื่อนไหวดังกล่าวเป็นเพียงการที่องค์กรรับรองทั้งสองแห่งทดลองทางเทคนิคในยอมรับใบรับรองของกันและกันในช่วงเวลาสั้น ๆ เป็นเวลา 2 สัปดาห์เท่านั้น โดยไม่ได้มีข้อตกลงที่เป็นทางการระหว่างกันแต่อย่างใด

2.7 การจัดตั้งองค์กรออกใบรับรองในประเทศไทย

ที่ผ่านมาการจัดตั้งองค์กรออกใบรับรองในประเทศไทยเป็นเรื่องที่ได้รับการกล่าวถึงมาก โดยมักมีข้อเสนอให้รัฐเป็นผู้จัดตั้งและให้บริการออกใบรับรอง โดยอ้างว่าธุรกิจออกใบรับรองเป็นธุรกิจที่ใช้เทคโนโลยีชั้นสูง ต้องอาศัยการวิจัยและพัฒนามากและมีระยะเวลาในการถึงจุดคุ้มทุนช้าทำให้เอกชนไม่สนใจที่จะลงทุน ในขณะที่ธุรกิจดังกล่าวเป็นโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญที่จะช่วยให้การพาณิชย์อิเล็กทรอนิกส์ในประเทศไทยเติบโตและพัฒนาต่อไป ในความเห็นของผู้วิจัย เหตุผลสนับสนุนให้ภาครัฐเป็นผู้ให้บริการออกใบรับรองที่กล่าวมาบางประการเป็นเหตุผลที่ถูกต้องทั้งการที่ธุรกิจดังกล่าวเป็นธุรกิจที่ลงทุนสูงต้องอาศัยการวิจัยและพัฒนามาก และการที่องค์กรออกใบรับรองเป็นโครงสร้างพื้นฐานในการพัฒนาการพาณิชย์อิเล็กทรอนิกส์ในประเทศไทย

อย่างไรก็ตามจากที่กล่าวมาในหัวข้อ 2.5 จะเห็นว่าสาเหตุสำคัญของการที่ธุรกิจออกใบรับรองยังไม่ถึงจุดคุ้มทุนเป็นปัญหาด้านอุปสงค์ (demand) ไม่ใช่ปัญหาด้านอุปทาน (supply) กล่าวคือความต้องการบริการดังกล่าวยังมีไม่มากเพียงพอในขณะที่มีผู้ให้บริการหลายราย แม้ว่าผู้ให้บริการออกใบรับรองทั้งหมดจะอยู่ในต่างประเทศก็ตาม ผู้บริโภคในประเทศไทยก็สามารถเข้าถึงบริการดังกล่าวผ่านเครือข่ายอินเทอร์เน็ตได้โดยไม่ประสบปัญหาแต่อย่างใด ข้อเสนอให้รัฐเป็นผู้ให้บริการดังกล่าวจึงยังมีน้ำหนักไม่เพียงพอ นอกจากจะสามารถพิสูจน์ได้ว่าหากรัฐเข้าร่วมในการให้บริการแล้วผู้บริโภคในประเทศจะได้รับบริการในราคาที่ถูกลงหรือมีคุณภาพที่ดีขึ้น นอกจากนี้ในส่วนของตลาดที่มีความต้องการความปลอดภัยสูงเช่นการทำธุรกรรมทางการเงิน ภาคเอกชนเช่นธนาคารพาณิชย์บางแห่งก็เริ่มแสดงความสนใจที่จะประกอบธุรกิจดังกล่าว ซึ่งชี้ให้เห็นว่ากลไกตลาดไม่ได้มีความล้มเหลวแต่อย่างใด[12]

จากที่กล่าวมาข้างต้น ผู้วิจัยจึงสรุปว่าไม่มีเหตุผลด้านเศรษฐศาสตร์ที่ชี้ว่ารัฐควรเป็นผู้ให้บริการธุรกิจออกใบรับรองเอง อย่างไรก็ตามอาจมีเหตุผลอื่นเช่นเหตุผลด้านความมั่นคงที่รัฐจำเป็นต้องเป็นผู้ให้บริการเองในการใช้งานในภาครัฐที่ต้องการความปลอดภัยสูง นอกจากนี้รัฐยังมีเหตุผลในด้านเศรษฐศาสตร์ในการให้การสนับสนุนผู้ประกอบธุรกิจดังกล่าวในกิจกรรมที่มีผลกระทบภายนอก (externality) เช่นการวิจัยและพัฒนาตลอดจนการพัฒนาทรัพยากรมนุษย์ที่เกี่ยวข้องเป็นต้น

---

[12] ข่าว "3 แบงก์รวมตัวตั้งซีเอไทยขึ้นทะเบียนอี-คอมเมิร์ซ", กรุงเทพธุรกิจฉบับวันศุกร์ที่ 8 ตุลาคม 2542, หน้า 1

บทที่ 3 นโยบายควบคุมเทคโนโลยีเข้ารหัส

ในบทนี้ผู้วิจัยจะกล่าวถึงความจำเป็นของนโยบายควบคุมการใช้เทคโนโลยีเข้ารหัสในการรักษาความลับ (confidentiality) ของข้อมูล สำรวจนโยบายดังกล่าวของประเทศต่าง ๆ และเสนอแนะแนวทางในการกำหนดนโยบายดังกล่าวในประเทศไทย

3.1 นโยบายการเข้ารหัส

เดิมเทคโนโลยีเข้ารหัสถือเป็นเทคโนโลยีที่ใช้เฉพาะในการทหาร อย่างไรก็ตามการประยุกต์ใช้เทคโนโลยีเข้ารหัสในด้านอื่น ๆ ในปัจจุบันทำให้เทคโนโลยีดังกล่าวพ้นสภาพจากการเป็นเทคโนโลยีด้านการทหารอย่างเดียว (single use) มาสู่เทคโนโลยีที่สามารถใช้งานสองด้าน (dual use) ทั้งด้านการทหารและด้านพลเรือน กล่าวคือในปัจจุบันธุรกิจอาจใช้เทคโนโลยีดังกล่าวในการประกอบการพาณิชย์อิเล็กทรอนิกส์ ทั้งการซื้อขายสินค้าผ่านเครือข่ายอินเทอร์เน็ตซึ่งถือเป็นการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและผู้บริโภค การใช้ในเครือข่ายเอกชนเสมือน (virtual private network) ในการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและธุรกิจ การเข้ารหัสสัญญาณภาพของเคเบิลทีวีเพื่อป้องกันผู้ที่ไม่ใช่สมาชิกสามารถรับชมรายการได้ ตลอดจนการที่ประชาชนทั่วไปใช้เทคโนโลยีดังกล่าวเพื่อป้องกันการถูกดักฟังในการติดต่อสื่อสารทางโทรศัพท์เป็นต้น

การที่เทคโนโลยีดังกล่าวกลายเป็นเทคโนโลยีที่ใช้ทั้งในด้านการทหารและด้านพลเรือนทำให้เกิดปัญหาว่า เราจะสามารถสร้างความสมดุลย์ระหว่างการสร้างความสามารถของรัฐในการคุ้มครองประชาชนจากภัยคุกคามต่าง ๆ กับการคุ้มครองความเป็นอยู่ส่วนตัว (privacy) และเสรีภาพในการสื่อสารของประชาชนตลอดจนความมั่นใจในการดำเนินธุรกิจได้อย่างไร กล่าวคือหากรัฐมีนโยบายปล่อยให้ประชาชนและธุรกิจสามารถใช้เทคโนโลยีดังกล่าวอย่างเสรีโดยไม่มีข้อจำกัดแล้ว รัฐอาจประสบปัญหาในการบังคับใช้กฎหมายในการตรวจจับการสื่อสารของผู้ก่อการร้าย อาชญากร หรือรัฐบาลของประเทศศัตรู ในทางตรงกันข้ามหากรัฐมีนโยบายในการควบคุมการใช้เทคโนโลยีดังกล่าวอย่างเข้มงวดเกินไป ก็จะปิดโอกาสของธุรกิจและประชาชนในการใช้ประโยชน์จากเทคโนโลยีดังกล่าว และละเมิดความเป็นอยู่ส่วนตัวและเสรีภาพในการสื่อสารของประชาชน

ประเทศต่าง ๆ พยายามแก้ไขปัญหาดังกล่าวโดยอนุญาตให้ประชาชนมีเสรีภาพในการใช้เทคโนโลยีดังกล่าวได้ในในสภาวะปรกติ แต่กำหนดให้รัฐสามารถเข้าถึงและถอดรหัสข้อมูลที่เข้ารหัสได้โดยชอบด้วยกฎหมายหรือที่เรียกกันว่า "การเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยหน่วยงานรัฐ" (lawful state access) ในบางสถานการณ์เช่น เมื่อสงสัยว่าจะมีการก่อการร้าย

หรือการละเมิดกฎหมายต่าง ๆ เช่นการฟอกเงิน การหลบเลี่ยงภาษี การฝ่าฝืนกฎหมายการแข่งขันเป็นต้น เราสามารถเรียกนโยบายการควบคุมเทคโนโลยีเข้ารหัสในลักษณะดังกล่าวตลอดจนนโยบายอื่นที่เกี่ยวกับการควบคุมการผลิต การใช้ประโยชน์ การส่งออก และการนำเข้าเทคโนโลยีเข้ารหัสโดยรวม ๆ ว่า "นโยบายเทคโนโลยีเข้ารหัส" (encryption policy)

ประเทศอุตสาหกรรมในตะวันตกส่วนใหญ่มักไม่มีข้อจำกัดในนำเข้าเทคโนโลยีดังกล่าวจากประเทศอื่น แต่มักควบคุมการส่งออกผลิตภัณฑ์ที่มีเทคโนโลยีเข้ารหัสไปยังประเทศที่เคยปกครองในระบบสังคมนิยมหรือประเทศอื่น ๆ ที่มีความสัมพันธ์ทางการเมืองที่ตึงเครียด เพื่อป้องกันการส่งออกเทคโนโลยีเข้ารหัสและผลิตภัณฑ์ที่มีความอ่อนไหวในด้านความมั่นคงไปยังประเทศเหล่านั้น ประเทศตะวันตกส่วนใหญ่ได้ทำความตกลงที่เรียกว่า "ความตกลงวัสเซนน่าร์ว่าด้วยการควบคุมการส่งออกอาวุธยุทโธปกรณ์และสินค้าและเทคโนโลยีที่ใช้ได้ทั้งในด้านการทหารและพลเรือน" (Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies)[1] ส่วนประเทศในค่ายสังคมนิยมเดิมเช่นจีนและรัสเซียหรือประเทศที่มีความเป็นห่วงด้านความมั่นคงสูงเช่นเกาหลีใต้ มักมีข้อจำกัดในการนำเข้าเทคโนโลยีดังกล่าว[2]

นอกเหนือจากการควบคุมการส่งออกหรือการนำเข้าแล้ว วิธีการในการควบคุมเทคโนโลยีเข้ารหัสที่สำคัญอื่น ๆ คือการจำกัดความยาวของกุญแจ (key length) ที่สามารถใช้ได้ และการกำหนดให้มีระบบการเก็บหรือกู้กุญแจ การจำกัดความยาวของกุญแจที่สามารถใช้ได้จะทำให้หน่วยงานรัฐสามารถใช้เครื่องคอมพิวเตอร์ที่มีขีดความสามารถสูงในการถอดรหัสของข้อมูลที่ต้องการตรวจสอบได้ อย่างไรก็ตามการควบคุมโดยวิธีนี้จะทำให้ระบบข้อมูลโดยรวมมีความปลอดภัยต่ำลงและเสี่ยงต่อการถูกผู้อื่นนอกจากหน่วยงานรัฐถอดรหัสด้วยวิธีการเดียวกัน การอนุญาตให้ใช้เทคโนโลยีเข้ารหัสที่มีขีดความสามารถสูง (strong encryption) แต่กำหนดให้หน่วยงานรัฐที่เกี่ยวข้องสามารถเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย โดยใช้ระบบการเก็บกุญแจหรือการกู้กุญแจจึงเป็นวิธีที่ดีกว่า[3]

---

[1] ในยุคสงครามเย็นประเทศตะวันตกเคยห้ามการส่งออกเทคโนโลยีที่ใช้ได้ทั้งในด้านการทหารและพลเรือนตลอดจนอาวุธนิวเคลียร์ไปยังประเทศในกลุ่มของสหภาพโซเวียตตามความตกลงโคคอม (COCOM) ภายหลังสงครามเย็น ความตกลงดังกล่าวได้ถูกยกเลิกไปและถูกแทนที่ด้วยความตกลงวัสเซนน่าร์ เช่นเดียวกับความตกลงระหว่างประเทศอื่น ๆ ประเทศสมาชิกของความตกลงดังกล่าวจะต้องออกกฎหมายในประเทศขึ้นรองรับ

[2] จากการสัมภาษณ์ Korea Information Society Development Institute (KISDI) ซึ่งเป็นหน่วยงานวิจัยนโยบายในเกาหลีใต้ เกาหลีใต้ห้ามธุรกิจและประชาชนนำเข้าและใช้เทคโนโลยีเข้ารหัส เนื่องจากมีความวิตกกังวลเกี่ยวกับปัญหาความมั่นคงภายในประเทศอันเนื่องมาจากความสัมพันธ์อันตึงเครียดกับเกาหลีเหนือ รัฐบาลเกาหลีใต้ใช้นโยบายพัฒนาเทคโนโลยีดังกล่าวเองเพื่อให้สามารถควบคุมได้

[3] นอกจากนี้ระบบเก็บหรือกู้กุญแจยังเป็นสิ่งที่ธุรกิจและผู้ใช้โดยทั่วไปมักมีความต้องการอยู่แล้วเพื่อให้มีหลักประกันว่าตนสามารถถอดรหัสข้อมูลในกรณีที่ทำกุญแจสูญหายหรือในกรณีที่พนักงานที่เป็นผู้เก็บรักษากุญแจลาออกไปโดยไม่ได้ส่งมอบกุญแจให้แก่ผู้อื่น

การเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยหน่วยงานรัฐโดยใช้ระบบเก็บกุญแจ (key archiving) หมายถึงการที่รัฐกำหนดให้ผู้ใช้เทคโนโลยีเข้ารหัสต้องทำกุญแจลับสำรองแล้วจัดเก็บไว้ที่ใดที่หนึ่ง ตัวอย่างที่รู้จักกันดีของระบบดังกล่าวคือระบบฝากกุญแจ (key escrow) ซึ่งกำหนดให้เจ้าหน้าที่หรือบุคคลที่รัฐแต่งตั้ง (authorized people) เช่นองค์กรออกใบรับรองของผู้ใช้เก็บกุญแจสำรองไว้เพื่อใช้ในการถอดรหัสในกรณีที่รัฐต้องการตรวจสอบ ในช่วงต้นปี 1996 รัฐบาลสหรัฐเคยจะนำระบบดังกล่าวมาใช้แต่ไม่สามารถดำเนินการได้เนื่องจากได้รับการต่อต้านอย่างรุนแรงจากองค์กรสิทธิมนุษยชนต่าง ๆ ในประเทศ ด้วยเหตุผลว่ามาตรการดังกล่าวเป็นการละเมิดสิทธิเสรีภาพในการแสดงออกและความเป็นส่วนตัวของประชาชน

ส่วนการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยหน่วยงานรัฐโดยใช้ระบบกู้กุญแจ (key recovery) เป็นวิธีการที่ผู้ใช้เทคโนโลยีเข้ารหัสไม่ต้องฝากกุญแจลับของตนไว้กับผู้อื่น แต่จะใช้กุญแจสาธารณะของหน่วยงานกู้กุญแจเข้ารหัสกุญแจลับของตนแล้วผนวกลงไปในข้อมูลที่ต้องการเข้ารหัสด้วย เมื่อรัฐต้องการตรวจสอบก็จะสามารถใช้กุญแจลับของหน่วยงานกู้กุญแจถอดรหัสกุญแจลับของผู้ใช้มาถอดรหัสดูข้อมูลอีกทีหนึ่ง เมื่อปี 1997 หน่วยงานสอบสวนกลาง (FBI) ของสหรัฐ เคยประกาศห้ามใช้เทคโนโลยีเข้ารหัสที่มีขีดความสามารถสูงที่ไม่มีระบบการกู้กุญแจ (key recovery) อย่างไรก็ตามการควบคุมดังกล่าวก็ถูกต่อต้านอย่างหนักเช่นเดียวกัน

3.2 ตัวอย่างนโยบายเทคโนโลยีเข้ารหัสของประเทศต่าง ๆ

ตามกฎหมายของสหรัฐในปัจจุบันเทคโนโลยีเข้ารหัสถือเป็นสินค้ายุทธภัณฑ์ (munition) เช่นเดียวกับอาวุธยุทโธปกรณ์ทั้งหลาย การส่งออกเทคโนโลยีดังกล่าวถูกควบคุมด้วยกฎหมายว่าด้วยการค้าอาวุธ (Defense Trade Regulation) ซึ่งเดิมเรียกว่ากฎหมายการค้าอาวุธระหว่างประเทศ (International Traffic in Arms Regulation หรือ ITAR) กฎหมายดังกล่าวกำหนดให้การส่งออกเทคโนโลยีดังกล่าวจะกระทำได้ก็ต่อเมื่อได้รับใบอนุญาตจากกระทรวงพาณิชย์ของสหรัฐ (Ministry of Commerce) เท่านั้น อย่างไรก็ตามในระยะหลังรัฐบาลสหรัฐเริ่มตระหนักว่านโยบายดังกล่าวไม่เป็นผลดีต่ออุตสาหกรรมคอมพิวเตอร์ของสหรัฐเองโดยจะผลักดันให้ผู้ประกอบการสหรัฐต้องย้ายฐานการผลิตไปต่างประเทศ จึงได้เริ่มผ่อนคลายข้อจำกัดดังกล่าวลงจนในที่สุดยินยอมให้ผู้ผลิตสามารถส่งออกเทคโนโลยีเข้ารหัสที่มีความยาวของกุญแจไม่เกิน 40 บิท และ 56 บิทในกรณีการส่งออกเพื่อใช้ในสถาบันการเงิน และต่อมาในเดือนกันยาน 1999 รัฐบาลได้ผ่อนคลายกฎระเบียบในการส่งออกอีกครั้ง โดยลดข้อจำกัดในการส่งออกผลิตภัณฑ์เทคโนโลยีเข้ารหัสที่มีความยาวของกุญแจไม่เกิน 64 บิท โดยให้ผู้ส่งออกขออนุญาตกระทรวงพาณิชย์ครั้งเดียวสำหรับผลิตภัณฑ์แต่ละรุ่น ส่วนผลิตภัณฑ์เทคโนโลยีเข้ารหัสที่มีความยาวของกุญแจเกิน 64 บิท ก็จะสามารถส่งออกได้เป็นกรณีพิเศษหากเป็นเทคโนโลยีที่

ออกแบบให้ใช้กับผู้ใช้ทั่วไป (end user) ที่ไม่ต้องการการสนับสนุนทางเทคนิคมาก และประเทศที่ส่งออกไม่ใช่ประเทศในบัญชีรายชื่อต้องห้าม

แคนาดาไม่มีข้อจำกัดในการส่งออกเทคโนโลยีเข้ารหัสใด ๆ ไปยังสหรัฐ และสามารถส่งออกผลิตภัณฑ์ลายมือชื่อดิจิตัลได้โดยไม่มีข้อจำกัด นอกจากนี้แคนาดายังไม่มีข้อจำกัดในการนำเข้าและการใช้เทคโนโลยีดังกล่าวในประเทศ อย่างไรก็ตามแคนาดามีนโยบายการควบคุมการส่งออกเทคโนโลยีเข้ารหัสเช่นเดียวกับสหรัฐ ในอดีตแคนาดาเคยอนุญาตให้ส่งออกเทคโนโลยีเข้ารหัสที่มีความยาวของกุญแจไม่เกิน 40 บิทเท่านั้น ยกเว้นสถาบันการเงินต่าง ๆ ได้รับอนุญาตให้ส่งออกเทคโนโลยี DES ที่มีความยาวของกุญแจไม่เกิน 56 บิทได้ ต่อมาในปี 1996 แคนาดาได้ทดลองเปิดการส่งออกเทคโนโลยีเข้ารหัสที่มีความยาวของกุญแจไม่เกิน 56 บิทไปยังประเทศต่างเป็นการทั่วไป[4]

ตารางที่ 3.1 สรุปข้อจำกัดในการใช้ ส่งออกและนำเข้าเทคโนโลยีเข้ารหัสของประเทศต่างๆ บางประเทศ

3.3 แนวคิดในการกำหนดนโยบายควบคุมเทคโนโลยีเข้ารหัส

ในการกำหนดนโยบายเทคโนโลยีเข้ารหัส ผู้กำหนดนโยบายควรมุ่งรักษาสมดุลย์ระหว่างการส่งเสริมการพาณิชย์อิเล็กทรอนิกส์ การคุ้มครองเสรีภาพในการสื่อสารของประชาชนและการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยรัฐ ตลอดจนรักษาความสอดคล้องทางนโยบายกับประเทศต่าง ๆ ตัวอย่างการกำหนดนโยบายในลักษณะดังกล่าวที่ประเทศไทยสามารถอ้างอิงเป็นต้นแบบได้คือแนวทางการใช้เทคโนโลยีเข้ารหัสขององค์กรความร่วมมือด้านเศรษฐกิจและการพัฒนา (OECD) ซึ่งบางประเทศเช่นเกาหลีได้ใช้เป็นแนวทางในการออกกฎหมายควบคุมเทคโนโลยีการเข้ารหัส (cryptography law)

แนวทางการใช้เทคโนโลยีเข้ารหัสขององค์กรความร่วมมือด้านเศรษฐกิจและการพัฒนาประกอบด้วยหลักการ 8 ข้อดังต่อไปนี้

1. วิธีการในการใช้เทคโนโลยีเข้ารหัสจะต้องน่าเชื่อถือ (trustworthy) เพื่อสร้างความมั่นใจในการใช้ระบบสารสนเทศและระบบสื่อสาร
2. ผู้ใช้ควรมีสิทธิในการเลือกใช้วิธีการเข้ารหัสใด ๆ ตามกรอบของกฎหมาย

---

[4] Task Force on Electronic Commerce, *Industry Canada, A Cryptograhiy Policy Framework for Electronic Commerce,* February 1998

3. วิธีการเข้ารหัสควรได้รับการพัฒนาขึ้นเพื่อตอบสนองความจำเป็น ความต้องการและความรับผิดชอบของประชาชน ธุรกิจและหน่วยงานรัฐ
4. มาตรฐานทางเทคนิค (technical standard) ข้อกำหนด (criteria) และโปรโตคอล (protocol) ในการเข้ารหัสควรได้รับการพัฒนาขึ้นในระดับชาติและระดับนานาชาติ
5. สิทธิพื้นฐานของประชาชนในการรักษาความเป็นอยู่ส่วนตัว (privacy) ตลอดจนการรักษาความลับในการติดต่อสื่อสารและการคุ้มครองข้อมูลส่วนตัวควรได้รับการยอมรับในนโยบายของประเทศในการควบคุมเทคโนโลยีเข้ารหัส การออกแบบและการใช้เทคโนโลยีดังกล่าว
6. นโยบายควบคุมเทคโนโลยีเข้ารหัสของประเทศอาจยินยอมให้รัฐเข้าถึงกุญแจลับที่ใช้ในการเข้ารหัส ข้อมูลที่ถอดรหัส (plaintext) หรือข้อมูลที่เข้ารหัสโดยชอบด้วยกฎหมาย อย่างไรก็ตามนโยบายเหล่านี้จะต้องสอดคล้องกับหลักการข้ออื่น ๆ มากที่สุดเท่าที่จะเป็นไปได้
7. หน้าที่และความรับผิดชอบซึ่งเกิดขึ้นตามสัญญาหรือผลของกฎหมายของประชาชนหรือหน่วยงานที่ให้บริการเข้ารหัส เก็บรักษาหรือเข้าถึงกุญแจที่ใช้ในการเข้ารหัส ควรได้รับการประกาศอย่างชัดแจ้ง
8. รัฐบาลของประเทศต่าง ๆ ควรร่วมมือและประสานนโยบายเทคโนโลยีเข้ารหัส และควรระวังการอ้างนโยบายดังกล่าวในการกีดกันทางการค้า

ในปัจจุบันประเทศไทยควบคุมการนำเข้าสินค้า 20 รายการและควบคุมการส่งออกสินค้าประมาณ 10 รายการโดยใช้ระบบใบอนุญาต ตามพ.ร.บ. การส่งออกไปนอกและการนำเข้ามาในราชอาณาจักรซึ่งสินค้า พ.ศ. 2522 โดยมีเหตุผลต่าง ๆ เช่นเหตุผลในการห้ามการนำเข้าได้แก่ การปกป้องอุตสาหกรรมในประเทศ (เช่นหินอ่อน เส้นใยไหม) การรักษาสิ่งแวดล้อม (เช่น จักรยานยนต์ใช้แล้ว) การป้องกันการละเมิดทรัพย์สินทางปัญญา (เช่นชิ้นส่วนและเครื่องจักรสำหรับทำซ้ำเทปและแผ่นซีดี) และห้ามส่งออกสินค้าบางรายการซึ่งส่วนใหญ่มีจุดประสงค์เพื่อป้องกันความขาดแคลนในประเทศ (เช่นปุ๋ยต่าง ๆ ยกเว้นปุ๋ยเคมี) การรักษาทรัพยากรธรรมชาติ (เช่นทราย) แต่ไม่มีการห้ามส่งออกและนำเข้าเทคโนโลยีเข้ารหัสแต่อย่างใด การผลิต การส่งออกและการนำเข้าตลอดจนการใช้เทคโนโลยีดังกล่าวจึงสามารถดำเนินไปได้อย่างเสรี

ในฐานะที่ประเทศไทยไม่ใช่ประเทศผู้ผลิตเทคโนโลยีดังกล่าว การเปิดกว้างให้ประชาชนและธุรกิจสามารถเลือกใช้เทคโนโลยีได้ตามความต้องการของตนเองโดยไม่มีข้อจำกัดเรื่องการนำเข้าและการใช้น่าจะมีผลดีในการเอื้ออำนวยให้เกิดการรับนวัตกรรมทางเทคโนโลยีใหม่ ๆ จากต่างประเทศและส่งเสริมการใช้เทคโนโลยีดังกล่าวในการพาณิชย์อิเล็กทรอนิกส์ อย่างไร

ก็ตามในอนาคตหน่วยงานด้านความมั่นคงและหน่วยงานที่บังคับใช้กฎหมายต่าง ๆ อาจเห็นความจำเป็นในการควบคุมเทคโนโลยีเข้ารหัส โดยเฉพาะการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยหน่วยงานรัฐเพื่อป้องกันการก่อการร้าย การก่ออาชญากรรม การฟอกเงิน การเผยแพร่สารสนเทศที่ขัดกับกฎหมายเช่นภาพลามกอนาจารหรือการละเมิดกฎหมายอื่น ๆ ในประเด็นนี้ผู้กำหนดนโยบายควรให้ความสนใจต่อบทบัญญัติในมาตรา 37 ของรัฐธรรมนูญฉบับปัจจุบันคือ

> *บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางที่ชอบด้วยกฎหมาย การตรวจการกักหรือการเปิดเผยสิ่งสื่อสารที่บุคคลมีติดต่อถึงกันรวมทั้งการกระทำด้วยประการอื่นใดเพื่อให้ล่วงรู้ถึงข้อความในสิ่งสื่อสารทั้งหลายที่บุคคลมีติดต่อถึงกันจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อรักษาความมั่นคงของรัฐ หรือเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน*

จะเห็นได้ว่าเจตนารมย์ของบทบัญญัติดังกล่าวคือการรับประกันเสรีภาพในการสื่อสารและความเป็นส่วนตัวของประชาชน อย่างไรก็ตามมาตราดังกล่าวมิได้ห้ามมิให้รัฐกำหนดนโยบายเทคโนโลยีเข้ารหัสเพื่อประโยชน์ในการรักษาความมั่นคงของรัฐ ความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ซึ่งอาจตีความได้ว่ารัฐธรรมนูญมิได้ปิดกั้นการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายของหน่วยงานรัฐ อย่างไรก็ตามเพื่อคุ้มครองเสรีภาพในการสื่อสารของประชาชนและส่งเสริมการใช้เทคโนโลยีเข้ารหัสในการพาณิชย์อิเล็กทรอนิกส์ นโยบายการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายของรัฐควรมีแนวทางดังต่อไปนี้

- กำหนดขอบเขตการแทรกแซงของรัฐเฉพาะในกรณีการใช้เทคโนโลยีเข้ารหัสในการรักษาความลับ (confidentiality) ของข้อมูลเท่านั้น โดยไม่ให้รัฐแทรกแซงการใช้เทคโนโลยีดังกล่าวในการระบุตัวบุคคล (authentication) หรือรักษาความถูกต้องของข้อมูล (integrity)
- กำหนดหลักเกณฑ์ที่ชัดเจนในการอนุญาตให้รัฐเข้าถึงข้อมูลโดยชอบด้วยกฎหมายเช่น ให้ทำได้ต่อเมื่อได้รับคำสั่งหรือหมายศาลเท่านั้น[5]
- กำหนดระยะเวลาที่แน่นอนในการอนุญาตให้รัฐเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย และอนุญาตให้เข้าถึงเฉพาะข้อมูลที่เกี่ยวข้องกับเรื่องที่ตรวจสอบอยู่เท่านั้น

---

[5] ข้อเสนอดังกล่าวมีเนื้อหาคล้ายคลึงกับบทบัญญัติในมาตราที่ 238 ของรัฐธรรมนูญที่ว่า *ในคดีอาญา การค้นในที่รโหฐานจะกระทำมิได้ เว้นแต่จะมีคำสั่งหรือหมายของศาล หรือมีเหตุให้ค้นได้โดยไม่ต้องมีคำสั่งหรือหมายของศาล ทั้งนี้ ตามที่กฎหมายบัญญัติ* โดยอาจเทียบเคียงระหว่างถอดรหัสข้อมูลที่เข้ารหัสกับการค้นสถานที่

- กำหนดให้บุคคลซึ่งช่วยเหลือรัฐในการเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย เช่นผู้รักษากุญแจลับที่เกี่ยวข้องไม่มีความผิดจากการกระทำดังกล่าว
- วางระบบตรวจสอบที่มีความโปร่งใสเช่น กำหนดให้มีการเก็บบันทึกการเข้าถึงโดยชอบด้วยกฎหมายเพื่อให้สามารถตรวจสอบจากภายนอกได้

ในทางปฏิบัติการกำหนดนโยบายดังกล่าวอาจทำได้โดยออกบทบัญญัติในกฎหมายคุ้มครองข้อมูล (data protection law) หรือกฎหมายอาชญากรรมทางคอมพิวเตอร์ (computer crime law) ซึ่งศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติกำลังอยู่ในระหว่างเตรียมการยกร่าง การพิจารณาว่าเนื้อหาดังกล่าวควรถูกบัญญัติในกฎหมายฉบับใดนั้นอาจขึ้นอยู่กับแนวทางการปฏิบัติเช่นหากต้องการกำหนดแนวทางของรัฐในการสืบค้นและยึดหลักฐานในการประกอบอาชญากรรมทางคอมพิวเตอร์ก็อาจกำหนดบทบัญญัติดังกล่าวในกฎหมายอาชญากรรมคอมพิวเตอร์

ในการยกร่างกฎหมายดังกล่าว ผู้เกี่ยวข้องควรติดตามความเคลื่อนไหวของการออกกฎหมายหรือกำหนดหลักเกณฑ์ในลักษณะเดียวกันในต่างประเทศโดยเฉพาะความตกลงขององค์กรความร่วมมือด้านเศรษฐกิจและการพัฒนา เนื่องจากมีความเป็นไปได้สูงว่าในอนาคตประเทศไทยจำเป็นต้องมีความร่วมมือกับต่างประเทศในระดับพหุภาคีหรือทวิภาคีในการปราบปรามอาชญากรรมทางคอมพิวเตอร์ และควรเปิดรับข้อคิดเห็นจากประชาชนในวงกว้างในการออกกฎหมายดังกล่าว เนื่องจากกฎหมายดังกล่าวเป็นกฎหมายที่อยู่ในข่ายละเมิดสิทธิเสรีภาพของประชาชน

ตารางที่ 3.1 นโยบายการเข้ารหัสของประเทศต่างๆ

ประเทศ	ข้อจำกัดในการส่งออก-นำเข้า	ข้อจำกัดในการใช้ในประเทศ
ออสเตรเลีย	ต้องขออนุญาตเป็นรายลักษณ์อักษรในการส่งออกอุปกรณ์และซอฟต์แวร์ที่ใช้เทคโนโลยีเข้ารหัส	ไม่มีข้อจำกัด
แคนาดา	เป็นไปตามความตกลงวัสเซนนาร์ ไม่มีข้อจำกัดในการส่งออกไปยังหรือนำเข้าจากสหรัฐ	ไม่มีข้อจำกัด
ฝรั่งเศส	ต้องสำแดงอุปกรณ์ที่รักษาความถูกต้อง (authentication-only or integrity-only) และต้องขออนุญาตนำเข้าหรือส่งออกอุปกรณ์ที่ใช้เทคโนโลยีเข้ารหัสอื่น ๆ	สามารถใช้การเข้ารหัสในการรักษาความลับได้หากมีการเก็บกุญแจไว้กับบุคคลที่สามที่เชื่อถือได้ การใช้งานอื่น ๆ เช่นเพื่อรับรอง และระบุตัวบุคคลไม่มีข้อจำกัด
ญี่ปุ่น	เป็นไปตามความตกลงวัสเซนนาร์ และการส่งออกเกินกว่า 5 หมื่นหน่วยต้องขออนุญาตเป็นพิเศษ	ไม่มีข้อจำกัด
สิงคโปร์	ไม่ทราบแน่ชัด	การเข้ารหัสโดยฮาร์ดแวร์ (hardware encryption) จะต้องได้รับอนุญาตก่อน
เกาหลีใต้	ห้ามการนำเข้า	ห้ามการส่งออก
สหรัฐ	ห้ามการส่งออกเทคโนโลยีเข้ารหัสที่มีขีดความสามารถสูง	ไม่มีข้อจำกัด
ปากีสถาน	ไม่มีข้อจำกัด	ห้ามการเข้ารหัสเสียง (voice-encryption)
รัสเซีย	ต้องมีใบอนุญาตในการส่งออกหรือนำเข้า	ห้ามการเข้ารหัสโดยไม่ได้รับอนุญาต
จีน	ห้ามนำเข้าและส่งออกอุปกรณ์ที่เข้ารหัสเสียง (voice-encryption device)	ไม่ทราบสถานะ

ที่มา: ปรับปรุงจาก Simson Garfinkel and Gene Spafford, *Web Security & Commerce*, O' Reilly, 1997

บทที่ 4
แนวทางในการออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์ในประเทศไทย

ในอนาคตอันใกล้ประเทศไทยคงจะมีกฎหมายพื้นฐานสำหรับการพาณิชย์อิเล็กทรอนิกส์ ซึ่งยอมรับฐานะทางกฎหมายของเอกสารและลายมือชื่ออิเล็กทรอนิกส์ จุดมุ่งหมายของการออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์เพิ่มเติมจากกฎหมายดังกล่าวคือการกำหนดลักษณะของลายมือชื่ออิเล็กทรอนิกส์ที่ยอมรับได้ และส่งเสริมให้เกิดการใช้เทคโนโลยีดังกล่าวอย่างแพร่หลายในการพาณิชย์อิเล็กทรอนิกส์โดยสร้างสภาวะแวดล้อมทางกฎหมายที่มีความแน่นอนและสามารถคาดหมายผลลัพท์ได้

ในบทนี้ผู้วิจัยจะนำเสนอแนวทางในการออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์ในประเทศไทย โดยจะวิเคราะห์ประเด็นสำคัญที่ต้องพิจารณา 4 ประเด็นดังต่อไปนี้คือ

1. ควรกำหนดขอบเขตของกฎหมายให้มุ่งใช้กับลายมือชื่อและใบรับรองอิเล็กทรอนิกส์ที่ใช้เทคโนโลยีใดเป็นการเฉพาะเจาะจงหรือไม่
2. ควรกำกับดูแลองค์กรออกใบรับรองด้วยระบบใบอนุญาตหรือไม่ อย่างไร
3. ควรแบ่งหน้าที่และความรับผิดชอบของฝ่ายต่าง ๆ ที่เกี่ยวข้องเช่น เจ้าของลายมือชื่ออิเล็กทรอนิกส์ ผู้ใช้ลายมืออิเล็กทรอนิกส์ของผู้อื่นและองค์กรออกใบรับรองอย่างไร
4. ควรยอมรับลายมือชื่ออิเล็กทรอนิกส์ที่ออกโดยองค์กรออกใบรับรองที่ตั้งอยู่ในต่างประเทศหรือไม่ ภายใต้เงื่อนไขใด

คำตอบของคำถามดังกล่าวจะเป็นอย่างไรย่อมขึ้นอยู่กับหลักการและจุดประสงค์ในการออกกฎหมาย ผู้วิจัยเสนอว่าหลักการและจุดประสงค์ในการออกกฎหมายดังกล่าวในประเทศไทยควรประกอบไปด้วย

1. หลักความเป็นกลางทางเทคโนโลยี (technology neutrality) ไม่บิดเบือนกลไกตลาด เพื่อให้ตลาดสามารถคัดเลือกเทคโนโลยีที่เหมาะสมที่สุด
2. หลักการที่ถือว่าเอกชนควรเป็นผู้นำในการพาณิชย์อิเล็กทรอนิกส์ โดยรัฐจะไม่เข้าไปแทรกแซงโดยไม่มีเหตุผลอันสมควร
3. หลักการส่งเสริมความสอดคล้องกับสากลเนื่องจากการพาณิชย์อิเล็กทรอนิกส์เป็นรูปแบบของการพาณิชย์ซึ่งอาจเกี่ยวข้องกับผู้ซื้อและผู้ขายที่อยู่ในคนละประเทศ ความสอดคล้องของกฎหมายไทยกับกฎหมายสากลจึงเป็นสิ่งที่มีความสำคัญเป็นอย่างยิ่ง

ในการวิเคราะห์ประเด็นต่าง ๆ ในบทนี้ ผู้วิจัยจะอ้างอิงร่างข้อกำหนดมาตรฐานว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ของคณะกรรมาธิการด้านกฎหมายของสหประชาชาติ (UNCITRAL Uniform Rules on Electronic Signatures) และกฎหมายที่เกี่ยวข้องของประเทศอื่นๆ เช่น กฎหมายธุรกรรมอิเล็กทรอนิกส์ของสิงคโปร์ (Singapore's Electronic Transaction Act) และร่างข้อกำหนดของสหภาพยุโรป (EU Directive) ประกอบ[1]

4.1 ขอบเขตของกฎหมาย

ปัญหาแรกที่ผู้ออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์จะต้องตัดสินใจคือจะออกกฎหมายให้สามารถใช้ได้กับเทคโนโลยีในการออกใบรับรองทั้งหมดเช่นการเข้ารหัสโดยใช้กุญแจสาธารณะ การตรวจสอบลักษณะทางชีวภาพ (biometrics) ตลอดจนเทคโนโลยีอื่น ๆ ที่ยังไม่ถูกคิดค้นขึ้นในปัจจุบัน หรือจะออกกฎหมายที่มุ่งใช้กับเทคโนโลยีที่แพร่หลายอยู่ในปัจจุบันคือเทคโนโลยีการเข้ารหัสด้วยกุญแจสาธารณะโดยเฉพาะ

หากยึดหลักการความเป็นกลางทางเทคโนโลยีแล้ว การออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์ไม่ควรที่จะมุ่งเน้นเฉพาะเทคโนโลยีใดเทคโนโลยีหนึ่ง เนื่องจากการออกกฎหมายที่มุ่งเน้นเฉพาะเทคโนโลยีนอกจากจะบิดเบือนกลไกลตลาดจากการทำให้เทคโนโลยีแต่ละชนิดมีฐานะทางกฎหมายที่แตกต่างกันแล้ว ยังจะทำให้กฎหมายล้าสมัยได้ง่ายเมื่อเกิดเทคโนโลยีใหม่มาทดแทนเทคโนโลยีเดิมเช่นในปี 1995 ผู้ออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์ส่วนใหญ่เชื่อกันว่าการเข้ารหัสด้วยกุญแจสาธารณะเป็นวิธีการเดียวในการระบุตัวบุคคล อย่างไรก็ตามหลังจากนั้นเราจะเห็นว่าเกิดเทคโนโลยีในการระบุตัวบุคคลชนิดต่าง ๆ มากมายเช่นการตรวจสอบลักษณะทางชีวภาพ หรือการกำหนดเลขหมาย (serial number) ของไมโครโปรเซสเซอร์เพนเทียมรุ่นที่สาม (Pentium III) ของบริษัทอินเทล ซึ่งจะช่วยให้ระบุตัวผู้ใช้เครื่องคอมพิวเตอร์ได้ง่ายขึ้น แม้ว่าวิธีดังกล่าวได้รับการคัดค้านจนต้องล้มเลิกไปในที่สุดก็ตาม

นอกจากนี้หากเรายึดถือหลักความเป็นกลางทางเทคโนโลยีอย่างเคร่งครัด เราก็ไม่ควรแบ่งลายมือชื่อออกเป็นชั้นต่าง ๆ เช่นแบ่งเป็น 2 ระดับ (two-tier approach) คือลายมือชื่อดิจิตัลหรือที่เรียกกันว่า "ลายมือชื่อขั้นสูง" (enhanced signature หรือ secure signature) กับลายมือชื่ออิเล็กทรอนิกส์อื่น ๆ ดังที่ปรากฏอยู่ในกฎหมายของบางประเทศซึ่งกำหนดให้ลายมือชื่อ

---

[1] ร่างข้อกำหนดมาตรฐานว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ของคณะกรรมาธิการด้านกฎหมายของสหประชาชาติที่จะอ้างอิงในบทนี้เป็นร่างที่ใช้ในการประชุมครั้งที่ 35 ของคณะทำงานด้านการพาณิชย์อิเล็กทรอนิกส์ (Working Group on Electronic Commerce) ดู United Nations Commission on International Trade Law, Working Group on Electronic Commerce, *Draft Uniform Rules on Electronics Signatures* และ *Report of the Working Group on Electronic Commerce on the Work of Its Thirty-Fifth Session*, Vienna, 6-17 September 1999

ทั้งสองแบบนี้มีผลทางกฎหมายที่แตกต่างกันเช่น ในการลงลายมือชื่อดิจิตัลให้สันนิษฐานว่าเจ้าของกุญแจส่วนตัวที่ใช้ในการลงลายมือชื่อนั้นเป็นผู้ลงลายมือชื่อ (presumption of identity) และได้แสดงเจตนาในการลงลายมือชื่อในเอกสาร (presumption of intent to sign) ในขณะที่การลงลายมือชื่ออิเล็กทรอนิกส์แบบอื่นจะไม่มีผลทางกฎหมายในลักษณะดังกล่าว[2]

4.2 การกำกับดูแลด้วยระบบใบอนุญาต

ประเด็นปัญหาอีกประการหนึ่งซึ่งผู้ยกร่างกฎหมายลายมือชื่ออิเล็กทรอนิกส์ต้องตัดสินใจคือจะกำหนดให้ธุรกิจออกใบรับรองเป็นธุรกิจที่ต้องได้รับใบอนุญาตในการประกอบการหรือจะปล่อยเป็นธุรกิจที่ประกอบการได้โดยเสรี เหตุผลในการใช้ระบบใบอนุญาตคือรัฐจะสามารถกำกับดูแลธุรกิจดังกล่าวได้สะดวกขึ้น ซึ่งอาจมีความจำเป็นในการคุ้มครองผู้ถือใบรับรองหรือผู้ที่ใช้ใบรับรองในการระบุตัวผู้อื่น

ตัวอย่างของกฎหมายที่กำกับดูแลธุรกิจออกใบรับรองในระบบใบอนุญาตได้แก่ กฎหมายของอิตาลีซึ่งกำหนดให้องค์กรออกใบรับรองทุกแห่งต้องจดทะเบียนกับหน่วยงานกำกับดูแล และต้องปฏิบัติตามข้อกำหนดด้านการเงินและด้านเทคนิคต่าง ๆ เช่นจะต้องมีเงินทุนจดทะเบียนไม่น้อยกว่า 7.5 ล้านดอลลาร์สหรัฐ และพนักงานขององค์กรออกใบรับรองจะต้องมีคุณสมบัติเช่นเดียวกับพนักงานธนาคารพาณิชย์ เป็นต้น

นอกจากทางเลือกในการกำกับดูแลด้วยระบบใบอนุญาตแบบบังคับ (mandatory licensing scheme) ดังตัวอย่างของอิตาลีแล้ว รัฐยังสามารถกำกับดูแลธุรกิจออกใบรับรองได้ด้วยระบบใบอนุญาตแบบสมัครใจ (voluntary licensing scheme) ดังที่ปรากฏในกฎหมายธุรกรรมอิเล็กทรอนิกส์ของสิงคโปร์ซึ่งอนุญาตให้มีทั้งองค์กรออกใบรับรองที่ได้รับอนุญาต (licensed CA) และองค์กรออกใบรับรองอื่น ๆ (unlicensed CA) โดยกำหนดให้องค์กรออกใบรับรองในกลุ่มแรกมีเงื่อนไขในการประกอบกิจการที่เข้มงวดกว่า ในขณะเวลาเดียวกันก็จูงใจให้องค์กรออกใบรับรองต่าง ๆ เข้าสู่ระบบใบอนุญาตโดยกำหนดให้องค์กรออกใบรับรองที่ได้รับใบอนุญาตไม่ต้องมีความรับผิดชอบในกรณีที่มีผู้ปลอมแปลงใบรับรอง และสามารถจำกัดความรับผิดชอบสูงสุดในบางกรณีได้

---

[2] ตัวอย่างในการออกกฎหมายที่กำหนดให้มีวิธีการลงลายมือชื่ออิเล็กทรอนิกส์ 2 ระดับได้แก่กฎหมายธุรกรรมอิเล็กทรอนิกส์ของสิงคโปร์ (Singapore's Electronic Transaction Act) และข้อกำหนดของสหภาพยุโรป (EU Electronic Signatures Directive) เงื่อนไขของลายมือชื่ออิเล็กทรอนิกส์ที่จะได้รับการยอมรับให้เป็นลายมือชื่อขั้นสูงภายใต้กฎหมายทั้งสองได้แก่ ลายมือชื่อเป็นของเฉพาะตัวของผู้ลงลายมือชื่อ (uniqueness) สามารถใช้ระบุผู้ลงลายมือชื่อได้ (identity) ถูกสร้างขึ้นโดยวิธีที่ผู้สร้างสามารถควบคุมได้แต่เพียงผู้เดียว (security) และเชื่อมโยงเข้ากับข้อมูลที่เกี่ยวข้องในลักษณะที่ช่วยให้ทราบว่าข้อมูลนั้นถูกเปลี่ยนแปลงแก้ไขหรือไม่ (integrity) ในปัจจุบันมีเฉพาะเทคโนโลยีการลงลายมือชื่อดิจิตัลเท่านั้นที่เป็นการลง "ลายมือชื่อขั้นสูง" ตามกฎหมายดังกล่าว

ตัวอย่างของเงื่อนไขในการประกอบการขององค์กรออกใบรับรองที่ได้รับใบอนุญาตตามกฎหมายธุรกรรมอิเล็กทรอนิกส์ของสิงคโปร์ได้แก่

- เงื่อนไขในการขอรับใบอนุญาต การต่ออายุและการเพิกถอนใบอนุญาต
- เงินทุนจดทะเบียนขั้นต่ำในการประกอบการ ซึ่งจะช่วยให้องค์กรองค์กรออกใบรับรองมีความสามารถชดใช้ความเสียหายแก่ผู้ได้รับความเสียหายจากการออกใบรับรองที่ผิดพลาด
- มาตรฐานในการออกใบรับรองในด้านต่าง ๆ เช่นความสามารถของบุคลากรที่เป็นพนักงานขององค์กรออกใบรับรอง
- รูปแบบและเนื้อหาของใบรับรองที่ออก
- สิ่งที่ต้องรายงานต่อหน่วยงานกำกับดูแลและเอกสารที่ต้องจัดเก็บ
- การแต่งตั้งและจ่ายค่าตอบแทนให้แก่ผู้ตรวจสอบ (auditor)

แนวทางการกำกับดูแลองค์กรออกใบรับรองด้วยระบบใบอนุญาตแบบสมัครใจของสิงคโปร์เป็นแนวทางที่สอดคล้องกับร่างข้อกำหนดของสหภาพยุโรป (EU Directive) ซึ่งห้ามประเทศสมาชิกออกกฎหมายบังคับให้องค์กรออกใบรับรองทุกแห่งต้องขอใบอนุญาตประกอบการ ในกรณีที่ประเทศสมาชิกต้องการใช้ระบบใบอนุญาต ร่างข้อกำหนดดังกล่าวก็ให้ใช้นำระบบใบอนุญาตแบบสมัครใจมาใช้โดยเงื่อนไขในการขอใบอนุญาตต้องมีความที่ชัดเจนโปร่งใส และไม่มีลักษณะเลือกปฏิบัติ[3]

ผู้วิจัยมีข้อสังเกตว่าระบบใบอนุญาตไม่ได้เป็นเงื่อนไขที่จำเป็นในการกำกับดูแล ดังจะเห็นได้จากการที่กฎหมายธุรกรรมอิเล็กทรอนิกส์ของสิงคโปร์กำหนดให้องค์กรออกใบรับรองทุกแห่งต้องประกาศถ้อยแถลงแนวทางปฏิบัติในการออกใบรับรอง (Certification Practice Statement) และต้องปฏิบัติตามมาตรฐานในการเปิดเผยข้อมูลต่าง ๆ แก่สาธารณะและขั้นตอนในการยกเลิกหรือระงับใบรับรองชั่วคราว ไม่ว่าองค์กรออกใบรับรองนั้นจะได้รับใบอนุญาตหรือไม่ ระบบใบอนุญาตเพียงแต่ช่วยให้สามารถกำกับดูแลองค์กรออกใบรับรองได้สะดวกขึ้นเท่านั้น

ข้อพึงระวังในการยกร่างกฎหมายลายมือชื่ออิเล็กทรอนิกส์ในประเทศไทยก็คือหากรัฐต้องการนำระบบใบอนุญาตมาใช้ ระบบใบอนุญาตนั้นควรเป็นระบบใบอนุญาตแบบสมัครใจเพื่อ

---

[3] หากร่างข้อกำหนดดังกล่าวได้รับความเห็นชอบจากรัฐสภาของสหภาพยุโรป ประเทศที่มีกฎหมายไม่สอดคล้องเช่นอิตาลีจะต้องปรับปรุงแก้ไขกฎหมายของตนไม่ให้ขัดกับข้อกำหนดดังกล่าว

ป้องกันมิให้กฎหมายสร้างต้นทุนที่สูงขึ้นโดยไม่จำเป็นแก่องค์กรออกใบรับรองโดยเฉพาะอย่างยิ่งองค์กรออกใบรับรองที่ให้บริการในสภาพแวดล้อมแบบปิดซึ่งฝ่ายต่าง ๆ ที่เกี่ยวข้องมีความสัมพันธ์กันโดยสัญญาทั้งหมด ทำให้ความจำเป็นในการคุ้มครองจากความเสียหายจากการออกใบรับรองที่ผิดพลาดมีไม่มาก

4.3 หน้าที่และความรับผิดชอบของฝ่ายต่าง ๆ

กฎหมายลายมือชื่ออิเล็กทรอนิกส์ควรกำหนดหน้าที่ของฝ่ายต่าง ๆ ที่เกี่ยวข้องกับการใช้ลายมือชื่ออิเล็กทรอนิกส์คือผู้ลงลายมือชื่อ (signature holder) ผู้ใช้ลายมือชื่อ (relying party) และองค์กรออกใบรับรอง (certification authority) เพื่อให้การใช้ลายมือชื่ออิเล็กทรอนิกส์นั้นเป็นไปอย่างระมัดระวังไม่ก่อให้เกิดความเสียหายโดยไม่สมควรจากความประมาทหรือการกระทำที่เสี่ยงภัยเกินเหตุ (moral hazard)[4] โดยหลักการแล้วแต่ละฝ่ายควรจะมีหน้าที่ในการใช้ลายมือชื่ออิเล็กทรอนิกส์อย่างระมัดระวังตามสมควร (due care) ดังต่อไปนี้

ผู้ลงลายมือชื่อควรมีหน้าที่ในการใช้ลายมือชื่อของตนอย่างระมัดระวังโดย

- ใช้ความระมัดระวังตามสมควรในการยื่นหลักฐานที่ถูกต้องและสมบูรณ์ในการขอใบรับรอง การขอระงับหรือยกเลิกการใช้ใบรับรอง
- แจ้งให้ฝ่ายต่าง ๆ ที่เกี่ยวข้องทราบโดยเร็วที่สุดเมื่อลายมือชื่อของตนถูกล่วงรู้ (compromised) หรือสงสัยว่าอาจจะถูกล่วงรู้
- มีความระมัดระวังในการรักษาลายมือชื่อของตนนับตั้งแต่ครอบครอง

ผู้ใช้ลายมือชื่อของผู้อื่นควรมีความระมัดระวังตามสมควรโดย

- ใช้ลายมือชื่อหลังจากการดำเนินการตามขั้นตอนต่าง ๆ ในการตรวจสอบความถูกต้องและเชื่อถือได้เช่นตรวจสอบว่าลายมือนั้นหมดอายุ ถูกระงับหรือถูกยกเลิกไปแล้วหรือไม่ เป็นต้น
- ใช้ใบรับรองโดยคำนึงถึงข้อจำกัดที่ระบุไว้ในใบรับรองนั้น

---

[4] ร่างข้อกำหนดมาตรฐานว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ของคณะกรรมาธิการด้านกฎหมายของสหประชาชาติใช้คำว่า "ผู้รับรองสารสนเทศ" (information certifier) แทนคำว่าองค์กรออกใบรับรอง (certification authority) เพื่อป้องกันมิให้กฎหมายใช้ได้กับเฉพาะระบบที่มีผู้เกี่ยวข้อง 3 ฝ่าย เนื่องจากในหลายกรณีองค์กรออกใบรับรองและผู้ใช้ลายมือชื่ออาจเป็นบุคคลหรือหน่วยงานเดียวกัน ดังที่กล่าวมาแล้วในบทที่ 1

องค์กรออกใบรับรองมีภาระหน้าที่ขั้นต่ำในการให้บริการดังต่อไปนี้

- ดำเนินการตามแนวทางปฏิบัติหรือนโยบายที่ตนประกาศให้ผู้ใช้ได้ทราบ
- ใช้ความระมัดระวังในการตรวจสอบความถูกต้องของหลักฐานต่าง ๆ ที่ใช้ในการออก ระงับหรือเพิกถอนใบรับรอง
- อำนวยความสะดวกให้แก่ผู้ลงลายมือชื่อในการแจ้งการระงับหรือยกเลิกการใช้ลายมือชื่อ
- อำนวยความสะดวกแก่ผู้ใช้ในการตรวจสอบข้อมูลต่าง ๆ เช่นวิธีการใช้ลายมือชื่อในการระบุตัวบุคคล ข้อจำกัดในการใช้ใบรับรองที่ออก และข้อมูลเกี่ยวกับสถานะของใบรับรองว่าถูกระงับหรือยกเลิกไปแล้วหรือไม่ เป็นต้น
- ใช้ระบบ ขั้นตอนและบุคลากรที่เชื่อถือได้ในการให้บริการออกใบรับรอง

หากฝ่ายใดไม่ทำตามหน้าที่ดังกล่าวของตนโดยมีสาเหตุจากความประมาทเลินเล่อ ผู้นั้นก็จะต้องรับผิดชอบในการชดใช้ความเสียหายให้แก่ผู้เสียหาย ซึ่งมูลค่าของความเสียหายที่จะต้องชดใช้ให้แก่กันนั้นอาจถูกกำหนดล่วงหน้าในสัญญาระหว่างฝ่ายต่าง ๆ ส่วนในกรณีที่ไม่มีการทำสัญญาล่วงหน้าระหว่างองค์กรออกใบรับรองและผู้ใช้ใบรับรอง ซึ่งอาจเกิดขึ้นได้ในสภาพแวดล้อมแบบเปิด การชดใช้ค่าเสียหายก็จะเป็นไปตามหลักแห่งกฎหมายละเมิด[5] ในกรณีนี้กฎหมายของบางประเทศอาจอนุญาตให้องค์กรออกใบรับรองสามารถกำหนดขอบเขตของความรับผิดชอบสูงสุดของตนได้เช่น กฎหมายของสิงคโปร์อนุญาตให้องค์กรออกใบรับรองที่ได้รับใบอนุญาต (licensed CA) สามารถจำกัดความรับผิดชอบสูงสุดของตนได้โดยระบุมูลค่าสูงสุดในใบรับรอง ซึ่งอาจใช้เป็นแบบอย่างในการออกกฎหมายลายมือชื่ออิเล็กทรอนิกส์ในประเทศไทยได้

สิ่งที่จะเกิดขึ้นจากการยินยอมให้ธุรกิจออกใบรับรองสามารถจำกัดภาระความรับผิดชอบได้ก็คือผู้ใช้ใบรับรองจะต้องประเมินความเสี่ยงของตนที่อาจเกิดขึ้นโดยเทียบกับประโยชน์ที่จะได้รับ ในกรณีที่ธุรกรรมมีมูลค่าสูงผู้ใช้อาจไม่ยอมใช้ใบรับรองนั้นหากเห็นว่าอาจไม่ได้รับการชดเชยอย่างเพียงพอ ผู้วิจัยเสนอว่าก่อนที่รัฐจะทำการแทรกแซงตลาดโดยวิธีการใดเพื่อแก้ไขปัญหาดังกล่าว ก็ควรปล่อยให้กลไกตลาดแก้ไขปัญหาเองก่อน เพราะหากตลาดสามารถทำงานได้อย่างสมบูรณ์ ในที่สุดจะมีองค์กรออกใบรับรองบางแห่งที่จะยอมชดใช้ความเสียหายในมูลค่าที่สูงขึ้น โดยปรับค่าธรรมเนียมในการออกใบรับรองให้เหมาะสม

---

[5] มาตรา 420 ของประมวลกฎหมายแพ่งและพาณิชย์บัญญัติว่า *ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี ทรัพย์หรือสิทธิอย่างใดอย่างหนึ่งก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้สินไหมทดแทนเพื่อการนั้น*

4.4 การยอมรับลายมือชื่ออิเล็กทรอนิกส์หรือใบรับรองที่ออกในต่างประเทศ

ผู้วิจัยเชื่อว่าในเวทีการเจรจาการค้าระหว่างประเทศว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ในอนาคต ประเด็นที่จะมีความสำคัญเป็นอย่างสูงคือการยอมรับลายมือชื่อหรือใบรับรองที่ออกโดยหน่วยงานรับรองในต่างประเทศ โดยประเทศพัฒนาแล้วคงจะพยายามผลักดันให้ประเทศอื่น ๆ ไม่เลือกปฏิบัติ (non-discrimination) ต่อใบรับรองของตน[6]

ตัวอย่างบทบัญญัติที่ป้องกันการเลือกปฏิบัติต่อใบรับรองต่างชาติได้แก่

1. ในการพิจารณาว่าใบรับรองอิเล็กทรอนิกส์ใดจะมีผลทางกฎหมายหรือไม่ จะไม่นำสถานที่ที่ออกใบรับรอง ตลอดจนประเทศที่เป็นที่ตั้งของหน่วยงานที่ออกใบรับรองนั้นมาพิจารณา
2. ใบรับรองที่ออกโดยหน่วยงานออกใบรับรองในต่างประเทศจะมีผลทางกฎหมายเช่นเดียวกันกับใบรับรองที่ออกโดยหน่วยงานออกใบรับรองในประเทศ หากแนวทางปฏิบัติในการออกใบรับรองของหน่วยงานดังกล่าวมีความเชื่อถือได้ที่ไม่น้อยไปกว่าแนวทางปฏิบัติที่กำหนดในกฎหมายในประเทศ
3. ลายมือชื่ออิเล็กทรอนิกส์ที่ออกตามข้อกำหนดของกฎหมายต่างประเทศจะมีผลทางกฎหมายเทียบเท่ากับลายมือชื่อที่ออกในประเทศ หากกฎหมายของต่างประเทศกำหนดมาตรฐานความเชื่อถือได้ไม่ต่ำกว่ามาตรฐานที่กำหนดไว้ในกฎหมายในประเทศ
4. ให้อิสระกับคู่สัญญาซึ่งทำธุรกรรมอิเล็กทรอนิกส์ในการกำหนดองค์กรรับรอง หรือมาตรฐานขององค์กรรับรอง หรือใบรับรองในการติดต่อกันที่ทั้งสองฝ่ายยอมรับ

ต่อประเด็นนี้ ผู้วิจัยเห็นว่าหลักการปฏิบัติเยี่ยงคนชาติดังกล่าวเป็นหลักการที่ประเทศไทยควรยอมรับ เพราะการยอมรับใบรับรองต่างชาติที่ได้มาตรฐานให้มีฐานะทางกฎหมายจะช่วยเพิ่มทางเลือกให้แก่ผู้ใช้ในประเทศไทย อย่างไรก็ตามข้อควรระวังก็คือต่างประเทศอาจจะไม่ยอมรับใบรับรองของประเทศไทย ทั้งจากการไม่กำหนดบทบัญญัติในลักษณะดังกล่าวข้างต้น

---

[6] หากจะกล่าวด้วยคำศัพท์ที่ใช้ในวงการกฎหมายระหว่างประเทศ การไม่เลือกปฏิบัติในที่นี้มีความหมายเช่นเดียวกับ "การปฏิบัติเยี่ยงคนชาติ" (national treatment) ในธุรกิจดังกล่าว

[7] Variant A ของมาตราที่ 13 ของร่างข้อกำหนดมาตรฐานว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ของคณะกรรมาธิการด้านกฎหมายของสหประชาชาติจาก Report of the Working Group on Electronic Commerce on the Work of Its Thirty-Fifth Session, Vienna 6-17 September 1999

ในกฎหมายของตน หรือแม้จะกำหนดบทบัญญัติดังกล่าวลงในกฎหมาย ก็อาจจะอ้างว่าการออกลายมือชื่อหรือใบรับรองในประเทศไทยไม่ได้มาตรฐานเพื่อกีดกันทางการค้าได้ ทั้งนี้เนื่องจากการเปรียบเทียบมาตรฐานในการออกใบรับรองของแต่ละประเทศไม่สามารถหลีกเลี่ยงความเป็นอัตวิสัย (subjectivity) ได้ทั้งหมด ทางออกในเรื่องดังกล่าวน่าจะได้แก่การเสนอให้มีการกำหนดมาตรฐานขั้นต่ำซึ่งมีความโปร่งใส ซึ่งทุกประเทศที่ทำความตกลงร่วมกันจะต้องยอมรับใบรับรองที่ผ่านมาตรฐานดังกล่าว[8]

นอกจากประเด็นต่าง ๆ ดังกล่าวข้างต้นแล้ว กฎหมายลายมือชื่ออิเล็กทรอนิกส์ของประเทศไทยควรพิจารณาให้คู่สัญญามีอิสระในการทำสัญญาที่แตกต่างจากข้อกำหนดในกฎหมายได้ตามสมควรตราบเท่าที่การกระทำเช่นนั้นไม่ส่งผลกระทบร้ายแรงต่อบุคคลที่สามเช่น ควรยินยอมให้คู่สัญญาสามารถเปลี่ยนแปลงหน้าที่และความรับผิดชอบได้ตามสมควรเพื่อป้องกันมิให้กฎหมายเป็นอุปสรรคต่อการทำธุรกรรมทางการพาณิชย์อิเล็กทรอนิกส์ โดยเฉพาะการทำธุรกรรมในสภาพแวดล้อมแบบปิดซึ่งแต่ละฝ่ายมีความสัมพันธ์เชิงสัญญากันอยู่แล้ว

นอกจากนี้เพื่อให้กฎหมายลายมือชื่ออิเล็กทรอนิกส์ของไทยมีความสอดคล้องกับกฎหมายของนานาประเทศ ผู้ดำเนินการยกร่างกฎหมายดังกล่าวควรติดตามความเคลื่อนไหวในการออกกฎหมายที่เกี่ยวข้องในต่างประเทศอย่างใกล้ชิด โดยเฉพาะร่างข้อกำหนดมาตรฐานว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ของคณะกรรมาธิการด้านกฎหมายของสหประชาชาติ ซึ่งอาจจะกลายเป็นกฎหมายต้นแบบของประเทศต่าง ๆ ในอนาคต

---

[8] ใน Variant B ของมาตราที่ 13 ของร่างข้อกำหนดมาตรฐานว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ของคณะกรรมาธิการด้านกฎหมายของสหประชาชาติ มีความพยายามกำหนดปัจจัยต่าง ๆ เช่นความมั่นคงทางการเงิน ความปลอดภัยของระบบฮาร์ดแวร์และซอฟต์แวร์ ขั้นตอนในการออกใบรับรองและเก็บบันทึกเป็นต้น ซึ่งจะนำพิจารณาว่าการออกใบรับรองขององค์กรรับรองได้มาตรฐานหรือไม่ อย่างไรก็ตามแม้ว่าข้อเสนอดังกล่าวจะทำให้การยอมรับใบรับรองต่างชาติมีความโปร่งใสมากขึ้นก็ตาม ความเป็นอัตวิสัยในการพิจารณาก็ยังมีเหลืออยู่เช่นเดิม

บรรณานุกรม

Certification Authority Working Group, "Certification Authority Guidelines (Alpha version)", ECOM, (www.ecom.or.jp)

Dow Jones Business News, Investors See Differences in Two Leading Web Security Companies, September 1, 1999

OECD, "Inventory of Approaches to Authentication and Certification in a Global Networked Society", 1999

Simson Garfinkel and Gene Spafford, "Web Security & Commerce", O' Reilly, 1997

Task Force on Electronic Commerce, Industry Canada, "A Cryptograhy Policy Framework for Electronic Commerce", February 1998

United Nations Commission on International Trade Law, Working Group on Electronic Commerce, Draft Uniform Rules on Electronics Signatures

United Nations Commission on International Trade Law, Working Group on Electronic Commerce, Report of the Working Group on Electronic Commerce on the Work of Its Thirty-Fifth Session, Vienna, 6-17 September 1999