ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล.

ระบบผู้ให้บริการออกใบรับรอง

CERTIFICATION AUTHORITY SYSTEM

H003462

โดย

กาญจนี ลิ้มศรีสกุลวงศ์

อาจารย์ที่ปรึกษา

ผศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์

วัน เดือน ปี 04 ธ.ค. 2550
เลขทะเบียน H003462
เลขเรียกหนังสือ วพ. ก428ร 2549
"ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล."

b18400 ก1
i1111669

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 2 ปีการศึกษา 2549

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

CERTIFICATION AUTHORITY SYSTEM

KANCHANI LIMSRISAKULWONG

A SYSTEM DEVELOPMENT PROJECT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2 / 2006

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

COPYRIGHT 2007

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่อนุญาตให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อ	ระบบผู้ให้บริการออกใบรับรอง
นักศึกษา	นางสาว กาญจนี ลิ้มศรีสกุลวงศ์
รหัสนักศึกษา	47066117
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2549
อาจารย์ที่ปรึกษา	ผศ.ดร. จันทร์บูรณ์ สถิตวิริยวงศ์

บทคัดย่อ

ปัจจุบันการทำธุรกรรมต่างๆ นั้นนิยมกระทำกันผ่านเครือข่ายสาธารณะที่เราเรียกว่าอินเทอร์เน็ต ใบรับรองดิจิทัลจึงมีความสำคัญในการที่จะช่วยยืนยันการมีตัวตนของบุคคลทั้ง 2 ฝ่ายในติดต่อสื่อสาร โครงงานนี้ได้ทำการพัฒนาระบบการเป็นผู้ประกอบการออกใบรับรองดิจิทัล โดยจำลองการทำงานระหว่างไคล์เอนท์และเซิร์ฟเวอร์ไว้ภายในเครื่องเดียวกัน มีการใช้ Apache 2.2.2 เป็นเว็บเซิร์ฟเวอร์ และพัฒนาระบบด้วยภาษา PHP ซึ่งใช้ตัวแปรภาษา PHP 5.2 มีการใช้ Openssl 0.9.8b ในการจัดการใบรับรองดิจิทัล ระบบมีการแจ้งข้อความเพื่อใช้ในการยืนยันการทำงานต่างๆ ถึงผู้ใช้ผ่านอีเมล์ โดยมี ArGosoft 1.8.8.8 เป็นเมล์เซิร์ฟเวอร์ และใช้ Outlook Express เป็นเมล์ไคล์เอนท์ ซึ่งซอฟต์แวร์ต่างๆ ทำงานบนระบบปฏิบัติการ Microsoft Windows XP

โครงงานนี้ได้ทำการพัฒนาระบบการเป็นผู้ประกอบการออกใบรับรองดิจิทัลที่สามารถทำการออกใบรับรองดิจิทัลสำหรับบุคคลให้แก่นักศึกษาและบุคคลกร สำหรับใช้ในการยืนยันตัวบุคคล และสามารถออกใบรับรองดิจิทัลสำหรับเครื่องแม่ข่ายภายในสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เพื่อใช้ในการรักษาความลับของข้อมูลในการสื่อสารระหว่างผู้ใช้งานกับเซิร์ฟเวอร์ ซึ่งจะทำงานผ่าน SSL

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Title	Certification Authority System
Student	Miss Kanchani Limsrisakulwong
Student ID	47066117
Degree	Master of Science
Programme	Information Science
Academic Year	2006
Advisor	Assist.Prof.Dr. Chanboon Sathitviriyawong

ABSTRACT

Nowadays the business affairs are popularly done through the public network which is called "Internet". So the Digital Certificate came to be important for mutual existence proof. This project is to develop the Certificate Authority: CA system by modeling the operation between client and server on the same computer. Apache 2.2.2 is used for web server and CA was developed by PHP with PHP 5.2 Interpreter, Management certificate by Openssl 0.9.8b. The message of process confirmation will be sent to used via e-mail which the mail server is ArGosoft 1.8.8.8 and mail client is Outlook Express. All software used in CA are operated on Microsoft Windows XP.

This project is to develop the Digital Certificate Issuing system for students and staff to prove the existence. It can also issue the Digital Certificate for network computer in KMITL to keep secret of the communications between users and server which is run on Security Socket Layer protocol (SSL).

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

ขอกราบขอบพระคุณ ผศ.ดร. จันทร์บูรณ์ สถิตวิริยวงศ์ อาจารย์ที่ปรึกษาโครงงาน ที่กรุณาให้ความรู้ คำปรึกษา และคำแนะนำต่างๆในการพัฒนาโครงงานนี้ให้สำเร็จลุล่วงไปด้วยดี

ขอกราบขอบพระคุณคณาจารย์ทุกท่านในคณะเทคโนโลยีสารสนเทศที่กรุณาถ่ายทอดความรู้ต่างๆที่สามารถนำมาใช้เป็นแนวทางในการศึกษาเพื่อเป็นประโยชน์ในการพัฒนาโครงงาน

ขอบคุณพี่ๆ และเพื่อนๆ ทุกคนที่คอยให้คำแนะนำ ช่วยเหลือและให้กำลังใจเสมอมา รวมทั้งเจ้าหน้าที่ทุกคนในคณะเทคโนโลยีสารสนเทศทุกคนที่ให้คำปรึกษาในการติดต่อสอบถามในทุกเรื่อง

สุดท้ายขอกราบขอบพระคุณคุณพ่อ คุณแม่ และบุคคลในครอบครัว ที่ให้กำลังและให้การอุปการะมาโดยตลอด ขอกราบขอบพระคุณเป็นอย่างสูง

คุณความดีที่ได้รับจากโครงงานนี้ ผู้เขียนขอมอบแด่ผู้มีพระคุณทุกท่าน

กาญจนี ลิ้มศรีสกุลวงศ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1

บทนำ

1.1. ความเป็นมาของโครงงาน

ในปัจจุบันเครือข่ายอินเทอร์เน็ตเป็นช่องทางการสื่อสารที่นิยมกันอย่างแพร่หลาย การทำธุรกรรม อิเล็กทรอนิกส์ต่างๆ ผ่านช่องทางนี้จึงนับว่าเป็นวิธีการที่สะดวกรวดเร็ว แต่ปัญหาที่ตามมาคือ ปัญหาด้านความปลอดภัยของและความน่าเชื่อถือของข้อมูล เนื่องจากเป็นเครือข่ายสาธารณะทุกคนสามารถเข้ามาใช้งานในเครือข่ายนี้ได้โดยที่เราไม่ทราบตัวตนที่แท้จริงของทั้งผู้ให้บริการและผู้ใช้บริการ ทำให้เกิดความเสี่ยงสูง ในการปลอมแปลงหรือการโจรกรรมข้อมูล ซึ่งเป็นสาเหตุของการติดต่อสื่อสารที่ผิดพลาดและล้มเหลว การสร้างความปลอดภัยและความน่าเชื่อถือสามารถทำได้โดยการใช้ใบรับรองดิจิทัล (Digital Certificate) ซึ่งเป็นการนำมาใช้สำหรับยืนยันตัวบุคคลและรักษาความลับในการติดต่อสื่อสารระหว่างกันและกัน ใบรับรองดิจิทัลเป็นเอกสารที่สร้างขึ้นโดยใช้หลักการของเทคโนโลยีการรักษาความปลอดภัยข้อมูล (Cryptographic) องค์ประกอบที่สำคัญที่ใช้ในการสร้างใบรับรองดิจิทัล คือ กุญแจส่วนตัว (Private key) กุญแจสาธารณะ (Public key) และข้อมูลส่วนบุคคล (Personal Information) ออกโดยหน่วยงานด้านเทคโนโลยีสารสนเทศที่เรียกว่า ผู้ให้บริการออกใบรับรอง (Certification Authority : CA) ที่ได้รับการยอมรับและมีความน่าเชื่อถือซึ่งในขณะนี้มีหลายองค์กรได้ดำเนินการเป็นผู้ประกอบการออกใบรับรองดิจิทัล ให้แก่องค์กรและบุคคลทั่วไป ซึ่งเป็นองค์กรกลางในการสร้างความเชื่อมั่นในการมีตัวตนอยู่จริงของบุคคลที่ทำธุรกรรมกันผ่านเครือข่ายอินเทอร์เน็ตแต่ยังพบว่ามีใช้แค่เพียงบางองค์กรเท่านั้นเนื่องจากมีค่าใช้จ่ายสูงในการขอใช้บริการ โดยการศึกษานี้จะทำการวิเคราะห์โครงสร้างภายในระบบของหน่วยผู้ให้บริการออกใบรับรอง (Certification Authority : CA) รวมทั้งทำการออกแบบระบบการออกใบรับรองดิจิทัล เพื่อเป็นทางเลือกหนึ่งในการลดค่าใช้จ่ายสำหรับองค์กรในขอใช้บริการนี้

โครงการพัฒนาระบบการออกใบรับรองดิจิทัลนี้ จึงเป็นระบบที่ออกใบรับรองดิจิทัลให้แก่บุคคลทั่วไป และเว็บไซต์ต่างๆ ที่เข้ามาลงทะเบียน เพื่อที่จะนำไปใช้ให้เกิดความปลอดภัยในการติดต่อสื่อสาร รวมทั้งให้บริการในการเผยแพร่ใบรับรองในสถานะต่างๆ เพื่อให้บุคคลภายนอกเข้ามานำข้อมูลไปใช้งานได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.2. วัตถุประสงค์ในการพัฒนาระบบ

1. เพื่อศึกษาเทคโนโลยีการเข้ารหัสข้อมูลโดยอาศัยหลักการของเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure :PKI) ด้วยอัลกอริทึม RSA ซึ่งจะใช้ซอฟต์แวร์ OpenSSL ที่เป็นซอฟต์แวร์แบบ Open Source ทำให้ประหยัดค่าใช้จ่ายในการพัฒนาและติดตั้งการใช้งานภายในองค์กร
2. เพื่อศึกษาระบบการเป็นผู้ประกอบการออกใบรับรองดิจิทัล เช่น ขั้นตอนในการเข้าลงทะเบียนของบุคคลหรือองค์กรต่างๆ ในการร้องขอใบรับรองดิจิทัล รวมทั้งการเผยแพร่และเพิกถอนใบรับรองดิจิทัล
3. เพื่อพัฒนาระบบการออกใบรับรองดิจิทัลในเรื่องของการเข้ารหัสถอดรหัสในการรักษาความลับของข้อมูลที่มีการติดต่อสื่อสารกันทำให้ข้อมูลมีความปลอดภัยรวมถึงการยืนยันการมีตัวตนอยู่จริงโดยจะไม่สามารถให้ผู้อื่นที่ไม่ได้รับอนุญาตเปิดอ่านข้อมูลได้
4. เพื่อเป็นการสนับสนุนการใช้งานใบรับรองดิจิทัลภายในองค์กรต่างๆ ที่มีค่าใช้จ่ายไม่สูงมากและแพร่หลายให้มากขึ้น

1.3. ประโยชน์ที่คาดว่าจะได้รับ

จากการศึกษาและพัฒนาระบบการออกใบรับรองดิจิทัล คาดว่าจะได้ประโยชน์และเป็นแนวทางในการสร้างความปลอดภัยของการสื่อสาร ดังนี้

1. เป็นการหลีกเลี่ยงค่าใช้จ่ายที่สูงในเชิงพาณิชย์ เนื่องจากระบบสามารถออกใบรับรองดิจิทัลสำหรับบุคคลทั่วไปที่เข้ามาลงทะเบียน โดยไม่เสียค่าใช้จ่าย จึงเป็นการลดค่าใช้จ่ายภายในองค์กรซึ่งจะสามารถนำไปใช้งานและพัฒนาต่อไป
2. ทำให้ข้อมูลที่ติดต่อสื่อสารกันผ่านทางอินเทอร์เน็ตนั้นมีความปลอดภัยโดยใช้หลักการทำงานของเทคโนโลยีการเข้ารหัส
3. ช่วยทำให้เกิดความเชื่อมั่นในการติดต่อสื่อสารกันระหว่างผู้ใช้บริการและผู้รับบริการ
4. เป็นที่รวบรวมใบรับรองดิจิทัลของสมาชิกที่เข้ามาลงทะเบียน เผยแพร่ใบรับรองดิจิทัลให้แก่บุคคลภายนอกที่ต้องการนำไปใช้งาน รวมทั้งทำการเพิกถอนใบรับรองที่หมดอายุโดยอัตโนมัติ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.4. ขอบเขตของการพัฒนาระบบ

1. พัฒนาระบบการให้บริการผ่านเว็บบราวซ์เซอร์ โดยมี Apache ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์
2. ใช้ SSL เพื่อรักษาความปลอดภัยของข้อมูล ในการสื่อสารระหว่างผู้ใช้กับระบบ
3. สามารถออกใบรับรองดิจิทัลแบบบุคคล ตามฟอร์แมทต่างๆ ได้ โดยใช้ OpenSSL
4. รองรับการขอยกเลิกใบรับรองดิจิทัล
5. มีขั้นตอนการยืนยันการทำงานระหว่างผู้ใช้กับระบบผ่านอีเมล
6. จำลองการทำงานระหว่างไคลเอนท์กับเซิร์ฟเวอร์ภายในเครื่องเดียวกัน

1.5. ขั้นตอนในการพัฒนาระบบงาน

1. การศึกษาความเป็นไปได้ในการพัฒนาระบบ
2. การศึกษาและวิเคราะห์ทฤษฎีที่เกี่ยวข้องและเลือกใช้ให้เข้ากับระบบ
3. การพัฒนาและทดสอบระบบให้สามารถออกใบรับรองดิจิทัลได้
4. การทดลองเพื่อนำใบรับรองดิจิทัลไปใช้ในกระบวนการในการเข้าและถอดรหัสข้อมูล
5. การตรวจสอบความผิดพลาดและแนวทางการแก้ไข
6. การกำหนดแนวทางการพัฒนาระบบต่อไปและอนาคตของการใช้งานใบรับรองดิจิทัล
7. สามารถนำใบรับรองที่ได้มานั้นไปใช้ให้เกิดผล

1.6. วิธีการดำเนินงาน

ในการศึกษาและพัฒนาระบบการออกใบรับรองดิจิทัลนี้ เพื่อให้ศึกษาครอบคลุมวัตถุประสงค์และขอบเขตในการพัฒนาระบบ จึงได้กำหนดขั้นตอนในการศึกษาไว้ดังนี้

1. ในการขอใบรับรองดิจิทัล ผู้ใช้ต้องทำการลงทะเบียนเพื่อขอเข้าใช้งานระบบการออกใบรับรองดิจิทัลผ่านทางเว็บไซต์
2. ผู้ดูแลระบบทำการตรวจสอบผู้ใช้ที่เข้ามาในระบบเพื่อร้องขอใบรับรองดิจิทัล และส่งรหัสผ่านเพื่อสามารถเข้าใช้ระบบผ่านทางอีเมล
3. ผู้ที่ต้องการขอใบรับรองดิจิทัลเข้าใช้งานในระบบจากรหัสผ่านที่ได้รับทางอีเมลและทำการกรอกรายละเอียดในการร้องขอใบรับรองดิจิทัล รวมทั้งสามารถดาวน์โหลด Private Key ไปเก็บไว้ในเครื่องตัวเองโดยที่จะต้องเก็บไว้เป็นความลับ
4. ผู้ดูแลระบบทำการตรวจสอบการร้องขอใบรับรองดิจิทัล และทำการออกใบรับรองดิจิทัลให้กับผู้ที่มาร้องขอ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5. ผู้ทำการร้องขอได้รับใบรับรองดิจิทัล รวมทั้งสามารถดาวน์โหลดใบรับรองดิจิทัล หรือ Public Key ไปเก็บไว้ในเครื่องตัวเอง เพื่อเผยแพร่และใช้ในกระบวนการเข้ารหัสและถอดรหัส

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่2

ทฤษฎีที่เกี่ยวข้อง

ปัจจุบันเครือข่ายอินเทอร์เน็ตเป็นช่องทางการติดต่อสื่อสารนิยมและแพร่หลายมากที่สุด การทำธุรกรรมที่ใช้ข้อมูลในการสื่อสารระหว่างกันมีหลากหลายรูปแบบซึ่งกระทำผ่านระบบเครือข่ายอินเทอร์เน็ตในรูปแบบต่างๆ โดยที่บุคคลหรือองค์กรที่ติดต่อด้วยนั้น อาจจะไม่เคยมีความสัมพันธ์หรือรู้จักกันมาก่อน กลายเป็นช่องทางหนึ่งที่ทำให้ข้อมูลนั้นขาดความปลอดภัย เนื่องจากเราไม่สามารถมั่นใจได้ว่า บุคคลหรือองค์กรที่ติดต่อด้วยคือใคร มีตัวตนจริงหรือไม่ ดังนั้นจึงจำเป็นที่จะต้องมีกลไกในการยืนยันการมีตัวตน นั่นคือ ใบรับรองดิจิทัล (Digital Certificate)

ผู้ให้บริการออกใบรับรอง (Certification Authority : CA) จะเป็นผู้ออกใบรับรองดิจิทัลให้แก่บุคคลหรือองค์กรต่างๆ ที่เข้ามาทำการลงทะเบียน ซึ่งข้อมูลในใบรับรองดิจิทัลนั้น จะแสดงถึงการมีตัวตนอยู่จริงระหว่างผู้ที่ทำการติดต่อสื่อสารกัน โดยที่สามารถนำมาประยุกต์ใช้งานได้ 2 รูปแบบ คือ การเข้ารหัส/การถอดรหัสลับ (Encryption/Decryption) และการลงลายมือชื่อดิจิทัล (Digital Signature) กับข้อมูลที่กระทำการรับส่งระหว่างกัน ระบบการออกใบรับรองดิจิทัลนี้ จะใช้เทคโนโลยีของการเข้ารหัสเป็นเทคโนโลยีหลัก ที่มีชื่อเรียกว่า เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI) ซึ่งมีระบบกุญแจคู่เป็นพื้นฐานสำคัญ อันประกอบด้วย กุญแจส่วนตัว (Private Key) และ กุญแจสาธารณะ (Public Key)

2.1 ระบบการรักษาความปลอดภัยที่ผู้ประกอบการออกใบรับรองควรมี

ความปลอดภัยเป็นหัวใจสำคัญที่จะสร้างความเชื่อมั่นในการทำธุรกรรมกันระหว่างผู้ใช้บริการและผู้ให้บริการผ่านทางเครือข่ายอินเทอร์เน็ต ซึ่งเทคโนโลยีความปลอดภัยของข้อมูลควรจะสามารถรองรับองค์ประกอบของการรักษาความปลอดภัยของข้อมูลทั้ง 4 ด้าน ดังนี้

1. การพิสูจน์สิทธิ์ (Authentication) หมายถึง การพิสูจน์ตัวตนว่าเป็นตัวจริง คือ ความสามารถในการระบุได้ว่าบุคคลที่ติดต่อด้วยนั้นเป็นบุคคลตามที่กล่าวอ้างถึงจริง
2. การรักษาความลับของข้อมูล (Data Confidentiality) หมายถึง ความสามารถในการรักษาความลับโดยผู้ที่ไม่ได้รับอนุญาตจะไม่สามารถเปิดอ่านข้อมูลที่เก็บไว้หรือข้อมูลที่มีการส่งผ่านเครือข่ายได้
3. การรักษาความถูกต้องครบถ้วนของข้อมูล (Data Integrity) หมายถึง ความสามารถในการรักษาความถูกต้องของข้อมูลและไม่มีการเปลี่ยนแปลงแก้ไขข้อมูลก่อนถึงผู้รับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. การป้องกันการปฏิเสธความรับผิดชอบ (Non-repudiation) หมายถึง ความสามารถในการป้องกันการปฏิเสธความรับผิดชอบจากฝ่ายต่างๆ ที่เกี่ยวข้องว่าไม่ได้มีการส่งหรือรับข้อมูล

2.2 เทคโนโลยีในการรักษาความปลอดภัย

เทคโนโลยีระบบการรหัสแบบกุญแจสาธารณะ (PKI) ได้ถูกนำมาใช้ในการรักษาความปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ในปัจจุบัน โดยการทำให้ข้อมูลที่ส่งผ่านไปทางเครือข่ายอยู่ในรูปแบบที่ไม่สามารถอ่านออกได้ ด้วยการเข้ารหัส (Encryption) ทำให้ข้อมูลนั้นเป็นความลับซึ่งผู้มีสิทธิ์จริงเท่านั้นถึงจะสามารถอ่านข้อมูลนั้นได้ด้วยการถอดรหัส (Decryption) สำหรับการเข้ารหัสถอดรหัสนั้นต้องอาศัยสมการทางคณิตศาสตร์ที่ซับซ้อนและต้องอาศัยกุญแจซึ่งอยู่ในรูปของพารามิเตอร์ที่กำหนดไว้ สำหรับอัลกอริทึมที่ใช้ในการสร้างกุญแจและขนาดของคู่กุญแจจะถูกกำหนดโดยผู้ให้บริการออกใบรับรอง อัลกอริทึมที่นิยมใช้คือ RSA (Ron Rivest, Adi Shamir and Leonard Adleman), DSA (Digital Signature Algorithm) ขนาดบิตที่ใช้ขึ้นอยู่กับความเหมาะสมของแต่ละอัลกอริทึม หากมีจำนวนบิตสูงขึ้นจะยิ่งมีความปลอดภัยมากขึ้น แต่จะส่งผลให้การเข้ารหัสและการถอดรหัสข้อมูลใช้เวลามากขึ้น ซึ่งความปลอดภัยจะขึ้นอยู่กับความยาวของกุญแจ สำหรับกุญแจของผู้ให้บริการออกใบรับรองที่นิยมใช้จะถูกสร้างด้วยอัลกอริทึม RSA ที่มีขนาด 512 บิตขึ้นไป

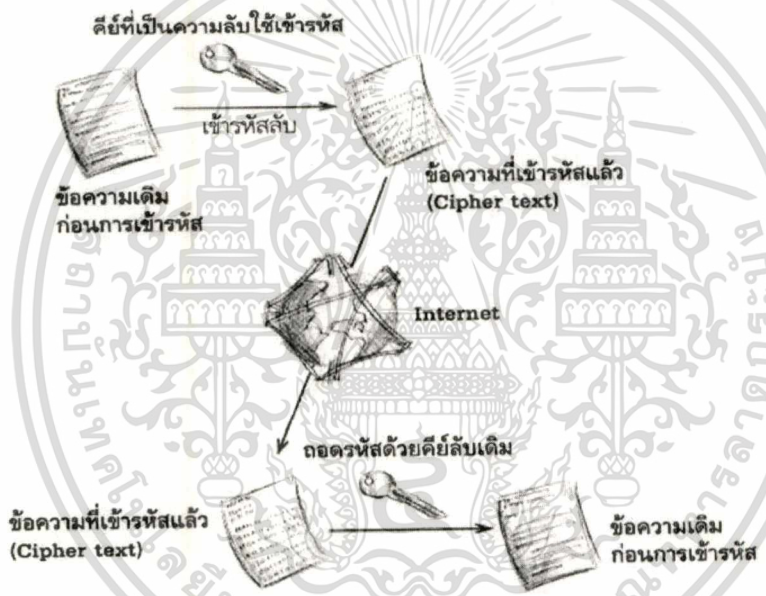
2.2.1 การเข้ารหัส (Encryption)

การเข้ารหัสเป็นกระบวนการสำหรับแปลงข้อมูลธรรมดา (Plaintext) ที่เราสามารถอ่านได้ไปอยู่ในรูปของข้อมูลลับ (Cipher text) ที่ไม่สามารถอ่านได้ ข้อมูลที่อยู่ในรูปแบบของการเข้ารหัสเรียกว่า Cryptogram การเข้ารหัสมีหลักการสำคัญคือ เมื่อเข้ารหัสไปแล้วต้องสามารถถอดรหัสกลับคืนมาได้ และสำหรับการถอดรหัส (Decipher) เป็นวิธีที่ใช้เพื่อทำให้อักขระที่ไม่สามารถ อ่านได้ กลับมาเป็นข้อความธรรมดาเหมือนเดิม เราเรียกวิธีการที่ใช้ในการถอดรหัสว่า Cryptanalysis การเข้ารหัสและถอดรหัส เราจะใช้สิ่งที่เรียกว่า กุญแจ ซึ่งจะนำไปใช้ในกระบวนการแปลงข้อมูลที่ทราบเพียงผู้รับและผู้ส่งข้อมูลเท่านั้น สำหรับการเข้ารหัสข้อมูลแบ่งออกได้เป็น 3 ประเภท คือ

<u>การเข้ารหัสข้อมูลแบบกุญแจสมมาตร (Symmetric Key Cryptography หรือ Secret Key Cryptography) [1]</u> เป็นการเข้าและถอดรหัสโดยใช้กุญแจส่วนตัวที่เหมือนกัน กุญแจที่ใช้เราเรียกว่า กุญแจลับ (Secret Key) ที่จะทราบเฉพาะผู้เข้ารหัสข้อมูลและผู้รับข้อมูลเท่านั้น การเข้ารหัสแบบนี้เป็นการเข้ารหัสโดยใช้วิธีการแทนที่ (Substitution) และวิธีสลับตำแหน่ง (Transposition) เหมาะสำหรับในสภาวะแวดล้อมที่สามารถแลกเปลี่ยนกุญแจระหว่างผู้ใช้กันได้ง่าย เช่น ตาม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หน่วยงานทั่วไป หรืออาจใช้เพื่อเข้ารหัสข้อมูลที่เก็บอยู่ในดิสก์ ซึ่งผู้ใช้ทุกคนจะต้องใช้ อัลกอริทึมเดียวกันหมด ข้อดีคือในการเข้ารหัสและถอดรหัสข้อมูลใช้เวลาน้อยเพราะว่าอัลกอริทึมที่ใช้ไม่สลับซับซ้อน รวมทั้งขนาดของข้อมูลหลังจากทำการเข้ารหัสแล้วมีการเปลี่ยนแปลงไม่มากนัก แต่ข้อเสียคือ ชื่อผู้ส่งอาจถูกปลอมแปลงได้ และเกิดปัญหาในการบริหารจัดการกุญแจ (key management) เช่น ถ้าเรามีการติดต่อระหว่างผู้ใช้ n คน เราจำเป็นที่จะต้องมีรหัสทั้งหมด n รหัสและต้องคอยจดจำว่ารหัสใดใช้กับใคร ซึ่งเป็นการยุ่งยากมาก ดังนั้นในการแก้ปัญหาเราอาจจะต้องมีกุญแจทั้งหมด n(n-1)/2 อันจึงจะทำให้การส่งข้อมูลของทุกคู่มีความปลอดภัย เพราะถึงผู้รับจะเป็นคนเดียวกัน แต่ผู้ส่งมีมากกว่าหนึ่งคน ก็ควรจะมีกุญแจที่แตกต่างกันมิฉะนั้นจะทำให้ผู้ส่งที่มีกุญแจเหมือนกันสามารถอ่านข้อมูลของอีกผู้หนึ่งได้ ดังรูปที่ 2.1

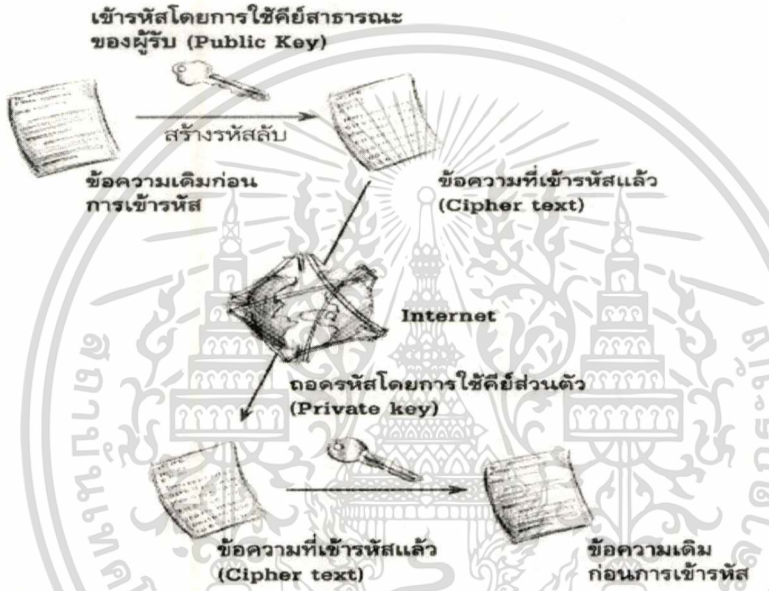


รูปที่ 2.1 ขั้นตอนการเข้ารหัสและถอดรหัส แบบกุญแจสมมาตร [2]

การเข้ารหัสข้อมูลแบบกุญแจอสมมาตร (Asymmetric Key Cryptography หรือ Public Key Cryptography) [1] เป็นการเข้ารหัสและถอดรหัสด้วยกุญแจต่างกันคือมีกุญแจสองดอก มักใช้ในสภาวะแวดล้อมที่การแลกเปลี่ยนกุญแจเป็นไปได้ยาก เช่น เน็ทเวิร์กสาธารณะใหญ่ๆ อย่างอินเทอร์เน็ต เป็นต้น ระบบการเข้าและถอดรหัสแบบกุญแจสาธารณะนี้จะใช้แนวคิดของการมีกุญแจเป็นคู่ๆ ที่สามารถ เข้าและถอดรหัสของกันและกันเท่านั้นได้ กุญแจแรกเรียกว่า กุญแจส่วนตัว (private key) ซึ่งจะเก็บเป็นความลับมีเจ้าของคนเดียวเท่านั้นที่รู้ และจะมีคู่ของกุญแจดังกล่าวที่ส่งให้ผู้อื่นใช้ได้ เรียกว่า กุญแจสาธารณะ (Public Key)โดยจะถูกแจกจ่ายให้ผู้อื่นที่ต้องการทำการติดต่อด้วย โดยจะเน้นที่ ผู้รับเป็นหลัก คือ จะใช้กุญแจสาธารณะของผู้รับซึ่งเป็นที่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เปิดเผยในการเข้ารหัส และจะใช้กุญแจส่วนตัวของผู้รับในการถอดรหัส ข้อดีคือ สามารถบริหารจัดการกับกุญแจได้ง่ายเนื่องจากใช้กุญแจ เพียง 2n อัน(n คือ จำนวนผู้ใช้) เท่านั้น คือ กุญแจส่วนตัว และ กุญแจสาธารณะของแต่ละคนและไม่ต้องจำว่าใช้กุญแจคู่ไหนกับใครเพราะสามารถเปิดเผยให้กับใครก็ได้ที่เราต้องการติดต่อด้วย นอกจากนี้กุญแจอสมมาตรยังสามารถนำมาใช้ในการสร้างลายมือชื่ออิเล็กทรอนิกส์ได้อีกด้วย แต่มีข้อเสียคือ ต้องใช้เวลามากเพราะว่าอัลกอริทึมที่ใช้มีความซับซ้อนมาก และข้อมูลหลังจากทำการเข้ารหัสแล้วจะมีขนาดใหญ่กว่าเดิมมาก จะทำให้เกิดปัญหาในการใช้งานผ่านเครือข่ายอินเทอร์เน็ต ดังรูปที่ 2.2



รูปที่ 2.2 ขั้นตอนการเข้ารหัสและถอดรหัส แบบกุญแจอสมมาตร [2]

One-Way Function หรือ Hash Function การเข้ารหัสแบบ Hash Function คือการเข้ารหัสประเภทเดียวที่ไม่มีการใช้กุญแจในการเข้ารหัส-ถอดรหัส จึงไม่มีการถอดรหัสกลับมายังข้อความเดิม โดยเป็นการใส่ข้อมูลเข้าไปยังฟังก์ชันที่เรียกว่า Hash function แล้วคำนวณค่าๆ หนึ่งออกมาเรียกว่าค่า Hash-value ซึ่งมีความยาวประมาณ 128 หรือ 160 bits โดยยึดหลักว่า จะไม่มี 2 inputs ใดๆ เมื่อคำนวณค่า Hash-value แล้ว ค่า Hash-value จะมีค่าเดียวกัน ใช้สำหรับงานประเภท Digital Signature หรือการยืนยันความคงเดิมของข้อมูล (data integrity) เพื่อตรวจสอบว่าข้อมูลที่ส่งมานั้นได้ถูกเปิดอ่านแล้วหรือไม่หรือเป็นการที่ข้อมูลถูกเข้ารหัส แล้วสร้างลายเซ็นขึ้นมา เพื่อนำมาใช้พิสูจน์สิทธิ์ความเป็นเจ้าของในภายหลังนั่นเอง มักใช้ควบคู่ไปกับ Public Key System

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2.2 มาตรฐานขบวนการรหัสข้อมูล

ในปัจจุบันได้มีมาตรฐานในการเข้ารหัสข้อมูลหลายวิธี ซึ่งในการเข้ารหัสแบบสมมาตรและอสมมาตรนั้นก็จะมีอัลกอริทึมมาตรฐานให้เลือกใช้แตกต่างกันตามความเหมาะสม ขึ้นอยู่กับความยาวของรหัสข้อมูลรวมถึงขั้นตอนการรหัสที่ใช้ ดังตัวอย่างในตารางที่ 2.1

ตารางที่ 2.1 เปรียบเทียบมาตรฐานต่างๆ ของการรหัสข้อมูล [3]

ประเภท	มาตรฐาน	ความยาวของกุญแจ(บิต)	เจ้าของเทคโนโลยี	ขั้นความปลอดภัย	หมายเหตุ
กุญแจสมมาตร	DES	56 หรือ 128	NSA, ANSI	ปานกลาง	เป็นมาตรฐานที่นิยมใช้มากที่สุดของการรหัสแบบกุญแจสมมาตร
	3DES	168	NSA, ANSI	สูง	ใช้ 2 หรือ 3 กุญแจ และระบบผ่านหลายขั้นตอน
	RC5	ไม่ตายตัว	RSA	สูง	ถูกนำไปใช้ทางการพาณิชย์มาก
กุญแจอสมมาตร	RSA	512 - 2048	RSA	สูง	ใช้เวลามากและความยาวกุญแจควรจะเป็นอย่างต่ำ 1,024 บิต
	ECC	160	Certicom	สูง	เร็วกว่า RSA

อัลกอริทึมมาตรฐานสำหรับการเข้ารหัสแบบสมมาตร ตัวอย่างเช่น

- **DES (Digital Encryption Standard)** เกิดขึ้นมาจากทีมพัฒนาของบริษัท IBM ประเทศสหรัฐอเมริกา ในปี ค.ศ. 1960โดย US Federal Standard มาตรฐานการเข้ารหัสแบบ DES นี้จะมีความปลอดภัยสูงมากเนื่องจากมีการเข้ารหัสข้อมูลโดยวิธี Feistel Ciphers ถึง 16 ครั้ง สามารถทนทานต่อผู้ต้องการเจาะรหัส (cryptanalysis)โดยหลักการทำงานจะทำการแบ่งข้อมูลที่จะทำการเข้ารหัสหรือถอดรหัสออกเป็นบล็อก (Block) แต่ละบล็อกจะมีขนาด 64 บิต และจำนวนความยาวของกุญแจลับที่ใช้ในปัจจุบันจะมีขนาด 56 บิต จากเดิม 128 บิต แต่การทำ DES นั้นมีข้อจำกัด คือ ขนาดของกุญแจรหัสลับนั้นอาจไม่มีเพียงพอในการรักษาความปลอดภัย เราสามารถใช้อีกมาตรฐานหนึ่งที่เรียกว่า Triple DES (3DES) ซึ่งเป็นการนำ DES มาทำการเข้ารหัสซ้ำ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กันถึง 3 ครั้ง โดยมาตรฐานนี้จะใช้กุญแจลับที่มีขนาดความยาว 168 บิต แต่สำหรับองค์กรใดที่ต้องการใช้มาตรฐานนี้จะต้องทำการขออนุญาตใช้งานกับรัฐบาลอเมริกาก่อน จึงจะสามารถนำมาใช้งานได้

- **AES (Advanced Encryption Standard)** ได้เข้ามาแทนที่ Triple DES ถูกพัฒนาขึ้นโดย Joan Daemen และ Vincent Rijmen ในปี 2000 และได้รับการคัดเลือกโดยหน่วยงาน National Institute of Standard and Technology (NIST) ของสหรัฐอเมริกาให้เป็นมาตรฐานในการเข้ารหัสชั้นสูงของประเทศ เป็นอัลกอริทึมที่มีความเร็วสูงและมีขนาดกะทัดรัดโดยสามารถใช้กุญแจที่มีความยาวขนาด 128, 192 และ 256 บิต

อัลกอริทึมมาตรฐานสำหรับการเข้ารหัสแบบอสมมาตร ตัวอย่างเช่น

- **RSA (Rivest-Shamir-Adelman Encryption)** การเข้ารหัสข้อมูลแบบนี้ถูกประดิษฐ์ขึ้นใน ค.ศ. 1978 โดย Ronal L. Rivest, Adi Sharmir, และ Leonard Adleman และในปัจจุบันนี้ยังสามารถใช้รักษาความปลอดภัยของข้อมูลได้เป็นอย่างดี อัลกอริทึมนี้สามารถถูกใช้เข้ารหัส แลกเปลี่ยนกุญแจ และการลงลายเซ็นอิเล็กทรอนิกส์

  คุณสมบัติของการเข้ารหัสแบบ RSA

  ก. การเข้ารหัสแบบ RSA นั้นเป็นการเข้ารหัสแบบ Block Cipher

  ข. ปกติการเข้ารหัสแบบ RSA จะช้ากว่าการเข้ารหัสแบบอื่นๆ มาก เนื่องจากว่าต้องใช้การคำนวณที่สลับซับซ้อนและขนาดกุญแจที่ใช้มีขนาดใหญ่มากเมื่อเทียบกับการเข้ารหัสแบบ DES แล้วนั้น การเข้ารหัสแบบ RSA จะช้ากว่าประมาณ 1,000 เท่า

  ค. เนื่องจากความช้าในการเข้ารหัสข้อมูล จึงไม่นิยมเอา RSA ไปใช้ในการเข้ารหัสข้อความที่มีขนาดใหญ่ แต่จะเอาไปใช้ในการเข้ารหัสข้อมูลขนาดเล็กที่ต้องการความปลอดภัยสูงมากๆ เช่น ใช้ในการเข้ารหัสและแจกจ่าย Secret Key ที่ใช้เป็น Session Key ในการติดต่อ สื่อสารกันระหว่างเครื่องคอมพิวเตอร์ในแต่ละครั้ง

- **ECC (Elliptic-Curve Cryptography)** เป็นทางเลือกหนึ่งที่ส่ง Public key cryptography ซึ่ง Elliptic curves เป็นวิธีที่กำหนดฟิลด์ที่แน่นอน เช่น ความจริง และเลขที่มีที่มา และมีการวางอนาล็อกไปที่ปัญหาพิจารณาลอการิทึม

  อัลกอริทึม Elliptic-curve เหมือนกับอัลกอริทึม RSA หรือ Diffie-Hellman ที่ใช้ระหว่างสองเครื่องในการจัดการ หรือคล้ายกับลายมือชื่ออิเล็กทรอนิกส์ อัลกอริทึมนี้มีความปลอดภัย และเร็วกว่า RSA และ Diffie-Hellman ที่ทำหน้าที่ในการใช้กุญแจเข้ารหัสสั้น คือ Hacker สามารถที่จะแก้ปัญหาในการเจาะการเข้ารหัสได้ยากกว่า โดย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Hacker ต้องหาจุดที่กำหนดได้ใน theoretical curve แทนที่การคาดเดาหมายเลข ซึ่งเป็นอัลกอริทึมที่ทำให้มีความปลอดภัยในระดับสูง

- **DSS (Digital Signature Standard)** อัลกอริทึมนี้ได้รับการพัฒนาขึ้นมาโดย National Security Agency ในประเทศสหรัฐอเมริกาและได้รับการรับรองโดย NIST ให้เป็นมาตรฐานกลางสำหรับการลงลายมือชื่ออิเล็กทรอนิกส์ในประเทศสหรัฐอเมริกา โดยใช้ SHA (Secure Hash Algorithm) มาตรฐาน DSS ใช้อัลกอริทึมที่ออกแบบสำหรับการทำหน้าที่ลงลายมือชื่อดิจิทัล (Digital Signature Function) แต่เพียงอย่างเดียว ไม่ได้ใช้สำหรับเข้ารหัสลับ (encryption) หรือการแลกเปลี่ยนกุญแจ (key exchange) ซึ่งแตกต่างจาก RSA
- **Message Digest** หรือเรียกสั้นๆ ว่าไดเจสต์ แปลว่าข้อความสรุปจากเนื้อหาข้อความตั้งต้น โดยปกติข้อความสรุปจะมีความยาวน้อยกว่าความยาวของข้อความตั้งต้นมาก จุดประสงค์สำคัญของอัลกอริทึมนี้คือ การสร้างข้อความสรุปที่สามารถใช้เป็นตัวแทนของข้อความตั้งต้นได้ โดยทั่วไปข้อความสรุปจะมีความยาวอยู่ระหว่าง 128 ถึง 256 บิต และจะไม่ขึ้นกับขนาดความยาวของข้อความตั้งต้น

ไดเจสต์เป็นเครื่องมือที่สำคัญที่สามารถใช้ในการตรวจสอบว่าไฟล์ในระบบที่ใช้งานมีการเปลี่ยนแปลงแก้ไขหรือไม่ (ไม่ว่าจะโดยเจตนาหรือไม่เจตนา) บางครั้งการเปลี่ยนแปลงแก้ไขอาจถูกกระทำโดยผู้ที่ไม่มีสิทธิ์ เช่น ผู้บุกรุก เป็นต้น วิธีการใช้ไดเจสต์เพื่อตรวจสอบไฟล์ในระบบคือให้เลือกใช้อัลกอริทึมหนึ่ง เช่น MD5 เพื่อสร้างไดเจสต์ของไฟล์ในระบบและเก็บไดเจสต์นั้นไว้อีกที่หนึ่งนอกระบบ ภายหลังจากระยะเวลาหนึ่งที่กำหนดไว้ เช่น 1 เดือน ก็มาคำนวณไดเจสต์ของไฟล์เดิมอีกครั้งหนึ่ง แล้วเปรียบเทียบไดเจสต์ใหม่นี้กับไดเจสต์ที่เก็บไว้นอกระบบว่าตรงกันหรือไม่ ถ้าตรงกัน ก็แสดงว่าไฟล์ในระบบยังเป็นปกติเช่นเดิม และยังเป็นส่วนหนึ่งของการลงลายมือชื่ออิเล็กทรอนิกส์ กล่าวคือการลงลายมือชื่ออิเล็กทรอนิกส์ในปัจจุบันจะใช้การลงลายมือชื่อกับไดเจสต์ของข้อความตั้งต้นแทนการลงลายมือชื่อกับข้อความตั้งต้นทั้งข้อความ

<u>คุณสมบัติที่สำคัญของอัลกอริทึมสำหรับสร้างไดเจสต์ มีดังนี้</u>

ก. ทุกๆ บิตของไดเจสต์จะขึ้นอยู่กับทุกบิตของข้อความตั้งต้น

ข. ถ้าบิตใดบิตหนึ่งของข้อความตั้งต้นเกิดการเปลี่ยนแปลง เช่น ถูกแก้ไข ทุกๆ บิตของไดเจสต์จะมีโอกาสร้อยละ 50 ที่จะแปรเปลี่ยนค่าไปด้วย ซึ่งหมายถึงว่า 0 เปลี่ยนค่าเป็น 1 และ 1 เปลี่ยนเป็น 0

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คุณสมบัติข้อนี้สามารถอธิบายได้ว่าการเปลี่ยนแปลงแก้ไขข้อความตั้งต้นโดยผู้ไม่ประสงค์ดีแม้ว่าอาจแก้ไขเพียงเล็กน้อยก็ตาม เช่น เพียง 1 บิตเท่านั้น ก็จะส่งผลให้ผู้รับข้อความทราบว่าข้อความที่ตนได้รับไม่ใช่ข้อความตั้งต้น

ค. โอกาสที่ข้อความตั้งต้น 2 ข้อความใดๆ ที่มีความแตกต่างกัน จะสามารถคำนวณได้ค่าไดเจสต์เดียวกันมีโอกาสน้อยมาก

คุณสมบัติข้อนี้ทำให้แน่ใจได้ว่า เมื่อผู้ไม่ประสงค์ดีทำการแก้ไขข้อความตั้งต้น ผู้รับข้อความที่ถูกแก้ไขไปแล้วนั้นจะสามารถตรวจพบได้ถึงความผิดปกติที่เกิดขึ้นอย่างแน่นอน

อย่างไรก็ตามในทางทฤษฎีแล้ว มีโอกาสที่ข้อความ 2 ข้อความที่แตกต่างกันจะสามารถคำนวณแล้วได้ค่าไดเจสต์เดียวกัน ปัญหานี้เรียกกันว่าการชนกันของไดเจสต์ (Collision) อัลกอริทึมสำหรับสร้างไดเจสต์ที่ดีควรจะมีโอกาสน้อยมากๆ ที่จะก่อให้เกิดปัญหาการชนกันของไดเจสต์

<u>อัลกอริทึมสำหรับสร้างไดเจสต์ [1] ตัวอย่างเช่น</u>

ก. **อัลกอริทึม MD5** ผู้พัฒนาคือ Rivest โดยพัฒนาต่อจาก MD4 เพื่อให้มีความปลอดภัยที่สูงขึ้น ถึงแม้จะเป็นที่นิยมใช้งานกันอย่างแพร่หลาย แต่ต่อมาในปี 1996 ก็มีผู้พบจุดบกพร่องของ MD5 (เช่นเดียวกับ MD4) จึงทำให้ความนิยมเริ่มลดลง MD5 ผลิตไดเจสต์ที่มีขนาด 128 บิต

ข. **อัลกอริทึม SHA (Secure Hash Algorithm)** อัลกอริทึม SHA ได้รับแนวคิดในการพัฒนามาจาก MD4 และได้รับการพัฒนาขึ้นมาเพื่อใช้งานร่วมกับอัลกอริทึม DSS (ซึ่งใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์) หลังจากที่ได้มีการตีพิมพ์เผยแพร่อัลกอริทึมนี้ได้ไม่นาน NIST ก็ประกาศต่อมาว่าอัลกอริทึมจำเป็นต้องได้รับการแก้ไขเพิ่มเติมเล็กน้อยเพื่อให้สามารถใช้งานได้อย่างเหมาะสม SHA สร้างไดเจสต์ที่มีขนาด 160 บิต

ค. **อัลกอริทึม SHA-1** เป็นอัลกอริทึมที่แก้ไขเพิ่มเติมเล็กน้อยจาก SHA การแก้ไขเพิ่มเติมนี้เป็นที่เชื่อกันว่าทำให้อัลกอริทึม SHA-1 มีความปลอดภัยที่สูงขึ้น SHA-1 สร้างไดเจสต์ที่มีขนาด 160 บิต

2.2.3 ลักษณะของการเข้ารหัสข้อมูลที่ดี (Characteristics of Good Cipher)

1. ระดับความปลอดภัยของข้อมูลที่ได้ ควรจะแปรผันกับความยากของการเข้ารหัสข้อมูลนั้นคือวิธีการเข้ารหัสนั้นมีความซับซ้อนมากควรให้ระดับความปลอดภัยของข้อมูลที่สูงด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. ไม่ควรมีข้อจำกัดในการเลือกใช้กุญแจเข้ารหัส และในการเลือกใช้วิธีการเข้าสำหรับข้อความลักษณะใดลักษณะหนึ่ง เพราะหากการเลือกใช้นั้นมีความยากและไม่สะดวกแล้วการเข้ารหัสนั้นไม่เป็นที่นิยมใช้
3. กระบวนการนำวิธีการเข้ารหัสไปใช้จะต้องมีความสะดวกและง่าย เพราะหากการเข้ารหัสยากมากเกินไปแล้ว อาจทำให้เกิดความผิดพลาดในระหว่างกระบวนการพัฒนาและนำไปใช้งานได้
4. ความผิดพลาดของการเข้ารหัส ณ จุดใดจุดหนึ่งของข้อมูลจะต้องไม่ขยายไปสู่ส่วนอื่นๆ
5. เมื่อเสร็จสิ้นจากการเข้ารหัสข้อมูลแล้ว ขนาดของข้อมูล Cipher Text ต้องมีขนาดไม่ใหญ่กว่าขนาดของ Clear Text

ปัญหาประการหนึ่งในการแจกจ่ายกุญแจสาธารณะในระบบเครือข่ายไปยังผู้ใช้ในระบบ คือ การพิสูจน์ว่าผู้ใช้นั้นได้รับกุญแจจริงหรือไม่ เพราะอาจเกิดการปลอมแปลงกุญแจจากผู้ไม่ประสงค์ดีบุกรุกเข้ามาในระบบได้ ดังนั้นจึงต้องมีวิธีที่สามารถบอกได้ว่ากุญแจนั้นเป็นกุญแจจริง (Genuine Key) วิธีการที่นำมาใช้พิสูจน์ก็คือการใช้ลายมือชื่อดิจิทัล (Digital Signature)

2.3 ลายมือชื่อดิจิทัล

เป็นลายมือชื่ออิเล็กทรอนิกส์ ที่สร้างจากเทคโนโลยีเข้ารหัสด้วยกุญแจสาธารณะ ในการลงลายมือชื่อ ดิจิตอลกำกับข้อความที่ต้องการส่งผ่านเครือข่าย ผู้ส่งข้อความจะใช้กุญแจส่วนตัวของตนในการลงลายมือชื่อโดยผ่านกระบวนการทางคณิตศาสตร์ ผู้รับจะสามารถตรวจสอบความถูกต้องของลายมือชื่อดังกล่าวโดยใช้กุญแจสาธารณะของผู้ส่ง ซึ่งลายมือชื่อของผู้ส่งจะถูกรับรองด้วยองค์กรออกใบรับรอง (Certification Authority) ซึ่งจะแสดงอยู่ในรูปของ "ใบรับรองดิจิตอล" (Digital Certification) ประโยชน์ของลายมือชื่อดิจิตอลนั้น นอกจากจะช่วยระบุตัวผู้ส่งข้อมูลแล้วยังช่วยป้องกันข้อมูลให้มีความถูกต้องไม่ได้ผ่านการแก้ไข หรือหากมีการแก้ไขมาก่อนก็สามารถตรวจสอบได้

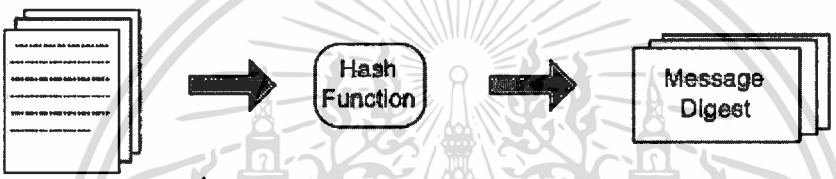
ลายมือชื่อดิจิทัล (Digital Signature) เป็นส่วนหนึ่งของข้อมูลที่สกัดมาจากข้อมูลที่เป็นเนื้อหา และทำให้ไม่สามารถถูกปลอมแปลงได้โดยใช้เทคโนโลยีการเข้ารหัสแบบที่เรียกว่า การเข้ารหัสแบบกุญแจสาธารณะ (Public Key Cryptography) ติดผนึกแนบไปกับข้อความที่ต้องการส่ง ดังนั้นทุกลายมือชื่อจะเป็นหนึ่งเดียวกับข้อความที่ส่ง กล่าวคือ หากข้อความที่ส่งถูกแก้ไขเปลี่ยนแปลงจะส่งผลให้ไม่สามารถใช้กุญแจสาธารณะ (Public Key) ถอดรหัสเพื่อเปิดดูข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ดังกล่าวได้ ทำให้สามารถรู้ได้ทันทีว่าข้อมูลที่ลงลายมือชื่อดิจิตอลดังกล่าวถูกเปลี่ยนแปลงแก้ไข หรือมีปัญหาเกิดขึ้น

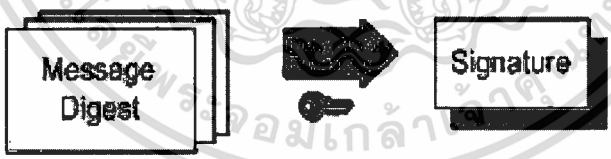
2.4 ขั้นตอนการทำงานของลายมือชื่อดิจิทัล [4]

1. นำข้อมูลต้นฉบับที่จะส่งไปนั้นมาผ่านกระบวนการทางคณิตศาสตร์ที่เรียกว่าฟังก์ชันย่อยข้อมูล (Hash function) เพื่อให้ได้ข้อมูลที่สั้นๆ ที่เรียกว่าข้อมูลที่ย่อยแล้ว (Message Digest) ก่อนที่จะทำการเข้ารหัส เนื่องจากข้อมูลต้นฉบับมักจะมีความยาวมากซึ่งจะทำให้กระบวนการเข้ารหัสใช้เวลานานมาก ข้อมูลที่ย่อยแล้วสร้างได้โดยการนำเอาข้อมูลต้นฉบับไปผ่าน one-way hash function ดังรูปที่ 2.3



รูปที่ 2.3 การส่งข้อมูลเข้าไปใน Hash Function

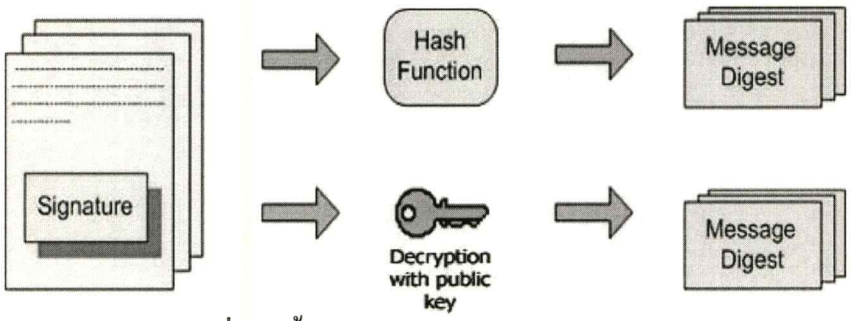
2. จากนั้นจึงทำการเข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่งเอง ซึ่งจุดนี้เปรียบเสมือนการลงลายมือชื่อของผู้ส่ง เพราะผู้ส่งเท่านั้นที่มีกุญแจส่วนตัวของผู้ส่งเองและจะได้ข้อมูลที่เข้ารหัสแล้ว เรียกว่าลายมือชื่อดิจิทัล ดังรูปที่ 2.4



รูปที่ 2.4 การเข้ารหัสเมสเซสไดเจสต์ด้วยกุญแจส่วนตัวเพื่อลงลายมือชื่อ

3. ทำการส่งลายมือชื่อพร้อมกับข้อมูลต้นฉบับไปยังผู้รับ ผู้รับก็จะทำการตรวจสอบว่าข้อมูลที่ได้รับถูกแก้ไขระหว่างทางหรือไม่ โดยการนำข้อมูลต้นฉบับที่ได้รับมาผ่านกระบวนการย่อยด้วยฟังก์ชันย่อยข้อมูลจะได้ข้อมูลย่อยมาชุดหนึ่ง
4. นำลายมือชื่อดิจิทัล มาทำการถอดรหัสด้วยกุญแจสาธารณะของผู้ส่ง ก็จะได้ข้อมูลที่ย่อยแล้วอีกชุดหนึ่ง ทำการเปรียบเทียบข้อมูลที่ย่อยแล้วทั้งสองชุด ถ้าหากว่าเหมือนกันก็แสดงว่าข้อมูลที่ได้รับนั้นไม่ได้ถูกแก้ไข แต่ถ้าข้อมูลที่ย่อยแล้ว แตกต่างกันก็แสดงว่าข้อมูลที่ได้รับถูกเปลี่ยน แปลงระหว่างทาง ดังรูปที่ 2.5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.5 ขั้นตอนการเปรียบเทียบความถูกต้อง

2.5 ใบรับรองดิจิทัล (Digital Certificate)

ด้วยการเข้ารหัส และ ลายมือชื่อดิจิทัล ที่สร้างจากเทคโนโลยีการเข้ารหัสแบบอสมมาตร โดยอาศัยโครงสร้างพื้นฐานของกุญแจสาธารณะในการทำธุรกรรม เราสามารถรักษาความลับของข้อมูล สามารถรักษาความถูกต้องของข้อมูล และสามารถระบุตัวบุคคลได้ระดับหนึ่ง เพื่อเป็นเพิ่มระดับความปลอดภัยในการระบุตัวบุคคล โดยสร้างความเชื่อถือมากขึ้นด้วย ใบรับรองดิจิทัล (Digital Certificate) ซึ่งออกโดยองค์กรกลางที่เป็นที่เชื่อถือ เรียกว่า ผู้ให้บริการออกใบรับรอง (Certification Authority: CA) จะถูกนำมาใช้สำหรับยืนยันในการทำธุรกรรมว่าเป็นบุคคลนั้นจริงตามที่ได้อ้างไว้ ในใบรับรองดิจิตอลที่ออกตามมาตรฐาน X.509 Version 3 ซึ่งเป็นมาตรฐานที่ได้รับความนิยมอย่างแพร่หลาย ดังตัวอย่างในรูปที่ 2.6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/Email=server-certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/Email=server-certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                   68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                   85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                   6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                   6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                   29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                   6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                   5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                   3a:c2:b5:66:22:12:d6:87:0d
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
   Signature Algorithm: md5WithRSAEncryption
       07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
       a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
       3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
       4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
       8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
       e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
       b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
       70:47
```

รูปที่ 2.6 ตัวอย่างใบรับรองดิจิทัล

ใบรับรองดิจิทัลที่ออกโดยผู้ให้บริการออกใบรับรองจะมีรูปแบบที่ตรงตามมาตรฐานใบรับรองดิจิทัล แบบ X.509 Version 3 กำหนดโดย ITU-T X.509 International Standard ซึ่งเป็นที่นิยมใช้งานในปัจจุบัน สามารถนำไปใช้งานกับซอฟต์แวร์ใดๆ ก็ได้ที่สนับสนุนใบรับรองอิเล็กทรอนิกส์ ตามมาตรฐานนี้ แต่ในทางปฏิบัติผู้ให้บริการออกใบรับรองบางรายมีการกำหนดรายละเอียดเพิ่มเติมในใบรับรอง (Certificate Extension) ที่แตกต่างกัน ทำให้ซอฟต์แวร์บางชนิดไม่สามารถอ่านใบรับรองอิเล็กทรอนิกส์ที่ถูกสร้างโดยผู้ให้บริการออกใบรับรองบางรายได้ โดยทั่วไปมาตรฐานของใบรับรองดิจิทัลจะประกอบด้วยข้อมูลดังต่อไปนี้

1. หมายเลขของใบรับรอง (serial number) คือ เลขที่ของใบรับรองดิจิทัล
2. วิธีการที่ใช้ในการเข้ารหัสข้อมูล (algorithm) ระบุถึงมาตรฐานที่ใช้ในการตรวจสอบสอบความถูกต้องของข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล.

3. หน่วยงานที่ออกใบรับรอง (issuer) ระบุองค์กรหรือหน่วยงานที่ออกใบรับรองนี้ เพื่อใช้ในการตรวจสอบว่าองค์กรที่ออกใบรับรองนี้เชื่อถือได้แค่ไหน
4. เวลาที่ใบรับรองเริ่มใช้ได้ (starting time)
5. เวลาที่ใบรับรองหมดอายุ (expiring time)
6. ผู้ได้รับการรับรอง (subject) ในส่วนนี้รวมถึงอีเมลของผู้ได้รับการรับรองด้วย
7. กุญแจสาธารณะของผู้ได้รับการรับรอง (subject's public key)
8. ลายมือชื่อดิจิทัลของหน่วยงานที่ออกใบรับรอง (CA signature) เพื่อเป็นการยืนยันว่าใบรับรองฉบับนี้ได้ออกมาโดยองค์กรหรือหน่วยงานนี้จริง

2.6 Secure Socket Layer (SSL)

เป็นโพรโทคอลจัดการความปลอดภัยในระบบอินเทอร์เน็ตที่พัฒนาขึ้นโดย Netscape Communications Corporation เป็นการรักษาตัวข้อมูลให้ไปถึงจุดหมายโดยปลอดภัย ซึ่งปกติข้อมูลที่ทำการสื่อสารกันนั้นจะไม่มีการเข้ารหัสข้อมูลแต่อย่างใด ทำให้การดักจับข้อมูลเป็นไปอย่างง่ายดาย แต่ถ้าเรานำระบบ SSL เข้ามาใช้ ข้อมูลที่ทำการส่งจากไคลเอนต์ไปยังเซิร์ฟเวอร์นั้นจะถูกเข้ารหัสก่อนที่จะส่งไปให้ยังเซิร์ฟเวอร์ ทำให้ข้อมูลที่รับส่งกันนั้นมีความปลอดภัยมากยิ่งขึ้น การเข้ารหัสของ SSL นั้นมีได้ 2 แบบ คือ การเข้ารหัสแบบ 40 บิต และการเข้ารหัสแบบ 128 บิต ซึ่งการเข้ารหัสแบบหลังนี้มีใช้แค่ในประเทศสหรัฐอเมริกาเท่านั้น เมื่อเราทำการเข้ารหัสข้อมูลที่ถูกส่งออกไปจะไม่อยู่ในรูปของ Cleartext ทำให้ไม่สามารถดูข้อมูลได้โดยตรงหรือเปลี่ยนแปลงข้อมูลได้ อีกทั้ง SSL ยังสามารถตรวจสอบและยืนยันโฮสต์ต้นทางหรือปลายทางว่าเป็นโฮสต์จริงที่กำลังติดต่ออยู่และต้องการส่งข้อมูลที่สำคัญไปให้ เป็นการช่วยเพิ่มความมั่นใจในการทำงานที่เป็นความลับต่างๆ

2.6.1. ส่วนประกอบของ SSL

SSL เป็นโพรโทคอลที่อยู่ระหว่างชั้นแอพพลิเคชันเลเยอร์กับชั้นทรานสปอร์ตเลเยอร์ ที่ออกแบบมาให้ทำงานกับแอพพลิเคชันโพรโทคอล เช่น HTTP, FTP, IMAP, LDAP secure SSL, WEB secure SSL เป็นต้น โดยอาศัย TCP/IP ทำให้ แอพพลิเคชันเลเยอร์ สามารถใช้เซิร์ฟเวอร์ที่อนุญาตให้ SSL (SSL-Enable) ในการให้สิทธิ์ (Authenticate) ตัวเองกับลูกข่ายที่ใช้ SSL เพื่อยืนยันว่าเป็นเซิร์ฟเวอร์ ตัวจริงหรือให้เครื่องไคลเอนต์สามารถ Authenticate ตัวเองกับเซิร์ฟเวอร์ได้ SSL ทำงานโดยอาศัยหลักการทำงานที่ใช้ Public Key Cryptography มีการใช้ Strong Authentication, Signing และ Encryption รูปแบบต่างๆ ซึ่งส่วนประกอบของ SSL มีด้วยกัน 2 ส่วน ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

SSL Record Protocol อยู่ในเลเยอร์ที่ต่ำกว่าติดกับ TCP ทำหน้าที่ห่อหุ้ม (Encapsulate) โพรโทคอลอื่นๆ ที่สูงกว่าและระบุรูปแบบของการรับส่งข้อมูล

SSL Handshake Protocol ซึ่งทำให้ไคลเอนท์และเซิร์ฟเวอร์สามารถตรวจสอบสิทธิ์ของกันและกัน (Authentication) และตกลงอัลกอริทึมในการเข้ารหัสที่จะใช้ รวมถึงกุญแจที่ใช้ในระบบก่อนที่จะแลกเปลี่ยนข้อมูล ประโยชน์ของ SSL คือ ไม่ขึ้นต่อการทำงานของเลเยอร์ที่สูงกว่า กล่าวคือ โพรโทคอลใดๆ ในเลเยอร์ที่สูงกว่าสามารถทำงานอยู่บน SSL ได้

2.6.2. คุณสมบัติของการสื่อสารผ่าน SSL

การเชื่อมต่อเป็นส่วนตัว หลังจากตกลงกันถึงกุญแจ (Secret Key) ที่จะใช้แล้ว จะมีการเข้ารหัสข้อมูล ซึ่งจะใช้ระบบรหัสแบบสมมาตร เช่น DES ส่วนในการระบุช่องทางสื่อสาร จะมีการตรวจสอบสิทธิ์โดยใช้การเข้ารหัสอสมมาตร เช่น RSA หรือ DSS เป็นการเชื่อมต่อที่มีความน่าเชื่อถือโดยข้อมูลที่ส่งไปจะมี Message Integrity Check ที่ใช้ Keyed MAC ในการคำนวณเกี่ยวกับ MAC ซึ่งใช้ Secure Hash Function เช่น MD5 หรือ SHA เป็นต้น

ปัจจุบันมีบริการมากมายที่ทำงานกับ SSL เช่น http, ftp, telnet, pop3, smtp หรือแม้แต่ VPN การทำงานของ SSL จะเริ่มจากเซิร์ฟเวอร์ส่งใบรับรองเพื่อยืนยันตัวตนกับผู้ใช้ ขั้นตอนนี้เรียกว่า authentication certificate ที่ใช้กันเป็นมาตรฐาน X.509 Version 3 จะรับรองด้วยลายมือชื่อดิจิทัล (digital signature)โดยผู้ที่เชื่อถือได้เช่น US Post Service , Verisign ซึ่งจะต้องเสียค่าใช้จ่ายตามความปลอดภัยที่สูงขึ้นของใบรับรองนั้น แต่ในที่นี้เราสามารถลดค่าใช้จ่ายได้โดยใช้วิธี self signing คือการสร้างใบรับรองที่มีลายมือชื่อรับรองตนเอง (POP3S, SMTPS ของ gear/intania จะเป็น self signed certificate)หากผู้ใช้ยอมรับใบรับรองนั้นโปรแกรมก็จะเริ่มตกลงกันว่าจะใช้โพรโทคอลอะไรในการเข้าและถอดรหัส ขึ้นกับว่าโปรแกรมและตัว SSL server ที่รองรับ อย่างเช่น HTTPS ของ IE4 จะใช้ RC4 stream cipher เป็น secret key cryptography ขนาด 40-bit (ซึ่งแกะได้ด้วยเครื่องซูเปอร์คอมพิวเตอร์ความเร็วสูงๆ ได้ในเวลาวินาทีเดียว) หรือถ้าเป็น IE5 ก็จะเป็น 1024-bit RSA Public Key Encryption กับ MD5/RSA Digital Signature ส่วน Opera 3.6 รองรับ SSLv3.1 จะใช้ 1024-bit RSA Public Key Encryption กับ SHA/RSA Digital Signature เป็นต้น

2.6.3. หน้าที่ของ SSL

ไคลเอนท์กับเซิร์ฟเวอร์ทำการแลกเปลี่ยนกุญแจสาธารณะ (Public Key Cryptography) หลังจากนั้น SSL จะทำหน้าที่เข้ารหัสข้อมูลโดยการนำกุญแจสาธารณะของอีกฝ่ายหนึ่งมาใช้เข้ารหัส ส่วนการถอดรหัสจะทำได้ก็ต่อเมื่อฝ่ายรับต้องใช้กุญแจส่วนตัวเฉพาะซึ่งไม่เปิดเผยให้ใครรู้ ขั้นตอนการเข้ารหัสจะอาศัยเทคนิค RSA (Rivest, Shamir and Aldeman) ซึ่งเป็นเทคนิคการเข้ารหัสลับที่นิยมใช้กันอย่างแพร่หลาย หน้าที่ของ SSL จะแบ่งออกเป็น 3 ส่วน ใหญ่ๆ คือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การตรวจสอบเซิร์ฟเวอร์ ว่าเป็นตัวจริง ตัวโปรแกรมไคลเอนท์ที่มีขีดความสามารถในการสื่อสารแบบ SSL จะสามารถตรวจสอบเครื่องเซิร์ฟเวอร์ที่ตนกำลังจะไปเชื่อมต่อได้ว่า เซิร์ฟเวอร์นั้นเป็น เซิร์ฟเวอร์ตัวจริงหรือไม่โดยใช้เทคนิคการเข้ารหัสแบบ public key ในการตรวจสอบใบรับรอง (certificate) และ public ID ของเซิร์ฟเวอร์นั้น (โดยที่มีองค์กรที่ ไคลเอนท์ เชื่อถือเป็นผู้ออกใบรับรองและ public ID ให้แก่ server นั้น) หน้าที่นี้ของ SSL เป็นหน้าที่ที่สำคัญ โดยเฉพาะอย่างยิ่งในกรณีที่ไคลเอนท์ต้องการที่จะส่งข้อมูลที่เป็นความลับ (เช่น หมายเลขเครดิตการ์ด) ให้กับเซิร์ฟเวอร์ซึ่ง ไคลเอนท์จะต้องตรวจสอบก่อนว่าไคลเอนท์ เป็นตัวจริงหรือไม่

การตรวจสอบว่าไคลเอนท์ เป็นตัวจริง เซิร์ฟเวอร์ที่มีขีดความสามารถในการสื่อสารแบบ SSL จะใช้เทคนิคเช่นเดียวกับในหัวข้อที่แล้วในการตรวจสอบไคลเอนท์ หรือผู้ใช้ว่าเป็นตัวจริงหรือไม่ โดยจะตรวจสอบใบรับรองและ public ID (ที่มีองค์กรที่เซิร์ฟเวอร์ เชื่อถือเป็นผู้ออกให้) ของไคลเอนท์หรือผู้ใช้นั้น

การเข้ารหัสลับการเชื่อมต่อ ในกรณีนี้ข้อมูลทั้งหมดที่ถูกส่งระหว่างไคลเอนท์และเซิร์ฟเวอร์จะถูกเข้ารหัสลับ โดยโปรแกรมที่ส่งข้อมูลเป็นผู้เข้ารหัสและโปรแกรมที่รับข้อมูลเป็นผู้ถอดรหัส (โดยใช้วิธี public key) นอกจากการเข้ารหัสลับในลักษณะนี้แล้ว SSL ยังสามารถปกป้องความถูกต้องสมบูรณ์ของข้อมูลได้อีกด้วย กล่าวคือ ตัวโปรแกรมรับข้อมูลจะทราบได้หากข้อมูลถูกเปลี่ยนแปลงไปในขณะกำลังเดินทางจากผู้ส่งไปยังผู้รับ

2.6.4. ประโยชน์ของการใช้ SSL

SSL สามารถเพิ่มความปลอดภัยของการส่งข้อมูลผ่านระบบเครือข่ายได้ในด้าน

1. การอนุญาต (Authorization) หรือ การรักษาความลับ (Confidentiality) ว่าไม่มีใครในระบบเครือข่ายนอกจากผู้รับสามารถอ่านข้อมูลได้
2. การระบุตัวบุคคล (Authentication) ไม่มีใครสามารถแอบอ้างเป็นผู้รับหรือผู้ส่งเพื่อส่งข้อมูลได้
3. การรักษาความถูกต้องของข้อมูล (Integrity) ไม่มีใครสามารถเปลี่ยนแปลงข้อมูลให้ผิดพลาดได้โดยที่ผู้รับไม่ทราบ

อย่างไรก็ตามการใช้ SSL มิได้หมายความว่าข้อมูลที่เป็นความลับจะรั่วไหลออกไปภายนอกไม่ได้เลย เพราะจุดที่รั่วไหลก็อาจจะมาจากที่ตัวผู้รับหรือผู้ส่งข้อมูลเอง เช่นผู้รับข้อมูลนำข้อมูลไปเปิดเผย หรือการเก็บข้อมูลไว้บนเครื่องคอมพิวเตอร์โดยไม่ได้ป้องกันการสำเนาข้อมูลโดยผู้ใช้คนอื่น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.6.5. SSL กับ Digital Certificate

โพรโทคอล SSL จะใช้ใบรับรองดิจิทัลในการสร้างท่อสื่อสารที่มีความปลอดภัยสูง ระหว่างจุดที่ทำการติดต่อสื่อสารกัน ข้อมูลที่ส่งผ่านท่อสื่อสาร SSL นี้ผู้ที่ทำการส่งข้อมูลระหว่างสองจุดจะสามารถทราบได้ทันทีเมื่อมีการโจรกรรมข้อมูล

Web Server Certificate ได้มีบทบาทเข้ามามีส่วนช่วยในการเพิ่มความปลอดภัย ในการส่งข้อมูลต่างๆ เหล่านี้ ผ่านเครือข่ายอินเทอร์เน็ต การติดตั้งใบรับรองลงบนเว็บเซิร์ฟเวอร์ จะทำให้การสื่อสารระหว่างผู้ใช้ที่ใช้บราวเซอร์ติดต่อเข้ามานั้นทำการเข้ารหัสด้วย SSL ซึ่งเป็นโพรโทคอลมาตรฐานที่ใช้ในการเข้ารหัสข้อมูลเพื่อความปลอดภัย ในการรับส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต มีบทบาทสำคัญในการเพิ่มความปลอดภัย ในการทำธุรกรรมบนอินเทอร์เน็ต โดยทำงานร่วมกับตัวบราวเซอร์ผ่านใบรับรองดิจิทัล ในปัจจุบันโพรโทคอล SSL ได้ถูกติดตั้งบนบราวเซอร์ทุกตัว เช่น IE, Netscape, Opera เป็นต้น

2.6.6. SSL กับ HTTPS

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) เนื่องจาก HTTP ที่เรารู้เป็นโพรโทคอล มาตรฐานที่ใช้รับส่งข้อมูลของเว็บเพจต่างๆ บนอินเทอร์เน็ตนั้น ยังขาดคุณสมบัติในการรักษาความปลอดภัยของข้อมูลระหว่างบราวเซอร์กับเว็บเซิร์ฟเวอร์ จึงมีการพัฒนาให้ HTTP มีความปลอดภัยมากขึ้น โดย Netscape ได้ประยุกต์การรับส่งข้อมูลบน HTTP เข้ากับ Netscape's SSL (Secure Socket Layer) โดยเรียกว่า Hypertext Transfer Protocol over Secure Socket Layer หรือ HTTPS หลักการของ HTTPS คือ การรับส่ง HTTP message บน SSL ผ่านทาง Port 443 (HTTP ใช้ Port 80) หรือเป็นการ Implement HTTP บน SSL อีกชั้นหนึ่ง ซึ่ง SSL นั้นสามารถประยุกต์เข้ากับโพลโตคอลในชั้นแอพพลิเคชันเลเยอร์ได้หลากหลาย

สำหรับ Netscape ให้สังเกตที่มุมล่างซ้ายของโปรแกรม ในส่วนที่เป็นรูปแม่กุญแจจะแสดงสถานะของ SSL ในขณะนั้นว่าข้อมูลที่ผู้ใช้กำลังอ่านอยู่ถูกส่งมาโดยผ่าน SSL โพรโทคอล หรือไม่ ดังรูปที่ 2.7

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

(ก) การส่งผ่าน SSL โดย http

(ข) การส่งผ่าน SSL โดย https

รูปที่ 2.7 Netscape Security Information on SSL

สำหรับ Internet Explorer มีลักษณะเหมือนกัน เพียงแต่สัญลักษณ์แสดงสถานะของ SSL จะปรากฏอยู่ ณ มุมขวาล่างของโปรแกรมดังรูปที่ 2.8

(ก) การส่งผ่าน SSL โดย http

(ข) การส่งผ่าน SSL โดย https

รูปที่ 2.8 Internet Explorer SSL Information

<u>ขั้นตอนการทำงานของ SSL โดยการประยุกต์เข้ากับ HTTP</u>

1. ไคลเอนท์ ส่งคำขอเอกสารโดยส่งด้วยโพรโตคอล HTTPS ซึ่งขึ้นต้น URL ด้วย "https"
2. เซิร์ฟเวอร์ส่งใบรับรอง ของตนเองให้กับไคลเอนท์
3. ไคลเอนท์ ตรวจสอบว่าใบรับรอง นั้นออกโดย Certificate Authority (CA) ที่เชื่อถือได้หรือไม่ ถ้าไม่ใช่ก็จะให้ผู้ใช้เลือกว่าจะทำงานต่อหรือยกเลิกการติดต่อนี้
4. ไคลเอนท์เปรียบเทียบข้อมูลในใบรับรองกับข้อมูลที่เพิ่งรับมา (เปรียบเทียบ ชื่อโดเมน และกุญแจสาธารณะของเว็บไซต์) ถ้าข้อมูลตรงกันไคลเอนท์จะถือว่าเว็บไซต์นั้นผ่านการรับรองและปลอดภัย
5. ไคลเอนท์บอกเซิร์ฟเวอร์ว่าตัวมันสามารถใช้อัลกอริทึมเข้ารหัสแบบไหนได้บ้าง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6. เซิร์ฟเวอร์เลือกการเข้ารหัสที่ดีที่สุดและแจ้งให้ไคลเอนท์ทราบ
7. ไคลเอนท์สร้าง กุญแจส่วนตัว ที่จะใช้ร่วมกันสำหรับการติดต่อนี้
8. ไคลเอนท์เข้ารหัส Session key ด้วยการใช้กุญแจสาธารณะของเซิร์ฟเวอร์และส่งไปให้เซิร์ฟเวอร์
9. เซิร์ฟเวอร์รับ Session key ที่ถูกเข้ารหัสมาและทำการถอดรหัสมันด้วยกุญแจส่วนตัวของเซิร์ฟเวอร์เอง
10. หลังจากนั้นไคลเอนท์และเซิร์ฟเวอร์จะใช้ Session key นี้ในขั้นตอนที่เหลือของการติดต่อ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

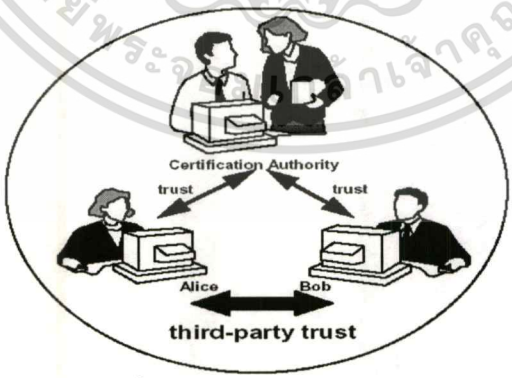
บทที่ 3

การดำเนินการเป็นผู้ให้บริการออกใบรับรอง

3.1 องค์กรออกใบรับรอง

การระบุตัวบุคคลโดยใช้ใบรับรองดิจิทัลอาจทำได้โดยการออกใบรับรองให้แก่บุคคลอื่น ซึ่งรู้จักกันที่มีรูปแบบการแนะนำกันเป็นทอดๆ ในลักษณะของ “สายใยแห่งความน่าเชื่อถือ” (web of trust) อย่างไรก็ตามการตรวจสอบการระบุตัวบุคคลในลักษณะดังกล่าวเป็นสิ่งที่มีความยุ่งยาก และมีความน่าเชื่อถือต่ำ เนื่องจากเป็นการรับรองกันเป็นทอดๆ โดยผู้รับรองแต่ละคนมีมาตรฐานในการรับรองที่แตกต่างกัน

โครงสร้างพื้นฐานซึ่งจะช่วยให้สามารถระบุตัวบุคคลได้อย่างสะดวกและมีความน่าเชื่อถือสูงคือ หน่วยงานที่เรียกว่า “องค์กรออกใบรับรอง” (Certification Authority หรือ CA) หรือที่เรียกกันว่า “โครงสร้างพื้นฐานของระบบกุญแจสาธารณะ” (Public Key Infrastructure หรือ PKI) ซึ่งจะเป็นตัวกลางในการตรวจสอบและออกใบรับรองให้แก่ผู้อื่น ตามแนวทางจะมีบุคคลต่างๆ ที่เกี่ยวข้องกัน 3 ฝ่าย (three-party model) คือ ผู้ถือใบรับรอง (certificate holder) ซึ่งเราอาจเรียกว่าเป็นบุคคลที่หนึ่ง ผู้ใช้ใบรับรองในการระบุตัวผู้ถือใบรับรอง (relying party) ซึ่งอาจเรียกว่าเป็นบุคคลที่สอง และองค์กรออกใบรับรองซึ่งเรียกว่าบุคคลที่สาม หรือที่นิยมเรียกกันว่า “บุคคลที่สามที่เชื่อถือได้” (trusted third party) ดังรูปที่ 3.1



รูปที่ 3.1 การไว้ใจแบบ 3 ฝ่าย

3.2 ผู้ให้บริการออกใบรับรองดิจิทัล

เป็นรูปแบบหนึ่งของเทคโนโลยีระบบรหัสแบบกุญแจสาธารณะ ซึ่งประกอบไปด้วยผู้ให้บริการออกใบรับรอง และหน่วยงานในการลงทะเบียน (Registration Authority) โดยผู้ให้บริการ

เอกสารนี้มีไว้เพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

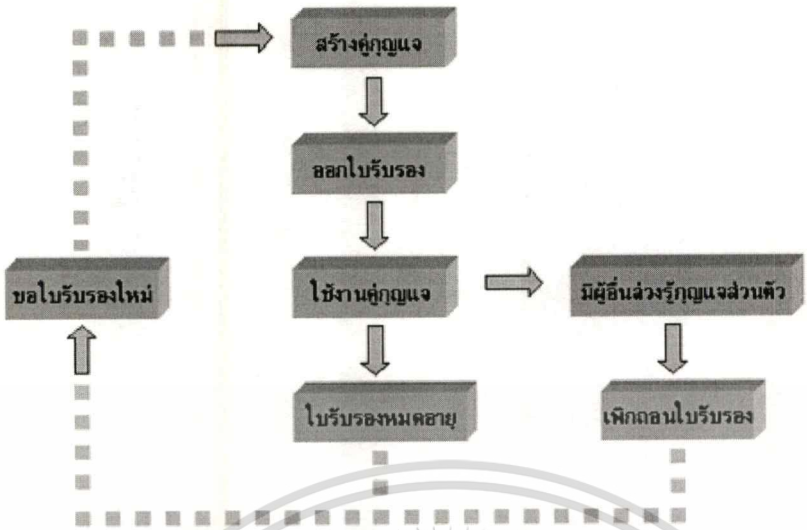
ออกใบรับรองมีหน้าที่รับรองข้อมูลของผู้ใช้และออกใบรับรองดิจิทัล (Digital Certificate) ซึ่งข้อมูลของผู้ใช้ประกอบไปด้วยข้อมูลส่วนบุคคลและกุญแจสาธารณะของผู้ใช้ ก่อนที่ผู้ใช้จะได้รับใบรับรองดิจิทัลจะต้องมีกระบวนการในการตรวจสอบตัวบุคคลที่เชื่อถือได้ โดยจะถูกดำเนินการโดยหน่วยงานรับลงทะเบียนนั่นเอง

3.2.1. กระบวนการในการออกใบรับรอง

กระบวนการในการออกใบรับรองนั้นจะมีลักษณะเป็นวงจรดังรูปที่ 3.2 ซึ่งมีรายละเอียดดังนี้

- ผู้ขอใบรับรองสร้างกุญแจคู่และส่งเฉพาะกุญแจสาธารณะมาพร้อมกับข้อมูลส่วนบุคคลที่อยู่ในรูปของคำขอใบรับรอง (Certificate Request) ไปยังผู้ให้บริการออกใบรับรอง ซึ่งจะต้องผ่านกระบวนการตรวจสอบตัวบุคคลอย่างละเอียดโดยหน่วยงานรับลงทะเบียน ซึ่งอาจใช้วิธีตรวจสอบจากเอกสารทางราชการต่างๆ หรือติดต่อเป็นรายบุคคลเพื่อยืนยันว่าบุคคลนั้นเป็นผู้ที่อ้างถึงจริง
- คำขอใบรับรองที่ผ่านการตรวจสอบจะถูกนำไปสร้างเป็นใบรับรองโดยผู้ให้บริการออกใบรับรอง และถูกส่งกลับมายังผู้ขอเพื่อนำไปใช้งานต่อไป โดยใบรับรองที่ได้จะถูกทำสำเนาไว้ที่ระบบบริการไดเร็คทอรี (Directory Service) อีกชุดหนึ่ง เพื่อให้บุคคลทั่วไปสามารถค้นหาได้สะดวก
- การใช้งานใบรับรองดิจิทัลและกุญแจส่วนตัว ในกรณีที่มีผู้อื่นล่วงรู้กุญแจส่วนตัว ผู้ที่เป็นเจ้าของใบรับรองจะต้องทำการขอเพิกถอนใบรับรอง โดยใบรับรองที่ถูกเพิกถอนนั้นจะปรากฏอยู่ในรายการเพิกถอนใบรับรอง (Certificate Revocation List : CRL)
- เมื่อใบรับรองดิจิทัลหมดอายุ ผู้ที่เป็นเจ้าของใบรับรองจะต้องทำการขอใบรับรองใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.2 วงจรการใช้งานใบรับรองดิจิทัล (Certificate Life Cycle)

3.2.2. รูปแบบการมอบความไว้วางใจของผู้ให้บริการออกใบรับรอง

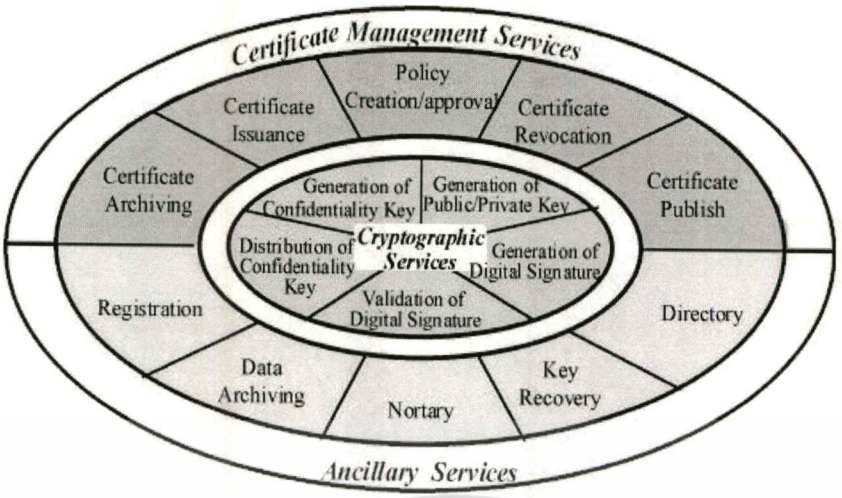
รูปแบบการมอบความไว้วางใจ (Trust Model) ของผู้ให้บริการออกใบรับรองจะเป็นแบบลำดับชั้นที่แน่นอน (Strict Certification Hierarchy) กล่าวคือใบรับรองดิจิทัลของบุคคลใดๆ จะถูกสร้างโดยผู้ให้บริการออกใบรับรองเท่านั้น โดยผู้ให้บริการออกใบรับรองสามารถมีได้หลายลำดับชั้น ชั้นบนสุดจะเรียกว่า ผู้ให้บริการออกใบรับรองหลัก (Root CA) โดยที่ใบรับรองของผู้ให้บริการออกใบรับรองหลักจะเป็นแบบการรับรองตนเอง (Self-signed) และจะเป็นผู้ออกใบรับรองสำหรับผู้ให้บริการออกใบรับรองในชั้นถัดลงมา (Intermediate CA) ที่อยู่ติดกันเป็นลำดับไปเรื่อยๆ จนไปสิ้นสุดที่การออกใบรับรองสำหรับผู้ใช้งาน

การมีผู้ใช้บริการออกใบรับรองแบบหลายลำดับชั้น มีประโยชน์ในแง่ของการแบ่งกลุ่มผู้ใช้งานออกเป็นหลายๆ กลุ่ม เนื่องจากมีผู้ใช้จำนวนมาก ดังนั้นจึงมีการแบ่งกลุ่มผู้ใช้ตามหน่วยงานของผู้ใช้ ตามความสามารถในการใช้งานใบรับรองหรือตามระดับความรับผิดชอบของผู้ให้บริการออกใบรับรอง เป็นต้น

3.3 ประเภทบริการของ Certification Authority

องค์กรออกใบรับรองโดยทั่วไปจะมีบทบาทในการให้บริการใน 3 ด้านที่สำคัญ จากรูปที่ 3.3 ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.3 การให้บริการขององค์กรออกใบรับรอง

1. การให้บริการเทคโนโลยีการเข้ารหัส (Crpytographic Service) ซึ่งจะประกอบไปด้วย
   - การผลิตกุญแจลับ (Generation of Private Key)
   - การส่งมอบกุญแจลับ (Distribution of Private Key)
   - การผลิตกุญแจสาธารณะและกุญแจลับ (Generation of Public/Private Key)
   - การผลิตรายมือชื่อดิจิทัล (Generation of Digital Signature)
   - การรับรองลายมือชื่อดิจิทัล (Validation of Digital Signature)
2. บริการที่เกี่ยวข้องกับการออกใบรับรอง (Certification Management Service)ซึ่งประกอบไปด้วย
   - การออกใบรับรอง (Certificate Issuance) คือบริการที่ CA จะทำการออกใบรับรองให้แก่ผู้ร้องขอใบรับรอง เช่น บุคคลทั่วไป หรือองค์กรต่างๆ
   - การยกเลิกใบรับรอง (Certificate Revocation) คือ บริการที่ทาง CA จะทำการระงับและยกเลิกใบรับรองที่ออกให้ไปแล้ว เนื่องจากบุคคลที่ถือใบรับรองอยู่นั้นได้ทำกุญแจส่วนตัวหายหรือถูกขโมยกุญแจส่วนตัวไป ผู้ถือใบรับรองสามารถแจ้งให้ CA เพิกถอนใบรับรองนั้นได้ เพื่อความปลอดภัยของข้อมูล เพราะอาจมีบุคคลอื่นแอบอ้างเอากุญแจส่วนตัวนี้ไปใช้ ดังนั้นหลังจาก CA ทำการยกเลิกใบรับรองแล้ว บุคคลที่เคยทำธุรกรรมกับผู้ถือใบรับรองนี้จะไม่สามารถทำธุรกรรมกันได้จนกว่า CA จะออกใบรับรองใหม่ให้แก่ผู้ถือใบรับรองนี้
   - บริการเผยแพร่รายการเพิกถอนใบรับรอง (Certificate Revocation List Publication) เมื่อมีการเพิกถอนใบรับรอง CA จะทำการเผยแพร่รายการใบรับรอง (Certificate) ที่ถูกเพิกถอนเพื่อให้ผู้ใช้ประโยชน์รายอื่นได้ทราบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- การเผยแพร่ใบรับรองแก่บุคคลทั่วไป (Certificate publishing) คือ บริการที่ทาง CA ทำการเก็บใบรับรองที่ออกให้ไปกับบุคคลทั่วไปสามารถเข้ามาตรวจสอบข้อมูลของใบรับรองของบุคคลที่กำลังทำธุรกรรมอยู่ด้วยได้ เพื่อผู้ใช้ประโยชน์จะได้ทราบว่า ใครเป็นเจ้าของกุญแจสาธารณะนั้นและมาจากหน่วยงานใด เนื่องจากระบบกุญแจคู่เป็นระบบที่รองรับผู้ใช้บริการขนาดใหญ่ และเจ้าของใบรับรองอาจจะไม่มีความสัมพันธ์ซึ่งกันและกันแต่อย่างใด
- การเก็บต้นฉบับใบรับรอง (Certificate Archiving) คือ บริการที่ทาง CA จะทำการเก็บต้นฉบับของใบรับรองทั้งหมดของบุคคลทั่วไป เพราะว่าใบรับรองของแต่ละบุคคลจะมีวันหมดอายุ บุคคลที่ต้องการที่จะใช้ใบรับรองของตนต่อไป ก็ต้องทำการต่ออายุใบรับรองใหม่ ซึ่ง CA จะต้องทำการเก็บข้อมูลของใบรับรองเดิมและใบรับรองใหม่ด้วย เพื่อให้เอกสารที่เคยลงลายมือชื่อดิจิทัลกำกับอยู่ซึ่งใช้ใบรับรองเดิมที่หมดอายุไปแล้วยังสามารถที่จะเชื่อถือได้อยู่
- บริการเผยแพร่รายการใบรับรองที่หมดอายุ (Certificate Expiration List Publication) เพื่อให้ผู้ใช้ประโยชน์รายอื่นได้ทราบว่าใบรับรองนั้นหมดอายุแล้ว
- การกำหนดนโยบายการออกและอนุมัติใบรับรอง (Policy Creation/Approval) คือ บริการที่ CA กำหนดนโยบายหรือกฎเกณฑ์ต่างๆ ว่าทาง CA จะมีนโยบายอย่างไรในการที่จะออกและอนุมัติใบรับรองให้กับบุคคลที่ทำการขอใบรับรอง เพื่อที่จะสามารถออกใบรับรองได้อย่างมีมาตรฐาน

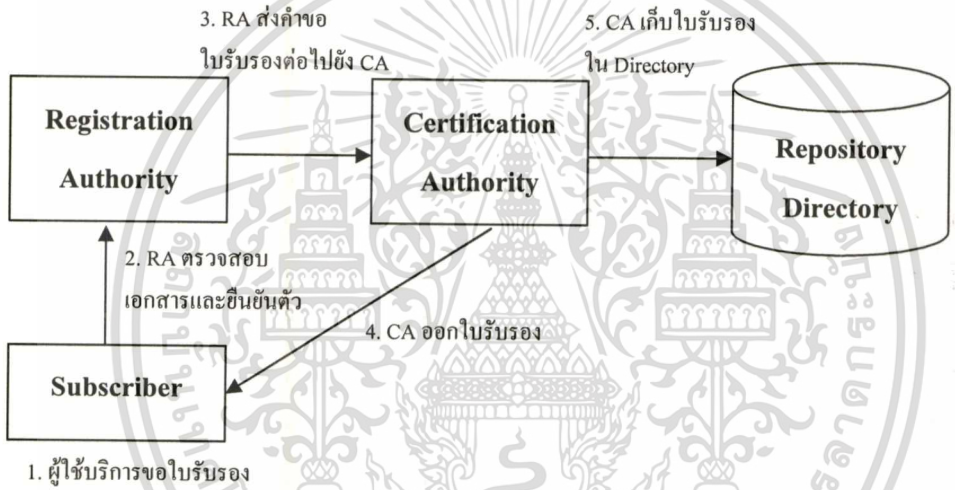
3. บริการเสริมอื่นๆ (Ancillary Service) ซึ่งได้แก่
   - การบันทึก (Registration) เป็นบริการที่ทาง CA จะทำการบันทึกข้อมูลต่างๆ ของใบรับรองที่ออกไปแล้วทั้งหมดและทำการจัดการกับข้อมูลของใบรับรองทั้งหมด เช่น การเปลี่ยนแปลงข้อมูลต่างๆ ของบุคคลที่เป็นเจ้าของใบรับรอง
   - การเก็บต้นฉบับข้อมูล (Data Achieving) เป็นบริการที่ทาง CA จะทำการเก็บข้อมูลของใบรับรองโดยทำการสำรองข้อมูลของใบรับรองทั้งหมดที่มี เพื่อเป็นการการันตีว่าข้อมูลของใบรับรองทั้งหมดจะยังคงอยู่ เพื่อให้สามารถใช้ข้อมูลเหล่านี้ได้ตลอดไป ไม่ว่าจะผ่านมานานแค่ไหน สามารถกลับมาตรวจสอบข้อมูลเหล่านี้ได้ตลอดเวลา
   - การตรวจสอบสัญญาต่างๆ (Notarial Authentication)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- การกู้กุญแจ (Key Recovery) เป็นการบริการที่ทาง CA จะทำการก๊อปปี้กุญแจส่วนตัวเก็บไว้ เพื่อที่จะสามารถกู้คืนกุญแจให้กับบุคคลที่ถือใบรับรองในกรณีที่ผู้ถือใบรับรองทำกุญแจหาย หรือลืมรหัสผ่านที่ใช้ป้องกันกุญแจส่วนตัว
- การทำทะเบียนของผู้ใช้บริการ (Directory) เป็นบริการที่ทาง CA จะทำการบันทึกข้อมูลต่างๆ ที่เกี่ยวกับผู้ขอใช้บริการ โดยข้อมูลนี้จะไม่ได้เกี่ยวข้องกับข้อมูลที่อยู่ในใบรับรอง เช่น ที่อยู่ หมายเลขโทรศัพท์และอีเมล เป็นต้น

3.3.1 ขั้นตอนที่เกี่ยวข้องกับการขอ/ออกใบรับรอง

กระบวนการในการขอและออกใบรับรองมีขั้นตอน ดังรูปที่ 3.4



รูปที่ 3.4 ขั้นตอนการออกใบรับรอง

3.3.2 ลักษณะการใช้งานของใบรับรองดิจิทัล

ใบรับรองดิจิทัลสามารถนำไปใช้ในการรับรองในลักษณะต่างๆ โดยทั่วไปเป็นกรณีที่ผู้ประกอบการรับรองแต่ละรายจะเป็นผู้กำหนดเอง ซึ่งเราสามารถแบ่งออกเป็นกลุ่มได้ดังนี้

1. ใบรับรองบุคคล (Personal Certificate) หรือใบรับรองเครื่องลูกข่าย (client certificate) คือ ใบรับรองที่ใช้รับรองให้กับบุคคลทั่วไป เหมาะสำหรับบุคคลที่ต้องการติดต่อสื่อสารผ่านเครือข่ายคอมพิวเตอร์แบบปลอดภัย โดยที่ในใบรับรองลักษณะนี้จะมีข้อมูลตามมาตรฐาน X.509 เวอร์ชัน 3 และที่ขาดไม่ได้คือจะต้องมีข้อมูลกุญแจสาธารณะของบุคคลนั้นๆ ด้วย
2. ใบรับรองเครื่องแม่ข่าย (Server Certificate) เป็นบริการใบรับรองดิจิทัลสำหรับเว็บไซต์ เหมาะสำหรับหน่วยงานที่ต้องการสร้างความเชื่อมั่นในการเผยแพร่ข้อมูลแก่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บุคคลทั่วไปผ่านเครือข่ายคอมพิวเตอร์เพื่อยืนยันว่าข้อมูลดังกล่าวมาจากเว็บไซต์ของหน่วยงานที่กำลังติดต่อด้วยจริง ซึ่งจะระบุชื่อบุคคลนั้นและข้อมูลอื่นๆ เช่น รหัสไปรษณีย์อิเล็กทรอนิกส์หรือที่อยู่ โดยข้อมูลที่ขาดไม่ได้คือจะต้องมีกุญแจสาธารณะของเครื่องแม่ข่าย นอกจากนี้ยังสามารถใช้ในการสร้างช่องทางการสื่อสารแบบปลอดภัยระหว่างเว็บไซต์กับบุคคลทั่วไปได้อีกด้วย

3. ใบรับรององค์กรออกใบรับรอง (Certification Authority Certificate) เป็นการบริการบริหารจัดการใบรับรองดิจิทัลส่วนตัวสำหรับองค์กร เหมะสำหรับองค์กรที่ต้องการใช้เทคโนโลยีกุญแจสาธารณะในการรักษาความปลอดภัยของข้อมูลที่สื่อสารผ่านเครือข่ายคอมพิวเตอร์ เช่น อินเทอร์เน็ต (Internet) อินทราเน็ต (Intranet) หรือ เอ็กซ์ทราเน็ต (Extranet) โดยองค์กรสามารถออกใบรับรองดิจิทัลส่วนตัวเองโดยใช้ระบบของผู้ประกอบการออกใบรับรอง ซึ่งจะมีชื่อองค์กรออกใบรับรองที่ได้รับการรับรองและกุญแจสาธารณะขององค์กรนั้น และลายมือชื่อดิจิทัลขององค์กรออกใบรับรองที่ให้การรับรอง ซึ่งอาจเป็นการรับรองตนเอง (self-certified) ก็ได้ในกรณีที่องค์กรออกใบรับรองทั้งสองเป็นหน่วยงานเดียวกัน

3.3.3 สภาพแวดล้อมแบบเปิดและสภาพแวดล้อมแบบปิด

สภาพแวดล้อมในการออกใบรับรองสามารถแบ่งออกได้เป็น 2 ลักษณะ ดังนี้

- สภาพแวดล้อมแบบเปิด (open PKI) ซึ่งพบมากในการค้าปลีกผ่านเครือข่ายอินเทอร์เน็ตและการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและผู้บริโภคอื่น ฝ่ายต่างๆ ที่เกี่ยวข้องมักไม่รู้จักกันมาก่อนและไม่มีความสัมพันธ์ในเชิงสัญญา (contractual relationship) กันล่วงหน้า ในสภาพแวดล้อมนี้ บทบาทขององค์กรออกใบรับรองคือการออกใบรับรองตัวบุคคล (identity certificate) เพื่อให้ทั้งสองฝ่ายสามารถระบุตัวบุคคลอีกฝ่ายหนึ่งได้
- สภาพแวดล้อมแบบปิด (close PKI) ฝ่ายต่างๆ ที่เกี่ยวข้องจะรู้จักกันและมักมีความสัมพันธ์ในเชิงสัญญากันอยู่แล้ว ซึ่งพบบ่อยในการพาณิชย์ อิเล็กทรอนิกส์ระหว่างธุรกิจ-ธุรกิจ เช่น การซื้อขายสินค้าผ่านเครือข่ายเอ็กซ์ทราเน็ต (extranet) หรือเครือข่ายอีดีไอ (EDI) การติดต่อระหว่าง บุคคลต่างๆ ในองค์กรเดียวกันผ่านเครือข่ายอินทราเน็ต (intranet) หรือแม้แต่การพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจและผู้บริโภคในบางรูปแบบ เช่น การทำธุรกรรมด้านการเงินระหว่างธนาคารและลูกค้าของธนาคาร เป็นต้น ในบางกรณีบุคคลที่สองและบุคคลที่สาม อาจเป็นบุคคลเดียวกัน ทำให้เหลือเพียงฝ่ายต่างๆ ที่เกี่ยวข้องเพียงสองฝ่าย (two-party model) เช่น ธนาคารเป็นผู้ออก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ใบรับรองให้แก่ลูกค้า และใช้ใบรับรองนั้นในการระบุตัวลูกค้าของตนในการทำธุรกรรม หรือบริษัทเป็นผู้ออกใบรับรองให้แก่พนักงานและใช้ใบรับรองนั้น ในการกำหนดสิทธิในการใช้เครื่องคอมพิวเตอร์ ในสภาพแวดล้อมนี้บทบาทขององค์กรออกใบรับรองอาจเปลี่ยนจากการออกใบรับรอง ตัวบุคคลไปสู่การออกใบรับรองสิทธิหรืออำนาจหน้าที่ (authority certificate) แทน เช่น การออกใบรับรองว่าผู้สั่งซื้อสินค้าเป็นเจ้าหน้าที่ ซึ่งมีอำนาจในการสั่งซื้อจริง

3.3.4 ข้อจำกัดในการระบุตัวบุคคลด้วยใบรับรองดิจิทัล

แม้ว่าการใช้ใบรับรองดิจิทัลจะช่วยแก้ปัญหาความปลอดภัยในการทำธุรกรรมทางการพาณิชย์อิเล็กทรอนิกส์ได้ในระดับหนึ่ง จากการช่วยให้ฝ่ายต่างๆ สามารถระบุตัวบุคคลอื่นที่ติดต่อด้วยได้ก็ตาม วิธีการตรวจสอบและออกใบรับรองในปัจจุบันยังมีข้อจำกัดที่สำคัญหลายประการคือ

- การระบุตัวบุคคลด้วยใบรับรองดิจิทัลยึดหลักในการระบุตัวบุคคลด้วยกุญแจลับซึ่งเป็นสิ่งที่บุคคลนั้นมีในครอบครอง ในทางปฏิบัติผู้ครอบครองกุญแจลับอาจไม่ใช่เจ้าของใบรับรองนั้นก็ได้ซึ่งแตกต่างจากการระบุตัวบุคคลด้วยลักษณะทางชีวภาพ (biometrics)
- ใบรับรองตามมาตรฐาน X.509 v3 ซึ่งเป็นมาตรฐานหลักไม่มีข้อมูลที่เพียงพอในการระบุตัวบุคคลในบางสถานการณ์ เช่น ไม่ระบุอายุหรือเพศของผู้ถือใบรับรอง ซึ่งอาจจำเป็นต้องใช้ในเว็บไซต์บางแห่งเช่นเว็บไซต์ที่ให้บริการเฉพาะผู้ที่มีอายุเกิน 20 ปีขึ้นไป หรือเว็บไซต์ที่ให้บริการเฉพาะผู้หญิง
- ในการใช้ใบรับรองตามมาตรฐาน X.509 v3 ผู้ถือใบรับรองไม่สามารถเลือกเปิดเผยข้อมูลบางส่วนในใบรับรองได้แต่ต้องเปิดเผยทั้งหมด ทั้งที่ในบางสถานการณ์ข้อมูลอื่นในใบรับรองอาจไม่เกี่ยวข้องในการใช้เลยก็ตามเช่น ในการใช้เว็บไซต์ที่จำกัดเพียงอายุของผู้ใช้ ผู้ใช้อาจไม่ต้องการเปิดเผยชื่อและที่อยู่
- การตรวจสอบหลักฐานว่าบุคคลนั้นเป็นบุคคลตามที่กล่าวอ้างหรือไม่นั้นมักใช้วิธีง่ายๆ เพื่อประหยัดต้นทุนในการตรวจสอบ ทำให้ผู้ใช้ใบรับรองในการระบุตัวผู้อื่นไม่มีความมั่นใจอย่างเต็มที่
- การออกใบรับรองตัวบุคคลในการพาณิชย์อิเล็กทรอนิกส์ระหว่างธุรกิจกับผู้บริโภคส่วนใหญ่ยังเป็นการออกใบรับรองให้แก่เฉพาะธุรกิจ หรือการรับรองเครื่องแม่ข่ายแบบ SSL ซึ่งทำให้ผู้บริโภคสามารถระบุตัวผู้ขายได้ แต่ผู้ขายยังไม่สามารถระบุตัวผู้ซื้อได้ ทั้งนี้เนื่องจากผู้ซื้อยังไม่มีแรงจูงใจในการขอใบรับรองดังกล่าว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.4 ซอฟต์แวร์ที่ใช้ในการดำเนินงาน

ระบบปฏิบัติการและซอฟต์แวร์ที่เลือกใช้ต่อไปนี้

1. ระบบปฏิบัติการ Window XP

Microsoft Windows XP คือระบบปฏิบัติการสมบูรณ์แบบสำหรับระบบคอมพิวเตอร์ที่ต้องการประสิทธิภาพ และเสถียรภาพในการทำงาน ได้รับการออกแบบมาเพื่อให้มีความเชื่อถือได้ มีระบบรักษาความปลอดภัย มีประสิทธิภาพสูง และใช้งานได้ง่าย

2. ภาษาในการพัฒนาเว็บแอพพลิเคชัน PHP

PHP หมายถึง PHP Hypertext Preprocessor ซึ่งเป็นภาษาสคริปต์แบบหนึ่งที่เรียกว่า Server Side Script หรือ HTML-embedded scripting language เป็นภาษาจำพวก scripting language คำสั่งต่างๆ จะเก็บอยู่ในไฟล์ที่เรียกว่า สคริปต์ (script) และเวลาใช้งานต้องอาศัยตัวแปลชุดคำสั่ง ตัวอย่างของภาษาสคริปต์ เช่น JavaScript, Perl เป็นต้น เป็นเครื่องมือที่สำคัญชนิดหนึ่งที่ช่วยให้เราสามารถสร้างเอกสารแบบ Dynamic HTML ได้อย่างมีประสิทธิภาพและมีลูกเล่นมากขึ้น ลักษณะของ PHP ที่แตกต่างจากภาษาสคริปต์แบบอื่นๆ คือ PHP ได้รับการพัฒนาและออกแบบมา เพื่อใช้งานในการสร้างเอกสารแบบ HTML โดยสามารถสอดแทรกหรือแก้ไขเนื้อหาได้โดยอัตโนมัติ

PHP เป็นผลงานที่มาจากกลุ่มของนักพัฒนาในเชิงเปิดเผยรหัสต้นฉบับ หรือ OpenSource ดังนั้น PHP จึงมีการพัฒนาไปอย่างรวดเร็ว และแพร่หลายโดยเฉพาะอย่างยิ่งเมื่อใช้ร่วมกับ Apache Webserver ในปัจจุบัน PHP สามารถใช้ร่วมกับเว็บเซิร์ฟเวอร์ หลายๆ ตัวบนระบบปฏิบัติการอย่างเช่น Windows 95/98/NT/XP เป็นต้น เป็นภาษาที่ใช้ในการพัฒนาโปรแกรมบนเว็บรวมทั้งยังสามารถเข้าถึงระบบฐานข้อมูลได้หลายประเภทอีกด้วย

3. โครงสร้างพื้นฐานระบบเว็บแอพลิเคชั่นด้วย PHP-Nuke

PHP-Nuke เป็นเว็บแอปพลิเคชันหรือเว็บไซต์สำเร็จรูปที่เขียนขึ้นจากสคริปต์ PHP จัดเป็นโปรแกรมประเภท CMS (Content Management System) ด้วยการใช้งานภาษา PHP ร่วมกับระบบฐานข้อมูล MySQL โดยนาย Francisco Burzi ได้คิดค้นและพัฒนาโปรแกรมกึ่งสำเร็จรูปในการสร้างเว็บไซต์ที่ครอบคลุมความต้องการส่วนใหญ่ของงานทางด้านเว็บไซต์ไว้อย่างครบถ้วน ต่อมาได้มีการพัฒนารูปแบบ และมีความสามารถในการปรับแต่งได้หลากหลาย จึงทำให้ผู้สร้างเว็บไซต์นิยมนำเอา PHP-Nuke มาใช้ทำเว็บไซต์กันมากขึ้น เนื่องจากรูปแบบที่ปรับเปลี่ยนได้ง่าย และมีความสวยงามโดยที่ผู้สร้างเว็บไซต์ ไม่จำเป็นต้องทราบการเขียนสคริปต์ต่าง ๆ มากนัก PHP-Nuke สามารถทำงานได้ทั้งบนระบบวินโดวส์ และลีนุกซ์ รวมทั้งสนับสนุนการใช้งานภาษาต่างๆ ทั่วโลกได้มากกว่า 25 ภาษา รวมถึงภาษาไทยด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ข้อดีของ PHP-Nuke คือ เป็นโปรแกรมที่มีเครื่องมือในการสร้างเว็บไซต์ที่จำเป็นทุกอย่าง ไม่ว่าจะเป็นการเปลี่ยนหน้าตาของเว็บ การสร้างเนื้อหา การสร้างเว็บลิงค์ การสร้างเว็บบอร์ด ห้องดาวน์โหลด การสร้างระบบสมาชิก ที่สำคัญสามารถส่งข่าวสารถึงกันโดยไม่ต้องใช้อีเมล และสามารถดึงข่าวสารจากเว็บอื่นๆ มาแสดงที่หน้าเว็บเพจได้อย่างอัตโนมัติ

4. ระบบการจัดการเว็บเซิร์ฟเวอร์ด้วย Apache

Apache คือ ซอฟต์แวร์ที่ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์ที่มีผู้ใช้กันอย่างแพร่หลายมีหน้าที่ในการจัดเก็บโฮมเพจและส่งโฮมเพจไปยังเว็บบราวเซอร์ที่มีการเรียกเข้ายังเว็บเซิร์ฟเวอร์ที่เก็บโฮมเพจนั้นอยู่ ซึ่งปัจจุบันจัดได้ว่าเป็นเว็บเซิร์ฟเวอร์ที่มีความน่าเชื่อถือมาก และเป็นเว็บเซิร์ฟเวอร์เพียงหนึ่งเดียวที่อยู่คู่กับระบบปฏิบัติการลีนุกซ์ จากจุดเริ่มต้นที่อาศัยโค้ดจากเว็บเซิร์ฟเวอร์มาตรฐาน NCSA (องค์กรกลางผู้กำหนดมาตรฐานโพรโทคอล HTTP มาตรฐานภาษา HTML และมาตรฐานอื่นๆ ที่เกี่ยวข้องกับงานบริการบนเว็บทั้งหมด) เป็นซอฟต์แวร์ที่เริ่มต้นจากส่วนประกอบเล็กๆ หรือ "patch" จำนวนมากมาย จนถูกเรียกว่า "a patchy" พัฒนาอย่างต่อเนื่องผ่านโมเดลการพัฒนาแบบฟรีซอฟต์แวร์ ภายใต้การกำกับดูแลของ Apache Foundation (http://www.apache.org) ทำให้เกิดซอฟต์แวร์เว็บเซิร์ฟเวอร์ที่มีเสถียรภาพการทำงานที่เชื่อถือได้ มีประสิทธิภาพสูง และแข็งแกร่ง เป็นแม่แบบของฟรีซอฟต์แวร์ที่ประสบความสำเร็จอย่างมาก

5. ระบบการจัดการฐานข้อมูลด้วย MySQL

MySQL เป็นฐานข้อมูลเชิงสัมพันธ์ (RDBMS: Relational Database Management System) เป็น Database Server ที่เหมาะสมกับองค์กรขนาดกลางที่มีข้อมูลไม่มากนัก พัฒนาโดยบริษัท MySQL AB ประเทศสวีเดน ผู้ก่อตั้งเป็นชาวสวีเดนสองคนคือ David Axmark และ Allan Larsson และชาวฟินด์แลนด์อีกหนึ่งคนคือ Michael "Monty" Widenius ซึ่งมีวัตถุประสงค์ให้ MySQL เป็นซอฟต์แวร์ฟรีที่เปิดเผยซอร์สโค้ดภายใต้ GNU Public License (GPL) MySQL เป็นฐานข้อมูลในระดับไคล์เอนท์เซิร์ฟเวอร์ ประกอบไปด้วย 2 ส่วนหลักๆ คือ ส่วนของผู้ให้บริการ (Server) และส่วนของผู้ใช้บริการ (Client) โดยในแต่ละส่วนจะมีโปรแกรมสำหรับการทำงานตามหน้าที่ของตน ส่วนของผู้ให้บริการ หรือ เซิร์ฟเวอร์เป็นส่วนที่ทำหน้าที่บริหารจัดการระบบฐานข้อมูลในที่นี้หมายถึง MySQL Server และยังเป็นที่จัดเก็บข้อมูลทั้งหมด ซึ่งมีทั้งข้อมูลที่จำเป็นสำหรับการทำงานกับระบบฐานข้อมูล และข้อมูลที่เกิดจากการที่ผู้ใช้แต่ละคนสร้างขึ้นมา ส่วนของผู้ใช้บริการ หรือ ไคล์เอนท์คือส่วนของผู้ใช้ โดยโปรแกรมสำหรับใช้งานในส่วนนี้ได้แก่ MySQL Client , Access,VB, Delphi หรือ Web Development Platform ต่างๆ เช่น PHP , Perl หรือ ASP เป็นต้น MySQL มีความสามารถในการจัดการกับฐานข้อมูลด้วยภาษา SQL (Structures Query Language) ได้อย่างมีประสิทธิภาพ มีความรวดเร็ว รองรับการทำงานจากผู้ใช้หลายคนและหลายงานได้ในเวลาเดียวกัน เพราะฉะนั้นนอกจากเราจะใช้ MySQL เป็นฐานข้อมูลบนเว็บแล้ว ยังสามารถนำ MySQL

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

มาใช้ในการพัฒนาโปรแกรมฐานข้อมูลแบบ Client/Server ได้ด้วย รวมทั้ง MySQL ยังเป็นฐานข้อมูลของระบบสารสนเทศวิสาหกิจชุมชนที่พัฒนาขึ้นด้วย PHP ทำงานบนเว็บเซิร์ฟเวอร์ Apache ซึ่งเป็นโอเพ่นซอร์สทั้งหมด ทำให้ค่าใช้จ่ายในการพัฒนาระบบลดลงเป็นอย่างมาก

6. การสร้างใบรับรองดิจิทัลด้วย OpenSSL

OpenSSL เกิดจากกลุ่มองค์กรอิสระที่พัฒนา ssl ในมาตรฐานเปิด (มาตรฐานเปิด หมายถึงกลุ่มที่ร่วมกันพัฒนาแอพพลิเคชันที่เปิดเผย source code และสามารถดาวน์โหลดซอฟต์แวร์ได้โดยไม่เสียค่าใช้จ่าย) เป็นความพยายามในการพัฒนาทูลคิดที่มีประสิทธิภาพเทียบเท่าผลิตภัณฑ์เชิงพาณิชย์ ซึ่งมีพื้นฐานมาจากไลบรารี SSLeay ที่พัฒนาโดย Eric Young โดยมีโพรโทคอล ssl เป็นโพรโทคอลการทำงานของ Transport Layer Security ที่ออกแบบมาให้ทำงานกับแอพพลิเคชัน LDAP secure SSL, WEB secure SSL เป็นต้น สิ่งที่เพิ่มเติมคือ ได้รวบรวมประโยชน์สำหรับการจัดการเกี่ยวกับการสร้างใบรับรองดิจิทัล เช่น public key cryptography, Strong Authentication, Signing และ encryption รวมทั้งยังสามารถจะทำงานร่วมกับการ encryption รูปแบบต่างๆ และทำงานกับแอพพลิเคชันที่มีระดับของความปลอดภัยต่างๆ กัน

7. การจัดการระบบเมล์เซิร์ฟเวอร์ด้วย ArGoSoft

ArGoSoft Mail Server เป็นโปรแกรมประเภทฟรีแวร์ ใช้ติดตั้งเพื่อทดสอบการส่งอีเมลจากเว็บไซต์โดยไม่ต้องเชื่อมต่ออินเทอร์เน็ตจริง นั่นคือสามารถจำลองคอมพิวเตอร์พีซีธรรมดาเป็น mail server เสมือนได้สามารถตั้ง Email Account ได้ถึง10 บัญชี และกำหนดโดเมนเนมได้ตามที่ต้องการโดยไม่จำเป็นต้องมีโดเมนจริง

8. การจัดการระบบเมล์ไคลเอนท์ด้วย Outlook Express

โปรแกรม Microsoft Outlook Express ถูกพัฒนาขึ้นมาพร้อมกับโปรแกรมชุด Microsoft Officeที่มาพร้อมกับ Microsoft Internet Explorer และ Microsoft Windows รองรับโพรโทคอล Post Office Protocol 3 (POP3) หรือ Internet Message Access Protocol (IMAP) เป็นโปรแกรมที่จัดการกับข้อมูลส่วนบุคคลและการส่งจดหมายอีเล็กทรอนิกส์ ที่มีประสิทธิภาพและใช้งานง่าย มุ่งเน้นอำนวยความสะดวกของการรับส่งอีเมล ในเครือข่ายอินเทอร์เน็ตเป็นหลัก โดยลักษณะการทำงานของ Outlook คือ สามารถส่งจดหมายในรูปแบบของ E-Mail เหมือนกับการบริการ E-Mail ของเว็บไซต์ต่างๆ แต่เป็นการทำงานโดยใช้ Outlook และการสร้างตารางนัดหมาย หรือปฏิทินการทำงาน สามารถบันทึกข้อมูลของผู้ที่เราติดต่อไว้เพื่อใช้ในการติดต่อในภายหลัง รวมทั้งมีการข้อความและเสียงเตือนเมื่อถึงเวลานัดหมายนั้นๆ ซึ่งจะทำให้การทำงานขององค์กรเกิดประสิทธิภาพมากขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

การวิเคราะห์และออกแบบระบบการออกใบรับรองดิจิทัล

4.1. ขั้นที่ 1 : Problem Definition

ปัจจุบัน การติดต่อสื่อสารข้อมูลผ่านทางเครือข่ายอินเทอร์เน็ตเป็นสิ่งที่เราต้องให้ความสำคัญอย่างมากโดยเฉพาะในเรื่องของความปลอดภัยของข้อมูลที่ใช้ในการสื่อสารและการสร้างความน่าเชื่อถือในการมีตัวตนอยู่จริงระหว่างผู้รับและผู้ส่ง เนื่องจากการแลกเปลี่ยนข้อมูลผ่านเครือข่ายนั้นสามารถเข้าถึงได้ง่ายทำให้มีความเสี่ยงสูงต่อการถูกคุกคามจากผู้ที่ไม่ประสงค์ดี หรือจากโปรแกรมบางประเภท ทั้งการดักฟัง การโจรกรรมข้อมูล หรือการปลอมแปลงข้อมูล เป็นสาเหตุทำให้เกิดความเสียหาย ต่อองค์กรเป็นอย่างมาก ทางผู้พัฒนาระบบได้เห็นความสำคัญในจุดนี้ จึงได้พยายามศึกษาและพัฒนาระบบการเป็นผู้ให้บริการออกใบรับรองดิจิทัล (Digital Certificate) ทำหน้าที่ในการออกใบรับรองให้กับหน่วยงานของตนเองและสามารถเผยแพร่ใบรับรองให้กับผู้อื่นเพื่อใช้ติดตั้งในการติดต่อสื่อสารระหว่างกันแสดงถึงการมีตัวตนอยู่จริงผ่านทางช่องทางสื่อสารที่ปลอดภัย แต่เนื่องจากโดยส่วนใหญ่หน่วยงานหรือองค์กรที่ต้องการเป็นผู้ให้บริการออกใบรับรองนั้นต้องเสียค่าใช้จ่ายสูง ทางผู้พัฒนาระบบจึงได้นำมาเป็นกรณีศึกษาในการนำมาพัฒนาระบบในรูปแบบของโอเพ่นซอร์ส เพื่อเป็นแนวทางในการนำระบบนี้ไปพัฒนาหรือประยุกต์ใช้กับหน่วยงานหรือองค์กรของตนเองต่อไป

จากการวิเคราะห์ความเป็นไปได้ในด้านต่างๆ ในการพัฒนาระบบ มีข้อสรุปด้าน Economical Feasibility, Technical Feasibility และ Operation Feasibility ดังนี้

- **Operation Feasibility:** มีการเพิ่มคุณสมบัติให้กับโพรโทคอล HTTP มากขึ้นในการรักษาความปลอดภัยของข้อมูลระหว่างเบราเซอร์กับเว็บเซิร์ฟเวอร์ โดยประยุกต์เข้ากับ Open SSL กลายเป็นช่องทางการสื่อสารที่ปลอดภัย HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) หลักการของ HTTPS คือ การรับส่ง HTTP message บน SSL ผ่านทาง Port 443 (HTTP ใช้ Port 80) หรือเป็นการ Implement HTTP บน SSL อีกชั้นหนึ่ง ทำให้ระบบมีความปลอดภัยสูง
- **Economical Feasibility:** เนื่องจากสามารถสร้างระบบออกใบรับรองดิจิทัลใช้เอง ทำให้ลดค่าใช้จ่ายภายในหน่วยงานหรือองค์กรที่ต้องการสร้างความปลอดภัยในการสื่อสาร เนื่องจากในปัจจุบันระบบที่ทำหน้าที่ในการออกใบรับรองดิจิทัลส่วนใหญ่นั้นจะต้องเสียค่าใช้จ่ายสูงเพื่อขอใช้ใบรับรองขององค์กรนั้น รวมถึงทำให้พนักงานหรือบุคคลที่อยู่ภายในองค์กรนั้นได้ตระหนักถึงความปลอดภัยในการส่งข้อมูลได้อีกด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ ดัดแปลง เผยแพร่ หรือแสวงหาประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- **Technical Feasibility:** ได้เลือกซอฟต์แวร์ต่างๆ ที่เป็นโอเพ่นซอร์สเข้ามาใช้ในระบบ เช่น PHP ทำหน้าที่เป็นแอพพลิเคชันเซิร์ฟเวอร์, My SQL ทำหน้าที่เป็นเดต้าเบสเซิร์ฟเวอร์, Open SSL ทำหน้าที่เป็นโพรโทคอลช่องทางการสื่อสารที่ปลอดภัย และ Apache ทำหน้าที่เป็นเว็บ

4.2. ขั้นที่ 2 : Requirement Definition

จากการวิเคราะห์ความต้องการ สามารถสรุปได้ดังนี้

1. ผู้ใช้ต้องทำการสมัครเป็นสมาชิกของระบบ
2. สมาชิกที่เข้ามาร้องขอใบรับรองดิจิทัลจะต้องทำการกรอกข้อมูล จากนั้นหน่วยงานที่ดูแลระบบ (Registration Authority)จะทำการตรวจสอบความถูกต้อง ของข้อมูลเพื่อดำเนินการออกใบรับรองดิจิทัลให้แก่สมาชิก
3. สมาชิกทำการยืนยันกับทางระบบผ่านทางอีเมลภายใน 1 วัน ถ้าเกินจากนั้นสมาชิกจะต้องทำการร้องขอใบรับรองดิจิทัลใหม่
4. สมาชิก 1 คนสามารถทำการร้องขอใบรับรองดิจิทัลได้หลายใบแต่ห้ามใช้อีเมลเดิม เนื่องจากอีเมล 1 อีเมลจะสามารถมีใบรับรองได้ 1ใบเท่านั้น
5. สมาชิกสามารถทำการดาวน์โหลด Private key ,CSR file, Certificate เพื่อนำไปใช้งานได้โดย Certificate จะมีอายุการใช้งานภายใน 1 ปี
6. สมาชิกสามารถทำการขอยกเลิกใบรับรองได้ตามแต่กรณี
7. สมาชิกสามารถทำการต่ออายุใบรับรองได้ โดยจะมีอีเมลแจ้งเตือนก่อน 15 วัน
8. สมาชิกสามารถทำการค้นหาและทำการดาวน์โหลดใบรับรองดิจิทัลของบุคคลอื่นที่ต้องการติดต่อด้วยได้ และสามารถตรวจสอบสถานะใบรับรองดิจิทัลของผู้ใช้คนอื่นได้ โดยทำการดาวน์โหลด CRL มาติดตั้งไว้ที่เครื่อง
9. ผู้ดูแลระบบ (Administrator) สามารถทำการรับรองตนเอง และมีสิทธิ์ในการจัดการใบรับรองของสมาชิกทุกคนในระบบ เช่นการดาวน์โหลดใบรับรองดิจิทัล การยกเลิกหรือยกเลิกใบรับรองของสมาชิกในทุกกรณี ไม่ว่าจะเป็นกรณีที่สมาชิกขอยกเลิกเองหรือผู้ดูแลระบบเห็นสมควรในการยกเลิก

4.3. ขั้นที่ 3 : Design

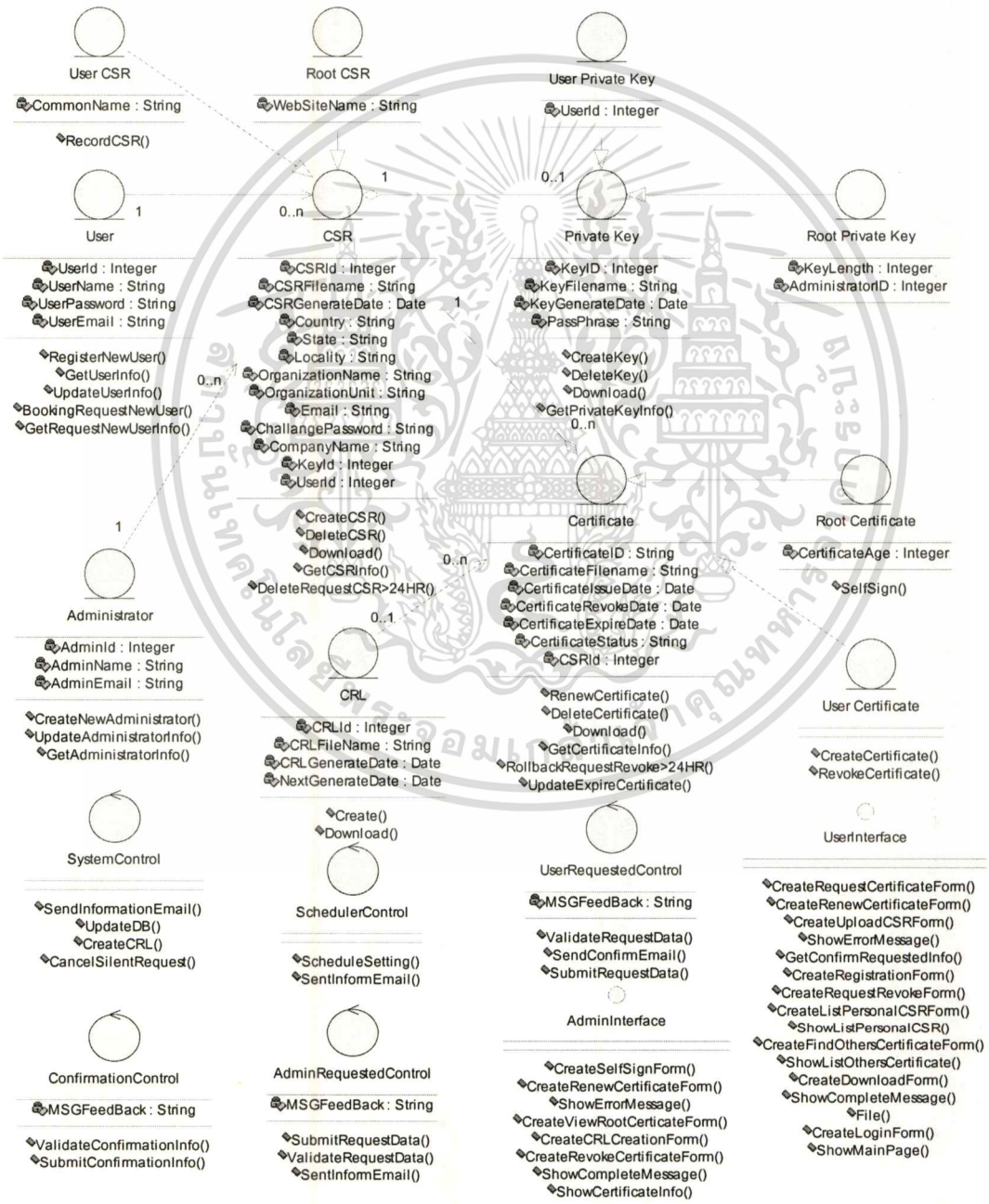
จากการวิเคราะห์ความต้องการพร้อมทั้งความสามารถที่ระบบควรจะต้องมีแล้ว เราจะใช้ UML (Unified Modeling Language) ซึ่งเป็นภาษามาตรฐานที่ใช้สำหรับอธิบายแบบจำลองของ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ซอฟต์แวร์แนวคิดเชิงวัตถุ เพื่ออธิบายแบบจำลองการทำงานระบบที่สร้างขึ้น โดยในการพัฒนาระบบงานนี้ เราจะเลือกใช้ไดอะแกรมเพียง 3 ไดอะแกรม ดังนี้

4.3.1 คลาสไดอะแกรม (Class Diagram)

คลาสไดอะแกรมเป็นแผนภาพแสดงกลุ่มของคลาสเพื่อให้เรารู้และสามารถกำหนดว่าแต่ละออบเจ็กต์ควรจะมีคุณสมบัติและพฤติกรรมอย่างไรต่อระบบงานของเรา โดยโครงสร้างของคลาสที่ใช้ในการอธิบายจะแบ่งเป็น3 ส่วนคือ แอตทริบิวต์ โอเปอร์เรชัน และความสัมพันธ์



รูปที่ 4.1 คลาสไดอะแกรมของระบบผู้ให้บริการออกใบรับรองดิจิทัล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 4.1 แสดงคลาสไดอะแกรมของระบบ ซึ่งประกอบด้วย เอนทิตีคลาส คอนโทรลคลาส และ อินเทอร์เฟสคลาส ที่เกี่ยวข้องกับระบบผู้ให้บริการออกใบรับรองดิจิทัล

4.3.2 ยูสเคสไดอะแกรม (Use Case Diagram)

ยูสเคสไดอะแกรมเป็นเครื่องมือที่สามารถช่วยให้ผู้ใช้ระบบสามารถสื่อสารให้ผู้ออกแบบระบบได้รับรู้ว่าต้องการใช้ระบบลักษณะไหนอย่างเป็นรูปธรรม เพื่อให้ผู้ออกแบบสามารถสร้างระบบได้ตรงตามความต้องการของผู้ใช้ได้อย่างครบถ้วน

ในการวิเคราะห์ออกแบบระบบใบรับรองดิจิทัลนี้เราสามารถกำหนดได้ ดังนี้

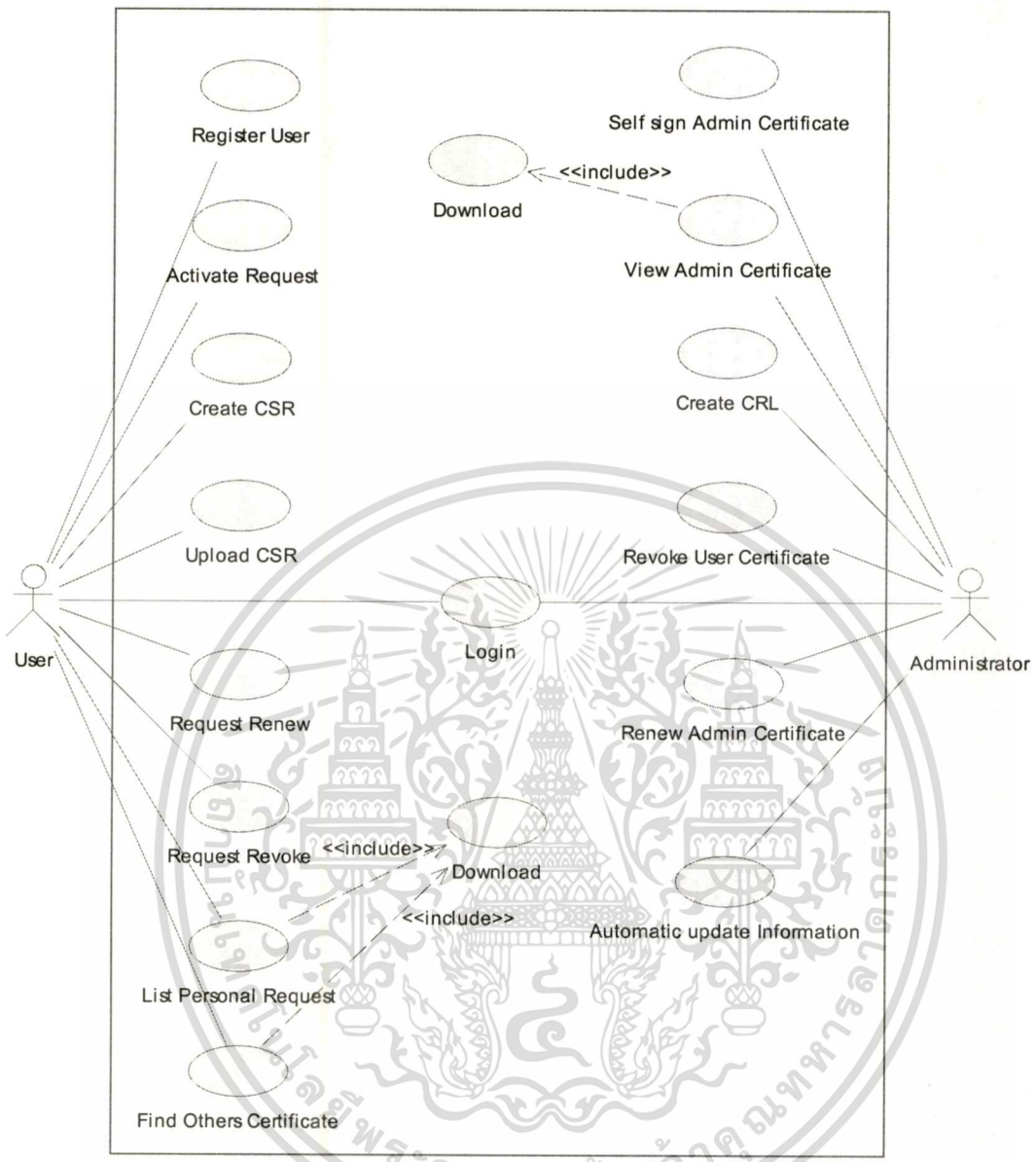
- Actor ผู้ที่เกี่ยวข้องกับระบบ
  1. ผู้ใช้ (User) คือผู้ใช้ที่เข้ามาทำการใช้บริการของระบบในกรณีต่างๆ เช่น สมัครสมาชิก ร้องขอใบรับรอง ดาวน์โหลดใบรับรอง เป็นต้น
  2. ผู้ดูแลระบบ (Administrator) คือผู้ที่มีสิทธิ์ในการควบคุมดูแลจัดการระบบทั้งหมด เช่น การอนุมัติการออกใบรับรอง การยกเลิกใบรับรอง เป็นต้น
- Use Case การทำงานของระบบ
  1. Register : การลงทะเบียนเพื่อสมัครเป็นสมาชิกของระบบ
  2. Login : การเข้าใช้งานระบบ
  3. Activate Request : การยืนยันกับระบบเกี่ยวกับการดำเนินการในเรื่องของการลงทะเบียนผู้ใช้ การร้องขอใบรับรองดิจิทัล และการขอยกเลิกใบรับรอง
  4. Create CSR : การร้องขอใบรับรองดิจิทัลกับระบบ
  5. Upload CSR : การที่ผู้ใช้สามารถนำไฟล์นามสกุล .CSR ที่มีอยู่มาทำการร้องขอใบรับรองดิจิทัลจากระบบได้
  6. Request Renew : การต่ออายุใบรับรองดิจิทัล
  7. Request Revoke : การที่ผู้ใช้ทำการยกเลิกใบรับรองดิจิทัล
  8. List Personal Request : แสดงรายการการร้องขอใบรับรองส่วนตัวของผู้ใช้ เช่น สถานะร้องขอ วันที่ใบรับรองอนุมัติ วันที่ใบรับรองหมดอายุ เป็นต้น
  9. Find Others Certificate : การแสดงหรือค้นหาใบรับรองของผู้ใช้ทั้งหมดที่มีในระบบ
  10. Download : ผู้ใช้สามารถทำการดาวน์โหลดไฟล์ต่างๆ ได้ เช่น กุญแจส่วนตัว (.key) ไฟล์การร้องขอ (.csr) ใบรับรองดิจิทัล (.crt , .cer, .p12)
  11. Self sign Admin Certificate : การที่ผู้ดูแลระบบทำการรับรองตนเอง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

12. View Admin Certificate : แสดงข้อมูลใบรับรองดิจิทัลของผู้ดูแลระบบพร้อมทั้งสามารถทำการดาวน์โหลดไฟล์ต่างๆ ได้ เหมือนกับของผู้ใช้ ที่พิเศษกว่าคือ สามารถดาวน์โหลดไฟล์กุญแจส่วนตัวที่ไม่มี PassPhrase เพื่อประยุกตีใช้กับเว็บเซิร์ฟเวอร์ผ่านช่องทางการสื่อสารที่ปลอดภัย (HTTPS)
13. Create CRL : การที่ผู้ดูแลระบบต้องการให้ระบบทำการสร้าง CRL ใหม่เพื่อให้การยกเลิกใบรับรองนั้นๆ มีผลทันที
14. Revoke User Certificate : ผู้ดูแลระบบสามารถทำการยกเลิกใบรับรองของผู้ใช้ในกรณีจำเป็นได้
15. Renew Admin Certificate : ผู้ดูแลระบบทำการต่ออายุใบรับรองดิจิทัลของตนเอง
16. Automatic Update Information : การใช้ฟังก์ชัน Windows Schedule Task ที่ตั้งไว้อัตโนมัติในดำเนินการต่างๆ เช่น การแจ้งผู้ใช้ทราบล่วงหน้า 15 วัน ก่อนที่ใบรับรองดิจิทัลจะหมดอายุ เป็นต้น

จากรูปที่ 4.2 เป็นยูสเคสไดอะแกรมภาพรวมการทำงานของระบบผู้ให้บริการออกใบรับรองดิจิทัล แสดงความสัมพันธ์ที่เกิดขึ้นระหว่างแอคเตอร์กับยูสเคสในระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.2 ยูสเคสไดอะแกรมของระบบผู้ให้บริการออกใบรับรองดิจิทัล

4.3.3 ซีเควนซ์ไดอะแกรม (Sequence Diagram)

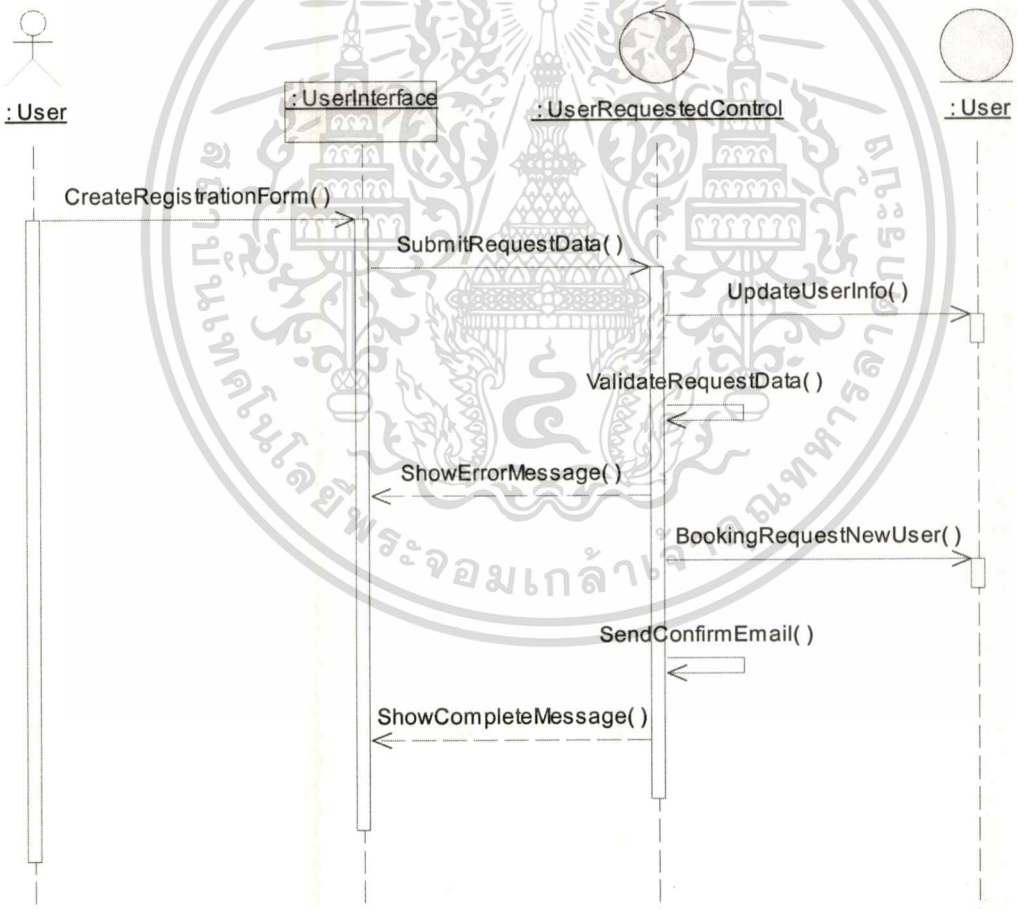
ซีเควนซ์ไดอะแกรมเป็นแผนภาพที่ใช้แสดงถึงการมีปฏิสัมพันธ์ (Interaction) กันระหว่างออบเจ็กต์ในระบบงานว่ามีการติดต่อสื่อสารกันอย่างไร ณ เวลาหนึ่ง ซึ่งจะเน้นช่วงเวลาการทำงานเป็นสำคัญ

จากยูสเคสในหัวข้อที่ 4.3.2 เราสามารถนำมาใช้ในการอธิบายเพื่อแสดงถึงช่วงเวลาการทำงานที่เกิดขึ้นระหว่างแอคเตอร์ที่มีในระบบ เป็นแผนภาพซีเควนซ์ไดอะแกรมได้ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.1 อธิบายยูสเคส Register

ยูสเคส	Register
วัตถุประสงค์	ลงทะเบียนผู้ใช้
เงื่อนไขเมื่อเริ่มต้น	-
เมื่อทำงานสำเร็จ	จัดส่งอีเมลเพื่อยืนยันการลงทะเบียนให้แก่ผู้ใช้
เมื่อทำงานไม่สำเร็จ	ระบบแจ้งความผิดพลาดที่เกิดขึ้น
ผู้ใช้ที่เกี่ยวข้อง	ผู้ใช้ทั่วไป (User)
ข้อมูลเข้า	ชื่อผู้ใช้, รหัสผ่าน และอีเมลหลักของผู้ใช้
ข้อมูลออก	ระบบแสดงข้อความการรับลงทะเบียนเรียบร้อย และแจ้งให้ผู้ใช้ทำการยืนยันการลงทะเบียนจากอีเมลที่ระบบจัดส่งให้



รูปที่ 4.3 ซีเควนซ์ไดอะแกรมของยูสเคส Register User

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

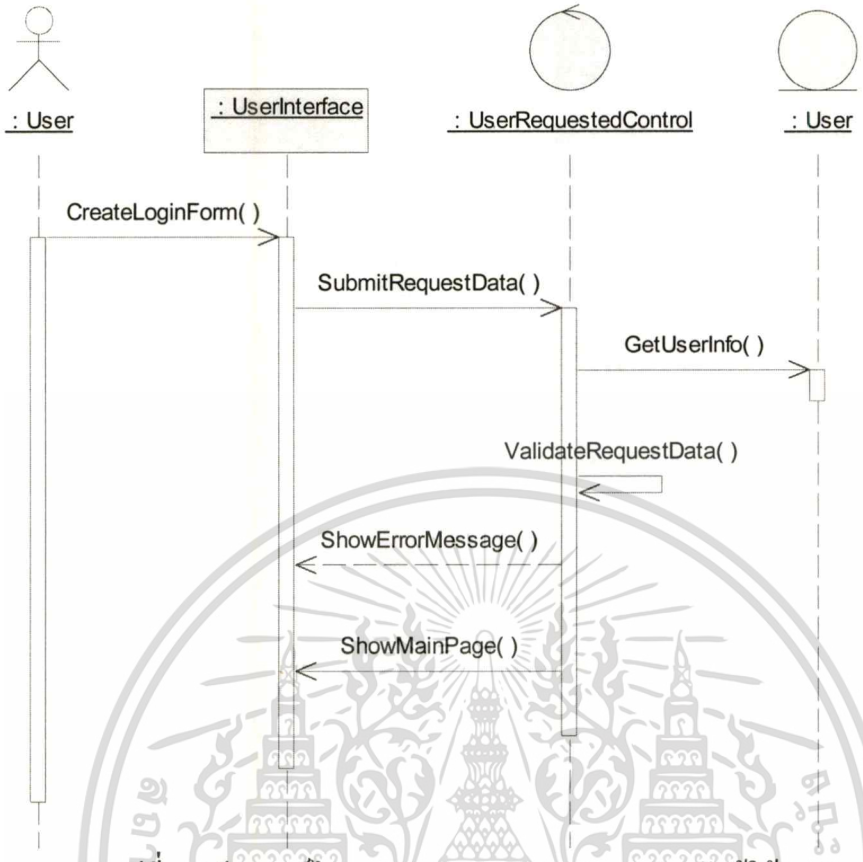
จากรูปที่ 4.3 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Register ซึ่งมีลำดับการทำงาน ดังนี้

1. ผู้ใช้เข้าสู่หน้าต่างการลงทะเบียน
2. ผู้ใช้ป้อนชื่อผู้ใช้พร้อมรหัสผ่านที่ต้องการ และอีเมลที่มีการใช้งานอยู่จริง เพื่อใช้ติดต่อกับระบบ
3. ระบบเรียกดูรายชื่อผู้ใช้ที่มีในระบบ
4. ทำการตรวจสอบความถูกต้องของชื่อผู้ใช้
5. แสดงข้อความการผิดพลาด ในกรณีที่ชื่อผู้ใช้หรืออีเมลของผู้ใช้รายใหม่ ซ้ำกับชื่อผู้ใช้หรืออีเมลที่มีการใช้งานอยู่ในระบบ
6. ระบบจัดส่งอีเมลสำหรับยืนยันการลงทะเบียนให้ผู้รับ
7. แสดงข้อความแจ้งการจบขั้นตอนการลงทะเบียน

ตารางที่ 4.2 อธิบายยูสเคส Login ในกรณีเป็นผู้ใช้

ยูสเคส	Login
วัตถุประสงค์	ตรวจสอบสิทธิ์ในการเข้าใช้งานระบบ
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ใช้ที่ได้มีการลงเบียนเรียบร้อยแล้ว
เมื่อทำงานสำเร็จ	ผู้ใช้สามารถเข้าใช้งานระบบได้
เมื่อทำงานไม่สำเร็จ	ผู้ใช้ไม่สามารถเข้าใช้งานระบบได้
ผู้ใช้ที่เกี่ยวข้อง	ผู้ใช้ทั่วไป (User) และ ผู้ดูแลระบบ (Admin)
ข้อมูลเข้า	ชื่อผู้ใช้ และรหัสผ่าน
ข้อมูลออก	แสดงหน้าจอหลักของผู้ใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.4 ซีเควนซ์ไดอะแกรมของยูสเคส Login สำหรับผู้ใช้

จากรูปที่ 4.4 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Login ซึ่งมีลำดับการทำงาน ดังนี้

1. ผู้ใช้เข้าสู่หน้าต่างล็อคอิน
2. ผู้ใช้ป้อน ชื่อและรหัสผ่าน
3. ระบบเรียกดูรายชื่อผู้ใช้ที่มีในระบบ
4. ทำการตรวจสอบชื่อผู้ใช้และรหัสผ่าน
5. แสดงข้อความผิดพลาด ในกรณีที่ชื่อผู้ใช้ไม่มีอยู่ในระบบ หรือรหัสผ่านของผู้ใช้ไม่ตรงกับชื่อผู้ใช้
6. แสดงหน้าจอหลักของผู้ใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.3 อธิบายยูสเคส Activate Request ในกรณียืนยันการลงทะเบียนผู้ใช้

ยูสเคส	Activate Request
วัตถุประสงค์	ยืนยันการลงทะเบียนเพื่อใช้งานระบบ
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ใช้ที่ได้รับอีเมลเพื่อยืนยันการลงทะเบียนจากระบบ
เมื่อทำงานสำเร็จ	ระบบปรับปรุงสถานะผู้ใช้ให้มีสถานะพร้อมเข้าใช้งานระบบ
เมื่อทำงานไม่สำเร็จ	ผู้ใช้ยังไม่มีสถานะพร้อมเข้าใช้งานระบบ
ผู้ใช้ที่เกี่ยวข้อง	ผู้ใช้ทั่วไป (User)
ข้อมูลเข้า	URL จากอีเมล ซึ่งประกอบด้วย รหัสผู้ใช้ที่ถูกเข้ารหัส และชื่อผู้ใช้
ข้อมูลออก	แสดงข้อความแจ้งสถานะการผู้ใช้งานระบบ

รูปที่ 4.5 ซีเควนซ์ไดอะแกรมของยูสเคส Activate Request ในกรณี ยืนยันการลงทะเบียนผู้ใช้

จากรูปที่ 4.5 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Activate Request ในกรณีการลงทะเบียนผู้ใช้ซึ่งมีลำดับการทำงาน ดังนี้

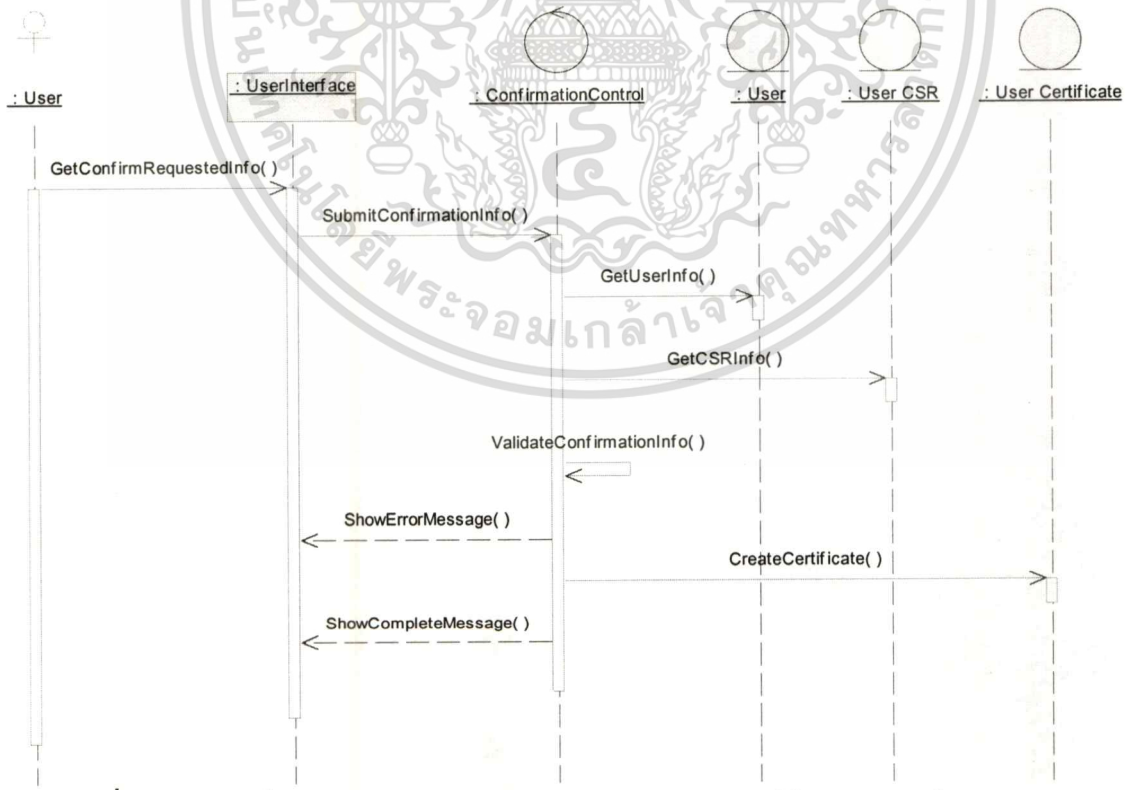
1. ผู้ใช้เข้าสู่หน้าต่างการยืนยันการลงทะเบียน โดยใช้ URL จากอีเมลที่ระบบส่งให้
2. ข้อมูลถูกส่งเข้าสู่ระบบ
3. ระบบเรียกดูข้อมูลการขอลงทะเบียน
4. ทำการตรวจสอบความถูกต้องของข้อมูลที่ได้รับจาก URL

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5. แสดงข้อความผิดพลาด ในกรณีไม่พบข้อมูลการขอลงทะเบียนในระบบ
6. ระบบทำการปรับปรุงสถานะผู้ใช้
7. แสดงข้อความแจ้งสถานการณ์ผู้ใช้งานระบบ

ตารางที่ 4.4 อธิบายยูสเคส Activate Request ในกรณียืนยันการขอใบรับรอง

ยูสเคส	Activate Request
วัตถุประสงค์	ยืนยันการขอใบรับรองเพื่อให้ระบบออกใบรับรอง
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ใช้ที่ได้รับอีเมลเพื่อยืนยันการขอใบรับรองจากระบบ และได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบสร้างใบรับรองดิจิทัลเพื่อรับรองข้อมูลที่ผู้ใช้ให้ไว้
เมื่อทำงานไม่สำเร็จ	ระบบไม่ออกใบรับของดิจิทัล
ผู้ใช้ที่เกี่ยวข้อง	ผู้ใช้ทั่วไป (User)
ข้อมูลเข้า	URL จากอีเมล ซึ่งประกอบด้วย รหัสผู้ใช้ที่ถูกเข้ารหัส และรหัสคำร้องขอ
ข้อมูลออก	แสดงข้อความแจ้งการสร้างใบรับรองดิจิทัลตามคำร้องขอ



รูปที่ 4.6 ซีเควนซ์ไดอะแกรมของยูสเคส Activate Request กรณียืนยันการขอใบรับรอง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

DC.ปี <Date> ปีที่เกี่ยวข้องกับเหตุการณ์ในวงจรชีวิตของทรัพยากรสารสนเทศ

โดยทั่วไป ข้อมูลปีจะสัมพันธ์กับการสร้างสรรค์และเผยแพร่ทรัพยากรสารสนเทศ ข้อแนะนำวิธีปฏิบัติที่ดีที่สุด คือเขียนตามแบบแผน ISO 8601 นั่นคือ ปี-เดือน-วัน YYYY-MM-DD

DC.ประเภท <Type> ธรรมชาติหรือชนิดของเนื้อหาของทรัพยากรสารสนเทศ

ประเภทหมายถึงคำที่อธิบายหมวดวิชา ภาระหน้าที่ ชนิด หรือ ลำดับชั้น ข้อเสนอวิธีปฏิบัติที่ดีที่สุด คือให้เลือกใช้ศัพท์ควบคุม ตัวอย่าง เช่น รายการที่ระบุในคู่มือปฏิบัติสำหรับดับลินคอร์ฉบับร่าง ส่วนการอธิบายลักษณะรูปร่างของทรัพยากรสารสนเทศให้ใช้ส่วนคำย่อย รูปแบบ

DC.รูปแบบ<Format> การอธิบายลักษณะ รูปร่างของทรัพยากรสารสนเทศเชิงกายภาพและดิจิทัล

โดยทั่วไป รูปแบบอาจรวมประเภทของสื่อหรือมิติของทรัพยากร รูปแบบอาจใช้บอกว่าเป็นซอฟต์แวร์หรืออุปกรณ์ที่ต้องใช้ในการแสดงผลหรือเพื่อปฏิบัติการ

DC.รหัส <Identifier> การอ้างอิงถึงทรัพยากรสารสนเทศในรูปแบบปัจจุบัน

ข้อเสนอวิธีปฏิบัติที่ดีที่สุด คือให้ระบุทรัพยากร โดยใช้สายอักขระหรือตัวเลข ตามแบบแผนการกำหนดรหัสประจำตัว ตัวอย่าง ระบบรหัสเลขประจำตัว เช่น URI, URL, DOI, ISBN

DC.ต้นฉบับ <Source> การอ้างอิงถึงที่มาของทรัพยากรสารสนเทศ

ทรัพยากรสารสนเทศฉบับปัจจุบันอาจดัดแปลงบางส่วนหรือทั้งเรื่อง ข้อเสนอวิธีปฏิบัติที่ดีที่สุดคือให้ระบุทรัพยากร โดยใช้สายอักขระหรือตัวเลขตามแบบแผนการกำหนดรหัสประจำตัว

DC.ภาษา <Language> ภาษาที่ใช้ในการเรียบเรียงสารสนเทศ

ข้อเสนอวิธีปฏิบัติที่ดีที่สุดสำหรับข้อความในส่วนคำย่อย ภาษาใช้ตามแบบ RFC 1766 คือใช้รหัสพยัญชนะ 2 ตัวอักษร (ISO 639) ตามด้วยรหัสประเทศ 2 ตัวอักษร (ISO 3166) ตัวอย่าง 'en-uk' สำหรับภาษาอังกฤษที่ใช้ในประเทศอังกฤษ

DC.เรื่องที่เกี่ยวข้อง <Relation> การอ้างอิงถึงทรัพยากรสารสนเทศที่เกี่ยวข้อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

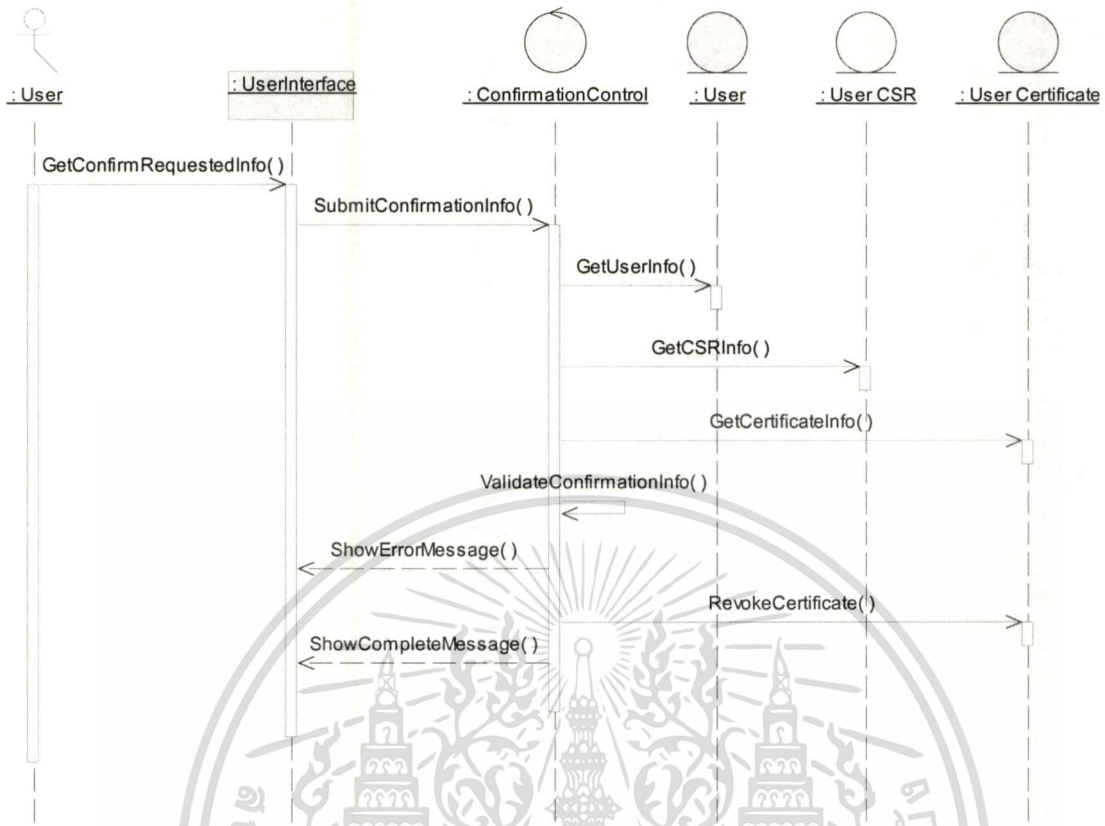
จากรูปที่ 4.6 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Activate Request ในกรณีการร้องขอใบรับรองซึ่งมีลำดับการทำงาน ดังนี้

1. ผู้ใช้เข้าสู่หน้าต่างการยืนยันการร้องขอใบรับรอง โดยใช้ URL จากอีเมลที่ระบบส่งให้
2. ข้อมูลถูกส่งเข้าสู่ระบบ
3. ระบบเรียกดูข้อมูลผู้ใช้
4. ระบบเรียกดูข้อมูลการคำร้องขอใบรับรองดิจิทัล
5. ระบบทำการตรวจสอบข้อมูลผู้ใช้ และคำร้องขอที่ได้รับจาก URL
6. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ใช้ไม่ถูกต้อง หรือไม่พบข้อมูลการร้องขอใบรับรองดิจิทัล หรือสถานะของคำร้องขอใบรับรองดิจิทัลไม่ถูกต้อง
7. ระบบทำการสร้างใบรับรองดิจิทัลสำหรับคำร้องขอนั้นๆ
8. แสดงข้อความแจ้งการสร้างใบรับรองดิจิทัลตามคำร้องขอ

ตารางที่ 4.5 อธิบายยูสเคส Activate Request ในกรณียืนยันการยกเลิกใบรับรอง

ยูสเคส	Activate Request
วัตถุประสงค์	ยืนยันการขอยกเลิกใบรับรองที่ระบบออกให้
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ใช้ที่ได้รับอีเมลเพื่อยืนยันการขอยกเลิกใบรับรองที่ระบบออกให้และได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบทำการยกเลิกยกเลิกใบรับรองดิจิทัลที่ผู้ใช้ระบุ
เมื่อทำงานไม่สำเร็จ	ระบบไม่ทำการยกเลิกใบรับของดิจิทัลที่ผู้ใช้ระบุ
ผู้ใช้ที่เกี่ยวข้อง	ผู้ใช้ทั่วไป (User)
ข้อมูลเข้า	URL จากอีเมล ซึ่งประกอบด้วย รหัสผู้ใช้ที่ถูกเข้ารหัส และรหัสคำร้องขอ
ข้อมูลออก	แสดงข้อความการยกเลิกใบรับรองดิจิทัลจากระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.7 ซีเควนซ์ไดอะแกรมของยูสเคส Activate Request กรณี ยืนยันการยกเลิกใบรับรอง

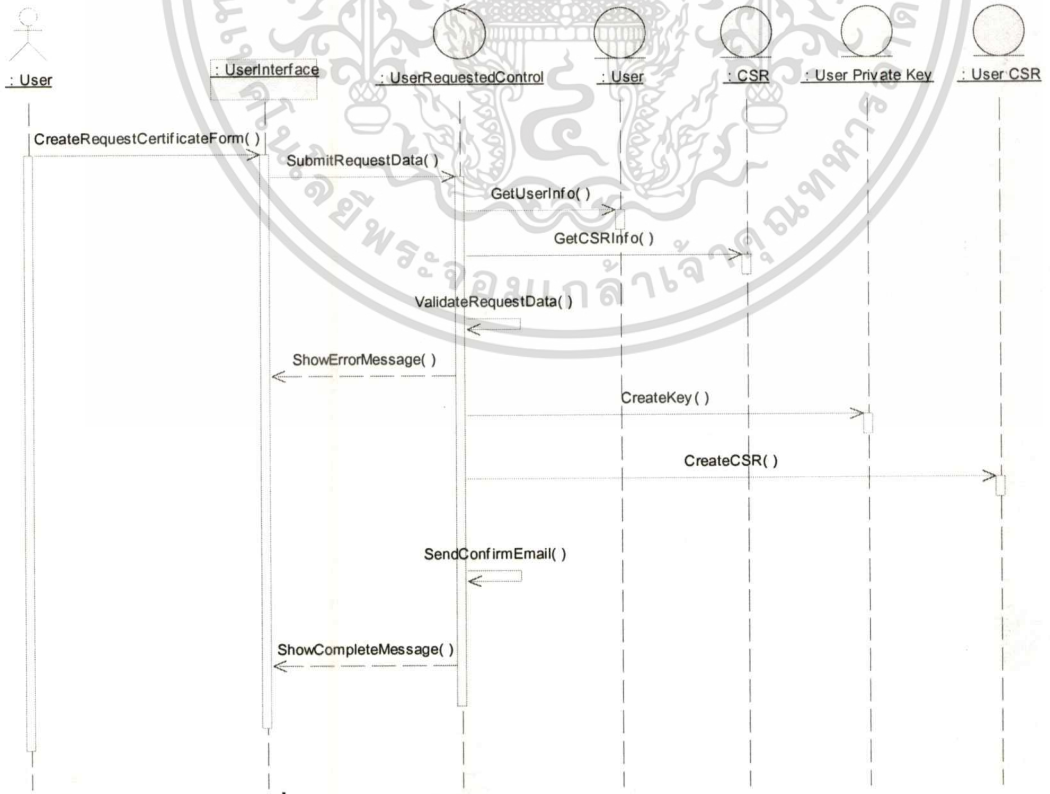
จากรูปที่ 4.7 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Activate Request ในกรณีการยกเลิกใบรับรองซึ่งมีลำดับการทำงาน ดังนี้

1. ผู้ใช้เข้าสู่หน้าต่างการยืนยันการขอยกเลิกใบรับรอง โดยใช้ URL จากอีเมลที่ระบบส่งให้
2. ข้อมูลถูกส่งเข้าสู่ระบบ
3. ระบบเรียกดูข้อมูลผู้ใช้
4. ระบบเรียกดูข้อมูลคำร้องขอใบรับรองดิจิทัล
5. ระบบเรียกดูข้อมูลใบรับรองดิจิทัล
6. ระบบทำการตรวจสอบข้อมูลผู้ใช้ และคำร้องขอที่ได้รับจาก URL
7. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ใช้ไม่ถูกต้อง หรือไม่พบข้อมูลการขอใบรับรองดิจิทัล หรือสถานะของคำร้องขอใบรับรองดิจิทัลไม่ถูกต้อง
8. ระบบทำการยกเลิกใบรับรองดิจิทัลสำหรับคำร้องขอนั้นๆ
9. แสดงข้อความแจ้งการยกเลิกใบรับรองดิจิทัลตามคำร้องขอ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.6 อธิบายยูสเคส Create CSR

ยูสเคส	Create CSR
วัตถุประสงค์	เพื่อสร้างคำร้องขอใบรับรองดิจิทัลจากระบบ
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ใช้ที่ได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบสร้างไฟล์ Private Key (.key) และ Certificate Signing Request (.csr) พร้อมทั้งจัดส่งอีเมลเพื่อยืนยันการร้องขอใบรับรองดิจิทัลให้แก่ผู้ใช้ (จัดส่งไปยังอีเมลที่ระบุในใบรับรองดิจิทัลที่ร้องขอ)
เมื่อทำงานไม่สำเร็จ	ระบบไม่สร้างไฟล์ Private Key (.key) และ Certificate Signing Request (.csr)
ผู้ใช้ที่เกี่ยวข้อง	ผู้ใช้ทั่วไป (User)
ข้อมูลเข้า	ข้อมูลที่ต้องการระบุในใบรับรองดิจิทัล ได้แก่ ประเทศ, รัฐ หรือ จังหวัด, อำเภอ หรือ เขต, ชื่อองค์กร, ชื่อหน่วยงาน, อีเมล และรหัสลับสำหรับใช้ในการสร้างกุญแจส่วนตัว (Private Key)
ข้อมูลออก	ระบบแสดงข้อความการรับคำร้องขอใบรับรองดิจิทัลเรียบร้อย และแจ้งให้ผู้ใช้ทำการยืนยันการร้องขอใบรับรองดิจิทัลจากอีเมลที่ระบบจัดส่งให้



รูปที่ 4.8 ซีเควนซ์ไดอะแกรมของยูสเคส Create CSR

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

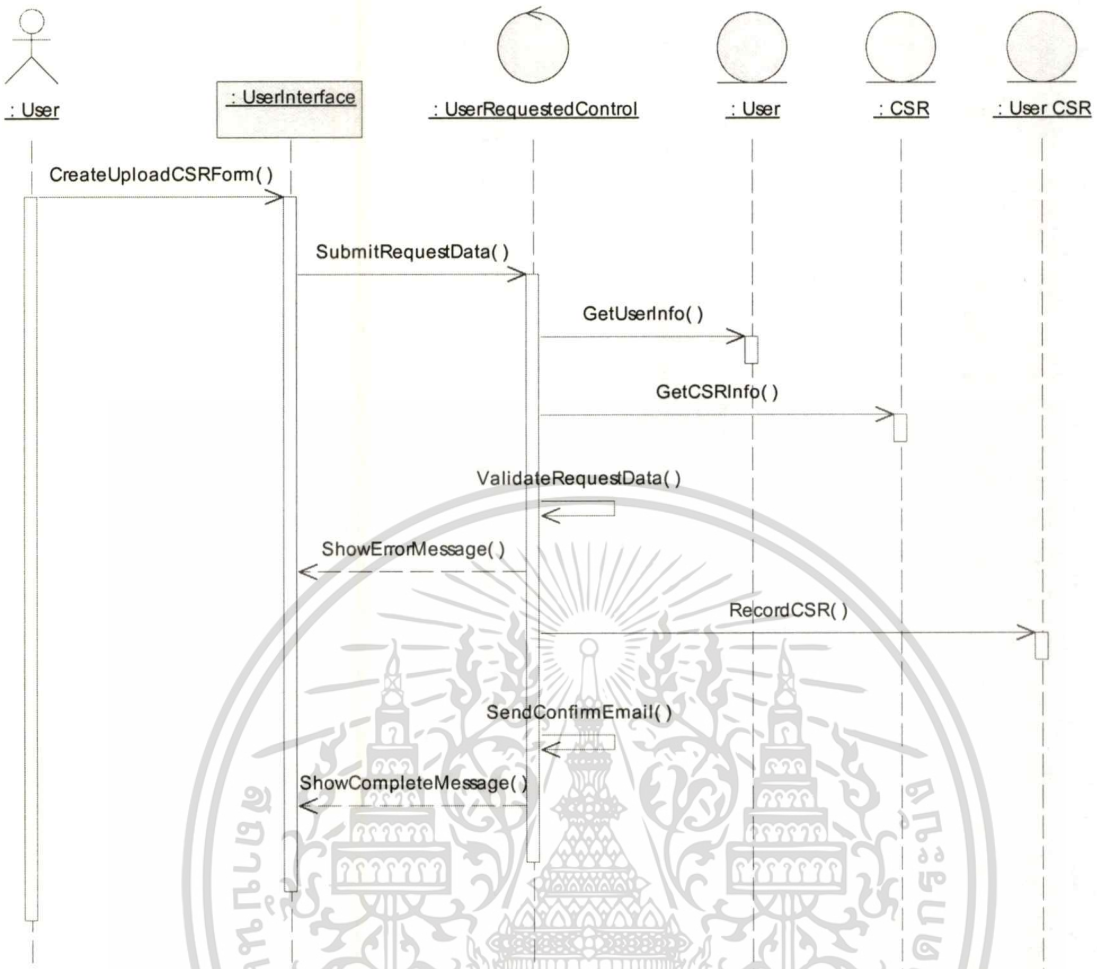
จากรูปที่ 4.8 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Create CSR ซึ่งมีลำดับการทำงาน ดังนี้

1. ผู้ใช้เข้าสู่หน้าต่างการร้องขอใบรับรองดิจิทัล
2. ผู้ใช้ป้อนข้อมูลต่างๆ ที่ต้องการใช้ในการสร้างใบรับรองดิจิทัล
3. ระบบเรียกดูข้อมูลผู้ใช้
4. ระบบเรียกดูข้อมูลคำร้องขอใบรับรองดิจิทัลที่มีอยู่
5. ระบบทำการตรวจสอบข้อมูลผู้ใช้ และอีเมลที่ทำการร้องขอใบรับรองดิจิทัล
6. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ใช้ไม่ถูกต้อง หรืออีเมลที่ทำการร้องขอใบรับรองดิจิทัลเป็นอีเมลที่มีใบรับรองดิจิทัลที่มีการใช้งานอยู่
7. ระบบสร้างกุญแจส่วนตัว (Private Key)
8. ระบบสร้างคำร้องขอใบรับรองดิจิทัล (Certificate Signing Request)
9. ระบบจัดส่งอีเมลสำหรับยืนยันการขอใบรับรองดิจิทัลให้ผู้รับ
10. แสดงข้อความแจ้งการจบขั้นตอนการขอใบรับรองดิจิทัลเรียบร้อย และแจ้งให้ผู้ใช้ทำการยืนยันการร้องขอใบรับรองดิจิทัลจากอีเมลที่ระบบจัดส่งให้

ตารางที่ 4.7 อธิบายยูสเคส Upload CSR

ยูสเคส	Upload CSR
วัตถุประสงค์	เพื่ออัพโหลดไฟล์การร้องขอใบรับรองดิจิทัลจากผู้ใช้
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ใช้ที่ได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบสร้างไฟล์ Certificate Signing Request (.csr) พร้อมทั้งจัดส่งอีเมลเพื่อยืนยันการร้องขอใบรับรองดิจิทัลให้แก่ผู้ใช้ (จัดส่งไปยังอีเมลที่ระบุในใบรับรองดิจิทัลที่ร้องขอ)
เมื่อทำงานไม่สำเร็จ	ระบบไม่สร้างไฟล์ Certificate Signing Request (.csr)
ผู้ใช้ที่เกี่ยวข้อง	ผู้ใช้ทั่วไป (User)
ข้อมูลเข้า	คำร้องขอที่ถูกเข้ารหัสไว้
ข้อมูลออก	ระบบแสดงข้อความการรับคำร้องขอใบรับรองดิจิทัลเรียบร้อย และแจ้งให้ผู้ใช้ทำการยืนยันการร้องขอใบรับรองดิจิทัลจากอีเมลที่ระบบจัดส่งให้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.9 ซีเควนซ์ไดอะแกรมของยูสเคส Upload CSR

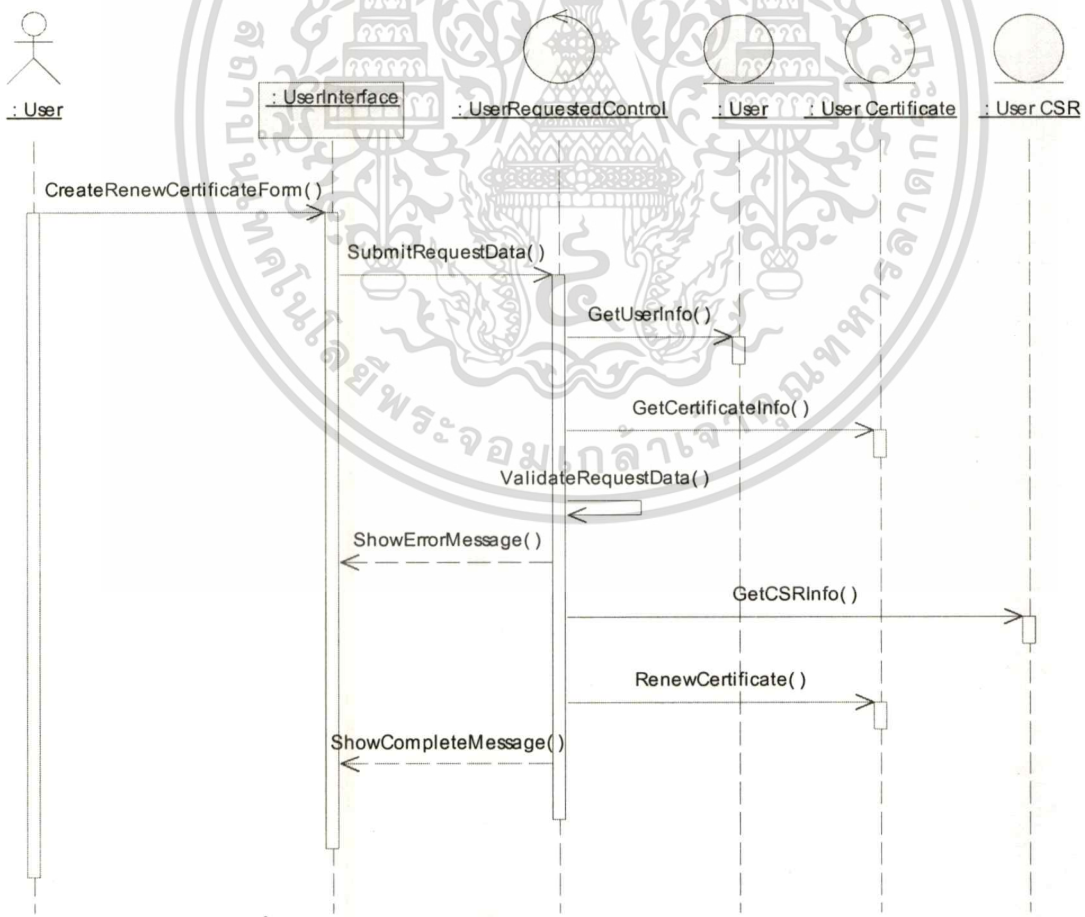
จากรูปที่ 4.9 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Upload CSR ซึ่งมีลำดับการทำงาน ดังนี้

1. ผู้ใช้เข้าสู่หน้าต่างการอัพโหลดคำร้องขอใบรับรองดิจิทัล
2. ผู้ใช้ป้อนคำร้องขอใบรับรองดิจิตัลที่ถูกเข้ารหัสแล้ว
3. ระบบเรียกดูข้อมูลผู้ใช้
4. ระบบเรียกดูข้อมูลคำร้องขอใบรับรองดิจิทัลที่มีอยู่
5. ระบบทำการตรวจสอบข้อมูลผู้ใช้ และอีเมลที่ทำการร้องขอใบรับรองดิจิทัล
6. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ใช้ไม่ถูกต้อง หรืออีเมลที่ทำการร้องขอใบรับรองดิจิทัลเป็นอีเมลที่มีใบรับรองดิจิทัลที่มีการใช้งานอยู่
7. ระบบสร้างคำร้องขอใบรับรองดิจิทัล (Certificate Signing Request)
8. ระบบจัดส่งอีเมลสำหรับยืนยันการขอใบรับรองดิจิทัลให้ผู้รับ
9. แสดงข้อความแจ้งการจบขั้นตอนการขอใบรับรองดิจิทัลเรียบร้อย และแจ้งให้ผู้ใช้ทำการยืนยันการร้องขอใบรับรองดิจิทัลจากอีเมลที่ระบบจัดส่งให้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.8 อธิบายยูสเคส Request Renew

ยูสเคส	Request Renew
วัตถุประสงค์	การขอใบรับรองดิจิทัลใบใหม่เพื่อใช้แทนใบเก่าที่หมดอายุ หรือใกล้หมดอายุ
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ใช้ที่ได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบออกใบรับรองดิจิทัลใบใหม่เพื่อใช้แทนใบเก่าที่หมดอายุ หรือใกล้หมดอายุ
เมื่อทำงานไม่สำเร็จ	ระบบไม่ออกใบรับรองดิจิทัลใบใหม่ให้ผู้ใช้
ผู้ใช้ที่เกี่ยวข้อง	ผู้ใช้ทั่วไป (User)
ข้อมูลเข้า	รหัสลับ (Passphrase) ของกุญแจส่วนตัวที่เป็นคู่กับใบรับรองดิจิทัลที่ต้องการขอ
ข้อมูลออก	ระบบแสดงข้อความจบขั้นตอนการขอใบรับรองดิจิทัลแทนใบเก่า



รูปที่ 4.10 ซีเควนซ์ไดอะแกรมของยูสเคส Request Renew

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

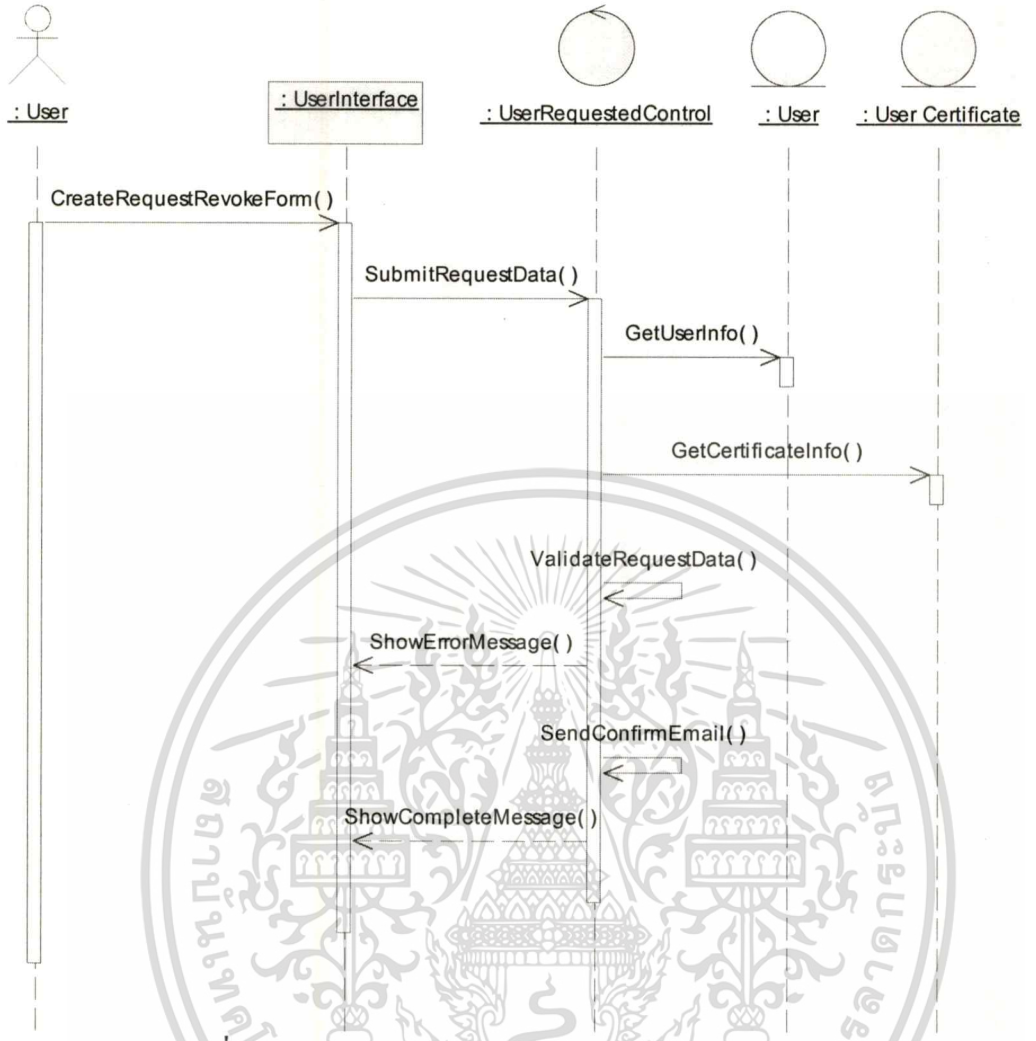
จากรูปที่ 4.10 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Request Renew ซึ่งมีลำดับการทำงานดังนี้

1. ผู้ใช้เข้าสู่หน้าต่างการขอใบรับรองดิจิทัลแทนใบเก่า
2. ผู้ใช้ป้อนรหัสลับ (Passphrase) ของกุญแจส่วนตัวที่เป็นคู่กับใบรับรองดิจิทัลที่ขอ
3. ระบบเรียกดูข้อมูลผู้ใช้
4. ระบบเรียกดูข้อมูลใบรับรองดิจิทัลที่ขอใบใหม่แทน
5. ระบบทำการตรวจสอบข้อมูลผู้ใช้ และข้อมูลใบรับรองดิจิทัลที่ขอใบใหม่แทน
6. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ใช้ไม่ถูกต้อง หรือสถานะใบรับรองไม่ถูกต้อง หรือ อายุของใบรับรองที่ยังเหลืออยู่เกินกว่าที่ระบบตั้งไว้
7. ระบบเรียกดูข้อมูลคำร้องขอใบรับรองดิจิทัลที่ขอใบใหม่แทน
8. ระบบสร้างใบรับรองดิจิทัลใหม่เพื่อใช้แทนใบเก่า
9. แสดงข้อความแจ้งการจบขั้นตอนการขอใบรับรองดิจิทัลแทนใบเก่า

ตารางที่ 4.9 อธิบายยูสเคส Request Revoke

ยูสเคส	Request Revoke
วัตถุประสงค์	ขอยกเลิกใบรับรองดิจิทัล
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ใช้ที่ได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	จัดส่งอีเมลเพื่อยืนยันการลงทะเบียนให้แก่ผู้ใช้
เมื่อทำงานไม่สำเร็จ	ระบบแสดงข้อความผิดพลาดในการขอยกเลิกใบรับรองดิจิทัล
ผู้ใช้ที่เกี่ยวข้อง	ผู้ใช้ทั่วไป (User)
ข้อมูลเข้า	รหัสผู้ใช้ที่ถูกเข้ารหัส และรหัสคำร้องขอของใบรับรองดิจิทัล
ข้อมูลออก	ระบบแสดงข้อความการรับคำร้องขอยกเลิกใบรับรองดิจิทัล และแจ้งให้ผู้ใช้ทำการยืนยันการขอยกเลิกใบรับรองดิจิทัลจากอีเมลที่ระบบจัดส่งให้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.11 ซีเควนซ์ไดอะแกรมของยูสเคส Request Revoke

จากรูปที่ 4.11 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Request Revoke ซึ่งมีลำดับการทำงานดังนี้

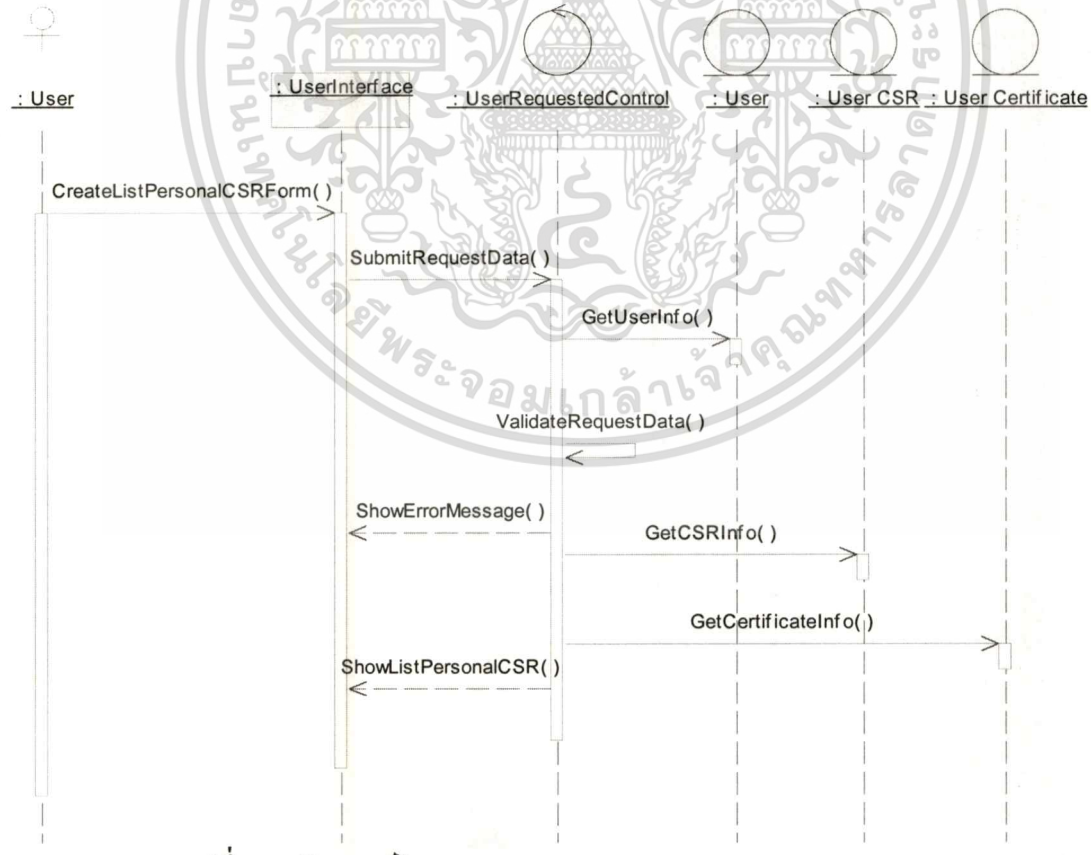
1. ผู้ใช้เข้าสู่หน้าต่างการขอยกเลิกใบรับรองดิจิทัลผ่านเมนู
2. ข้อมูลถูกส่งเข้าสู่ระบบ
3. ระบบเรียกดูข้อมูลผู้ใช้
4. ระบบเรียกดูข้อมูลใบรับรองดิจิทัลที่ขอยกเลิก
5. ระบบทำการตรวจสอบข้อมูลผู้ใช้ และข้อมูลใบรับรองดิจิทัลที่ขอยกเลิก
6. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ใช้ไม่ถูกต้อง หรือสถานะใบรับรองไม่ถูกต้อง
7. ระบบจัดส่งอีเมลสำหรับยืนยันการขอยกเลิกใบรับรองดิจิทัลให้ผู้รับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

8. แสดงข้อความแจ้งการจบขั้นตอนการขอยกเลิกใบรับรองดิจิทัล และแจ้งให้ผู้ใช้ทำการยืนยันการขอยกเลิกใบรับรองดิจิทัลจากอีเมลที่ระบบจัดส่งให้

ตารางที่ 4.10 อธิบายยูสเคส List Personal Request

ยูสเคส	List Personal Request
วัตถุประสงค์	แสดงรายการข้อมูลคำร้องขอที่เกิดจากตัวผู้ใช้เอง รวมถึงข้อมูลใบรับรองดิจิทัลที่ผ่านการยืนยันการร้องขอแล้ว
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ใช้ที่ได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบแสดงรายการข้อมูลคำร้องขอและข้อมูลใบรับรองดิจิทัลของผู้ใช้
เมื่อทำงานไม่สำเร็จ	ระบบแสดงข้อความผิดพลาด
ผู้ใช้ที่เกี่ยวข้อง	ผู้ใช้ทั่วไป (User)
ข้อมูลเข้า	รหัสผู้ใช้
ข้อมูลออก	รายการข้อมูลคำร้องขอและข้อมูลใบรับรองดิจิทัลของผู้ใช้



รูปที่ 4.12 ซีเควนซ์ไดอะแกรมของยูสเคส List Personal Request

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

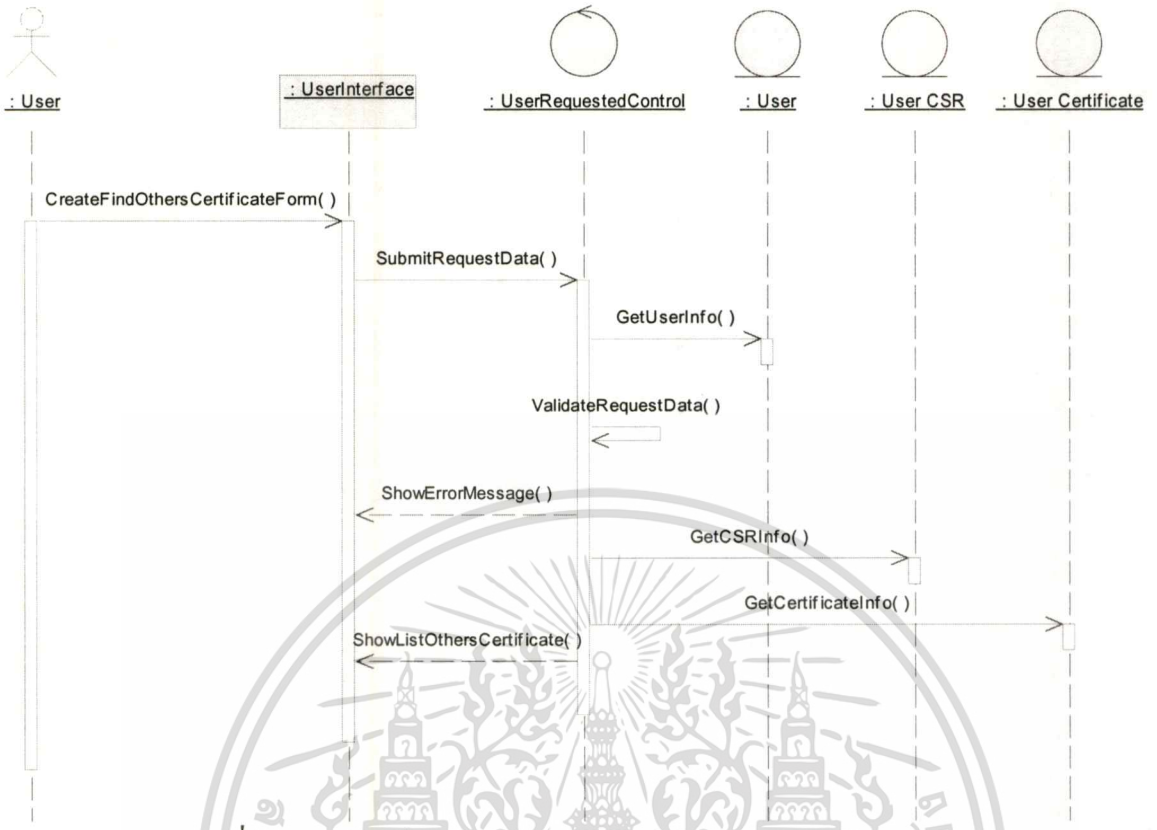
จากรูปที่ 4.12 แสดงซีเควนซ์ไดอะแกรมของยูสเคส List Personal Request ซึ่งมีลำดับการทำงาน ดังนี้

1. ผู้ใช้เข้าสู่หน้าต่างการแสดงข้อมูลคำร้องขอและข้อมูลใบรับรองดิจิทัลของผู้ใช้ผ่านเมนู
2. ข้อมูลถูกส่งเข้าสู่ระบบ
3. ระบบเรียกดูข้อมูลผู้ใช้
4. ระบบทำการตรวจสอบข้อมูลผู้ใช้
5. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ใช้ไม่ถูกต้อง
6. ระบบเรียกดูรายการข้อมูลคำร้องขอใบรับรองดิจิทัลของผู้ใช้
7. ระบบเรียกดูรายการข้อมูลใบรับรองดิจิทัลของผู้ใช้
8. แสดงข้อรายการข้อมูลคำร้องขอใบรับรองดิจิทัลและใบรับรองดิจิทัลของผู้ใช้

ตารางที่ 4.11 อธิบายยูสเคส Find Others Certificate

ยูสเคส	Find Others Certificate
วัตถุประสงค์	ค้นหาและแสดงรายการใบรับรองดิจิทัลของผู้ใช้ทุกรายในระบบ
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ใช้ที่ได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบแสดงรายการข้อมูลใบรับรองดิจิทัลของผู้ใช้ทุกราย
เมื่อทำงานไม่สำเร็จ	ระบบแสดงข้อความผิดพลาด
ผู้ใช้ที่เกี่ยวข้อง	ผู้ใช้ทั่วไป (User)
ข้อมูลเข้า	รหัสผู้ใช้
ข้อมูลออก	แสดงรายการข้อมูลใบรับรองดิจิทัลของผู้ใช้ทุกราย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.13 ซีเควนซ์ไดอะแกรมของยูสเคส Find Others Certificate

จากรูปที่ 4.13 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Find Others Certificate ซึ่งมีลำดับการทำงาน ดังนี้

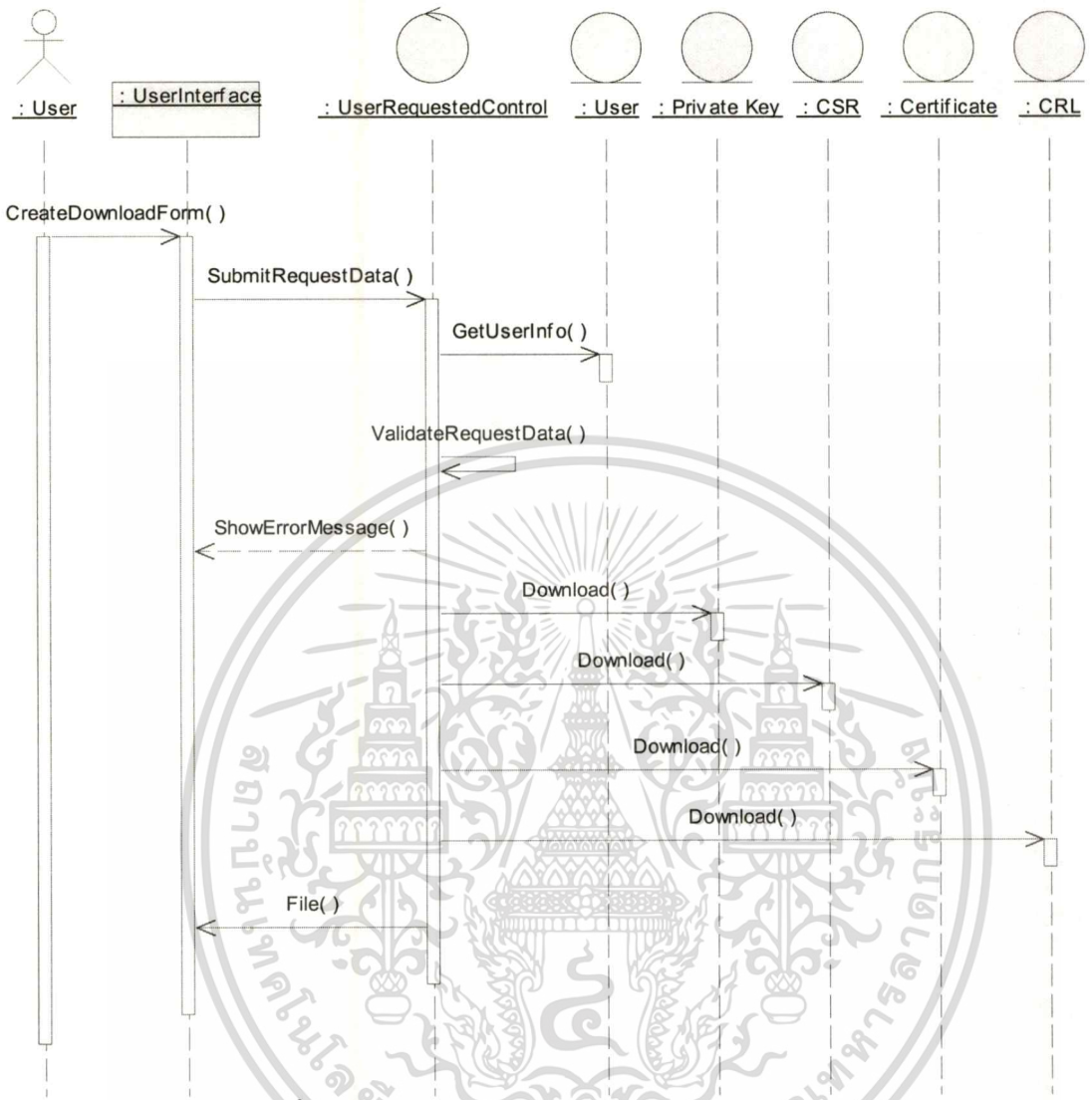
1. ผู้ใช้เข้าสู่หน้าต่างการแสดงข้อมูลคำร้องขอและข้อมูลใบรับรองดิจิทัลของผู้ใช้ผ่านเมนู
2. ข้อมูลถูกส่งเข้าสู่ระบบ
3. ระบบเรียกดูข้อมูลผู้ใช้
4. ระบบทำการตรวจสอบข้อมูลผู้ใช้
5. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ใช้ไม่ถูกต้อง
6. ระบบเรียกดูรายการข้อมูลคำร้องขอใบรับรองดิจิทัลของผู้ใช้ทุกราย
7. ระบบเรียกดูรายการข้อมูลใบรับรองดิจิทัลของผู้ใช้ทุกรายที่มีสถานะยังใช้งาน
8. แสดงข้อรายการข้อมูลคำร้องขอใบรับรองดิจิทัลและใบรับรองดิจิทัลของผู้ใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.12 อธิบายยูสเคส Download

ยูสเคส	Download
วัตถุประสงค์	ดาวน์โหลดไฟล์ต่างๆ เช่น กุญแจส่วนตัว(Private Key) คำร้องขอใบรับรองดิจิทัล(Certificate Signing Request) ใบรับรองดิจิทัล (Certificate) รายการยกเลิกใบรับรอง (Certificate Revoke List)
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ใช้ที่ได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบส่งไฟล์ที่ผู้ใช้ร้องขอ
เมื่อทำงานไม่สำเร็จ	ระบบไม่ส่งไฟล์ที่ผู้ใช้ร้องขอ
ผู้ใช้ที่เกี่ยวข้อง	ผู้ใช้ทั่วไป (User) และ ผู้ดูแลระบบ (Admin)
ข้อมูลเข้า	รหัสผู้ใช้ หรือรหัสผู้ดูแลระบบ และชนิดของไฟล์ข้อมูลที่ร้องขอ
ข้อมูลออก	แสดงหน้าจอสำหรับบันทึกไฟล์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.14 ซีเควนซ์ไดอะแกรมของยูสเคส Download

จากรูปที่ 4.14 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Download ซึ่งมีลำดับการทำงาน ดังนี้

1. ผู้ใช้เข้าสู่หน้าต่างการดาวน์โหลดไฟล์ผ่านเมนู
2. ข้อมูลถูกส่งเข้าสู่ระบบ
3. ระบบเรียกดูข้อมูลผู้ใช้
4. ระบบทำการตรวจสอบข้อมูลผู้ใช้
5. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ใช้ไม่ถูกต้อง
6. ระบบอ่านไฟล์กุญแจส่วนตัว ในกรณีไฟล์ที่ผู้ใช้ร้องขอเป็นไฟล์กุญแจส่วนตัว
7. ระบบอ่านไฟล์คำร้องขอใบรับรองดิจิทัล ในกรณีไฟล์ที่ผู้ใช้ร้องขอเป็นไฟล์คำร้องขอใบรับรองดิจิทัล

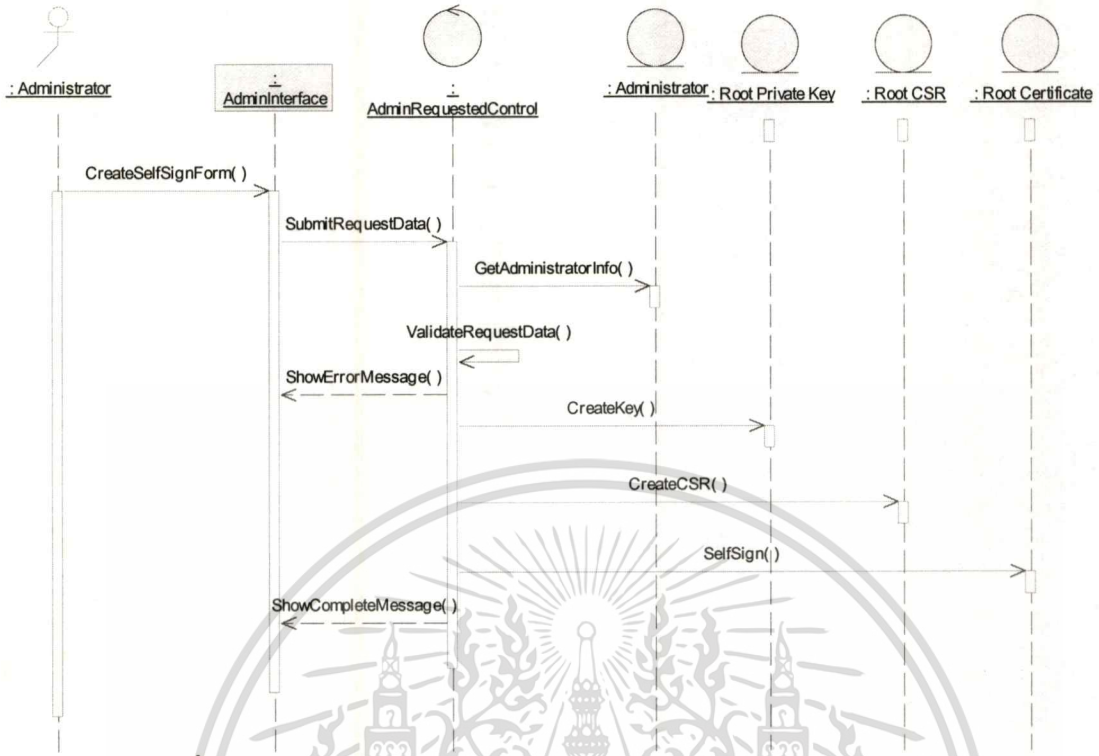
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

8. ระบบอ่านไฟล์ใบรับรองดิจิทัล ในกรณีไฟล์ที่ผู้ใช้ร้องขอเป็นไฟล์ใบรับรองดิจิทัล
9. ระบบอ่านไฟล์รายการใบรับรองดิจิทัลที่ถูกยกเลิก ในกรณีไฟล์ที่ผู้ใช้ร้องขอเป็นไฟล์รายการใบรับรองดิจิทัลที่ถูกยกเลิก
10. ระบบส่งไฟล์ให้แก่ผู้ใช้

ตารางที่ 4.13 อธิบายยูสเคส Self Sign Admin Certificate

ยูสเคส	Self Sign Admin Certificate
วัตถุประสงค์	ตรวจสอบสิทธิในการเข้าใช้งานระบบ
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ดูแลระบบที่ได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบสร้างไฟล์ Private Key (.key) ไฟล์ Certificate Signing Request (.csr) และไฟล์ Certificate (.crt)
เมื่อทำงานไม่สำเร็จ	ระบบไม่มีการสร้างไฟล์ใดๆ
ผู้ใช้ที่เกี่ยวข้อง	ผู้ดูแลระบบ (Admin)
ข้อมูลเข้า	ข้อมูลที่ต้องการระบุในใบรับรองดิจิทัล ได้แก่ ประเทศ จังหวัด เขต ชื่อองค์กร ชื่อหน่วยงาน ชื่อเว็บไซต์ อีเมล และรหัสลับสำหรับใช้ในการสร้างกุญแจส่วนตัว (Private Key)
ข้อมูลออก	ระบบแสดงข้อความจบขั้นตอนการ Self Sign

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.15 ซีเควนซ์ไดอะแกรมของยูสเคส Self Sign Admin Certificate

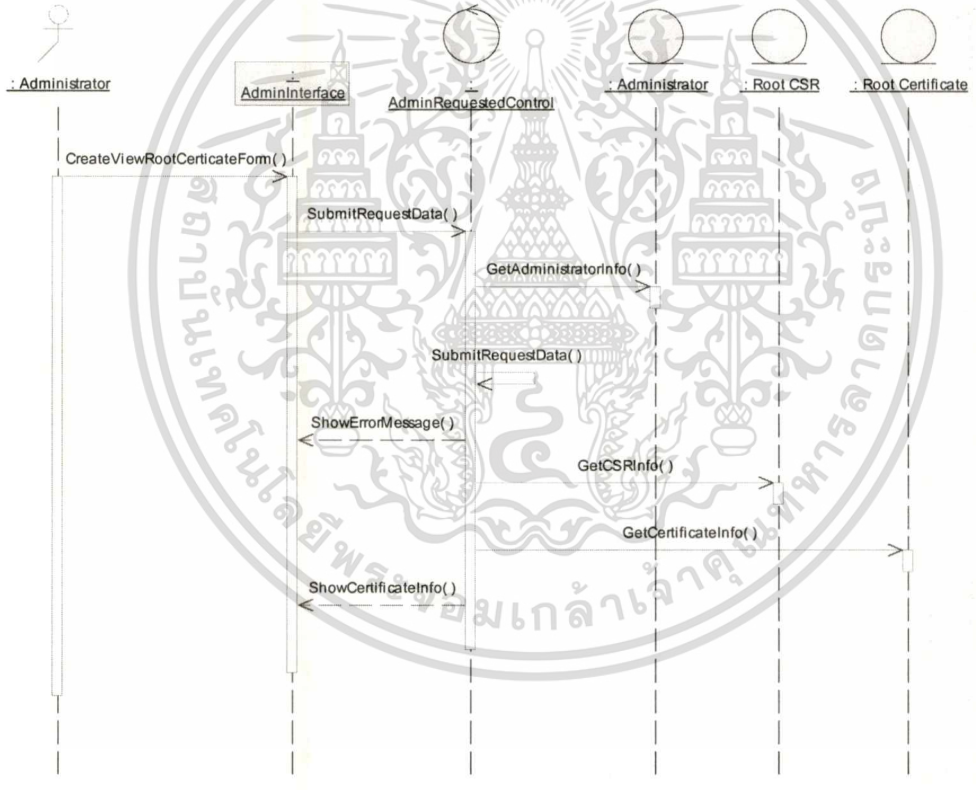
จากรูปที่ 4.15 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Self Sign Admin Certificate ซึ่งมีลำดับการทำงาน ดังนี้

1. ผู้ดูแลระบบเข้าสู่หน้าต่างการ Self Sign
2. ผู้ดูแลระบบป้อนข้อมูลต่างๆ ที่ต้องการใช้ในการสร้างใบรับรองดิจิทัล
3. ระบบเรียกดูข้อมูลผู้ดูแลระบบ
4. ระบบทำการตรวจสอบข้อมูลผู้ดูแลระบบ
5. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ดูแลระบบไม่ถูกต้อง
6. ระบบสร้างกุญแจส่วนตัว (Private Key)
7. ระบบสร้างคำร้องขอใบรับรองดิจิทัล (Certificate Signing Request)
8. ระบบสร้างใบรับรองดิจิทัล (Certificate)
9. แสดงข้อความจบขั้นตอนการ Self Sign

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.14 อธิบายยูสเคส View Admin Certificate

ยูสเคส	View Admin Certificate
วัตถุประสงค์	แสดงข้อมูลใบรับรองดิจิทัลของ CA
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ดูแลระบบที่ได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบแสดงข้อมูลใบรับรองดิจิทัลของ CA
เมื่อทำงานไม่สำเร็จ	ระบบแสดงข้อความผิดพลาด
ผู้ใช้ที่เกี่ยวข้อง	ผู้ดูแลระบบ (Admin)
ข้อมูลเข้า	รหัสผู้ดูแลระบบ
ข้อมูลออก	แสดงข้อมูลใบรับรองดิจิทัลของ CA



รูปที่ 4.16 ซีเควนซ์ไดอะแกรมของยูสเคส View Admin Certificate

จากรูปที่ 4.16 แสดงซีเควนซ์ไดอะแกรมของยูสเคส View Admin Certificate ซึ่งมีลำดับการทำงาน ดังนี้

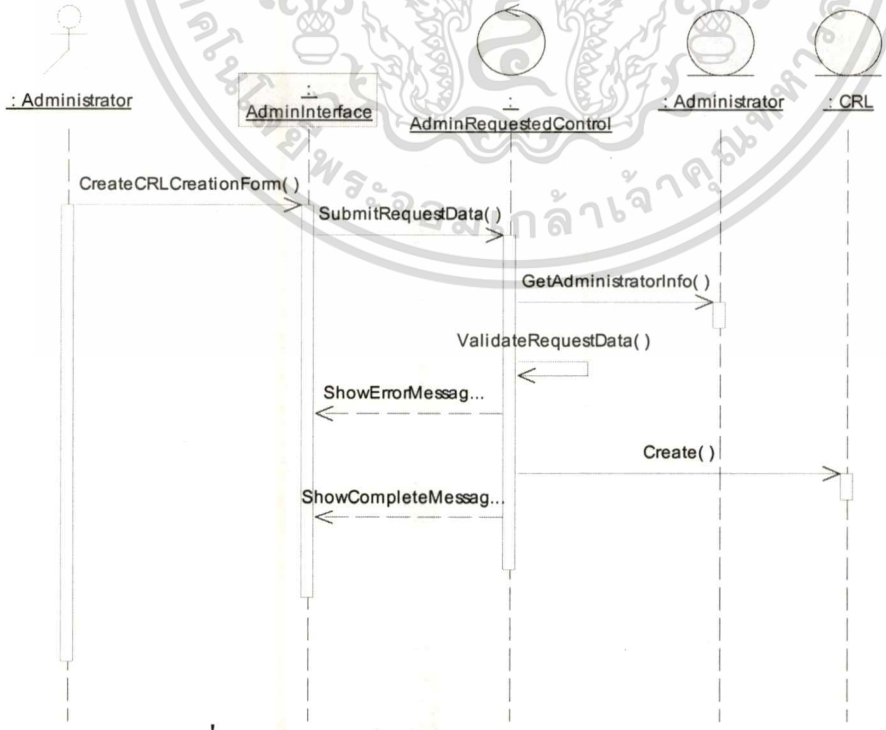
1. ผู้ดูแลระบบเข้าสู่หน้าต่างการแสดงข้อมูลใบรับรองดิจิทัลของ CA ผ่านเมนู
2. ข้อมูลถูกส่งเข้าสู่ระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. ระบบเรียกดูข้อมูลผู้ดูแลระบบ
4. ระบบทำการตรวจสอบข้อมูลผู้ดูแลระบบ
5. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ดูแลระบบไม่ถูกต้อง
6. ระบบเรียกดูข้อมูลคำร้องขอใบรับรองดิจิทัลของ CA
7. ระบบเรียกดูข้อมูลใบรับรองดิจิทัลของ CA
8. แสดงข้อความลำดับการทำงานใบรับรองดิจิทัลของ CA

ตารางที่ 4.15 อธิบายยูสเคส Create CRL

ยูสเคส	Create CRL
วัตถุประสงค์	สร้างไฟล์รายการใบรับรองดิจิทัลที่ถูกยกเลิก
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ดูแลระบบที่ได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบสร้างไฟล์รายการใบรับรองดิจิทัลที่ถูกยกเลิก
เมื่อทำงานไม่สำเร็จ	ระบบไม่สร้างไฟล์ใดๆ
ผู้ใช้ที่เกี่ยวข้อง	ผู้ดูแลระบบ (Admin)
ข้อมูลเข้า	รหัสผู้ดูแลระบบ
ข้อมูลออก	แสดงข้อความเสร็จสิ้นการสร้างไฟล์รายการใบรับรองดิจิทัลที่ถูกยกเลิก



รูปที่ 4.17 ซีเควนซ์ไดอะแกรมของยูสเคส Create CRL

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

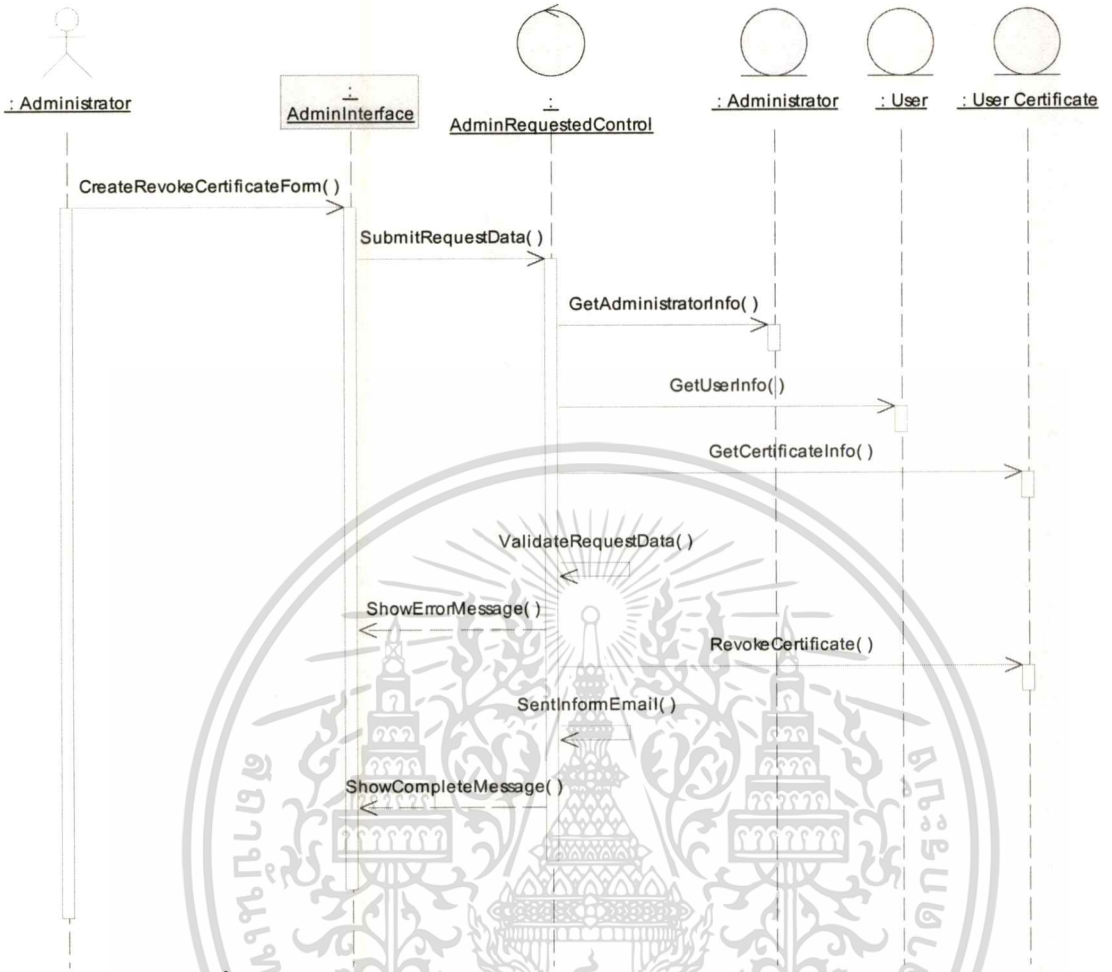
จากรูปที่ 4.17 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Create CRL ซึ่งมีลำดับการทำงานดังนี้

1. ผู้ดูแลระบบเข้าสู่หน้าต่างการสร้างไฟล์รายการใบรับรองดิจิทัลที่ถูกยกเลิกผ่านเมนู
2. ข้อมูลถูกส่งเข้าสู่ระบบ
3. ระบบเรียกดูข้อมูลผู้ดูแลระบบ
4. ระบบทำการตรวจสอบข้อมูลผู้ดูแลระบบ
5. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ดูแลระบบไม่ถูกต้อง
6. ระบบสร้างไฟล์รายการใบรับรองดิจิทัลที่ถูกยกเลิก
7. แสดงข้อความเสร็จสิ้นการสร้างไฟล์รายการใบรับรองดิจิทัลที่ถูกยกเลิก

ตารางที่ 4.16 อธิบายยูสเคส Revoke User Certificate

ยูสเคส	Revoke User Certificate
วัตถุประสงค์	ยกเลิกใบรับรองดิจิทัลของผู้ใช้
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ดูแลระบบที่ได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบยกเลิกใบรับรองดิจิทัลของผู้ใช้ พร้อมอีเมลแจ้งการถูกยกเลิกใบรับรองดิจิทัลของผู้ใช้
เมื่อทำงานไม่สำเร็จ	ระบบไม่ทำการยกเลิกใบรับรองดิจิทัลของผู้ใช้
ผู้ใช้ที่เกี่ยวข้อง	ผู้ดูแลระบบ (Admin)
ข้อมูลเข้า	รหัสผู้ดูแลระบบ รหัสผู้ใช้ และรหัสคำร้องของขอใบรรับรองดิจิทัลที่ต้องการยกเลิก
ข้อมูลออก	แสดงหน้าจอเสร็จสิ้นการยกเลิกใบรับรองดิจิทัล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.18 ซีเควนซ์ไดอะแกรมของยูสเคส Revoke User Certificate

จากรูปที่ 4.18 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Revoke User Certificate ซึ่งมีลำดับการทำงาน ดังนี้

1. ผู้ดูแลระบบเข้าสู่หน้าต่างการยกเลิกใบรับรองดิจิทัลของผู้ใช้ผ่านเมนู
2. ข้อมูลถูกส่งเข้าสู่ระบบ
3. ระบบเรียกดูข้อมูลผู้ดูแลระบบ
4. ระบบเรียกดูข้อมูลผู้ใช้
5. ระบบเรียกดูข้อมูลใบรับรองดิจิทัลของผู้ใช้ที่จะยกเลิก
6. ระบบทำการตรวจสอบข้อมูลผู้ดูแลระบบ ข้อมูลผู้ใช้ และข้อมูลใบรับรองดิจิทัลที่จะยกเลิก
7. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ดูแลระบบไม่ถูกต้อง หรือข้อมูลของผู้ใช้ไม่ถูกต้อง หรือสถานะใบรับรองไม่ถูกต้อง

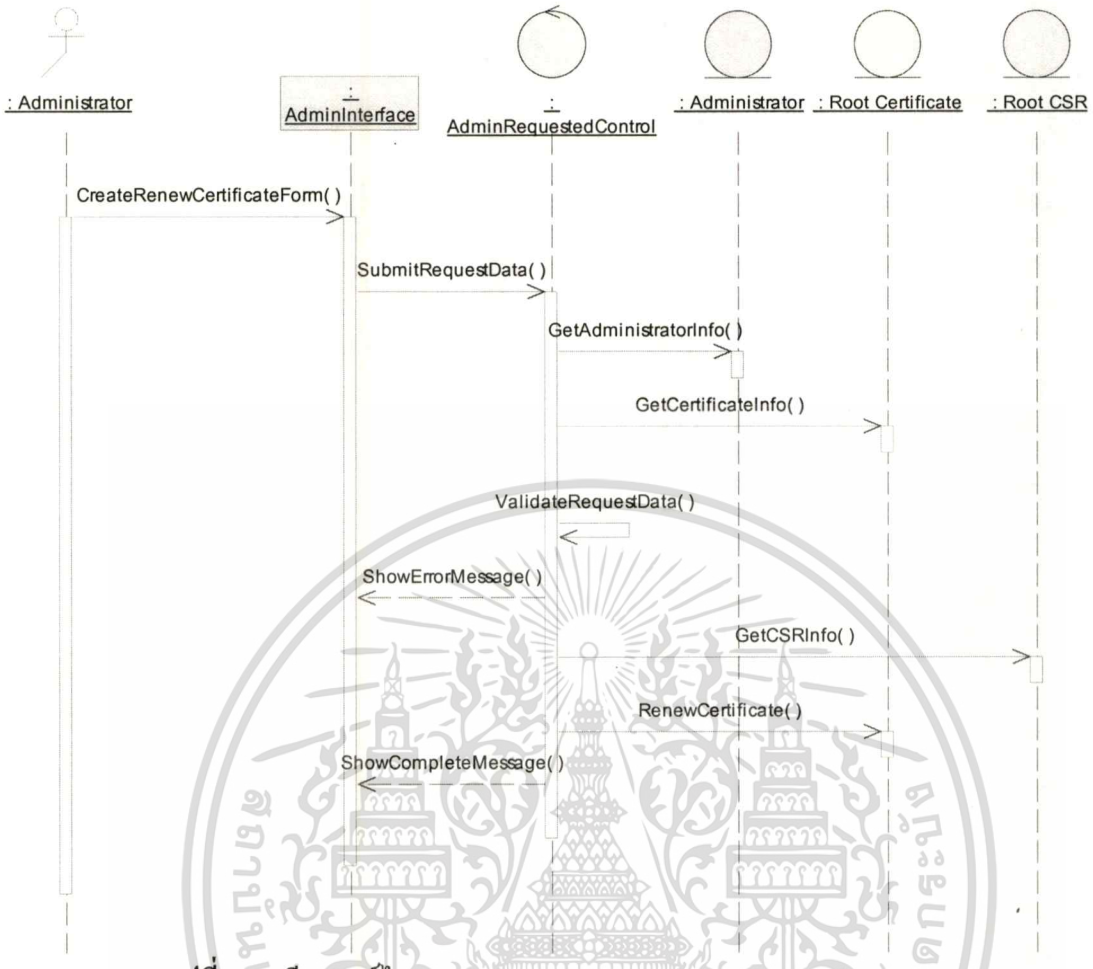
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

8. ระบบทำการยกเลิกใบรับรองดิจิทัลของผู้ใช้
9. ระบบจัดส่งอีเมลแจ้งการถูกยกเลิกใบรับรองดิจิทัลให้ผู้รับ
10. แสดงข้อความเสร็จสิ้นการยกเลิกใบรับรอง

ตารางที่ 4.17 อธิบายยูสเคส Renew Admin Certificate ในกรณียืนยันการลงทะเบียนผู้ใช้

ยูสเคส	Renew Admin Certificate
วัตถุประสงค์	ออกใบรับรองดิจิทัลของ CA เพื่อใช้แทนใบเก่าที่หมดอายุ หรือใกล้หมดอายุ
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ดูแลระบบที่ได้ทำการล็อคอินแล้ว
เมื่อทำงานสำเร็จ	ระบบสร้างใบรับรองดิจิทัลของ CA ใบใหม่
เมื่อทำงานไม่สำเร็จ	ระบบไม่สร้างใบรับรองดิจิทัลของ CA ใบใหม่
ผู้ใช้ที่เกี่ยวข้อง	ผู้ดูแลระบบ (Admin)
ข้อมูลเข้า	รหัสผู้ดูแลระบบ รหัสลับ (Passphrase) ของกุญแจส่วนตัวที่เป็นคู่กับใบรับรองดิจิทัลของ CA
ข้อมูลออก	แสดงข้อความเสร็จสิ้นการสร้างใบรับรองดิจิทัลของ CA ใบใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.19 ซีเควนซ์ไดอะแกรมของยูสเคส Renew Admin Certificate

จากรูปที่ 4.19 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Renew Admin Certificate ซึ่งมีลำดับการทำงานดังนี้

1. ผู้ดูแลระบบเข้าสู่หน้าต่างการขอใบรับรองดิจิทัลแทนใบเก่า
2. ผู้ดูแลระบบป้อนรหัสลับ (Passphrase) ของกุญแจส่วนตัวที่เป็นคู่กับใบรับรองดิจิตัลของ CA
3. ระบบเรียกดูข้อมูลผู้ดูแลระบบ
4. ระบบเรียกดูข้อมูลใบรับรองดิจิทัลที่ขอใบใหม่แทน
5. ระบบทำการตรวจสอบข้อมูลผู้ดูแลระบบ และรหัสลับ
6. แสดงข้อความผิดพลาด ในกรณีข้อมูลของผู้ดูแลระบบไม่ถูกต้อง หรือสถานะใบรับรองไม่ถูกต้อง หรือ อายุของใบรับรองที่ยังเหลืออยู่เกินกว่าที่ระบบตั้งไว้
7. ระบบเรียกดูข้อมูลคำร้องขอใบรับรองดิจิทัลที่ขอใบใหม่แทน
8. ระบบสร้างใบรับรองดิจิทัลใหม่เพื่อใช้แทนใบเก่า

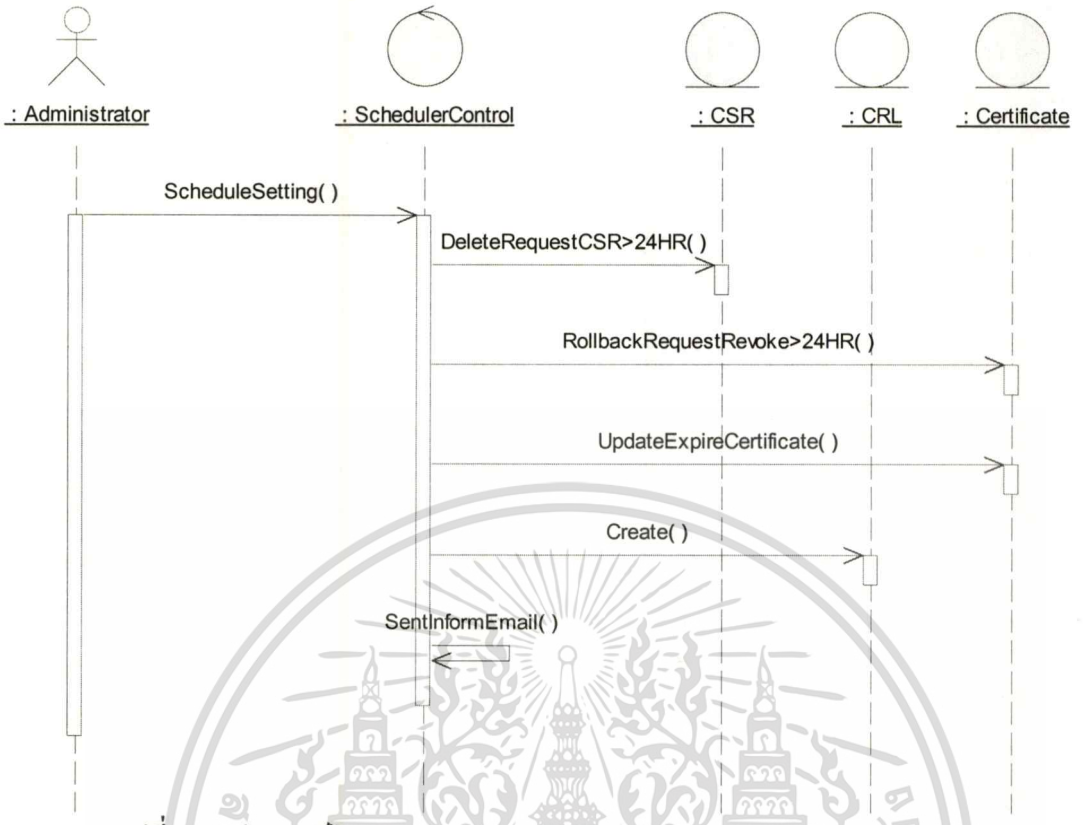
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

9. แสดงข้อความแจ้งการจบขั้นตอนการขอใบรับรองดิจิทัลแทนใบเก่า

ตารางที่ 4.18 อธิบายยูสเคส Automatic Update Information

ยูสเคส	Automatic Update Information
วัตถุประสงค์	• ลบการร้องขอใบรับรองดิจิทัลที่ไม่มีการยืนยันภายในเวลาที่กำหนด • ยกเลิกการร้องขอการยกเลิกใบรับรองดิจิทัลที่ไม่มีการยืนยันภายในเวลาที่กำหนด • สร้างไฟล์รายการใบรับรองดิจิทัลที่ถูกยกเลิก • ปรับปรุงฐานข้อมูลสำหรับใบรับรองที่หมดอายุ • ส่งอีเมลแจ้งเตือนการหมดอายุของใบรับรองดิจิทัลให้แก่ผู้ใช้ล่วงหน้า
เงื่อนไขเมื่อเริ่มต้น	เป็นผู้ดูแลระบบระบบ
เมื่อทำงานสำเร็จ	การทำงานต่างๆ ทำงานตามเวลาที่กำหนด
เมื่อทำงานไม่สำเร็จ	การทำงานต่างๆ ไม่ทำงาน
ผู้ใช้ที่เกี่ยวข้อง	ผู้ดูแลระบบ (Admin)
ข้อมูลเข้า	เวลาที่ต้องการให้มีการทำงาน
ข้อมูลออก	ไฟล์บันทึกการทำงาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.20 ซีเควนซ์ไดอะแกรมของยูสเคส Automatic Update Information

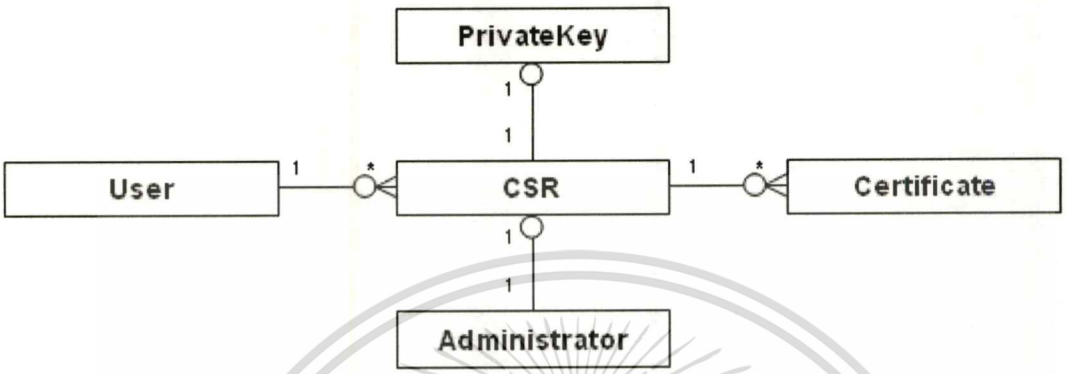
จากรูปที่ 4.20 แสดงซีเควนซ์ไดอะแกรมของยูสเคส Automatic Update Information ซึ่งมีลำดับการทำงานดังนี้

1. ผู้ดูแลระบบทำการตั้งเวลาในทำงานผ่านโปรแกรม Window Schedule
2. เมื่อตรงกับเวลาที่ตั้งไว้ Window Schedule ทำการลบคำร้องขอใบรับรองดิจิทัลที่ไม่มีการยืนยันภายในเวลาที่กำหนด
3. เมื่อตรงกับเวลาที่ตั้งไว้ Window Schedule ทำงานเพื่อทำการยกเลิกคำร้องขอการยกเลิกใบรับรองดิจิทัลที่ไม่มีการยืนยันภายในเวลาที่กำหนด
4. เมื่อตรงกับเวลาที่ตั้งไว้ Window Schedule ทำงานเพื่อทำการปรับปรุงฐานข้อมูลสำหรับใบรับรองที่หมดอายุ
5. เมื่อตรงกับเวลาที่ตั้งไว้ Window Schedule ทำงานเพื่อทำการสร้างไฟล์รายการใบรับรองดิจิทัลที่ถูกยกเลิก
6. เมื่อตรงกับเวลาที่ตั้งไว้ Window Schedule ทำงานเพื่อส่งอีเมลแจ้งเตือนการหมดอายุของใบรับรองดิจิทัลให้แก่ผู้ใช้ล่วงหน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.4 E-R Model ของระบบการออกใบรับรองดิจิทัล

จากขั้นตอนการวิเคราะห์ระบบ สามารถออกแบบฐานข้อมูลจากคลาสไดอะแกรม โดยการนำเอนทิตีคลาสมาสร้างเป็น E-R Model ได้ดังรูปที่ 4.21



รูปที่ 4.21 อีอาร์ไดอะแกรมของระบบผู้ให้บริการใบรับรองดิจิทัล

4.3.5 พจนานุกรมข้อมูล (Data Dictionary)

เป็นเครื่องมือที่ช่วยในการจัดเก็บลำดับการทำงานต่างๆ เกี่ยวกับข้อมูลให้เป็นหมวดหมู่ ทำให้สามารถค้นหาลำดับการทำงานที่ต้องการได้สะดวก สร้างขึ้นมาโดยเฉพาะเพื่อใช้กับระบบฐานข้อมูล

จากอีอาร์ไดอะแกรมในหัวข้อ 4.3.4 เราสามารถเขียนพจนานุกรมของเอนทิตีที่อยู่ในระบบได้ดังนี้

ตารางที่ 4.19 พจนานุกรมข้อมูลของตาราง User

ชื่อฟิลด์	ลำดับการทำงาน	ประเภท	ชนิดคีย์	ชื่อตารางอ้างอิง
UserId	รหัสผู้ใช้	Integer	PK	
UserName	ชื่อผู้ใช้ในระบบ	String		
UserFullName	ชื่อเต็มผู้ใช้	String		
UserPasswordEncrypt	รหัสผ่าน	String		
UserEmail	อีเมลผู้ใช้	String		

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.20 พจนานุกรมข้อมูลของตาราง PrivateKey

ชื่อฟิลด์	ลำดับการทำงาน	ประเภท	ชนิดคีย์	ชื่อตารางอ้างอิง
KeyId	รหัสคีย์	Integer	PK	
KeyFileName	ชื่อไฟล์ของคีย์	String		
KeyGenerateDate	วันที่สร้างคีย์	Date		
PassPhraseEncrypt	รหัสลับ	String		

ตารางที่ 4.21 พจนานุกรมข้อมูลของตาราง CSR

ชื่อฟิลด์	ลำดับการทำงาน	ประเภท	ชนิดคีย์	ชื่อตารางอ้างอิง
CSRId	รหัสคำร้องขอ	Integer	PK	
CSRFileName	ชื่อไฟล์ของคำร้องขอ	String		
CSRGenerateDate	วันที่สร้างคำร้องขอ	Date		
Country	ประเทศ	String		
State	รัฐ หรือ จังหวัด	String		
Locality	อำเภอ หรือ เขต	String		
OrganizationName	ชื่อองค์กร	String		
OrganizationUnit	ชื่อหน่วยงาน	String		
Email	อีเมล	String		
ChallengePassword	รหัสสำรอง	String		
CompanyName	ชื่อบริษัท	String		
KeyId	รหัสคีย์	Integer	FK	PrivateKey
UserId/AdminId	รหัสผู้ใช้ หรือ รหัสผู้ดูแลระบบ	Integer	FK	User หรือ Administrator

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5

การพัฒนาระบบผู้บริการออกใบรับรองดิจิทัล

เนื่องจากความสะดวกในการพัฒนาและทดลอง การทำงานทั้งหมดได้กระทำบนเครื่องคอมพิวเตอร์ส่วนบุคคลที่มีหน่วยประมวลผลกลาง Centino 1.6 กิกะเฮิร์ต หน่วยความจำ 512 เมกะไบท์ โดยนำมาใช้ทำหน้าที่เสมือนเซิร์ฟเวอร์ และระบบผู้ให้บริการใบรับรองดิจิทัลนี้ได้มีการนำซอฟต์แวร์ต่างๆ มาใช้งาน เพื่อทำงานร่วมกันให้เกิดเป็นระบบที่สามารถทำงานได้ครบถ้วน ซอฟต์แวร์ต่างๆ ที่นำมาใช้งานประกอบด้วย

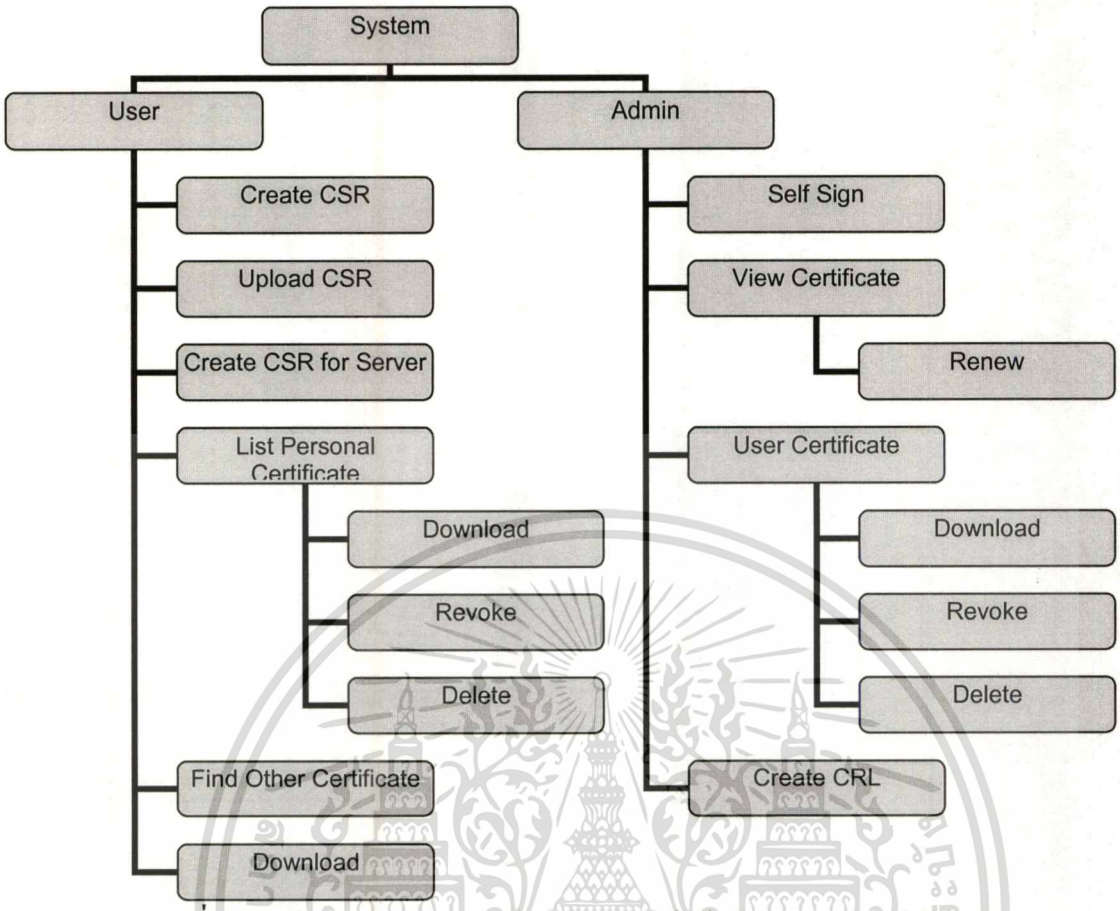
1. Microsoft Window XP
2. Apache เวอร์ชัน 2.2.2
3. Openssl เวอร์ชัน 0.9.8b
4. PHP เวอร์ชัน 5.2
5. PHP-Nuke เวอร์ชัน 7.8
6. MySQL เวอร์ชัน 5.0.20
7. ArGoSoft เวอร์ชัน 1.8.8.8
8. Outlook Express

5.1. โครงสร้างการทำงานของระบบผู้ประกอบการออกใบรับรองดิจิทัล

ระบบผู้ให้บริการออกใบรับรองดิจิทัลที่ได้พัฒนาขึ้น ประกอบด้วยการทำงาน 2 ส่วนหลัก ได้แก่ ส่วนของผู้ใช้ทั่วไป และส่วนของผู้ดูแลระบบ โดยในแต่ละส่วนยังได้มีการทำงานย่อยซึ่งสามารถอธิบายได้ดังแผนผังโครงสร้างการทำงานดังรูปที่ 5.1

การทำงานในส่วนของผู้ใช้ทั่วไป ประกอบด้วยฟังก์ชันการทำงานหลัก 5 รายการ ได้แก่ การสร้างคำร้องขอใบรับรองดิจิทัล (Create CSR) การขอใบรับรองดิจิทัลโดยการอัพโหลด CSR (Upload CSR) การแสดงรายการคำร้องและใบรับรองดิจิทัลส่วนตัว (List Personal Certificate) การค้นหาใบรับรองดิจิทัลในระบบ (Find Others Certificate) และการดาวน์โหลดไฟล์รายการใบรับรองที่ถูกเพิกถอน (Download CRL) และในส่วนของผู้ดูแลระบบ ประกอบด้วยฟังก์ชันการทำงานหลัก 4 รายการ ได้แก่ การสร้างใบรับรองตนเอง (Self Sign) การแสดงข้อมูลใบรับรองของ CA (View Certificate) การแสดงรายการใบรับรองของผู้ใช้ (User Certificate) และการสร้างไฟล์รายการใบรับรองที่ถูกยกเลิก (Create CRL)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

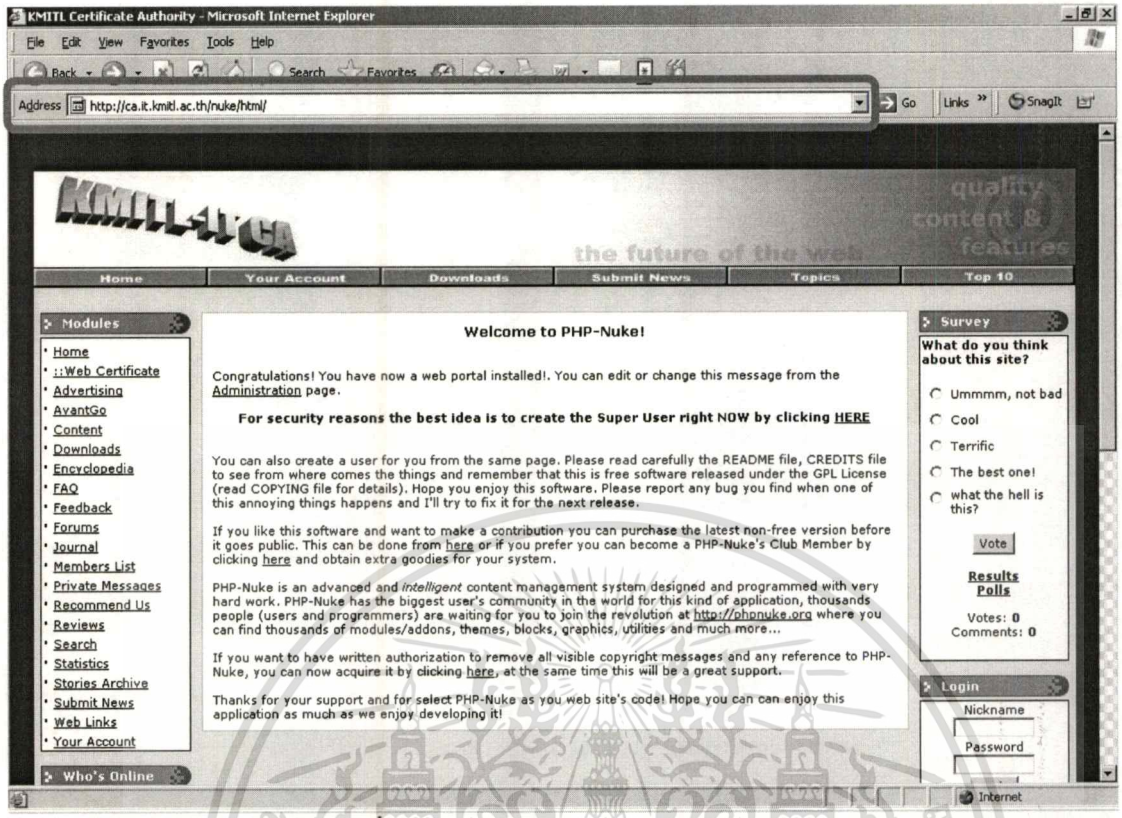


รูปที่ 5.1 แผนภาพแสดงโครงสร้างของระบบผู้ให้บริการใบรับรองดิจิทัล

5.2. ฟังก์ชันการทำงานของระบบผู้ประกอบการออกใบรับรองดิจิทัล

การเข้าสู่ระบบจะต้องใช้ตาม URL ที่ได้มีการตั้งค่าไว้ซึ่งสามารถดูรายละเอียดได้ในส่วนของภาคผนวก ผู้ใช้และผู้ดูแลระบบสามารถใช้โปรแกรมเว็บบราวเซอร์เช่น Internet Explorer หรือ Opera เป็นต้น โดยเมื่อเข้าสู่ระบบผ่าน http://ca.it.kmitl.ac.th/nuke/html/ จะปรากฏหน้าจอแรกของระบบดังรูปที่ 5.2

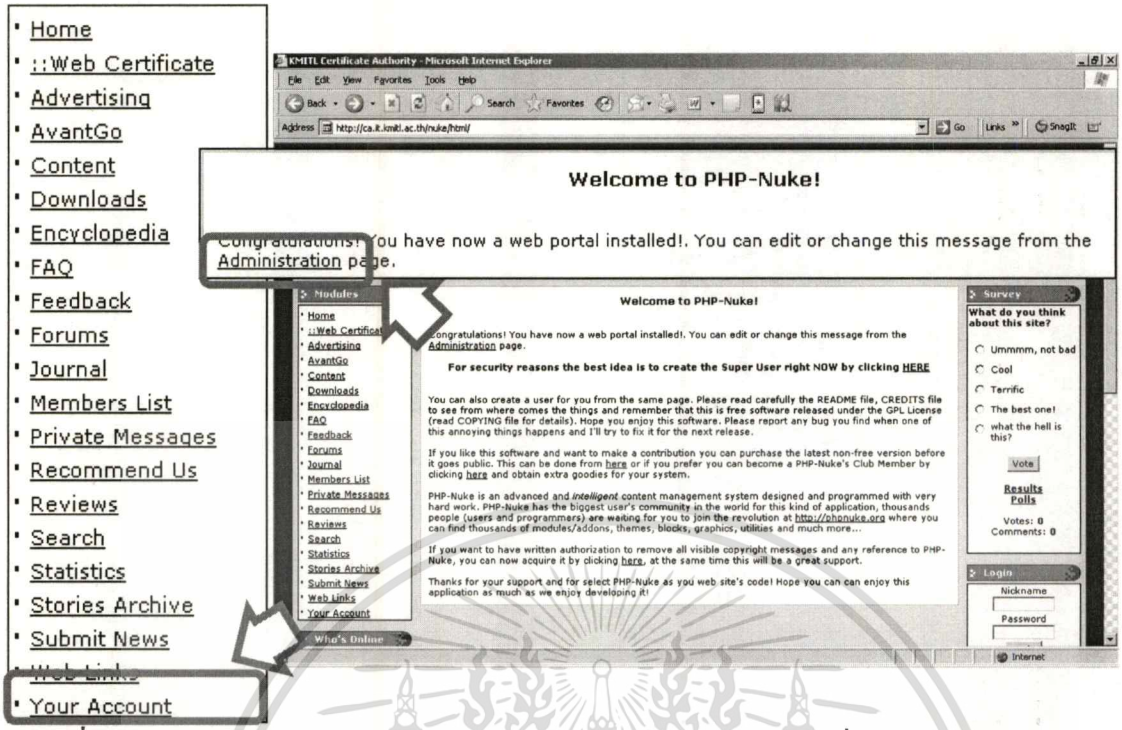
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.2 หน้าจอแสดงหน้าแรกของระบบ

จากหน้าแรกของระบบนี้สามารถเข้าสู่การทำงานในส่วนของผู้ใช้ทั่วไปได้โดยผ่านเมนู “Your Account” และสามารถเข้าสู่การทำงานในส่วนของผู้ดูแลระบบได้โดยผ่านเมนู “Administration” ซึ่งแสดงดังรูปที่ 5.3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.3 หน้าจอแสดงหน้าแรกเมนูหลักในการเข้าสู่การทำงานของผู้ใช้ทั่วไป และผู้ดูแลระบบ

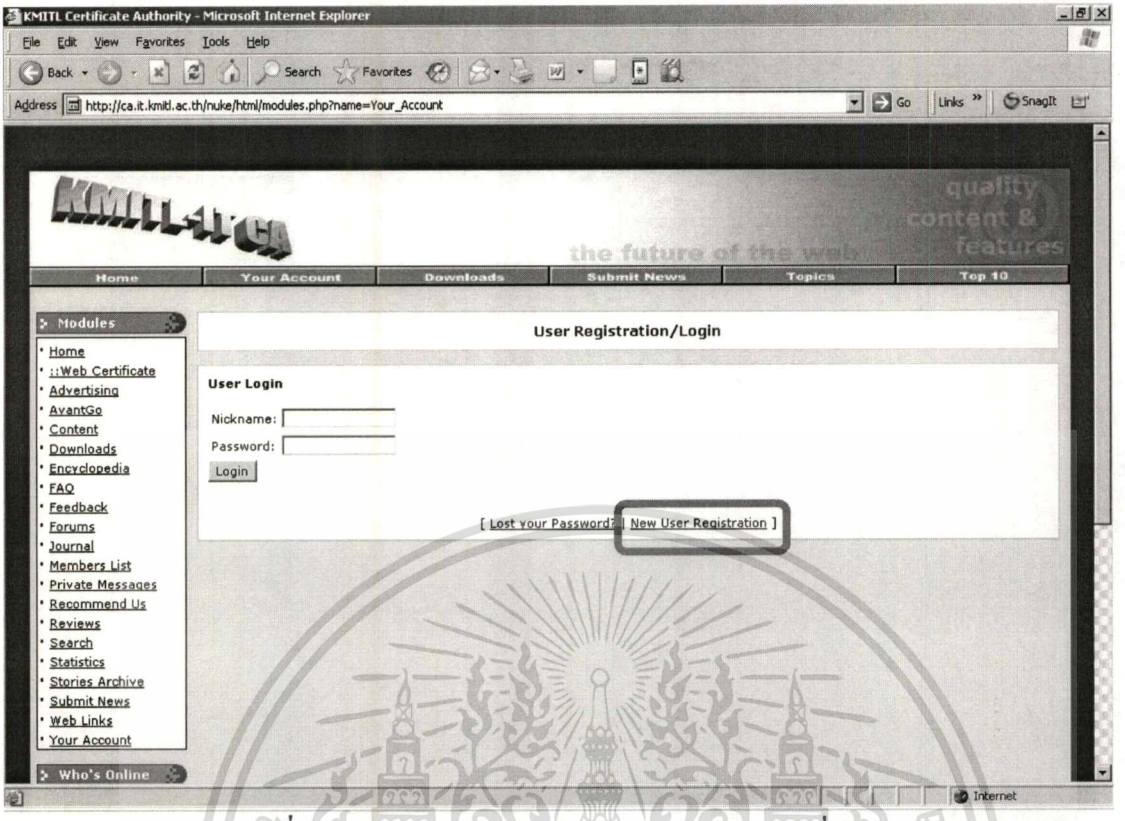
5.2.1 ฟังก์ชันการทำงานของผู้ใช้ (User)

การใช้งานระบบในส่วนของการทำงานเกี่ยวกับใบรับรองดิจิทัลผู้ใช้จำเป็นต้องทำการล็อคอินเข้าสู่ระบบก่อน โดยเมื่อผู้ใช้เข้าเมนู “Your Account” จากรูปที่ 5.3 ผู้ใช้จะพบหน้าจอให้ทำการล็อคอินเข้าสู่ระบบ ซึ่งในกรณีนี้ผู้ใช้ยังไม่มีการลงทะเบียนจะต้องทำการลงทะเบียนโดยเข้าเมนู “New User Registration” ดังรูปที่ 5.4 และทำการป้อนข้อมูลต่างๆ ได้แก่

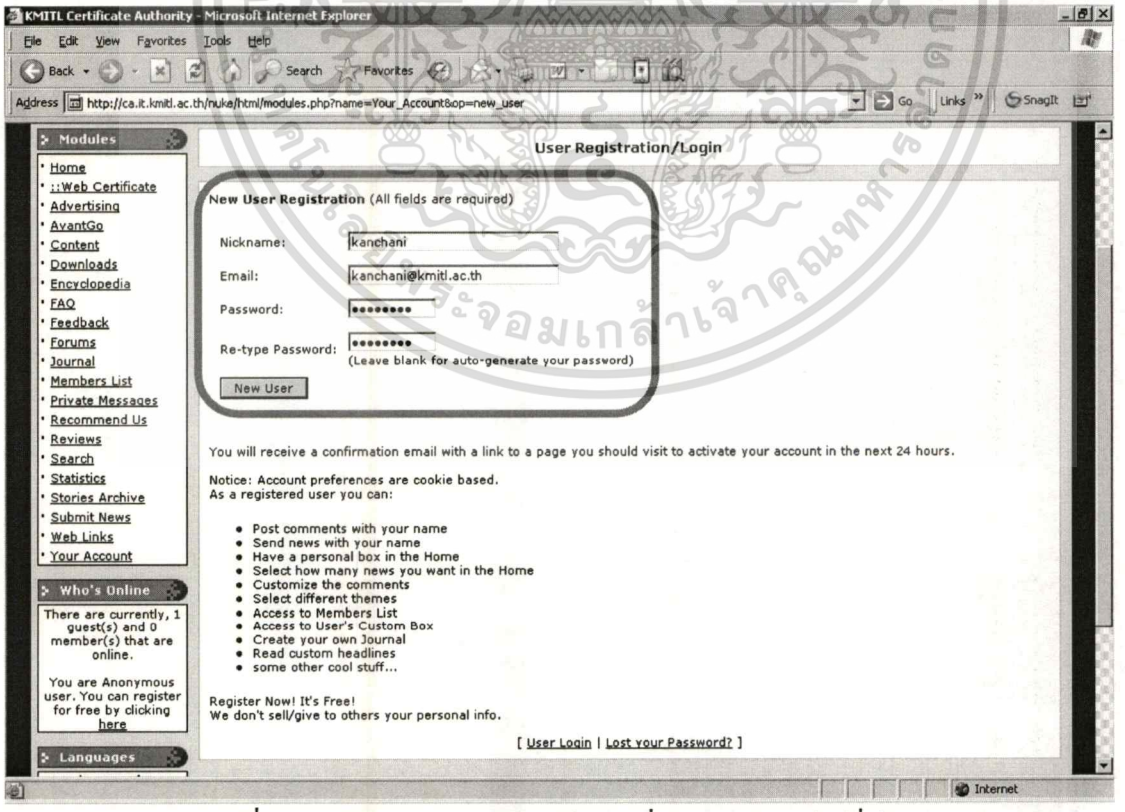
- ชื่อผู้ใช้ในระบบ (Nickname)
- อีเมล (Email)
- รหัสผ่าน (Password และ Re-type Password)

จากข้อมูลที่ผู้ใช้ป้อนในรูปที่ 5.5 ชื่อผู้ใช้ในระบบ และรหัสผ่านนี้จะใช้ในการเข้าสู่ระบบเท่านั้น จะไม่มีการเชื่อมโยงกับใบรับรองดิจิทัลที่ผู้ใช้จะขอในส่วนถัดไป และในส่วนของอีเมลนี้ผู้ใช้จำเป็นต้องป้อนอีเมลที่มีการใช้งานอยู่จริง เนื่องจากเมื่อผู้ใช้ป้อนข้อมูลในการเรียบร้อยแล้ว ระบบจะมีขั้นตอนการยืนยันการมีตัวตนของผู้ใช้จริง โดยระบบจะส่งอีเมลไปยังอีเมลแอดเดรสที่ผู้ใช้ระบุ เพื่อใช้สำหรับยืนยันการลงทะเบียนไปให้แก่ผู้ใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



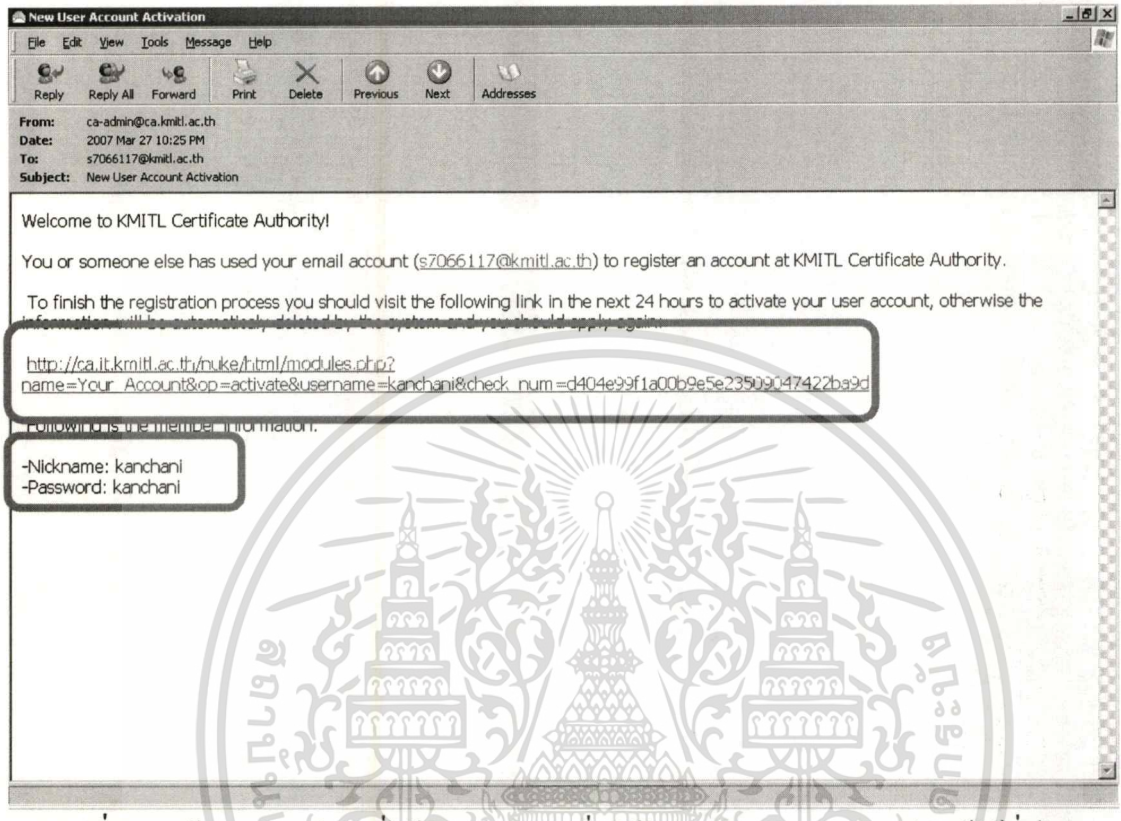
รูปที่ 5.4 หน้าจอแสดงการเข้าสู่การลงทะเบียนผู้ใช้ทั่วไป



รูปที่ 5.5 หน้าจอแสดงการป้อนข้อมูลเพื่อลงทะเบียนผู้ใช้ทั่วไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

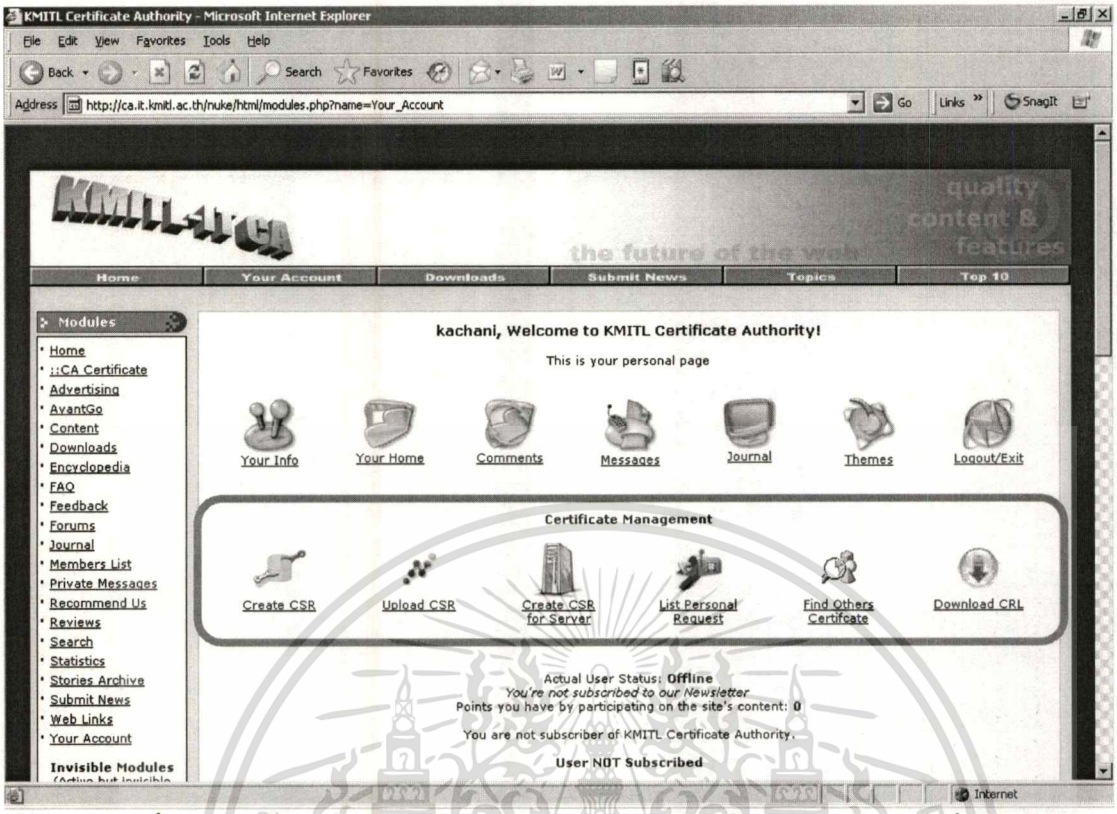
ผู้ใช้สามารถทำการยืนยันการลงทะเบียนได้โดยการตรวจสอบอีเมลที่ได้รับจากระบบซึ่งแสดงดังรูปที่ 5.6 โดยในนี้จะระบุถึง URL ที่ผู้ใช้จะใช้ในการยืนยันการมีตัวตนเพื่อลงทะเบียน



รูปที่ 5.6 หน้าจอแสดงอีเมลที่ได้รับจากระบบเพื่อใช้ในการยืนยันการลงทะเบียนผู้ใช้ทั่วไป

เมื่อผู้ใช้ทำการยืนยันการลงทะเบียนเรียบร้อยแล้ว ผู้ใช้จะสามารถเข้าสู่ระบบจากหน้าจอดังรูปที่ 5.4 ได้โดยใช้ “Nickname” และ “Password” ที่แสดงในอีเมลดังรูปที่ 5.6 และจะปรากฏหน้าจอแสดงเมนูหลักของสำหรับผู้ใช้ดังรูปที่ 5.7 ซึ่งมีเมนูการทำงานเกี่ยวกับใบรับรองดิจิทัล ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



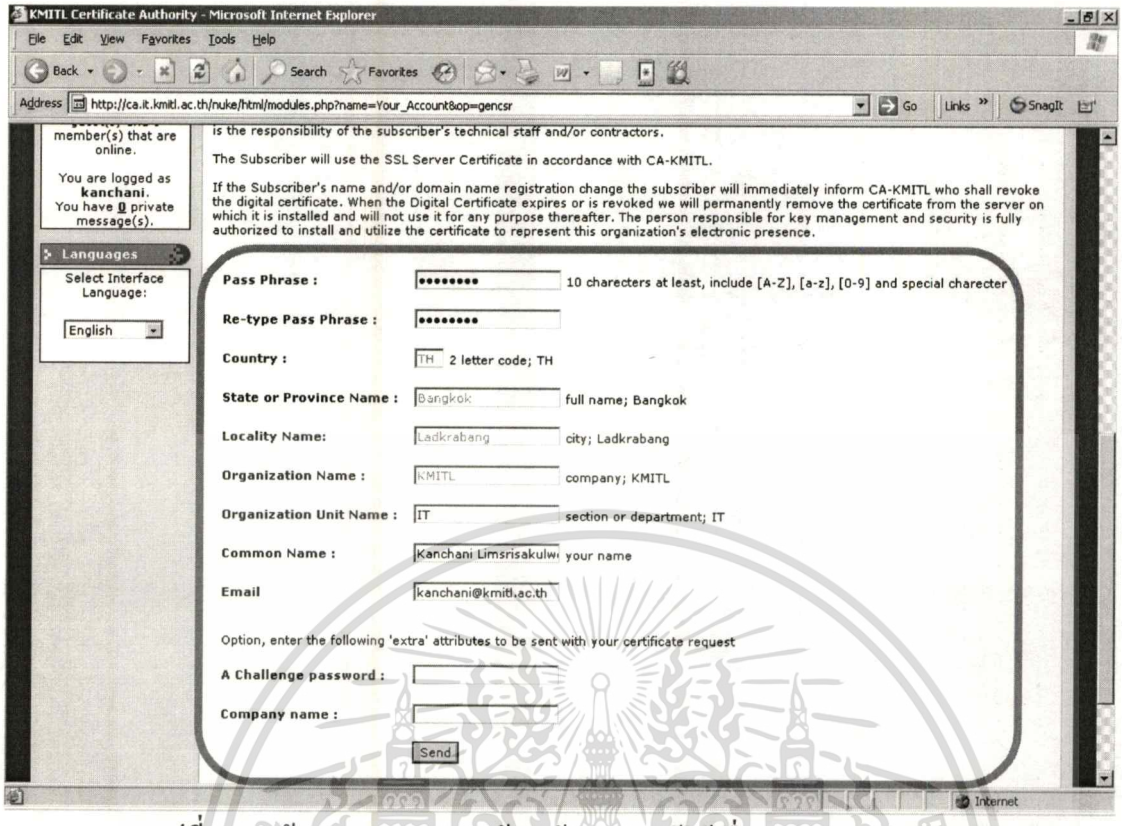
รูปที่ 5.7 หน้าจอแสดงเมนูการทำงานเกี่ยวใบรับรองดิจิทัลในส่วนของผู้ใช้ทั่วไป

- **การสร้างคำร้องขอใบรับรองดิจิทัล (Create CSR)**

การขอใบรับรองดิจิทัลผู้ใช้จำเป็นจะต้องมีไฟล์คำร้องขอ (Certificate Signing Request) ก่อน ดังนั้นในกรณีผู้ใช้ที่ยังไม่มีไฟล์คำร้องขอ จะสามารถสร้างคำร้องขอได้โดยผ่านเมนู "Create CSR" เมื่อผู้ใช้เข้าสู่การสร้างไฟล์คำร้องขอใบรับรองดิจิทัลจะพบกับหน้าจอดังรูปที่ 5.8 เพื่อป้อนข้อมูลต่างๆ ของใบรับรองดิจิทัลที่ผู้ใช้ต้องการร้องขอ โดยข้อมูลต่างๆ มีดังนี้

1. รหัสลับสำหรับการสร้างกุญแจส่วนตัว (Pass Phrase และ Re-type Pass Phrase)
2. ประเทศที่อยู่ของผู้ขอ (Country)
3. รัฐหรือจังหวัดที่อยู่ของผู้ขอ (State or Province Name)
4. ตำบลที่อยู่ของผู้ขอ (Locality Name)
5. องค์กรของผู้ขอ (Organization Name)
6. หน่วยงานในองค์กรของผู้ขอ (Organization Unit Name)
7. ชื่อผู้ใช้ (Common Name)
8. อีเมล (Email)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

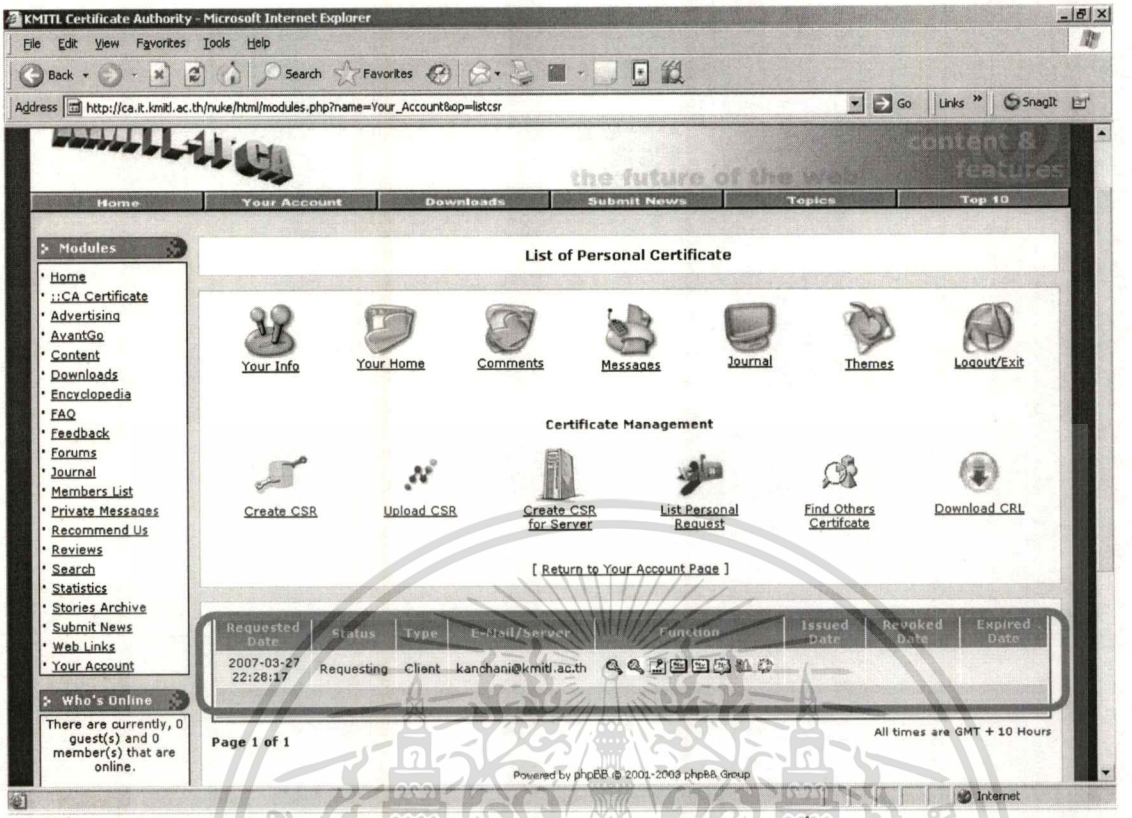


รูปที่ 5.8 หน้าจอแสดงเมนูการป้อนข้อมูลของผู้ใช้เพื่อขอใบรับรองดิจิทัล

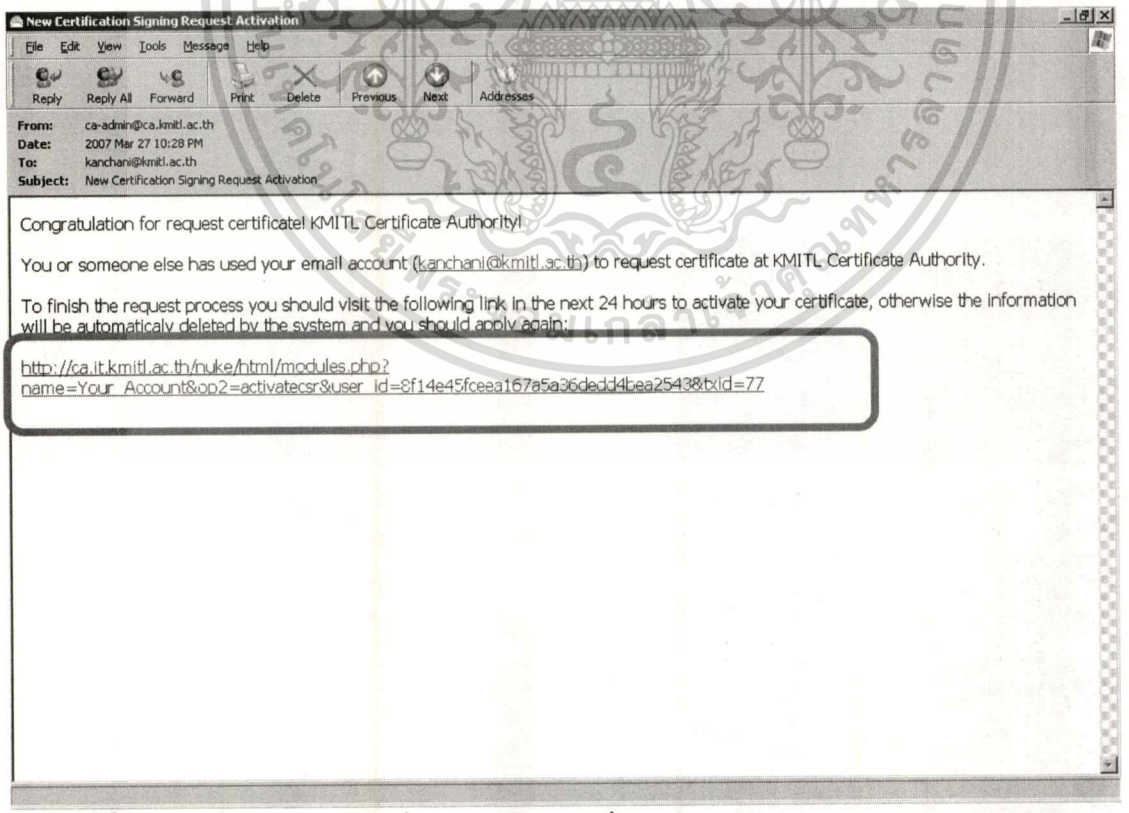
ระบบจะนำข้อมูลในส่วนของรหัสลับไปใช้ในการสร้างกุญแจส่วนตัว (Private Key) สำหรับใช้งานคู่กับใบรับรองดิจิทัลที่ผู้ใช้ขอ และส่วนของข้อมูลถัดมาได้แก่ ประเทศที่อยู่ของผู้ขอ รัฐหรือจังหวัดที่อยู่ของผู้ขอ ตำบลที่อยู่ของผู้ขอ องค์กรของผู้ขอ หน่วยงานในองค์กรของผู้ขอ ชื่อผู้ขอ และอีเมล จะถูกนำมาใช้เป็นข้อมูลที่ใช้ในการสร้างไฟล์คำร้องขอ เพื่อนำไปเป็นข้อมูลในการสร้างใบรับรองดิจิทัล ข้อมูลในส่วนสุดท้ายเป็นข้อมูลเสริมซึ่งจะมีหรือไม่มีก็ได้ ได้แก่ คำถามสำหรับร้องถามรหัสลับ (A Challenge password) และชื่อบริษัท (Company Name)

ในการป้อนอีเมลสำหรับของใบรับรองดิจิทัลนี้ ผู้ใช้สามารถใช้อีเมลอื่นที่มิใช่อีเมลเดียวกับที่ใช้ในการลงทะเบียนผู้ใช้ได้ แต่อีเมลที่ผู้ใช้ป้อนจะต้องไม่มีผู้ใช้รายใดมีการขอและใช้ใบรับรองเพื่อรับรองอีเมลนั้นๆ ในขณะนั้น ยกเว้นแต่ใบรับรองดิจิทัลที่รับรองอีเมลนั้นๆ ถูกยกเลิกหรือหมดอายุแล้ว เมื่อผู้ใช้ป้อนข้อมูลที่ต้องให้ระบุในใบรับรองเรียบร้อยแล้ว ระบบจะยังไม่ทำการสร้างใบรับรองดิจิทัลให้แก่ผู้ใช้ในทันที ดังนั้นสถานะของคำร้องขอนี้จะถูกแสดงเป็น “Requesting” ดังรูปที่ 5.9 โดยระบบจะทำการส่งอีเมลไปยังอีเมลที่ผู้ใช้ระบุในการร้องขอใบรับรองเพื่อเป็นการยืนยันการมีตัวตนอยู่จริงของผู้ใช้อีเมลนั้นๆ ดังนั้นผู้ใช้จะได้รับอีเมลตามตัวอย่างรูปที่ 5.10

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



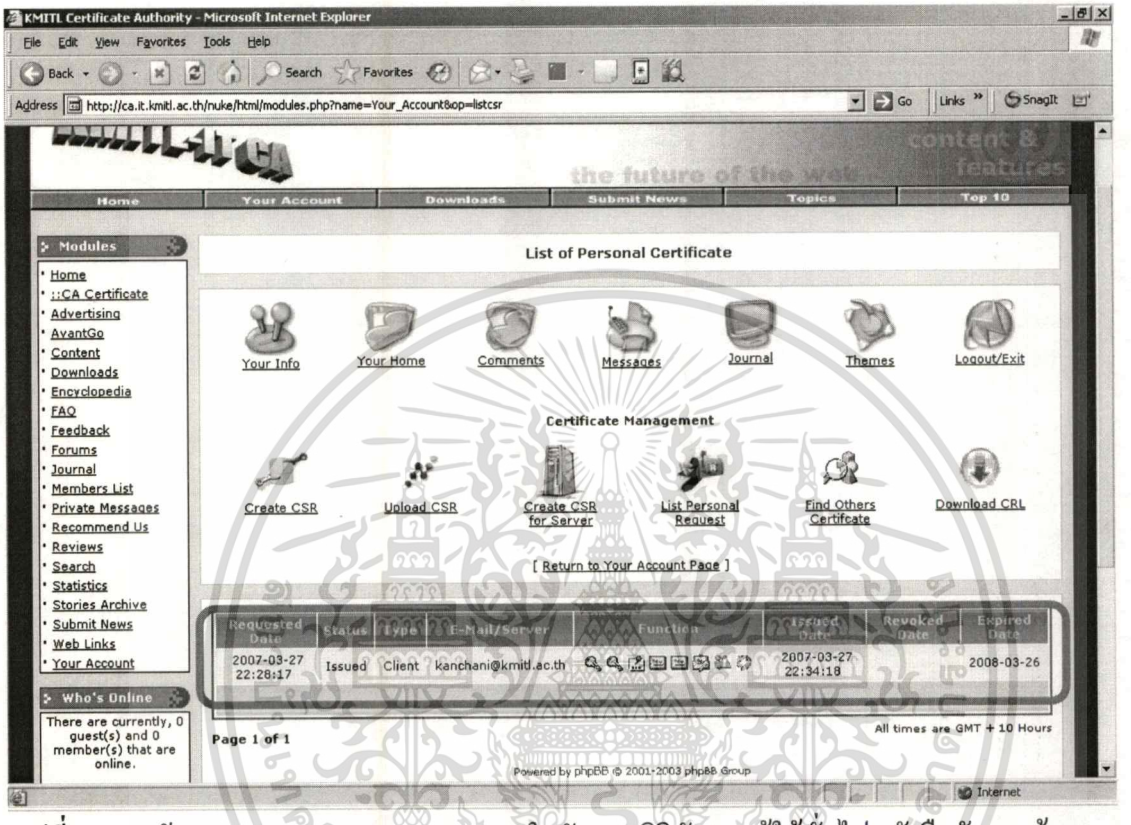
รูปที่ 5.9 หน้าจอแสดงสถานะรายการการขอใบรับรองดิจิทัลของผู้ใช้ทั่วไปก่อนยืนยันการร้องขอ



รูปที่ 5.10 หน้าจอแสดงอีเมลที่ได้รับจากระบบเพื่อใช้ในการยืนยันการขอใบรับรองดิจิทัล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ผู้ใช้สามารถยืนยันการขอใบรับรองดิจิทัลได้โดยใช้ URL ที่ระบุในอีเมลตามรูปที่ 5.10 และเมื่อผู้ใช้ได้ทำการยืนยันเรียบร้อยแล้วสถานะของคำร้องขอใบรับรองดิจิทัลจะถูกเปลี่ยนเป็น "Issued" ตามรูปที่ 5.11



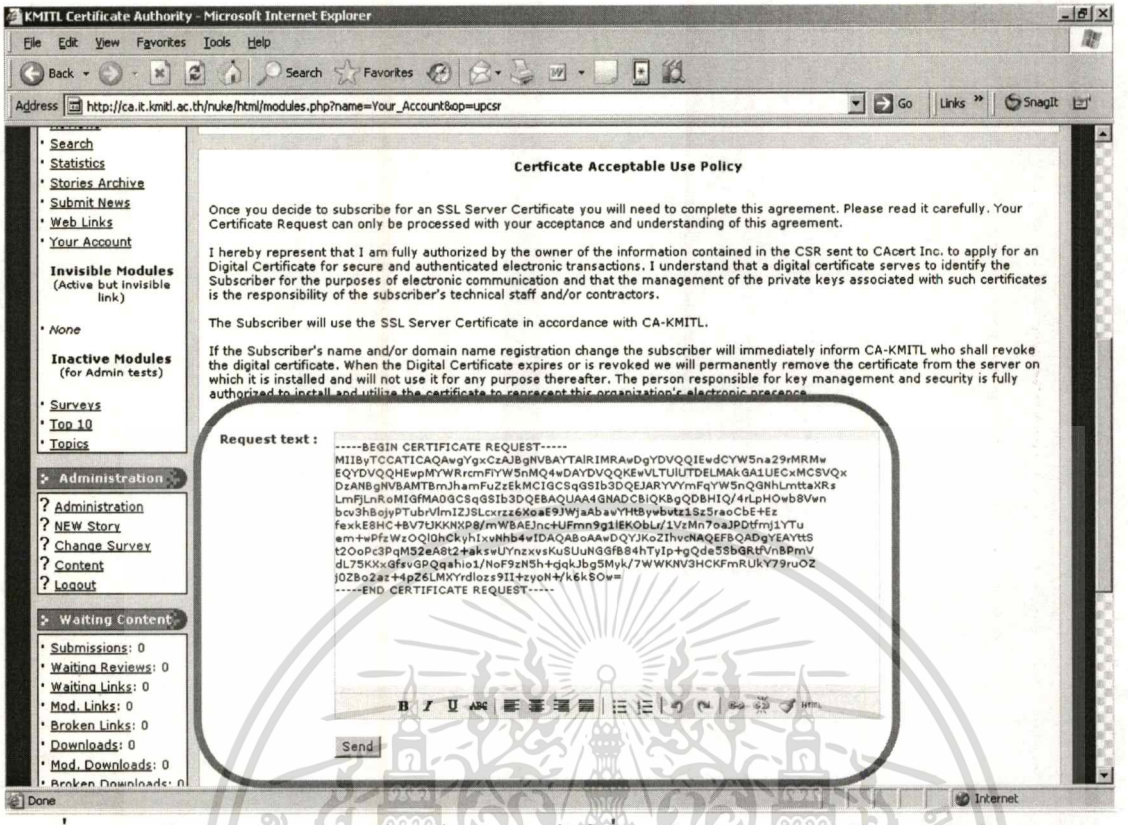
รูปที่ 5.11 หน้าจอแสดงสถานะรายการการขอใบรับรองดิจิทัลของผู้ใช้ทั่วไปหลังยืนยันการร้องขอ

- **การขอใบรับรองดิจิทัลโดยการอัพโหลด CSR (Upload CSR)**

ในกรณีที่ผู้ใช้ต้องการร้องขอใบรับรองดิจิทัลแต่ไม่ต้องการให้ระบบสร้างกุญแจส่วนตัวและไฟล์คำร้องขอใบรับรองดิจิทัล ผู้ใช้จำเป็นที่จะต้องมีไฟล์คำร้องขออยู่ก่อนแล้วและนำมาอัพโหลดเข้าสู่ระบบเพื่อใช้ในการสร้างใบรับรองดิจิทัลต่อไป โดยใช้เมนู "Upload CSR" ซึ่งจะแสดงหน้าจอดังรูปที่ 5.12

ระบบจะทำการตรวจสอบอีเมลที่อยู่ในคำร้องขอที่มีการเข้ารหัส ซึ่งจะต้องไม่มีผู้ใช้รายใดมีการขอและใช้ใบรับรองเพื่อรับรองอีเมลนั้นๆ ในขณะนั้น ยกเว้นแต่ใบรับรองดิจิทัลที่รับรองอีเมลนั้นๆ ถูกยกเลิกหรือหมดอายุแล้ว และจากนั้นระบบจะทำการส่งอีเมลไปยังอีเมลที่อยู่ใบคำร้องขอเพื่อให้ผู้ใช้ใช้ในการยืนยันการขอใบรับรองดิจิทัล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.12 หน้าจอแสดงเมนูการป้อนข้อมูลของผู้ใช้เพื่อขอใบรับรองดิจิทัลโดยการอัพโหลด CSR

- **การสร้างคำร้องขอใบรับรองดิจิทัลสำหรับเครื่องแม่ข่าย (Create CSR for Server)**

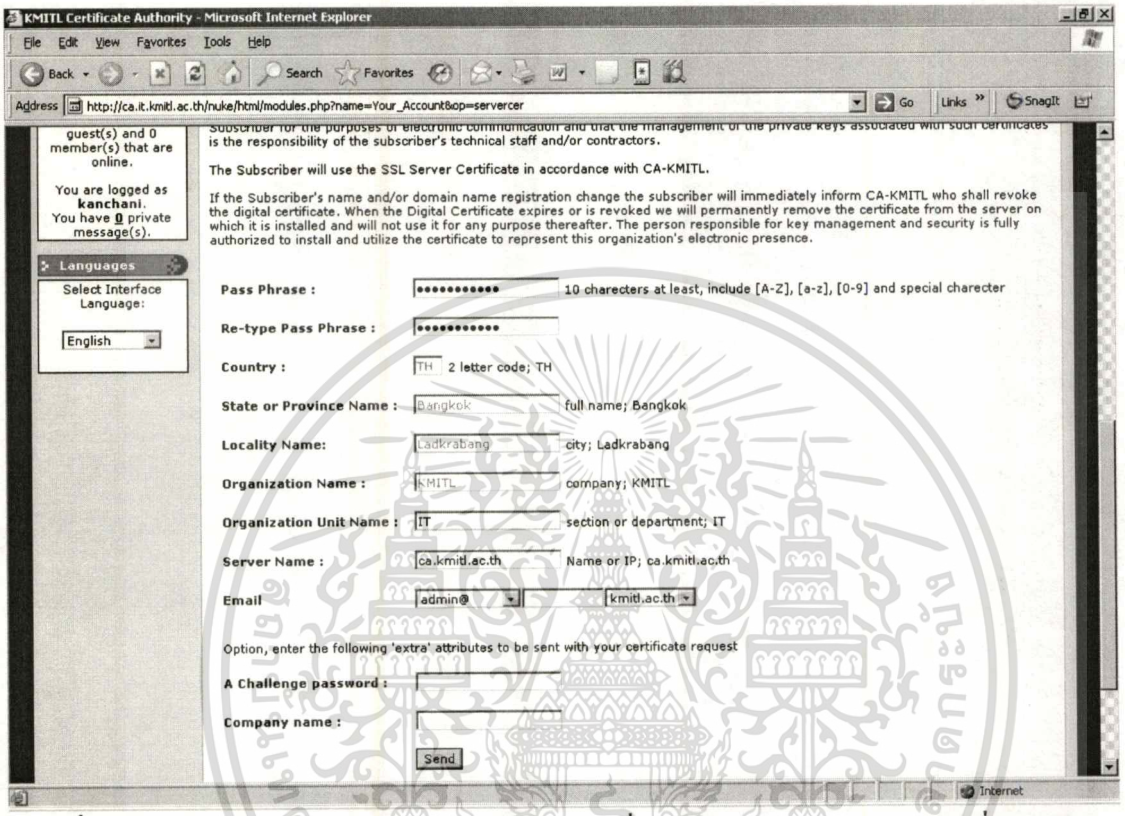
ผู้ใช้สามารถทำการของใบรับรองสำหรับเครื่องแม่ข่ายได้ โดยระบบจะอนุญาตให้กับผู้ใช้ที่เป็นผู้ดูแลระบบเครือข่ายย่อยในภายในสถาบันสามารถสร้างคำร้องขอใบรับรองดิจิทัลสำหรับเครื่องแม่ข่าย โดยจะมีการกำหนดชื่ออีเมลที่ใช้สำหรับการส่งข้อความเพื่อยืนยันการลงทะเบียนเป็นชื่อเฉพาะสำหรับผู้ดูแลระบบ เช่น admin root webmaster เป็นต้น และมีการกำหนดแอดเดรสของอีเมลที่เป็นแอดเดรสของสถาบันเท่านั้น เช่น kmitl.ac.th เป็นต้น

เมื่อผู้ใช้เข้าสู่เมนู “Create CSR for Server” เพื่อสร้างไฟล์คำร้องขอใบรับรองดิจิทัลจะพบกับหน้าจอดังรูปที่ 5.13 เพื่อป้อนข้อมูลต่างๆ ของใบรับรองดิจิทัลที่ผู้ใช้ต้องการร้องขอ โดยข้อมูลต่างๆ มีดังนี้

1. รหัสลับสำหรับการสร้างกุญแจส่วนตัว (Pass Phrase และ Re-type Pass Phrase)
2. ประเทศที่อยู่ของผู้ขอ (Country)
3. รัฐหรือจังหวัดที่อยู่ของผู้ขอ (State or Province Name)
4. ตำบลที่อยู่ของผู้ขอ (Locality Name)
5. องค์กรของผู้ขอ (Organization Name)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6. หน่วยงานในองค์กรของผู้ขอ (Organization Unit Name)
7. ชื่อเครื่องแม่ข่าย (Server Name)
8. อีเมล (Email)



รูปที่ 5.13 หน้าจอแสดงเมนูการป้อนข้อมูลของผู้ใช้เพื่อขอใบรับรองดิจิทัลสำหรับเครื่องแม่ข่าย

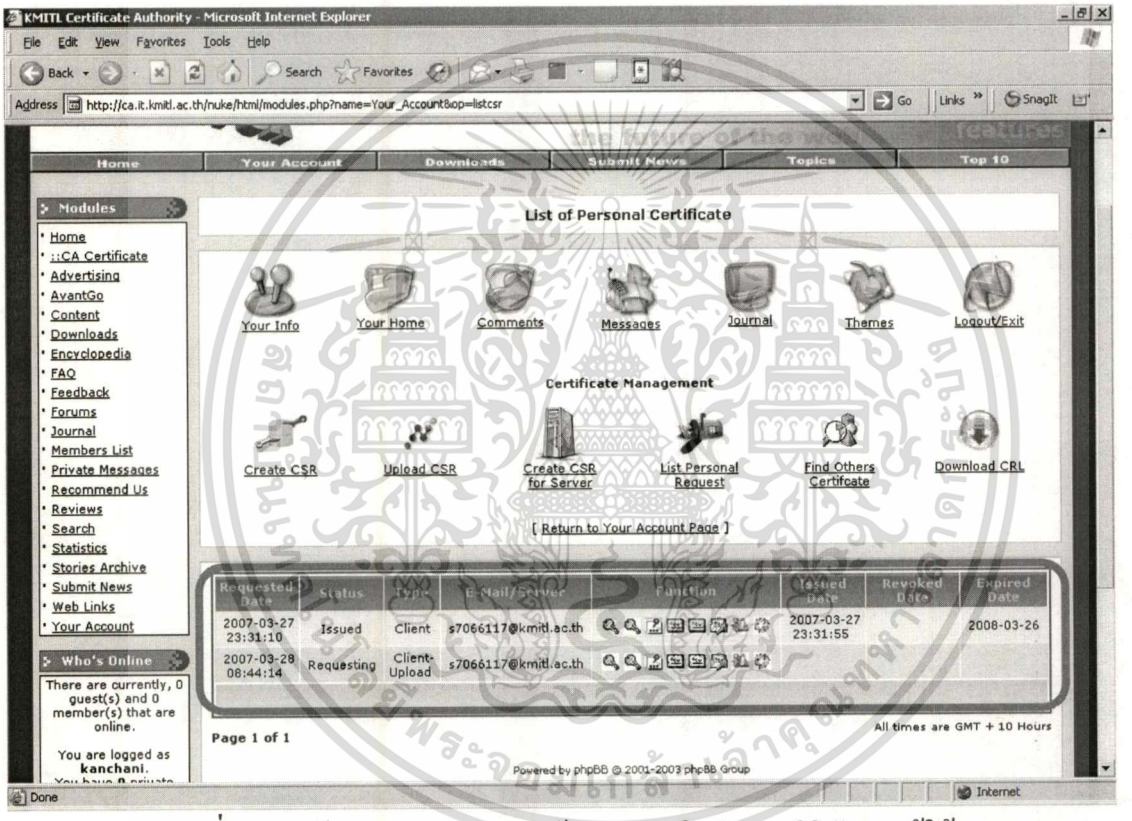
ระบบจะทำการตรวจสอบชื่อเครื่องแม่ข่ายที่อยู่ในระบบ ซึ่งจะต้องไม่เคยมีเครื่องแม่ข่ายที่มีการขอและใช้ใบรับรองเพื่อรับรองเครื่องแม่ข่ายนั้นๆ ในขณะนั้น ยกเว้นแต่ใบรับรองดิจิทัลที่รับรองเครื่องแม่ข่ายนั้นๆ ถูกยกเลิกหรือหมดอายุแล้ว และจากนั้นระบบจะทำการส่งอีเมลไปยังอีเมลที่อยู่ใบคำร้องขอ เพื่อให้ผู้ใช้ใช้ในการยืนยันการขอใบรับรองดิจิทัล

- **การแสดงรายการคำร้องและใบรับรองดิจิทัลส่วนตัว (List Personal Certificate)**

เมื่อผู้ใช้ได้มีการร้องขอใบรับรองดิจิทัลผู้ใช้สามารถตรวจสอบสถานะของแต่ละรายการคำร้องขอได้โดยเข้าเมนู “List Personal Certificate” ระบบจะแสดงข้อมูลต่างๆ ได้แก่ วันที่ร้องขอใบรับรองดิจิทัล สถานะของคำร้องขอ ประเภทการร้องขอ อีเมลที่ร้องขอใบรับรอง วันที่ออกใบรับรอง วันที่ใบรับรองถูกยกเลิก วันที่ใบรับรองหมดอายุ ซึ่งแสดงในรูปที่ 5.14 และมีฟังก์ชันย่อยในการทำงานดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1. ดาวน์โหลดกุญแจส่วนตัว (Private Key)
2. ดาวน์โหลดไฟล์คำร้องขอ (CSR)
3. ดาวน์โหลดใบรับรองดิจิทัลแบบ DER (DER Encoded Binary X.509)
4. ดาวน์โหลดใบรับรองดิจิทัลแบบ Base64 (Base64 Encoded X.509)
5. ดาวน์โหลดใบรับรองดิจิทัลแบบ PKCS12 (Personal Information Exchange)
6. ขอยกเลิกใบรับรอง
7. ขอต่ออายุใบรับรอง

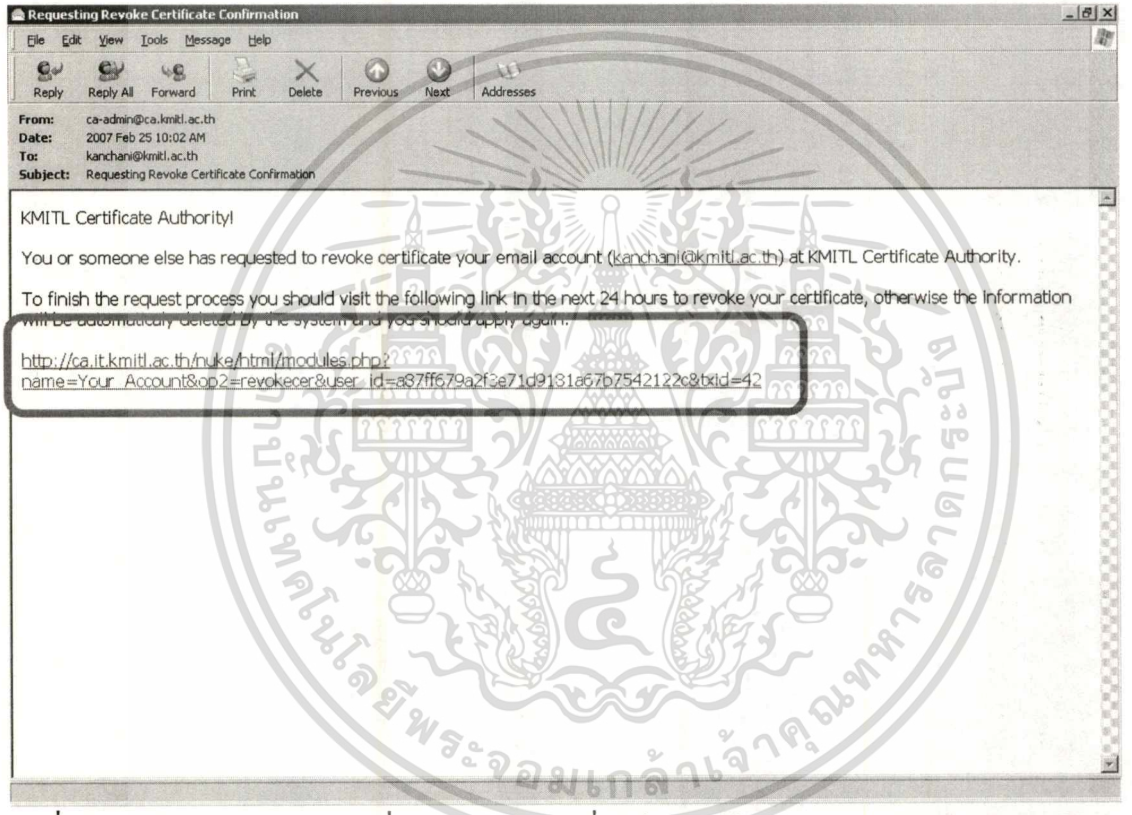


รูปที่ 5.14 หน้าจอแสดงรายการคำร้องขอและใบรับรองดิจิทัลของผู้ใช้

การดาวน์โหลดกุญแจส่วนตัวจะสามารถทำได้ในกรณีที่ผู้ใช้ทำการสร้างคำร้องขอจากระบบ และการดาวน์โหลดใบรับรองต่างๆ นั้นผู้ใช้จะสามารถดาวน์โหลดได้เมื่อผู้ใช้มีการยืนยันการร้องขอใบรับรองดิจิทัลสำหรับรายการนั้นๆ แล้ว ในกรณีรายการคำร้องของที่ผู้ใช้ทำการร้องขอใบรับรองดิจิทัลด้วยวิธีการอัพโหลดไฟล์คำร้องขอเข้าสู่ระบบ ผู้ใช้จะไม่สามารถดาวน์โหลดใบรับรองดิจิทัลแบบ PKCS12 ได้ เนื่องจากใบรับรองในรูปแบบ PKCS12 จะต้องประกอบไปด้วยข้อมูลที่เป็นกุญแจส่วนตัว และข้อมูลที่เป็นกุญแจสาธารณะ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รายการคำร้องขอใดที่มีสถานะเป็น “Issued” จะหมายถึงรายการร้องขอนั้นผู้ใช้ได้มีการยืนยันการร้องขอใบรับรองดิจิทัลนั้นๆ แล้ว และใบรับรองดิจิทัลที่ระบบออกให้ยังไม่หมดอายุ ผู้ใช้สามารถทำการร้องขอให้ทำการยกเลิกหรือเพิกถอนใบรับรองดิจิทัลที่ตนใช้งานอยู่ได้ (ซึ่งอาจเนื่องมาจากกุญแจส่วนตัวตกอยู่ในมือของผู้อื่น) โดยระบบจะทำการส่งอีเมลไปยังอีเมลที่ระบุอยู่ในใบรับรองดิจิทัลเพื่อให้ผู้ใช้ใช้ในการยืนยันการของเพิกถอนใบรับรองดิจิทัล และปรับสถานะใบรับรองดิจิทัลในระบบเป็น “Revoking” ตัวอย่างอีเมลที่ใช้ในการยืนยันการขอเพิกถอนใบรับรองดิจิทัลแสดงดังรูปที่ 5.15



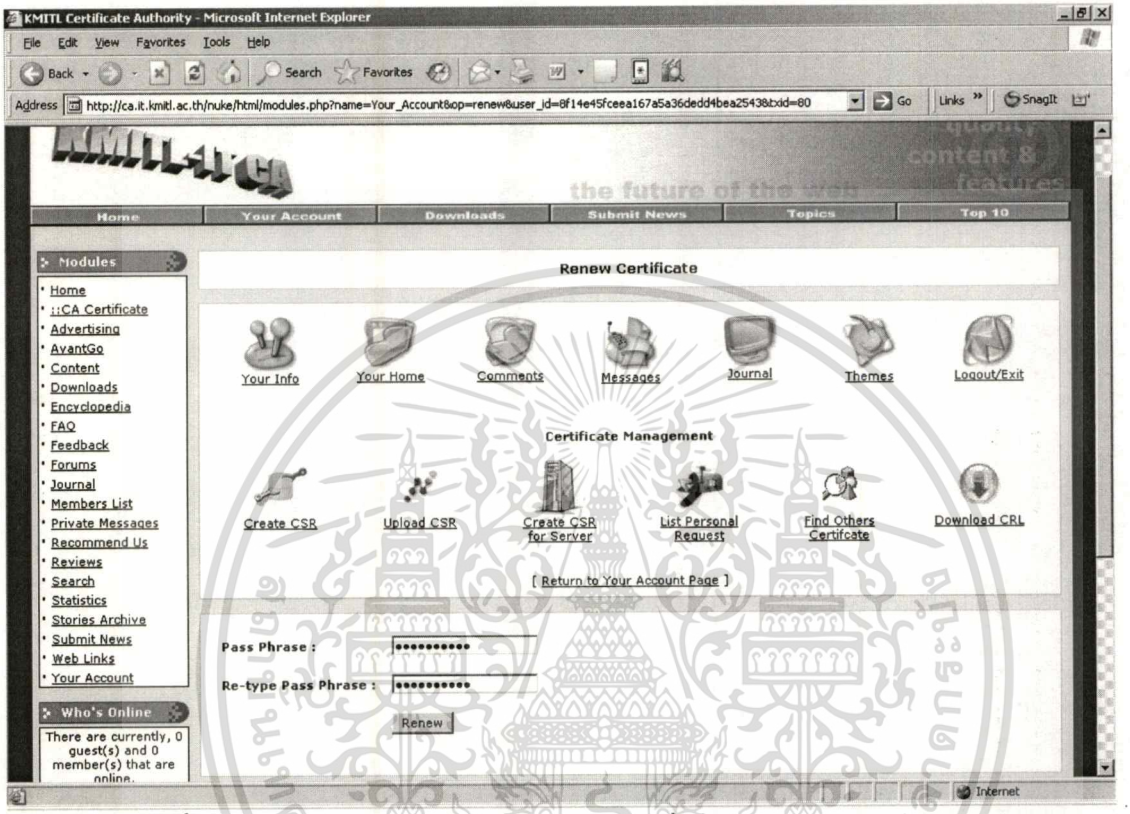
รูปที่ 5.15 หน้าจอแสดงจดหมายที่ได้รับจากระบบเพื่อใช้ในการยืนยันการขอยกเลิกใบรับรองดิจิทัล

เมื่อผู้ใช้ทำการยืนยันการขอเพิกถอนใบรับรองแล้ว ระบบจะทำการเพิกถอนใบรับรองดิจิทัลและเปลี่ยนสถานะใบรับรองดิจิทัลในระบบเป็น “Revoked”

ในกรณีที่ใบรับรองของผู้ใช้หมดอายุหรือใกล้หมดอายุ (จำนวนวันก่อนหมดอายุสามารถกำหนดได้จากไฟล์ตั้งค่า) ผู้ใช้สามารถทำการร้องขอต่ออายุใบรับรองดิจิทัลได้ โดยผู้ใช้จะต้องป้อนรหัสลับ (Pass Phrase) ดังรูปที่ 5.16

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในกรณีที่ผู้ใช้ของต่ออายุใบรับรองดิจิทัลที่ยังไม่หมดอายุ ระบบจะทำการเพิกถอนใบรับรองดิจิทัลใบเดิมของผู้ใช้ก่อน และทำการสร้างใบรับรองดิจิทัลใบใหม่โดยใช้ข้อมูลคำร้องขอเดิม



รูปที่ 5.16 หน้าจอแสดงการป้อน Pass Phrase เพื่อขอต่ออายุใบรับรองดิจิทัล

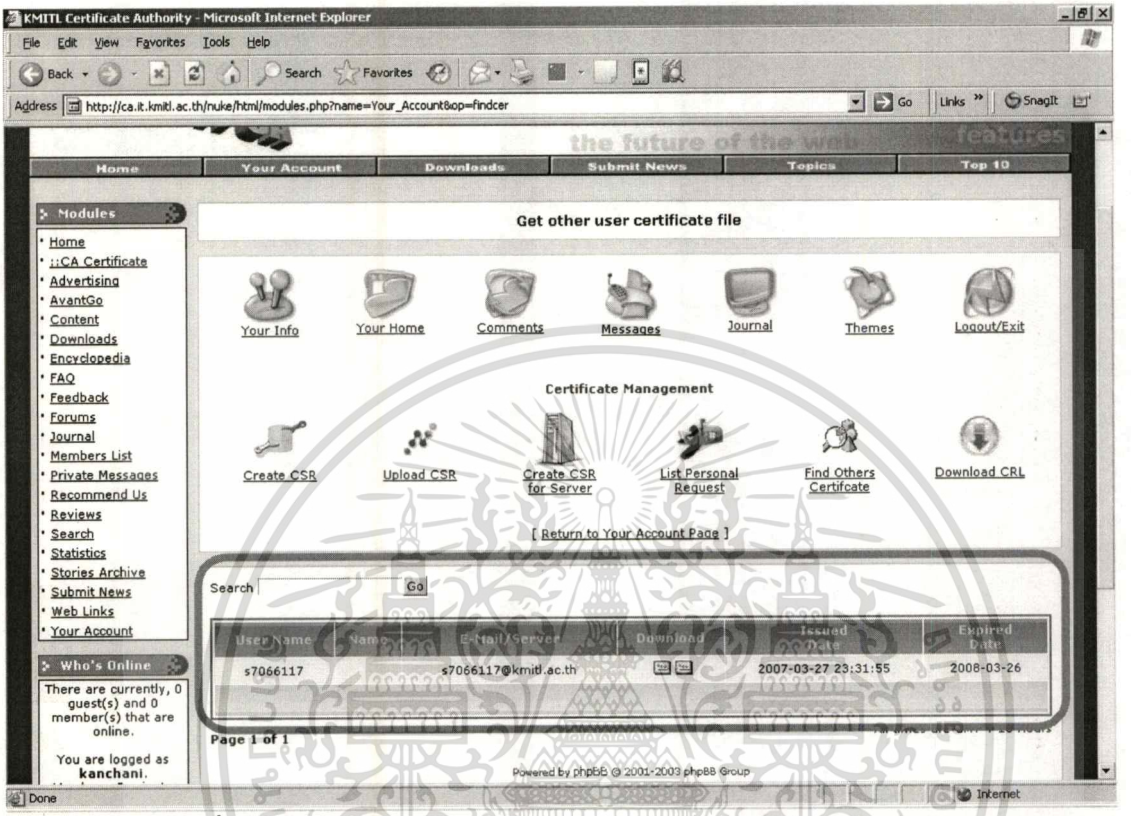
- **การค้นหาใบรับรองดิจิทัลในระบบ (Find Others Certificate)**

ในกรณีที่ผู้ใช้ต้องการติดต่อกับผู้ใช้รายอื่นและต้องการให้เกิดความปลอดภัยในการสื่อสาร ผู้ใช้สามารถทำการค้นหาใบรับรองดิจิทัลของผู้ใช้รายอื่นที่ตนต้องการติดต่อด้วย เพื่อทำการดาวน์โหลดใบรับรองดิจิทัลของผู้ใช้รายนั้นซึ่งเป็นใบรับรองดิจิทัลที่มีกุญแจสาธารณะ ไปทำการติดตั้งในโปรแกรมที่ใช้ในการสื่อสาร เช่น โปรแกรมอีเมลไคลเอนต์ เป็นต้น เพื่อให้โปรแกรมใช้กุญแจสาธรณะของผู้รับที่อยู่ในใบรับรองทำการเข้ารหัสข้อมูล

การค้นหาใบรับรองดิจิทัลของผู้ใช้รายอื่นในระบบ ผู้ใช้สามารถเข้าจากเมนู “Find Others Certificate” ระบบจะแสดงใบรับรองที่มีสถานะเป็น “Issued” ทั้งหมดในซึ่งแสดงดังรูปที่ 5.17 และผู้ใช้สามารถค้นหาชื่อผู้ใช้ที่ต้องการติดต่อได้โดยพิมพ์ ชื่อผู้ใช้ ชื่อ หรืออีเมล ของผู้ที่ต้องการค้นหาได้ในช่อง “Search” ระบบจะอนุญาตให้ผู้ใช้สามารถดาวน์โหลดใบรับรองดิจิทัลของผู้ใช้รายอื่นได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เพียง 2 แบบ ได้แก่ แบบ DER และแบบ Base64 โดยแบบ DER สามารถนำไปใช้ได้กับโปรแกรมอีเมลไคลเอนต์เช่น Outlook Express

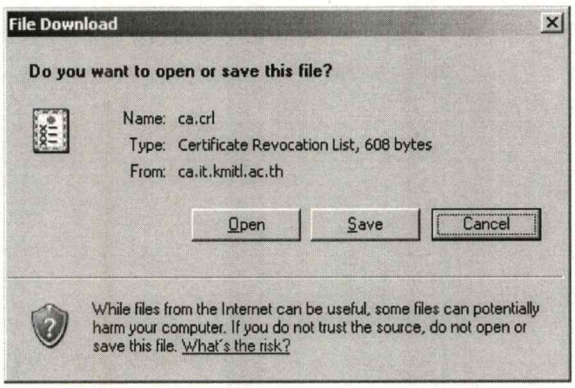


รูปที่ 5.17 หน้าจอแสดงรายการใบรับรองดิจิทัลของผู้ใช้จากการค้นหา

- **การดาวน์โหลดไฟล์รายการใบรับรองที่ถูกเพิกถอน (Download CRL)**

เมื่อผู้ใช้มีการดาวน์โหลดใบรับรองดิจิทัลของผู้ใช้รายอื่นไปใช้งานเพื่อสร้างความปลอดภัยในการติดต่อสื่อสาร ผู้ใช้จำเป็นต้องคอยปรับปรุงข้อมูลในเครื่องของผู้ใช้ให้ทราบถึงใบรับรองดิจิทัลที่ถูกยกเลิกด้วย เนื่องจากถ้าผู้ใช้ยังคงทำการสื่อสารกับผู้ใช้รายอื่นด้วยใบรับรองดิจิทัลที่ถูกเพิกถอน อาจทำให้การสื่อสารไม่เกิดความปลอดภัยได้ ผู้ใช้สามารถดาวน์โหลดไฟล์แสดงรายการใบรับรองดิจิทัลที่ถูกยกเลิกได้โดยใช้เมนู “Download CRL” ระบบจะแสดงหน้าจอให้ผู้ใช้ทำการบันทึกไฟล์ดังรูปที่ 5.18 จากนั้นผู้ใช้สามารถทำการติดตั้งไฟล์รายการใบรับรองที่ถูกเพิกถอนได้โดยการคลิ๊กขวาที่ไฟล์ และเลือกรายการ “Install CRL”

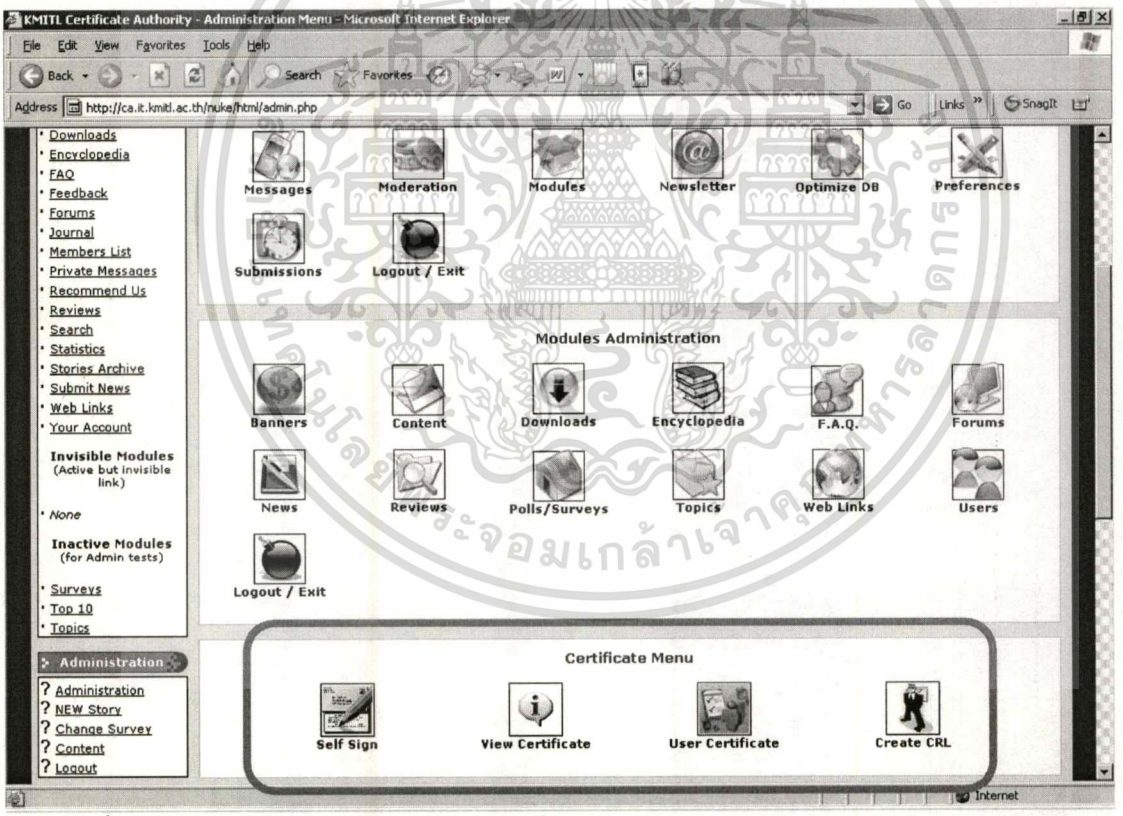
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.18 หน้าจอแสดงการดาวน์โหลดไฟล์แสดงรายการใบรับรองดิจิทัลของผู้ใช้ที่ถูกเพิกถอน

5.2.2 การใช้งานระบบในกรณีเป็นผู้ดูแลระบบ

เมื่อผู้ดูแลระบบเข้าสู่เมนูการทำงานหลักซึ่งแสดงดังรูปที่ 5.19 โดยจะมีเมนูการทำงานที่เกี่ยวกับใบรับรองดิจิทัลดัง ดังนี้



รูปที่ 5.19 หน้าจอแสดงเมนูในการทำงานเกี่ยวกับใบรับรองดิจิทัลในส่วนของผู้ดูแลระบบ

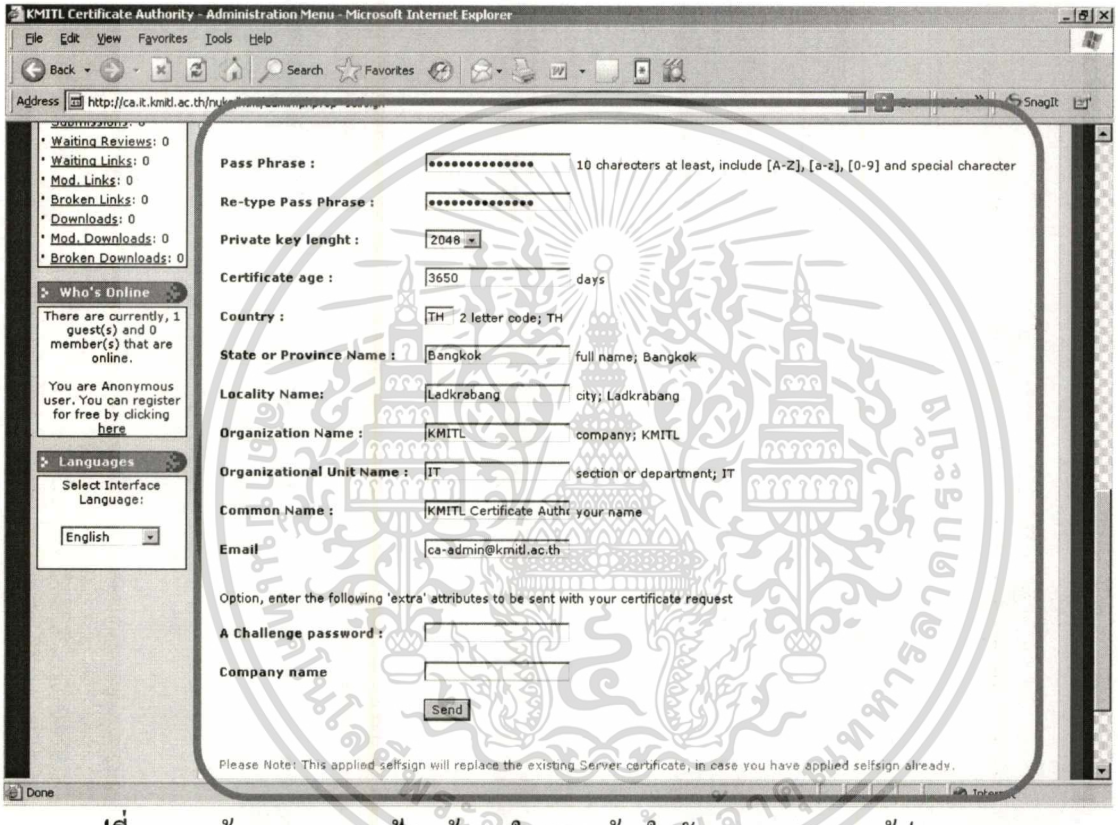
- **การสร้างใบรับรองตนเอง (Self Sign)**

ในการให้บริการออกใบรับรองดิจิทัลให้กับผู้ใช้นั้น ผู้ประกอบการจำเป็นที่จะต้องมีใบรับรองของผู้ประกอบการเองเสียก่อน ซึ่งใบรับรองของผู้ประกอบการนี้อาจได้มาจากการของ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ใบรับรองจากผู้ประกอบการออกใบรับรองดิจิทัลรายอื่น หรือการสร้างใบรับรองตนเอง (Self Sign) ในกรณีที่เป็นการใช้ภายในหน่วยงาน

ในกรณีที่ผู้ประกอบการต้องการสร้างใบรับรองตนเองนั้น สามารถทำได้โดยเข้าเมนู "Self Sign" ระบบจะแสดงหน้าจอให้ป้อนข้อมูลดังรูปที่ 5.20 ซึ่งในการสร้างใบรับรองตนเองนี้จะต้องมีการป้อนต่างๆ เช่นเดียวกับการขอใบรับรองดิจิทัลของผู้ใช้ทั่วไป แต่จะสามารถระบุขนาดของกุญแจส่วนตัว และอายุของใบรับรองได้



รูปที่ 5.20 หน้าจอแสดงการป้อนข้อมูลในการสร้างใบรับรองตนเองของผู้ประกอบการ

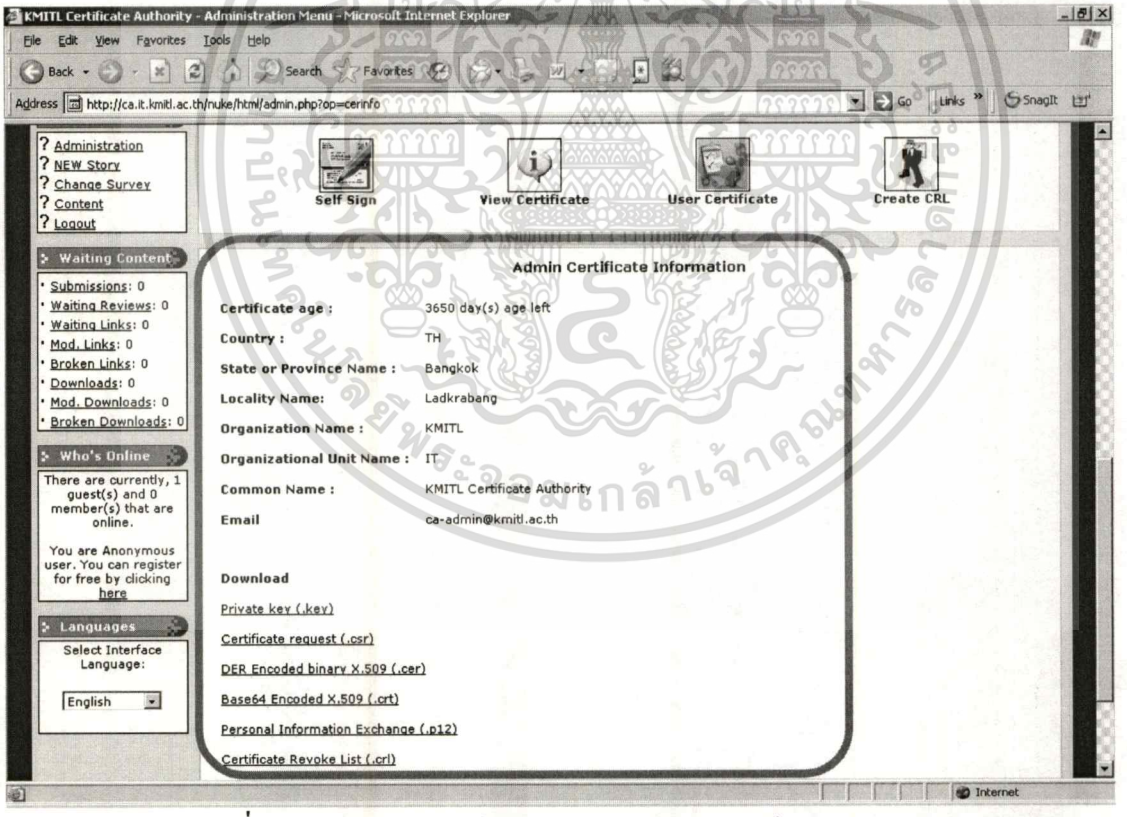
เมื่อผู้ดูแลระบบป้อนข้อมูลเรียบร้อยแล้วระบบจะทำการสร้างใบรับรองตนเองขึ้นทันที ในกรณีที่มีการสร้างใบรับรองตนเองอยู่ก่อนแล้วระบบจะทำการแทนที่ใบรับรองตนเองด้วยใบใหม่ซึ่งจะมีผลทำให้ใบรับรองใบดิจิทัลที่ระบบออกให้กับผู้ใช้ก่อนหน้าไม่ถูกต้อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- **การแสดงข้อมูลใบรับรองของ CA (View Certificate)**

ผู้ดูแลระบบสามารถแสดงรายละเอียดของใบรับรองดิจิทัลของผู้ประกอบการได้โดยการเข้าเมนู “View Certificate” ระบบจะแสดงหน้าจอดังรูปที่ 5.21 โดยในหน้าจอจะแสดงรายละเอียดของใบรับรองดิจิทัลและให้ผู้ดูแลระบบสามารถทำการดาวน์โหลดไฟล์ต่างๆ ได้แก่

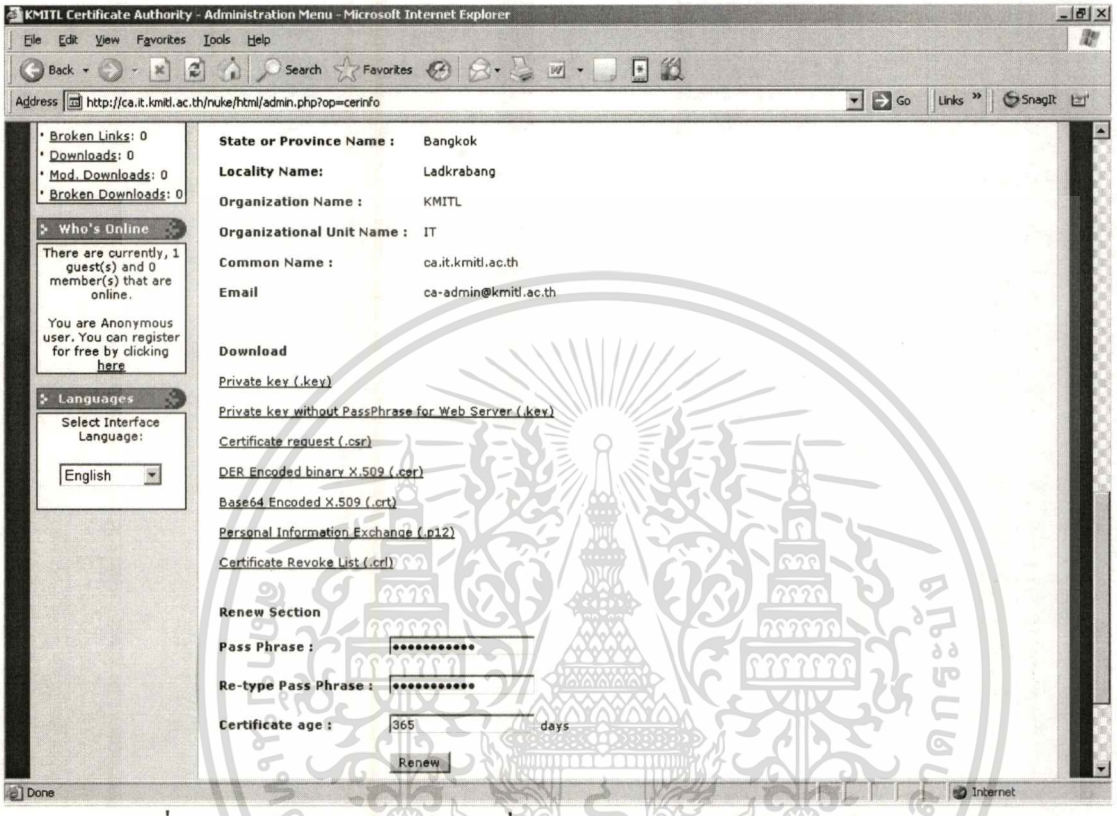
1. กุญแจส่วนตัว (Private key)
2. กุญแจส่วนตัวสำหรับเว็บเซิร์ฟเวอร์ (Private key without PassPhrase for Web Server)
3. ไฟล์คำร้องขอใบรับรอง (Certificate Signing Request)
4. ใบรับรองรูปแบบ DER (DER Encoded binary X.509)
5. ใบรับรองรูปแบบ Base64 (Base64 Encoded X.509)
6. ใบรับรองรูปแบบ PKCS12 (Personal Information Exchange)
7. ไฟล์รายการใบรับรองดิจิทัลที่ถูกเพิกถอน (Certificate Revoke List)



รูปที่ 5.21 หน้าจอแสดงข้อมูลใบรับรองดิจิทัลของผู้ประกอบการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในกรณีที่ใบรับรองของผู้ประกอบการหมดอายุหรือใกล้หมดอายุ ระบบจะแสดงส่วนของการต่ออายุใบรับรองดังรูปที่ 5.22 โดยผู้ดูแลระบบจะต้องป้อนรหัสลับ (Pass Phrase) และอายุของใบรับรองที่ต้องการต่อ



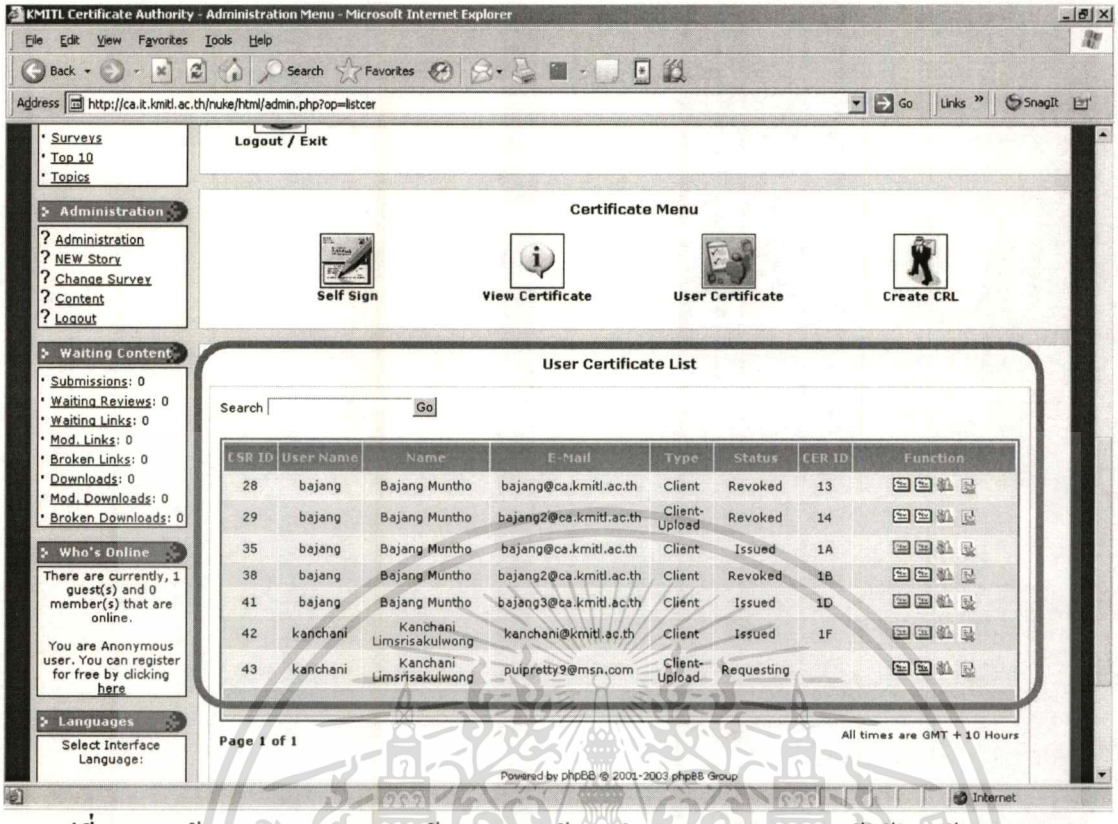
รูปที่ 5.22 หน้าจอการป้อนข้อมูลเพื่อต่ออายุใบรับรองดิจิทัลของผู้ประกอบการ

- **การแสดงรายการใบรับรองของผู้ใช้ (User Certificate)**

ผู้ดูแลระบบสามารถเรียกดูรายการการร้องขอใบรับรองและสถานะของใบรับรองดิจิทัลของผู้ใช้ทั่วไปที่มีอยู่ในระบบได้โดยเข้าเมนู "User Certificate" ระบบจะแสดงข้อมูลของรายการคำร้องขอ ได้แก่ หมายเลขคำร้องขอ ชื่อผู้ใช้ในระบบ ชื่อ อีเมล รูปแบบการร้องขอ สถานะ หมายเลขใบรับรองดิจิทัล ดังรูปที่ 5.23 และมีฟังก์ชันย่อยให้ผู้ดูแลระบบใช้งานดังนี้

1. ดาวน์โหลดใบรับรองดิจิทัลแบบ DER (DER Encoded Binary X.509)
2. ดาวน์โหลดใบรับรองดิจิทัลแบบ Base64 (Base64 Encoded X.509)
3. การเพิกถอนใบรับรองโดยไม่ต้องไม่มีการยืนยันจากผู้ใช้ (Revoke Certificate)
4. การลบข้อมูลออกจากระบบ (Delete)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.23 หน้าจอแสดงรายการคำร้องขอและข้อมูลใบรับรองดิจิทัลของผู้ใช้โดยผู้ดูแลระบบ

- **การสร้างไฟล์รายการใบรับรองดิจิทัลที่ถูกเพิกถอน (Create CRL)**

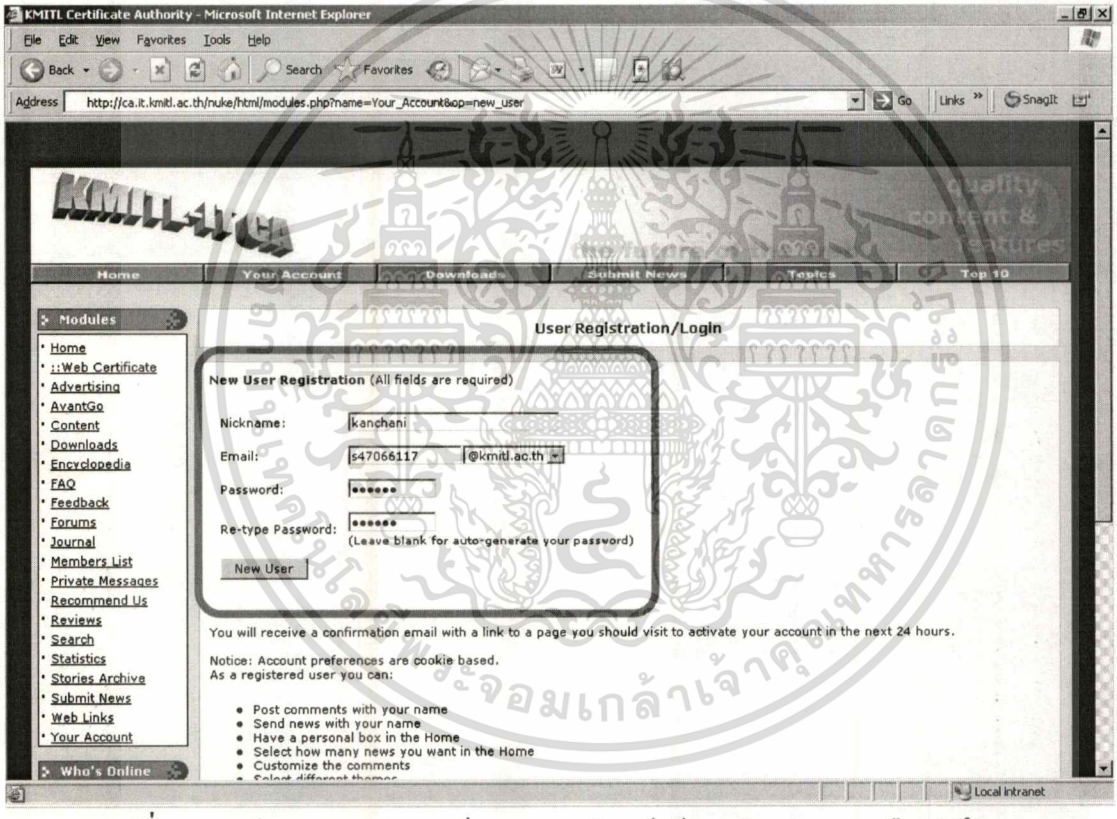
ผู้ดูแลระบบสามารถสร้างไฟล์รายการใบรับรองดิจิทัลที่ถูกเพิกถอนได้โดยการเข้าเมนู "Create CRL" การทำในลักษณะนี้จะเป็นการสร้างไฟล์เพียงเฉพาะเมื่อผู้ดูแลระบบต้องการให้มีการปรับปรุงไฟล์แบบฉุกเฉิน เนื่องการสร้างไฟล์นี้จะสามารถสร้างได้โดยผ่านการรันไฟล์ "overall.bat" ซึ่งผู้ดูแลระบบ จะต้องทำการตั้งโปรแกรม "Window Scheduler" ให้ทำงานเป็นรอบๆ โดยอาจตั้งให้รันทุกสัปดาห์ หรือทุกวัน หรือวันละมากกว่า 1 เวลาได้

การตั้งการทำงานของไฟล์ "C:\apache\htcocs\nuke\html\overall.bat" ผ่านโปรแกรม "Window Scheduler" ได้โดยการเรียก "Start->Settings...->Control Panel->Scheduled Tasks->Add Scheduled Task" และเมื่อไฟล์ "overall.bat" มีการเรียกทำงานจะมีการบันทึกการทำงานไว้ที่ไฟล์ "C:\apache\htdocs\nuke\html\overall.log"

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.3. การประยุกต์ใช้งานระบบเพื่อให้บริการออกใบรับรองดิจิทัลแก่บุคลากรและนักศึกษาในมหาวิทยาลัยลาดกระบัง

การใช้งานระบบผู้ให้บริการใบรับรองดิจิทัลที่กล่าวข้างต้น เป็นการเปิดให้ใช้งานได้สำหรับผู้ใช้ทั่วๆ ไป ซึ่งในกรณีที่ต้องการให้ใช้งานได้เฉพาะผู้ที่เป็นบุคลากร หรือเป็นนักศึกษาของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง สามารถทำได้โดยการประยุกต์ขั้นตอนในการลงทะเบียน ซึ่งจากเดิมผู้ใช้สามารถใช้อีเมลแอดเดรสจากหน่วยงานอื่นๆ ในการลงทะเบียนได้ เปลี่ยนเป็นบังคับให้ผู้ใช้จำเป็นต้องใช้อีเมลที่มีแอดเดรสเป็นของทางสถาบันฯ เท่านั้นโดยแสดงดังรูปที่ 5.24



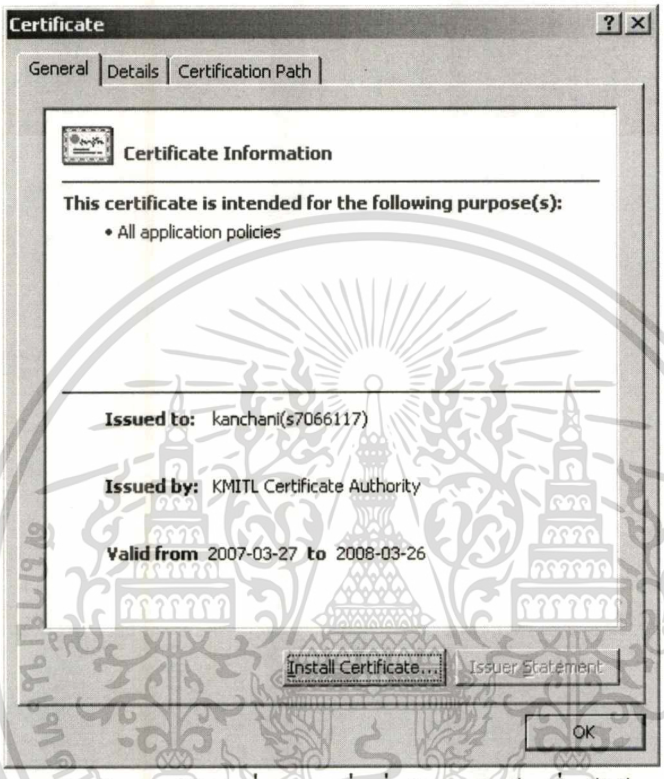
รูปที่ 5.24 หน้าจอแสดงประยุกต์การลงทะเบียนผู้ใช้สำหรับบุคลากรหรือนักศึกษา

จากการประยุกต์ดังกล่าวผู้ใช้จะต้องเลือกแอดเดรสของอีเมลจากรายการที่เตรียมไว้ให้เท่านั้น จึงทำให้ผู้ที่มีสิทธิ์ที่ลงทะเบียนจะต้องเป็นเพียงบุคลากร หรือนักศึกษาของทางสถาบันฯ เท่านั้น เนื่องจากบุคคลภายนอกจะไม่สามารถมีอีเมลแอดเดรสของทางสถาบันได้

จากขั้นตอนของการร้องขอใบรับรองดิจิทัลจากรูปที่ 5.8 ผู้ใช้สามารถกรอกข้อมูลในส่วนของชื่อผู้ใช้ (Common Name) ได้ตามที่ต้องการ จึงทำให้ใบรับรองดิจิทัลสามารถระบุตัวบุคคลของ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ผู้ใช้ได้ ในส่วนนี้ต้องนำชื่ออีเมลของผู้ใช้ที่ได้รับจากขั้นตอนการลงทะเบียนมาเป็นข้อมูลส่วนหนึ่งของใบรับรอง เช่น เมื่อผู้ใช้ป้อนชื่อผู้ใช้เป็น “kanchani” ระบบจะทำการเพิ่ม “(s47066117)” ต่อท้ายให้โดยอัตโนมัติ ดังนั้นข้อมูลในใบรับรองดิจิทัลของผู้ใช้รายนี้จะมีชื่อผู้ใช้เป็น “kanchani(s47066117)” ดังแสดงในรูปที่ 5.25



รูปที่ 5.25 ภาพแสดงใบรับรองดิจิทัลที่ระบบเพิ่มชื่ออีเมลต่อท้ายชื่อผู้ใช้ (Common Name)

หลังจากที่ได้ทำการร้องขอใบรับรองเป็นอันสำเร็จเรียบร้อยแล้ว ผู้ใช้จะสามารถเข้าใช้งานต่างๆ ของระบบได้เหมือนกับการใช้งานของผู้ใช้ทั่วๆ ไปตามที่ได้กล่าวมาแล้วข้างต้น

จากการประยุกต์ใช้งานการเป็นผู้ให้บริการออกใบรับรองดิจิทัลของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เป็นการนำเอาระบบที่พัฒนาขึ้นมานี้เข้ามาช่วยในการติดต่อสื่อสารระหว่างบุคลากรหรือนักศึกษาภายในสถาบัน ซึ่งนอกจากข้อมูลจะมีความปลอดภัยแล้วยังทำให้เราสามารถมั่นใจได้ว่าบุคคลากรหรือนักศึกษาที่เรากำลังติดต่ออยู่ด้วยนั้นมีตัวตนอยู่จริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 6

บทสรุปและแนวทางในการพัฒนาระบบในอนาคต

6.1 สรุปผลการทำงานของระบบ

จากการทำงานของระบบผู้ประกอบการออกใบรับรองดิจิทัล (Certificate Authority) สรุปได้ว่าระบบสามารถทำหน้าที่เปรียบเสมือนเป็นหน่วยงานหนึ่งในการออกใบรับรองให้แก่บุคคลทั่วไปได้ เพื่อเป็นการสร้างความเชื่อมั่นและความปลอดภัยในการติดต่อสื่อสารระหว่างผู้ที่ต้องการทำธุรกรรมผ่านเครือข่าย โดยระบบจะทำการตรวจสอบข้อมูลของผู้ที่เข้ามาร้องขอใบรับรองดิจิทัลก่อนที่จะมีการอนุมัติออกใบรับรองพร้อมทั้ง สร้างกุญแจลับ (Private Key) และกุญแจสาธารณะ (Public Key) เพื่อให้ผู้ใช้สามารถทำการดาวน์โหลดไปใช้ในการเข้ารหัสถอดรหัสข้อมูลในการส่งอีเมล นอกจากนี้ระบบยังให้ผู้ใช้บริการที่เป็นสมาชิกของระบบสามารถทำการดาวน์โหลดใบรับรองของบุคคลอื่นที่ต้องการติดต่อสื่อสารด้วย และสามารถทำการเพิกถอนหรือต่ออายุใบรับรองได้

6.2 ปัญหาและแนวทางในการแก้ไขระบบ

ปัญหาที่จะพบของระบบคือ

1. ระบบนี้สร้างขึ้นเพื่อเป็นกรณีศึกษาระบบสามารถทำได้แค่จำลองการติดต่อสื่อสารของเซิร์ฟเวอร์และไคลเอนท์ภายในคอมพิวเตอร์เครื่องเดียวกัน ซึ่งในการนำมาใช้งานจริงระบบอาจจะต้องทำการแยกเซิร์ฟเวอร์และไคล์เอนท์ออกจากกัน หรือตัวระบบจะต้องมีความซับซ้อนมากขึ้น
2. ระบบยังสามารถดำเนินการออกใบรับรองเฉพาะส่วนบุคคลเท่านั้น ซึ่งในการดำเนินการจริงเราสามารถที่จะพัฒนาเพื่อออกใบรับรองเครื่องแม่ข่ายหรือใบรับรองอุปกรณ์ ได้อีกด้วย

6.3 อนาคตและการพัฒนาของระบบ

ในอนาคตคาดว่าระบบผู้ประกอบการออกใบรับรองดิจิทัลจะสามารถนำมาใช้งานได้อย่างแพร่หลาย เนื่องจากเป็นระบบที่พัฒนาขึ้นจากส่วนหนึ่งของโปรแกรมที่เป็นโอเพ่นซอร์ส จึงเป็นการลดค่าใช้จ่ายภายในองค์กรที่มีความต้องการใช้ใบรับรองเพื่อรักษาความปลอดภัยของข้อมูลที่มีติดต่อสื่อสารกัน และสามารถให้บริการออกใบรับรองให้แก่องค์กรหรือบุคคลภายนอกได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แนวทางในการพัฒนาอาจจะมีอัลกอริทึมในการเข้ารหัสข้อมูลที่มีประสิทธิภาพมากกว่าเดิมมาประยุกต์ใช้กับแอพลิเคชันที่เกี่ยวข้องกับความปลอดภัยของข้อมูลในด้านอื่นๆ ได้มากขึ้น รวมทั้งยังสามารถดำเนินการออกใบรับรองในรูปแบบต่างๆ ได้เพื่อให้เกิดความหลากหลายในการทำธุรกรรมบนอินเทอร์เน็ตได้อย่างปลอดภัย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

กิตติ ภักดีวัฒนะกุล, อังศุมาลิน เวชนารายณ์, กิตติพงษ์ ธีรวัฒน์เสถียร. 2545. **PHP : ฉบับโปรแกรมเมอร์.** กรุงเทพมหานคร : เคทีพี คอมพ์ แอนด์ คอนซัลท์.

ณัฐภัชร ณ เขาวงกต. 2546. **PHP+MySQL = PHP-Nuke สร้างเว็บได้โดยไม่ต้องเขียนสคริปต์เอง.** กรุงเทพมหานคร : วิตตี้ กรุ๊ป.

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

บริษัท เอ็ม เอ เอส เน็ตเวิร์ค จำกัด. 2547. **การรักษาความปลอดภัย (ภัยคุกคาม และเทคโนโลยีการป้องกัน).** [Online]. เข้าถึงได้จาก : http://www.viewthailand.com/3.asp.

มหาวิทยาลัยราชภัฏสวนดุสิต. 2547. **การสื่อสารข้อมูลคอมพิวเตอร์ และระบบเครือข่าย.** [Online]. เข้าถึงได้จาก : http://dusithost.dusit.ac.th/~phitsanulok/e-learning/Ch96.htm.

วศิน เพิ่มทรัพย์. 2544. **กลไกการทำงานของ Digital Signature.** [Online]. เข้าถึงได้จาก : http://www.provision.co.th/pcdirect/index.php?itemid=64&catid=6.

สงกรานต์ ทองสว่าง. 2544. **MySQL ระบบฐานข้อมูลสำหรับอินเทอร์เน็ต.** กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น.

สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ. 2547. **วงจรการใช้งานใบรับรองอิเล็กทรอนิกส์.** [Online]. เข้าถึงได้จาก : http://gca.thaigov.net/content/intro0.php.

Apache Software Foundation. 2005. **Apache HTTP Server Version 2.2 Documentation.** [Online]. Available : http://httpd.apache.org/docs/2.2/.

ArGo Software Design. 2005. **ArGoSoft 1.8.8.8.** [Online]. Available : http://www.argosoft.com/RootPages/MailServer/Default.aspx.

MySQL AB. 2005. **MySQL 5.0.20.** [Online]. Available : http://www.mysql.com/.

OpenSSL Project. 2005. **OpenSSL 0.98b.** [Online]. Available : http://www.openssl.org/source/.

PHP Group. 2005. **PHP 5.2.** [Online]. Available : http://www.php.net/.

PHP Nuke Org. 2005. **PHP-Nuke 7.8.** [Online]. Available : http://www.phpnuke.org/.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้