การพัฒนาระบบซื้อสินค้าและชำระค่าสินค้าบนอินเตอร์เน็ต ด้วยมาตรฐาน SET

The Development of Purchase and Payment System in E-Commerce with SET Standard

โดย

น.ส. บงกชเกษ สุขตระกูล

รหัส 41067104

H001664

อาจารย์ที่ปรึกษา

ดร. นพพร โชติกกำธร

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 1 ปีการศึกษา 2543

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	การพัฒนาระบบซื้อสินค้าและชำระค่าสินค้าบนอินเตอร์เน็ตด้วยมาตรฐาน SET
นักศึกษา	น.ส. บงกชเกษ สุขตระกูล
อาจารย์ที่ปรึกษา	ดร. นพพร โชติกกำธร
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2543

บทคัดย่อ

ในการทำธุรกิจบนเครือข่ายขนาดใหญ่ เช่น อินเตอร์เน็ต ความปลอดภัยของข้อมูลที่ติดต่อสื่อสารกันเป็นสิ่งสำคัญ ทั้งในด้าน Confidentiality, Authentication, Non-repudiation และ Integrity ในโครงการนี้จะศึกษาและวิเคราะห์ถึงระบบงานที่ใช้ในการซื้อขายสินค้าบนอินเตอร์เน็ต และพัฒนาระบบการซื้อขายสินค้าที่มีการตรวจสอบความถูกต้องของข้อมูลและบุคคลต่างๆในระบบ โดยนำหลักการทำงานของ SET มาเป็นมาตรฐานในการทำรายการซื้อสินค้าและชำระค่าสินค้า

Title	The Development of Purchase and Payment System in E-commerce with SET Standard
Student	Miss. Bongkochgate Suktrakul
Advisor	Dr. Nopporn Chotikakamtorn
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2000

ABSTRACT

The business on E-commerce, data security is the most important in the part of confidentiality, authentication, non-repudiation and integrity. This system development project studies and analyzes the business on E-commerce as well as verifies information and persons by using the concept of SET standard in purchase and payment transactions.

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญภาพ

สารบัญภาพ (ต่อ)

สารบัญตาราง

บทที่ 1
บทนำ

ในการทำธุรกิจบนอินเตอร์เน็ตสิ่งที่จะต้องคำนึงถึงคือความปลอดภัยของข้อมูลที่ติดต่อสื่อสารกัน ซึ่งในปัจจุบันข้อมูลในการซื้อขายสินค้าบนอินเตอร์เน็ตยังสามารถที่จะถูกเปลี่ยนแปลงแก้ไขหรือปลอมแปลงได้ เนื่องมาจากวิธีการป้องกันหรือการรักษาความปลอดภัยในการทำธุรกิจซื้อขายสินค้าบนอินเตอร์เน็ตในปัจจุบันนั้นสามารถที่จะถอดรหัสข้อมูลออกเพื่อทำการขโมยข้อมูลหรือปลอมแปลงรายการเพื่อทำการซื้อสินค้าได้

การซื้อขายสินค้าบนอินเตอร์เน็ตข้อมูลที่สำคัญคือ หมายเลขบัตรเครดิต ซึ่งเป็นข้อมูลส่วนบุคคลที่ควรรู้เฉพาะเจ้าของบัตรเครดิตที่ทำรายการและบริษัทที่รับชำระบัตรเครดิตเท่านั้น ร้านค้าที่ให้บริการขายสินค้าหรือบุคคลอื่นไม่จำเป็นต้องทราบหมายเลขบัตรเครดิต จากแนวคิดนี้จึงนำไปสู่โครงการการพัฒนาการตรวจสอบความถูกต้องของข้อมูลและบุคคลในงานซื้อขายสินค้าผ่านอินเตอร์เน็ตโดยใช้ Certification Authority Server เพื่อเป็นการป้องกันข้อมูลที่สำคัญจากผู้ที่ไม่เกี่ยวข้องและเป็นการยืนยันถึงบุคคลนั้นด้วย

1.1 วัตถุประสงค์

1. เพื่อการตรวจสอบและป้องกันข้อมูลการซื้อขายสินค้าบนอินเตอร์เน็ต เช่น หมายเลขบัตรเครดิต จากบุคคลที่ไม่เกี่ยวข้อง
2. เพื่อนำหลักการทำงานของระบบ SET (Secure Electronic Transaction) มาประยุกต์ใช้ในการซื้อขายสินค้าบนอินเตอร์เน็ต

1.2 ขั้นตอนการศึกษา

1. ศึกษาหลักการทำงานของ Certification Authority (CA) และระบบ SET (Secure Electronic Transaction)
2. ศึกษาซอฟต์แวร์ที่ใช้ในการเข้ารหัสและถอดรหัสด้วยวิธี Public Key Cryptography
3. พัฒนาโปรแกรมการลงทะเบียนข้อมูลและหมายเลขบัตรเครดิตและการ Import Public Key เข้าสู่ระบบ

4. พัฒนาโปรแกรมการสั่งซื้อสินค้าและการเข้ารหัสและถอดรหัสข้อมูลการสั่งซื้อสินค้าบนอินเตอร์เน็ต

1.3 ขอบเขตการศึกษา

การวิจัยนี้จะทำการเข้ารหัสข้อมูลที่ใช้ติดต่อซื้อขายสินค้าบนอินเตอร์เน็ตทั้งในส่วนของข้อมูลการสั่งซื้อสินค้าและข้อมูลการชำระค่าสินค้า โดยนำหลักการทำงานของระบบ SET มาใช้เป็นแบบแผนในการพัฒนา

1.4 ประโยชน์ที่ได้รับ

1. ได้เรียนรู้และเข้าใจหลักการทำงานของ Certification Authority Server และระบบ SET
2. ได้เรียนรู้และเข้าใจหลักการทำงานในการเข้ารหัสและถอดรหัสโดยวิธี Public Key Cryptography
3. สามารถตรวจสอบและป้องกันข้อมูลที่รับส่งบนอินเตอร์เน็ตจากบุคคลที่ไม่เกี่ยวข้องได้

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 วิวัฒนาการของการค้าอิเล็กทรอนิกส์

การค้าอิเล็กทรอนิกส์นั้นเกิดขึ้นมาตั้งแต่ ปี ค.ศ. 1960 โดยเริ่มจากบริษัทในสหรัฐอเมริกาได้นำการส่งเอกสารทางอิเล็กทอนิกส์ที่เรียกว่าระบบ EDI (Electronic Data Interchange) คือการส่งเอกสารหรือแบบฟอร์มอิเล็กทรอนิกส์ที่เป็นมาตรฐานเพื่อการติดต่อทำการค้าระหว่างกัน มาช่วยในการซื้อขายสินค้าระหว่างบริษัท นอกจากนี้สถาบันการเงินและธนาคารต่างๆ ได้มีการสร้างเครือข่ายคอมพิวเตอร์ที่เรียกว่า EFT (Electronic Funds Transfer) คือใช้ส่งผ่านรายการโอนเงินในเครือข่ายคอมพิวเตอร์ของสถาบันการเงิน เพื่อใช้ในการโอนเงินตราระหว่างธนาคาร ในช่วงเวลาดังกล่าวการติดตั้ง EDI จะต้องสร้างเครือข่ายสื่อสารส่วนตัวขึ้นมาเองซึ่งเป็นการลงทุนที่สูง และราคาแพง การใช้งานของ EDI จึงจำกัดอยู่ที่บริษัทขนาดใหญ่และสถาบันการเงินที่มีทุนทรัพย์เท่านั้น แต่ในปัจจุบันความแพร่หลายของอินเตอร์เน็ต ทำให้โลกการค้าอิเล็กทรอนิกส์เปลี่ยนแปลงไป อินเตอร์เน็ตได้กลายเป็นช่องทางสื่อสารรูปแบบใหม่ที่มีการนำไปใช้งานอย่างกว้างขวาง จนทำให้ระบบการค้าอิเล็กทรอนิกส์ในปัจจุบันขยายตัวอย่างรวดเร็วและไม่ได้จำกัดอยู่แต่เฉพาะสถาบันการเงินและบริษัทขนาดใหญ่เหมือนแต่ก่อน

2.2 ประเภทของการค้าอิเล็กทรอนิกส์

โครงสร้างของระบบการค้าอิเล็กทรอนิกส์สามารถจำแนก ออกเป็นประเภทต่างๆ ได้ดังต่อไปนี้

2.2.1 การค้าอิเล็กทรอนิกส์จัดแบบตามโครงสร้าง

จัดแบ่งได้ดังนี้

1. Consumer-to-Business คือ การค้าอิเล็กทรอนิกส์ระหว่างผู้บริโภคกับธุรกิจ
2. Intra-Org E-commerce คือ การค้าอิเล็กทรอนิกส์ภายในองค์กร เพื่อช่วยในการปรับปรุงการทำงานภายใน และให้บริการลูกค้าได้ดีขึ้น
3. Inter-Org E-commerce คือ การค้าอิเล็กทรอนิกส์ระหว่างองค์กร เป็นแบบเดียวกับการค้าอิเล็กทรอนิกส์ระดับ B2B (Business-to-Business) ซึ่งเป็นการค้าทางอิเล็กทรอนิกส์ระหว่างองค์กรกับองค์กร ด้วยกัน

2.2.2 การค้าอิเล็กทรอนิกส์เชิงพาณิชย์

จัดแบ่งได้ดังนี้

1. B2B (Business-to-Business) เป็นการค้าขนาดใหญ่ระหว่างองค์กรกับองค์กร ซึ่งโดยทั่วไปจะเป็นสินค้าส่งออกหรือนำเข้าที่ต้องส่งสินค้าเป็นจำนวนมาก ซึ่งการชำระเงินจะผ่านระบบธนาคาร
2. B2C (Business-to-Consumer) เป็นการค้าปลีกไปยังผู้บริโภคทั่วโลก หรือภายในท้องถิ่นของตน ในส่วนนี้อาจจะรวมการค้าปลีกแบบจำนวนมากไว้ด้วย ซึ่งการชำระเงินโดยส่วนใหญ่จะเป็นการชำระเงินผ่านระบบบัตรเครดิต แต่อย่างไรก็ตามการค้าแบบ B2C นี้ก็มักจะทำให้เกิดการค้าแบบ B2B ได้ในอนาคต และหลายบริษัทจะทำกิจกรรมสองอย่างนี้ในคราวเดียวกัน
3. C2C (Consumer-to-Consumer) เป็นการค้าปลีกระหว่างบุคคลทั่วไป หรือระหว่างผู้ใช้อินเตอร์เน็ตด้วยกัน เช่น การขายสินค้าที่ใช้งานแล้ว รวมถึงการขายซอฟต์แวร์ด้วย ซึ่งปัจจุบันมีเป็นจำนวนมาก โครงสร้างไม่ซับซ้อนมากนัก

2.3 ระบบการเงินบนการค้าอิเล็กทรอนิกส์

วิธีการชำระเงินบนอินเตอร์เน็ตนั้นจะเป็นเพียงแค่การส่งข้อมูลการตัดชำระเงินโดยใช้สื่อทางอิเล็กทรอนิกส์แทนการใช้เงินสด บัตรเครดิต หรือเช็คเท่านั้น ความแตกต่างที่สำคัญคือสื่อแทนเงินอันใหม่นี้เป็นข้อมูลดิจิตอลที่ไม่สามารถจับต้องได้ โดยจะมีการใช้ระบบอิเล็กทรอนิกส์มาประมวลผลการจ่ายหรือรับเงินแทนการรับเหรียญหรือธนบัตรจากมือหรือกระเป๋าเงิน การที่ข้อมูลทั้งหมดเป็นดิจิตอลทำให้ระบบชำระเงินต่างๆ ที่เกิดขึ้นบนอินเตอร์เน็ตมีพื้นฐานความคิดของระบบที่คล้ายคลึงกันเพียงแต่มีองค์กร ผู้พัฒนา และใช้ซอฟต์แวร์ที่แตกต่างกันไปเท่านั้น โดยสามารถแบ่งการชำระเงินออกได้เป็นแบบต่าง ๆ ดังนี้

2.3.1 การชำระเงินด้วยบัตรเครดิต

สำหรับการใช้บัตรเครดิตเพื่อใช้ในการชำระเงินบนอินเตอร์เน็ตนั้น จะมีลักษณะเช่นเดียวกับการชำระเงินด้วยบัตรเครดิตทั่วไป แต่จะมีการเพิ่มขั้นตอนเกี่ยวกับการรักษาความปลอดภัยของการส่งข้อมูลการทำรายการระหว่างลูกค้ากับร้านค้า รวมทั้งเพิ่มระบบที่ใช้ตรวจสอบว่าผู้ทำรายการซื้อขายเป็นบุคคลที่มีสิทธิจริง บัตรเครดิตสามารถนำมาใช้ซื้อสินค้าบนอินเตอร์เน็ตได้สองแบบคือ แบบการส่งผ่านข้อมูลของบัตรเครดิตโดยตรงโดยไม่มีการเข้ารหัสในการส่งข้อมูล และการเข้ารหัสก่อนแล้วจึงส่งข้อมูลไปให้ร้านค้า โดยการเข้ารหัสจะสามารถทำบางส่วนของข้อมูล ขึ้นอยู่กับข้อตกลงระหว่างกันว่าจะเข้ารหัสข้อมูลส่วนใด ถ้าลูกค้าเข้ารหัสข้อมูลทั้งหมดอย่างน้อยร้านค้าก็ต้อง

สามารถถอดรหัสส่วนที่เป็นรายละเอียดของสินค้าที่สั่งซื้อได้ จึงจะสามารถประมวลผลรายการของลูกค้านั้น และเพื่อป้องกันร้านค้าหรือผู้อื่นที่ไม่เกี่ยวข้องนำเอาข้อมูลหรือเลขที่บัตรเครดิตของลูกค้าไปใช้ ข้อมูลส่วนที่เป็นรายละเอียดของบัตรเครดิตจะถูกเข้ารหัสและถูกส่งต่อไปยังธนาคารหรือบริษัทที่ออกบัตรเครดิตเพื่อถอดรหัสและตรวจสอบความถูกต้อง แล้วจึงตัดเงินต่อไป

2.3.2 การชำระเงินด้วย เช็คอิเล็กทรอนิกส์

เป็นระบบที่พัฒนาขึ้นเพื่อให้ลูกค้าสามารถสั่งจ่ายเงินได้เหมือนกับการใช้เช็คสั่งจ่ายโดยตรงให้กับร้านค้าบนเครือข่ายอินเตอร์เน็ต ระบบเช็คอิเล็กทรอนิกส์จะมีลักษณะเดียวกับเช็คปกติเกือบทุกประการเพียงแต่เอกสารบนกระดาษถูกเปลี่ยนเป็นข้อมูลอิเล็กทรอนิกส์แทน ในการซื้อสินค้าหรือโอนเงิน ผู้สั่งจ่ายจะส่งข้อมูลไปให้ร้านค้าหรือผู้รับเงิน ทางร้านก็จะส่งผ่านข้อมูลนี้ต่อไปยังธนาคารหรือสถาบันการเงินเพื่อทำการโอนเงินเข้าบัญชี จากนั้นข้อมูลก็จะถูกส่งกลับมายังผู้สั่งจ่ายเพื่อบอกว่าได้โอนเงินเรียบร้อยแล้ว

ข้อดีของเช็คอิเล็กทรอนิกส์คือสามารถป้องกันการปลอมเช็คได้โดยการเข้ารหัสเลขที่บัญชีในแบบที่ธนาคารเท่านั้นที่จะสามารถถอดรหัสได้ ส่วนร้านค้าหรือผู้รับเช็คไปขึ้นเงินจะไม่สามารถทราบเลขที่บัญชีได้เลย นอกจากนี้ในการส่งผ่านข้อมูลอาจมีการใช้โปรโตคอล SET และใบรับรองดิจิตอล เข้ามาช่วยในการตรวจสอบข้อมูลที่ส่งมาว่ามาจากผู้สั่งจ่ายหรือจากธนาคารจริง ๆ

2.3.3 การชำระเงินด้วยเงินสดดิจิตอล (Digital Cash)

เงินสดดิจิตอลหรือ E-cash หรือ Digital Cash คือการนำข้อมูลดิจิตอลมาแทนการใช้เงินสด โดยระบบนี้จะเหมาะสำหรับการซื้อขายที่มีมูลค่าการซื้อขายน้อย และเป็นการขายสินค้าที่ลูกค้ารับสินค้าได้ทันทีบนอินเตอร์เน็ต เช่น การซื้อโปรแกรม ข้อมูลภาพ หรือข้อมูลข่าวสาร

ในระบบ Digital Cash ค่าของเงินจะเป็นเพียงชุดข้อมูลดิจิตอลเท่านั้น ทางธนาคารจะทำหน้าที่ออกชุดข้อมูลเหล่านี้ที่เรียกว่า Tokens และจะตัดเงินในบัญชีเป็นจำนวนเท่ากับมูลค่าของ Tokens เหล่านั้นที่ออกไป ในการออก Digital Cash นั้นทางธนาคารจะตรวจสอบข้อมูลของจำนวนเงิน พร้อมกับเพิ่มรายละเอียดในชุดข้อมูลของ Digital Cash ว่าสามารถชำระเงินจากชุดข้อมูลนี้ได้จริง จากนั้นจึงส่งชุดข้อมูลดังกล่าวมาให้ที่เครื่องคอมพิวเตอร์ของลูกค้า

เมื่อลูกค้าต้องการใช้ E-cash จะทำการส่งชุดข้อมูลดังกล่าวให้กับร้านค้า ทางร้านค้าจะนำชุดข้อมูล E-cash ที่ได้ไปตรวจสอบกับทางธนาคาร ถ้าทุกอย่างเรียบร้อย ทางธนาคารจะโอนเงินไปเข้าบัญชีของร้านค้าตามจำนวน E-cash ชุดหนึ่งจะสามารถใช้ได้เพียงครั้งเดียวโดยจะมีหมายเลขประจำแต่ละชุดข้อมูลที่จะไม่ซ้ำกัน

2.4 ปัญหาของการค้าอิเล็กทรอนิกส์

ระบบการค้าอิเล็กทรอนิกส์จะสมบูรณ์ได้ต้องมีขั้นตอนของการชำระเงิน ซึ่งขั้นตอนการชำระเงินดังกล่าวมีความแตกต่างกันไปตามประเภทของการค้าแต่ละชนิด วิธีการชำระเงินจึงถูกออกแบบมาให้เหมาะกับแต่ละประเภทการค้า เช่น การชำระเงินแบบ On-line Internet EDI (Electronics Data Interchange) เหมาะกับการค้าขนาดใหญ่ (Business-To-Business) ส่วนการชำระเงินสำหรับการค้าขนาดเล็กๆ จะใช้บัตรเครดิตเป็นหลัก ซึ่งสามารถใช้ได้ทั้งในประเทศและระหว่างประเทศมีสัดส่วนถึง 80% (ข้อมูลจากวีซ่า) ในการซื้อขายแบบปกติผู้ซื้อสามารถมั่นใจในสินค้าหรือบริการและตัวผู้ขายได้มากกว่าบนระบบออนไลน์ เนื่องจากสามารถมองเห็นและตรวจสอบได้ก่อนตัดสินใจซื้อ และเมื่อมีการชำระเงินด้วยบัตรเครดิต ผู้ขายจะได้รับลายเซ็นของผู้ซื้อบน Slip ซึ่งทำให้มั่นใจได้ว่าจะได้รับเงินอย่างแน่นอน แต่ในการชำระเงินด้วยบัตรเครดิตบนระบบการค้าอิเล็กทรอนิกส์หากไม่มีการรักษาความปลอดภัย ทั้งผู้ซื้อและผู้ขายอาจมีปัญหาดังตารางที่ 2 .1

จากปัญหาที่กล่าวมาทำให้มีความจำเป็นที่จะต้องมีการรักษาความปลอดภัยสำหรับการชำระเงินแบบออนไลน์ ซึ่งสามารถที่จะช่วยตรวจสอบและยืนยันการสั่งซื้อสินค้า ตลอดจนการรักษาความถูกต้องของข้อมูลได้

ปัญหาของผู้ซื้อ	ปัญหาของผู้ขาย
1. ความไม่ไว้วางใจในผู้ขายว่าเป็นบุคคลหรือองค์กรนั้นๆจริงตามที่กล่าวอ้างหรือไม่ 2. การชำระเงิน เมื่อชำระเงินไปแล้วไม่แน่ใจว่าจะได้รับสินค้าหรือบริการจริงหรือไม่ 3. ไม่มีการเซ็นสลิป ทำให้อาจมีผู้อื่นนำหมายเลขบัตรของเราไปใช้ได้ 4. การหลอกลวง ผู้ซื้อไม่แน่ใจว่าสินค้าหรือบริการที่จะได้รับจะมีคุณภาพตรงตามที่ผู้ขายโฆษณาหรือไม่และหากสินค้าไม่ได้มาตรฐานหรือชำรุดระหว่างการขนส่งจะมีหลักประกันอย่างไรในการคืนสินค้า 5. ความเป็นส่วนตัว ผู้ซื้อไม่แน่ใจว่าข้อมูลบัตรเครดิตของตนจะรั่วไหลไปยังบุคคลที่ 3 หรือไม่ 6. ผู้ซื้ออาจไม่ได้รับใบเสร็จ จึงไม่สามารถหักค่าใช้จ่ายได้	1. ความไม่ไว้วางใจในผู้ซื้อว่าเป็นบุคคลหรือองค์กรนั้นๆจริงตามที่กล่าวอ้างหรือไม่ 2. การชำระเงิน แม้จะได้ชำระเงินจากผู้ซื้อ เสียค่าธรรมเนียมบัตรเครดิตและได้ส่งสินค้าหรือให้บริการไปแล้ว ก็ยังไม่อาจแน่ใจได้ว่าจะถูกผู้ซื้อปฏิเสธว่าไม่ได้เป็นผู้ทำรายการ และต้องคืนเงินให้แก่ผู้ซื้อหรือไม่ 3. ไม่มีการเซ็นสลิป ผู้ขายไม่แน่ใจว่าหมายเลขบัตรเครดิตที่ได้รับเป็นของผู้ซื้อจริง 4. การตรวจสอบบัตรเครดิต หากมีปริมาณการซื้อมากๆผู้ขายควรมีระบบการตรวจสอบบัตรเครดิตแบบออนไลน์อัตโนมัติ หรือหากสินค้าที่ขายอยู่ในรูปอิเล็กทรอนิกส์ที่สามารถดาวน์โหลดได้ทันทีก็ยิ่งจำเป็น 5. ค่าบริการบัตรเครดิต บางกรณีผู้ขายอาจต้องเสียค่าธรรมเนียมมากกว่าปกติ

ตารางที่ 2.1 แสดงปัญหาของผู้ซื้อและผู้ขายในการชำระเงินด้วยบัตรเครดิตบนระบบออนไลน์

2.5 เทคโนโลยีที่ช่วยในการรองรับความปลอดภัย

การทำงานในปัจจุบันอาจมีผู้ไม่หวังดีกระทำการอันก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ ซึ่งประกอบด้วย ข้อมูล ซอฟต์แวร์ และฮาร์ดแวร์ ซึ่งสามารถแบ่งได้เป็น 4 ลักษณะ คือ การดักจับข้อมูล การเปลี่ยนแปลงแก้ไขข้อมูล การปลอมแปลงข้อมูล และการขัดจังหวะการทำงานของคอมพิวเตอร์ โดยพื้นฐานของการทำการค้าอิเล็กทรอนิกส์จะประกอบด้วยส่วนสำคัญ ดังนี้คือ

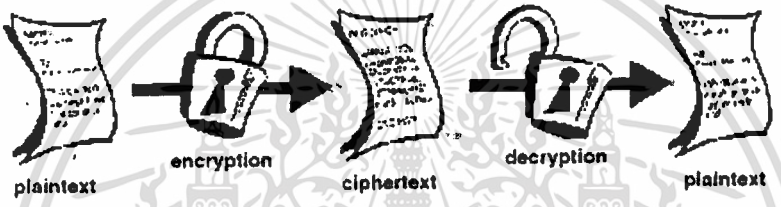
1. Authentication คือการยืนยันถึงผู้ส่งข้อความและเป็นการแจ้งว่าข้อความที่ได้รับมาจากใคร
2. Integrity คือ ความน่าเชื่อถือและความถูกต้องสมบูรณ์ของข้อความ
3. Non-repudiation คือ ผู้ส่งไม่สามารถยกเลิกข้อความที่ถูกส่งออกไปได้

4. Confidentiality คือ ความลับของการทำรายการ ซึ่งมีเฉพาะผู้ส่งหรือผู้รับที่กำหนดเท่านั้นที่จะสามารถอ่านข้อความนั้นได้

วิธีการป้องกันเหตุการณ์ดังกล่าวสามารถทำได้ดังนี้ คือ

2.5.1 การเข้ารหัสและถอดรหัสข้อมูล (Data Encryption and Decryption)

การรักษาความปลอดภัยหรือการป้องกันข้อมูลโดยเบื้องต้นคือการเข้ารหัสข้อมูล (Data Encryption) เพื่อแปลงข้อมูลที่อ่านได้ (Plaintext) ให้อยู่ในรูปรหัส (Ciphertext) ที่ไม่สามารถอ่านได้ดังรูปที่ 1.1 เพื่อเป็นการป้องกันข้อมูลไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถอ่านข้อมูลนั้นได้



รูปที่ 2.1 แสดงการเข้ารหัสและถอดรหัส (Encryption and Decryption)

การเข้ารหัสข้อมูลประกอบด้วยส่วนประกอบที่สำคัญ 2 ส่วนคือ Algorithm และ Key โดยที่ Algorithm จะเป็นฟังก์ชันการคำนวณทางคณิตศาสตร์ที่ทำงานร่วมกับข้อมูลที่เป็นตัวอักษรหรือตัวเลขที่เรียกว่า Key โดยผลลัพธ์ที่ได้จะเป็นข้อมูลที่ถูกเข้ารหัสแล้ว การเข้ารหัสที่ใช้ระบบ Key เป็นพื้นฐานนี้จะมีข้อดีคือ

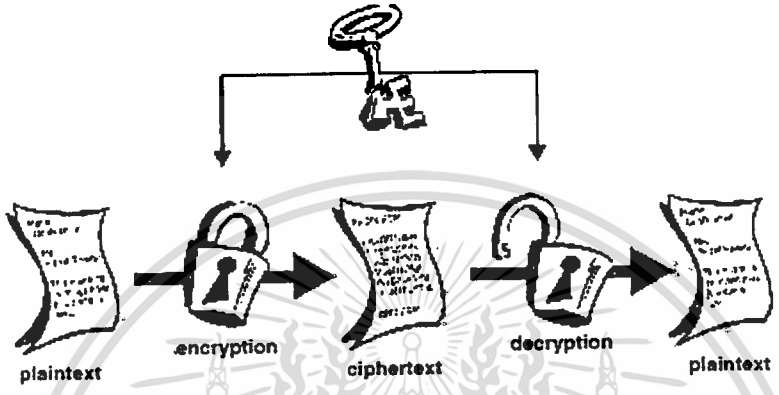
1. Algorithm ที่ใช้ในการเข้ารหัสนั้นยากที่จะคิดขึ้นมาใหม่และไม่จำเป็นต้องทำการสร้าง Algorithm ขึ้นมาใหม่ทุกครั้งที่ต้องการติดต่อสื่อสารกับผู้ที่ต้องการติดต่อด้วยรายใหม่ เราสามารถที่จะใช้ Algorithm ที่เหมือนเดิมได้เพียงแต่ใช้ Key ที่แตกต่างกันออกไปตามกลุ่มบุคคลที่ติดต่อด้วย
2. ถ้ามีคนต้องการที่จะลักลอบทำการถอดรหัสข้อมูลที่เราเข้ารหัสไว้ เราสามารถที่จะหา Key ใหม่มาใช้ในการเข้ารหัสได้โดยที่ยังคงใช้ Algorithm เดิม

การเข้ารหัสข้อมูลด้วย Key นี้สามารถแบ่งออกได้เป็น 2 ประเภทด้วยกันคือ

1. Symmetric Cryptography
2. Asymmetric Cryptography หรือ Public Key Cryptography

2.5.1.1 Symmetric Cryptography

รูปแบบของการเข้ารหัสข้อมูลแบบ Symmetric Key นี้ ทั้งผู้ส่งและผู้รับจะใช้ Key ที่เหมือนกันในการเข้ารหัสและการถอดรหัสข้อมูลดังรูปที่ 2.2



รูปที่ 2.2 แสดงการเข้ารหัสโดยวิธี Symmetric Cryptography

การเข้ารหัสข้อมูลด้วยวิธีนี้จะมีอุปสรรคเกิดขึ้นคือทั้งผู้ส่งและผู้รับจะต้องใช้ Key ร่วมกัน ถ้ามีการส่งข้อความถึงผู้รับจำนวน N คนจะต้องเก็บ Key ไว้เป็นจำนวน N Key ถ้าใช้ Key ที่เหมือนกันสำหรับผู้รับมากกว่า 1 คน จะทำให้บุคคลอื่นๆที่ถือ Key นั้นอยู่สามารถอ่านข้อมูลได้ ทำให้เกิดปัญหากับการทำ Authentication เพราะการระบุถึงผู้ส่งหรือผู้รับไม่สามารถพิสูจน์ได้ และข้อมูลขาด Confidentiality

Algorithm ที่ใช้วิธีการเข้ารหัสแบบ Symmetric Key ได้แก่

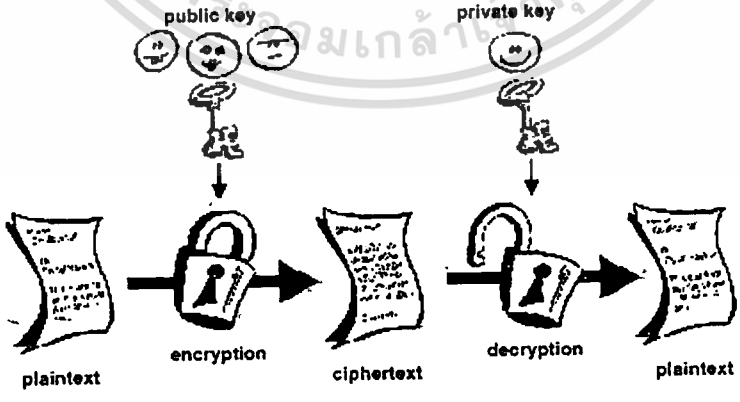
- DES (Data Encryption Standard) เป็นการเข้ารหัสข้อมูลที่ถูกสร้างโดย IBM และได้รับการรองรับจากรัฐบาลของสหรัฐอเมริกาในปี 1977 ความยาวของ Key ที่ใช้ใน DES มีขนาด 56 Bits แต่การเข้ารหัสข้อมูลจะกระทำบนขนาด 64 Bits ข้อดีของ DES คือทำงานได้รวดเร็วและง่ายในการใช้งานเหมาะกับการส่งข้อมูลที่มีขนาดใหญ่ไปในครั้งเดียว
- Triple DES ลักษณะการทำงานจะอยู่บนพื้นฐานการเข้ารหัสด้วย Algorithm DES โดยจะเข้ารหัสข้อมูลเป็นจำนวน 3 ครั้งด้วย Key ที่แตกต่างกัน 2 Keys หลักการทำงานคือจะทำการเข้ารหัสข้อความด้วย Key ที่ 1 หลังจากนั้นจะทำการถอดรหัสด้วย Key ที่ 2 และท้ายสุดจะทำการเข้ารหัสอีกครั้งด้วย Key ที่ 1 ด้วยวิธีการนี้จะให้ได้ Key ที่มีขนาด 168 Bits การเข้ารหัสแบบ Triple DES เป็นอีกทางเลือกหนึ่งของการเข้ารหัสแบบ DES เพราะปัจจุบันการลักลอบถอดรหัสโดยวิธีของ DES สามารถทำได้ง่ายและเร็วขึ้น

- RC2 และ RC4 (Rivert's Code #2 และ #4) เป็น Algorithm เฉพาะที่ถูกสร้างขึ้นโดย RSA Data Security ขนาดของ Key ที่ใช้ในการเข้ารหัสจะไม่คงที่ โดยมีขนาดสูงสุด 2048 Bits RC2 จะมีลักษณะของ Key เป็นแบบกลุ่มของรหัสเหมือน DES และ RC4 จะมีลักษณะของ Key เป็นแบบสายของรหัส Algorithm นี้นิยมใช้ในการเข้ารหัส Web Browser และ Server
- IDEA (International Data Encryption Algorithm) เป็น Algorithm ที่ถูกสร้างขึ้นในปี 1991 มีความปลอดภัยมากกว่า DES เพราะขนาดของ Key ที่ใช้ในการเข้ารหัสคือ 128 Bits IDEA ถูกนำไปใช้กับซอฟต์แวร์ที่เข้ารหัส E-mail เช่น PGP (Pretty Good Privacy)

2.5.1.2 Asymmetric Cryptography หรือ Public Key Cryptography

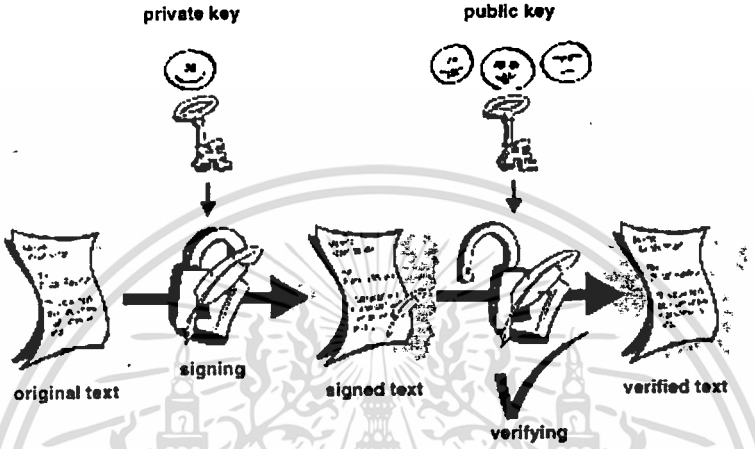
การเข้ารหัสแบบ Public Key Cryptography นี้จะอยู่บนพื้นฐานแนวความคิดของ Key ที่เป็นคู่คือ Private Key และ Public Key โดยที่ Key ทั้งสองนี้จะไม่เหมือนกันและ Key หนึ่งทำหน้าที่เป็น Key ที่ใช้ในการเข้ารหัส ส่วนอีก Key ทำหน้าที่เป็น Key ที่ใช้ในการถอดรหัส และ Private Key จะมีเพียงเจ้าของ Key เท่านั้นที่จะรู้ได้ ส่วน Public Key จะถูกส่งไปให้กับผู้อื่นทราบ ในการเข้ารหัสข้อมูลจะใช้ Private Key หรือ Public Key ในการเข้ารหัสก็ได้เพียงแต่ผู้รับจะต้องใช้ Key ที่เป็นคู่กับ Key ที่ใช้เข้ารหัสมาทำการถอดรหัส การนำ Key เหล่านี้ไปใช้จะทำได้ 2 วิธีคือ

1. ผู้ส่งจะใช้ Public Key ของผู้รับทำการเข้ารหัสข้อมูลและผู้รับจะใช้ Private Key ของผู้รับทำการถอดรหัสข้อมูล เป็นการยืนยันว่าข้อมูลนี้จะเป็นความลับมีเฉพาะผู้รับเท่านั้นที่สามารถอ่านได้ดังรูปที่ 2.3



รูปที่ 2.3 แสดงการเข้ารหัสโดยวิธี Public Key Cryptography โดยใช้ Public Key ในการเข้ารหัส

2. ผู้ส่งจะใช้ Private Key ของผู้ส่งทำการเข้ารหัสและผู้รับใช้ Public Key ของผู้ส่งทำการถอดรหัส เป็นการยืนยันว่าข้อมูลนี้ถูกส่งมาจากผู้ส่งที่ถูกต้องจริงดังรูปที่ 2.4 และวิธีนี้เป็นการทำ Digital Signature ด้วย



รูปที่ 2.4 แสดงการเข้าโดยรหัสวิธี Public Key Cryptography โดยใช้ Private Key ในการเข้ารหัส

Algorithm ที่ใช้วิธีการเข้ารหัสแบบ Public Key Cryptography ได้แก่

- Diffie-Hellman ออกแบบเพื่อใช้ในการติดต่อระหว่างบุคคล 2 ฝ่าย โดยแต่ละฝ่ายจะมี Secret Key เป็นของตนเอง และทำการแลกเปลี่ยนข้อมูล Secret Key ของแต่ละฝ่าย ในการแลกเปลี่ยนข้อมูลนั้นจะทำการสร้าง Session Key ที่ได้มาจาก Secret Key ของทั้งสองฝ่าย และเข้ารหัสข้อมูลด้วย Session Key นั้น ดังนั้นถ้าผู้รับไม่ใช่ผู้ที่ทำการแลกเปลี่ยน Secret Key กันจะไม่สามารถสร้าง Session Key ในการถอดรหัสได้
- RSA (Ronald Rivert, Adi Shamir and Leonard Adelman) เป็น Algorithm ที่ใช้ในการทำ Digital Signature โดยจะทำการเข้ารหัสข้อมูลด้วย Public Key และถอดรหัสข้อมูลด้วย Private Key และขนาดความยาวของ Key ที่ใช้ไม่คงที่จะอยู่ในช่วงตั้งแต่ 512 Bits ถึงมากกว่า 1,024 Bits

2.5.1.3 การเปรียบเทียบวิธีการเข้ารหัส

ระบบการเข้ารหัสด้วยวิธีใดวิธีหนึ่งนั้นไม่สามารถแก้ปัญหาได้ทั้งหมด โดยการเข้ารหัสแต่ละวิธีจะมีข้อดีและข้อเสียดังตารางที่ 2.2

ประเภทของการเข้ารหัส	ข้อดี	ข้อเสีย
Symmetric Cryptography	• รวดเร็ว • ง่ายในการนำไปใช้งาน	• Key ที่ใช้ในการติดต่อต้องเหมือนกันทั้งผู้รับและผู้ส่ง • มีความยุ่งยากในการที่จะส่ง Key ออกไปยังคนอื่นๆ • ไม่สามารถใช้กับการทำ Digital Signature ได้
Public Key Cryptography	• ใช้สอง Key ที่แตกต่างกัน • ง่ายที่จะทำการส่ง Key ออกไปยังคนอื่นๆ • มีความน่าเชื่อถือและมีการรับรองการส่งข้อมูลโดยใช้ Digital Signature	• ช้าและการคำนวณค่อนข้างยาก

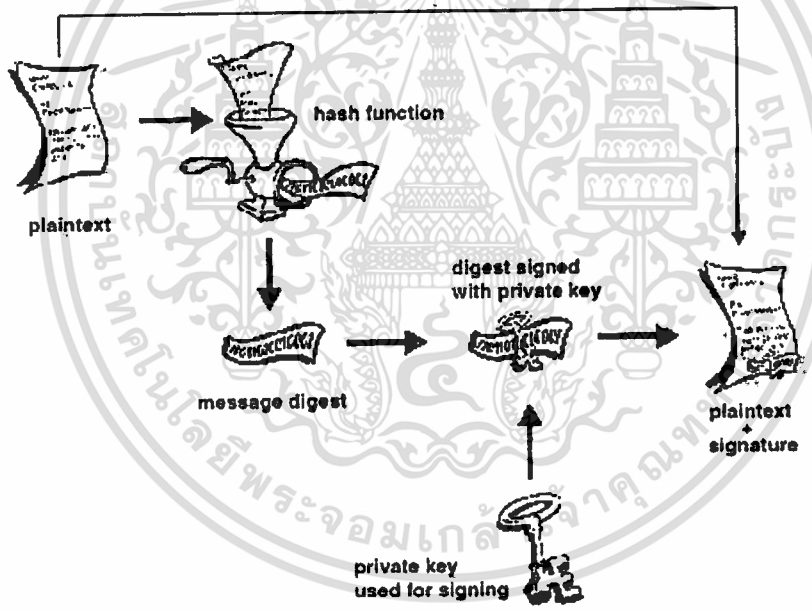
ตารางที่ 2 .2 แสดงข้อดีและข้อเสียของการเข้ารหัสในแต่ละวิธี

ในความเป็นจริงการเข้ารหัสด้วย Public Key Cryptography และ Symmetric Cryptography สามารถที่จะทำร่วมกันได้โดยเข้ารหัสข้อมูลด้วยวิธี Symmetric Cryptography ก่อนแล้วจึงเข้ารหัสด้วย Public Key Cryptography อีกครั้งหนึ่ง ซึ่งการเข้ารหัสด้วย Symmetric Cryptography นี้จะมีประสิทธิภาพมากในกรณีที่ข้อมูลมีขนาดใหญ่ แต่จะมีปัญหาในเรื่องความปลอดภัยในการที่จะส่ง Key ไปยังผู้อื่น และในทางตรงกันข้ามการเข้ารหัสด้วย Public Key Cryptography สามารถที่จะส่ง Key ออกไปยังผู้อื่นได้สะดวกกว่าแต่ไม่มีประสิทธิภาพเพียงพอสำหรับข้อมูลที่มีขนาดใหญ่ ดังนั้นจึงนำกลไกของ Symmetric Cryptography มาใช้ในการเข้ารหัสข้อมูลที่จะส่ง พร้อมทั้งแนบ Key ที่ใช้ในการเข้ารหัสไปด้วย วิธีที่จะป้องกัน Key ที่ส่งออกไปจากผู้อื่นที่ไม่ใช่ผู้รับ สามารถทำได้โดยการนำกลไกของ Public Key Cryptograohy มาใช้ในการเข้ารหัส Key ที่ส่งออกไป นั่นคือจะเข้ารหัส Key ที่ส่งออกไปด้วย Public Key ของผู้รับ เมื่อผู้รับได้รับข้อมูลจะทำการถอดรหัสข้อมูลด้วย

Private Key ของตนเอง จะได้ Key ที่ใช้ในการถอดรหัสข้อมูล นำ Key นี้ไปใช้ในการถอดรหัสข้อมูลทำให้ได้ข้อมูลที่ต้องการออกมา

2.6 Digital Signature

ในการส่งข้อมูลไปยังผู้รับถ้าข้อมูลมีขนาดใหญ่จะไม่สะดวกในการเข้ารหัสและถอดรหัสข้อมูล จึงเกิดความคิดที่จะส่งข้อมูลที่จะทำการเข้ารหัสให้มีขนาดเล็กและสามารถยืนยันถึงผู้ส่งได้ คือการทำ Digital Signature หรือลายเซ็นดิจิตอล ที่เป็นลายเซ็นทางอิเล็กทรอนิกส์ที่ใช้ในการรับประกันว่าข้อความที่ส่งไปนั้นจะไม่ถูกเปลี่ยนแปลงในระหว่างการส่งและสามารถยืนยันถึงผู้ส่งได้ และผู้รับสามารถมั่นใจได้ว่าข้อมูลที่ได้รับมีความถูกต้อง



รูปที่ 2.5 แสดง Digital Signature

การทำ Digital Signature ดังรูปที่ 2.5 เป็นการนำเอาข้อมูลที่ต้องการส่งมาผ่านฟังก์ชันทางคณิตศาสตร์คือ Hash Function ได้เป็น Message Digest ออกมา ขนาดของ Message Digest ที่ได้จะขึ้นอยู่กับฟังก์ชันที่ใช้ เช่น ถ้า Hash Function มีขนาด 60 Bits จะได้ Message Digest ขนาด 60 Bits และทำการเข้ารหัส Message Digest นั้นด้วย Private Key ของผู้ส่งได้เป็นลายเซ็นดิจิตอล นำลายเซ็นดิจิตอลของผู้ส่งนี้แนบไปกับข้อมูลที่ต้องการส่ง เมื่อผู้รับได้รับข้อมูลจะทำการตรวจสอบลายเซ็นดิจิตอลนั้นโดยการถอดรหัสลายเซ็นดิจิตอลนั้นด้วย Public Key ของผู้ส่ง ได้เป็น Message

Digest และนำข้อมูลที่ได้รับไปผ่าน Hash Function ที่เป็นฟังก์ชันเดียวกับที่ผู้ส่งใช้ ได้เป็น Message Digest ออกมา นำ Message Digest ที่ได้จากการคำนวณไปเปรียบเทียบกับ Message Digest ที่ได้รับ ถ้าเหมือนกันแสดงว่าข้อมูลที่ได้รับถูกต้อง

ปัญหาที่เกี่ยวกับการส่งข้อมูลด้วยลายเซ็นดิจิตอล คือข้อมูลจะถูกส่งมาในลักษณะที่สามารถอ่านได้ ไม่มีการป้องกันการเรียกดูข้อมูลจากผู้ที่ไม่ได้รับอนุญาต ดังนั้นจึงควรใช้วิธีการเข้ารหัสข้อมูลควบคู่ไปกับการทำลายเซ็นดิจิตอลด้วย

2.7 Digital Certificate

ใบรับรองดิจิตอล (Digital Certificate) เป็นชุดของข้อมูลที่ใช้รับรองบุคคลหรือองค์กรว่าเป็นผู้ส่งเอกสารนั้นจริง โดยมีผู้ที่ได้รับความไว้วางใจให้เป็นผู้ออกใบรับรองคือ Certificate Authority (CA) ในการสร้างใบรับรองดิจิตอลนั้น ขั้นตอนแรกเครื่องคอมพิวเตอร์ของผู้ขอใบรับรองจะสร้าง Key ขึ้นมา 1 คู่ โดยเก็บ Private Key ไว้กับตัวเอง แล้วส่ง Public Key พร้อมกับข้อมูลส่วนตัวที่ต้องการให้ปรากฏบนใบรับรองให้กับ CA จากนั้น CA จะสร้างใบรับรองดิจิตอลขึ้น โดยในใบรับรองจะเก็บข้อมูลส่วนตัว เช่น ชื่อ ที่อยู่ วันที่ระบุถึง Certificate Authority Public Key ของผู้ขอใบรับรอง ระยะเวลาที่สามารถใช้ใบรับรองนี้ได้ เป็นต้น แล้วทำการเข้ารหัสใบรับรองด้วย Public Key ของผู้ขอใบรับรอง แล้วส่งกลับไปให้ผู้ขอใบรับรอง ในขั้นตอนสุดท้าย ผู้ขอใบรับรองจะต้องใช้เครื่องคอมพิวเตอร์เครื่องเดิมซึ่งมี Private Key เก็บอยู่ในการขอรับใบรับรองทำการถอดรหัสใบรับรองที่ได้จาก CA

จากวิธีการดังกล่าวจะเห็นว่าใบรับรองดิจิตอล คือชุดของข้อมูลที่ Public Key ของบุคคลหรือองค์กร ที่ถูกลงนาม (Signed) โดยผู้รับรอง ใบรับรองดิจิตอลจะถูกใช้ในการแลกเปลี่ยนข้อมูลบนอินเตอร์เน็ตที่ต้องการรับรองตัวผู้ส่งข้อมูลนั้น โดยผู้ส่งมาสามารถทำสำเนาใบรับรองดิจิตอลของตนเองแนบไปกับข้อมูลได้ หากปราศจากใบรับรองดิจิตอลจะไม่สามารถทราบได้เลยว่า Public Key นั้นเป็นของบุคคลหรือองค์กรที่อ้างความเป็นเจ้าของจริงหรือไม่ จึงเห็นได้ว่าใบรับรองดิจิตอลมีประโยชน์อยู่ 2 ประการ คือ ช่วยให้ผู้รับข้อมูลมั่นใจได้ว่าข้อมูลนั้นมาจากผู้ส่งจริง และผู้ส่งไม่สามารถบอกปัดความรับผิดชอบต่อการเป็นผู้ส่งข้อมูลนั้นได้

2.8 Transaction Security protocol

2.8.1 Secure Socket Layer (SSL)

พัฒนาโดย Netscape ออกแบบมาเพื่อรักษาความปลอดภัยบนระบบเครือข่าย TCP/IP สามารถใช้ได้กับโปรแกรมประยุกต์ที่ทำงานบนโพรโตคอล TCP/IP และ Web Browser ที่

สนับสนุน SSL โดยมีเครื่องหมายที่แสดงว่า Web Page นั้นได้รับการรักษาความปลอดภัย เช่น กรณีของ Netscape Navigator จะแสดงด้วยรูปกุญแจที่มุมล่างด้านซ้าย SSL ถูกนำไปใช้อย่างแพร่หลายทั้งบน Intranet, Internet Server และ Browser

การเข้ารหัสสำหรับ SSL จะใช้วิธีการเข้ารหัสทั้งแบบ Public Key Cryptography และ Symmetric Cryptography โดย Public Key Cryptography จะใช้ในการทำ Authentication ระหว่าง Server กับ Client และ Symmetric Cryptography จะใช้ในการเข้ารหัสข้อความและ Session ที่ใช้ในการติดต่อกันระหว่าง Server กับ Client

ขั้นตอนการทำงานของ SSL คือเมื่อ Client เข้ามายัง Web Page ที่ได้รับการรักษาความปลอดภัยเอาไว้ด้วย SSL Client จะขอติดต่อกับ Server โดยส่งข้อความไปยัง Server เมื่อ Server ได้รับข้อความจาก Client จะตอบกลับข้อความนั้นไปยัง Client ถ้า Client รองรับ SSL จะตอบรับกลับมายัง Server และถือเป็นการเริ่มติดต่อแบบ SSL (SSL Handshake) โดย Server และ Client จะแลกเปลี่ยนข้อมูลการรักษาความปลอดภัยซึ่งกันและกัน ในข้อมูลที่ Client ส่งกลับมายัง Server จะระบุหมายเลขของการติดต่อครั้งนี้ Algorithm ของการเข้ารหัส และวิธีการบีบอัดข้อมูล จากนั้น Server จะติดต่อกลับไปยัง Client และทำการส่งสำเนาใบรับรองดิจิตอลให้กันและกันเพื่อตรวจสอบ โดย Server จะส่ง Public Key เฉพาะสำหรับการติดต่อครั้งนั้น (Session Key) ไปยัง Client ด้วย Client จะใช้ Key ที่ได้รับทำการเข้ารหัสข้อมูลก่อนส่งไปยัง Server และ Server จะสามารถถอดรหัสข้อมูลนั้นได้ด้วย Private Key ที่คู่กัน ทำให้ Server และ Client สามารถติดต่อกันได้อย่างปลอดภัย ทั้งนี้ในการติดต่อกับแต่ละ Client จะใช้ Key ที่ต่างกัน และ Key ที่สร้างขึ้นเฉพาะนั้นจะหมดอายุหลังจาก 24 ชั่วโมงโดยอัตโนมัติ โดยสรุป SSL ได้จัดเตรียมบริการด้านความปลอดภัยพื้นฐานเอาไว้ให้ 3 อย่างดังตารางที่ 2.3 ที่แสดงถึงบริการด้านความปลอดภัยพื้นฐานของระบบ SSL

ความเป็นส่วนตัวของข้อความ เกิดจากการใช้การเข้ารหัสทั้งแบบ Public Key Cryptograpy ร่วมกับแบบ Symmetric Cryptography เพื่อให้สามารถทำการเข้ารหัสและถอดรหัสได้อย่างรวดเร็ว และในขณะเดียวกันก็ยังคงไว้ซึ่งความปลอดภัยในระดับสูงโดยที่ข้อมูลทุกอย่างที่ส่งไปมาระหว่าง Server และ Client จะถูกเข้ารหัสโดยใช้ Key และ Algorithm การเข้ารหัสที่ตกลงกันตอนทำ SSL Handshake ทำให้แม้ผู้ลักลอบอ่านข้อความจะใช้อุปกรณ์ตรวจจับกลุ่มข้อมูลไอพี (IP Packet Sniffer) มาอ่านข้อความก็จะมองเห็นแต่ข้อความที่ถูกเข้ารหัสเอาไว้

ความถูกต้องของข้อความ บริการนี้ช่วยให้สามารถมั่นใจได้ว่าข้อมูลจะไม่ถูกแก้ไขในระหว่างทางที่ส่งไปมาระหว่าง Server และ Client โดยอาศัย Hash Function ประกอบกัน

บริการ	เทคโนโลยีที่ใช้	สิ่งที่ป้องกันได้
ความเป็นส่วนตัวของข้อความ	การเข้ารหัส	ผู้ลักลอบอ่านข้อความ
ความถูกต้องของข้อความ	รหัสตรวจสอบข้อความ(ใช้ hash function และการเข้ารหัส)	ผู้ลักลอบแก้ไขข้อความ
การตรวจสอบซึ่งกันและกัน	ใบรับรองดิจิตอลตามมาตรฐาน X.509	ผู้แอบอ้างเป็นบุคคลอื่น

ตารางที่ 2.3 แสดงบริการด้านความปลอดภัยพื้นฐานของ SSL

การตรวจสอบซึ่งกันและกัน Client สามารถตรวจสอบใบรับรองดิจิตอลของ Server ได้ และบน SSL หากผู้ใช้ทางด้าน Client มีใบรับรองดิจิตอล Server ก็สามารถจะขอตรวจสอบผู้ใช้ได้ด้วยเช่นกัน ในการแลกเปลี่ยนใบรับรองดิจิตอลจะเกิดขึ้นในขั้นตอน SSL Handshake เพื่อให้มั่นใจว่าฝ่ายที่แสดงใบรับรองดิจิตอลเป็นเจ้าของใบรับรองนั้นจริง และต้องมีลายเซ็นดิจิตอล (Digital Signature) กำกับข้อมูลทุกอย่างที่ส่งให้อีกฝ่ายหนึ่ง ในขั้นตอน SSL Handshake ข้อมูลที่ถูกเซ็นกำกับจะต้องมีใบรับรองด้วย เพื่อป้องกันไม่ให้ผู้อื่นปลอมแปลงเพราะจะมีเพียงผู้ที่มี Private Key ที่คู่กับ Public Key บนใบรับรองเท่านั้นที่สามารถเซ็นกำกับข้อมูลได้อย่างถูกต้อง

2.8.2 Secure Electronic Transaction (SET)

คิดค้นโดย VISA และ Master Card และพัฒนาร่วมกับ MicroSoft, CyberCash, GTE, IBM และ Netscape SET มีความแตกต่างจาก SSL อย่างมาก มีการรักษาความปลอดภัยสูงกว่า SSL โดยมีการตรวจสอบ 3 ฝ่ายหลักๆ คือ ลูกค้า ผู้ขาย และธนาคาร (ธนาคารเป็นตัวกลางในการทำรายการชำระเงิน) ผู้ขายจะไม่ทราบหมายเลขบัตรเครดิตของผู้ซื้อ เนื่องจากข้อมูลเกี่ยวกับบัตรเครดิตจะถูกส่งไปยังธนาคารของผู้ขายโดยตรวจสอบความถูกต้องข้อมูลบัตรเครดิต และวงเงินกับธนาคารเจ้าของบัตร เมื่อได้รับการอนุมัติวงเงิน ธนาคารผู้ขายก็จะนำเงินเข้าสู่บัญชีผู้ขาย

การค้าอิเล็กทรอนิกส์โดยใช้ SET จะเริ่มจากผู้ถือบัตรเครดิตของธนาคารที่สนับสนุนระบบ SET ทำการดาวน์โหลดกระเป๋าสตางค์อิเล็กทรอนิกส์ (E-wallet) มาติดตั้งลงบนคอมพิวเตอร์ และขอใบรับรองดิจิตอลตามมาตรฐาน SET จาก CA ที่สนับสนุน SET ซึ่งได้แก่ธนาคารที่ออกบัตรเครดิตนั้นๆ มาติดตั้งไว้บน Web Browser หลังจากนั้นจะกรอกแบบฟอร์มลงทะเบียนบัตรเครดิตเพื่อเข้าสู่ระบบ SET บน Web Site ของธนาคาร การที่จะมั่นใจได้ว่า Web Site นั้นเป็นของธนาคารผู้ออกบัตรเครดิตให้จริงหรือไม่กระทำโดยการตรวจสอบใบรับรองของ Web Site ธนาคารที่ส่งมายัง Web Browser โดยผ่าน SSL เมื่อระบบของทางธนาคารตรวจสอบข้อมูลกับฐานข้อมูลแล้ว

ตรงกัน ก็จะสามารถ Download ใบรับรองมาติดตั้งบนกระเป๋าสตางค์อิเล็กทรอนิกส์ พร้อมที่จะชำระเงินด้วยบัตรเครดิตบนอินเตอร์เน็ต

ผู้ซื้อซึ่งถือใบรับรองของธนาคารและเข้าไปเลือกซื้อสินค้าหรือบริการบนเว็บไซท์ที่สนับสนุน SET หลังจากเลือกสินค้าหรือบริการใส่ลงในรถเข็นหรือตะกร้าอิเล็กทรอนิกส์ แล้วจึงคลิกปุ่มสั่งซื้อทาง Server ของผู้ขายจะส่งใบสั่งซื้อที่ระบุรายการสินค้าหรือบริการพร้อมจำนวนและราคามาแสดงบนหน้าจอผู้ซื้อ ให้ผู้ซื้อกรอกที่อยู่สำหรับส่งสินค้าลงไป แล้วเลือกวิธีการชำระเงิน หากเลือกชำระเงินผ่านระบบ SET โปรแกรมกระเป๋าสตางค์อิเล็กทรอนิกส์จะถูกเรียกขึ้นมาโดยอัตโนมัติ ผู้ซื้อป้อนรหัสผ่านแล้วจึงเลือกบัตรเครดิตที่จะใช้ชำระเงิน จากนั้นเซ็นกำกับใบสั่งซื้อและข้อมูลการชำระเงินด้วยใบรับรองดิจิตอลตามมาตรฐาน SET ของผู้ซื้อส่งกลับคืนไปยังผู้ขาย ผู้ขายจะตรวจสอบลายเซ็นดิจิตอลของผู้ซื้อบนใบสั่งซื้อ และส่งต่อข้อมูลการชำระเงินไปยังธนาคารของผู้ขาย เพื่อขออนุมัติการชำระเงิน ธนาคารของผู้ขายจะตรวจสอบกับธนาคารผู้ออกบัตรฯ ว่าข้อมูลบัตรเครดิตถูกต้องและมีวงเงินพอจ่ายหรือไม่ และส่งผลการตรวจสอบไปยังธนาคารของผู้ขาย จากนั้นธนาคารของผู้ขายจะแจ้งผลไปยังผู้ขายอีกทอดหนึ่ง ซึ่งหากข้อมูลถูกต้องและมีวงเงินพอจ่าย ธนาคารผู้ออกบัตรจะบันทึกรายการชำระเงินของผู้ซื้อเพื่อเรียกเก็บเงินต่อไป ส่วนธนาคารของผู้ขายจะโอนเงินเข้าสู่บัญชีของผู้ขาย และในขั้นตอนสุดท้ายผู้ขายจะส่งใบเสร็จให้ผู้ซื้อเก็บไว้ในกระเป๋าสตางค์อิเล็กทรอนิกส์ต่อไป ในทุกขั้นตอนจะมีการเข้ารหัสข้อมูลระหว่างการส่งทั้งหมด รายละเอียดเกี่ยวกับการทำงานของ SET จะกล่าวถึงโดยละเอียดในบทต่อไป

หัวข้อที่ทำการเปรียบเทียบ	ลักษณะที่แตกต่างของแต่ละโพรโตคอล	
	SSL	SET
จำนวนฝ่ายที่เกี่ยวข้อง	2 ฝ่าย (Server กับ Browser)	3 ฝ่าย (ผู้ซื้อ ผู้ขาย และธนาคาร)
ใบรับรองดิจิตอล	มีเฉพาะฝั่ง Server	ทุกฝ่ายที่เกี่ยวข้องต้องมี
การตรวจสอบ	Server กับ Browser ต่างตรวจสอบซึ่งกันและกัน	ต้องมี CA ตรวจสอบทุกฝ่ายที่เกี่ยวข้อง
การป้อนข้อมูลบัตรเครดิต	ผู้ซื้อต้องป้อนทุกครั้ง	ข้อมูลบัตรถูกเก็บไว้ใน E-Wallet จึงป้อนเก็บไว้เพียงครั้งเดียว
การจำกัดการเข้าถึง	สามารถควบคุมการเข้าถึง Server Directory, File และบริการต่างๆ	-ธนาคารผู้ออกบัตรฯไม่ทราบรายละเอียดการซื้อ รักษาความเป็นส่วนตัวของลูกค้า -ผู้ขายไม่ทราบข้อมูลบัตรเครดิตลูกค้า รักษาความปลอดภัย
การใช้ข้อมูลร่วมกัน	Browser สามารถใช้ข้อมูลร่วมกับ Server และป้องกันบุคคลที่ 3 ไม่ให้เข้าถึงข้อมูลได้	คำสั่งซื้อที่เข้ารหัสแล้วถูกส่งให้ผู้ขาย ส่วนข้อมูลบัตรเครดิตที่เข้ารหัสแล้วถูกส่งให้ธนาคารผู้ออกบัตรเครดิต
การป้องกันข้อมูล	เซอร์ฟเวอร์สร้างกุญแจขึ้นสำหรับการสั่งซื้อครั้งนั้นโดยเฉพาะแล้วส่งให้กับ Browser เพื่อเข้ารหัสคำสั่งซื้อส่งกลับมา	ข้อมูลถูกเข้ารหัสด้วยกุญแจส่วนตัวของผู้ซื้อ
การพิสูจน์ตัวตนของลูกค้าและยอดเครดิตแบบทันที	ไม่สนับสนุน แต่สามารถทำได้โดยเขียนซอฟต์แวร์จัดการเอง	สนับสนุน
การเข้ารหัสข้อมูลบัตรเครดิต	เข้ารหัสรายละเอียดคำสั่งซื้อกับข้อมูลบัตรรวมกัน จึงมีความแข็งแรงน้อยกว่า	เข้ารหัสคำสั่งซื้อกับข้อมูลบัตรแยกจากกัน และเนื่องจากข้อมูลบัตรมีขนาดตายตัว จึงสามารถเข้ารหัสได้แข็งแรงกว่า

ตารางที่ 2.4 แสดงข้อมูลการเปรียบเทียบระหว่าง SSL และ SET

2.8.3 Point-to-Point Tunneling Protocal (PPTP)

เป็นเทคนิคการรักษาความปลอดภัยแบบหนึ่งโดยใช้ VPN Technology (Virtual Private Network Technology) ซึ่งจะช่วยในการสร้าง Secure Web มีค่าใช้จ่ายต่ำเมื่อเทียบกับวิธี SSL และ SET การ Implement สามารถทำได้ด้วยตัวเองไม่ยุ่งยากเหมือน 2 วิธีแรก เหมาะกับการทำงานในระดับ Local เช่น LAN หรือ Intranet สนับสนุนการทำงานบน Windows NT Workstation และ Windows95

บทที่ 3

หลักการทำงานของระบบ SET

3.1 วัตถุประสงค์

วัตถุประสงค์ในการทำงานของ SET จะแบ่งออกเป็นวัตถุประสงค์ในด้านต่างๆ ดังนี้

3.1.1 วัตถุประสงค์เพื่อความปลอดภัยในการชำระค่าสินค้า คือ

- เพื่อเป็นการรับรองเจ้าของบัตรเครดิต ร้านค้า และธนาคาร
- เพื่อให้ข้อมูลการชำระค่าสินค้าเป็นความลับ
- เพื่อป้องกันข้อมูลการชำระค่าสินค้าให้มีความถูกต้องสมบูรณ์
- เพื่อกำหนด Algorithm และโพรโตคอลที่จำเป็นสำหรับบริการที่มีความปลอดภัย

3.1.2 วัตถุประสงค์เพื่อความสามารถในการทำงานข้ามเครื่อง คือ

- เพื่อกำหนดรายละเอียดของข้อมูลให้ชัดเจนเพื่อความมั่นใจว่า Application ที่พัฒนาโดยผู้ขายหลายรายสามารถติดต่อกันได้
- เพื่อสร้างและสนับสนุนมาตรฐานของการชำระค่าสินค้าด้วยบัตรเครดิต
- เพื่อกำหนดเทคโนโลยีให้มีความสามารถในการทำงานข้ามเครื่องได้ รวมทั้งสนับสนุนซอฟต์แวร์ที่สามารถทำงานข้ามเครื่องได้ให้เป็นที่แพร่หลาย
- สร้างอยู่บนมาตรฐานการปฏิบัติงานที่มีอยู่
- เพื่อความมั่นใจว่าสามารถเข้าได้กับมาตรฐานที่เหมาะสม

3.2 ผู้เกี่ยวข้องในระบบ SET

วิธีการติดต่อเพื่อชำระค่าสินค้าในระบบ SET จะต่างจากระบบอื่นๆ คือ ในระบบอื่นๆ ขบวนการทางอิเล็กทรอนิกส์จะเริ่มต้นที่ผู้ขาย แต่ในระบบ SET จะเริ่มที่ผู้ถือบัตรเครดิต และผู้ที่เกี่ยวข้องกับระบบ SET ทั้งหมดประกอบด้วย

1. Cardholder คือ เจ้าของบัตรเครดิตหรือผู้ซื้อสินค้า ในสภาพแวดล้อมของการทำการค้าเชิงพาณิชย์อิเล็กทรอนิกส์ ผู้บริโภคที่เป็นรายย่อยหรือที่เป็นบริษัทจะทำการสั่งซื้อสินค้ากับร้านค้าโดยผ่านทางเครื่องคอมพิวเตอร์ส่วนบุคคล ผู้ซื้อสินค้าจะใช้บัตรเครดิตที่ออกให้โดยสถาบันการเงินหรือหน่วยงานที่ออกบัตรเครดิตทำการชำระค่าสินค้า ระบบ SET ทำให้เกิดความมั่นใจว่าการติดต่อระหว่างผู้ซื้อกับร้านค้านั้น ข้อมูลที่เกี่ยวกับบัตรเครดิตหรือข้อมูลที่เป็นข้อมูลส่วน

บุคคลจะเป็นความลับ

2. Issuer คือ สถาบันการเงินที่สร้างบัญชีให้กับเจ้าของบัตรเครดิตและเป็นผู้ออกบัตรเครดิตที่ใช้ในการชำระค่าสินค้าให้กับเจ้าของบัตรหรือ Cardholder
3. Merchant คือ ร้านค้าที่ทำการเสนอขายสินค้าและบริการ ด้วยระบบ SET ผู้ขายสามารถนำเสนอความปลอดภัยในการทำรายการแบบอิเล็กทรอนิกส์กับเจ้าของบัตรได้ ร้านค้าที่ยอมรับบัตรเครดิตนั้นจะต้องมีความเกี่ยวข้องหน่วยงานที่เป็นผู้อนุมัติการทำรายการด้วย
4. Acquirer คือ สถาบันการเงินที่สร้างบัญชีให้กับร้านค้า และเป็นผู้อนุมัติการทำรายการด้วยบัตรเครดิตในการชำระค่าสินค้า
5. Payment Gateway เป็นอุปกรณ์ที่ใช้ในการทำงานของ Acquirer เพื่อใช้ในการประมวลผลข้อความในการชำระค่าสินค้าที่ส่งมาจากร้านค้า รวมทั้งคำสั่งในการชำระค่าสินค้าจากเจ้าของบัตรเครดิต

3.3 ลายเซ็นดิจิตอลแบบคู่

การทำลายเซ็นดิจิตอลในระบบ SET นอกจากจะเป็นลายเซ็นดิจิตอลแบบธรรมดาแล้วนั้น ยังมีการทำลายเซ็นดิจิตอลแบบคู่ด้วย และวิธีการสร้างลายเซ็นดิจิตอลแบบคู่นั้นทำได้โดย นำข้อความที่ต้องการส่ง 2 ข้อความมาสร้าง Message Digest ได้เป็น Message Digest1 จากข้อความที่ 1 และ Message Digests2 จากข้อความที่ 2 และรวม Message Digest ทั้งสองนั้นเข้าด้วยกัน และทำการคำนวณ Message Digest ใหม่พร้อมทั้งเข้ารหัส Message Digest ใหม่นี้ด้วย Private Signature Key ของผู้ส่งได้เป็นลายเซ็นดิจิตอลคู่ เมื่อส่งข้อมูลไปยังผู้รับจะส่งข้อความที่ต้องการส่ง (ข้อความที่ 1) ลายเซ็นดิจิตอลคู่พร้อมทั้ง Message Digest ของอีกข้อความหนึ่ง (Message Digest2) แนบไปด้วย เมื่อผู้รับได้รับข้อความนั้นจะทำการตรวจสอบลายเซ็นดิจิตอล โดยถอดรหัสลายเซ็นดิจิตอลด้วย Public Signature Key ของผู้ส่งได้ Message Digest คู่ออกมา และคำนวณ Message Digest1 จากข้อความที่ได้รับ นำ Message Digest1 ที่คำนวณได้มารวมกับ Message Digest2 ที่แนบมา และทำการคำนวณ Message Digest คู่ นำ Message Digest ทั้งสองมาเปรียบเทียบกัน ถ้าเหมือนกันแสดงว่าลายเซ็นดิจิตอลนั้นถูกต้อง

ตัวอย่างการใช้งานลายเซ็นดิจิตอลคู่คือ ผู้ซื้อจะส่งคำสั่งซื้อสินค้าสำหรับร้านค้าและคำสั่งการโอนเงินให้กับร้านค้าสำหรับธนาคารไปยังร้านค้า แต่ผู้ซื้อไม่ต้องการให้ธนาคารเห็นข้อมูลเกี่ยวกับการสั่งซื้อและร้านค้าเห็นข้อมูลบัญชีของผู้ซื้อ ผู้ซื้อจะทำลายเซ็นดิจิตอลคู่ลงบนข้อความทั้งสอง เมื่อร้านค้ายอมรับคำสั่งซื้อนั้นจะส่งข้อความการยอมรับและ Message Digest ของคำสั่งซื้อสินค้าไปยังธนาคาร ธนาคารจะตรวจสอบการอนุญาตโอนเงินของผู้ซื้อเพื่อให้มั่นใจว่าการยอมรับนั้นมา

จากคำสั่งซื้อเดียวกัน ธนาคารจะใช้ Message Digest ของคำสั่งโอนเงินและ Message Digest ของคำสั่งซื้อสินค้าของร้านค้ามาตรวจสอบลายเซ็นดิจิตอลคู่ และธนาคารไม่สามารถที่จะเห็นข้อมูลการสั่งซื้อได้

ในระบบ SET การทำลายเซ็นดิจิตอลคู่จะกระทำเมื่อต้องการส่งข้อมูลการสั่งซื้อสินค้าไปยังร้านค้าและคำสั่งการชำระค่าสินค้าที่มีข้อมูลเกี่ยวกับบัญชีอยู่ด้วยไปยัง Acquirer เมื่อร้านค้าส่งคำร้องขออนุญาตไปยัง Acquirer จะรวมคำสั่งการชำระค่าสินค้าจากผู้ซื้อสินค้าและ Message Digest ของข้อมูลการสั่งซื้อสินค้า และ Acquirer จะคำนวณ Message Digest จากคำสั่งการชำระค่าสินค้าและ Message Digest ที่ได้จากร้านค้ามาทำการตรวจสอบลายเซ็นดิจิตอลคู่

การทำลายเซ็นดิจิตอลคู่ในระบบ SET เป็นการทำรายการระหว่างบุคคล 3 ฝ่าย โดยมีวัตถุประสงค์เพื่อไม่ให้บุคคลที่ 3 สามารถเห็นข้อมูลที่เป็นส่วนตัวในการติดต่อระหว่างบุคคลที่ 1 และบุคคลที่ 2 และเป็นการยืนยันว่าข้อมูลมาจากบุคคลนั้นจริง

3.4 การเข้ารหัสในระบบ SET

การเข้ารหัสในระบบ SET ใช้วิธีการเข้ารหัสทั้งแบบ Symmetric Cryptography และ Public Key Cryptography โดยจะทำการเข้ารหัสข้อความด้วย Secret Key ที่ได้จากการสุ่ม และเข้ารหัส Secret Key นี้ด้วย Public Key ของผู้รับ ซึ่งเป็นขั้นตอนการทำ Digital Envelope ข้อความที่ถูกเข้ารหัสและ Digital Envelope นี้จะถูกส่งไปยังผู้รับ เมื่อผู้รับได้รับข้อความจะทำการถอดรหัส Digital Envelope ด้วย Private Key ของผู้รับ เพื่อให้ได้ Key ที่นำไปใช้ในการถอดรหัสข้อความต่อไป

ในระบบ SET จะสร้าง Key ของ Public Key Cryptography ทั้งหมด 2 ชุดด้วยกัน คือ

1. Exchange Key เป็น Key ที่ใช้ในการเข้ารหัสและถอดรหัส Key ที่ใช้ในการเข้ารหัส
2. Signature Key เป็น Key ที่ใช้ในการสร้างและตรวจสอบลายเซ็นดิจิตอล

3.5 ขั้นตอนและวิธีการชำระค่าสินค้าในระบบ SET

ขั้นตอนในการทำงานของระบบ SET สามารถแบ่งได้เป็น 5 ขั้นตอน คือ

1. การลงทะเบียนของเจ้าของบัตรเครดิต
2. การลงทะเบียนของร้านค้า
3. การสั่งซื้อสินค้า
4. การขออนุญาตชำระค่าสินค้า
5. การชำระค่าสินค้า

3.5.1 การลงทะเบียนของเจ้าของบัตรเครดิต

การลงทะเบียนของเจ้าของบัตรเครดิตกับ Certificate Authority (CA) ประกอบด้วยขั้นตอน คือ เจ้าของบัตรเครดิตหรือผู้ซื้อสินค้าต้องลงทะเบียนกับ CA ก่อนที่จะส่งข้อความในรูปแบบของ SET ไปยังร้านค้า การที่จะส่งข้อความในรูปแบบของ SET ไปยัง CA ผู้ถือบัตรจะต้องมี Public Exchange Key ของ CA เพื่อใช้เป็น Key ในการแลกเปลี่ยนข้อมูลกัน โดย Key นี้จะได้มาจากใบรับรองดิจิตอลของ CA เจ้าของบัตรหรือผู้ซื้อจะต้องมีแบบฟอร์มการลงทะเบียนจากสถาบันการเงินที่ออกบัตรเครดิตเพื่อให้ CA ออกแบบฟอร์มในการลงทะเบียนให้ เจ้าของบัตรเครดิตจะต้องแจ้งกับ CA ว่าหน่วยงานที่ออกบัตรเครดิตให้นั้นเป็นใคร จึงจะสามารถเริ่มขั้นตอนการลงได้ และขั้นตอนในการลงทะเบียนของเจ้าของบัตรเครดิตจะประกอบด้วยขั้นตอนทั้งหมด 7 ขั้นตอนดังนี้

1. เจ้าของบัตรเครดิตเริ่มต้นการลงทะเบียน

   เจ้าของบัตรเครดิตจะส่งคำร้องขอเริ่มต้นการติดต่อไปยัง CA

2. Certificate Authority ตอบกลับการเริ่มต้นการลงทะเบียน

เมื่อ CA ได้รับคำร้องขอเริ่มต้นการติดต่อ CA จะสร้างข้อความที่จะตอบกลับคำร้องขอนั้น พร้อมทั้งสร้างลายเซ็นดิจิตอลด้วย Private Signature Key ของ CA แนบไปกับข้อความนั้น และส่งข้อความตอบกลับพร้อมทั้งใบรับรองดิจิตอลที่มี Public Exchange Key และ Public Signature Key ของ CA กลับไปยังเจ้าของบัตรเครดิต

3. เจ้าของบัตรเครดิตร้องขอแบบฟอร์มการลงทะเบียน

เมื่อเจ้าของบัตรเครดิตได้รับข้อความตอบกลับมาจาก CA จะทำการตรวจสอบใบรับรองดิจิตอล ถ้าใบรับรองถูกต้องโปรแกรมที่เครื่องเจ้าของบัตรเครดิตจะเก็บใบรับรองนั้นไว้เพื่อใช้ในขั้นตอนการลงทะเบียนต่อไป และตรวจสอบลายเซ็นดิจิตอลของ CA โดยใช้ Public Signature Key ของ CA ในการถอดรหัส เมื่อการตรวจสอบสำเร็จ เจ้าของบัตรจะส่งคำร้องขอลงทะเบียนไปยัง CA โดยเข้ารหัสคำร้องขอนั้นด้วย Secret Key ที่ได้จากการสุ่ม และทำการเข้ารหัส Secret Key และเลขที่บัญชีของเจ้าของบัตรเครดิตด้วย Public Exchange Key ของ CA ซึ่งเป็นการทำ Digital Envelope และส่งคำร้องขอนี้กลับไปยัง CA

ข้อมูลทั้งหมดที่ส่งกลับไปยัง CA ประกอบด้วย

- คำร้องขอแบบฟอร์มการลงทะเบียนที่ถูกเข้ารหัสไว้
- Digital Envelope ที่ประกอบด้วย Secret Key ที่ใช้ในการเข้ารหัสคำร้องขอแบบฟอร์มการลงทะเบียนและเลขที่บัญชีของเจ้าของบัตรเครดิต

4. Certificate Authority ประมวลผลคำร้องขอและส่งแบบฟอร์มการลงทะเบียน

เมื่อ CA ได้รับคำร้องขอแบบฟอร์มการลงทะเบียนจะทำการถอดรหัส Digital Envelope

ด้วย Private Exchange Key ของ CA เอง และนำ Secret Key ที่ได้ไปถอดรหัสคำร้องขอนั้น และ CA จะทำการส่งแบบฟอร์มการลงทะเบียนพร้อมลายเซ็นดิจิตอลที่ถูกเข้ารหัสด้วย Private Signature Key ของ CA และใบรับรองดิจิตอลของ CA ที่มี Public Signature Key ของ CA อยู่ด้วย กลับไปยังผู้ร้องขอ

5. ผู้ถือบัตรได้รับแบบฟอร์มการลงทะเบียนและร้องขอใบรับรองจาก CA

เมื่อเจ้าของบัตรเครดิตได้รับแบบฟอร์มการลงทะเบียนตอบกลับมาจาก CA จะทำการตรวจสอบใบรับรองและลายเซ็นดิจิตอลของ CA โดยใช้ Public Signature Key ของ CA ในการถอดรหัสลายเซ็น ถ้าข้อมูลถูกต้องเจ้าของบัตรจะทำการสร้าง Key สำหรับตัวเอง 1 คู่คือ Public Signature Key และ Private Signature Key และทำการกรอกข้อมูลส่วนตัวลงในแบบฟอร์มการลงทะเบียน พร้อมทั้งแนบ Public Signature Key ของเจ้าของบัตรและ Secret Key (Key1) ที่ได้จากการสุ่มเพื่อใช้ในการเข้ารหัสข้อความที่ CA จะตอบกลับมายังเจ้าของบัตร (เจ้าของบัตรเครดิตจะต้องเก็บ Secret Key (Key1) นี้ไว้ใช้ถอดรหัสข้อมูลที่ตอบกลับมาจาก CA ด้วย) และทำการเข้ารหัสข้อมูลการลงทะเบียนทั้งหมดนี้ด้วย Secret Key (Key2) ที่ได้จากการสุ่ม พร้อมทั้งทำ Digital Envelope กับ Secret Key (Key2) และเลขที่บัญชีของเจ้าของบัตรด้วย Public Exchange Key ของ CA

ข้อมูลทั้งหมดที่ส่งไปยัง CA ประกอบด้วย

- Digital Envelope ที่ประกอบด้วย Secret Key (Key2) ที่ใช้ในการเข้ารหัสข้อมูลการลงทะเบียนและเลขที่บัญชีของเจ้าของบัตร
- ข้อมูลการลงทะเบียน Public Signature Key ของเจ้าของบัตร และ Secret Key (Key1) พร้อมทั้งลายเซ็นดิจิตอลของเจ้าของบัตรเครดิต และเข้ารหัสข้อมูลทั้งหมดด้วย Secret Key (Key2)

6. Certificate Authority ประมวลผลการลงทะเบียนและออกใบรับรองดิจิตอลให้กับเจ้าของบัตรเครดิต

เมื่อ CA ได้รับข้อมูลการลงทะเบียนจะทำการถอดรหัส Digital Envelope ด้วย Private Exchange Key ของ CA และนำ Secret Key (Key2) ที่ได้นี้ไปถอดรหัสข้อมูลการลงทะเบียนที่ได้รับพร้อมทั้งตรวจสอบลายเซ็นดิจิตอลของเจ้าของบัตรเครดิตด้วย Public Signature Key ที่ได้รับ และทำการตรวจสอบข้อมูลการลงทะเบียนโดยใช้ข้อมูลจากเลขที่บัญชีของเจ้าของบัตรเป็นข้อมูลอ้างอิงในการตรวจสอบข้อมูลกับ Issuer ถ้าข้อมูลถูกต้อง CA จะทำการสร้างใบรับรองดิจิตอลสำหรับเจ้าของบัตรที่มีลายเซ็นดิจิตอลของ CA แนบไปด้วย พร้อมทั้งข้อความตอบกลับการลงทะเบียนที่มีลายเซ็นดิจิตอลของ CA แนบไปด้วย และเข้ารหัสข้อความตอบกลับนี้ด้วย Secret Key (Key1) ที่เจ้าของบัตรเครดิตแนบมากับข้อมูลการลงทะเบียน และส่งข้อมูลนี้กลับไปยังเจ้าของบัตร

ข้อมูลที่ CA ส่งกลับไปยังเจ้าของบัตรเครดิตจะประกอบด้วย

- ข้อความตอบกลับที่แนบลายเซ็นดิจิตอลของ CA และถูกเข้ารหัสด้วย Secret Key (Key1)
- ใบรับรองดิจิตอลของเจ้าของบัตรเครดิตที่มี Public Signature Key ของเจ้าของบัตรเครดิตอยู่ด้วย
- ใบรับรองดิจิตอลของ CA ที่มี Public Signature Key ของ CA อยู่ด้วย

7. เจ้าของบัตรเครดิตได้รับใบรับรอง

เมื่อเจ้าของบัตรเครดิตได้รับข้อมูลที่ตอบกลับมาจาก CA จะตรวจสอบใบรับรองดิจิตอลของ CA และถอดรหัสข้อความตอบกลับด้วย Secret Key (Key1) ที่เก็บไว้พร้อมทั้งตรวจสอบลายเซ็นดิจิตอลของ CA โดยใช้ Public Signature Key ของ CA ถ้าข้อมูลที่ตรวจสอบถูกต้องเจ้าของบัตรเครดิตจะเก็บใบรับรองดิจิตอลนั้นไว้เพื่อใช้ในโอกาสต่อไป

3.5.2 การลงทะเบียนของร้านค้า

ร้านค้าจะต้องทำการลงทะเบียนกับ CA ก่อนจึงจะสามารถรับคำสั่งการชำระค่าสินค้าแบบ SET จากผู้ซื้อได้หรือสามารถประมวลผลรายการในรูปแบบ SET โดยผ่าน Payment Gateway ได้ การที่ร้านค้าจะสามารถส่งทำรายการในรูปแบบของ SET ไปยัง CA ได้นั้น ร้านค้าจะต้องมี Public Exchange Key ของ CA ก่อน โดย Key นี้จะได้มาจากใบรับรองดิจิตอลของ CA

ร้านค้าจะต้องมีแบบฟอร์มการลงทะเบียนของสถาบันการเงินที่สร้างเบัญชีให้กับร้านค้าเพื่อให้ CA ออกแบบฟอร์มในการลงทะเบียนให้ และร้านค้าจะต้องแจ้งกับ CA ว่าสถาบันการเงินนั้นเป็นใคร

ขั้นตอนในการลงทะเบียนของร้านค้าประกอบด้วย 5 ขั้นตอน คือ

1. ร้านค้าร้องขอแบบฟอร์มการลงทะเบียน

   ร้านค้าส่งคำร้องขอเริ่มต้นการลงทะเบียนไปยัง CA

2. Certificate Authority ประมวลผลคำร้องขอนั้นและส่งแบบฟอร์มการลงทะเบียนกลับมายังร้านค้า

   เมื่อ CA ได้รับคำร้องขอนั้นจะส่งแบบฟอร์มการลงทะเบียนพร้อมลายเซ็นดิจิตอล และใบรับรองดิจิตอลที่มี Public Exchange Key และ Public Signature Key ของ CA กลับมายังร้านค้า

3. ร้านค้าได้รับแบบฟอร์มการลงทะเบียนและร้องขอใบรับรองดิจิตอลจาก Certificate Authority

เมื่อร้านค้าได้รับแบบฟอร์มการลงทะเบียนจาก CA จะตรวจสอบใบรับรองดิจิตอลของ CA และตรวจสอบลายเซ็นดิจิตอลของ CA ด้วย Public Signature Key ของ CA ถ้าข้อมูลถูกต้องร้านค้าจะทำการสร้างชุดของ Key ขึ้นมา 2 ชุดคือ

- Exchange Key ที่เป็น Key ที่ใช้ในการเข้ารหัสและถอดรหัสข้อมูล
- Signature Key ที่เป็น Key ที่ใช้ในการสร้างและตรวจสอบลายเซ็นดิจิตอล

ร้านค้าจะกรอกข้อมูลลงในแบบฟอร์มการลงทะเบียนและสร้างคำร้องขอใบรับรองดิจิตอลจาก CA พร้อมทั้งแนบ Public Key ทั้ง 2 ชุดไปกับคำร้องขอนั้น พร้อมทั้งสร้างลายเซ็นดิจิตอลของร้านค้าแนบไปกับข้อมูลชุดนั้นด้วย และทำการเข้ารหัสข้อมูลทั้งหมดด้วย Secret Key ที่ได้จากการสุ่ม และส่ง Secret Key นี้พร้อมด้วยข้อมูลบัญชีร้านค้าไปใน Digital Envelope ที่ส่งกลับไปยัง CA

ข้อมูลทั้งหมดที่ส่งกลับไปยัง CA ประกอบด้วย

- คำร้องขอใบรับรองดิจิตอล Public Exchange Key และ Public Signature Key พร้อมลายเซ็นดิจิตอลของร้านค้าที่ถูกเข้ารหัสด้วย Secret Key
- Digital Envelope ที่ประกอบด้วย Secret Key ที่ใช้เข้ารหัสคำร้องขอใบรับรองดิจิตอล และข้อมูลบัญชีร้านค้า

4. Certificate Authority ประมวลผลคำร้องขอและสร้างใบรับรองดิจิตอลให้กับร้านค้า

เมื่อ CA ได้รับคำร้องขอใบรับรองดิจิตอลจากร้านค้าจะถอดรหัส Digital Envelope ด้วย Private Exchange Key ของ CA และนำ Secret Key ที่ได้ไปถอดรหัสข้อมูลคำร้องขอนั้น พร้อมทั้งตรวจสอบลายเซ็นดิจิตอลของร้านค้าด้วย Public Signature Key ที่ร้านค้าส่งมาให้ และตรวจสอบข้อมูลของร้านค้ากับ Acquirer ถ้าลายเซ็นและข้อมูลถูกต้อง CA จะสร้างใบรับรองดิจิตอลสำหรับร้านค้าและคำตอบกลับการสร้างใบรับรองดิจิตอลพร้อมทั้งแนบลายเซ็นดิจิตอลของ CA ไปกับใบรับรองนั้น และส่งใบรับรองนั้นกลับไปยังร้านค้า

ข้อมูลที่ CA ส่งกลับมายังร้านค้าประกอบด้วย

- คำตอบกลับการสร้างใบรับรองดิจิตอลที่มีลายเซ็นดิจิตอลของ CA แนบไปด้วย
- ใบรับรองดิจิตอลของร้านค้าที่มี Public Exchange Key และ Public Signature Key ของร้านค้าอยู่ด้วย
- ใบรับรองดิจิตอลของ CA ที่มี Public Signature Key ของ CA อยู่ด้วย

5. ร้านค้าได้รับใบรับรองดิจิตอล

เมื่อร้านค้าได้รับใบรับรองดิจิตอลจะทำการตรวจสอบใบรับรองดิจิตอลของ CA และลายเซ็นดิจิตอลของ CA ถ้าลายเซ็นถูกต้องร้านค้าจะเก็บใบรับรองดิจิตอลนั้นไว้ใช้ในโอกาสต่อไป

3.5.3 การสั่งซื้อสินค้า

การสั่งซื้อสินค้าโดยใช้รูปแบบของ SET จะเกิดขึ้นหลังจากที่ผู้ซื้อสินค้าได้ตัดสินใจเลือกซื้อสินค้าแล้ว และเลือกการชำระค่าสินค้าด้วยบัตรเครดิต ซึ่งจะต้องส่งข้อความในรูปแบบของ SET ไปยังร้านค้า การที่จะส่งข้อมูลการสั่งซื้อสินค้าในรูปแบบ SET ไปยังร้านค้าได้นั้น ผู้ซื้อจะต้องมี Exchange Key ของ Payment Gateway เก็บไว้ การประมวลผลคำสั่งซื้อด้วย SET จะเริ่มเมื่อผู้ซื้อร้องขอใบรับรองดิจิตอลของ Gateway และขั้นตอนในการสั่งซื้อสินค้าประกอบด้วย 5 ขั้นตอนคือ

1. ผู้ซื้อเริ่มต้นส่งคำร้องขอสั่งซื้อสินค้า

   ผู้ซื้อส่งคำร้องขอเริ่มต้นการสั่งซื้อสินค้าไปยังร้านค้า

2. ร้านค้าตอบกลับคำร้องขอโดยส่งใบรับรองดิจิตอลของร้านค้าไปยังผู้ซื้อ

   เมื่อร้านค้าได้รับคำร้องขอนั้นแล้วจะตอบกลับคำร้องขอนั้นโดยสร้างข้อความตอบกลับที่มีลายเซ็นดิจิตอลของร้านค้า ใบรับรองดิจิตอลของร้านค้าที่มี Public Signature Key ของร้านค้า และใบรับรองดิจิตอลของ Gateway ที่มี Public Exchange Key ของ Gateway ส่งกลับไปยังผู้ซื้อ

3. ผู้ซื้อส่งคำร้องขอสั่งซื้อสินค้า

   เมื่อผู้ซื้อได้รับคำตอบกลับมาจากร้านค้าจะทำการตรวจสอบใบรับรองและลายเซ็นดิจิตอลของร้านค้าจาก CA ถ้าข้อมูลที่ได้รับถูกต้อง โปรแกรมที่เครื่องของผู้ซื้อจะสร้างชุดของข้อมูลขึ้นมา 2 ชุดคือข้อมูลการสั่งซื้อสินค้าและข้อมูลการชำระค่าสินค้า โดยในข้อมูลแต่ละชุดจะมีลายเซ็นดิจิตอลคู่ของผู้ซื้อที่มาจากการคำนวณ Message Digest ของข้อมูลการสั่งซื้อสินค้าและข้อมูลการชำระค่าสินค้าแนบไปด้วย และผู้ซื้อจะทำการเข้ารหัสข้อมูลการชำระค่าสินค้าด้วย Secret Key ที่ได้จากการสุ่มขึ้นมา และ Secret Key ที่ใช้ในการเข้ารหัสนี้พร้อมทั้งข้อมูลเกี่ยวกับบัญชีของผู้ซื้อจะเก็บรวมกันไว้ใน Digital Envelope โดยเข้ารหัส Digital Envelope นี้ด้วย Public Exchange Key ของ Gateway

   ข้อมูลที่ผู้ซื้อจะส่งไปให้กับร้านค้าจะประกอบไปด้วย

   - ข้อมูลการสั่งซื้อสินค้าที่แนบลายเซ็นดิจิตอลคู่ของผู้ซื้อ
   - ข้อมูลการชำระค่าสินค้าที่แนบลายเซ็นดิจิตอลคู่ของผู้ซื้อ และถูกเข้ารหัสโดย Secret Key
   - Digital Envelope ที่ประกอบด้วย Secret Key ที่ใช้ในการเข้ารหัสข้อมูลการชำระค่าสินค้าและข้อมูลเกี่ยวกับบัญชีของผู้ซื้อ
   - ใบรับรองของผู้ซื้อสินค้าที่มี Public Signature Key ของผู้ซื้อสินค้า

4. ร้านค้าประมวลผลคำสั่งซื้อสินค้า

   เมื่อร้านค้าได้รับข้อมูลจากผู้ซื้อจะทำการตรวจสอบใบรับรองของผู้ซื้อจาก CA ถ้าข้อมูลถูกต้องร้านค้าจะตรวจสอบลายเซ็นดิจิตอลคู่ของผู้ซื้อในข้อมูลการสั่งซื้อสินค้า ถ้าลายเซ็นถูกต้องร้าน

ค้าจะทำการประมวลผลการสั่งซื้อสินค้า และส่งข้อมูลการชำระค่าสินค้าไปยัง Payment Gateway เพื่อขออนุญาตการทำรายการชำระค่าสินค้า ซึ่งจะกล่าวถึงในหัวข้อต่อไป เมื่อการทำรายการสำเร็จ ร้านค้าจะส่งข้อความตอบกลับเพื่อเป็นการยืนยันการทำรายการของผู้ซื้อพร้อมทั้งแนบลายเซ็นดิจิตอลของร้านค้าไปกับคำตอบนั้นด้วยและใบรับรองของร้านค้าที่มี Public Signature Key ของร้านค้าไปยังผู้ซื้อ

5. ผู้ซื้อได้รับคำตอบกลับการทำรายการจากร้านค้า

เมื่อผู้ซื้อได้รับคำตอบกลับจากร้านค้าจะทำการตรวจสอบใบรับรองดิจิตอลของร้านค้าจาก CA ถ้าใบรับรองถูกต้องผู้ซื้อจะทำการตรวจสอบลายเซ็นดิจิตอลของร้านค้า ถ้าลายเซ็นถูกต้องผู้ซื้อจะทำการเก็บคำตอบกลับนั้นไว้

3.5.4 การขออนุญาตชำระค่าสินค้า

เมื่อผู้ซื้อส่งคำสั่งในการสั่งซื้อสินค้ามายังร้านค้า ร้านค้าจะขออนุญาตทำรายการนั้นจาก Payment Gateway โดยขั้นตอนในการขออนุญาตชำระค่าสินค้าประกอบด้วย 3 ขั้นตอน ดังนี้

1. ร้านค้าร้องขออนุญาตทำรายการ

เมื่อร้านค้าได้รับคำสั่งซื้อสินค้ามาจากผู้ซื้อ ร้านค้าจะสร้างคำร้องขอการอนุญาตโดยมีลายเซ็นดิจิตอลของร้านค้าแนบอยู่ด้วย และทำการเข้ารหัสคำร้องขอนั้นด้วย Secret Key ที่ได้จากการสุ่ม และส่งข้อมูลคำร้องขอนี้พร้อมทั้งข้อมูลการชำระค่าสินค้าไปยัง Payment Gateway

ข้อมูลที่ร้านค้าจะส่งให้กับ Payment Gateway ประกอบด้วย

- คำร้องขออนุญาตในการทำรายการที่มีลายเซ็นดิจิตอลของร้านค้าแนบอยู่ด้วย และถูกเข้ารหัสไว้ด้วย
- Digital Envelope ที่ประกอบด้วย Secret Key ที่ใช้เข้ารหัสคำร้องขอ
- ข้อมูลการชำระค่าสินค้าของผู้ซื้อและ Digital Envelope ที่มาจากผู้ซื้อ
- ใบรับรองของผู้ซื้อที่มี Public Signature Key ของผู้ซื้อ
- ใบรับรองของร้านค้าที่มี Public Signature Key และ Public Exchange Key ของร้านค้า

2. Payment Gateway ประมวลผลคำร้องขออนุญาตทำรายการ

เมื่อ Payment Gateway ได้รับคำร้องขอจากร้านค้าจะทำการตรวจสอบใบรับรองของร้านค้าจาก CA ถ้าใบรับรองถูกต้องจะทำการถอดรหัส Digital Envelope ของร้านค้าด้วย Private Exchange Key ของ Payment Gateway และนำ Secret Key ที่ได้มาทำการถอดรหัสคำร้องขอพร้อมทั้งทำการตรวจสอบลายเซ็นดิจิตอลของร้านค้าด้วย Public Signature Key ของร้านค้า

เมื่อข้อมูลของร้านค้าถูกต้อง Payment Gateway จะทำการตรวจสอบใบรับรองของผู้ซื้อกับ CA ถ้าใบรับรองของผู้ซื้อถูกต้องจะทำการถอดรหัส Digital Envelope ของผู้ซื้อด้วย Private Exchange Key ของ Gateway และนำ Secret Key ที่ได้มาถอดรหัสข้อมูลการชำระค่าสินค้าพร้อมทั้งตรวจสอบลายเซ็นดิจิตอลคู่ของลูกค้า

Payment Gateway จะทำการตรวจสอบรายการที่ได้รับจากร้านค้าว่าตรงกับคำสั่งในการชำระค่าสินค้าของผู้ซื้อหรือไม่ ถ้าตรงกัน Payment Gateway จะส่งคำร้องขออนุญาตในการทำรายการไปยัง Issuer และเมื่อได้รับคำตอบกลับมาจาก Issuer Payment Gateway จะสร้างข้อความตอบกลับไปยังร้านค้าโดยแนบลายเซ็นดิจิตอลของ Payment Gateway ไปด้วย และเข้ารหัสข้อความตอบกลับนั้นด้วย Secret Key (Key3) ที่ได้จากการสุ่ม พร้อมทั้งทำการจัดเก็บ Secret Key (Key3) นั้นใน Digital Envelope ที่ถูกเข้ารหัสโดย Public Exchange Key ของร้านค้า

Payment Gateway จะสร้าง Token ที่นำไปใช้ในการชำระค่าสินค้าพร้อมทั้งแนบลายเซ็นดิจิตอลของ Payment Gateway ไปด้วย และทำการเข้ารหัส Token นี้ด้วย Secret Key (Key4) ที่ได้จากการสุ่ม พร้อมทั้งทำการจัดเก็บ Secret Key (Key4) นี้และข้อมูลเกี่ยวกับบัญชีของผู้ซื้อใน Digital Envelope ที่ถูกเข้ารหัสโดย Public Exchange Key ของ Gateway

ข้อมูลที่ Payment Gateway จะส่งให้กับร้านค้า ประกอบด้วย

- คำตอบกลับยังร้านค้าที่มีลายเซ็นดิจิตอลของ Payment Gateway แนบอยู่ด้วย และถูกเข้ารหัสด้วย Secret Key (Key3)
- Digital Envelope ที่ประกอบด้วย Secret Key (Key3) ที่ใช้เข้ารหัสคำตอบกลับ และถูกเข้ารหัสด้วย Public Exchange Key ของร้านค้า
- Token ที่มีลายเซ็นดิจิตอลของ Payment Gateway แนบอยู่ด้วย และถูกเข้ารหัสด้วย Secret Key (Key4)
- Digital Envelope ที่ประกอบด้วย Secret Key (Key4) ที่ใช้เข้ารหัส Token และข้อมูลเกี่ยวกับบัญชีของผู้ซื้อ และถูกเข้ารหัสด้วย Public Exchange Key ของ Payment Gateway
- ใบรับรองของ Payment Gateway ที่มี Public Signature Key ของ Payment Gateway อยู่ด้วย

3. ร้านค้าประมวลผลคำตอบรับจาก Payment Gateway

เมื่อร้านค้าได้รับคำตอบกลับมาจาก Payment Gateway จะทำการตรวจสอบใบรับรองของ Payment Gateway กับ CA ถ้าใบรับรองนั้นถูกต้องจะทำการถอดรหัส Digital Envelope ของคำตอบกลับด้วย Private Exchange Key ของร้านค้าและนำ Secret Key (Key3) ที่ได้มาใช้ในการถอดรหัส

คำตอบกลับจาก Payment Gateway พร้อมทั้งตรวจสอบลายเซ็นของ Payment Gateway ด้วย Public Signature Key ของ Payment Gateway และร้านค้าจะเก็บ Token และ Digital Envelope ของ Payment Gateway ไว้เพื่อใช้ในขั้นตอนการชำระค่าสินค้าต่อไป

3.5.5 การชำระค่าสินค้า

การชำระค่าสินค้าประกอบด้วยขั้นตอนการทำงาน 3 ขั้นตอนคือ

1. ร้านค้าร้องขอชำระค่าสินค้า

ร้านค้าจะสร้างคำร้องขอพร้อมทั้งแนบลายเซ็นดิจิตอลของร้านค้า และเข้ารหัสคำร้องขอนั้นด้วย Secret Key ที่ได้จากการสุ่ม พร้อมทั้งเข้ารหัส Secret Key ใน Digital Envelope ด้วย Public Exchange Key ของ Gateway และส่งข้อมูลไปยัง Payment Gateway

ข้อมูลที่ร้านค้าส่งไปให้กับ Payment Gateway ประกอบด้วย

- คำร้องขอที่มีลายเซ็นดิจิตอลของร้านค้าแนบอยู่ด้วย และถูกเข้ารหัสด้วย Secret Key
- Digital Envelope ที่ประกอบด้วย Secret Key ที่ใช้เข้ารหัสคำร้องขอ และถูกเข้ารหัสด้วย Public Exchange Key ของ Payment Gateway
- Token ที่ได้ร้านค้าในขั้นตอนการขออนุญาตชำระค่าสินค้า
- Digital Envelope ที่เก็บ Secret Key ที่เข้ารหัส Token ที่ได้จากร้านค้าในขั้นตอนการขออนุญาตชำระค่าสินค้า
- ใบรับรองของร้านค้าที่มี Public Exchange Key และ Public Signature Key ของร้านค้าอยู่ด้วย

2. Payment Gateway ประมวลผลคำร้องขอชำระค่าสินค้า

เมื่อ Payment Gateway ได้รับคำร้องขอชำระค่าสินค้าจากร้านค้าจะทำการตรวจสอบใบรับรองร้านค้าจาก CA ถ้าใบรับรองถูกต้องจะทำการถอดรหัส Digital Envelope ของคำร้องขอด้วย Private Exchange Key ของ Gateway และนำ Secret Key ที่ได้ไปถอดรหัสคำร้องขอนั้น พร้อมทั้งตรวจสอบลายเซ็นดิจิตอลของร้านค้า และทำการถอดรหัส Digital Envelope ของ Token ด้วย Private Exchange Key ของ Gateway เพื่อนำ Secret Key (Key4) ไปใช้ในการถอดรหัส Token

Gateway จะส่งคำร้องขอและ Token นี้ไปยังสถาบันการเงินของผู้ซื้อ และสร้างข้อความตอบกลับที่มีลายเซ็นดิจิตอลของ Payment Gateway แนบไปด้วย และเข้ารหัสข้อความตอบกลับด้วย Secret Key ที่ได้จากการสุ่ม และ Key นี้จะถูกเข้ารหัสเป็น Digital Envelope ด้วย Public Exchange Key ของร้านค้า

ข้อมูลที่ Payment Gateway ส่งกลับไปยังร้านค้าประกอบด้วย

- คำตอบกลับยังร้านค้าที่มีลายเซ็นดิจิตอลของ Payment Gateway แนบอยู่ด้วย และถูกเข้ารหัสด้วย Secret Key
- Secret Key ที่ใช้เข้ารหัสคำตอบกลับ ซึ่งถูกจัดเก็บอยู่ใน Digital Envelope ที่ถูกเข้ารหัสด้วย Public Exchange Key ของร้านค้า
- ใบรับรองของ Payment Gateway ที่มี Public Signature Key ของ Payment Gateway อยู่ด้วย

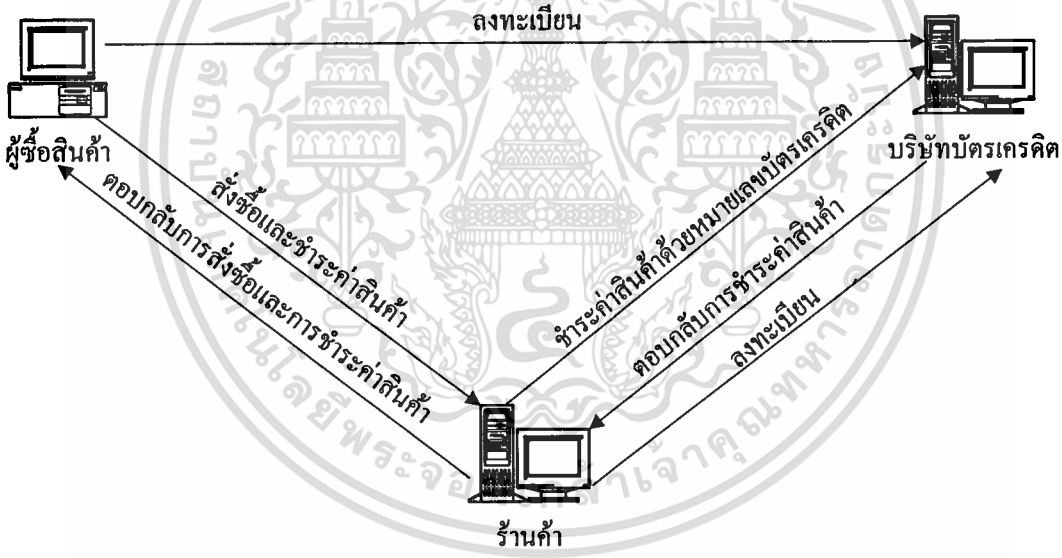
3. ร้านค้าได้รับคำตอบกลับจาก Payment Gateway

เมื่อร้านค้าได้รับคำตอบกลับจาก Payment Gateway จะทำการตรวจสอบใบรับรองนั้นกับ CA และร้านค้าจะทำการถอดรหัส Digital Envelope ด้วย Private Exchange Key ของร้านค้า เพื่อนำ Secret Key มาใช้ในการถอดรหัสข้อความที่ตอบกลับมาจาก Payment Gateway พร้อมทั้งตรวจสอบลายเซ็นดิจิตอลของร้านค้าด้วย Public Signature Key ของร้านค้าด้วย

บทที่ 4

การพัฒนาระบบงาน

การพัฒนาโปรแกรมในโครงการนี้เป็นการทำงานในส่วนการซื้อขายสินค้าบนอินเตอร์เน็ต และชำระค่าสินค้าด้วยบัตรเครดิตที่อ้างอิงหลักการทำงานมาจากระบบ SET ที่มีการเข้ารหัสข้อมูลที่ติดต่อกันด้วยวิธี Public Key Cryptography และการพัฒนาโปรแกรมในโครงการนี้ประกอบด้วยผู้เกี่ยวข้องทั้งหมด 3 ฝ่ายคือ ผู้ซื้อสินค้า ร้านค้า และบริษัทบัตรเครดิตที่หน้าที่เป็น Certificate Authority โดยความสัมพันธ์ของแต่ละฝ่ายแสดงดังรูปที่ 4.1



รูปที่ 4.1 แสดงความสัมพันธ์ขององค์ประกอบในโครงการ

ฝ่ายต่างๆในโครงการนี้จะมีการเก็บ Key ที่ใช้ในการเข้ารหัสและถอดรหัสข้อมูลไว้ที่เครื่องของตัวเอง โดยรายละเอียดของ Key ที่แต่ละฝ่ายเก็บแสดงดังตารางที่ 4.1

ผู้ซื้อสินค้า	ร้านค้า	บริษัทบัตรเครดิต
Private Key ของผู้ซื้อ	Private Key ของร้านค้า	Public Key ของผู้ซื้อ
Public Key ของบริษัทบัตรเครดิต	Public Key ของบริษัทบัตรเครดิต	Public Key ของร้านค้า
		Private Key ของบริษัทบัตรเครดิต

ตารางที่ 4.1 แสดง Key ที่เก็บในแต่ละฝ่าย

การพัฒนาโปรแกรมในโครงการนี้แบ่งการทำงานออกเป็น 3 ส่วน คือ

1. การสร้าง Private Key และ Public Key โดยซอฟต์แวร์ PGP
2. การลงทะเบียนของผู้ถือบัตรเครดิตและร้านค้ากับบริษัทบัตรเครดิต ประกอบด้วยการทำงานทั้งหมด 4 ส่วน คือ
   - การลงทะเบียนข้อมูลบัตรเครดิต
   - การลงทะเบียนข้อมูลร้านค้า
   - การลงทะเบียน Public Key
   - การ Download Public Key ของบริษัทบัตรเครดิต
3. การชำระค่าสินค้าด้วยหมายเลขบัตรเครดิต ประกอบด้วยการทำงาน 3 ส่วน คือ
   - การทำงานในส่วนของผู้ซื้อ
   - การทำงานในส่วนของร้านค้า
   - การทำงานในส่วนของบริษัทบัตรเครดิต

ซอฟต์แวร์ที่นำมาใช้ในการพัฒนาระบบงาน ประกอบด้วย

1. PGP (Pretty Good Privacy) ที่เป็นซอฟต์แวร์ที่ใช้ในการสร้างและจัดการ Key ทั้ง Public Key และ Private Key ที่ใช้ในระบบ
2. Library SPGP (Simple PGP DLL) เป็น Library ที่ใช้ในการเข้าถึง Key ใน PGP และการติดต่อกับ SPGP จะกระทำได้โดยผ่านโปรแกรมภาษา Visual Basic ในการใช้งาน Library SPGP มีฟังก์ชันการทำงานคือ
   - เข้ารหัสและถอดรหัสข้อมูล
   - การทำลายเซ็นดิจิตอล
   - การ Import Key เข้าสู่ PGPkeys

4.1 ฟังก์ชันที่เรียกใช้จาก SPGP

การพัฒนาโปรแกรมในระบบนี้มีการเรียกใช้ฟังก์ชันของ SPGP ได้แก่

1. ฟังก์ชันการเข้ารหัสข้อมูล

```
Declare Function spgp_encode Lib "spgp.dll" (
        ByVal BufferIn As String,
        ByVal BufferOut As String,
        ByVal BufferOutLen As Long,
        ByVal Encrypt As Long,
        ByVal Sign As Long,
        ByVal SignAlg As Long,
        ByVal Conventional As Long,
        ByVal ConventionalAlg As Long,
        ByVal Armor As Long,
        ByVal TextMode As Long,
        ByVal Clear As Long,
        ByVal Compress As Long,
        ByVal EyesOnly As Long,
        ByVal MIME As Long,
        ByVal CryptKeyID As String,
        ByVal SignKeyID As String,
        ByVal SignKeyPass As String,
        ByVal ConventionalPass As String,
        ByVal Comment As String,
        ByVal MIMESeparator As String
        ) As Long
```

Parameter ในฟังก์ชันนี้ประกอบด้วย

- BufferIn หมายถึง ข้อมูลที่ต้องการเข้ารหัส
- BufferOut หมายถึง ข้อมูลที่ได้จากการเข้ารหัส
- BufferOutLen หมายถึง ความยาวของข้อมูลที่ได้จากการเข้ารหัส

- Encrypt หมายถึง การเข้ารหัสข้อมูลใน BufferIn โดยมีค่าเป็น 0 หรือ 1 ถ้ามีค่าเป็น 1 ข้อมูลที่อยู่ใน BufferIn จะถูกเข้ารหัสด้วย Public Key ที่กำหนดใน Parameter CryptKeyID
- Sign หมายถึง การทำลายเซ็นดิจิตอลบนข้อมูลที่ถูกเข้ารหัส โดยมีค่าเป็น 0 หรือ 1 ถ้ามีค่าเป็น 1 ข้อมูลที่อยู่ใน BufferIN จะถูกทำลายเซ็นดิจิตอลด้วย Private Key ที่กำหนดใน Parameter SignKeyID และรหัสที่ใช้ในการทำลายเซ็นดิจิตอลจะถูกกำหนดใน Parameter SignKeyPass
- SignAlg หมายถึง Hashing Algorithm ที่ใช้ในการทำลายเซ็นดิจิตอล

  ค่าของ Algorithm ที่ใช้กับ Key ประเภท RSA ได้แก่

  - 0 หมายถึง PGPHashAlgorithm_Default
  - 1 หมายถึง PGPHashAlgorithm_MD5
  - 2 หมายถึง PGPHashAlgorithm_SHA
  - 3 หมายถึง PGPHashAlgorithm_RIPEMD5
  - 4 หมายถึง PGPHashAlgorithm_SHADouble

  สำหรับ Default Algorithm ที่ใช้กับ Key ประเภท RSA คือ MD5 ส่วน Key ประเภทอื่นๆ ใช้ Algorithm SHA และ Key ประเภท DH/DSS (ElGamal) จะใช้ได้กับ Algorithm SHA เท่านั้น
- Conventional หมายถึง การเข้ารหัสข้อมูลด้วย Algorithm ที่กำหนดให้ โดยมีค่าเป็น 0 หรือ 1 ถ้ามีค่าเป็น 1 ข้อมูลที่อยู่ใน BufferIn จะถูกเข้ารหัสด้วย Algorithm ที่ระบุใน Parameter ConventionalAlg และรหัสที่ใช้ร่วมกับการเข้ารหัสที่ระบุใน Parameter ConventionalPass
- ConventionalAlg หมายถึง การกำหนด Algorithm ที่ใช้ในการเข้ารหัสข้อมูลใน BufferIn ได้แก่
  - 1 หมายถึง PGPCipherAlgorithm_IDEA
  - 2 หมายถึง PGPCipherAlgorithm_3DES
  - 3 หมายถึง PGPCipherAlgorithm_CAST5

  Default Algorithm ที่ใช้ในการเข้ารหัสคือ IDEA
- Armor หมายถึง การกำหนดลักษณะของข้อมูลที่ได้จากการเข้ารหัส โดยมีค่าเป็น 0 หรือ 1 ถ้ามีค่าเป็น 1 หมายถึง ข้อมูลที่ได้จากการเข้ารหัสจะอยู่ในรูปแบบ ASCII Radix-64 ที่ใช้กับ E-mail
- TextMode หมายถึง การกำหนดลักษณะของข้อมูลที่จะทำการเข้ารหัส โดยมีค่าเป็น 0 หรือ 1 ถ้ามีค่าเป็น 1 หมายถึง ข้อมูลที่ทำการเข้ารหัสจะถูกจัดให้อยู่ในรูปแบบที่มีการ Carriage Return อยู่ในตำแหน่งสุดท้ายของแต่ละบรรทัด
- Clear หมายถึง การกำหนดให้ข้อมูลของลายเซ็นดิจิตอลอยู่ในรูปแบบ Binary หรือข้อความที่สามารถอ่านได้ โดยมีค่าเป็น 0 หรือ 1 ถ้ามีค่าเป็น 1 ลายเซ็นดิจิตอลที่ทำจะอยู่ในรูปแบบของข้อความที่สามารถอ่านได้

- Compress หมายถึง การบีบอัดข้อมูลก่อนทำการเข้ารหัสโดยมรค่าเป็น 0 หรือ 1 ถ้ามีค่าเป็น 1 ข้อมูลจะถูกบีบอัดก่อนเข้ารหัส
- EyesOnly หมายถึง การ Flag ลงในข้อความที่ถูกเข้ารหัสแล้วเพื่อแจ้งให้ผู้รับทราบว่าไม่ควรบันทึกข้อมูลที่ถูกถอดรหัสแล้วลงเครื่อง โดยมีค่าเป็น 0 หรือ 1 ถ้ามีค่าเป็น 1 จะมีข้อความเตือนที่ผู้รับ
- MIME หมายถึง การกำหนดรูปแบบของข้อมูลที่ถูกเข้ารหัสให้เป็นแบบ PGP/MIME โดยมีค่าเป็น 0 หรือ 1 ถ้ามีค่าเป็น 1 ข้อมูลที่ได้จากการเข้ารหัสจะอยู่ในรูปแบบ PGP/MIME การกำหนดค่าให้ Parameter MIME นี้ต้องสอดคล้องกับ Parameter Armor
- CryptKeyID หมายถึง Public Key ของผู้รับ โดยจะอ้างถึง Public Key นี้จาก E-mail ของผู้รับใน PGPkeys
- SignKeyID หมายถึง Private Key ของผู้ส่ง โดยจะอ้างถึง Private Key นี้จาก E-mail ของผู้ส่งใน PGPkeys
- SignKeyPass หมายถึง รหัสที่ใช้ในการเข้าถึง Private Key ของผู้ส่ง
- ConvetionalPass หมายถึง รหัสที่ใช้ในการเข้ารหัสข้อมูล
- Comment หมายถึง ข้อความอธิบาย
- MIMESeperator หมายถึง ตัวแบ่งข้อความในรูปแบบ PGP/MIME ขนาดสูงสุดของ Parameter นี้คือ 80 ตัวอักษร

2. ฟังก์ชันการถอดรหัสข้อมูล

```
Declare Function spgpdecode Lib "spgp.dll" (
    ByVal BufferIn As String,
    ByVal BufferOut As String,
    ByVal BufferOutLen As Long,
    ByVal Pass As String,
    ByVal SigProps As String
    ) As Long
```

Parameter ในฟังก์ชันนี้ประกอบด้วย

- BufferIn หมายถึง ข้อมูลที่ต้องการถอดรหัสรหัส
- BufferOut หมายถึง ข้อมูลที่ได้จากการถอดรหัส
- BufferOutLan หมายถึง ความยาวของข้อมูลที่ได้จากการถอดรหัส
- Pass หมายถึง รหัสที่ใช้ในการถอดรหัสข้อมูลหรือรหัสที่ใช้ในการเข้าถึง Private Key

- SigProps หมายถึง ลักษณะต่างๆ ของลายเซ็นดิจิตอล ที่มีความยาวไม่เกิน 256 ตัวอักษร โดยลักษณะของลายเซ็นดิจิตอลที่ได้ประกอบไปด้วย
  1. สถานะของลายเซ็นดิจิตอล โดยมีสถานะต่างๆ ดังนี้
     - SIGNED_GOOD = 0 หมายถึง มีลายเซ็นดิจิตอลนั้นใน PGPkeys และเป็นลายเซ็นที่ดี
     - SIGNED_NOT = 1 หมายถึง ไม่มีข้อมูลลายเซ็นดิจิตอลนั้นใน PGPkeys
     - SIGNED_BAD = 2 หมายถึง มีลายเซ็นดิจิตอลนั้นใน PGPkeys แต่เป็นลายเซ็นที่ไม่ถูกต้อง
     - SIGNED_NO_KEY = 3 หมายถึง มีลายเซ็นดิจิตอลนั้นใน PGPkeys แต่ไม่พบ Key ของลายเซ็นนี้ใน PGPkeys
  2. รหัสผู้ใช้ (UserID) ของ Key ที่ทำลายเซ็นดิจิตอล ตัวอย่างเช่น Test Key <test@test.key>
  3. หมายเลข Key (KeyID) ของ Key ที่ทำลายเซ็นดิจิตอล ตัวอย่างเช่น 0xD71F6FE5
  4. วันและเวลาของลายเซ็นที่อยู่ในรูปแบบของวันที่และเวลา ตัวอย่างเช่น Thu Oct 01 20:42:41 1998
  5. วันและเวลาของลายเซ็นที่อยู่ในรูปแบบของวินาที ตัวอย่างเช่น 907299761
  6. การตรวจสอบลายเซ็น เป็นการบอกว่า Key นี้สามารถใช้ได้หรือไม่และข้อมูลอยู่ในรูปแบบที่ถูกต้อง โดยมีค่าเป็นจริงหรือเท็จ
  7. การพิสูจน์ลายเซ็น เป็นการพิสูจน์ว่าลายเซ็นนี้ไม่ถูกเปลี่ยนแปลง โดยมีค่าเป็นจริงหรือเท็จ ลายเซ็นนั้นจะน่าเชื่อถือก็ต่อเมื่อค่าของการตรวจสอบลายเซ็นและการพิสูจน์ลายเซ็นเป็นจริงทั้งคู่
  8. ความถูกต้องของ Key จะบอกถึงระดับความถูกต้องของ Key โดยมีค่าดังนี้
     - PGPValidity_Unknown = 0
     - PGPValidity_Invalid = 1
     - PGPValidity_Marginal = 2
     - PGPValidity_Complete = 3
  9. การยกเลิก Key เป็นการบอกว่า Key นี้ถูกยกเลิกหรือไม่ โดยมีค่าเป็นจริงหรือเท็จ
  10. การอนุญาตให้ใช้ Key เป็นการบอกว่า Key นี้สามารถใช้ได้หรือไม่ โดยมีค่าเป็นจริงหรือเท็จ
  11. การหมดอายุของ Key เป็นการบอกว่า Key นี้หมดอายุหรือไม่ โดยมีค่าเป็นจริงหรือเท็จ

3. ฟังก์ชันการ Import Key

```
Declare Function spgp_keyimport Lib "spgp.dll" (
    ByVal BufferIn As String,
    ByVal KeyProps As String,
    ByVal KeyPropsLen As Long,
    ByVal Import As Long,
    ByVal AllProps As Long
    ) As Long
```

Parameter ในฟังก์ชันนี้ประกอบด้วย

- BufferIn หมายถึง ข้อมูลของ Key ที่ต้องการ Import
- KeyProps หมายถึง คุณสมบัติของ Key ที่ถูก Import สำเร็จ
- KeyPropsLen หมายถึง ขนาดของ KeyProps ถ้าขนาดของ Key ที่ Import เกินขนาดของ KeyPropsLen การ Import Key นั้นจะถูกยกเลิก และฟังก์ชันนี้จะส่งค่ากลับเป็นค่าของขนาดของ Key ที่ Import
- Import หมายถึง การ Import Key หรือไม่ โดยมีค่าเป็น 1 (จริง) หรือ 0 (เท็จ) ถ้ามีค่าเป็น 1 Key ใน BufferIn จะถูก Import เข้า PGPkeys
- AllProps หมายถึง การส่งค่าของคุณสมบัติของ Key กลับมาหรือไม่ โดยมีค่าเป็น 1 (จริง) หรือ 0 (เท็จ) ถ้ามีค่าเป็น 1 คุณสมบัติของ Key จะถูกส่งกลับมาใน KeyProps

4.2 การสร้าง Private Key และ Public Key โดยซอฟต์แวร์ PGP

PGP (Pretty Good Privacy) เป็นซอฟต์แวร์ที่ใช้หลักการเข้ารหัสโดยวิธี Public Key Cryptography ที่ประกอบไปด้วย Private Key และ Public Key ซึ่ง Key ทั้งสองนี้จะถูกจัดเก็บไว้ใน Keyring File ของ PGP และสามารถเข้าถึง Key เหล่านี้ได้โดยผ่านทางหน้าจอ PGPkeys โดยรายละเอียดเกี่ยวกับการใช้งานซอฟต์แวร์ PGP ในการสร้าง Key มีดังต่อไปนี้

4.2.1 การติดตั้ง PGP

PGP เป็นซอฟต์แวร์ที่ไม่ต้องเสียค่าใช้จ่ายในการใช้งาน สามารถดาวน์โหลดได้จากอินเตอร์เน็ตที่ http://www.pgpi.org/products/pgp/versions/freeware/ และ PGP ยังเป็นซอฟต์แวร์ที่สามารถใช้งานได้กับหลาย Platform โดยในโครงการนี้จะใช้ซอฟต์แวร์ PGP สำหรับ Windows คือ PGP 6.5.1i

ความต้องการสำหรับการติดตั้งซอฟต์แวร์ PGP บน Platform Windows ได้แก่

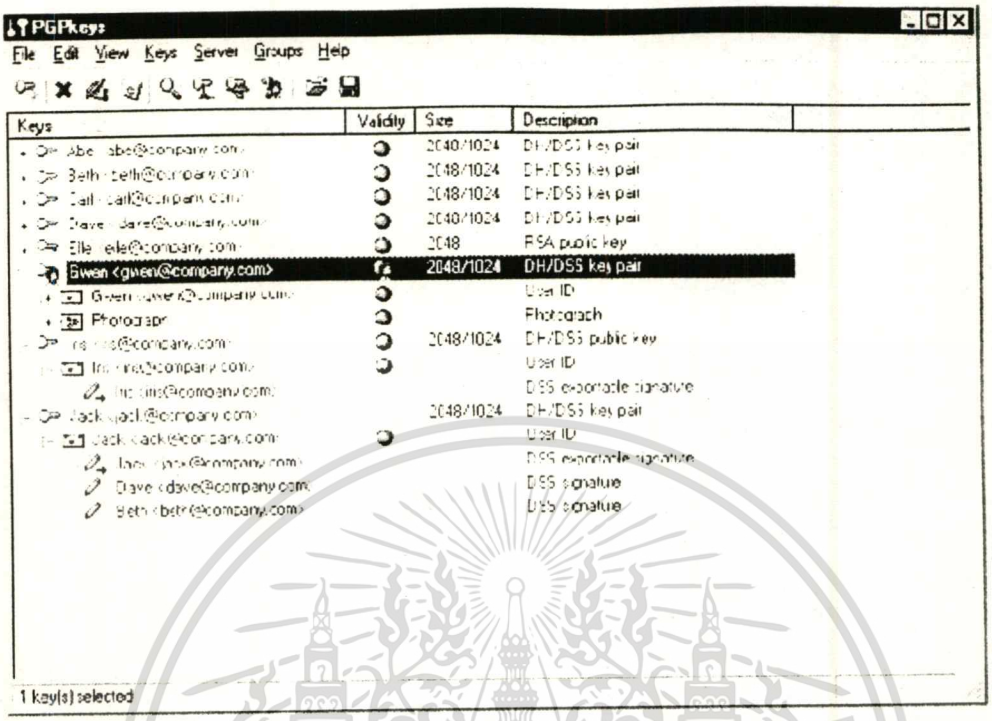
- Windows 95, Windows 98 หรือ Windows NT 4.0 (Service Pack 3 หรือสูงกว่า)
- หน่วยความจำ 32 MB
- เนื้อที่บน Hard Disk อย่างน้อย 16 MB

4.2.2 การสร้าง Key โดยใช้ PGPkeys

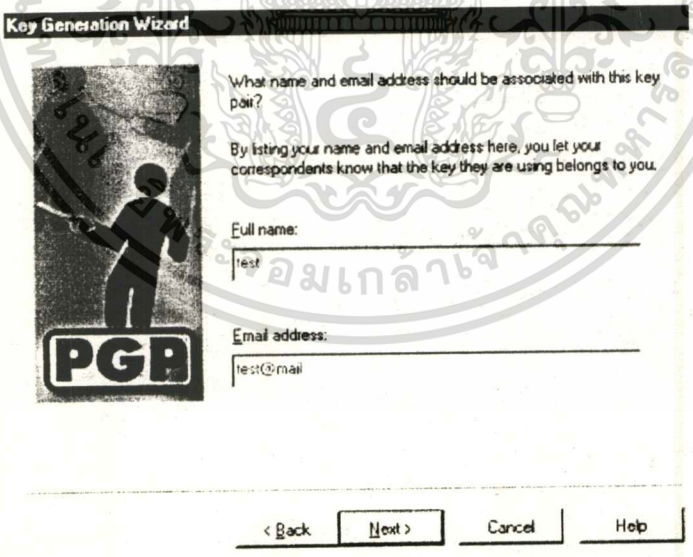
PGPKeys เป็นหน้าจอที่แสดงถึงคู่ของ Private Key และ Public Key ที่เราทำการสร้างขึ้นมา รวมทั้ง Public Key ที่สร้างโดยผู้อื่น ดังรูปที่ 4.2

จากหน้าจอ PGPkeys เราสามารถที่จะสร้างและจัดการเกี่ยวกับ Key ทั้งหมดได้ การอ้างอิงถึง Key ที่ต้องการสร้างหรือจัดการจะอ้างถึงด้วย E-mail Address ของเจ้าของ Key นั้นดังรูปที่ 4.3 และในการสร้าง Key ด้วย PGP เราสามารถเลือกประเภทของ Key ที่ต้องการได้ โดยใน PGP จะรองรับประเภทของ Key 2 ประเภทคือ Diffie-Hellman/DSS หรือ RSA ดังรูปที่ 4.4 การเลือก Key ประเภทใดนั้นขึ้นอยู่กับบุคคลที่เราติดต่อด้วยนั้นใช้ประเภทของ Key แบบใด

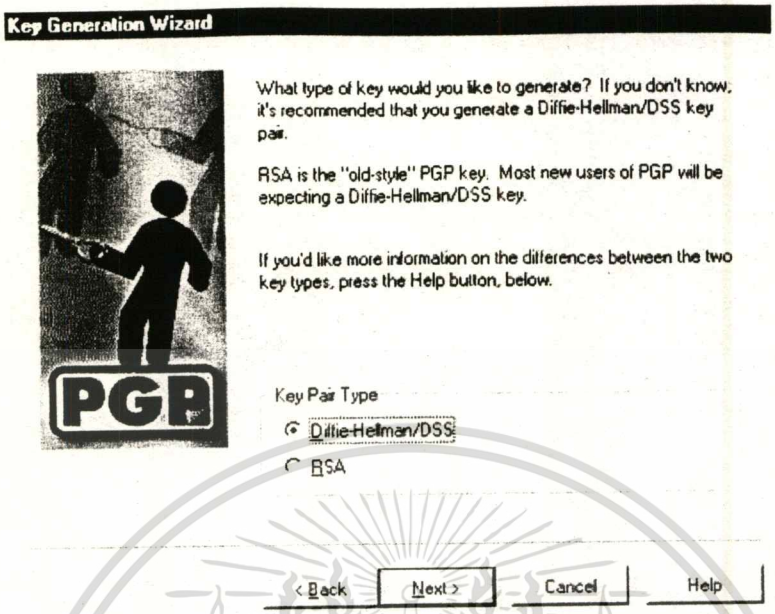
ความยาวของ Key ที่ PGP รองรับคือ 1,024 – 4,096 Bits โดยสามารถเลือกความยาวของ Key ที่ต้องการได้ ดังรูปที่ 4.5 ถ้า Key มีขนาดยาวย่อมมีความปลอดภัยในการป้องกันการถอดรหัสได้แต่จะมีความช้าในการสร้าง Key และในการสร้าง Key เจ้าของ Key จะต้องกำหนดรหัสที่ใช้ในการทำงานเข้ารหัส Private Key ด้วย ดังรูปที่ 4.6



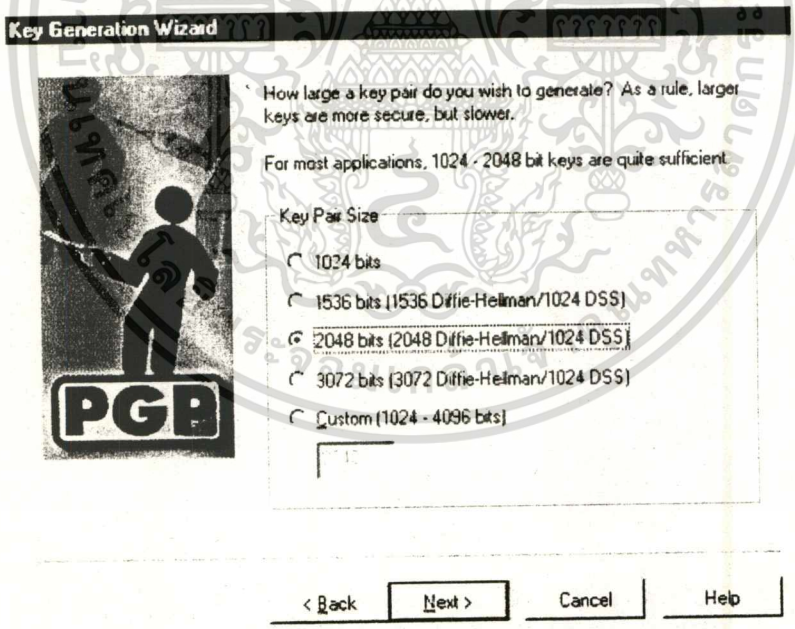
รูปที่ 4.2 แสดงหน้าจอ PGPkeys



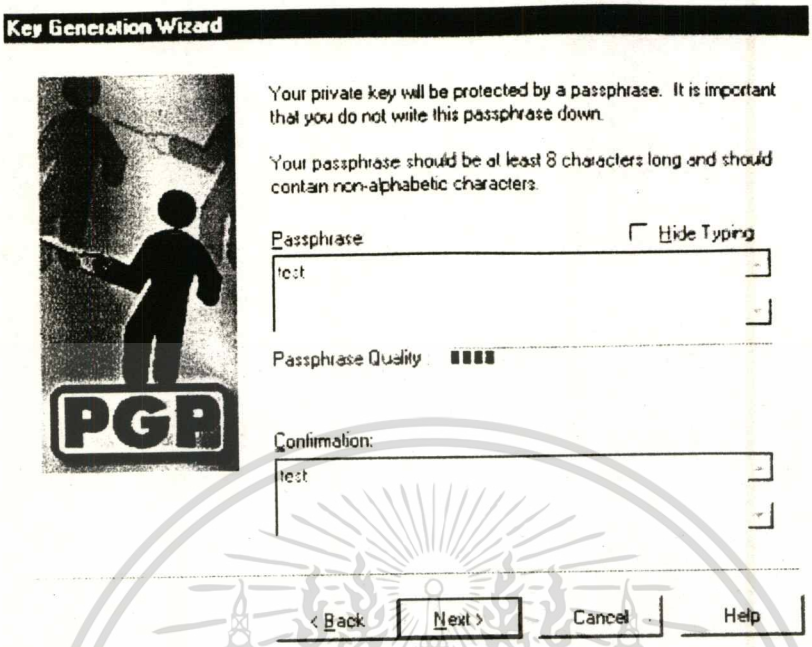
รูปที่ 4.3 แสดงหน้าจอ Wizard การใส่ E-mail เพื่อสร้าง Key ใหม่



รูปที่ 4.4 แสดงหน้าจอ Wizard การเลือกประเภทของ Key ในการสร้าง Key



รูปที่ 4.5 แสดงหน้าจอ Wizard การเลือกความยาวของ Key ในการสร้าง Key

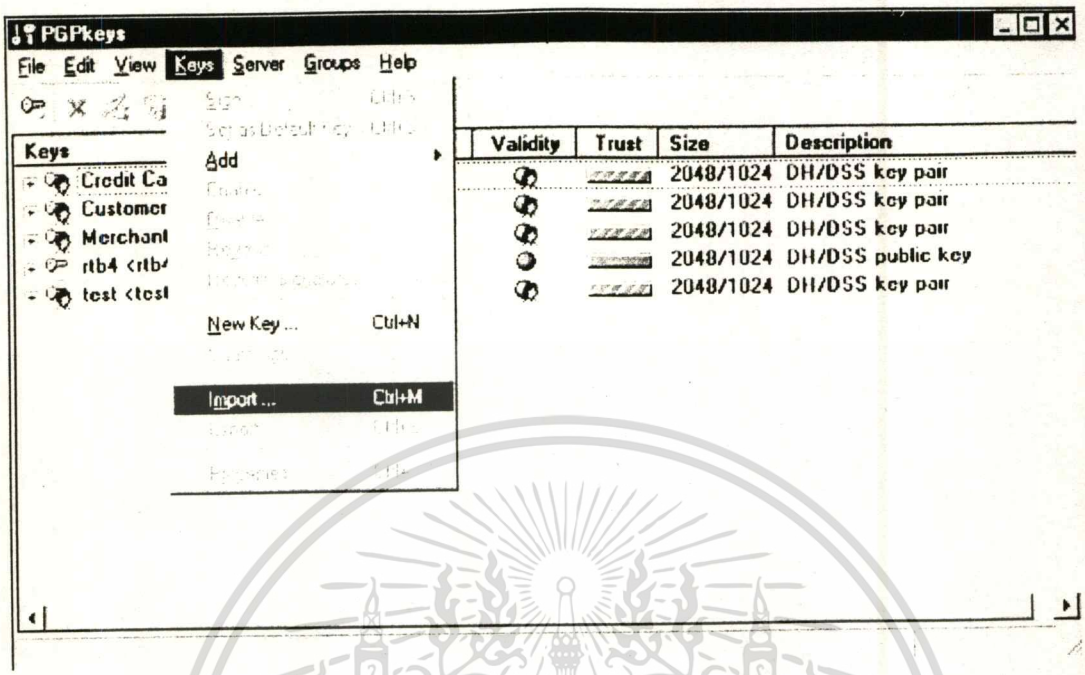


รูปที่ 4.6 แสดงหน้าจอ Wizard การใส่รหัสเพื่อใช้คู่กับ Private Key

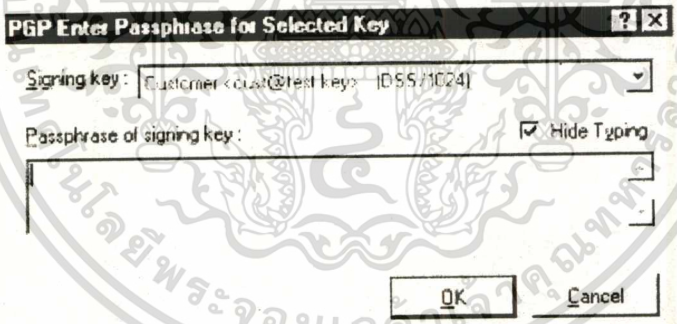
ข้อมูลของ Key ที่แสดงอยู่ใน PGPkeys ทั้งหมดจะถูกเก็บอยู่ใน File ทั้งหมด 2 File คือ Secring.skr ซึ่งเป็น File ที่เก็บ Private Key และ Pubring.pkr ซึ่งเป็น File ที่เก็บ Public Key

4.2.3 การอนุญาตให้ Public Key ของผู้อื่นสามารถใช้งานได้

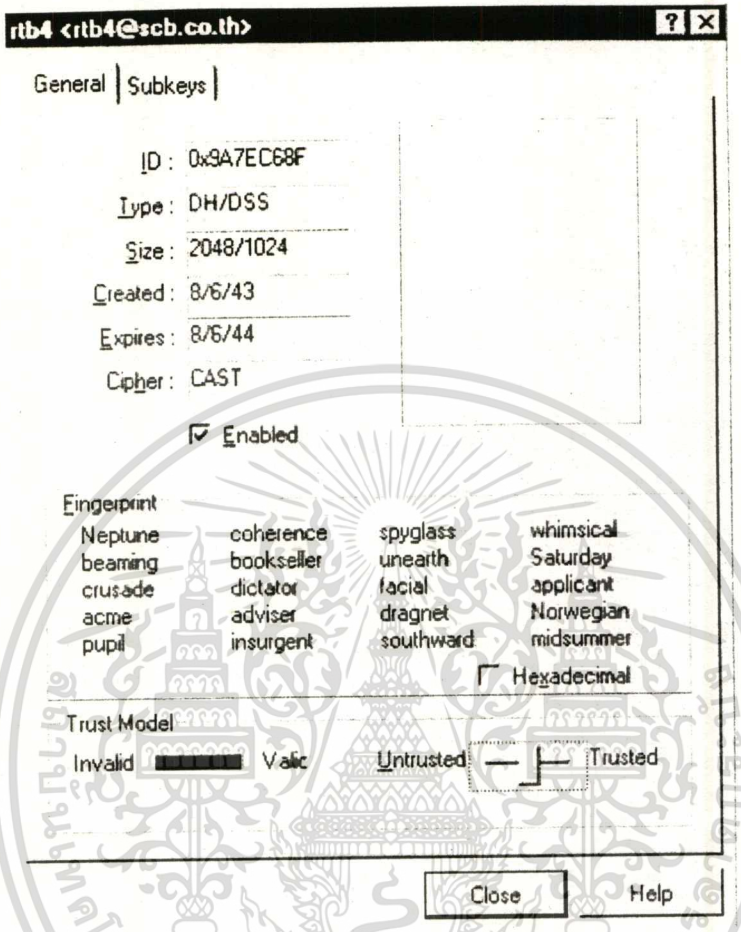
เมื่อได้รับ Public Key ของผู้อื่นจะทำการเพิ่ม Key นี้เข้าสู่ PGPKeys ได้โดยการ Import Public Key นั้นเข้าสู่ PGPkeys ดังรูปที่ 4.7 แต่ Key ที่ถูก Import เข้านี้ยังไม่สามารถใช้งานได้จนกว่าเราจะทำการอนุญาตให้ Key นี้สามารถใช้งานได้ เพื่อเป็นการป้องกันการนำ Key ของผู้อื่นมาติดตั้งที่เครื่องโดยที่เจ้าของเครื่องไม่ทราบ และขั้นตอนในการอนุญาตให้ Public Key ของผู้อื่นสามารถใช้งานที่เครื่องเราได้นั้น โดยการลงนาม (Signed) Public Key นั้นด้วย Private Key ของเรา ดังรูปที่ 4.8 หลังจากนำ Public Key เข้า PGPkeys แล้วเราต้องดำเนินการเพื่อให้ Key นั้นถูกต้องสามารถนำไปใช้งานได้ โดยการเลือก Property ของ Key นั้นแล้วทำการแก้ไขข้อมูลในส่วน Trust Model โดยเปลี่ยนจาก Untrusted เป็น Trusted ดังรูปที่ 4.9



รูปที่ 4.7 แสดงหน้าจอการ Import Key ใน PGPkeys



รูปที่ 4.8 แสดงหน้าจอการลงนาม Public Key ของผู้อื่น



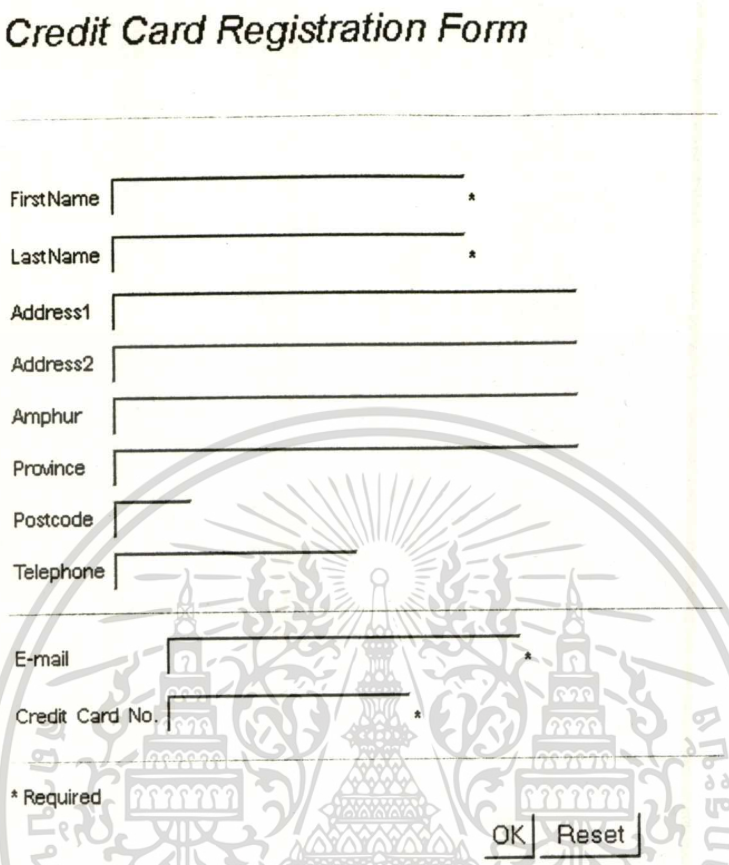
รูปที่ 4.9 แสดงหน้าจอการดำเนินการเพื่อให้ Public Key สามารถใช้งานได้

4.3 การลงทะเบียนของเจ้าของบัตรเครดิตและร้านค้ากับบริษัทบัตรเครดิต

การลงทะเบียนของผู้ถือบัตรเครดิตกับบริษัทบัตรเครดิต ประกอบด้วยขั้นตอน 4 ขั้นตอน คือ

4.3.1 การลงทะเบียนข้อมูลส่วนตัวและหมายเลขบัตรเครดิต

เจ้าของบัตรเครดิตจะลงทะเบียนข้อมูลส่วนตัวและหมายเลขบัตรเครดิตกับบริษัทบัตรเครดิตดังรูปที่ 4.10 โปรแกรมในส่วนการลงทะเบียนนี้จะทำการตรวจสอบข้อมูลของเจ้าของบัตรเครดิตว่ามีอยู่หรือไม่ ถ้าไม่มีจะทำการบันทึกข้อมูลนั้น และสร้างรหัสผ่านให้กับเจ้าของบัตรเครดิตดังรูปที่ 4.11 เพื่อใช้ในการลงทะเบียน Public Key ของเจ้าของบัตรเครดิตกับบริษัทบัตรเครดิตต่อไป

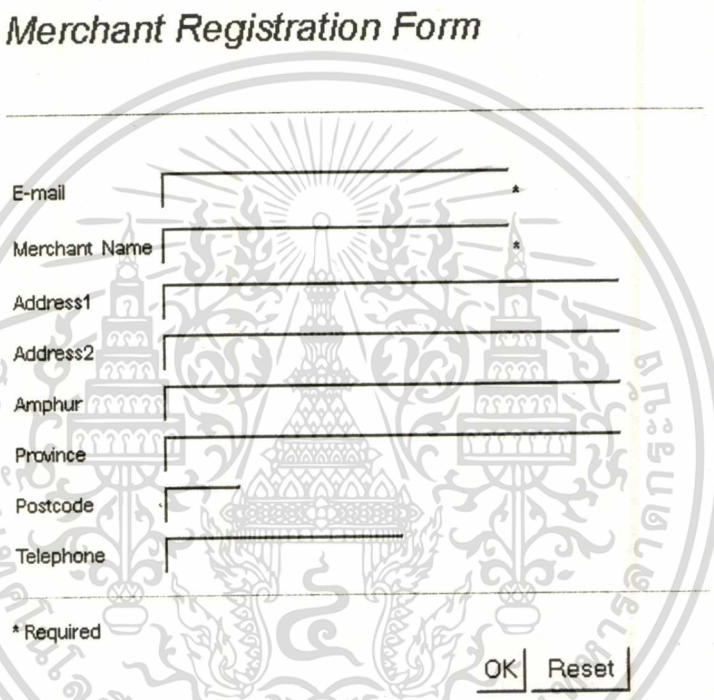


รูปที่ 4.10 แสดงตัวอย่างหน้าจอการลงทะเบียนข้อมูลบัตรเครดิต

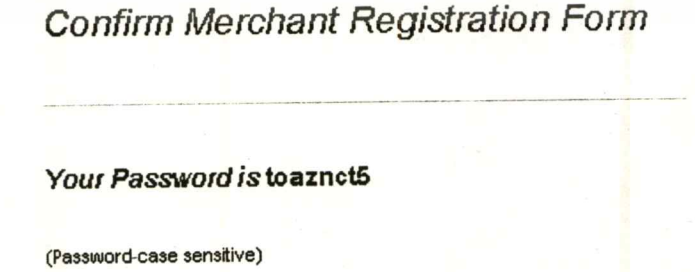
รูปที่ 4.11 แสดงตัวอย่างหน้าจอรหัสผ่านของเจ้าของบัตรเครดิต

4.3.2 การลงทะเบียนข้อมูลร้านค้า

ร้านค้าจะลงทะเบียนข้อมูลส่วนตัวกับบริษัทบัตรเครดิตดังรูปที่ 4.12 โปรแกรมในส่วนการลงทะเบียนนี้จะทำการตรวจสอบข้อมูลของร้านค้าว่ามีอยู่หรือไม่ ถ้าไม่มีจะทำการบันทึกข้อมูลนั้นและสร้างรหัสผ่านให้กับร้านค้าดังรูปที่ 4.13 เพื่อใช้ในการลงทะเบียน Public Key ของร้านค้ากับบริษัทบัตรเครดิตต่อไป



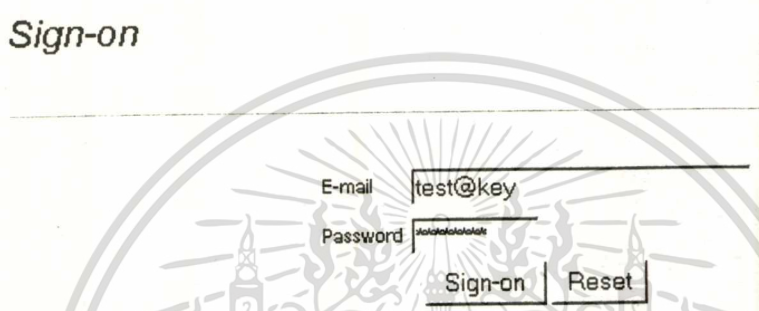
รูปที่ 4.12 แสดงตัวอย่างหน้าจอการลงทะเบียนข้อมูลร้านค้า



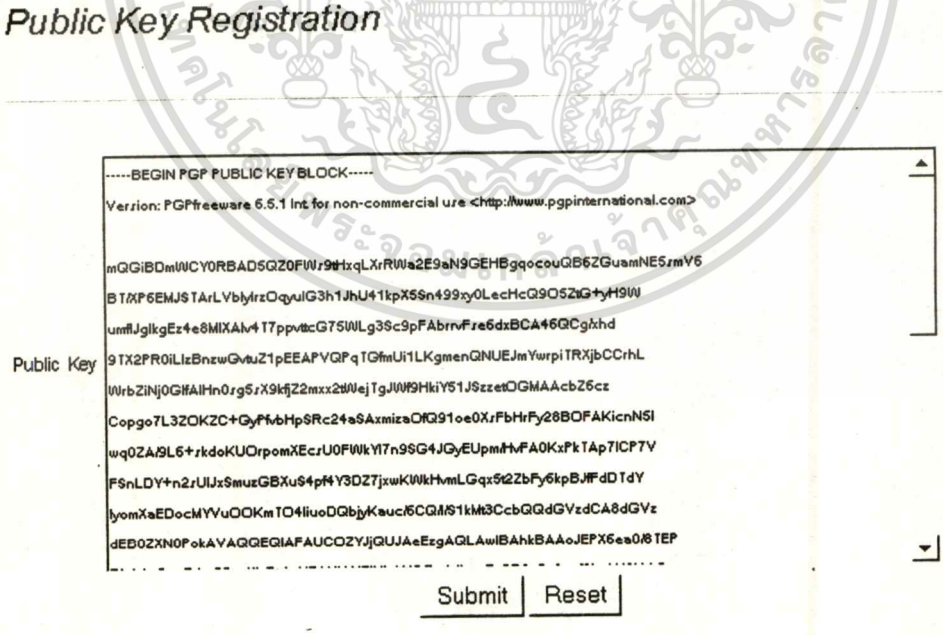
รูปที่ 4.13 แสดงตัวอย่างหน้าจอรหัสผ่านของร้านค้า

4.3.3 การลงทะเบียน Public Key

ก่อนที่จะทำการลงทะเบียน Public Key ทั้งผู้ถือบัตรเครดิตและร้านค้าจะต้อง Sign-on เข้าสู่ระบบด้วย E-mail และรหัสผ่านที่ได้รับจากบริษัทบัตรเครดิตดังรูปที่ 4.14 ถ้าข้อมูลที่ Sign-on ถูกต้องเจ้าของบัตรเครดิตและร้านค้าจะใส่ Public Key ของตนเองดังรูปที่ 4.15 และโปรแกรมในส่วนนี้จะทำการ Import Public Key นี้ลงใน PGPkeys ของบริษัทบัตรเครดิต



รูปที่ 4.14 แสดงตัวอย่างหน้าจอการ Sign-on เพื่อลงทะเบียน Public Key



รูปที่ 4.15 แสดงตัวอย่างหน้าจอการลงทะเบียน Public Key

4.3.4 การ Download Public Key ของบริษัทบัตรเครดิต

ผู้ถือบัตรเครดิตและร้านค้าจะทำการ Download Public Key ของบริษัทบัตรเครดิตมาติดตั้งที่เครื่องของตัวเองเพื่อใช้ในการเข้ารหัสข้อมูลที่ส่งให้กับบริษัทบัตรเครดิต เป็นการป้องกันข้อมูลไม่ให้บุคคลอื่นสามารถเห็นข้มูลได้นอกจากบริษัทบัตรเครดิต

4.4 การชำระค่าสินค้าด้วยหมายเลขบัตรเครดิต

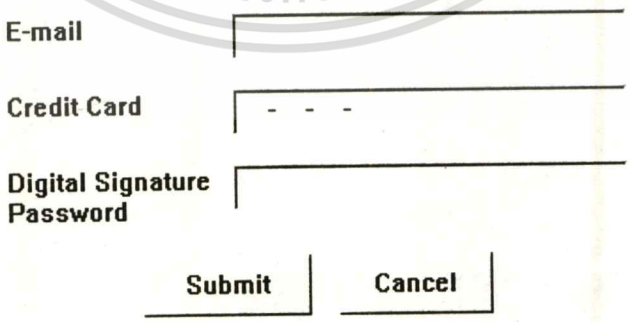
ในการชำระค่าสินค้าด้วยหมายเลขบัตรเครดิตนั้นเครื่องคอมพิวเตอร์ในโครงการนี้ต้องทำการติดตั้งซอฟต์แวร์ PGP เพื่อใช้ในการเข้ารหัสและถอดรหัสข้อมูล โดย Key ที่นำมาใช้จะถูกเก็บอยู่ใน PGPkeys การเข้าถึง Key เหล่านั้นสามารถทำได้โดยผ่านซอฟต์แวร์ SPGP (Simple PGP DLL) ซึ่งเป็น Library ที่ช่วยในการเรียกใช้งาน Key ที่เก็บอยู่ใน PGPkeys

การชำระค่าสินค้าด้วยหมายเลขบัตรเครดิตในโครงการนี้ ประกอบด้วยขั้นตอนการทำงาน 3 ขั้นตอนคือ

1. การทำงานในส่วนของผู้ซื้อสินค้า
2. การทำงานในส่วนของร้านค้า
3. การทำงานในส่วนของบริษัทบัตรเครดิต

4.4.1 การทำงานในส่วนของผู้ซื้อสินค้า

เมื่อผู้ซื้อเลือกซื้อสินค้าที่ต้องการได้แล้ว ผู้ซื้อจะต้องใส่ข้อมูลที่จะนำไปใช้ในการเข้ารหัสซึ่งประกอบด้วย E-mail Address ของผู้ซื้อ หมายเลขบัตรเครดิต และรหัสที่ใช้ร่วมกับ Private Key ในการทำลายเซ็นดิจิตอล ดังรูปที่ 4.17



รูปที่ 4.16 แสดงหน้าจอการใส่ข้อมูลสั่งซื้อสินค้า

ข้อมูลจากการเลือกซื้อสินค้าและข้อมูลที่ผู้ซื้อใส่มานั้นจะถูกเข้ารหัสแบบ Public Key Cryptography โดยแบ่งข้อมูลที่ทำการเข้ารหัสเป็น 2 ส่วนคือ

- ข้อมูลการสั่งซื้อสินค้า ประกอบด้วย
  - E-mail Address ของผู้ซื้อ
  - หมายเลขอ้างอิงถึงผู้ซื้อสินค้า
- ข้อมูลการชำระค่าสินค้า ประกอบด้วย
  - หมายเลขบัตรเครดิต
  - จำนวนเงินที่ต้องชำระ

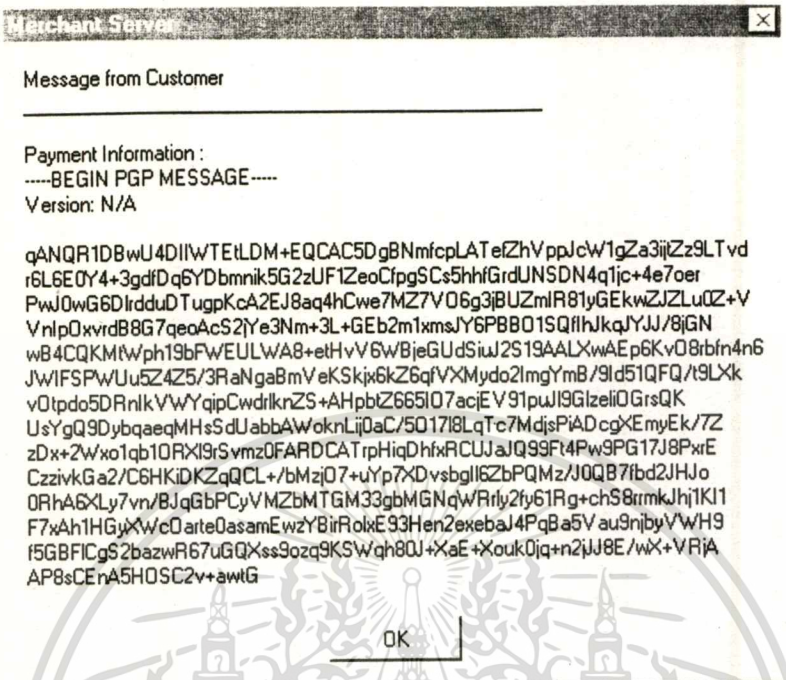
ขั้นตอนการเข้ารหัสข้อมูลในส่วนนี้คือ

1. เข้ารหัสข้อมูลหมายเลขบัตรเครดิตและจำนวนเงินด้วย Public Key ของบริษัทบัตรเครดิตพร้อมทั้งทำลายเซ็นดิจิตอลของผู้ซื้อแนบไปด้วย โดยรูปแบบของข้อมูลเป็นดังรูปที่ 4.17

รูปที่ 4.17 แสดงรูปแบบข้อมูลการชำระค่าสินค้าของผู้ซื้อ

ในขั้นตอนนี้จะมีการตรวจสอบ E-mail Address ที่ผู้ซื้อใส่เข้ามานั้นตรงกับที่ได้ลงนามไว้กับ PGP หรือไม่ ถ้า E-mail ตรงกับที่ลงนามไว้ก็จะสามารถทำลายเซ็นดิจิตอลของผู้ซื้อได้ การทำลายเซ็นดิจิตอลของผู้ซื้อทำโดยการนำข้อมูลหมายเลขบัตรเครดิตมาผ่าน Hash Function ที่เลือกไว้ เพื่อให้ได้ Message Digest แล้วนำ Message Digest นี้ไปเข้ารหัสด้วย Private Key ของผู้ซื้อร่วมกับรหัสที่ใช้ในการทำลายเซ็นดิจิตอลที่ผู้ซื้อใส่มาด้วย และฟังก์ชันที่ใช้ในการเข้ารหัสข้อมูลคือ spgp_encode ใน Library ของ SPGP ตัวอย่างของข้อมูลแสดงดังรูปที่ 4.18

การเข้ารหัสหมายเลขบัตรเครดิตในขั้นตอนนี้เพื่อเป็นการป้องกันหมายเลขบัตรเครดิตจากร้านค้าหรือบุคคลอื่นๆ และการทำลายเซ็นดิจิตอลยังเป็นการยืนยันว่าข้อมูลส่วนนี้มาจากผู้ซื้อจริง



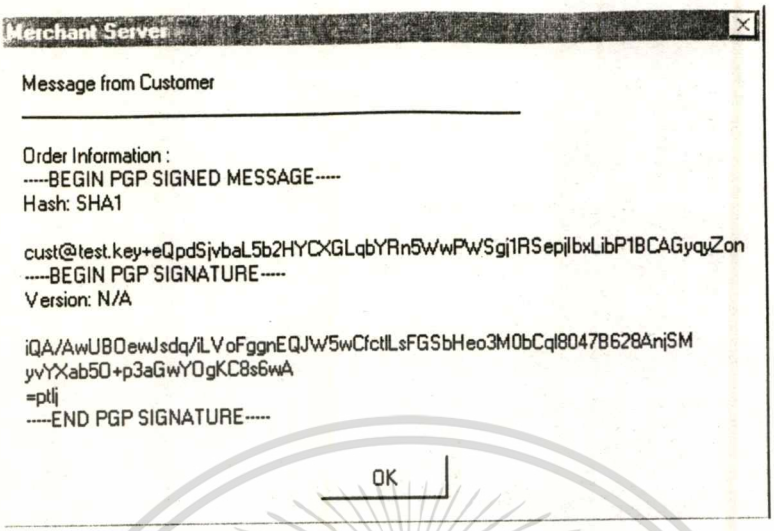
รูปที่ 4.18 แสดงตัวอย่างข้อมูลการชำระค่าสินค้าของผู้ซื้อ

2. ทำลายเซ็นดิจิตอลผู้ซื้อกับข้อมูลการสั่งซื้อสินค้า โดยมีรูปแบบของข้อมูลเป็นดังรูปที่ 4.19

E-mail ผู้ซื้อ+หมายเลขอ้างอิง	ลายเซ็นดิจิตอลผู้ซื้อ

รูปที่ 4.19 แสดงรูปแบบข้อมูลการสั่งซื้อสินค้าของผู้ซื้อ

การทำลายเซ็นดิจิตอลข้อมูลการสั่งซื้อในขั้นตอนนี้เพื่อเป็นการยืนยันว่าข้อมูลการสั่งซื้อนี้มาจากผู้ซื้อจริงไม่ได้ถูกปลอมแปลงมาจากผู้อื่น และฟังก์ชันที่ใช้ในการเข้ารหัสข้อมูลคือ spgp_encode ใน Library ของ SPGP ตัวอย่างของข้อมูลแสดงดังรูปที่ 4.20



รูปที่ 4.20 แสดงตัวอย่างข้อมูลการสั่งซื้อสินค้าของผู้ซื้อ

4.4.2 การทำงานในส่วนของร้านค้า

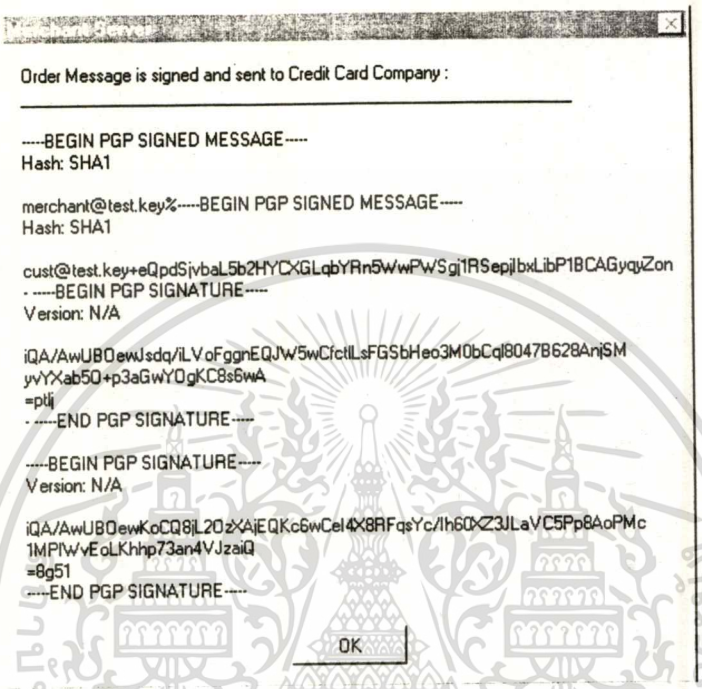
เมื่อร้านค้าได้รับข้อมูลจากผู้ซื้อจะตรวจลายเซ็นดิจิตอลของผู้ซื้อในข้อมูลการสั่งซื้อสินค้ากับบริษัทบัตรเครดิต โดยข้อมูลที่ส่งไปนั้นจะทำการจัดรูปแบบของข้อมูลใหม่พร้อมทั้งแนบลายเซ็นดิจิตอลของร้านค้าที่เข้ารหัสโดย Private Key ของร้านค้าไปกับข้อมูลชุดนี้ด้วย รูปแบบของข้อมูลที่ส่งให้กับบริษัทบัตรเครดิตแสดงดังรูปที่ 4.21

E-mail ร้านค้า	E-mail ผู้ซื้อ+หมายเลขอ้างอิง	ลายเซ็นดิจิตอลผู้ซื้อ	ลายเซ็นดิจิตอลร้านค้า

รูปที่ 4.21 แสดงรูปแบบข้อมูลการสั่งซื้อสินค้าของร้านค้า

ร้านค้าจะส่งข้อมูลชุดนี้ไปตรวจสอบที่บริษัทบัตรเครดิต โดยตัวอย่างของข้อมูลชุดนี้แสดงดังรูปที่ 4.22 เมื่อบริษัทบัตรเครดิตทำการตรวจสอบลายเซ็นดิจิตอลเสร็จจะส่งผลการตรวจสอบพร้อมด้วยข้อมูลสั่งซื้อสินค้ากลับมายังร้านค้า เมื่อร้านค้าได้รับคำตอบกลับจากบริษัทบัตรเครดิตถ้าลายเซ็นดิจิตอลของผู้ซื้อถูกต้องร้านค้าจะส่งข้อมูลการชำระค่าสินค้าให้กับบริษัทบัตรเครดิตเพื่อดำเนินการชำระค่าสินค้า โดยร้านค้าจะทำการจัดรูปแบบข้อมูลการชำระค่าสินค้าใหม่พร้อมทั้งแนบลายเซ็นดิจิตอลของร้านค้าไปด้วย และรูปแบบของข้อมูลการชำระค่าสินค้าของร้านค้าแสดงดังรูปที่ 4.23 และตัวอย่างของข้อมูลแสดงดังรูปที่ 4.24 เมื่อร้านค้าได้รับคำตอบผลการดำเนินการจากบริษัท

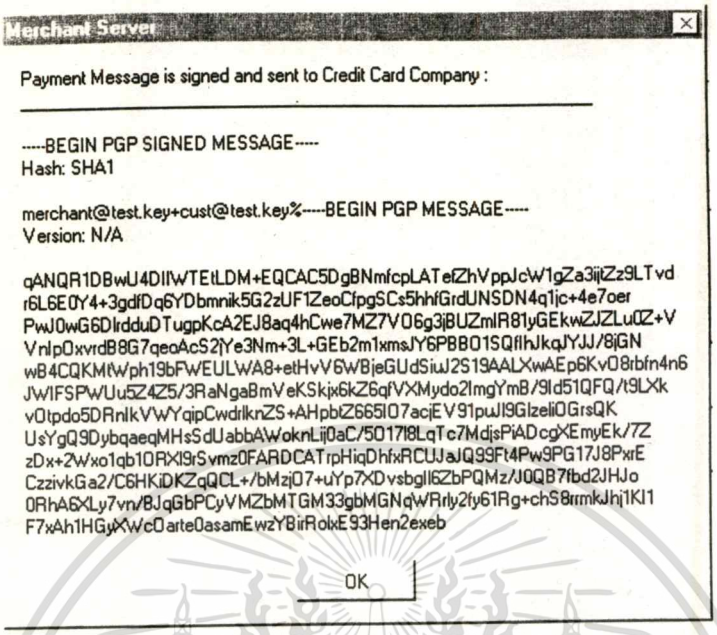
บัตรเครดิตจะส่งผลการดำเนินการนี้ไปยังผู้ซื้อสินค้า ถ้าคำตอบที่ได้บอกถึงการทำรายการที่บริษัทบัตรเครดิตสำเร็จ ร้านค้าจะทำการปรับปรุงข้อมูลการสั่งซื้อสินค้าด้วย



รูปที่ 4.22 แสดงตัวอย่างข้อมูลการสั่งซื้อสินค้าของร้านค้า

E-mailร้านค้า+E-mail ผู้ซื้อ	หมายเลขบัตรเครดิต+จำนวนเงิน	ลายเซ็นดิจิตอลผู้ซื้อ	ลายเซ็นดิจิตอลผู้ซื้อ

รูปที่ 4.23 แสดงรูปแบบข้อมูลการชำระค่าสินค้าของร้านค้า

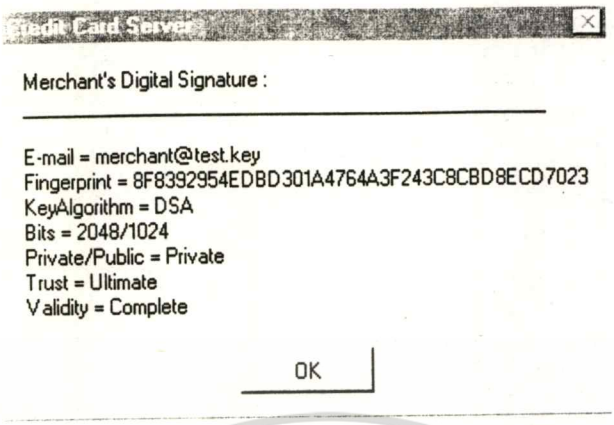


รูปที่ 4.24 แสดงตัวอย่างข้อมูลการชำระค่าสินค้าของร้านค้า

4.4.3 การทำงานในส่วนของบริษัทบัตรเครดิต

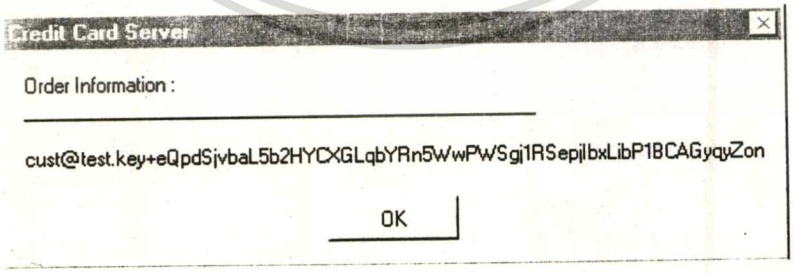
บริษัทบัตรเครดิตจะได้รับข้อมูลจากร้านค้า 2 ชุดคือ ข้อมูลการสั่งซื้อสินค้าและข้อมูลการชำระค่าสินค้า โดยขั้นตอนในการทำงานกับข้อมูลแต่ละชุดเป็นดังนี้

1. บริษัทบัตรเครดิตได้รับข้อมูลการสั่งซื้อสินค้าจากร้านค้าจะถอดรหัสลายเซ็นดิจิตอลของร้านค้าด้วย Public Key ของร้านค้า โดยข้อมูลลายเซ็นดิจิตอลที่ได้แสดงดังรูปที่ 4.25 และทำการตรวจสอบข้อมูลลายเซ็นดิจิตอลที่ได้กับ E-mail Address ของร้านค้าที่แนบมากับข้อมูลชุดนี้ว่าตรงกันหรือไม่ ถ้าข้อมูลถูกต้องบริษัทบัตรเครดิตจะทำการถอดรหัสลายเซ็นดิจิตอลของผู้ซื้อด้วย Public Key ของผู้ซื้อ โดยข้อมูลลายเซ็นดิจิตอลที่ได้แสดงดังรูปที่ 4.26 พร้อมทั้งได้ข้อมูลการสั่งซื้อแสดงดังรูปที่ 4.27 บริษัทบัตรเครดิตจะทำการตรวจสอบลายเซ็นดิจิตอลของผู้ซื้อกับ E-mail Address ของผู้ซื้อที่ปรากฏอยู่ในข้อมูลการสั่งซื้อ และแจ้งผลการตรวจสอบพร้อมทั้งข้อมูลการสั่งซื้อกลับไปยังร้านค้า



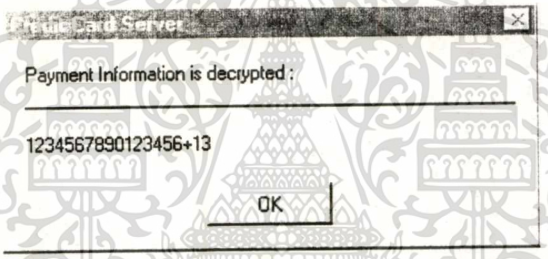
รูปที่ 4.25 แสดงตัวอย่างข้อมูลลายเซ็นดิจิตอลของร้านค้า

รูปที่ 4.26 แสดงตัวอย่างข้อมูลลายเซ็นดิจิตอลของผู้ซื้อ



รูปที่ 4:27 แสดงตัวอย่างข้อมูลการสั่งซื้อสินค้า

2. บริษัทบัตรเครดิตได้รับข้อมูลการชำระค่าสินค้าจากร้านค้าจะถอดรหัสลายเซ็นดิจิตอลของร้านค้าด้วย Public Key ของร้านค้า และทำการตรวจสอบข้อมูลลายเซ็นดิจิตอลที่ได้กับ E-mail Address ของร้านค้าที่แนบมากับข้อมูลชุดนี้ว่าตรงกันหรือไม่ ถ้าข้อมูลถูกต้องบริษัทบัตรเครดิตจะทำการถอดรหัสลายเซ็นดิจิตอลของผู้ซื้อด้วย Public Key ของผู้ซื้อ และทำการตรวจสอบข้อมูลลายเซ็นดิจิตอลที่ได้กับ E-mail Address ของผู้ซื้อที่ร้านค้าแนบมากับข้อมูลชุดนี้ว่าตรงกันหรือไม่ ถ้าข้อมูลถูกต้องบริษัทบัตรเครดิตจะทำการถอดรหัสข้อมูลการชำระค่าสินค้าด้วย Private Key ของบริษัทบัตรเครดิต โดยข้อมูลที่ได้แสดงดังรูปที่ 4.28 และทำการตรวจสอบหมายเลขบัตรเครดิตและ E-mail Address ว่าตรงกับที่ได้ลงทะเบียนไว้กับบริษัทบัตรเครดิตหรือไม่ ถ้าข้อมูลตรงกันบริษัทบัตรเครดิตจะทำการบันทึกข้อมูลการชะรำค่าสินค้านี้ไว้และส่งผลการทำรายการกลับไปยังร้านค้าเพื่อแจ้งกับผู้ซื้อต่อไป



รูปที่ 4.28 แสดงตัวอย่างข้อมูลการชำระค่าสินค้า

จากการทำงานของโปรแกรมทั้งหมดสามารถสรุปเป็น Flow การทำงาน ได้ดังนี้

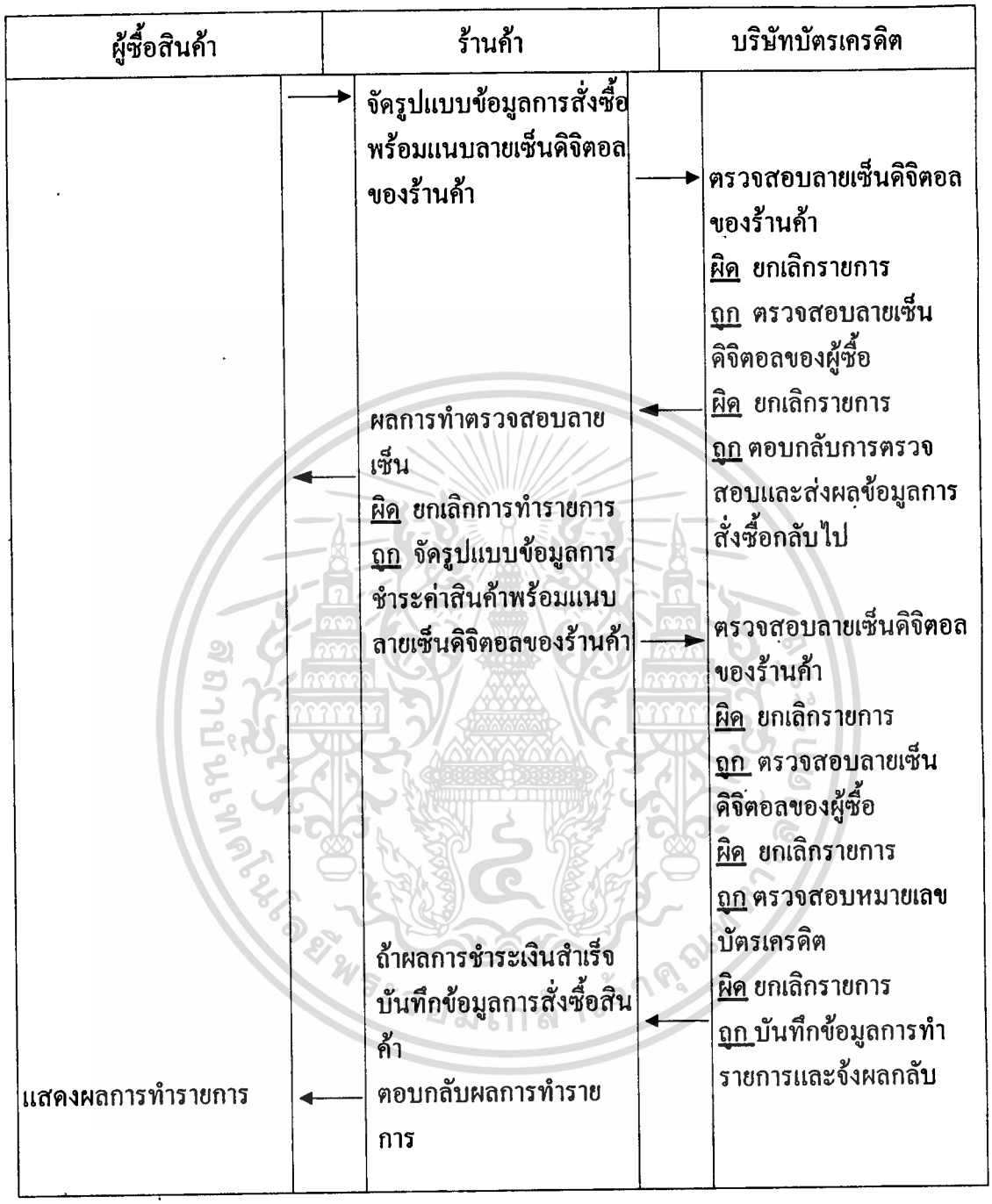
1. Flow การลงทะเบียน Public Key

ผู้ซื้อสินค้า		ร้านค้า		บริษัทบัตรเครดิต
ข้อมูลแบ่งเป็น 2 ส่วนคือ - หมายเลขบัตรเครดิตและจำนวนเงินที่ถูกเข้ารหัสด้วย Public Key ของบริษัทบัตรเครดิต และทำลายเซ็นดิจิตอลด้วย Private Key ของผู้ซื้อ - ข้อมูลการสั่งซื้อสินค้าที่มีลายเซ็นดิจิตอลของร้านค้าแนบไปด้วย				

ตารางที่ 4.2 แสดง Flow การลงทะเบียน Public Key

2 Flow การซื้อสินค้าด้วยหมายเลขบัตรเครดิต

การทำงานในส่วนการซื้อสินค้าด้วยหมายเลขบัตรเครดิตจะกล่าวถึงเฉพาะข้อมูลที่รับส่งระหว่างผู้ซื้อสินค้า ร้านค้า และบริษัทบัตรเครดิต



ตารางที่ 4.3 แสดง Flow การซื้อสินค้าด้วยหมายเลขบัตรเครดิต

จากการพัฒนาระบบสามารถแบ่งโปรแกรมการทำงานได้เป็น 2 ส่วนคือ

1. โปรแกรมที่พัฒนาขึ้นเอง ได้แก่
   - การลงทะเบียนข้อมูลผู้ถือบัตร
   - การลงทะเบียนร้านค้า
   - การ Download Public Key ของบริษัทบัตรเครดิต
   - การขายสินค้าของร้านค้า
   - การสั่งซื้อสินค้าของผู้ซื้อ
   - การตรวจสอบลายเซ็นดิจิตอล
   - การชำระเงินด้วยบัตรเครดิต
2. โปรแกรมที่เรียกใช้งาน SPGP Library
   - การ Import Public Key ของผู้ถือบัตรและร้านค้าเข้าสู่ PGPkeys ของบริษัทบัตรเครดิต
   - การเข้ารหัสข้อมูลด้วย Public Key
   - การถอดรหัสข้อมูลด้วย Private Key
   - การทำลายเซ็นดิจิตอล

4.4.4 การนำระบบไปใช้งาน

การใช้งานระบบนี้จะต้องทำการติดตั้งซอฟต์แวร์ PGP และ SPGP Library ในทุกเครื่องที่ใช้งาน และการติดตั้งโปรแกรมในระบบนี้แบ่งได้เป็น 3 ส่วนคือ

1. โปรแกรมการสั่งซื้อสินค้าในส่วนของผู้ซื้อซึ่งเป็นโปรแกรม ActiveX Control
2. โปรแกรมในส่วนการทำงานของร้านค้าในการจัดรูปแบบของข้อมูลที่ส่งให้กับบริษัทบัตรเครดิต
3. โปรแกรมในส่วนการทำงานของบริษัทบัตรเครดิตซึ่งประกอบด้วยโปรแกรมในส่วนการลงทะเบียนที่เป็น WEB Page และโปรแกรมในการชำระค่าสินค้าโดยตัดบัตรเครดิตซึ่งเป็นโปรแกรม ActiveX EXE

4.5 ฐานข้อมูลในระบบ

ระบบฐานข้อมูลที่ใช้ในการพัฒนาระบบนี้คือ Microsoft Access โดยแบ่งข้อมูลที่จัดเก็บออกเป็น 2 ส่วนคือ

1. ข้อมูลที่จัดเก็บที่ร้านค้า ประกอบด้วยข้อมูลการสั่งซื้อสินค้า
2. ข้อมูลที่จัดเก็บที่บริษัทบัตรเครดิต ประกอบด้วย
   - ข้อมูลผู้ถือบัตร ประกอบด้วย ข้อมูลส่วนตัวและหมายเลขบัตรเครดิต

- ข้อมูลส่วนตัวของร้านค้า
- ข้อมูล User ในระบบ ประกอบด้วย E-mail Address ของผู้ถือบัตรและร้านค้า และรหัสผ่านที่ใช้ในการ Sign-on เข้าสู่ระบบการลงทะเบียน Public Key
- ข้อมูลการชำระค่าสินค้า

การเข้าถึงข้อมูลของบริษัทบัตรเครดิตจะเข้าถึงด้วย E-mail Address ของผู้ใช้

4.6 ข้อแตกต่างระหว่าง SET และระบบที่พัฒนา

ระบบ SET และระบบที่พัฒนานี้มีความแตกต่างในการทำงานในเรื่องต่างๆ ดังนี้คือ

1. การเข้ารหัสข้อมูลด้วย Key
   - ระบบ SET จะทำการสร้าง Secret Key ที่ได้จากการสุ่มมาใช้ในการเข้ารหัสข้อมูล
   - ระบบที่พัฒนาใช้ Public Key ในการเข้ารหัสข้อมูล
2. การใช้งาน Public และ Private Key
   - ระบบ SET จะสร้าง Public และ Private Key ขึ้นมา 2 ชุดคือ Signature Key เพื่อใช้ในการทำลายเซ็นดิจิตอลและ Exchange Key เพื่อใช้ในการเข้ารหัสและถอดรหัส Secret Key
   - ระบบที่พัฒนามี Public และ Private Key 1 ชุดสำหรับการเข้ารหัสและถอดรหัสข้อมูลและทำลายเซ็นดิจิตอล
3. การทำลายเซ็นดิจิตอลสำหรับการสั่งซื้อสินค้าและชำระค่าสินค้า
   - ระบบ SET จะสร้าง Dual Signature สำหรับการทำลายเซ็นดิจิตอลในข้อมูลการสั่งซื้อสินค้าและข้อมูลการชำระค่าสินค้า
   - ระบบที่พัฒนาจะสร้างลายเซ็นดิจิตอลแบบที่ใช้ทั่วไปสำหรับข้อมูลการสั่งซื้อสินค้าและข้อมูลการชำระค่าสินค้า
4. ขั้นตอนการทำงาน
   - ระบบ SET มีขั้นตอนการทำงานมากและซับซ้อนในการสั่งซื้อสินค้าและชำระค่าสินค้า
   - ระบบที่พัฒนามีขั้นตอนการทำงานน้อยกว่า SET ในการสั่งซื้อสินค้าและชำระค่าสินค้า
5. การตรวจสอบลายเซ็นดิจิตอล
   - ระบบ SET สามารถตรวจสอบลายเซ็นดิจิตอลได้ที่เครื่องของผู้รับ เพราะมีการแนบใบรับรองดิจิตอลที่มี Public Key สำหรับใช้ถอดรหัสลายเซ็นดิจิตอลไปด้วย
   - ระบบที่พัฒนาไม่สามารถตรวจสอบลายเซ็นดิจิตอลได้ที่เครื่องของผู้รับ เนื่องจากผู้ส่งไม่สามารถส่ง Public Key ไปให้กับผู้รับได้ เพราะติดข้อจำกัดในการใช้งานซอฟต์แวร์ PGP

6. การลงทะเบียนของร้านค้าและผู้ถือบัตรเครดิต
   - ระบบ SET ผู้ถือบัตรและร้านค้าจะลงทะเบียนกับ CA
   - ระบบที่พัฒนาผู้ถือบัตรและร้านค้าต้องลงทะเบียนกับบริษัทบัตรเครดิต
7. การติดต่อระหว่างร้านค้ากับบริษัทบัตรเครดิต

ระบบ SET จะทำการติดต่อแบบ Public Network

ระบบที่พัฒนาติดต่อแบบ Private Network โดย Protocol ที่ใช้ในการติดต่อคือ DCOM

4.7 ข้อจำกัดของระบบที่พัฒนา

ในการพัฒนาระบบนี้มีข้อจำกัดเนื่องมาจากระบบที่พัฒนาได้นำซอฟต์แวร์ PGP มาใช้งาน ซึ่งการทำงานบางส่วนของ PGP ไม่สามารถทำได้แบบอัตโนมัติด้วยโปรแกรม ต้องอาศัยบุคคลในการทำงาน เช่น การ Import Public Key เข้า PGPkeys นั้น หลังจากการ Import จะต้องมีบุคคลมาลงนามใน Public Key นั้นด้วย รวมทั้งการ Export Public Key ที่ไม่สามารถทำได้แบบอัตโนมัติด้วยโปรแกรม ดังนั้นข้อมูลที่ติดต่อในระบบจึงไม่สามารถแนบ Public Key ของผู้ส่งไปพร้อมกับข้อมูลได้ ผู้รับจึงไม่สามารถตรวจสอบลายเซ็นดิจิตอลของผู้ส่ง ต้องทำการตรวจสอบที่บริษัทบัตรเครดิตแทน

บทที่ 5

สรุปผลโครงการและการพัฒนาระบบ

การศึกษาและวิจัยในโครงการนี้นำมาตรฐานและขั้นตอนการชำระค่าสินค้าบนอินเตอร์เน็ตของระบบ SET (Secure Electronic Transaction) มาใช้อ้างอิงในการพัฒนาโปรแกรมการชำระค่าสินค้าด้วยบัตรเครดิต และนำซอฟต์แวร์ PGP (Pretty Good Privacy) ซึ่งเป็นซอฟต์แวร์ที่ไม่เสียค่าใช้จ่ายมาใช้ในการสร้าง Private Key และ Public Key พร้อมทั้งฟังก์ชันการเข้ารหัสและถอดรหัสข้อมูลด้วย Public Key หรือ Private Key และการทำลายเซ็นดิจิตอลจาก Private Key จาก Library SPGP

การพัฒนาโปรแกรมในการชำระค่าสินค้าด้วยบัตรเครดิตบนอินเตอร์เน็ตนี้มีผู้เกี่ยวข้องด้วยกัน 3 ฝ่ายคือ ผู้ซื้อสินค้าหรือเจ้าของบัตรเครดิต ร้านค้า และบริษัทบัตรเครดิตที่ทำหน้าที่เหมือนเป็น Certificate Authority (CA) และแบ่งการทำงานออกเป็น 3 ส่วน คือ

1. การสร้าง Private Key และ Public Key โดยซอฟต์แวร์ PGP
2. การลงทะเบียนของผู้ถือบัตรเครดิตและร้านค้ากับบริษัทบัตรเครดิต
3. การชำระค่าสินค้าด้วยบัตรเครดิต

ระบบที่พัฒนานี้ใช้หลักการทำงานของ SET เป็นมาตรฐานในการทำงาน แต่มีการทำงานบางส่วนที่ไม่สามารถเป็นไปตามมาตรฐานของ SET ได้เนื่องจากติดข้อจำกัดของซอฟต์แวร์ที่นำมาใช้ในการจัดการ Key คือ PGP เช่น การ Import และ Export Key แบบ Automatic ดังนั้น สิ่งที่ควรจะปรับปรุงในการพัฒนาระบบนี้ต่อไปคือ ข้อมูลที่ทำการติดต่อระหว่างผู้รับและผู้ส่งแต่ละรายควรมีการแนบ Public Key ที่ใช้ในการตรวจสอบลายเซ็นดิจิตอล เพราะในระบบนี้การตรวจสอบลายเซ็นดิจิตอลจะต้องทำที่บริษัทบัตรเครดิตเท่านั้น เนื่องจาก Public Key ทั้งหมดในระบบจะถูกเก็บอยู่ที่บริษัทบัตรเครดิต ซึ่งทำให้เสียเวลาในการทำงานมากขึ้นด้วย

การชำระค่าสินค้าจากระบบที่พัฒนาขึ้นเมื่อเปรียบเทียบกับระบบความปลอดภัยอื่นๆ เช่น SSL ระบบที่พัฒนานี้มีความปลอดภัยที่ดีกว่า เพราะใช้ Key ในการเข้ารหัสและถอดรหัสเป็นคนละ Key กัน ซึ่งเป็นการยากที่จะรู้ Key ที่ใช้ในการถอดรหัสได้ แต่ SSL ใช้ Key เดียวกับในการเข้าและถอดรหัสซึ่งมีโอกาสที่จะรู้ Key ที่ใช้ได้มากกว่า

บรรณานุกรม

Bernstein, T. et. al. 1996. INTERNET SECURITY FOR BUSINESS John Wiley & Son Inc.

Ghosh, A. K. 1998. E-COMMERCE SECURITY Weak Links, Best Defenses John Wiley & Son Inc.

Heller, Steve. 2000. SPGP : A Simple PGP DLL [On-line] Available : http://www.oz.net/~srheller/privacy/pgp/spgp/spgp.htm

Kosiur, D. 1997. Understanding Electronic Commerce Washington : Microsoft Press

Network Associates International. 1999. An Introduction to Cryptography [On-line] Available : HTTP://www.pgpi.org/doc/6.5

Network Associates International. 1999. PGP Freeware for Windows 95, Windows 98, and Windows NT User's Guide Version 6.5 [On-line] Available : HTTP://www.pgpi.org/doc/6.5

Stein, Linboln D. 1997. Web Security A Step-by-Step Reference Guide Massachusetts : Addison Wesley LongMan Inc.

ประวัติผู้เขียน

ชื่อผู้แต่ง	น.ส. บงกชเกษ สุขตระกูล
วันเดือนปีเกิด	8 ตุลาคม 2513
สถานที่เกิด	กรุงเทพมหานคร
วุฒิการศึกษาระดับปริญญาตรี	วิทยาศาสตรบัณฑิต (วิทยาการคอมพิวเตอร์)
สถานที่สำเร็จการศึกษา	คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่
สถานที่ทำงาน	ธนาคารไทยพาณิชย์ จำกัด (มหาชน)