ระบบการจองตั๋วภาพยนตร์ผ่านโทรศัพท์มือถือโดยอาศัยความปลอดภัยแบบ PKI

Cinema Booking System on Mobile Phones with PKI Security

โดย

นายอุดมพร ชุมใหม่

รหัส 44067087

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงงานพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2545

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	ระบบการจองตั๋วภาพยนตร์ผ่านโทรศัพท์มือถือโดยอาศัยความปลอดภัยแบบ PKI
นักศึกษา	นายอุดมพร ชุมใหม่
อาจารย์ที่ปรึกษา	ดร.จันทร์บูรณ์ สถิตวิริยวงศ์
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2545

บทคัดย่อ

ในปัจจุบันมีการใช้งานโทรศัพท์มือถือกันมากขึ้น และมีแนวโน้มมากขึ้นเรื่อย ๆ ในอนาคต โดยมีการนำการทำธุรกรรมหลาย ๆ อย่างมาประยุกต์มาทำงานบนระบบโทรศัพท์มือถือมากขึ้นด้วย เช่น ระบบการรายงานหุ้นออนไลน์ การจองตั๋วชมภาพยนตร์ออนไลน์ เป็นต้น ซึ่งทำให้ผู้ใช้สะดวกในการใช้งานมากขึ้น ดังนั้นในโครงงานนี้จึงมีการประยุกต์ระบบการจองตั๋วชมภาพยนตร์ขึ้นมาใช้งานบนระบบโทรศัพท์มือถือ พร้อมกับการใช้งานระบบความปลอดภัยแบบ PKI เพื่อให้ผู้ใช้มั่นใจในการใช้งานระบบมากขึ้นในการใช้หมายเลขบัตรเครดิตในการทำการจองตั๋วภาพยนตร์

Title	Cinema Booking System on Mobile Phones with PKI Security
Student	Mr. Udomporn Chummai
Advisor	Dr. Chanboon Satitviriyawong
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2002

ABSTRACT

Nowadays, mobile phones technology is widely used and it has the trend to be increased in the future. It brings many businesses to be operated within mobile phone such as stock online report, online ticketing service, etc. which is convenient and friendly for users. Ticketing system is brought to operate on mobile system with PKI security system in this project. User will convince to give the credit card number to reserve the ticket in the system.

กิตติกรรมประกาศ

ขอขอบคุณ คุณพ่อ คุณแม่ คุณยายและน้อง ๆ ที่ให้กำลังใจ และเป็นแรงใจตลอดมา

ขอขอบคุณ ดร.จันทร์บูรณ์ สถิตวิริยวงศ์ ที่ได้ให้คำแนะนำ คำชี้แนะ และเป็น Advisor มาตั้งแต่สัมมนา 1 สัมมนา 2 และวิชาโครงงานพัฒนาระบบงาน

ขอขอบคุณเพื่อน ๆ พี่ ๆ น้อง ๆ ที่ให้ความช่วยเหลือเป็นอย่างดีทั้งคำแนะนำดี ๆ ความรู้ใหม่ ๆ และสิ่งอื่น ๆ อีกหลาย ๆ อย่าง รวมทั้งให้ความสนใจในเรื่องที่ผมได้นำเสนอด้วย

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

ตารางที่

สารบัญรูป

หน้า

รูปที่

สารบัญรูป (ต่อ)

หน้า

รูปที่

บทที่ 1
บทนำ

1.1 เครือข่าย Internet และเครือข่าย Wireless

ปัจจุบันเครือข่ายอินเทอร์เน็ตได้เจริญเติบโตและมีอัตราการใช้งานเพิ่มขึ้นอย่างรวดเร็ว ทั้งในด้านการค้นคว้าวิจัย การสืบค้นหาข้อมูลที่ต้องการ การทำการค้า การทำธุรกรรมด้านการเงินต่าง ๆ แต่ยังมีข้อจำกัดก็คือการใช้งานยังขึ้นอยู่กับสถานที่ คือต้องมีการใช้เครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์กระเป๋าหิ้ว แล้วต้องมีโมเด็ม สายโทรศัพท์ หรือการ์ดแลน กับสายแลน ซึ่งจะไม่ค่อยสะดวกนักถ้าผู้ใช้มีการเดินทางบ่อย หรือต้องการใช้งานในการค้นหาข้อมูลในบางสถานที่ ดังนั้นนี้เป็นเหตุผลหนึ่งที่ได้เริ่มใช้งานระบบเครือข่ายแบบ Wireless มากขึ้น อีกทั้งเป็นผลมาจากการที่มีการใช้งานและมีการพัฒนาระบบโทรศัพท์มือถือ หรืออุปกรณ์ไร้สายให้มีประสิทธิภาพดีขึ้นเพื่อรองรับการทำงานบางประเภทตามที่ต้องการได้ ซึ่งอุปกรณ์ไร้สายนั้นสามารถใช้งานได้ไม่จำกัดสถานที่ จึงสะดวกต่อการใช้งานมากขึ้น

ดังนั้นอนาคตจึงมีแนวโน้มในการใช้งานระบบเครือข่าย Wireless เพิ่มขึ้น รวมทั้งมีการปรับปรุงระบบบางระบบที่ใช้งานบนระบบอินเทอร์เน็ตให้สามารถทำงานบนระบบเครือข่ายแบบ Wireless ได้อีกด้วยเช่นระบบ E-Commerce เป็นต้น

1.2 Electronic Commerce และ Mobile Commerce

ธุรกิจแบบ E-Commerce เกิดขึ้นในช่วงประมาณปี 2542-2543 เป็นจำนวนมาก ซึ่งเกี่ยวกับการค้าขายสินค้าแบบต่าง ๆ หรือการสั่งซื้อบริการแบบต่าง ๆ ซึ่งเป็นที่นิยมกันแบบอย่างมาก ข้อดีคือผู้ที่ต้องการขายสินค้าลงทุนในการขายสินค้าน้อยลง สามารถให้รายละเอียดของสินค้าได้ง่ายขึ้น ซึ่งทำให้ค่าใช้จ่ายโดยรวมน้อยลง และผู้ที่ต้องการซื้อสินค้าก็สะดวกในการเลือกซื้อสินค้าด้วย และก็ได้มีการปรับเปลี่ยนหรือเพิ่มเติมส่วนต่าง ๆ เพื่อให้สามารถให้สามารถใช้งานบนระบบเครือข่ายแบบ Wireless เช่น โทรศัพท์มือถือ หรือ PDA ต่าง ๆ ได้ เพื่ออำนวยความสะดวกแก่ผู้ใช้งานเพิ่มขึ้น ซึ่งเรียกว่า Mobile Commerce

แต่ในปัจจุบันความนิยมในการซื้อขายสินค้าผ่านระบบเครือข่ายแบบ E-Commerce หรือ M-Commerce ลดน้อยลงเพราะเรื่องของความปลอดภัยที่เกิดขึ้นในการทำธุรกรรมนั้นเอง ซึ่งอาจเกิดจากความไม่สามารถรับรองบุคคลที่ทำธุรกรรมได้ ความปลอดภัยในการใช้บัตรเครดิตในการซื้อสินค้า การไม่ยอมรับในการทำธุรกรรมที่ตนเองได้ทำรายการนั้นไว้ ความไม่ถูกต้องของข้อมูล

เป็นต้น ดังนั้นระบบความปลอดภัยที่ต้องการในการทำธุรกรรมจึงเป็นสิ่งที่จำเป็นมาก ซึ่งในปัจจุบันได้มีการนำวิธีการที่เรียกว่า PKI (Public Key Infrastructure) มาให้ในระบบ E-Commerce รวมทั้งได้มีประยุกต์มาใช้งานบนระบบ Wireless อีกด้วย

1.3 วัตถุประสงค์และขอบเขตของโครงงาน

วัตถุประสงค์ของโครงงานนี้เพื่อออกแบบและพัฒนาระบบการจองตั๋วภาพยนตร์ผ่านโทรศัพท์มือถือ โดยอาศัยความปลอดภัยแบบ PKI โดยมีการจำลองระบบการจองตั๋วภาพยนตร์ผ่านโทรศัพท์มือถือ และจำลองระบบความปลอดภัยแบบ PKI ที่ใช้บนระบบโทรศัพท์มือถือ เพื่อให้เห็นถึงหลักการทำงานของ M-Commerce และระบบความปลอดภัยแบบ PKI คร่าว ๆ และแสดงให้เห็นถึงแนวทางในการพัฒนาระบบ M-Commerce เพื่อประยุกต์ในการใช้งานจริงในอนาคตต่อไป

โดยมีขอบเขตของโครงงานดังนี้

1.3.1 ออกแบบโครงสร้างของระบบจองตั๋วภาพยนตร์ผ่านโทรศัพท์มือถือ โดยจะแสดงผลผ่านทางระบบที่พัฒนาบนมาตรฐานของ WAP

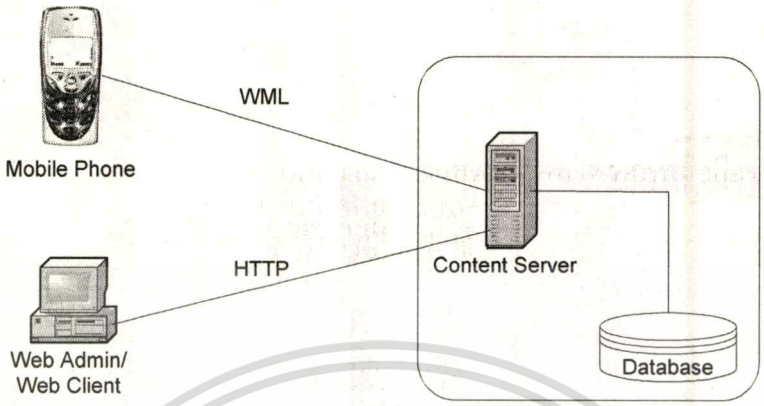
1.3.2 ออกแบบและจำลองระบบความปลอดภัยแบบ PKI ที่ใช้งานบนระบบโทรศัพท์มือถือ

1.3.3 พัฒนาเพื่อจำลองระบบการจองตั๋วภาพยนตร์ผ่านโทรศัพท์มือถือ โดยสามารถค้นหา และจองตั๋วภาพยนตร์ที่ต้องการได้ ตามที่ต้องการได้

1.3.4 พัฒนาระบบการจัดการข้อมูลเกี่ยวกับภาพยนตร์ การจองภาพยนตร์ เช่นการเพิ่ม-ลดรอบฉาย การเพิ่ม-ลบชื่อภาพยนตร์ รายละเอียดของภาพยนตร์ เป็นต้น

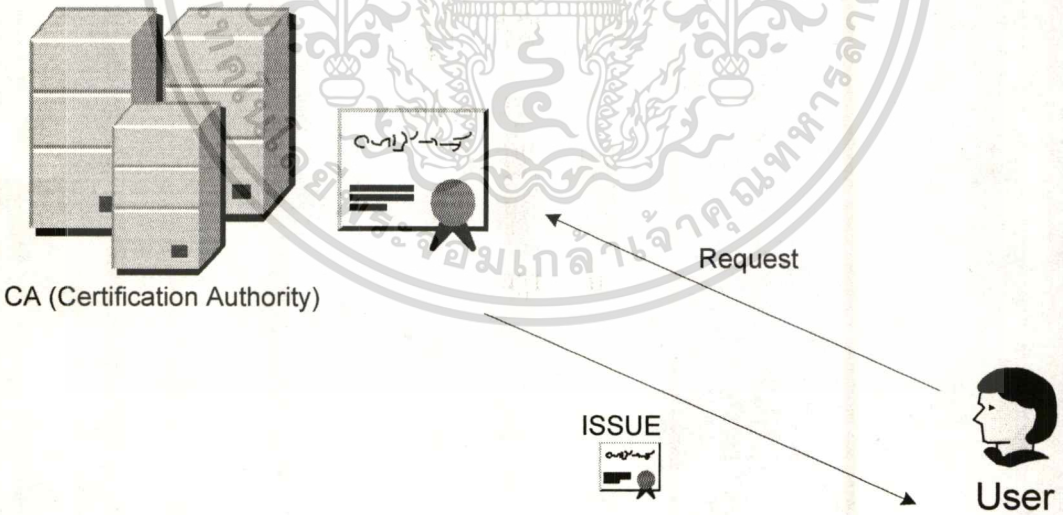
1.4 แนวความคิดของโครงงาน

รูปแบบการทำงานของระบบที่เป็นแอพพลิเคชันจะทำงานในลักษณะแบบไคลเอนท์และเซิร์ฟเวอร์ (Client-Server) โดยจะมีการทำงานเป็น 2 ส่วนคือ ส่วนแรกจะเป็นแบบเซิร์ฟเวอร์ ที่ทำหน้าที่ในการให้บริการหรือเกี่ยวกับการจัดการข้อมูลที่เป็น Database Server Web หรือ WAP Server ส่วนที่สองเป็นส่วนไคลเอนท์ ที่พัฒนามาเพื่อแสดงผลบนโทรศัพท์มือถือของผู้ใช้ ซึ่งเพื่อให้สามารถเรียกใช้ข้อมูล เพิ่มข้อมูล ลบข้อมูล และแก้ไขข้อมูลได้ตามที่ผู้ใช้ต้องการ ซึ่งระบบได้ถูกออกแบบมาเพื่อให้เหมาะสมกับการทำงาน หรือการใช้งานของผู้ใช้ ดังรูปที่ 1.1



รูปที่ 1.1 แสดงรูปแบบการทำงาน

รูปแบบการทำงานของระบบที่เป็นระบบความปลอดภัยแบบ PKI จะเป็น 2 ส่วนเช่นกัน คือ เซิร์ฟเวอร์คือผู้ออกใบรับรอง หรือผู้รับรอง (CA) ส่วนที่สองเป็นไคล์เอนท์คือผู้ที่ขอใบรับรอง หรือผู้ที่ได้รับการรับรอง (User) ดังรูปที่ 1.2

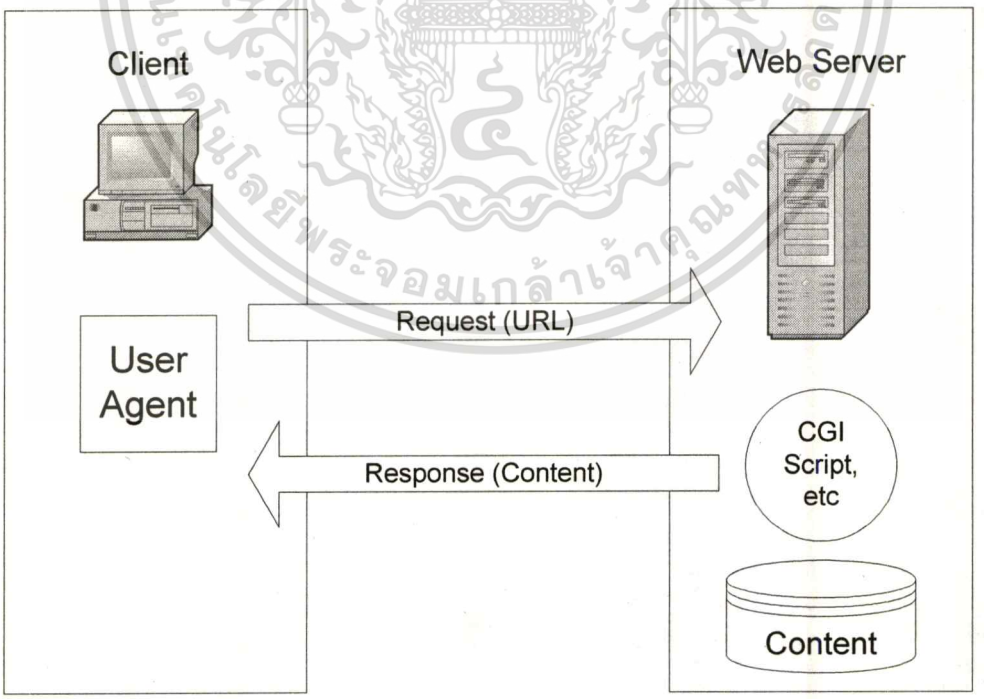


รูปที่ 1.2 แสดงรูปแบบการขอใบรับรอง

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 World Wide Web Model

ระบบเครือข่ายอินเทอร์เน็ตได้มีการใช้งานกันเป็นเวลาหลายปีแล้วและอัตราการขยายตัวการใช้งานก็ได้เพิ่มขึ้นอย่างรวดเร็ว รวมทั้งมีการพัฒนาความสามารถของระบบอินเทอร์เน็ตมากขึ้นอีกด้วย จึงทำให้สามารถในการรองรับการพัฒนาระบบที่สามารถใช้งานได้บนอินเทอร์เน็ต และพัฒนาต่อไปเรื่อย ๆ จนมีเรียกว่า E-Commerce ต่อมาเมื่อการปรับปรุงเครือข่ายโทรศัพท์เคลื่อนที่ให้ดีขึ้น อัตราการใช้งานโทรศัพท์มือถือก็เพิ่มสูงขึ้นด้วย ดังนั้นระบบอินเทอร์เน็ตจึงเริ่มใช้งานกันบนระบบโทรศัพท์เคลื่อนที่ด้วย จึงเป็นที่มาของ M-Commerce โดยในระบบอินเทอร์เน็ตก็มีการใช้งานบนเครือข่ายที่เรียกว่า World Wide Web ที่มีโครงสร้างพื้นฐานคือ มี World Wide Web Server และ Client (Browser) จะมีโปรโตคอล TCP/IP เป็นหลักในการทำงาน โดยจะแสดงในรูปที่ 2.1

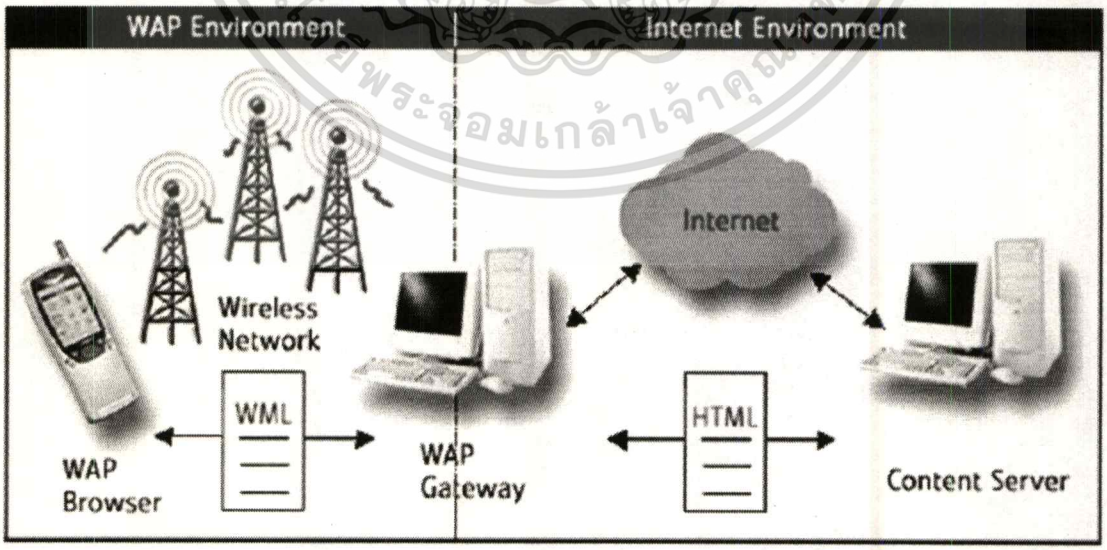


รูปที่ 2.1 แสดง World Wide Web Model

2.2 WAP

ยุคของการใช้งานเครื่องคอมพิวเตอร์ในปัจจุบันได้เพิ่มมากขึ้นอย่างมาก และรวดเร็ว ในยุคนี้เองก็ได้เริ่มมีการใช้งานระบบโทรศัพท์มือถือหรืออุปกรณ์ไร้สายเพิ่มมากขึ้นอย่างรวมเร็วเช่นเดียวกัน จะเห็นได้ว่ายุคนี้จึงเป็นยุครอยต่อสำคัญของเทคโนโลยี เพราะเป็นการเริ่มเปลี่ยนแปลงจากการใช้งานเครื่องคอมพิวเตอร์เพียงอย่างเดียว มาเป็นการรวมเอาอุปกรณ์ไร้สายอื่น ๆ เข้ามาในระบบการสื่อสารข้อมูลอื่น ๆ ด้วย นอกจาก WAP แล้ว ยังมีเทคโนโลยีสื่อสารไร้สายแบบอื่น ๆ ที่เป็นทางเลือกเพิ่มเติมอีก ที่เห็นชัดคือ I-Mode และ Bluetooth แต่ WAP ก็ได้รับการตอบรับมากขึ้นเพราะว่าเป็นเทคโนโลยีเปิดหรือเป็นระบบเปิด ที่ได้รับการพัฒนามาอย่างต่อเนื่อง และพัฒนาต่อไปในอนาคต โดยจะมีกลุ่มบริษัทผู้ผลิตและจำหน่ายอุปกรณ์มือถือ ผู้ผลิตซอฟต์แวร์ที่เรียกว่า WAP Forum ซึ่งปัจจุบันได้ได้พัฒนามาเรื่อยตั้งแต่ WAP 1.1 WAP 1.2 WAP 1.3 และ WAP 2.0 ที่กำลังพัฒนาอยู่ในปัจจุบัน (WAP forum. 2001)

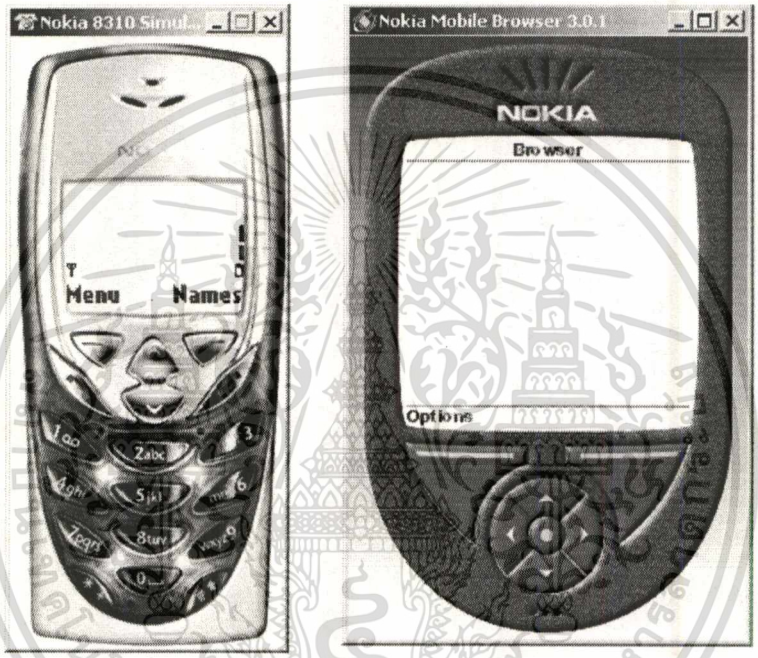
WAP (Wireless Application Protocol) เป็นโปรโตคอลหรือเป็นข้อกำหนดในการสื่อสารในเครือข่ายแบบไร้สาย หรือโทรศัพท์มือถือ โดยการใช้งานโทรศัพท์มือถือให้สามารถใช้งาน WAP ได้นั้นจำเป็นต้องมี WAP Gateway เพราะว่าระบบโทรศัพท์มือถืออยู่บนระบบเครือข่ายแบบไร้สาย แต่ข้อมูล WAP Site ที่ต้องการอยู่ในเครือข่ายอินเทอร์เน็ต ซึ่งเครือข่ายทั้งสองเป็นคนละระบบกัน จึงต้องอาศัย WAP Gateway เป็นตัวกลางในการเชื่อมต่อ เพื่อจะได้แลกเปลี่ยนข้อมูลกันได้ ดังรูปที่ 2.2



รูปที่ 2.2 แสดงส่วนประกอบของ WAP-internet Environment

การใช้งาน WAP จำเป็นต้องมีโปรแกรมที่ใช้แสดงผลบนโทรศัพท์มือถือคือโปรแกรม WAP Browser หรือ WAP Emulator

- WAP Browser เป็นซอฟต์แวร์ที่ทำงานในเครื่องพีซี ลักษณะหน้าตาจะเหมือน Browser อย่าง IE หรือ Netscape ถ้าบนระบบโทรศัพท์มือถืออาจเรียกว่า Micro Browser
- WAP Emulator เป็นซอฟต์แวร์ที่ทำงานในเครื่องพีซี แต่จะแสดงการจำลองโทรศัพท์มือถือจริง ๆ ดังรูปที่ 2.3 (Nokia forum. 2002)



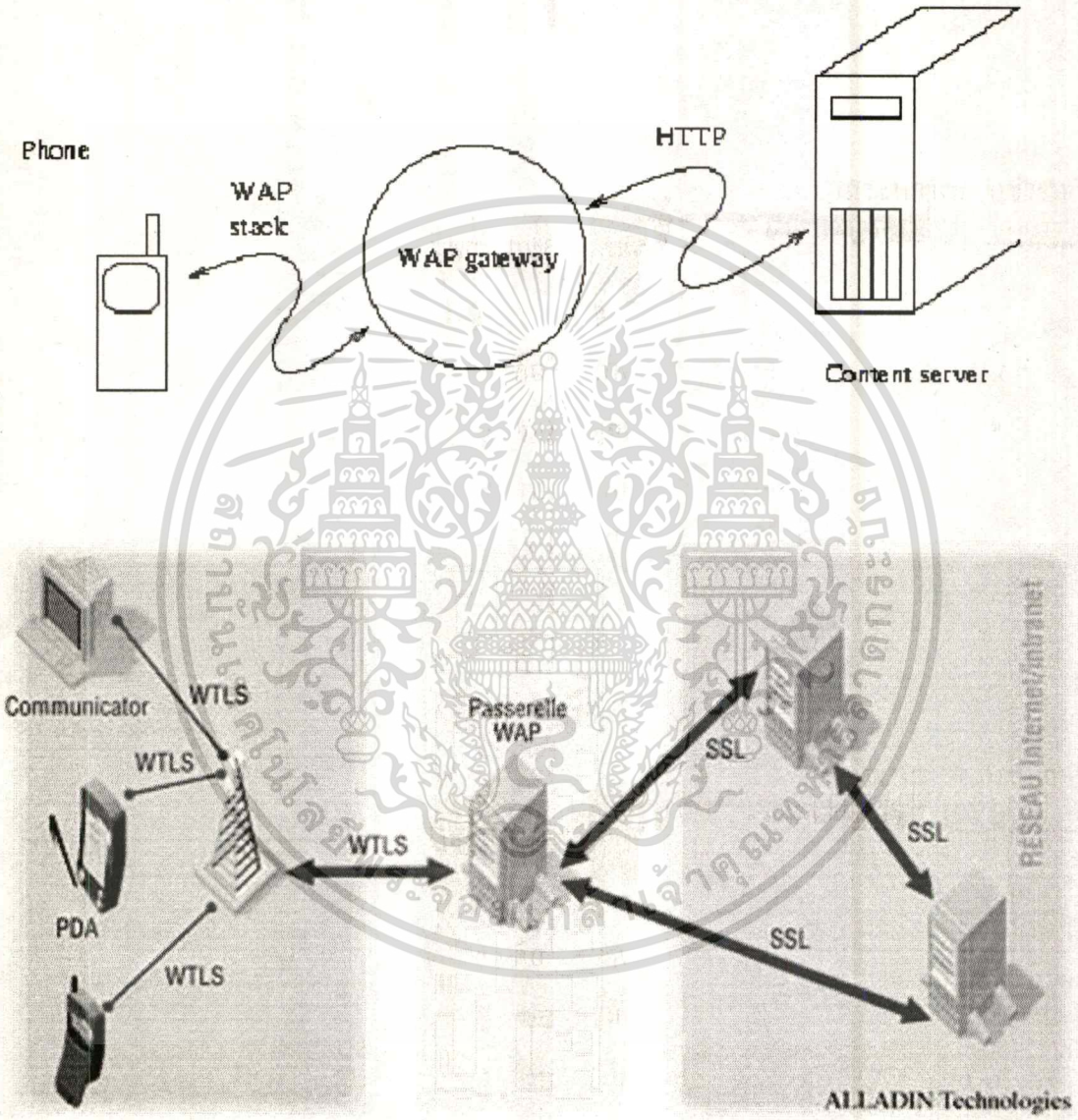
รูปที่ 2.3 แสดง WAP Emulator

2.2.1 ส่วนประกอบของ WAP (Wireless Application Protocol)

โดยมาตรฐานของ WAP จะต้องมีส่วนประกอบ หรือองค์ประกอบที่สำคัญแบ่งได้เป็น 3 ส่วน คือ ส่วนที่ทำหน้าที่เป็นเซิร์ฟเวอร์ ส่วนที่ทำหน้าที่เป็น WAP Gateway และส่วนที่ทำหน้าที่เป็นไคลเอนต์ (Micro Browser)

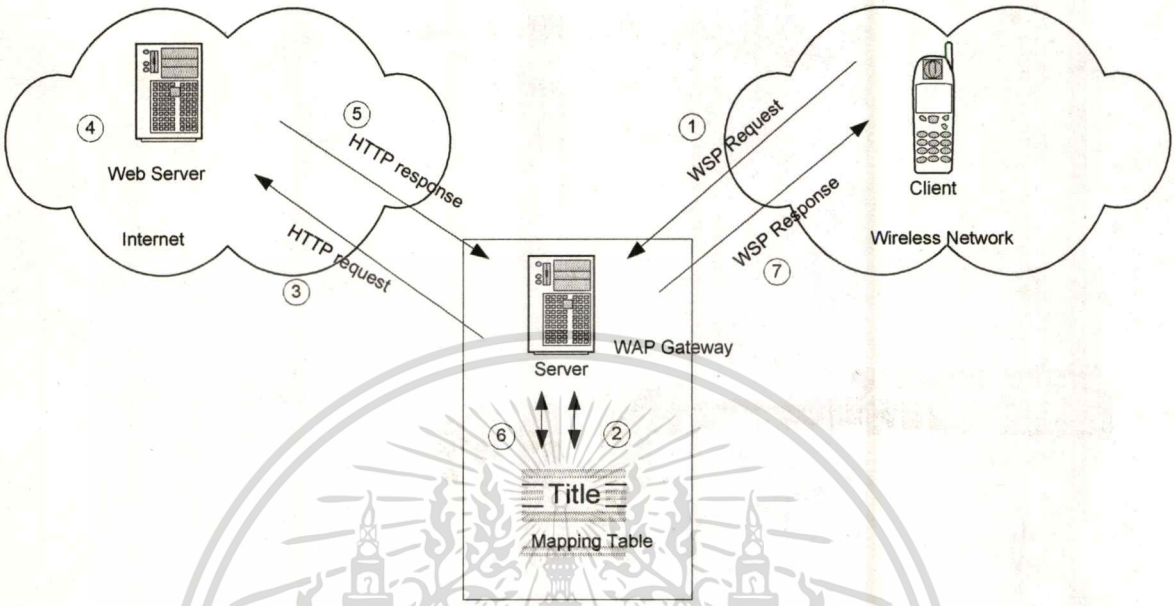
- ส่วนที่ทำหน้าที่เป็นเซิร์ฟเวอร์ (WAP/Web Server) คือ Web/WAP Server ที่ทำหน้าที่ให้บริการข้อมูลแก่ไคลเอนต์ต่าง ๆ
- ส่วนที่ทำหน้าที่เป็น WAP Gateway ทำหน้าที่ในการเชื่อมต่อกันระหว่างเครือข่ายที่ต่างกัน 2 เครือข่ายคือ เครือข่ายอินเทอร์เน็ตและเครือข่ายไร้สายให้สามารถแลกเปลี่ยนข้อมูลกันได้

- ส่วนที่ทำหน้าที่เป็นไคลเอนต์ คือโทรศัพท์มือถือ อุปกรณ์ไร้สายต่าง ๆ โดยที่มี Micro browser ทำหน้าที่ในการเรียกดูข้อมูลจาก Web/WAP Server ดังแสดงในรูปที่ 2.4



รูปที่ 2.4 แสดงส่วนประกอบของ WAP Environment and Security

2.2.2 ขั้นตอนการทำงานของ WAP



รูปที่ 2.5 แสดงการทำงานของ WAP

จากรูปที่ 2.5 จะอธิบายถึงการทำงานของ WAP เป็นขั้นตอนดังนี้

1. ผู้ใช้โทรศัพท์มือถือ (ไคลเอนต์) ส่ง URL ของเอกสารที่ต้องการไปยัง WAP Gateway โดยส่งเป็นคำร้องขอในรูปแบบโปรโตคอล WSP (WSP Request)
2. WAP Gateway ถอดรหัส (decode) คำร้องขอที่อยู่ในรูปแบบไบนารี (WSP request) เพื่อแปลงให้อยู่ในรูปของคำร้องขอแบบ HTTP (HTTP request) โดยอาจอาศัยตาราง mapping table ที่มีอยู่ใน WAP Gateway เป็นตัวช่วย (วิธีการถอดรหัสขึ้นอยู่กับเทคนิคของผู้ผลิตและพัฒนาระบบ WAP Gateway แต่ละราย)
3. WAP Gateway สร้างการเชื่อมต่อ (Connection) ไปยังเว็บเซิร์ฟเวอร์แล้วส่งคำร้องขอตามไปในรูปแบบโปรโตคอล HTTP (HTTP request)
4. เว็บเซิร์ฟเวอร์จะประมวลผลคำร้องขอนั้นและตรวจสอบดูว่า เอกสารตามที่ร้องขอเป็นลักษณะซอร์ซโค้ด WML ธรรมดา (static) หรือไม่ หากเอกสารนั้นเรียกการทำงานของสคริปต์ต่าง ๆ เช่น CGI ASP ก็จะต้องประมวลผลสคริปต์นั้นก่อน เพื่อให้กลายเป็นเอกสาร WML ธรรมดา ซึ่งประกอบไปด้วยแท็ก และข้อความ
5. เว็บเซิร์ฟเวอร์ส่งเอกสารกลับมายัง WAP Gateway โดยส่งเป็นคำตอบกลับในรูปแบบโปรโตคอล HTTP (HTTP response)

6. WAP Gateway ก็จะเข้ารหัสเอกสาร (encode) ไปเป็นรูปแบบไบนารี โดยอาจจะอาศัยตาราง mapping table เป็นตัวช่วย
7. WAP Gateway สร้างการติดต่อ (Connection) ไปยังไคลเอนต์ แล้วส่งข้อมูลไบนารีนั้นเป็นคำตอบกลับในรูปแบบโปรโตคอล WSP (WSP response) ไปยังไคลเอนต์ต่อไป

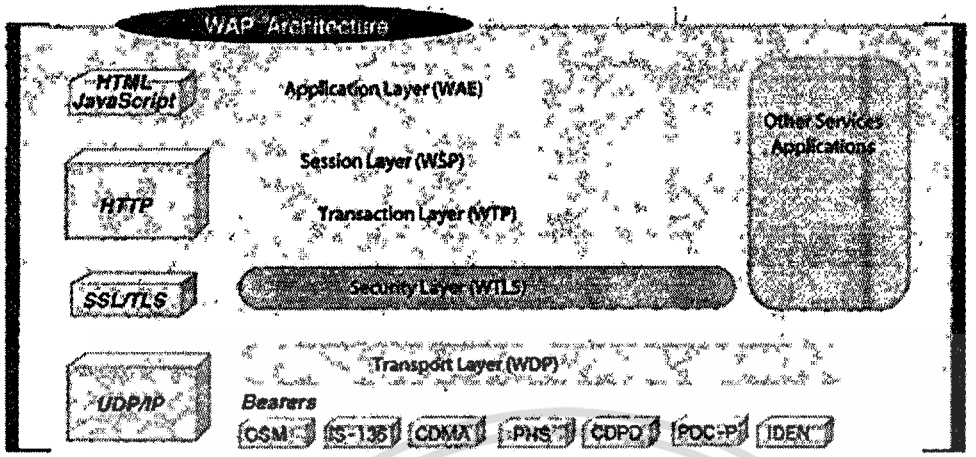
2.2.3 หน้าที่หลักของ WAP Gateway

คุณสมบัติของโปรแกรม WAP Gateway แต่ละตัวไม่เหมือนกัน เนื่องจากผู้ผลิตแต่ละรายอาจเพิ่มหน้าที่บางอย่างเสริมเข้าไป แต่โดยทั่วไป WAP Gateway มีหน้าที่ดังนี้

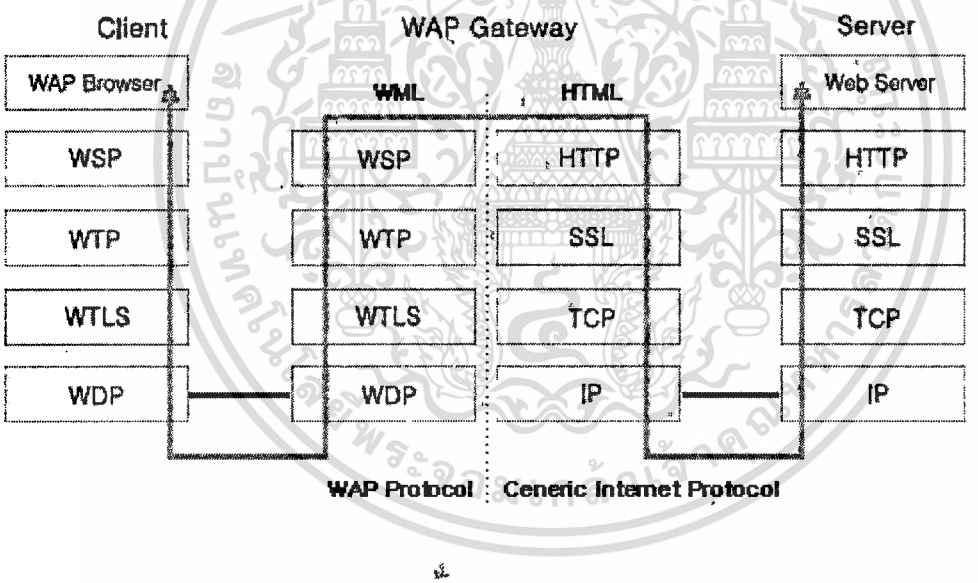
1. รองรับโปรโตคอล WAP และชุดโปรโตคอลในอินเทอร์เน็ต
2. Protocol conversion
3. เข้ารหัสเอกสาร WML ให้เป็นข้อมูลรูปแบบไบนารี
4. คอมไพล์โค้ด WMLScript
5. เป็น proxy server เพื่อให้บริการข้อมูลที่ถูกเรียกใช้บ่อย ๆ
6. ดูแลจัดการด้านการรักษาความปลอดภัยของข้อมูล
7. เปลี่ยนเอกสาร HTML ที่ได้รับจากเว็บเซิร์ฟเวอร์ให้เป็นเอกสาร WML

2.2.4 โครงสร้างของ WAP Gateway

ชั้นสื่อสารในโปรโตคอล WAP เป็นแนวคิดที่พัฒนามาจากชั้นสื่อสารในระบบอินเทอร์เน็ตที่มีโปรโตคอลหลัก ๆ ได้แก่ HTTP TCP และ IP ช่วยในการรับ-ส่งข้อมูลระหว่างเว็บเบราเซอร์และเว็บเซิร์ฟเวอร์ สำหรับชั้นสื่อสารใน WAP ก็ประกอบไปด้วยโปรโตคอลต่าง ๆ หลายตัวเช่นกัน คือ WSP WTP WTLS และ WDP ดังรูปที่ 2.6 และรูปที่ 2.7



รูปที่ 2.6 แสดงการทำงานของ WAP



รูปที่ 2.7 แสดงการทำงานของ WAP

รายละเอียดของโปรโตคอลแต่ละโปรโตคอลดังนี้

- **WAE** (Wireless Application Environment) เป็นโปรโตคอลมาตรฐานที่เอื้ออำนวยในการพัฒนาแอปพลิเคชันสำหรับเครือข่ายแบบไร้สาย จะบอกว่าถ้าต้องการพัฒนาแอปพลิเคชันสำหรับ WAP จะต้องมีอะไรมาเกี่ยวข้องบ้าง ที่เห็นได้ชัดเจนคือภาษา WML กับ WMLScript หรือแม้กระทั่ง WAP Browser เป็นต้น

  WAE มี User Agent 2 ตัว คือ

- WML User Agent เช่น WAP Browser หรือ Micro browser ซึ่งติดตั้งอยู่ในโทรศัพท์มือถือ หรือใน WAP Emulator ต่าง ๆ
- WTA User Agent จะทำงานในส่วนที่เกี่ยวกับฟังก์ชันการทำงานของโทรศัพท์

ในบรรดาองค์ประกอบของ WAE นอกจาก User Agent ดังที่กล่าวมาแล้ว ยังมีอีกส่วนหนึ่งคือ รูปแบบของข้อมูลและบริการ ซึ่งหมายถึงสิ่งที่จะนำไปใช้กับ User Agent ยกตัวอย่าง เช่น WML WMLScript ก็สามารถนำไปแสดงใน WML User Agent (WAP Browser) ได้ ในที่นี้จะกล่าวถึงเพียง 3 อย่างคือ WML WMLScript และ URL ดังนี้

- **WML**

ภาษา WML เป็นภาษาที่เกี่ยวข้องกับแท็กต่าง ๆ เหมือนกับภาษา HTML ที่เราคุ้นเคย ภาษานี้ได้รับการพัฒนาโดย WAP Forum และได้รับอิทธิพลมาจาก 2 ภาษา คือ ภาษา HDML เวอร์ชัน 2 ของบริษัท Phone.com (ชื่อเดิมคือ บริษัท Unwired Planet) และภาษา HTML เวอร์ชัน 4 โดยนำมาดัดแปลงและปรับปรุงให้เหมาะกับสภาพของเครือข่ายไร้สายและอุปกรณ์มือถือ

ถ้าเป็นเอกสาร HTML แล้ว 1 หน้าจอที่แสดงคือ 1 ไฟล์ แต่ในเอกสาร WML นั้น 1 หน้าจอเรียกว่า 1 คาร์ด (card) หลาย ๆคาร์ด จะรวมกันเป็น 1 เดค (deck) ซึ่ง 1 เดคก็เปรียบเหมือน 1 ไฟล์ เหตุผลที่ต้องทำเช่นนี้เพราะหน้าจอของอุปกรณ์มือถือมีขนาดเล็กเกินกว่าจะแสดงผลข้อมูลจำนวนมาก จึงต้องแบ่งเป็นคาร์ดย่อย ๆ และให้ผู้ใช้ทำงานโต้ตอบกับคาร์ดได้ โดยเลือกคำสั่งการทำงานหรือป้อนข้อมูลในแต่ละคาร์ด เช่น ใส่ข้อความ (input) เข้าไปในช่องที่กำหนดไว้ เลือกคำตอบที่ต้องการจากรายการที่แสดงออกมาให้เลือก เป็นต้น

เอกสาร WML จะถูกส่งจากเว็บเซิร์ฟเวอร์หรือ WAP Application Server ทีละเดค มาเก็บในหน่วยความจำของ User Agent ดังนั้นหลังจากเราโต้ตอบกับคาร์ดหนึ่ง แล้วเปลี่ยนไปยังอีกคาร์ดหนึ่งในเดคเดียวกัน User Agent ก็ไม่ต้องร้องขอคาร์ดใหม่จากเซิร์ฟเวอร์ เพราะมีอยู่ในหน่วยความจำแล้ว

คุณสมบัติของ WML มีดังนี้

- แสดงข้อมูลได้ทั้งข้อความและรูปภาพ คุณสมบัตินี้คล้ายกับภาษา HTML โดยการใช้แท็กต่าง ๆ ในการควบคุมการแสดงผลข้อมูลเช่น การย่อหน้า ตัวอักษรเอน-หนา การจัดตำแหน่งข้อความให้ชิดซ้าย-ชิดขวา แต่ส่วนที่แตกต่างอย่างมากก็คือ ภาษา HTML รองรับการแสดงรูปภาพหลายรูปแบบ เช่น GIF JPG ส่วนภาษา WML รองรับการแสดงรูปภาพได้เพียงรูปแบบเดียวคือ WBMP (Wireless Bitmap) ซึ่งเป็น

ลักษณะภาพขาวดำและไฟล์มีขนาดเล็ก แต่ถึงแม้ WML จะมีข้อจำกัดกว่า HTML ในการแสดงรูปภาพก็ตาม ยังดีที่เราสามารถใช้ซอฟต์แวร์ช่วยแปลงภาพจาก JPG GIF หรือรูปแบบอื่น ๆ มาเป็นภาพชนิด WBMP ได้ไม่ยาก

- แสดงแบบรับข้อมูลในลักษณะต่าง ๆ ได้เช่นเดียวกับภาษา HTML ทั้งแบบฟอร์มที่ให้ผู้ใช้กรอกข้อความ ตัวเลือกแบบ checkbox ให้กาเครื่องหมายเลือก และตัวเลือกแบบ radio button แต่มีข้อแตกต่างกันในแง่การใช้งาน คือ ภาษา HTML จะแสดงปุ่มให้คลิกในตัวแบบฟอร์มเลย แต่ภาษา WML จะต้องใช้ปุ่มซอฟต์คีย์ที่อยู่บนโทรศัพท์มือถือแทน

- สามารถลิงค์จากคาร์ดหนึ่งไปยังคาร์ดอื่นหรือเอกสารอื่น โดยอาจจะกำหนดโฮเปอร์ลิงก์หรือใช้ปุ่ม Back ซึ่งคล้ายคลึงกับในภาษา HTML

- รองรับตัวอักษรแบบ Unicode ซึ่งเป็นชุดอักษรที่เป็นมาตรฐานสากล

- **WMLScript**

จัดเป็นภาษาสคริปต์ที่ได้รับการออกแบบมาเพื่ออุปกรณ์มือถือไร้สายโดยเฉพาะ และมีส่วนคล้ายคลึงกับภาษา Javascript ซึ่งเป็นภาษาสคริปต์ทางฝั่งไคลเอนต์ (client-side script) สำหรับรูปแบบการใช้งานภาษา WMLScript มีอาทิเช่น

- ตรวจสอบความถูกต้องของข้อมูลจากฟอร์ม ก่อนส่งไปยังเว็บเซิร์ฟเวอร์
- ใช้ติดต่อกับฟังก์ชันในโทรศัพท์มือถือ
- สร้างแอปพลิเคชันในลักษณะโต้ตอบกับผู้ใช้ โดยไม่ต้องอาศัยความสามารถของเว็บเซิร์ฟเวอร์ เช่น แสดงข้อความ error เมื่อมีสิ่งผิดปกติเกิดขึ้น

- **URL**

ในระบบ WAP มีการอ้างถึงที่อยู่ของเอกสารด้วย URL เช่นเดียวกับระบบ WWW และใช้มาตรฐานเดียวกัน โดยต้องระบุโปรโตคอลนำหน้า เช่น http://wap.nectec.or.th/ เป็นต้น

- **WSP** (Wireless Session Protocol) เปรียบเสมือนเป็นโปรโตคอล HTTP (เวอร์ชัน 1.1) ในรูปแบบไบนารี เพราะทำหน้าที่จัดการเกี่ยวกับการรับ-ส่งข้อมูลระหว่างไคลเอนต์และเซิร์ฟเวอร์ทางฝั่งเครือข่ายไร้สาย ซึ่งในมุมมองของ WSP นั้น ไคลเอนต์ก็คือโทรศัพท์มือถือ ส่วนเซิร์ฟเวอร์ก็คือ WAP Gateway หรือ WAP Server ด้วยก็ได้ (เนื่องจาก WAP Server ก็คือ WAP Gateway + WAP Application Server) ข้อมูลส่วนที่เป็น WSP header ก็ต้องอยู่ในรูปแบบไบนารี เพื่อความเหมาะสมในการรับ-ส่งผ่านเครือข่ายไร้สายที่มีข้อจำกัด

โดยปกติเราสามารถถือได้ว่า โปรโตคอล WSP อยู่ในชั้น Session Layer แต่ในความจริงแล้วในชั้น Session Layer ยังแบ่งออกเป็น 2 โปรโตคอลย่อย ๆ คือ WSP/B และ WSP ซึ่งมีข้อแตกต่างกันเล็กน้อย

WSP/B เป็นโปรโตคอล ที่ไม่ต้องสร้างการเชื่อมต่อหรือ session ระหว่างไคลเอนต์กับ WAP Gateway ก่อน การส่งข้อมูลจะไม่มีการตรวจสอบความถูกต้องด้วย WTP แต่จะอาศัย WDP ในการส่งข้อมูลโดยตรงเลย

WSP มีข้อกำหนดในลักษณะตรงกันข้าม คือ ต้องมีการสร้าง session หรือการเชื่อมต่อระหว่างไคลเอนต์กับ WAP Gateway ที่มั่นคงและยาวนาน เพื่อให้การรับ-ส่งข้อมูลไม่มีเหตุขัดข้อง และในอีกแง่หนึ่งยังต้องระงับการติดต่อชั่วคราว (suspend) และสามารถเรียกการเชื่อมต่อกลับมาใหม่ (resume) โดยไม่เปลืองทรัพยากรของระบบมากนัก เหตุผลที่บางครั้งต้องระงับการเชื่อมต่อชั่วคราวก็คือ ในกรณีที่มีการหยุดนิ่งนาน ๆ โดยไม่มีการรับ-ส่งข้อมูล ซึ่งเป็นการเปลืองทรัพยากรของระบบ เช่นแบตเตอรี่ นอกจากนี้ต้องมีการตรวจสอบความถูกต้องของข้อมูลตามข้อกำหนดของโปรโตคอล WTP ด้วยจากนั้นอาศัยโปรโตคอล WDP ให้ส่งข้อมูลเหมือนกับใน WSP/B สำหรับการติดต่อแบบ Connection-Oriented คือกรณีที่ใช้โปรโตคอล WSP และอาศัยโปรโตคอล WTP ที่อยู่ถัดไปในการจัดการตรวจสอบความถูกต้องของข้อมูล และจากนั้นก็อาศัยโปรโตคอล WDP ส่งข้อมูลไปในเครือข่ายไร้สาย (WSP -> WTP -> WDP) ส่วนการติดต่อแบบ Connectionless ก็คือ กรณีที่ใช้โปรโตคอล WSP/B และอาศัยโปรโตคอล WDP ให้ช่วยจัดการส่งข้อมูลโดยตรงเลย (WSP/B -> WDP) ไม่ต้องมีการตรวจสอบความถูกต้องของข้อมูลด้วยโปรโตคอล WTP

แต่มีการป้องกันความปลอดภัยของข้อมูล ก็ต้องผ่าน WTLS ด้วย สรุปลำดับชั้นของโปรโตคอลก็คือ WSP -> WTP -> WTLS -> WDP หรือ WSP/B -> WTLS -> WDP แล้วแต่ว่าการติดต่อแบบ Connection-Oriented หรือแบบ Connectionless

การใช้งานการติดต่อแบบ Connection-Oriented หรือ Connectionless ขึ้นอยู่กับการตัดสินใจของผู้พัฒนา WAP Gateway แต่ละราย ส่วนใหญ่ในปัจจุบันใช้การติดต่อแบบ Connectionless เนื่องจากความรวดเร็วในการรับ-ส่งข้อมูล ไม่ต้องมาคอยตรวจสอบความถูกต้อง วิธีสังเกตว่าเป็นการติดต่อแบบใดก็คือ ถ้าเป็นการติดต่อแบบ Connection-Oriented แล้วจะใช้พอร์ต 9201 แต่หากเป็น Connectionless จะใช้พอร์ต 9200 ซึ่งดูได้จากการตั้งค่าในโทรศัพท์มือถือที่รองรับระบบ WAP เพื่อขอใช้บริการของ WAP Gateway ซึ่งนอกจากต้องระบุ IP Address ของ WAP Gateway แล้ว จะต้องระบุพอร์ตด้วย โดยที่ผู้ให้บริการ WAP Gateway จะกำหนดไว้ชัดเจนว่าจะเป็น 9200 หรือ 9201

- **WTP** (Wireless Transaction Protocol) เกี่ยวข้องกับการรับประกันความน่าเชื่อถือของการส่งข้อมูล ซึ่งมองดูแล้วก็คล้ายคลึงกับหน้าที่บางส่วนของโปรโตคอล TCP แต่สิ่งที่แตกต่างกันก็มีหลายประการ อย่างเช่น โปรโตคอล TCP จะมองในเชิงการเชื่อมต่อ หรือ Connection-Oriented ระหว่างผู้รับและผู้ส่ง (ไคลเอนต์และเซิร์ฟเวอร์) รวมถึงควบคุมการส่งข้อมูลด้วย แต่โปรโตคอล WTP จะเอนเอียงไปในเชิงกระบวนการรับ-ส่งข้อมูลไปมา หรือ Transaction-Oriented มากกว่า เพราะหน้าที่ในการเชื่อมต่ออยู่ที่โปรโตคอล WSP แล้ว

  ถ้ายังมองความแตกต่างระหว่างโปรโตคอล WSP และโปรโตคอล WTP ไม่ออก จะขอยกตัวอย่างดังนี้ สมมติว่ามีท่อขนาดใหญ่อยู่ท่อหนึ่ง ที่ปลายแต่ละข้างก็มีผู้ส่งของและผู้รับของ ท่อก็เปรียบเสมือน session ระหว่างผู้ส่งและผู้รับ เพราะว่า session นี้จะเป็นของผู้รับส่งและผู้รับคู่นี้เท่านั้น คนอื่น ๆ ไม่สามารถมายุ่งเกี่ยวได้ โปรโตคอล WSP จะเป็นตัวจัดการ session ดังกล่าว

  ส่วนการตรวจสอบความถูกต้องและรับประกันความน่าเชื่อถือในการส่งข้อมูลตามข้อกำหนดของโปรโตคอล WTP นั้น เปรียบเสมือนกรณีที่ผู้ส่งจะส่งห่อข้าวไปให้ผู้รับผ่านท่อ โดยมีกฎกำหนดว่า เมื่อผู้รับได้รับห่อข่าวแล้วจะต้องส่งก้อนหินผ่านท่อกลับมายังผู้ส่ง เพื่อแสดงให้รู้ว่าได้รับของโดยสมบูรณ์

  นอกจากนี้ โปรโตคอล WTP ยังพยายามลดกระบวนการส่งข้อมูลไป-มาให้เหลือน้อยที่สุด เพราะข้อจำกัดของเครือข่ายแบบไร้สาย ซึ่งมี bandwidth แคบและ latency สูงเมื่อผ่านการควบคุมความน่าเชื่อถือในการรับ-ส่งข้อมูลด้วยโปรโตคอล WTP แล้ว ข้อมูลก็จะถูกส่งต่อให้แก่โปรโตคอล WDP ซึ่งทำหน้าที่จัดส่งข้อมูลไปในเครือข่ายแบบไร้สาย

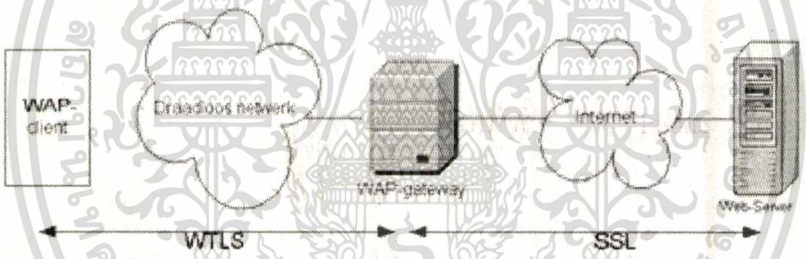
- **WDP** (Wireless Datagram Protocol) จะคอยดูแลการส่งข้อมูลไปในเครือข่าย แต่เนื่องจากชนิดของเครือข่ายไร้สาย (bearer) มีหลายรูปแบบ เช่น GSM , CDMA , GPRS ฯลฯ ดังนั้นคุณลักษณะสำคัญของโปรโตคอล WDP ก็คือ ความอิสระไม่ผูกติดกับเครือข่าย (bearer independence) โดย WDP จะคอยอำพรางโปรโตคอลซึ่งอยู่เหนือขึ้นไปว่ากำลังทำงานกับเครือข่ายชนิดไหน ดังนั้นด้วยคุณลักษณะของโปรโตคอล WDP นี้เอง ผู้พัฒนา WAP Application จึงไม่ต้องกังกลเรื่องเครือข่ายไร้สายเลย

  จากตัวอย่างเรื่องท่อข้าว สามารถเปรียบเทียบได้ว่าโปรโตคอล WDP จะจัดการส่งไปในท่อ ส่วนเครือข่ายก็เปรียบเสมือนที่อยู่ในท่อเช่น อากาศ น้ำ น้ำมัน เป็นต้น หากเครือข่ายเป็นน้ำ โปรโตคอล WDP ก็ต้องหาวิธีห่อข้าวไม่ให้น้ำเข้า โดยที่เมื่อข้าวถึงมือผู้รับแล้ว จะต้องไม่ทราบเลยว่าห่อข้าวนี้ถูกส่งผ่านท่อน้ำมา ซึ่งคือคุณสมบัติของโปรโตคอล WDP ที่จะคอยอำพรางโปรโตคอลข้างบนว่ากำลังทำงานกับเครือข่ายชนิดไหนอยู่ โดยทั่วไป โปรโตคอลที่อยู่เหนือจาก WDP ก็คือ โปรโตคอล WTP แต่ในบางกรณีที่มีการป้องกันความปลอดภัยของข้อมูล

ก็จะมีอีกโปรโตคอลหนึ่งที่เป็นตัวจัดการเกี่ยวกับความปลอดภัยโดยเฉพาะ โปรโตคอลนั้นคือ WTLS

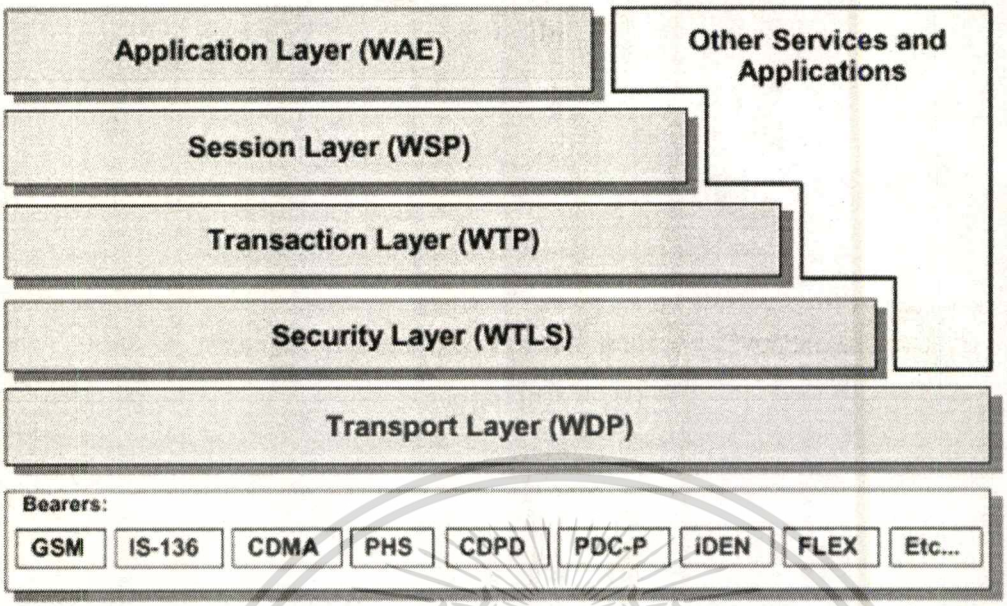
- **WTLS** (Wireless Transport Layer Security) โปรโตคอลนี้เป็นทางเลือกเสริมเท่านั้น จะมีหรือไม่ก็ได้ ทั้งนี้ขึ้นอยู่ที่ WAP Gateway และโทรศัพท์มือถือ WAP Phone ว่ารองรับโปรโตคอล WTLS หรือไม่ แต่ถึงแม้จะเป็นเพียงทางเลือกเสริม โปรโตคอล WTLS ก็มีความสำคัญและน่าติดตามเป็นอย่างยิ่ง

SSL (Secure Sockets Layer) เป็นโปรโตคอลจัดการความปลอดภัยในระบบอินเทอร์เน็ต โปรโตคอลนี้จะจัดการเข้ารหัส-ถอดรหัสข้อมูลด้วยเทคนิคและกลไลต่าง ๆ เมื่อกระบวนการทำงาน WAP รับแนวความคิดมาจากอินเทอร์เน็ตเป็นส่วนใหญ่ ดังนั้นจึงรับแนวคิดของโปรโตคอล SSL ที่เกี่ยวกับการรักษาความปลอดภัยมาด้วยเช่นกัน แล้วดัดแปลงให้เหมาะสมกับเครือข่ายไร้สาย กลายเป็นโปรโตคอลใหม่ชื่อ WTLS ซึ่งอิงอยู่กับโปรโตคอล SSL 3.0 ดังรูปที่ 2.8



รูปที่ 2.8 แสดงโครงสร้างของโปรโตคอล WTLS

จากภาพที่ 2.9 ผู้อ่านคงจะเดาได้ว่า อุปกรณ์ WAP Gateway ต้องเข้ามามีบทบาทกับโปรโตคอล WTLS และ SSL อย่างแน่นอน และน่าจะคล้ายกับกรณีโปรโตคอล WSP และ HTTP ด้วย



รูปที่ 2.9 แสดงบทบาทของ WTLS และโครงสร้างแบบ Wireless

การเข้ารหัสด้วยโปรโตคอล WTLS จะเกิดขึ้นได้ ก็ต่อเมื่อ WAP Gateway และโทรศัพท์มือถือล้วนรองรับ โปรโตคอล WTLS ทั้งคู่ซึ่งในกรณีนี้ข้อมูลที่จะส่งไป-มาระหว่าง WAP Gateway และโทรศัพท์มือถือ จะต้องถูกเข้ารหัสด้วยข้อกำหนดของโปรโตคอล WTLS และบีบอัดให้มีขนาดเล็ก จะได้เหมาะกับการส่งไปในเครือข่ายไร้สาย ส่วนลำดับการทำงานก็เป็นไปได้ซึ่งแบ่งออกเป็น 2 กรณีคือ ขาส่ง (จากโทรศัพท์มือถือ -> เว็บเซิร์ฟเวอร์) และขารับ (เว็บเซิร์ฟเวอร์ -> โทรศัพท์มือถือ)

กรณีของขาส่ง ทางฝั่งโทรศัพท์มือถือจะเข้ารหัสข้อมูลด้วยข้อกำหนดของโปรโตคอล WTLS แล้วข้อมูลจะถูกส่งผ่านเครือข่ายไร้สายมาถึง WAP Gateway ถึงตรงนี้จะมีเกิดขึ้น 2 ขั้นตอนย่อย ๆ ซึ่งจะกินเวลาสั้นมาก ๆ ในหน่วยมิลลิวินาที คือการถอดรหัสข้อมูลด้วยข้อกำหนดของโปรโตคอล WTLS จากนั้นก็เข้ารหัสอีกครั้งตามข้อกำหนดของโปรโตคอล SSL เพื่อส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต และเมื่อมาถึงเซิร์ฟเวอร์ ข้อมูลก็จะถูกถอดรหัสตามข้อกำหนดของโปรโตคอล SSL เพื่อนำไปใช้หรือประมวลผลอีกที

จุดที่สำคัญคือกระบวนการที่เกิดขึ้นในหน่วยความจำของ WAP Gateway อันเป็นช่วงรอยต่อระหว่างเปลี่ยนโปรโตคอล (WTLS <-> SSL) ซึ่งข้อมูลจะมิได้เข้ารหัสใด ๆ เลย ถึงแม้ช่วงเวลานี้จะสั้นมาก ๆ เพียงแค่ระดับมิลลิวินาทีก็ตาม แต่ผู้พัฒนา WAP Gateway ก็จำเป็นต้องให้ความสำคัญและระมัดระวังอย่างมากในการออกแบบ อย่าให้มีการเก็บข้อมูลที่ถูกถอดรหัสไว้ใน

แหล่งเก็บข้อมูลอื่น ๆ รวมทั้งต้องมีระบบป้องกันความปลอดภัยในเสี้ยววินาทีที่ถอดรหัสจากโปรโตคอลหนึ่งและเข้ารหัสใหม่ด้วยอีกโปรโตคอลหนึ่ง (สราวุธ อ้อยศรีสกุล. 2544 : 32-148)

2.3 Digital Signature

Cryptographic Algorithm (เทคนิคและวิธีการเข้ารหัส)

1. Symmetric Key (ระบบรหัสแบบสามาตร) คือการเข้ารหัสข้อมูลด้วยกุญแจเดี่ยว (Secret Key) ทั้งผู้ส่งและผู้รับ โดยวิธีนี้ได้แนวคิดมาจากวิธีการของ จูเลียส ซีซาร์ (Julius Caesar) เมื่อพันกว่าปีมาแล้ว ตั้งแต่สมัยโรมันยังรุ่งเรืองอยู่ โดยที่ จูเลียส ซีซาร์ ได้ส่งสารลับเพื่อใช้ติดต่อกับกรุงโรมมาโดยตลอด เพื่อป้องกันข้าศึกล่วงรู้ความลับในกรณีที่สารไม่ถึงมือผู้รับหรือโดนขโมยในระหว่างทาง โดยวิธีการนี้ผู้รับกับผู้ส่งต้องตกลงกันก่อนว่าจะใช้รูปแบบไหนในการเข้ารหัสข้อมูล ซึ่งรูปแบบไหนในการเข้ารหัสข้อมูลที่ผู้รับกับผู้ส่งตกลงกันแท้ที่จริงก็คือ กุญแจลับ (Secret Key) นั่นเอง เช่น ผู้ส่งกับผู้รับตกลงจะใช้เทคนิคการแทนที่ตัวอักษรที่อยู่ถัดไป 1 ตำแหน่ง เช่น ถ้าเห็นตัวอักษร A ก็ให้เปลี่ยนไปเป็น B หรือเห็นตัวอักษร B ก็ให้เปลี่ยนไปเป็น C เป็นต้น นั้นก็คือผู้ส่งกับผู้รับตกลงใช้รูปแบบนี้เป็นกุญแจลับ

ข้อด้อยของการเข้ารหัสแบบสมมาตร

1. การจัดการกับกุญแจลับที่ยุ่งยาก เพราะถ้าผู้รับมีจำนวนมากผู้ส่งต้องมีการสร้างกุญแจลับจำนวนมาก ทำให้ผู้ส่งต้องมีการเก็บกุญแจลับจำนวนมาก อาจทำให้ผู้ส่งสับสนได้ และต้องทำให้กุญแจลับมีความแตกต่างกันด้วยเพื่อป้องกันการเข้าถึงข้อมูลของผู้รับแต่ละคนหรือคนอื่นด้วย และถ้าใช้กุญแจดอกเดียวกัน ก็อาจทำให้ผู้รับคนอื่นรู้กุญแจลับ และอาจไม่เป็นกุญแจลับอีกต่อไปเหมือนกัน
2. การกระจายกุญแจลับ เนื่องจากการเข้ารหัสวิธีนี้ต้องใช้กุญแจลับ 1 ดอกต่อผู้รับ 1 คน ดังนั้นถ้าผู้ส่งต้องติดต่อกับคนมาก ๆ ผู้ส่งก็ต้องส่งกุญแจลับที่ใช้ไปให้กับทุกคน มี 100 คน ก็ต้องมีกุญแจลับ 100 ดอก และต้องส่งแต่ละดอกไปให้แต่ละคน ถ้ามีพันคน ทำให้ผู้ส่งสับสนได้

ข้อดีของการเข้ารหัสแบบสมมาตร

1. การเข้ารหัส และถอดรหัสข้อมูลใช้เวลาน้อย เพราะว่าอัลกอริทึมที่ใช้ไม่สลับซับซ้อน
2. ขนาดของข้อมูลหลังจากทำการเข้ารหัสแล้ว มีการเปลี่ยนแปลงไม่มาก หรือพูดอีกนัยหนึ่งว่า ข้อมูลหลังจากทำการเข้ารหัสแล้ว จะมีขนาดไม่ใหญ่ไปกว่าเดิมมากนัก

สำหรับวิธีเข้ารหัสแบบนี้ ก็จะมีมาตรฐานมารองรับเหมือนกัน มาตรฐานที่ว่าก็คือ มาตรฐาน DES (Digital Encryption Standard) หรือเรียกว่าเดส ที่มาของ DES เกิดขึ้นมาจากทีมพัฒนาของ

บริษัท IBM เมื่อราว ๆ ปลายยุค ค.ศ. 1960 ทำการพัฒนาระบบเข้าและถอดรหัสนี้ โดยหลักการทำงานจะทำการแบ่งข้อมูลที่จะทำการเข้าหรือถอดรหัสออกเป็นบล็อก (block) โดยที่แต่ละบล็อกจะมีขนาด 64 บิต และจำนวนความยาวของกุญแจลับจะมีขนาด 128 บิตในช่วงแรก หลังจากนั้นทางบริษัท IBM ก็ได้เพิ่มทุนให้ทำการพัฒนาและปรับปรุงต่อเรื่อย ๆ มาโดยในครั้งนี้ได้มีที่ปรึกษาจากสำนักงานความมั่นคงแห่งชาติ (National Security Agency: NSA) ของสหรัฐอเมริกาเข้าร่วมด้วย ผลที่ได้จากการพัฒนานี้ ทำให้ระบบ DES สามารถทนทานต่อผู้ต้องการเจาะรหัส (Cryptanalysis) ได้ ขณะเดียวกัน ก็ได้ทำการลดความยาวของกุญแจเหลือแค่ 56 บิตจากเดิน 128 บิต

เหตุผลที่ทำการลดความยาวของกุญแจลับลง ก็เพราะว่าสำนักงานความมั่นคงแห่งชาติของสหรัฐอเมริกา เกรงว่าจะไม่สามารถตรวจสอบข้อมูลที่เข้ารหัสด้วยความยาวของกุญแจลับที่ 128 บิตได้ เช่น ในกรณีที่ผู้ก่อการร้ายหรือกลุ่มบุคคลที่ไม่ปรารถนาดีต่อประเทศสหรัฐอเมริกาใช้มาตรฐานแบบ DES ในการติดต่อสื่อสารกันในกลุ่มเพื่อทำก่อนการร้าย สหรัฐอเมริกาเกรงว่าถ้าสามารถดักจับข้อความที่กลุ่มผู้ก่อการร้ายติดต่อสื่อสารกันได้แล้ว รัฐบาลของตัวเองจะไม่สามารถถอดรหัสของข้อความเหล่านั้นได้ ทำให้ไม่สามารถป้องกันเหตุการณ์ก่อการร้ายได้ทันท่วงที ซึ่งการลดความยาวของกุญแจลับก็โดนกระแสต่อต้านกลุ่มธุรกิจองค์กรต่าง ๆ มากมาย เพราะพวกกลุ่มธุรกิจองค์กรต่าง ๆ เหล่านี้ต้องการให้ข้อมูลมีความลับมาก ๆ เพราะยิ่งกุญแจลับมีความยาวมากเท่าไร ข้อมูลที่เข้ารหัสก็ยิ่งต้องใช้เวลาในการถอดรหัสออกนานมากขึ้น ทำให้ข้อมูลมีความปลอดภัยยิ่งขึ้น แต่รัฐบาลสหรัฐก็ออกมาโต้ว่า ด้วยความยาวกุญแจลับขนาด 56 บิตนี้ ก็ทำให้ต้องใช้เวลาในการถอดรหัสนานมากที่เดียว เพื่อให้เห็นภาพว่า ทำไมยิ่งขนาดของกุญแจลับมีความยาวมากยิ่งทำให้ต้องใช้เวลาในการถอดรหัสนานมา

- กุญแจมีขนาดความยาว 52 บิต
- จะมีกุญแจที่ต้องลองใช้ในการถอดรหัสได้ทั้งสิ้น 256 เท่ากับ 72,057,594,037,927,936 ดอก สมมติ ถ้าใช้เครื่องคอมพิวเตอร์ที่มีความเร็วในการลองใช้กุญแจ 1 ล้านดอกได้ในเวลา 1 วินาที เพราะฉะนั้น
- ต้องใช้เวลาทั้งสิ้นประมาณ 72,057,594,038 วินาที
- ใน 1 วัน จะมีทั้งหมด 86,400 วินาที
- ต้องใช้เวลาทั้งสิ้น ประมาณ 833,999 วัน หรือประมาณ 2,284 ปี
- กุญแจมีขนาดความยาว 128 บิต
- จะมีกุญแจที่ต้องลองใช้ในการถอดรหัสได้ทั้งสิ้น 2^{128} เท่ากับ 340,282,366,920,938,463,463,374,607,431,768,211,456 ดอก

สมมติ ถ้าใช้เครื่องคอมพิวเตอร์ที่มีความเร็วในการลองใช้กุญแจ 1 ล้านดอกได้ในเวลา 1 วินาที เพราะฉะนั้น

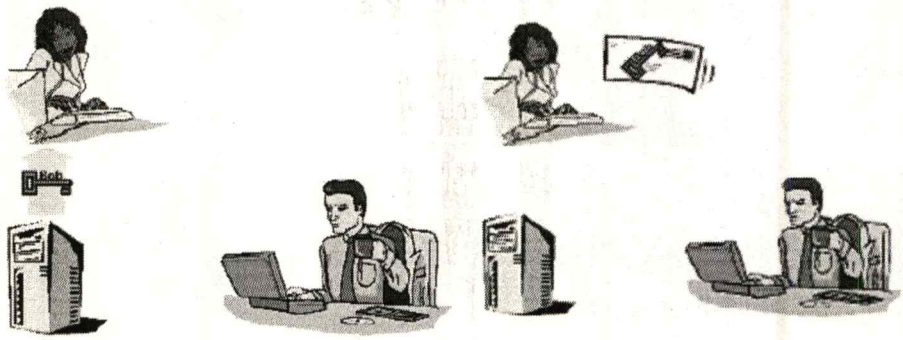
- ต้องใช้เวลาทั้งสิ้นประมาณ 340,282,366,920,938,463,463,374,607,431,768 วินาที
- ใน 1 ปี จะมีทั้งหมดประมาณ 31 ล้านวินาที
- ต้องใช้เวลาทั้งสิ้นประมาณ 10,790,283,070,806,014,188,970,529 ปี

จะเห็นได้ว่ายิ่งขนาดของกุญแจมีความยาวมากก็ต้องใช้เวลาในการถอดรหัสนานขึ้นไปอีก จะเห็นได้ว่าจากที่รัฐบาลสหรัฐอเมริกาว่ากุญแจที่ยาว 56 บิต ก็เพียงพอแล้ว เพราะจากการคำนวณดูจะเห็นว่าต้องใช้เวลาทั้งสิ้นประมาณ 2 พันกว่าปีในการที่จะถอดรหัส แต่ในปัจจุบันเครื่องคอมพิวเตอร์ที่มีประสิทธิภาพสูง สามารถที่จะถอดรหัสที่ใช้กุญแจขนาด 56 บิต ได้ในเวลาแค่ 56 ชั่วโมง และมีแนวโน้มว่าจะสามารถถอดรหัสโดยใช้เวลาลดลงกว่านี้ได้อีก แต่สำหรับข้อมูลที่เข้ารหัสด้วยกุญแจขนาด 128 บิต ในปัจจุบันนี้ยังถือว่าปลอดภัยอยู่มาก เพราะว่ายังไม่สามารถถอดรหัสได้เร็วเกินที่จะรอคอยได้ เพราะกว่าจะถอดรหัสได้ ข้อมูลเหล่านั้นก็อาจจะไม่มีประโยชน์ต่อการนำกลับไปใช้งานได้อีกแล้ว ซึ่งในปัจจุบันนี้ก็ได้มีมาตรฐานที่เรียกว่า 3DES เกิดขึ้นมาแล้ว โดยมาตรฐานนี้จะใช้กุญแจลับที่มีขนาดความยาว 168 บิต แต่สำหรับธุรกิจองค์กรใดที่จะใช้มาตรฐานนี้จะต้องทำเรื่องขออนุญาตใช้งานกับรัฐบาลอเมริกาก่อน ถ้าได้รับอนุญาตจากรัฐบาลอเมริกาจึงจะสามารถนำมาใช้งานได้

สรุป คือ กุญแจลับเพียง 1 ดอกสามารถเข้าและถอดรหัสข้อมูลได้

2. Asymmetric Key หรือ เทคโนโลยี Public Key (ระบบรหัสแบบอสมมาตร) ระบบการเข้ารหัสแบบนี้ได้ถูกคิดค้นโดย นายวิทฟิลด์ ดิฟฟี (Whitfield Diffie) ซึ่งเป็นนักวิจัยแห่งมหาวิทยาลัยสแตนฟอร์ด สหรัฐอมริกา ในปี พ.ศ.2518 โดยการเข้ารหัสแบบนี้จะใช้หลักกุญแจคู่ทำการเข้ารหัสและถอดรหัส โดยกุญแจคู่ที่ว่านี้จะประกอบไปด้วย กุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) โดยหลักการทำงานจะทำดังนี้ ถ้าใช้กุญแจลูกใดข้ารหัสก็ต้องใช้กุญแจอีกลูกหนึ่งถอดรหัส เช่น ถ้าใช้กุญแจสาธารณะเข้ารหัสก็ต้องใช้กุญแจส่วนตัวถอดรหัส เป็นกุญแจคู่ที่มหัศจรรย์มากเลยครับ สำหรับการเข้ารหัสและถอดรหัสด้วยกุญแจคู่นี้จะใช้ฟังก์ชันทางคณิตศาสตร์เข้ามาช่วย โดยที่ฟังก์ชันทางคณิตศาสตร์ที่นำมาใช้ ได้รับการพิสูจน์แล้วว่าจะมีเฉพาะกุญแจคู่ของมันเท่านั้นที่สามารถถอดรหัสได้ ไม่สามารถนำกุญแจคู่อื่นมาถอดรหัสได้อย่างเด็ดขาด ดังรูปที่ 2.10 และรูปที่ 2.11 (ศุภชัย สุขะนินทร์ และธน กันธิพันธ์ . 2544 : 26-46)

1. Alice ต้องการที่จะส่งข้อความไปยัง Bob ดังนั้น Alice ต้องไปดึง public key ของ Bob มาจาก Directory แล้วใช้ Public Key ของ Bob เข้ารหัส email ส่งไปให้ Bob



รูปที่ 2.10 แสดงโครงสร้างการทำงานแบบ PKI (1)

2. เมื่อ Bob ได้รับ email เขาจะใช้ private key ของเขาเพื่อถอดรหัสของข้อความ

รูปที่ 2.11 แสดงโครงสร้างการทำงานแบบ PKI (2)

แต่จะทำอย่างไรให้แนวคิดของ นายวิทฟิลด์ ดิฟฟี นำมาประยุกต์ ใช้งานได้จริงในโลกของข้อมูลอิเล็กทรอนิกส์ ดังนั้นจึงมีอัศวินสามนายขี่ม้าขาวมาช่วยนายวิทฟิลด์ ดิฟฟี โดยอัศวินทั้งสามทำการค้นคว้าและวิจัยอยู่ที่สถาบันเทคโนโลยีแห่งแมสสาซูเซตต์ (MIT :Massachusetts Institute of Technology) นักวิจัยทั้งสามก็คือ นายรอน ริเวสท์ (Ron Rivest) นายเอดิ ชาร์เมียร์ (Adi Shamir) และนายเลียวนาร์ด เอเดิลแมน (Leonard Adleman) ในปี พ.ศ.2520 และตีพิมพ์เผยแพร่เป็นครั้งแรกในปี พ.ศ. 2521 ดังนั้นเราจึงเรียกฟังก์ชันที่ทั้งสามาค้นพบนี้ตามอักษรแรกของชื่อนักวิจัยทั้งสามนี้ว่า ฟังก์ชันอาร์เอสเอ (RSA ย่อมาจาก Rivest , Shamir และ Adleman) แต่โดยทั่วไป มักจะนิยมเรียกว่าอัลกอริทึมอาร์เอสเอ (RSA Algorithm) สำหรับการทำงานของอัลกอริทึมนี้ จะเห็นว่าวิธีการเข้ารหัสแบบนี้จะมีข้อดีกว่าการเข้ารหัสแบบสมมาตร คือ

1. การจัดการกับกุญแจทำได้ง่าย เพราะว่าผู้ส่งไม่ต้องจำเลยว่าได้ใช้กุญแจคู่ไหนกับใคร ผู้ส่งแค่ใช้กุญแจส่วนตัวของตัวเองทำการถอดรหัสข้อมูลที่ผู้รับส่งมาให้ หรือเอากุญแจส่วนตัวเข้ารหัส

ส่งไปให้ผู้รับ ผู้รับก็สามารถอ่านได้ซึ่งวิธีนี้จะง่ายมาก เพราะว่าผู้ส่งใช้แค่กุญแจส่วนตัวของตัวเองดอกเดียวก็สามารถติดต่อกับผู้รับ หรือใคร ๆ ก็ได้ตามต้องการ

2. การกระจายกุญแจลับ เนื่องจากการเข้ารหัสโดยวิธีนี้ ใช้แค่กุญแจสาธารณะเพียงดอกเดียวในการเข้ารหัสและถอดรหัส และกุญแจสาธารณะของนายดำก็สามารถที่จะเปิดเผยให้กับใครก็ได้ที่ต้องการจะติดต่อด้วย ไม่ว่าจะเป็น ผู้รับ ผู้ส่ง หรือคนอื่น ๆ เหล่านี้เป็นต้น เพราะฉะนั้นการแจกจ่ายกุญแจสาธารณะของผู้ส่งไปให้คนสักพันคน หรือหมื่นคน จะไม่เป็นปัญหาอีกต่อไป

ส่วนวิธีการเข้ารหัสแบบนี้จะมีข้อด้อยกว่าการเข้ารหัสแบบสมมาตร

1. การเข้ารหัสและถอดรหัสข้อมูลใช้เวลามาก เพราะว่าอัลกอริทึมที่ใช้ค่อนข้างจะสลับซับซ้อนมาก

2. ขนาดของข้อมูลหลังจากทำการเข้ารหัสแล้ว มีการเปลี่ยนแปลงมาก หรือพูดอีกนัยหนึ่งว่า ข้อมูลหลังจากทำการเข้ารหัสแล้ว จะมีขนาดใหญ่กว่าเดิมมากขึ้น เพราะฉะนั้นจะเป็นปัญหาในการใช้งานผ่านเครือข่ายอินเทอร์เน็ต เนื่องจากความเร็วที่ใช้ในการติดต่อสื่อสารกันผ่านเครือข่ายอินเทอร์เน็ตไม่ได้เร็วมากนัก แค่ข้อมูลขนาดเดิมก่อนที่ยังไม่ได้ทำการเข้ารหัส ก็ใช้เวลาพอสมควรแล้ว กว่าที่จะส่งข้อมูลเหล่านั้นไปให้กับบุคคลที่เราต้องการติดต่อด้วย ยิ่งถ้ามีการเข้ารหัสด้วยวิธีนี้ ยิ่งเพิ่มขนาดของข้อมูลขึ้นไปอีก ก็จะยิ่งทำให้การติดต่อกับบุคคลนั้น ๆ ต้องใช้เวลาเพิ่มขึ้นอีก (Certicom Corporation. 2001)

2.4 PKI

การทำให้ข้อมูลมีความลับก็ยังไม่เพียงพอที่จะนำมาใช้งานกับการทำธุรกรรมอิเล็กทรอนิกส์ ดังนั้นถ้าต้องการทำธุรกรรมอิเล็กทรอนิกส์นั้น เรื่องความปลอดภัยของข้อมูลเป็นสิ่งที่จำเป็นที่สุดและการที่จะทำให้ข้อมูลมีความปลอดภัยจะต้องมี 4 องค์ประกอบต่อไปนี้ คือ

1. **Confidentiality** (การรักษาความลับ) - ต้องมีการรักษาความลับของข้อมูลได้ ก็คือความสามารถในการที่จะรักษาความลับที่ไม่ให้ผู้อื่นที่ไม่สิทธิ์แอบดูข้อมูลที่เก็บไว้ หรือข้อมูลที่ส่งผ่านไปทางเครือข่ายอินเทอร์เน็ตจากตัวอย่างที่ผู้ส่งที่เข้าซื้อหนังสือจากเว็บไซต์ของเรา ข้อมูลที่ผู้ส่งส่งผ่านเข้ามาผ่านเครือข่ายอินเทอร์เน็ต เช่น ชื่อหนังสือ จำนวนหนังสือที่สั่งซื้อ ต้องไม่มีผู้ใดสามารถแอบอ่านข้อมูลเหล่านั้นได้โดยเด็ดขาด ยกเว้นเราเพียงคนเดียวเท่านั้นที่สามารถทราบว่าผู้ส่งต้องการหนังสืออะไรและจำนวนเท่าไร
2. **Authenticity** (การระบุตัวบุคคล) - ต้องสามารถระบุตัวบุคคลได้ ก็คือการที่เราสามารถที่จะระบุตัวตนของผู้ที่ทำธุรกรรมกับเราได้ ยกตัวอย่างง่าย ๆเช่น ถ้าเราเปิดเว็บไซต์ขายหนังสือแล้วมีลูกค้าคือผู้ส่งได้เข้ามาที่เว็บไซต์ของเรา เพื่อทำการซื้อหนังสือสักเล่มหนึ่ง ลูกค้าคนที่

บอกเราว่าเขาคือผู้ส่ง ระบบต้องสามารถที่จะตรวจสอบได้ว่าลูกค้าคนนี้เป็นผู้ส่งจริง ๆ ไม่ใช่คนอื่น

3. **Integrity** (การรักษาความถูกต้อง) - ต้องสามารถตรวจสอบความถูกต้องของข้อมูลได้ ก็คือความสามารถในการรักษาความถูกต้องของข้อมูลไม่ให้มีการแก้ไขข้อมูลโดยเด็ดขาด ยกตัวอย่างให้เห็นภาพ หลังจากที่ผู้ส่งส่งข้อมูลชื่อของหนังสือและจำนวนหนังสือที่ต้องการมาที่เรา โดยที่ข้อมูลที่ส่งจากผู้ส่งมาถึงเราจะเป็นความลับที่รู้กันระหว่างเรากับผู้ส่งเท่านั้นก็ตาม แต่ก็ไม่ใช่ว่าข้อความที่เป็นความลับที่ผู้ส่งส่งเข้ามาจะถูกต้องตรงตามที่ผู้ส่ง เพราะว่าอาจมีคนที่สามารถแกะข้อความลับได้ ดังนั้นอาจจะมีคนที่มีความสามารถแกะข้อความลับที่ผู้ส่งเข้ามาหาเรา แล้วทำการเปลี่ยนเชื่อหนังสือ และจำนวนหนังสือที่ต้องการ แล้วทำการส่งต่อมาที่เราอีกทีหนึ่ง เพราะฉะนั้นเราต้องมีวิธีที่จะตรวจสอบข้อมูลที่ผู้ส่งส่งมาถึงเรา ว่าชื่อหนังสือและจำนวนหนังสือที่ต้องการถูกต้องหรือไม่ เพื่อไม่ให้เกิดความเสียหาย
4. **Non-repudiation** (การป้องกันการปฏิเสธความรับผิดชอบ) - ต้องไม่สามารถปฏิเสธความรับผิดชอบใด ๆ ที่เกิดขึ้นได้ ก็คือความสามารถในการป้องกันการปฏิเสธความรับผิดชอบจากคู่ค้าที่เกี่ยวข้องได้ ขอยกตัวอย่าง เช่น หลังจากที่ผู้ซื้อบอกกับเราว่าผู้ซื้อ ผู้ซื้อก็ทำการส่งชื่อหนังสือกับจำนวนหนังสือที่ต้องการเข้ามา โดยที่ข้อมูลหนังสือของผู้ซื้อเป็นความลับที่รู้กันระหว่างเรากับผู้ซื้อ พอเราได้รับข้อมูลสั่งซื้อหนังสือของผู้ซื้อแล้วนั้น เราก็ได้ทำการตรวจสอบข้อมูลที่ได้มาว่า ชื่อหนังสือที่ต้องการคืออะไร จำนวนเท่าไร ว่าถูกต้องครบถ้วนไม่มีการแก้ไขใด ๆ เลยหรือไม่ ถ้าทุกอย่างเรียบร้อยหมด เราก็ทำการส่งหนังสือและจำนวนที่ผู้ซื้อต้องการไปให้ผู้ซื้อ เพราะฉะนั้นค่าหนังสือที่เกิดขึ้น ผู้ซื้อไม่มีสิทธิ์ที่จะปฏิเสธความรับผิดชอบได้เลย จะมาโวยวายว่าเขาไม่ได้สั่งซื้อหนังสือจากเรา หรือโวยวายว่าจำนวนหนังสือที่สั่งซื้อผิด ไม่ได้โดยเด็ดขาด ผู้ซื้อจะต้องรับผิดชอบค่าใช้จ่ายทั้งหมดเลย

จากทั้ง 4 องค์ประกอบนี้สำหรับในโลกการค้าปัจจุบันนี้ จะไม่เกิดปัญหาอะไร เพราะว่าในการค้าขายโดยส่วนมากจะเป็นลูกค้าเดินทางไปที่ร้านค้าเอง ไม่ว่าจะเป็นตามห้างสรรพสินค้า หรือแหล่งขายสินค้าต่าง ๆ ซึ่งพ่อค้าสามารถเห็นตัวตนของลูกค้าได้ และหลังจากตกลงซื้อขายกันเรียบร้อยแล้ว ก็ชำระเงินค่าสินค้ากันตรงนั้นเลย ถ้าเป็นการชำระด้วยบัตรเครดิต ลูกค้าก็จะต้องลงชื่อในใบเรียกเก็บเงิน เพื่อเป็นการยินยอมตามเงื่อนไขต่าง ๆ รวมไปถึงรายละเอียดและจำนวนเงินค่าสินค้า โดยไม่สามารถที่จะปฏิเสธการชำระเงินได้ ดังนั้นลายเซ็นหรือลายมือชื่อจึงเป็นหัวใจหลักของการทำการค้าขาย แต่ในโลกของการค้าขายแบบอิเล็กทรอนิกส์ เราจะต้องนำเอาเทคโนโลยีมาใช้เพื่อทำให้เกิดลายมือชื่ออิเล็กทรอนิกส์ขึ้นมา โดยที่ลายมือชื่ออิเล็กทรอนิกส์นี้อย่างน้อยจะต้องมีคุณสมบัติไม่น้อยกว่าคุณสมบัติของลายมือชื่อ นั่นก็คือ

- สามารถระบุตัวบุคคลได้ คือ ลายมือชื่ออิเล็กทรอนิกส์นั้นต้องระบุได้ว่าเป็นผู้ซื้อ หรือคนอื่น
- ต้องแสดงว่าบุคคลยอมรับข้อความ ก็คือ ข้อมูลทางอิเล็กทรอนิกส์ที่ได้รับการเซ็นชื่อรับรอง โดยลายมือชื่ออิเล็กทรอนิกส์ของผู้ซื้อหรือคนอื่น เป็นที่ยอมรับแล้วถูกต้อง ไม่สามารถปฏิเสธความรับผิดชอบได้

สำหรับเทคโนโลยีที่ใช้ในการสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ได้แก่

1. การใช้เทคโนโลยี PKI (Public Key Infrastructure) : ระบบกุญแจคู่
2. การใช้เทคโนโลยีชีวภาพ (Biometrics) เช่น Finger Print (เทคโนโลยีการตรวจสอบลายนิ้วมือ) Voice Print (เทคโนโลยีความสามารถในการจดจำเสียง)

จะเห็นได้ว่าลายมือชื่อดิจิตอลก็เป็นลายมือชื่ออิเล็กทรอนิกส์ประเภทหนึ่ง แต่ลายมือชื่อดิจิตอลได้ใช้เทคโนโลยีที่เรียกว่า PKI หรือระบบกุญแจคู่ ส่วนลายมือชื่ออิเล็กทรอนิกส์อื่น ๆ ที่ใช้เทคโนโลยีอื่น ๆ ที่ใช้ในปัจจุบัน เช่น เทคโนโลยีชีวภาพ หรือเทคโนโลยีอื่น ๆ ที่ไม่ใช่เทคโนโลยี PKI

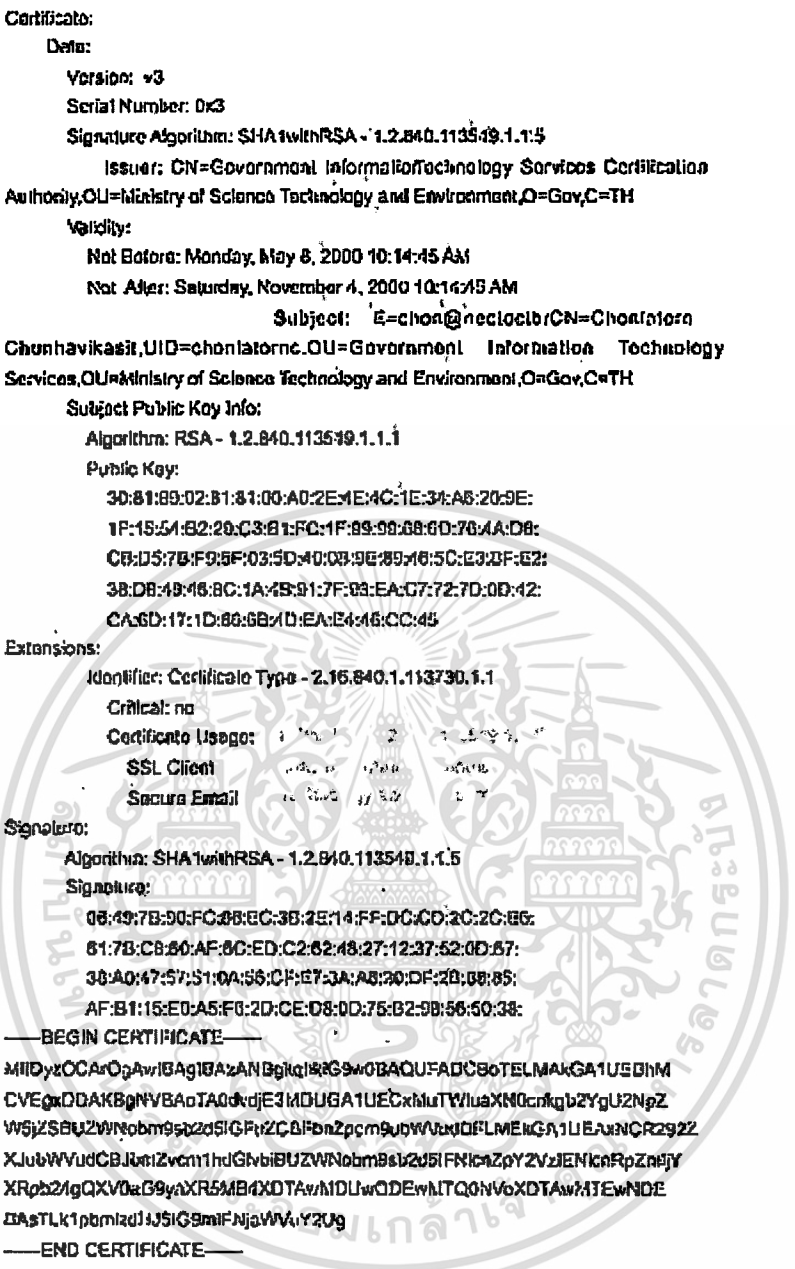
เพื่อให้มีครบทุกองค์ประกอบในการทำธุรกรรมทางอิเล็กทรอนิกส์ได้ เขาจึงได้นำเอาเทคโนโลยีระบบรหัสแบบอสมมาตร (Public Key) มาใช้สำหรับเทคโนโลยีระบบรหัสแบบอสมมาตร ส่วนมากจะรู้จักกันในชื่อว่าเทคโนโลยี Public Key ทำไมเทคโนโลยี Public Key จึงถูกนำมาใช้ ถ้ายังจำกันได้เทคโนโลยี Public Key จะใช้เทคนิคของกุญแจคู่ คือ กุญแจส่วนตัว (Private Key) กับกุญแจสาธารณะ (Public Key) มาใช้ในการเข้ารหัสและถอดรหัส การนำเทคโนโลยี Public Key มาใช้ทำให้เกิดสิ่งหนึ่งขึ้นมานั่นก็คือ ลายมือชื่อดิจิตอล (Digital Signature) โดยลายมือชื่อดิจิตอลนี้ก็เป็นตัวเริ่มต้นที่ทำให้การทำธุรกรรมอิเล็กทรอนิกส์เกิดขึ้นได้มาจนถึงปัจจุบันนี้ จะเห็นว่ามีองค์ประกอบในเรื่องความปลอดภัยของข้อมูลในการทำธุรกรรมอิเล็กทรอนิกส์เกิดขึ้นมาแล้ว 3 ตัวคือ

1. การรักษาความลับของข้อมูลได้ ก็เพราะว่าผู้ส่งมีการเข้ารหัสข้อมูลก่อนจึงจะส่งไปให้ผู้รับ
2. สามารถระบุตัวบุคคลได้ ก็เพราะว่าผู้รับต้องใช้กุญแจสาธารณะของผู้ส่งเท่านั้นจึงจะถอดรหัสได้ แสดงว่าข้อมูลต้องมาจากผู้ส่งอย่างแน่นอน
3. ต้องไม่สามารถปฏิเสธความรับผิดชอบใด ๆ ที่เกิดขึ้นได้ ก็สืบเนื่องมาจากการที่ผู้รับสามารถระบุได้ว่าข้อมูลนั้นมาจากผู้ส่ง ดังนั้นผู้ส่งจะต้องรับผิดชอบทุกสิ่งที่เกิดขึ้นอย่างหลีกเลี่ยงไม่ได้อย่างเด็ดขาด

แต่เทคโนโลยีกุญแจสาธารณะ (PKI) ยังมีจุดอ่อนอยู่ คือจะทำอย่างไรให้มั่นใจหรือตรวจสอบได้ว่ากุญแจสาธารณะเป็นของบุคคลนั้นจริง ๆ วิธีแก้จุดอ่อนตรงนี้ก็คือ ต้องมีองค์กรหนึ่งตั้งขึ้นมาเพื่อทำหน้าที่ในการรับรองกุญแจสาธารณะของแต่ละบุคคลนั่นเอง โดยที่องค์กรที่ว่าก็คือ องค์กรออกใบรับรอง (Certification Authority หรือ CA) โดยที่องค์กรออกใบรับ หรือ CA ที่ว่านี้ หน้าที่หลักก็คือออกใบรับรองดิจิตอล (Digital Certificate) ซึ่งใบรับรองดิจิตอลจะมีกุญแจสาธารณะของผู้ส่งเก็บอยู่ในนี้ด้วย ทำให้ผู้รับสามารถที่จะตรวจสอบกุญแจสาธารณะที่อยู่ในใบรับรองดิจิตอลอันนี้กลับไปยังองค์กรที่ออกใบรับรองฉบับนี้ ก็จะทำให้ผู้รับทราบได้ทันทีว่ากุญแจสาธารณะนี้เป็นของบุคคลนั้นจริง ๆ แต่เจ้าใบรับรองดิจิตอลนี้ไม่ได้จะใช้เก็บแค่กุญแจสาธารณะเท่านั้น ยังมีอีกหลายสิ่งที่เก็บอยู่ในใบรับรองดิจิตอล โดยที่มาตรฐานของใบรับรองดิจิตอลที่ใช้กันอย่างแพร่หลายในปัจจุบัน ก็คือมาตรฐาน X.509 เวอร์ชัน 3 จะบังคับให้ใบรับรองดิจิตอลอย่างน้อยต้องมีข้อมูลดังต่อไปนี้

- หมายเลขของใบรับรอง (Serial Number) ก็คือ เลขที่ของใบรับรองดิจิตอลนั่นเอง เปรียบเสมือนเลขที่ของบัตรประชาชนจะไม่ซ้ำกัน
- วิธีการที่ใช้ในการสร้างลายมือชื่อดิจิตอล จะต้องระบุถึงมาตรฐานที่ใช้ในการตรวจสอบความถูกต้องของข้อมูล เช่น นำมาตรฐาน SHA-1 มาใช้ และมาตรฐานที่ใช้ในการเข้ารหัสข้อมูล เช่นนำมาตรฐาน RSA มาใช้ เป็นต้น
- หน่วยงานที่ออกใบรับรอง จะต้องระบุไว้ในใบรับรองดิจิตอลด้วยว่าองค์กร หรือหน่วยงานเป็นคนออกใบรับรองฉบับนี้ เพื่อจะเอาไว้ใช้ตรวจสอบว่าองค์กรที่ออกใบรับรองนี้เชื่อถือได้แค่ไหน
- วันเวลาที่ใบรับรองหมดอายุ จะต้องระบุวันเวลาที่ใบรับรองนี้หมดอายุด้วย
- ชื่อของผู้ถือใบรับรอง ในส่วนนี้ยังรวมถึง E-mail address ของผู้ถือใบรับรองด้วย ไม่ใช่แค่ชื่อและนามสกุล
- กุญแจสาธารณะของผู้ถือใบรับรอง
- ลายมือชื่อดิจิตอลของหน่วยงานที่ออกใบรับรองที่จะต้องมีข้อมูลตรงนี้ เพื่อเป็นการยืนยันว่าใบรับรองฉบับนี้ได้ออกมาโดยองค์กรหรือหน่วยงานนี้จริง ๆ

ดูตัวอย่างใบรับรองดิจิตอล ดังรูปที่ 2.12



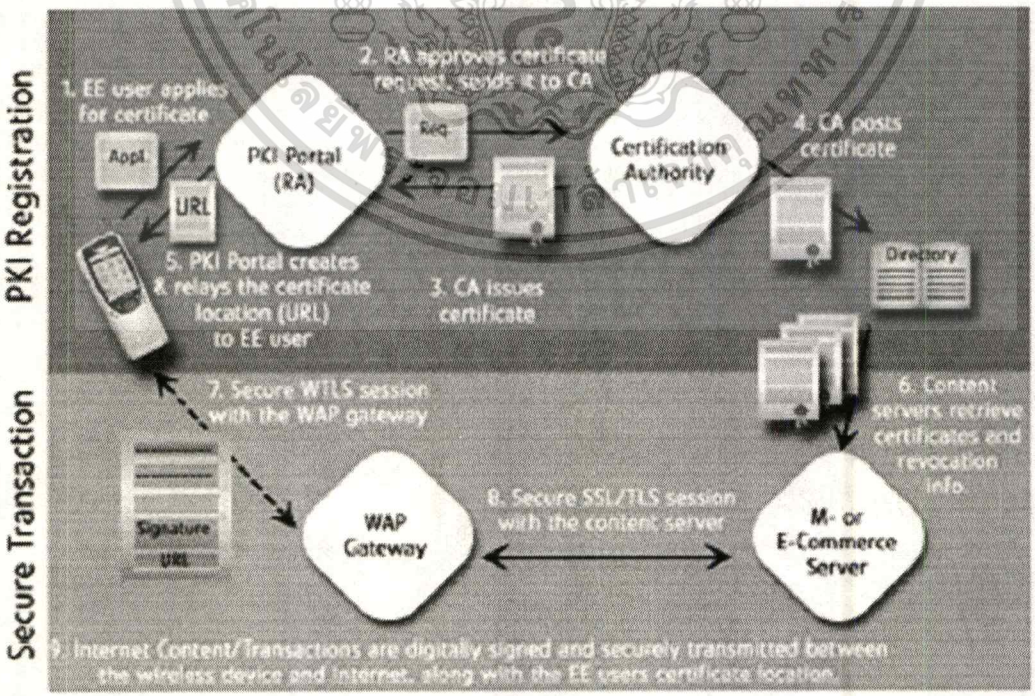
รูปที่ 2.12 แสดงตัวอย่างใบรับรองดิจิตอล

องค์กรออกใบรับรอง ก็มีหน้าที่ออกใบรับรอง เพื่อให้มีการกระบวนการตรวจสอบต่าง ๆ ในการทำงานก็ต้องมีการตรวจเป็นส่วน ๆ ไป โดยจะต้องแสดงตนด้วยว่าเราเป็นใคร และได้รับหนังสือรับรองมาจากองค์กรใด

ใบรับรองดิจิตอลจะแบ่งออกตามลักษณะการใช้งานได้ 3 ประเภท หรือ 3 กลุ่มลักษณะการใช้งาน ได้แก่

1. **ใบรับรองบุคคล** (Personal Certificate) ก็คือใบรับรองที่ใช้รับรองให้กับบุคคลทั่วไป โดยที่ในใบรับรองลักษณะนี้ก็จะมีข้อมูลตามมาตรฐาน X.500 เวอร์ชัน 3 แต่ที่ขาดไม่ได้ก็คือจะต้องมีข้อมูลกุญแจสาธารณะของบุคคลนั้น ๆ ด้วย
2. **ใบรับรองเครื่องแม่ข่าย** (Server Certification) ก็คือใบรับรองใช้รับรองเครื่องแม่ข่าย หรือเว็บไซต์ โดยข้อมูลบที่จะขาดไม่ได้ก็คือจะต้องมีกุญแจสาธารณะของเครื่องแม่ข่าย หรือเว็บไซต์นี้ สาเหตุที่ต้องมีใบรับรองเครื่องแม่ข่าย ก็เพราะว่าในการทำธุรกรรมอิเล็กเทอนิกส์ในปัจจุบัน ส่วนมากจะเป็นการทำธุรกรรมในลักษณะผู้ซื้อเข้าไปซื้อสินค้าหรือทำธุรกรรมผ่านเว็บไซต์ของผู้ขายสินค้า ดังนั้นเพื่อเป็นการยืนยันให้กับผู้ซื้อว่า เว็บไซต์ที่ผู้ซื้อกำลังติดต่ออยู่ด้วยนี้เป็นเว็บไซต์ที่ต้องการติดต่อจริง ๆ
3. **ใบรับรองสำหรับองค์กรออกใบรับรอง** (Certification Authority Certificate) ที่ต้องมีเพราะว่าจะได้เป็นเครื่องยืนยันว่า องค์กรที่ออกใบรับรองเป็นองค์กรที่มีสิทธิ์ในการออกใบรับรองให้กับบุคคลหรือเครื่องแม่ข่ายได้ ใบรับรองดิจิตอลที่ตามมาตรฐาน X.509 เวอร์ชัน 3 หนึ่งในข้อมูลที่จะต้องมีก็คือ ลายมือชื่อดิจิตอล และชื่อหน่วยงานขององค์กรที่ออกใบรับรอง ซึ่งจากข้อมูลตรงนี้ที่จะถูกนำไปใช้ในการตรวจสอบว่าใบรับรองที่ออกด้วยองค์กรนี้ เป็นใบรับรองที่ออกมาจากองค์กรนี้จริง ๆ (ศุภชัย สุขะนินทร์ และธน กันธิพันธ์ . 2544 : 51-82)

ขั้นตอนที่เกี่ยวข้องกับการขอ และออกใบรับรองว่าจะมีขั้นตอนอย่างไรบ้าง ดังรูปที่ 2.13



รูปที่ 2.13 แสดงขั้นตอนการขอ และการทำงานของ PKI Environment

ขั้นตอนที่ 1 ผู้ใช้บริการทำการส่งใบสมัครที่จะขอใช้บริการ หรือขอใบรับรองโดยระบุข้อมูลส่วนตัวที่ทางองค์กรออกใบรับรองต้องการเช่น ชื่อ ที่อยู่ E-mail address เป็นต้น แล้วส่งใบสมัครไปที่องค์กรที่ทำหน้าที่ตรวจสอบข้อมูล และยืนยันตัวบุคคลของผู้ขอใช้บริการ (Registration Authority หรือ RA) โดยที่ RA นี้จะไม่ได้นำเอาเทคนิคทางคอมพิวเตอร์มาใช้ในการตรวจสอบ แต่จะใช้เจ้าหน้าที่ทำการตรวจสอบ และหาข้อมูลของผู้ขอใช้บริการ เพื่อทำการยืนยันตัวบุคคลของผู้ขอใช้บริการว่ามีข้อมูลตรงตามที่ให้มา และมีตัวตนจริงหรือไม่

ขั้นตอนที่ 2 หลังจากที่ RA ได้รับใบสมัครมาจากผู้ขอใช้บริการแล้ว RA ก็จะทำการตรวจสอบข้อมูลที่ได้รับมา เพื่อทำการตรวจสอบข้อมูลของผู้ขอใช้บริการ ถ้าข้อมูลของผู้ขอใช้บริการถูกต้องตรงตามที่ส่งมาในใบสมัคร RA ก็จะส่งใบคำของใบรับรองต่อไปยัง CA อีกทีหนึ่ง

ขั้นตอนที่ 3 หลังจากที่ CA ได้รับใบคำขอใบรับรองที่มาจาก RA แล้วทาง CA ก็จะทำการสร้างใบรับรองให้กับบุคคลตามใบสมัคร โดย CA จำไม่ทำการตรวจสอบข้อมูลของบุคคลตามใบสมัครนี้อีกแล้ว เพราะ CA ถือว่าข้อมูลของบุคคลตามใบสมัครนี้เชื่อถือได้ เพราะว่าทาง RA ได้ทำการตรวจสอบมาให้แล้ว หลังจากนั้น CA ก็จะส่งใบรับรองที่สร้างขึ้นมานี้ กลับไปยังผู้สมัคร

ขั้นตอนที่ 4 หลังจากนี้ CA ส่งใบรับรองให้กับผู้สมัครแล้ว CA ก็จะนำเอาใบรับรองนี้ไปเก็บไว้ในไดเรกทอรีของ CA เพื่อให้บุคคลทั่วไปสามารถเข้ามาตรวจสอบใบรับรองของคู่กรณีที่ทำธุรกรรมอยู่ด้วย เช่น ถ้านายขาวทำการขอใบรับรองจาก CA หลังจากที่ CA ทำการออกใบรับรองให้แต่นายขาวแล้ว CA ก็จะทำการเก็บใบรับรองของนายขาวไว้ในไดเรกทอรีของ CA เพื่อให้นายเขียวสามารถเข้ามาตรวจสอบว่ากุญแจสาธารณะของนายขาวนี้เป็นของนายยาวจริง ๆ เวลาที่นายเขียวต้องทำธุรกรรมอิเล็กทรอนิกส์กับนายขาวจริง ๆ แล้วไดเรกทอรีที่ใช้สำหรับเก็บใบรับรองที่ทาง CA จัดเก็บนั้น จะเก็บไว้ในเว็บไซต์ของ CA เพื่อให้บุคคลทั่วไปสามารถเข้าไปตรวจสอบได้ตลอดเวลา

บริการของ CA จะมีการให้บริการ 2 ด้านใหญ่ ๆ ก็คือ

1. บริการเกี่ยวข้องกับการออกใบรับรอง (Certification Management Service)
2. บริการเสริมต่าง ๆ (Ancillary Service)

ซึ่งบริการต่าง ๆ จะประกอบไปด้วยบริการต่าง ๆ ใน แต่ละด้านอีกมาก

บทที่ 3

วิเคราะห์และออกแบบระบบ

WAP Environment มีองค์ประกอบคล้ายกับ World Wide Web (WWW) Environment แต่ WAP Environment จะข้อแตกต่างกับ WAP Environment หลายอย่างด้วยกัน แต่สิ่งที่ WAP Environment มีก็คือ

1. ผู้ใช้อุปกรณ์ไร้สายจะใช้ความสามารถในการทำงานน้อยกว่าเมื่อเปรียบเทียบกับผู้ใช้ Web โดยทั่วไป โดยจะมีดังนี้

- ใช้ความสามารถของหน่วยประมวลผลน้อย
- ใช้หน่วยความจำน้อย
- ใช้หน่วยเก็บข้อมูลเพื่อเก็บข้อมูลและโปรแกรมน้อย
- ใช้ทรัพยากรของระบบเครือข่ายน้อย มี Bandwidth ที่แคบกว่า
- การเชื่อมต่อที่มีเสถียรภาพน้อยกว่า
- ใช้จอภาพแสดงผลขนาดเล็ก

2. ข้อจำกัดในการคำนวณของอุปกรณ์ไร้สายที่ใช้ในการทำงานของ WAP Environment จะต้องใช้ให้เกิดประสิทธิภาพอย่างเต็มที่ทั้งหน่วยประมวลกลาง หน่วยความจำและหน่วยเก็บข้อมูล

3. โปรโตคอลของ Web-based และ WAP-based จะมีการทำงานที่แตกต่างกัน โดยที่ WAP-based จะมี WAP Gateway เพื่อใช้ในการแปลงข้อมูลที่ได้รับจากโปรโตคอล Web-based แล้วแปลงให้ไปอยู่ในรูปแบบโปรโตคอล WAP-based

สำหรับอุปกรณ์มือถือ และโครงข่ายการสื่อสารไร้สาย จะรวมกันเรียกว่า Mobile Network ซึ่งคาดว่าจะมีการขยายตัวมากขึ้น ซับซ้อน ยุ่งยากมากขึ้น ดังนั้น Mobile Network จึงจำเป็นต้องมีคุณสมบัติดังต่อไปนี้

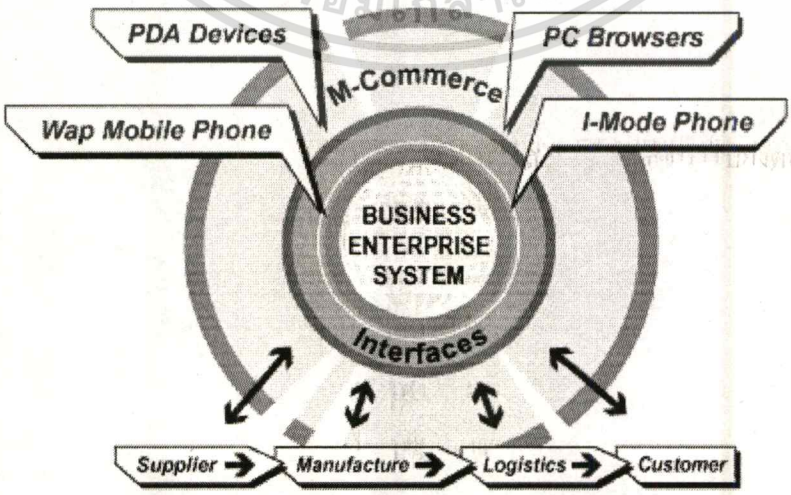
- Interoperable เครื่องลูกข่ายจากผู้ผลิตต่างกัน สามารถใช้บริการจาก Mobile Network ได้
- Scaleable สามารถขยายบริการต่าง ๆ ไปสู่ลูกค้าได้ตามความต้องการ
- Efficient ให้บริการด้วยคุณภาพ
- Reliable ให้บริการที่ไว้ใจได้ ในทุกบริการ

- Secure สามารถรักษาความถูกต้องของข้อมูลของลูกค้า และปกป้องอุปกรณ์ไม่ให้ได้รับ

ข้อดีในการใช้งานของระบบการสื่อสารไร้สาย

- ผู้ใช้มีอิสระในการใช้งาน - มีการความเป็นส่วนตัวในการใช้งานตามที่ผู้ใช้ต้องการ โดยผู้ใช้สามารถติดต่อเข้าไปทำงานกับบริษัท หรือทางบริษัทของผู้ใช้สามารถติดต่อผู้ใช้ได้โดยตรง โดยสามารถพิสูจน์ได้จาก Mobile Session ได้
- การใช้งานไม่ขึ้นกับสถานที่กับเวลาในการใช้งาน - ผู้ใช้อุปกรณ์สื่อสารไร้สายส่วนใหญ่ต้องการทำงานอย่างอิสระจากสถานที่ในการใช้งาน เช่น การค้นหาข้อมูลขณะนั่งบนรถ
- การใช้งานอินเทอร์เน็ตในอุปกรณ์สื่อสารไร้สายเป็นเรื่องใหม่ - การใช้งานอุปกรณ์ไร้สายง่ายขึ้น โดยผู้ใช้งาน ส่วนใหญ่สามารถใช้งานได้อย่างถูกต้องและรวดเร็ว เนื่องจากอินเตอร์เฟตที่ใช้งานง่าย

ในปัจจุบันระบบเครือข่ายโทรศัพท์ไร้สายหรือระบบไร้สายได้ถูกพัฒนาไปยังต่อเนื่อง และก้าวล้ำหน้าไปเรื่อย ๆ เพื่อให้เพียงพอต่อความต้องการในการใช้งานของผู้ใช้และแอบพลิเคชันที่ใช้งานบนระบบเครือข่ายไร้สาย โดยจะเห็นการพัฒนาการของระบบเครือข่ายไร้สาย ซึ่งเริ่มจากความเร็วที่เพียง 9.6 kbps เท่านั้นเอง แต่ในปัจจุบันได้เปลี่ยนไปใช้งานระบบเครือข่ายแบบ GPRS ที่ความเร็ว 40 kbps ซึ่งเพียงพอต่อความต้องการในการใช้งานในระดับหนึ่ง แต่มีแนวโน้มของความเร็วที่เพิ่มสูงขึ้นเพื่อให้สามารถรองรับสิ่งที่จะใช้งานต่าง ๆ ในอนาคตด้วย โดยจะมีองค์ประกอบและโครงสร้างดังรูปที่ 3.1



รูปที่ 3.1 แสดงองค์ประกอบโครงสร้างทางธุรกิจของ M-Commerce

3.1 หลักการพัฒนา WAP Application

- ข้อมูลที่แสดงไม่ควรมากกว่า 4-5 หน้าจอ (16-20 บรรทัด)
- ข้อมูล และข้อความที่แสดงควรสั้นและสื่อความหมาย
- ควรหลีกเลี่ยงการใช้คำที่ยาวหรือตัวย่อที่อาจทำให้ผู้ใช้ตีความหมายผิดได้
- ไม่ควรออกแบบเมนูให้มีหลายระดับมากหรือลึกเกินไป พึงระลึกเสมอว่าผู้ใช้อาจจะหลงทางในระหว่างการใช้งานได้
- ผู้พัฒนาควรทราบข้อจำกัดของเทอร์มินอลแบบต่าง ๆ เพื่อจะได้พัฒนาโปรแกรมประยุกต์ให้เหมาะสม ควรพัฒนาโปรแกรมประยุกต์ให้สามารถใช้ได้กับทุกเทอร์มินอลมินัล ความสามารถและข้อจำกัดต่างของเทอร์มินอลที่ควรทราบ ได้แก่
  - ขนาดของ Card สูงสุดที่สนับสนุน
  - ขนาดของรูปภาพสูงสุดที่สนับสนุน
  - ขนาดของหน้าจอแสดงผล จำนวนแถวและคอลัมน์
  - อัตราส่วนการแสดงผล (Pixel Display ratio)
  - รูปแบบข้อความ (Text Style)
  - การจัดวางข้อความ (Text alignment)
  - การจัดวางรูปภาพ (Image alignment) และการลิงค์จากรูปภาพ
  - ลักษณะของตาราง
  - การจัดวาง Icon Button ต่าง ๆ
  - WTAI ที่รองรับ
  - ลำดับการโหลด Deck

3.2 เครื่องมือที่ใช้ในการพัฒนาระบบ

Web / WAP Server - Microsoft Internet Information Server 5.0

- IIS 5.0 เป็น Web / WAP Server ที่มีการปรับปรุงความสามารถในการทำงานให้สูงกว่า IIS 4.0 มาก ทั้งด้านการรองรับการสร้างการติดต่อจากผู้ใช้ได้มากขึ้น ความเร็วในการทำงานที่มากขึ้น รวมทั้งการใช้งาน การติดตั้งและการบำรุงรักษาที่ง่ายและสะดวกมากขึ้น เลือกเพราะมีความสามารถในการทำงานสูง ติดตั้ง ปรับแต่งและบำรุงรักษาได้ง่าย [ภาคผนวก ข และ ค]

Database Server - MySQL 3.23 Server

- MySQL Server เป็น Database Server ขนาดกลางที่มีความสามารถในการทำงานที่สูง สามารถรองรับการทำงานได้ดี เหมาะกับระบบที่มีขนาดเล็กและขนาดกลาง รวมทั้งง่ายต่อการติดตั้ง การจัดการ และการดูแลรักษาด้วย การเรียกใช้ข้อมูลทำได้ง่าย มีเครื่องมือที่ช่วยในการจัดการที่ดี สามารถนำมาใช้งานได้โดยไม่มีค่าใช้จ่าย เลือกเพราะเหมาะสมกับการใช้งานกับข้อมูลขนาดเล็ก ทำงานได้เร็ว ติดตั้ง ปรับแต่ง และบำรุงรักษาได้ง่าย

Certification Authority Server (CA)

- Microsoft Certification Authority Server เป็น Server ที่บริการเกี่ยวกับใบรับรองแบบ PKI เพื่อให้ผู้ใช้บริการสามารถขอใช้ ยกเลิก ใบรับรองได้ มีเครื่องมือที่สามารถใช้งานได้ง่าย ทั้งในการติดตั้ง การปรับแต่งระบบ การบำรุงรักษาระบบ และการจัดการระบบ เหมาะกับการใช้งานในทุกระดับ ขึ้นอยู่กับการปรับแต่งให้เหมาะสมกับระบบ เช่นสามารถใช้งานได้ทั้งแบบ Standalone และ Enterprise มีความยืดหยุ่นในการปรับแต่งระบบ เลือกเพราะติดตั้ง ปรับแต่งได้ง่าย ยืดหยุ่นในการปรับแต่งระบบ [ภาคผนวก ก และ ค]

WAP Gateway

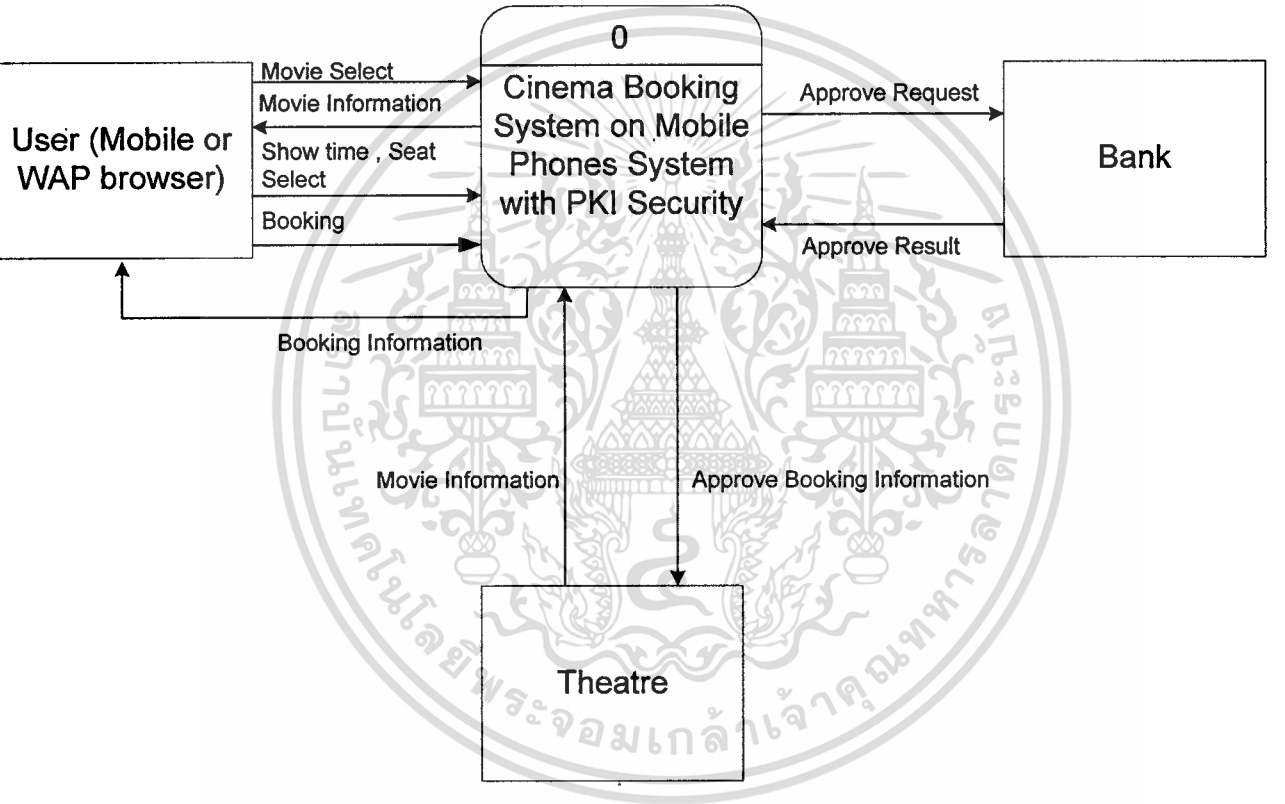
- Captaris Infinite WAP Gateway เป็น WAP Gateway ที่รองรับมาตรฐานโปรโตคอล WAP 1.2.1 รองรับมาตรฐานโปรโตคอลที่เกี่ยวกับความปลอดภัยด้วยเช่น WTLS SSL และรองรับความสามารถในการทำโปรโตคอล Convert อีกด้วย ซึ่งถือได้ว่าเป็น WAP Gateway ที่มีความสามารถครบถ้วนในการใช้งาน เลือกเพราะมีความสามารถในการรองรับการจัดการด้านความปลอดภัย สามารถทำหน้าที่เป็นโปรโตคอล Convert ได้อย่างสมบูรณ์

WAP Browser Agent

- Nokia Internet Toolkit with Nokia Mobile Browser เป็น Mobile Phones Simulation ที่สามารถแสดงผล และทำงานร่วมกับแอพพลิเคชั่นที่รองรับมาตรฐาน WAP ได้เป็นอย่างดี มีความเร็ว ความเสถียร และความยืดหยุ่นในการทำงานสูง เลือกเพราะมีความยืดหยุ่นในการใช้งานสูง ใช้งานง่าย

3.3 การออกแบบโครงสร้างการทำงานของระบบ

ภาพรวมของการทำงานของระบบการจองตั๋วภาพยนตร์ผ่านโทรศัพท์มือถือโดยอาศัยความปลอดภัยแบบ PKI จะแสดงในรูปแบบของ Context Diagram ดังรูปที่ 3.2 ส่วนการแสดงการไหลของข้อมูล จะแสดงโดย Data Flow Diagram Level 1 ซึ่งจะแสดงให้เห็นถึงข้อมูลต่างๆที่สัมพันธ์กันในแต่ละการทำงาน โดยจะแสดงในรูปที่ 3.3



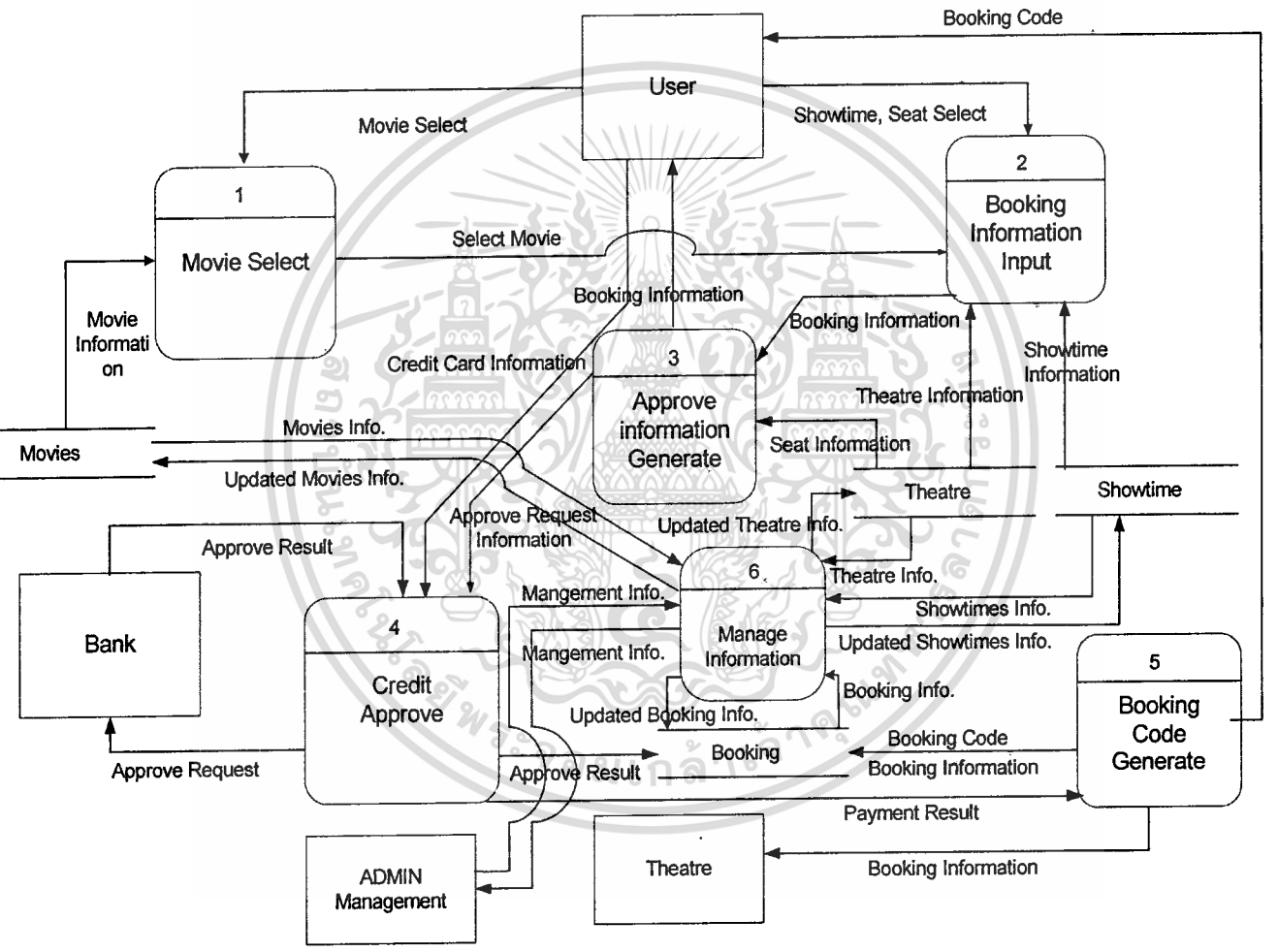
รูปที่ 3.2 แสดง Context Data Flow Diagram ของระบบจองตั๋วภาพยนตร์ผ่านโทรศัพท์มือถือโดยอาศัยความปลอดภัยแบบ PKI

ข้อมูลที่ส่งผ่านในแต่ละส่วน

- ระหว่างระบบกับธนาคาร
  - ◆ รหัสบัตรเครดิต (ชื่อผู้ถือบัตร/หมายเลขบัตรเครดิต/วันที่หมดอายุ)
  - ◆ ผลจากการอนุมัติ
- ระหว่างระบบกับโรงภาพยนตร์

- ◆ ข้อมูลการจองตั๋วชมภาพยนตร์
- ◆ ข้อมูลโรงภาพยนตร์

- ระหว่างระบบกับผู้ใช้
  - ◆ รายชื่อภาพยนตร์ รอบภาพยนตร์ จำนวนที่นั่ง รหัสรับตั๋วภาพยนตร์
  - ◆ รายละเอียดการจองตั๋วภาพยนตร์

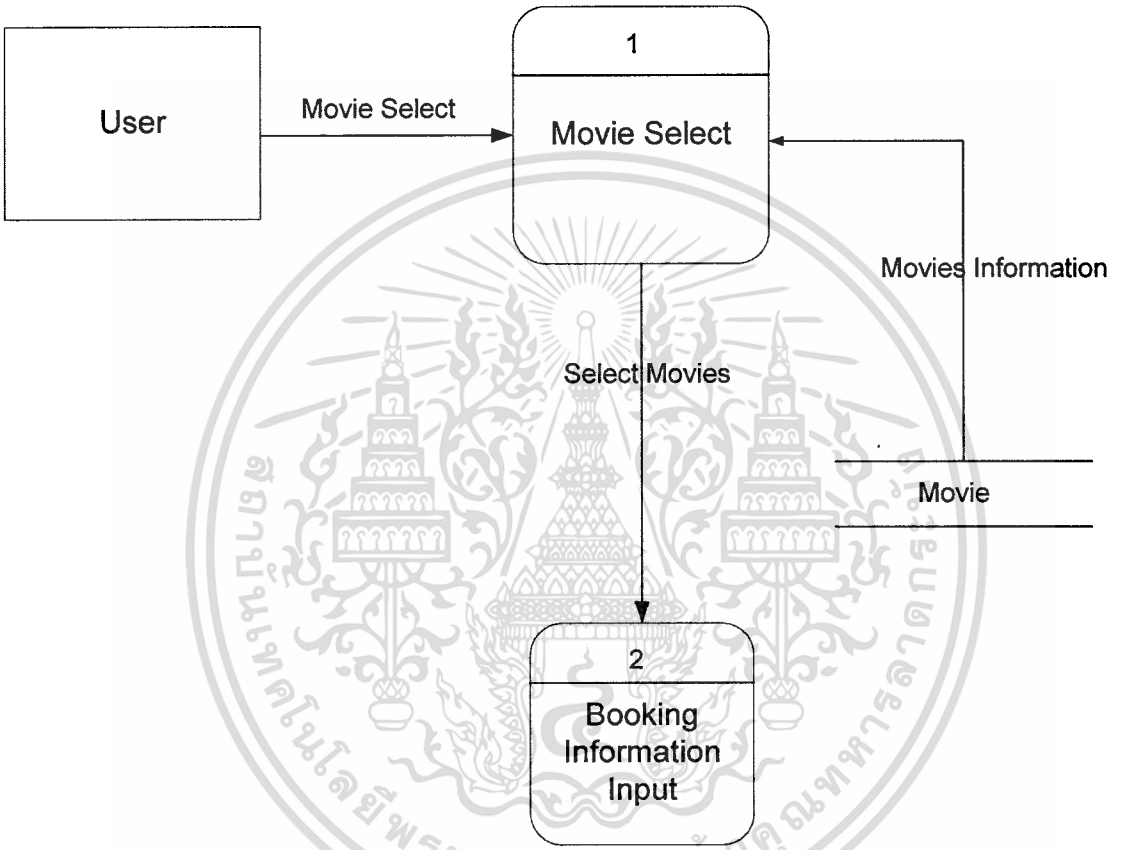


รูปที่ 3.3 แสดง Data Flow Diagram Level 1 ของระบบจองตั๋วภาพยนตร์ผ่านโทรศัพท์มือถือโดยอาศัยความปลอดภัยแบบ PKI

Data Flow Diagram Level 1

- เริ่มจากผู้ใช้จะทำการเรียก URL เพื่อค้นหาภาพยนตร์หรือเวลาฉายภาพยนตร์ที่ต้องการ
- ผู้ใช้จะเลือกภาพยนตร์ที่ต้องการจอง และทำการจองภาพยนตร์

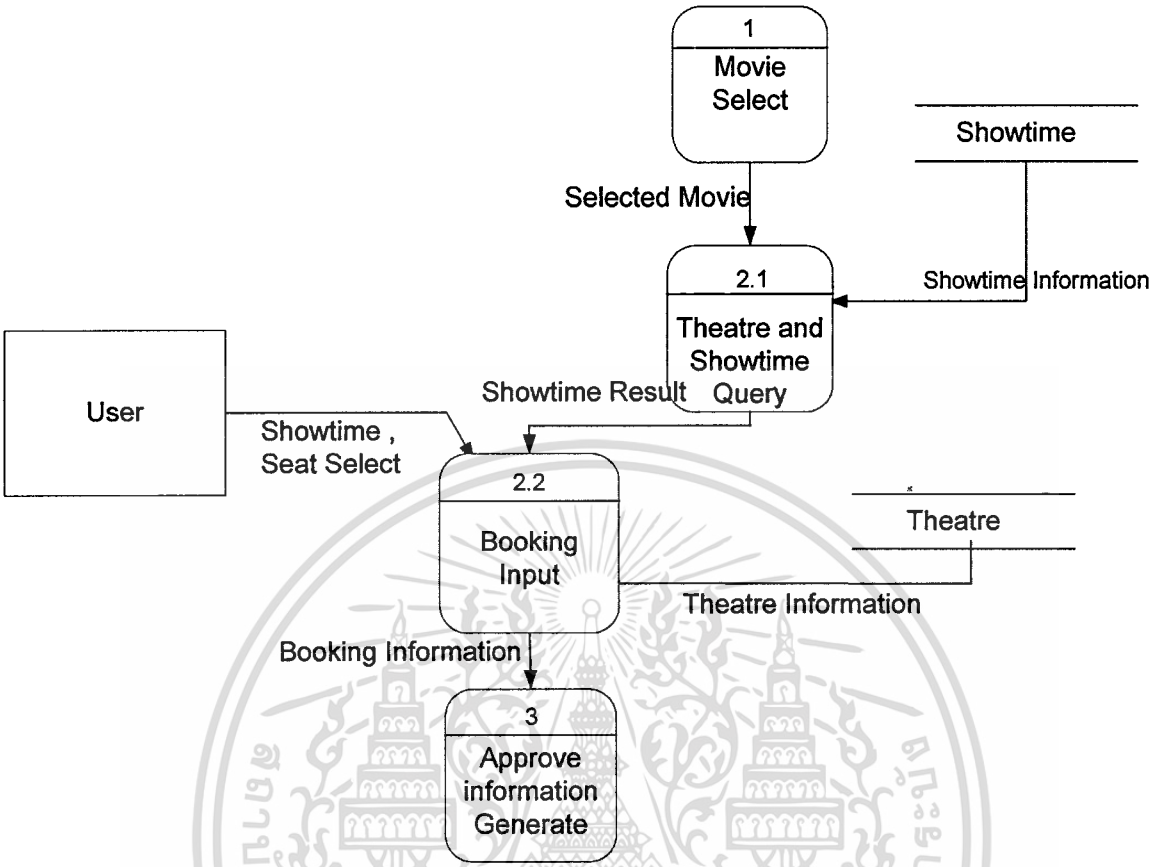
- ระบบจะติดต่อกับธนาคารเพื่อทำการ Approve วงเงินที่ใช้ในการจองภาพยนตร์
- ผู้ใช้จะได้รับ Code ในการจองภาพยนตร์



รูปที่ 3.4 แสดง Data Flow Diagram Level 1 ใน Process ที่ 1

การทำงานของ Process ที่ 1

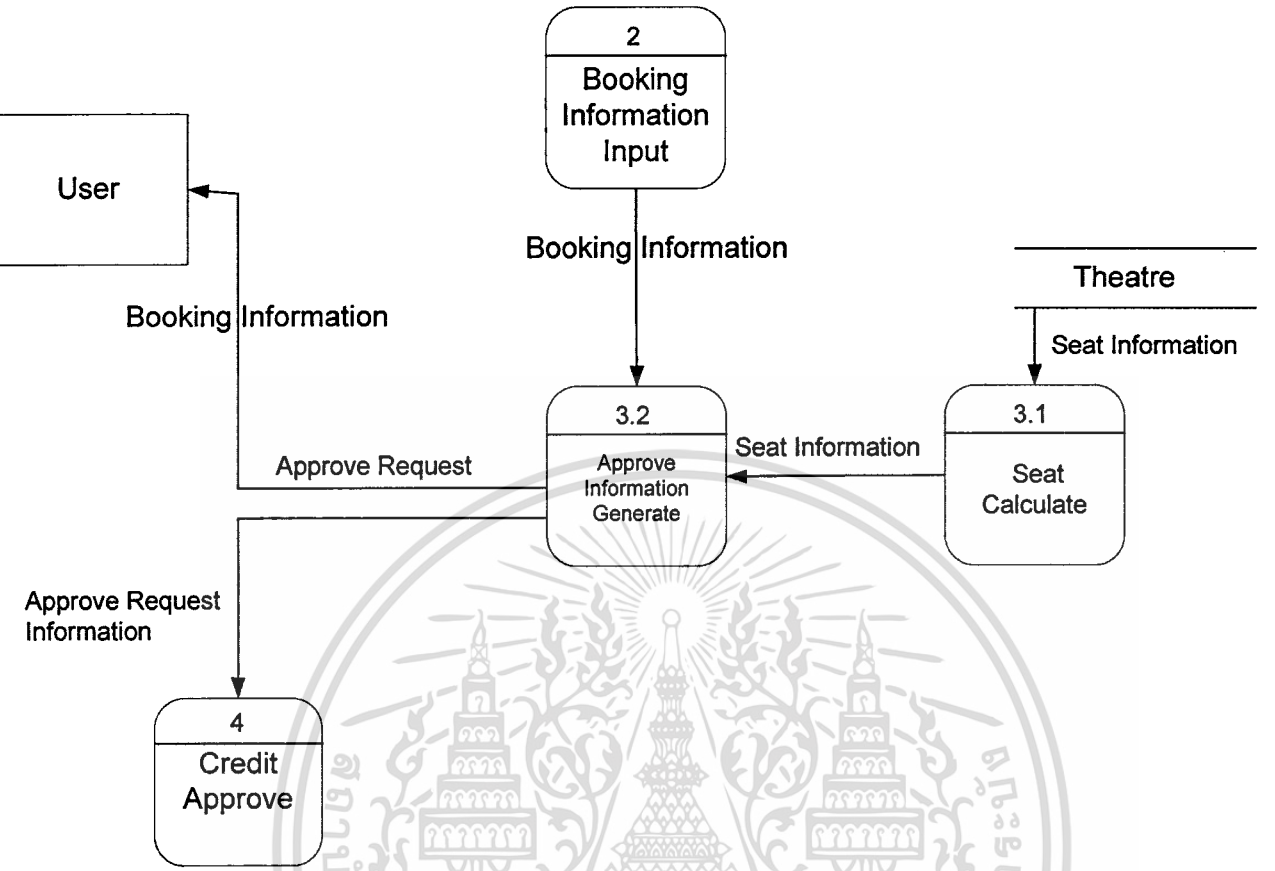
- เริ่มต้นจากผู้ใช้จะทำการเรียก URL สำหรับเพื่อค้นหารายชื่อภาพยนตร์
- ระบบจะทำการดึงข้อมูลจากตาราง Movie เพื่อแสดงรายชื่อภาพยนตร์ที่กำลังฉายอยู่ และรอบฉายทั้งหมดของภาพยนตร์เรื่องนั้น
- ผู้ใช้ทำการเลือกภาพยนตร์ที่ต้องการจะชม



รูปที่ 3.5 แสดง Data Flow Diagram Level 2 ใน Process ที่ 2

การทำงานของ Process ที่ 2

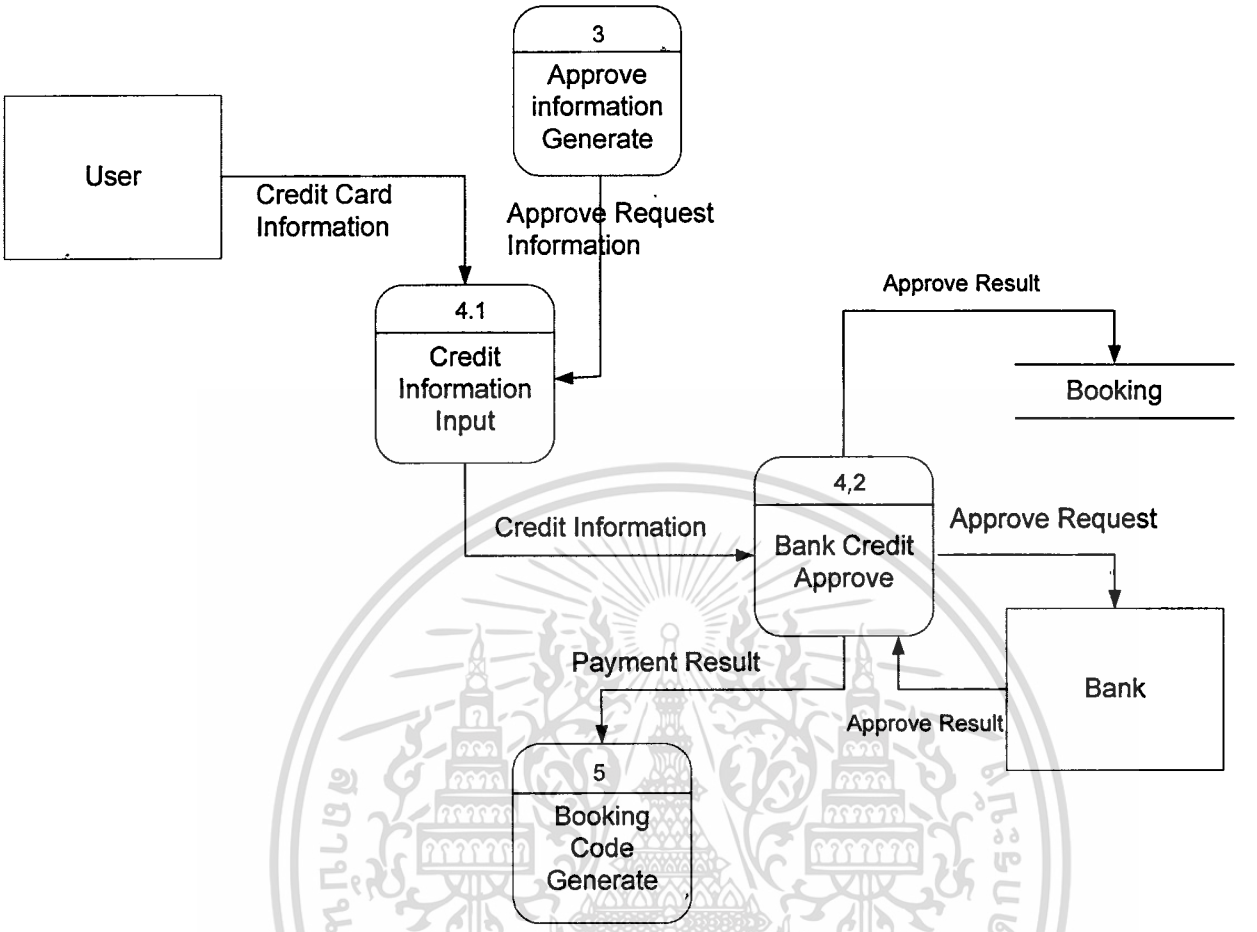
- เมื่อผู้ใช้เลือกภาพยนตร์ที่ต้องการชมแล้วให้ทำการเลือกโรงภาพยนตร์ที่ต้องการชมโดยดึงข้อมูลจากตาราง Theatre แล้วระบบจะแสดงเวลารอบที่เปิดให้จองได้ โดยจะดึงข้อมูลจาก ตาราง Showtime
- ผู้ใช้ทำการกรอกข้อมูลเพื่อเริ่มทำการจองภาพยนตร์และจำนวนที่นั่งที่ต้องการ



รูปที่ 3.6 แสดง Data Flow Diagram Level 2 ใน Process ที่ 3

การทำงานของ Process ที่ 3

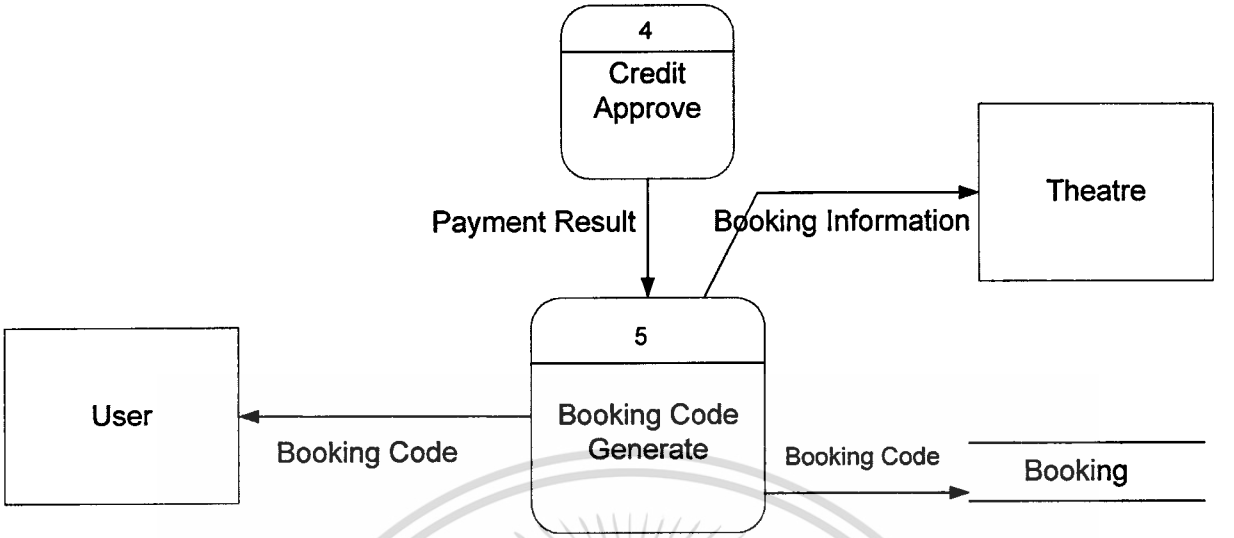
- เมื่อผู้ใช้ทำการเลือกข้อมูลเกี่ยวกับการจองภาพยนตร์แล้ว ก็จะมีการคำนวณเกี่ยวกับจำนวนที่นั่งและราคาของที่นั่งที่ได้ทำการจองไว้ โดยการดึงข้อมูลจากตาราง Theatre
- เมื่อคำนวณราคาแล้วจะตรวจสอบความถูกต้องของข้อมูลการจองอีกครั้ง



รูปที่ 3.7 แสดง Data Flow Diagram Level 2 ใน Process ที่ 4

การทำงานของ Process ที่ 4

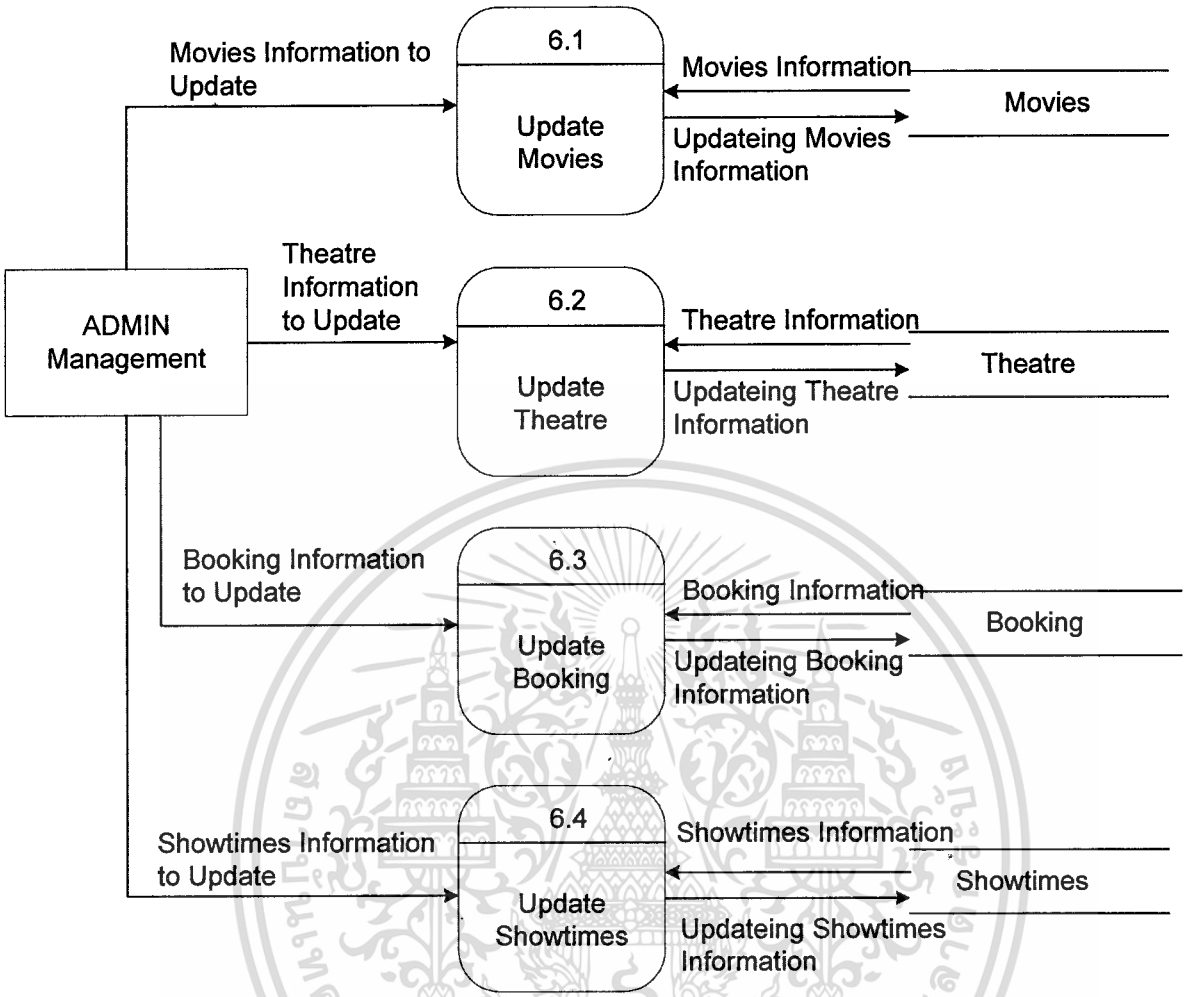
- เมื่อขั้นตอนเกี่ยวกับการจองตั๋วภาพยนตร์ เสร็จแล้ว ก็จะมาถึงการจ่ายเงินโดยผ่านบัตรเครดิต โดยผู้ใช้จะทำการกรอกข้อมูลของบัตรเครดิต
- ระบบจะทำการติดต่อไปยังธนาคารเพื่อทำการตรวจสอบและอนุมัติวงเงินในการใช้จ่ายและแจ้งผลกลับมายังระบบ และทำการบันทึกผลการดำเนินการลงตาราง Booking ด้วย
- ระบบจะแจ้งผลในการดำเนินการกับธนาคารให้กับผู้ใช้ทราบ โดยจะแจ้ง Code ที่ได้จองสำเร็จแล้วแก่ผู้ใช้ได้ทราบ



รูปที่ 3.8 แสดง Data Flow Diagram Level 1 ใน Process ที่ 5

การทำงานของ Process ที่ 5

- ระบบรับผลจากการดำเนินงานจาก Process ที่ 4 เพื่อทำการบันทึกข้อมูลเกี่ยวกับการจองลงตาราง Booking และจะทำการแก้ไขจำนวนที่นั่งที่เหลือที่สามารถจองได้ในตาราง Theatre
- ระบบจะทำการแจ้งผลการจอง และ Booking Code กลับไปยังผู้ใช้เพื่อนำ Booking Code ไปทำการรับตั๋วชมภาพยนตร์ที่ได้ทำการจองไว้



รูปที่ 3.9 แสดง Data Flow Diagram Level 2 ใน Process ที่ 6

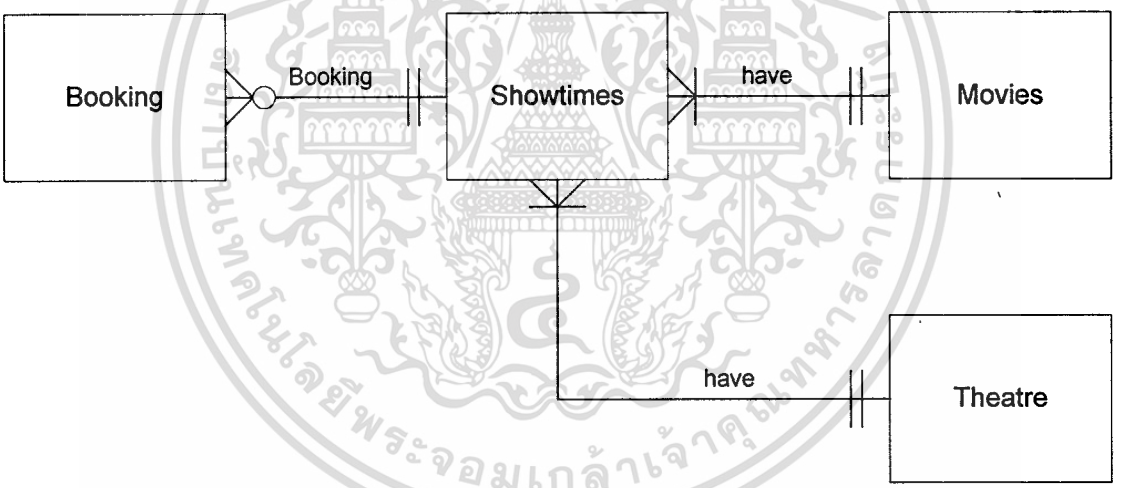
การทำงานของ Process ที่ 6

- การทำงานในส่วนนี้เป็นส่วนของผู้ดูแลระบบที่จะต้องจัดการข้อมูลคือผู้ดูแลระบบสามารถที่จะจัดการเกี่ยวกับข้อมูลในฐานข้อมูลทั้งหมด
- ผู้ดูแลระบบจะสามารถดึงข้อมูลจากตาราง Movies ขึ้นมาตรวจสอบและสามารถเพิ่มเติมข้อมูลหรือปรับปรุงข้อมูลในตาราง Movies ได้
- ผู้ดูแลระบบจะสามารถดึงข้อมูลจากตาราง Theatre ขึ้นมาตรวจสอบและสามารถเพิ่มเติมข้อมูลหรือปรับปรุงข้อมูลในตาราง Theatre ได้
- ผู้ดูแลระบบจะสามารถดึงข้อมูลจากตาราง Booking ขึ้นมาตรวจสอบและสามารถเพิ่มเติมข้อมูลหรือปรับปรุงข้อมูลในตาราง Booking ได้

- ผู้ดูแลระบบจะสามารถดึงข้อมูลจากตาราง Showtimes ขึ้นมาตรวจสอบและสามารถเพิ่มเติมข้อมูลหรือปรับปรุงข้อมูลในตาราง Showtimes ได้

3.4 การออกแบบฐานข้อมูล

ฐานข้อมูลของระบบจองตั๋วภาพยนตร์ จะมีความสัมพันธ์กัน หรืออาจจะไม่มีความสัมพันธ์กัน หรือมีความสัมพันธ์กันบางส่วนขึ้นอยู่รายละเอียดข้อมูลที่จัดเก็บ โดยการออกแบบฐานข้อมูลของระบบนี้ จะแสดงด้วย Entity Relationship Data Model ดังรูปที่ 3.10



รูปที่ 3.10 Entity Relationship Data Model ของระบบจองตั๋วชมภาพยนตร์

3.5 ตารางแสดงรายละเอียดของข้อมูลทั้งหมดที่จัดเก็บในระบบ

ตารางที่ 3.1 ตารางในฐานข้อมูลทั้งหมดของระบบ

Field Name	Description
Booking	ตารางข้อมูลการจองตั๋วภาพยนตร์
Theatre	ตารางข้อมูลของโรงภาพยนตร์
Showtimes	ตารางข้อมูลรอบฉายภาพยนตร์
Movies	ตารางข้อมูลเกี่ยวกับภาพยนตร์

ตารางที่ 3.2 คุณลักษณะต่าง ๆของ Entity Booking (การจองตั๋ว)

Key	Field Name	Data Type	Description
P.K.	BID	Int(8)	รหัสเกี่ยวกับการจองตั๋วชมภาพยนตร์
	Bphone	Varchar(10)	เบอร์โทรศัพท์ของผู้จองตั๋ว
F.K. (Showtimes)	SID	Int(5)	รหัสของรอบฉายภาพยนตร์
	Tbooking	Varchar(22)	รอบภาพยนตร์ที่ทำการจอง (วัน-เวลาที่จอง)
	Bseat	Int(3)	จำนวนที่นั่งที่ทำการจอง
	Bcode	Int(6)	รหัสสำหรับการรับตั๋วที่จอง
	Bstatus	char(1)	สถานะของการจองตั๋ว (1=ผ่าน 2=ไม่ผ่าน)
	Bref_Code	Varchar(7)	รหัสที่ได้จากการอนุมัติวงเงิน
	Bprint	Varchar(22)	วันและเวลาที่พิมพ์ตั๋ว

ตารางที่ 3.3 คุณลักษณะต่าง ๆของ Entity Theatre (ข้อมูลโรงภาพยนตร์)

Key	Field Name	Data Type	Description
P.K.	TID	Int(3)	รหัสโรงภาพยนตร์
	Tname	Varchar(30)	ชื่อโรงภาพยนตร์
	Ttotal	Int(4)	จำนวนที่นั่งของโรงภาพยนตร์
	Tsseat	Int(3)	จำนวนที่นั่งสำหรับการขาย
	Tbseat	Int(3)	จำนวนที่นั่งสำหรับการจองตั๋ว

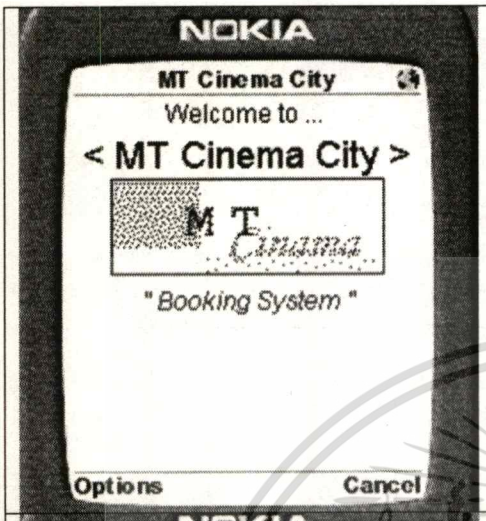
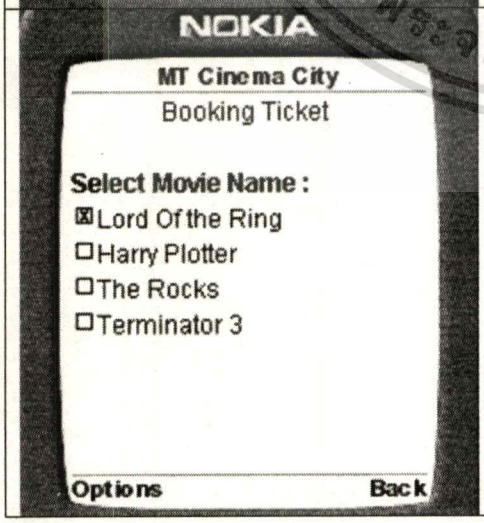
ตารางที่ 3.4 คุณลักษณะต่าง ๆของ Entity Showtimes (ข้อมูลรอบฉายภาพยนตร์)

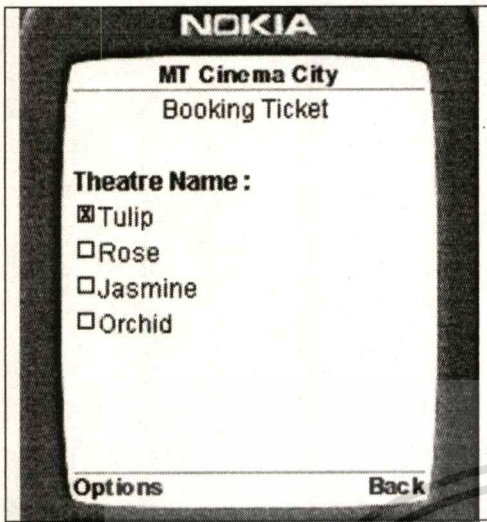
Key	Field Name	Data Type	Description
P.K.	SID	Int(5)	รหัสของรอบฉายภาพยนตร์
F.K. (Movies)	MID	Int(5)	รหัสของภาพยนตร์
F.K. (Theatre)	TID	Int(3)	รหัสของโรงภาพยนตร์
	Stime1	Varchar(12)	เวลาฉาย
	Sseatavail	int(3)	จำนวนที่นั่งที่สามารถจองได้
	Price	int(3)	ราคาของตั๋วของแต่ละที่นั่ง

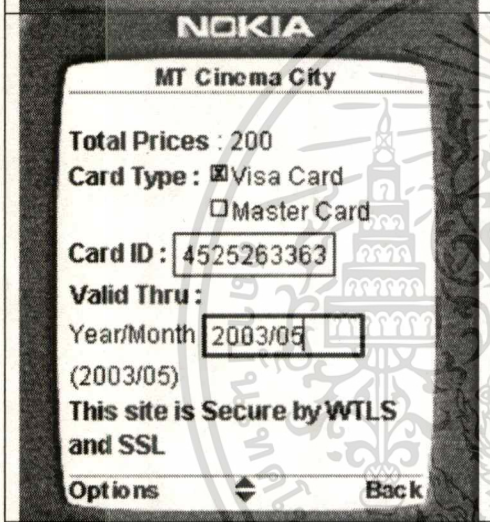
ตารางที่ 3.5 คุณลักษณะต่าง ๆของ Entity Movies (ข้อมูลเกี่ยวกับภาพยนตร์)

Key	Field Name	Data Type	Description
P.K.	MID	Int(5)	รหัสภาพยนตร์
	Thtitle	Varchar(255)	ชื่อเรื่องภาพยนตร์ภาษาไทย
	Engtitle	Varchar(255)	ชื่อเรื่องภาพยนตร์ภาษาอังกฤษ
	Mstart	Varchar(10)	วันที่เริ่มเข้าฉาย
	Mstop	Varchar(10)	วันที่สิ้นสุดการฉาย
	Mstatus	Char(1)	สถานะการฉายของภาพยนตร์ (c=current, o=out)

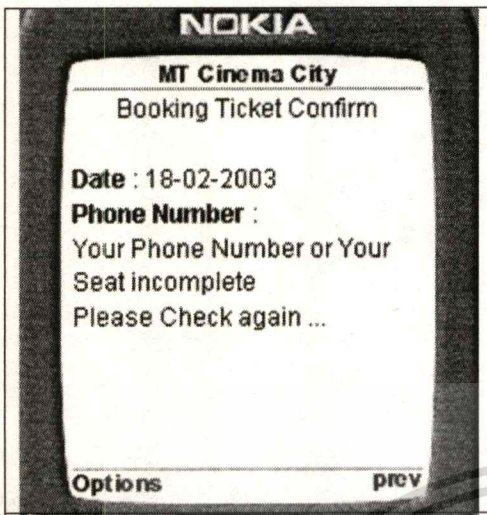
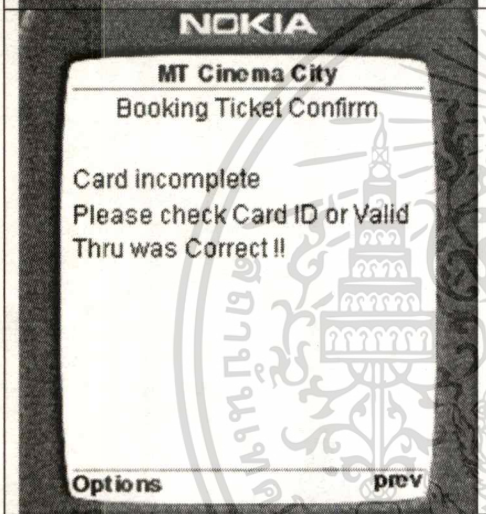
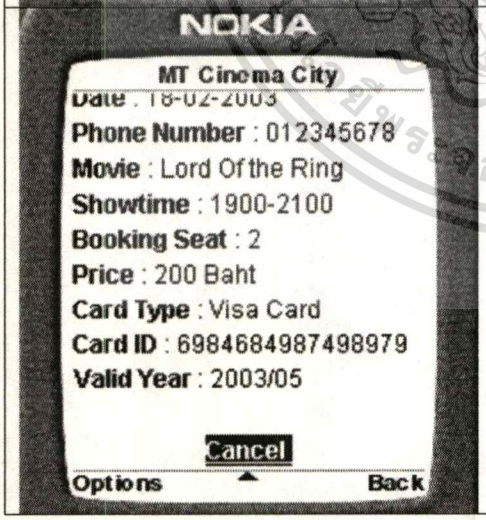
3.6 โครงสร้างการทำงานของ Cinema Booking System (ส่วน Mobile Client)

	- หน้าจอแรกที่จะแสดงข้อความต้อนรับผู้ใช้สู่การใช้งานระบบ
	- เป็นเมนูให้เลือกว่าผู้ใช้ต้องการค้นหาภาพยนตร์หรือต้องการจองตั๋วภาพยนตร์
	- เป็นเมนูที่ให้เลือกชื่อภาพยนตร์ที่มีฉายในวันนั้น ๆ ให้ผู้ใช้เลือก

	- เลือกโรงภาพยนตร์ที่ต้องการจองตั๋วภาพยนตร์
	- เลือกรอบ ที่ต้องการดูภาพยนตร์
	- กรอกหมายเลขโทรศัพท์มือถือของผู้จอง และจำนวนที่นั่งที่ต้องการจอง

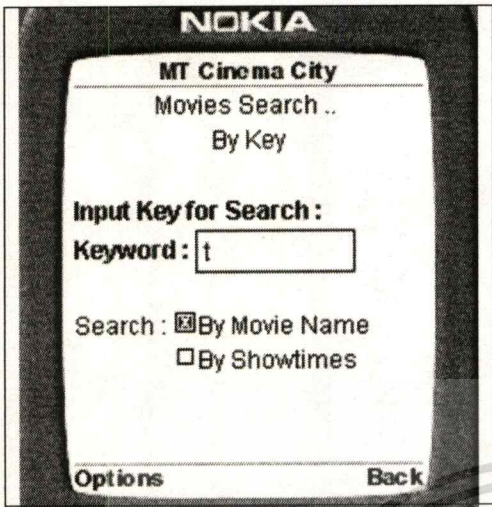
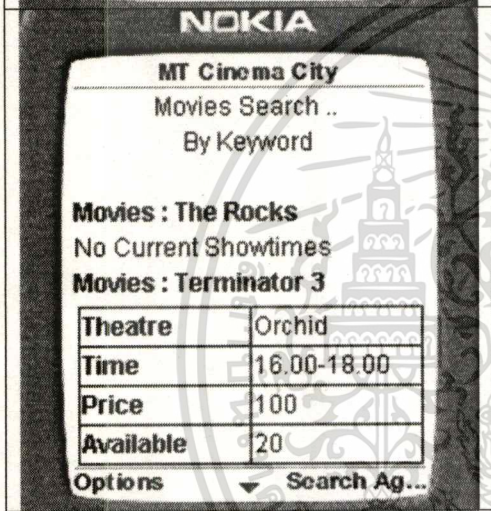
	- สรุปรายละเอียดครั้งที่ 1 ในการดำเนินการจอง
	- กรอกหมายเลขบัตรเครดิตและวันหมดอายุของบัตร เพื่อตรวจความถูกต้องของบัตร โดยในขั้นตอนการทำงานขั้นตอนนี้ ได้ทำงานบนพื้นฐานความปลอดภัยแบบ PKI โดยอาศัย WTLS และ SSL เป็นตัวดำเนินการ
	- ยืนยันการทำรายการทั้งหมด

	- การทำรายการได้ดำเนินไปอย่างถูกต้อง และการดำเนินรายการได้เสร็จสิ้น โดยผู้จองตั๋วจะได้รับหมายเลขการจองเพื่อนำไปรับตั๋วต่อไป
	- เป็นกรณีที่เลือกภาพยนตร์แล้วไม่มีรอบการฉายภาพยนตร์เรื่องนั้น ๆ
	- เป็นกรณีที่กรอกหมายเลยโทรศัพท์ไม่ถูกต้อง หรือกรอกจำนวนที่นั่งไม่ถูกต้อง

	- เป็นกรณีที่กรอกหมายเลยโทรศัพท์ไม่ถูกต้อง หรือ กรอกจำนวนที่นั่งไม่ถูกต้อง เช่นกัน
	- เป็นกรณีที่เรากรอกข้อมูลของบัตรเครดิตไม่ครบถ้วน หรือไม่ถูกต้อง หรือ วันหมดอายุของบัตรไม่ถูกต้อง
	- เป็นการยกเลิกการทำรายการทั้งหมดก่อนการดำเนินการการจ่ายเงินจะเสร็จสิ้น โดยเลือกที่ Cancel

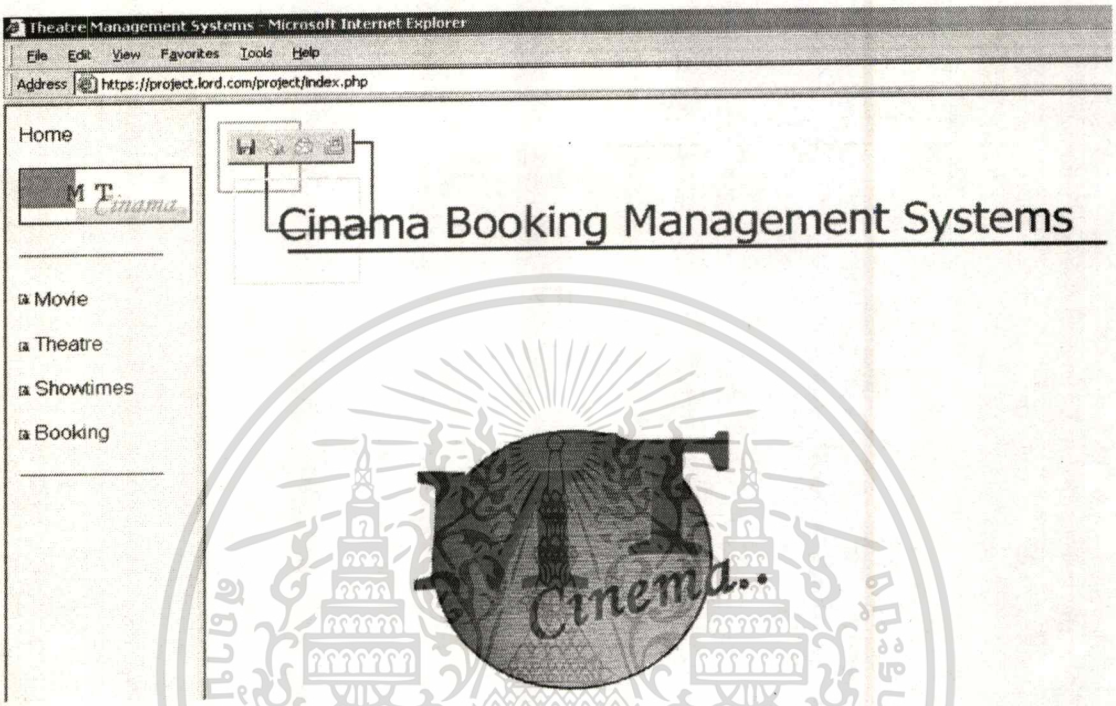
	- ส่วนการค้นหาข้อมูลของภาพยนตร์ โดยค้นได้จาก 2 ประเภท คือ ค้นโดยชื่อของภาพยนตร์ หรือ ค้นโดย Keyword
	- เลือกการค้นหาโดยค้นโดยการใช้ชื่อภาพยนตร์
	- เลือกชื่อภาพยนตร์ที่ต้องการค้นหารายละเอียดเพิ่มเติม

<table>
<tr>
<td> 
</td>
<td>- รายละเอียดของภาพยนตร์ที่ได้รับ</td>
</tr>
<tr>
<td> 
</td>
<td>- ค้นหารายละเอียดภาพยนตร์โดยอาศัย Keyword</td>
</tr>
<tr>
<td> 
</td>
<td>- สามารถค้นหาได้จาก 2 ประเภทของ Keyword คือ จากชื่อภาพยนตร์ หรือ จากเวลาที่ฉายในแต่ละรอบ</td>
</tr>
</table>

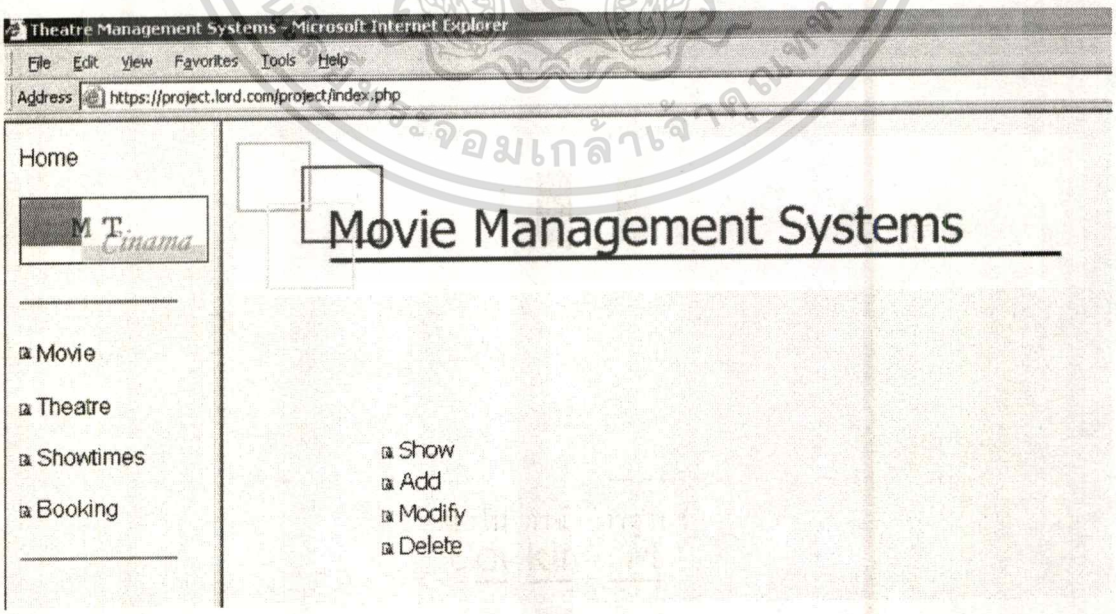
<table>
<tr>
<td> 
</td>
<td>- กรอก Keyword และเลือกประเภทของการค้นหา</td>
</tr>
<tr>
<td> 
</td>
<td>- รายละเอียดที่ได้รับจากการค้นหา</td>
</tr>
<tr>
<td> 
</td>
<td>- กรณีที่ไม่ได้กรอก Keyword ให้กรอก Keyword แล้วให้ค้นหาอีกครั้งหนึ่ง</td>
</tr>
</table>

<table>
<tr>
<td> 
</td>
<td>- การค้นหารายละเอียดโดยใช้ Keyword และเลือกประเภทการค้นหาเป็น ค้นหาโดยเวลาฉายภาพยนตร์</td>
</tr>
<tr>
<td> 
</td>
<td>- รายละเอียดที่ได้จากการค้นหา</td>
</tr>
</table>

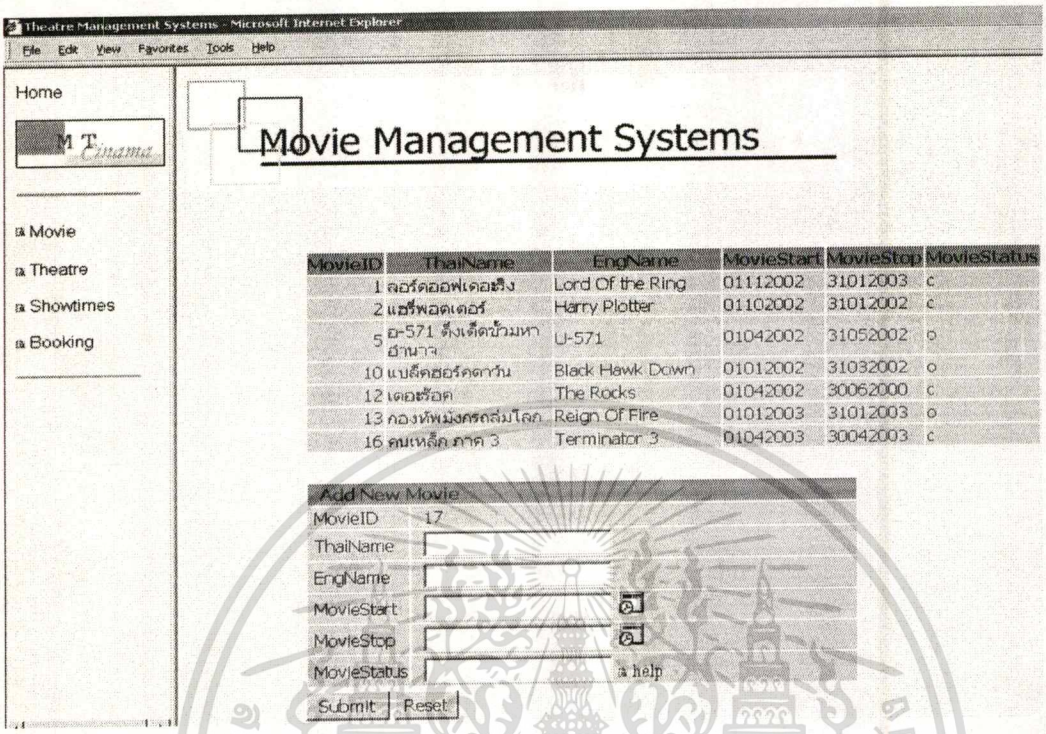
3.7 โครงสร้างการทำงานของ Cinema Booking System (ส่วนการจัดการฐานข้อมูลของผู้ดูแลระบบ)



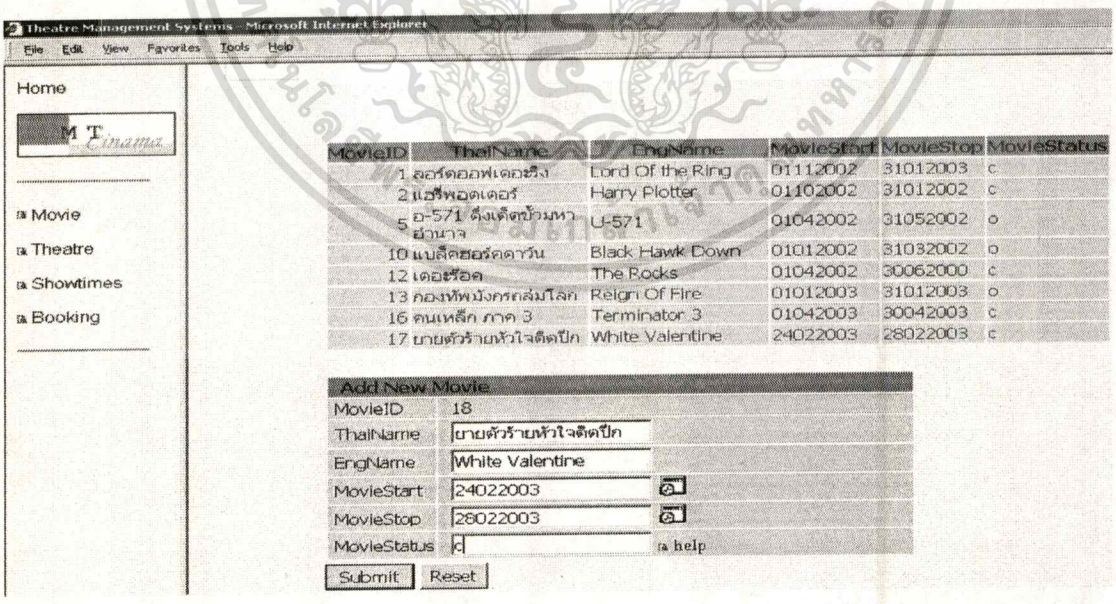
รูปที่ 3.11 แสดงเมนูหลักในการจัดการฐานข้อมูลของผู้ดูแลระบบ



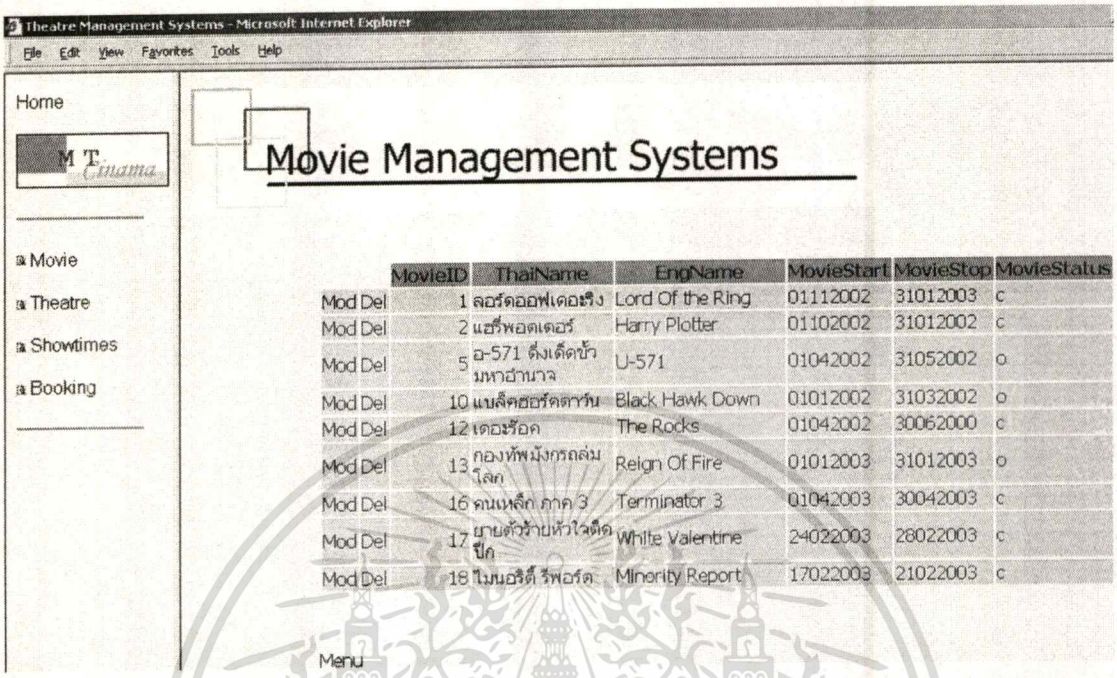
รูปที่ 3.12 แสดงเมนูย่อยของแต่ละหมวดในการจัดการฐานข้อมูล



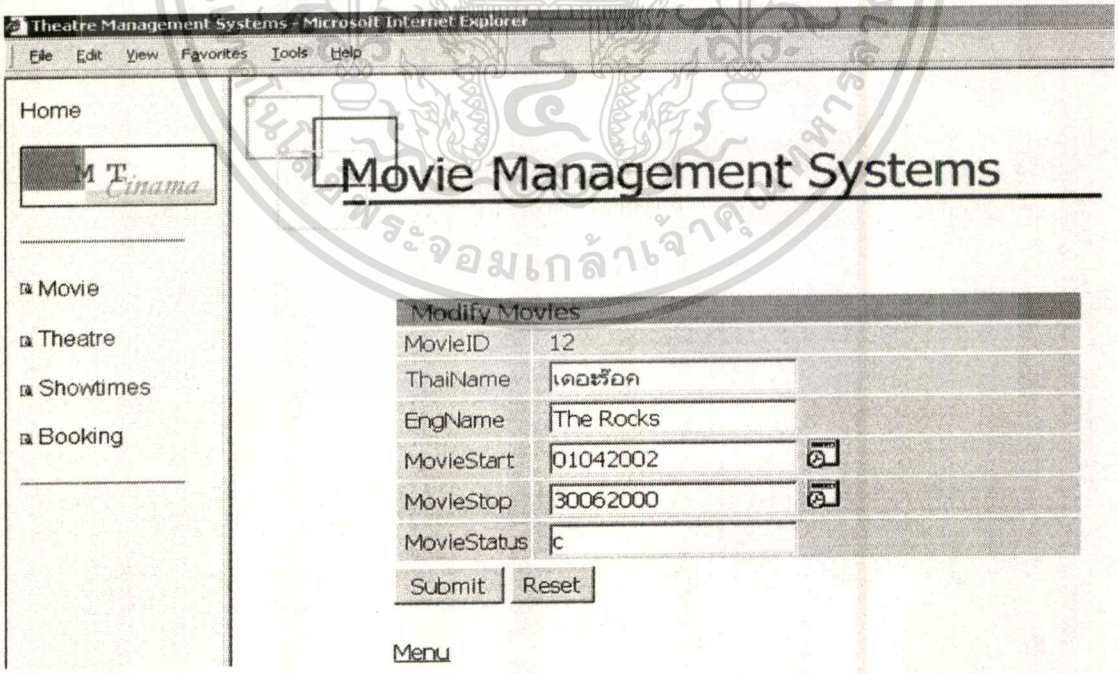
รูปที่ 3.13 แสดงการแสดงข้อมูลของแต่ละหมวด



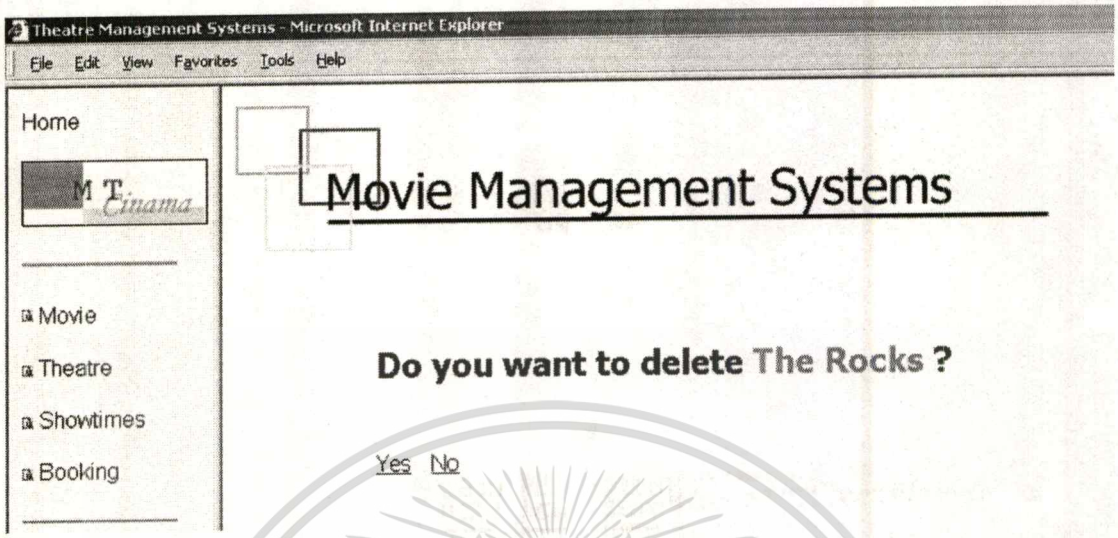
รูปที่ 3.14 แสดงวิธีการเพิ่มข้อมูลของแต่ละหมวด



รูปที่ 3.15 แสดงส่วนของการปรับปรุงข้อมูล และการลบข้อมูล



รูปที่ 3.16 แสดงการปรับปรุงข้อมูลที่ต้องการ



รูปที่ 3.17 แสดงส่วนของการลบข้อมูลของฐานข้อมูล

บทที่ 4
สรุปการพัฒนาโครงการ

วัตถุประสงค์หลักของโครงการพัฒนาระบบงานฉบับนี้ คือการประยุกต์ใช้เทคนิคการวิเคราะห์และออกแบบระบบงาน เพื่อให้สามารถนำมาใช้งานกับระบบงานจริงได้ และเป็นการจำลองระบบบางส่วนเพื่อให้มองเห็นการทำงานโดยรวมของการทำธุรกรรมผ่านทางระบบโทรศัพท์หรือระบบการสื่อสารแบบไร้สาย ซึ่งจะสามารถตอบสนองความต้องการ และเพิ่มความสะดวกในการใช้งานให้แก่ผู้ใช้ที่ต้องการใช้งานได้โดยไม่ขึ้นกับสถานที่ใช้งาน หรือไม่จำกัดกับสถานที่ที่ต้องการใช้งานระบบได้ ซึ่งก็คือการพัฒนาระบบมาใช้งานได้ตรงความต้องการของผู้ใช้มากขึ้น

ปัญหาที่เกิดขึ้นในการออกแบบและพัฒนาระบบ

ในขั้นตอนการพัฒนาต่าง ๆ ได้พบปัญหาหรือข้อจำกัดต่าง ๆ ทั้งทางด้านซอฟต์แวร์และฮาร์ดแวร์ของเทคโนโลยีของ WAP และเทคโนโลยีของระบบรักษาความปลอดภัยของข้อมูล ซึ่งทั้งยังเป็นส่วนที่ยังไม่สมบูรณ์หรือยังอยู่ในการค้นคว้าวิจัย และพัฒนาอยู่ ซึ่งการออกแบบและพัฒนาระบบจึงค่อนข้างไม่สะดวก เพราะถือได้ว่าระบบ WAP หรือเทคโนโลยีที่เกี่ยวกับความปลอดภัยบนระบบธุรกรรมแบบอิเล็กทรอนิกส์ยังเป็นเรื่องที่ค่อนข้างใหม่และไม่ได้แพร่หลายมากนัก ซึ่งในโครงงานนี้จะแสดงให้เห็นถึงการทำงานร่วมกันของระบบธุรกรรมบน WAP และระบบความปลอดภัยที่อยู่บนสภาพแวดล้อมแบบ PKI อย่างคร่าว ๆ โดยการออกแบบและการพัฒนาในครั้งนี้จะใช้ซอฟต์แวร์ที่เป็นซอฟต์แวร์จำลองการทำงานบนโทรศัพท์มือถือมาใช้แทนโทรศัพท์มือถือจริงซึ่งใช้ Nokia Internet WAP Toolkit 3.1 และได้มีการสร้างคำสั่งที่เป็น Script เพื่อไปติดต่อกับฐานข้อมูลเพื่อทำธุรกรรมที่เกิดขึ้นได้

สิ่งที่เป็นข้อจำกัดในการพัฒนาระบบโดยรวมที่เห็นได้ชัดเจนคือความสามารถของ WAP Gateway ซึ่ง WAP Gateway ถือว่าเป็นส่วนที่สำคัญมากส่วนหนึ่งที่มีส่วนในการรองรับการทำงานของระบบโทรศัพท์มือถือ เพราะว่าจะเป็นตัวกลางในการติดต่อระหว่าง Client และ Server ทำหน้าที่ในการแลกเปลี่ยนข้อมูลระหว่าง Client และ Server ดังนั้น WAP Gateway จำเป็นต้องมีการปรับปรุงความสามารถให้รองรับมาตรฐานใหม่ตลอดเวลาเช่น WTLS หรือ WPKI ซึ่งในปัจจุบันยังไม่มี WAP Gateway ที่รองรับการทำงานร่วมกันของ SSL WTLS และ WPKI ได้อย่างสมบูรณ์ เพราะว่า WAP Gateway ส่วนใหญ่ยังทำงานบนมาตรฐาน WAP 1.2.1 ซึ่งยังไม่รองรับการทำงานกับ WPKI

ได้ ดังนั้นในอนาคต เมื่อ WAP Gateway ได้ก้าวสู่มาตรฐาน WAP 1.3 ขึ้นไป จึงจะมีการรองรับมาตรฐานแบบ WPKI มาใช้กันมากขึ้น

ข้อเสนอแนะ

ดังนั้นในการออกแบบและพัฒนาระบบนี้ก็จะทำให้สามารถเข้าใจถึงหลักการทำงานของระบบธุรกรรมบนโทรศัพท์มือถือให้มีความปลอดภัยยิ่งขึ้น และอาจนำความรู้ที่ได้รับไปใช้ในการประยุกต์พัฒนาระบบที่สามารถใช้งานจริงได้ในอนาคต ถึงแม้ว่าจะข้อจำกัดหลายประการ แต่ในอนาคต ข้อจำกัดเหล่านี้น่าจะได้รับแก้ไขปรับปรุงให้ดีขึ้นเพื่อรองรับการใช้งานที่เพิ่มมากขึ้นได้ต่อไป

บรรณานุกรม

Kannel Group. 2002. **Kannal Open Source WAP Gateway.** [Online]. Available : http://www.kannel.org

Nokia Corporation. 2002. **Forum Nokia WAP Technology.** [Online]. Available : http://www.forum.nokia.com

OpenCA Research and Development Labs. 2002. Implementation OpenCA System. [Online]. Available : http://www.openca.org

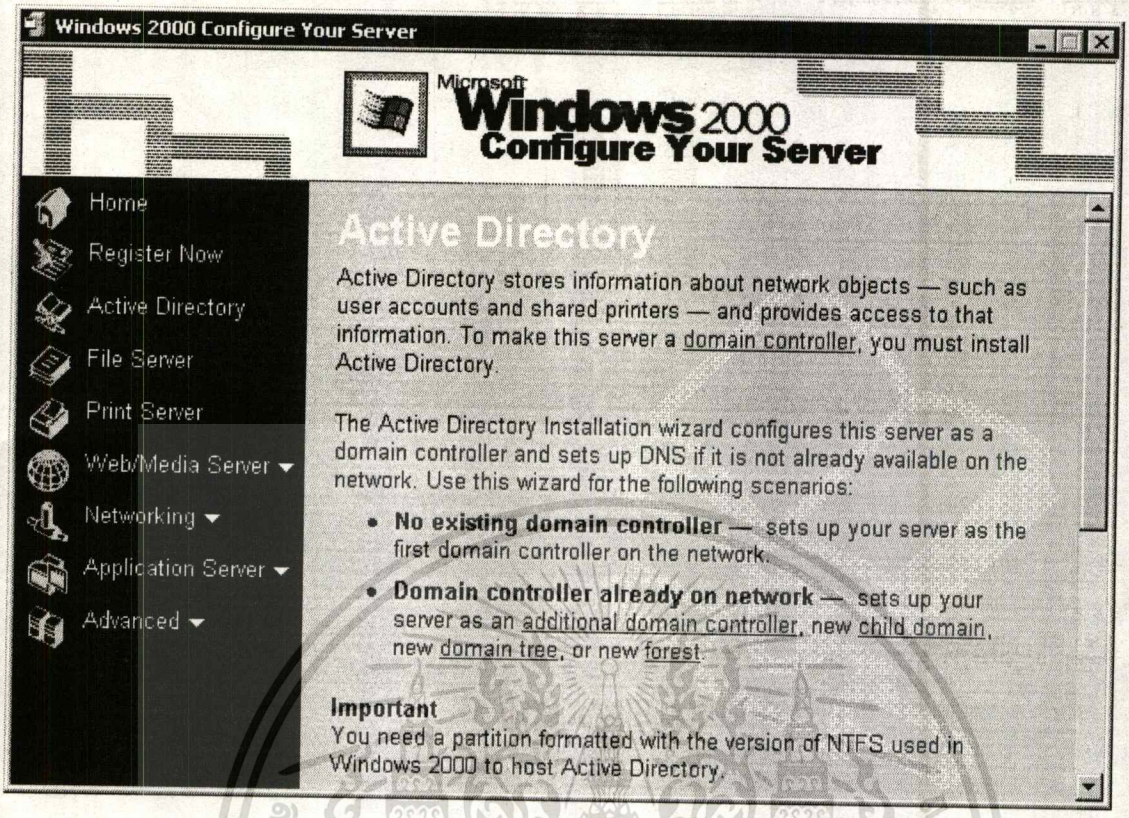
Wireless Application Protocol Forum 2002. **Wireless Application Protocol Forum Technical.** [Online]. Available : http://www.wapforum.org/what/technical.htm

ภาคผนวก ก

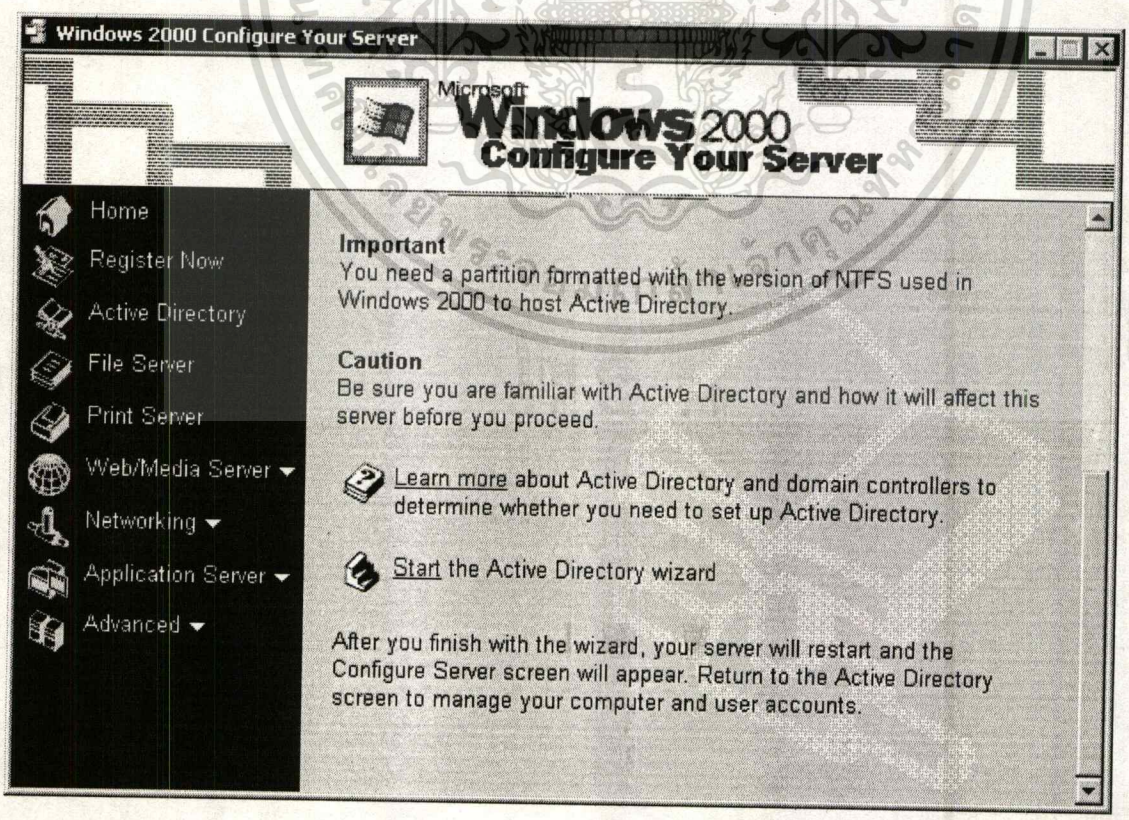
(Microsoft Active Directory and Certificate Service Installation and Configuration)

Install Microsoft Active Directory

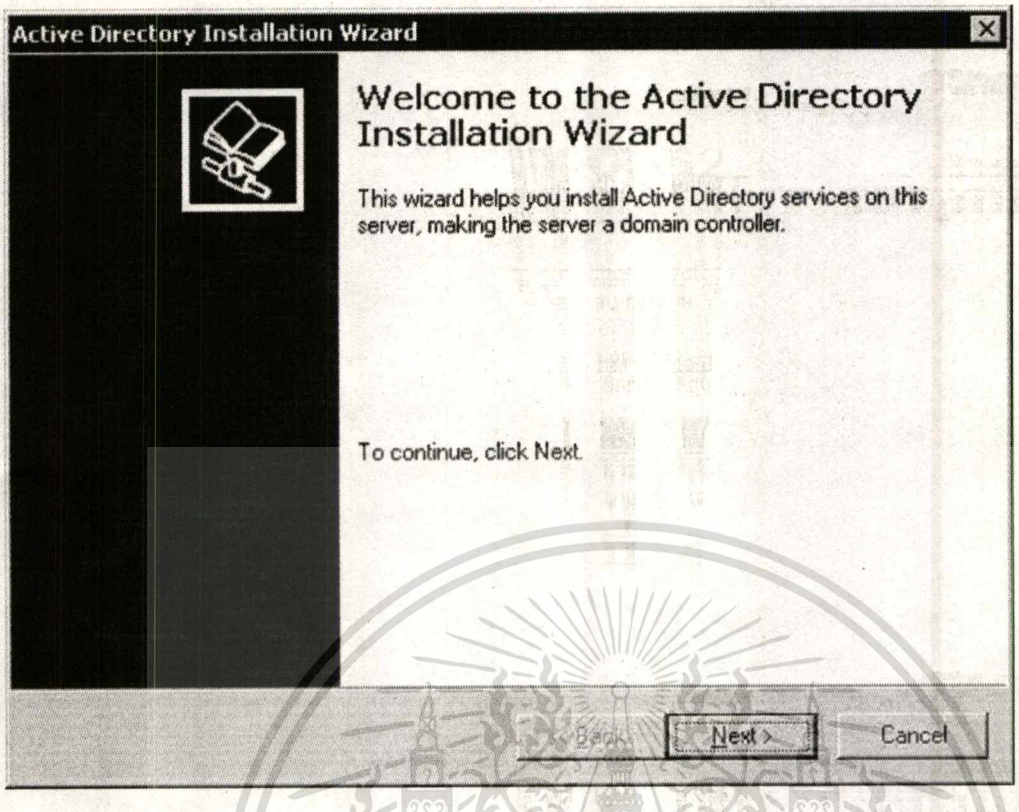
1. Run Windows 2000 Configure Your Server



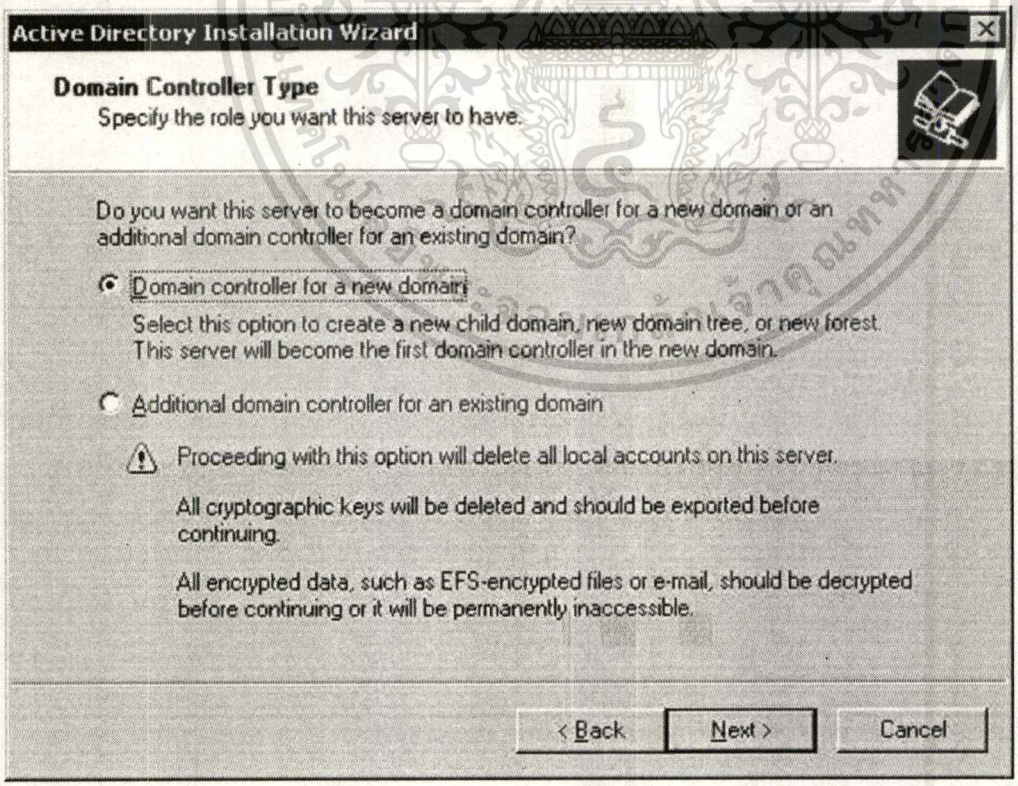
2. Select Active Directory Menu



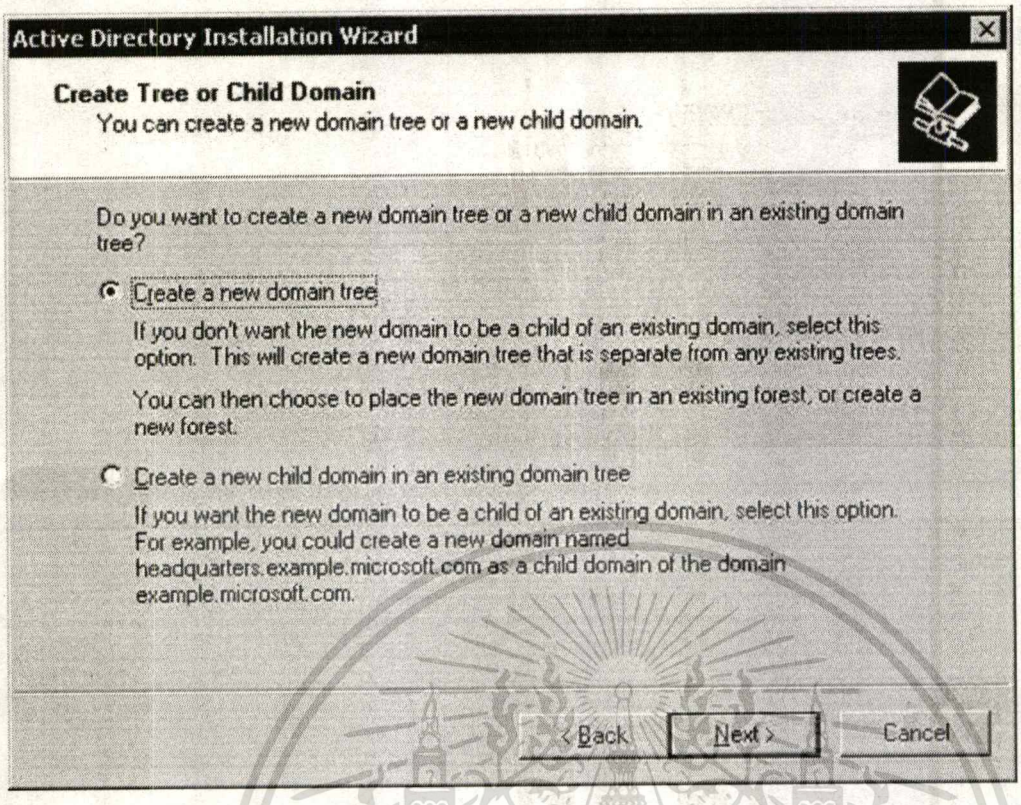
3. Start Setup Active Directory Service



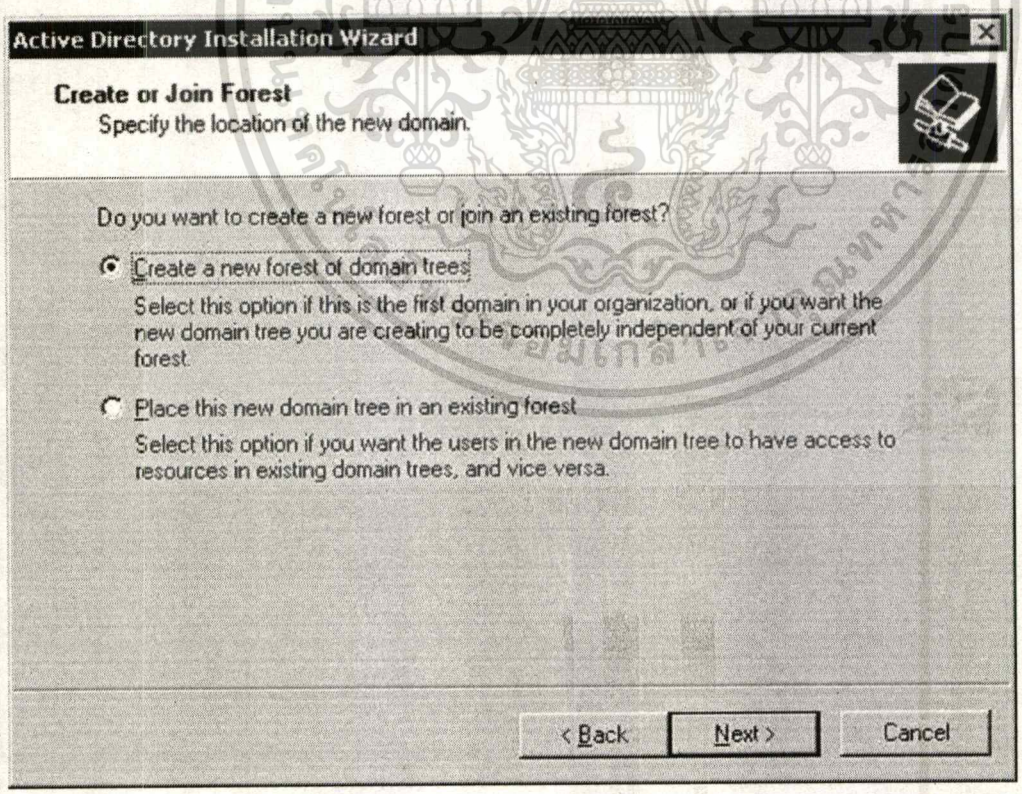
4. Create Domain Controller



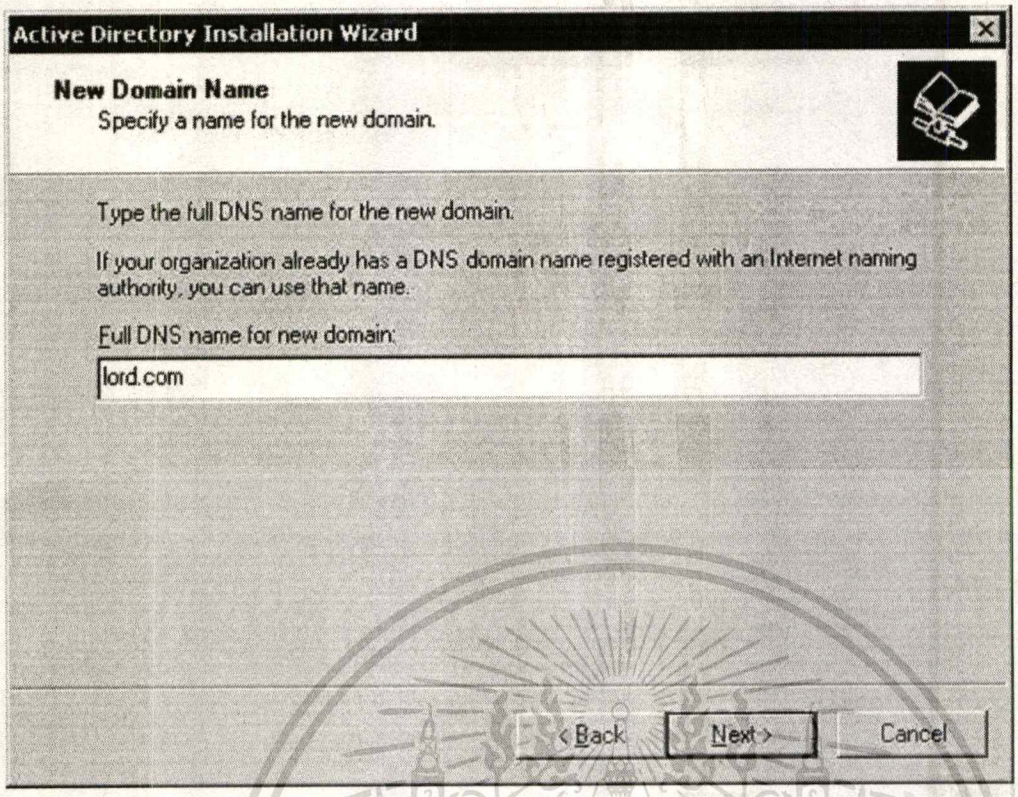
5. Create New Domain Tree



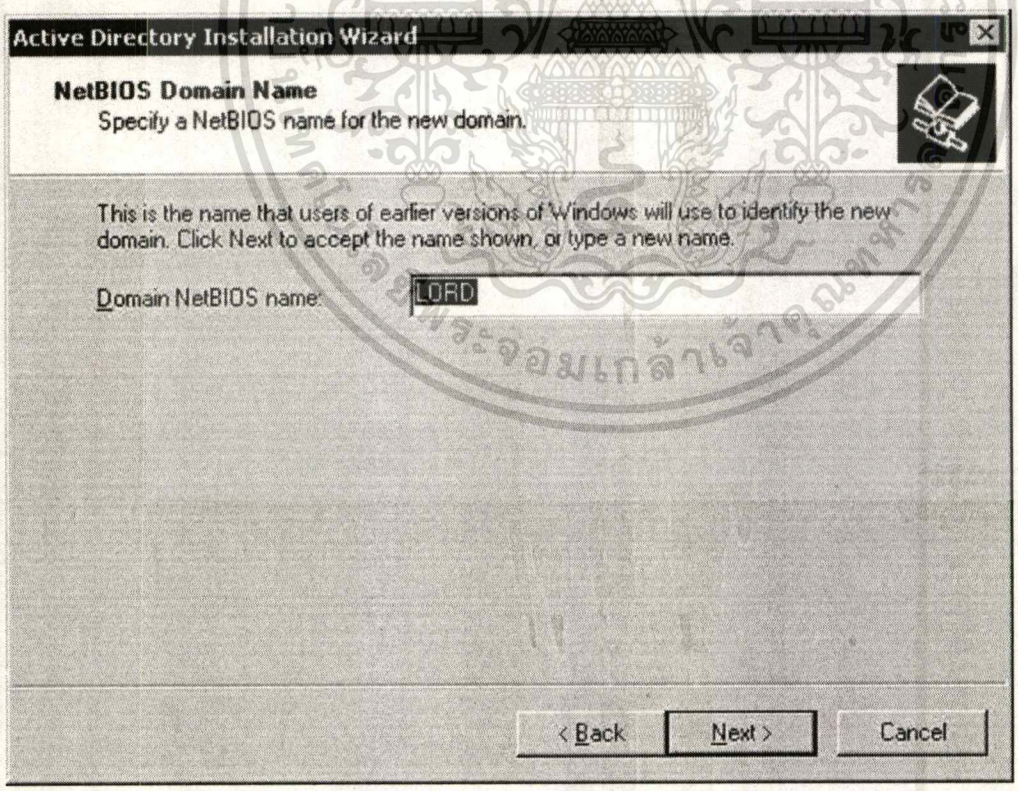
6. Create New Forest of Domain trees



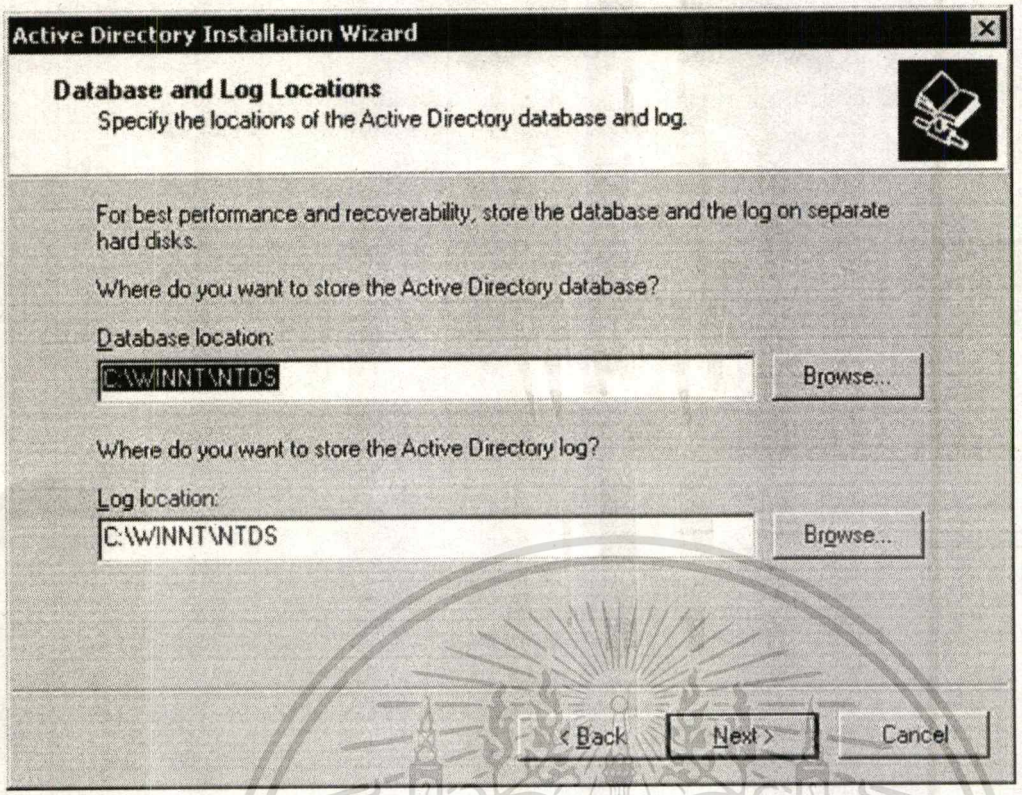
7. Create New Domain Name



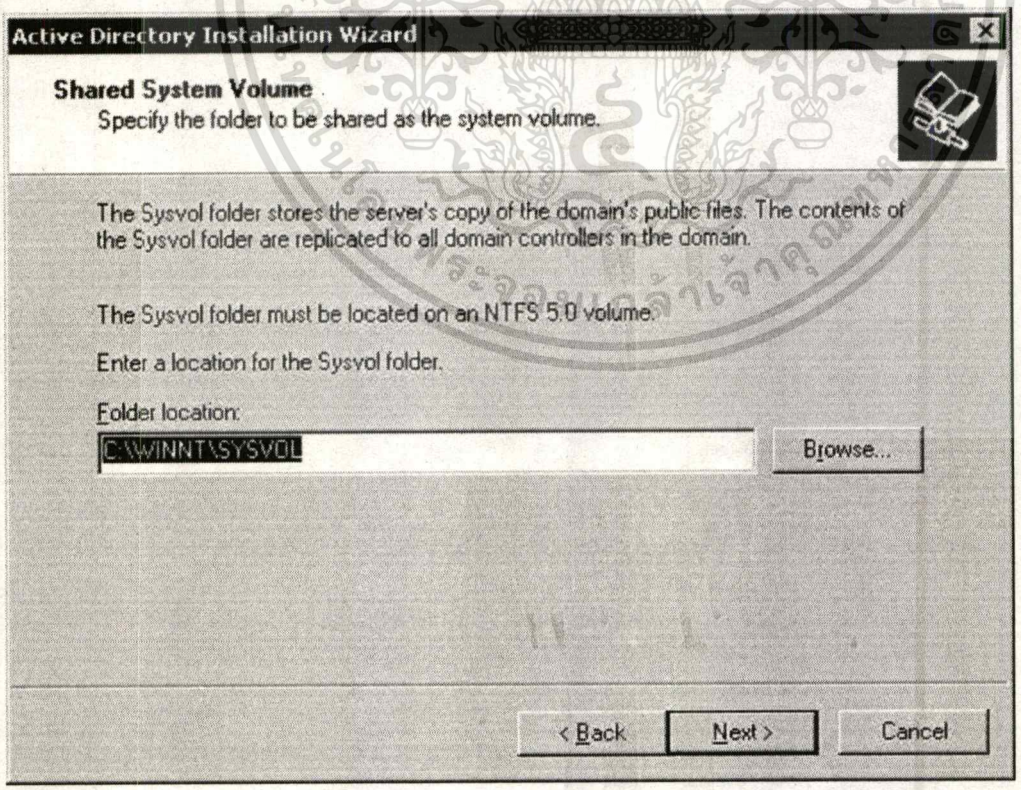
8. Create NetBIOS Domain Name



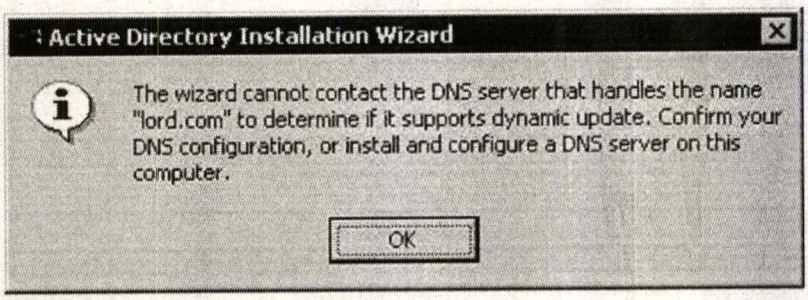
9. Active Directory Database and Log Locations



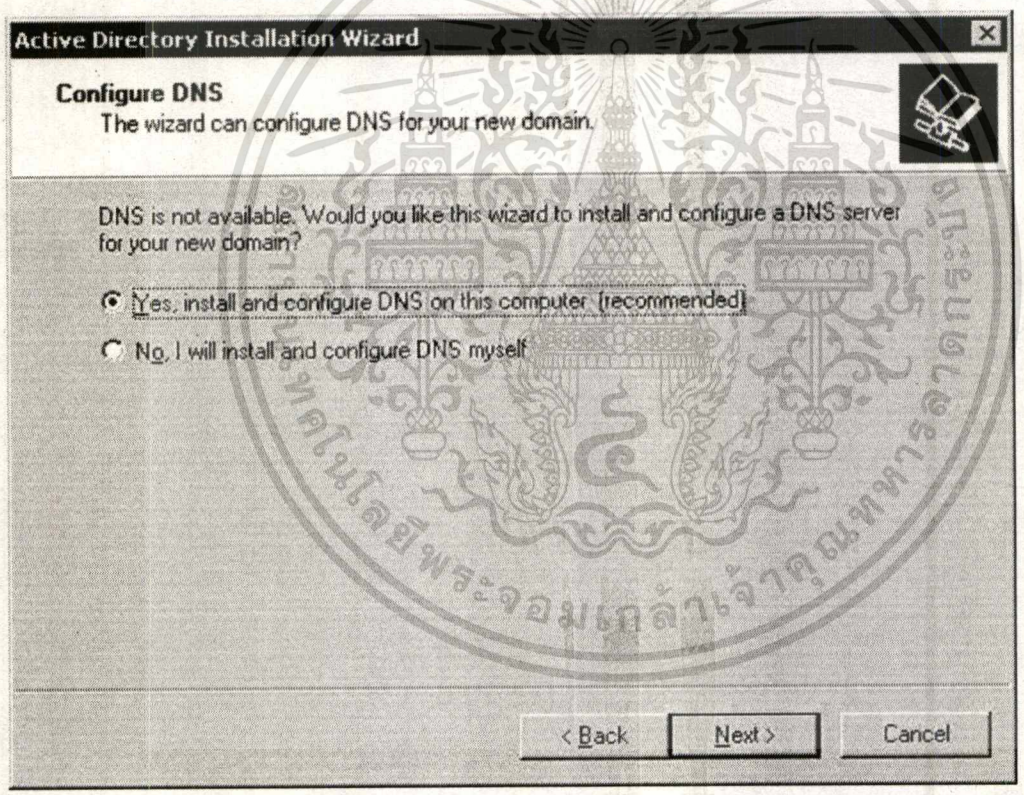
10. Active Directory Shared System Volume



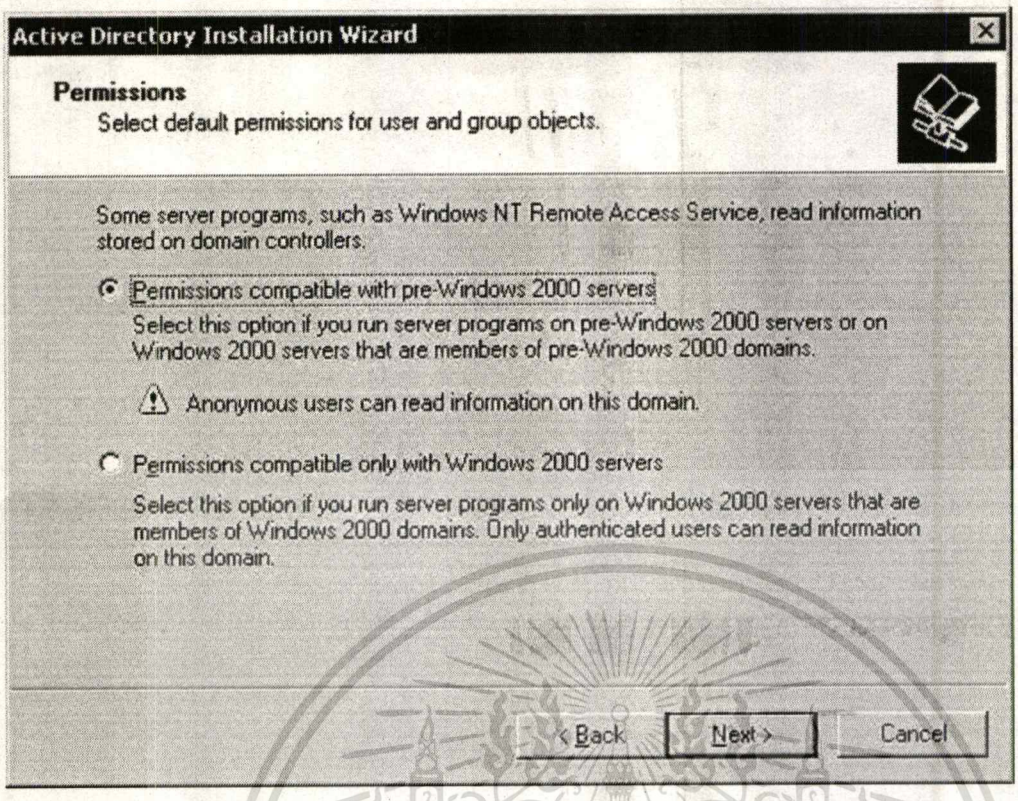
11. Confirm Active Directory DNS Server



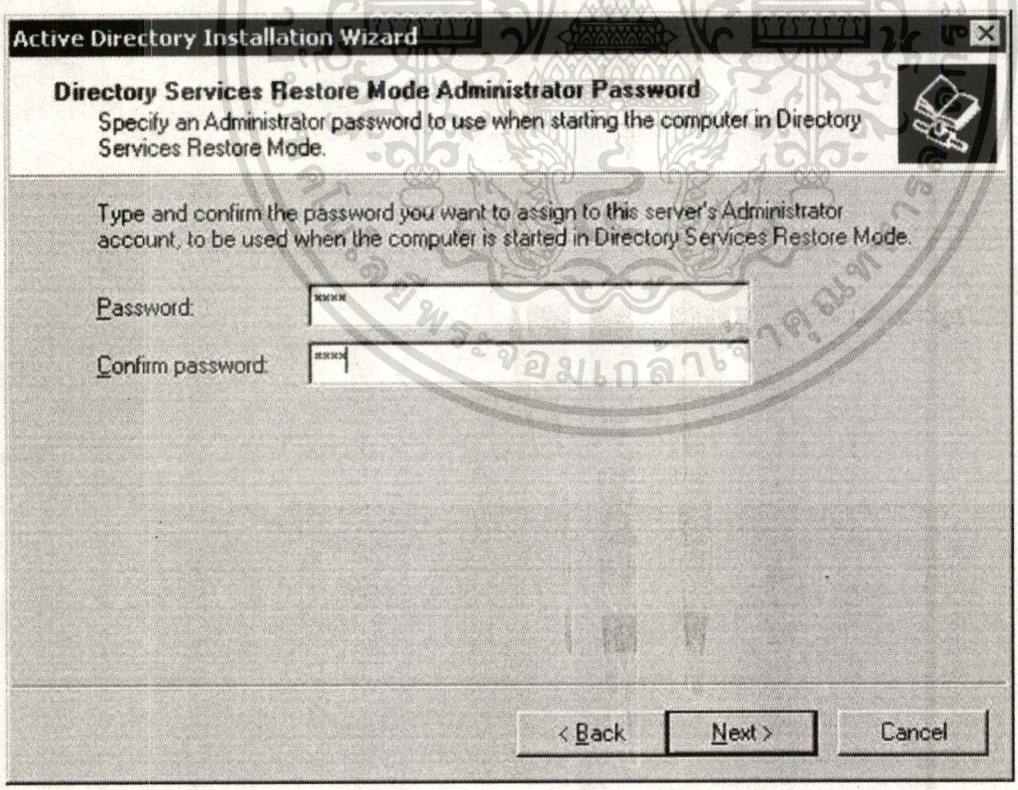
12. Install and Configure DNS



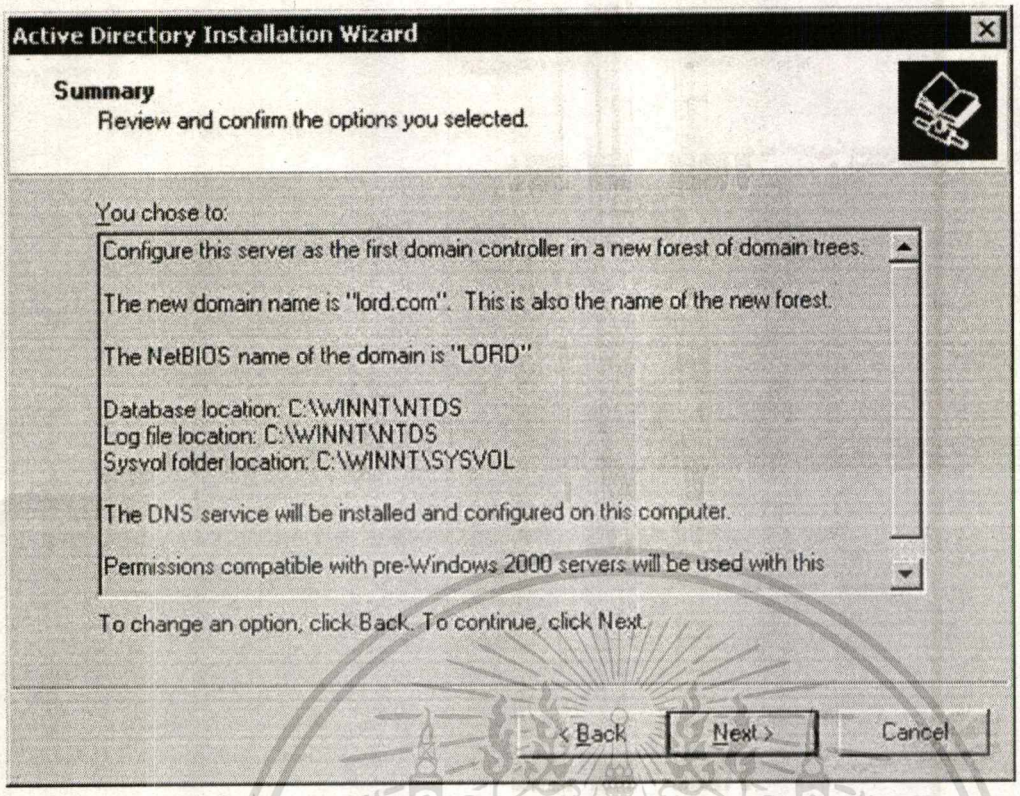
13. Select Permission Mode for Domain Controller



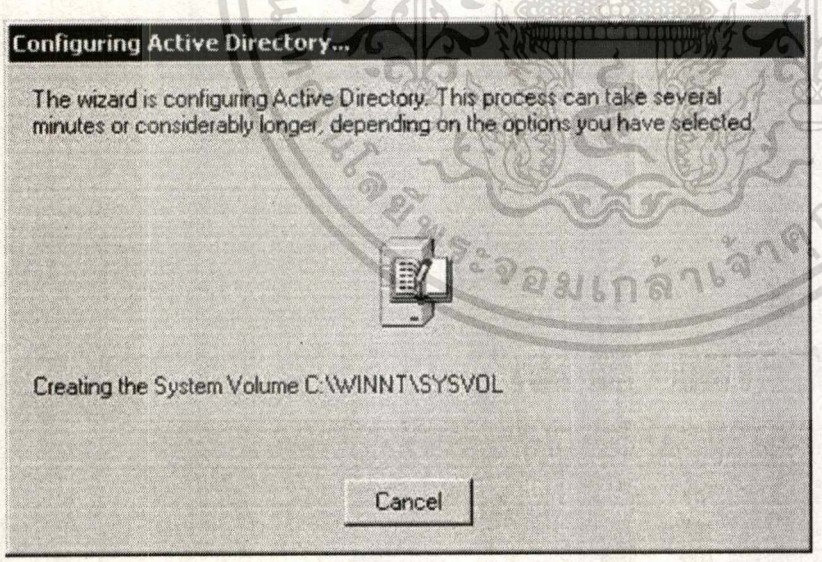
14. Directory Services Restore Mode Administrator Password



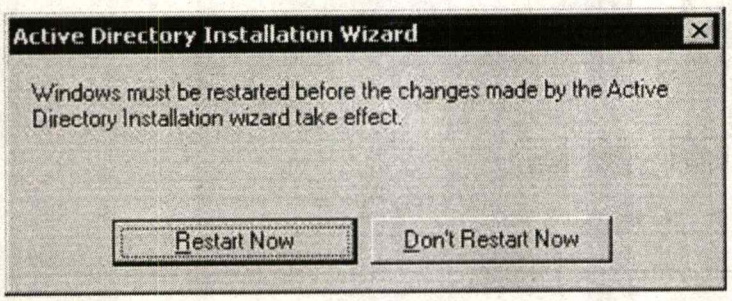
15. Summary All Detail of Active Directory Configuration



16. Microsoft Active Directory Configuration



17. Restart Windows

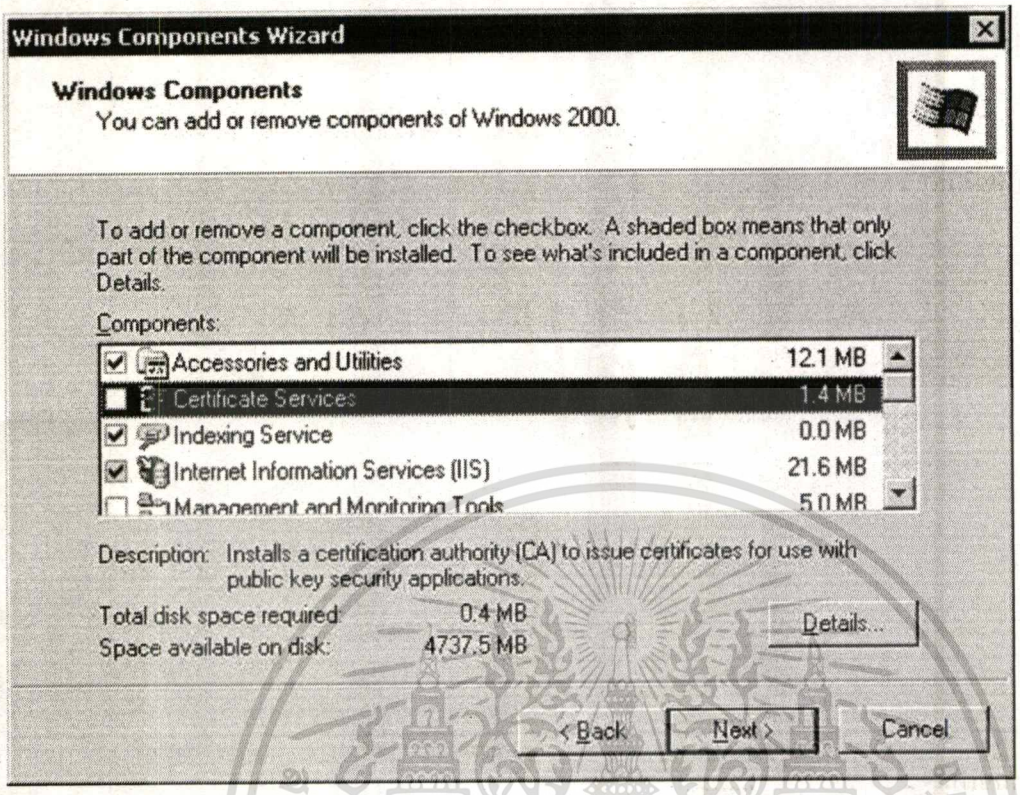


Remark

- Microsoft Active Directory must be run on NTFS Partitions only

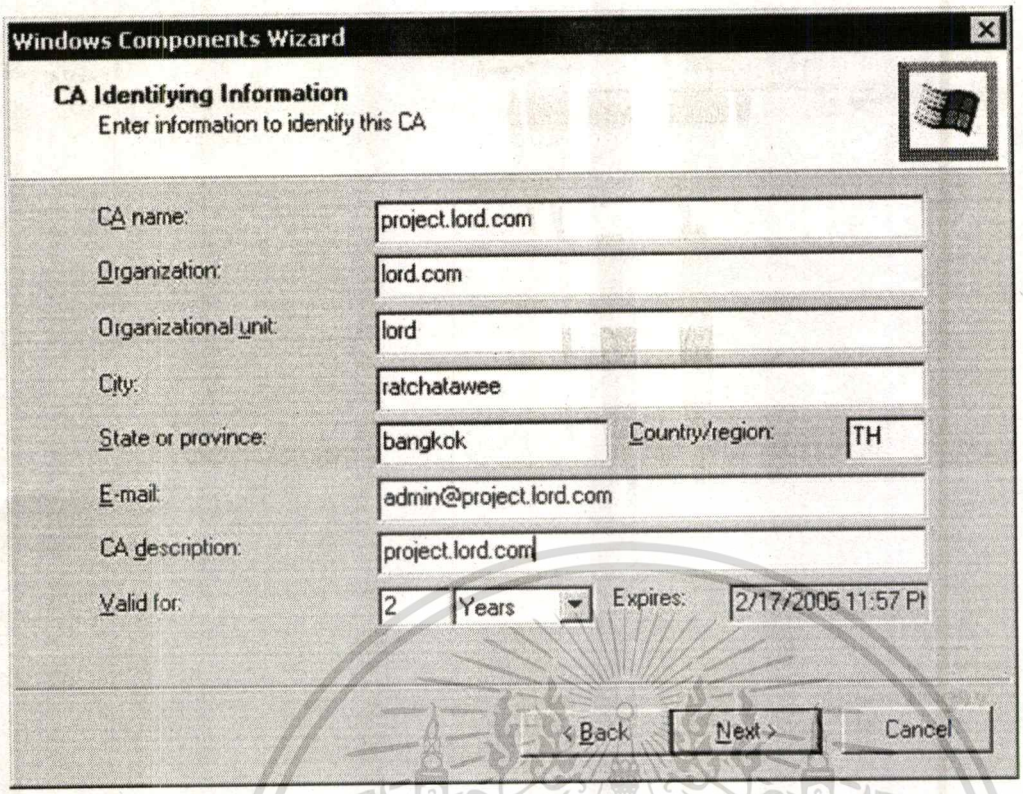
Install Microsoft Certificate Services

1. Install Window Component for Certificate Services

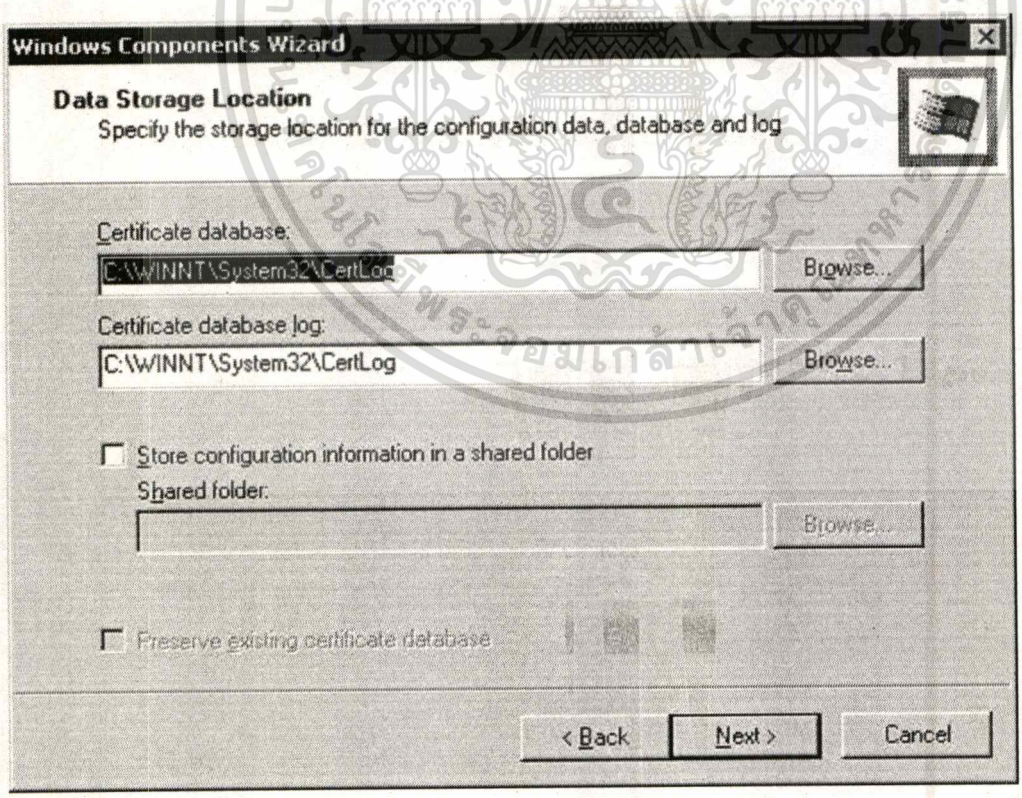


2. Warning you can not Change Computer Name after Install Certificate Services

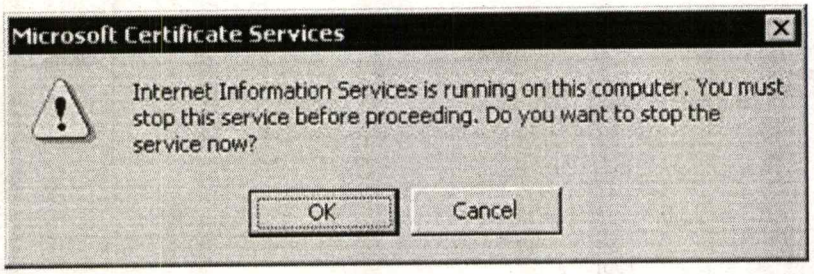
5. Input CA Identifying Information



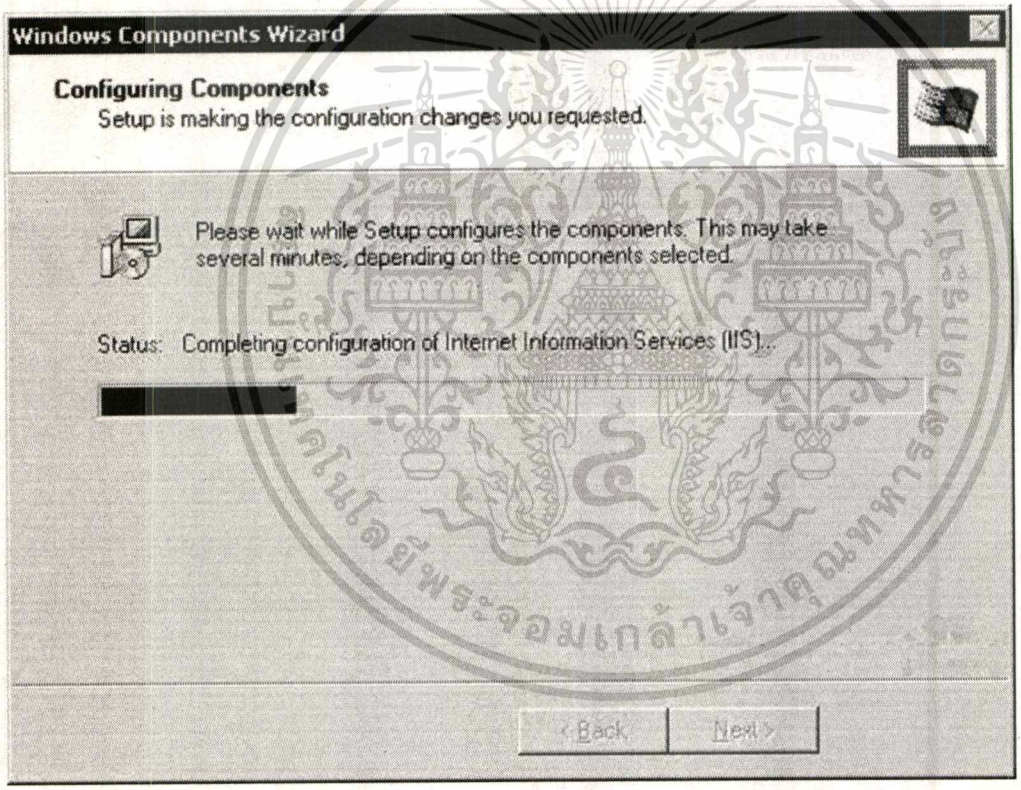
6. Select Data Storage Location for Certificate Services



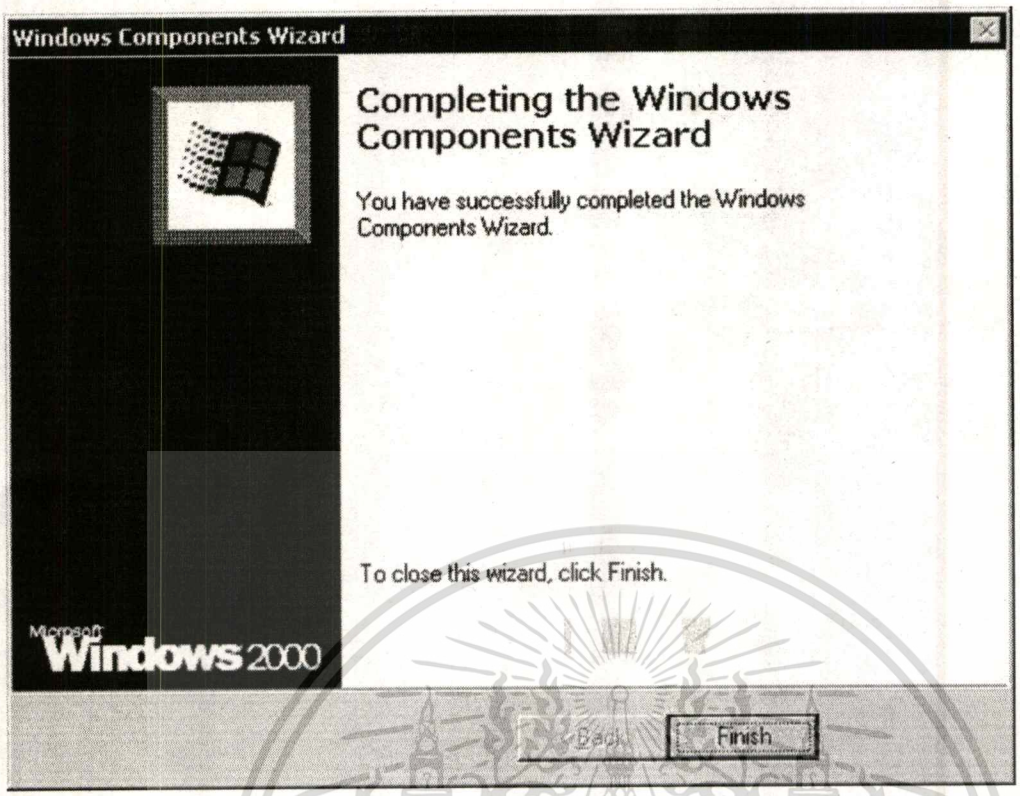
7. Stop Internet Information Services



8. Install Components



9. Complete to install Microsoft Certificate Services

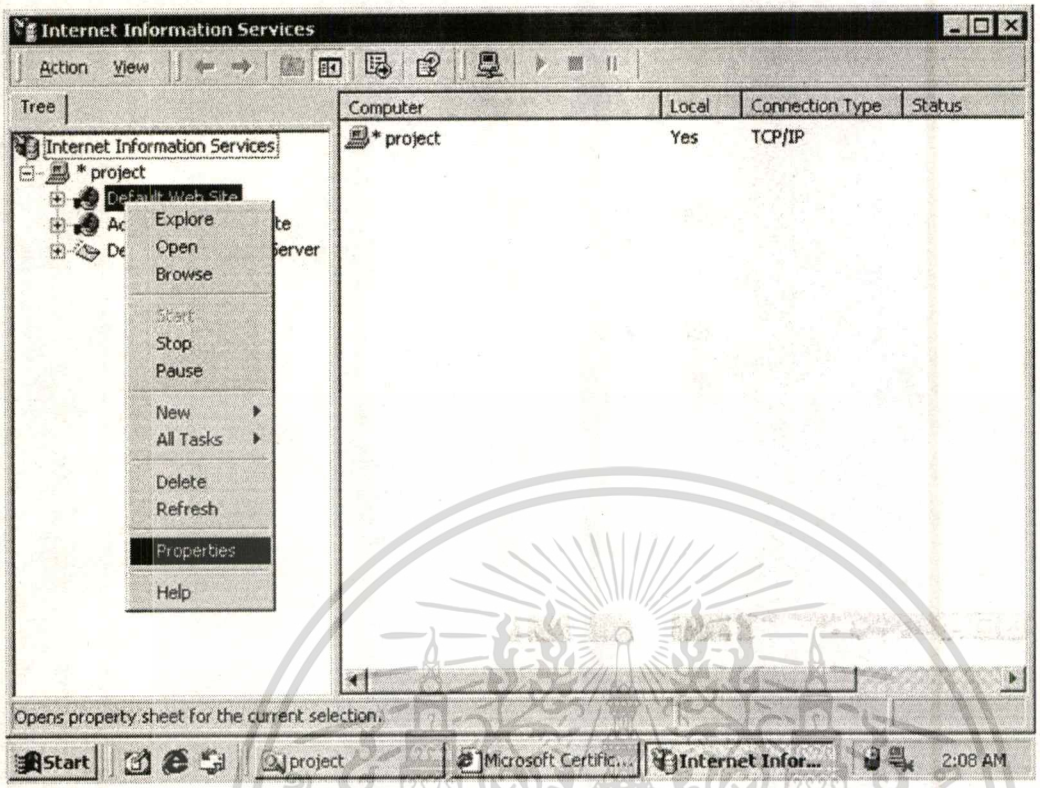


ภาคผนวก ข

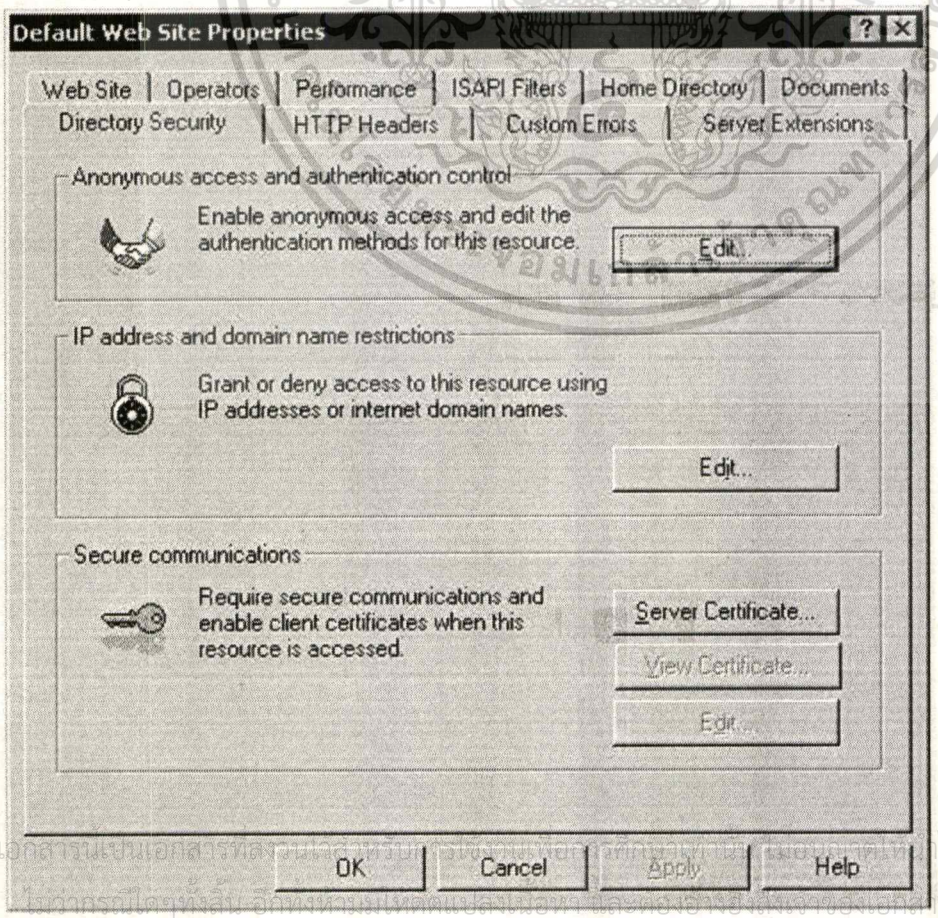
(การบริหารจัดการ Certification Authories)

Configuration Internet Information Service for SSL Security

1. Select Web Site to use Security

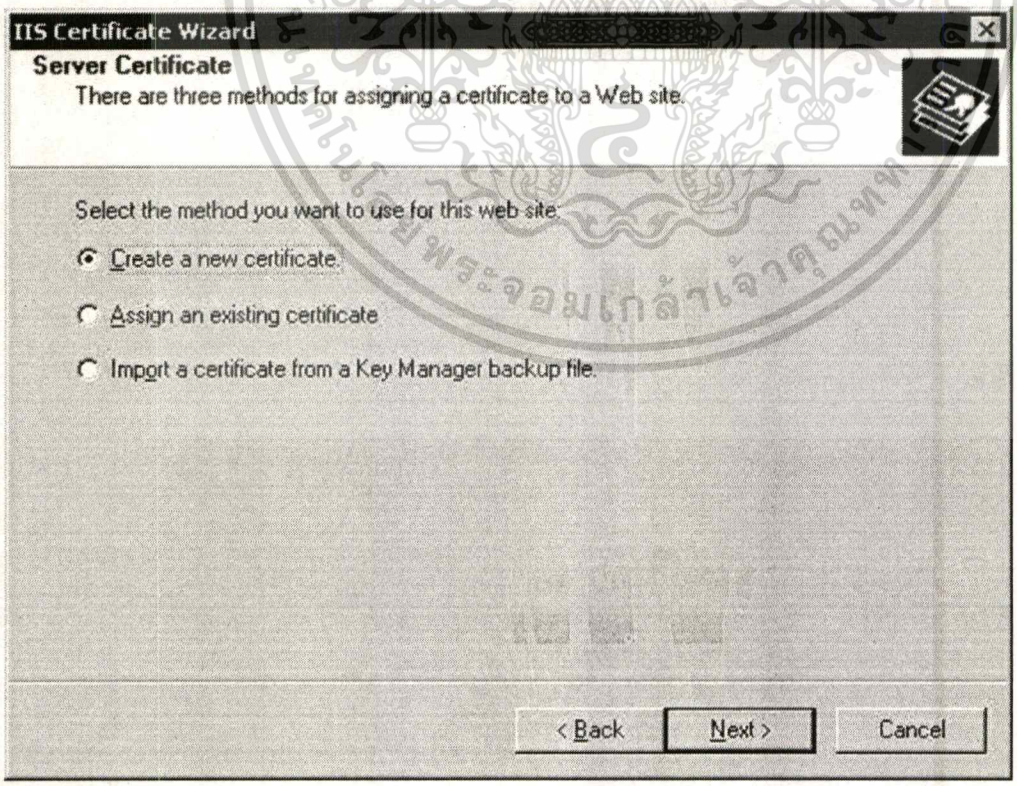


2. Select Server Certificate

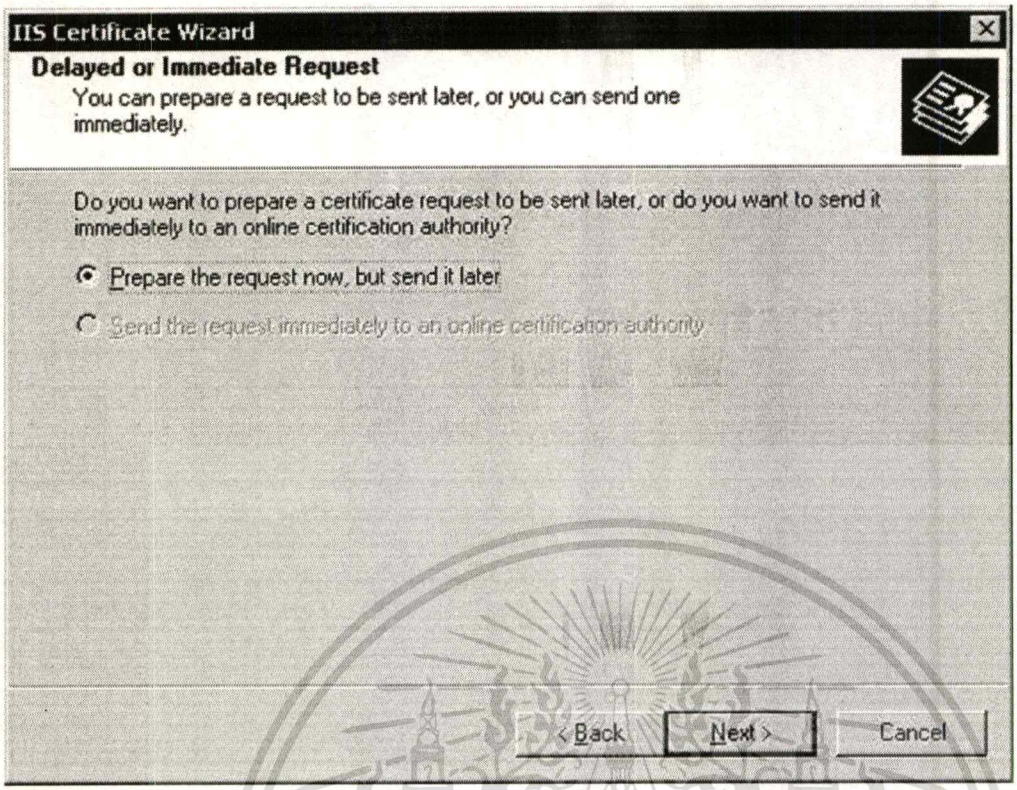


3. Start to Web Server Certificate

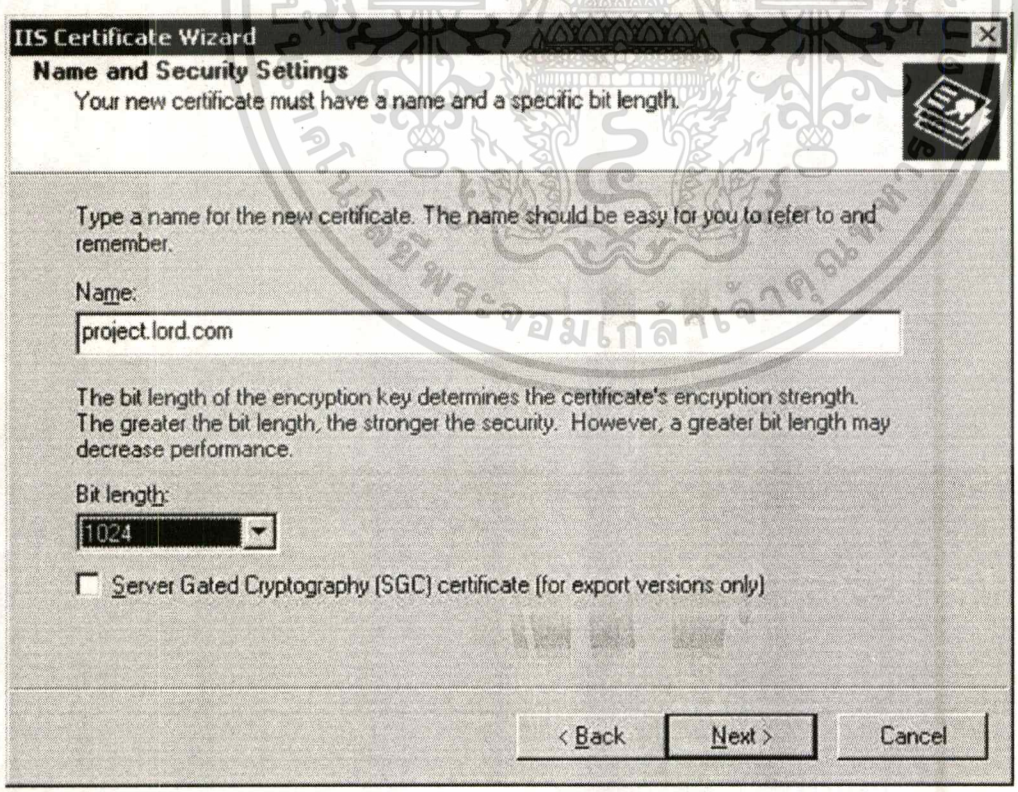
4. Create a New Certificate



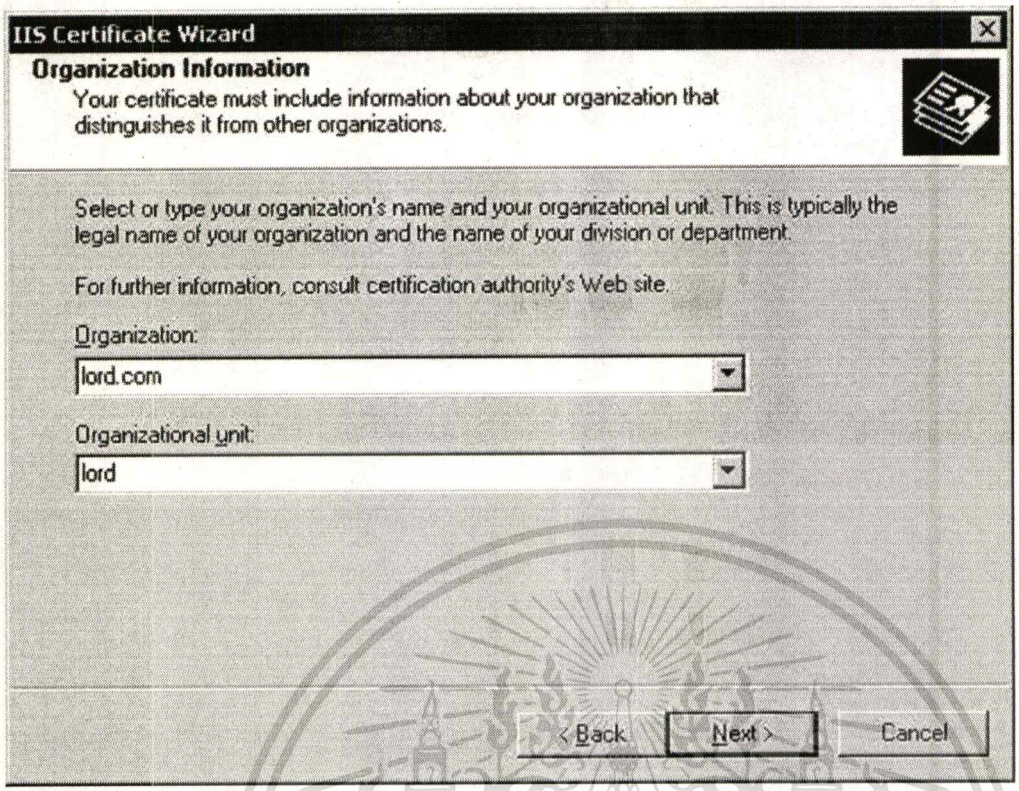
5. Prepare the request



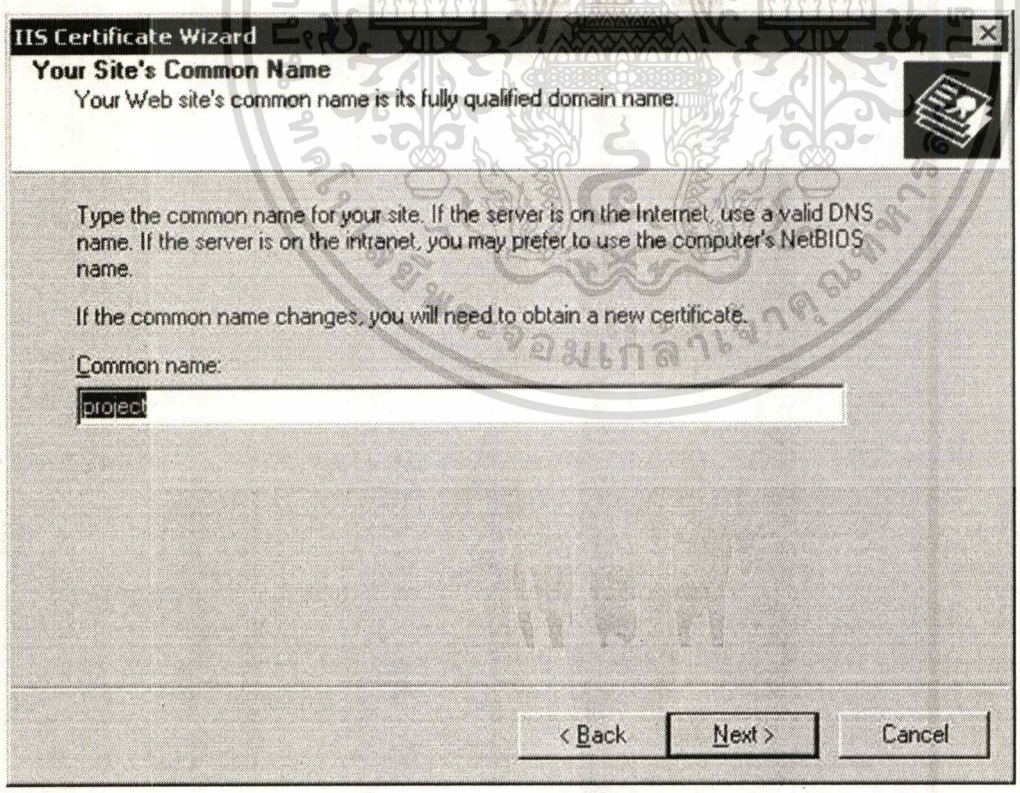
6. Input Name and Security Setting



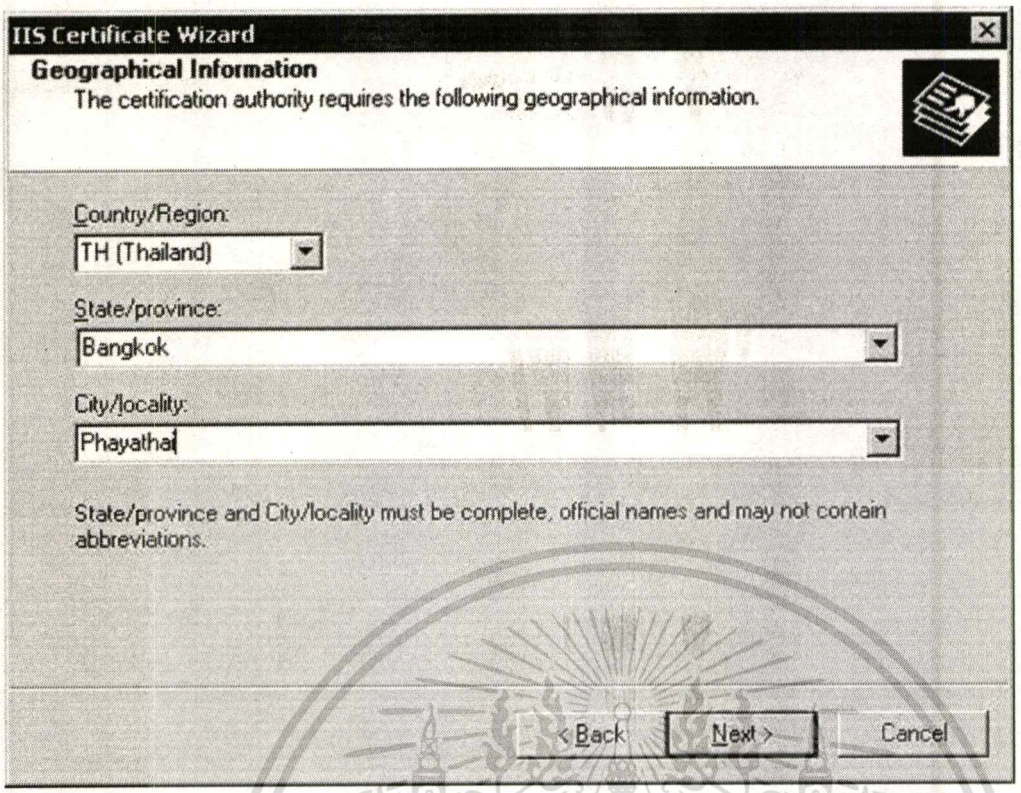
7. Input Organization Information



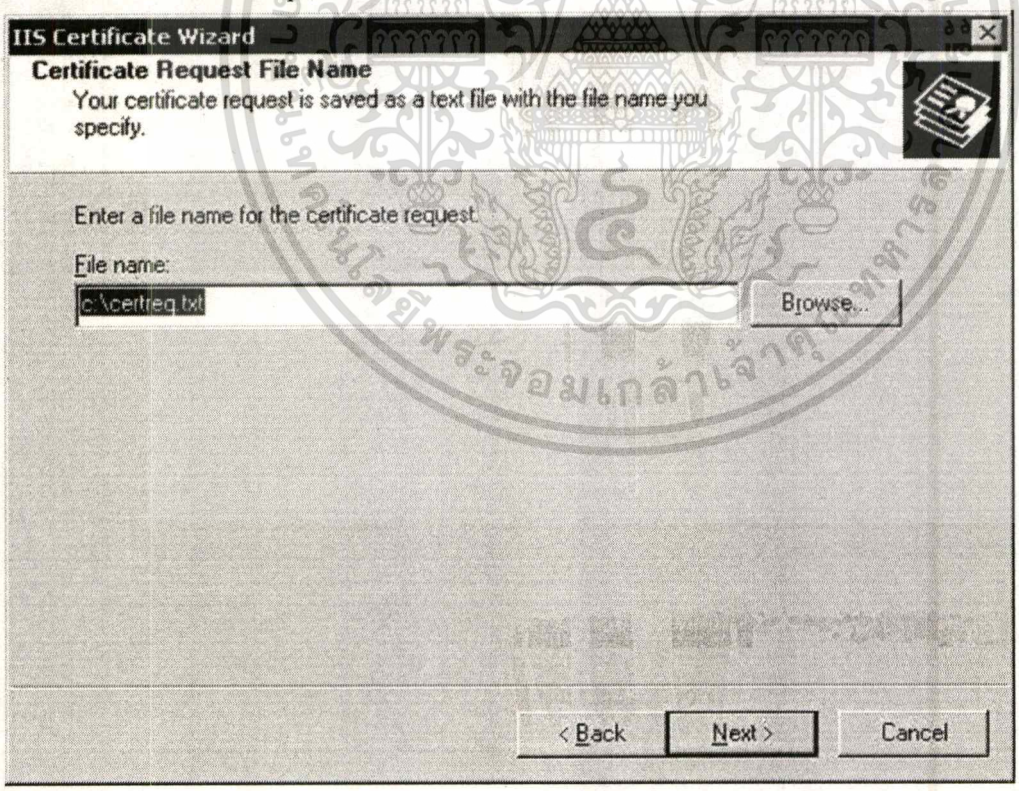
8. Input Common Name



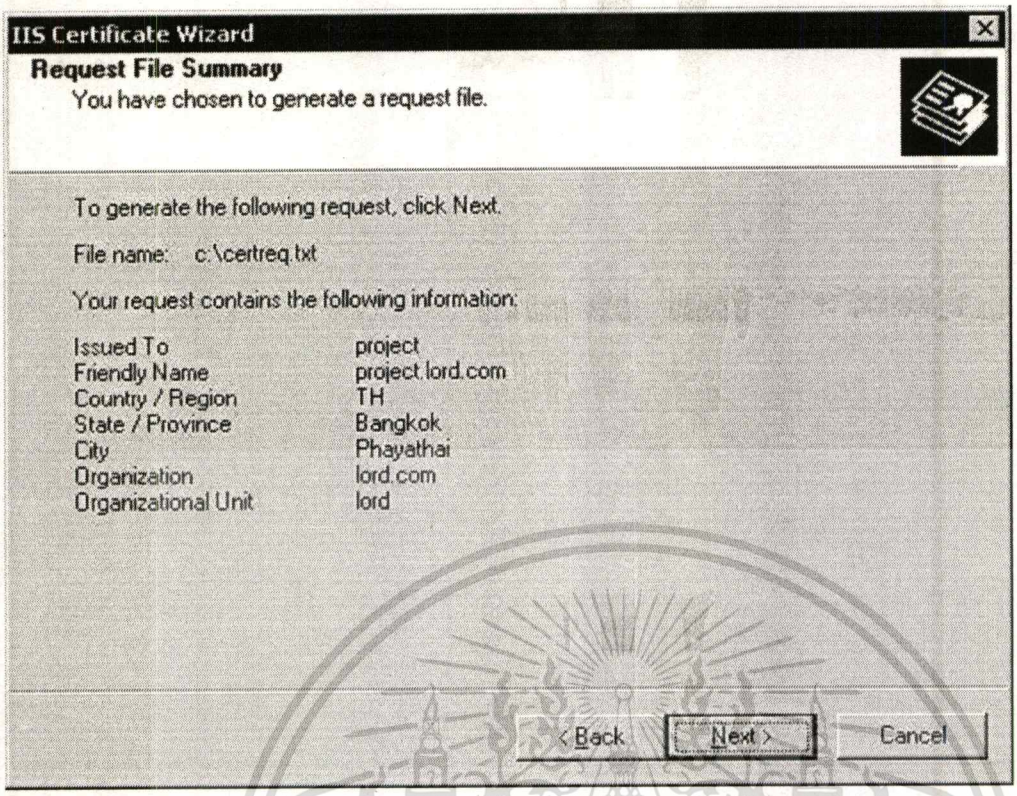
9. Geographic Information



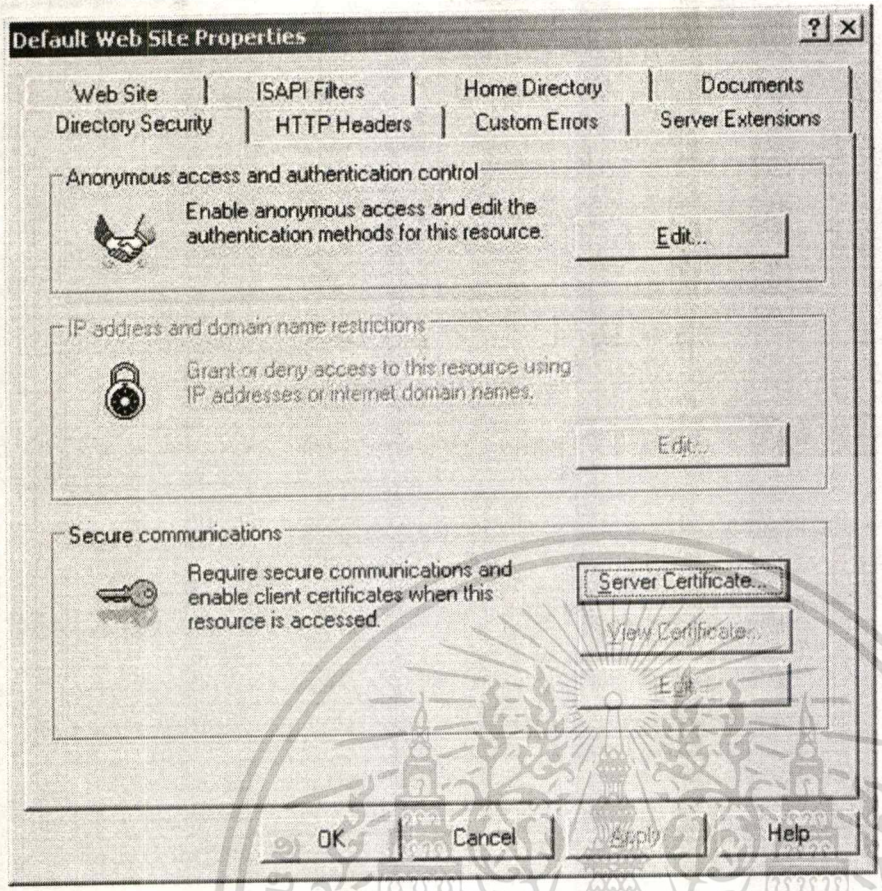
10. Select Certificate Request File Name



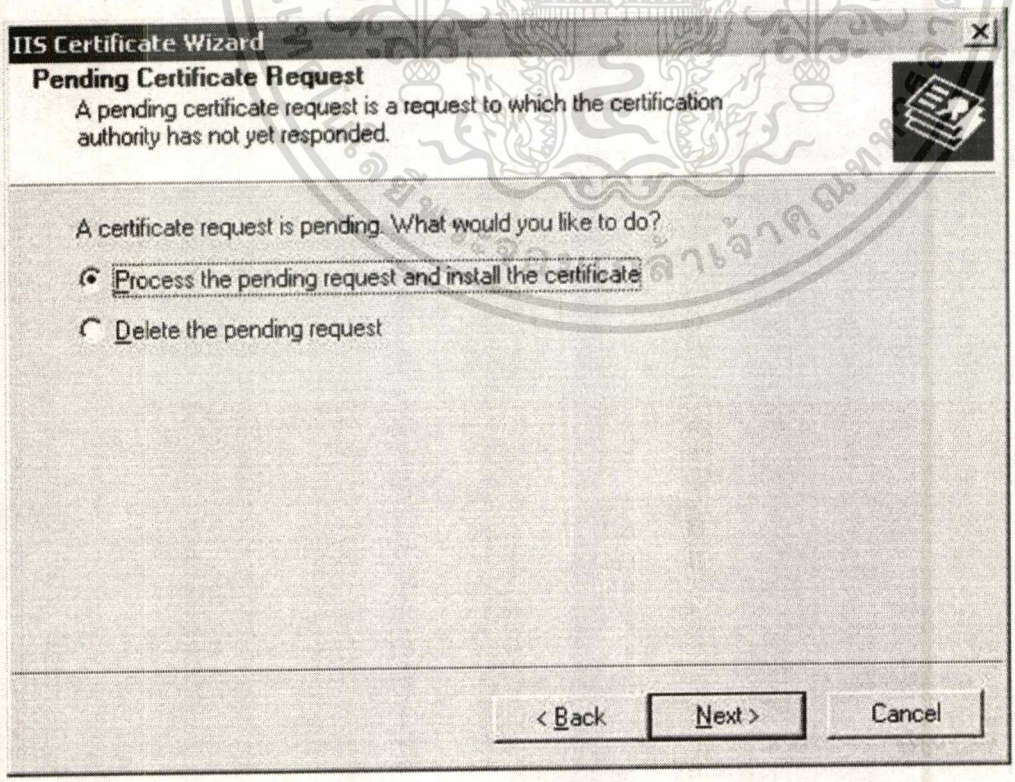
11. Request File Summary and Finish



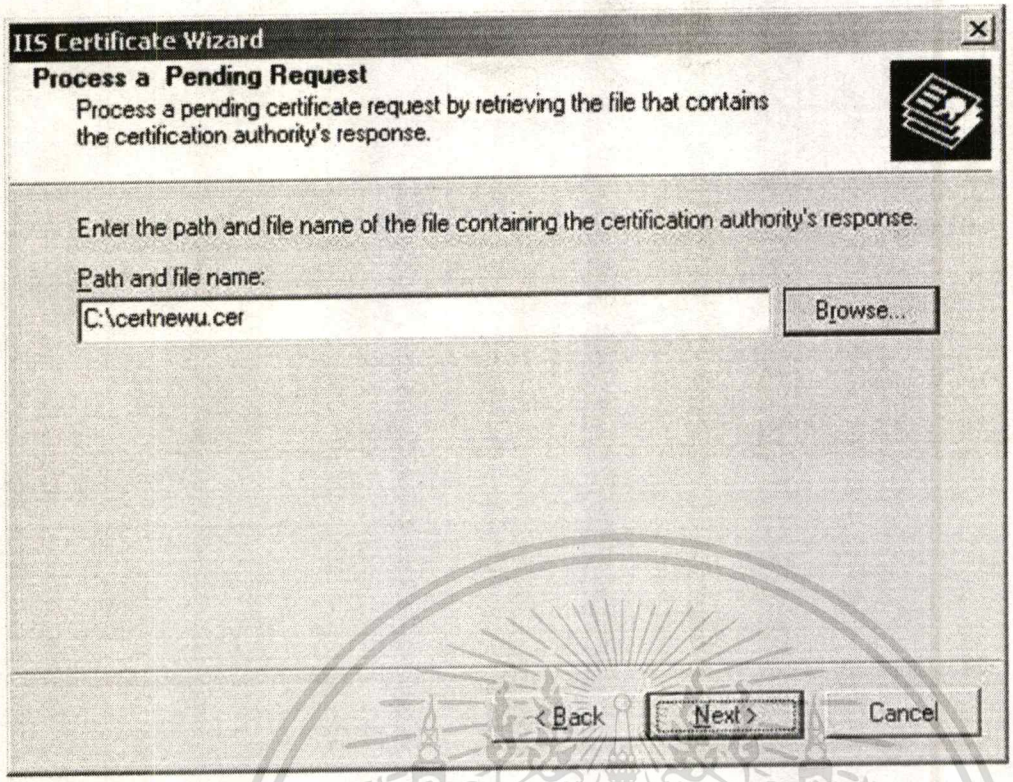
12. Installation Certificate for IIS Web Server



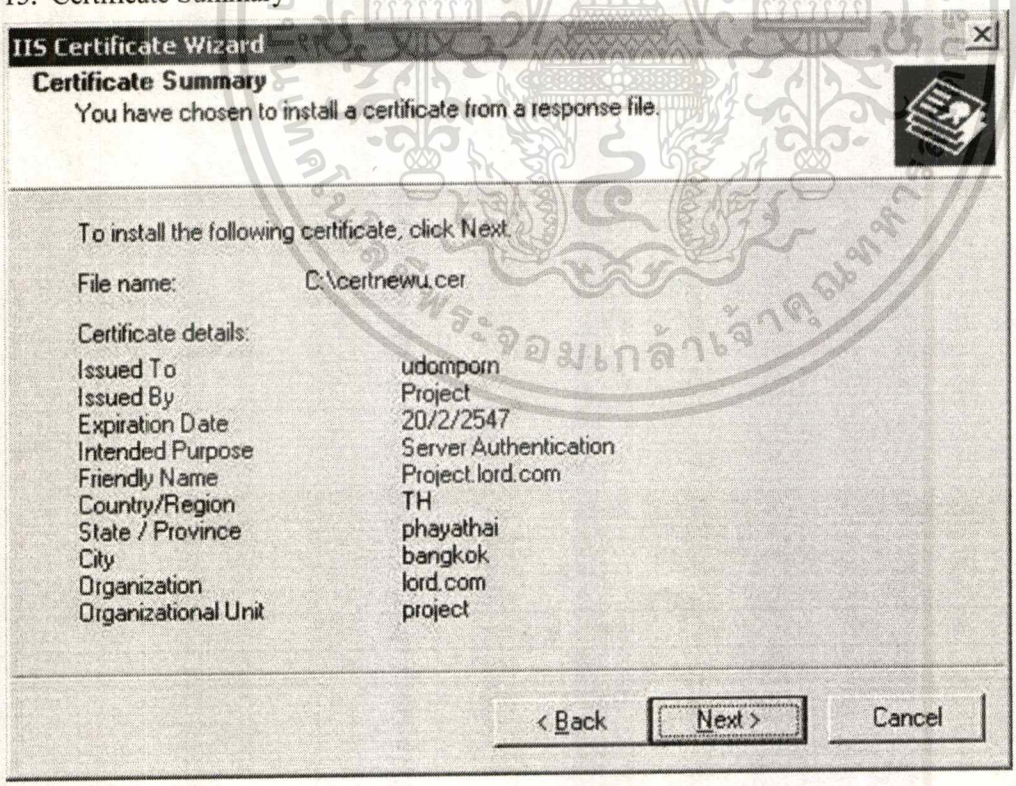
13. Select Process the pending request and installation Certificate



14. Select the certificate for installation

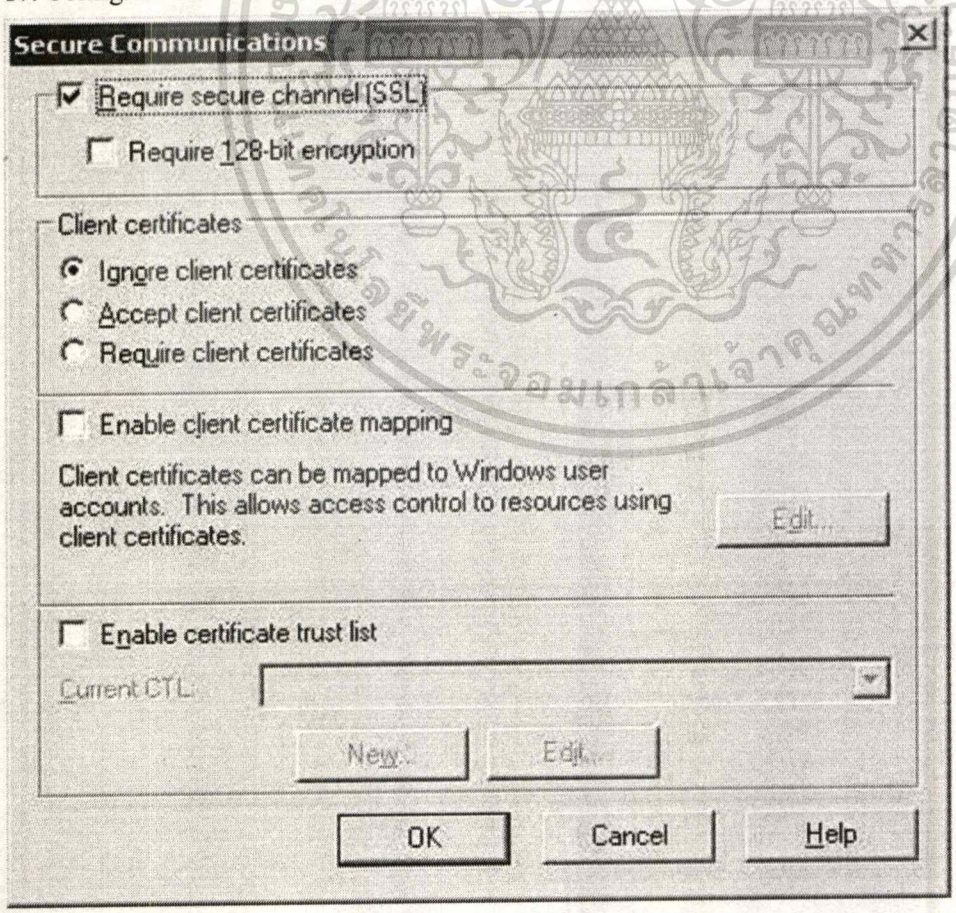


15. Certificate Summary

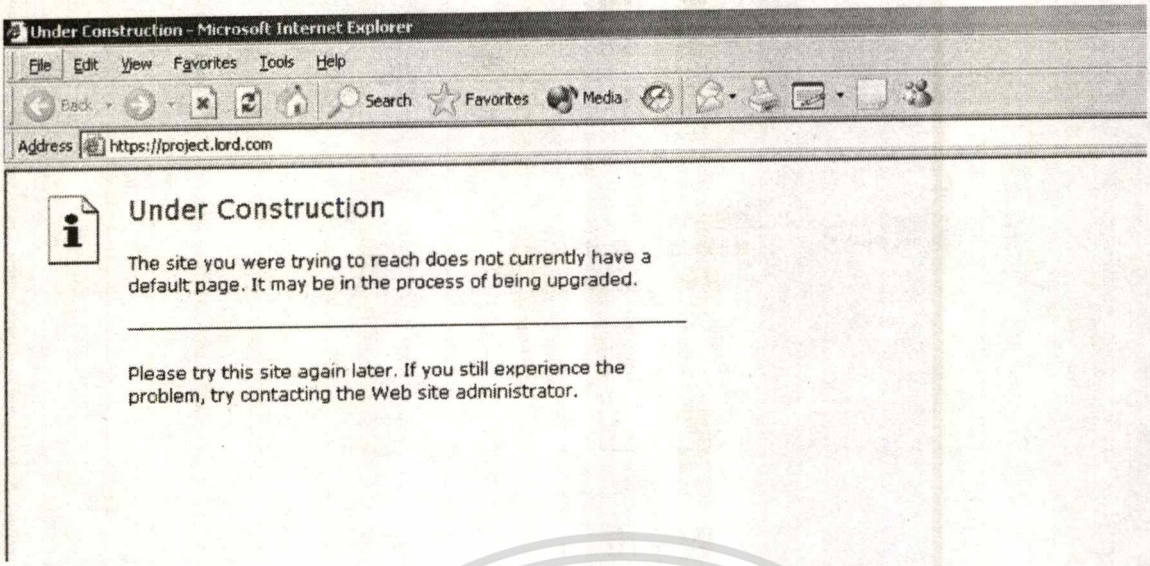


16. Complete installation Certificate for Web Server

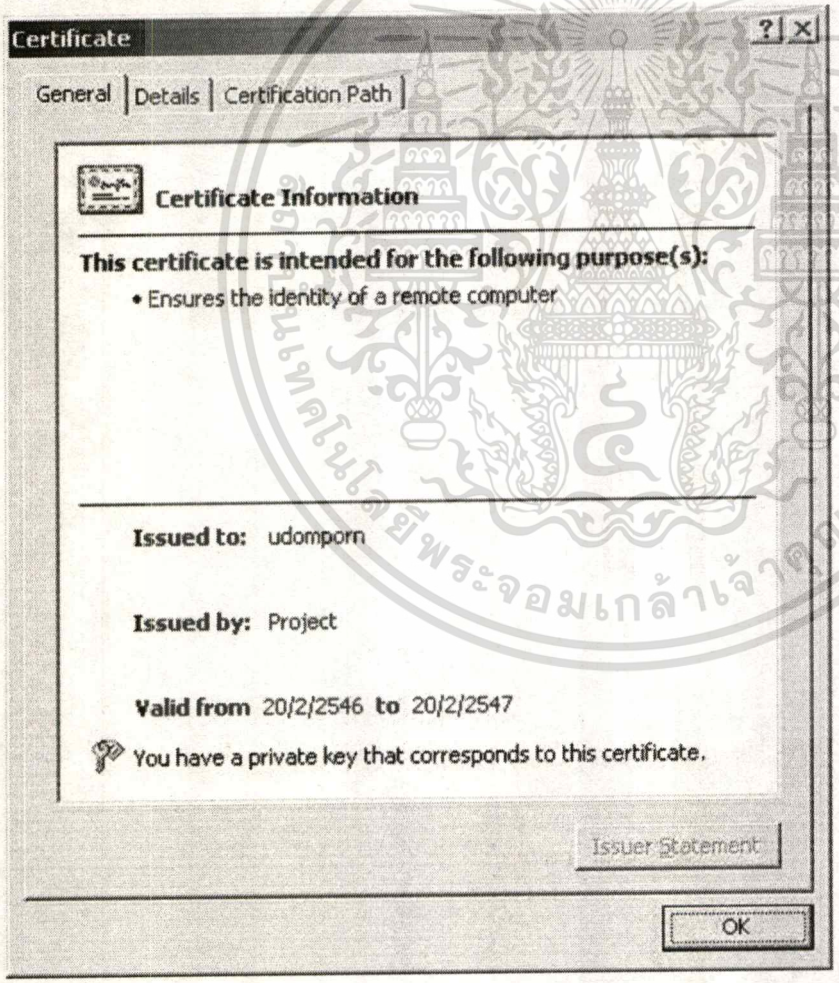
17. Configuration Web Server



18. Web Site with use SSL Security



19. Certificate information file

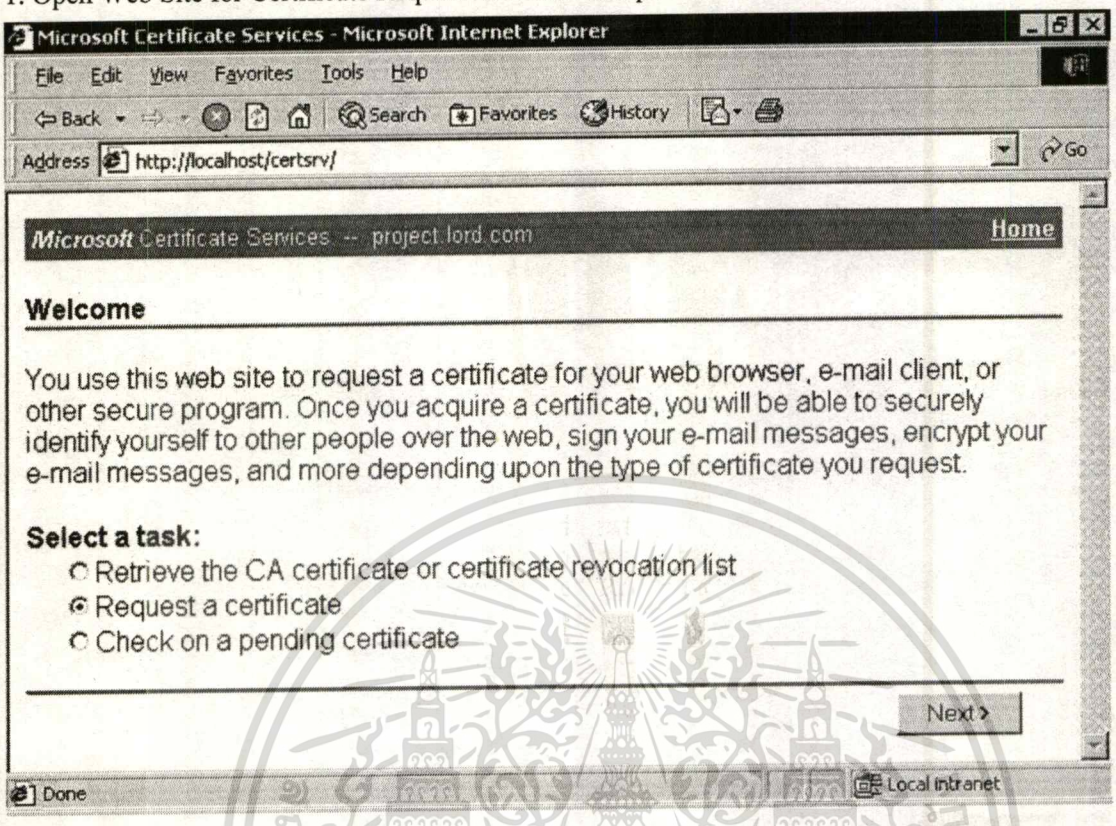


ภาคผนวก ค

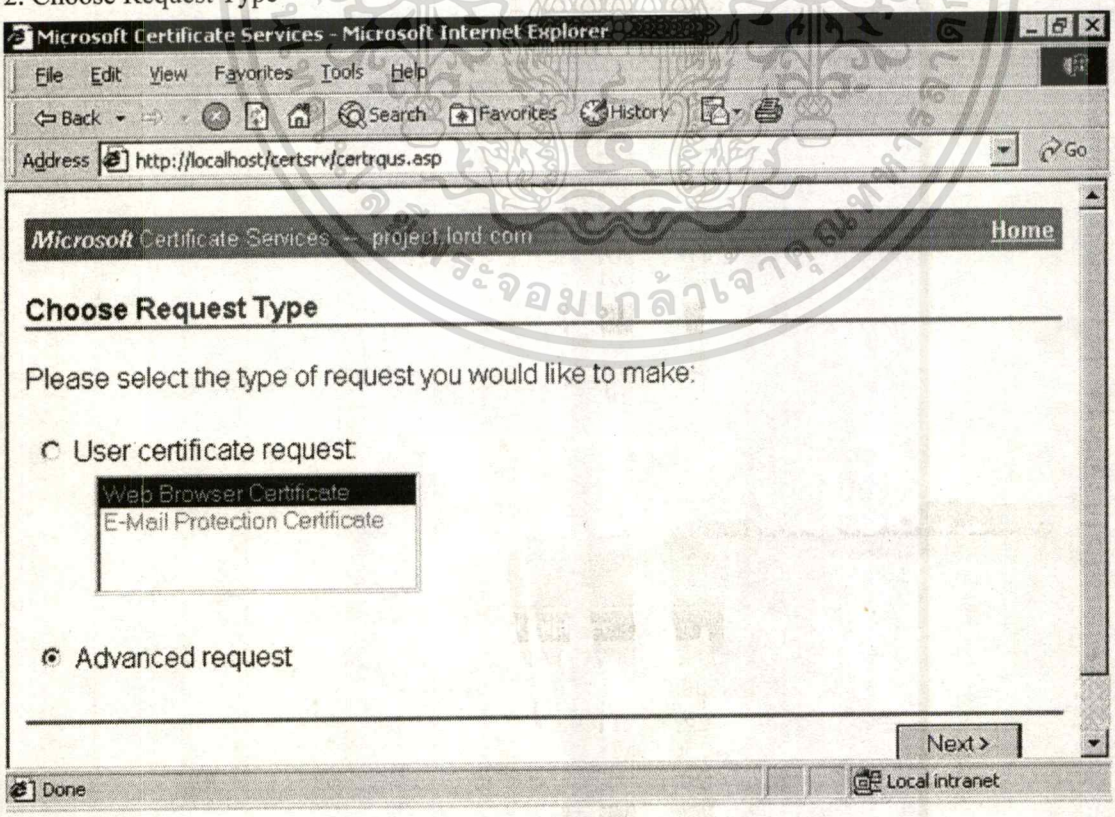
(ขั้นตอนการขอ Certificate และการรับ Certificate)

ขั้นตอนการขอ Certificate และการรับ Certificate

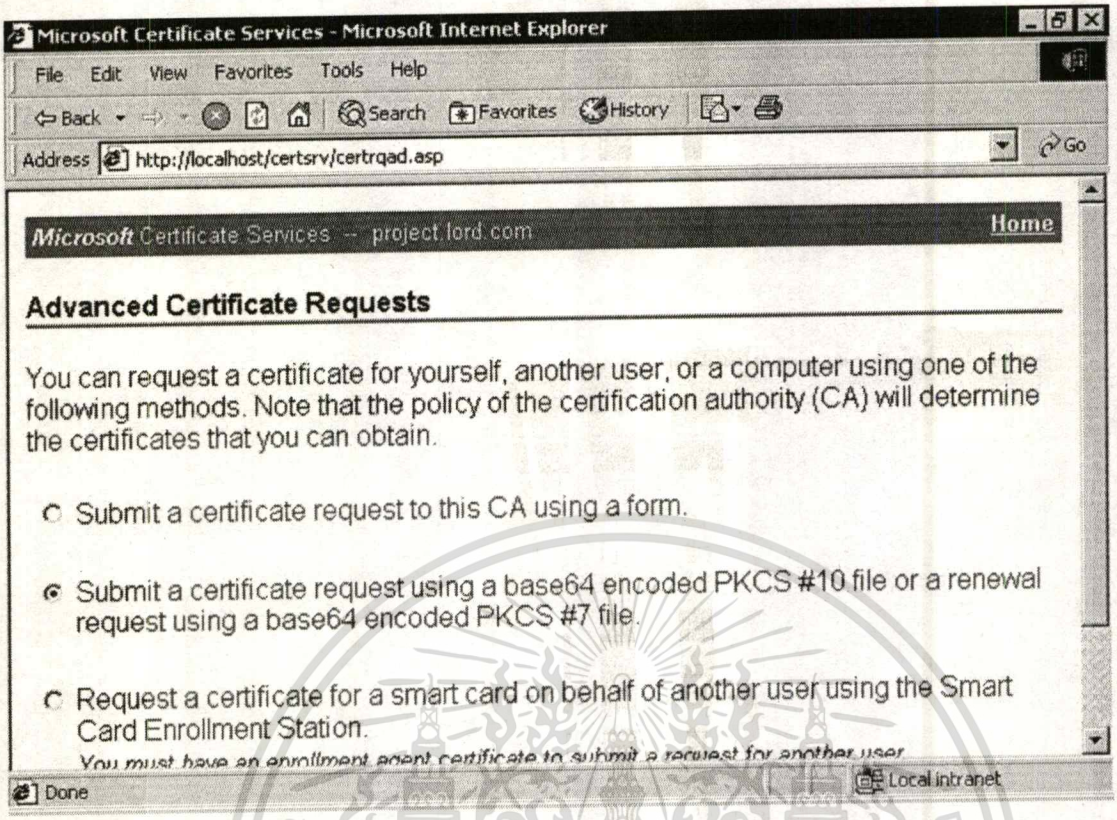
1. Open Web Site for Certificate Request and Select Request a Certificate



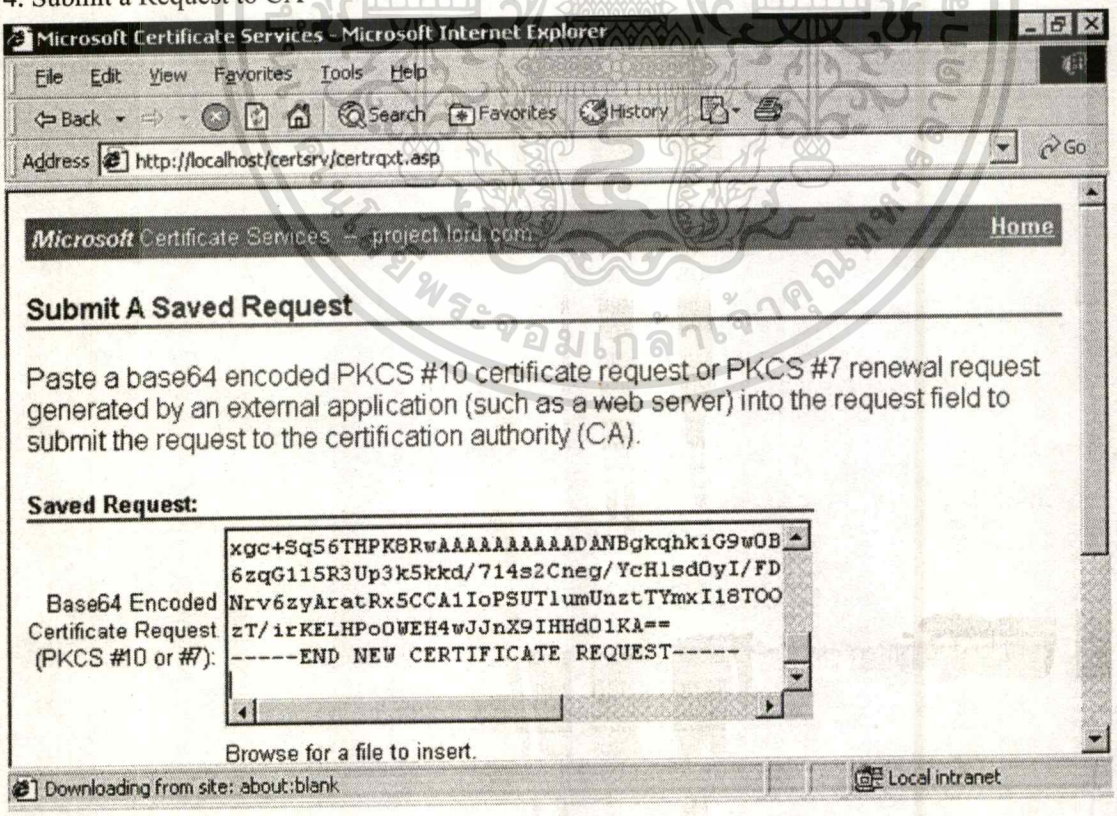
2. Choose Request Type



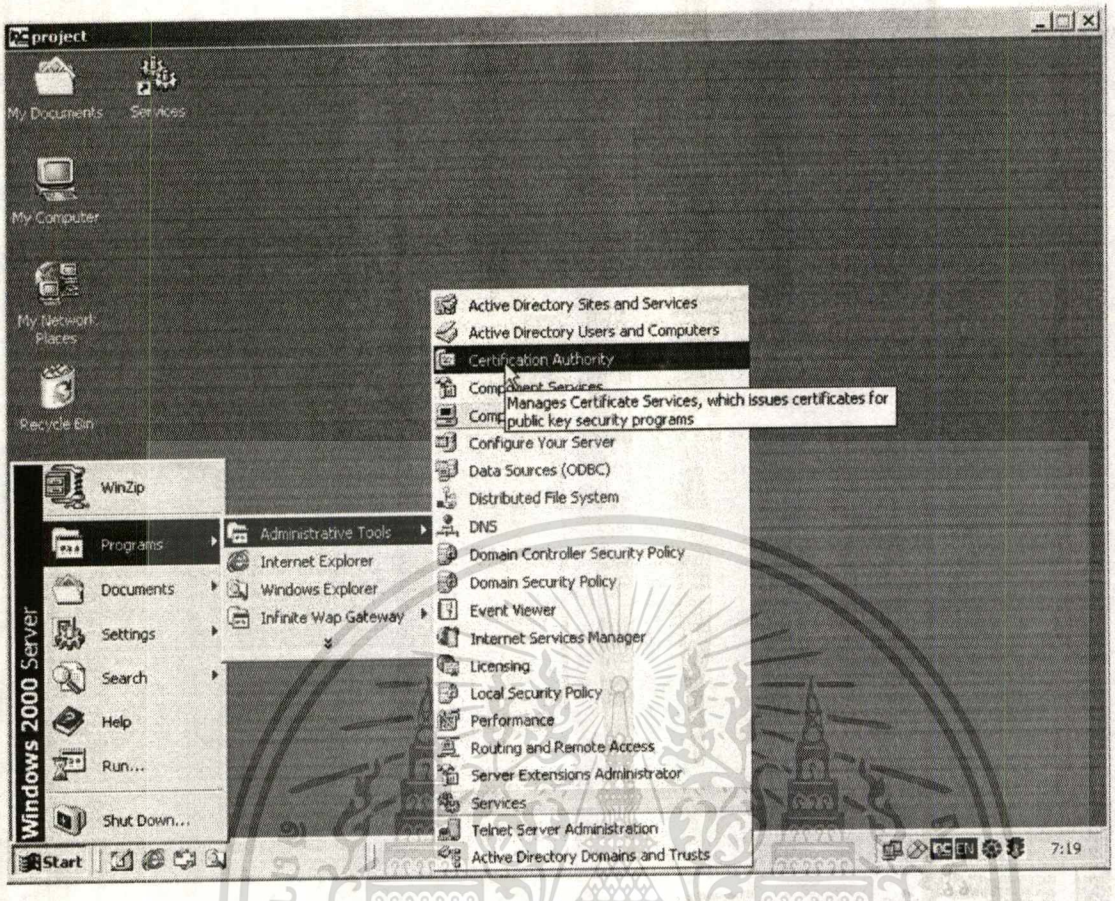
3. Select Advanced Certificate Request



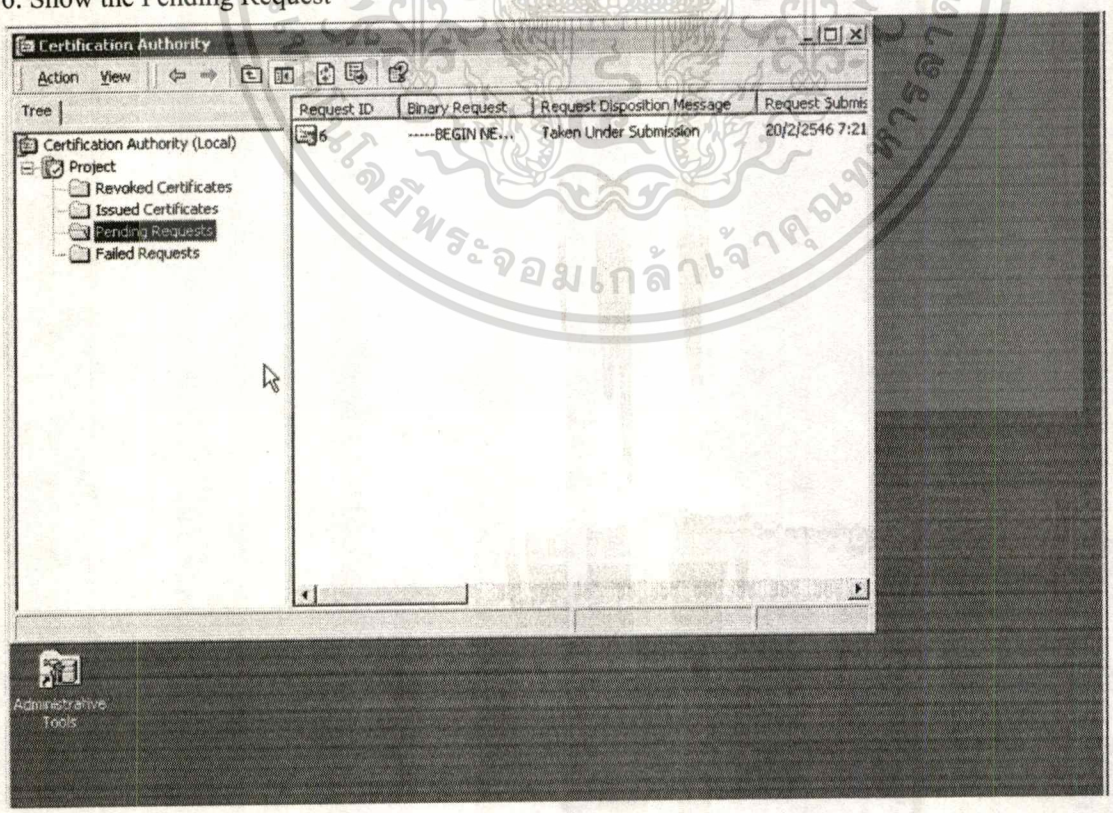
4. Submit a Request to CA



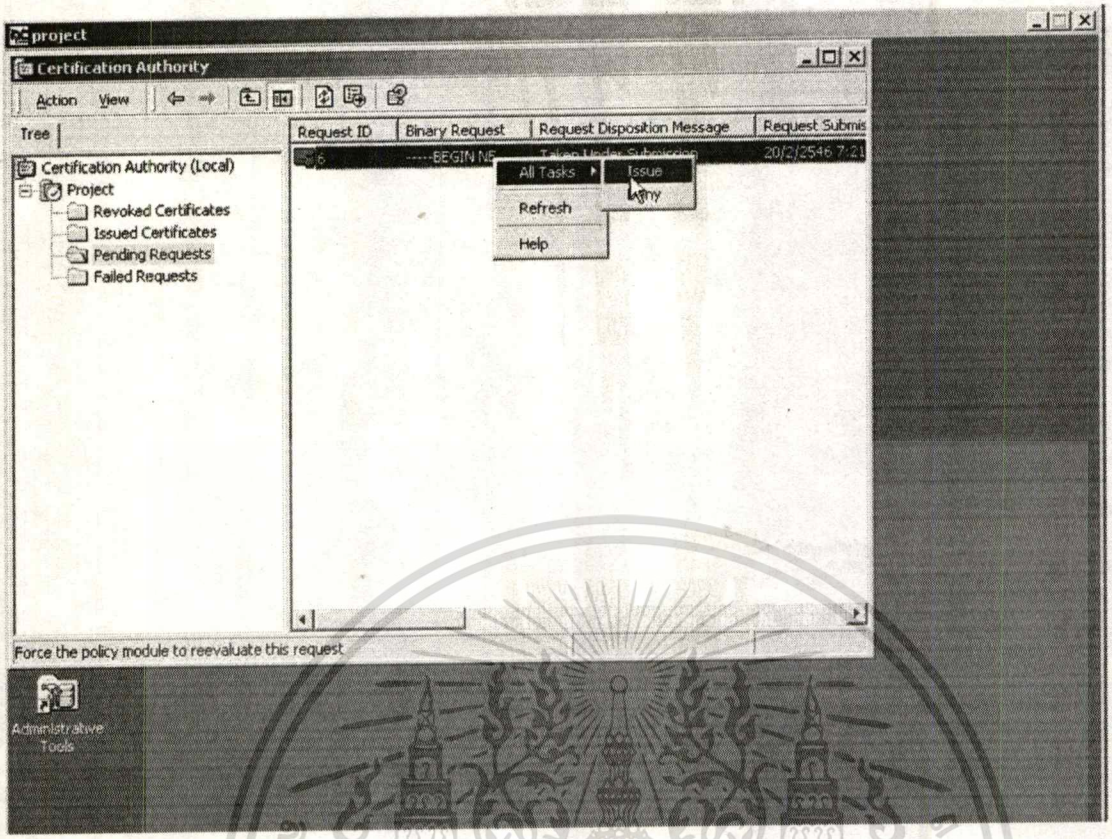
5. Open Certification Authority



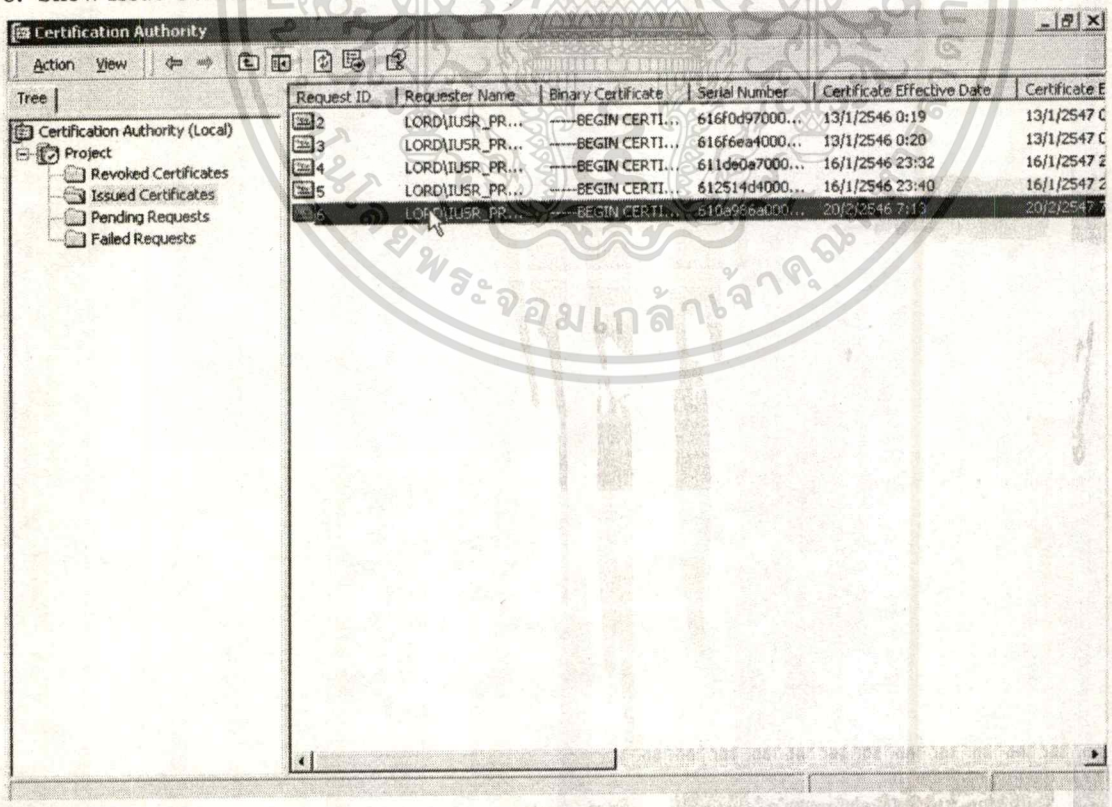
6. Show the Pending Request



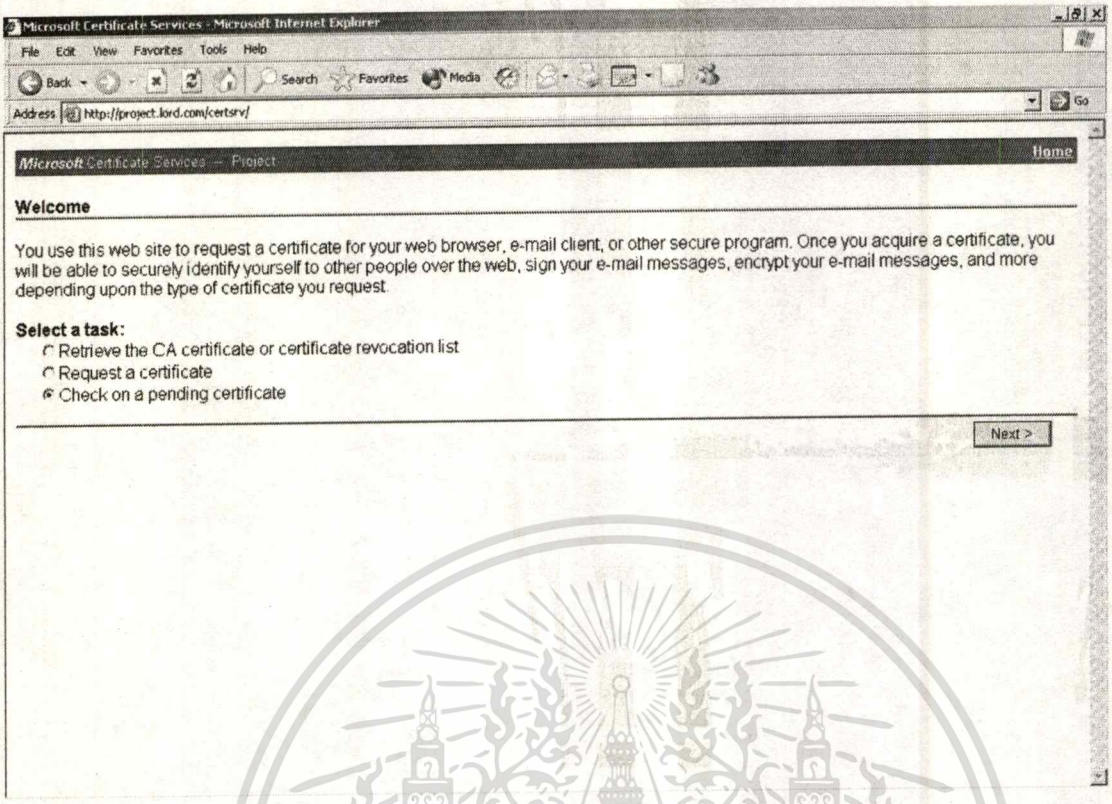
7. Issue the Certificate for Pending Request



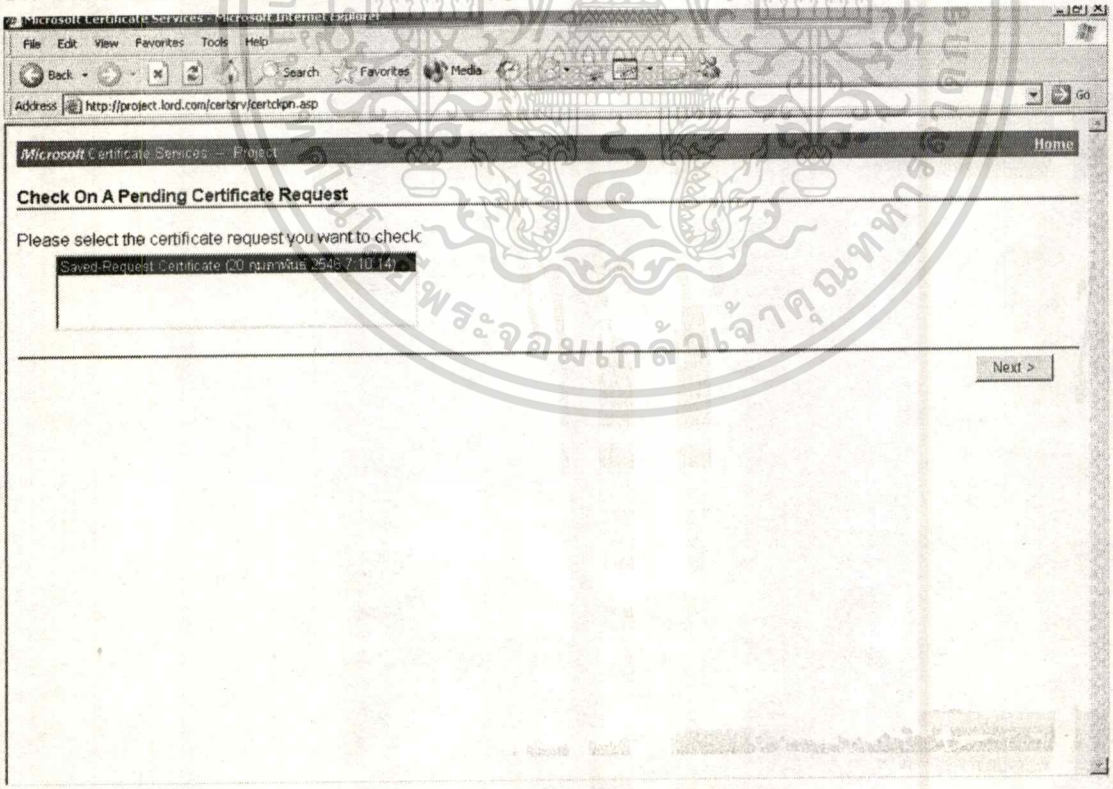
8. Show Issue Certificate



9. Check the Pending Request



10. Select the Certificate that was Issued by CA



11. Download Certificate that was issued by CA