ระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัย

Secured Electronic Financial Data Submission System

โดย

นาย วิษณุ ชวนเกษม

รหัส 41067118

H001681

อาจารย์ที่ปรึกษา

อาจารย์ อัครินทร์ คุณกิตติ

รายงานนี้เป็นส่วนหนึ่งของโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 1 ปีการศึกษา 2543

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	ระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัย
นักศึกษา	นาย วิษณุ ชวนเกษม
อาจารย์ที่ปรึกษา	อาจารย์ อัครินทร์ คุณกิตติ
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2543

บทคัดย่อ

โครงการพัฒนาระบบงานนี้เป็นการพัฒนารูปแบบของการส่งข้อมูลทางการเงินให้อยู่ในรูปอิเล็กทรอนิกส์เพื่อเพิ่มประสิทธิภาพในการส่งข้อมูลได้รวดเร็วและปลอดภัยยิ่งขึ้น โดยข้อมูลจะถูกส่งข้ามเครือข่ายเฉพาะด้วยการเชื่อมต่อแบบทางไกลผ่านโมเด็ม (Remote Access Connection) และมีรูปแบบการใช้งานแบบโปรแกรมประยุกต์ผ่าน เวิลด์ ไวด์ เว็บ (Web Application) ซึ่งมีลักษณะการทำงานแบบกระจายและสามารถรองรับการใช้งานจากภูมิภาคต่างๆของประเทศได้ โดยระบบได้มีการประยุกต์ใช้กลไกความปลอดภัยเข้ามารองรับการทำงานในขั้นตอนต่างๆ เริ่มจากการยืนยันผู้เข้าใช้งานด้วยการตรวจสอบใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ที่ผ่านการรับรองแล้วจากนั้นจึงมีการตรวจสอบสิทธิในการใช้งานของผู้ใช้งาน (Access Rights Control) ว่าสามารถส่งข้อมูลแบบใดได้บ้าง ทั้งนี้ในการส่งข้อมูล ระบบจะทำการบีบอัดข้อมูลให้มีขนาดเล็กลงและทำการลงลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) กับข้อมูลด้วย Private Key ของผู้ส่ง ก่อนที่จะทำการเชื่อมต่อกับศูนย์รับข้อมูลปลายทางโดยใช้โปรโตคอล SSL (Secure Sockets Layer) ซึ่งจะทำหน้าที่ในการเข้ารหัสเพื่อรักษาความลับของข้อมูลที่ถูกส่งผ่านเครือข่าย และเมื่อข้อมูลเดินทางมาถึงระบบจะทำการตรวจสอบลายเซ็นอิเล็กทรอนิกส์เพื่อยืนยันความดั้งเดิมของเนื้อข้อมูลและยืนยันว่าข้อมูลนั้นถูกส่งมาจากผู้ส่งข้อมูลที่ผ่านการรับรองแล้ว

Title	Secured Electronic Financial Data Submission System
Student	Mr. Visanu Chuankasem
Advisor	Mr. Akharin Khunkitti
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2000

ABSTRACT

This development project is an effort in improving the financial data submission from a manual process to an electronic submission system. Its purpose is to provide an efficient way in submitting the financial data in a fast and secured manner. The data will be securely submitted through remote access connection using a modem. Web Application methodology is used in developing the system for supporting its use for distributed environment so that users can submit data from locations around the country. The system utilizes numbers of security mechanisms working together to ensure reliable level of security. User authentication is handled by using digital certificate in checking the identity then the system checks access rights control for user's permission. Before submission, the system compresses the data by zipping files and digitally signs the data using sender's private key, then the SSL connection is established for transporting the encrypted data across the network. Finally, when the data arrive, the system verifies the digital signature to confirm the integrity of the data and identity of the sender.

กิตติกรรมประกาศ

ในการศึกษาและพัฒนาระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัยนี้ ผู้จัดทำขอขอบพระคุณ ท่าน อาจารย์ อัครินทร์ คุณกิตติ ที่ได้ให้คำปรึกษาและแนะนำแนวทางในการพัฒนาระบบจนเสร็จสมบูรณ์ และ โครงงานนี้ได้มีผู้เกี่ยวข้อง ที่สนับสนุนและให้ความช่วยเหลือหลายท่าน ดังนี้

- ขอกราบขอบพระคุณ คุณพ่อ คุณแม่ และน้องสาว ที่คอยดูแลเป็นกำลังใจ และสนับสนุนในการทำงานเสมอมา
- ขอขอบคุณเพื่อนๆ IS6 สมทบ ที่คอยช่วยเหลือ ให้คำแนะนำ และถามไถ่ โดยเฉพาะคุณกิตติชัย และ คุณธรรมจักร ที่เป็นเพื่อนร่วมงานและเพื่อนร่วมห้องที่ดีมาตลอด
- ขอขอบคุณพี่ๆน้องๆและเพื่อนๆที่ธนาคารแห่งประเทศไทย โดยเฉพาะพี่ดวงแก้วและทุกคนในทีมจัดการกรรมวิธีพัฒนาระบบงาน ที่ให้กำลังใจ และสนับสนุน ตลอดระยะเวลาของการศึกษา
- ขอขอบคุณ น้องอุ๋ย ที่คอยช่วยเหลือ สนับสนุน และ เป็นกำลังใจให้เสมอมา

วิษณุ ชวนเกษม

20 ตุลาคม 2543

สารบัญ

สารบัญตาราง

สารบัญภาพ

หน้า

ภาพที่

บทที่ 1
บทนำ

1.1 ความเป็นมาของโครงงาน

สถาบันการเงินมีภาระหน้าที่ในการนำส่งแบบฟอร์มรายงานทางการเงินต่างๆมายังองค์กรของรัฐที่ทำหน้าที่ควบคุมดูแลธุรกรรมทางการเงินตามคาบเวลาที่กำหนด พร้อมเอกสารแนบ หรือข้อมูลเฉพาะต่างๆ ที่ทางภาครัฐขอความร่วมมือในการนำส่งให้ ซึ่งส่วนใหญ่การนำส่งข้อมูลต่างๆ นั้นจะอยู่ในรูปของสื่อกระดาษ และมีบางส่วนที่ปรับให้มีการนำส่งทางด้านสื่อ อิเล็กทรอนิกส์ เช่น Magnetic Tape หรือ Diskette เป็นต้น เนื่องด้วยตัวข้อมูลนั้นเป็นข้อมูลทางการเงินที่มีความสำคัญ ซึ่งจำเป็นที่จะต้องอาศัยความถูกต้องของเนื้อข้อมูล ความรวดเร็วในการนำส่งและประมวลผล รวมถึงความปลอดภัยของตัวข้อมูลในช่วงของการนำส่งด้วย ซึ่งในลักษณะการทำงานแบบเดิมนั้น ส่วนใหญ่แล้วข้อมูลที่ส่งเข้ามาจะอยู่ในรูปของสื่อกระดาษ โดยทางแต่ละสถาบันการเงินจัดเตรียมขึ้นแล้วนำส่งผ่านผู้นำส่งเอกสารซึ่งเดินทางโดยยานพาหนะ เช่น จักรยานยนต์ มาส่งเอกสารให้กับทางเจ้าหน้าที่เพื่อรับแบบรายงานดังกล่าวไปพิมพ์ป้อนเข้าสู่ระบบเพื่อการนำไปใช้ต่อไป

จากรูปแบบการทำงานดังที่กล่าวมานั้น ก่อให้เกิดปัญหาอยู่หลายประการ กล่าวคือความไม่คล่องตัวของการส่งต่อของข้อมูล เนื่องจากถ้ากรณีที่เป็นสื่อกระดาษ ซึ่งเป็นรูปแบบส่วนใหญ่ จะต้องมีการป้อนข้อมูลจากสื่อกระดาษเข้าสู่ระบบเป็นประจำในปริมาณที่ค่อนข้างมากและใช้เวลานานในการนำเข้าสู่ระบบ อีกทั้งในกรณีที่มีความจำเป็นที่จะแก้ไขข้อมูลที่ส่งไปแล้วนั้นจะทำได้ไม่สะดวกนักเนื่องจากต้องทำการนำส่งข้อมูลที่แก้ไขมาใหม่แล้วจึงให้เจ้าหน้าที่ป้อนเข้าระบบ ส่วนการจัดส่งด้วยผู้ส่งเอกสารนั้น อาจมีผลให้เกิดการล่าช้า หรือ สูญหายของข้อมูลได้ ซึ่งจะส่งผลกระทบถึงเรื่องความปลอดภัยของตัวข้อมูล อีกทั้งในการส่งข้อมูลด้วยผู้ส่งเอกสารโดยใช้สื่อกระดาษนี้ จะยังผลให้เกิดการสิ้นเปลืองทรัพยากรต่างๆ เช่น น้ำมันเชื้อเพลิงในการขนส่ง และกระดาษสำหรับการพิมพ์รายงานที่ถูกใช้ไปอย่างมากมาย

ดังนั้นจึงได้มีการพัฒนาระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัยขึ้นมาเพื่อเพิ่มประสิทธิภาพในการส่งข้อมูลจากสถาบันการเงินมายังศูนย์รับข้อมูลในลักษณะ Online โดยมีกลไกความปลอดภัยเข้ามารองรับ ความลับของข้อมูล ความปลอดภัยของเครือข่าย และ การควบคุมการเข้าใช้งานของเจ้าหน้าที่ที่ได้รับอนุญาติให้ส่งและรับข้อมูล

1.2 วัตถุประสงค์

1. เพื่อพัฒนาระบบการส่งข้อมูลทางการเงินผ่านเครือข่าย จากสถาบันการเงินมายังศูนย์รับข้อมูล ด้วยความสะดวกรวดเร็วและมีประสิทธิภาพ
2. เพื่อนำกลไกทางด้านความปลอดภัยมาประยุกต์ใช้กับระบบการส่งข้อมูลผ่านเครือข่าย เพื่อความปลอดภัยของข้อมูล และการเข้าใช้ระบบงาน
3. เพื่อพัฒนาให้สามารถติดตามสถานะของข้อมูลที่ส่งว่าได้ถึงจุดปลายทางดังที่ต้องการ

1.3 ขอบเขตในการพัฒนาระบบงาน

การพัฒนาระบบงานมีขอบเขตที่ครอบคลุมส่วนต่างๆของระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัย ดังนี้

1. การนำส่งข้อมูล / แบบรายงานจากสถาบันการเงิน โดยจะเป็นการนำส่งในรูปสื่ออิเล็กทรอนิกส์ผ่านการเชื่อมต่อเข้าเครือข่ายโดยตรงมาที่ศูนย์รับข้อมูล
2. การยืนยันและรับรองตัวบุคคล โดยผู้ใช้งานทุกคนในระบบจะข้องผ่านการรับรองตัวบุคคลจากทางธนาคารแห่งประเทศไทยว่าเป็นบุคคลที่สามารถทำการส่งข้อมูล / แบบรายงานของสถาบันการเงินที่สังกัด เพื่อใช้ในการยืนยันบุคคลในขั้นตอนการใช้งานระบบ
3. การกำหนดสิทธิในการใช้งานระบบ โดยจะเป็นการกำหนดสิทธิการทำงานต่างๆในระบบให้กับผู้ใช้งานที่ผ่านการรับรองแล้ว
4. การตรวจสอบสถานะของข้อมูลที่นำส่ง โดยจะเป็นการแสดงสถานะปัจจุบันของข้อมูลที่ส่งผ่านระบบเพื่อติดตามผลการตรวจสอบของข้อมูล / แบบรายงาน ที่ได้ส่งไป
5. การรักษาความปลอดภัยของข้อมูล โดยจะเป็นการลงลายเซ็นอิเล็กทรอนิกส์ และเข้ารหัสข้อมูลระหว่างการนำส่งเพื่อรักษาความลับ และ ความถูกต้องของข้อมูล
6. การเข้าใช้ระบบ โดยจะเป็นลักษณะของการใช้งานผ่านเว็บ (Web Application) เพื่อความสะดวก และ ง่ายต่อการใช้งาน

1.4 หลักการในการพัฒนาระบบงาน

ในการพัฒนาระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัยให้มีประสิทธิภาพในการทำงานสูงสุด จึงจำเป็นที่จะต้องศึกษาหลักการและทฤษฎีต่างๆ ดังนี้

1. ศึกษาหลักการและการทำงานของกลไกความปลอดภัยที่เกี่ยวข้องในระบบการทำงานแบบกระจาย (Distributed Information System)

2. ศึกษาหลักการและการทำงานของ Web Application โดยรวมถึงการเชื่อมต่อระบบฐานข้อมูลผ่านเว็บ โดยใช้เทคโนโลยี ASP (Active Server Page) ในการพัฒนา
3. ศึกษาหลักการและการทำงานของ Remote Access Service
4. ศึกษาเทคนิคและหลักการในการวิเคราะห์และออกแบบระบบ

1.5 องค์ประกอบของระบบงาน

ระบบจะประกอบไปด้วยองค์ประกอบดังนี้คือ

- เครื่องคอมพิวเตอร์ Server เป็นระบบปฏิบัติการ Windows 2000 Advance Server โดยมีการติดตั้ง Service ต่อไปนี้
  - Internet Information Service ซึ่งเป็นส่วนที่ให้บริการในการทำงานของ Web Application ในระบบ ซึ่งจะใช้ Visual Interdev 6.0 ในการพัฒนา Application ดังกล่าว
  - Certificate Service ซึ่งเป็นส่วนที่ให้บริการในการทำงานของ Certificate Authority และทำการจัดการ Certificate ของผู้ใช้งานในระบบ
  - Remote Access Service ซึ่งเป็นส่วนที่ให้บริการในการเชื่อมต่อ (Dial Up) ผู้ใช้งานเข้ากับทาง Server
  - ระบบฐานข้อมูลที่ใช้เป็น RDBMS (Relational Database Management System) โดยใช้ซอฟต์แวร์การจัดการฐานข้อมูล Microsoft SQL Server โดยใช้เก็บฐานข้อมูล ของผู้ใช้งาน ระดับสิทธิการใช้งาน สถานะของข้อมูล และ ประวัติของการส่งข้อมูลต่างๆ
  - Server Component ต่างๆที่พัฒนาขึ้นมาเพื่อใช้ในตรวจสอบ Digital Signature กับข้อมูลที่ส่ง และ Unzip ข้อมูลที่ส่งมา
- เครื่องคอมพิวเตอร์ Client เป็นระบบปฏิบัติการ Windows 2000 Professional โดยมีการติดตั้ง Software และ Hardware ดังนี้
  - โปรแกรม Web Browser ซึ่งใช้เรียก Web Application โดยในที่นี้จะใช้ Internet Explorer ซึ่งมีความสามารถทำ SSL ได้ที่ระดับ 128-bit
  - โปรแกรมสำหรับทำการเชื่อมต่อ (Dial-Up) มาที่ Server เพื่อเรียกใช้ระบบงาน
  - Client Component ต่างๆที่พัฒนาขึ้นมาเพื่อใช้ในการส่งข้อมูล เลือกไฟล์ และ ทำการลง Digital Signature กับข้อมูลที่ส่ง เป็นต้น

1.6 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับจากการพัฒนาระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัยสามารถจำแนกออกเป็น 3 หัวข้อหลัก ๆ ดังนี้

1. ประโยชน์ต่อผู้ทำการพัฒนาระบบ
    - ได้พัฒนาความรู้และความสามารถในการวิเคราะห์ ออกแบบ และพัฒนาระบบ
    - ทำให้มีความรู้หลากหลายและกว้างขวางมากขึ้น ทั้งในด้านคอมพิวเตอร์และการทำงาน
    - เพื่อประโยชน์ต่อการทำงานในอนาคต
2. ประโยชน์ต่อองค์กร
    - ลดความล่าช้าในการทำงาน และลดความซ้ำซ้อนของข้อมูลในระบบ
    - ได้ระบบที่ช่วยให้การทำงานของการส่งข้อมูลทางการเงินมีประสิทธิภาพมากขึ้น ทั้งในด้านการปฏิบัติงานและด้านบริหาร
    - เป็นแนวทางในการปรับปรุงขั้นตอนการทำงานในระบบเดิมให้มีประสิทธิภาพมากยิ่งขึ้น
3. ประโยชน์ทั่วไป
    - สามารถนำไปศึกษาเพื่อเป็นแนวทางในการพัฒนาระบบงานอื่น ๆ ได้ต่อไปในอนาคต

บทที่ 2
หลักการและทฤษฎี

2.1 ระบบสารสนเทศแบบกระจาย (Distributed Information System)

ในปัจจุบัน องค์กรส่วนใหญ่ได้มีการพัฒนารูปแบบการทำงานให้มีประสิทธิภาพมากยิ่งขึ้น ด้วยการนำระบบคอมพิวเตอร์เข้ามาใช้งานในส่วนงานหลายส่วนที่มีปริมาณข้อมูลจำนวนมาก และต้องการความสามารถในการประมวลผลที่ถูกต้องและรวดเร็ว โดยอาจมีการเชื่อมต่อระบบงานเข้าด้วยกันเพื่อแลกเปลี่ยนข้อมูลระหว่างส่วนงานหรือทำการประมวลผลข้อมูลที่มีขนาดใหญ่ ซึ่งแนวโน้มในการนำระบบต่างๆมาใช้มากขึ้นนี้ ก่อให้เกิดระบบคอมพิวเตอร์แบบกระจายในระดับองค์กร (Enterprise distributed computing system) ซึ่งเป็นลักษณะการทำงานที่มีประสิทธิภาพสูงและรองรับการใช้งานจากผู้ใช้งานที่อาจอยู่กระจายออกไป และอาจมีความต้องการที่จะเรียกใช้ทรัพยากรที่มีอยู่ในระบบ โดยระบบดังกล่าว จะประกอบไปด้วยโปรแกรมต่างๆที่ทำการประมวลผลของงานที่แตกต่างกันไป ซึ่งรวมเป็นลักษณะการทำงานแบบรวม (Integrated system) เพื่อร่วมมือกันทำงานให้เกิดผลลัพธ์ที่สามารถนำไปใช้ในองค์กรได้

ในหัวข้อนี้จะกล่าวถึงระบบสารสนเทศโดยทั่วไป และ ลักษณะการทำงานของระบบสารสนเทศแบบกระจาย รวมถึงหลักการพัฒนาระบบดังกล่าวในรายละเอียดต่อไป

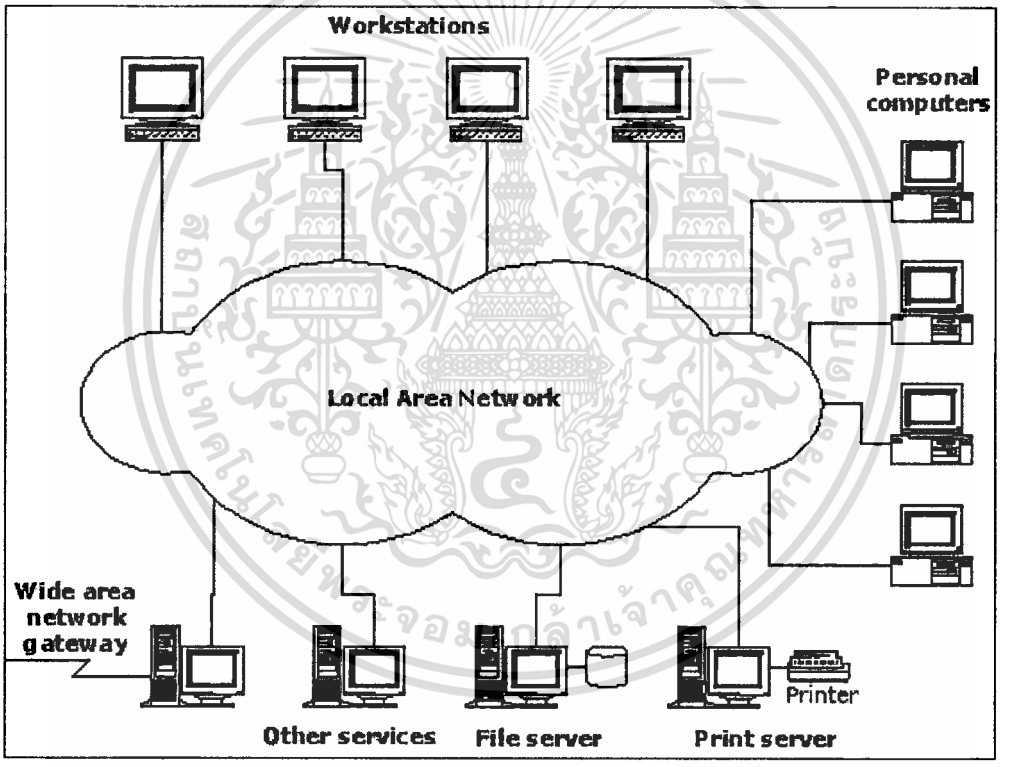
2.1.1 ระบบสารสนเทศ (Information System)

สารสนเทศ (Information) หมายถึง ข่าวสารที่ได้จากการนำข้อมูลดิบ (Raw data) มาคำนวณทางสถิติ หรือ ประมวลผลอย่างใดอย่างหนึ่ง ซึ่งข่าวสารที่ได้ออกมานั้นจะอยู่ในรูปที่สามารถนำไปใช้งานได้ทันที และ เทคโนโลยีสารสนเทศ (Information Technology) หมายถึง กระบวนการ เทคนิควิธีการ หรือ ระบบงานที่ช่วยให้ได้สารสนเทศที่ต้องการ โดยจะรวมถึง เครื่องมืออุปกรณ์ต่างๆซึ่งส่วนมากจะหมายถึง เครื่องคอมพิวเตอร์ เครื่องใช้สำนักงาน อุปกรณ์โทรคมนาคม และ ซอฟต์แวร์ต่างๆ ซึ่งเครื่องมือเหล่านี้จัดเป็นเครื่องมือสมัยใหม่และใช้เทคโนโลยีระดับสูง (High Technology)

ระบบสารสนเทศ (Information System) เป็นระบบที่เกิดจากการนำอุปกรณ์เครื่องมือข้างต้นมาใช้งานเพื่อรวบรวมจัดเก็บ ประมวลผล และ แสดงผลลัพธ์เป็นสารสนเทศในรูปแบบต่างๆที่สามารถนำไปใช้ประโยชน์ได้ต่อไป

2.1.2 ระบบสารสนเทศแบบกระจาย (Distributed Information System)

ระบบสารสนเทศแบบกระจาย คือรูปแบบหนึ่งของระบบสารสนเทศที่รองรับการทำงานของผู้ใช้งานที่อยู่กระจัดกระจายออกไปที่ต้องการเรียกใช้ทรัพยากรในระบบ ซึ่งระบบงานดังกล่าวจะประกอบไปด้วยอุปกรณ์คอมพิวเตอร์ต่างๆ ที่ติดตั้งโปรแกรมสนับสนุนระบบการทำงานแบบกระจาย (Distributed system software) และเชื่อมต่อเข้าด้วยกันผ่านเครือข่าย โดยโปรแกรมที่สนับสนุนระบบการทำงานแบบกระจายนี้จะช่วยให้เครื่องคอมพิวเตอร์ในระบบ สามารถประสานการทำงาน และแบ่งการใช้ทรัพยากรของระบบระหว่างกัน ไม่ว่าจะเป็นทรัพยากรประเภท อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ หรือ ข้อมูล ต่างๆ ดังแสดงเป็นแผนภาพในรูปที่ 2.1



รูปที่ 2.1 แสดงลักษณะทั่วไปของระบบสารสนเทศแบบกระจาย

จากรูปที่ 2.1 แสดงถึงส่วนประกอบต่างๆใน ระบบสารสนเทศแบบกระจาย ที่ใช้การเชื่อมต่อแบบ Local area network (LAN) ซึ่งระบบจะประกอบไปด้วยอุปกรณ์ที่หลากหลาย และมีการเชื่อมต่อเข้าด้วยกันเพื่อทำงานเป็นระบบ

2.1.3 คุณสมบัติหลักของระบบสารสนเทศแบบกระจาย

ปัจจัยสำคัญที่สามารถนำมาใช้ระบุถึงประโยชน์ในการใช้งานของระบบสารสนเทศแบบกระจาย คือ คุณสมบัติของระบบในด้านต่างๆดังนี้

1. **ความสามารถในการจัดสรรทรัพยากรเพื่อการใช้ร่วมกัน (Resource Sharing)**

ความสามารถในการจัดสรรทรัพยากรเพื่อการใช้ร่วมกัน (Resource Sharing) เป็นหลักการขั้นพื้นฐานของระบบการทำงานแบบกระจาย โดยทรัพยากรในระบบอาจเป็น เนื้อข้อมูล ซอฟต์แวร์ หรือ อุปกรณ์ฮาร์ดแวร์ ซึ่งเป็นทรัพยากรที่หลายๆ Process มีความต้องการในการใช้งาน ดังนั้นระบบการทำงานแบบกระจายที่ดีจึงจำเป็นที่จะต้องมีการจัดการของทรัพยากร (Resource management) ที่ดีและมีประสิทธิภาพ

2. **ความสามารถในลักษณะเปิด (Openness)**

ความสามารถในลักษณะเปิด (Openness) คือ ลักษณะความสามารถของระบบในการขยายการทำงานในอนาคต และ ความสามารถของระบบในการเชื่อมต่อเข้ากับซอฟต์แวร์ และ อุปกรณ์ฮาร์ดแวร์ที่หลากหลาย ดังตัวอย่างเช่น ระบบ UNIX ซึ่งมากับภาษาที่ใช้ในการพัฒนาโปรแกรม คือ ภาษาซี (C programming language) ที่อนุญาตให้นักพัฒนาโปรแกรม สามารถพัฒนาซอฟต์แวร์เพื่อเข้าถึงทรัพยากรที่ถูกจัดการโดยระบบปฏิบัติการ ทั้งนี้ภาษาซีเป็นภาษาแบบระดับสูง ทำให้สามารถทำการ Compile และประมวลผลโปรแกรมเพื่อใช้สำหรับเครื่องคอมพิวเตอร์ที่หลากหลายได้ จึงทำให้ UNIX สามารถเชื่อมต่อเข้ากับอุปกรณ์ใหม่ๆได้ด้วย เพียงการพัฒนาโปรแกรมเพื่อเสริมความสามารถใหม่ (Extension) เข้าไปให้กับระบบ

3. **ความสามารถในการทำงานหลายงานในช่วงเวลาเดียวกัน (Concurrency)**

ความสามารถในการทำงานหลายงานในช่วงเวลาเดียวกัน (Concurrency) เป็นคุณสมบัติที่ช่วยทำให้เกิดประสิทธิภาพที่สูงขึ้นในการประมวลผลโดยรวมของระบบซึ่ง โดยลักษณะของระบบการทำงานแบบกระจายโดยทั่วไป จะมีกระบวนการเกิดขึ้นภายในเป็นจำนวนมากมายจากผู้ใช้ระบบ การทำงานหลายงานในช่วงเวลาเดียวกัน จึงเกิดขึ้นเพราะ Process ต่างๆในระบบมีการทำงานที่พร้อมกัน ทั้งนี้การที่ระบบจะสามารถทำงานหลายงานในช่วงเวลาเดียวกันได้นั้น ระบบจะต้องถูกออกแบบมาเพื่อรองรับความสามารถในด้านนี้โดยเฉพาะ (System of concurrent processes)

4. **ความสามารถในการปรับขนาดการทำงาน (Scalability)**

ในระบบการทำงานแบบกระจายที่ดี ควรสามารถรองรับการปรับขนาด (Scale) ของการทำงานของระบบได้ โดยไม่ต้องปรับเปลี่ยน แกนหลักของระบบ หรือ โปรแกรม

ประยุกต์ที่ใช้งานอยู่แล้ว เนื่องจากโดยลักษณะของระบบแบบกระจายนั้น จะมีอุปกรณ์เชื่อมต่อเพิ่มเติม และ ผู้ใช้งานใหม่ที่ต้องการเข้ามาใช้ทรัพยากรของระบบ อยู่เป็นประจำ วิธีการทำข้อมูลแบบขนาน (Data replication) และ วิธีการกระจายความสมดุลในการทำงาน (Load balancing) ระหว่าง Server เป็น 2 วิธีที่นิยมใช้ในการเสริมความสามารถนี้

5. ความสามารถในการต้านทานต่อความผิดพลาด (Fault Tolerance)

ความสามารถในการต้านทานต่อความผิดพลาด คือ การที่ระบบสามารถตรวจพบและฟื้นฟูแก้ไขข้อผิดพลาดที่เกิดขึ้นระหว่างการทำงานได้ ทั้งนี้หนึ่งในวิธีการทำให้ระบบมีความสามารถในการต้านทานต่อความผิดพลาดคือ การทำ Hardware redundancy เพื่อรองรับสถานการณ์เมื่อฮาร์ดแวร์ส่วนหนึ่งเกิดความผิดพลาด ก็ยังมีอีกส่วนหนึ่งที่ทำงานต่อหรือทำหน้าที่แทนได้

6. ความสามารถในการทำงานแบบโปร่งใส (Transparency)

ความสามารถในส่วนของการทำงานแบบโปร่งใส คือ การที่ผู้ใช้งาน และ นักพัฒนาโปรแกรมของระบบ สามารถเรียกใช้งาน ระบบเครือข่ายของอุปกรณ์คอมพิวเตอร์ที่หลากหลาย เปรียบเสมือนการเรียกใช้งาน ระบบที่ทำงานรวมเป็นหนึ่งเดียว (Integrated system) โดยที่ผู้ใช้งานเหล่านั้นไม่จำเป็นที่จะต้องทราบถึงโครงสร้างการทำงานภายใน ที่เป็นระบบแบบกระจายซึ่งเชื่อมต่อทรัพยากรที่หลากหลายเพื่อตอบสนองความต้องการในการใช้งานในแง่ต่างๆ

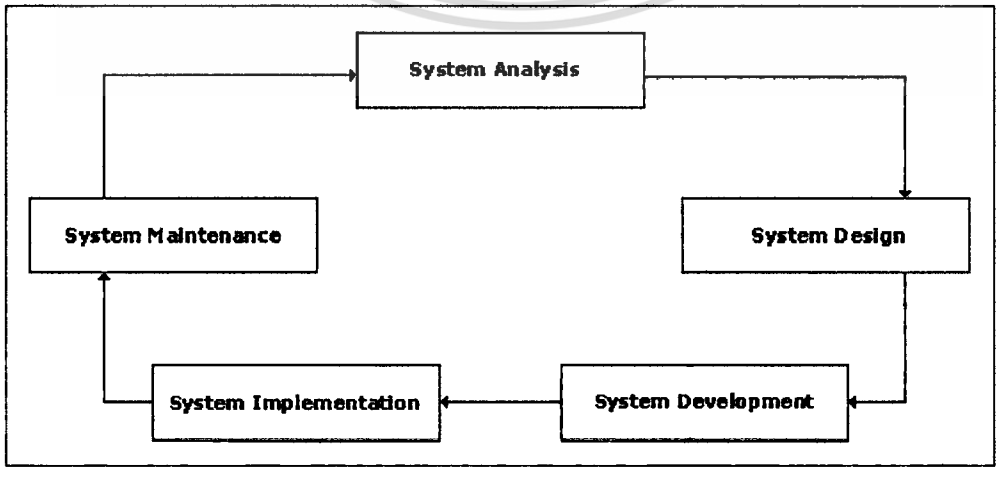
2.1.4 การพัฒนาระบบสารสนเทศแบบกระจาย

หลักการสำหรับการพัฒนาระบบสารสนเทศแบบกระจายนั้น มีลักษณะในการพัฒนาที่คล้ายกับหลักการใน การพัฒนาระบบสารสนเทศทางคอมพิวเตอร์โดยทั่วไป ซึ่งมีวิธีการซึ่งเป็นที่นิยมใช้กันอยู่ 3 วิธี คือ การพัฒนาระบบสารสนเทศตามวงจรการพัฒนาระบบ การพัฒนาโดยวิเคราะห์โครงสร้าง และการพัฒนาโดยการสร้างต้นแบบ ซึ่งมีรายละเอียดดังต่อไปนี้

2.1.4.1 การพัฒนาระบบสารสนเทศตามวงจรการพัฒนาระบบ (System Development Life Cycle)

การพัฒนาระบบสารสนเทศตามวงจรการพัฒนาระบบ (SDLC) เป็นแนวคิดที่เกี่ยวข้องกับชุดของกิจกรรมที่นักวิเคราะห์ นักออกแบบ และผู้ใช้ จะนำไปใช้ในการพัฒนาและนำไปปฏิบัติ ซึ่งจะประกอบไปด้วยกิจกรรมหลักต่างๆ ที่มีความสัมพันธ์กันอย่างต่อเนื่อง โดยรายละเอียดของแต่ละกิจกรรมมีดังนี้

1. **การวิเคราะห์ระบบงาน (System Analysis)** เป็นขั้นตอนของการศึกษาระบบงานเดิมที่ใช้ในปัจจุบัน (Current system) ปัญหาที่เกิดจากระบบงานเดิม ตลอดจนการศึกษาถึงความต้องการของระบบงาน พร้อมกับการประเมินเหตุการณ์ต่างๆ เพื่อหาทางเลือกที่เหมาะสมมาแก้ปัญหา
2. **การออกแบบระบบ (System Design)** เป็นขั้นตอนในการวางโครงสร้างของระบบงานทั้งในรูปลักษณะทั่วไป และในรูปลักษณะที่เฉพาะ โดยมีการแจกแจงรายละเอียดที่แน่ชัดของแต่ละงาน เช่น การออกแบบระบบงาน (Procedure design) การออกแบบการรับข้อมูลเข้าและแสดงผล (Input – output design) การออกแบบการประมวลผล (Process design) เป็นต้น
3. **การพัฒนาระบบเพื่อการใช้งาน (System Development)** เป็นขั้นตอนต่อจากการออกแบบระบบ คือ การพัฒนาโปรแกรมที่ได้ทำการออกแบบไว้ ทำการพัฒนาต้นแบบขึ้นมาทดสอบโปรแกรมให้ทำงานได้ตามวัตถุประสงค์ที่ตั้งไว้ ก่อนนำไปใช้งานจริง
4. **การนำไปใช้งานจริง (System Implementation)** เป็นขั้นตอนของการนำโปรแกรมที่พัฒนาไปติดตั้ง (Program installation) ให้กับผู้ใช้งาน พร้อมกับการฝึกอบรม (Training) ให้กับผู้ใช้งานเพื่อให้สามารถที่จะใช้ระบบงานได้อย่างถูกต้องและมีประสิทธิภาพ
5. **การบำรุงรักษาระบบ (System Maintenance)** เป็นขั้นตอนหลังจากการนำโปรแกรมไปใช้งานจริง นั่นคือ ผู้พัฒนาโปรแกรมจำเป็นที่จะต้องให้คำแนะนำแก่ผู้ใช้งานระบบอย่างต่อเนื่อง รวมทั้งรวบรวมความต้องการต่างๆที่อาจเกิดขึ้นหรือเปลี่ยนแปลงภายหลังจากการติดตั้งระบบแล้ว ซึ่งอาจจะกล่าวได้ว่าเป็นการบำรุงรักษาระบบงาน (System maintenance) และการปรับปรุงระบบงาน (System improvement)



รูปที่ 2.2 แสดงวงจรของการพัฒนาระบบงาน

จากรูปที่ 2.2 ซึ่งแสดงถึงวงจรของการพัฒนาระบบ เมื่อความต้องการมีการเปลี่ยนแปลงไป และระบบงานที่ใช้งานอยู่มีความจำเป็นที่จะต้องทำการปรับปรุงใหม่ นักวิเคราะห์ระบบจะต้องกลับไปทำขั้นตอนวิเคราะห์ระบบ (System analysis) อีกครั้ง

2.1.4.2 การพัฒนาระบบสารสนเทศโดยการวิเคราะห์โครงสร้าง

การพัฒนาระบบสารสนเทศโดยการวิเคราะห์โครงสร้าง เป็นการแบ่งการวิเคราะห์ระบบออกเป็นส่วนย่อยและทำการสร้างแบบจำลองของระบบขึ้น เพื่อที่จะระบุให้แน่ชัดลงไปว่า ระบบหรือการทำงานนั้นๆต้องการที่จะทำอะไร โดยไม่ต้องระบุว่าควรจะทำอย่างไร ทั้งนี้เพื่อแสดงให้เห็นถึงส่วนประกอบทางกระบวนการ (Process) และ ระบบการจัดเก็บข้อมูล (Storage) และสิ่งอื่นๆที่อยู่ในระบบ

ส่วนประกอบของการวิเคราะห์โครงสร้างที่จำเป็น จะรวมถึงรูปสัญลักษณ์ที่เป็น แผนภาพการไหลเวียนของข้อมูล (Data Flow Diagram: DFD) และ พจนานุกรมข้อมูลส่วนกลาง (Data Dictionary) โดยแผนภาพการไหลเวียนของข้อมูล จะแสดงถึงการไหลเวียนของข้อมูลในระบบระหว่างกระบวนการและแหล่งเก็บข้อมูล การพัฒนารายละเอียดโดยการวิเคราะห์โครงสร้างนั้น จะทำการวิเคราะห์ตามหลักของกระบวนการจากบนลงล่าง (Top – down) ซึ่งเป็นลักษณะของการกระจายไปสู่รายละเอียดที่มากยิ่งขึ้น ซึ่งแผนภาพในระดับล่างจะแสดงให้เห็นถึงรายละเอียดที่เพิ่มเติมเข้าไปในระบบ โดยที่ในแต่ละกระบวนการนั้น จะถูกแยกแยะไปเป็นแผนภาพการไหลเวียนของข้อมูลที่มีรายละเอียดมากขึ้น ซึ่งกระบวนการดังกล่าวนี้จะเกิดขึ้นซ้ำๆ จนมีรายละเอียดเพียงพอ

การออกแบบโครงสร้าง จะมุ่งประเด็นไปที่การพัฒนาข้อกำหนดต่างๆของซอฟต์แวร์ (Software specification) และเป้าหมายของการออกแบบโครงสร้าง คือเพื่อที่จะสร้างโปรแกรมซึ่งประกอบไปด้วยชิ้นส่วน (Module) ที่ทำหน้าที่อิสระแยกจากกัน แต่มีความสัมพันธ์ซึ่งกันและกัน ดังนั้น การออกแบบโครงสร้าง จึงเป็นเทคนิคของการออกแบบโปรแกรมที่เฉพาะเจาะจง โดยไม่จำเป็นที่จะต้องระบุถึง แฟ้มข้อมูลหรือการออกแบบฐานข้อมูล ลำดับขั้นตอนของกระบวนการหรือฮาร์ดแวร์

2.1.4.3 การพัฒนาระบบสารสนเทศแบบการสร้างระบบต้นแบบ (Prototype)

การสร้างระบบต้นแบบ เป็นวิธีการที่เกี่ยวกับผู้ใช้โดยตรง โดยใช้เพื่อการวิเคราะห์และออกแบบมากกว่า วิธีการพัฒนาระบบงานตามวงจรการพัฒนาระบบ (SDLC) หรือ การวิเคราะห์โครงสร้าง การสร้างต้นแบบจะเป็นไปอย่างมีประสิทธิผลภายใต้สิ่งแวดล้อมที่เหมาะสม ซึ่งวิธีการพัฒนาต้นแบบเป็นการสร้างระบบต้นแบบที่ใช้เวลาน้อยเพียงไม่เกินสัปดาห์ และเสียค่าใช้จ่ายต่ำ

การสร้างต้นแบบ จะอาศัยตัวช่วยสร้างโปรแกรม (Application generator) เป็นตัวสนับสนุนระบบต้นแบบ เครื่องมือเหล่านี้จะสร้างต้นแบบโดยอัตโนมัติ ซึ่งนักวิเคราะห์สามารถที่จะกำหนดโครงสร้างของรายละเอียดต่างๆ บนจอภาพบันทึกข้อมูลนำเข้าและรูปแบบของรายงาน ซึ่งผลที่ได้คือ โปรแกรมคอมพิวเตอร์ที่ใช้เวลาในการสร้างไม่นานนัก และอาจจะใช้เวลาเพียงไม่กี่ชั่วโมงจากกระบวนการพัฒนาให้เป็นโปรแกรมประยุกต์ที่ใช้งานได้อย่างสมบูรณ์

2.2 ฐานข้อมูล (Database)

ฐานข้อมูล (Database) คือ การจัดการกับข้อมูลอย่างมีระบบ ซึ่งผู้ใช้สามารถเรียกใช้ข้อมูลในลักษณะต่างๆ ได้แก่ การเพิ่มเติมข้อมูล การเรียกดูข้อมูล การแก้ไขหรือลบข้อมูล เป็นต้น โดยทั่วไปแล้ว การจัดเก็บข้อมูลจะมีการนำระบบคอมพิวเตอร์เข้ามาช่วยในการจัดการฐานข้อมูล และมีโปรแกรมหรือซอฟต์แวร์ที่ช่วยในการจัดการข้อมูลที่เรียกว่า ระบบจัดการฐานข้อมูล (Database Management System: DBMS)

ความหมายของฐานข้อมูลอีกนัยหนึ่งคือ ฐานข้อมูล เป็นการนำไฟล์ข้อมูลที่ใช้ในองค์กรที่อยู่กระจัดกระจายตามที่ต่างๆ ที่อาจจะมีข้อมูลที่ซ้ำซ้อนกัน ทำให้สิ้นเปลืองเนื้อที่ในการจัดเก็บ และข้อมูลที่จัดเก็บอาจจะเกิดความขัดแย้งกัน กล่าวคือ เมื่อมีการเปลี่ยนแปลงข้อมูล อาจจะเกิดการหลงลืมในการเปลี่ยนแปลงให้ครบทุกไฟล์ที่เกี่ยวข้อง จากปัญหาของการประมวลผลแบบไฟล์นั้น ทำให้เกิดแนวคิดของระบบฐานข้อมูลขึ้น ซึ่งการประมวลผลด้วยฐานข้อมูลจะสามารถช่วยขจัดปัญหาของการประมวลผลด้วยระบบไฟล์ ดังต่อไปนี้

1. **ลดความซ้ำซ้อน** และความไม่สอดคล้องของข้อมูล โดยข้อมูลที่เป็นข้อมูลชนิดเดียวกัน จะถูกเก็บไว้ที่เดียว ทำให้การเปลี่ยนแปลงหรือการปรับปรุงข้อมูลสามารถทำได้กับข้อมูลชุดเดียวกัน ทำให้ได้ข้อมูลที่มีความถูกต้อง สมบูรณ์ และ สอดคล้องอยู่ตลอดเวลา
2. **ลดความซับซ้อนในการเข้าถึงข้อมูล** ในระบบฐานข้อมูลจะมีภาษาที่ใช้ในการเข้าถึงข้อมูลที่ให้ผู้ใช้สามารถเข้าใจได้ง่าย และในระบบฐานข้อมูลจะมีซอฟต์แวร์ที่เรียกว่า ระบบการจัดการฐานข้อมูล (Database Management System) หรือเรียกสั้นๆว่า DBMS เป็นตัวคอยจัดการฐานข้อมูลให้
3. **สามารถใช้ข้อมูลร่วมกันได้** ผู้ใช้งานสามารถเรียกใช้ข้อมูลที่มีอยู่ในฐานข้อมูลร่วมกันได้ ทำให้ไม่เปลืองเนื้อที่ในการจัดเก็บข้อมูล และ สามารถทำการแก้ไขข้อมูลได้ง่าย
4. **ข้อมูลมีความปลอดภัย** ในระบบฐานข้อมูลจะมีการกำหนด View หรือ Sub Schema ให้กับผู้ใช้แต่ละคนได้ ทำให้สามารถกำหนดสิทธิในการเข้าถึงฐานข้อมูลของผู้ใช้แต่ละคนได้ โดยผู้บริหารฐานข้อมูล (Database Administrator: DBA) ซึ่งจะเป็นบุคคลเดียวหรือกลุ่มคน

ก็ได้ และการเข้าถึงข้อมูลนั้นจะต้องผ่าน DBMS ทุกครั้ง อีกทั้งมีการเข้ารหัสของเนื้อข้อมูล เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้ผ่าน DBMS

5. **ข้อมูลมีความคงสภาพ** ในระบบฐานข้อมูลจะมีการควบคุมความคงสภาพของข้อมูล (Integrity Constraint) คือ สามารถที่จะกำหนดค่าของ Attribute แต่ละตัวได้ โดยจะกำหนดให้มีลักษณะอย่างไรนั้นจะขึ้นอยู่กับเงื่อนไขต่าง ๆ เช่น ยอดเงินของการเปิดบัญชีใหม่ของธนาคารจะต้องมีค่าไม่ต่ำกว่า 500 บาท หรือการใช้รหัสของนักศึกษาเป็นตัวอ้างอิงถึงข้อมูลนักศึกษา ก็จะต้องทำการสร้างรหัสของนักศึกษาขึ้นมาก่อน เป็นต้น
6. **ข้อมูลที่จัดเก็บมีความเป็นอิสระ** การจัดเก็บข้อมูลในดิสก์นั้น อาจถูกจัดเก็บอยู่ในระดับภายใน (Internal) หรือ ระดับภายนอก (Physical) โดยเมื่อมีการเปลี่ยนแปลงเทคนิควิธีการจัดเก็บ หรือ การเรียกใช้ข้อมูล ผู้ใช้ไม่จำเป็นที่จะต้องเขียนโปรแกรมขึ้นมาใหม่ เพราะ DBMS จะทำหน้าที่เป็นตัวกลางในการจัดการเชื่อมโยงข้อมูลจากระดับภายนอก เข้ากับข้อมูลระดับหลักการ (Logical) และ ทำการเชื่อมโยงข้อมูลระหว่าง ระดับหลักการ เข้ากับ ข้อมูลที่ระดับภายใน

2.2.1 แนวคิดในการออกแบบฐานข้อมูล

เมื่อพูดถึงการออกแบบฐานข้อมูล จะหมายรวมถึงการออกแบบฐานข้อมูลระดับแนวคิด (Conceptual level) และการออกแบบฐานข้อมูลในระดับภายในหรือเชิงกายภาพ (Internal หรือ Physical level) การออกแบบฐานข้อมูลในระดับแนวคิด เป็นการออกแบบเค้าร่างของความสัมพันธ์ว่า ความสัมพันธ์นั้นจะประกอบด้วยแอททริบิวต์อะไร การออกแบบฐานข้อมูลในระดับนี้ จะช่วยให้ผู้ใช้ทั่วไปสามารถเข้าใจถึงข้อมูลที่เก็บในแอททริบิวต์ต่าง ๆ รวมถึงการเรียกใช้ข้อมูลด้วย ส่วนการออกแบบฐานข้อมูลในระดับภายใน เป็นการออกแบบที่เน้นในเรื่องของการจัดเก็บข้อมูลว่าควรจะมีการจัดเก็บอย่างไร

แนวคิดที่สำคัญที่ใช้เป็นเครื่องมือในการออกแบบฐานข้อมูลในระดับแนวคิด ประกอบด้วยหลักการเรื่อง ความสัมพันธ์ระหว่างค่าของแอททริบิวต์ในแต่ละแบบ (Dependency) การทำความสัมพันธ์ให้อยู่ในรูปแบบบรรทัดฐาน (Normalization) และ รูปแบบบรรทัดฐาน (Normal Form)

2.2.1.1 ความสัมพันธ์ระหว่างแอททริบิวต์ในแต่ละแบบ (Dependency)

เนื่องจากค่าของแอททริบิวต์ในแต่ละความสัมพันธ์ อาจจะมีความสัมพันธ์กันในลักษณะของการทราบค่าของแอททริบิวต์หนึ่ง จะสามารถทราบถึงค่าของแอททริบิวต์อื่น ในความสัมพันธ์ได้ โดยลักษณะของความสัมพันธ์ระหว่างค่าของแอททริบิวต์ในแต่ละรีเลชันที่จะกล่าวมีดังต่อไปนี้

1. **ความสัมพันธ์ระหว่างค่าของแอททริบิวต์แบบฟังก์ชัน (Functional dependency)** คือ การที่แอททริบิวต์หนึ่ง หรือ หลายแอททริบิวต์ที่ประกอบกัน สามารถระบุค่าของแอททริบิวต์อื่น ในความสัมพันธ์หนึ่ง ได้ชัดเจน โดยความสัมพันธ์ในการระบุค่าของแอททริบิวต์ จะเกี่ยวข้องกับคีย์หลัก (Primary key) เพราะคุณสมบัติของคีย์หลักคือการเป็นแอททริบิวต์ที่มีค่าเป็นเอกลักษณ์ (unique) ที่สามารถใช้ระบุค่าของแอททริบิวต์อื่นในความสัมพันธ์ได้
2. **ความสัมพันธ์ระหว่างค่าของแอททริบิวต์แบบทรานซิทีฟ (Transitive dependency)** คือ การที่แอททริบิวต์ที่มีคุณสมบัติเป็นหลักสามารถระบุค่าของแอททริบิวต์ในแต่ละ Tuple ได้ อย่างไรก็ตามในบางความสัมพันธ์นั้น อาจจะมีกรณีที่แอททริบิวต์ที่ไม่มีคุณสมบัติเป็นคีย์หลัก (Primary key) หรือ คีย์คู่แข่ง (Non – key attribute) สามารถที่จะระบุค่าของแอททริบิวต์อื่นใน Tuple ได้ ลักษณะของความสัมพันธ์ในการระบุค่าของแอททริบิวต์แบบนี้เรียกว่า ความสัมพันธ์ระหว่างค่าของแอททริบิวต์แบบทรานซิทีฟ (Transitive dependency)
3. **ความสัมพันธ์ระหว่างค่าของแอททริบิวต์แบบหลายค่า (Multivalued dependency)** ในบางกรณี ความสัมพันธ์บางอย่างอาจจะมีความสัมพันธ์ระหว่างค่าของแอททริบิวต์แบบหลายค่าเกิดขึ้นได้ โดยความสัมพันธ์นี้จะเกิดกับความสัมพันธ์ที่ประกอบด้วยแอททริบิวต์อย่างน้อยสามแอททริบิวต์ และเป็นความสัมพันธ์ที่แอททริบิวต์หนึ่ง สามารถระบุค่าของแอททริบิวต์อื่น ๆ ในความสัมพันธ์ได้มากกว่าหนึ่งค่า กรณีเช่นนี้เรียกว่า ความสัมพันธ์นั้นมีความสัมพันธ์ในการระบุค่าของแอททริบิวต์แบบหลายค่า (Multivalued dependency)

สำหรับความสัมพันธ์ระหว่างค่าของแอททริบิวต์แบบทรานซิทีฟและแบบหลายค่า จะต้องผ่านกระบวนการ การทำรีเลชันให้อยู่ในรูปแบบบรรทัดฐาน (Normalization) เพื่อไม่ให้การออกแบบฐานข้อมูลนั้น มีปัญหาในด้านการเพิ่ม ลบ หรือปรับปรุงข้อมูลได้

2.2.1.2 การทำความสัมพันธ์ให้อยู่ในรูปแบบบรรทัดฐาน (Normalization)

แนวคิดในการทำความสัมพันธ์ให้อยู่ในรูปแบบบรรทัดฐาน (Normalization process) ถูกคิดค้นโดย อี.เอฟ.คอดด์ (E.F. Codd) โดยเป็นกระบวนการที่นำเค้าร่างของความสัมพันธ์มาทำให้

อยู่ในรูปแบบที่เป็นบรรทัดฐาน (Normal form) เพื่อให้แน่ใจว่าการออกแบบเค้าร่างของความสัมพันธ์ เป็นการออกแบบที่เหมาะสม โดยที่วัตถุประสงค์ของการทำให้เป็นบรรทัดฐานมีดังนี้คือ

1. **เพื่อลดเนื้อที่ในการจัดเก็บข้อมูล** กล่าวคือ การทำให้ความสัมพันธ์อยู่ในรูปแบบบรรทัดฐานจะเป็นการลดความซ้ำซ้อนของข้อมูลในความสัมพันธ์ ซึ่งเป็นการลดเนื้อที่ในการจัดเก็บข้อมูลด้วย
2. **เพื่อลดปัญหาที่ข้อมูลไม่ถูกต้อง (Inconsistency)** เนื่องจากข้อมูลในความสัมพันธ์หนึ่งจะมีข้อมูลที่ไม่ซ้ำกัน เมื่อมีการปรับปรุงข้อมูล จะส่งผลให้สามารถทำการปรับปรุง Tuple นั้นครั้งเดียวโดยไม่ต้องปรับปรุงหลายแห่ง ทำให้โอกาสที่จะเกิดความผิดพลาดจากการปรับปรุงข้อมูลไม่ครบถ้วน จะไม่สามารถเกิดขึ้นได้
3. **เพื่อเป็นการลดปัญหาที่เกิดจากการเพิ่ม ปรับปรุงและลบข้อมูล (Insert Update and Delete Anomalies)** การทำความสัมพันธ์ให้อยู่ในรูปแบบบรรทัดฐานนั้น จะทำให้ข้อมูลที่อยู่ในฐานข้อมูลไม่เกิดการสูญหายจากการเพิ่ม ลบ หรือ ปรับปรุงเปลี่ยนแปลงแก้ไขข้อมูลในฐานข้อมูล

2.2.1.3 รูปแบบบรรทัดฐาน (Normal Form)

รูปแบบบรรทัดฐานที่ใช้ในการกำหนดแอททริบิวต์ที่เหมาะสมให้กับความสัมพันธ์นั้นสามารถแบ่งออกได้ดังนี้

1. **รูปแบบบรรทัดฐานขั้นที่ 1 (First normal form: 1NF)** ความสัมพันธ์หนึ่ง ๆ จะอยู่ในรูปแบบบรรทัดฐานขั้นที่ 1 ก็ต่อเมื่อ "ค่าของแอททริบิวต์หนึ่งๆ ในแต่ละ Tuple จะมีค่าของข้อมูลเพียงค่าเดียว" หากความสัมพันธ์ใดไม่มีคุณสมบัติดังกล่าว จะต้องทำการปรับให้อยู่ในรูปแบบบรรทัดฐานขั้นที่ 1 โดยการแยกกลุ่มของข้อมูลที่ซ้ำกันเป็นความสัมพันธ์ใหม่ และกำหนดให้แอททริบิวต์ที่เป็นตัวกำหนดค่าของกลุ่มข้อมูลที่ซ้ำกันนี้ (Multivalued attribute) เป็นคีย์หลักของความสัมพันธ์ใหม่
2. **รูปแบบบรรทัดฐานขั้นที่ 2 (Second Normal Form: 2NF)** ความสัมพันธ์หนึ่ง ๆ จะอยู่ในรูปแบบบรรทัดฐานขั้นที่ 2 ก็ต่อเมื่อ "ความสัมพันธ์นั้น อยู่ในรูปแบบบรรทัดฐานขั้นที่ 1 และมีคุณสมบัติอีกประการหนึ่งคือ แอททริบิวต์ทุกแอททริบิวต์ที่ไม่ได้เป็นคีย์หลัก จะต้องมีความสัมพันธ์ระหว่างค่าของแอททริบิวต์แบบฟังก์ชันกับคีย์หลัก (Fully functional dependency) กล่าวอีกนัยหนึ่งคือ ค่าของแอททริบิวต์ที่ไม่ได้เป็นคีย์หลักจะสามารถถูกระบุค่าโดยแอททริบิวต์ที่เป็นคีย์หลักหรือแอททริบิวต์ทั้งหมดที่ประกอบกันเป็นคีย์หลักในกรณีที่เป็นคีย์ผสม

3. **รูปแบบบรรทัดฐานขั้นที่ 3 (Third Normal Form: 3NF)** ความสัมพันธ์หนึ่ง ๆ จะอยู่ในรูปแบบบรรทัดฐานขั้นที่ 3 ได้ก็ต่อเมื่อ "ความสัมพันธ์นั้น อยู่ในรูปแบบบรรทัดฐานขั้นที่ 2 และมีคุณสมบัติอีกประการหนึ่งคือ แอททริบิวต์ที่ไม่ได้เป็นคีย์หลัก จะต้องไม่มีคุณสมบัติในการกำหนดค่าของแอททริบิวต์อื่นที่ไม่ใช่คีย์หลัก"
4. **รูปแบบบรรทัดฐานของบอยส์และคอดด์ (Boyce/Codd Normal Form: BCNF)** ความสัมพันธ์หนึ่ง ๆ จะอยู่ในรูปแบบบรรทัดฐานของบอยส์และคอดด์ก็ต่อเมื่อ "รีเลชันนั้น อยู่ในรูปแบบบรรทัดฐานขั้นที่ 3 และไม่มีแอททริบิวต์อื่นในความสัมพันธ์ที่สามารถระบุค่าของแอททริบิวต์ที่เป็นคีย์หลักหรือส่วนหนึ่งส่วนใดของคีย์หลัก ในกรณีที่คีย์หลักเป็นคีย์ผสม"

2.2.2 รูปแบบของฐานข้อมูล

สำหรับรูปแบบของฐานข้อมูลนั้น สามารถแบ่งได้เป็น 3 รูปแบบ ได้แก่ ฐานข้อมูลเชิงสัมพันธ์ ฐานข้อมูลแบบลำดับขั้น และฐานข้อมูลแบบข่ายงาน โดยมีรายละเอียดดังนี้

1. **ฐานข้อมูลเชิงสัมพันธ์ (Relational Database)** เป็นการจัดเก็บข้อมูลของเอนติตี้ในรูปแบบของตารางที่มีลักษณะเป็นสองมิติคือ เป็นแถว (Row) และเป็นคอลัมน์ (Column) ในการเชื่อมโยงข้อมูลระหว่างตาราง จะทำการเชื่อมโยงโดยใช้แอททริบิวต์ที่มีอยู่ในทั้งสองตารางเป็นตัวเชื่อมข้อมูลกัน ซึ่งในปัจจุบันนี้ ฐานข้อมูลเชิงสัมพันธ์เป็นรูปแบบของฐานข้อมูลที่นิยมใช้กันมาก
2. **ฐานข้อมูลแบบลำดับขั้น (Hierarchical Database)** โครงสร้างของฐานข้อมูลแบบลำดับขั้น เป็นโครงสร้างที่จัดเก็บข้อมูลในลักษณะของความสัมพันธ์แบบพ่อ-ลูก (Parent-Child Relationship Type: PCR Type) โดยที่คำว่า ข้อมูล ที่กล่าวในที่นี้คือ เรคคอร์ด (Record) นั่นเอง ซึ่งจะประกอบด้วยค่าของฟิลด์ของเอนติตี้หนึ่ง ๆ
3. **ฐานข้อมูลแบบข่ายงาน (Network Database)** โครงสร้างของข่ายงานประกอบด้วยประเภทของเรคคอร์ด และกลุ่มของข้อมูลของเรคคอร์ดนั้น ๆ เช่นเดียวกับโครงสร้างของฐานข้อมูลเชิงสัมพันธ์และเชิงลำดับขั้น

ในระบบ Hierarchical และ Network Database จะมีข้อดีที่เหมือนกันคือ ไม่เกิดความซ้ำซ้อนกันของคีย์ฟิลด์ และการประมวลผลในฐานข้อมูลทั้งสองชนิดจะใช้เวลาที่น้อยกว่าแบบ Relational Database แต่ข้อเสียซึ่งผลอย่างมากที่ทำให้ระบบทั้งสองชนิดนี้ไม่เป็นที่นิยมก็คือ ความไม่ยืดหยุ่นของโครงสร้างฐานข้อมูล ทำให้การบำรุงรักษาฐานข้อมูลทำได้ลำบาก เมื่อเทียบกับ

ระบบ Relational Database นอกจากนี้ การที่ระบบจะเข้าถึงข้อมูลก็ค่อนข้างจะซับซ้อนไม่ตรงไปตรงมาเหมือนกับแบบ Relational Database ซึ่งส่งผลทำให้ผู้ใช้เกิดความสับสนได้ง่าย

2.3 ความปลอดภัยในเครือข่าย

ในระบบการทำงานแบบกระจาย (Distributed Information System) การสื่อสารที่เกิดขึ้นระหว่างส่วนต่างๆในระบบจะใช้โปรโตคอลในการสื่อสาร เช่น Transmission Control Protocol / Internet Protocol (TCP/IP) ซึ่ง TCP/IP นั้นทำให้สามารถส่งข้อมูลจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องโดยอาศัย สื่อ อุปกรณ์และเครือข่ายคอมพิวเตอร์ต่างๆระหว่างทางจนถึงจุดหมาย ซึ่งการที่ TCP/IP ทำให้สามารถส่งข้อมูลโดยอาศัยสื่อและเครือข่ายคอมพิวเตอร์ระหว่างทางนี้ เป็นการเปิดโอกาสให้บุคคลที่สามสามารถแอบแฝงเข้ามาทำกิจกรรมที่ไม่พึงประสงค์เช่น

- **การดักฟังข้อมูล (Eavesdropping)** ด้วยวิธีการนี้ข้อมูลจะยังอยู่เช่นเดิม แต่เนื้อข้อมูลนั้นได้ถูกบุคคลที่สามดักเอาไปใช้งานหรือบันทึกเก็บไว้
- **การดักเปลี่ยนแปลงข้อมูล (Tampering)** ข้อมูลจะถูกปรับเปลี่ยนระหว่างทางก่อนที่จะถึงจุดหมาย
- **การแอบอ้างว่าเป็นบุคคลอื่น (Impersonating)** โดยข้อมูลจะถูกส่งไปที่บุคคลที่แอบอ้างว่าเป็นผู้รับที่ต้องการ หรือในทางกลับกัน ข้อมูลนั้นรับมาจากแหล่งที่แอบอ้างว่าเป็นผู้ส่งที่น่าเชื่อถือ

โดยทั่วไปแล้วผู้ใช้งานในเครือข่ายมักจะไม่เข้าไปยุ่งเกี่ยวหรือแอบดูข้อมูลต่างๆที่วิ่งผ่านเครื่องคอมพิวเตอร์ของตนไป แต่ทว่าข้อมูลบางประเภทซึ่งเป็นความลับและมีความสำคัญนั้นมีความจำเป็นที่จะต้องถูกเก็บรักษาไว้อย่างปลอดภัยจากกิจกรรมอันไม่พึงประสงค์ที่กล่าวมาข้างต้น ปัจจุบันด้วยวิธีการที่เรียกว่า Public Key Cryptography ทำให้สามารถทำการป้องกันข้อมูลให้ปลอดภัยได้ดังนี้

1. **การเข้าและถอดรหัส (Encryption and Decryption)** ทำให้สามารถปลอมแปลงข้อมูลที่สื่อสารระหว่างกันได้ โดยผู้ส่งจะทำการเข้ารหัสข้อมูลก่อนที่จะส่งออกไปให้ผู้รับซึ่งจะทำการ ถอดรหัสข้อมูลที่ได้รับมา โดยในช่วงระหว่างที่ข้อมูลเดินทางนั้นข้อมูลที่เข้ารหัสแล้วจะไม่สามารถอ่านออกได้โดยบุคคลที่สาม
2. **การตรวจสอบความดั้งเดิมของข้อมูล (Tamper Detection)** ทำให้ผู้รับข้อมูลสามารถตรวจสอบและยืนยันว่าข้อมูลที่ได้รับนั้นไม่ได้ถูกเปลี่ยนแปลงกลางทาง โดยถ้าข้อมูลได้ถูกปรับเปลี่ยนไปจากเดิม จะสามารถถูกตรวจพบได้

3. **การยืนยันตัวบุคคล (Authentication)** ทำให้ผู้รับข้อมูลสามารถแหล่งที่มา หรือ Identity ของผู้ส่ง โดยทั้งนี้แหล่งที่มาของข้อมูลอาจเป็นได้ทั้ง บุคคล (Client authentication) หรือ เครื่องคอมพิวเตอร์ (Machine authentication)
4. **การยืนยันเป็นหลักฐานว่าได้เคยส่งข้อมูลแล้ว (Non – repudiation)** ใช้ป้องกันการที่ผู้ส่งข้อมูลมาอ้างในภายหลังว่าตนไม่เคยส่งข้อมูลดังกล่าว

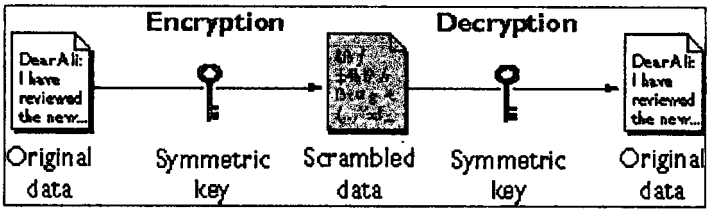
2.3.1 การเข้าและถอดรหัสข้อมูล (Encryption and Decryption)

การเข้ารหัสข้อมูล (Encryption) คือขบวนการรักษาข้อมูลที่เป็นความลับ โดยทำการปกปิดข้อมูลเดิมให้อยู่ในรูปที่ไม่สามารถเข้าใจโดยผู้อื่นได้ (Cipher Text) ซึ่งเป็นกลไกในการสื่อสารความลับระหว่างผู้เกี่ยวข้องเท่านั้น ส่วนการถอดรหัส (Decryption) คือขบวนการปรับข้อมูลที่ถูกเข้ารหัสไว้ ให้กลับมาอยู่ในรูปของข้อมูลเดิมที่สามารถเข้าใจได้อีกครั้ง โดยขบวนการทำการเข้าและถอดรหัส (Cryptographic Algorithm หรือ Cipher) คือฟังก์ชันทางคณิตศาสตร์ซึ่งสร้างขึ้นมาเพื่อทำการเข้าและถอดรหัสโดยเฉพาะ ซึ่งโดยทั่วไปจะประกอบไปด้วย 2 ฟังก์ชัน คือ ฟังก์ชันเข้ารหัส และ ฟังก์ชันถอดรหัส

ในขบวนการของการเข้าและถอดรหัสข้อมูลในปัจจุบันนั้น ความสามารถในการเก็บความลับของข้อมูลที่ถูกเข้ารหัสนั้นไม่ได้ขึ้นอยู่กับ Cryptographic Algorithm ซึ่งเป็นที่รู้จักอย่างแพร่หลาย แต่จะขึ้นอยู่กับรหัสตัวเลข หรือ กุญแจ (Key) ที่จะต้องนำมาใช้กับ Algorithm เพื่อทำการเข้าหรือถอดรหัส ซึ่งการถอดรหัสด้วย Key ที่ถูกต้องนั้นสามารถทำได้ง่าย แต่การถอดรหัสโดยไม่มี Key ที่ถูกต้องนั้นทำได้ยากมาก ซึ่งในบางกรณีนั้นแทบจะเป็นไปไม่ได้ในทางปฏิบัติ

2.3.1.1 การเข้ารหัสแบบ Symmetric – Key Encryption

ในการเข้ารหัสแบบ Symmetric – Key นั้น Key ที่ใช้ในการเข้ารหัสจะสามารถถูกคำนวณได้จาก Key ที่ใช้ในการถอดรหัส ซึ่งใน Symmetric Algorithm นั้นจะใช้ Key เดียวกันสำหรับการเข้าและถอดรหัสดังรูปที่ 2.3



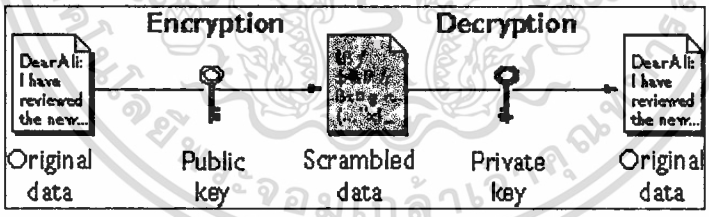
รูปที่ 2.3 แสดงการทำงานของการเข้ารหัสแบบ Symmetric – Key Encryption

จากรูปที่ 2.3 ก่อนที่จะส่งข้อมูลออกไป ผู้ส่งจะทำการเข้ารหัสข้อมูลด้วย Symmetric Key ที่ได้ตกลงไว้กับผู้รับแล้วว่าถ้าได้รับข้อมูลที่ถูกเข้ารหัสเอาไว้จากผู้ส่ง ให้ใช้ Symmetric Key แบบเดียวกันถอดรหัส แล้วจะได้ข้อมูลดั้งเดิม

การเข้ารหัสแบบ Symmetric – Key Encryption นั้นสามารถนำไปใช้ได้อย่างมีประสิทธิภาพ เนื่องจากสามารถนำไปเข้าและถอดรหัสได้อย่างสะดวกและรวดเร็ว และ ยังสามารถช่วยในการยืนยัน (Authentication) ในระดับหนึ่งเพราะการเข้าและถอดรหัสจะต้องใช้แค่ Key เดียวเท่านั้น ไม่สามารถใช้ Key อื่นได้ แต่การการเข้ารหัสแบบ Symmetric – Key Encryption นั้นจะมีประสิทธิภาพก็ต่อเมื่อทั้งผู้รับและผู้ส่งเก็บ Symmetric Key ไว้เป็นความลับ ซึ่งถ้า Key ถูกค้นพบโดยบุคคลอื่นแล้ว ข้อมูลความลับจะถูกเปิดเผยและอาจถูกปลอมแปลงในการเข้ารหัสแทนที่ผู้รับและผู้ส่ง

2.3.1.2 การเข้ารหัสแบบ Public – Key Encryption

การเข้ารหัสแบบ Public – Key Encryption (หรือ Asymmetric Encryption) จะใช้ Key เป็นคู่ คือ Public Key และ Private Key โดยบุคคลหรือเครื่องคอมพิวเตอร์ที่ต้องการยืนยันตนเอง หรือลงลายเซ็นอิเล็กทรอนิกส์ หรือเข้ารหัสข้อมูลจะต้องมี Key คู่ดังกล่าว โดย Public Key จะเป็น Key สาธารณะซึ่งจะถูกแจกออกไป ส่วน Private Key จะเก็บไว้เป็นความลับที่เจ้าของ ในการเข้ารหัสนั้น ข้อมูลที่ถูกเข้ารหัสด้วย Public Key นั้นจะต้องถอดรหัสด้วย Private Key เท่านั้นดังรูปที่ 2.4



รูปที่ 2.4 แสดงการทำงานของการเข้ารหัสแบบ Public – Key Encryption

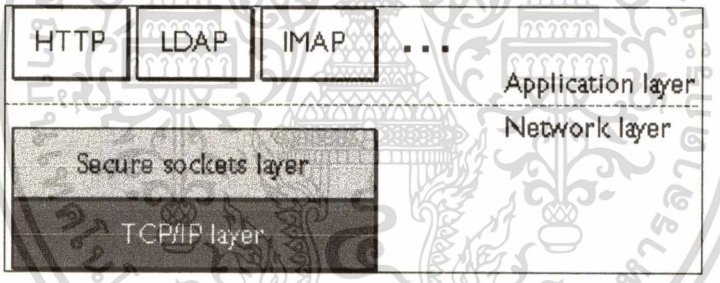
จากรูปที่ 2.4 ผู้ส่งข้อมูลทำการเข้ารหัสข้อมูลด้วย Public Key ของผู้รับซึ่งได้แจกจ่ายออกไป ซึ่งเฉพาะผู้รับเท่านั้นผู้ซึ่งมี Private Key ที่ใช้ในการถอดรหัสสามารถถอดเอาข้อมูลเดิมออกมาได้

เมื่อเปรียบเทียบกับวิธีการเข้ารหัสแบบ Symmetric – Key Encryption การเข้ารหัสแบบ Public – Key Encryption จะเกี่ยวข้องกับการคำนวณที่ซับซ้อนกว่า ดังนั้นจะไม่ค่อยเหมาะกับปริมาณข้อมูลขนาดใหญ่ แต่สามารถนำมาใช้ในกรณีที่นำเอาการเข้ารหัสแบบ Public Key Encryption เพื่อเข้ารหัส Symmetric Key เพื่อนำไปเข้ารหัสข้อมูลต่อไป ซึ่งวิธีการนี้ได้ถูกนำไปใช้ใน SSL Protocol ดังจะกล่าวรายละเอียดในหัวข้อถัดไป

ในทางกลับกัน การเข้ารหัสข้อมูลด้วย Private Key นั้นสามารถถอดรหัสได้ด้วย Public Key เท่านั้นแต่ในทางปฏิบัติแล้วคงไม่มีใครต้องการที่จะเข้ารหัสข้อมูลด้วย Private Key ของตน ซึ่งสามารถถอดรหัสได้โดยใช้ Public Key ซึ่งแจกจ่ายออกไปให้สาธารณะ อย่างไรก็ดี การเข้ารหัสด้วย Private Key นั้นสามารถนำไปใช้ประโยชน์ในการลงลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) ได้เพื่อยืนยันว่าข้อมูลนั้นมาจากผู้ส่งจริงและข้อมูลไม่ได้ถูกเปลี่ยนกลางทาง ในหัวข้อต่อๆไปจะกล่าวถึงหลักการทำงานของลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) ในรายละเอียดต่อไป

2.3.2 Secure Sockets Layer Protocol (SSL)

โปรโตคอล TCP/IP (Transmission Control Protocol/Internet Protocol) ใช้สำหรับการเคลื่อนย้ายข้อมูลผ่านเครือข่ายเช่น อินเตอร์เน็ต โดยมีโปรโตคอลอื่นๆเช่น Hypertext Transport Protocol (HTTP) ทำงานอยู่บน TCP/IP ดังรูปที่ 2.5



รูปที่ 2.5 แสดงการทำงานของ SSL ซึ่งอยู่ระหว่าง TCP/IP และ Application Layer

จากรูปที่ 2.5 Secure Socket Layer Protocol หรือ SSL นั้นทำงานอยู่บน TCP/IP และอยู่ภายใต้โปรโตคอลที่ทำงานระดับ Application Layer เช่น HTTP โดย SSL ใช้งาน TCP/IP แทนโปรโตคอลที่ทำงานอยู่ในระดับบน ซึ่ง SSL จะทำการยืนยัน (Authenticate) Server ที่ใช้ SSL เพื่อติดต่อกับ Client ที่ใช้ SSL ซึ่งทำการยืนยันตัวเองกับ Server เช่นกัน เป็นผลให้สามารถสร้างช่องทางการติดต่อที่มีความปลอดภัยขึ้นมาได้

2.3.2.1 การทำ SSL Handshake

โปรโตคอล SSL ใช้เทคนิคของการเข้ารหัสแบบ Public Key และ Symmetric Key Encryption มาประยุกต์ใช้เข้าด้วยกัน โดยอาศัยหลักการที่ Symmetric Key Encryption นั้นสามารถทำได้รวดเร็วกว่า Public Key Encryption แต่ Public Key Encryption สามารถทำการยืนยัน

(Authentication) ได้ดีกว่า โดยการทำ SSL นั้นจะเริ่มต้นด้วยการแลกเปลี่ยนข้อมูลซึ่งเรียกว่า SSL Handshake ซึ่งเป็นวิธีการยืนยันของทาง Server กับ Client และในทางกลับกันยังสามารถยืนยัน Client กับทาง Server โดยใช้ Public Key Encryption หลังจากนั้นทาง Client และ Server จึงร่วมกันสร้าง Symmetric Key เพื่อใช้สำหรับการเข้าและถอดรหัสที่รวดเร็วต่อไป

2.3.3 ความยาวของ Key และความแข็งแรงของการเข้ารหัส

โดยทั่วไปแล้วความแข็งแรงของการเข้ารหัสนั้นขึ้นอยู่กับ ความยากในการค้นพบ Key ที่ใช้เข้ารหัส ซึ่งเกี่ยวเนื่องไปถึง Algorithm และความยาวของ Key ที่ใช้ ดังนั้นความแข็งแรงของของการเข้ารหัส มักจะถูกอธิบายด้วยขนาดความยาวของ Key ที่ใช้ทำการเข้ารหัส กล่าวคือการที่ Key มีความยาวมาก ความแข็งแรงในการเข้ารหัสนั้นจะแข็งแรงมากขึ้นด้วย โดยการวัดขนาดของ Key นั้นมีหน่วยเป็น บิต (Bits) ยกตัวอย่างเช่น 128-bit key ที่ใช้ใน RC4 Symmetric – Key Algorithm ซึ่งใช้เข้ารหัสใน SSL นั้นข้อมูลมีความปลอดภัยสูงกว่าการเข้ารหัสด้วย 40-bit Key ในการใช้ Algorithm เดียวกันมาก กล่าวคือ การเข้ารหัสด้วย 128-bit RC4 นั้นมีความแข็งแรงกว่าแบบ 40- bit Key ถึง 3×10^{26} เท่า

เนื่องจากความแข็งแรงของ Key ที่ใช้ในการเข้าและถอดรหัสข้อมูลนั้นมีส่วนกระทบต่อข้อมูลความลับทางการทหาร รัฐบาลของประเทศสหรัฐอเมริกาซึ่งเป็นประเทศที่มีบริษัทผลิตซอฟต์แวร์ชั้นนำของโลกเป็นจำนวนมาก รวมถึงเว็บบราวเซอร์ เช่น Internet Explorer เป็นต้น ซึ่งในอดีตมีการออกกฎหมายจำกัดการส่งออกของซอฟต์แวร์ที่มีความสามารถในการเข้าและถอดรหัสให้มีความยาวของ Key ได้ไม่เกิน 40-bit แต่ในปัจจุบันด้วยความก้าวหน้าของเทคโนโลยีกฎหมายดังกล่าวได้ถูกปรับเปลี่ยนและผ่อนผันให้ทางผู้ผลิตซอฟต์แวร์ในอเมริกาสามารถส่งออกผลิตภัณฑ์ที่ใช้ Key ขนาด 128-bit ได้

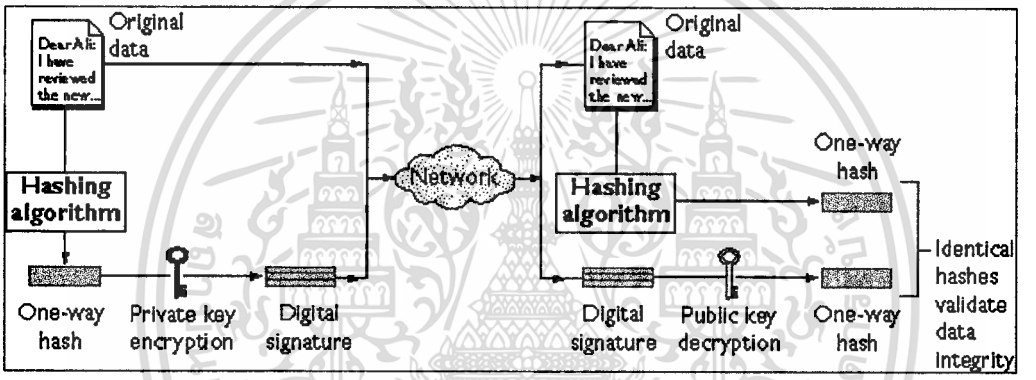
2.3.4 ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature)

การเข้าและถอดรหัสสามารถแก้ไขปัญหาของการแอบดักดูข้อมูลระหว่างการนำส่ง อย่างไรก็ตามการเข้าและถอดรหัสไม่สามารถแก้ปัญหาของการแอบเปลี่ยนแปลงข้อมูลกลางทาง และการแอบอ้างว่าเป็นผู้รับหรือผู้ส่ง

การใช้ ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) สามารถนำมาช่วยตรวจสอบความดั้งเดิมของข้อมูลและใช้ยืนยันเป็นหลักฐานว่าผู้ส่งได้เคยส่งข้อมูลแล้ว โดยลายเซ็นอิเล็กทรอนิกส์นี้อาศัยหลักการทำงานของฟังก์ชันทางคณิตศาสตร์คือ One – Way Hash (หรือ Message Digest) โดย One –Way Hash จะมีคุณสมบัติดังนี้

- ค่าของ Hash นั้นเป็นเอกลักษณ์สำหรับแต่ละข้อมูล ถ้าข้อมูลถูกเปลี่ยนแปลง ค่าของ Hash จะเปลี่ยนไป
- ข้อมูลที่ถูก Hash แล้วนั้นไม่สามารถนำกลับมาอยู่ในรูปแบบข้อมูลเดิมได้อีก กล่าวคือเป็นลักษณะ "one-way" นั่นเอง

จากการทำงานของ One – Way Hash นี้เอง เมื่อนำมาใช้กับ Public – Key Encryption โดยนำข้อมูลไปทำ One – Way Hash ซึ่งจะได้ค่า Hash ออกมาจากนั้นจึงใช้ Private Key เพื่อเข้ารหัสค่า Hash ซึ่งค่า Hash ที่ได้ถูกเข้ารหัสแล้วรวมกับข้อมูลอื่นที่จำเป็นเช่น Hashing Algorithm โดยรวมแล้วเรียกว่า ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) ดังแสดงการทำงานในรูปที่ 2.6



รูปที่ 2.6 แสดงการใช้งานของลายเซ็นอิเล็กทรอนิกส์

จากรูปที่ 2.6 แสดงให้เห็นถึงการส่งข้อมูลสองชนิดไปให้ผู้รับเมื่อทำการส่งข้อมูลที่ลงลายเซ็นอิเล็กทรอนิกส์แล้ว คือ ข้อมูลดั้งเดิม และ ลายเซ็นอิเล็กทรอนิกส์ ซึ่งก็คือค่า One – Way Hash ของข้อมูลดั้งเดิมแล้วเข้ารหัสด้วย Private Key ของผู้ส่ง โดยในการตรวจสอบความถูกต้องของข้อมูลที่ได้รับนั้น ผู้รับจะใช้ Public Key ของผู้ส่งเพื่อทำการถอดรหัสค่า Hash ที่ถูกเข้ารหัสมา จากนั้นจึงใช้ Hash Algorithm เดียวกันที่สร้างค่า Hash เดิมมาสร้างค่า Hash อีกครั้งแต่ด้วยตัวข้อมูลที่ได้รับมา สุดท้ายจึงทำการเปรียบเทียบค่า Hash ที่สร้างขึ้นใหม่และ ค่า Hash ที่ได้รับมา โดยถ้าค่า Hash ทั้งสองมีค่าตรงกัน จะแสดงว่าข้อมูลนั้นไม่ได้ถูกปรับเปลี่ยนตั้งแต่ลงลายเซ็นอิเล็กทรอนิกส์ ซึ่งผู้รับสามารถมั่นใจได้ว่า Public Key ที่ใช้ถอดรหัสของลายเซ็นอิเล็กทรอนิกส์ นั้นเป็นคู่ของ Private Key ที่ที่ใช้ลงลายเซ็นนั้น แต่การยืนยันว่าผู้ลงลายเซ็นนั้นเป็นบุคคลที่น่าเชื่อถือนั้น จะต้องมีการยืนยันว่า Public Key ที่ใช้นั้นเป็นของบุคคลนั้นจริง ซึ่งจะอธิบายหลักการใช้ ใบรับรองอิเล็กทรอนิกส์ ในหัวข้อถัดไปเพื่อนำมาใช้ประโยชน์ในจุดนี้

จะเห็นได้ว่าการลงลายเซ็นอิเล็กทรอนิกส์นั้นมีความสำคัญอย่างยิ่ง โดยในแง่ที่ถ้าได้ทำการลงลายเซ็นไปแล้วนั้น เป็นการยากที่จะปฏิเสธภายหลังว่าไม่ได้ทำ นอกเสียจากว่า Private Key ของผู้ใช้ได้ถูกลักลอบนำไปใช้ ซึ่งในบางกรณี การลงลายเซ็นอิเล็กทรอนิกส์นั้น สามารถนำไปใช้เป็นหลักฐานทางกฎหมายแทนลายมือชื่อได้

2.3.5 ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)

ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) คือ เอกสารทางอิเล็กทรอนิกส์ที่ใช้ระบุและยืนยัน บุคคล เซิร์ฟเวอร์ บริษัท หรือ สิ่งอื่นๆ โดยอิงกับ Public Key ของบุคคลหรือสิ่งนั้น ซึ่งกลไกการทำ Public – Key Cryptography นั้นจะอาศัยใบรับรองอิเล็กทรอนิกส์ ใช้แก้ปัญหาของการปลอมแปลงหรือแอบอ้างเป็นบุคคลอื่น (Impersonation)

โดยการใช้งานของใบรับรองอิเล็กทรอนิกส์ จะมีรูปแบบการใช้งานเหมือนเอกสารรูปแบบอื่นที่ใช้ทั่วไป เช่น บัตรประจำตัวประชาชน ใบขับขี่ และ หนังสือเดินทาง เป็นต้น สำหรับใบรับรองอิเล็กทรอนิกส์นั้น จะมี Certificate Authority (CA) ซึ่งมีหน้าที่ออกใบรับรองให้กับบุคคล หรือสิ่งที่ผ่านการตรวจสอบ และ ยืนยันหลักฐานเป็นที่เรียบร้อยแล้ว โดย CA นั้นอาจเป็นองค์กรอิสระที่ทำหน้าที่ของ CA (Trusted third party CA) หรือ เป็น CA ระดับองค์กร (Enterprise CA) ดังจะกล่าวในรายละเอียดถึงความแตกต่างต่อไป

ใบรับรองอิเล็กทรอนิกส์ที่ CA ออกให้นั้นจะทำการผูก Public Key เข้ากับชื่อของสิ่งที่ต้องการยืนยัน เช่น ชื่อของบุคคล หรือ ชื่อของเซิร์ฟเวอร์ เป็นต้น ซึ่งใบรับรองอิเล็กทรอนิกส์สามารถช่วยป้องกันการใช้ Public Key ปลอม ทั้งนี้เฉพาะ Public Key ที่ถูกรับรองด้วยใบรับรองอิเล็กทรอนิกส์เท่านั้น ที่จะสามารถนำมาทำงานร่วมกับ Private Key ของเจ้าของที่ระบุในใบรับรอง

2.3.5.1 รูปแบบการยืนยันตัวบุคคล (Forms of Authentication)

การยืนยันตัวบุคคล (Authentication) เป็นกระบวนการตรวจสอบเพื่อยืนยัน บุคคล หรือสิ่งต่างๆ ในกรณีของการติดต่อผ่านเครือข่าย Authentication จะเป็นไปในลักษณะของการติดต่อระหว่าง ไคลเอนท์ ซึ่งอาจเป็นโปรแกรม Web browser ทำงานอยู่บนเครื่องคอมพิวเตอร์ และ เซิร์ฟเวอร์ ที่ประกอบไปด้วยซอฟต์แวร์ และ ฮาร์ดแวร์ที่ใช้ในการให้บริการเว็บไซต์ (Web hosting) โดยแบ่งเป็น

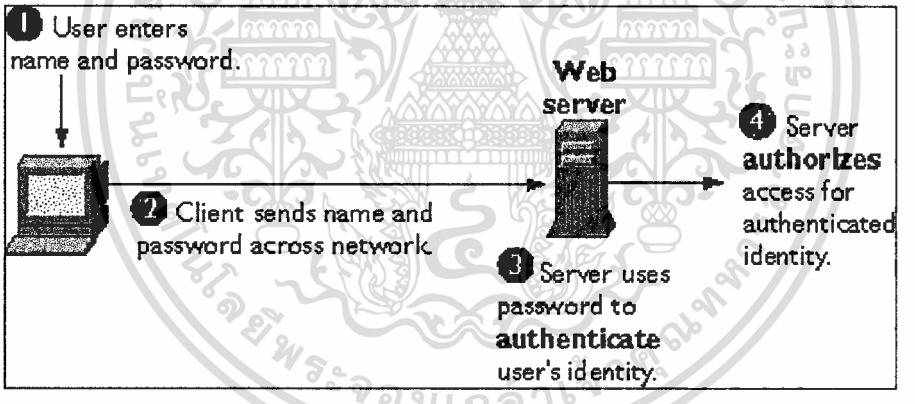
- **การยืนยันผู้เข้าใช้บริการ (Client Authentication)** คือกระบวนการยืนยันตัวบุคคลที่ต้องการใช้บริการจากทางเซิร์ฟเวอร์

- **การยืนยันผู้ให้บริการ (Server Authentication)** คือกระบวนการยืนยันถึงผู้ให้บริการหรือเครื่องเซิร์ฟเวอร์ที่ผู้ใช้บริการติดต่อ

การยืนยันผู้ใช้และผู้ให้บริการนั้นเป็นกลไกสำคัญอย่างหนึ่งของความปลอดภัยในเครือข่ายไม่ว่าจะเป็น เครือข่ายแบบภายใน (Intranet) หรือแบบเฉพาะ (Extranet) ซึ่งในส่วนถัดไปจะทำการเปรียบเทียบวิธีการยืนยันแบบต่างๆต่อไป

2.3.5.2 การยืนยันตัวบุคคลโดยใช้รหัสผ่าน (Password – Based Authentication)

เซิร์ฟเวอร์ซอฟต์แวร์ส่วนใหญ่สามารถใช้วิธีการยืนยันของผู้เข้าใช้บริการ ด้วยการใช้ ชื่อ และ รหัสผ่าน กล่าวคือทางเซิร์ฟเวอร์อาจต้องการให้ทางผู้ใช้งานพิมพ์ชื่อและรหัสผ่านก่อนที่จะให้สิทธิในการเข้าใช้ระบบงาน เพื่อตรวจสอบกับ โดยทางเซิร์ฟเวอร์จะมีรายชื่อและรหัสผ่านที่เก็บไว้ เมื่อตรวจสอบแล้วพบว่ามีชื่ออยู่ในรายชื่อจริงและใส่รหัสผ่านที่ถูกต้อง ทางเซิร์ฟเวอร์ก็จะให้สิทธิผู้ใช้งานดังกล่าวเพื่อเข้าใช้ระบบ



รูปที่ 2.7 แสดงขั้นตอนการยืนยันตัวบุคคลโดยใช้รหัสผ่าน

จากรูปที่ 2.7 แสดงถึงขั้นตอนในการยืนยันตัวบุคคลโดยใช้รหัสผ่าน ดังนี้

1. เมื่อทางเซิร์ฟเวอร์ต้องการให้ผู้ใช้งาน (User) ยืนยันตัวเอง จะปรากฏหน้าจอให้ใส่ ชื่อ และ รหัสผ่านสำหรับเซิร์ฟเวอร์นั้น โดยผู้ใช้งานจะต้องใส่ชื่อ และ รหัสผ่าน ของแต่ละเซิร์ฟเวอร์ที่ผู้ใช้ต้องการใช้บริการในช่วงการทำงาน
2. จากนั้นผู้ใช้งานจึงส่ง ชื่อ และ รหัสผ่าน ข้ามเครือข่ายมาที่เซิร์ฟเวอร์ ด้วยการเชื่อมต่อแบบธรรมดา (ไม่มีการเข้ารหัส) หรือ ด้วยการเชื่อมต่อแบบเข้ารหัสด้วย SSL
3. เซิร์ฟเวอร์ตรวจสอบ ชื่อ และ รหัสผ่านกับฐานข้อมูลรหัสผ่านที่เซิร์ฟเวอร์เก็บไว้ ถ้าชื่อและรหัสตรงกัน จะถือเป็นหลักฐานได้ว่าผู้ใช้งานได้ทำการยืนยันตัวเองแล้ว

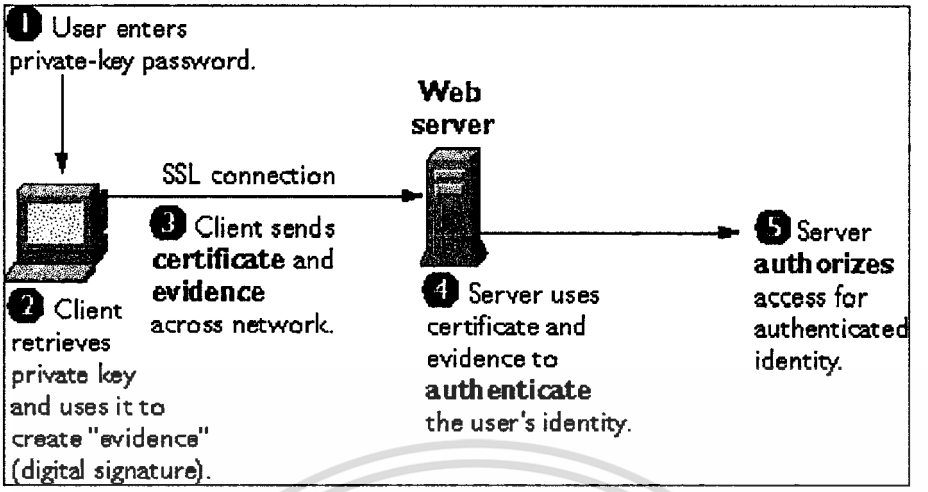
4. จากนั้นเซิร์ฟเวอร์จึงตรวจสอบสิทธิการใช้งานในระบบของผู้ใช้งานเพื่ออนุญาตให้เข้าไปใช้ทรัพยากรที่ขอมาต่อไป

จะเห็นได้ว่าการยืนยันตัวบุคคลโดยใช้รหัสผ่านนั้นมีจุดบกพร่องอยู่มากมาย กล่าวคือ

1. ผู้ใช้งานจะต้องจดจำ ชื่อและรหัสผ่าน สำหรับแต่ละเซิร์ฟเวอร์ (การใช้ชื่อและรหัสผ่านเดียวกันสำหรับทุกเซิร์ฟเวอร์นั้นไม่ปลอดภัย) และผู้ใช้งานมักจะลืมรหัสผ่านอยู่บ่อยๆ ส่งผลให้ผู้จัดการระบบ (Administrator) จะต้องคอยจัดการชื่อและรหัสผ่านของผู้ใช้งานอยู่เป็นประจำ
2. ลักษณะการส่งรหัสผ่านซึ่งเป็นข้อมูลที่เป็นความลับ โดยทำการส่งข้ามเครือข่ายทุกครั้งที่ต้องการทำการยืนยัน เป็นขั้นตอนที่เสี่ยงต่อความปลอดภัย เช่น อาจถูกดักอ่านรหัสผ่านกลางทาง ถ้าการเชื่อมต่อไม่ได้เข้ารหัสที่แข็งแรงเพียงพอ
3. ทางเซิร์ฟเวอร์จะต้องเก็บฐานข้อมูล ชื่อและรหัสผ่านซึ่งถึงแม้จะมีการเข้ารหัสฐานข้อมูลดังกล่าว แต่กรณีเหตุการณ์การโจรกรรม และ เจาะการเข้ารหัสฐานข้อมูลของรหัสผ่านนั้น มีเกิดขึ้นมากมาย
4. การใช้รหัสผ่านนั้น ไม่มีหลักฐานใดที่สามารถระบุและยืนยันได้ว่าบุคคลใดคือผู้ใช้รหัสผ่านนั้นเข้ามาที่เซิร์ฟเวอร์ ซึ่งอาจมีการนำรหัสผ่านของผู้อื่นมาใช้และแอบอ้างว่าเป็นบุคคลนั้น

2.3.5.3 การยืนยันตัวบุคคลโดยใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate – Based Authentication)

วิธีการยืนยันของผู้เข้าใช้บริการ ด้วยการใช้ใบรับรองอิเล็กทรอนิกส์นั้นเป็นส่วนหนึ่งของกลไกการทำโปรโตคอล SSL กล่าวคือทางผู้ใช้บริการจะทำการลงลายเซ็นอิเล็กทรอนิกส์กับข้อมูลที่สุ่มขึ้นมา และ ส่งใบรับรองอิเล็กทรอนิกส์มากับข้อมูลที่ได้ลงลายเซ็นแล้ว ผ่านเครือข่ายมายังเซิร์ฟเวอร์ซึ่งใช้กระบวนการถอดรหัสแบบ Public Key cryptography เพื่อทำการตรวจสอบ (Validate) ลายเซ็น และ ใบรับรองอิเล็กทรอนิกส์ที่ส่งมา โดยทั่วไปแล้วการยืนยันโดยใช้ใบรับรองอิเล็กทรอนิกส์นี้เป็นวิธีการยืนยันที่ควรทำมากกว่าแบบการใช้รหัสผ่าน เนื่องจากเป็นวิธีการที่ใช้สิ่งที่ผู้ใช้งานมีอยู่ ก็คือ Private Key และ สิ่งที่ผู้ใช้งานรู้ ก็คือ รหัสผ่านที่ใช้ควบคุมการใช้ Private Key (ใช้ที่เครื่องผู้ใช้ ไม่มีการส่งผ่านเครือข่าย)



รูปที่ 2.8 แสดงขั้นตอนการยืนยันตัวบุคคลโดยใช้ใบรับรองอิเล็กทรอนิกส์

จากรูปที่ 2.8 แสดงถึงขั้นตอนการยืนยันตัวบุคคล โดยใช้ใบรับรองอิเล็กทรอนิกส์ ดังนี้

1. ผู้ใช้งานจะต้องใส่รหัสผ่านสำหรับเข้าถึงส่วนจัดเก็บ Private Key ของผู้ใช้งาน ซึ่งจะถูกจัดการโดยระบบปฏิบัติการหรือซอฟต์แวร์ที่ใช้ในเครื่องของผู้ใช้งาน
2. หลังจากที่ผู้ใช้งานได้เปิดส่วนจัดเก็บ Private Key ของตน และนำ Private Key ที่สอดคล้องกับคู่กุญแจ Public Key ที่ระบุในใบรับรองมาทำการลงลายเซ็นอิเล็กทรอนิกส์กับข้อมูลที่สุ่มขึ้นมา โดยใช้ข้อมูล และ ลายเซ็นนี้ เป็นหลักฐานในการยืนยัน Private Key ที่ใช้ ซึ่งลายเซ็นอิเล็กทรอนิกส์นี้จะสามารถถูกสร้างได้ด้วย Private Key นี้เท่านั้น และ ตรวจสอบได้ด้วย Public Key ที่เป็นคู่กัน
3. จากนั้นผู้ใช้งานทำการส่งใบรับรองอิเล็กทรอนิกส์ และ "หลักฐาน" คือ ข้อมูลที่สุ่มขึ้นมาที่ถูกลงลายเซ็นอิเล็กทรอนิกส์เรียบร้อยแล้ว ผ่านเครือข่ายมายังเซิร์ฟเวอร์
4. เซิร์ฟเวอร์ตรวจสอบความถูกต้องของลายเซ็นอิเล็กทรอนิกส์ด้วย Public Key ที่ระบุในใบรับรอง (ดังรายละเอียดการตรวจสอบที่ได้กล่าวไปในหัวข้อ 2.3.4)
5. จากนั้นทางเซิร์ฟเวอร์อาจตรวจสอบใบรับรองที่ได้รับกับส่วนจัดเก็บใบรับรองที่เซิร์ฟเวอร์มีอยู่ และตรวจสอบสิทธิการใช้งานในระบบของผู้ใช้งานเพื่ออนุญาตให้เข้าไปใช้ทรัพยากรที่ขอมาต่อไป

ด้วยการใช้ใบรับรองในการยืนยันบุคคล ทำให้สามารถช่วยแก้ปัญหาของการใช้รหัสผ่าน คือ ผู้ใช้งานไม่จำเป็นที่จะต้องจดจำรหัสผ่านที่มากมาย แค่จำรหัสผ่านที่ใช้ควบคุมการเข้าถึง Private Key ของตนก็เพียงพอ ซึ่งรหัสผ่านนี้เป็นรหัสที่ใช้เฉพาะในเครื่องของผู้ใช้งานเท่านั้น ซึ่งไม่มีการส่งผ่านเครือข่ายให้เกิดความเสี่ยง และทางเซิร์ฟเวอร์จะมีเพียงแต่ฐานข้อมูลจัดเก็บใบรับ

รอง ซึ่งถึงแม้ฐานข้อมูลดังกล่าวจะถูกโจรกรรมไป ก็ไม่มีผลกระทบต่อข้อมูลที่ลงลายเซ็นอิเล็กทรอนิกส์มาภายหลังเพราะ Private Key ยังอยู่กับผู้ใช้งาน ทำให้ผู้โจรกรรมนั้นไม่สามารถปลอมแปลงลายเซ็นอิเล็กทรอนิกส์ได้เลย (ไม่สามารถทำ Impersonation ได้)

แต่ทั้งนี้ประเด็นที่สำคัญคือไม่ว่าจะเป็นการยืนยันด้วยรหัสผ่าน หรือ ใบรับรองอิเล็กทรอนิกส์ ต่างก็ไม่สามารถแก้ปัญหาในเรื่องทางกายภาพของการลักลอบเข้าใช้ระบบ ซึ่งขอบเขตของ Public Key Cryptography คือการยืนยันว่า Private Key ที่ใช้ลงลายเซ็นอิเล็กทรอนิกส์นั้น เป็นกุญแจคู่กับ Public Key ที่ระบุในใบรับรอง โดยผู้ใช้งานจะต้องรับผิดชอบในการรักษาความปลอดภัยทางกายภาพของเครื่องคอมพิวเตอร์ และ รักษาความลับของรหัสผ่านที่ใช้ควบคุมการใช้ Private Key ของตน

2.3.5.4 Certificate Authority

Certificate Authority (CA) มีหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ให้กับบุคคล หรือ สิ่งที่ผ่านการตรวจสอบ และ ยืนยันหลักฐานเป็นที่เรียบร้อยแล้ว โดย CA นั้นอาจเป็นองค์กรอิสระที่ทำหน้าที่ของ CA โดยเฉพาะ (Trusted third party CA) ซึ่งอาจเรียกว่าเป็น CA เพื่อการพาณิชย์ (Commercial CA) หรือ อาจเป็น CA ในระดับองค์กร (Enterprise CA) โดยมีรายละเอียดดังนี้

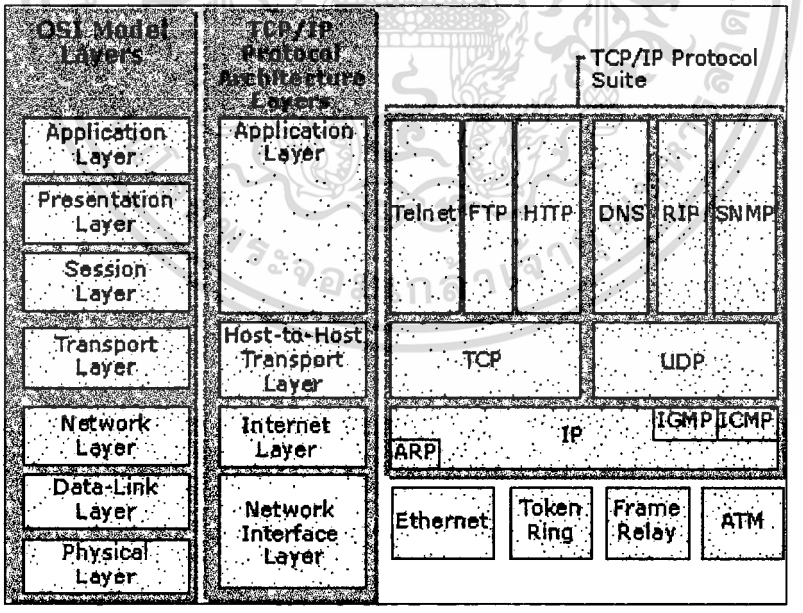
1. **CA เพื่อการพาณิชย์ (Commercial CA หรือ Trusted third party CA)** คือ CA ที่จัดตั้งขึ้นเพื่อเป็นบุคคลกลางทำหน้าที่ในการยืนยันบุคคล บริษัท หรือสิ่งต่างๆที่ต้องการการยืนยัน โดยอิงกับ Public Key ของบุคคลหรือสิ่งนั้น และออกใบรับรองอิเล็กทรอนิกส์เพื่อพิสูจน์ว่าบุคคลนั้น หรือ สิ่งนั้นเป็นตัวจริง และ เป็นเจ้าของ Public Key ที่ระบุไว้ในใบรับรอง ลักษณะการใช้งานของ CA เพื่อการพาณิชย์นั้น จะใช้สำหรับการออกใบรับรองของกลุ่มผู้ใช้ในระดับกว้างเช่นผู้ใช้งานในเครือข่าย อินเตอร์เน็ต เนื่องจากลักษณะเครือข่ายมีขนาดที่ใหญ่และมีผู้ใช้งานเป็นจำนวนมากซึ่งต้องการบุคคลกลางที่น่าเชื่อถือเข้ามารับรองบุคคลในแต่ละฝ่ายที่ต้องการติดต่อกันด้วยความมั่นใจ
2. **CA ในระดับองค์กร (Enterprise CA หรือ Organization CA)** คือ CA ที่จัดตั้งขึ้นเพื่อตอบสนองความต้องการในระดับองค์กรในการออกใบรับรองอิเล็กทรอนิกส์ เพื่อทำจัดการผู้ใช้งานที่ต้องการติดต่อและใช้งานระบบ ดังตัวอย่างเช่นในกรณีของเครือข่ายเฉพาะกิจเช่น Virtual Private Network หรือ Extranet ที่ต้องการให้กลุ่มผู้ใช้งานที่ได้รับอนุญาติสามารถติดต่อเข้ามาทำธุรกรรม ในลักษณะที่มีความปลอดภัย ซึ่งในกรณีเช่นนี้ องค์กรจะมีความต้องการที่จะจัดตั้ง CA เป็นของตนเพื่อควบคุมการออกใบรับรองอิเล็กทรอนิกส์ที่สามารถนำไปใช้ยืนยันตัวบุคคลที่ต้องการทำการติดต่อกับองค์กรต่อไป

2.4 หลักการทำงานของโปรแกรมประยุกต์ผ่าน เวิลด์ ไวด์ เว็บ

เครือข่ายอินเตอร์เน็ต (Internet) เป็นสื่อทางอิเล็กทรอนิกส์ ที่ใช้ในการแลกเปลี่ยนข้อมูลข่าวสารกันทั่วโลก โดยมี เวิลด์ ไวด์ เว็บ (World Wide Web) เป็นตัวกลางทำให้ผู้ใช้งานสามารถเรียกดูข้อมูลข่าวสารที่มีอยู่ในระบบอินเตอร์เน็ตจาก เว็บเพจ (Web page) ที่เขียนด้วยภาษา Hypertext Markup Language (HTML) ผ่านโปรโตคอล HTTP ด้วยซอฟต์แวร์ Web Browser ซึ่งในปัจจุบันได้ถูกพัฒนาให้มีความสามารถรองรับเทคโนโลยีใหม่ๆที่หลากหลาย เช่นความสามารถในการเรียกใช้ Java, ActiveX Control และ Dynamic HTML เป็นต้น ทำให้ เว็บเพจ สามารถทำงานได้มากกว่าการเชื่อมต่อไปยัง เว็บเพจอื่นๆ แต่สามารถถูกพัฒนาให้เป็นโปรแกรมประยุกต์เพื่อการใช้งานได้จริง

2.4.1 สถาปัตยกรรมชุดโปรโตคอล TCP / IP และ โปรโตคอล HTTP

TCP / IP เป็นสถาปัตยกรรม มาตรฐานออกแบบสำหรับการทำงานในเครือข่ายระดับใหญ่ เช่น Wide Area Network (WAN) โดยลักษณะโครงสร้างของโปรโตคอล TCP/IP นั้นจะอิงกับ DARPA model ประกอบไปด้วย 4 ระดับชั้นคือ Application, Transport, Internet และ Network Interface เทียบเท่ากับโครงสร้างของ Open Systems Interconnection (OSI) model ได้ดังรูปที่ 2.9



รูปที่ 2.9 แสดงถึงสถาปัตยกรรมของโปรโตคอล TCP/IP

จากรูปที่ 2.9 Application Layer ของโปรโตคอล TCP/IP นั้นจะเทียบเท่ากับ Application, Presentation และ Session Layer ของ OSI model โดยในแต่ละLayer นั้นจะมีลักษณะขั้นตอนการทำงานดังนี้

1. **Network Interface Layer** จะประกอบไปด้วยโปรโตคอลที่ทำหน้าที่ติดต่อสื่อสารเข้ากับเครือข่าย หน้าที่ของโปรโตคอลใน Layer ชั้นนี้คือจัดเส้นทางของข้อมูลให้ระหว่างโฮสต์กับโฮสต์ ควบคุมการไหลของข้อมูล และควบคุมความผิดพลาดของข้อมูล
2. **Internet Layer** ประกอบด้วยขั้นตอนการอนุญาตให้ข้อมูลไหลผ่านไปมาระหว่างโฮสต์ของเครือข่าย 2 เครือข่ายหรือมากกว่า ดังนั้นโปรโตคอลใน Layer ชั้น Internet นอกจากจะมีหน้าที่จัดเส้นทางของข้อมูลแล้ว ยังต้องทำหน้าที่เป็น Gateway สำหรับการติดต่อกับเครือข่ายอื่นอีกด้วย
3. **Host-to-Host Transport Layer** ประกอบด้วยโปรโตคอลที่ทำหน้าที่ส่งผ่านแลกเปลี่ยนข้อมูลระหว่างเอนทิตี้ของโฮสต์ต่างเครื่องกัน นอกจากนั้นโปรโตคอลใน Layer นี้ยังมีหน้าที่ควบคุมการไหลของข้อมูลและควบคุมความผิดพลาดของข้อมูลด้วย
4. **Application Layer** ประกอบด้วยโปรโตคอลที่ทำหน้าที่ แลกเปลี่ยนข้อมูลซึ่งกันและกันระหว่างคอมพิวเตอร์กับคอมพิวเตอร์ หรือ คอมพิวเตอร์กับ Terminal ที่อยู่ไกลออกไป

Hypertext Transfer Protocol (HTTP) เป็นโปรโตคอลที่ใช้งานในระดับชั้น Application Layer ใช้สำหรับสื่อสารระหว่างเครื่องคอมพิวเตอร์ของผู้ใช้งาน กับ HTTP เซิร์ฟเวอร์เพื่อโอนย้ายข้อมูล การเรียกใช้บริการนั้นมักมาจากซอฟต์แวร์ Web browser มายัง HTTP เซิร์ฟเวอร์ ลักษณะการทำงานของโปรโตคอล HTTP นั้นเป็นแบบ Request / Response กล่าวคือทางไคลเอนท์จะทำการส่ง Request message ไปยังเซิร์ฟเวอร์ที่ต้องการขอใช้ทรัพยากร ซึ่งโดยทั่วไปแล้วจะส่งผ่าน TCP port 80 เมื่อทางเซิร์ฟเวอร์ได้รับ Request แล้วจะทำการตอบ Response message ที่ระบุถึงผลของคำขอว่าสำเร็จหรือไม่

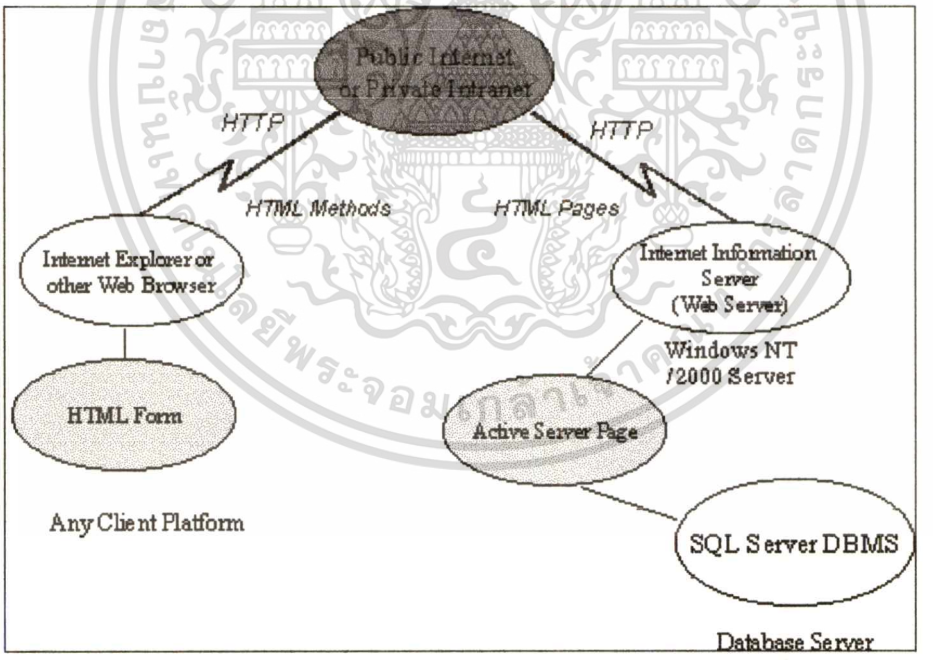
2.4.2 หลักการทำงานของโปรแกรมประยุกต์ผ่าน เวิลด์ ไวด์ เว็บ

เวิลด์ ไวด์ เว็บ (World Wide Web: WWW) หรือ เว็บ (Web) เป็นตัวกลางของการสื่อสารที่สามารถนำข้อมูลที่อยู่แบบกระจายมารวมอยู่ในสื่อเดียวกันได้ ดังเช่น เว็บเพจที่สามารถประกอบไปด้วย ข้อความ แผนภาพ และสื่ออื่นๆในเพจเดียวกัน โปรแกรมประยุกต์ผ่านเว็บ (Web – Base Application) คือรูปแบบของโปรแกรมประยุกต์ชนิดหนึ่งซึ่งอาศัยกลไกการทำงานของเว็บซึ่งมีคุณสมบัติที่เหมาะต่อการนำไปเป็น Platform ในการพัฒนาโปรแกรมที่ใช้งานในสภาพแวดล้อมแบบกระจาย กล่าวคือ

- มีรูปแบบสถาปัตยกรรมแบบเปิด (Open Architecture) สามารถรองรับการใช้งานได้จากหลากหลาย Platform (Platform independent)

- มีลักษณะการทำงานของระบบแบบกระจาย (Distributed system) สามารถกระจายการทำงานออกไปได้โดยครอบคลุมพื้นที่ได้กว้างไกลถึง ทั่วโลก
- มีกลไกทางด้านความปลอดภัยของเครือข่ายรองรับหลากหลายวิธีการ
- ง่ายต่อการนำไปใช้งานและบำรุงรักษา (Ease of deployment) เนื่องจากการปรับเปลี่ยนของโปรแกรมนั้นสามารถทำที่เซิร์ฟเวอร์ที่เดียว โดยไม่ต้องติดตั้งโปรแกรมใหม่ที่ไคลเอนท์

โดยสถาปัตยกรรมของโปรแกรมประยุกต์ผ่านเว็บนั้น จะใช้ภาษา HTML ในการสร้างหน้าจอสำหรับการเข้าใช้งาน (User Interface) ซึ่งจะถูกเรียกใช้โดยผู้ใช้งานมาที่ Web เซิร์ฟเวอร์ เมื่อผู้ใช้งานทำการส่งฟอร์ม ข้อมูลจะถูกส่งมาที่ Web เซิร์ฟเวอร์ โดยใช้ HTML method แบบ Post ซึ่งทางเซิร์ฟเวอร์ ในกรณีที่เป็น Internet Information Server (IIS) ที่ทำงานกับ Windows NT/2000 นั้น จะมีกลไกที่เรียกว่า Active Server Page (ASP) ทำการประมวลผลข้อมูลที่ได้รับ และส่งผลลัพธ์ของการประมวลกลับไปให้ผู้ใช้งานในรูปของ HTML ดังรูปที่ 2.10

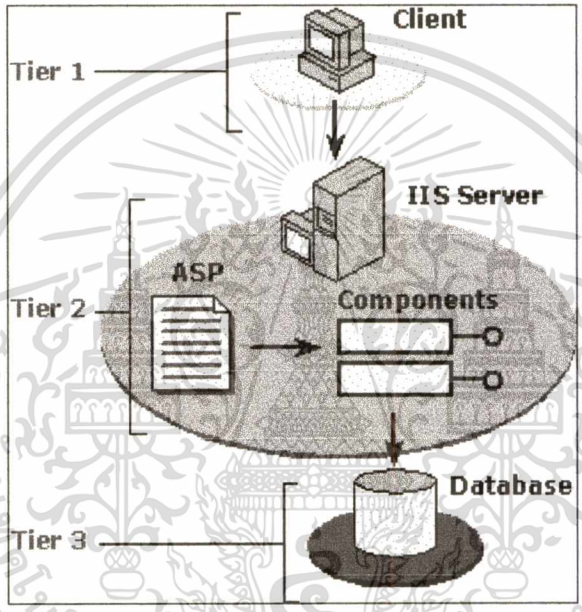


รูปที่ 2.10 แสดงถึงสถาปัตยกรรมของ Web Application

จากรูปที่ 2.10 แสดงถึงสถาปัตยกรรมของ Web Application ซึ่งผู้ใช้งานทำการติดต่อสื่อกับตัว Web Application ผ่าน HTML Form ดังแสดงใน Web browser และส่ง HTML method ผ่านเครือข่ายมายัง เซิร์ฟเวอร์เพื่อประมวลผลด้วยกลไกของ Active Server Page

2.4.3 Active Server Page

ASP เป็นเทคนิคแบบ Server Based พัฒนาโดยบริษัท Microsoft โดยเป็นส่วนหนึ่งของเทคนิคทางด้าน Active Server ที่ Microsoft ใช้ในการพัฒนาโปรแกรม Web Server ที่ชื่อว่า Internet Information Server (IIS) ปัจจุบันเวอร์ชัน 3.0 เป็นเวอร์ชันล่าสุดของ ASP และ 5.0 เป็นเวอร์ชันล่าสุดของ IIS ซึ่งมาพร้อมกับระบบปฏิบัติการ Windows 2000 โดย IIS จะทำงานอยู่ใน Tier ที่ 2 ซึ่งเป็น Business Logic ทำการประมวลผลข้อมูลต่างๆ ดังแสดงในรูปที่ 2.11



รูปที่ 2.11 แสดงถึงสถาปัตยกรรมของ IIS

การทำงานของ ASP จะมีลักษณะเป็น Server – side scripting ซึ่งหมายความถึง ภาษาที่ใช้ในการโปรแกรมนั้นทำงานอยู่ในเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น Web Server ที่ให้บริการการเรียกดูเอกสารหรือข้อมูลผ่านหน้าจอ Web Browser โดยใช้เสริมความสามารถในการทำงานของ HTML แบบธรรมดาให้สามารถทำงานได้ดีขึ้น เช่นการปรับข้อมูลบนหน้าจอที่แสดงแบบอัตโนมัติเมื่อมีข้อมูลเข้ามาใหม่ที่ฐานข้อมูล โดยที่ผู้สร้างเว็บเพจไม่ต้องทำการเปลี่ยนแปลงด้วยมือทุกครั้งที่ข้อมูลเปลี่ยน ซึ่งการทำงานเช่นนี้จะเหมาะสำหรับงานประเภทการเรียกใช้ข้อมูลผ่านเว็บที่มีการเปลี่ยนแปลงบ่อย และทำให้ง่ายต่อการพัฒนาโปรแกรมประยุกต์ผ่านเว็บ เช่น การพัฒนากระดานสนทนา (Web board) การพัฒนาห้องสนทนา (Chat room) หรือ ใช้ในการพัฒนาโปรแกรมประยุกต์ ที่ต้องมีการปรับปรุงเปลี่ยนแปลงบ่อยครั้ง

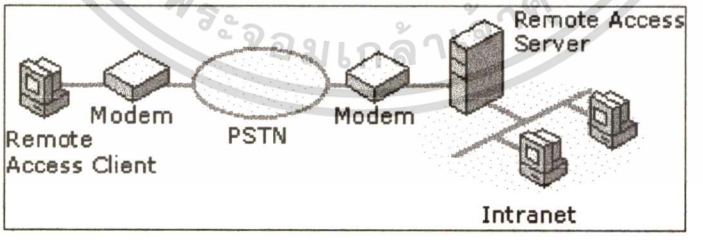
หลักการทำงานของ ASP เริ่มจากผู้ใช้ ASP สร้างไฟล์ที่มีนามสกุล .asp ขึ้นมา จากนั้นนำไฟล์นั้นไปไว้ในเครื่องที่ทำหน้าที่เป็น Web Server ที่ติดตั้ง IIS ไว้ และเชื่อมต่ออยู่กับเครือข่าย จากนั้นเมื่อผู้ใช้งานทำการเรียกใช้ไฟล์นั้นผ่านโปรแกรม Web Browser ตัวโปรแกรม ASP ใน Web server จะเรียกไฟล์นั้นขึ้นมาประมวลผล ตามที่เขียนไว้เป็นลักษณะ Server – Side Scripting ที่ผู้สร้างได้กำหนดไว้ เมื่อประมวลผลเสร็จแล้วจึงส่งผลลัพธ์ที่อยู่ในรูป HTML กลับไปแสดงผลบนหน้าจอ Web Browser ของผู้ใช้งาน

2.5 หลักการทำงานของ Remote Access Service

Remote Access Service คือบริการการเชื่อมต่อผ่านเครือข่ายจากผู้ใช้งานที่อยู่นอกสถานที่เพื่อเข้ามาใช้บริการในระบบ ทั้งนี้การทำ Remote Access มีส่วนประกอบของการทำงานคือ

1. **Remote Access Client** คือ ผู้ใช้งานที่ต้องการทำการเชื่อมต่อเข้ามาขอใช้บริการ
2. **Remote Access Server** คือ เซิร์ฟเวอร์ที่ทำหน้าที่ให้บริการในการเชื่อมต่อ เช่น การทำ Dial – up connection และเซิร์ฟเวอร์จะทำหน้าที่คอย Forward Packet ต่างๆระหว่าง Remote Access Client และ เครือข่ายที่ Remote Server เชื่อมต่ออยู่

หนึ่งในลักษณะการเชื่อมต่อเข้ากับ Remote Access Service ที่นิยมใช้คือการทำ Dial – Up connection ผ่านเครือข่ายชุมสายโทรศัพท์ (Public Switched Telephone Network หรือ PSTN) โดยเป็นระบบชุมสายโทรศัพท์แบบ Analog ออกแบบมาเพื่อใช้กับสัญญาณเสียง จึงทำให้มีข้อจำกัดในความสามารถในการส่งข้อมูลได้สูงสุดที่ 33,600 บิต ต่อ วินาที



รูปที่ 2.12 แสดงถึงการทำ Dial – up ผ่านชุมสายโทรศัพท์ (PSTN)

จากรูปที่ 2.12 แสดงถึงอุปกรณ์ที่ใช้ในการทำ Dial – up ผ่านชุมสายโทรศัพท์ (PSTN) โดยทาง Remote Access Client จะมี Modem เพื่อทำการหมุนเข้ามาที่ Remote Access Server ซึ่งจะมี Modem Pool ที่คอยรับ Dial – Up connection จาก Client ทั้งนี้โปรโตคอลที่นิยมใช้ในปัจจุบันคือ Point – to – Point Protocol (PPP) เนื่องจากเป็นโปรโตคอลมาตรฐานที่รองรับกลไกความปลอดภัยและ การเชื่อมต่อที่เสถียร ซึ่งเป็นคุณสมบัติที่เหมาะสำหรับการทำ Remote Access อย่างยิ่ง

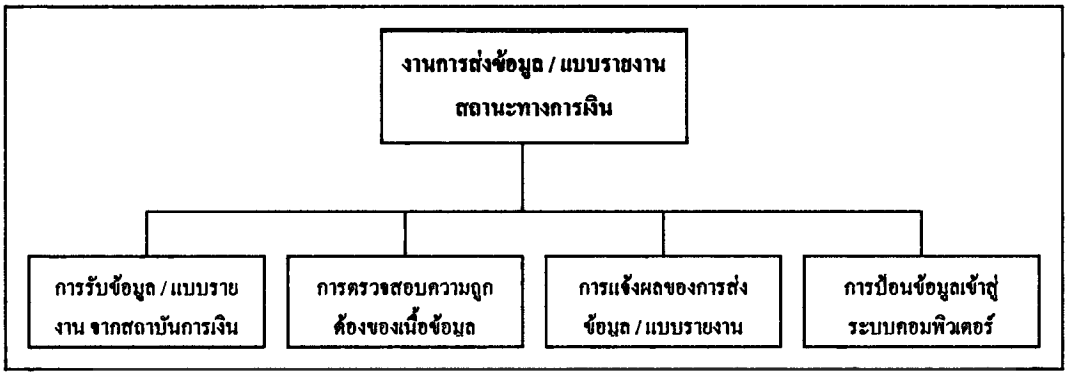
บทที่ 3
การวิเคราะห์ระบบงาน

ในบทนี้จะกล่าวถึงการวิเคราะห์ระบบงานปัจจุบันของ การส่งข้อมูล / แบบรายงานสถานะทางการเงินของสถาบันการเงินมาที่ศูนย์รับข้อมูลของธนาคารแห่งประเทศไทย ซึ่งจะครอบคลุมถึงการวิเคราะห์การปฏิบัติงานในปัจจุบัน ลำดับขั้นตอนของการทำงาน ตลอดจนปัญหาและอุปสรรคที่พบจากการวิเคราะห์ เพื่อเป็นการนำไปสู่การออกแบบระบบงาน โดยใช้แผนภาพรวมของระบบ (Context Diagram) และแผนภาพการไหลเวียนของข้อมูล (Data Flow Diagram) เป็นเครื่องมือในการวิเคราะห์

3.1 การปฏิบัติงานในปัจจุบัน

การทำงานของ การส่งข้อมูล / แบบรายงานสถานะทางการเงินของสถาบันการเงิน มาที่ศูนย์รับข้อมูลของธนาคารแห่งประเทศไทยในปัจจุบันนั้น จะมีลักษณะการทำงานเป็นแบบ Manual System ซึ่งต้องอาศัยการทำงานของเจ้าหน้าที่เป็นหลัก แม้ว่าจะมีการนำเครื่องคอมพิวเตอร์มาใช้แล้วก็ตาม แต่การใช้งานคอมพิวเตอร์ดังกล่าวนั้น จะเป็นเพียงการใช้งานในด้านของการป้อนข้อมูลเข้าและพิมพ์เอกสารเป็นหลัก และยังคงต้องมีการจัดเก็บแบบรายงานและเอกสารกระดาษที่เกี่ยวข้องเป็นจำนวนมาก ซึ่งจากการศึกษาถึงการทำงานของระบบนั้น สามารถสรุปหน้าที่หลักของงานการส่งข้อมูล / แบบรายงานสถานะทางการเงินของสถาบันการเงิน มาที่ศูนย์รับข้อมูลได้ดังต่อไปนี้

- ดำเนินการเกี่ยวกับ การรับข้อมูล / แบบรายงานสถานะทางการเงิน จากสถาบันการเงิน
- ดำเนินการเกี่ยวกับ การตรวจสอบความถูกต้องของเนื้อข้อมูลที่ได้รับ
- ดำเนินการเกี่ยวกับ การแจ้งผลของการส่งข้อมูล / แบบรายงาน
- ดำเนินการเกี่ยวกับ การบันทึกข้อมูล / แบบรายงานเข้าสู่ระบบคอมพิวเตอร์

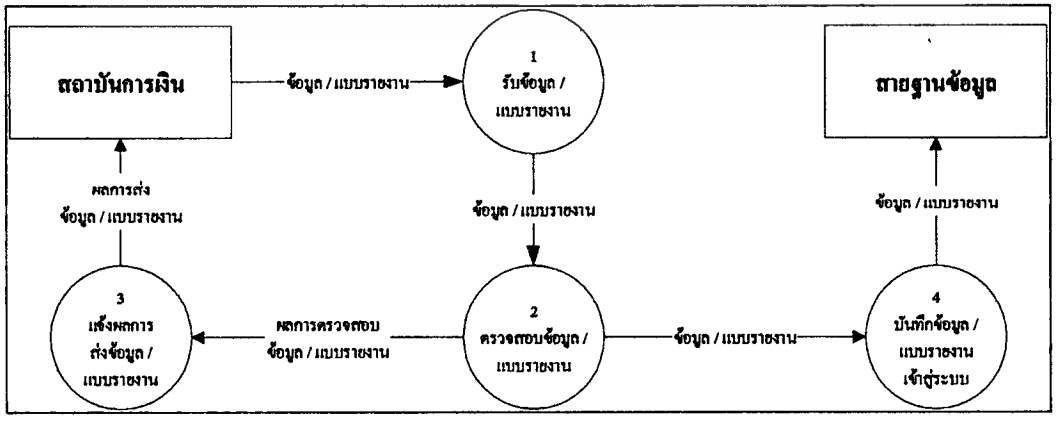


รูปที่ 3.1 แสดงหน้าที่หลักของงาน การส่งข้อมูล / แบบรายงานสถานะทางการเงิน

3.2 ลำดับขั้นตอนการทำงาน

จากการศึกษาระบบงานปัจจุบัน สามารถนำมาแสดงรายละเอียดด้วยลำดับขั้นตอนการทำงาน ตลอดจนทิศทางการส่งผ่านและไหลเวียนของข้อมูลและเอกสารต่างๆ โดยสรุปเป็นแผนภาพรวมของระบบ (Context Diagram) และแผนภาพรวมของการไหลเวียนของข้อมูล (Data Flow Diagram) ได้ดังต่อไปนี้

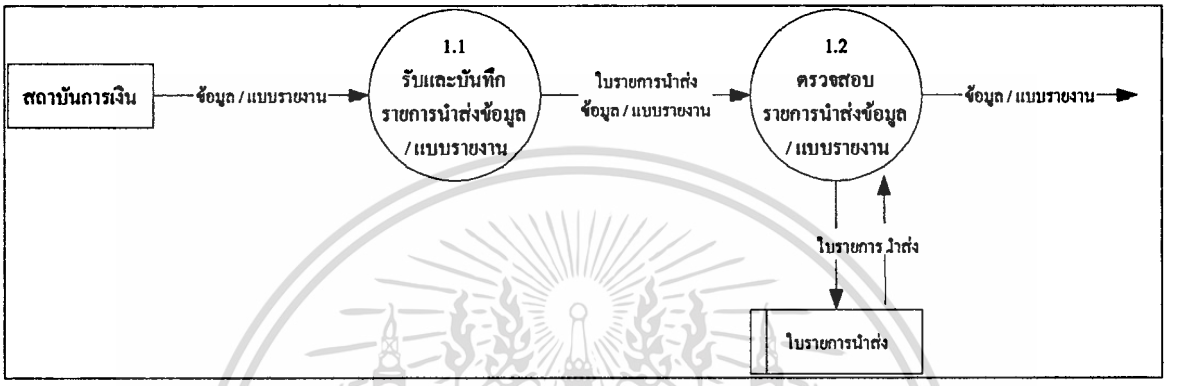
รูปที่ 3.2 แผนภาพรวมของระบบ (Context Diagram)



รูปที่ 3.3 แผนภาพรวมของการไหลเวียนของข้อมูลในระบบ (Context Diagram)

โดยที่รายละเอียดของการทำงานในแต่ละงานนั้นสามารถแสดงออกมาเป็นแผนภาพการไหลเวียนของข้อมูลต่างๆ ได้ดังต่อไปนี้

3.2.1 การรับข้อมูล / แบบรายงาน จากสถาบันการเงิน



รูปที่ 3.4 แผนภาพการไหลเวียนของข้อมูลในส่วนของการรับข้อมูล / แบบรายงาน

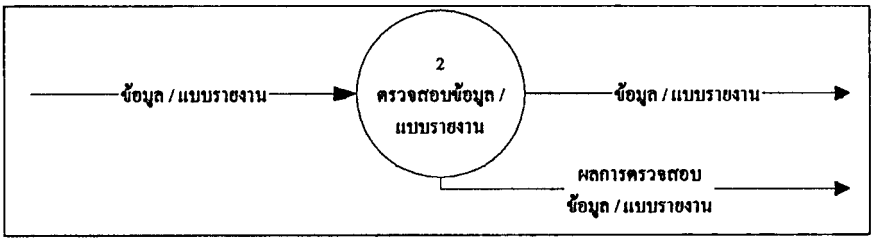
การรับข้อมูล / แบบรายงานจากสถาบันการเงินนั้นมีขั้นตอนดังนี้

3.2.1.1 สถาบันการเงินทำการส่งข้อมูล / แบบรายงานผ่านผู้นำส่งเอกสาร ซึ่งข้อมูล / แบบรายงานอาจอยู่ในรูปแบบของสื่อกระดาษ แผ่นดิสก์ และ เทปแม่เหล็ก

3.2.1.2 เจ้าหน้าที่รับข้อมูล / แบบรายงาน และ ทำการบันทึกรายการการนำส่ง ลงในใบรายการนำส่ง

3.2.1.3 เจ้าหน้าที่ตรวจสอบรายการของข้อมูล / แบบรายงานที่นำส่ง ถ้าเป็นการส่งข้อมูล / แบบรายงานที่ได้เคยส่งแล้ว เจ้าหน้าที่จะตรวจสอบเอกสารแนบชี้แจงการส่งข้อมูล / แบบรายงานซ้ำ และนำใบรายการนำส่งเก็บไว้ในตู้เก็บเอกสาร

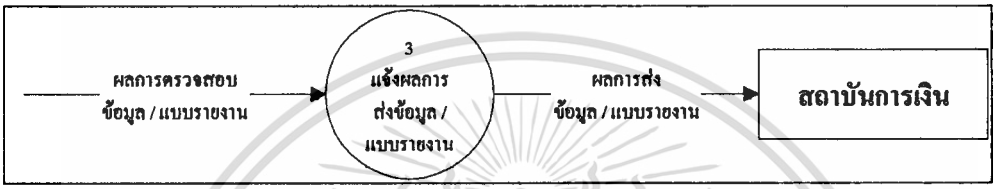
3.2.2 การตรวจสอบความถูกต้องของเนื้อข้อมูล / แบบรายงาน ที่ได้รับ



รูปที่ 3.5 แผนภาพการไหลเวียนของข้อมูลในส่วนของการตรวจสอบความถูกต้องของข้อมูล

การตรวจสอบความถูกต้องของเนื้อข้อมูล / แบบรายงานที่ได้รับนั้น จะเป็นขั้นตอนที่ตรวจสอบว่าเนื้อข้อมูล / แบบรายงานที่ส่งมานั้นมีรูปแบบที่ถูกต้อง ตรงตามรูปแบบที่ได้กำหนดไว้ให้สถาบันการเงินปฏิบัติตาม ทั้งนี้จะมีลักษณะรูปแบบเฉพาะตามรายงาน / ข้อมูลในแต่ละแบบ

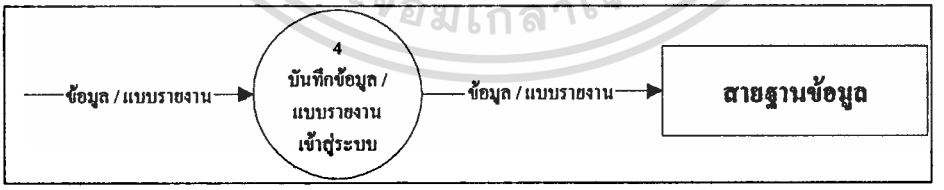
3.2.3 การแจ้งผลการส่งข้อมูล / แบบรายงาน



รูปที่ 3.6 แผนภาพการไหลเวียนของข้อมูลในส่วนของการแจ้งผลการส่งข้อมูล / แบบรายงาน

การแจ้งผลการส่งข้อมูล / แบบรายงานนั้น จะเป็นขั้นตอนที่ทางศูนย์รับข้อมูลแจ้งให้ทางสถาบันการเงินทราบถึงผลของการส่งข้อมูล / แบบรายงาน ว่าสิ่งที่ส่งมานั้นมีความถูกต้องหรือมีข้อผิดพลาดอย่างไร เพื่อทางสถาบันการเงินจะได้แก้ไขและนำส่งข้อมูล / แบบรายงาน ที่ถูกต้องมาอีกครั้งหนึ่ง

3.2.4 การบันทึกข้อมูล / แบบรายงานเข้าสู่ระบบคอมพิวเตอร์



รูปที่ 3.7 แผนภาพการไหลเวียนของข้อมูลในส่วนของการบันทึกข้อมูล / แบบรายงานเข้าสู่ระบบ

การบันทึกข้อมูล / แบบรายงานเข้าสู่ระบบคอมพิวเตอร์นั้น จะเป็นขั้นตอนการนำข้อมูล / แบรายงานที่ได้รับที่ผ่านการตรวจสอบความถูกต้องแล้ว โดยข้อมูล / แบบรายงานดังกล่าวที่อยู่ในรูปสื่อที่เป็นเทปแม่เหล็กหรือแผ่นดิสก์นั้น สามารถนำมาบันทึกเข้าสู่ระบบคอมพิวเตอร์ได้ทันที แต่ในส่วนของสื่อที่เป็นเอกสารกระดาษนั้น เจ้าหน้าที่จะทำการป้อน

ข้อมูลให้อยู่ในรูปอิเล็กทรอนิกส์เป็นไฟล์เสียก่อนแล้วจึงทำการบันทึกเข้าสู่ระบบ เพื่อสายฐานข้อมูลจะนำข้อมูลไปใช้งานต่อไป

3.3 ปัญหาที่พบจากการวิเคราะห์ระบบ

จากการวิเคราะห์ระบบการทำงานของ การส่งข้อมูล / แบบรายงานสถานะทางการเงินของสถาบันการเงิน มาที่ศูนย์รับข้อมูลของธนาคารแห่งประเทศไทยนั้น จะพบว่ามีปัญหาเกิดขึ้นดังนี้

1. ลักษณะการนำส่งข้อมูล / แบบรายงานนั้นยังเป็นแบบ Manual กล่าวคือทำการนำส่งด้วยผู้นำส่งเอกสารซึ่งทำให้เกิดความไม่คล่องตัว และอาจเกิดการล่าช้าหรือการสูญหายของข้อมูลในกรณีที่มีอุปสรรคระหว่างการเดินทาง อีกทั้งยังเสี่ยงต่อความปลอดภัยของข้อมูลซึ่งส่วนใหญ่เป็นข้อมูล / แบบรายงานทางการเงินที่มีความสำคัญ และ เป็นความลับ
2. ข้อมูลในระหว่างการนำส่งโดยผู้นำส่งเอกสารนั้นยากต่อการติดตามสถานะ
3. ข้อมูล / แบบรายงานที่นำส่งมีความหลากหลายในรูปของสื่อ เช่น เอกสารกระดาษ เทปแม่เหล็ก และ แผ่นดิสก์ ทั้งนี้ในกรณีของเอกสารกระดาษซึ่งเป็นรูปแบบของสื่อส่วนใหญ่นั้นทางเจ้าหน้าที่จะต้องทำการป้อนข้อมูลให้อยู่ในรูปอิเล็กทรอนิกส์เป็นไฟล์เสียก่อนแล้วจึงทำการบันทึกเข้าสู่ระบบเพื่อนำไปใช้งาน เนื่องจากข้อมูล / แบบรายงานนั้นมีปริมาณจำนวนมากฉะนั้นขั้นตอนการป้อนข้อมูลดังกล่าวจะใช้เวลามากในการเตรียมข้อมูลให้พร้อมสำหรับการใช้งาน และเป็นการสิ้นเปลืองทรัพยากรกระดาษเป็นจำนวนมาก
4. ระบบงานปัจจุบันไม่สามารถรองรับการนำส่งข้อมูล / แบบรายงานจากสถาบันการเงินที่มีสาขาในต่างจังหวัดที่ไกลออกไปได้อย่างสะดวก
5. ในกรณีที่มีความจำเป็นที่จะต้องแก้ไขข้อมูล / แบบรายงาน ที่ได้เคยส่งไปแล้วนั้นจะทำได้ไม่สะดวก เนื่องจากสถาบันการเงินต้องทำการนำส่งข้อมูล / แบบรายงาน ที่แก้ไขมาใหม่ผ่านผู้นำส่งเอกสาร แล้วจึงให้เจ้าหน้าที่ป้อนข้อมูลเข้าสู่ระบบอีกครั้ง

จากปัญหาที่เกิดขึ้น ทำให้ต้องมีการพัฒนาระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัย เพื่อเพิ่มประสิทธิภาพในการทำงานให้มากขึ้น โดยการนำคอมพิวเตอร์เข้ามาช่วยในการส่งข้อมูล / แบบรายงาน เพื่อให้การทำงานมีความคล่องตัว สะดวก รวดเร็ว และ ปลอดภัยขึ้น

บทที่ 4

การออกแบบระบบงาน

การออกแบบระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัยนั้น จะมุ่งเน้นตามความต้องการในด้านความคล่องตัว สะดวก รวดเร็ว และ ปลอดภัยเป็นหลัก โดยเริ่มจากการอธิบายความต้องการและขอบเขตของระบบงานใหม่ คุณสมบัติของระบบงานใหม่ ตลอดจนรายละเอียดของการออกแบบระบบงาน โดยจะแสดงถึงความสัมพันธ์ระหว่างระบบและผู้ที่เกี่ยวข้องกับระบบด้วยแผนภาพการไหลเวียนของข้อมูล (Data Flow Diagram) ตลอดจนการออกแบบฐานข้อมูลเชิงสัมพันธ์โดยใช้แผนภาพความสัมพันธ์ของข้อมูล (Entity Relationship Diagram) เป็นเครื่องมือและการจัดทำพจนานุกรมข้อมูล (Data Dictionary) ของข้อมูลภายในฐานข้อมูลที่พัฒนาขึ้น

4.1 ความต้องการของระบบงานใหม่

ความต้องการของระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัยที่จะทำการพัฒนาขึ้นนั้น มีรายละเอียดดังต่อไปนี้

1. จัดทำระบบรักษาความปลอดภัยข้อมูลที่ส่ง เพื่อยืนยันได้ว่าข้อมูลที่ได้รับนั้นถูกส่งมาจากแหล่งที่ได้รับการรับรองและยังคงความถูกต้องของข้อมูลเดิม
2. จัดทำระบบการควบคุมสิทธิในการส่งและเรียกดูสถานะของข้อมูลของเจ้าหน้าที่ตามระดับของตำแหน่งหน้าที่ที่กำหนดไว้
3. จัดทำระบบส่งข้อมูลที่ส่งได้รวดเร็ว ช่วยลดภาระของเจ้าหน้าที่ในการป้อนข้อมูลเข้าระบบ และ ช่วยลดการสิ้นเปลืองทรัพยากรของสื่อที่ใช้ในการนำส่งข้อมูล
4. จัดทำระบบที่มีลักษณะการทำงานที่สะดวก และง่ายต่อการใช้งาน

4.2 ขอบเขตของระบบงานใหม่

ระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัยที่พัฒนาขึ้นนั้น จะมุ่งเน้นตามความต้องการในด้านความคล่องตัว สะดวก รวดเร็ว และ ปลอดภัยเป็นหลัก ดังนั้นระบบงานใหม่จึงมีขอบเขตของงานดังต่อไปนี้

1. การนำส่งข้อมูล / แบบรายงานจากสถาบันการเงิน โดยจะเป็นการนำส่งในรูปสื่ออิเล็กทรอนิกส์ผ่านการเชื่อมต่อเข้าเครือข่ายโดยตรงมาที่ศูนย์รับข้อมูล
2. การยืนยันและรับรองตัวบุคคล โดยผู้ใช้งานทุกคนในระบบจะต้องผ่านการรับรองตัวบุคคลจากทางธนาคารแห่งประเทศไทยว่าเป็นบุคคลที่สามารถทำการส่งข้อมูล / แบบรายงานของสถาบันการเงินที่สังกัด เพื่อใช้ในการยืนยันบุคคลในขั้นตอนการใช้งานระบบ
3. การกำหนดสิทธิในการใช้งานระบบ โดยจะเป็นการกำหนดสิทธิการทำงานต่างๆในระบบให้กับผู้ใช้งานที่ผ่านการรับรองแล้ว
4. การตรวจสอบสถานะของข้อมูลที่นำส่ง โดยจะเป็นการแสดงสถานะปัจจุบันของข้อมูลที่ส่งผ่านระบบเพื่อติดตามผลการตรวจสอบของข้อมูล / แบบรายงาน ที่ได้ส่งไป
5. การรักษาความปลอดภัยของข้อมูล โดยจะเป็นการลงลายเซ็นอิเล็กทรอนิกส์ และเข้ารหัสข้อมูลระหว่างการนำส่งเพื่อรักษาความลับ และ ความถูกต้องของข้อมูล
6. การเข้าใช้ระบบ โดยจะเป็นลักษณะของการใช้งานผ่านเว็บ (Web Application) เพื่อความสะดวก และ ง่ายต่อการใช้งาน

4.3 คุณสมบัติของระบบงานใหม่

ระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัยที่พัฒนาขึ้น จะมีคุณสมบัติดังต่อไปนี้

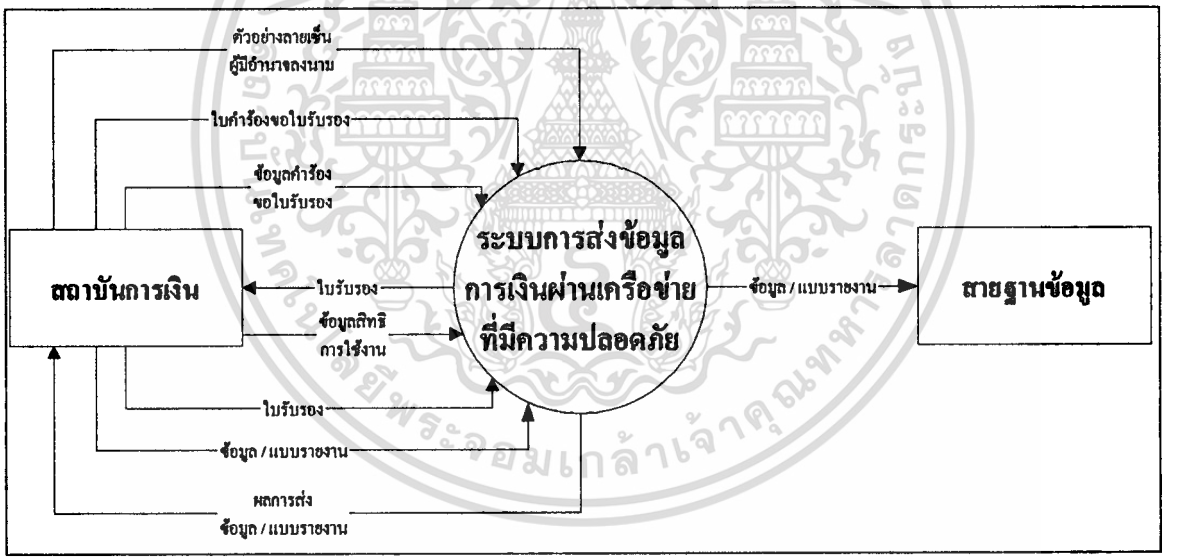
1. มีการรักษาความปลอดภัยและความถูกต้องของข้อมูลดั้งเดิมที่ส่งมาจากแหล่งต้นทาง โดยมีการตรวจสอบว่าข้อมูลไม่ได้ถูกเปลี่ยนแปลงระหว่างการส่ง และยืนยันได้ว่าข้อมูลนั้นถูกส่งมาจากแหล่งที่ได้รับการรับรอง
2. มีการควบคุมการเข้าถึงตัวข้อมูล โดยจำกัดสิทธิในการส่งและเรียกดูสถานะของข้อมูลของเจ้าหน้าที่ตามระดับของตำแหน่งหน้าที่ที่กำหนดไว้
3. สามารถรองรับการเข้าถึงระบบจากผู้ใช้ในสถาบันการเงินที่อยู่ไกลออกไปในต่างจังหวัด เพื่อความคล่องตัวในการส่งข้อมูล
4. สามารถติดตามและแสดงสถานะของข้อมูลที่ถูกส่งออกไปได้
5. สามารถช่วยลดระยะเวลาในการนำส่งข้อมูลจากต้นทางมายังปลายทางที่ต้องการได้
6. สามารถช่วยลดภาระของเจ้าหน้าที่ศูนย์รับข้อมูลในการป้อนข้อมูลจากสื่อกระดาษ โดยนำส่งข้อมูลให้อยู่ในรูปแบบเดียวกันคือ ไฟล์อิเล็กทรอนิกส์ เพื่อลดการสิ้นเปลืองทรัพยากรของสื่อที่ใช้ในการนำส่งข้อมูล
7. มีลักษณะการทำงานที่สะดวก และง่ายต่อการใช้งาน

4.4 การออกแบบระบบงาน

การออกแบบระบบงานของระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัย นั้น จะพิจารณาจากความต้องการและขอบเขตของระบบงานมาสรุปเป็นแผนภาพรวมของระบบ (Context Diagram) แผนภาพการไหลเวียนของข้อมูล (Data Flow Diagram) แผนภาพความสัมพันธ์ของข้อมูล (Entity Relationship Diagram) และ พจนานุกรมข้อมูล (Data Dictionary) ได้ดังต่อไปนี้

4.4.1 แผนภาพรวมของระบบ (Context Diagram)

แผนภาพรวมของระบบ (Context Diagram) ของระบบงานใหม่นั้น จะแสดงให้เห็นถึงความสัมพันธ์ระหว่างระบบกับผู้ที่เกี่ยวข้องกับระบบ และเนื่องจากรูปแบบการทำงานของระบบส่วนใหญ่ยังคงเป็นเช่นเดิม ดังนั้น แผนภาพรวมของระบบของระบบงานใหม่จึงมีลักษณะคล้ายคลึงกันกับ แผนภาพรวมของระบบของระบบงานปัจจุบัน



รูปที่ 4.1 แผนภาพรวมของระบบใหม่

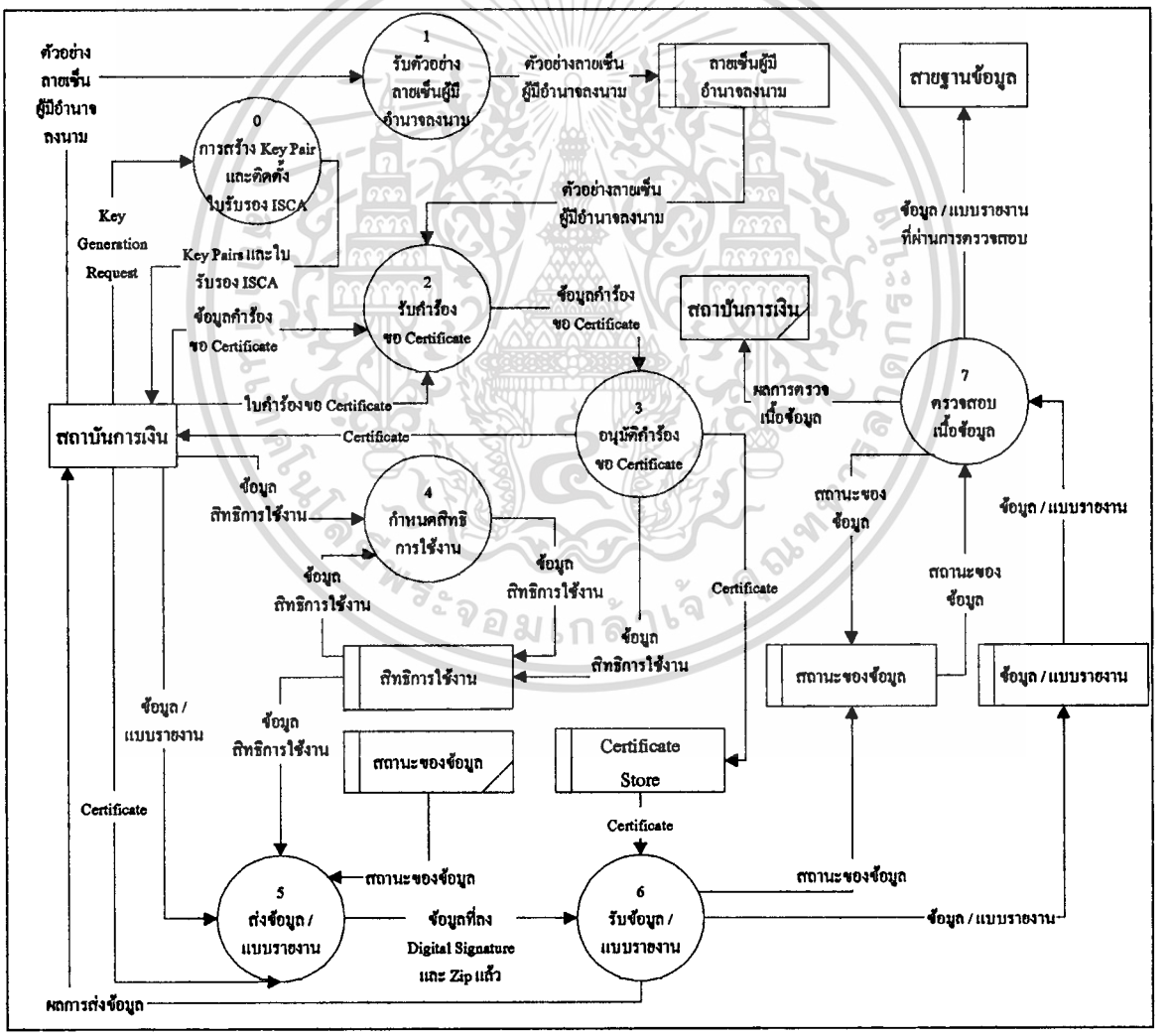
จากแผนภาพรวมของระบบดังแสดงในรูปที่ 4.1 จะประกอบไปด้วย Entity หลักคือ ผู้ใช้งานจาก สถาบันการเงิน และ สายฐานข้อมูล ซึ่งทำการแลกเปลี่ยนข้อมูลกับระบบ โดยสถาบันการเงินจะทำการส่งเอกสารต่างๆที่จำเป็นต่อการขอใบรับรอง ทั้งในรูปเอกสารกระดาษ และ ฟอร์มอิเล็กทรอนิกส์เพื่อรับใบรับรองไปติดตั้งและเข้าใช้งานในระบบต่อไป

ทั้งนี้บทบาทของผู้ใช้งานของสถาบันการเงินจะแบ่งออกเป็น 2 บทบาทดังนี้

- Certifier – ทำหน้าที่ควบคุมสิทธิของ Officer ที่อยู่ภายใต้การดูแล
- Officer – ทำหน้าที่ส่งข้อมูลในส่วนที่ถูกกำหนดให้มีสิทธิส่งโดย Certifier

4.4.2 แผนภาพการไหลเวียนของข้อมูล (Data Flow Diagram)

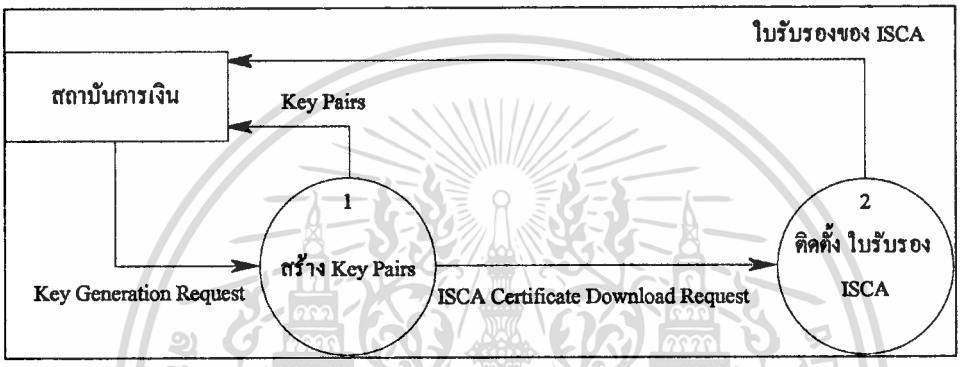
แผนภาพการไหลเวียนของข้อมูล (Data Flow Diagram) ของระบบงานใหม่นั้น จะแสดงให้เห็นถึงทิศทางการส่งผ่านและไหลเวียนของข้อมูลจากการทำงานต่างๆ ที่มีอยู่ในระบบ ซึ่งสามารถแบ่งการทำงานของระบบออกเป็นงานย่อยๆ ได้ดังรูปที่ 4.2



รูปที่ 4.2 แผนภาพรวมของการไหลเวียนของข้อมูลในระบบงานใหม่

4.4.2.1 การสร้าง Key Pair และติดตั้งใบรับรองของ ISCA

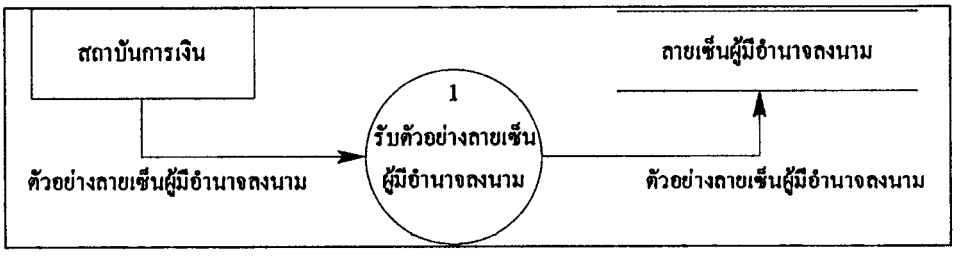
ขั้นตอนการสร้าง Key Pair และติดตั้งใบรับรองของ ISCA เป็นขั้นตอนที่ทางผู้ใช้งานของสถาบันการเงินใช้บริการการสร้าง Key Pair ของระบบเพื่อติดตั้ง Signature Key Pair ที่ใช้ในการลงลายเซ็นอิเล็กทรอนิกส์ และ Exchange Key Pair ที่ใช้ในการเข้ารหัส SSL Session โดย Key Pair ทั้งสองชนิดจะประกอบไปด้วย Public และ Private Key จากนั้นจึงทำการติดตั้งใบรับรองของ ISCA ซึ่งเป็น Trusted Root Certification Authority ของระบบ ดังแสดงการทำงานในรูปที่ 4.3



รูปที่ 4.3 แผนภาพการไหลเวียนข้อมูลในส่วนของการสร้าง Key Pair และติดตั้งใบรับรอง ISCA

4.4.2.2 การรับตัวอย่างลายเซ็นของผู้มีอำนาจลงนาม

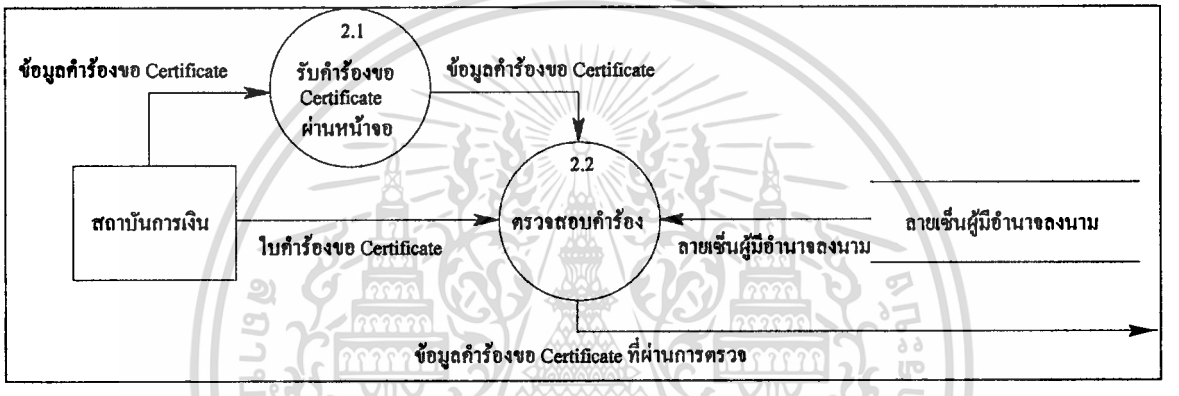
ขั้นตอนการรับตัวอย่างลายเซ็นของผู้มีอำนาจลงนาม เป็นขั้นตอนที่ทางศูนย์ข้อมูลทำการรับเอกสารตัวอย่างลายเซ็นผู้มีอำนาจลงนามที่ส่งมาจากสถาบันการเงินเก็บไว้เพื่อใช้เป็นหลักฐานในการตรวจสอบเอกสารที่ทางสถาบันการจะส่งมาในขั้นตอนการขอใบรับรองดังรูปที่ 4.4 โดยขั้นตอนนี้จะเป็นขั้นตอนที่ทำโดยบุคคล (Manual)



รูปที่ 4.4 แผนภาพการไหลเวียนข้อมูลในส่วนของการรับตัวอย่างลายเซ็นของผู้มีอำนาจลงนาม

4.4.2.3 การรับคำร้องขอ Certificate

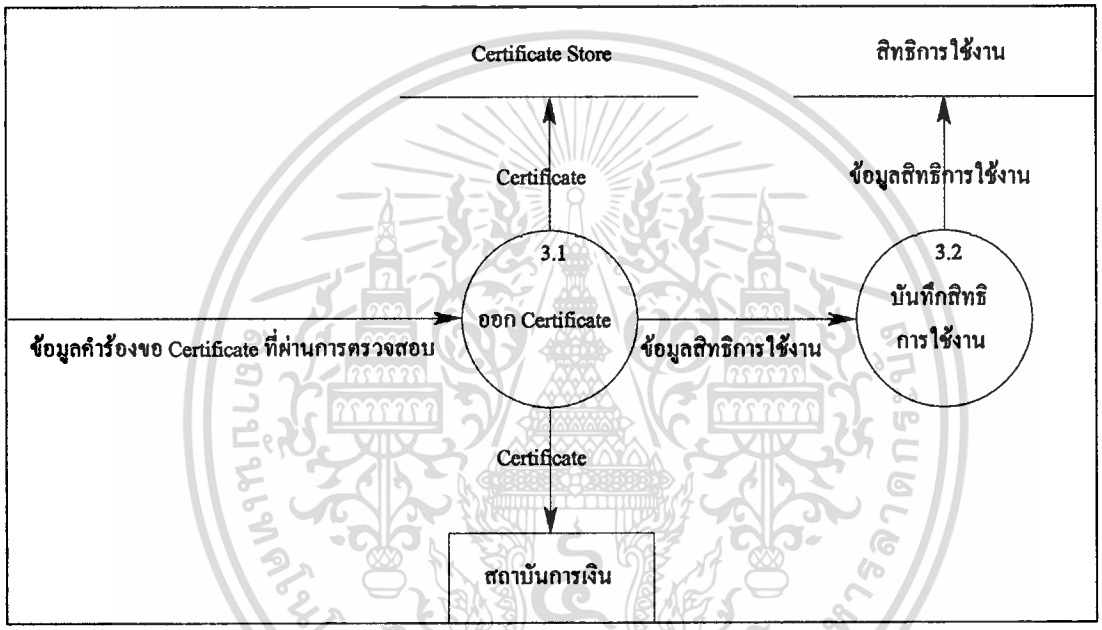
ขั้นตอนการรับคำร้องขอ Certificate เป็นขั้นตอนที่ทางศูนย์ข้อมูลทำการรับคำร้องขอใบรับรองที่อยู่ในรูปสื่อกระดาษ และรับข้อมูลคำร้องขอใบรับรองในรูปสื่ออิเล็กทรอนิกส์ จากสถาบันการเงิน และนำเอกสารทั้งสองมาตรวจสอบกับตัวอย่างลายเซ็นผู้มีอำนาจลงนามที่เก็บไว้ ดังแสดงการทำงานในรูปที่ 4.5 โดยถ้าข้อมูลในกระดาษและอิเล็กทรอนิกส์ตรงกัน และมีลายเซ็นของผู้มีอำนาจลงนามกำกับมาอย่างถูกต้อง ข้อมูลคำร้องนั้นจะถูกส่งต่อไปยังขั้นตอนการอนุมัติคำร้องขอใบรับรอง



รูปที่ 4.5 แผนภาพการไหลเวียนของข้อมูลในส่วนของการรับคำร้องขอ Certificate

4.4.2.4 การอนุมัติคำร้องขอ Certificate

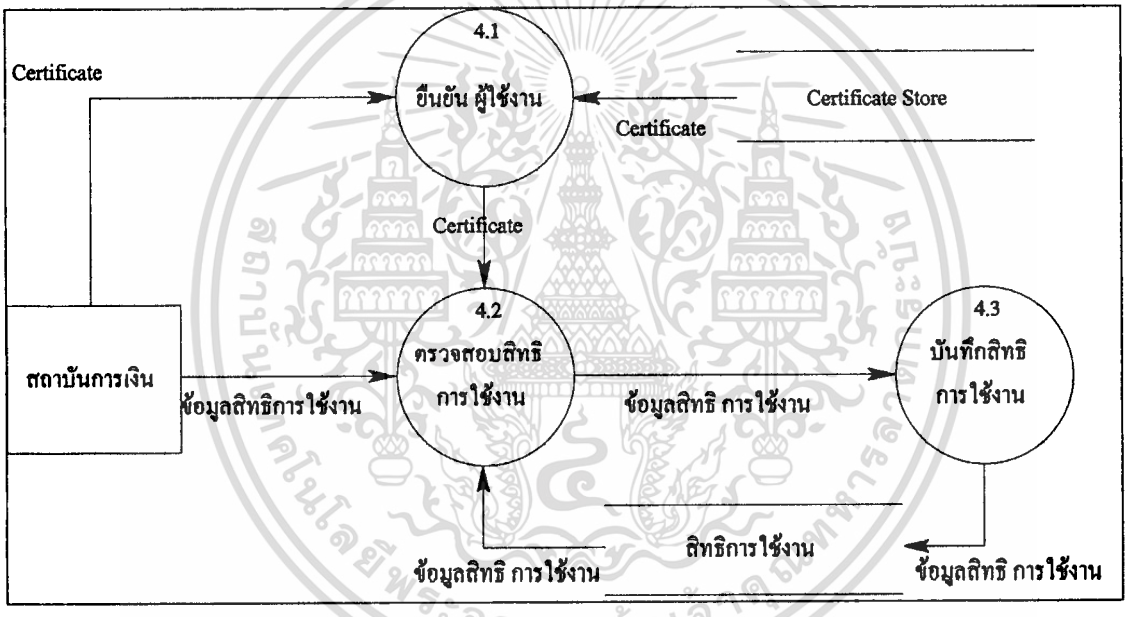
ขั้นตอนการอนุมัติคำร้องขอ Certificate จะมีขั้นตอนการทำงานดังรูปที่ 4.6 โดยในขั้นแรกจะนำเอาข้อมูลคำร้องขอใบรับรองที่ผ่านการตรวจสอบแล้วมาทำการออกใบรับรองให้แก่ผู้ใช้งานของสถาบันการเงินที่ยื่นคำขอมาเพื่อนำไปติดตั้งและใช้งานต่อไป ส่วนทางระบบจะเก็บใบรับรองนั้นใน Certificate Store เพื่อใช้อ้างอิงต่อไป จากนั้นถ้าผู้ใช้งานดังกล่าวเป็น Certifier บุคคลนั้นจะได้รับการกำหนดสิทธิในการให้สิทธิ กับผู้ใช้งานอื่นที่อยู่ในความดูแล (บทบาท Officer)



รูปที่ 4.6 แผนภาพการไหลเวียนของข้อมูลในส่วนของการอนุมัติคำร้องขอ Certificate

4.4.2.5 การกำหนดสิทธิการใช้งาน

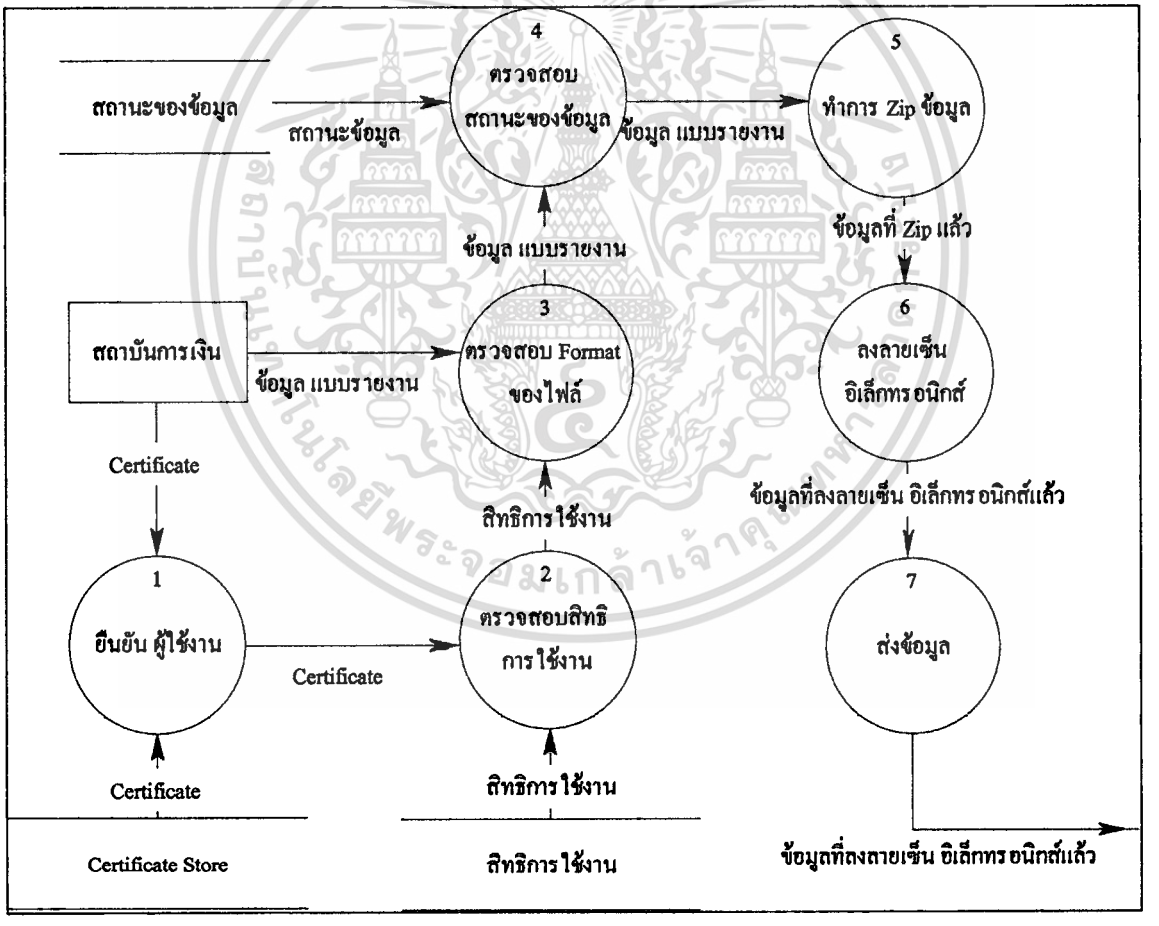
ขั้นตอนการกำหนดสิทธิการใช้งาน จะมีขั้นตอนการทำงานดังรูปที่ 4.7 โดยเมื่อผู้ใช้งานในระบบได้ทำการติดตั้งใบรับรองที่ได้รับการอนุมัติแล้ว ถ้าบุคคลนั้นมีบทบาทเป็น Certifier จะสามารถเข้ามาในขั้นตอนการกำหนดสิทธิให้กับตัวเอง และ Officer ผู้ที่อยู่ใต้การควบคุม โดยเมื่อเริ่มเข้าใช้งาน Certifier จะต้องแสดงใบรับรองของตน ซึ่งทางระบบจะตรวจสอบใบรับรอง และตรวจสอบสิทธิในการใช้งานในระบบของ Certifier ว่ามีสิทธิในการควบคุมดูแล Officer บุคคลใด และแบบรายงานประเภทใด จากนั้นถ้า Certifier มีการเปลี่ยนแปลงข้อมูลสิทธิในการใช้งาน ข้อมูลดังกล่าวจะถูกบันทึกในที่เก็บข้อมูลสิทธิการใช้งาน



รูปที่ 4.7 แผนภาพการไหลเวียนของข้อมูลในส่วนของการกำหนดสิทธิการใช้งาน

4.4.2.6 การส่งข้อมูล / แบบรายงาน

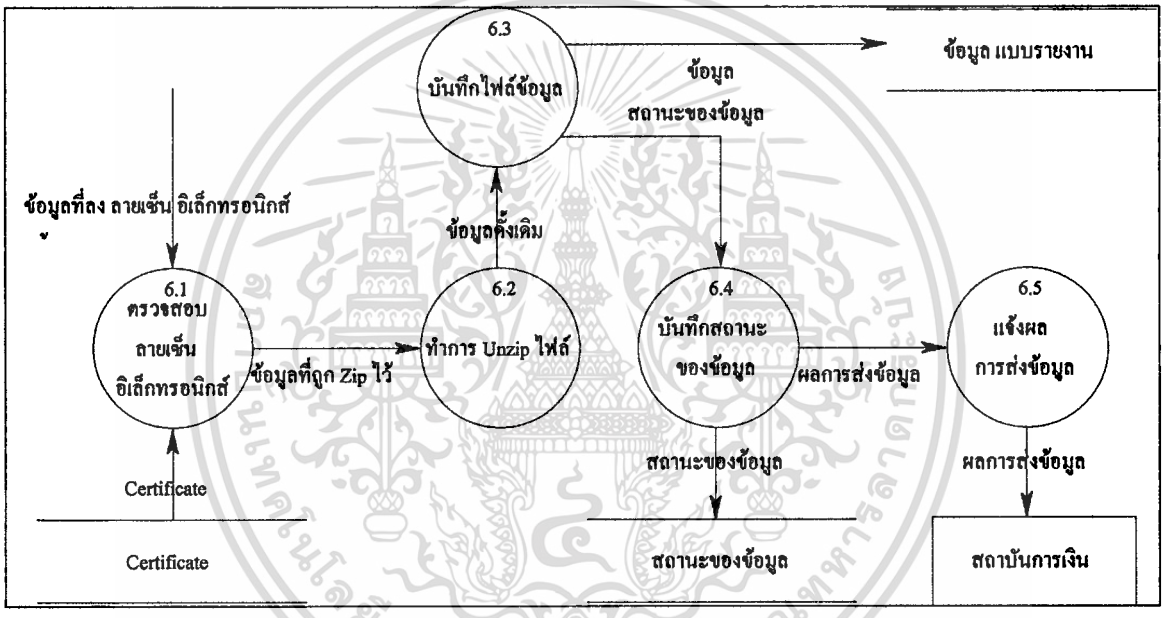
ขั้นตอนการส่งข้อมูล / แบบรายงาน จะมีขั้นตอนการทำงานดังรูปที่ 4.8 โดยเมื่อเริ่มเข้าใช้งาน ผู้ใช้งานจะต้องแสดงใบรับรองของตน ซึ่งทางระบบจะตรวจสอบใบรับรอง และตรวจสอบสิทธิในการใช้งานในระบบมีสิทธิในการส่งแบบรายงาน / ข้อมูล ประเภทใดบ้าง จากนั้นเมื่อผู้ใช้งานทำการเลือกไฟล์ที่ต้องการส่ง ระบบจะทำการตรวจสอบ Format ของชื่อไฟล์ว่าเป็นไปตาม Format หรือไม่ (ในบทที่ 5 จะกล่าวถึงรายละเอียดของ Format ชื่อไฟล์) ถ้า Format ถูกต้อง ระบบจะตรวจสอบฐานข้อมูลว่าไฟล์ข้อมูลที่เลือกนั้นเคยถูกส่งมาแล้วหรือไม่ (ถ้าเคยส่งแล้วจะต้องระบุว่าเป็นการส่งซ้ำเพื่อ Update) จากนั้นจะทำการบีบอัดข้อมูลให้มีขนาดเล็กลงก่อนที่จะทำการลงลายเซ็นอิเล็กทรอนิกส์กับข้อมูล แล้วจึงส่งข้อมูลไปยังขั้นตอนการรับข้อมูล



รูปที่ 4.8 แผนภาพการไหลเวียนของข้อมูลในส่วนของการส่งข้อมูล / แบบรายงาน

4.4.2.7 การรับข้อมูล / แบบรายงาน

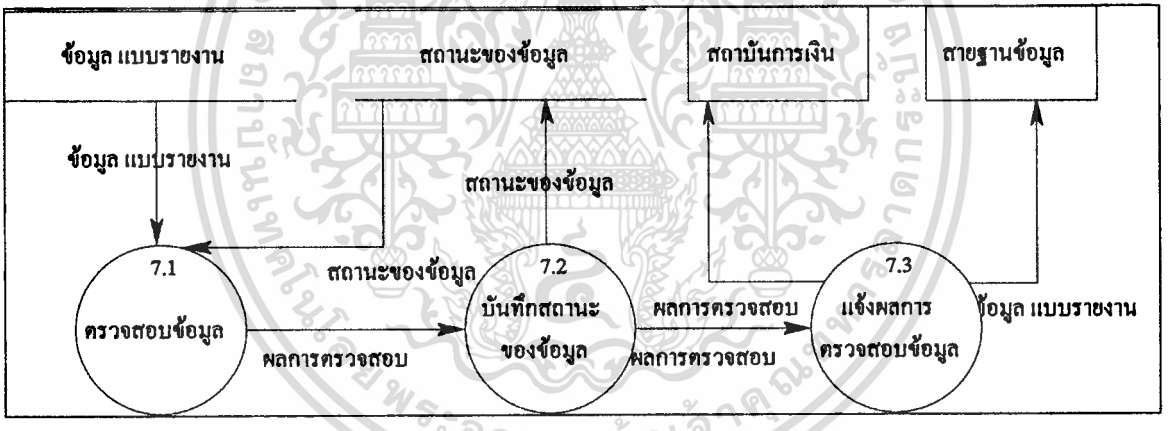
ขั้นตอนการรับข้อมูล / แบบรายงาน จะมีขั้นตอนการทำงานดังรูปที่ 4.9 เมื่อข้อมูลถูกส่งมาจากขั้นตอนการส่ง ข้อมูล / แบบรายงาน ข้อมูลจะถูกนำมาตรวจสอบลายเซ็นอิเล็กทรอนิกส์ เพื่อยืนยันว่าไม่ได้ถูกเปลี่ยนแปลงกลางทางและถูกส่งมาจากผู้ใช้งานที่มีใบรับรองที่ถูกต้อง จากนั้นจึงทำการ ขยายข้อมูลที่ถูกบีบอัดไว้ (Unzip) ให้กลับมาอยู่สภาพเดิม บันทึกไฟล์เก็บไว้ใน Storage และบันทึกสถานะของข้อมูลว่าได้เดินทางมาถึงปลายทางแล้ว โดยมีการแจ้งผลดังกล่าวให้ทางผู้ใช้งานทราบเพื่อติดตามสถานะของข้อมูล



รูปที่ 4.9 แผนภาพการไหลเวียนของข้อมูลในส่วนของการรับข้อมูล / แบบรายงาน

4.4.2.8 การตรวจสอบเนื้อข้อมูล

ขั้นตอนการตรวจสอบเนื้อข้อมูล จะมีขั้นตอนการทำงานดังรูปที่ 4.10 โดยจะมีการนำข้อมูลที่ได้รับมาจากสถาบันการเงิน มาตรวจสอบถึงเนื้อข้อมูลว่ามีความถูกต้องหรือไม่ โดยจะทำการ Update ผลการตรวจสอบในฐานข้อมูลสถานะของข้อมูล โดยทางสถาบันการเงินจะได้รับแจ้งผลการตรวจสอบ ซึ่งถ้าข้อมูลที่ส่งมานั้นผ่านการตรวจสอบ ทางสายฐานข้อมูลจะนำข้อมูลดังกล่าวไปใช้งานต่อไป (ทั้งนี้ในส่วนขั้นตอนการตรวจสอบเนื้อข้อมูลนั้นอยู่นอกเหนือขอบเขตในการพัฒนาโครงการจึงทำการออกแบบมาเพื่อให้เกิดความสมบูรณ์ของภาพรวมของระบบ แต่มิได้นำไปพัฒนาในขั้นต่อๆไป)

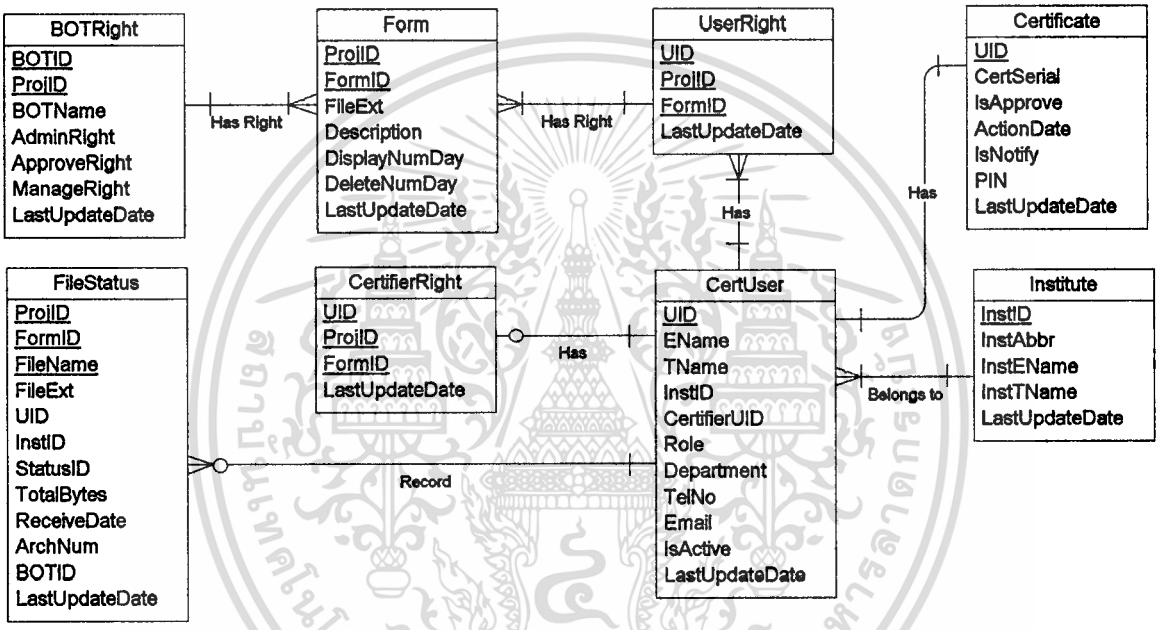


รูปที่ 4.10 แผนภาพการไหลเวียนของข้อมูลในส่วนของการตรวจสอบเนื้อข้อมูล

4.4.3 แผนภาพความสัมพันธ์ของข้อมูล (Entity Relationship Diagram)

แผนภาพความสัมพันธ์ของข้อมูล (Entity Relationship Diagram) ของระบบงานใหม่นั้น จะแสดงให้เห็นถึงความสัมพันธ์ของข้อมูลต่างๆที่มีอยู่ในระบบ ดังแสดงเป็น Fully Attributed Data Model โดยมีรายละเอียดดังต่อไปนี้

4.4.3.1 Fully Attributed Data Model



รูปที่ 4.11 Fully Attributed Data Model ของระบบ

4.4.4 พจนานุกรมข้อมูล (Data Dictionary)

พจนานุกรมข้อมูล (Data Dictionary) เป็นการแสดงรายละเอียดของข้อมูลในตาราง (Table) ต่างๆที่อยู่ในฐานข้อมูล ซึ่งจะแสดงถึงชื่อฟิลด์ คำอธิบาย ประเภทของข้อมูล และ หมายเหตุ โดยมีรายละเอียดดังนี้

4.4.4.1 ตาราง BOTRight

ใช้เก็บสิทธิของเจ้าหน้าที่ผู้ควบคุมระบบ โดยระบุถึงความสามารถในการเข้าจัดการระบบ

ชื่อฟิลด์	คำอธิบาย	ประเภท	ขนาด	หมายเหตุ
BOTID	รหัสพนักงานธปท.	Text	8	Key
ProjID	รหัสฟอร์มโปรเจค	Text	20	Key
BOTName	ชื่อ นามสกุล	Text	10	
AdminRight	สิทธิการเป็น Admin	Text	1	
ApproveRight	สิทธิการอนุมัติใบรับรอง	Text	1	
ManageRight	สิทธิการจัดการสิทธิ	Text	1	
LastUpdateDate	วันเวลาปรับปรุงล่าสุด	Date	8	

ตารางที่ 4.1 แสดงรายละเอียดของตาราง BOTRight

4.4.4.2 ตาราง Certificate

ใช้เก็บรายละเอียดของผลการพิจารณาคำขอใบรับรองและสถานะการแจ้งผลการพิจารณา

ชื่อฟิลด์	คำอธิบาย	ประเภท	ขนาด	หมายเหตุ
UID	รหัสผู้ใช้งาน	Text	20	Key
CertSerial	รหัส Serial ของ Certificate	Text	20	
IsApprove	ผลการพิจารณาคำขอใบรับรอง	Text	1	
ActionDate	วันที่พิจารณาคำขอใบรับรอง	Date	8	
IsNotify	สถานะการแจ้งผลการพิจารณา	Text	1	
PIN	รหัส PIN สำหรับติดตั้ง Certificate	Text	32	
LastUpdateDate	วันเวลาปรับปรุงล่าสุด	Date	8	

ตารางที่ 4.2 แสดงรายละเอียดของตาราง Certificate

4.4.4.3 ตาราง CertUser

ใช้เก็บรายละเอียดของผู้ใช้งานในระบบ และบทบาทในการใช้งาน

ชื่อฟิลด์	คำอธิบาย	ประเภท	ขนาด	หมายเหตุ
UID	รหัสผู้ใช้งาน	Text	20	Key
EName	ชื่อ นามสกุล (อังกฤษ)	Text	75	
TName	ชื่อ นามสกุล (ไทย)	Text	75	
InstID	รหัสสถาบัน	Text	3	
CertifierUID	รหัสผู้รับรอง	Text	20	
Role	บทบาทการใช้งาน	Text	1	
Department	หน่วยงาน	Text	30	
TelNo	เบอร์โทรศัพท์	Text	30	
Email	อีเมล	Text	30	
IsActive	สถานะปัจจุบัน	Text	1	
LastUpdateDate	วันเวลาปรับปรุงล่าสุด	Date	8	

ตารางที่ 4.3 แสดงรายละเอียดของตาราง CertUser

4.4.4.4 ตาราง FileStatus

ใช้เก็บรายละเอียดของการส่งข้อมูลและสถานะของข้อมูลที่เข้าสู่ระบบแล้ว

ชื่อฟิลด์	คำอธิบาย	ประเภท	ขนาด	หมายเหตุ
ProjID	รหัสฟอร์มโปรเจค	Text	20	Key
FormID	รหัสแบบฟอร์ม	Text	20	Key
FileName	ชื่อไฟล์ที่ส่ง	Text	8	Key
FileExt	ชื่อ Extension ของไฟล์	Text	3	
UID	รหัสผู้ใช้งาน	Text	20	
InstID	รหัสสถาบันการเงิน	Text	3	
StatusID	สถานะของไฟล์ที่ส่ง	Text	1	
TotalBytes	ขนาดของไฟล์	Integer	4	

ReceiveDate	วันเวลาที่ไฟล์มาถึง	Date	8	
ArchNum	เลขที่ของไฟล์	Integer	4	
BOTID	รหัสพนักงานธปท.	Text	8	
LastUpdateDate	วันเวลาปรับปรุงล่าสุด	Date	8	

ตารางที่ 4.4 แสดงรายละเอียดของตาราง FileStatus

4.4.4.5 ตาราง Form

ใช้เก็บรายละเอียดของแบบฟอร์มประเภทต่างๆที่มีอยู่ในระบบ

ชื่อฟิลด์	คำอธิบาย	ประเภท	ขนาด	หมายเหตุ
ProjID	รหัสฟอร์มโปรเจค	Text	20	Key
FormID	รหัสแบบฟอร์ม	Text	20	Key
FileExt	ชื่อ ไฟล์ Extension	Text	1	
Description	คำอธิบายของแบบรายงาน	Text	1	
DisplayNumDay	จำนวนวันที่แสดงผลบนหน้าจอ	Integer	4	
DeleteNumDay	จำนวนวันที่เก็บข้อมูลก่อนลบ	Integer	4	
LastUpdateDate	วันเวลาปรับปรุงล่าสุด	Date	8	

ตารางที่ 4.5 แสดงรายละเอียดของตาราง Form

4.4.4.6 ตาราง Institute

ใช้เก็บรายละเอียดของสถาบันการเงินต่างๆ

ชื่อฟิลด์	คำอธิบาย	ประเภท	ขนาด	หมายเหตุ
InstID	รหัสสถาบันการเงิน	Text	3	Key
InstAbbr	รหัสอักษรย่อ	Text	12	
InstEName	ชื่อสถาบันการเงิน (อังกฤษ)	Text	80	
InstTName	ชื่อสถาบันการเงิน (ไทย)	Text	80	
LastUpdateDate	วันเวลาปรับปรุงล่าสุด	Date	8	

ตารางที่ 4.6 แสดงรายละเอียดของตาราง Institute

4.4.4.7 ตาราง UserRight

ใช้เก็บรายละเอียดสิทธิของผู้ใช้งานแต่ละรายว่าสามารถส่งข้อมูลแบบใดได้บ้าง

ชื่อฟิลด์	คำอธิบาย	ประเภท	ขนาด	หมายเหตุ
UID	รหัสผู้ใช้งาน	Text	20	Key
ProjID	รหัสฟอร์มโปรเจค	Text	20	Key
FormID	รหัสแบบฟอร์ม	Text	20	Key
LastUpdateDate	วันเวลาปรับปรุงล่าสุด	Date	8	

ตารางที่ 4.7 แสดงรายละเอียดของตาราง UserRight

4.4.4.8 ตาราง CertifierRight

ใช้เก็บรายละเอียดสิทธิของ Certifier ในการควบคุมสิทธิของ Officer

ชื่อฟิลด์	คำอธิบาย	ประเภท	ขนาด	หมายเหตุ
UID	รหัสผู้ใช้งาน (Certifier)	Text	20	Key
ProjID	รหัสฟอร์มโปรเจค	Text	20	Key
FormID	รหัสแบบฟอร์ม	Text	20	Key
LastUpdateDate	วันเวลาปรับปรุงล่าสุด	Date	8	

ตารางที่ 4.8 แสดงรายละเอียดของตาราง CertifierRight

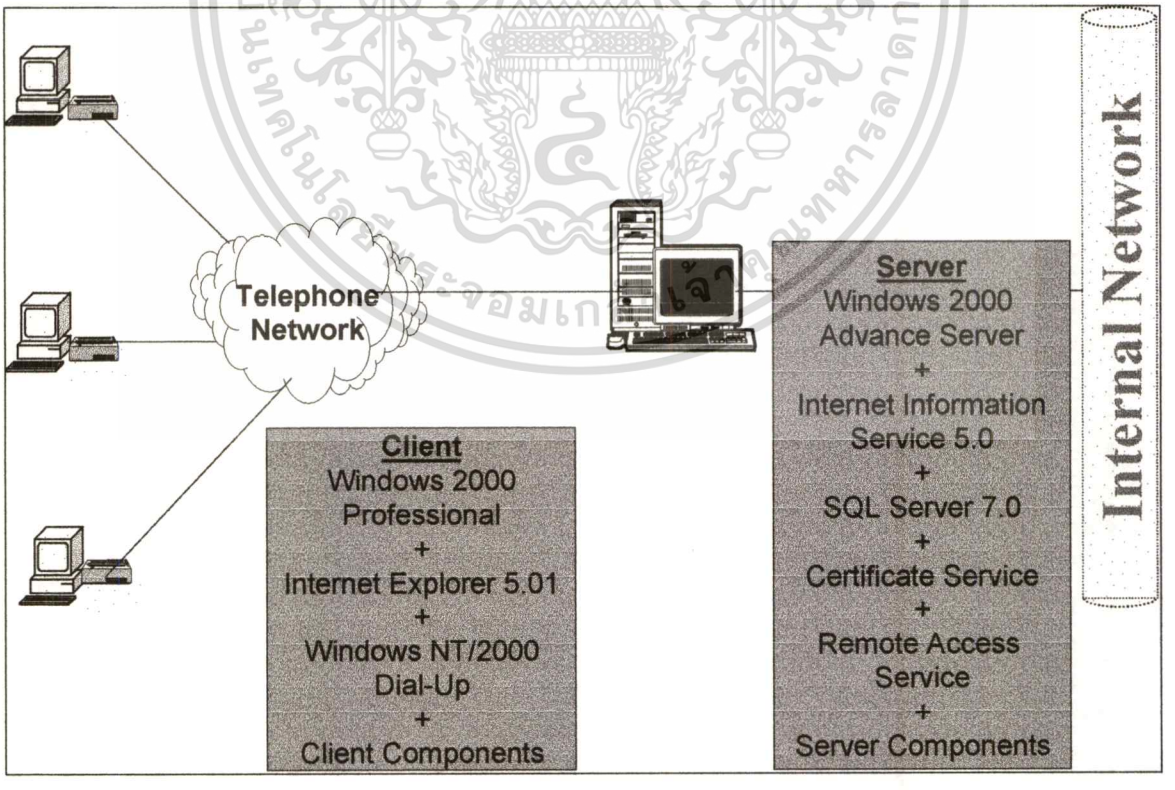
บทที่ 5

การดำเนินการพัฒนาระบบ

จากขั้นตอนการออกแบบระบบงานที่ได้รายละเอียดถึงการทำงานและการไหลเวียนของข้อมูลภายในระบบ รวมถึงโครงสร้างของฐานข้อมูลที่ใช้ จึงนำรายละเอียดเหล่านี้มาพัฒนาให้เป็นระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัย โดยจะเริ่มต้นจากองค์ประกอบของระบบที่พัฒนาขึ้น ส่วนการพัฒนาส่วนประกอบซอฟต์แวร์ และ ส่วนการพัฒนาระบบงานรวมตามลำดับ

5.1 องค์ประกอบของระบบที่พัฒนา

ระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัยที่พัฒนาขึ้นนั้น ประกอบไปด้วยส่วนต่างๆ ดังแสดงในรูปที่ 5.1



รูปที่ 5.1 แสดงองค์ประกอบของระบบที่พัฒนาขึ้น

5.1.1 เครื่องคอมพิวเตอร์ Server

เครื่องคอมพิวเตอร์ Server เป็นระบบปฏิบัติการ Windows 2000 Advance Server โดยมีส่วนประกอบต่างๆ ดังต่อไปนี้

- **Internet Information Service 5.0** ทำหน้าที่เป็น Web Server ซึ่งเป็นส่วนที่ให้บริการในการทำงานของ Web Application ในระบบ ซึ่งจะใช้ Visual Interdev 6.0 ในการพัฒนา Application ดังกล่าว
- **Certificate Service** ทำหน้าที่เป็น Certificate Authority (CA) ของระบบ ซึ่งเป็นส่วนที่ให้บริการในการทำงานของ Certificate Authority และทำการจัดการ Certificate ของผู้ใช้งานในระบบ
- **Remote Access Service** ทำหน้าที่เป็น Remote Access Server ซึ่งเป็นส่วนที่ให้บริการในการเชื่อมต่อ (Dial Up) ผู้ใช้งานเข้ากับทาง Server
- **SQL Server 7.0 Enterprise Edition** ทำหน้าที่เป็น Database Server ซึ่งเป็นส่วนที่ทำการจัดการฐานข้อมูล โดยระบบฐานข้อมูลที่ใช้เป็นแบบ RDBMS (Relational Database Management System) ซึ่งใช้เก็บฐานข้อมูล ของผู้ใช้งาน ระดับสิทธิการใช้งาน สถานะของข้อมูล และ ประวัติของการส่งข้อมูลต่างๆ
- **Server Component** เป็น Module ที่พัฒนาขึ้นมาเพื่อทำให้ Server สามารถทำการตรวจสอบ Digital Signature กับข้อมูลที่ส่ง และ Unzip ข้อมูลที่ส่งมา

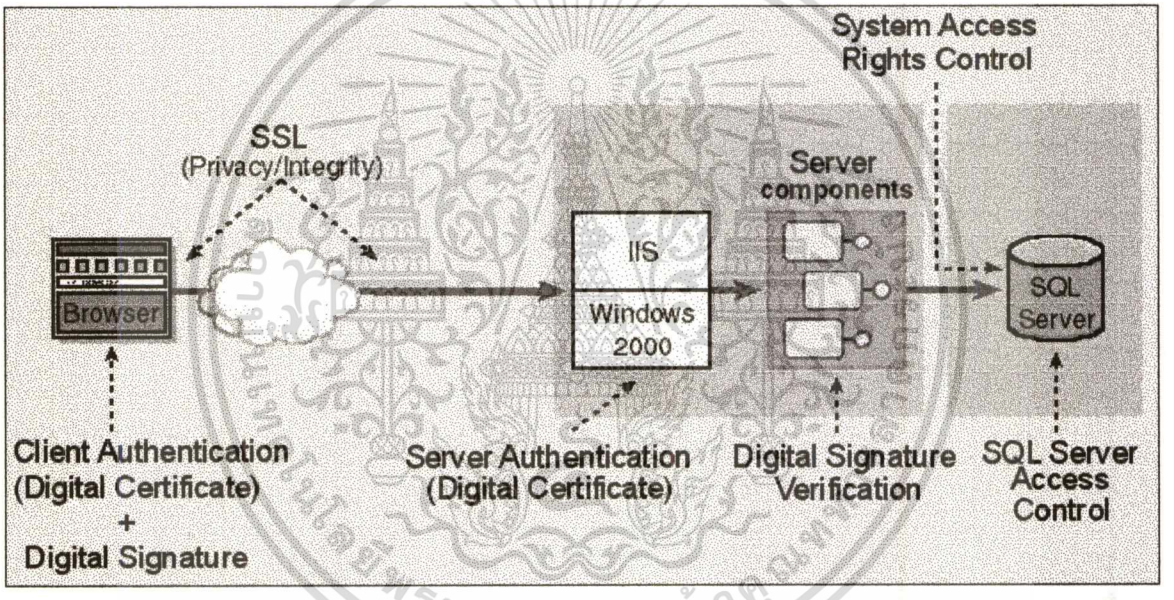
5.1.2 เครื่องคอมพิวเตอร์ Client

เครื่องคอมพิวเตอร์ Client เป็นระบบปฏิบัติการ Windows 2000 Professional โดยมีส่วนประกอบต่างๆ ดังต่อไปนี้

- **Internet Explorer 5.01 SP1** เป็นโปรแกรม Web Browser ซึ่งใช้เรียก Web Application โดย Internet Explorer 5.01 SP1 นั้นมีความสามารถทำ SSL ได้ที่ระดับ 128-bit
- **Windows NT/2000 Dial – Up** เป็นโปรแกรมสำหรับทำการเชื่อมต่อ (Dial-Up) มาที่ Server เพื่อเรียกใช้ระบบงาน
- **Client Component** เป็น Module ที่พัฒนาขึ้นมาเพื่อทำให้ Client สามารถทำการส่งข้อมูล เลือกไฟล์ที่ต้องการ และ ทำการลง Digital Signature กับข้อมูลที่ส่งได้ เป็นต้น

5.1.3 องค์ประกอบความปลอดภัยของระบบ

ระบบที่พัฒนาขึ้นนั้นจะประกอบไปด้วยองค์ประกอบทางด้านความปลอดภัยดังรูปที่ 5.2 โดยทางด้านผู้ใช้งานจะมีการทำ Client Authentication ด้วยการใช้ Digital Certificate และทำการลงลายเซ็นอิเล็กทรอนิกส์กับข้อมูลที่นำส่ง ซึ่งทำการเชื่อมต่อด้วยโปรโตคอล SSL เพื่อเป็นการเข้ารหัสข้อมูล ในส่วนของทางเซิร์ฟเวอร์นั้นจะมีการทำ Server Authentication ด้วย Digital Certificate เช่นกันและมีการใช้ Server Component เพื่อตรวจสอบ Digital Signature ที่ส่งมากับข้อมูลทั้งนี้ SQL Server จะเก็บสิทธิการใช้งานของผู้ใช้งานและมีการควบคุมสิทธิการใช้งานของ SQL Server เองด้วย เช่นการเรียกใช้ฐานข้อมูลจาก Web Application เป็นต้น



รูปที่ 5.2 แสดงองค์ประกอบความปลอดภัยของระบบที่พัฒนาขึ้น

5.2 การพัฒนาส่วนประกอบซอฟต์แวร์

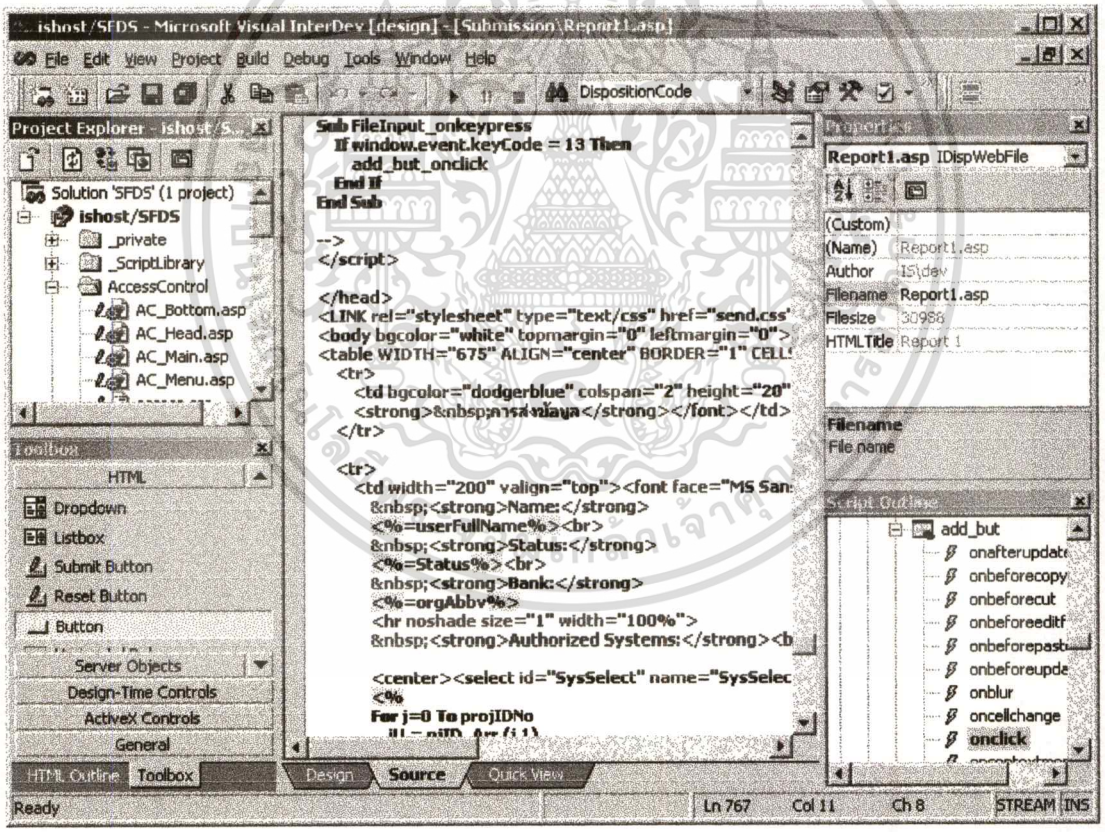
ส่วนประกอบซอฟต์แวร์ (Software components) ที่ใช้ในระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัย มีรายละเอียดในการพัฒนาดังต่อไปนี้

5.2.1 เครื่องมือที่ใช้ในการพัฒนา

เครื่องมือที่ใช้ในการพัฒนาระบบมีดังนี้

- **Microsoft Visual Interdev 6.0**

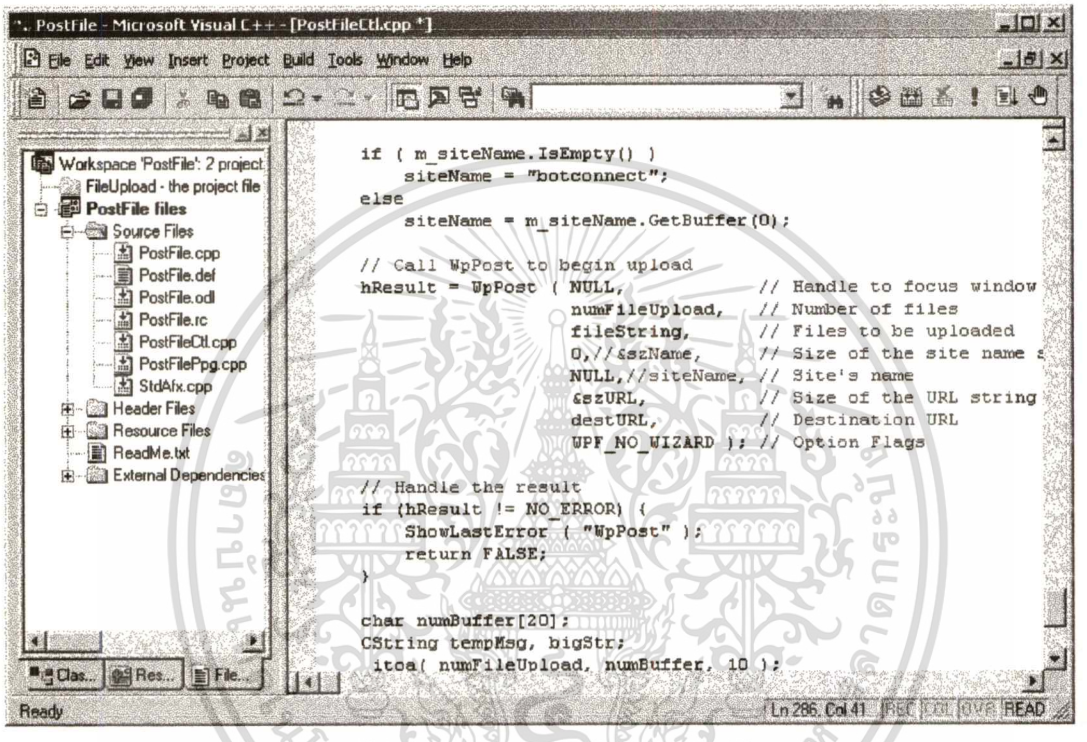
  เครื่องมือ Microsoft Visual Interdev 6.0 นั้นเป็นเครื่องมือที่ใช้สำหรับการพัฒนา Web Application โดยใช้ Active Server Page Technology ระบบงานในส่วน Web Application ทั้งหมดนั้นถูกพัฒนาด้วย เครื่องมือนี้



รูปที่ 5.3 แสดงหน้าจอการทำงานของ Microsoft Visual Interdev 6.0

- **Microsoft Visual C++ 6.0**

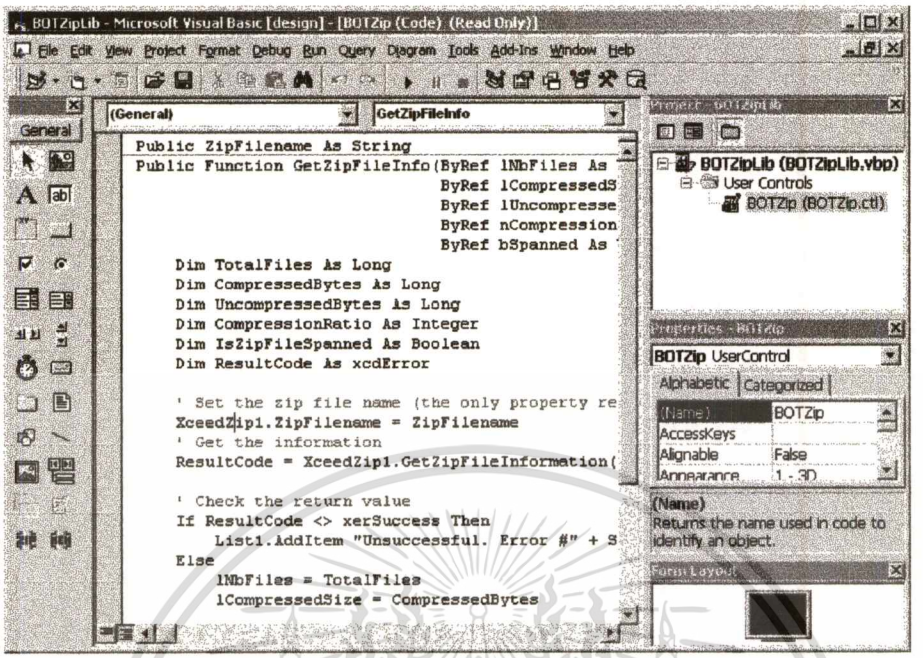
เครื่องมือ Microsoft Visual C++ 6.0 นั้นเป็นเครื่องมือที่ใช้สำหรับการพัฒนา ActiveX Control ต่างๆที่ต้องการติดต่อ Library ที่ซับซ้อนซึ่ง Visual Basic นั้นทำไม่ได้ หรือทำได้ยาก โดยใช้ภาษา C++ เป็นภาษาที่ใช้เขียนโปรแกรม



รูปที่ 5.4 แสดงหน้าจอการทำงานของ Microsoft Visual C++ 6.0

- **Microsoft Visual Basic 6.0**

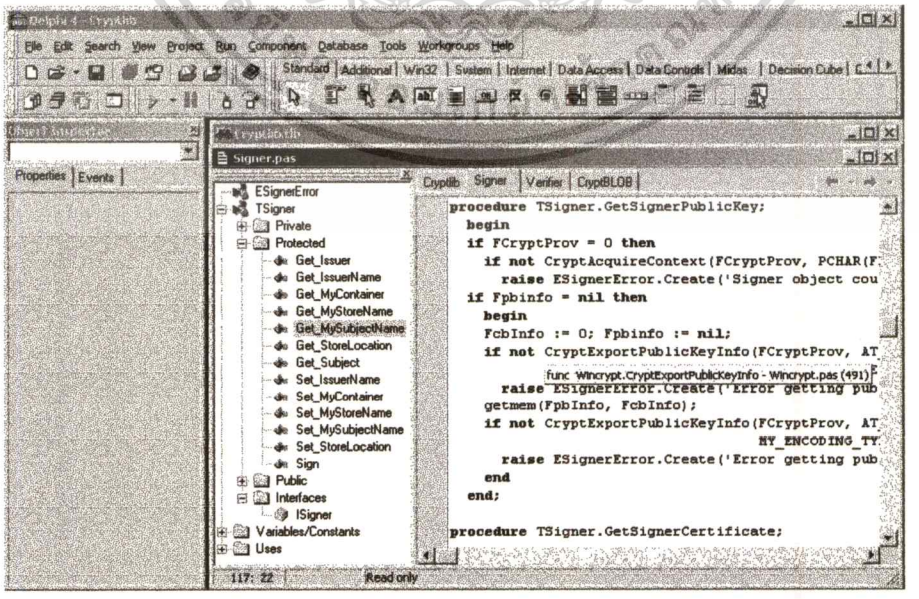
เครื่องมือ Microsoft Visual Basic 6.0 นั้นเป็นเครื่องมือที่ใช้สำหรับการพัฒนา Application ได้อย่างรวดเร็ว สำหรับ Application ที่เป็น Common User Interface จึงเหมาะต่อการใช้ Visual Basic มากกว่าในการพัฒนา OCX ที่ทำงานทั่วไป เพราะจะรวดเร็วในการพัฒนากว่า



รูปที่ 5.5 แสดงหน้าจอการทำงานของ Microsoft Visual Basic 6.0

- **Borland Delphi 4**

เครื่องมือ Borland Delphi 4 นั้นเป็นเครื่องมือที่ใช้สำหรับการพัฒนา Application ได้อย่างรวดเร็ว และสามารถพัฒนาส่วนประกอบซอฟต์แวร์ที่มีความซับซ้อนได้



รูปที่ 5.6 แสดงหน้าจอการทำงานของ Borland Delphi 4

5.2.2 การพัฒนา CryptLib.dll

CryptLib.dll นั้นเป็น Dll component ที่ถูกพัฒนาขึ้นด้วย Delphi 4 โดยใช้ CryptoAPI Library ที่มากับ Windows Platform SDK โดย CryptLib.dll จะทำหน้าที่ในส่วนของการลงลายเซ็นอิเล็กทรอนิกส์ และ ยืนยันลายเซ็นอิเล็กทรอนิกส์

```
...
  cbSignedMessageBlob := 0;
  if not CryptSignMessage(@SigParams, // Signature parameters
          FALSE,                  // Not detached
          1,                      // Number of messages
          @MsgArray,              // Messages to be signed
          @MsgSizeArray,          // Size of messages
          nil,                    // Buffer for signed msg
          cbSignedMessageBlob) then // Size of buffer
    raise    ESignerError.Create('Getting    Signed    Blob    Size    Failed
'+inttohex(GetLastError,8));

// Allocate memory for the signed blob.


  SignedMsg := CoCryptBLOB.Create;
  SignedMsg.ByteCount := cbSignedMessageBlob;

  if not CryptSignMessage(@SigParams,          // Signature parameters
          FALSE,                  // Not detached
          1,                      // Number of messages
          @MsgArray,              // Messages to be signed
          @MsgSizeArray,          // Size of messages
          PBYTE(SignedMsg.Bytes),        // Size of messages
          cbSignedMessageBlob) then // Size of buffer
    raise     ESignerError.Create('Sign     message     failed     '     +
inttostr(GetLastError));
  result := SignedMsg
  end;

function TSigner.Get_MyStoreName: WideString;
  begin
  result := ICertStore(FCertStore).StoreName
  end;
...
```

รูปที่ 5.7 แสดงตัวอย่าง Source Code ของ CryptLib.dll

5.2.3 การใช้งาน XceedZip.dll

XceedZip.dll เป็น Dll Component ที่ใช้สำหรับการบีบอัดข้อมูล ก่อนทำการส่งข้อมูล เพื่อทำการส่งข้อมูลได้รวดเร็วขึ้น และ XceedZip.dll นี้จะเป็นตัวทำการขยายข้อมูลให้ใหญ่ขึ้นเมื่อไฟล์มาถึงปลายทางด้วย (XceedZip.dll เป็น Third Party Software ที่นำมาใช้เสริมประสิทธิภาพให้กับระบบ ซึ่งผู้พัฒนาระบบมิได้พัฒนาขึ้นเอง)

5.2.4 การพัฒนา FileSelect.ocx

FileSelect.ocx เป็น ActiveX Control ใช้ในการเลือกไฟล์เพื่อส่งข้อมูล ซึ่งถูกพัฒนาขึ้นโดยใช้ Visual C++ และอาศัย Microsoft Foundation Class ในการพัฒนา

```
…
BSTR CFileSelectCtrl::Select()
{
	CString strResult;

	char BASED_CODE *szFilter;
	if (m_fileExt == "")
		szFilter = "All Files (*.*)|*.*||";
	else
		szFilter = m_fileExt.GetBuffer(0);
	CFileDialog dlgBrowse( TRUE, NULL, m_fileName.GetBuffer(0),
		OFN_HIDEREADONLY | OFN_OVERWRITEPROMPT | OFN_ALLOWMULTISELECT,
		szFilter, NULL);

	char BigBuff[25600];
	memset(BigBuff, '\0', sizeof(BigBuff));

	m_numSelect = 0;
	m_fileString.Empty();                    // Reset file name list

	dlgBrowse.m_ofn.lpstrFile = BigBuff;
	dlgBrowse.m_ofn.nMaxFile  = sizeof(BigBuff);


	if (dlgBrowse.DoModal()!=IDOK)
		;// Do nothing
	else
	{
		POSITION pos = dlgBrowse.GetStartPosition();
		if (pos)
			m_numSelect = 1;
		else
			m_numSelect = 0;
		m_fileString = dlgBrowse.GetNextPathName(pos);

		while(pos)
		{
			m_fileString = m_fileString+"," +
				dlgBrowse.GetNextPathName(pos);
			m_numSelect++;
		}
	}

	strResult = m_fileString;

	return strResult.AllocSysString();
}
…
```

รูปที่ 5.8 แสดงตัวอย่าง Source Code ของ FileSelect.ocx

5.2.5 การพัฒนา PostFile.ocx

PostFile.ocx เป็น ActiveX Control ใช้ในการส่งไฟล์มายัง Server ผ่าน HTTP Post Protocol และถูกพัฒนาขึ้นโดยใช้ Visual C++ และใช้ Web Publishing API เป็น API Libray ในการพัฒนาขึ้นมา

```
…
BOOL CPostFileCtrl::Upload()
{
	CString s;
	int pos = 0;
	int next_pos = 0;
	char**  fileString;                                  // Files to be uploaded

	if (m_fileList.IsEmpty()) {
	  MessageBox("File list is empty", "Error", MB_OK | MB_ICONWARNING);
	  return FALSE;
	}

	fileNameArray.RemoveAll();

	while (pos <= m_fileList.GetLength() && next_pos != -1) {
		next_pos = m_fileList.Find(", ", pos);
		if (next_pos == -1)
		 fileNameArray.Add(LPCTSTR (m_fileList.Mid(pos).GetBuffer(0)));
		else
		 fileNameArray.Add(LPCTSTR (m_fileList.Mid
				(pos, next_pos - pos).GetBuffer(0)));
		pos = next_pos + 2;
	}

	numFileUpload = fileNameArray.GetSize();
	CString *sTemp = fileNameArray.GetData();
	fileString = (char**) malloc(numFileUpload * sizeof(char*));

	for (int i=0; i < numFileUpload; i++)
	{	fileString[i] = sTemp[i].GetBuffer(0);  }

	// Set up variables for WpPost
	DWORD  szURL, szName;
	LPTSTR destURL, siteName;
	HRESULT hResult = NO_ERROR;

	if ( m_siteURL.IsEmpty() )
		destURL = "http://botconnect/upload";
	else
		destURL  = m_siteURL.GetBuffer(0);

	if ( m_siteName.IsEmpty() )
		siteName = "botconnect";
	else
		siteName = m_siteName.GetBuffer(0);
…
```

รูปที่ 5.9 แสดงตัวอย่าง Source Code ของ PostFile.ocx

5.2.6 การพัฒนา Username.ocx

Username.ocx เป็น ActiveX Control ใช้ในการตรวจสอบ Username ของผู้ใช้งานว่าเป็น User คนใดที่ Log in เข้ามา ซึ่งถูกพัฒนาขึ้นโดยใช้ Visual C++

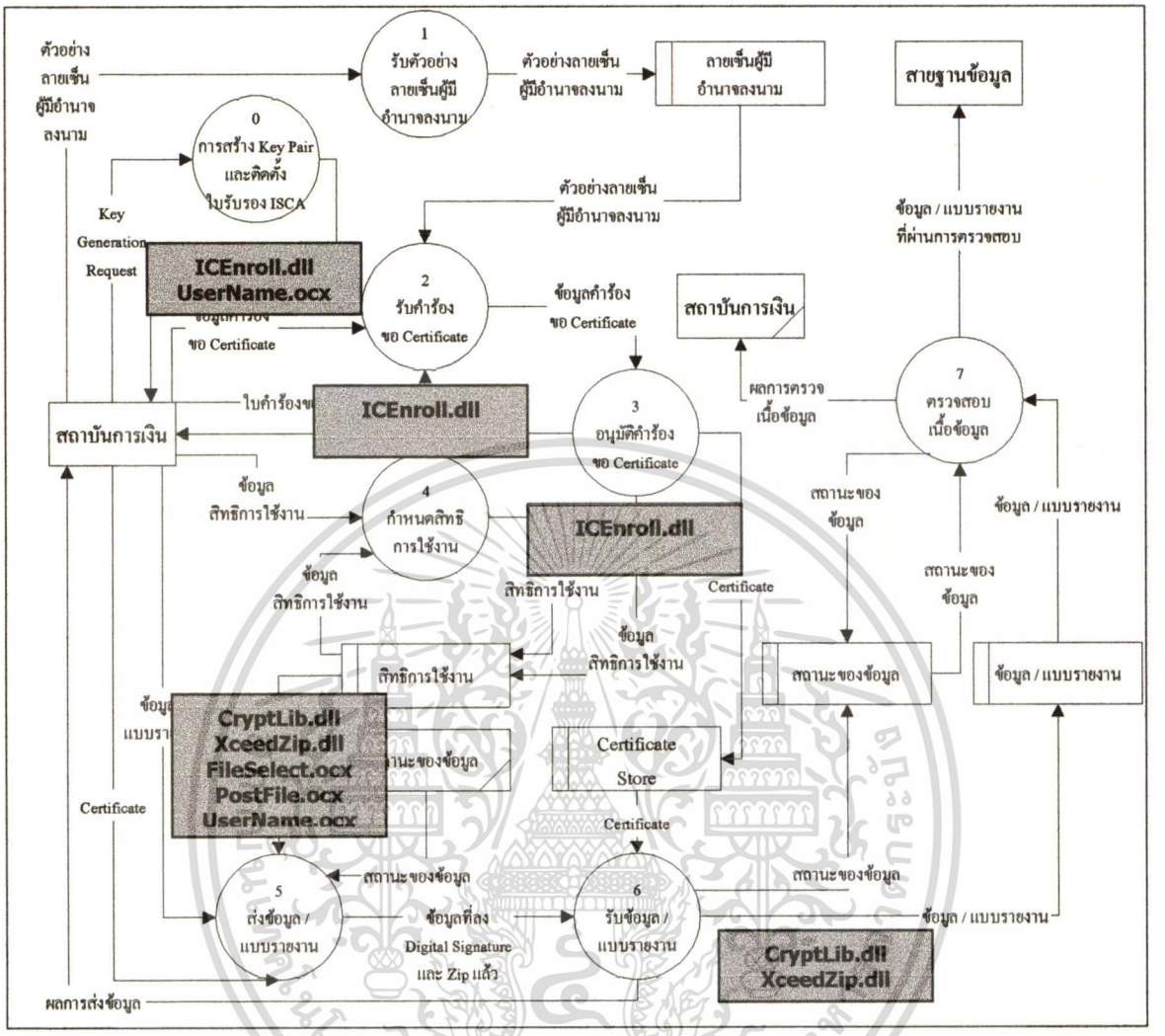
```
...
        // STEP 1: Computing Username length
        if (GetUserName(NULL, &nLength) == 0) {
        // Error: Computing Username length
              DisplayError("GetUserName");
              return NULL;
        }

        // STEP 2: Allocate memory for Username buffer
        if ((lpUserName = (LPTSTR) malloc(nLength)) == NULL) {
              // Error: Out of memory
              DisplayError("Memory Allocation");
              return NULL;
        }

        // STEP 3: Get Username and store it in buffer
        if (GetUserName(lpUserName, &nLength) == 0) {
              // Error: During GetUserName
              DisplayError("GetUserName");
              return NULL;
        }

        strResult = CString (lpUserName);
        free(lpUserName);
        return strResult.AllocSysString();
...
```

รูปที่ 5.10 แสดงตัวอย่าง Source Code ของ UserName.ocx

5.2.6 การใช้งาน ICEnroll.dll

ICEnroll.dll เป็น Software Component ที่มากับการติดตั้ง Certificate Service ซึ่งนำไปใช้ในสร้าง Key Pair และ แปล Format ของ Certificate Request ในขั้นตอนการขอและติดตั้งใบรับรอง (ส่วนนี้มิได้พัฒนาขึ้นเอง)

ทั้งนี้ส่วนประกอบซอฟต์แวร์ที่ทำการพัฒนาขึ้นนั้นมีหน้าที่และการทำงานในส่วนต่างๆ ของระบบ ซึ่งสามารถแสดงการใช้งานในแผนภาพการไหลวัยนของข้อมูลดังรูปที่ 5.11



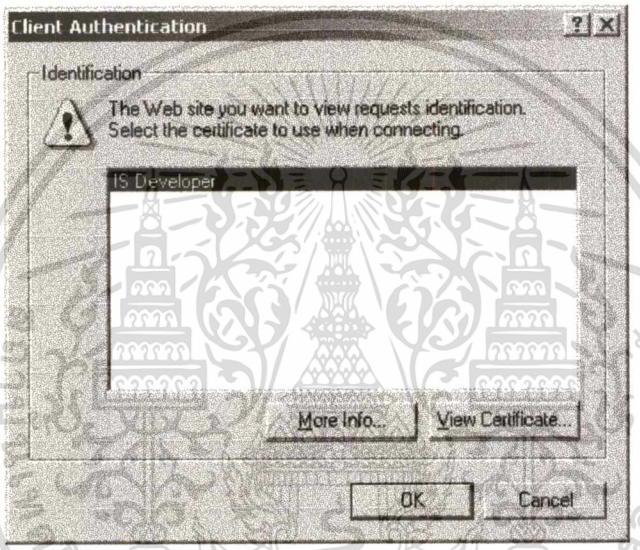
รูปที่ 5.11 แสดงการใช้งานของส่วนประกอบซอฟต์แวร์ที่พัฒนาขึ้นในขั้นตอนการทำงานในระบบ

จากรูปที่ 5.11 สามารถสรุปรายละเอียดการใช้งานได้ดังนี้

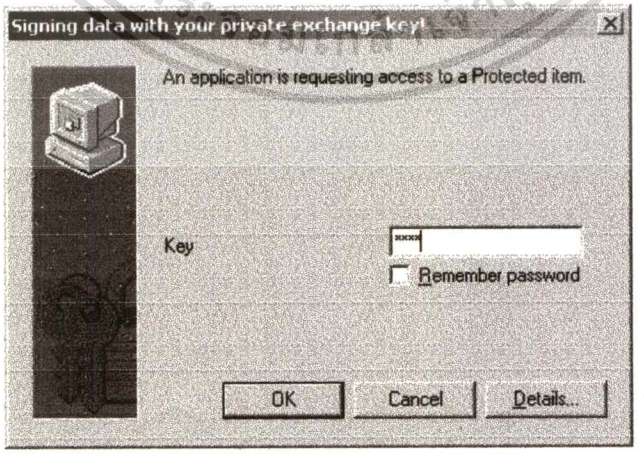
- ขั้นตอนการสร้าง Key Pair จะอาศัย ICEnroll.dll และ Username.ocx ในการช่วยสร้าง Key
- ขั้นตอนการรับ และอนุมัติคำร้องขอใบรับรอง จะอาศัย ICEnroll.dll เพื่อแปล Format การขอ / อนุมัติใบรับรองให้เป็น Format มาตรฐาน (PKCS10 และ PKCS7) แล้วจึงส่งให้ทาง Certificate Service ประมวลผลต่อไป
- ขั้นตอนการส่งข้อมูลจะใช้ Username.ocx เพื่อตรวจสอบผู้ใช้งาน และใช้ FileSelect.ocx เพื่อเลือกข้อมูล ใช้ XceedZip.dll เพื่อบีบอัดข้อมูลให้เล็กลง ใช้ CryptLib.dll เพื่อลงลายเซ็นอิเล็กทรอนิกส์ แล้วจึงใช้ PostFile.ocx เพื่อนำส่งข้อมูลไปยังเซิร์ฟเวอร์
- CryptLib.dll และ XceedZip.dll จะถูกใช้เพื่อตรวจสอบ ลายเซ็นอิเล็กทรอนิกส์ และขยายไฟล์ตามลำดับในขั้นตอนการรับข้อมูล

5.3 การพัฒนาระบบงาน Web Application

ในส่วนของการพัฒนาระบบงาน Web Application นั้นจะนำกลไกการทำ Client Authentication ในทุกหน้าจอที่ต้องการความปลอดภัยด้วยการตรวจสอบใบรับรอง และทำการสร้าง SSL connection (HTTPS) หลังจากผ่านการตรวจสอบแล้ว โดยผู้ใช้งานจะพบหน้าจอ Dialog ดังรูปที่ 5.12 ซึ่งแสดงถึงใบรับรองของผู้ใช้งานที่ระบบตรวจพบ และในกรณีที่มีการเรียกใช้ Key เพื่อเข้าหรือถอดรหัส จะปรากฏหน้าจอป้องกันการใช้ Key ดังรูปที่ 5.13 โดยจะต้องใส่ PIN ที่ถูกต้องเท่านั้นจึงจะสามารถใช้ Key ของผู้ใช้งานได้



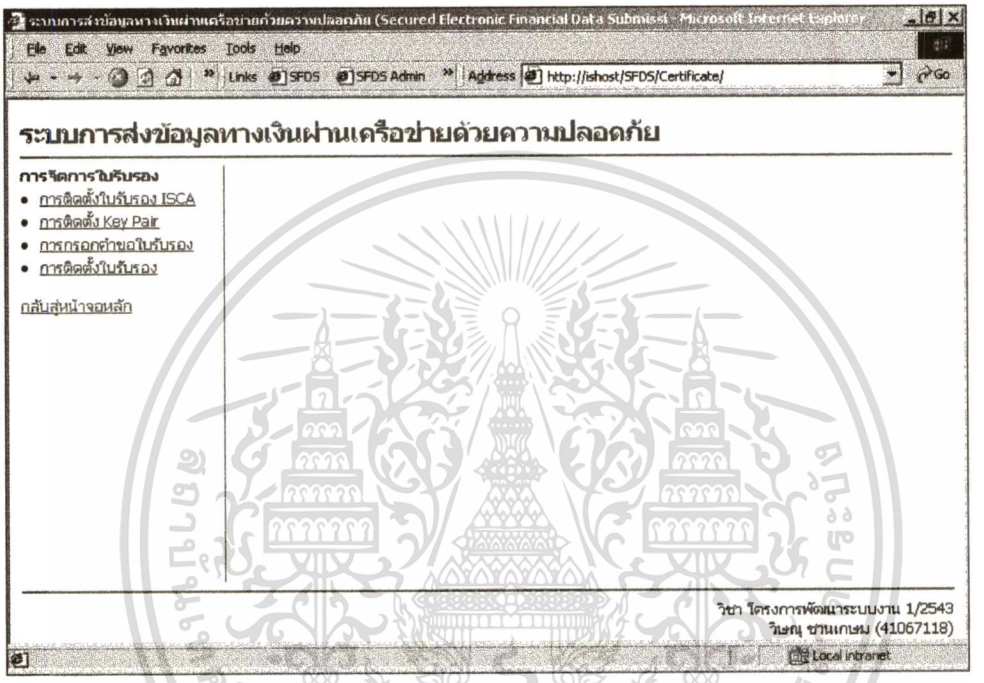
รูปที่ 5.12 แสดงหน้าจอการทำ Client Authentication



รูปที่ 5.13 แสดงหน้าจอการป้องกันการใช้ Key

5.3.1 ส่วนการจัดการใบรับรอง

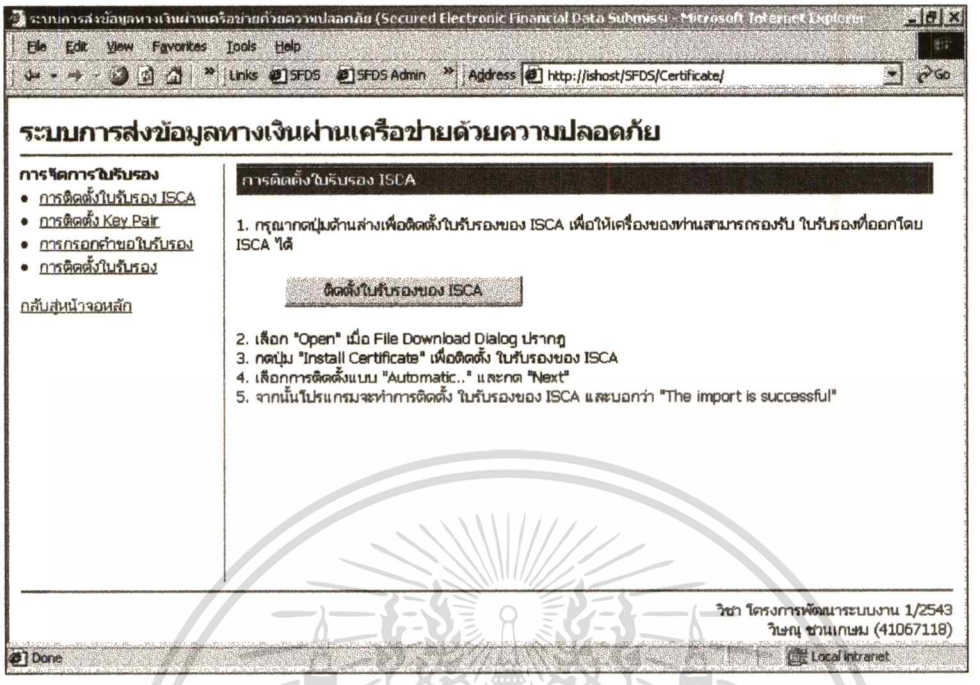
เนื่องจากระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัย ใช้เทคโนโลยี ของใบรับรองอิเล็กทรอนิกส์ (Digital Certificate หรือ Certificate) เป็นกลไกในการทำงาน ดังนั้นผู้ใช้งานจะต้องมีกุญแจรหัสลับ (Private/Public Key Pair) และ Certificate ในการทำงาน



รูปที่ 5.14 แสดงหน้าจอส่วนการจัดการใบรับรอง

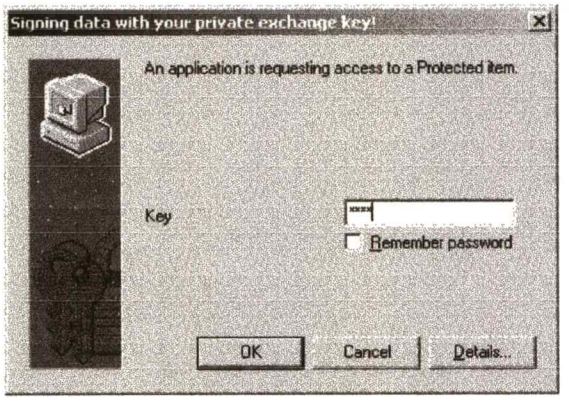
จากรูปที่ 5.14 มีรายละเอียดเมนูการใช้งานดังนี้

- **การติดตั้งใบรับรองของ ISCA** หรือ Certificate ของ Certificate Authority ของระบบ ซึ่งเป็นการติดตั้ง Trusted Root Certificate Authority ให้กับเครื่องของผู้ใช้งาน ซึ่งเมื่อเลือกหัวข้อนี้จะปรากฏหน้าจอดังรูปที่ 5.15 โดยผู้ใช้งานจะกดปุ่ม "ติดตั้งใบรับรองของ ISCA" เพื่อติดตั้งใบรับรองของ ISCA ให้กับเครื่องของตน

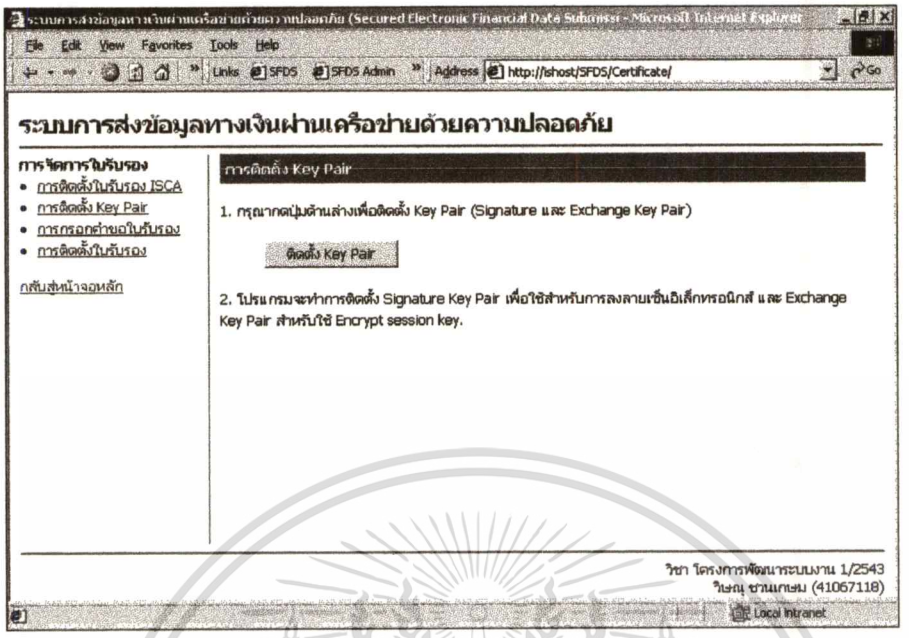


รูปที่ 5.15 แสดงหน้าจอส่วนการติดตั้งใบรับรองของ ISCA

- **การติดตั้ง Key Pair** จะเป็นการติดตั้ง Key Pair สำหรับการใช้งานคือ Signature Key Pair (ประกอบไปด้วย Public Signature Key และ Private Signature Key) และ Exchange Key Pair (ประกอบไปด้วย Public Exchange Key และ Private Exchange Key) ซึ่ง Signature Key Pair นั้นจะใช้สำหรับการลงลายเซ็นอิเล็กทรอนิกส์ ส่วน Exchange Key Pair นั้นจะใช้สำหรับการเข้ารหัส Session Key เมื่อมีการสร้าง SSL Connection ซึ่งเมื่อเลือกหัวข้อนี้จะปรากฏหน้าจอดังรูปที่ 5.17 โดยผู้ใช้งานจะกดปุ่ม "ติดตั้ง Key Pair" เพื่อติดตั้ง Key Pair ให้กับเครื่องของตน ทั้งนี้จะปรากฏหน้าจอให้ใส่ PIN เพื่อป้องกันการใช้ Key ดังรูปที่ 5.16

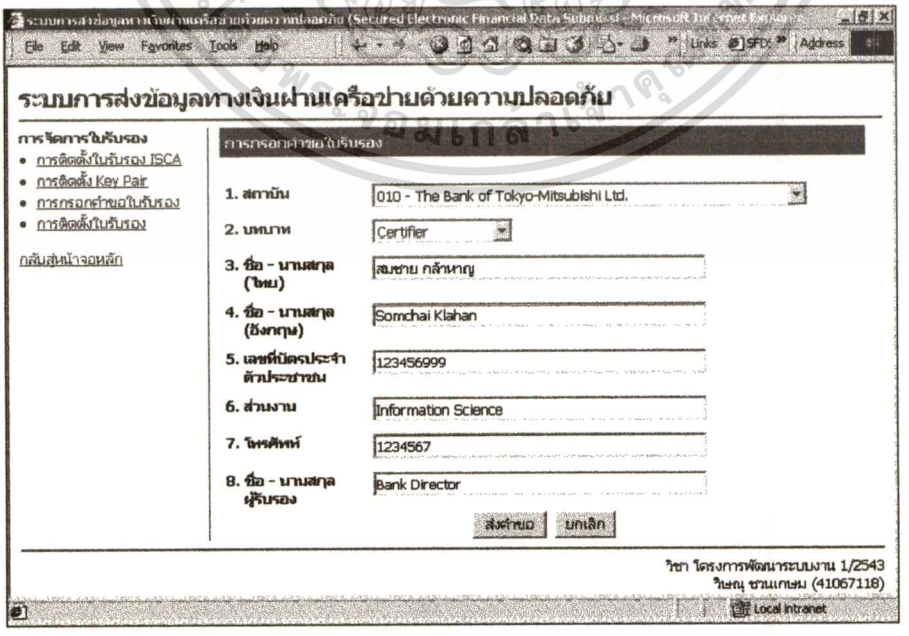


รูปที่ 5.16 แสดงหน้าจอติดตั้งการป้องกันการใช้ Key



รูปที่ 5.17 แสดงหน้าจอส่วนการติดตั้ง Key Pair

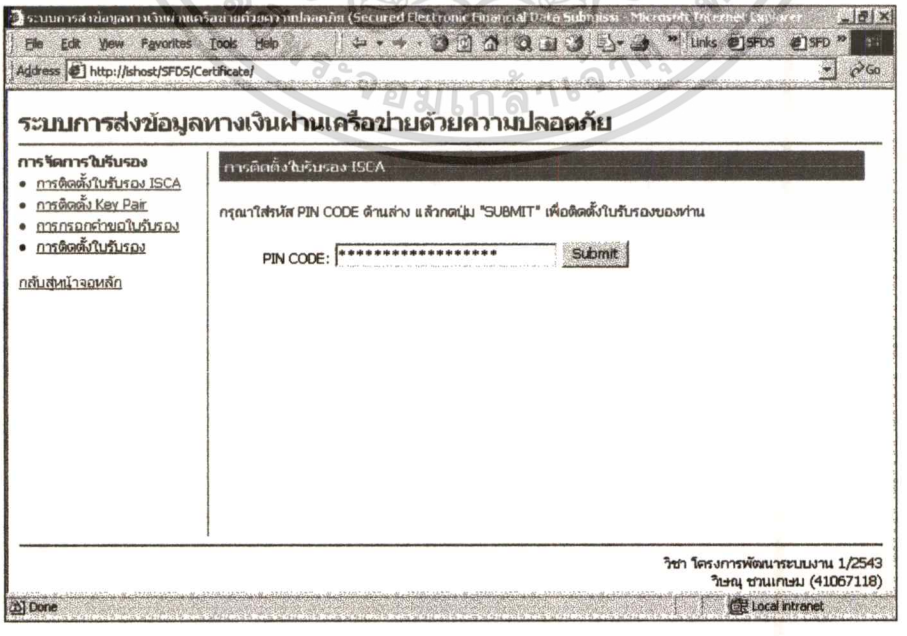
- **การกรอกคำขอใบรับรอง** จะเป็นการรับข้อมูลคำขอจากผู้ใช้งานเพื่อขอใบรับรอง ซึ่งเมื่อเลือกหัวข้อนี้จะปรากฏหน้าจอดังรูปที่ 5.18 โดยผู้ใช้งานจะทำการกรอกรายละเอียดของตน แล้วจึงกดปุ่ม "ส่งคำขอ" จะปรากฏหน้าจอยืนยันข้อมูลที่ได้กรอกไปดังรูปที่ 5.19 โดยถ้ากดปุ่มยืนยันข้อมูลคำขอจะถูกส่งมายังศูนย์รับข้อมูล



รูปที่ 5.18 แสดงหน้าจอส่วนการกรอกคำขอใบรับรอง

รูปที่ 5.19 แสดงหน้าจอส่วนการยืนยันคำขอใบรับรอง

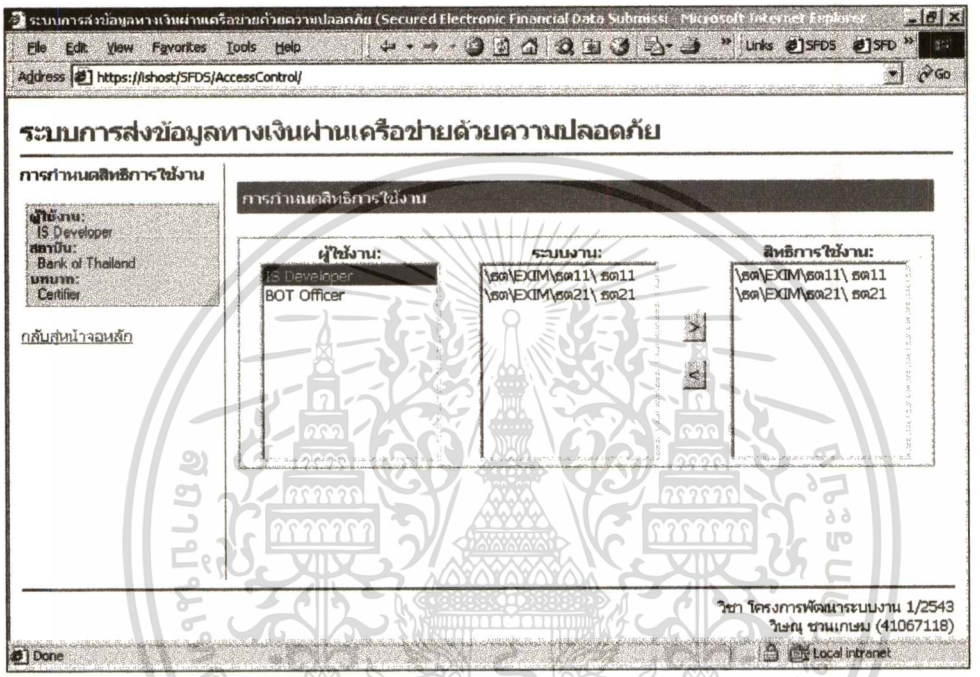
- **การติดตั้งใบรับรอง** จะเป็นการเข้าไปติดตั้งใบรับรองเมื่อได้รับการอนุมัติแล้ว ซึ่งเมื่อเลือกหัวข้อนี้จะปรากฏหน้าจอดังรูปที่ 5.20 โดยผู้ใช้งานจะทำการกรอก PIN Code ซึ่งจะใช้ปลดล๊อกให้ผู้ใช้งานสามารถติดตั้งใบรับรองได้



รูปที่ 5.20 แสดงหน้าจอส่วนการติดตั้งใบรับรอง

5.3.2 ส่วนการกำหนดสิทธิผู้ใช้งาน

ก่อนการส่งข้อมูลนั้น จะต้องมีการกำหนดสิทธิการส่งรายงานสำหรับผู้ใช้งานโดย Certifier ก่อน ซึ่งในส่วนการกำหนดสิทธินี้จะเข้าได้เฉพาะผู้มีสิทธิในการกำหนดสิทธิ (Certifier) ซึ่งจะแสดงรายชื่อ Officer ที่อยู่ในความควบคุม และสิทธิที่สามารถกำหนดได้ ดังรูปที่ 5.21



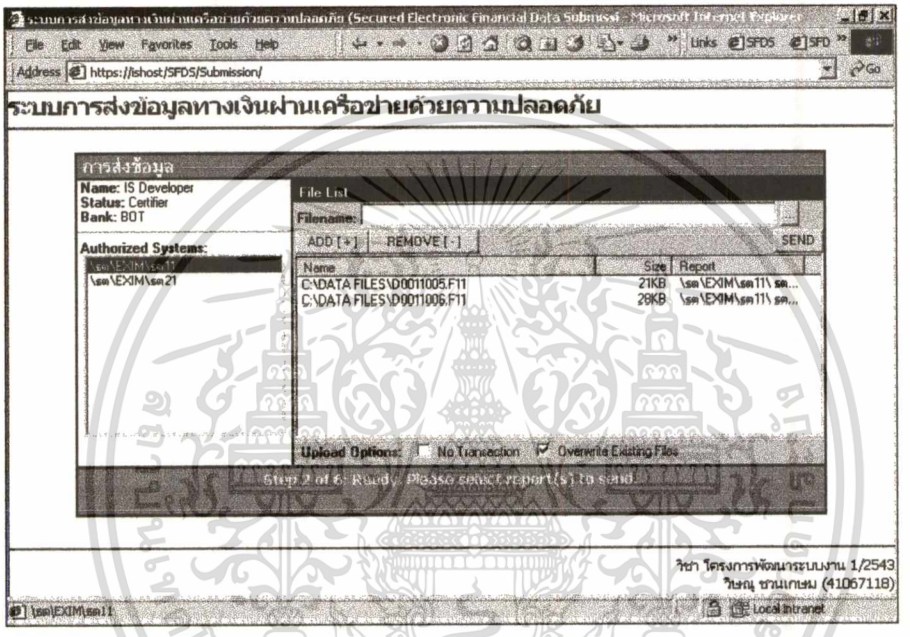
รูปที่ 5.21 แสดงหน้าจอส่วนการกำหนดสิทธิผู้ใช้งาน

จากรูปที่ 5.21 มีรายละเอียดดังนี้

- แสดงชื่อ บทบาท และสถาบันการเงินที่ Certifier สังกัดอยู่
- แสดงรายชื่อของผู้ใช้งานที่รับรองโดย Certifier รวมถึงชื่อของ Certifier เอง
- แสดงสถานะของการทำงานและรายชื่อผู้ใช้ที่ถูกเลือก (หน้าต่างด้านซ้าย)
- แสดงรายงานทั้งหมดที่ Certifier ผู้นี้มีสิทธิ (หน้าต่างตรงกลาง)
- แสดงรายงานที่ผู้ใช้ที่ถูกเลือก มีสิทธิส่งทั้งหมด (หน้าต่างด้านขวา)
- ปุ่ม “>” ใช้สำหรับการเพิ่มสิทธิให้กับผู้ใช้งาน
- ปุ่ม “<” ใช้สำหรับการยกเลิกสิทธิของผู้ใช้งาน

5.3.3 ส่วนการส่งข้อมูล

ถ้าผู้ใช้มี Certificate ที่ถูกต้องและมีสิทธิ์ในการส่งข้อมูล / แบบรายงาน โปรแกรมจะแสดงจอภาพหลักของการส่งข้อมูล / แบบรายงาน โดยในจอภาพนี้จะแสดงรายละเอียดและสิทธิ์ในการใช้ระบบของผู้ใช้งาน โดยผู้ใช้งานเลือก Authorized System ที่มีสิทธิและกดปุ่ม "ADD" เพื่อเลอกไฟล์ และกด "SEND" เพื่อส่งไฟล์ ดังรูปที่ 5.22



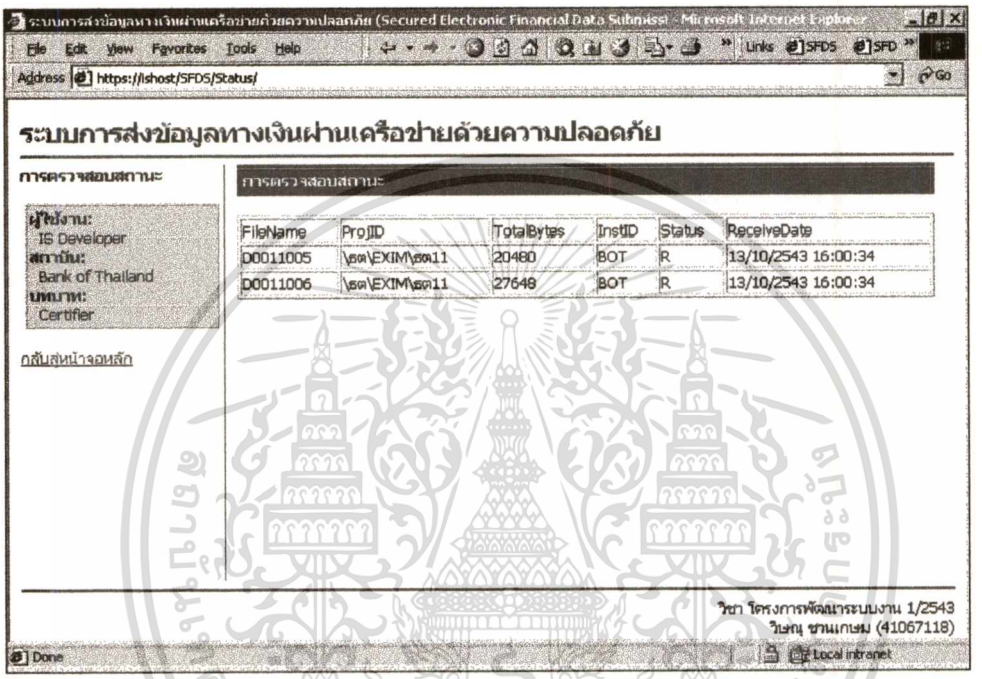
รูปที่ 5.22 แสดงหน้าจอส่วนการส่งข้อมูล / แบบรายงาน

จากรูปที่ 5.22 มีรายละเอียดดังนี้

- แสดงชื่อผู้ใช้งาน บทบาท และสถาบันการเงินที่ ผู้ใช้งานสังกัดอยู่
- แสดงรายชื่อของระบบที่ผู้ใช้งานมีสิทธิ์ส่งข้อมูล / แบบรายงาน
- กล่องรับชื่อไฟล์จากการพิมพ์โดยผู้ใช้งาน
- ปุ่ม "Add" ใช้สำหรับเพิ่มไฟล์ในรายการส่ง
- ปุ่ม "Remove" ใช้สำหรับลบไฟล์ออกจากรายการส่ง
- แสดงรายการไฟล์ต่างๆที่เลือกไว้เพื่อส่ง
- ข้อเลือกต่างๆที่ใช้ในการส่งข้อมูล / แบบรายงาน
- ปุ่ม "SEND" ใช้สำหรับสั่งเริ่มการส่งข้อมูล / แบบรายงาน
- บริเวณด้านล่างแสดงสถานะของการส่งข้อมูล / แบบรายงาน

5.3.4 ส่วนการตรวจสอบสถานะของข้อมูล

เมื่อผู้ใช้งานได้ส่งข้อมูลเรียบร้อยแล้ว ทางเครื่อง Server จะทำการตรวจสอบความถูกต้องของข้อมูลตามเงื่อนไขของแต่ละระบบ ซึ่งผู้ใช้งานต้องเข้ามาเรียกดูผลการตรวจสอบสถานะของ File ที่ส่งทางจอภาพ โดยจะมีสิทธิเรียกดูเฉพาะแบบรายงานที่ตนส่งมาเท่านั้น ดังรูปที่ 5.23



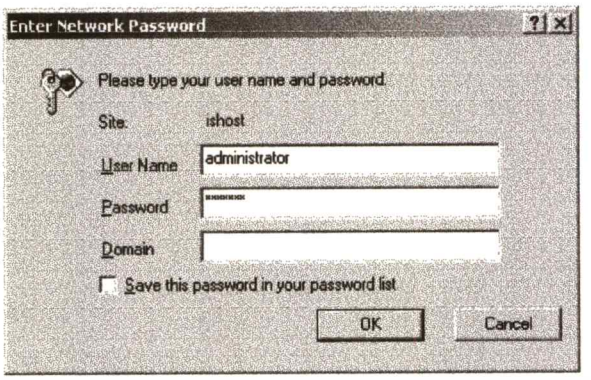
รูปที่ 5.23 แสดงหน้าจอส่วนการตรวจสอบสถานะของข้อมูล

จากรูปที่ 5.23 มีรายละเอียดดังนี้

- แสดงรายละเอียดของผู้ใช้งาน ได้แก่ ชื่อ บทบาท และสถาบันการเงินที่ผู้ใช้งานสังกัดอยู่
- แสดงรายละเอียดของสถานะของ File ข้อมูลที่ส่งมา

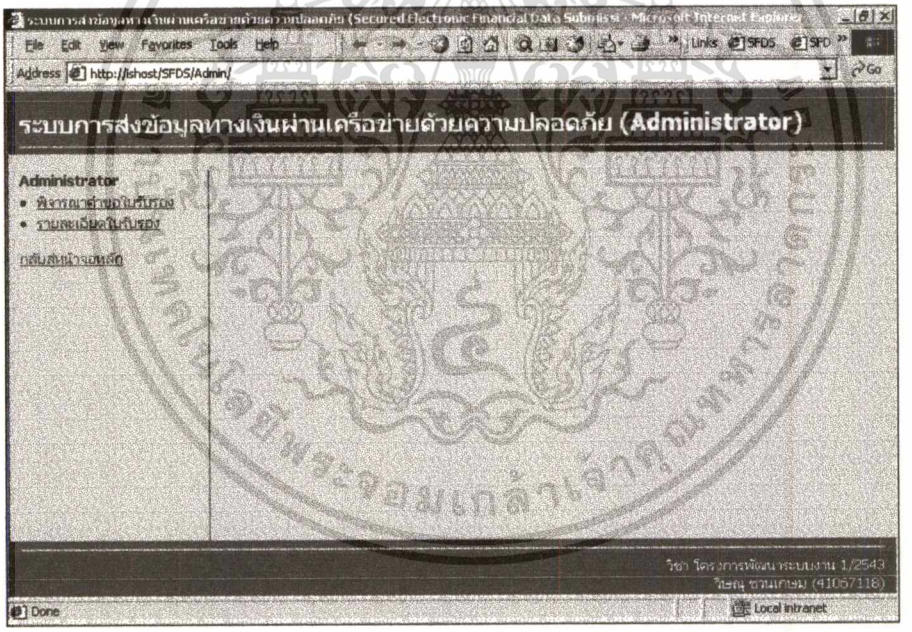
5.3.5 ส่วนการจัดการระบบ (Admin)

เมื่อผู้ใช้งานได้ส่งคำขอใบรับรองมาเรียบร้อยแล้ว ทางผู้จัดการระบบของศูนย์รับข้อมูลจะทำการตรวจสอบใบคำขอที่ส่งมาในรูปกระดาษ และ ข้อมูลคำขอที่ส่งมาในรูปอิเล็กทรอนิกส์ด้วยการเข้าใช้งาน ส่วนการจัดการระบบ โดยผู้ที่จะเข้าใช้งานได้นั้นจะต้องมีสิทธิในตาราง BOTRight ซึ่งทางระบบจะขึ้น Dialog ให้ใส่ Password ดังรูปที่ 5.24



รูปที่ 5.24 แสดงหน้าจอการ Logon เข้าหน้าจอ การจัดการระบบ

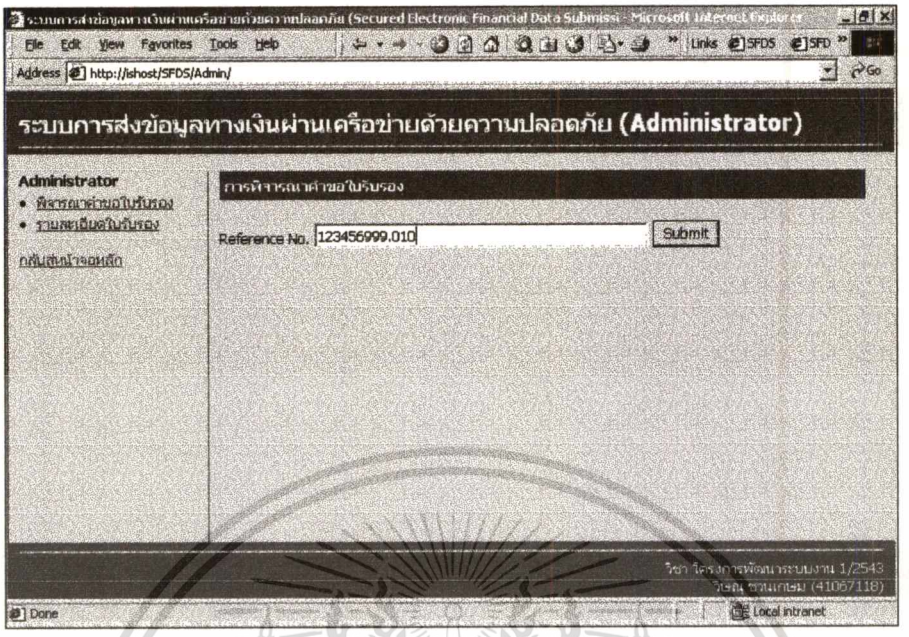
เมื่อผ่านการ Logon เข้าหน้าจอการจัดการระบบ แล้วจะปรากฏหน้าจอหลักดังรูปที่ 5.25



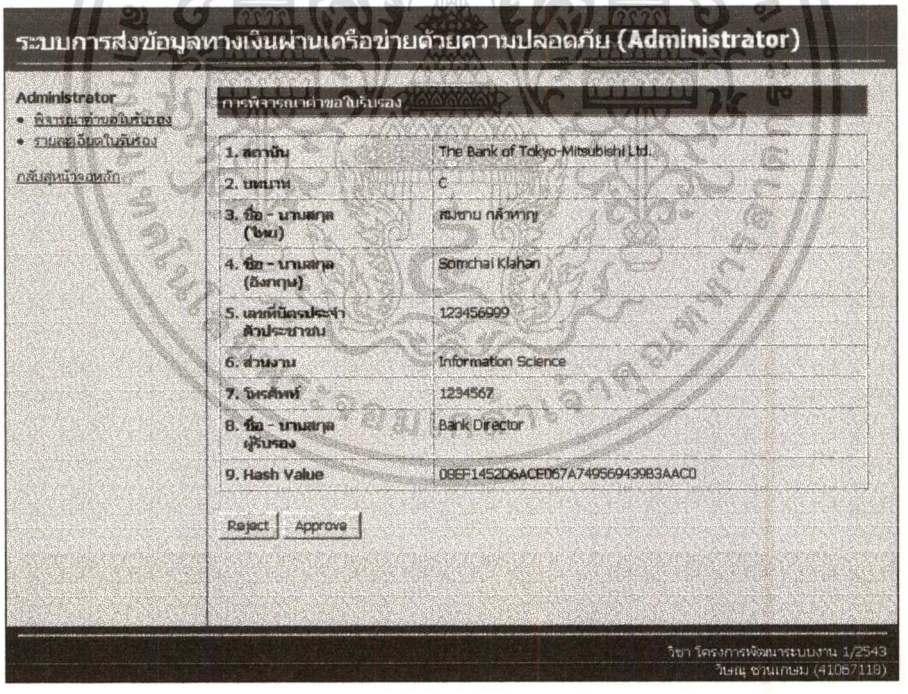
รูปที่ 5.25 แสดงหน้าจอ การจัดการระบบ

หน้าจอการจัดการระบบจะประกอบไปด้วยเมนูย่อยสองส่วนคือ

- **พิจารณาคำขอใบรับรอง** จะเป็นส่วนในการเรียกดูข้อมูลคำขอใบรับรองของผู้ใช้งานซึ่งเมื่อเลือกหัวข้อ "พิจารณาคำขอใบรับรอง" จะปรากฏหน้าจอดังรูปที่ 5.26 ซึ่งผู้จัดการระบบจะใส่หมายเลข Reference Number ที่ได้จากใบเอกสารคำขอใบรับรอง แล้วจึงกด "Submit" ดังจะปากฏหน้าจอรายละเอียดในรูปที่ 5.27



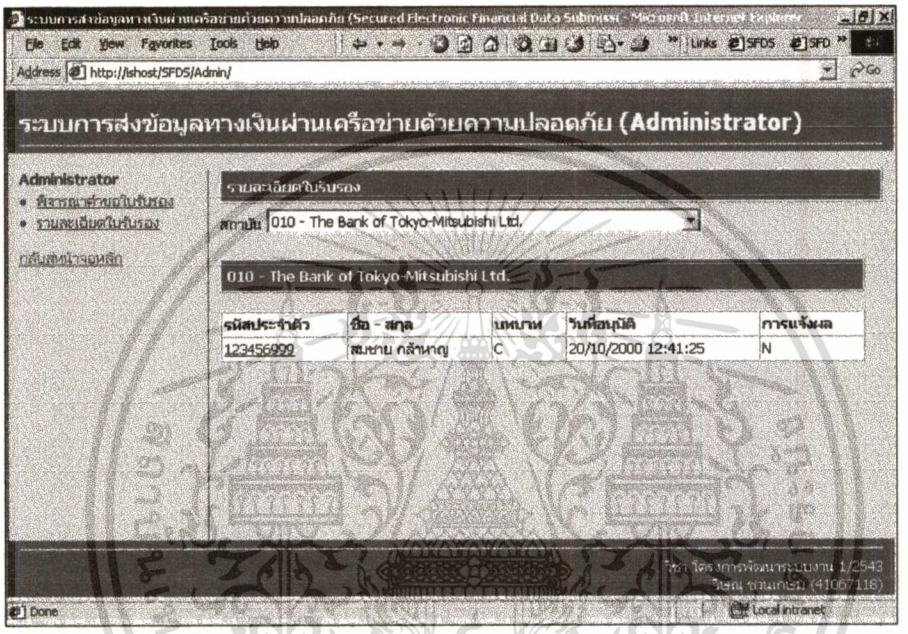
รูปที่ 5.26 แสดงหน้าจอ การพิจารณาคำขอใบรับรอง



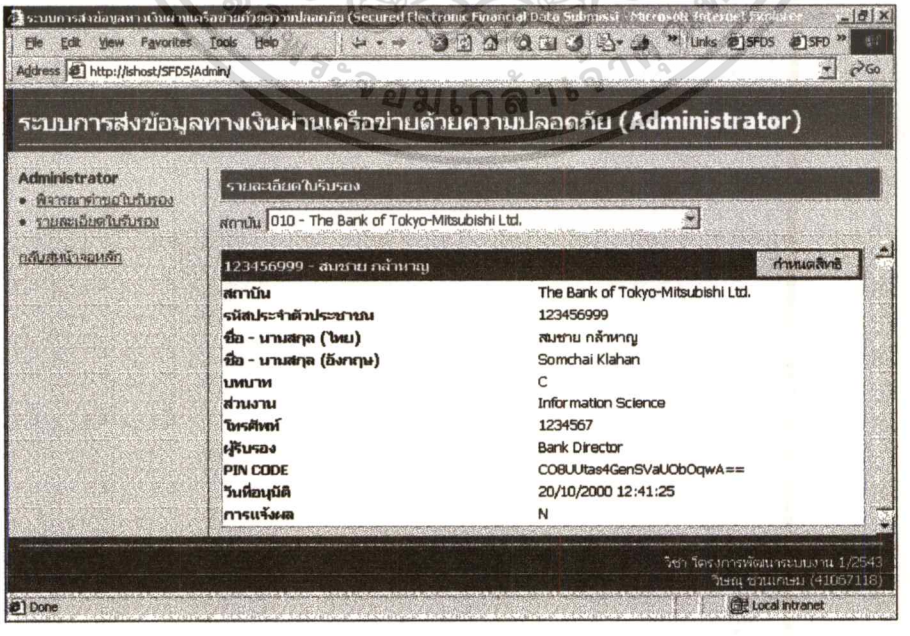
รูปที่ 5.27 แสดงหน้าจอรายละเอียดข้อมูลคำขอใบรับรอง

โดยผู้จัดการระบบจะตรวจสอบคำขอที่ได้รับและยืนยันว่าข้อมูลที่กรอกนั้นถูกต้อง โดยอิงกับค่า Hash Value ที่ได้จากการนำข้อมูลผ่าน Hash Function (Algorithm คือ MD5) ซึ่งเป็น One – Way Hash จะได้ค่าเฉพาะออกมาใช้ยืนยันได้ว่าข้อมูลทั้งสองชุดสอดคล้องกัน (ค่า Hash ได้เหมือนกัน) แล้วจึงกดปุ่ม “Approve” เพื่ออนุมัติ

- **รายละเอียดใบรับรอง** จะเป็นส่วนในการเรียกดูรายละเอียดผู้ใช้งานที่ผ่านการอนุมัติแล้ว เมื่อเลือกหัวข้อ “รายละเอียดใบรับรอง” จะปรากฏหน้าจอดังรูปที่ 5.28 ซึ่งผู้จัดการระบบจะทำการเลือก “สถาบัน” ซึ่งโปรแกรมจะทำการดึงรายชื่อผู้ใช้งานของสถาบันนั้นมาแสดงด้านล่างซึ่งผู้จัดการระบบสามารถเข้าไปดูรายละเอียดด้วยการคลิก “รหัสประจำตัว” ของผู้ใช้งาน ซึ่งจะไปเรียกหน้าจอดังรูปที่ 5.29 เพื่อแสดงรายละเอียด

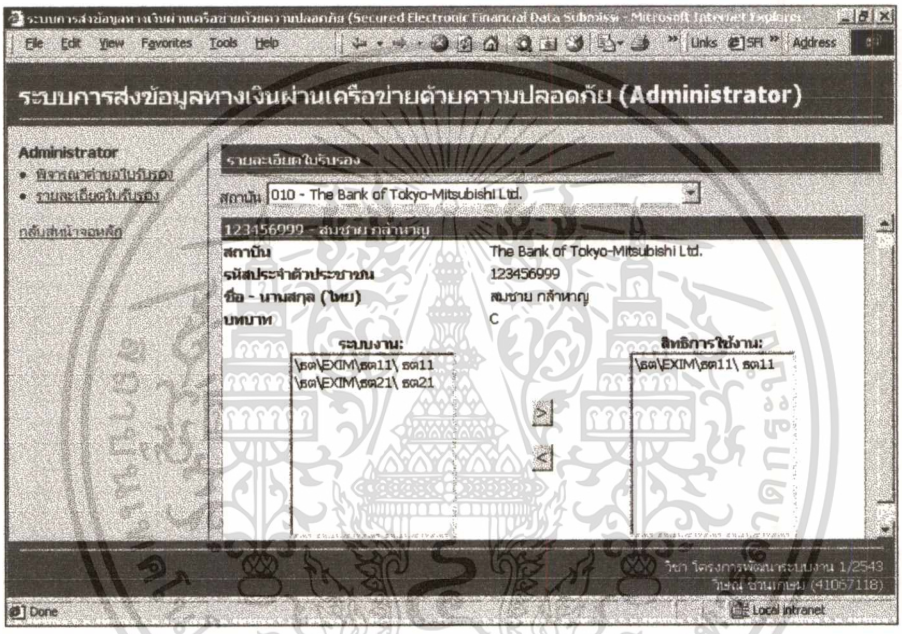


รูปที่ 5.28 แสดงหน้าจอรายละเอียดใบรับรอง



รูปที่ 5.29 แสดงหน้าจอรายละเอียดของผู้ใช้งาน

ในกรณีที่ผู้ใช้งานนั้นเป็น Certifier ซึ่งจะมีสิทธิในการกำหนดสิทธิให้กับ Officer ภายในการดูแล จะปรากฏปุ่ม “กำหนดสิทธิ” ให้ผู้จัดการระบบสามารถกำหนดสิทธิให้กับ Certifier ว่าสามารถควบคุมการกำหนดสิทธิของแบบรายงานใดบ้าง โดยเมื่อกดปุ่ม “กำหนดสิทธิ” จะปรากฏหน้าจอดังรูปที่ 5.30 โดยจะมีรายชื่อระบบงานทั้งหมดของระบบขึ้นมาทางหน้าต่างซ้าย ซึ่งผู้จัดการระบบจะทำการเลือกระบบที่ Certifier ขอสิทธิในการใช้งานมา แล้วกดปุ่ม “>” เพื่อ เพิ่มสิทธิ หรือปุ่ม “<” เพื่อลดสิทธิ



รูปที่ 5.30 แสดงหน้าจอการกำหนดสิทธิของ Certifier

บทที่ 6
บทสรุปและข้อเสนอแนะ

จากการพัฒนาระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัยนั้น ได้ผลสรุปและแนวทางข้อเสนอแนะดังนี้

6.1 บทสรุป

การพัฒนาระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายด้วยความปลอดภัยนี้ เป็นการพัฒนาระบบที่ช่วยอำนวยความสะดวกและเสริมประสิทธิภาพสำหรับผู้ใช้งานในการนำส่งข้อมูล และ สำหรับทางศูนย์ข้อมูลในการรับข้อมูลเพื่อนำไปใช้งานได้รวดเร็วขึ้น โดยอาศัยการส่งข้อมูลในรูปสื่ออิเล็กทรอนิกส์ผ่านเครือข่ายที่นำเอากลไกความปลอดภัยในระดับต่างๆมาประยุกต์ใช้ในระบบทำให้สามารถรักษาความลับและความดั้งเดิมของข้อมูลที่นำส่งโดยผู้ใช้งานที่มีสิทธิในการใช้งานซึ่งผ่านการยืนยันและรับรองแล้ว เนื่องจากระบบมีรูปแบบการทำงานแบบกระจาย จึงทำให้ผู้ใช้งานที่อยู่ไกลออกไปสามารถเรียกใช้งานระบบได้สะดวกยิ่งขึ้น

ในการทำงานของระบบนั้น ข้อมูลจะถูกส่งข้ามเครือข่ายเฉพาะด้วยการเชื่อมต่อแบบทางไกลผ่านโมเด็มและมีรูปแบบการใช้งานแบบโปรแกรมประยุกต์ผ่าน เวิลด์ ไวด์ เว็บ ซึ่งมีลักษณะการทำงานแบบกระจายและสามารถรองรับการใช้งานจากภูมิภาคต่างๆของประเทศได้ ส่วนกลไกความปลอดภัยที่นำมารองรับการทำงานนั้น จะเริ่มจากการยืนยันผู้เข้าใช้งานด้วยการตรวจสอบใบรับรองอิเล็กทรอนิกส์ที่ผ่านการรับรองแล้ว จากนั้นจึงมีการตรวจสอบสิทธิในการใช้งานของผู้ใช้งาน ว่าสามารถส่งข้อมูลแบบใดได้บ้าง โดยในการส่งข้อมูลนั้นระบบจะทำการบีบอัดข้อมูลให้มีขนาดเล็กลงและทำการลงลายเซ็นอิเล็กทรอนิกส์กับข้อมูลด้วย Private Key ของผู้ส่ง ก่อนที่จะทำการเชื่อมต่อกับศูนย์รับข้อมูลปลายทางโดยใช้โปรโตคอล SSL ซึ่งจะทำหน้าที่ในการเข้ารหัสเพื่อรักษาความลับของข้อมูลที่ส่งผ่านเครือข่าย และเมื่อข้อมูลเดินทางมาถึง ระบบจะทำการตรวจสอบลายเซ็นอิเล็กทรอนิกส์เพื่อยืนยันความดั้งเดิมของเนื้อข้อมูลมูลและยืนยันว่าข้อมูลนั้นถูกส่งมาจากผู้ส่งข้อมูลที่ผ่านการรับรองแล้ว

จากการทดลองใช้งานระบบที่พัฒนาขึ้นที่หน่วยงานของธนาคารแห่งประเทศไทยนั้น พบว่าระบบที่พัฒนาขึ้นสามารถนำไปใช้ส่งข้อมูลได้รวดเร็วและปลอดภัยโดยอาศัยกลไกความปลอดภัยที่ได้นำเสนอไว้ในข้างต้น โดยในส่วนการขอใบรับรองนั้นอาจยังมีความซับซ้อนในการใช้งาน

อยู่จึงทำให้ผู้ใช้งานที่ทดลองใช้ระบบยังสับสนอยู่ในตอนต้น แต่เมื่อมีการอธิบายรายละเอียดการทำงานเพิ่มเติมแล้วผู้ใช้งานสามารถทำความเข้าใจและใช้งานระบบได้ ในส่วนของการส่งข้อมูลนั้นพบปัญหาในการส่งบ้างในกรณีที่เครื่องผู้ใช้งานทำการติดตั้ง Software Component ไม่สมบูรณ์ซึ่งสามารถทำการแก้ไขได้ด้วยการติดตั้ง Software Component ดังกล่าวให้ครบถ้วน ทั้งนี้ในส่วนการกำหนดสิทธิการใช้งาน และ การตรวจสอบสถานะนั้น พบว่ามีการใช้งานได้ราบรื่นไม่มีปัญหา

6.2 ข้อเสนอแนะ

จากการทดลองใช้งานระบบที่พัฒนาขึ้นนั้น พบว่ายังคงมีหลายๆจุดที่ต้องปรับปรุงแก้ไขในส่วนรายละเอียดการทำงานของระบบ ไม่ว่าจะเป็นการเสริมความแข็งแรงของระบบให้ปลอดภัยยิ่งขึ้น หรือ การเพิ่มความสะดวกในการใช้งาน เช่น การทำโปรแกรมติดตั้งอัตโนมัติเพื่อให้ผู้ใช้งานสามารถติดตั้ง Client Software Component ได้สะดวก

ในส่วนของการเสริมความปลอดภัยนั้น เนื่องจากระบบที่พัฒนาขึ้นจะอิงการใช้งานกับ Windows 2000 User Account Profile เพื่อใช้เก็บ Public Key, Private Key และ Certificate ของผู้ใช้งาน ซึ่งเก็บอยู่ในบริเวณที่ปลอดภัยของ Windows 2000 Registry (เรียกว่า Secured Protected Storage) ทั้งนี้การเก็บไว้ในที่ดังกล่าวนั้นมีความเสี่ยง เนื่องจากถ้าในกรณีที่ Hard disk ของเครื่องเกิดทำงานผิดพลาด (Hard Disk Failure) จะทำให้ข้อมูลเหล่านี้สูญหายหมด

วิธีการแก้ไขนั้นอาจมีการนำเอา Smart Card และ Smart Card Reader ซึ่งเป็นสื่อที่กำลังได้รับความนิยมในการนำมาช่วยใช้เก็บรักษาข้อมูลที่มีความสำคัญเช่น Public Key, Private Key และ Certificate ของผู้ใช้งาน และสามารถพกติดตัวได้ โดยมีความปลอดภัยในการใช้งานและเก็บรักษากว่าการเก็บ Key และ Certificate ไว้ใน Hard Disk ซึ่งเสี่ยงต่อการโจรกรรมและการสูญหายได้

บรรณานุกรม

ธนาคารแห่งประเทศไทย. 2543. **แบบรายงานทางการเงิน.** [Online]. Available: http://www.bot.or.th/bothomepage/General/Laws_Notif_Forms/Forms.htm.

Bernstein, T. 1996. **Internet Security for Business.** New York: Wiley Computer Publishing.

Coulouris, G. and Dollimore, J. 1998. **Distributed Systems: Concepts and Design.** 2nd ed. New York: Addison – Westley.

Gemplus SA. 2000. **Network Security: Secure Solutions for Doing Business On – Line.** [Online]. Available: http://genplus.com/app/it/netsecurity.htm.

Howard, M. and Levy, M. 2000. **Designing Secure Web-Based Applications for Microsoft Windows 2000.** Washington: Microsoft Press.

Kaufman, C. and Perlman, R. 1995. **Network Security: PRIVATE Communication in a PUBLIC World.** New Jersey: Prentice Hall.

Kauffman, J. and Spencer, K. 1999. **Beginning ASP Databases.** Illinois: Wrox Press.

Lee, T. and Davies, J. 2000. **Windows 2000 TCP/IP Protocols and Services Technical Reference.** Washington: Microsoft Press.

Microsoft. 2000. **MSDN Library: Platform SDK: Security.** [CD-ROM]. Washington: Microsoft.

Microsoft. 2000. **Windows 2000 Server Resource Kit.** [CD-ROM]. Washington: Microsoft.

Netscape. 1998. **Introduction to Public-Key Cryptography.** [Online]. Available: http://developer.netscape.com/docs/manuals/security/pkin/contents.htm.

Netscape. 1998. **Introduction to SSL.** [Online]. Available: http://developer.netscape.com/docs/manuals/security/sslin/index.htm.

RSA Laboratory. 2000. **RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1.** [Online]. Available: http://www.rsasecurity.com/rsalabs/faq/index.html.

ภาคผนวก ก
ขั้นตอนการติดตั้งระบบ

ในการเตรียมอุปกรณ์ให้พร้อมใช้งานกับระบบการส่งข้อมูลทางการเงินผ่านเครือข่ายที่มีความปลอดภัยนั้น สามารถแบ่งขั้นตอนการเตรียมระบบงานได้ดังนี้

ส่วนการติดตั้ง Server

ขั้นตอนการทำงาน	รายละเอียด
1. ติดตั้ง Windows 2000 Advance Server	ทำการติดตั้ง Windows 2000 Advance Server โดย Set Regional Settings Default เป็น "Thai" และอาจแบ่ง Partition ออกเป็นย่อยๆ เช่น C, D และ E เพื่อความสะดวกในการจัดการ
2. ติดตั้ง Windows 2000 High Encryption Pack	ทำการติดตั้ง Windows 2000 High Encryption Pack เพื่อเพิ่มความสามารถในการเข้ารหัสของ SSL Session เป็นที่ระดับ 128 – bit (Default ของ Windows 2000 คือ 56 – bit)
3. ติดตั้ง Certificate Service	จาก Add/Remove Programs เลือก Add/Remove Windows Components แล้วเลือก "Certificate Services"
4. ติดตั้ง SQL Server 7.0	ทำการติดตั้ง SQL Server 7.0 Enterprise Edition
5. ติดตั้ง Content Publishing System Host ISAPI	Copy ไฟล์ "CPSHOST.DLL" และ "UploadExt.dll" ไปที่ Directory "E:\Inetpub\Scripts"
6. ติดตั้ง XCeedZip Compression Library	ทำการติดตั้ง XCeedZip Compression Library จากแผ่น Setup Floppy Disk

ส่วนการทำ Server Configuration

ขั้นตอนการทำงาน	รายละเอียด
1. สร้าง Folder ที่ใช้งาน	• Bank Folder = E:\Bank (คือ Folder ที่ใช้เก็บไฟล์ข้อมูลที่ได้รับจากสถาบันต่างๆ) • Upload Folder = E:\Upload (คือ Folder ที่ใช้เก็บไฟล์ข้อมูลตอนทำการ Upload)

2. ติดตั้งค่า IIS 5.0: สร้าง Virtual Directory	ใน IIS 5.0 MMC สร้าง Virtual Directory ใน Default Web ชื่อ: "Bank" ชี้ไปที่: "E:\Bank"
3. ติดตั้งค่า IIS 5.0: สร้าง SFDS Web Application Directory	จาก Interdev ทำการเชื่อมต่อมาที่ Server และสร้าง Project ชื่อ SFDS จากนั้นทำการ สร้างไฟล์ต่างๆของระบบ SFDS ลงใน Directory ดังกล่าว
4. ติดตั้งค่า IIS 5.0: สร้าง Certificate Request และติดตั้ง Certificate สำหรับ IIS	ใน IIS 5.0 MMC เลือก Properties ของ Default Web ขึ้นมา และเลือก Directory Security และ Server Certificate เพื่อสร้าง Certificate Request เพื่อนำไปใช้กับ CA ที่จะออก Certificate ให้กับ Server เพื่อนำไปติดตั้ง
5. ติดตั้งค่า IIS 5.0: ระบุ Directory ที่ต้องใช้ SSL ในการเชื่อมต่อ	ใน IIS 5.0 MMC ภายใต้ Directory \SFDS จะกำหนดให้ Directory • \AccessControl • \Submission • \Status เป็น Directory ที่ต้องเข้า SSL Connection ที่ 128 – bit และ Set ให้ "Require Client Certificate" ในการเรียกใช้งาน
6. สร้างฐานข้อมูล SQL Server 7.0	Create Database ชื่อ ISDB และ Create Table ต่างๆดังนี้ • BOTRight • CertifierRight • UserRight • Certificate • CertUser • FileStatus • Form • Institute โดยมีโครงสร้างตามที่ระบุในบทที่ 4
8. สร้าง โฟลเดอร์ของสถาบันการเงินและระบบต่างๆ	สร้าง Folder ภายใต้ Bank Folder ตามโครงสร้าง \<ตัวย่อของสถาบันการเงิน>\<รหัสโปรเจค>\<รหัสฟอร์ม> เช่น "\BOT\ธต\EXIM\ธต11"

ส่วนการติดตั้งและ Configuration ที่ Client

ขั้นตอนการทำงาน	รายละเอียด
1. ติดตั้ง Windows 2000 Professional	ทำการติดตั้ง Windows 2000 Professional โดยใช้ Regional Setting เป็น "Thai"
2. ติดตั้ง Windows 2000 High Encryption Pack	ทำการติดตั้ง Windows 2000 High Encryption Pack เพื่อเพิ่มความสามารถในการเข้ารหัสของ SSL ที่ 128 – bit (Default ของ Windows 2000 คือ 56 – bit)
3. ติดตั้ง Internet Explorer 5.01 SP1	ติดตั้ง Internet Explorer 5.01 SP1 โดยใช้เป็น Web Browser ในการเรียกใช้ Web Application ซึ่งมีความสามารถในการเข้ารหัสของ SSL ที่ 128 – bit
4. ติดตั้ง Client Components	ทำการติดตั้ง Client Software Components ต่างๆดังนี้ • CryptLib.dll • XceedZip.dll • FileSelect.ocx • PostFile.ocx • UserName.ocx • ICEnroll.dll ด้วยการพิมพ์คำสั่งจาก Command Prompt ว่า Regsvr32 <ชื่อ component>
5. ติดตั้ง Dial – Up Icon	ทำการติดตั้ง Dial – Up Icon เพื่อทำการ Dial เข้ามาเชื่อมต่อและใช้งาน

(หมายเหตุ: วิธีการใช้งานระบบนั้นจะถูกอธิบายในส่วนของบทที่ 5)

ประวัติผู้เขียน

ชื่อผู้เขียน	นาย วิษณุ ชวนเกษม
สถานที่เกิด	ประจวบคีรีขันธ์
สถานที่สำเร็จการศึกษา	
ระดับมัธยม	โรงเรียนเตรียมอุดมศึกษา (พญาไท)
ระดับปริญญาตรี	Bachelor of Science, Computer Science Virginia Polytechnic Institute and State University Virginia, USA
ปีที่สำเร็จการศึกษา	1998 (2541)