ระบบการออกใบรับรองดิจิทัล

Digital Certificate System

โดย

พฤกษ์ อุบลเกิด

รหัส 46066227

อาจารย์ที่ปรึกษา

ผศ.ดร. จันทร์บูรณ์ สถิตวิริยวงศ์

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 1 ปีการศึกษา 2548

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	ระบบการออกใบรับรองดิจิทัล
นักศึกษา	พฤกษ์ อุบลเกิด
อาจารย์ที่ปรึกษา	ผศ.ดร. จันทร์บูรณ์ สถิตวิริยวงศ์
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2548

บทคัดย่อ

บริการ Certificate Service เป็นบริการหนึ่งที่ช่วยออกใบรับรองดิจิทัลให้กับแอปพลิเคชันที่ต้องการนำไปใช้ประโยชน์ อย่างเช่น การขอตรวจสอบหรือพิสูจน์ตัวตนระหว่างกัน เราสามารถเปรียบเทียบได้ว่า ใบรับรองดิจิทัล (digital certificate) คือบัตรประชาชน หรือหนังสือเดินทาง (passport) ที่ประกอบด้วยข้อมูลสำคัญ เพียงพอที่จะใช้บ่งชี้ได้ว่าผู้ที่ถือบัตรนั้นเป็นใครมีตัวตนจริงหรือไม่ สำหรับใบรับรองดิจิตอล นอกจากจะเก็บรายละเอียดสำคัญของผู้ถือแล้ว ยังเก็บค่าคีย์สำคัญที่ช่วยในการสร้างเซลซันของ SSL ระหว่างไคลเอนต์กับเซิร์ปเวอร์ด้วย

Title	Digital Certificate System
Student	Mr. Prueg Ubonkerd
Advisor	Asst. Prof. Dr. Chanboon Sathitviriyawong
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2005

ABSTRACT

Certificate Service is one of services that issue a digital certificate for application such as authentication. It can assume that digital certificate is as same as identification personal or passport that consists of important data. It can indicate the person who has a digital certificate. Moreover, it can collect the important information and a master key for making session of SSL between clients and servers.

สารบัญ

สารบัญ(ต่อ)

สารบัญรูป

หน้า

รูปที่

สารบัญรูป(ต่อ)

หน้า

รูปที่

สารบัญรูป(ต่อ)

หน้า

รูปที่

สารบัญตาราง

หน้า

ตารางที่

บทที่ 1
บทนำ

1.1 ความเป็นมาของโครงงาน

ปัจจุบัน มีการให้ความสำคัญกับการรักษาความปลอดภัยของข้อมูลมากขึ้น เนื่องจากอินเตอร์เน็ตซึ่งเป็นช่องทางการสื่อสารสาธารณะได้รับความนิยมและใช้งานอย่างแพร่หลาย ซึ่งการทำธุรกรรมบนอินเตอร์เน็ตนั้นถือว่าความปลอดภัยเป็นหัวใจของการพาณิชย์อิเล็กทรอนิกส์ ซึ่งสิ่งที่สร้างความเชื่อมั่นให้เกิดความปลอดภัยดังกล่าวประกอบด้วยความสามารถ 4 ด้านคือ การระบุตัวบุคคล การรักษาความลับ การรักษาความถูกต้อง และการป้องกันการปฏิเสธความรับผิดชอบ โดยตัวอย่างของเทคโนโลยีที่มีครบทั้ง 4 ความสามารถก็คือ เทคโนโลยีการเข้ารหัสด้วยกุญแจสาธารณะ" (Secret Key / Public Key) และ เทคโนโลยีการเข้ารหัสด้วยกุญแจดอกเดียว หรือตัวอย่างเทคโนโลยีที่มีบางความสามารถ เช่น Password หรือ หมายเลขประจำตัวบุคคล เป็นต้น และยังรวมทั้งการใช้งานใบรับรองดิจิทัล (Digital Certificate) ซึ่งได้รับการยอมรับและมีความน่าเชื่อถือ โดยหน่วยงานด้านไอทีขององค์กรต่างต้องการทำหน้าที่เป็นหน่วยผู้ประกอบการรับรอง (Certification Authority - CA) ซึ่งในขณะนี้มีหลายองค์กรที่จะทำการออกใบรับรองดิจิทัล ให้แก่องค์กรและบุคคลทั่วไป ซึ่งจะเป็นการบ่งบอกว่าผู้ถือใบรับรองดิจิทัลเป็นใครและมีการเข้ารหัสป้องกันการโจรกรรมข้อมูลหรือมีความปลอดภัยในการติดต่อสื่อสารมากน้อยเพียงใด โดยการศึกษานี้จะทำการวิเคราะห์โครงสร้างภายในระบบของหน่วยผู้ประกอบการรับรอง (Certification Authority - CA) รวมทั้งทำการออกแบบระบบการออกใบรับรองดิจิทัล เพื่อที่จะนำไปใช้ในองค์กรและยังสามารถลดค่าใช้จ่ายภายในองค์กรให้ลดน้อยลงได้อีกทาง

โครงการพัฒนาระบบการออกใบรับรองดิจิทัลนี้ จึงเป็นระบบที่ออกใบรับรองดิจิทัลให้แก่บุคคลทั่วไป และเว็บไซต์ต่างๆที่เข้ามาลงทะเบียน เพื่อที่จะนำไปใช้ให้เกิดความปลอดภัยในการติดต่อสื่อสาร รวมทั้งให้บริการในการเผยแพร่ใบรับรองในสถานะต่างๆเพื่อให้บุคคลภายนอกเข้ามานำข้อมูลไปใช้งานได้

1.2 วัตถุประสงค์ในการพัฒนาระบบ

1. เพื่อศึกษาเรื่องการออกใบรับรองดิจิทัลโดยเป็นผู้ให้บริการในการออกใบรับรองดิจิทัลประเภทบุคคลซึ่งได้เข้ามาลงทะเบียนและกรอกข้อมูลการร้องขอใบรับรองดิจิทัล รวมทั้งทำการเผยแพร่ใบรับรองดิจิทัลนั้นให้แก่ผู้อื่น
2. เพื่อศึกษาเทคโนโลยีการเข้ารหัสข้อมูลโดยอาศัยหลักการของเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure) ด้วยอัลกอริทึม RSA ซึ่งจะใช้ซอฟต์แวร์ OpenSSL ที่เป็นซอฟต์แวร์แบบ Open Source ทำให้ประหยัดค่าใช้จ่ายในการพัฒนาและติดตั้ง
3. เพื่อพัฒนาระบบให้แสดงถึงความปลอดภัยในการส่งข้อมูลบนระบบเครือข่าย โดยใช้ใบรับรองดิจิทัลเข้ามาเกี่ยวข้องในเรื่องของการเข้ารหัสและถอดรหัส เพื่อรักษาความลับของข้อมูลมิให้ผู้อื่นที่ไม่ได้รับอนุญาตสามารถเปิดอ่านได้
4. เพื่อเป็นการสนับสนุนการใช้งานใบรับรองดิจิทัลให้แพร่หลายให้มากขึ้น

1.3 ขอบเขตของการพัฒนาระบบ

โครงการพัฒนาระบบออกใบรับรองดิจิทัลนี้ ได้กำหนดขอบเขตการศึกษาไว้ ดังนี้

1. ทำการติดตั้ง WAMP5 ซึ่งทำหน้าที่จำลองเว็บเซิร์ฟเวอร์สำเร็จรูปเป็นลักษณะ Intranet Site
2. ทำการติดตั้ง OpenSSL ไว้ที่เซิร์ฟเวอร์เพื่อเป็นซอฟต์แวร์ที่ช่วยในการออกใบรับรองดิจิทัลและทำให้เกิดความปลอดภัยในการรับส่งข้อมูล
3. ทำการสร้าง Web Directory เพื่อเก็บข้อมูลของระบบออกใบรับรองดิจิทัล โดยจะทำหน้าที่เป็น Web Root ส่งข้อมูลและติดต่อไปยังเว็บเซิร์ฟเวอร์
4. ระบบสามารถสร้าง Private Key , Certificate เพื่อใช้ในกระบวนการตรวจสอบความถูกต้องในการรับส่งข้อมูล ด้วยวิธีการเข้ารหัสและถอดรหัส

1.4 ขั้นตอนในการพัฒนาระบบงาน

1. การศึกษาความเป็นไปได้ในการพัฒนาระบบ
2. การศึกษาและวิเคราะห์ทฤษฎีที่เกี่ยวข้องและเลือกใช้ให้เข้ากับระบบ
3. การวิเคราะห์และออกแบบระบบในรูปแบบของ UML
4. การพัฒนาและทดสอบระบบให้สามารถออกใบรับรองดิจิทัลได้
5. การทดลองเพื่อนำใบรับรองดิจิทัลไปใช้ในกระบวนการในการเข้าและถอดรหัสข้อมูล

6. การตรวจสอบความผิดพลาดและแนวทางการแก้ไข
7. การกำหนดแนวทางการพัฒนาระบบต่อไปและอนาคตของการใช้งานใบรับรองดิจิทัล

1.5 วิธีการดำเนินงาน

ในการศึกษาและพัฒนาระบบการออกใบรับรองดิจิทัลนี้ เพื่อให้ศึกษาคลอบคลุมวัตถุประสงค์และขอบเขตในการพัฒนาระบบ จึงได้กำหนดขั้นตอนในการศึกษาไว้ดังนี้

1. ผู้ที่ต้องการขอใบรับรองดิจิทัลทำการลงทะเบียนเพื่อขอเข้าใช้งานระบบการออกใบรับรองดิจิทัลผ่านทางเว็บไซต์
2. ผู้ดูแลระบบทำการตรวจสอบผู้ที่ขอเข้าใช้ระบบ และส่งรหัสผ่านเพื่อสามารถเข้าใช้ระบบผ่านทางอีเมล์
3. ผู้ที่ต้องการขอใบรับรองดิจิทัลเข้าใช้งานในระบบและทำการกรอกรายละเอียดในการร้องขอใบรับรองดิจิทัล รวมทั้งสามารถดาวน์โหลด Private Key ไปเก็บไว้ในเครื่องตัวเองโดยที่จะต้องเก็บไว้เป็นความลับ
4. ผู้ดูแลระบบทำการตรวจสอบการร้องขอใบรับรองดิจิทัล และทำการออกใบรับรองดิจิทัลให้กับผู้ที่มาร้องขอ
5. ผู้ที่ต้องการขอใบรับรองดิจิทัลได้รับใบรับรองดิจิทัล รวมทั้งสามารถดาวน์โหลดใบรับรองดิจิทัลหรือ Public Key ไปเก็บไว้ในเครื่องตัวเอง เพื่อเผยแพร่และใช้ในกระบวนการเข้ารหัสและถอดรหัส

1.6 ประโยชน์ที่คาดว่าจะได้รับ

จากการศึกษาและพัฒนาระบบการออกใบรับรองดิจิทัล คาดว่าจะได้ประโยชน์และเป็นแนวทางในการสร้างความปลอดภัยของการสื่อสาร ดังนี้

1. ช่วยทำให้เข้าใจการทำงานของเทคโนโลยีการเข้ารหัส เพื่อสร้างความปลอดภัยในการติดต่อสื่อสารและส่งข้อมูลผ่านทางอีเมล์
2. สามารถออกใบรับรองดิจิทัลสำหรับบุคคลทั่วไปที่เข้ามาลงทะเบียน โดยไม่คิดค่าใช้จ่ายอะไร จึงเป็นการลดค่าใช้จ่ายหากองค์กรใดจะนำไปใช้งานและพัฒนาต่อไป
3. เป็นที่รวบรวมใบรับรองดิจิทัลของสมาชิกที่เข้ามาลงทะเบียน รวมทั้งให้บริการในการเผยแพร่ใบรับรองดิจิทัลให้แก่บุคคลภายนอกที่ต้องการนำไปใช้งาน

บทที่ 2
ทฤษฎีที่เกี่ยวข้องกับระบบการออกใบรับรองดิจิทัล

ปัจจุบันการติดต่อสื่อสารมักทำผ่านระบบเครือข่ายอินเทอร์เน็ต โดยที่บุคคลหรือองค์กรที่ติดต่อด้วยนั้น อาจจะไม่เคยมีความสัมพันธ์หรือรู้จักกันมาก่อน ก่อให้เกิดความไม่มั่นใจว่า บุคคลหรือองค์กรที่ติดต่อด้วยคือใคร มีตัวตนจริงหรือไม่ ฉะนั้น จึงจำเป็นที่จะต้องมีกลไกในการยืนยันตัวบุคคลสำหรับโลกอิเล็กทรอนิกส์ สิ่งที่ใช้ในการยืนยันก็คือ ใบรับรองอิเล็กทรอนิกส์ (Certificate)

ใบรับรองอิเล็กทรอนิกส์ เป็นข้อมูลในรูปแบบอิเล็กทรอนิกส์ที่ออกให้โดยผู้ให้บริการออกใบรับรอง (Certification Authority - CA) ซึ่งข้อมูลในใบรับรองอิเล็กทรอนิกส์นั้น บ่งบอกถึงความมีตัวตนในโลกแห่งอิเล็กทรอนิกส์ โดยที่ใบรับรองอิเล็กทรอนิกส์ดังกล่าวสามารถนำมาประยุกต์ใช้งานได้ 2 รูปแบบ คือ การเข้ารหัส/ถอดรหัสลับ (Encryption/Decryption) และการลงลายมือชื่อดิจิทัล (Digital Signature) กับข้อมูลที่กระทำการรับส่งระหว่างกัน

ระบบการออกใบรับรองดิจิทัลนี้ จะใช้เทคโนโลยีของการเข้ารหัสเป็นเทคโนโลยีหลัก ที่มีชื่อเรียกว่า เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure) ซึ่งมีระบบกุญแจคู่เป็นพื้นฐานสำคัญ อันประกอบด้วยกุญแจส่วนตัว (Private Key) และ กุญแจสาธารณะ (Public Key)

2.1 องค์ประกอบของการรักษาความปลอดภัย (สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ. 2547.)

การรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์เป็นเทคนิคและวิธีการต่าง ๆ ที่ใช้ป้องกันการลักลอบดูข้อมูล การเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลนั้น ๆ โดยเทคโนโลยีต่าง ๆ ที่จะนำมาใช้ในการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์นั้นควรจะสามารถรองรับองค์ประกอบดังต่อไปนี้ได้

- Confidentiality คือ การปกปิดข้อมูลทั้งหมดเป็นความลับ สามารถเปิดอ่านได้เฉพาะผู้ที่ถูกระบุว่าเป็นผู้รับเท่านั้น
- Data Integrity คือ ความแน่ใจว่าข้อมูลที่ได้รับมีข้อความถูกต้องครบถ้วน และไม่ถูกเปลี่ยนแปลงโดยบุคคลอื่นในระหว่างการส่งข้อมูล

- Authentication คือ ความแน่ใจว่าบุคคลที่ติดต่อด้วยในการสื่อสารเป็นผู้ซึ่งอ้างถึงจริงNon-repudiation คือ ความแน่ใจว่าคู่สื่อสารไม่สามารถที่จะปฏิเสธการกระทำทางอิเล็กทรอนิกส์ที่เกิดขึ้นได้

2.2 การเข้ารหัสข้อมูล (Cryptography) (บรรจง หะรังษี. 2547.)

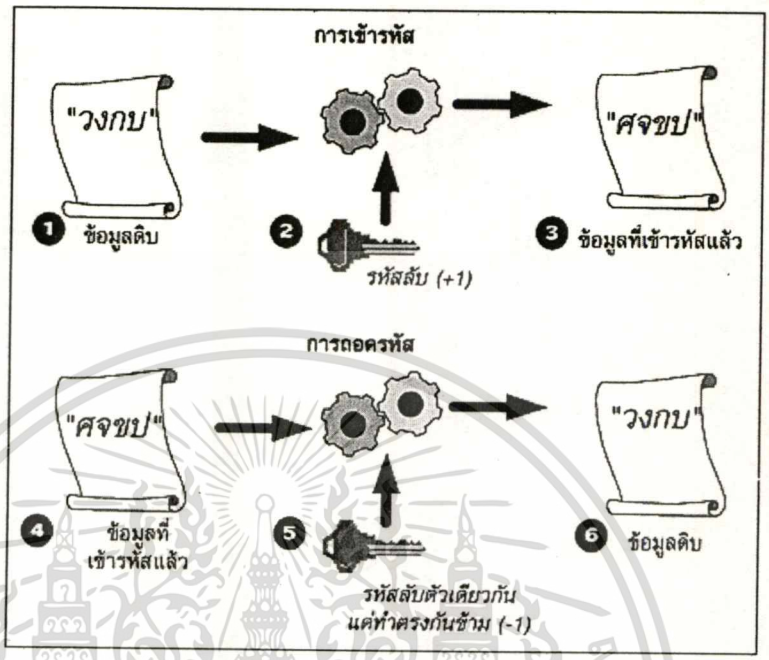
การเข้ารหัสข้อมูลโดยพื้นฐานแล้วจะเกี่ยวข้องกับวิธีการทางคณิตศาสตร์เพื่อใช้ในการป้องกันข้อมูลหรือข้อความตั้งต้นที่ต้องการส่งไปถึงผู้รับ ข้อมูลตั้งต้นจะถูกแปรเปลี่ยนไปสู่ข้อมูลหรือข้อความอีกรูปแบบหนึ่งที่ไม่สามารถอ่านเข้าใจได้โดยใครก็ตามที่ไม่มีกุญแจสำหรับเปิดดูข้อมูลนั้น เราเรียกกระบวนการในการแปรรูปของข้อมูลตั้งต้นว่า "การเข้ารหัสข้อมูล" (Encryption) และกระบวนการในการแปลงข้อความที่ไม่สามารถอ่าน และทำความเข้าใจให้กลับไปสู่ข้อความดั้งเดิม ว่าการถอดรหัสข้อมูล (Decryption)

2.2.1 อัลกอริทึมในการเข้ารหัสข้อมูล

อัลกอริทึมในการเข้ารหัสข้อมูลมี 2 ประเภทหลัก คือ

- อัลกอริทึมแบบสมมาตร (Symmetric key algorithms)

อัลกอริทึมแบบนี้จะใช้กุญแจที่เรียกว่า กุญแจลับ (Secret key) ซึ่งมีเพียงหนึ่งเดียวเพื่อใช้ในการเข้าและถอดรหัสข้อความที่ส่งไปดังรูปที่ 2.1 อัลกอริทึมยังสามารถแบ่งย่อยออกเป็น 2 ประเภท ได้แก่ แบบบล็อค (Block Algorithms) ซึ่งจะทำการเข้ารหัสทีละบล็อค (1 บล็อคประกอบด้วยหลายไบต์ เช่น 64 ไบต์ เป็นต้น) และแบบสตรีม (Stream Algorithms) ซึ่งจะทำการเข้ารหัสทีละไบต์อัลกอริทึมแบบนี้จะใช้กุญแจที่เรียกว่า กุญแจลับ (Secret key) ซึ่งมีเพียงหนึ่งเดียวเพื่อใช้ในการเข้าและถอดรหัสข้อความที่ส่งไป อัลกอริทึมยังสามารถแบ่งย่อยออกเป็น 2 ประเภท ได้แก่ แบบบล็อค (Block Algorithms) ซึ่งจะทำการเข้ารหัสทีละบล็อค (1 บล็อคประกอบด้วยหลายไบต์ เช่น 64 ไบต์ เป็นต้น) และแบบสตรีม (Stream Algorithms) ซึ่งจะทำการเข้ารหัสทีละไบต์



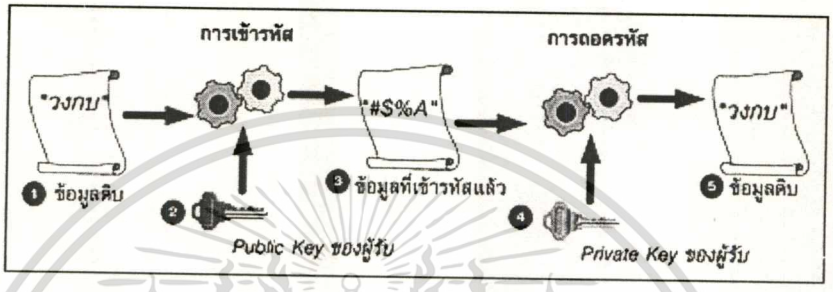
รูปที่ 2.1 การเข้ารหัสและการถอดรหัส

- อัลกอริทึมแบบอสมมาตร (Asymmetric key algorithms)

อัลกอริทึมนี้จะใช้กุญแจสองตัวเพื่อทำงาน ตัวหนึ่งใช้ในการเข้ารหัสและอีกตัวหนึ่งใช้ในการถอดรหัสข้อมูลที่เข้ารหัสมาโดยกุญแจตัวแรก อัลกอริทึมกลุ่มสำคัญในแบบอสมมาตรนี้คือ อัลกอริทึมแบบกุญแจสาธารณะ (Public keys Algorithms) ซึ่งใช้กุญแจที่เรียกกันว่า กุญแจสาธารณะ (Public keys) ในการเข้ารหัสและใช้กุญแจที่เรียกกันว่า กุญแจส่วนตัว (Private keys) ในการถอดรหัสข้อมูลนั้น กุญแจสาธารณะนี้สามารถส่งมอบให้กับผู้อื่นได้ เช่น เพื่อนร่วมงานที่เราต้องการติดต่อด้วย หรือแม้กระทั่งวางไว้บนเว็บไซต์เพื่อให้ผู้อื่นสามารถดาวน์โหลดไปใช้งานได้ สำหรับกุญแจส่วนตัวนั้นต้องเก็บไว้กับผู้เป็นเจ้าของกุญแจส่วนตัวเท่านั้นและห้ามเปิดเผยให้ผู้อื่นทราบโดยเด็ดขาดดังรูปที่ 2.2

อัลกอริทึมแบบกุญแจสาธารณะยังสามารถประยุกต์ใช้ได้กับการลงลายมือชื่ออิเล็กทรอนิกส์ (ซึ่งเปรียบเสมือนการลงลายมือชื่อของเราที่ใช้กับเอกสารสำนักงานทั่วไป) การลงลายมือชื่อนี้จะเป็นการพิสูจน์ความเป็นเจ้าของและสามารถใช้ได้กับการทำธุรกรรมต่างๆ บนอินเทอร์เน็ต เช่น การซื้อสินค้า เป็นต้น วิธีการใช้งานคือ ผู้เป็นเจ้าของกุญแจส่วนตัวลง

ลายมือชื่อของตนกับข้อความที่ต้องการส่งไปด้วยกุญแจส่วนตัว แล้วจึงส่งข้อความนั้นไปให้กับผู้รับ เมื่อได้รับข้อความที่ลงลายมือชื่อมา ผู้รับสามารถใช้กุญแจสาธารณะ (ที่เป็นคู่ของกุญแจส่วนตัวนั้น) เพื่อตรวจสอบว่าเป็นข้อความที่มาจากผู้ส่งนั้นหรือไม่



รูปที่ 2.2 การเข้ารหัสแบบอสมมาตร

2.2.2 ความแข็งแกร่งของอัลกอริทึมสำหรับการเข้ารหัส (บรรจง หะรังษี. 2547.)

ความแข็งแกร่งของอัลกอริทึมหมายถึงความยากในการที่ผู้บุกรุกจะสามารถถอดรหัสข้อมูลได้โดยปราศจากกุญแจที่ใช้ในการเข้ารหัส ซึ่งจะขึ้นอยู่กับปัจจัยดังนี้

- การเก็บกุญแจเข้ารหัสไว้อย่างเป็นความลับ ผู้เป็นเจ้าของกุญแจลับหรือส่วนตัวต้องมีความระมัดระวังไม่ให้กุญแจสูญหายหรือล่วงรู้โดยผู้อื่น
- ความยาวของกุญแจเข้ารหัส ปกติกุญแจเข้ารหัสจะมีความยาวเป็นบิต ยิ่งจำนวนบิตของกุญแจยิ่งมาก ยิ่งทำให้การเดาเพื่อสุ่มหากุญแจที่ถูกต้องเป็นไปได้ยากยิ่งขึ้น (เช่น กุญแจขนาด 1 บิต จะสามารถแทนตัวเลขได้ 2 ค่าคือ 0 กับ 1 กุญแจขนาด 2 บิต จะเป็นไปได้ 4 ค่าคือ 0, 1, 2, 3 เป็นต้น)
- ความไม่เกรงกลัวต่อการศึกษาหรือดูอัลกอริทึมเพื่อหารูปแบบของการเข้ารหัส อัลกอริทึมที่ดีต้องเปิดให้ผู้รู้ทำการศึกษาในรายละเอียดได้โดยไม่เกรงว่าผู้ศึกษาจะสามารถจับรูปแบบของการเข้ารหัสได้ล
- การมีประตูลับในอัลกอริทึม อัลกอริทึมที่ดีต้องไม่แฝงไว้ด้วยประตูลับที่สามารถใช้เป็นทางเข้าไปสู่อัลกอริทึม แล้วอาจใช้เพื่อทำการถอดรหัสข้อมูลได้ ประตูลับนี้ทำให้ไม่จำเป็นต้องใช้กุญแจในการถอดรหัส

- ความไม่เกรงกลัวต่อปัญหาการหาความสัมพันธ์ในข้อมูลที่ได้รับ กล่าวคือเมื่อผู้บุกรุกทราบข้อมูลบางอย่างที่เป็นข้อมูลตั้งต้นซึ่งยังไม่ได้เข้ารหัส รวมทั้งมีข้อมูลที่เข้ารหัสแล้ว (ของข้อมูลตั้งต้นนั้น) ผู้บุกรุกอาจจะสามารถหาความสัมพันธ์ระหว่างข้อความทั้งสองนั้นได้ ซึ่งจะเป็นวิธีการในการถอดรหัสข้อมูลได้ ปัญหานี้เรียกกันว่า Known plaintext attack (คำว่า plaintext หมายถึงข้อความตั้งต้นที่ยังไม่ได้ผ่านการเข้ารหัส)
- คุณสมบัติของข้อความตั้งต้น คุณสมบัตินี้อาจใช้เป็นช่องทางในการถอดรหัสข้อมูลได้ อัลกอริทึมที่ดีต้องไม่ใช้คุณสมบัติของข้อความเป็นกลไกในการเข้ารหัสข้อมูล

2.2.3 ความยาวของกุญแจที่ใช้ในการเข้ารหัส (บรรจง หะรังษี. 2547.)

ความยาวของกุญแจเข้ารหัสมีหน่วยนับเป็นบิต หนึ่งบิตในคอมพิวเตอร์เป็นตัวเลขฐานสองที่ประกอบด้วยค่า 0 และ 1 กุญแจที่มีความยาว 1 บิต ตัวเลขที่เป็นไปได้เพื่อแทนกุญแจนั้น จึงอาจมีค่าเป็น 0 หรือ 1 กุญแจที่มีความยาว 2 บิต ตัวเลขที่เป็นไปได้จึงเป็น 0, 1, 2 และ 3 ตามลำดับ กุญแจที่มีความยาว 3 บิต ตัวเลขที่เป็นไปได้จะอยู่ระหว่าง 0 ถึง 7 ดังนั้นเมื่อเพิ่มความยาวของกุญแจทุกๆ 1 บิต ค่าที่เป็นไปได้ของกุญแจจะเพิ่มขึ้นเป็นสองเท่าตัว หรือจำนวนกุญแจที่เป็นไปได้จะเพิ่มขึ้นเป็น 2 เท่าตัวนั่นเอง

ฉะนั้นจะเห็นได้ว่ากุญแจยิ่งมีความยาวมาก โอกาสที่ผู้บุกรุกจะสามารถคาดเดากุญแจที่ตรงกับหมายเลขที่ถูกต้องของกุญแจจะยิ่งยากมากขึ้นตามลำดับ ในการที่ผู้บุกรุกลองผิดลองถูกกับกุญแจโดยใช้กุญแจที่มีหมายเลขต่างๆ กัน เพื่อหวังที่จะพบกุญแจที่ถูกต้องและสามารถใช้ถอดรหัสข้อมูลได้ การลองผิดลองถูกนี้เราเรียกกันว่า Key search หรือการค้นหากุญแจนั่นเอง ทฤษฎีได้กล่าวไว้ว่าการลองผิดลองถูกนี้โดยเฉลี่ยจะต้องทดลองกับกุญแจเป็นจำนวนครึ่งหนึ่งของกุญแจทั้งหมดก่อนที่จะพบกุญแจที่ถูกต้อง

ความยาวของกุญแจที่มีขนาดเหมาะสมจึงขึ้นอยู่กับความเร็วในการค้นหากุญแจของผู้บุกรุกและระยะเวลาที่ต้องการให้ข้อมูลมีความปลอดภัย ตัวอย่างเช่น ถ้าผู้บุกรุกสามารถลองผิดลองถูกกับกุญแจเป็นจำนวน 10 กุญแจภายในหนึ่งวินาทีแล้ว กุญแจที่มีความยาว 40 บิต จะสามารถป้องกันข้อมูลไว้ได้ 3,484 ปี ถ้าผู้บุกรุกสามารถลองได้เป็นจำนวน 1 ล้านกุญแจในหนึ่งวินาที (เทคโนโลยีปัจจุบันสามารถทำได้) กุญแจที่มีความยาว 40 บิตจะสามารถป้องกันข้อมูลไว้ได้เพียง 13 วันเท่านั้น (ซึ่งอาจไม่เพียงพอสำหรับในบางลักษณะงาน) ด้วยเทคโนโลยีในปัจจุบันหากผู้บุกรุกสามารถทดลองได้เป็น

จำนวน 1,000 ล้านกุญแจในหนึ่งวินาที กุญแจขนาด 128 บิตจะสามารถป้องกันข้อมูลไว้ได้ 1022 ปี ดังนั้นด้วยลักษณะงานทั่วไปกุญแจขนาด 128 บิตจะพอเพียงต่อการรักษาความลับของข้อมูลเอาไว้ได้

2.2.4 ตัวอย่างอัลกอริทึมที่ใช้สำหรับการเข้ารหัส (บรรจง หะรังษี. 2547.)

1. **อัลกอริทึมสำหรับการเข้ารหัสแบบสมมาตร** เช่น DES , AES เป็นต้น

- DES ย่อมาจาก Data Encryption Standard อัลกอริทึมนี้ได้รับการรับรองโดยรัฐบาลสหรัฐอเมริกาในปี ค.ศ. 1977 ให้เป็นมาตรฐานการเข้ารหัสข้อมูลสำหรับหน่วยงานของรัฐทั้งหมด ในปี 1981 อัลกอริทึมยังได้รับการกำหนดให้เป็นมาตรฐานการเข้ารหัสข้อมูลในระดับนานาชาติตามมาตรฐาน ANSI (American National Standards) อีกด้วย และ DES เป็นอัลกอริทึมแบบบล็อกที่ใช้กุญแจที่มีขนาดความยาว 56 บิตและเป็นอัลกอริทึมที่มีความแข็งแกร่ง แต่เนื่องด้วยขนาดความยาวของกุญแจที่มีขนาดเพียง 56 บิต ซึ่งในปัจจุบันถือได้ว่าสั้นเกินไป ผู้บุกรุกอาจใช้วิธีการลองผิดลองถูกเพื่อค้นหากุญแจที่ถูกต้องสำหรับการถอดรหัส
- AES เป็นอัลกอริทึมนี้ได้รับการพัฒนาโดย Joan Daemen และ Vincent Rijmen ในปี 2000 อัลกอริทึมได้รับการคัดเลือกโดยหน่วยงาน National Institute of. Standard and Technology (NIST) ของสหรัฐอเมริกาให้เป็นมาตรฐานในการเข้ารหัสชั้นสูงของประเทศ อัลกอริทึมมีความเร็วสูงและมีขนาดกะทัดรัดโดยสามารถใช้กุญแจที่มีความยาวขนาด 128, 192 และ 256 บิต

2. **อัลกอริทึมสำหรับการเข้ารหัสแบบกุญแจสาธารณะ (หรือการเข้ารหัสแบบอสมมาตร)** แบ่งตามลักษณะการใช้งานได้เป็น 2 ประเภท ได้แก่ ใช้สำหรับการเข้ารหัส และใช้สำหรับการลงลายมือชื่ออิเล็กทรอนิกส์ โดยมีตัวอย่างเช่น RSA, DSS, MD5, SHA

- อัลกอริทึม RSA ได้รับการพัฒนาขึ้นที่มหาวิทยาลัย MIT ในปี 1977 โดยศาสตราจารย์ 3 คน ซึ่งประกอบด้วย Ronald Rivest, Adi Shamir และ Leonard Adleman ชื่อของอัลกอริทึมได้รับการตั้งชื่อตามตัวอักษรตัวแรกของนามสกุลของศาสตราจารย์ทั้งสามคน อัลกอริทึมนี้สามารถใช้ในการเข้ารหัสข้อมูลรวมทั้งการลงลายมือชื่ออิเล็กทรอนิกส์ด้วย

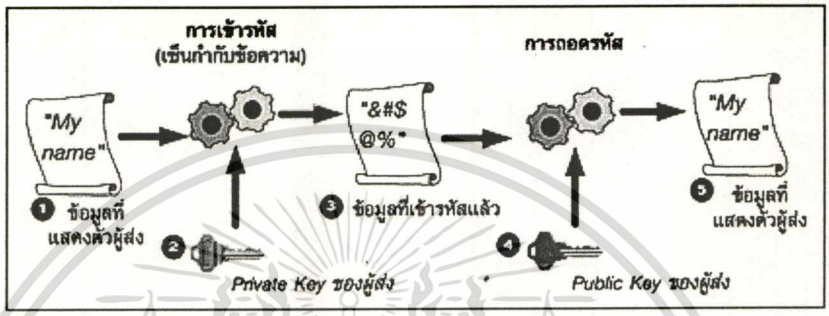
- อัลกอริทึม DSS ย่อมาจาก Digital Signature Standard เป็นอัลกอริทึมนี้ได้รับการพัฒนาขึ้นมาโดย National Security Agency ในประเทศสหรัฐอเมริกาและได้รับการรับรองโดย NIST ให้เป็นมาตรฐานกลางสำหรับการลงลายมือชื่ออิเล็กทรอนิกส์ในประเทศสหรัฐอเมริกา
- Message Digest หรือเรียกสั้นๆ ว่า Digest แปลว่าข้อความสรุปจากเนื้อหาข้อความตั้งต้น โดยปกติข้อความสรุปจะมีความยาวน้อยกว่าความยาวของข้อความตั้งต้นมาก จุดประสงค์สำคัญของอัลกอริทึมนี้คือ การสร้างข้อความสรุปที่สามารถใช้เป็นตัวแทนของข้อความตั้งต้นได้ โดยทั่วไปข้อความสรุปจะมีความยาวอยู่ระหว่าง 128 ถึง 256 บิต และจะไม่ขึ้นกับขนาดความยาวของข้อความตั้งต้น
- อัลกอริทึม MD5 พัฒนาโดย Rivest เช่นกันโดยพัฒนาต่อจาก MD4 เพื่อให้มีความปลอดภัยที่สูงขึ้น ถึงแม้จะเป็นที่นิยมใช้งานกันอย่างแพร่หลาย ทว่าในปี 1996 ก็มีผู้พบจุดบกพร่องของ MD5 (เช่นเดียวกับ MD4) จึงทำให้ความนิยมเริ่มลดลง โดย MD5 ผลิตไดเจสต์ที่มีขนาด 128 บิต
- อัลกอริทึม SHA ย่อจาก Secure Hash Algorithm อัลกอริทึม SHA ได้รับแนวคิดในการพัฒนามาจาก MD4 และได้รับการพัฒนาขึ้นมาเพื่อใช้งานร่วมกับอัลกอริทึม DSS (ซึ่งใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์) หลังจากที่ได้มีการตีพิมพ์เผยแพร่อัลกอริทึมนี้ได้ไม่นาน NIST ก็ประกาศตามมาว่าอัลกอริทึมจำเป็นต้องได้รับการแก้ไขเพิ่มเติมเล็กน้อยเพื่อให้สามารถใช้งานได้อย่างเหมาะสม โดย SHA สร้างไดเจสต์ที่มีขนาด 160 บิต

2.3 ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) (สถาบันวิจัยเพื่อการพัฒนา. 2548.)

คือ ข้อมูลอิเล็กทรอนิกส์ที่ได้มาจากการเข้ารหัสของข้อมูลด้วยกุญแจส่วนตัวของผู้ส่งซึ่งเปรียบเสมือนเป็นลายเซ็นของผู้ส่ง คุณสมบัติของลายเซ็นอิเล็กทรอนิกส์ นอกจากจะสามารถระบุตัวบุคคลและเป็นกลไกการป้องกันการปฏิเสธความรับผิดชอบแล้ว ยังสามารถป้องกันข้อมูลที่ส่งไปไม่ให้ถูกแก้ไข หรือหากถูกแก้ไขไปจากเดิมก็สามารถล่วงรู้ได้ดังรูปที่ 2.3

ลายมือชื่ออิเล็กทรอนิกส์เป็นการประยุกต์ใช้เทคโนโลยีต่าง ๆ ดังกล่าวข้างต้น ในการระบุตัวบุคคล ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างจาก เทคโนโลยีเข้ารหัสด้วยกุญแจสาธารณะ เรียกว่า “ลายมือชื่อดิจิทัล” (Digital Signature) ในการลงลายมือชื่อดิจิทัลกำกับข้อความที่ต้องการ ส่งผ่านทางเครือข่าย ผู้ส่งข้อความจะใช้กุญแจลับของตนในการลงลายมือชื่อโดยผ่านกระบวนการคำนวณทางคณิตศาสตร์ ผู้รับจะสามารถ ตรวจสอบความถูกต้องของลายมือชื่อดังกล่าวได้โดยใช้กุญแจสาธารณะ

ของผู้ส่งที่แสดงอยู่ใน “ใบรับรองดิจิทัล” (Digital Certificate) ซึ่งมักจัดเก็บโดยบุคคลหรือองค์กรซึ่งเป็นผู้ออกใบรับรองนั้น



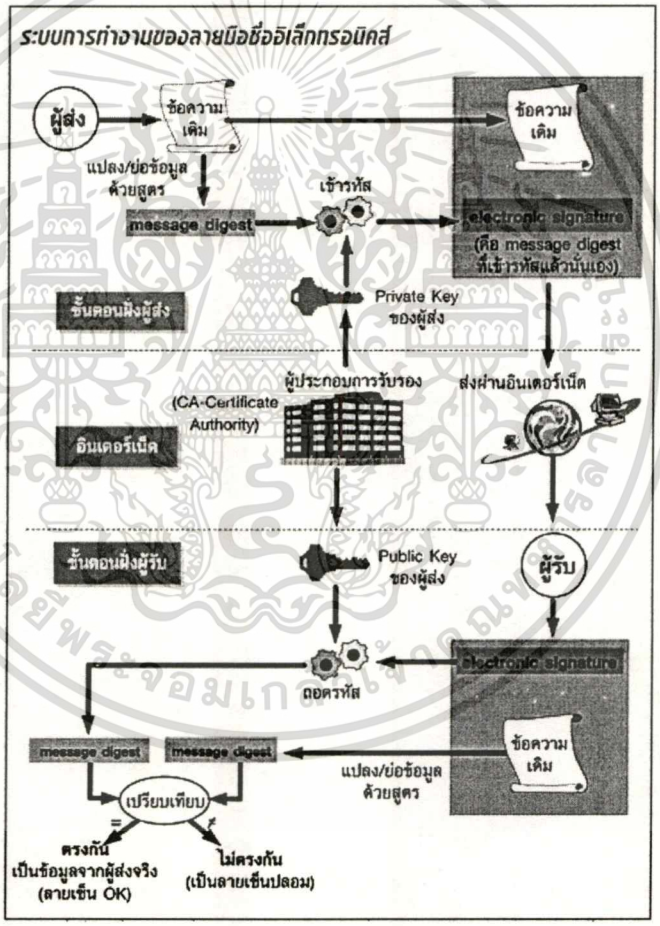
รูปที่ 2.3 ระบบการทำงานของลายมือชื่ออิเล็กทรอนิคส์

การใช้ลายมือชื่อดิจิทัลมีข้อดีคือ สามารถตรวจสอบได้ว่าผู้ส่งข้อมูลเป็นตัวจริง (Authentication) เพื่อเพิ่มความมั่นใจให้กับคู่ค้าว่าทำธุรกิจกับบุคคลที่มีตัวตนอยู่จริง คู่ค้ายินดีที่จะทำการค้ากับเว็บไซต์ที่มีการใช้ลายมือชื่อดิจิทัลมากกว่าเว็บไซต์ที่ไม่มีการใช้ลายมือชื่อดิจิทัล ตรวจสอบได้ว่าข้อมูลที่ได้รับมาไม่ได้มีการดัดแปลงหรือแก้ไข (Integrity) เพื่อให้คู่ค้าสามารถตรวจสอบได้ว่าข้อมูลนั้นเป็นข้อมูลจริงๆไม่ได้มีคนอื่นเปิดอ่านหรือดัดแปลง ทำให้เกิดความสบายใจและความเชื่อถือในการซื้อขาย ปกป้องข้อมูลให้เป็นความลับจากบุคคลที่ไม่ได้รับอนุญาต (Confidentiality) และปกป้องสิทธิจากบุคคลที่จงใจจะทำผิดสัญญา (Non-repudiation) ในกรณีที่ผู้ส่งทำสัญญาโดยมีการใช้ลายมือชื่อดิจิทัลแล้ว และผู้ส่งจะทำผิดสัญญาโดยบอกว่าไม่ได้ส่งข้อมูลและทำสัญญากับผู้รับ ผู้รับสามารถใช้ลายมือชื่อดิจิทัลเป็นหลักฐานในการเอาผิดทางกฎหมายได้

2.3.1 ขั้นตอนการทำงานของลายมือชื่อดิจิทัล (สถาบันวิจัยเพื่อการพัฒนา. 2548.)

- ข้อมูลที่ต้องการจะส่งจะถูกคำนวณให้ได้ข้อความที่สั้นลงโดยใช้ Hash Function ผลที่ได้จะเป็นข้อมุลสั้นๆ และความยาวคงที่ ซึ่งเรียกว่า Message Digest
- ผู้ส่งจะเซ็นชื่อในข้อความโดยการเข้ารหัส Message Digest โดยใช้ Private Key ของตัวเอง ซึ่งข้อมูลที่ได้จะเรียกว่า Digital Signature ของเอกสารนั้น
- ข้อความเดิมจะถูกส่งไปพร้อมกับ Digital Signature ไปให้ผู้รับ

- ผู้รับจะตรวจสอบข้อมูลที่ได้รับโดย
  1. จะ คำนวณ Message Digest โดยใช้ Hash Function เดียวกัน
  2. ใช้ Public key ของผู้ส่งทำการถอดรหัส Digital Signature ที่ส่งมากับข้อความซึ่งจะได้ Message Digest อีกชุดหนึ่ง
  3. ทำการเปรียบเทียบ Message Digest ที่คำนวณได้กับที่ถอดรหัสได้ ถ้าเหมือนกันแสดงว่าข้อความไม่ได้ถูกเปลี่ยนแปลงนับตั้งแต่มีการเซตเอกสารนั้นดังรูปที่ 2.4



รูปที่ 2.4 ระบบการทำงานของลายมือชื่ออิเล็กทรอนิคส์

ลายมือชื่อดิจิทัลเหมือนกับการเซ็นชื่อโดยทั่วไป แต่มีข้อแตกต่างกันคือ ลายมือชื่อดิจิทัลใช้ลายเซ็นที่อยู่ในรูปบิต (Bit) และ ตัวอักษร (Byte) ที่คอมพิวเตอร์สามารถเข้าใจได้ดังรูปที่ 2.5

รูปที่ 2.5 ตัวอย่างลายมือชื่อดิจิทัล

ผู้ใช้งานเพียงติดตั้งโปรแกรมลายมือชื่อดิจิทัล (Digital Signature Software) ไว้ในเครื่องคอมพิวเตอร์ โปรแกรมนี้จะทำงานเองทั้งหมด ตัวอย่างเช่น ต้องการส่ง E-mail ผู้ใช้งานเพียงแค่คลิกปุ่ม Sign เพื่อเป็นการบอกว่าต้องการให้จดหมายฉบับนี้มีการเซ็น

2.3.2 ตัวอย่างการใช้งานลายมือชื่อดิจิทัล (สถาบันวิจัยเพื่อการพัฒนา. 2548.)

อินเตอร์เน็ตเปรียบเสมือนสะพานที่เชื่อมผู้คนเข้าหากันจากทุกที่ในโลก และทำให้ระยะทางในการติดต่อสื่อสารสั้นลง จึงเกิดการใช้อินเตอร์เน็ตเป็นช่องทางในการทำธุรกรรมบนอินเตอร์เน็ต (Electronic Commerce) ขึ้นอย่างมากมาย จึงสามารถพูดได้ว่าการทำการค้าขายบนอินเตอร์เน็ตก็จะถือว่าเป็น International Business โดยปริยาย เมื่อบริษัทแห่งหนึ่งสร้างเว็บเพื่อใช้ในการโฆษณาขายสินค้าและบริการต่างๆ ก็ถือว่าบริษัทนั้นได้แข่งขันกับบริษัทอื่นทั่วโลกเช่นกัน (Global Environment) บุคคลทั่วไปจะทำธุรกิจก็จะต้องเลือกทำกับบริษัทที่รู้จักและน่าเชื่อถือ ไม่มีใครอยากทำธุรกิจกับคนแปลกหน้า ความคิดนี้มีอยู่นานแล้วและจะเป็นแบบนี้ต่อไป ดังนั้นก่อนที่บริษัทจะทำธุรกิจระหว่างประเทศต้องทำให้บริษัทเป็นที่ยอมรับและน่าเชื่อถือในประเทศนั้นเหมือนกัน แต่การจะให้บริษัทเป็นที่รู้จักและน่าเชื่อถือในโลกดิจิทัลการเป็นไปได้ยาก เพราะผู้ซื้อไม่สามารถเห็นหน้าของผู้ขายสินค้าและบริการ ดังนั้นจึงมีการคิดกลไกที่สามารถทำให้การค้าขายบนอินเตอร์เน็ตมีความน่าเชื่อถือ กลไกนั้นคือลายมือชื่อดิจิทัล (Digital Signature) สมมุติว่ามีธนาคารแห่งหนึ่งต้องให้บริการบนอินเตอร์เน็ต Online Banking Service แก่ลูกค้า และคาดว่าบริการทางอินเตอร์เน็ตนี้จะทำให้ลูกค้าของธนาคารมีความสะดวกมากขึ้น ลูกค้าที่อยู่ในต่างประเทศไม่ต้องเดินทางมาที่ธนาคาร ลูกค้าก็สามารถทำที่จะใช้บริการของธนาคารได้ แต่ปัญหาที่เกิดขึ้นคือ จะทำอย่างไรให้ลูกค้ามั่นใจว่า Online Banking Service มีความปลอดภัยและน่าเชื่อถือจริง ดังนั้น Online Banking Service ต้องมีคุณสมบัติ 4 ข้อคือ

- ลูกค้าต้องตรวจสอบได้ว่ากำลังติดต่อกับธนาคารอยู่จริง (Authentication)
- ข้อมูลที่ลูกค้าได้รับจาก Online Banking Service ไม่ได้มีการดัดแปลงหรือแก้ไขจากบุคคลอื่นที่ไม่ใช่ธนาคาร (Integrity) เช่นผู้เจาะระบบ (Hacker)
- ข้อมูลอิเล็กทรอนิกส์ที่ลูกค้าได้รับเป็นหลักฐานทางกฎหมายที่ถูกต้อง (Non-repudiation)
- ข้อมูลที่ส่งในระบบอินเตอร์เน็ตจะต้องเป็นความลับ (Confidentiality)

2.4 มาตรฐาน X.500 และ X.509 สำหรับใบรับรองดิจิทัล (กรองรัตน์ คามตะ 2545.)

ในชีวิตประจำวัน เมื่อมีการติดต่อกับบุคคลหรือองค์กรที่ไม่มีความสัมพันธ์กันมาก่อน ถ้าต้องการตรวจสอบสถานะมักจะต้องใช้เอกสารที่เชื่อถือได้เพื่อยืนยันสถานะ เช่น การยืนยันสถานะของบริษัท ใช้เอกสารจากกรมธุรกิจการค้า การยืนยันตัวบุคคลภายในประเทศ ใช้บัตรประชาชน เป็นต้น เอกสารหรือหนังสือเหล่านี้คือตัวอย่างของใบรับรองประเภทต่างๆ ที่ใช้รับรองสถานะหรือความสามารถของบุคคลหรือนิติบุคคล สำหรับโลกของอิเล็กทรอนิกส์ สามารถทำการตรวจสอบสถานะของผู้ที่ต้องการติดต่อได้โดยการตรวจสอบจากใบรับรองดิจิทัล ซึ่งใช้ในการยืนยันตัวบุคคล

เนื่องจากการนำระบบ Certificate Authority ไปใช้ จะต้องมีการเก็บกุญแจรหัสไว้ในระบบคอมพิวเตอร์ จึงจำเป็นต้องมีระบบที่สามารถใช้เก็บกุญแจนี้ได้อย่างปลอดภัย ในอนาคตมาตรฐาน X.500 และ X.509 นี้จะถูกนำมาใช้ในการเก็บกุญแจรหัสได้เป็นอย่างดีเพราะมีโครงสร้างในการรับรองทางอิเล็กทรอนิกส์ที่ดี ระบบการรับรองทางอิเล็กทรอนิกส์ถูกพัฒนาขึ้นครั้งแรกโดยอาศัยพื้นฐานของระบบการใช้ชื่อ แบบ X.500 ซึ่งถูกออกแบบเป็นครั้งแรกในการป้องกันการเข้าถึงข้อมูลโดยบุคคลต่างๆ ระบบที่นำมาใช้ในการกำหนดว่าบุคคลนี้อยู่ในส่วนใดเรียกว่า X.500 Naming Convention

2.4.1 ระบบการตั้งชื่อของ X.500 (กรองรัตน์ คามตะ 2545.)

ระบบการตั้งชื่อที่นำมาใช้ใน X.500 คือระบบที่เรียกว่า DN – Distinguish Name ซึ่งเป็นระบบที่สามารถรับกระกันได้ว่าทุกๆคนที่อยู่ในระบบจะมีชื่อที่ไม่ซ้ำกันเลย ส่วนประกอบของระบบนั้นจะจัดชื่อเป็นลำดับขั้นตามแผนภาพดังที่แสดงไว้ โดยจะมีลำดับจากสูงไปต่ำดังนี้คือ

- Country => C ,
- State or Province => SP ,
- Locality => L
- Organization => O
- Organization Unit => OU
- Common Name => CN

:: ระบบนี้จะเป็นระบบที่สามารถบ่งบอกถึงบุคคลใดๆที่อยู่ในระบบได้โดยใช้ชื่อที่ต่างกัน ::

2.4.2 มาตรฐาน X.509 v3 (กรองรัตน์ คามตะ 2545.)

ระบบการตั้งชื่อแบบ X.500 นั้นมีปัญหาอยู่มากในการนำไปใช้ทางปฏิบัติ เนื่องจากว่ามีการข้ามลำดับขั้นของผู้ใช้ที่อยู่ในระดับต่างกัน เพราะลักษณะของสังกัดหรือหน่วยงานที่แตกต่างกันออกไปมากมาย ดังนั้นระบบนี้ถึงแม้ว่าจะมีประโยชน์มากสำหรับหน่วยงานทางด้านธุรกิจแล้วระบบ X.500 นี้ไม่มีความอ่อนตัวเท่าที่ควร ดังนั้นในการประยุกต์ใช้ระบบนี้จึงได้มีการปรับปรุงเพิ่มเติมระบบให้เป็น X.509 v3 ซึ่งสามารถนำไปใช้กับระบบคอมพิวเตอร์ได้เป็นอย่างดี โดยมีการเพิ่มเติม

- E-mail Address
- DNS Name
- URL's
- IP Address
- EDI และ X.400 Name
- อื่นๆ

:: การประยุกต์ใช้ในระบบการรับรองทางอิเล็กทรอนิกส์ (Certificate) นั้น ระบบจะใช้แต่ละขั้นเป็น Certificate Authority (CA) ในการรับรองขั้นที่ต่ำกว่าโดยจะเติมชื่อ CA ลงไปหลังชื่อ DN ::

จะเห็นได้ว่าในขั้นสูงสุดในการรับรองทางอิเล็กทรอนิกส์คือ Root Certificate ซึ่งจะเป็นตัวที่น่าเชื่อถือที่สุดในระบบ ดังนั้นตัว Root Certificate นี้จะต้องได้รับการป้องกันอย่างดีที่สุด ปัจจุบันนี้การเก็บกุญแจรหัสยังไม่ได้ถูกเก็บไว้ใน X.500 Directories มากเท่าใดนัก เพราะส่วนมากยังเก็บไว้ใน

Relational Database (RDBMS) เป็นส่วนใหญ่แต่ในอนาคตก็ควรจะมีการเก็บกุญแจรหัสลับไว้ใน X.500 Directories ด้วยเพื่อความปลอดภัยที่ดีกว่า

มาตรฐาน X.509 v3 นั้นได้รับการรับรองโดย ISO และนำไปใช้ในผลิตภัณฑ์หลายอย่าง เช่น S/MINE, SSL, S-HTTP, PEM, IPsec Key Management มาตรฐานนี้สนับสนุนส่วนประกอบต่อไปนี้คือ

- Subject Name
- Subject Attributes
- Subject Public Key
- Validity Date
- Issuer Name
- Certificate Serial Number
- Issuer Signature
- Internet E-mail Address

2.4.2 การทำงานของมาตรฐาน X.509 (กรองรัตน์ คามตะ 2545.)

ใบรับรองตามมาตรฐาน X.509 จะจับคู่ระหว่าง Subject ใดๆกับกุญแจคู่ ซึ่งประกอบไปด้วยกุญแจสาธารณะ (Public Key) กับกุญแจส่วนตัว (Private Key) โดยกุญแจสาธารณะจะเปิดเผยต่อทุกคน สามารถใช้ในการตรวจสอบข้อมูลที่ได้รับการรับรอง (Sign) โดยกุญแจส่วนตัวใช้เพื่อเข้ารหัสข้อมูลที่จะส่งให้ให้เป็นเจ้าของกุญแจซึ่งจะมีกุญแจส่วนตัวที่จะใช้ถอดรหัสข้อมูลนั้นได้ ผู้ที่เป็นเจ้าของกุญแจคู่จะต้องเก็บรักษากุญแจส่วนตัวที่สามารถใช้ในการเข้าและถอดรหัสและรับรองข้อมูล โดยป้องกันจากคนอื่นที่ไม่ใช่เจ้าของหรือไม่มีสิทธ์ในการใช้กุญแจส่วนตัวโดยมิให้ล่วงรู้ได้

2.5 Secure Sockets Layer (SSL) (กรองรัตน์ คามตะศิลา 2545.)

SSL ย่อมาจากคำว่า Secure Sockets Layer เป็นโปรโตคอลที่เพิ่มความปลอดภัยในการรับส่งข้อมูลผ่านระบบเครือข่าย ทำให้เราสามารถส่งข้อมูลที่เป็นความลับ เช่น รหัสผ่าน หรือ หมายเลขบัตรเครดิตผ่านระบบเครือข่ายได้ด้วยความปลอดภัย นอกจากผู้ส่งและผู้รับข้อมูลแล้วไม่มีใครในระบบเครือข่ายสามารถดึงข้อมูลที่เป็นความลับไปใช้ได้

โปรโตคอล SSL จะใช้ Digital Certificate ในการสร้างท่อสื่อสาร ที่มีความปลอดภัยสูง ระหว่างจุดที่ทำการติดต่อสื่อสาร 2 จุด ข้อมูลที่ส่งผ่านท่อสื่อสาร SSL นี้ ไม่สามารถถูก โจรกรรมข้อมูล โดยที่ผู้ทำการส่งข้อมูลระหว่าง 2 จุดไม่รู้ได้โดยเด็ดขาด

SSL เป็นโปรโตคอลที่เสนอโดยบริษัท Netscape เพื่อให้ใช้โปรโตคอลมาตรฐานในการรักษาความปลอดภัยของการส่งข้อมูลบน WWW ปัจจุบัน SSL กำลังอยู่ในระหว่างการพิจารณาโดย W3C (World Wide Web Consortium) และ IETF (Internet Engineering Task Force) เพื่อยอมรับเป็นมาตรฐาน ปัจจุบัน SSL มีเวอร์ชันล่าสุดคือเวอร์ชัน 3

2.5.1 ส่วนประกอบของ SSL (กรองรัตน์ คามตะ 2545.)

SSL จัดเป็นโปรโตคอลที่อยู่ระหว่าง application layer และ transport layer SSLสามารถรองรับการทำงานกับ application โปรโตคอลต่าง ๆ เช่น HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), Telnet หรืออื่น ๆ ได้ SSL ทำงานโดยอาศัยหลักการการเข้ารหัสข้อมูล (encryption) , Message Digests และลายเซ็นดิจิทัล (Digital Signature) ซึ่งส่วนประกอบของ SSL มีด้วยกัน 2 ส่วน ดังนี้

1. **SSL Record Protocol** อยู่ในเลเยอร์ที่ต่ำกว่าติดกับ TCP ทำหน้าที่ห่อหุ้ม (Encapsulate) โปรโตคอลอื่นๆ ที่สูงกว่าและระบุรูปแบบของการรับส่งข้อมูล
2. **SSL Handshake Protocol** ซึ่งทำให้ไคลเอ็นท์และเซิร์ฟเวอร์สามารถตรวจสอบสิทธิของกันและกัน (Authentication) และตกลงอัลกอริทึมในการเข้ารหัสที่จะใช้ รวมถึงกุญแจที่ใช้ในระบบก่อนที่จะตกลงแลกเปลี่ยนข้อมูลได้ ประโยชน์ข้อหนึ่งของ SSL คือ ไม่ขึ้นต่อการทำงานของเลเยอร์ที่สูงกว่า กล่าวคือ โปรโตคอลใดๆในเลเยอร์ที่สูงกว่าสามารถทำงานอยู่บน SSL ได้

2.5.2 คุณสมบัติของการสื่อสารผ่าน SSL (กรองรัตน์ คามตะ 2545.)

- การเชื่อมต่อเป็นส่วนตัว หลังจากตกลงกันถึงกุญแจ (Secret Key) ที่จะใช้แล้ว จะมีการเข้ารหัสข้อมูล ซึ่งจะใช้ระบบรหัสแบบสมมาตร เช่น DES หรือ RC4 เป็นต้น
- การระบุช่องทางสื่อสาร จะมีการตรวจสอบสิทธิโดยใช้ระบบแบบอสมมาตร เช่น RSA หรือ DSS เป็นต้น
- การเชื่อมต่อมีความน่าเชื่อถือ ข้อมูลที่ส่งไปจะมี Message Integrity Check ที่ใช้ Keyed MAC การคำนวณเกี่ยวกับ MAC นี้จะใช้ Secure Hash Function เช่น MD5 หรือ SHA เป็นต้น

2.5.3 หน้าที่ของ SSL (กรองรัตน์ คามตะ 2545.)

SSL ใช้สำหรับตรวจสอบและเข้ารหัสลับการติดต่อสื่อสารระหว่าง client และ server มีหน้าที่ดังนี้

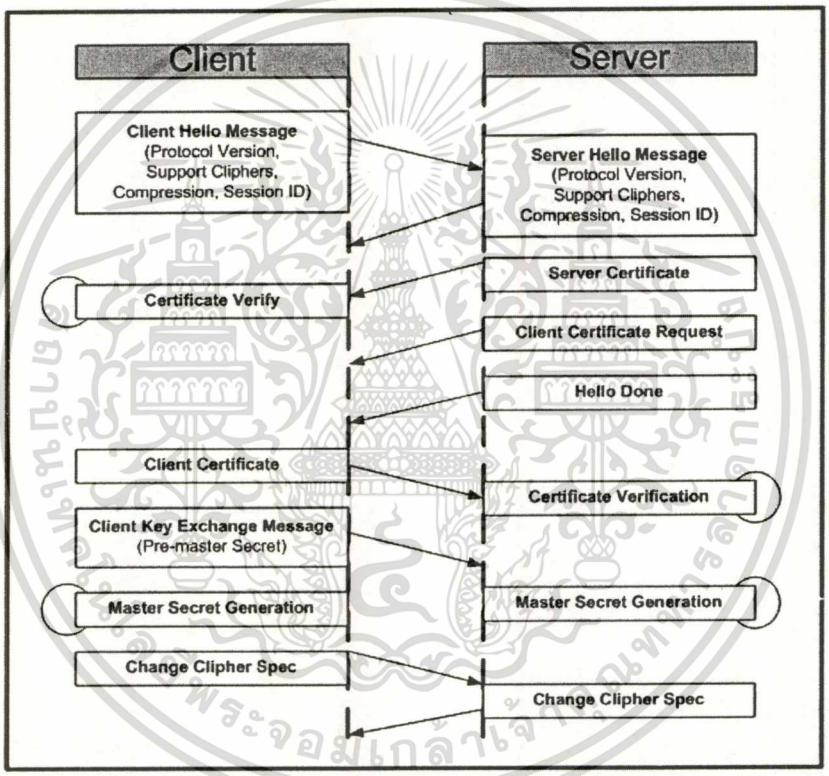
1. **การตรวจสอบ server ว่าเป็นตัวจริง**: ตัวโปรแกรม client ที่มีขีดความสามารถในการสื่อสารแบบ SSL จะสามารถตรวจสอบเครื่อง server ที่ตนกำลังจะไปเชื่อมต่อได้ว่า server นั้นเป็น server ตัวจริงหรือไม่ โดยใช้เทคนิคการเข้ารหัสแบบ public key ในการตรวจสอบใบรับรอง (certificate) และ public ID ของ server นั้น (โดยที่มีองค์กรที่ client เชื่อถือเป็นผู้ออกใบรับรองและ public ID ให้แก่ server นั้น) และหน้าที่นี้ของ SSL เป็นหน้าที่ที่สำคัญ โดยเฉพาะอย่างยิ่งในกรณีที่ client ต้องการที่จะส่งข้อมูลที่เป็นความลับ (เช่น หมายเลข credit card) ให้กับ server ซึ่ง client จะต้องตรวจสอบก่อนว่า server เป็นตัวจริงหรือไม่
2. **การตรวจสอบว่า client เป็นตัวจริง**: server ที่มีขีดความสามารถในการสื่อสารแบบ SSL จะใช้เทคนิคเช่นเดียวกับในหัวข้อที่แล้วในการตรวจสอบ client หรือผู้ใช้ว่าเป็นตัวจริงหรือไม่ โดยจะตรวจสอบใบรับรองและ public ID (ที่มีองค์กรที่ server เชื่อถือเป็นผู้ออกให้) ของ client หรือผู้ใช้นั้น และหน้าที่นี้ของ SSL จะมีประโยชน์ในกรณีเช่น ธนาคารต้องการที่จะส่งข้อมูลลับทางการเงินให้แก่ลูกค้าของตนผ่านทางเครือข่าย Internet (server ก็จะต้องตรวจสอบ client ก่อนว่าเป็น client นั้นจริง)
3. **การเข้ารหัสลับการเชื่อมต่อ**: ในกรณีนี้ ข้อมูลทั้งหมดที่ถูกส่งระหว่าง client และ server จะถูกเข้ารหัสลับ โดยโปรแกรมที่ส่งข้อมูลเป็นผู้เข้ารหัสและโปรแกรมที่รับข้อมูลเป็นผู้ถอดรหัส (โดยใช้วิธี public key) นอกจากการเข้ารหัสลับในลักษณะนี้แล้ว SSL ยังสามารถปกป้องความถูกต้องสมบูรณ์ของข้อมูลได้อีกด้วย กล่าวคือ ตัวโปรแกรมรับข้อมูลจะทราบได้หากข้อมูลถูกเปลี่ยนแปลงไปในขณะกำลังเดินทางจากผู้ส่งไปยังผู้รับ

2.5.4 หลักการทำงานของ SSL (กรองรัตน์ คามตะ 2545.)

- เมื่อผู้ใช้อินเทอร์เน็ตทำการติดต่อ กับเว็บไซต์ที่ทำการติดตั้ง Certificate เพื่อทำการซื้อสินค้าชนิดหนึ่งผ่านอินเทอร์เน็ต บราวเซอร์ของผู้ใช้จะทำการร้องขอไปยัง Web Server เพื่อบอกว่าต้องการใช้งาน SSL Web Server จะส่งสัญญาณตอบกลับมายังบราวเซอร์ถึงข้อมูลของ Certificate ที่ติดตั้งอยู่บนตัว Server นั้นๆ พร้อมกับส่ง Public Key มาด้วย บราวเซอร์จะทำการสร้าง Session พร้อมทั้ง เข้ารหัสข้อมูลด้วย Public Key ที่ได้รับส่งไปยัง Web Server จากนั้น Web Server จะทำการ ถอดรหัสเพื่อนำ Session ไปใช้งาน

- ดังนั้น Web Server Certificate ช่วยป้องกันการสื่อสาร ข้อมูลระหว่างคุณและลูกค้าของคุณ ช่วยให้วางใจได้ในกรณีที่ ลูกค้าของคุณส่งเลขบัตรเครดิต หรือข้อมูลสำคัญ อาทิ รหัสผ่านว่าไม่มีผู้ใดสามารถล่วงรู้ได้

2.5.5 ขั้นตอนการทำ Handshake ของ SSL (กรองรัตน์ คามตะ 2545.)



รูปที่ 2.6 ขั้นตอนการทำ SSL Handshake

- จากรูปที่ 2.6 ไคลเอ็นท์ส่งหมายเลขเวอร์ชันของ SSL, Clipher setting, ข้อมูลที่สุ่มสร้างขึ้นและข้อมูลอื่นๆ ที่เซิร์ฟเวอร์ต้องใช้ระหว่างการสื่อสารต่อไปยังเซิร์ฟเวอร์
- เซิร์ฟเวอร์ส่งหมายเลขเวอร์ชันของ SSL, Cipher setting, ข้อมูลที่สุ่มสร้างขึ้นและข้อมูลอื่นๆ ที่ไคลเอ็นท์ต้องการใช้ระหว่างการสื่อสาร ทั้งนี้ ยังส่งใบรับรองอิเล็กทรอนิกส์ของเซิร์ฟเวอร์ให้ด้วยและหากไคลเอ็นท์ร้องขอ

- ไคลเอ็นท์ใช้ข้อมูลบางอย่างที่ส่งมาจากเซิร์ฟเวอร์ในการตรวจสอบตัวตนเซิร์ฟเวอร์ หากไม่สามารถตรวจสอบได้ ผู้ใช้จะได้รับการเตือนและแจ้งให้ทราบว่าการเชื่อมต่อแบบที่มีการตรวจสอบตัวตนก่อนและมีการเข้ารหัสไม่สามารถทำได้
- ไคลเอ็นท์สร้าง Premaster secret สำหรับ Session แล้วเข้ารหัสด้วยกุญแจสาธารณะของเซิร์ฟเวอร์ (ได้จากใบรับรองอิเล็กทรอนิกส์ของเซิร์ฟเวอร์ ที่ส่งมาให้) และส่ง Premaster secret ที่เข้ารหัสแล้วไปยังเซิร์ฟเวอร์ ทั้งนี้ จะทำได้โดยอาศัยข้อมูลที่สร้างมาจากขั้นตอนข้างต้น และความร่วมมือจากเซิร์ฟเวอร์ ขึ้นอยู่กับ Cipher ที่ใช้
- ถ้าเซิร์ฟเวอร์ร้องขอที่จะตรวจสอบตัวตนของไคลเอ็นท์ด้วย ไคลเอ็นท์จะรับรองข้อมูลส่งหนึ่งที่ Unique ใน Handshake และทั้งเซิร์ฟเวอร์และไคลเอ็นท์รู้จัก ในกรณี ไคลเอ็นท์จะส่งทั้งข้อมูลที่รับรองแล้วและใบรับรองอิเล็กทรอนิกส์ของไคลเอ็นท์ไปยังเซิร์ฟเวอร์พร้อมกับ Premaster secret ที่เข้ารหัสแล้วด้วย
- ถ้าเซิร์ฟเวอร์ร้องขอที่จะตรวจสอบตัวตนของไคลเอ็นท์ แล้วไม่สามารถทำได้ session จะจบลง แต่ถ้าสามารถทำได้ เซิร์ฟเวอร์จะใช้กุญแจส่วนตัวถอดรหัส Premaster secret จากนั้นจะเกิดขั้นตอนตามมาอีกหลายข้อ ซึ่งจะทำทั้งบนเซิร์ฟเวอร์และไคลเอ็นท์ ทั้งนี้เพื่อสร้าง Master secret ขึ้น
- ทั้งไคลเอ็นท์และเซิร์ฟเวอร์จะใช้ Master secret สร้าง Session key ซึ่งเป็นกุญแจเดียวที่ใช้สำหรับเข้าและถอดรหัสข้อมูลที่แลกเปลี่ยนกันผ่าน SSL Session และใช้เพื่อตรวจสอบความถูกต้องข้อมูลด้วย คือตรวจหาว่าข้อมูลเปลี่ยนแปลงไปบ้างหรือไม่ระหว่างการส่ง
- ไคลเอ็นท์ส่ง Message มายังเซิร์ฟเวอรีเพื่อแจ้งว่าข้อมูลที่ส่งหลังจากนี้ไปจะได้รับการเข้ารหัสด้วย Session key จากนั้นจะส่ง Message อีกส่วนที่เข้ารหัสไว้ไปเพื่อบอกว่าส่วนการทำ Handshake ของไคลเอ็นท์สิ้นสุดลงแล้ว
- เซิร์ฟเวอร์ส่ง Message ไปยังไคลเอ็นท์แจ้งว่าข้อมูลที่จะส่งหลังจากนี้ไปจะได้รับการเข้ารหัสด้วย Session key จากนั้นจะส่ง Message อีกส่วนที่เข้ารหัสไว้ไปเพื่อบอกว่าส่วนการทำ Handshake ของเซิร์ฟเวอร์สิ้นสุดลงแล้ว
- SSL handshake สิ้นสุดลง และ SSL session ได้เริ่มต้นแล้ว ไคลเอ็นท์และเซิร์ฟเวอร์จะใช้ Session key เพื่อเข้าและถอดรหัสข้อมูลที่รับส่งระหว่างกันและเพื่อตรวจสอบความถูกต้องของข้อมูลด้วย

จากขั้นตอนการแลกเปลี่ยนรหัสนั้นใช้เวลานานพอสมควร ซึ่งโปรโตคอล SSL ก็มีคุณสมบัติที่ช่วยลดขั้นตอนในการทำงานนี้ลงไปได้ ถ้ามีเว็บบราวเซอร์ตัวใหม่ติดต่อไปยังเว็บเซิร์ฟเวอร์ตัวเดิมที่ทำงานกับ SSL ได้ เว็บบราวเซอร์อาจเพียงส่งแค่หมายเลขประจำตัวของช่องการสื่อสารให้กับเซิร์ฟเวอร์ และถ้าเซิร์ฟเวอร์นั้นยอมรับหมายเลขประจำตัวที่ส่งมา การติดต่อระหว่างเซิร์ฟเวอร์ตัวเดิมกับเว็บบราวเซอร์ตัวใหม่ ก็สามารถใช้อัลกอริทึมเดิมในการเข้ารหัสและบีบอัดข้อมูล รวมไปถึงรหัสเดิมที่เคยตกลงกันไว้ก่อนหน้านั้น โดยไม่ต้องทำขั้นตอนแลกเปลี่ยนรหัสครั้งใหม่เลย บราวเซอร์ของเน็ต สเคปยังสามารถส่งข้อความที่ชื่อ "Keep Alive" ที่เป็นคำร้องขอให้เปิดช่องการสื่อสาร TCP ค้างเอาไว้สักพักแม้ว่าจะแลกเปลี่ยนข้อมูลเสร็จสิ้นแล้วก็ตาม ทำให้การสื่อสารครั้งใหม่ที่อาจเกิดขึ้นในอนาคตไม่จำเป็นต้องเสียเวลากับการแลกเปลี่ยนรหัสซ้ำอีก

2.5.6 SSL กับ Digital Certificate (กรองรัตน์ คามตะ 2545.)

โปรโตคอล SSL จะใช้ Digital Certificate ในการสร้างท่อสื่อสาร ที่มีความปลอดภัยสูงระหว่างจุดที่ทำการติดต่อสื่อสาร 2 จุด ข้อมูลที่ส่งผ่านท่อสื่อสาร SSL นี้ ไม่สามารถถูก โจรกรรมข้อมูลโดยที่ผู้ทำการส่งข้อมูลระหว่าง 2 จุดไม่รู้ได้โดยเด็ดขาดดังนี้

- Web Server Certificate จึงมีบทบาทเข้ามา มีส่วนช่วยในการเพิ่มความปลอดภัย ในการส่งข้อมูลต่างๆเหล่านี้ ผ่านเครือข่ายอินเทอร์เน็ต การติดตั้ง Certificate ลงบน Web Server ของคุณจะทำให้การสื่อสารระหว่างลูกค้า ที่ใช้ บราวเซอร์ติดต่อมายัง Web Server ของคุณ ทำการเข้ารหัสด้วยเทคโนโลยี SSL ซึ่ง SSL เทคโนโลยี เป็นโปรโตคอลมาตรฐาน ที่ใช้ในการเข้ารหัส ข้อมูลเพื่อความปลอดภัย ในการรับส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต SSL เทคโนโลยีถูกติดตั้ง ลงบนบราวเซอร์ ชั้นนำทุกตัวอาทิ IE, Netscape, Opera เป็นต้น
- SSL มีบทบาทสำคัญในการเพิ่มความปลอดภัย ในการทำธุรกรรมบนอินเทอร์เน็ต SSL จะทำงานร่วมกับตัวบราวเซอร์โดยผ่าน Digital Certificate

2.5.7 SSL กับ HTTPS (กรองรัตน์ คามตะ 2545.)

โดยปกติแล้วเว็บจะใช้โปรโตคอล HTTP [Hyper text Transfer Protocol] ในการรับส่งเอกสาร HTTP ระหว่าง Web Server และ Browser ซึ่งโปรโตคอลนี้จะถ่ายโอนเอกสารในรูปแบบของ Clear Text ทำให้การสื่อสารไม่ปลอดภัยสำหรับการรับส่งข้อมูลที่สำคัญต่างๆ สำหรับเข้าใช้ระบบต่างๆ เนื่องจากคนอื่นอาจเฝ้าดูข้อมูลที่วิ่งผ่านเครือข่ายอยู่ก็ได้ ส่วนเว็บโปรโตคอลเวอร์ชันที่รองรับ SSL คือ

HTTPS [Hyper text Transfer Protocol Security] ซึ่งเป็นโปรโตคอลที่ถือว่าปลอดภัยสำหรับการสื่อสารผ่านอินเตอร์เน็ต โดยโปรโตคอลนี้มีรูปแบบการทำงานดังนี้

1. บราวเซอร์จะเป็นฝ่ายเริ่มสื่อสารโดยส่งการร้องขอไปยังเว็บเซิร์ฟเวอร์ ที่รองรับ ทัSSL พร้อมทั้ง SSL เวอร์ชันและอัลกอริทึมที่ใช้สำหรับการเข้ารหัสข้อมูล
2. เมื่อเซิร์ฟเวอร์ได้รับการร้องขอก็ส่ง SSL เวอร์ชันของเซิร์ฟเวอร์ พร้อมทั้งข้อตกลงเกี่ยวกับอัลกอริทึมที่จะใช้ และใบรับรองดิจิทัลที่ออกโดย CA ที่ไคลแอนท์เชื่อถือ ซึ่งในใบรับรองนี้จะประกอบด้วย Public Key ของเซิร์ฟเวอร์ด้วย
3. เมื่อบราวเซอร์ได้รับใบบรองดิจิทัลก็จะเช็คว่า CA ที่ออกใบรับรองนี้เชื่อถือได้หรือไม่ ถ้าไม่มี CA อยู่ในรายการที่ไคลแอนท์เชื่อถือก็จะแจ้งให้ยูสเซอร์ทราบ ถ้ามีบราวเซอ์ก็จะใช้ Public Key ของ CA ถอดรหัสใบรับรองเพื่อให้ได้ Public Key ของเซิร์ฟเวอร์
4. บราวเซอร์สร้างซิมเมทริกซ์คีย์แล้วใช้ Public Key ของเซิร์ฟเวอร์เข้ารหัสคีย์ดังกล่าวแลวส่งไปให้กับเซิร์ฟเวอร์
5. บราวเซอร์ส่งข้อความไปแจ้งให้เซิร์ฟเวอร์ทราบว่าต่อไปข้อมูลที่ส่งไปยังเซิร์ฟเวอร์จะถูกเข้ารหัสโดยใช้ซิมเมทริกซ์คีย์ที่สร้างและส่งไปยังเซิร์ฟเวอร์ก่อนหน้า และแจ้งการสิ้นสุดขั้นตอนเจรจา (Handshaking)
6. ฝั่งเซิร์ฟเวอร์ก็เช่นกัน จะส่งข้อความไปบอกว่าต่อไปนี้จะใช้เซสชันคีย์ในการเข้ารหัสข้อความที่รับส่งต่อไป พร้อมทั้งแจ้งการสิ้นสุดขั้นตอนการเจรจา
7. ขั้นตอนการเจรจาก็สิ้นสุด ต่อไปการรับส่งข้อมูลระหว่างเซิร์ฟเวอร์และบราวเซอร์ก็จะใช้เซสชันคีย์ในการเข้ารหัสข้อมูล

บทที่ 3
เนื้อหาและการทำงาน

ปัจจุบันการติดต่อสื่อสารมักทำผ่านระบบเครือข่ายอินเทอร์เน็ต โดยที่บุคคลหรือองค์กรที่ติดต่อด้วยนั้น อาจจะไม่เคยมีความสัมพันธ์หรือรู้จักกันมาก่อน ก่อให้เกิดความไม่มั่นใจว่า บุคคลหรือองค์กรที่ติดต่อด้วยคือใคร มีตัวตนจริงหรือไม่ ฉะนั้น จึงจำเป็นที่จะต้องมีกลไกในการยืนยันตัวบุคคลสำหรับโลกอิเล็กทรอนิกส์ สิ่งที่ใช้ในการยืนยันก็คือ ใบรับรองดิจิทัล (Digital Certificate)

ใบรับรองอิเล็กทรอนิกส์ เป็นข้อมูลในรูปแบบอิเล็กทรอนิกส์ที่ออกให้โดยผู้ให้บริการออกใบรับรอง (Certification Authority - CA) ซึ่งข้อมูลในใบรับรองอิเล็กทรอนิกส์นั้น บ่งบอกถึงความมีตัวตนในโลกแห่งอิเล็กทรอนิกส์ โดยที่ใบรับรองอิเล็กทรอนิกส์ดังกล่าวสามารถนำมาประยุกต์ใช้งานได้ 2 รูปแบบ คือ การเข้ารหัส/ถอดรหัสลับ (Encryption/Decryption) และการลงลายมือชื่อดิจิทัล (Digital Signature) กับข้อมูลที่กระทำการรับส่งระหว่างกัน

3.1 หน่วยผู้ประกอบการรับรอง (Certification Authority) (สถาบันวิจัยเพื่อการพัฒนา. 2548.)

Certification Authority เป็นหน่วยงานหรือเครื่องเซิร์ฟเวอร์ที่ให้บริการออกใบรับรองดิจิทัลให้แก่ผู้ใช้หน่วยงานดังกล่าวนี้ทำหน้าที่ คล้ายกับกับองค์กร ตรวจคนเข้าเมืองเพื่อตรวจตราหนังสือเดินทางของคุณ บทบาทของ CA ก็คือตรวจสอบและรับรอง Certificates หลังจากที่ CA ได้รับรอง Certificates แล้วผู้ถือ Certificate นั้นๆ ก็สามารถเผยแพร่ให้กับผู้ใช้งานทั่วไปได้รับรู้ เพื่อที่เป็นการบ่งบอกว่าผู้ถือ Certificate เป็นใครและมีการเข้ารหัสป้องกันการโจรกรรม ข้อมูลหรือมีความปลอดภัยในการติดต่อสื่อสาร บนเครือข่ายและต้องเป็นหน่วยงานที่ถูกต้องตามกฎหมาย

อีกความหมายคือ หน่วยผู้ประกอบการรับรองที่เป็นหน่วยงานภายนอก (Trusted Third Party) ซึ่งมีหน้าที่หลักคือ เป็นผู้ออกใบรับรองดิจิทัลให้กับบุคคลหรือสิ่งอื่น ๆ (ในที่นี้จะเรียกรวมว่าเป็น Subject) ทั้งนี้ Self-signed Certificate จะเป็นสิ่งที่ระบุตัวตนของหน่วยผู้ประกอบการรับรองเอง ดังนั้นหน่วยผู้ประกอบการรับรองจึงเป็นจุดเริ่มต้นของการสร้างความไว้วางใจ (Trust) แต่ละเอ็นทิตี้จะต้องมอบความไว้วางใจต่อหน่วยผู้ประกอบการรับรอง และสิ่งใดก็ตามที่หน่วยผู้ประกอบการรับรองได้ออกใบรับรองให้

3.1.1 หน้าที่หลักของ Certification Authority (สถาบันวิจัยเพื่อการพัฒนา. 2548.)

1. การให้บริการเทคโนโลยีการรหัส ได้แก่ การสร้างกุญแจสาธารณะ และกุญแจสำหรับผู้จดทะเบียน การส่งมอบกุญแจลับ การสร้าง และการรับรองลายมือชื่อดิจิทัล เป็นต้น
2. การให้บริการเกี่ยวกับการออกใบรับรอง ได้แก่ การออก การเก็บรักษา การยกเลิก การตีพิมพ์เผยแพร่ ใบรับรองดิจิทัล รวมทั้งการกำหนดนโยบายการออกและอนุมัติใบรับรอง เป็นต้น
3. บริการเสริมอื่น ๆ ได้แก่ การตรวจสอบสัญญาต่าง ๆ การทำทะเบียน การกู้กุญแจ เป็นต้น

3.1.2 โครงสร้างของ Certification Authority (สถาบันวิจัยเพื่อการพัฒนา. 2548.)

โครงสร้างพื้นฐานซึ่งจะช่วยให้สามารถระบุตัวบุคคลได้อย่างสะดวก และมีความน่าเชื่อถือสูง คือหน่วยงานที่เรียกว่า "องค์กรออกใบรับรอง" (Certification Authority หรือ CA) หรือที่เรียกกันว่า "โครงสร้างพื้นฐานของระบบกุญแจสาธารณะ" (Public Key Infrastructure หรือ PKI) ซึ่งจะเป็นตัวกลายในการตรวจสอบและออกใบรับรองให้แก่ผู้อื่น ตามแนวทางนี้จะมีบุคคลต่าง ๆ ที่เกี่ยวข้องกัน 3 ฝ่าย (three-party model) คือ ผู้ถือใบรับรอง (Certificate holder) ซึ่งเราอาจเรียกว่าเป็นบุคคลที่หนึ่ง ผู้ใช้ใบรับรองในการระบุตัวผู้ถือใบรับรอง (relying party) ซึ่งอาจเรียกว่าเป็นบุคคลที่สอง และองค์กรออกใบรับรอง ซึ่งอาจเรียกว่าเป็นบุคคลที่สาม หรือที่นิยมเรียกว่า "บุคคลที่สามที่เชื่อถือได้" (trusted third party)

3.1.3 ประเภทบริการของ Certification Authority (สถาบันวิจัยเพื่อการพัฒนา. 2548.)

- ใบรับรองอิเล็กทรอนิกส์สำหรับบุคคล (Personal Certificate Service) เป็นใบรับรองที่ใช้ในการยืนยันตัวบุคคลทางโลกอิเล็กทรอนิกส์ ทำให้ผู้ประกอบธุรกรรมสามารถมั่นใจได้ว่าบุคคลหรือองค์กรที่ติดต่อด้วยมีตัวตนและเป็นบุคคลที่อ้างถึงจริง รวมทั้งยังก่อให้เกิดความปลอดภัยของข้อมูลที่สื่อสารระหว่างกัน ทำให้ผู้อื่นไม่สามารถอ่านข้อมูลดังกล่าวได้ ซึ่งสามารถนำไปใช้ได้ในหลายลักษณะงาน เช่น การรับ-ส่งจดหมายอิเล็กทรอนิกส์แบบปลอดภัย (Secure e-mail) และการยืนยันตัวตนในการเข้าใช้งานเว็บไซต์ผ่านทางเว็บบราวเซอร์ (Client Authentication) เป็นต้น
- ใบรับรองอิเล็กทรอนิกส์สำหรับเครื่องให้บริการเว็บ (Web Server Certificate Service) ใช้สำหรับสร้างช่องทางสื่อสารแบบปลอดภัยระหว่างเครื่องให้บริการเว็บ (Web Server) และ

เครื่องใช้บริการ (Client) โดยบริการนี้จะช่วยเสริมความปลอดภัยของข้อมูลในด้านการรักษาความลับของข้อมูลที่รับ-ส่งระหว่างเครื่องให้บริการเว็บและเครื่องใช้บริการ และสร้างความเชื่อมั่นให้กับผู้ใช้บริการว่าคู่สื่อสารเป็นเครื่องซึ่งอ้างถึงจริง และบริการนี้สามารถนำไปประยุกต์ใช้งานในการรักษาความลับของข้อมูลที่รับ-ส่งผ่านทางเครือข่ายอินเทอร์เน็ต (เช่น รหัสผ่าน หมายเลขบัตรเครดิต ฯลฯ) ได้หลายลักษณะ อันได้แก่ การประกอบธุรกรรมทางการเงินต่างๆ ของธนาคาร การชำระค่าสินค้าและบริการ และการสั่งซื้อสินค้าแบบออนไลน์ เป็น

3.1.4 คำจำกัดความอื่นๆที่เกี่ยวข้องกับ Certificate Authority (สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ. 2548. หน้า 15.)

คำศัพท์	คำจำกัดความ
เจ้าหน้าที่รับลงทะเบียน (Registration Authority : RA)	ผู้ซึ่งทำหน้าที่รับลงทะเบียนเมื่อมีการยื่นคำขอใช้บริการ แจ้งเพิกถอนใบรับรอง หรือต่ออายุใบรับรอง โดยทำการตรวจสอบและยืนยันความถูกต้องของข้อมูลที่ผู้ขอใช้บริการให้ไว้
เจ้าหน้าที่ออกใบรับรอง (Issuing Authority : IA)	ผู้ซึ่งทำหน้าที่ออกใบรับรอง เมื่อมีการยื่นคำขอมาจากเจ้าหน้าที่รับลงทะเบียน
การเพิกถอนใบรับรอง (Certificate Revocation)	การทำให้ใบรับรองไม่สามารถใช้ได้อีกต่อไปหลังจากการเพิกถอนใบรับรอง ซึ่งส่งผลให้ต้องยกเลิกกุญแจส่วนตัวที่ผู้ขอใช้บริการเก็บไว้เป็นความลับสำหรับใช้ในการสร้างลายมือชื่อดิจิทัลหรือถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ไปด้วย ทั้งนี้ โดยไม่มีผลกระทบกับใบรับรองหรือกุญแจสาธารณะซึ่งยังคงสามารถใช้ในการตรวจสอบลายมือชื่อดิจิทัลที่สร้างขึ้นก่อนการเพิกถอนใบรับรองได้
กุญแจส่วนตัว (Private Key)	กุญแจที่ใช้ในการสร้างลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการถอดรหัสลับเมื่อมีการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้
กุญแจสาธารณะ	กุญแจที่ใช้ในการตรวจสอบลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการ

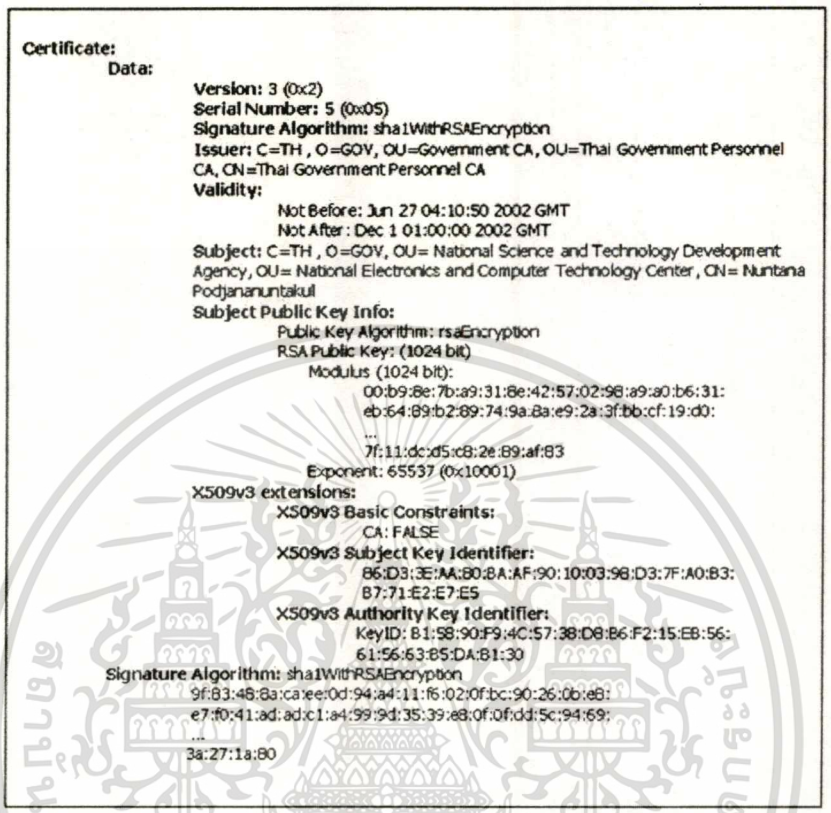
(Public Key)	เข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อมิให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์นั้น
คู่กรณีที่เกี่ยวข้อง (Relying Party)	ผู้ซึ่งกระทำการหรืองดเว้นกระทำการใดๆ เพราะเชื่อถือใบรับรองหรือลายมือชื่อดิจิทัล โดยการนำกุญแจสาธารณะที่อยู่ในใบรับรองใช้ในการตรวจสอบตัวตนที่แท้จริงของผู้ขอใช้บริการซึ่งเป็นเจ้าของลายมือชื่อดิจิทัลและมีชื่อปรากฏอยู่ในใบรับรอง
ผู้ขอใช้บริการ (Subscriber)	บุคคลทั่วไปหรือเวปไซต์ที่ผ่านหลักเกณฑ์ในการพิจารณาว่าผ่านข้อกำหนดเบื้องต้นของ CA ซึ่งได้แสดงความจำนงขอลงทะเบียนกับระบบออกใบรับรองดิจิทัลจาก CA เมื่อมีการออกใบรับรองจะมีการระบุชื่อหน่วยงานผู้ขอใช้บริการไว้ในใบรับรอง เพื่อแสดงว่าผู้ขอใช้บริการถือกุญแจส่วนตัวซึ่งทำงานสัมพันธ์ในเชิงตรรกะกับกุญแจสาธารณะที่มีการระบุไว้ในใบรับรอง
ผู้ให้บริการออกใบรับรอง / ผู้ให้บริการ (Certification Authority)	องค์กรซึ่งทำหน้าที่ในการให้บริการเกี่ยวกับการออกใบรับรองเพื่อรับรองเอนทิตีใดเอนทิตีหนึ่ง รวมทั้งการบริหารจัดการเกี่ยวกับใบรับรอง เช่น การเผยแพร่สถานะของใบรับรองที่มีการเพิกถอนในรายการเพิกถอนใบรับรอง เป็นต้น
ผู้ให้บริการออกใบรับรองเสมือน (Virtual CA)	องค์กรซึ่งทำหน้าที่ในการให้บริการเกี่ยวกับการออกใบรับรองเพื่อรับรองเอนทิตีใดเอนทิตีหนึ่ง รวมทั้งการบริหารจัดการเกี่ยวกับใบรับรอง เช่น การเผยแพร่สถานะของใบรับรองที่มีการเพิกถอนในรายการเพิกถอนใบรับรอง เป็นต้น
ไดเรกทอรี (Directory Service)	ที่เก็บรวบรวมข้อมูล โดยข้อมูลที่เก็บนั้นได้มีการถูกจัดการ เพื่อให้สามารถสืบค้นข้อมูลได้อย่างรวดเร็วตามมาตรฐานไดเรกทอรี (X.500 หรือ LDAP)
ฐานข้อมูล (Database)	ที่เก็บรวบรวมข้อมูล โดยข้อมูลที่เก็บนั้นได้มีการถูกจัดเก็บแบบที่เอื้อให้โปรแกรมคอมพิวเตอร์สามารถเข้าถึง จัดการและปรับเปลี่ยนข้อมูลได้ง่ายและรวดเร็ว
รายการเพิกถอน	รายการใบรับรองที่ถูกเพิกถอนการใช้งาน

3.2 ความหมายของใบรับรองดิจิทัล (Digital Certificate) (สถาบันวิจัยเพื่อการพัฒนา. 2548.)

Digital Certificate คือ อิเล็กทรอนิกส์ไฟล์ที่ใช้ในการจำแนกคุณลักษณะจำเพาะของแต่ละคน หรือทรัพยากรบนเครือข่าย เช่น อินเทอร์เน็ต Digital Certificate ยังใช้ในการเข้ารหัสการติดต่อสื่อสาร เพื่อเพิ่มความปลอดภัยระหว่างจุดหนึ่งไปยังอีกจุดหนึ่งบนเครือข่ายด้วย โดยที่ผู้อื่นไม่สามารถนำไปแอบอ้างหรือนำไปใช้ได้ ใบรับรองนี้ประกอบด้วยข้อมูลของผู้ใช้ที่เข้ารหัสไว้เพื่อเป็นการป้องกันความปลอดภัยของข้อมูล และจะใช้ในการเชื่อมต่อกับเครือข่ายหรือเครื่องเซิร์ฟเวอร์ที่มีการให้บริการแบบปลอดภัยดังรูปที่ 3.1

3.2.1 ข้อมูลที่แสดงใน Digital Certificate (สถาบันวิจัยเพื่อการพัฒนา. 2548.)

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

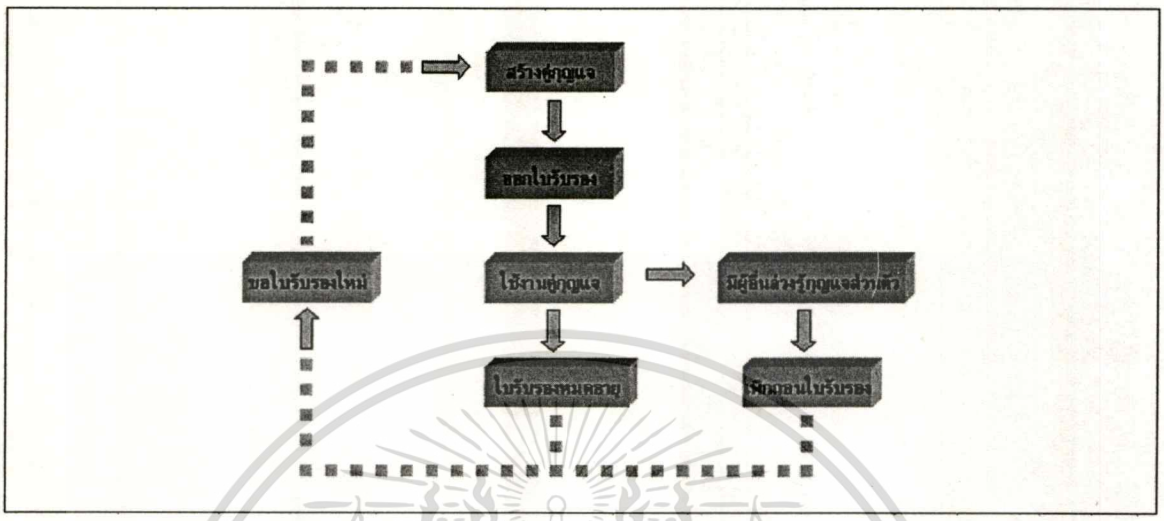


Certificate:
Data:
Version: 3 (0x2)
Serial Number: 5 (0x05)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=TH , O=GOV, OU=Government CA, OU=Thai Government Personnel CA, CN=Thai Government Personnel CA
Validity:
Not Before: Jun 27 04:10:50 2002 GMT
Not After : Dec 1 01:00:00 2002 GMT
Subject: C=TH , O=GOV, OU= National Science and Technology Development Agency, OU= National Electronics and Computer Technology Center, CN= Nuntana Podjananuntakul
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:b9:8e:7b:a9:31:8e:42:57:02:98:a9:a0:b6:31:
eb:64:89:b2:89:74:9a:8a:e9:2a:3f:bb:cf:19:d0:
...
7f:11:dc:d5:c8:2e:89:af:83
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA: FALSE
X509v3 Subject Key Identifier:
86:D3:3E:AA:80:8A:AF:90:10:03:98:D3:7F:A0:B3:
B7:71:E2:E7:E5
X509v3 Authority Key Identifier:
KeyID: B1:58:90:F9:4C:57:38:D8:B6:F2:15:EB:56:
61:56:63:B5:DA:B1:30
Signature Algorithm: sha1WithRSAEncryption
9f:83:46:8a:ca:ee:0d:94:a4:11:f6:02:0f:bc:90:26:0b:e8:
e7:f0:41:ad:ad:c1:a4:99:9d:35:39:e8:0f:0f:dd:5c:94:69:
...
3a:27:1a:80

รูปที่ 3.1 ตัวอย่างใบรับรองดิจิทัล

3.2.2 กระบวนการใช้งานใบรับรองดิจิทัล (TDRI. 2548.)

- ผู้ใช้สร้างกุญแจคู่ ซึ่งประกอบด้วยกุญแจส่วนตัว (Private key) และกุญแจสาธารณะ (Publick key)
- การออกใบรับรองอิเล็กทรอนิกส์ โดยผู้ให้บริการออกใบรับรองจะทำการรับรองกุญแจสาธารณะและข้อมูลของผู้ที่เป็นเจ้าของกุญแจสาธารณะ
- การใช้งานใบรับรองอิเล็กทรอนิกส์และกุญแจส่วนตัว ในกรณีที่มีผู้อื่นล่วงรู้กุญแจส่วนตัว ผู้ที่เป็นเจ้าของใบรับรองจะต้องทำการขอเพิกถอนใบรับรอง โดยใบรับรอง ที่ถูกเพิกถอนนั้นจะปรากฏอยู่ในรายการเพิกถอนใบรับรอง (Certificate Revocation List - CRL) หลังจากนั้นผู้ที่เป็นเจ้าใบรับรองจะต้องทำการขอใบรับรอง ใหม่
- เมื่อใบรับรองอิเล็กทรอนิกส์หมดอายุ ผู้ที่เป็นเจ้าของใบรับรองจะต้องทำการขอใบรับรองใหม่



รูปที่ 3.2 วงจรการใช้งานใบรับรองอิเล็กทรอนิกส์ (Certificate Life Cycle)

3.2.3 ใบรับรองดิจิทัลสำหรับบุคคลและการประยุกต์ใช้งาน (สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ. 2547.)

ใบรับรองดิจิทัลสำหรับบุคคล (Personal Certificate) เป็นใบรับรองที่ใช้ในการยืนยันตัวบุคคลทางโลกอิเล็กทรอนิกส์ ทำให้ผู้ประกอบธุรกรรมสามารถมั่นใจได้ว่าบุคคลหรือองค์กรที่ติดต่อด้วยมีตัวตนและเป็นบุคคลที่อ้างถึงจริง รวมทั้งยังก่อให้เกิดความปลอดภัยของข้อมูลที่สื่อสารระหว่างกัน ทำให้ผู้อื่นไม่สามารถอ่านข้อมูลดังกล่าวได้ ซึ่งสามารถนำไปใช้ได้ในหลายลักษณะงาน เช่น การรับ-ส่งจดหมายอิเล็กทรอนิกส์แบบปลอดภัย (Secure E-mail) และการยืนยันตัวตนในการเข้าใช้งานเว็บไซต์ผ่านทางเว็บบราวเซอร์ (Client Authentication) เป็นต้น และมีการประยุกต์ใช้งานดังนี้

- ระบบจดหมายอิเล็กทรอนิกส์แบบปลอดภัย (Secure Electronic Mail System) คือสามารถนำใบรับรองดิจิทัลมาใช้ในการเข้ารหัสลับและลงลายมือชื่อดิจิทัล เพื่อเป็นการยืนยันตัวผู้ส่ง ยืนยันความถูกต้องครบถ้วนของข้อมูล รวมทั้งยังสามารถรักษาความลับของข้อมูลในจดหมายให้อ่านได้เฉพาะผู้รับที่ถูกระบุไว้ได้อีกด้วย
- การยืนยันตัวตนของผู้ใช้บริการ (Client Authentication) คือ ผู้ใช้บริการสามารถใช้ใบรับรองดิจิทัลในการยืนยันตัวตนก่อนเข้าใช้บริการเว็บไซต์ได้ (ในกรณีที่เว็บไซต์นั้นต้องการยืนยันตัว

บุคคล) เพื่อเป็นการยืนยัน/ระบุตัวตนของผู้ใช้บริการ อีกทั้งยังเป็นการสร้างช่องทางการสื่อสารแบบปลอดภัยระหว่างเครื่องให้บริการ (Server) และเครื่องใช้บริการ (Client) ด้วย

- การประยุกต์ใช้งานกับแอปพลิเคชั่นอื่น ๆ คือ ใบรับรองดิจิทัลสามารถนำไปประยุกต์ใช้งานกับแอปพลิเคชั่นต่างๆ นอกเหนือจากที่ได้กล่าวข้างต้น โดยพิจารณาว่าส่วนใดของแอปพลิเคชั่นที่ต้องการความปลอดภัยของข้อมูล ก็สามารถนำเทคโนโลยีโครงสร้างพื้นฐานของระบบกุญแจสาธารณะไปผนวกกับส่วนนั้นๆ ซึ่งการประยุกต์ในลักษณะดังกล่าว จะต้องมีการพัฒนาแอปพลิเคชั่นเฉพาะ เพื่อให้สามารถทำงานร่วมกับใบรับรองดิจิทัลได้

3.3 การวางแผนปฏิบัติงาน

1. ระบบปฏิบัติการที่เลือกใช้คือ Window XP

เป็นระบบปฏิบัติการที่ได้รับความนิยมอย่างแพร่หลาย ออกแบบไว้สำหรับการใช้งานบนเครื่องคอมพิวเตอร์ส่วนบุคคล จึงสามารถทำการพัฒนาโปรแกรมต่อไปได้อย่างง่ายดาย

2. ภาษาที่ใช้ในการพัฒนาบนเครือข่ายอินเตอร์เน็ต คือ PHP

PHP เป็นภาษาที่ใช้ในการพัฒนาโปรแกรมการทำงานบน Web (Web Programming หรือ Web Development) ที่มีประสิทธิภาพสูง เนื่องจากการใช้งานที่ง่ายและรวดเร็ว อีกทั้งยังสามารถเข้าถึงระบบฐานข้อมูลได้อีกหลายประเภทอีกด้วย

PHP เป็นภาษาจำพวก Scripting Language คำสั่งต่างๆจะเก็บอยู่ในไฟล์ที่เรียกว่า สคริปต์ (Script) และเวลาใช้งานต้องอาศัยตัวแปลชุดคำสั่ง PHP ได้รับการพัฒนาและออกแบบมา เพื่อใช้งานในการสร้างเอกสารแบบ HTML โดยสามารถ สอดแทรกหรือแก้ไขเนื้อหาได้โดยอัตโนมัติ ดังนั้นจึงกล่าวว่า PHP เป็นภาษาที่เรียกว่า Server-side หรือ HTML-Embedded Scripting Language

PHP เป็นผลงานที่เติบโตมาจากกลุ่มของนักพัฒนาในเชิงเปิดเผยรหัสต้นฉบับ หรือ OpenSource ดังนั้น PHP จึงมีการพัฒนาไปอย่างรวดเร็ว และแพร่หลายโดยเฉพาะอย่างยิ่งเมื่อใช้ร่วมกับ Apache Webserver ในปัจจุบัน PHP สามารถใช้ร่วมกับ Web Server หลายๆตัวบนระบบปฏิบัติการอย่างเช่น Windows 95/98/NT/XP เป็นต้น

3. เว็บเซิร์ฟเวอร์ ที่ใช้คือ WAMP5

WAMP Server ซึ่งภายในมี Apache 1.3.29, PHP5 RC2, MySQL 4.0.18, SQLitemanager, phpMyAdmin จุดเด่นของเว็บเซิร์ฟเวอร์เวอร์ชั้นนี้ก็คือใช้ intepreter PHP5.0 ซึ่งเป็นเวอร์ชั่นล่าสุด และฝังตัว SQLitemanager เป็นทูลในการจัดการ SQL ที่น่าใช้งานมาก ซึ่งเว็บเซิร์ฟเวอร์ตัวนี้นับเป็นเซิร์ฟเวอร์อีกตัวที่น่าใช้และสามารถนำมาแทนที่เซิร์ฟเวอร์อย่าง IIS ได้อย่างสบายเหมาะสำหรับท่านที่ใช้ Windows NT, Windows 2000 Server, Windows Server 2003 และตั้งเป็นเว็บเซิร์ฟเวอร์สำหรับใช้งานจริง หรือทำเป็นลักษณะ Intranet Site ใช้เฉพาะในองค์กร หรือท่านที่ต้องการจำลองเครื่องพีซีให้กลายเป็นเว็บเซิร์ฟเวอร์ เพื่อใช้ทดสอบในการเขียนสคริปต์ต่างๆ อาทิ HTML,PHP, Perl หรือใช้สร้างไซต์สำหรับองค์กรโดยใช้ CMS Tools อาทิ PostNuke, MD-Pro, PHP-Nuke, A- Tutor ก็สามารถทำได้ง่ายและรวดเร็ว

WAMP5 FULLL 0.5.2 (16 MB) ภายในมี

- Apache 1.3.29
- PHP5 RC2 PHP5 RC2
- SQLitemanager SQLitemanager
- MySQL 4.0.18
- Phpmyadmin

ส่วน Apache Webserver เป็นซอฟต์แวร์สำหรับให้บริการเว็บเซิร์ฟเวอร์เหมือนกันโดยผ่านทางโปรโตคอล HTTP โดยจะเป็นซอฟต์แวร์แบบ Open Source สามารถนำไปใช้งานได้โดยไม่มีค่าใช้จ่าย เนื่องจากกลุ่มอาสาสมัครจากโลกทั่วโลกได้ร่วมกันพัฒนามาเรื่อยๆจนเป็น

ในกรณีของ Apache เราสามารถใช้ PHP ได้สองรูปแบบคือ ในลักษณะของ CGI และ Apache Module ความแตกต่างอยู่ตรงที่ว่า ถ้าใช้ PHP เป็นแบบโมดูล PHP จะเป็นส่วนหนึ่งของ Apache หรือเป็นส่วนขยายในการทำงานนั่นเอง ซึ่งจะทำงานได้เร็วกว่าแบบที่เป็น CGI เพราะว่า ถ้าเป็น CGI แล้ว ตัวแปลชุดคำสั่งของ PHP ถือว่าเป็นแค่โปรแกรมภายนอก ซึ่ง Apache จะต้องเรียกขึ้นมาทำงานทุกครั้ง ที่ต้องการใช้ PHP ดังนั้น ถ้ามองในเรื่องของประสิทธิ ภาพในการทำงาน การใช้ PHP แบบที่เป็นโมดูลหนึ่งของ Apache จะทำงานได้มีประสิทธิภาพมากกว่า

4. ระบบฐานข้อมูลที่ใช้ในการจัดการ คือ MySQL

MySQL เป็น Database Server ที่เหมาะสมกับองค์กรขนาดกลางที่มีข้อมูลไม่มากนัก และเป็นระบบจัดการฐานข้อมูลเชิงสัมพันธ์ (Relational Database Management System) ซึ่งเป็นฟรีแวร์ทางด้านฐานข้อมูลจึงได้รับความนิยมอย่างมากในปัจจุบัน สามารถดาวน์โหลด Source Code ได้จากอินเตอร์เน็ตโดยไม่เสียค่าใช้จ่าย และสามารถแก้ไขได้ตามความต้องการ พร้อมทั้งยังสนับสนุนการใช้งานบนระบบปฏิบัติการ เช่น Unix , Mac และ Window นอกจากนี้ยังสามารถทำงานร่วมกับ Java , C , C++ , PHP , ASP ได้ แต่ก่อนที่จะใช้ PHP ร่วมกับ MySQL ซึ่งปัจจุบันนั้นสามารถรองรับการใช้งานของผู้ใช้หลายๆคน จึงต้องมีระบบรักษาความปลอดภัยโดยการกำหนดสิทธิให้กับผู้ที่จะมาใช้งาน MySQL ก่อน และยังสามารถนำคำสั่ง SQL มาใช้ทำงานกับ MySQL ได้ด้วย เนื่องจาก MySQL ได้รับพัฒนาตามข้อกำหนดมาตรฐาน SQL

5. ซอฟต์แวร์ที่ใช้ คือ OpenSSL

โครงการ OpenSSL เป็นความพยายามในการพัฒนาทูลคิดที่มีประสิทธิภาพเทียบเท่าผลิตภัณฑ์เชิงพาณิชย์ โดยมีการอิมพลีเมนต์โพรโตคอล SSL v2/v3 และ Transport Layer Security (TLS v1) รวมไปถึงไลบรารีระบบรหัสต่างๆ ซึ่งโครงการนี้ได้รับความร่วมมือจากอาสาสมัครทั่วโลกที่มาจากเครือข่ายอินเตอร์เน็ต ในการสื่อสารวางแผนและพัฒนา OpenSSL และเอกสารอื่นๆที่เกี่ยวข้องกับ OpenSSL มีพื้นฐานมาจากไลบรารี SSLeay ที่พัฒนาโดย Eric A. Young และ Tim J.Hudson มีการจดลิขสิทธิ์ภายใต้รูปแบบเดียวกับ Apache สามารถนำไปใช้ได้ทั้งในเชิงพาณิชย์และไม่ใช่เชิงพาณิชย์

บทที่ 4

การวิเคราะห์และออกแบบระบบการออกใบรับรองดิจิทัล

4.1 ขั้นที่ 1 : Problem Definition

เนื่องจากปัจจุบัน การส่งข้อมูลบนระบบเครือข่าย Internet หรือ Intranet ก็ตาม จะมีความปลอดภัยน้อย เนื่องจากจากอาจจะถูกผู้อื่นดักจับข้อมูล อ่าน และเปลี่ยนแปลงข้อมูลนั้นๆ ทำให้เกิดความเสียหายหากข้อมูลนั้นเป็นข้อมูลที่สำคัญ ทางผู้พัฒนาระบบจึงเห็นความสำคัญในจุดนี้ ศึกษาหาความรู้เกี่ยวกับหน่วยงานที่ทำหน้าที่ในการออกใบรับรองดิจิทัล (Certificate Authority) ซึ่งจะใช้ใบรับรองนั้นที่เปรียบเสมือนเป็น Public Key ช่วยในกระบวนการเข้ารหัส เพื่อส่งข้อมูลไปให้ผู้รับ ซึ่งทางผู้รับก็จะใช้ Private Key ช่วยในกระบวนการถอดรหัส แต่เนื่องมาจากระบบที่มีให้ทดลองใช้นั้นสามารถออกใบรับรองดิจิทัลได้อย่างเดียว ไม่สามารถให้ Private Key จึงไม่สามารถเข้าใจกระบวนการทำงานได้ครบ ทางผู้พัฒนาระบบจึงได้ทำการสร้างระบบการออกใบรับรองดิจิทัลขึ้นเพื่อเป็นกรณีศึกษา และทำการพัฒนาระบบในรูปแบบของ Open Source ก็สามารถนำไปพัฒนาต่อไปเพื่อให้เกิดประสิทธิภาพสูงสุด

จากการวิเคราะห์ความเป็นไปได้ในด้านต่างๆในการพัฒนาระบบ มีข้อสรุปด้าน Economical Feasibility, Technical Feasibility และ Operation Feasibility ดังนี้

Economical Feasibility : เนื่องจากระบบที่ทำหน้าที่ในการออกใบรับรองดิจิทัลส่วนใหญ่ที่มีนั้น จะต้องเสียค่าใช้จ่ายหากองค์กรใดจะนำเข้าใช้งานในองค์กร จึงถือว่าการสร้างระบบออกใบรับรองดิจิทัลขึ้นมาใช้เองนั้นจะช่วยลดค่าใช้จ่ายลงไปได้ และยังทำให้พนักงานหรือบุคคลที่อยู่ภายในองค์กรนั้นได้ตระหนักถึงความปลอดภัยในการส่งข้อมูลได้อีกด้วย

Technical Feasibility : ซอฟต์แวร์ที่ใช้คือ OpenSSL ซึ่งมีรูปแบบเป็น Open Source ที่สามารถหา Source Code มาช่วยในการพัฒนาระบบได้ง่าย รวมทั้งการใช้ WAMP5 มาทำหน้าที่เป็น Web Server สำเร็จรูปก็จะทำให้การพัฒนาระบบง่ายขึ้นด้วย

Operation Feasibility : ระบบนี้มีความปลอดภัยที่สูงเนื่องจากต้องผ่านถึง 2 ขั้นตอนที่ผู้ดูแลระบบต้องเข้ามาตรวจสอบผู้ที่ทำการสมัครสมาชิกว่าจะให้เข้าใช้งานหรือไม่ และกระบวนการร้องขอใบรับรองดิจิทัล ว่าจะออกใบรับรองดิจิทัลให้หรือไม่ รวมทั้งยังใช้ความสามารถของ ซอฟต์แวร์ OpenSSL ในการทำให้การติดต่อระหว่าง Server และ Client มีความปลอดภัย

4.2 ขั้นที่ 2 : Requirement Definition

จากการวิเคราะห์ความต้องการ สามารถสรุปเป็น Requirement Definition เป็นข้อๆ เพื่อการนำไปออกแบบระบบได้ดังนี้

1. ผู้ที่จะเข้าใช้ระบบจะต้องสมัครสมาชิกก่อน
2. สมาชิกและผู้ดูแลระบบสามารถเปลี่ยนแปลงรหัสผ่านของตัวเองที่เข้าใช้งานระบบได้
3. สมาชิกที่ต้องการใบรับรองดิจิทัลจะต้องกรอกรายละเอียดการร้องขอใบรับรองดิจิทัล และได้รับการตรวจสอบจากผู้ดูแลระบบก่อน จึงจะได้รับใบรับรองดิจิทัล
4. สมาชิดสามารถดาวน์โหลด Digital Certificate (Public Key) และ Private Key นำไปใช้งานได้ โดยใบรับรองแต่ละใบมีอายุการใช้งาน 1 ปี
5. ผู้ดูแลระบบมีอำนาจในการจัดการกับใบรับรองของสมาชิก โดยสามารถออกและเพิกถอนใบรับรองดิจัลได้

4.3 ขั้นที่ 3 : Design

หลังจากได้วิเคราะห์ความต้องการ และได้รายการความสามารถที่ระบบจะต้องมีแล้ว ในหัวข้อนี้จะกล่าวถึง การออกแบบระบบ ในการทำงานของการออกแบบระบบการออกใบรับรองดิจิทัลจะใช้ Use Case Diagram, Class Diagram, Sequence Diagram ใช้อธิบายทั้งภาพรวม คลาสที่ควรมี และการสื่อสารการทำงานร่วมกันระหว่างคลาสต่างๆ

4.3.1 Use Case Diagram

เป็นภาพที่แสดงความสัมพันธ์ของการทำงานโดยรวมของระบบ ซึ่งจะอธิบายว่าในระบบมีการดำเนินงานอะไรบ้าง โดยจะแสดงการติดต่อระหว่างระบบกับผู้ใช้ ซึ่งประกอบด้วย

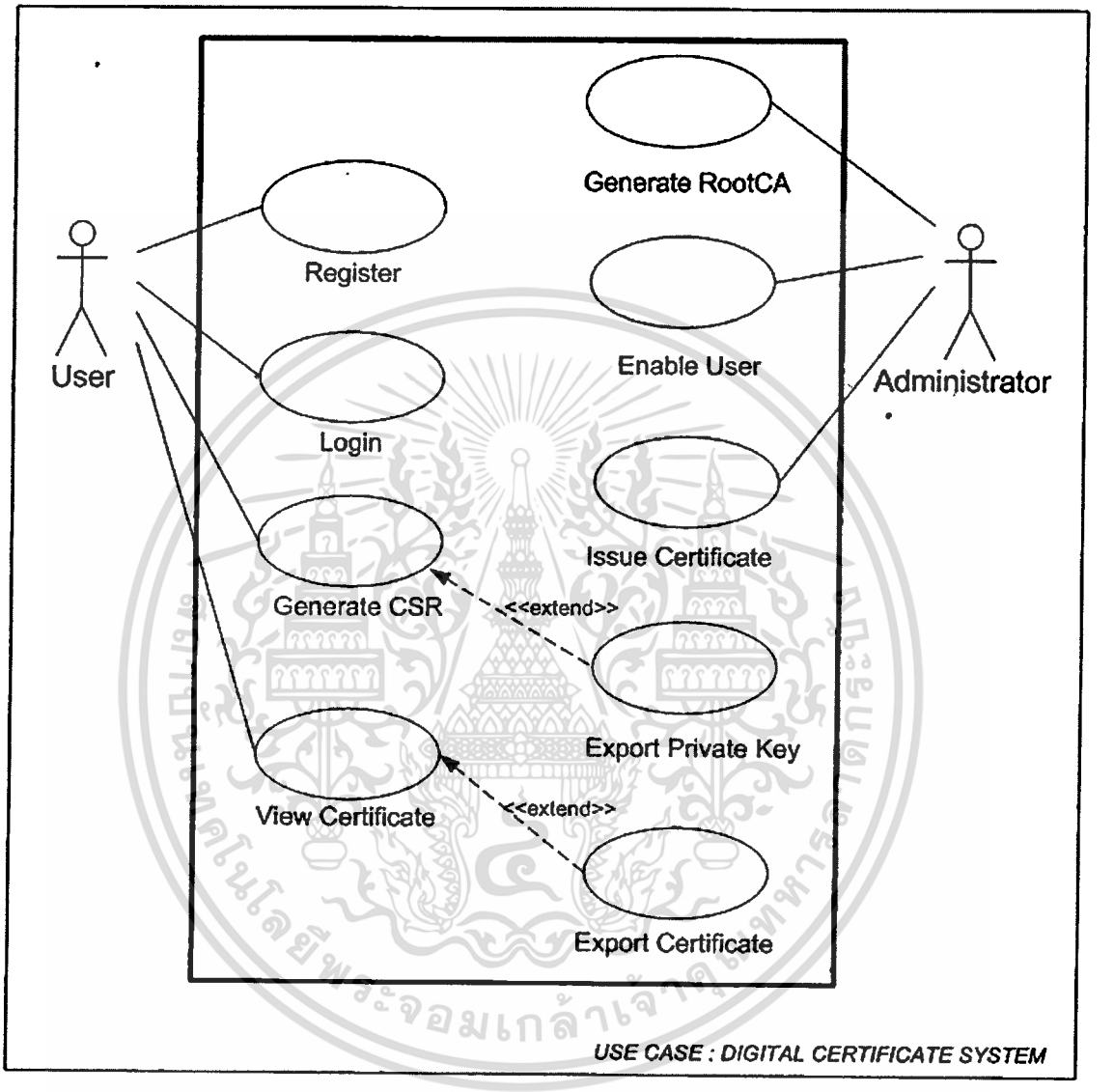
- **Actor** หมายถึง สิ่งใดๆก็ตามที่ใช้งานระบบหรือมีส่วนร่วมกับ Use Case ภายในระบบ โดยสิ่งดังกล่าวอาจเป็นคน อุปกรณ์ต่างๆหรือระบบอื่นๆ เป็นต้น โดย Actor จะมีการแลกเปลี่ยนข้อมูลข่าวสารกับระบบและมีสัญลักษณ์ที่ใช้คือ
- **Use Case** คือ กิจกรรมหลักๆที่เกิดขึ้นภายในระบบซึ่งอาจเป็นกิจกรรมระหว่างผู้ใช้กับระบบหรือระบบกับระบบ ซึ่งจะใช้รูปวงรีเป็นสัญลักษณ์ คือ
- **Relationship** เป็นการแสดงความสัมพันธ์แบบต่างๆ ระหว่าง Use Case กับ Use Case และ Use Case กับ Actor สำหรับความสัมพันธ์ระหว่าง Use Case สามารถแบ่งออกได้เป็นสองแบบ คือ

1. ความสัมพันธ์แบบขยาย (Extends Relationship) คือ Use case หนึ่งไปมีมีผลต่อการทำงานตามปกติของอีก Use case หนึ่ง นั่นหมายถึงว่า Use case ที่มาขยายมันจะมีผลทำให้การดำเนินการของ Use case ที่ถูกขยายมีการเปลี่ยนกิจกรรมไป สัญลักษณ์ที่ใช้คือ <<extends>> (เป็นเส้นประพร้อมหัวลูกศรที่ชี้จาก Use case ที่ขยายไปยัง Use case ที่ถูกขยาย โดยมีคำว่า <<extend>> กำกับอยู่บนเส้นลูกศร)
2. ความสัมพันธ์แบบใช้ (Uses Relationship) คือการที่ Use case หนึ่ง เรียกใช้งาน Use case อีกอันดับหนึ่ง คล้าย ๆ กับการเรียกใช้งานโปรแกรมย่อยโดยโปรแกรมหลัก สัญลักษณ์ที่ใช้คือ <<uses>> (ลูกศรหัวสามเหลี่ยมทึบชี้ไปยัง Use case ที่ถูกเรียกใช้งาน โดยมีคำว่า <<uses>> กำกับอยู่บนเส้นลูกศร)

ในการออกแบบระบบการออกใบรับรองดิจิทัลนี้ประกอบด้วย

- Actor ได้แก่
  1. ผู้ที่ต้องการเข้าใช้ระบบ จะทำการลงทะเบียน ทำการร้องขอใบรับรอง ดูใบรับรอง ดาวน์โหลด Digital Certificate (Public Key) และดาวน์โหลด Private Key
  2. ผู้ดูแลระบบ จะทำการตรวจสอบกรสมัครสมาชิก ทำการสร้าง RootCA และออกใบรับรองดิจิทัลให้แก่สมาชิก
- Use case ได้แก่
  1. Register : การลงทะเบียน
  2. Enable User : การกำหนดให้เข้าใช้งานระบบได้
  3. Login : การเข้าใช้งานระบบ
  4. Generate RootCA : ทำการสร้างรูทของผู้ออกใบรับรอง
  5. CSR (Certificate Signing Request) : การร้องขอใบรับรองดิจิทัล
  6. Issue Certificate :
  7. View Certificate : ดูใบรับรองดิจิทัล
  8. Export Private Key : ดาวน์โหลดกุญแจรหัสลับเก็บไว้
  9. Export Certificate : ดาวน์โหลดใบรับรองดิจิทัลเก็บไว้

จากข้อมูลข้างต้นสามารถเขียนเป็น Use Case Diagram ได้ดังรูปที่ 4.1



รูปที่ 4.1 Use Case Diagram ของระบบการออกใบรับรองดิจิทัล

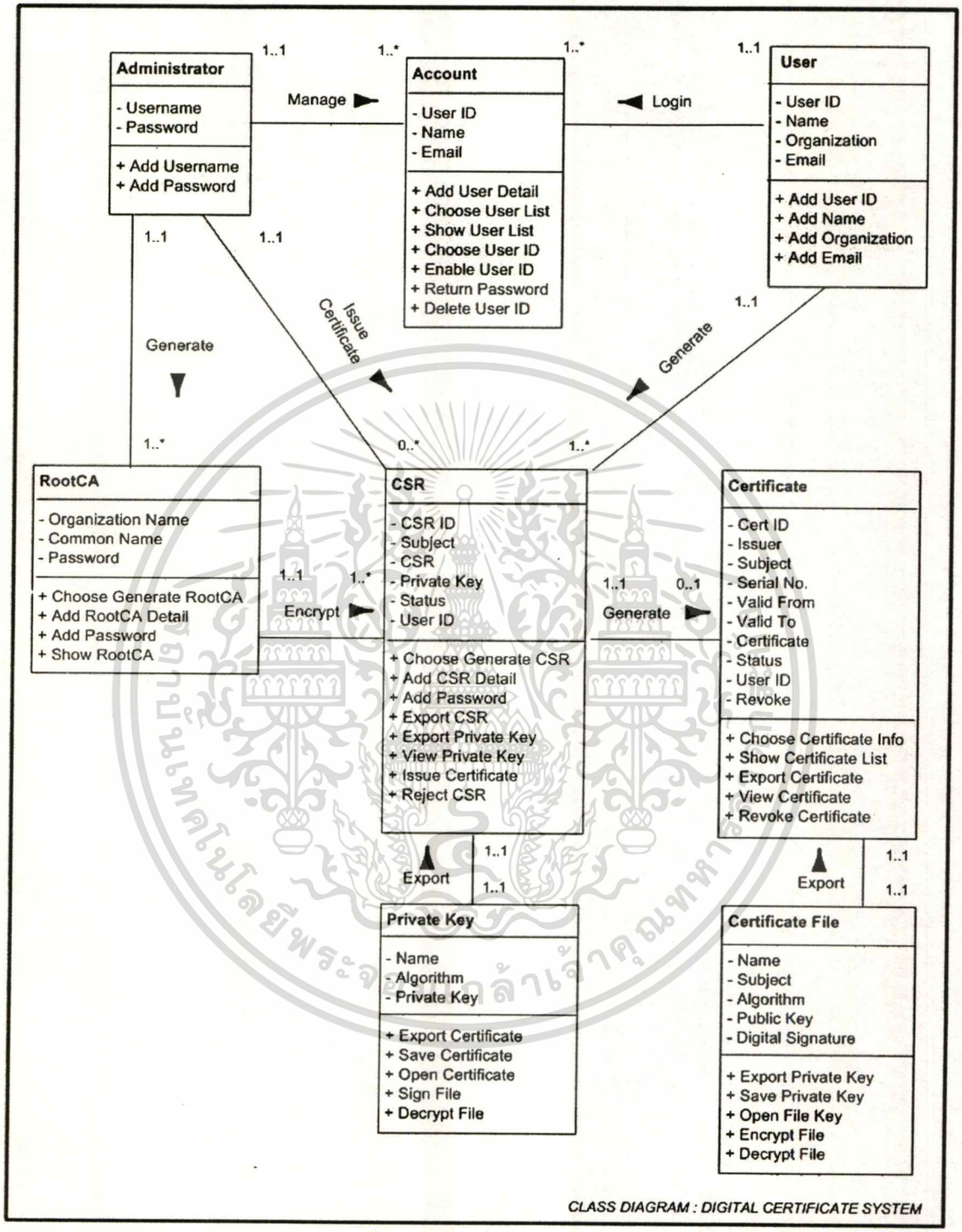
4.3.2 Class Diagram

ใช้แสดงคลาสและความสัมพันธ์ต่างๆระหว่างคลาส โดยคลาสใช้สัญลักษณ์เป็นสี่เหลี่ยมผืนผ้าภายในแบ่งเป็น 3 ส่วนคือ ชื่อคลาส (Name) คุณลักษณะ (Property) และพฤติกรรม (Method) เรียงจากบนลงล่างตามลำดับ และสามารถเขียน Class ที่เกี่ยวข้องจากขั้นตอนการทำงานของ Use Case ดังตารางที่ 4.1

ตารางที่ 4.1 Class ที่เกี่ยวข้องกับ Use case

Use Case	Class ที่เกี่ยวข้อง
Register	User, Account
Enable User	Administrator, Account
Login	User, Account
Generate RootCA	Administrator, RootCA
CSR (Certificate Signing Request)	User, CSR, PrivateKey
Issue Certificate	Administrator, CSR, Certificate
View Certificate	User, Certificate
Export Private Key	User, CSR, Private Key
Export Certtificate File	User, Certificate, Certificate File

จากข้อมูลข้างต้นสามารถเขียนเป็น Class Diagram โดยการทำงานเริ่มที่ผู้ใช้งานระบบจะทำการเข้าใช้งานระบบด้วยการสร้างใบร้องขอใบรับรองดิจิทัล หลังจากนั้นทางผู้ดูแลระบบจะทำการตรวจสอบการร้องขอและทำการออกใบรับรอง แล้วทางผู้ใช้งานระบบถึงจะสามารถโหลดกุญแจสาธารณะและกุญแจส่วนตัวได้ ดังรูปที่ 4.2



รูปที่ 4.2 Class Diagram ของระบบออกใบรับรองดิจิทัล

แต่ละคลาส มีรายละเอียดดังต่อไปนี้

คลาส Account เป็นคลาสที่เกี่ยวกับข้อมูลของผู้ที่มาลงทะเบียนเป็นสมาชิกเพื่อเข้าใช้งานระบบ โดยผู้ดูแลระบบจะเป็นผู้ตรวจสอบว่ายินยอมให้เข้าใช้งานระบบหรือไม่หรือจะลบทิ้งออกไปจากระบบดังตารางที่ 4.2

ตารางที่ 4.2 เมธอดของคลาส Account

เมธอด	หน้าที่
Add User Detail	กรอกข้อมูลของผู้ที่เข้ามาลงทะเบียน
Choose User List	เลือกข้อมูลของผู้ที่เข้ามาลงทะเบียนเก็บในฐานข้อมูล
Show User List	แสดงข้อมูลของผู้ที่เข้ามาลงทะเบียน
Choose User ID	เลือกข้อมูลของผู้ที่เข้ามาลงทะเบียนจากรหัสผู้เข้าใช้งาน
Enable User ID	ยินยอมให้เข้าใช้งานระบบได้
Return Password	ส่งรหัสเพื่อใช้เข้าระบบกลับทางอีเมล์
Delete User ID	ไม่ยินยอมให้เข้าใช้งานระบบได้และลบข้อมูลนั้นทิ้ง

คลาส RootCA เป็นคลาสที่เกี่ยวกับการสร้าง Root ของหน่อยงานที่ออกใบรับรอง โดยผู้ที่ดูแลระบบจะจัดการในส่วนนี้ดังตารางที่ 4.3

ตารางที่ 4.3 เมธอดของคลาส RootCA

เมธอด	หน้าที่
Choose Generate RootCA	เลือกการทำงานในส่วนของการสร้าง Root ของหน่อยงานที่ออกใบรับรอง
Add RootCA Detail	กรอกรายละเอียดของของการสร้าง
Add Password	กรอกรหัสผ่านที่ต้องการใช้ในกระบวนการของ Private Key
Show RootCA	แสดงรายละเอียดของการสร้าง RootCA

คลาส CSR เป็นคลาสที่เกี่ยวกับการขอใบรับรองดิจิทัล โดยสมาชิกผู้ต้องการขอใบรับรองจะต้องกรอกรายละเอียด จนได้ Private Key ออกมา และในขั้นตอนสุดท้ายผู้ดูแลระบบจะเป็นผู้ที่ทำหน้าที่ออกใบรับรองให้ดังตารางที่ 4.4

ตารางที่ 4.4 เมธอดของคลาส CSR

เมธอด	หน้าที่
Choose Generate CSR	เลือกการทำงานในส่วนของการขอใบรับรองดิจิทัล
Add CSR Detail	กรอกรายละเอียดของของการขอใบรับรองดิจิทัล
Add Password	กรอกรหัสผ่านที่ต้องการใช้ในกระบวนการของ Private Key
CSR has been generate	แสดงข้อความว่า CSR ได้ถูกสร้างแล้ว
Export CSR	ดาวน์โหลดข้อมูลการขอใบรับรองดิจิทัลไปเก็บไว้ในเครื่อง
Export Private Key	ดาวน์โหลดกุญแจส่วนตัวไปเก็บไว้ในเครื่อง
View Private Key	แสดงข้อมูลกุญแจส่วนตัว
Issue Certificate	ผู้ดูแลระบบทำการออกใบรับรองดิจิทัลให้แก่สมาชิกที่ทำการขอ
Reject CSR	ยกเลิกการขอใบรับรองดิจิทัล

คลาส Certificate เป็นคลาสที่เกี่ยวกับใบรับรองดิจิทัลของสมาชิก ซึ่งจะแสดงรายละเอียดต่างๆของใบรับรองดิจิทัลดังตารางที่ 4.5

ตารางที่ 4.5 เมธอดของคลาส Certificate

เมธอด	หน้าที่
Choose Certificate	เลือกการทำงานในส่วนของใบรับรองดิจิทัล
Show Certificate List	แสดงข้อมูลของใบรับรองดิจิทัล
Export Certificate	ดาวน์โหลดใบรับรองดิจิทัลไปเก็บไว้ในเครื่อง
View Certificate	แสดงข้อมูลใบรับรองดิจิทัล
Revoke Certificate	ยกเลิกการใช้งานใบรับรองดิจิทัลนี้

คลาส Private Key เป็นคลาสที่เกี่ยวกับกุญแจส่วนตัวที่อยู่ในเครื่องสมาชิกดังตารางที่ 4.6

ตารางที่ 4.6 เมธอดของคลาส Private Key

เมธอด	หน้าที่
Export Private Key	ดาวน์โหลดกุญแจส่วนตัว
Save Private Key	ทำการเก็บกุญแจส่วนตัวไว้ในเครื่อง
Open File Key	เปิดข้อมูลกุญแจส่วนตัว
Sign File	ใช้ทำการเข้ารหัสข้อมูลที่ถูกส่งไปเพื่อพิสูจน์ตัวตน

คลาส Certificate File เป็นคลาสที่เกี่ยวกับใบรับรองดิจิทัล ซึ่งมีกุญแจสาธารณะอยู่ภายในโดยจะต้องเผยแพร่ให้กับผู้อื่นดังตารางที่ 4.7

ตารางที่ 4.7 เมธอดของคลาส Certificate (Public Key)

เมธอด	หน้าที่
Export Certificate	ดาวน์โหลดใบรับรองดิจิทัล
Save Certificate	ทำการเก็บใบรับรองดิจิทัลไว้ในเครื่อง
Open Certificate	เปิดข้อมูลใบรับรองดิจิทัล
Encrypt File	ใช้ทำการเข้ารหัสข้อมูลที่จะส่งไป
Decrypt File	ใช้ทำการถอดรหัสข้อมูลที่ถูกส่งมา

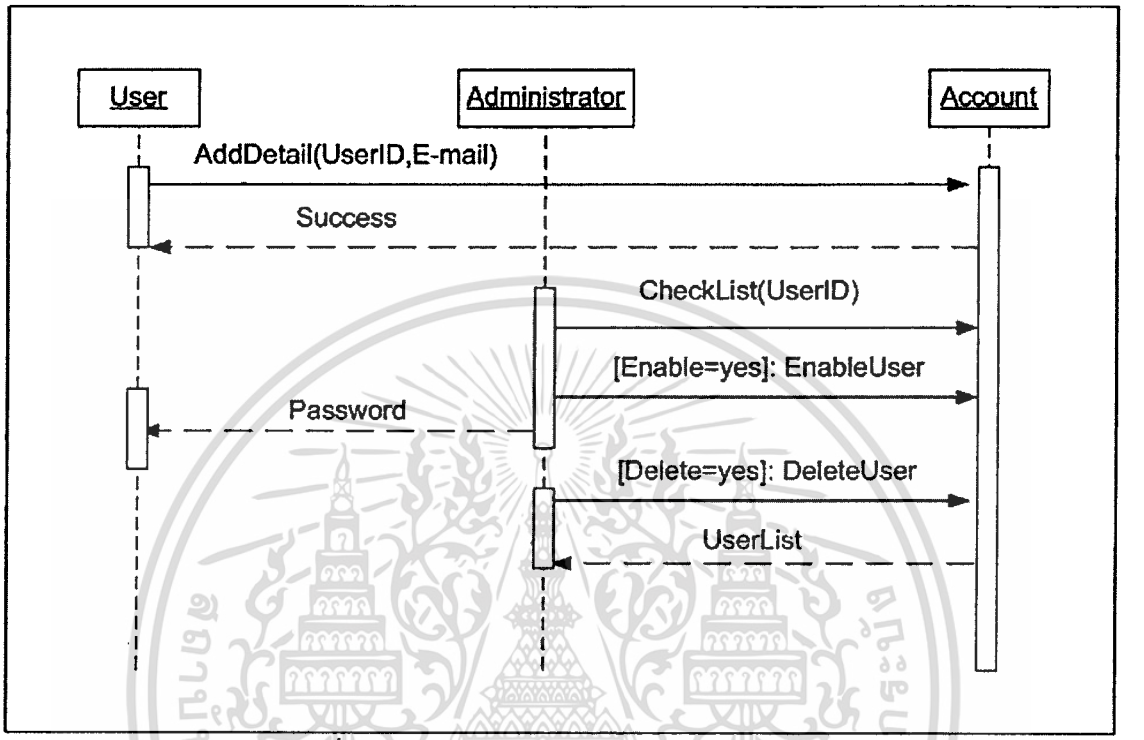
4.3.3 Sequence Diagram

เป็นไดอะแกรมที่ใช้แสดงถึงปฏิสัมพันธ์ Interaction ระหว่างวัตถุในระบบที่มีลำดับการเกิดกิจกรรมก่อน-หลังในช่วงระยะเวลาหนึ่ง

Sequence Diagram จะมีแกนสมมติอยู่ 2 แกน คือ แกนนอนและแกนตั้ง แกนนอนจะแสดงขั้นตอนของการทำงาน หรือการส่งข้อมูลระหว่างวัตถุ โดยแต่ละวัตถุจะส่งข้อมูลถึงกันว่าต้องทำอะไรเมื่อใด ส่วนแกนตั้งเป็นแกนเวลา แกนนอนและแกนตั้งต้องสัมพันธ์กัน สัญลักษณ์ใน Sequence Diagram ประกอบไปด้วย

- วัตถุหรือคลาส (Class) แทนด้วยรูปสี่เหลี่ยมผืนผ้าเรียงกันตามแนวนอน ภายในมีเครื่องหมายโคล่อนและตามด้วยชื่อวัตถุหรือคลาส
- เส้นแสดงเวลา(Lifelines) เป็นเส้นประที่อยู่ในแนวแกนตั้งซึ่งแสดงลำดับเวลา
- สี่เหลี่ยมใสในแนวตั้ง ที่วางบนเส้นแสดงเวลา เรียกว่า Activation ซึ่งแสดงช่วงเวลาที่วัตถุกำลังปฏิบัติงาน
- เส้นตรงมีหัวลูกศรสีดำทึบในแนวนอน แสดงถึงกิจกรรมที่เกิดขึ้น จากคลาสหรือวัตถุในไดอะแกรม
- ข้อความ (Message) เป็นเส้นประในแนวแกนนอนแสดงถึงกรณีที่มีการส่งข้อมูลระหว่างคลาส หรือวัตถุ

4.3.3.1 Sequence Diagram ของการลงทะเบียน

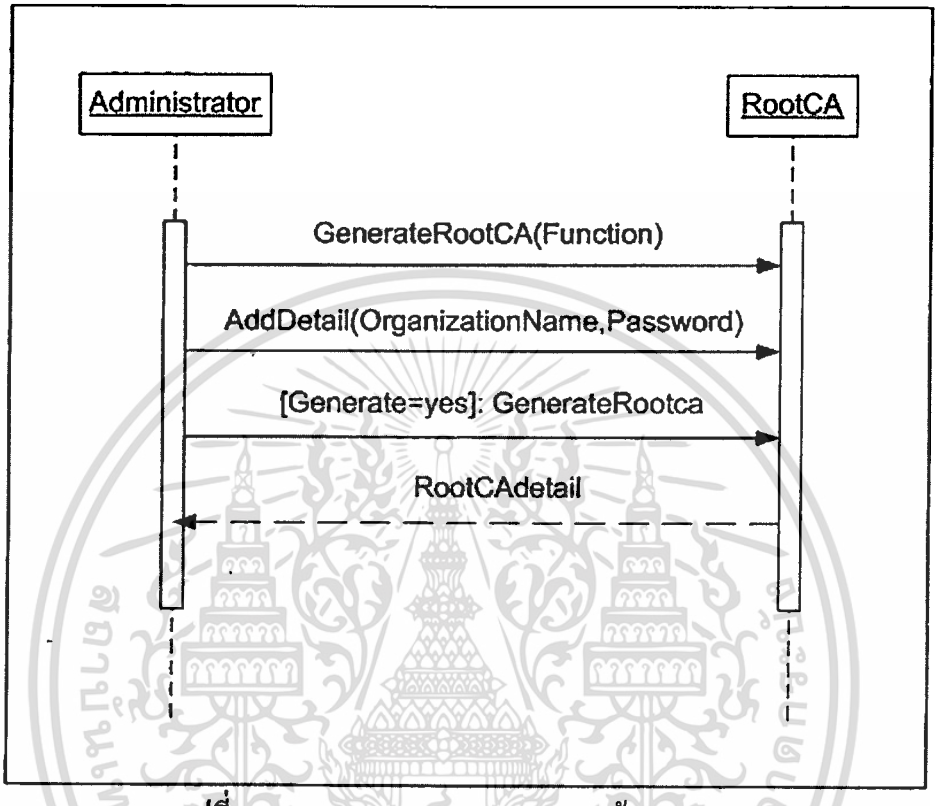


รูปที่ 4.3 Sequence Diagram ของการลงทะเบียน

ขั้นตอนการทำงานของการลงทะเบียน

1. เริ่มจากผู้ใช้งานระบบทำการลงทะเบียนเพื่อเข้าใช้งานระบบโดยการกรอกรายละเอียดของผู้ใช้งานแล้วทางระบบจะส่งข้อความกลับแสดงการลงทะเบียนสำเร็จแล้ว
2. ผู้ใช้งานระบบจะยังไม่สามารถทำการเข้าใช้งานระบบได้ทันที แต่จะต้องให้ผู้ดูแลระบบทำการอนุญาตก่อนโดยผู้ดูแลระบบจะทำการตรวจสอบการเข้ามาลงทะเบียนจากรหัสของผู้เข้ามาใช้งานระบบว่ามีใครทำการลงทะเบียนใหม่บ้าง และจะทำการยินยอมให้เข้าใช้งานระบบได้หรือจะสามารถลบข้อมูลการลงทะเบียนนั้นทิ้งได้
3. เมื่อการลงทะเบียนของผู้ใช้งานระบบถูกยอมรับให้เข้าใช้งานได้ ระบบจะส่งรหัสผ่านในการเข้าใช้งานระบบผ่านทางอีเมล์และทางผู้ใช้งานระบบก็สามารถเข้าใช้งานได้ทันที

4.3.3.2 Sequence Diagram ของการสร้าง RootCA

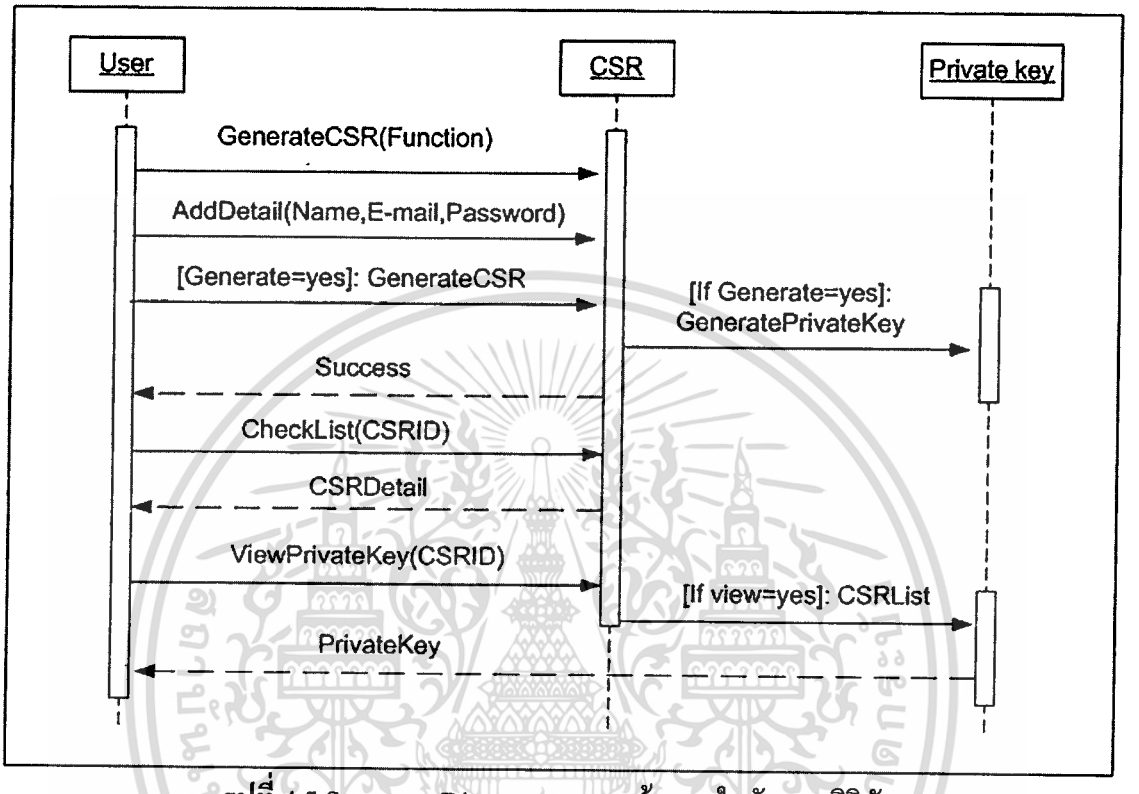


รูปที่ 4.4 Sequence Diagram ของการสร้าง RootCA

ขั้นตอนการทำงานของการสร้าง RootCA

1. เริ่มจากผู้ดูแลระบบจะทำการสร้าง RootCA โดยจะทำการเข้าใช้งานในส่วนของการสร้าง RootCA ซึ่งทางผู้ดูแลระบบสามารถเข้าใช้งานได้เพียงผู้เดียว
2. ผู้ดูแลระบบทำการกรอกรายละเอียดต่างๆของ RootCA แล้วทำการกดปุ่มในส่วนของการสร้าง
3. เมื่อทำการสร้าง RootCA สำเร็จระบบจะทำการแสดงรายละเอียดของ RootCA ให้ผู้ดูแลระบบได้รับ

4.3.3.3 Sequence Diagram ของการร้องขอใบรับรองดิจิทัล

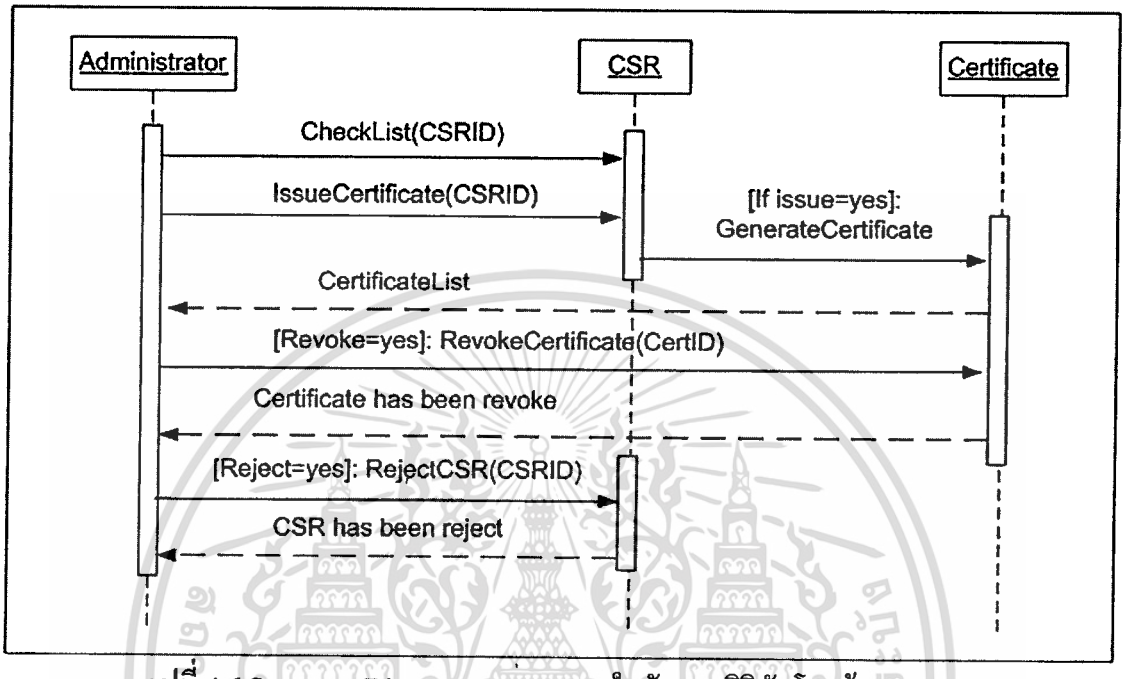


รูปที่ 4.5 Sequence Diagram ของการร้องขอใบรับรองดิจิทัล

ขั้นตอนการทำงานของการร้องขอใบรับรองดิจิทัล

1. เริ่มจากผู้เข้าใช้งานระบบ ทำการเข้าใช้งานในส่วนของการร้องขอใบรับรองดิจิทัล
2. ผู้ใช้งานระบบทำการกรอกรายระเอียดต่างๆ ของใบรับรองดิจิทัล และกำหนดรหัสที่จะใช้กับกุญแจส่วนตัวโดยจะต้องจำให้ได้เพราะจะต้องทำการใส่รหัสผ่านนี้ตอนใช้งานกุญแจส่วนตัว แล้วจึงกดปุ่มสร้างการร้องขอใบรับรองดิจิทัล
3. ระบบจะทำการสร้างกุญแจส่วนตัวให้กับผู้ใช้ระบบ และส่งข้อความกลับว่าใบร้องขอใบรับรองดิจิทัลได้ถูกสร้างแล้ว โดยจะปรากฏตามรหัสของการร้องขอใบรับรองซึ่งผู้ใช้งานระบบจะสามารถเห็นของตัวเองเท่านั้นและยังสามารถทำการลบการร้องขอนี้ได้หรือจะดูกุญแจส่วนตัวของตนเองได้ด้วย
4. เนื่องด้วยเมื่อทำการร้องขอใบรับรองดิจิทัลแล้วจะยังไม่ได้รับใบรับรองดิจิทัลในทันทีต้องให้ผู้ดูแลระบบทำการตรวจสอบก่อนและจะทำการออกใบรับรองดิจิทัลให้ผู้ใช้งานระบบได้ต่อไป

4.3.3.4 Sequence Diagram ของการออกใบรับรองดิจิทัลโดยผู้ดูแลระบบ

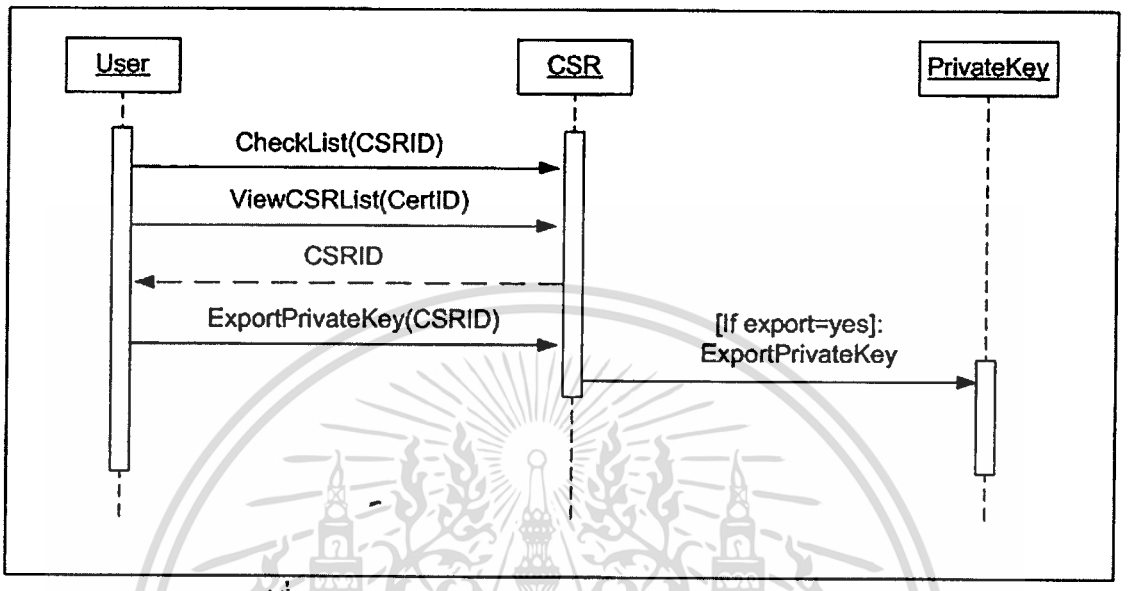


รูปที่ 4.6 Sequence Diagram ของการออกใบรับรองดิจิทัลโดยผู้ดูแลระบบ

ขั้นตอนการทำงานของการออกใบรับรองดิจิทัลโดยผู้ดูแลระบบ

1. เริ่มจากผู้ดูแลระบบทำการเข้าใช้งานในส่วนของรายการการร้องขอใบรับรองดิจิทัลจากรหัสการร้องขอใบรับรองดิจิทัล
2. ทำการตรวจสอบข้อมูลการร้องขอใบรับรองดิจิทัลของผู้ใช้งานระบบและทำการออกใบรับรองดิจิทัลให้กับผู้ใช้งานระบบ โดยจะทำการสร้างใบรับรองดิจิทัลไปไว้ในส่วนของใบรับรองดิจิทัล
3. ระบบจะแสดงรายการใบรับรองดิจิทัลตามรหัสของใบรับรองดิจิทัล
4. ผู้ดูแลระบบสามารถทำการยกเลิกใบรับรองดิจิทัลนั้นได้โดยเมื่อทำการยกเลิกการใช้งานใบรับรองดิจิทัลนั้น ระบบจะส่งข้อความกลับมาว่า ใบรับรองดิจิทัลได้ถูกยกเลิกแล้ว
5. หรือทางผู้ดูแลระบบสามารถทำการลบการร้องขอใบรับรองดิจิทัลได้ด้วย โดยระบบจะส่งข้อความกลับมาว่า การร้องขอใบรับรองดิจิทัลได้ถูกยกเลิกแล้ว

4.3.3.5 Sequence Diagram ของการโหลดกุญแจส่วนตัว

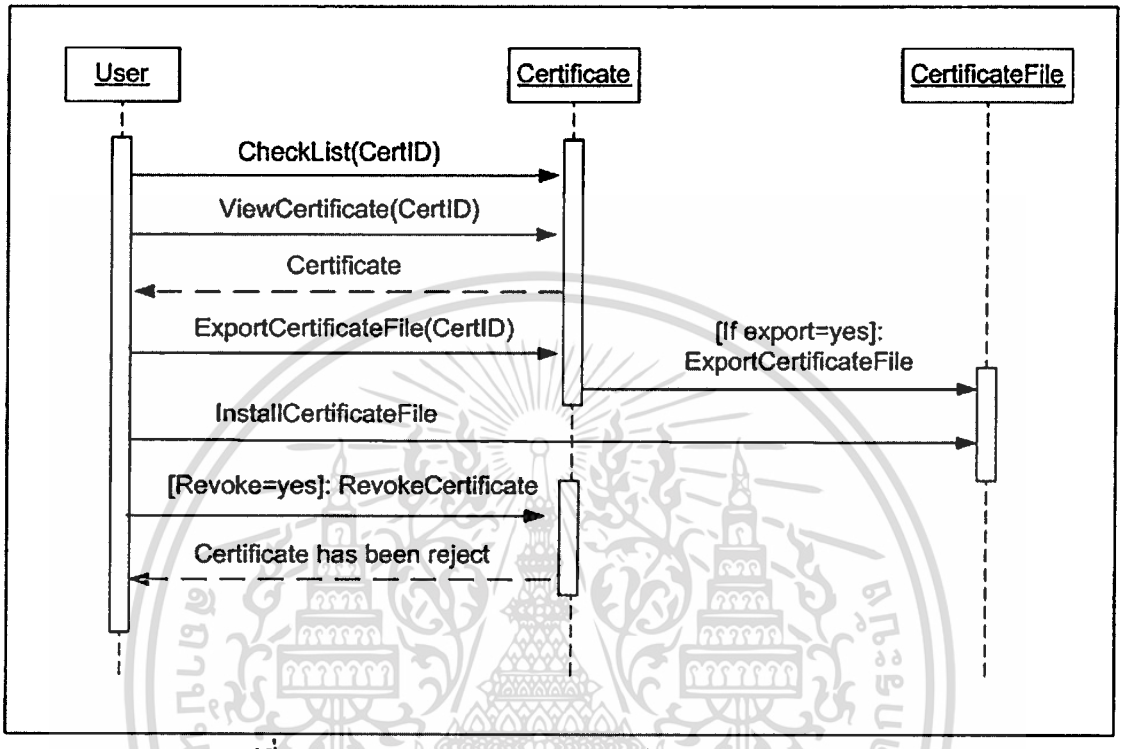


รูปที่ 4.7 Sequence Diagram ของการโหลดกุญแจส่วนตัว

ขั้นตอนการทำงานของการโหลดกุญแจส่วนตัว

1. เริ่มจากผู้เข้าใช้ระบบทำการใช้งานในส่วนของรายการการร้องขอใบรับรองดิจิทัลของตนเองตามรหัสการร้องขอใบรับรองดิจิทัล
2. ระบบจะแสดงข้อมูลการร้องขอใบรับรองดิจิทัล แล้วผู้ใช้งานระบบจะทำการโหลดกุญแจส่วนตัวไปเก็บไว้ในเครื่องของตนเองและต้องเก็บเป็นความลับ
3. ระบบจะแสดงส่วนของการเก็บกุญแจส่วนตัว ว่าจะใช้ชื่ออะไรและเก็บไว้ที่ใด

4.3.3.7 Sequence Diagram ของโหลดกุญแจสาธารณะ

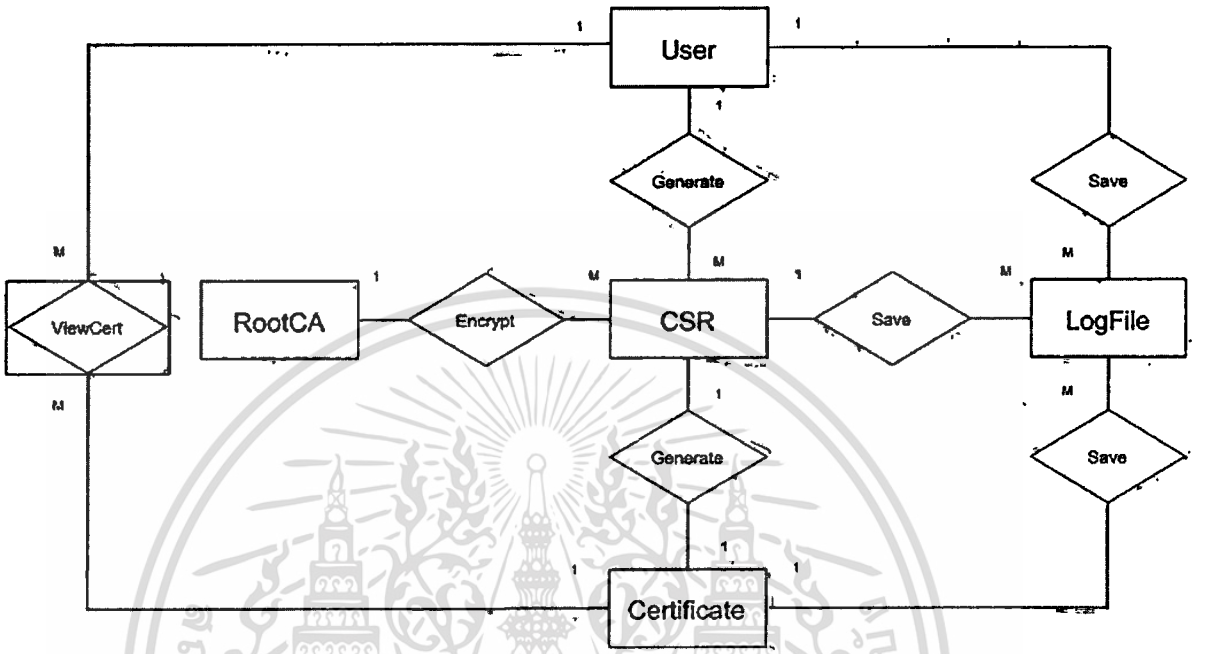


รูปที่ 4.8 Sequence Diagram ของการโหลดกุญแจสาธารณะ

ขั้นตอนการทำงานของการโหลดใบรับรองดิจิทัล

1. เริ่มจากผู้เข้าใช้ระบบทำการใช้งานในส่วนของรายการใบรับรองดิจิทัลของตนเองตามรหัสของใบรับรองดิจิทัล
2. ระบบจะแสดงข้อมูลของใบรับรองดิจิทัล แล้วผู้ใช้งานระบบจะทำการโหลดใบรับรองดิจิทัล ไปเก็บไว้ในเครื่องของตนเองและสามารถทำการเผยแพร่ให้กับผู้อื่นได้
3. ระบบจะแสดงส่วนของการเก็บใบรับรองดิจิทัล ว่าจะใช้ชื่ออะไรและเก็บไว้ที่ใด
4. ทำการติดตั้งใบรับรองดิจิทัลไว้ในเครื่องของตนเอง
5. ผู้เข้าใช้ระบบสามารถทำการยกเลิกใบรับรองดิจิทัลของตนเองได้ เมื่อทำการยกเลิกแล้ว ระบบจะส่งข้อความกลับมาว่า ใบรับรองดิจิทัลได้ถูกยกเลิกแล้ว

E-R Model ของระบบการออกใบรับรองดิจิทัล



รูปที่ 4.9 E-R Model ของระบบการออกใบรับรองดิจิทัล

Data Dictionary พจนานุกรมข้อมูล

รายละเอียดในพจนานุกรมข้อมูล (Data Dictionary) ซึ่งเป็นที่เก็บรวบรวมรายละเอียดของข้อมูลทั้งหมดที่เกี่ยวกับระบบแสดงได้ดังนี้

ตารางที่ 4.8 พจนานุกรมข้อมูลของตาราง User

Attibute	Descriptions	Data Type	Required	Key	Ref. Table
uid	รหัสของผู้ใช้งาน	int(11)	Y	PK	
name	ชื่อของผู้ที่จะเข้าใช้ระบบ	char(20)	Y		
passwd	รหัสผ่านของผู้ใช้งาน	char(50)	N		
name	ชื่อของผู้ใช้งาน	char(40)	Y		
email	ชื่อ E-mail ของผู้ใช้งาน	char(50)	Y		
lastlogin	วันและเวลาล่าสุดที่ใช้งาน	datetime	N		
lastip	รหัสเครื่องที่เข้าใช้งาน	char(15)	N		
logincnt	จำนวนครั้งที่เข้าใช้งาน	int(11)	N		
rdate	วันและเวลาของการทำงาน	datetime	N		
org	ชื่อหน่วยงานของผู้ใช้งาน	char(80)	Y		
valid	สถานะของการใช้งาน	char(1)	N		

ตารางที่ 4.9 พจนานุกรมข้อมูลของตาราง CSR

Attibute	Descriptions	Data Type	Required	Key	Ref. Table
csrid	รหัสการขอใบรับรอง	int(11)	Y	PK	
csr_info	ข้อมูลการขอใบรับรอง	text	Y		
privatekey	กุญแจส่วนตัว	text	Y		
subject	เจ้าของการขอใบรับรอง	varchar(255)	Y	FK	User
status	สถานะ	varchar(30)	N		
rdate	วันและเวลาของการทำงาน	datetime	N		
rootcahash	รหัสลับที่ใช้ออกใบรับรอง	varchar(255)	N	FK	RootCA

ตารางที่ 4.10 พจนานุกรมข้อมูลของตาราง Certificate

Attibute	Descriptions	Data Type	Required	Key	Ref. Table
certid	รหัสใบรับรอง	int(11)	Y	PK	
certificate_info	ข้อมูลของใบรับรอง	text	N		
issuer	ผู้ออกใบรับรอง	varchar(255)	N		
subject	เจ้าของใบรับรอง	varchar(255)	N		
d_not_before	วันที่ออกใบรับรอง	datetime	N		
d_not_after	วันที่หมดอายุใบรับรอง	datetime	N		
csrid	รหัสการขอใบรับรอง	int(11)	N	FK	CSR
status	สถานะของใบรับรอง	varchar(30)	N		

ตารางที่ 4.11 พจนานุกรมข้อมูลของตาราง RootCA

Attibute	Descriptions	Data Type	Required	Key	Ref. Table
rootcahash	รหัสลับที่ใช้ออกใบรับรอง	char(255)	Y	PK	
serial	จำนวนครั้งที่ใช้งานรหัสลับ	int(11)	N		

ตารางที่ 4.12 พจนานุกรมข้อมูลของตาราง ViewCert

Attibute	Descriptions	Data Type	Required	Key	Ref. Table
uid	รหัสของผู้ใช้งาน	int(11)	Y	PK,FK	User
certid	รหัสใบรับรอง	int(11)	Y	PK,FK	Certificate

ตารางที่ 4.13 พจนานุกรมข้อมูลของตาราง Logfile

Attibute	Descriptions	Data Type	Required	Key	Ref. Table
logid	รหัสการบันทึกรายการ	int(11)	Y	PK	
logmsg	ข้อมูลการบันทึกรายการ	char(255)	N		
rdate	วันและเวลาของการทำงาน	datetime	N		
uid	รหัสของผู้ใช้งาน	int(11)	Y	FK	User
csrid	รหัสการขอใบรับรอง	int(11)	Y	FK	CSR
certid	รหัสใบรับรอง	int(11)	Y	FK	Certificate

บทที่ 5

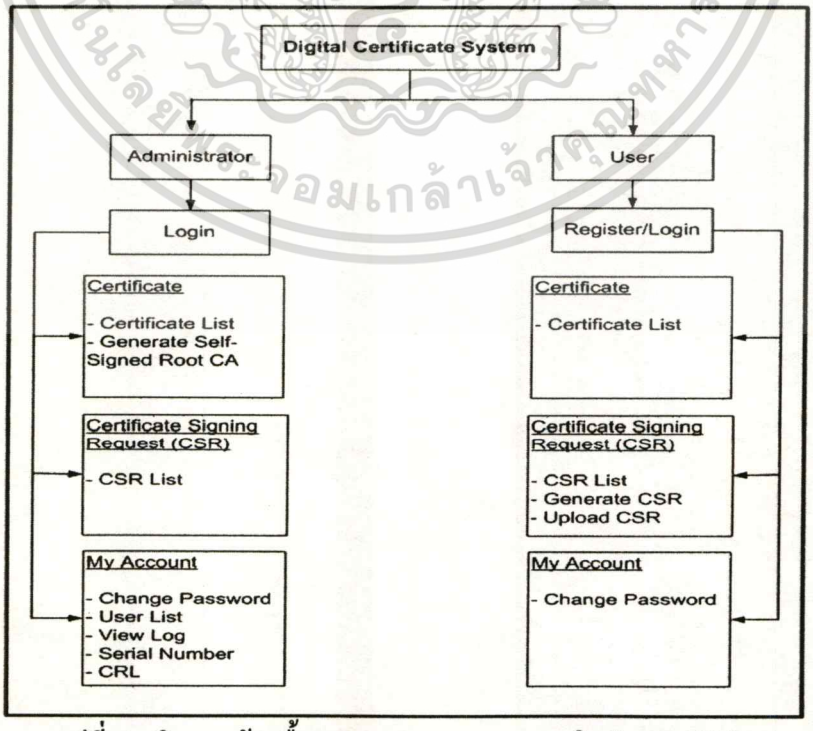
การพัฒนาระบบการออกใบรับรองดิจิทัล

5.1 ซอฟต์แวร์และข้อมูลต่างๆสำหรับการพัฒนาระบบการออกใบรับรองดิจิทัล

- Operation System ใช้ Window XP โดยจะแบ่งออกเป็น 2 Partition ได้แก่ C:\ เพื่อทำการติดตั้ง WebServer และ D:\ เพื่อเก็บข้อมูลของ WebPage ต่างๆของระบบ
- WebServer ทำการติดตั้ง WAMP5 บนไดเรกทรอรีที่มีชื่อว่า Server ใน C:\
- Software ที่ใช้ออกใบรับรองดิจิทัล ใช้ Win32OpenSSL บนไดเรกทรอรี่ที่มีชื่อว่า Server ใน C:\
- ข้อมูลต่างๆของระบบ จะอยู่ในไดเรกทรอรีที่มีชื่อว่า wwwroot ใน D:\

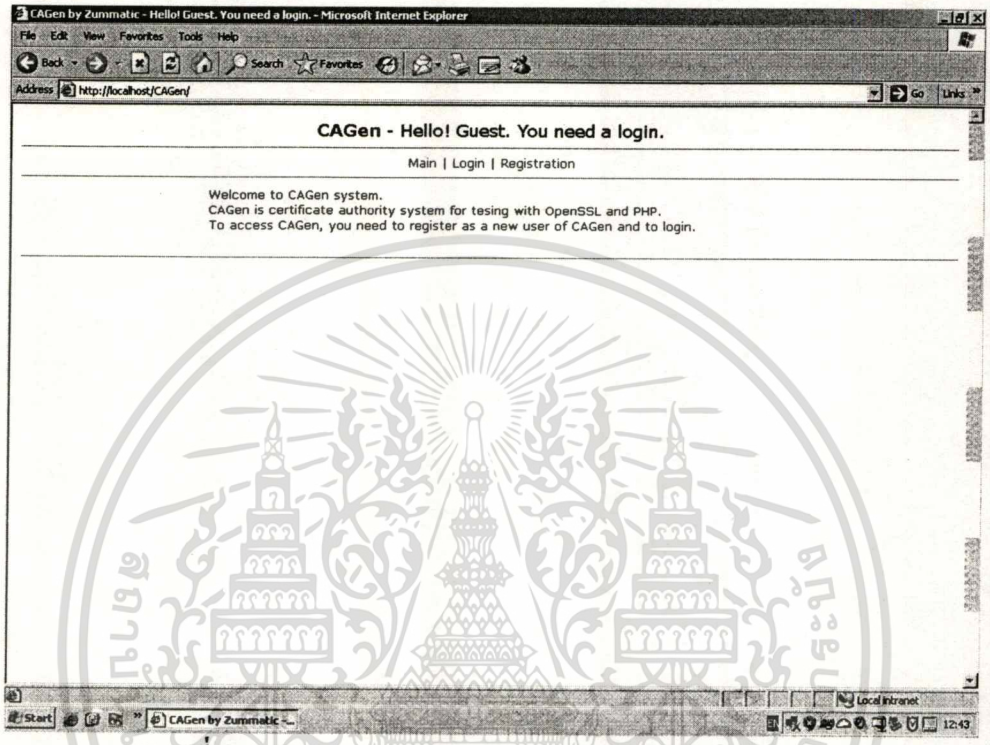
5.2 โครงสร้างการทำงานของระบบการออกใบรับรองดิจิทัล

เนื่องจาก ระบบการออกใบรับรองดิจิทัล มีรูปแบบของการทำงานเป็น WebPage ซึ่งมีโครงสร้างพื้นฐานดังรูปที่ 5.1



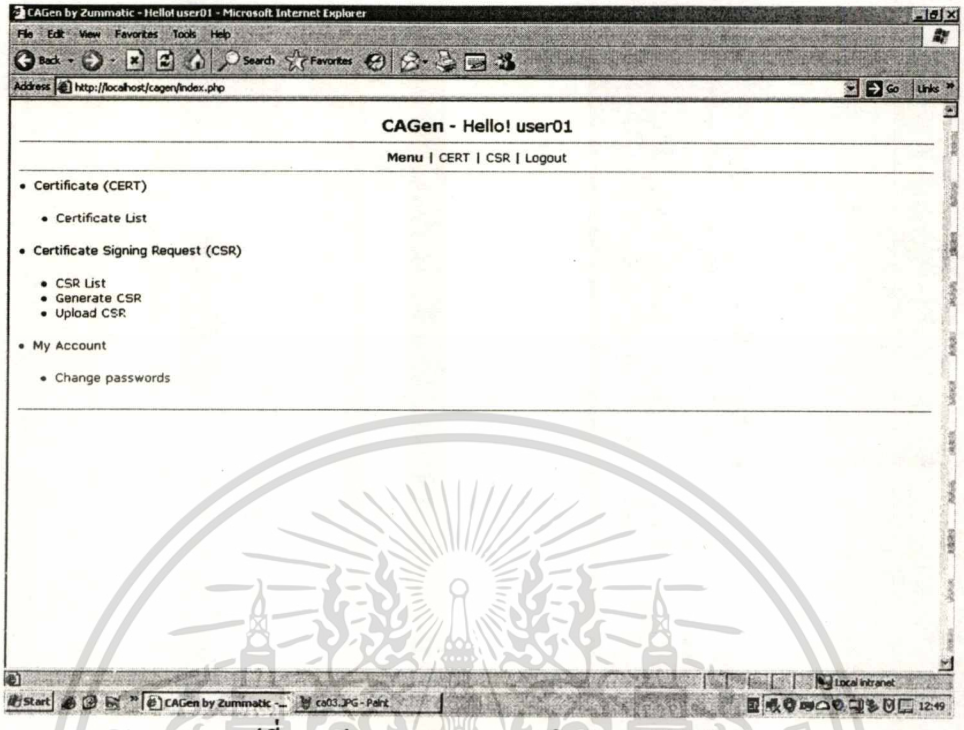
รูปที่ 5.1 โครงสร้างพื้นฐานของระบบการออกใบรับรองดิจิทัล

- Phase 1 คือส่วนของการ Login และส่วนขอการ Registration ซึ่งส่วนของการ Login จะมีผู้ที่เข้าใช้งานได้แก่ Administrator และ User โดยที่ User จะต้องทำการ Register ก่อนดังรูปที่ 5.2



รูปที่ 5.2 ส่วนของการ Login และส่วนของการ Registration

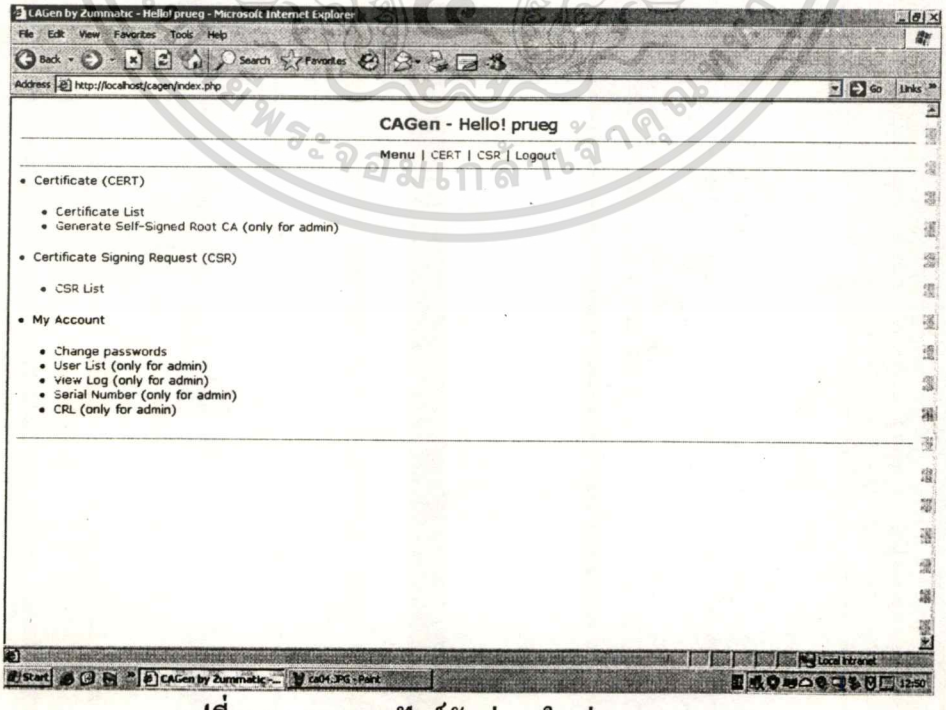
- Phase 2 คือส่วนของระบบออกใบรับรองดิจิทัล ซึ่งแบ่งออกเป็น 3 ส่วนย่อยๆดังนี้ คือ Certificate (CERT), Certificate Signing Request (CSR) และ My Account โดยทั้ง 3 ส่วนย่อยนี้จะแตกต่างกันระหว่าง Administrator และ User ดังรูปที่ 5.3



รูปที่ 5.3 ส่วนของระบบออกใบรับรองดิจิทัล

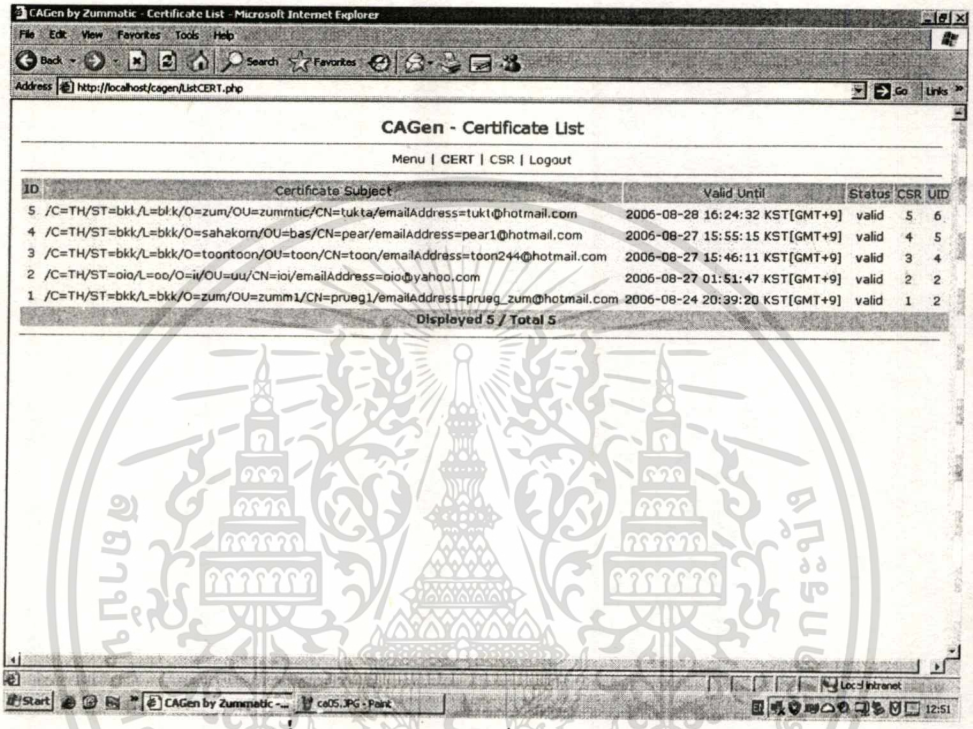
5.2.1 ฟังก์ชันการทำงานระบบการออกใบรับรองดิจิทัล

- **Administrator** เมื่อ Admin ทำการ Login เข้าระบบก็จะมีฟังก์ชันการทำงานดังรูปที่ ซึ่งมีลายละเอียดดังรูปที่ 5.4



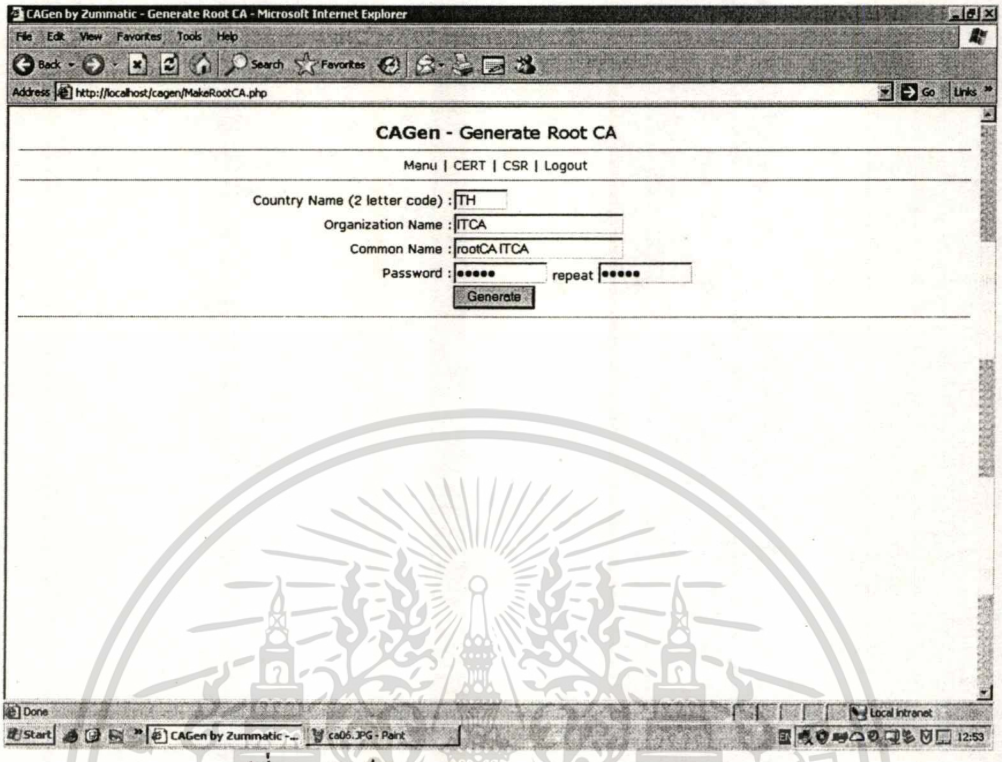
รูปที่ 5.4 ภาพแสดงฟังก์ชันต่างๆในส่วนของ Admin

1. Certificate List คือ ส่วนที่จะแสดงใบรับรองดิจิทัลทั้งหมดของระบบซึ่งจะแสดงรายละเอียดของใบรับรองดิจิทัล ได้แก่ ID, Certificate Subject, Valid Until, Status, CSR, UID ดังรูปที่ 5.5

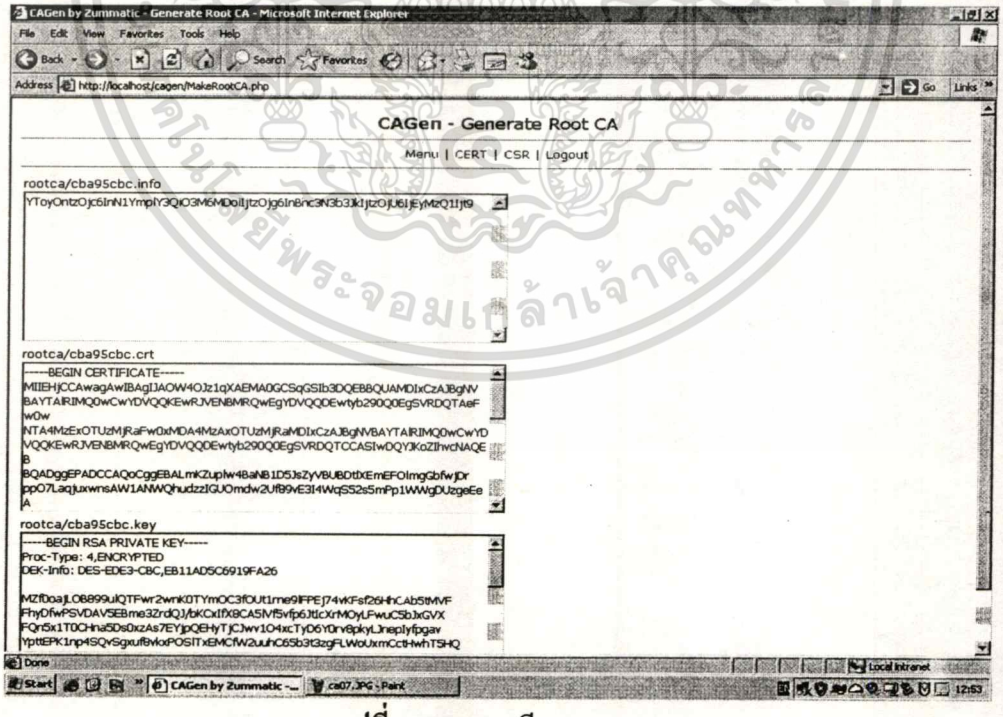


รูปที่ 5.5 ภาพแสดงฟังก์ชัน Certificate List

2. Generate Self – Signed Root CA คือ ส่วนที่ทำการสร้าง RootCA ดังรูปที่ 5.6 และรูปที่ 5.7

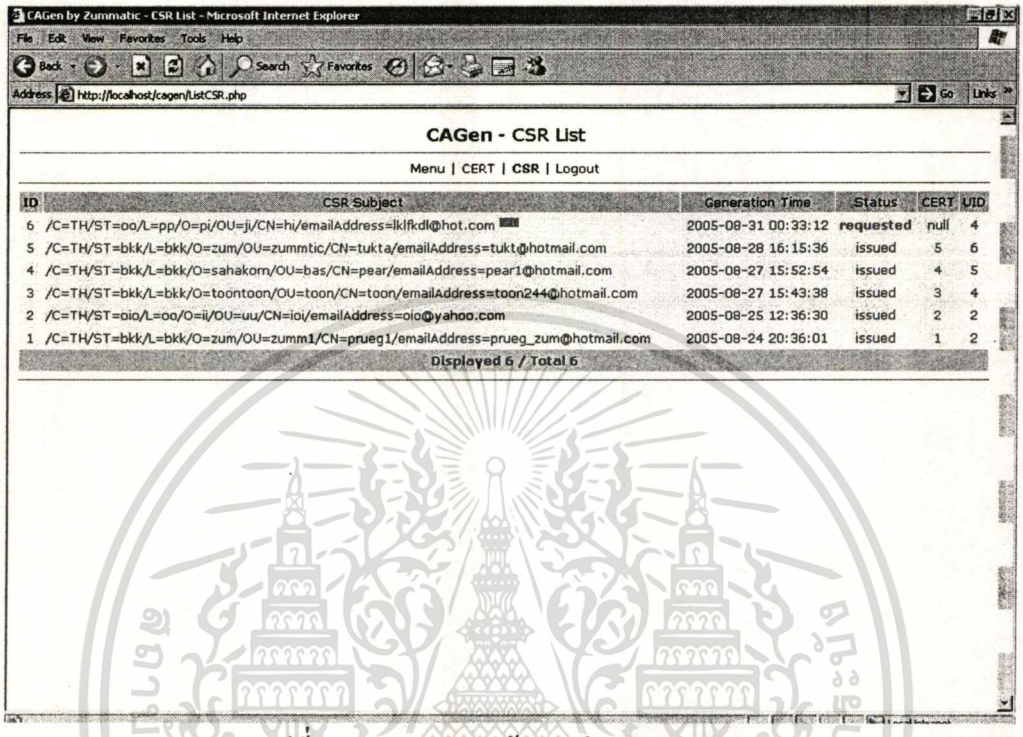


รูปที่ 5.6 ฟังก์ชัน Generate Self – Signed RootCA



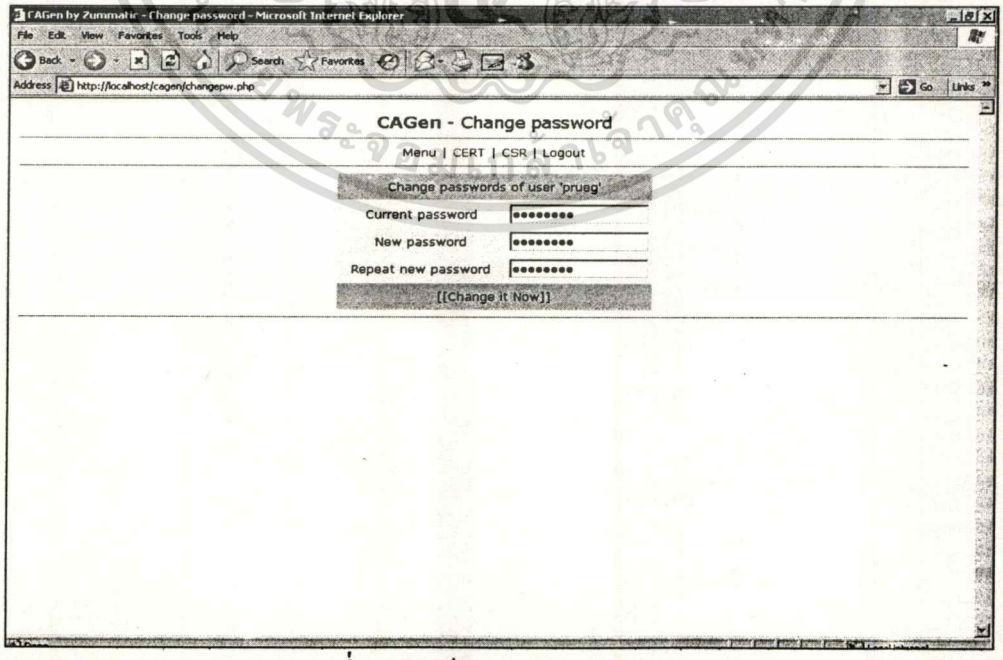
รูปที่ 5.7 รายละเอียดRootCA

3. CSR List คือ ส่วนที่แสดงรายการการขอใบรับรองดิจิทัลจาก User ทั้งหมดโดย Admin จะเป็นผู้รับรองและออกใบรับรองดิจิทัลให้แก่ User ดังรูปที่ 5.8



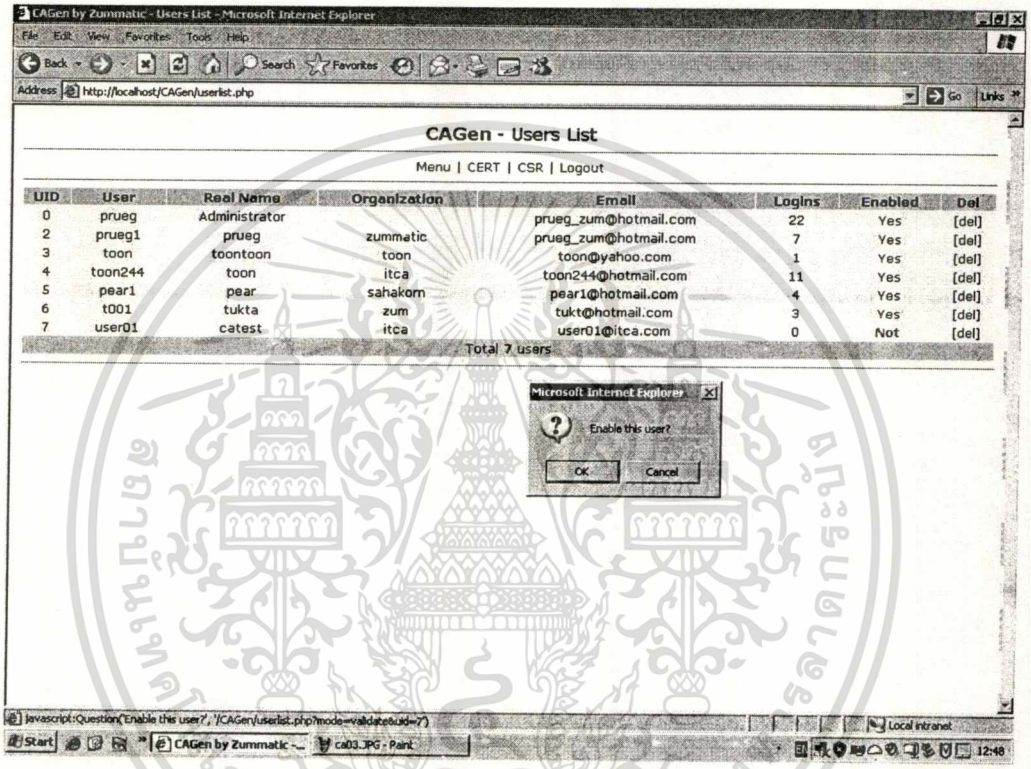
รูปที่ 5.8 List ของการร้องขอใบรับรองดิจิทัล

4. Change Password คือ ส่วนที่ใช้ในการเปลี่ยนรหัสผ่านของ Admin ดังรูปที่ 5.9



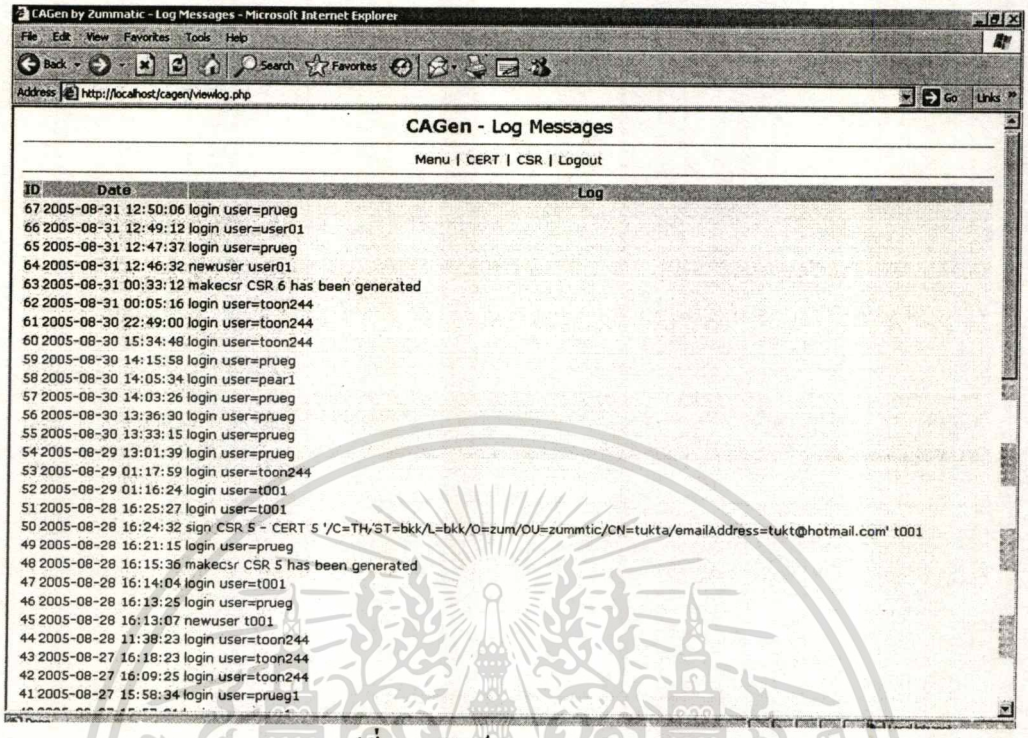
รูปที่ 5.9 ฟังก์ชัน Change Password

5. User List คือ ส่วนที่แสดงรายการการ Register ทั้งหมดของ User ซึ่งมีรายละเอียดได้แก่ UID, User, Real Name, Organization, Email, Login, Enable และ Del โดย Admin จะเป็นผู้ที่ทำการ Enable User ว่าสามารถเข้าใช้งานระบบได้หรือไม่เพื่อความปลอดภัย และยังสามารถทำการลบ User นั้นๆก็ได้ดังรูปที่ 5.10



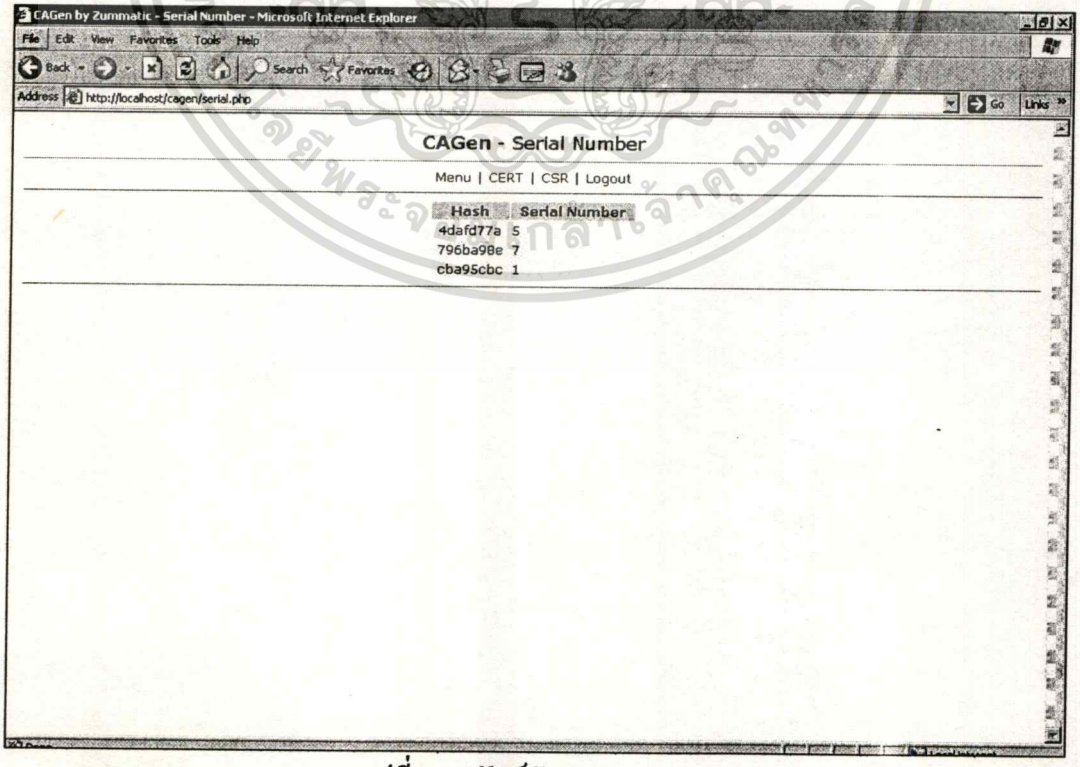
รูปที่ 5.10 ฟังก์ชันของ User List

6. View Log คือ ส่วนที่ใช้ในการแสดงการทำงานทั้งหมดของระบบดังรูปที่ 5.11



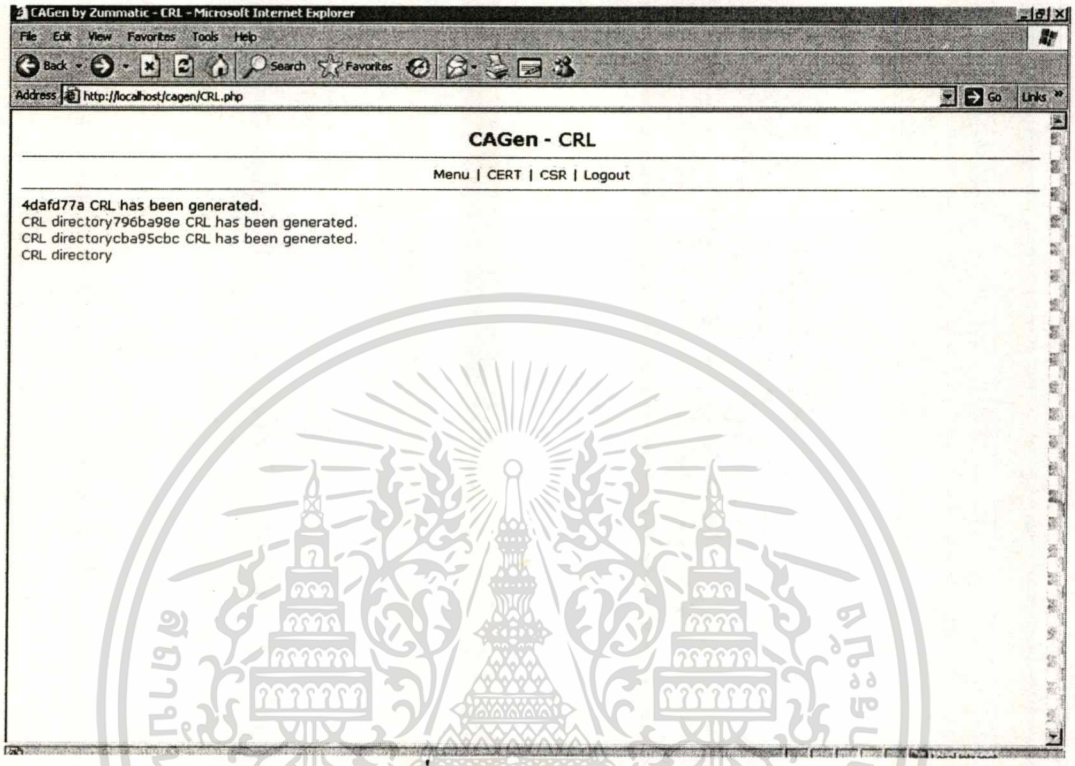
รูปที่ 511 ฟังก์ชันของ View Log

7. Serial Number คือ ส่วนที่แสดงรูปแบบการใช้งาน Hash Functionของ RootCA ดังรูปที่ 5.12



รูปที่ 5.12 ฟังก์ชันของ RootCA

8. CRL คือส่วนที่แสดงผลจากการสร้าง RootCA ดังรูปที่ 5.13



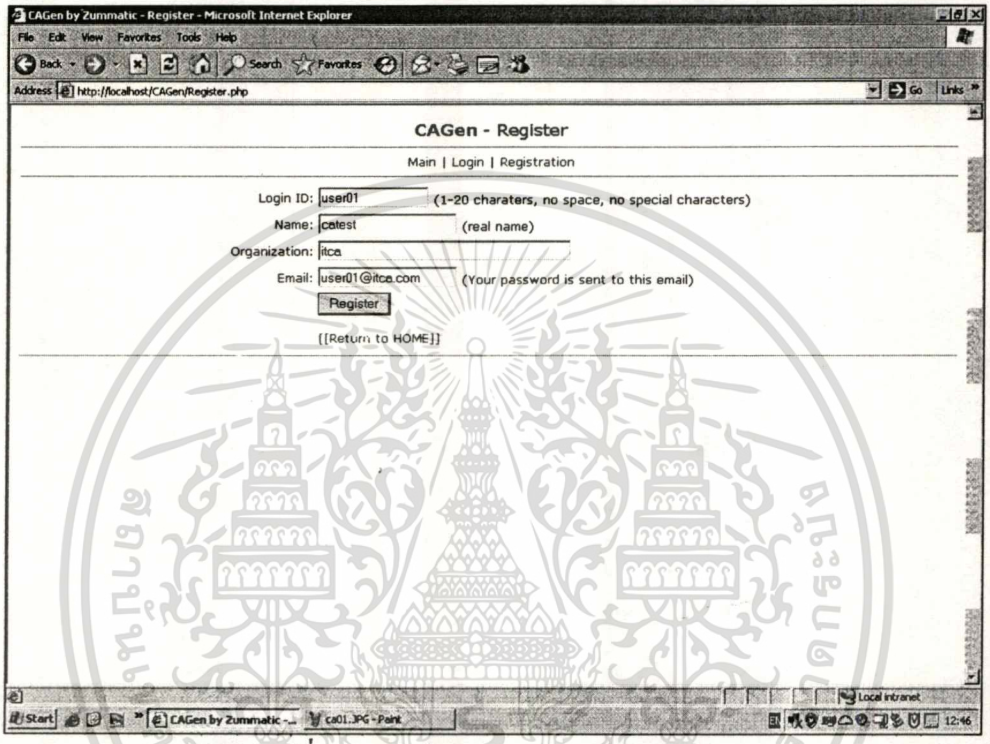
รูปที่ 5.13 ฟังก์ชันของ CRL

- **User** เมื่อ User ทำการ Login เข้าระบบก็จะมีฟังก์ชันการทำงานดังรูปที่ ซึ่งมีลายละเอียดดังนี้
    - Certificate List คือ ส่วนที่จะแสดงใบรับรองดิจิทัลของระบบ
    - CSR List คือ ส่วนที่แสดงรายการการขอใบรับรองดิจิทัลของระบบ
    - Generate CSR คือ ส่วนที่ทำการขอใบรับรองดิจิทัล
    - Upload CSR คือ ส่วนที่ทำการ Upload การร้องขอใบรับรองดิจิทัล
    - Change Passwords คือ ส่วนที่ทำหน้าที่ในการเปลี่ยนรหัสผ่านของ User

เมื่อเข้าใจฟังก์ชันต่างๆของการทำงานของระบบ ซึ่งใช้งานโดย User แล้ว ก็จะมีรายละเอียดของการทำงานทั้งหมดในส่วนของการใช้งานระบบโดย User เป็นลำดับขั้นตอนดังนี้

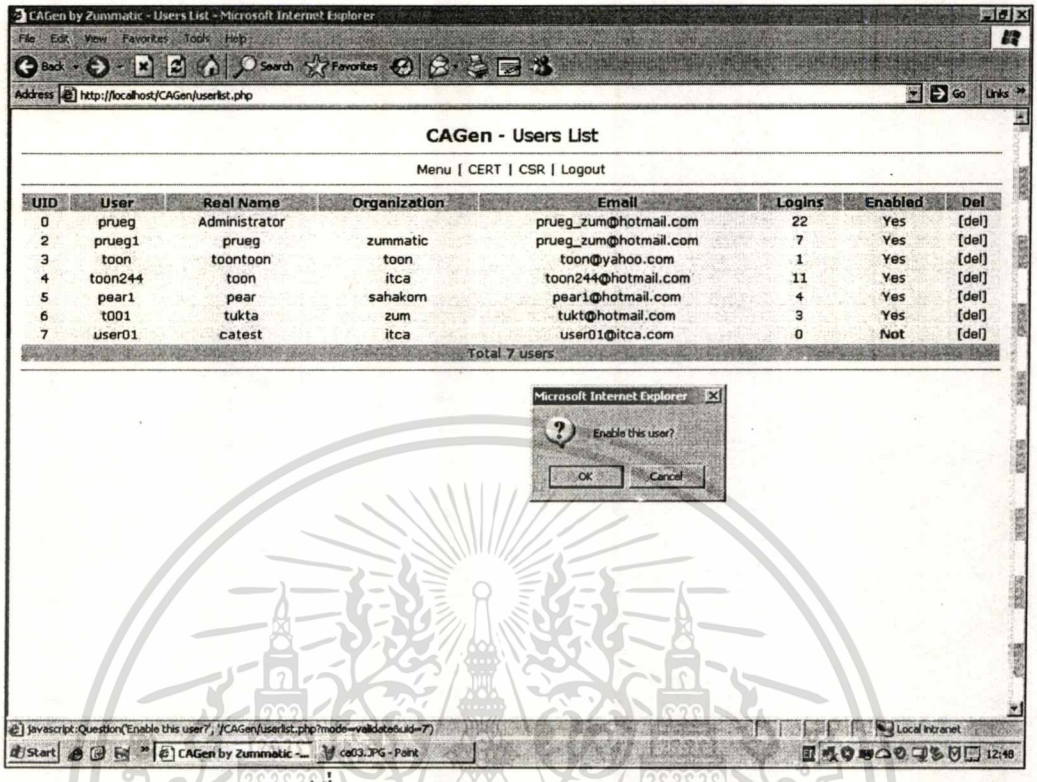
1. **Registration** เมื่อ User ใหม่ต้องการใช้งานระบบการออกใบรับรองดิจิทัลนั้น จะต้องทำการลงทะเบียนก่อนซึ่งจะต้องกรอกรายละเอียดทั้งหมดเป็นภาษาอังกฤษดังนี้
    - Login ID คือ ส่วนที่จะต้องกรอกเพื่อใช้เป็น Username ในการ Login

- Name คือ ชื่อจริงของบุคคลที่ต้องการจะทำการลงทะเบียน
- Organization คือ ชื่อองค์กรของบุคคลที่ต้องการจะทำการลงทะเบียน
- Email คือส่วนที่จะต้องกรอก Email ของบุคคลที่ต้องการจะทำการลงทะเบียน ซึ่งจะต้องใช้งานได้ เพราะใช้ในการส่ง Password กลับมาทาง Email ดังรูปที่ 5.14



รูปที่ 5.14 ฟังก์ชัน Registration ของ User

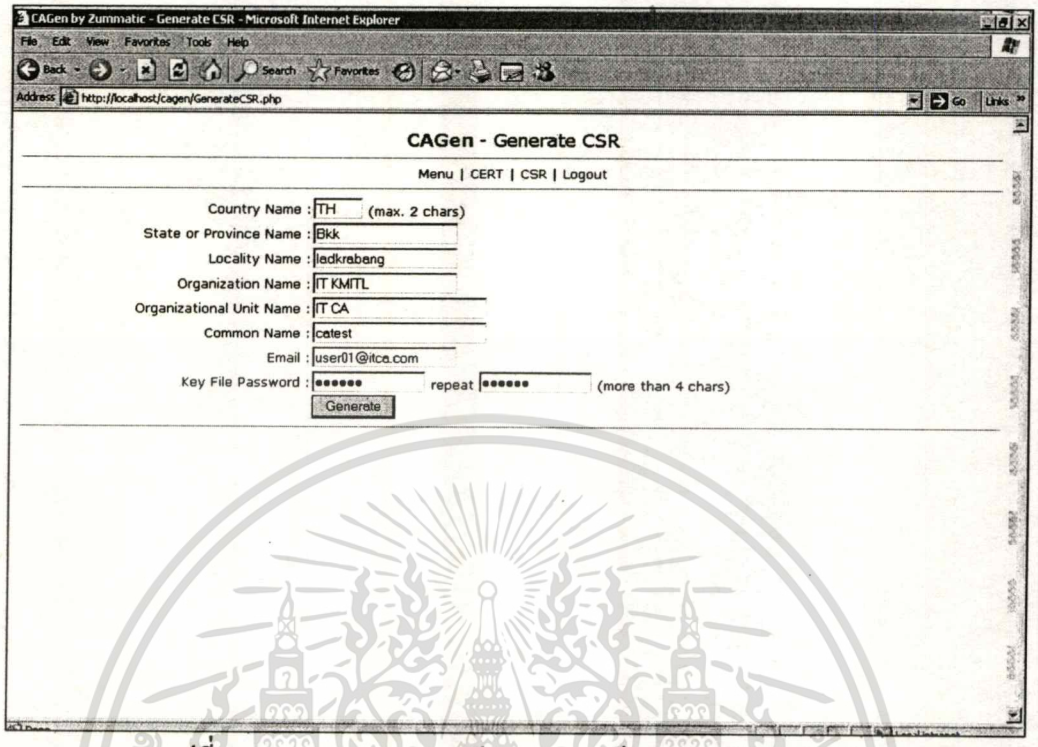
2. **Login** เมื่อลงทะเบียนเสร็จแล้วจะต้องรอ ทางฝ่าย Admin ให้รับรองก่อนแล้วถึงจะได้รับ Password กลับมาทาง Email แล้วจึงจะเข้าสู่ระบบการออกใบรับรองดิจิทัลได้ดังรูป



รูปที่ 5.15 การ Enable User จาก User List

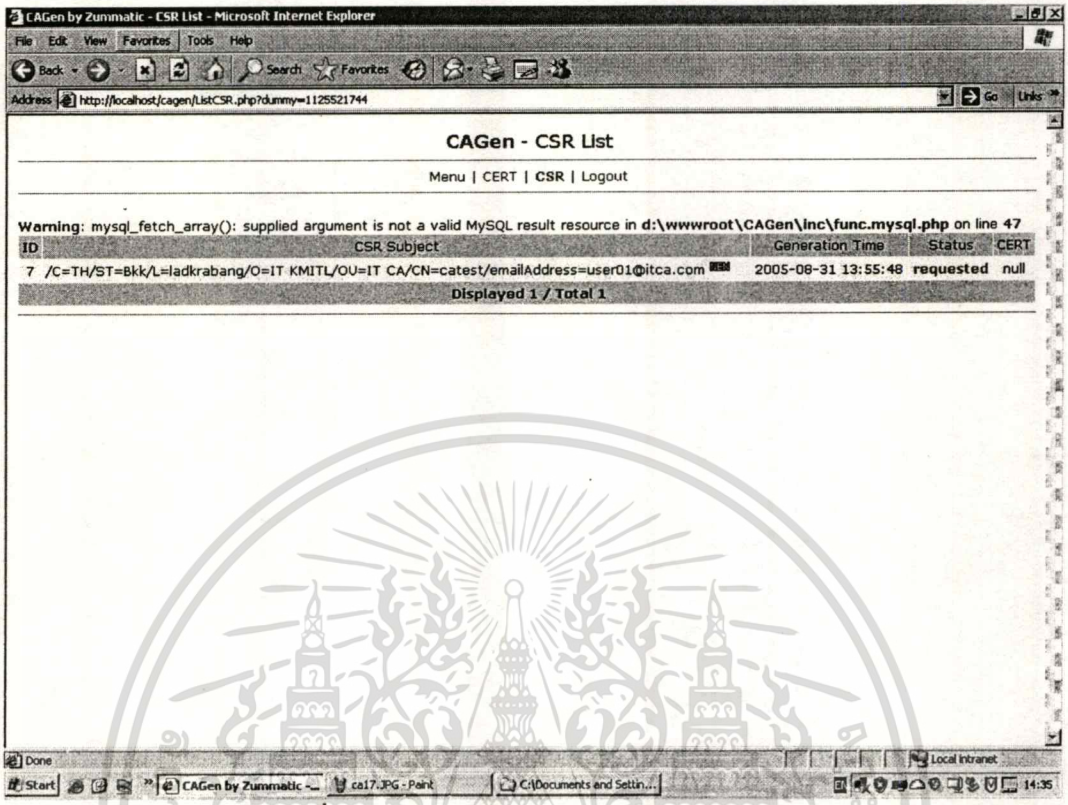
3. **Generate CSR** ทำการร้องขอใบรับรองดิจิทัล ซึ่งมีรายละเอียดให้กรอกเป็นภาษาอังกฤษทั้งหมด ตามมาตรฐานของ X.509 ดังนี้

- Country Name
- State or Province Name
- Locality Name
- Organization Name
- Organization Unit Name
- Common Name
- Email
- Key File Password
- Repeat Password



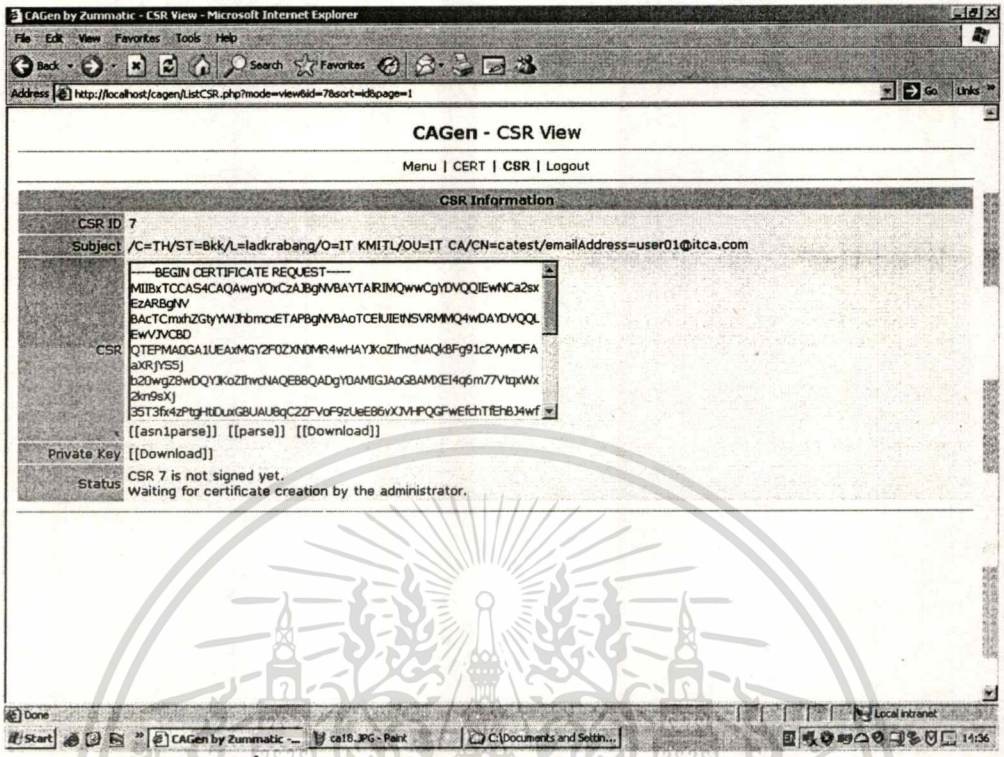
รูปที่ 5.16 การกรอกลายระเอียดของการร้องขอใบรับรองดิจิทัล

รูปที่ 5.17 การร้องขอใบรับรองดิจิทัลสำเร็จ



รูปที่ 5.18 List ของการร้องขอใบรับรองดิจิทัล

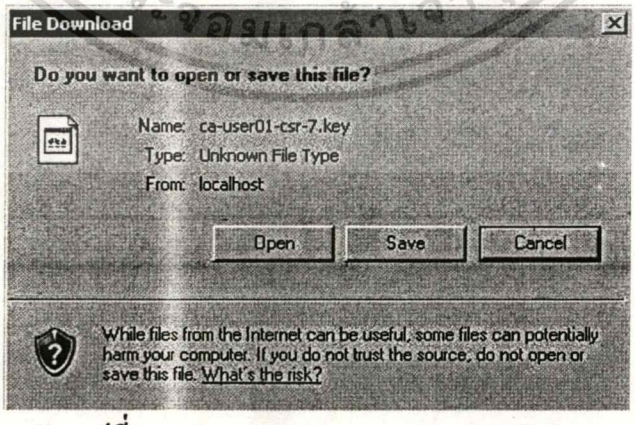
4. **CSR Information** จะเป็นส่วนของการแสดงข้อมูลการร้องขอใบรับรองดิจิทัล โดยจะได้หลังจาก Generate CSR แล้วหรือจะเปิดได้จากทาง CSR List ซึ่งมีรายละเอียดดังนี้
   - CSR ID
   - Subject
   - CSR
   - Private Key
   - Status



รูปที่ 5.19 ส่วนข้อมูลของการร้องขอใบรับรองดิจิทัล

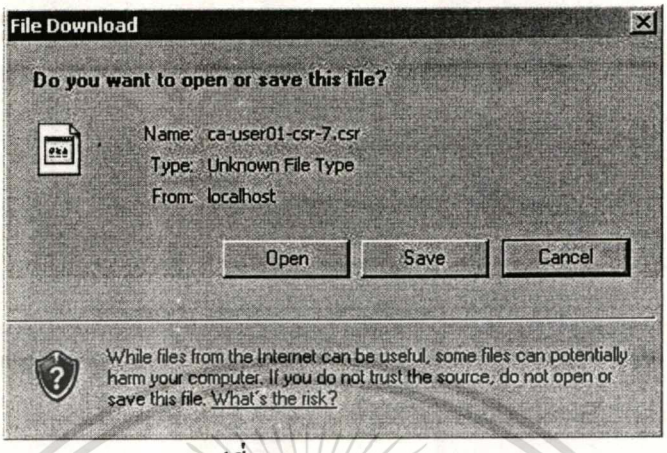
5. **Export Private Key** และ **Export CSR** สามารถทำการ Download ได้ที่ CSR Information ไปไว้ในเครื่องได้โดยเฉพาะ Private Key จะต้องรักษาความปลอดภัยโดยที่จะต้องไม่เปิดเผยให้ผู้อื่นรู้ เพราะเป็นส่วนหนึ่งในกระบวนการเข้ารหัสแล้วถอดรหัส ซึ่งจะมีรูปแบบดังนี้

- Private Key - ได้ File ชื่อ ca-*username*-csr-*csrid*.key



รูปที่ 5.20 ภาพแสดง File ของ Private Key

- CSR - ได้ File ชื่อ ca-*username*-csr-*csrid*.csr

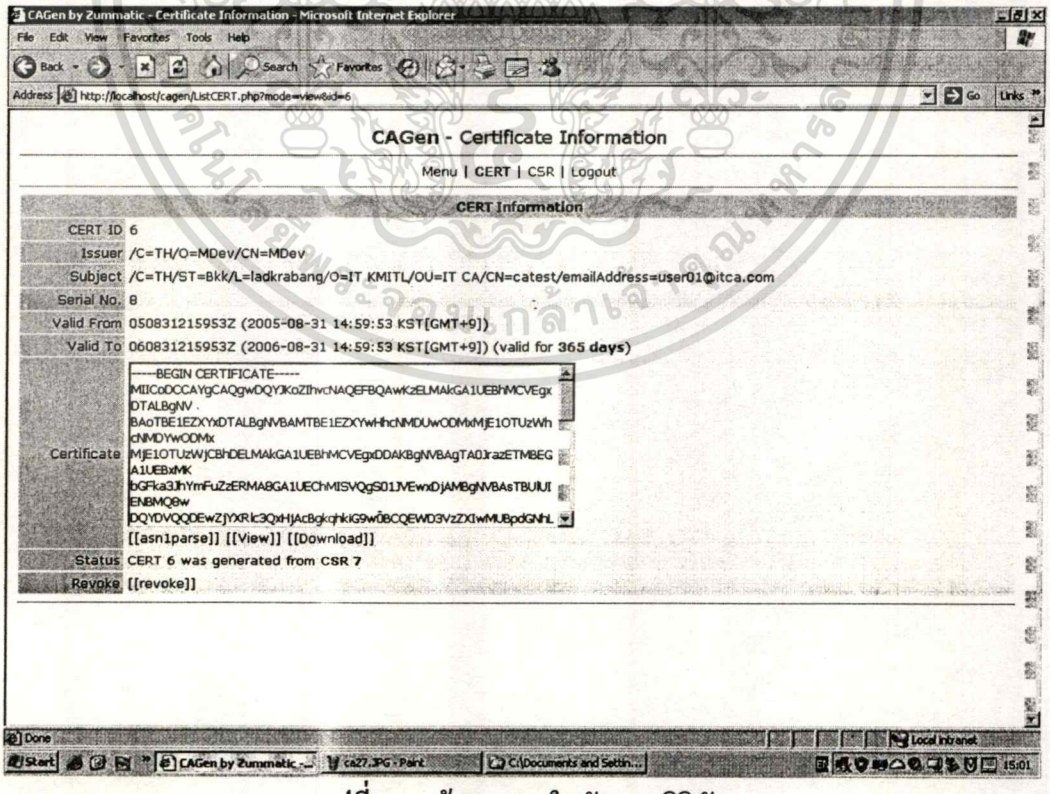


รูปที่ 5.21 File ของ CSR

6. **Cert Information** จะเป็นส่วนของการแสดงข้อมูลของใบรับรองดิจิทัล โดยจะได้หลังจากได้รับการรับรองจาก Admin แล้วหรือจะเปิดได้จากทาง Certificate List ดังรูปที่ 5.22 ซึ่งมีรายละเอียดดังนี้

- Cert ID
- Issuer
- Subject
- Serial No.
- Valid From
- Valid To
- Certificate
- Status
- Revoke

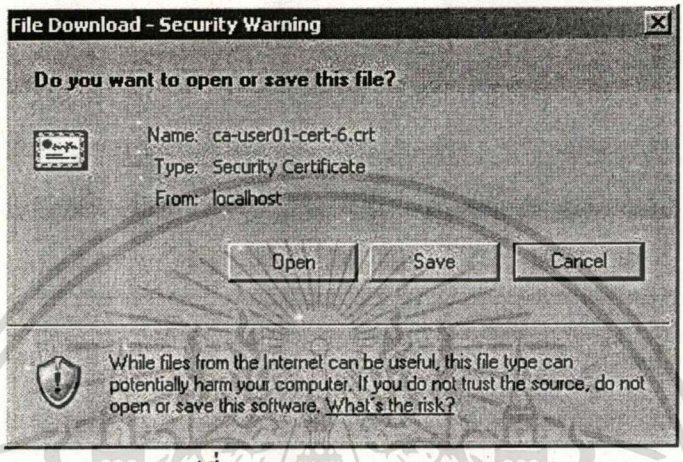
รูปที่ 5.22 List ของใบรับรองดิจิทัล



รูปที่ 5.23 ข้อมูลของใบรับรองดิจิทัล

7. **Export Public Key** สามารถทำการ Download ได้ที่ Cert Information ไปไว้ในเครื่องได้โดยในส่วนนี้สามารถเปิดเผยให้ผู้อื่นรู้ได้ ซึ่งจะมีรูปแบบดังนี้

- Public Key - ได้ File ชื่อ ca-*username*-cert-*certid*.crt ดังรูปที่ 5.24



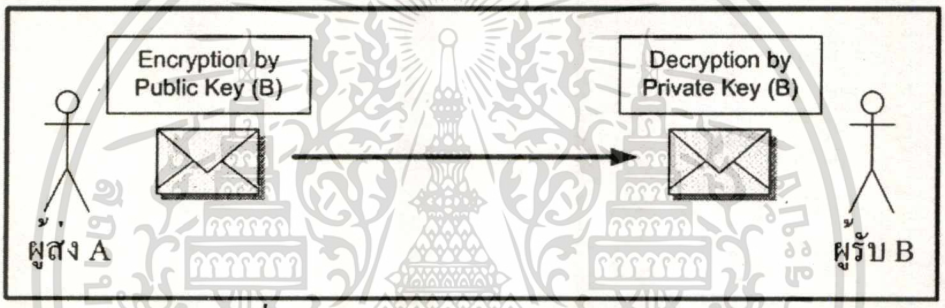
รูปที่ 5.24 File ของ Certificate

การทดลองการประยุกต์ใช้งานใบรับรองดิจิทัลต่อการส่งจดหมายอิเล็กทรอนิกส์

ในการส่งจดหมายอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับเพื่อรักษาความลับของข้อความที่ส่งไปยังผู้รับนั้น ผู้ส่งจำเป็นต้องมีกุญแจสาธารณะของผู้รับเพื่อใช้ในการเข้ารหัสลับเสียก่อน โดยกุญแจสาธารณะจะนำมาจากใบรับรองดิจิทัลของผู้รับ ซึ่งการนำใบรับรองดิจิทัลของผู้รับมาใช้นั้นมี 2 วิธี

วิธีที่ 1 ให้บุคคลที่ต้องการติดต่อส่งจดหมายอิเล็กทรอนิกส์ที่มีลายมือชื่อดิจิทัลมายังผู้ส่งก่อน เมื่อเปิดอ่านจดหมายอิเล็กทรอนิกส์ โปรแกรมจะทำการบันทึกข้อมูลของบุคคลดังกล่าวลงใน Address Book และบันทึกใบรับรองดิจิทัลลงในที่เก็บซึ่งอยู่ใน Internet Explorer โดยอัตโนมัติ

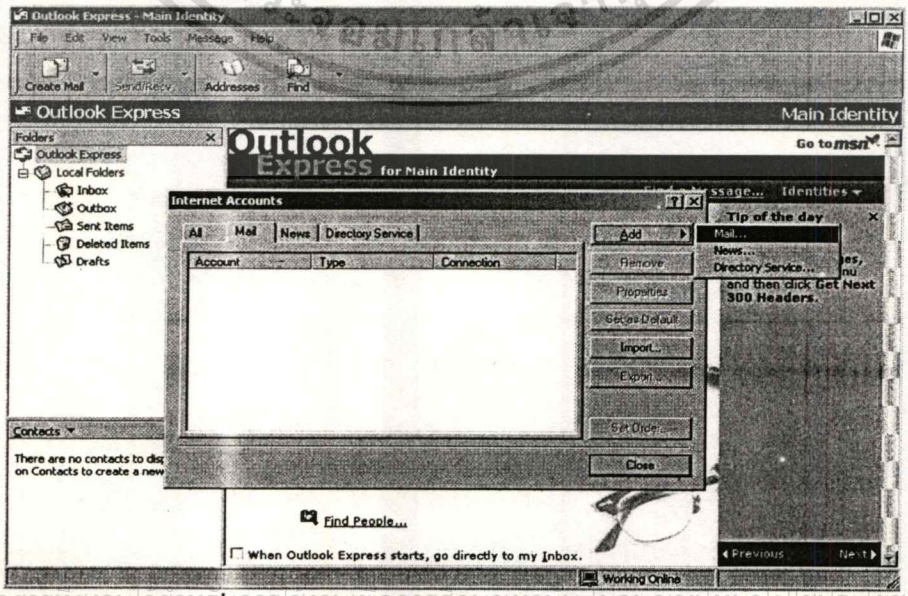
วิธีที่ 2 ค้นหาใบรับรองดิจิทัลจากไดเรกทรอรีของผู้ให้บริการออกใบรับรอง



รูปที่ 5.25 การเข้ารหัสจดหมายอิเล็กทรอนิกส์

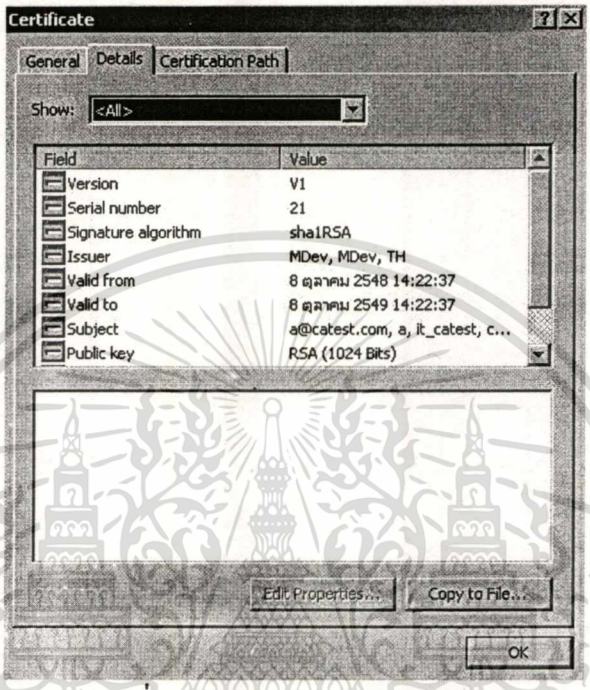
ขั้นตอนการใช้งาน Web Mail (Outlook Express)

1. เปิดโปรแกรม Outlook Express เลือกที่ Tool > Accounts > Add > Mail ทำการสร้าง mail ที่มีชื่อว่า a@catest.com (เป็น Mail ที่มีอยู่จริงจากการสร้างใน Mail Server) ดังรูปที่ 5.26

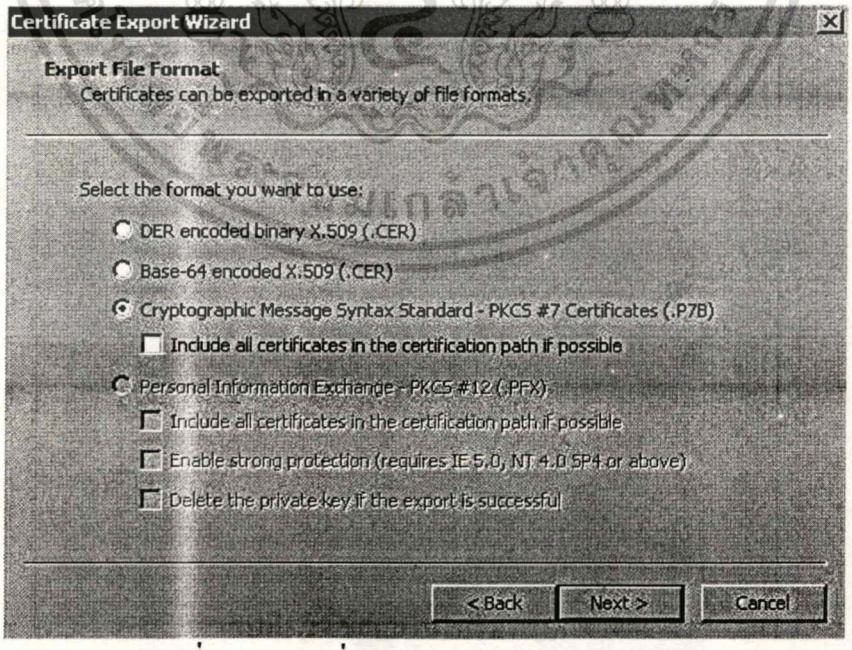


รูปที่ 5.26 การสร้าง Account ใน Outlook Express

2. ทำการติดตั้งใบรับรองดิจิทัลของ a@catest.com โดยโปรแกรม Outlook Express จะรู้จักใบรับรองดิจิทัลในรูปแบบของ Pkcs#7 โดยทำการเปิดใบรับรองของ a – File Cert a > Details > Copy to File แล้วเลือกที่ Export to Format Pkcs#7 ดังรูปที่ 5.27

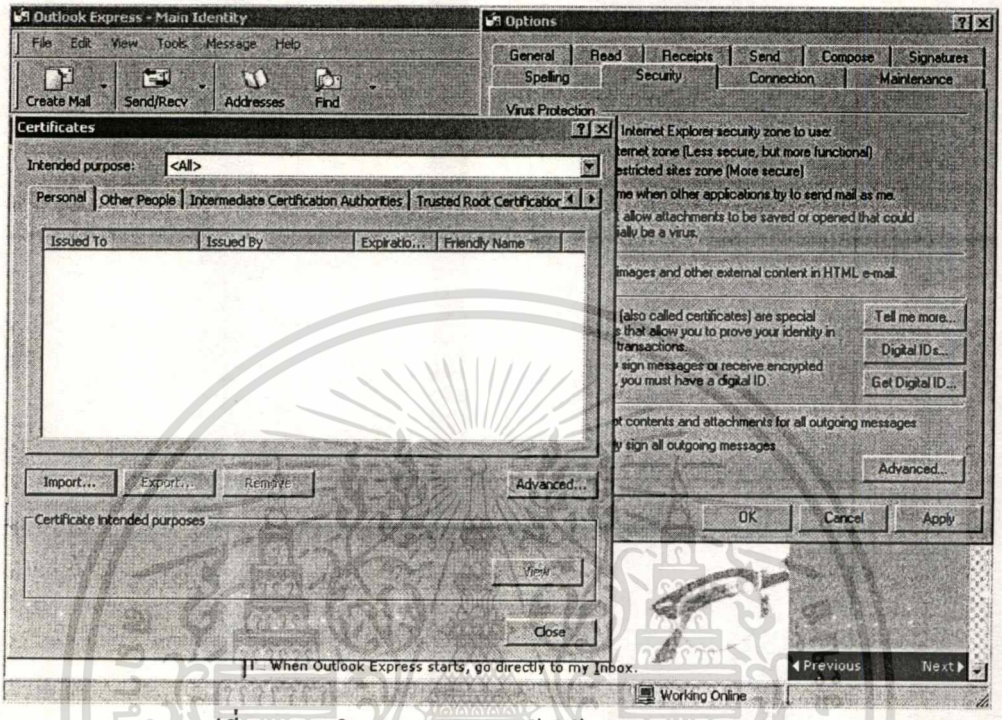


รูปที่5.27 ข้อมูลในใบรับรองดิจิทัล



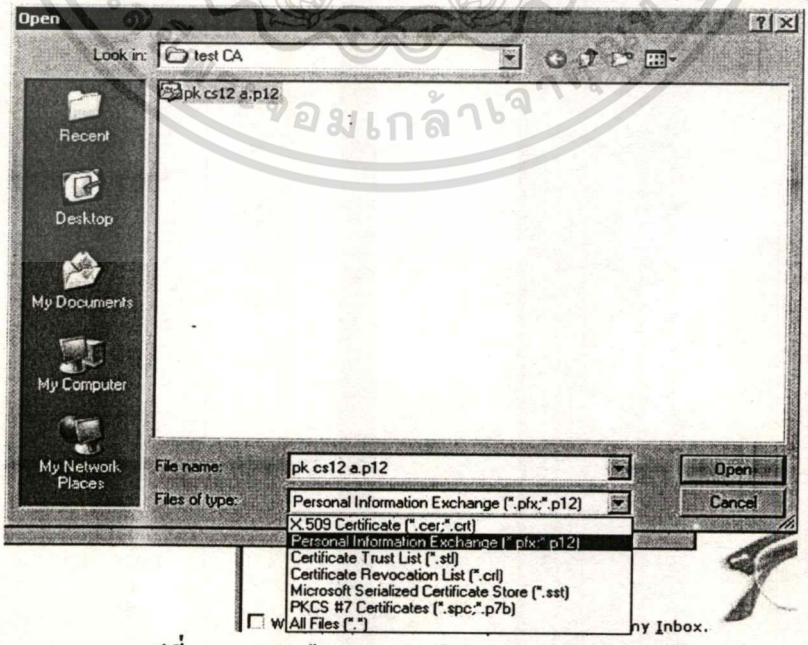
รูปที่5.28 การเปลี่ยนรูปแบบของใบรับรองดิจิทัล

3. ไปที่โปรแกรม Outlook Express เลือกที่ Tool > Option > Security > Digital IDs > Import เพื่อให้โปรแกรมรู้จักใบรับรองดิจิทัลของแต่ละบุคคลดังรูปที่ 5.29

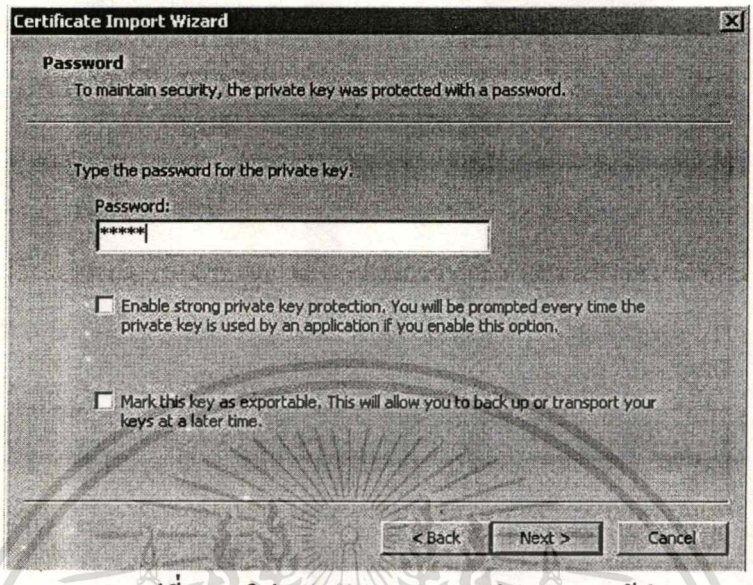


รูปที่ 5.29 นำใบรับรองดิจิทัลเข้าใช้งานใน Outlook Express

ทำการเลือกรูปแบบไฟล์ ที่ต้องการ Import เข้ามาไว้โดยจะต้องใช้รูปแบบของ PKCS#12 (Personal Information Exchange) แล้วใส่รหัสลับของ Private Key ให้ถูกต้องดังรูปที่ 5.30

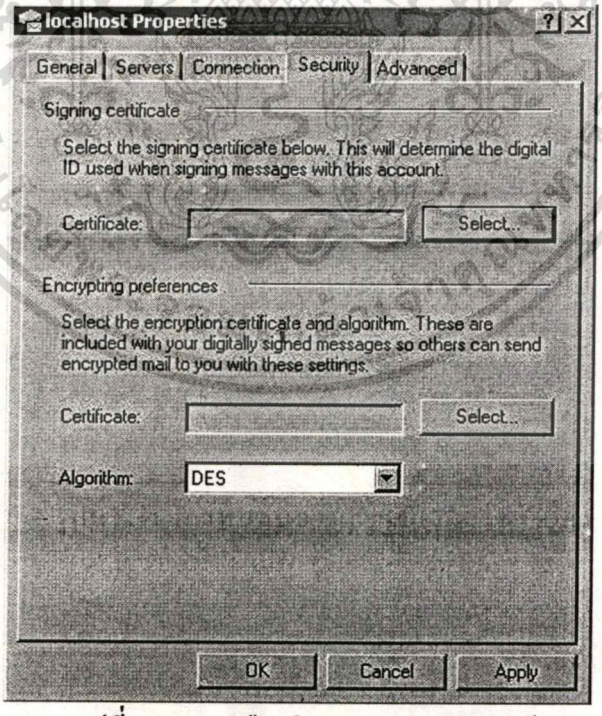


รูปที่ 5.30 การเลือกรูปแบบใบรับรองดิจิทัลของผู้ส่ง

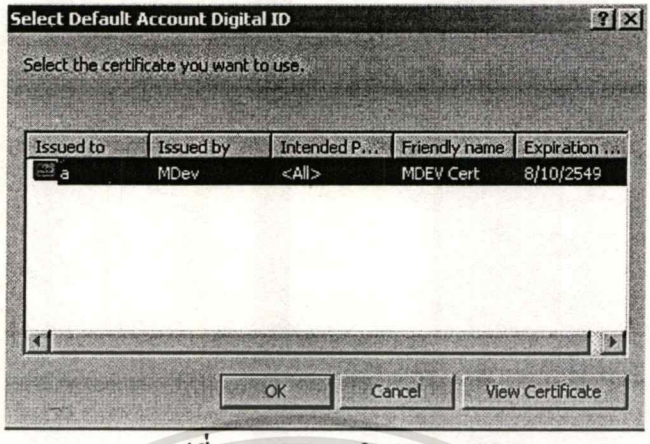


รูปที่ 5.31 ใส่รหัสลับของกุญแจส่วนตัวของผู้ส่ง

4. โปรแกรม Outlook Express เลือกที่ Tool > Accounts > Mail > a > Properties > Security หลังจากนั้นทำการ Select เลือก Digital IDs ของ a ดังรูปที่ 5.32

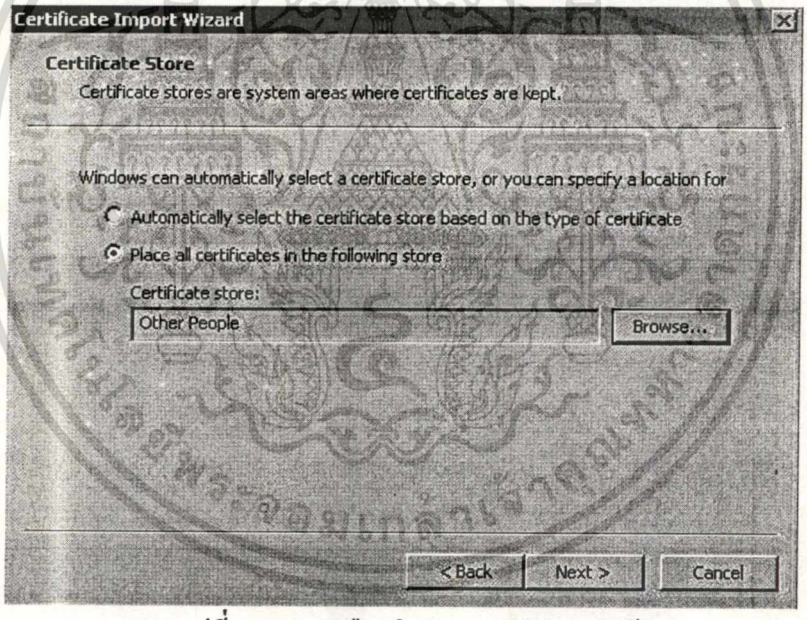


รูปที่ 5.32 การเลือกใบรับรองดิจิทัลของผู้ส่ง



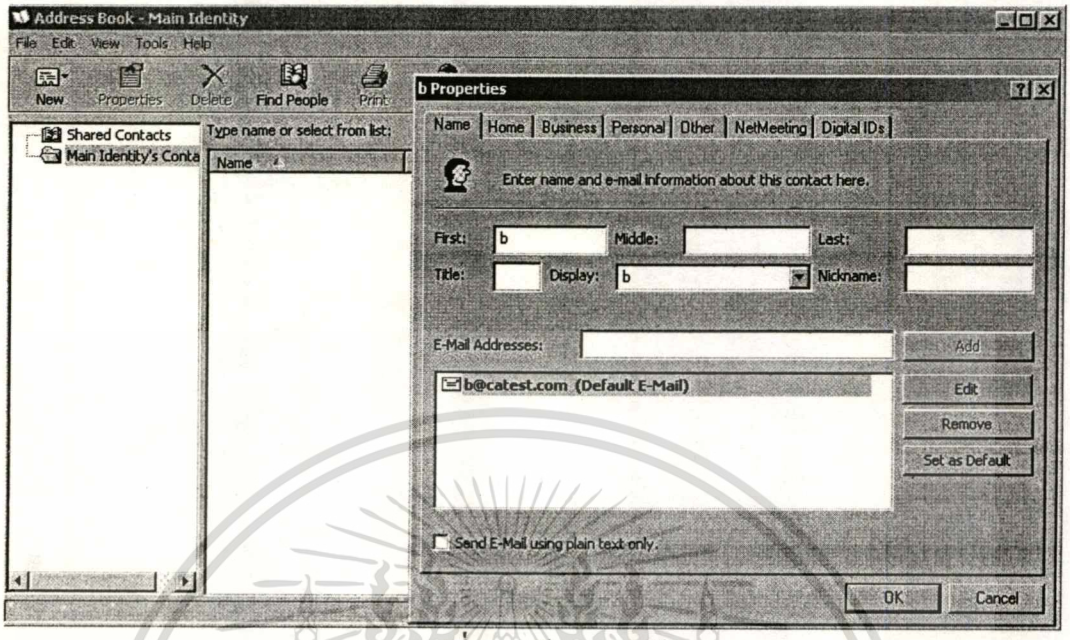
รูปที่ 5.33 รายการใบรับรองดิจิทัล

5. ทำการตรวจสอบกุญแจสาธารณะของผู้รับ (b)ได้ที่ Tool > Option > Security > Digital IDs โดยเลือกที่ Other People แล้วทำการ Import ใบรับรองดิจิทัลของ b ดังรูปที่ 5.34



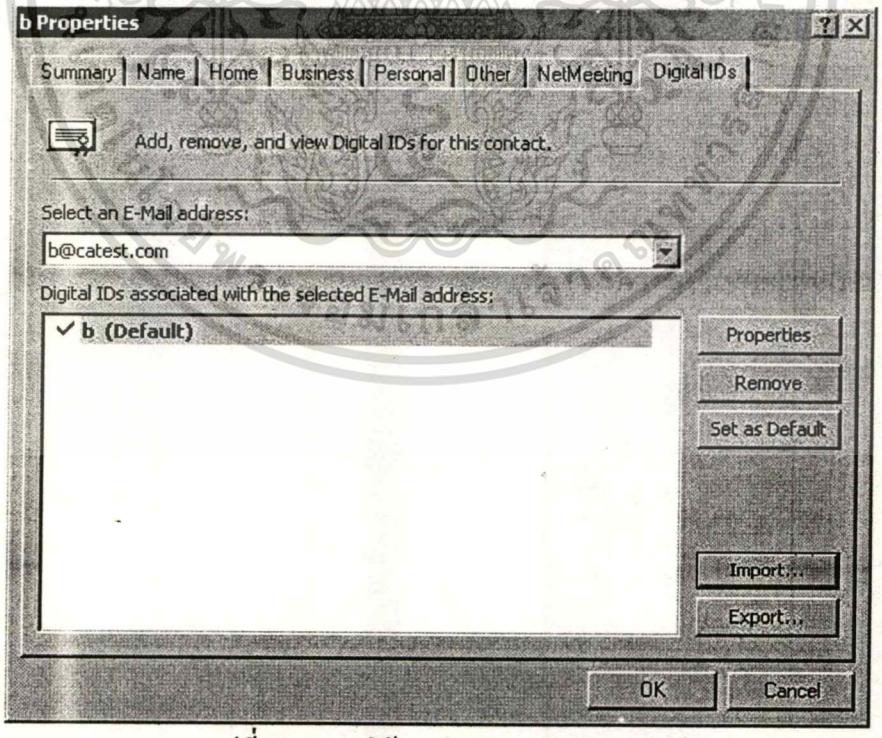
รูปที่ 5.34 การเลือกใบรับรองดิจิทัลของผู้รับ

6. ทำการกำหนดกุญแจสาธารณะให้กับ E-mail Address ของผู้รับ(b@catest.com) โดยเลือกที่ Tool > Address Book > New > New Contact > แล้วทำการกรอกรายละเอียดของผู้รับดังรูปที่ 5.35



รูปที่ 5.35 ข้อมูลของผู้รับ

หลังจากนั้นไปที่ E-mail Address ของผู้รับ (b@catest.com) ที่จะปรากฏอยู่ใน Address Book แล้วเลือกที่ Properties > Digital IDs > Import Certificate (Format PKCS#7)



รูปที่ 5.36 การใช้งานใบรับรองดิจิทัลของผู้รับ

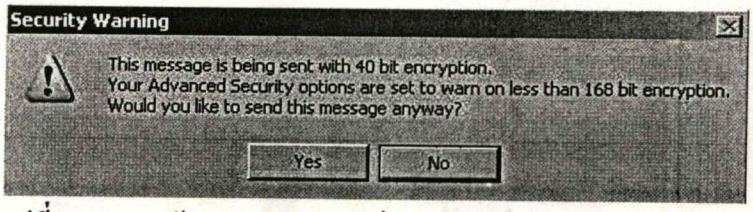
การเข้ารหัสลับจดหมายอิเล็กทรอนิกส์

ในการเข้ารหัสจดหมายอิเล็กทรอนิกส์สามารถทำได้ทั้งการส่งจดหมายอิเล็กทรอนิกส์ใหม่ (New Mail) ส่งจดหมายอิเล็กทรอนิกส์ตอบกลับ (Reply Mail) และจดหมายอิเล็กทรอนิกส์ต่อ (Forward Mail) โดยการเข้ารหัสลับยังรวมไปถึงการเข้ารหัสไฟล์แนบ (Attachment) ด้วย

1. ที่หน้าต่างการส่งจดหมายอิเล็กทรอนิกส์ ให้กรอก E-mail Address ของผู้รับ หัวข้อ และข้อความที่ต้องการ (เหมือนการส่งจดหมายธรรมดา) และถ้าหากต้องการส่งไฟล์แนบสามารถทำได้โดยการคลิกที่ปุ่ม Attach จากนั้นคลิกที่ปุ่ม Encrypt เพื่อเข้ารหัสลับจดหมายอิเล็กทรอนิกส์ สังเกตจากรูปแม่กุญแจที่ปรากฏด้านขวามือเมื่อกด Encrypt ดังรูปที่ 5.37

รูปที่ 5.37 ส่งจดหมายอิเล็กทรอนิกส์ที่มีการเข้ารหัส

2. หากผู้ส่งใช้ใบรับรองดิจิทัลที่ได้จากไดเรกทอรีมาใช้ในการเข้ารหัสเมื่อทำการส่งจะมีข้อความปรากฏว่ามีการใช้กุญแจที่มีความยาว 40 บิตในการเข้ารหัส จากนั้นกด Yes เพื่อทำการส่งจดหมายดังรูปที่ 5.38



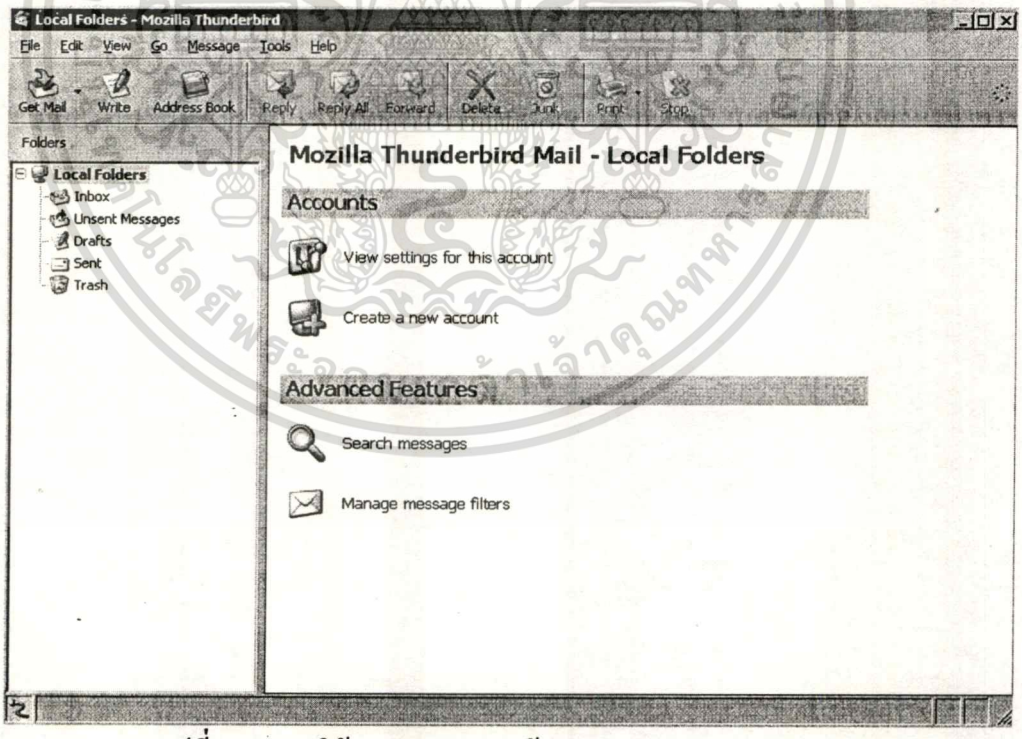
รูปที่ 5.38 การเข้ารหัสจดหมายอิเล็กทรอนิกส์ก่อนจะทำการส่ง

การอ่านจดหมายอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับ

ในการถอดรหัสจดหมายอิเล็กทรอนิกส์นั้น ผู้รับจะต้องใช้กุญแจส่วนตัวของตนเองมาทำการถอดรหัสลับซึ่งในการใช้กุญแจส่วนตัวมาถอดนี้เป็นการมั่นใจได้ว่าผู้รับที่เป็นเจ้าของคู่กุญแจ (กุญแจส่วนตัวและกุญแจสาธารณะที่อยู่ในใบรับรองดิจิทัล) เท่านั้นที่สามารถอ่านจดหมายอิเล็กทรอนิกส์ที่มีการเข้ารหัสได้

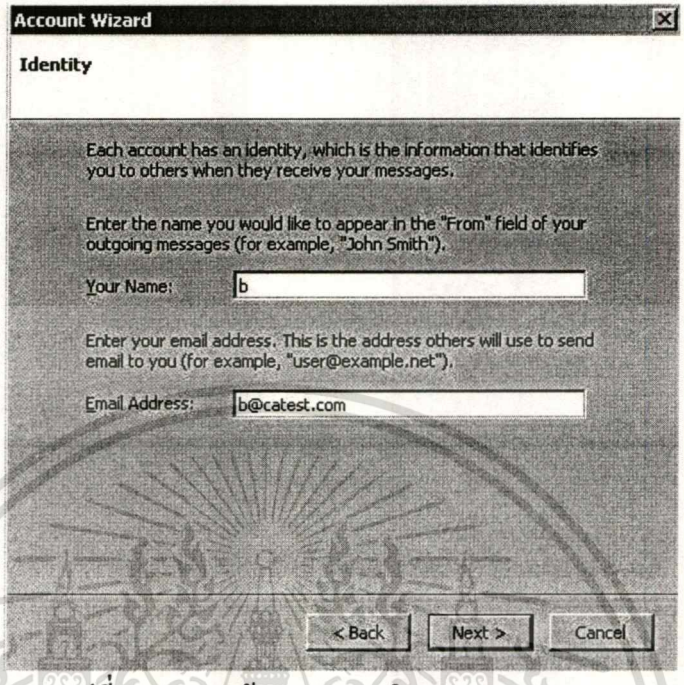
ขั้นตอนการใช้งานของผู้รับ (Web Mail : Mozilla Thunderbird)

1. ในการใช้งานการถอดรหัสจดหมายอิเล็กทรอนิกส์ โดยผู้รับจะทำการรับด้วย Web Mail ที่มีชื่อว่า Mozilla Thunderbird โดยใช้ Account ที่มีชื่อว่า b@catest.com หรือจะสามารถทำการเข้ารหัสจดหมายอิเล็กทรอนิกส์แล้วส่งไปหา Account ที่มีชื่อว่า a@catest.com ได้ด้วย ดังรูปที่ 5.39



รูปที่ 5.39 การใช้งาน Web Mail ด้วย Mozilla Thunderbird

2. ทำการสร้าง Account : b@catest.com โดยเลือกที่ Tool > Account Settings แล้วใส่รายละเอียดของผู้รับได้ทันทีดังรูปที่ 5.40

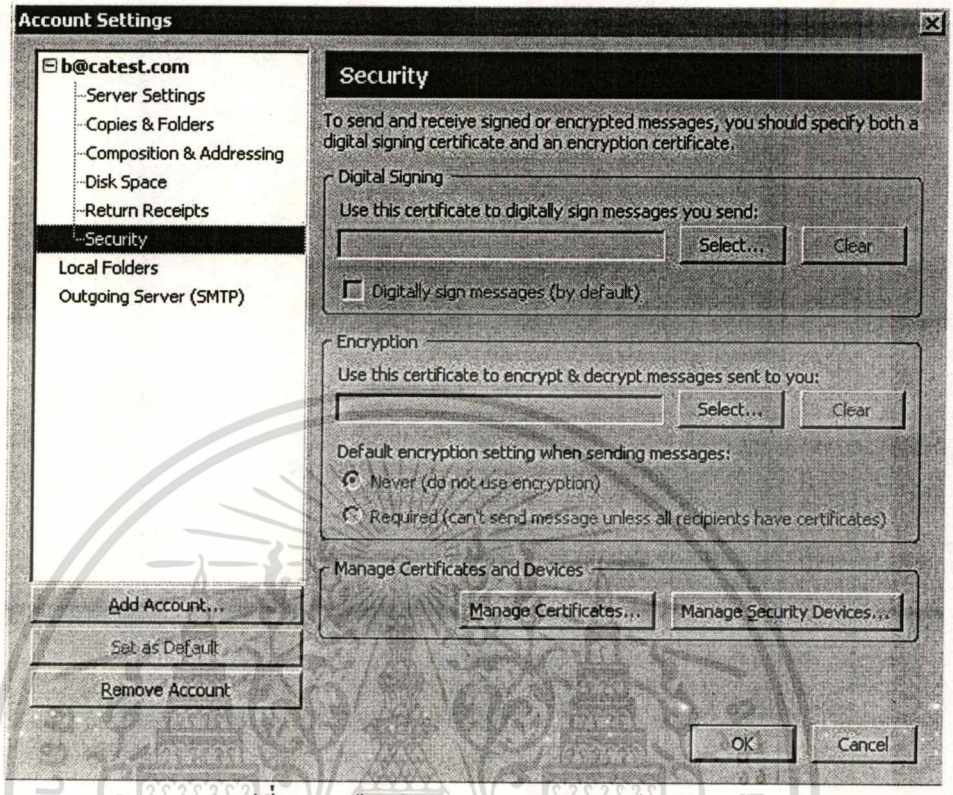


รูปที่ 5.40 การสร้าง Account ใน Thunderbird

3. เมื่อทำการเข้าใช้งาน b@catest.com ทางด้านโปรแกรมจะถามหา Password ของ Account ของผู้รับที่มีชื่อว่า b@catest.com ดังรูปที่ 5.41

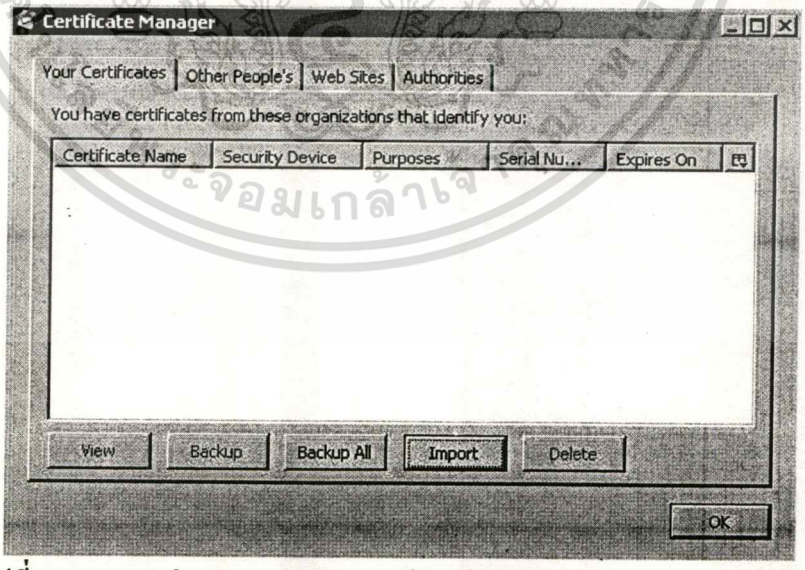
รูปที่ 5.41 การใส่รหัสของ E-mail

4. จะทำการ Select ใบรับรองดิจิทัลของผู้รับได้ที่ Tool > Account Settings > b@catest.com > Security > Manage Certificate ดังรูปที่ 5.42



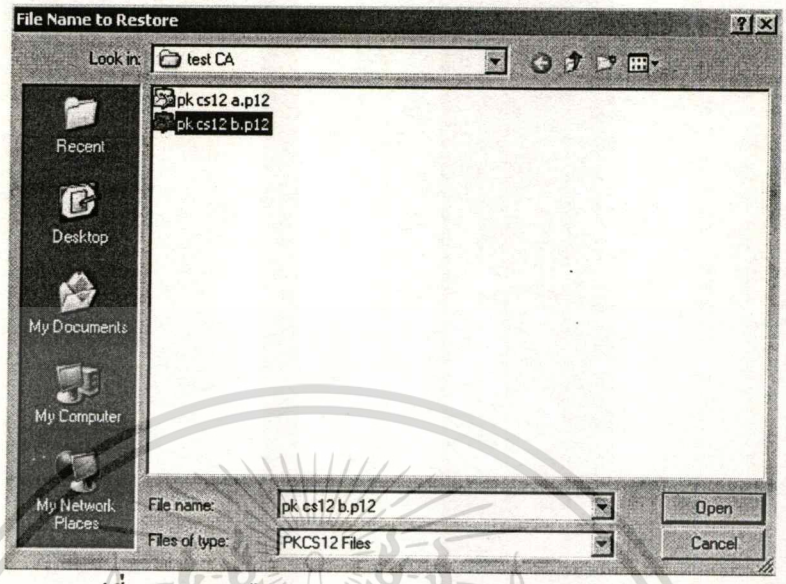
รูปที่ 5.42 เลือกใบรับรองดิจิทัลของผู้รับ

5. หลังจากนั้นทำการเลือกที่ Your Certificate > Import ใบรับรองดิจิทัลเข้ามาดังรูปที่ 5.43



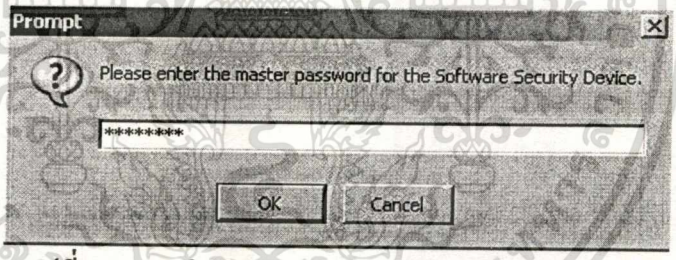
รูปที่ 5.43 การนำใบรับรองดิจิทัลของผู้รับเข้ามาใช้งานใน Thunderbird

6. ทำการเลือกใบรับรองดิจิทัลของผู้รับ (b) โดยใช้รูปแบบของใบรับรองดิจิทัลเป็น PKCS#12 ดังรูปที่ 5.44



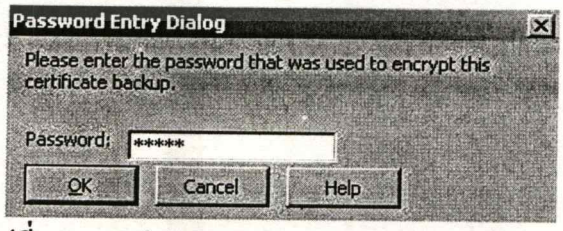
รูปที่ 5.44 การเลือกรูปแบบใบรับรองดิจิทัลของผู้รับ

7. หลังจากนั้นทางโปรแกรมจะถามหา Password ของ Software Security ที่เราใช้กรอกตอนติดตั้งโปรแกรมในที่นี้ใช้คำว่า "maverick" ดังรูปที่ 5.45



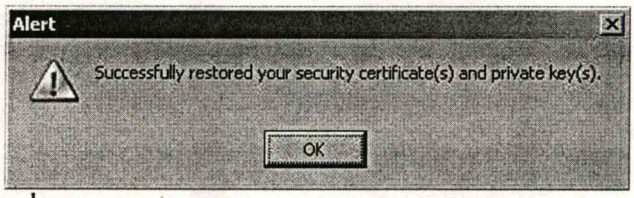
รูปที่ 5.45 การใส่รหัสความปลอดภัยของโปรแกรม

8. จากนั้นโปรแกรมจะถามหา Password ของใบรับรองดิจิทัลของผู้รับ นั่นก็คือ Password ที่ใช้ในขั้นตอนการร้องขอใบรับรองดิจิทัล ดังรูปที่ 5.46



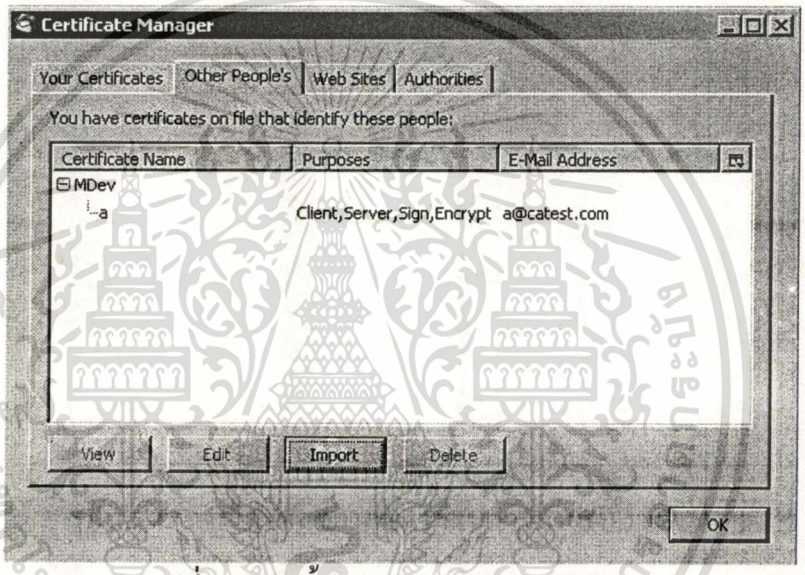
รูปที่ 5.46 การใส่รหัสของกุญแจส่วนตัวของผู้รับ

9. ทางโปรแกรมจะตอบกลับมาว่าการทำงานสมบูรณ์ระหว่างใบรับรองดิจิทัลกับกุญแจส่วนตัวดังรูปที่ 5.47



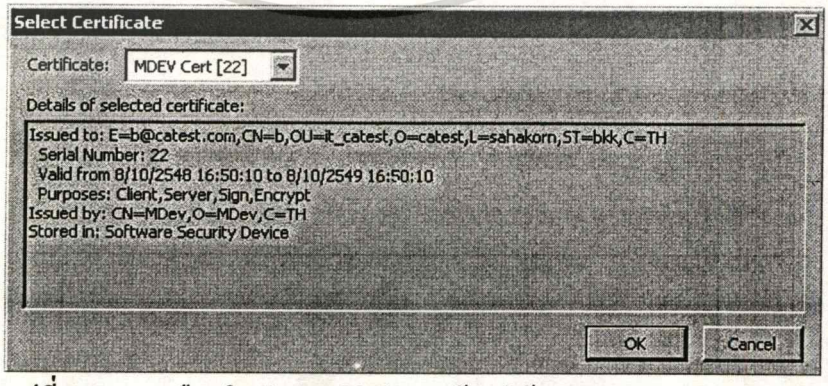
รูปที่ 5.47 การใส่รหัสของกุญแจส่วนตัวของผู้รับสำเร็จ

10. หลังจากนั้นทำการติดตั้งใบรับรองของผู้อื่นที่จะถูกใช้ในการเข้ารหัส เมื่อเสร็จสิ้นจะได้ผลดังรูปที่ 5.48



รูปที่ 5.48 ติดตั้งใบรับรองดิจิทัลของผู้ส่ง

11. ทำการ Select ใบรับรองดิจิทัลของผู้รับ (b) ในส่วนของ Security โดยเลือกที่ตรงกับ Account : b ดังรูปที่ 5.49



รูปที่ 5.49 การเลือกใบรับรองดิจิทัลของผู้รับให้ตรงกับกุญแจส่วนตัว

การถอดรหัสลับจดหมายอิเล็กทรอนิกส์

1. เมื่อเปิดอ่านจดหมายอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับ ผู้รับต้องใช้กุญแจส่วนตัวของตนในการถอดรหัสลับจดหมายอิเล็กทรอนิกส์ที่ส่งมา โดยโปรแกรมจะให้กรอกรหัสผ่านที่ป้องกันการใช้งานกุญแจส่วนตัวของผู้รับ
2. หากกรอกรหัสผ่านถูกต้องโปรแกรมจะถอดรหัสลับจดหมายอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับ พร้อมทั้งแสดงข้อความว่าจดหมายอิเล็กทรอนิกส์ฉบับนี้เป็นจดหมายอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับ และแสดงคำแนะนำเกี่ยวกับจดหมายอิเล็กทรอนิกส์นั้นๆ ซึ่งข้อความดังกล่าวจะปรากฏทุกครั้งที่มีการถอดรหัสจดหมายอิเล็กทรอนิกส์ ถ้าไม่ต้องการให้แสดงข้อความนี้อีก สามารถยกเลิกได้ดังรูปที่ 5.50

รูปที่ 5.50 จดหมายอิเล็กทรอนิกส์ที่มีการเข้ารหัสถูกส่งมา

3. โปรแกรมจะแสดงรูปแม่กุญแจ เพื่อเป็นการระบุว่าเป็นจดหมายอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับ ซึ่งการเข้ารหัสลับนี้จะรวมถึงการเข้ารหัสลับไฟล์แนบด้วย
4. ถ้าหากไม่สามารถเปิดอ่านจดหมายอิเล็กทรอนิกส์เนื่องจากโปรแกรมไม่สามารถทำการถอดรหัสลับจดหมายอิเล็กทรอนิกส์ได้ดังรูปที่ 5.51 อาจเกิดจากหลายสาเหตุดังนี้
    - ผู้รับกรอกรหัสผ่านสำหรับใช้งานกุญแจส่วนตัวผิด
    - ผู้รับทำกุญแจสูญหายหรือถูกลบ
    - ผู้รับทำการติดตั้งใบรับรองดิจิทัลบนเครื่องคอมพิวเตอร์เครื่องอื่น
    - โปรแกรมไม่สามารถทำการถอดรหัสลับจดหมายอิเล็กทรอนิกส์ เนื่องจากการติดตั้งโปรแกรมไม่สมบูรณ์

Error Decrypting Message

You cannot read the message.

This might be because:

- You may have lost or deleted the Digital ID that the message is encrypted to.
- You may have installed the Digital ID that the message is encrypted to on another computer.
- The sender may have meant the message for somebody else.
- You do not have the necessary security package installed on this computer.

Outlook Express

รูปที่ 5.51 การถอดรหัสจดหมายอิเล็กทรอนิกส์ที่ไม่สำเร็จ

บทที่ 6
บทสรุปและแนวทางในการพัฒนาระบบในอนาคต

6.1 สรุปผลการทำงานของระบบ

จากการทำงานของระบบการออกใบรับรองดิจิทัล สรุปได้ว่าระบบนี้สามารถทำหน้าที่เสมือนเป็นหน่อยงาน (Certificate Authority) ในการออกใบรับรองดิจิทัล (Digital Certificate) ให้แก่บุคคลที่เข้ามาร้องขอใบรับรองดิจิทัล ซึ่งจะต้องได้รับการตรวจสอบจากผู้ดูแลระบบก่อนว่าสมควรได้รับใบรับรองหรือไม่ หลังจากนั้นแล้วจึงได้รับกุญแจส่วนตัวและใบรับรองดิจิทัลซึ่งมีกุญแจสาธารณะบรรจุอยู่ภายใน รวมทั้งนำไปใช้ในการเข้ารหัสถอดรหัสข้อมูลที่ถูกส่งไปในรูปแบบของอีเมล์ เพื่อให้เกิดความปลอดภัยในการส่งข้อมูล

6.2 ปัญหาและแนวทางในการแก้ไขระบบ

ปัญหาที่จะพบของระบบคือ

1. ระบบนี้สร้างขึ้นเพื่อเป็นกรณีศึกษาจึงได้ทำการจำลองการติดต่อสื่อสารของ Server และ Client ไว้ในคอมพิวเตอร์เครื่องเดียว โดยทำการติดตั้ง Web Server และ Web Root ไว้คนละ Drive หากจะนำไปใช้งานจริงในองค์กร หรือบนระบบเครือข่ายคงจะมีความซับซ้อนมากขึ้นกว่าที่เป็นอยู่
2. ในเรื่องของความปลอดภัยอันเนื่องมาจาก รายละเอียดของแบบฟอร์มที่น้อยไม่สามารถระบุตัวบุคคลได้เท่าที่ควร ถ้าหากมีการพัฒนาต่อ คงจะต้องให้ความสำคัญในเรื่องนี้มากขึ้นด้วย เช่น รหัสพนักงาน หรือ รหัสนักศึกษา
3. ระบบนี้ยังมีข้อจำกัดด้านภาษาที่จะต้องใช้ภาษอังกฤษทั้งหมด หากสามารถพัฒนาได้โดยใช้ภาษาไทยก็จะง่ายต่อการใช้งานมากขึ้น
4. ในการส่งข้อมูลผ่านทางอีเมล์ ยังจำกัดในเรื่องของการเข้ารหัสและถอดในรูปของ Text File เท่านั้น

6.3 อนาคตและการพัฒนาของระบบ

ในอนาคตคาดว่าสามารถนำระบบการออกใบรับรองดิจิทัล มาพัฒนาและนำมาใช้ภายในองค์กรได้ ก็จะทำให้เกิดประโยชน์ในเรื่องของความปลอดภัยในการส่งข้อมูลของผู้ใช้งานและยัง

สามารถลดค่าใช้จ่ายต่างๆของการทำใบรับรองดิจิทัลภายในองค์กรลงได้ หรือแม้กระทั้งทำการสร้างเป็นองค์กรออกใบรับรองดิจิทัล (Certificate Authority) ให้บริการภายนอก เพื่อประกอบธุรกรรมบนอินเตอร์เน็ตให้เกิดความปลอดภัยได้อีกด้วย

สำหรับแนวทางในการพัฒนาระบบต่อไปในอนาคต อาจจะมีการใช้อัลกอริทึมที่แข็งแรงมากกว่านี้ หรือสามารถนำไปประยุกต์ใช้งานกับ แอพพลิเคชันด้านอื่นๆ ที่ต้องการคุณสมบัติของการเข้ารหัสและถอดรหัสลับ รวมทั้งการสร้างลายมือชื่อดิจิทัลให้กับแฟ้มข้อมูลได้

บรรณานุกรม

กรองรัตน์ คามตะศิลา. 2545. **"การออกแบบและพัฒนา OpenSSL/OpenCA เพื่อเป็นหน่วยผู้ประกอบการรับรองระบบปฏิบัติการลีนุกซ์"**.
การประชุมวิชาการธุรกิจผ่านสื่ออิเล็กทรอนิกส์. ปทุมธานี:มหาวิทยาลัยธรรมศาสตร์ รังสิต.

สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ. 2547. **"Personal Certificate"**. [Online]. เข้าถึงได้จาก: http://gca.thaigov.net/content/service_personal0.php.

สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ. 2548. **"นโยบายใบรับรองดิจิทัล"**. [Online]. เข้าถึงได้จาก: http://gca.thaigov.net/content/download/G-CA-CP-v2.1.pdf .

บรรจง หะรังษี. 2547. **"ความรู้เบื้องต้นของการเข้ารหัสข้อมูล"**. [Online]. เข้าถึงได้จาก: http://thaicert.nectec.or.th/paper/encryption/intro_crypt.php.

สถาบันวิจัยเพื่อการพัฒนา. 2548. **"ลายมือชื่อและใบรับรองดิจิทัล"**. [Online]. เข้าถึงได้จาก: http://www.info.tdri.or.th/r4_ch1.htm .